BECKHOFF New Automation Technology

Dokumentation | DE

Applikationshandbuch TwinSAFE

Beispiele für die Berechnung von sicherheitstechnischen Kenngrößen für Sicherheitsfunktionen

12.11.2024 | Version: 3.5.0

Inhaltsverzeichnis

1 Dokumentationshinweise

1.1 Disclaimer

Beckhoff Produkte werden fortlaufend weiterentwickelt. Wir behalten uns vor, die Betriebsanleitung jederzeit und ohne Ankündigung zu überarbeiten. Aus den Angaben, Abbildungen und Beschreibungen in dieser Betriebsanleitung können keine Ansprüche auf Änderung bereits gelieferter Produkte geltend gemacht werden.

Wir definieren in dieser Betriebsanleitung alle zulässigen Anwendungsfälle, deren Eigenschaften und Betriebsbedingungen wir zusichern können. Die von uns definierten Anwendungsfälle sind vollumfänglich geprüft und zertifiziert. Darüberhinausgehende Anwendungsfälle, die nicht in dieser Betriebsanleitung beschrieben werden, bedürfen eine Prüfung der Firma Beckhoff Automation GmbH & Co. KG.

1.1.1 Marken

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® und XPlanar® sind eingetragene und lizenzierte Marken der Beckhoff Automation GmbH.

Die Verwendung anderer Marken oder Kennzeichen durch Dritte kann zu einer Verletzung von Rechten der Inhaber der entsprechenden Bezeichnungen führen.

1.1.2 Patente

Die EtherCAT-Technologie ist patentrechtlich durch folgende Anmeldungen und Patente mit den entsprechenden Anmeldungen und Eintragungen in verschiedenen anderen Ländern geschützt:

- EP1590927
- EP1789857
- EP1456722
- EP2137893
- DE102015105702

EtherCAT® ist eine eingetragene Marke und patentierte Technologie, lizenziert durch die Beckhoff Automation GmbH.

Safety over EtherCAT® ist eine eingetragene Marke und patentierte Technologie, lizenziert durch die Beckhoff Automation GmbH.

1.1.3 Haftungsbeschränkungen

Die gesamten Komponenten des beschriebenen Produkts werden je nach Anwendungsbestimmungen in bestimmter Konfiguration von Hardware und Software ausgeliefert. Umbauten und Änderungen der Konfiguration von Hardware oder Software, die über die dokumentierten Möglichkeiten hinausgehen, sind verboten und führen zum Haftungsausschluss der Beckhoff Automation GmbH & Co. KG.

Folgendes wird aus der Haftung ausgeschlossen:

- Nichtbeachtung dieser Betriebsanleitung
- Nicht-bestimmungsgemäße Verwendung
- Einsatz nicht ausgebildeten Fachpersonals
- Erlöschen der Zertifizierungen
- Verwendung nicht zugelassener Ersatzteile

1.1.4 Copyright

1.2 Ausgabestände der Dokumentation

Version	Kommentar
3.5.0	• In Kapitel „Überwachung Drehzahl (Kategorie 3, PL d)“ und „Überwachung Drehzahl (über IO-Link) (Kategorie 3, PL d)“ weitere TwinSAFE SC-Klemme hinzugefügt
3.4.0	• Tabellen für alternative TwinSAFE SC-Produkte hinzugefügt
3.3.0	• Applikationsbeispiel „AdvPosMon mit integriertem Geber EnDat 3“ hinzugefügt • Rechtschreibfehler korrigiert
3.2.0	• In Kapitel *Erklärung der Begriffe* bei T_1 die Erklärung erweitert • Kapitel *Applikationsbeispiel C9900-M800* hinzugefügt • Konformitätsbestätigung aktualisiert
3.1.0	• Dokumentstruktur korrigiert: Kapitel *Projektierung eines Safety-Projektes mit TwinSAFE-Komponenten* jetzt wieder enthalten
3.0.0	• Beispiele für PROFIsafe hinzugefügt • Dokumentstruktur überarbeitet • Konformitätsbestätigung aktualisiert
2.2.0	• Beispiel EPP9022-9060 aktualisiert
2.1.0	• Migration • Beispiele AX8xxx, EL2911, EP1957 und EPP9022-9060 hinzugefügt • Hinweistext zu Schulungen hinzugefügt • Konformitätsbestätigung aktualisiert
2.0.0	• Beispiele EK1960 hinzugefügt • Berechnung in Kapitel 2.26 korrigiert
1.9.1	• Hinweis in Kapitel 2.17 und 2.18 hinzugefügt
1.9.0	• Kapitel 2.18 überarbeitet • Kapitel *Projektierung eines Safety Projektes* hinzugefügt
1.8.0	• TwinSAFE SC Beispiele hinzugefügt • Beispiel zu Bosch Rexroth IndraDrive Antriebsfamilie • Bezeichnung *SIL2 Kommunikation* durch *TwinSAFE SC* ersetzt • Beispiele 2.25 und 2.26 aktualisiert • Generelle Überarbeitung aller Kapitel
1.7.0	• Kapitel *Direktes Verdrahten der TwinSAFE Ausgänge auf TwinSAFE Eingänge (1-kanalig)* überarbeitet • Vorwort aktualisiert • Kapitel *Zweck und Anwendungsbereich* erweitert • Strukturbild Kapitel 2.25 und 2.26 aktualisiert • Kapitel 2.27 hinzugefügt • Kapitel 2.2.3.2, 2.3.3.2, 2.4.3.2, 2.5.3.2, 2.7.3.2 und 2.19.3.2. konkretisiert (Hinweise zu direktem / indirektem Zurücklesen entfernt) • Hinweistexte in Kapitel 2.19 hinzugefügt
1.6.2	• Konformitätsbestätigung aktualisiert • Grafiken in Kapitel 2.25 und 2.26 aktualisiert • Kapitel *Zweck und Anwendungsbereich* hinzugefügt
1.6.1	• Kapitel 2.25 und 2.26 hinzugefügt
1.6.0	• Kapitel 2.17 und 2.18 überarbeitet
1.5.0	• Kapitel 2.24 hinzugefügt • Ausgabestände der Dokumentation hinzugefügt • Dokumentenursprung hinzugefügt • Formatierung geändert

Version	Kommentar
1.4.0	• Überschriften mit Kategorien und Performance Level erweitert • Hinweistext Kapitel 2.6 verschoben
1.3.0	• Lieferbedingungen entfernt
1.2.0	• Korrektur an Kapitel 2.6
1.1.0	• erste freigegebene Version

1.3 Personalqualifikation

Diese Betriebsanleitung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungstechnik und Automatisierung mit den dazugehörigen Kenntnissen.

Das ausgebildete Fachpersonal muss sicherstellen, dass die Anwendungen und der Einsatz des beschriebenen Produkts alle Sicherheitsanforderungen erfüllen. Dazu zählen sämtliche anwendbare und gültige Gesetze, Vorschriften, Bestimmungen und Normen.

Ausgebildetes Fachpersonal

Ausgebildetes Fachpersonal verfügt über umfangreiche fachliche Kenntnisse aus Studium, Lehre oder Fachausbildung. Verständnis für Steuerungstechnik und Automatisierung ist vorhanden. Ausgebildetes Fachpersonal kann:

- Eigenständig Gefahrenquellen erkennen, vermeiden und beseitigen
- Relevante Normen und Richtlinien anwenden
- Vorgaben aus den Unfallverhütungsvorschriften umsetzen
- Das Arbeitsumfeld beurteilen, vorbereiten und einrichten
- Arbeiten selbständig beurteilen, optimieren und ausführen

1.4 Sicherheit und Einweisung

Lesen Sie die Inhalte, welche sich auf die von Ihnen durchzuführenden Tätigkeiten mit dem Produkt beziehen. Lesen Sie immer das Kapitel Zu Ihrer Sicherheit in der Betriebsanleitung.

Beachten Sie die Warnhinweise in den Kapiteln, sodass Sie bestimmungsgemäß und sicher mit dem Produkt umgehen und arbeiten.

Symbolerklärung

Für eine übersichtliche Gestaltung werden verschiedene Symbole verwendet:

1. Die Nummerierung zeigt eine Handlungsanweisung, die Sie ausführen sollen.
- Der Punkt zeigt eine Aufzählung.

[…] Die eckigen Klammern zeigen Querverweise auf andere Textstellen in dem Dokument.

[1] Die Zahl in eckigen Klammern zeigt die Nummerierung eines referenzierten Dokuments.

Im Folgenden werden die Signalwörter eingeordnet, die in der Dokumentation verwendet werden.

Signalwörter

Warnung vor Personenschäden

⚠ GEFAHR

Es besteht eine Gefährdung mit hohem Risikograd, die den Tod oder eine schwere Verletzung zur Folge hat.

⚠ WARNUNG

Es besteht eine Gefährdung mit mittlerem Risikograd, die den Tod oder eine schwere Verletzung zur Folge haben kann.

⚠ VORSICHT

Es besteht eine Gefährdung mit geringem Risikograd, die eine mittelschwere oder leichte Verletzung zur Folge haben kann.

Warnung vor Umwelt- oder Sachschäden

HINWEIS

Hinweise

Es besteht eine mögliche Schädigung für Umwelt, Geräte oder Daten.

Information zum Umgang mit dem Produkt

Diese Information beinhaltet z. B.:
Handlungsempfehlungen, Hilfestellungen oder weiterführende Informationen zum Produkt.

1.5 Support und Service

Beckhoff und seine weltweiten Partnerfirmen bieten einen umfassenden Support und Service, der eine schnelle und kompetente Unterstützung bei allen Fragen zu Beckhoff Produkten und Systemlösungen zur Verfügung stellt.

Downloadfinder

Unser Downloadfinder beinhaltet alle Dateien, die wir Ihnen zum Herunterladen anbieten. Sie finden dort Applikationsberichte, technische Dokumentationen, technische Zeichnungen, Konfigurationsdateien und vieles mehr.

Die Downloads sind in verschiedenen Formaten erhältlich.

Beckhoff Niederlassungen und Vertretungen

Wenden Sie sich bitte an Ihre Beckhoff Niederlassung oder Ihre Vertretung für den lokalen Support und Service zu Beckhoff Produkten!

Die Adressen der weltweiten Beckhoff Niederlassungen und Vertretungen entnehmen Sie bitte unserer Internetseite: www.beckhoff.com

Dort finden Sie auch weitere Dokumentationen zu Beckhoff Komponenten.

Beckhoff Support

Der Support bietet Ihnen einen umfangreichen technischen Support, der Sie nicht nur bei dem Einsatz einzelner Beckhoff Produkte, sondern auch bei weiteren umfassenden Dienstleistungen unterstützt:

- Support
- Planung, Programmierung und Inbetriebnahme komplexer Automatisierungssysteme
- umfangreiches Schulungsprogramm für Beckhoff Systemkomponenten

Hotline:	+49 5246 963-157
E-Mail:	support@beckhoff.com

Beckhoff Service

Das Beckhoff Service-Center unterstützt Sie rund um den After-Sales-Service:

- Vor-Ort-Service
- Reparaturservice
- Ersatzteilservice
- Hotline-Service

Hotline:	+49 5246 963-460
E-Mail:	service@beckhoff.com

Beckhoff Unternehmenszentrale

Beckhoff Automation GmbH & Co. KG

Hülshorstweg 20
33415 Verl
Deutschland

Telefon:	+49 5246 963-0
E-Mail:	info@beckhoff.com
Internet:	www.beckhoff.com

1.6 Hinweise zur Informationssicherheit

Die Produkte der Beckhoff Automation GmbH & Co. KG (Beckhoff) sind, sofern sie online zu erreichen sind, mit Security-Funktionen ausgestattet, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Trotz der Security-Funktionen sind die Erstellung, Implementierung und ständige Aktualisierung eines ganzheitlichen Security-Konzepts für den Betrieb notwendig, um die jeweilige Anlage, das System, die Maschine und die Netzwerke gegen Cyber-Bedrohungen zu schützen. Die von Beckhoff verkauften Produkte bilden dabei nur einen Teil des gesamtheitlichen Security-Konzepts. Der Kunde ist dafür verantwortlich, dass unbefugte Zugriffe durch Dritte auf seine Anlagen, Systeme, Maschinen und Netzwerke verhindert werden. Letztere sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn entsprechende Schutzmaßnahmen eingerichtet wurden.

Zusätzlich sollten die Empfehlungen von Beckhoff zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Informationssicherheit und Industrial Security finden Sie in unserem https://www.beckhoff.de/secguide.

Die Produkte und Lösungen von Beckhoff werden ständig weiterentwickelt. Dies betrifft auch die Security-Funktionen. Aufgrund der stetigen Weiterentwicklung empfiehlt Beckhoff ausdrücklich, die Produkte ständig auf dem aktuellen Stand zu halten und nach Bereitstellung von Updates diese auf die Produkte aufzuspielen. Die Verwendung veralteter oder nicht mehr unterstützter Produktversionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Hinweise zur Informationssicherheit zu Produkten von Beckhoff informiert zu sein, abonnieren Sie den RSS Feed unter https://www.beckhoff.de/secinfo.

2 Sicherheitshinweise

2.1 Auslieferungszustand

Die gesamten Komponenten werden je nach Anwendungsbestimmungen in bestimmten Hard- und Software-Konfigurationen ausgeliefert. Änderungen der Hard-, oder Software-Konfiguration, die über die dokumentierten Möglichkeiten hinausgehen sind unzulässig und bewirken den Haftungsausschluss der Beckhoff Automation GmbH & Co. KG.

2.2 Sorgfaltspflicht des Betreibers

Der Betreiber muss sicherstellen, dass

- die TwinSAFE-Produkte nur bestimmungsgemäß verwendet werden (siehe Kapitel Produktbeschreibung).
- die TwinSAFE-Produkte nur in einwandfreiem, funktionstüchtigem Zustand betrieben werden.
- nur ausreichend qualifiziertes und autorisiertes Personal die TwinSAFE-Produkte betreibt.
- dieses Personal regelmäßig in allen zutreffenden Fragen von Arbeitssicherheit und Umweltschutz unterwiesen wird, sowie die Betriebsanleitung und insbesondere die darin enthaltenen Sicherheitshinweise kennt.
- die Betriebsanleitung stets in einem leserlichen Zustand und vollständig am Einsatzort der TwinSAFE-Produkte zur Verfügung steht.
- alle an den TwinSAFE-Produkten angebrachten Sicherheits- und Warnhinweise nicht entfernt werden und leserlich bleiben.

2.3 Zweck und Anwendungsbereich

Das Applikationshandbuch gibt dem Anwender Beispiele für die Berechnung von sicherheitstechnischen Kenngrößen für Sicherheitsfunktionen entsprechend der Normen DIN EN ISO 13849-1 und EN 62061 bzw. EN 61508:2010 (soweit anwendbar), wie sie typischerweise an Maschinen Verwendung finden.

In den Beispielen wird für einen sicheren Eingang exemplarisch eine EL1904 bzw. für einen sicheren Ausgang eine EL2904 dargestellt. Dies ist nur als Beispiel zu sehen, es können natürlich auch andere sichere Eingänge oder Ausgänge verwendet werden, wie z.B. eine EP1908 oder eine EL2912. Dafür müssen dann in der Berechnung die passenden Kenngrößen, die der jeweiligen Produktdokumentation entnommen werden können, verwendet werden.

HINWEIS

Applikationsbeispiele

Diese Beispiele geben dem Anwender exemplarische Berechnungen vor. Sie entbinden Ihn nicht von der Pflicht eine Risiko- und Gefährdungsanalyse durchzuführen und die für die Anwendung zu berücksichtigenden Richtlinien, Normen und Gesetze anzuwenden.

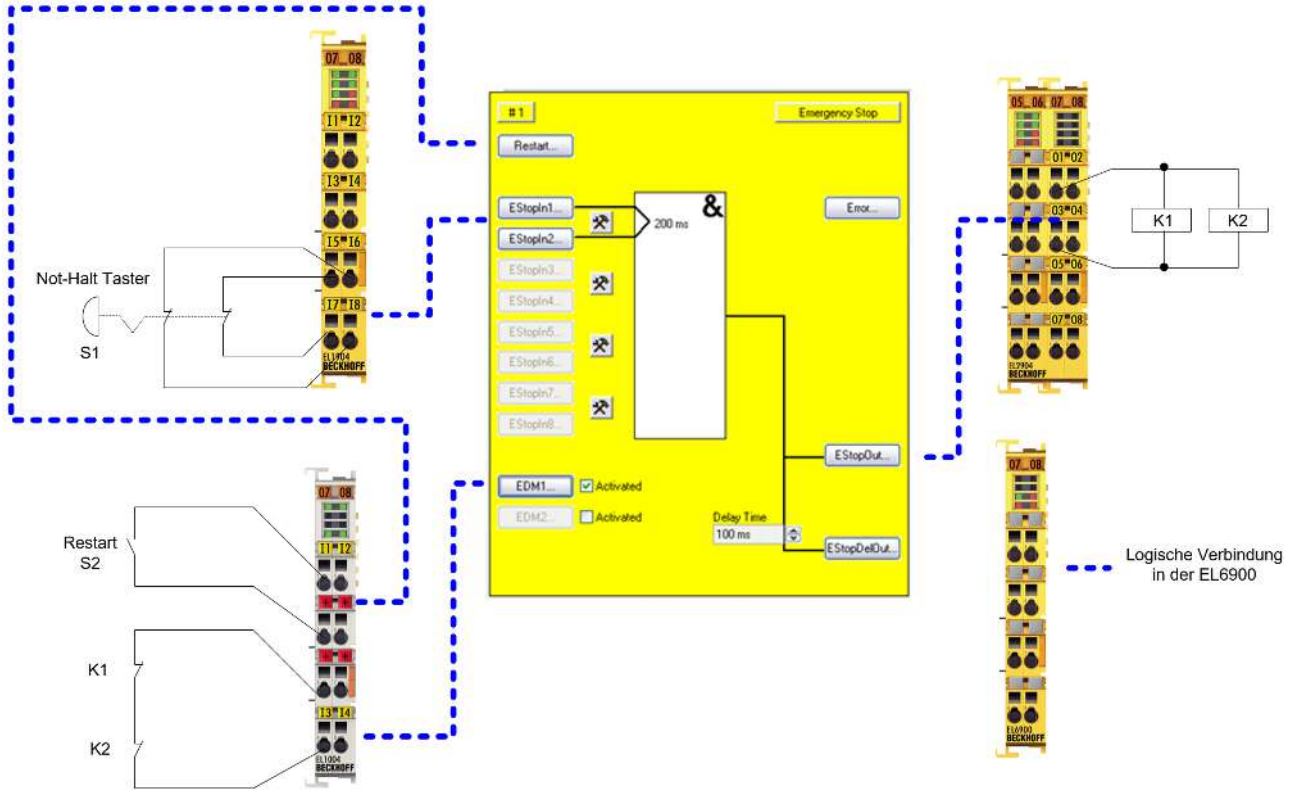
2.4 Erklärung der Begriffe

Bezeichnung	Erklärung
$B10_D$	Mittlere Anzahl der Zyklen nach der 10% der Bauteile gefährlich ausgefallen sind
CCF	Ausfälle gemeinsamer Ursache
d_{op}	Mittlere Betriebszeit in Tagen pro Jahr
DC_{avg}	Mittlerer Diagnosedeckungsgrad
h_{op}	Mittlere Betriebszeit in Stunden pro Tag
$MTTF_D$	Mittlere Zeit bis zum gefährlichen Ausfall
n_{op}	Mittlere Anzahl jährlicher Betätigungen
PFH_D	Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde
PL	Performance Level
PL_r	Erforderlicher Performance Level
T_{Zyklus}	Mittlere Zeit zwischen zwei aufeinanderfolgende Zyklen des Systems (in den folgenden Beispielen in Minuten angegeben, kann aber auch in Sekunden angegeben werden)
T_1	Der kleinere Wert von Proof-Test-Intervall oder Gebrauchsdauer (bei TwinSAFE Geräten typischerweise 20 Jahre)
λ_D	Gefahrbringende Ausfallrate angegeben in FIT (Ausfallzahl in 10^9 Bauelement-Stunden)
T_{10D}	Gebrauchsdauer - maximale Betriebszeit für z.B. elektromechanische Bauteile
TwinSAFE SC	Die TwinSAFE SC Technologie (SC - Single Channel) ermöglicht es ein Signal einer Standard-Klemme in ein FSoE Telegramm zu verpacken und dieses über den Standard Feldbus an die TwinSAFE Logik zu übermitteln. Dadurch können Verfälschungen auf dem Übertragungsweg ausgeschlossen werden. Innerhalb der TwinSAFE Logik wird dieses Signal mit einem weiteren unabhängigen Signal plausibilisiert. Mit diesem Vergleichsergebnis erhält man typischerweise einen Analogwert, der einer Kategorie 3 und PL d entspricht. **Diese Technologie unterstützt keine digitalen Eingangssignale und kann auch nicht in einer einkanaligen Struktur (nur ein TwinSAFE SC Kanal) verwendet werden.**

3 ESTOP-Funktionen

3.1 ESTOP Funktion Variante 1 (Kategorie 3, PL d)

Der Not-Halt-Taster ist mit zwei Öffnerkontakten auf eine sichere Eingangsklemme EL1904 verbunden. Die Testung und die Überwachung der Diskrepanz der beiden Signale sind eingeschaltet. Der Restart und das Rückführsignal sind auf Standard-Klemmen verdrahtet und werden über die Standard-SPS an TwinSAFE übergeben. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



3.1.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904

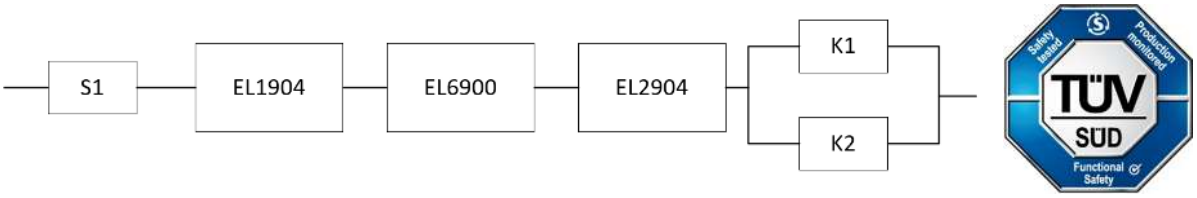
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

3.1.2 Blockbildung und Safety-Loops

3.1.2.1 Sicherheitsfunktion 1



3.1.3 Berechnung

3.1.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	100.000
S2 – $B10_D$	10.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche) (7 Tage, 24 Stunden)
Lebenszeit (T1)	20Jahre = 175200 Stunden

3.1.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung/Plausibilität	DC_{avg}=99%
K1/K2 mit Testung und EDM (Betätigung 1/Woche)	DC_{avg}=60%
K1/K2 mit Testung und EDM (Betätigung 1/Schicht)	DC_{avg}=90%

3.1.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_d$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1

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

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

K1/K2

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

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

und der Annahme, dass S1, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1

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

K1/K2 Betätigung 1/Woche

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

K1/K2 Betätigung 1/Schicht

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die B10d-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

bei Betätigung 1/Woche

oder

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

bei Betätigung 1/Schicht

Die Berechnung des $MTTF_D$-Wertes für Block 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

bzw.:

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

⚠ VORSICHT

Maßnahmen zum Erreichen der Kategorie 3!

Diese Struktur ist bis maximal Kategorie 3 möglich, da ein Fehler im Rücklesepfad der Relais unentdeckt sein kann. Um die Kategorie 3 zu erreichen, müssen in der Standard-Steuerung zur Erwartungshaltung des Rücklesens alle steigenden und fallenden Flanken zusammen mit der Zeitabhängigkeit ausgewertet werden!

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**
DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

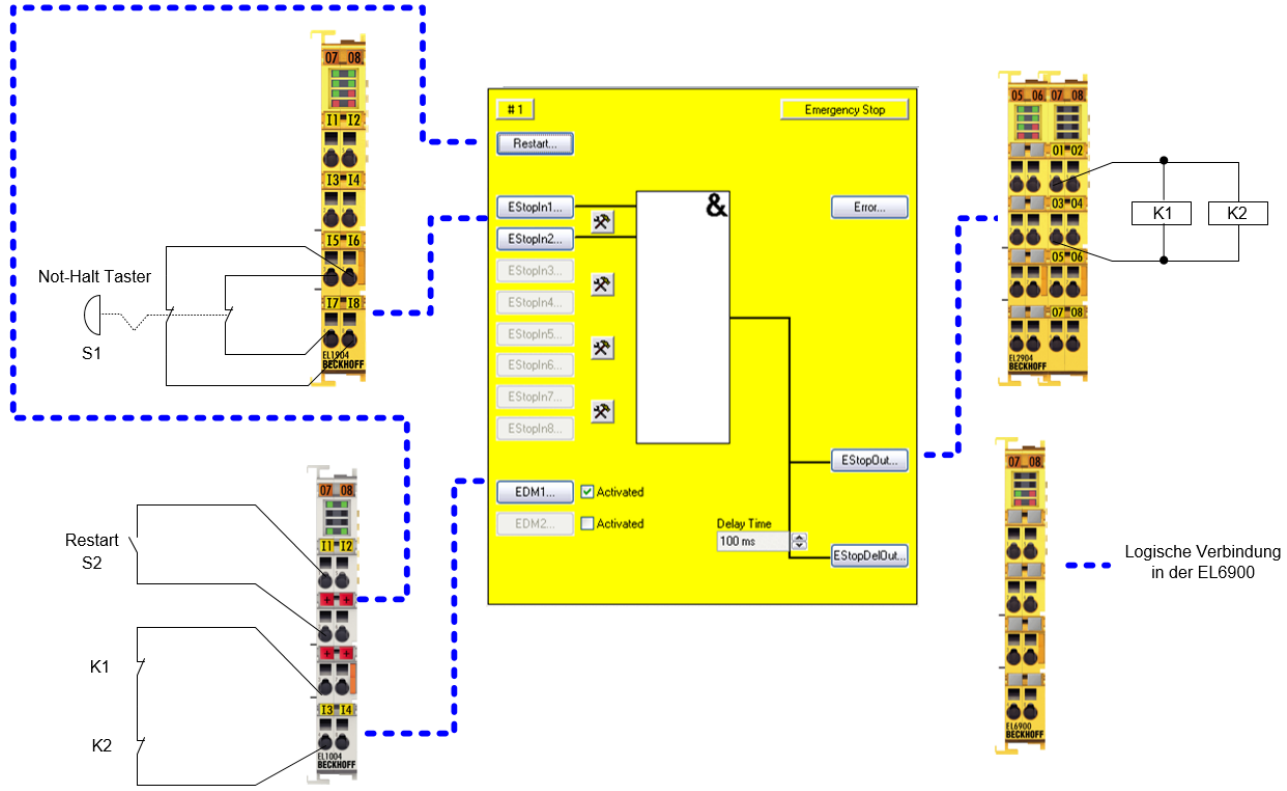
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

3.2 ESTOP Funktion Variante 2 (Kategorie 3, PL d)

Der Not-Halt-Taster ist mit zwei Öffnerkontakten auf eine sichere Eingangsklemme EL1904 verbunden. Die Testung der beiden Signale ist eingeschaltet. Eine Überprüfung auf Diskrepanz der Signale wird **nicht** durchgeführt. Der Restart und das Rückführsignal sind auf Standard-Klemmen verdrahtet und werden über die Standard-SPS an TwinSAFE übergeben. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



3.2.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904

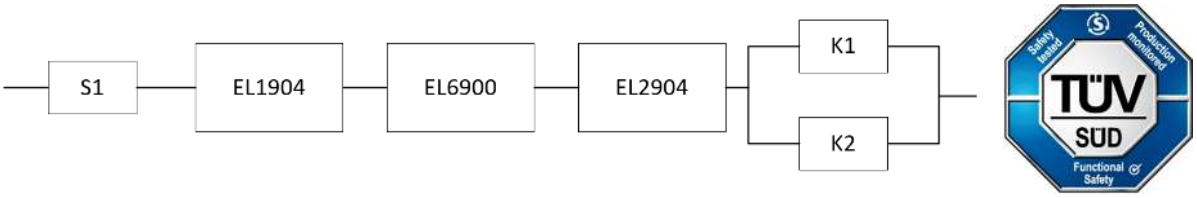
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

3.2.2 Blockbildung und Safety-Loops

3.2.2.1 Sicherheitsfunktion 1



3.2.3 Berechnung

3.2.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	100.000
S2 – $B10_D$	10.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

3.2.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung/ ohne Plausibilität	DC_{avg}=90%
K1/K2 mit Testung und EDM (Betätigung 1/Woche)	DC_{avg}=60%
K1/K2 mit Testung und EDM (Betätigung 1/Schicht)	DC_{avg}=90%

3.2.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

K1/K2:

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

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

und der Annahme, dass S1, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

K1/K2: Betätigung 1/Woche

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

K1/K2: Betätigung 1/Schicht

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β-Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

bei Betätigung 1/Woche

oder

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

bei Betätigung 1/Schicht

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

bzw.:

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

⚠ VORSICHT

Maßnahmen zum Erreichen der Kategorie 3!

Diese Struktur ist durch einen möglichen schlafenden Fehler nur bis maximal Kategorie 3 möglich. Um die Kategorie 3 zu erreichen, müssen in der Standard-Steuerung zur Erwartungshaltung des Rücklesens alle steigenden und fallenden Flanken zusammen mit der Zeitabhängigkeit ausgewertet werden!

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**
DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

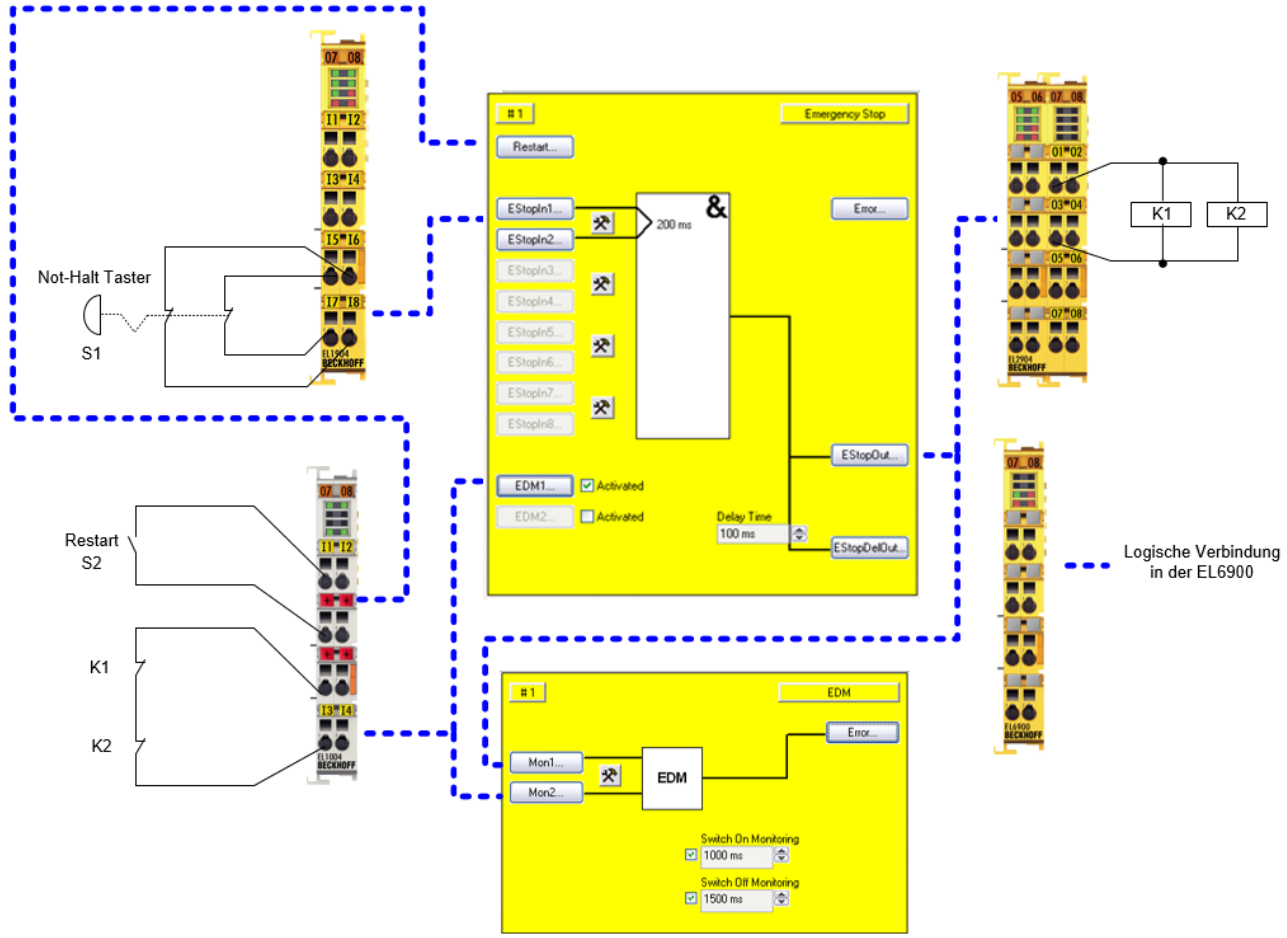
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

3.3 ESTOP-Funktion Variante 3 (Kategorie 4, PL e)

Der Not-Halt-Taster ist mit zwei Öffnerkontakten auf eine sichere Eingangsklemme EL1904 verbunden. Die Testung der beiden Signale ist eingeschaltet. Diese Signale werden auf Diskrepanz überprüft. Der Restart und das Rückführsignal sind auf Standard-Klemmen verdrahtet und werden über die Standard-SPS an TwinSAFE übergeben. Weiterhin werden der Ausgang des Funktionsbausteins ESTOP und das Rückführsignal auf einen EDM-Baustein verdrahtet. Dieser prüft, dass das Rückführsignal innerhalb der eingestellten Zeiten den gegengesetzten Zustand des ESTOP-Ausgangs einnimmt.
An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



3.3.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904

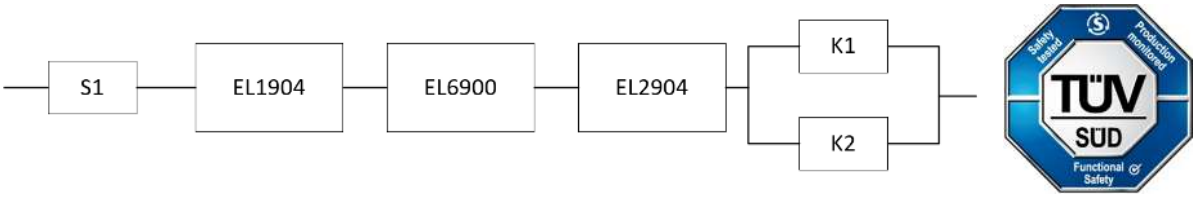
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

3.3.2 Blockbildung und Safety-Loops

3.3.2.1 Sicherheitsfunktion 1



3.3.3 Berechnung

3.3.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	100.000
S2 – $B10_D$	10.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

3.3.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung/Plausibilität	DC_{avg}=99%
K1/K2 mit Testung und EDM (Betätigung 1/Woche)	DC_{avg}=90%
K1/K2 mit Testung und EDM (Betätigung 1/Schicht)	DC_{avg}=99%

3.3.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

K1/K2:

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

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

und der Annahme, dass S1, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

K1/K2: Betätigung 1/Woche

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

K1/K2: Betätigung 1/Schicht

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die B10d-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

bei Betätigung 1/Woche

oder

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

bei Betätigung 1/Schicht

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

bzw.:

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

⚠ VORSICHT

Maßnahmen zum Erreichen der Kategorie 4!

Diese Struktur ist bis maximal Kategorie 4 möglich. Um die Kategorie 4 zu erreichen, müssen in der Steuerung zur Erwartungshaltung des Rücklesens alle steigenden und fallenden Flanken zusammen mit der Zeitabhängigkeit ausgewertet werden!

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**
DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

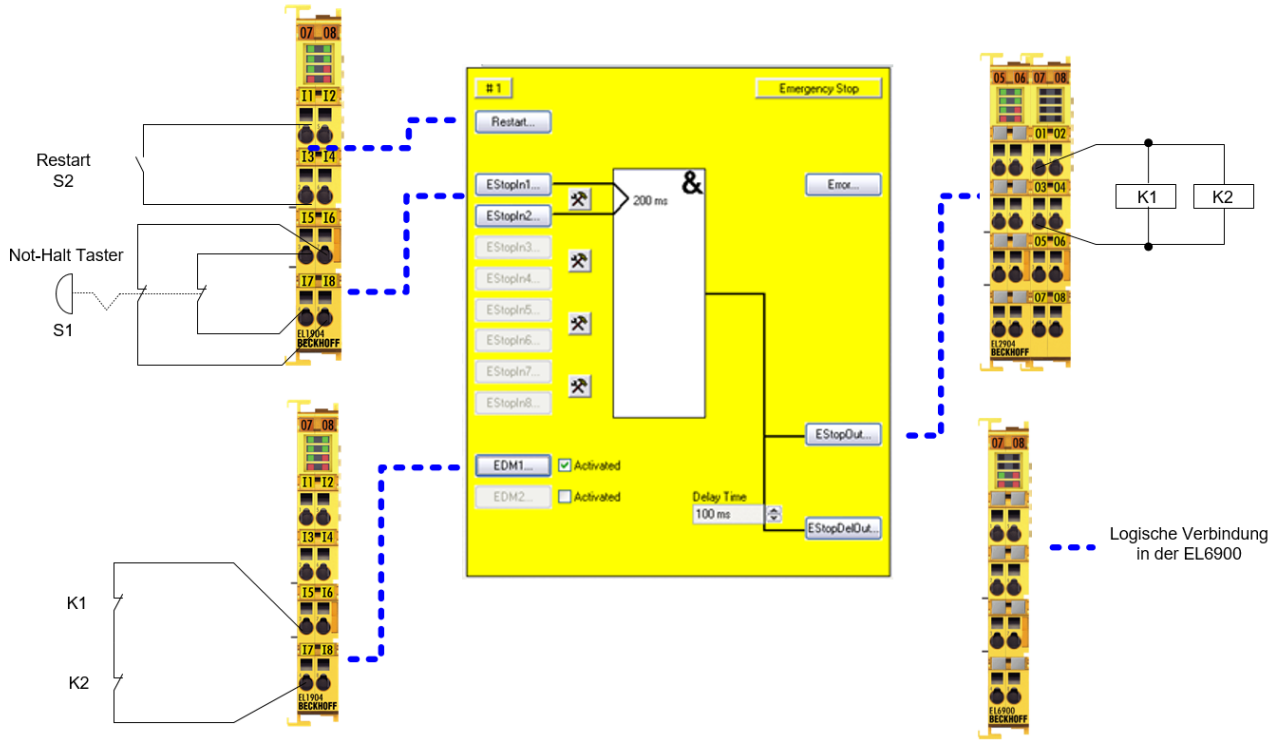
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

3.4 ESTOP Funktion Variante 4 (Kategorie 4, PL e)

Der Not-Halt-Taster mit zwei Öffnerkontakten, der Restart und der Rückführkreis sind auf sichere Kanäle einer Eingangsklemme EL1904 verbunden. Die Testung der Signale ist eingeschaltet. Eine Überprüfung auf Diskrepanz der beiden Not-Halt-Signale wird durchgeführt. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



3.4.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

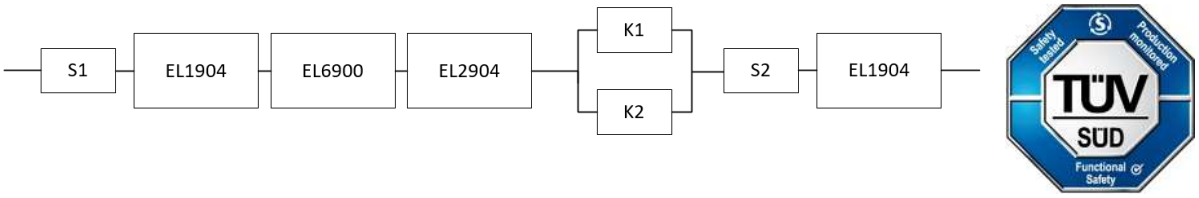
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

3.4.2 Blockbildung und Safety-Loops

3.4.2.1 Sicherheitsfunktion 1



3.4.3 Berechnung

3.4.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	100.000
S2 – $B10_D$	10.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

3.4.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung/Plausibilität	DC_{avg}=99%
S2 mit Plausibilität	DC_{avg}=90%
K1/K2 mit Testung und EDM (Betätigung 1/Schicht)	DC_{avg}=99%

3.4.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

K1/K2:

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

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

und der Annahme, dass S1, S2, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

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: Betätigung 1/Schicht

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

bei Betätigung 1/Schicht

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

bzw.:

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

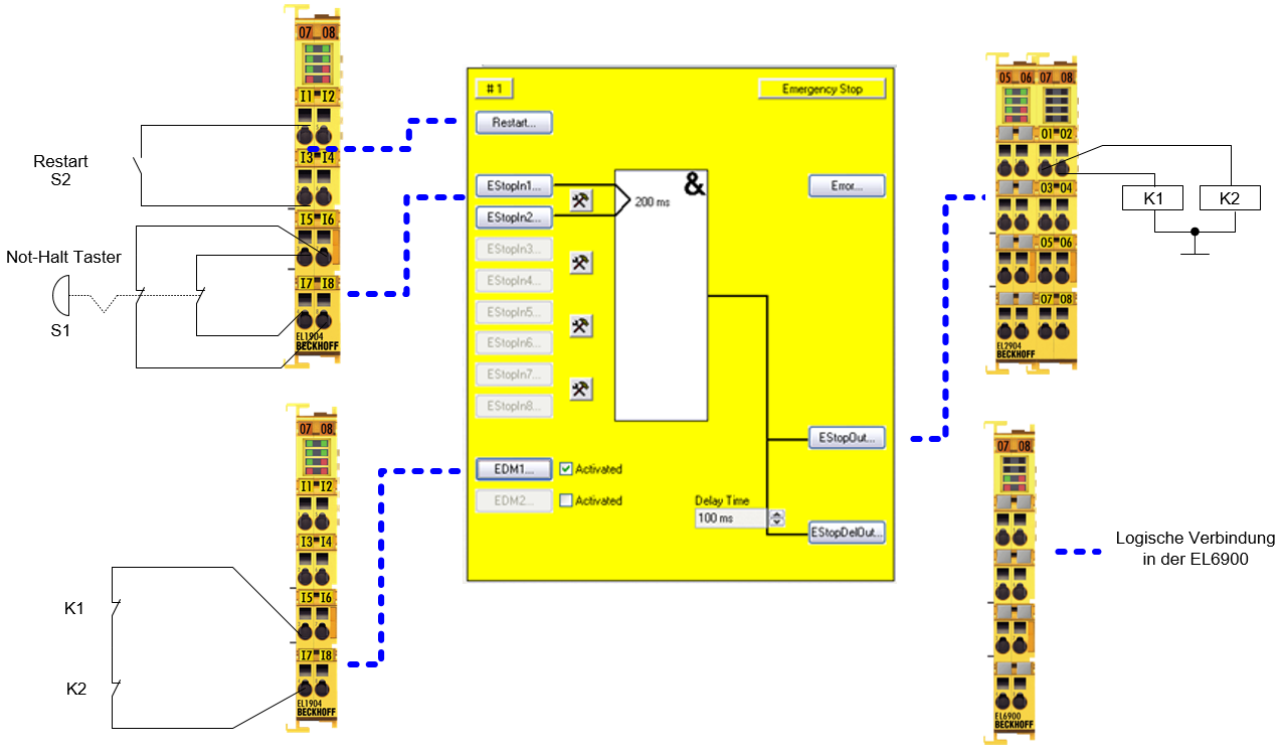
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

3.5 ESTOP Funktion Variante 5 (Kategorie 4, PL e)

Der Not-Halt-Taster mit zwei Öffnerkontakten, der Restart und der Rückführkreis sind auf sichere Kanäle einer Eingangsklemme EL1904 verbunden. Die Testung der Signale ist eingeschaltet. Eine Überprüfung auf Diskrepanz der beiden Not-Halt-Signale wird durchgeführt. Die Schütze K1 und K2 sind auf unterschiedliche Ausgangskanäle verdrahtet. Die Anschlüsse A2 der beiden Schütze sind zusammen auf Masse geführt. Für diese Beschaltung ist die Strommessung der Ausgangskanäle abgeschaltet. Die Testung der Ausgänge ist aktiv.



3.5.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

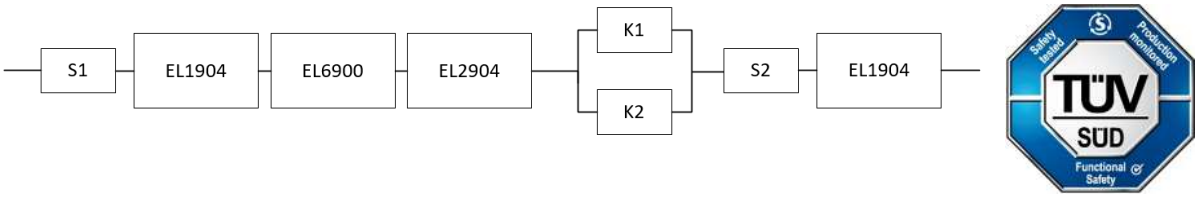
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Ja

3.5.2 Blockbildung und Safety-Loops

3.5.2.1 Sicherheitsfunktion 1



3.5.3 Berechnung

3.5.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	100.000
S2 – $B10_D$	10.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

3.5.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung/Plausibilität	DC_{avg}=99%
S2 mit Plausibilität	DC_{avg}=90%
K1/K2 mit Testung und EDM (Betätigung 1/Schicht)	DC_{avg}=99%

3.5.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_d$-Werte aus den $B10_d$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

K1/K2:

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

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

und der Annahme, dass S1, S2, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

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: Betätigung 1/Schicht

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die B10d-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

bei Betätigung 1/Schicht

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

bzw.:

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

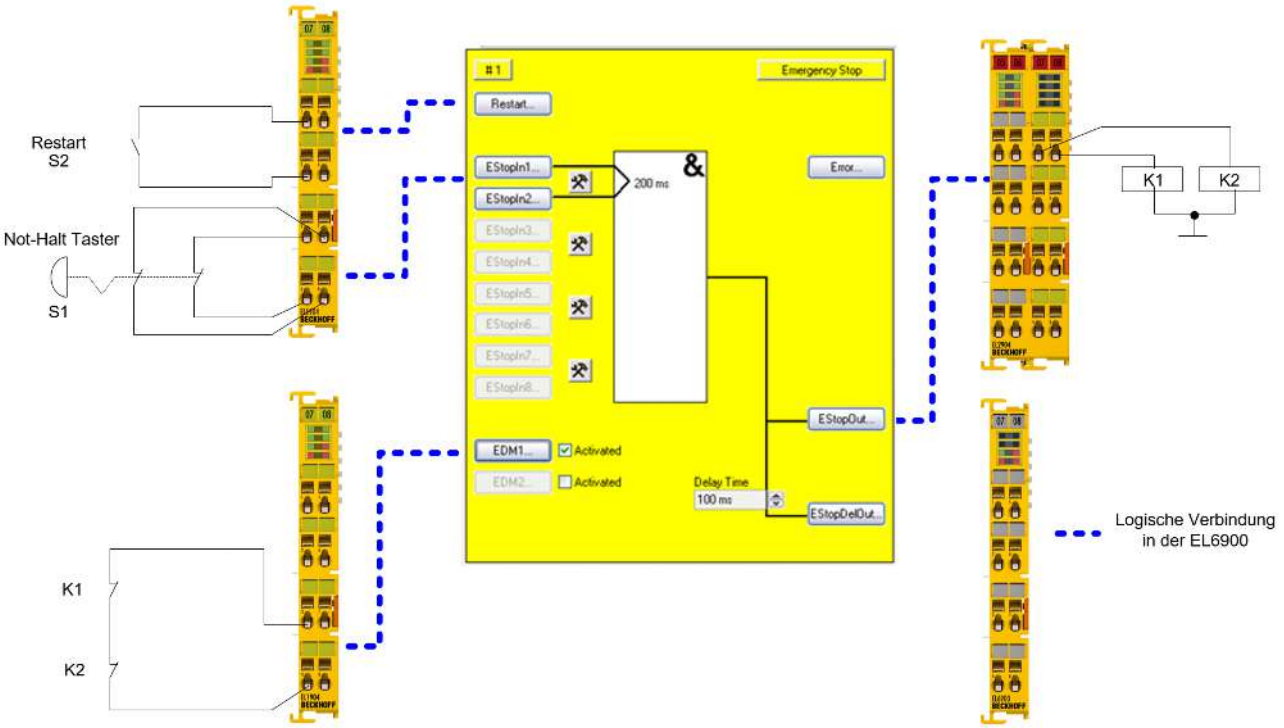
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

3.6 ESTOP Funktion Variante 6 (Kategorie 3, PL d)

Der Not-Halt-Taster mit zwei Öffnerkontakten, der Restart und der Rückführkreis sind auf sichere Kanäle einer Eingangsklemme EL1904 verbunden. Die Testung der Signale ist eingeschaltet. Eine Überprüfung auf Diskrepanz der beiden Not-Halt-Signale wird durchgeführt. Die Schütze K1 und K2 sind auf unterschiedliche Ausgangskanäle verdrahtet. Die Anschlüsse A2 der beiden Schütze sind zusammen auf Masse geführt. Für diese Beschaltung ist die Strommessung der Ausgangskanäle abgeschaltet. Die Testung der Ausgänge ist nicht aktiv.



⚠ VORSICHT

Kategorie

Diese Struktur ist durch einen möglichen schlafenden Fehler nur bis maximal Kategorie 3 möglich.

Da bei dieser Anwendung die Klemme EL2904 nur SIL2 hat, hat die gesamte Kette nur SIL2!

3.6.1 Parameter der sicheren Ein- und Ausgangsklemmen (SIL 2)

EL1904 (für alle verwendeten EL1904 gültig)

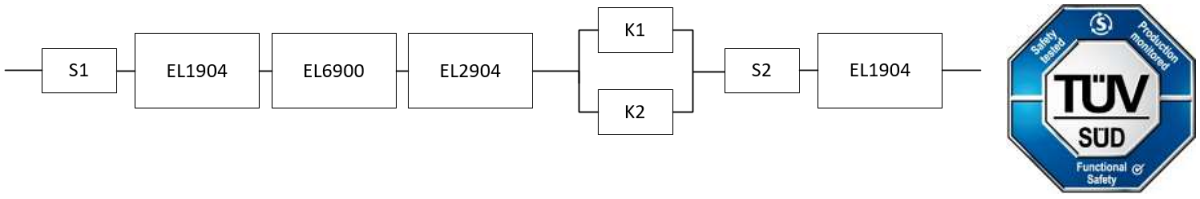
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Nein

3.6.2 Blockbildung und Safety-Loops

3.6.2.1 Sicherheitsfunktion 1



3.6.3 Berechnung

3.6.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	100.000
S2 – $B10_D$	10.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

3.6.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung/Plausibilität	DC_{avg}=99%
S2 mit Plausibilität	DC_{avg}=90%
K1/K2 ohne Testung und mit EDM über einen sicheren Eingang	DC_{avg}=90%

3.6.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

K1/K2:

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

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

und der Annahme, dass S1, S2, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

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: Betätigung 1/Schicht

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

bei Betätigung 1/Schicht

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

⚠ VORSICHT

Kategorie

Diese Struktur ist durch einen möglichen schlafenden Fehler nur bis maximal Kategorie 3 möglich.

Da bei dieser Anwendung die Klemme EL2904 nur SIL2 hat, hat die gesamte Kette nur SIL2!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

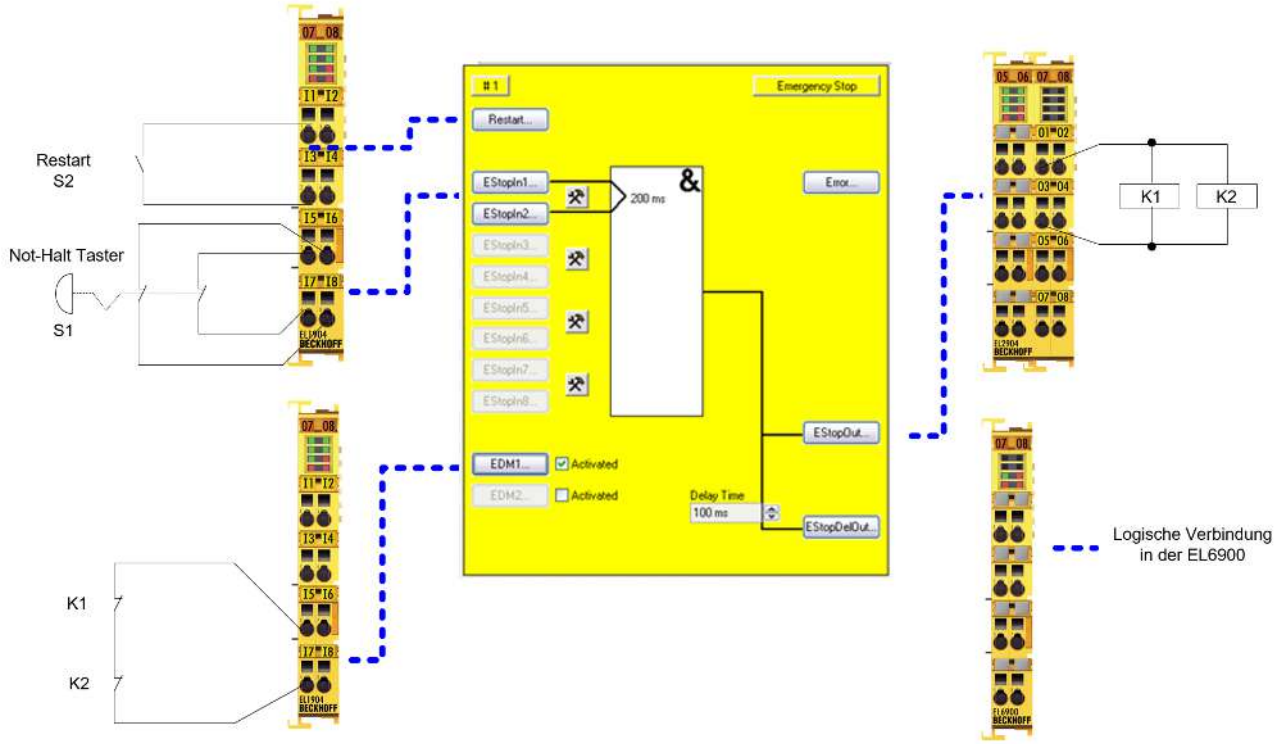
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

3.7 ESTOP Funktion Variante 7 (Kategorie 4, PL e)

Der Not-Halt-Taster mit zwei Öffnerkontakten, der Restart und der Rückführkreis sind auf sichere Kanäle einer Eingangsklemme EL1904 verbunden. Die Testung des Not-Halt-Tasters ist auf beiden Kanälen ausgeschaltet. Der Restart-Taster und der Rückführkreis haben den Sensortest eingeschaltet. Eine Überprüfung auf Diskrepanz der beiden Not-Halt-Signale wird durchgeführt. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



3.7.1 Parameter der sicheren Ein- und Ausgangsklemmen

1. EL1904

Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	nicht verwendet
Sensortest Kanal 3 aktiv	Nein
Sensortest Kanal 4 aktiv	Nein
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

2. EL1904

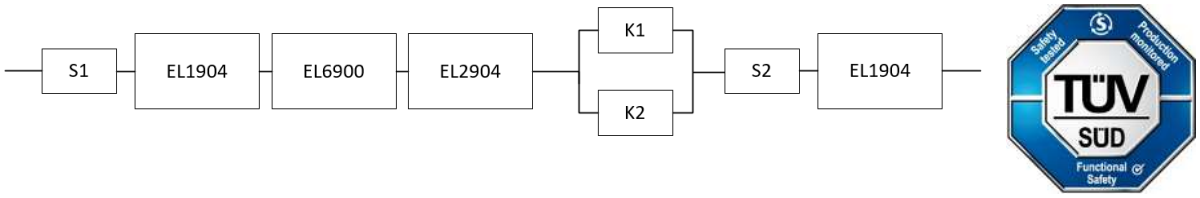
Parameter	Wert
Sensortest Kanal 1 aktiv	nicht verwendet
Sensortest Kanal 2 aktiv	nicht verwendet
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	nicht verwendet
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

3.7.2 Blockbildung und Safety-Loops

3.7.2.1 Sicherheitsfunktion 1



3.7.3 Berechnung

3.7.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	100.000
S2 – $B10_D$	10.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

3.7.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Plausibilität	DC_{avg}=90%
S2 mit Testung	DC_{avg}=90%
K1/K2 mit Testung und EDM (Betätigung 1/Schicht)	DC_{avg}=99%

3.7.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

K1/K2:

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

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

und der Annahme, dass S1, S2, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

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: Betätigung 1/Schicht

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

bei Betätigung 1/Schicht

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

bzw.:

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

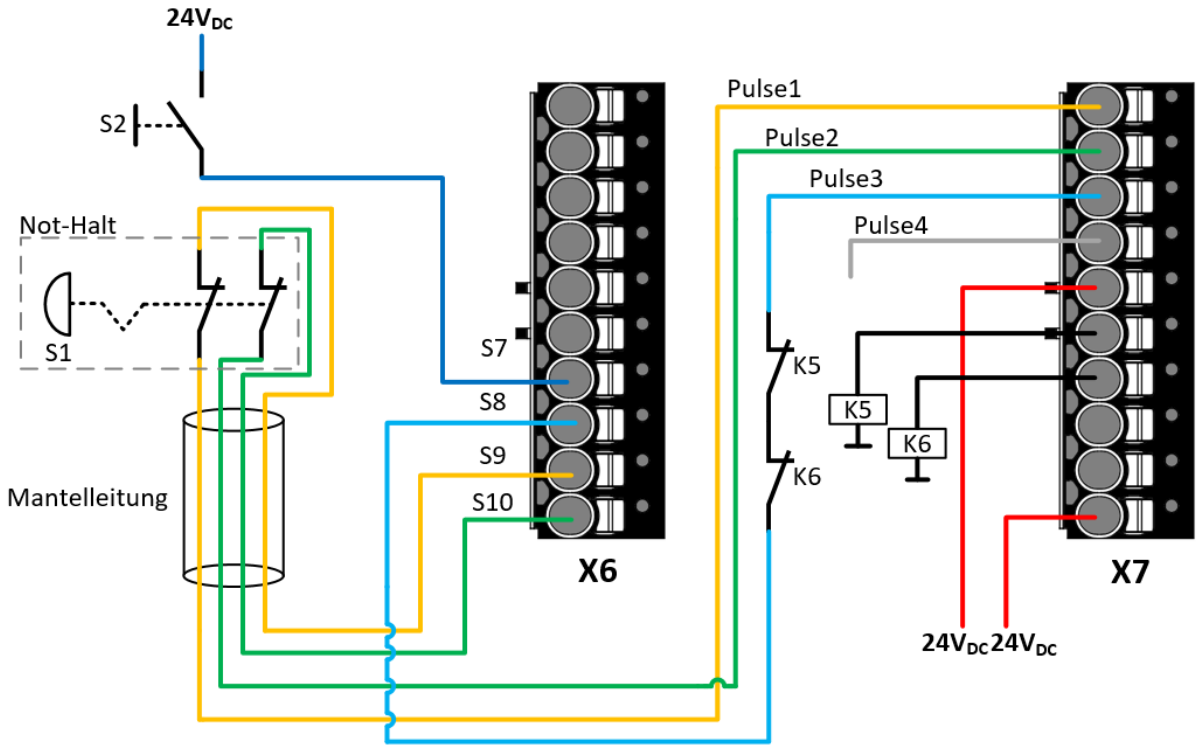
Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

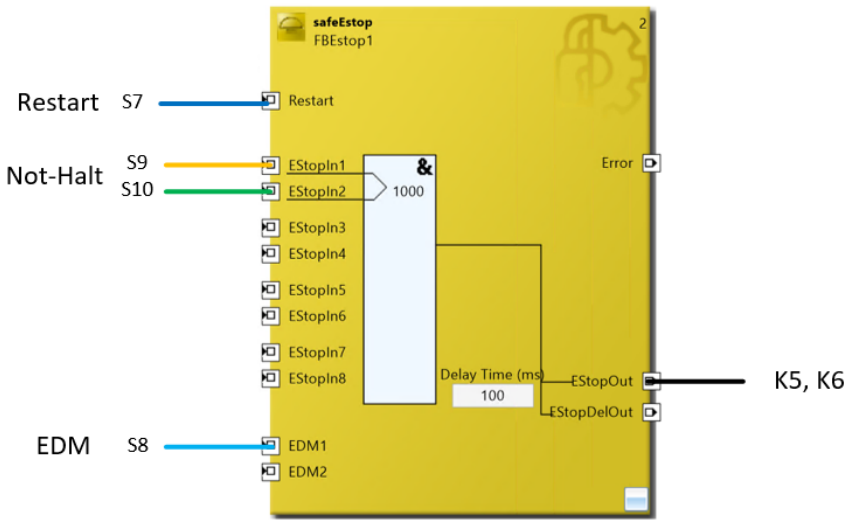
3.8 EK1960 digitale Ein- und Ausgänge (Kategorie 4, PL e)

Der Not-Halt-Taster S1 ist mit zwei Öffner-Kontakten auf die sicheren Eingänge S9 und S10 auf dem 10-poligen Stecker X6 verdrahtet. Die erste Ausgangsgruppe auf dem 10-poligen Stecker X7 ist als Taktquelle konfiguriert (bei FSOUT Module 3 ist der Parameter *Diag TestPulse for Inputs active* auf TRUE gesetzt). Für die Eingänge S9 und S10 ist der Parameter *Channel x.Testpulse Diag Mode* auf die entsprechenden Taktquellen konfiguriert.

Die Schütze K5 und K6 sind auf die Ausgänge 7.5 und 7.6 auf dem 2. Ausgangsmodul auf X7 verdrahtet. Der Anschluss A2 der Schütze ist auf die gemeinsame Masse der $24V_{DC}$ Einspeisung des Anschluss X7 verdrahtet. Die Rückführkreise der beiden Schütze sind in Reihe geschaltet von Pulse 3 auf den Eingang S8 verdrahtet.

Der Restart S2 ist auf den sicheren Eingang S7 verdrahtet ohne Verwendung einer Testung. Der Restart muss für die Anwendung vorhanden sein, wird in der Berechnung jedoch nicht berücksichtigt.





3.8.1 Parameter der sicheren Ein- und Ausgangsmodule

EK1960

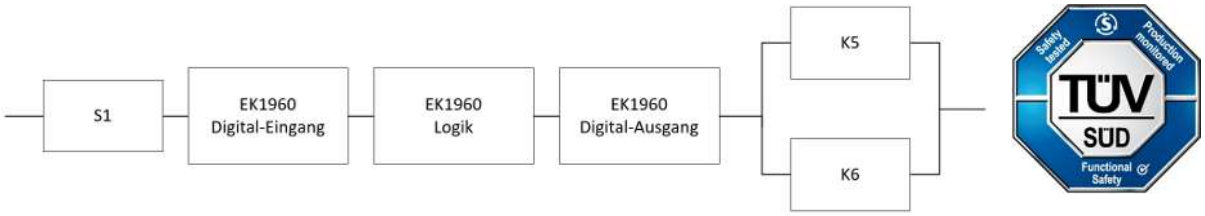
Parameter	Wert
FSOUT Module 3 (X7.1 – X7.4)	**-**
8020:01 ModuloDiagTestPulse	0x00
8020:02 MultiplierDiagTestPulse	0x02
8020:03 Standard Outputs active	FALSE
8020:04 Diag Testpulse active	TRUE
8020:05 Diag Testpulse for Inputs active	TRUE
FSOUT Module 4 (X7.5 – X7.8)	**-**
8030:01 ModuloDiagTestPulse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

ESTOP FB Parameter

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

3.8.2 Blockbildung und Safety-Loops

3.8.2.1 Sicherheitsfunktion 1



3.8.3 Berechnung

3.8.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EK1960 Digitaler Eingang – PFH_D	6,40E-11
EK1960 Eingang Trittmatte - PFH_D	8,84E-10
EK1960 Logik – PFH_D	5,18E-09
EK1960 Digitaler Ausgang – PFH_D	1,50E-10
EK1960 Relais-Ausgang (Kat. 4-zweikanalig) - PFH_D	1,46E-09 (Betätigung 1x pro Stunde)
EK1960 Relais – $B10_D$	1.500.000 (DC13 24V_{DC} und I_{max} ≤ 2A)
S1 – $B10_D$	100.000
K5 – $B10_D$	1.300.000
K6 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

Safety-over-EtherCAT Kommunikation

Der PFH_D Wert der Safety-over-EtherCAT (FSoE) Kommunikation ist im PFH_D Wert der EK1960 Logik-Komponente bereits enthalten.

3.8.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung und Plausibilität	DC_{avg}=99%
K5/K6 mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) mit Testung	DC_{avg}=99%

3.8.3.3 Berechnung Sicherheitsfunktion 1

Berechnung des Performance Levels nach EN ISO 13849-1:2015

Berechnung der $MTTF_D$-Werte aus den $B10_D$-Werten

aus:

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

und:

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

Eingesetzt ergibt das:

S1

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

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

K5/K6

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

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

Der Gesamt-$MTTF_D$ Wert ergibt sich aus der Formel:

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

als:

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

Sind für die EK1960 Komponenten nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist **NICHT** Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Berechnung der PFH_D Werte nach EN 62061

mit der Annahme, dass S1, K5 und K6 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

K5/K6:

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K5 und K6 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K5 und K6 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1 - \beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$ um Zehnerpotenzen kleiner ist, als der Rest, wird er als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	**≥ 10^{-8} bis < 10^{-7}**
2	≥ 10^{-7} bis < 10^{-6}
1	≥ 10^{-6} bis < 10^{-5}

HINWEIS

Sicherheits-Integritätslevel

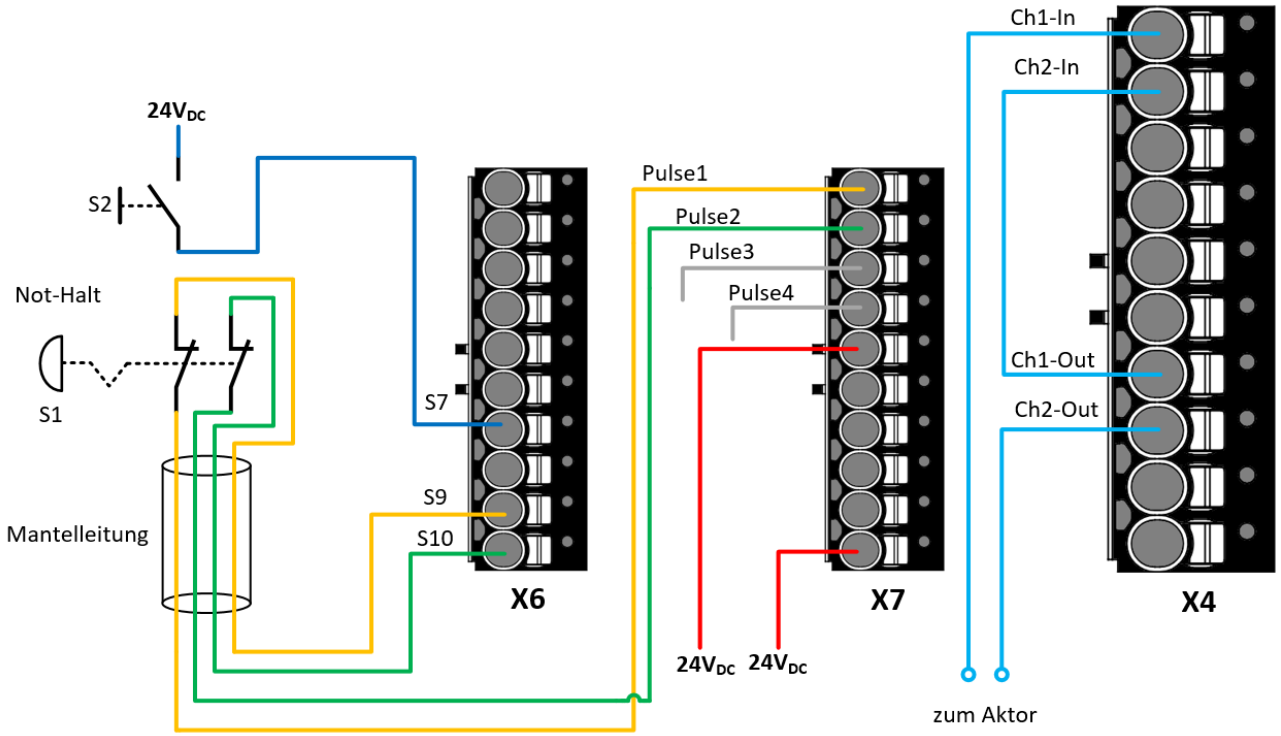
Die Anwendung entspricht einem Sicherheits-Integritätslevel von SIL3 nach EN 62061.

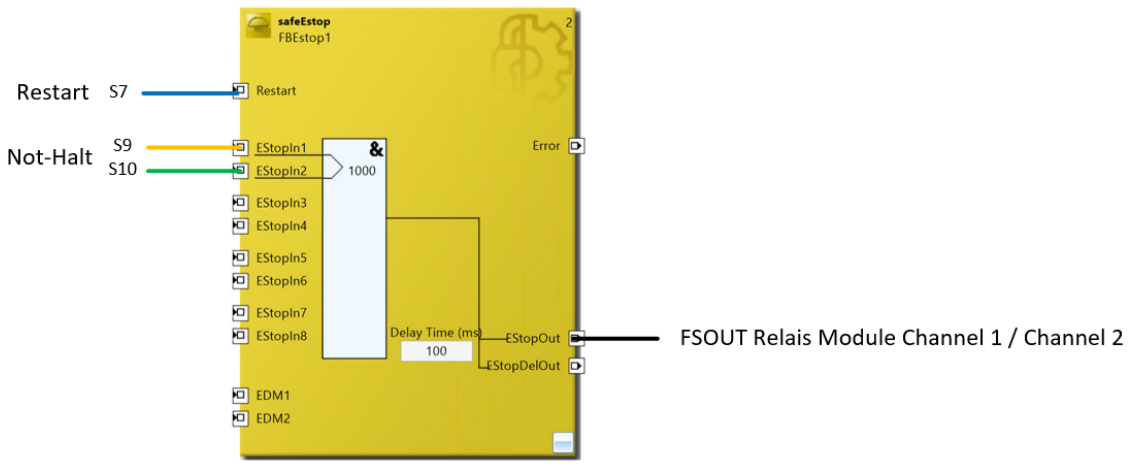
3.9 EK1960 digitale Eingänge / Relais-Ausgänge (Kategorie 4, PL e)

Der Not-Halt-Taster S1 ist mit zwei Öffner-Kontakten auf die sicheren Eingänge S9 und S10 auf dem 10-poligen Stecker X6 verdrahtet. Die erste Ausgangsgruppe auf dem 10-poligen Stecker X7 ist als Taktquelle konfiguriert (bei FSOUT Module 3 ist der Parameter *Diag TestPulse for Inputs active* auf TRUE gesetzt). Für die Eingänge S9 und S10 ist der Parameter *Channel x.Testpulse Diag Mode* auf die entsprechenden Taktquellen konfiguriert.

Die Relais-Ausgänge Channel 1 und Channel 2 werden in Reihe geschaltet und können dann für sicherheitstechnische Funktionen verwendet werden (z.B. Meldung eines Not-Halt an eine vor- oder nachgelagerte Maschine übergeben). Der EDM wird nicht auf den ESTOP-Eingang verdrahtet, da das Relais Modul die EDM-Überwachung durchführt und bei einem Fehler, einen Modulfehler für das Relais-Modul meldet. Auf diesen Modulfehler kann dann applikatorisch reagiert werden oder die TwinSAFE-Gruppe wird so konfiguriert, dass ein Modul Fehler zu einem Com-Error führt.

Der Restart S2 ist auf den sicheren Eingang S7 verdrahtet ohne Verwendung einer Testung. Der Restart muss für die Anwendung vorhanden sein, wird in der Berechnung jedoch nicht berücksichtigt.





3.9.1 Parameter der sicheren Ein- und Ausgangsmodule

EK1960

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

ESTOP FB Parameter

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

HINWEIS

Modul Fehler Relais Modul

Im Falle eines EDM-Fehlers wird ein Modul Fehler des Relais-Moduls gemeldet. Dieses Modul geht dann in den sicheren, abgeschalteten Zustand. Die Fehlerquittierung kann über das Signal *FSOUT Relais Module.Err Ack* erfolgen.

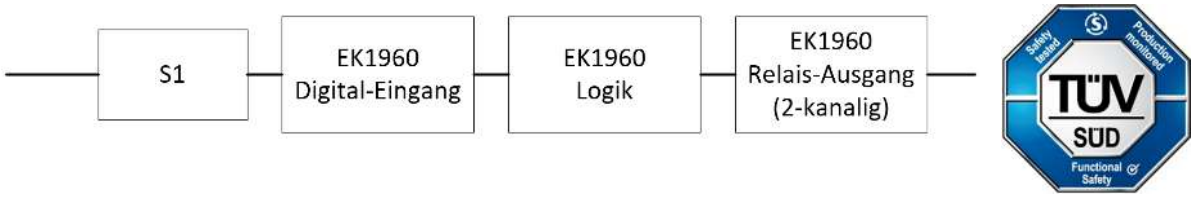
HINWEIS

Schalthäufigkeit

Zur Erlangung von PL e ist es erforderlich, dass die Relais-Ausgänge mindestens 1x pro Monat betätigt werden. In diesem Beispiel wird von einer Schalthäufigkeit von 1x pro Woche ausgegangen.

3.9.2 Blockbildung und Safety-Loops

3.9.2.1 Sicherheitsfunktion 1



3.9.3 Berechnung

3.9.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EK1960 Digitaler Eingang – PFH_D	6,40E-11
EK1960 Eingang Trittmatte - PFH_D	8,84E-10
EK1960 Logik – PFH_D	5,18E-09
EK1960 Digitaler Ausgang – PFH_D	1,50E-10
EK1960 Relais-Ausgang (Kat. 4-zweikanalig) - PFH_D	1,46E-09 (Betätigung 1x pro Stunde)
EK1960 Relais – $B10_D$	1.500.000 (DC13 24V_{DC} und I_{max} ≤ 2A)
S1 – $B10_D$	100.000
K5 – $B10_D$	1.300.000
K6 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

Safety-over-EtherCAT Kommunikation

Der PFH_D Wert der Safety-over-EtherCAT (FSoE) Kommunikation ist im PFH_D Wert der EK1960 Logik-Komponente bereits enthalten.

3.9.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung und Plausibilität	DC_{avg}=99%
Relais-Ausgang 2-kanalig mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken) mit Testung	DC_{avg}=99%

3.9.3.3 Berechnung Sicherheitsfunktion 1

Berechnung des Performance Levels nach EN ISO 13849-1:2015:

Berechnung der $MTTF_D$-Werte aus den $B10_D$-Werten.

aus:

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

und:

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

Eingesetzt ergibt das:

S1

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

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

Relais

Es sind sowohl $B10_D$ als auch PFH_D Wert für das Relais angegeben. In diesem Fall wird für die Berechnung des $MTTF_D$-Wertes der schlechtere der beiden Werte verwendet (hier der PFH_D-Wert – siehe weiter unten).

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

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

Der Gesamt-$MTTF_D$ Wert ergibt sich aus der Formel:

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

als:

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

Sind für die EK1960 Komponenten nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist **NICHT** Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre

$MTTF_D$	
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**
DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Berechnung der PFH_D Werte nach EN 62061:

mit der Annahme, dass S1 einkanalig ist:

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

ergibt sich für

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

S1:

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

zu:

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

Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	**≥ 10^{-8} bis < 10^{-7}**
2	≥ 10^{-7} bis < 10^{-6}

Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
1	≥ 10^{-6} bis < 10^{-5}

HINWEIS

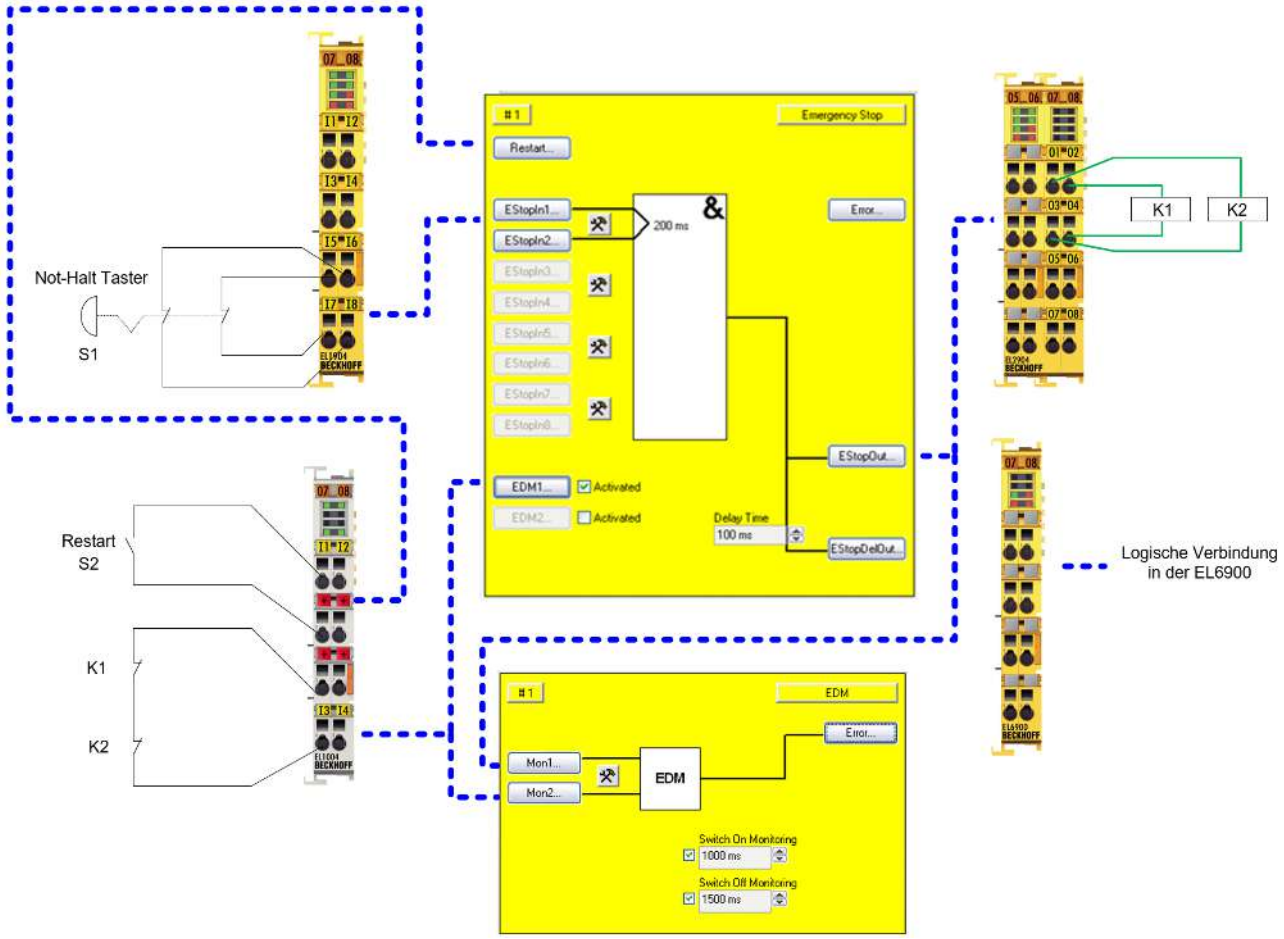
Sicherheits-Integritätslevel

Die Anwendung entspricht einem Sicherheits-Integritätslevel von SIL3 nach EN 62061.

3.10 ESTOP Funktion (Kategorie 3, PL d)

Der Not-Halt-Taster ist mit zwei Öffnerkontakten auf eine sichere Eingangsklemme EL1904 verbunden. Die Testung der beiden Signale ist ausgeschaltet. Diese Signale werden innerhalb des ESTOP Bausteins auf Diskrepanz überprüft. Der Restart und das Rückführsignal der Schütze K1 und K2 sind auf Standard-Klemmen verdrahtet und werden über die Standard-SPS an TwinSAFE übergeben. Weiterhin werden der Ausgang des Funktionsbausteins ESTOP und das Rückführsignal auf einen EDM-Baustein verdrahtet. Dieser prüft, dass das Rückführsignal innerhalb der eingestellten Zeiten den gegengesetzten Zustand des ESTOP-Ausgangs einnimmt.

Die Schütze K1 und K2 sind auf unterschiedliche Ausgangskanäle verdrahtet. Die Anschlüsse A2 der beiden Schütze sind auf die EL2904 zurückgeführt. Für diese Beschaltung ist die Strommessung der Ausgangskanäle abgeschaltet. Die Testung der Ausgänge ist ebenfalls nicht aktiv.



3.10.1 Parameter der sicheren Ein- und Ausgangsklemmen (SIL 2)

EL1904 (für alle verwendeten EL1904 gültig)

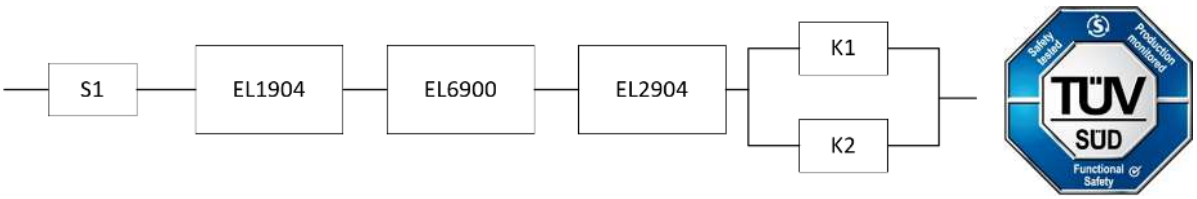
Parameter	Wert
Sensortest Kanal 1 aktiv	-
Sensortest Kanal 2 aktiv	-
Sensortest Kanal 3 aktiv	Nein
Sensortest Kanal 4 aktiv	Nein
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Nein

3.10.2 Blockbildung und Safety-Loops

3.10.2.1 Sicherheitsfunktion 1



3.10.3 Berechnung

3.10.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	100.000
S2 – $B10_D$	10.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

3.10.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Plausibilität	DC_{avg}=90%
K1/K2 mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) ohne Testung der einzelnen Kanäle	DC_{avg}=90%

3.10.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

K1/K2:

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

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

und der Annahme, dass S1, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

K1/K2: Betätigung 1/Woche und indirektes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

⚠ VORSICHT

Kategorie

Diese Struktur ist durch einen möglichen schlafenden Fehler nur bis maximal Kategorie 3 möglich.

Da bei dieser Anwendung die Klemme EL2904 nur SIL2 hat, hat die gesamte Kette nur SIL2!

⚠ VORSICHT

Weitere Maßnahmen zum Erreichen der Kategorie 3!

Diese Struktur ist bis maximal Kategorie 3 möglich. Um die Kategorie 3 zu erreichen, müssen in der Steuerung zur Erwartungshaltung des Rücklesens alle steigenden und fallenden Flanken zusammen mit der Zeitabhängigkeit ausgewertet werden!

Dies wird über den implementierten EDM-Baustein realisiert.

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**
DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

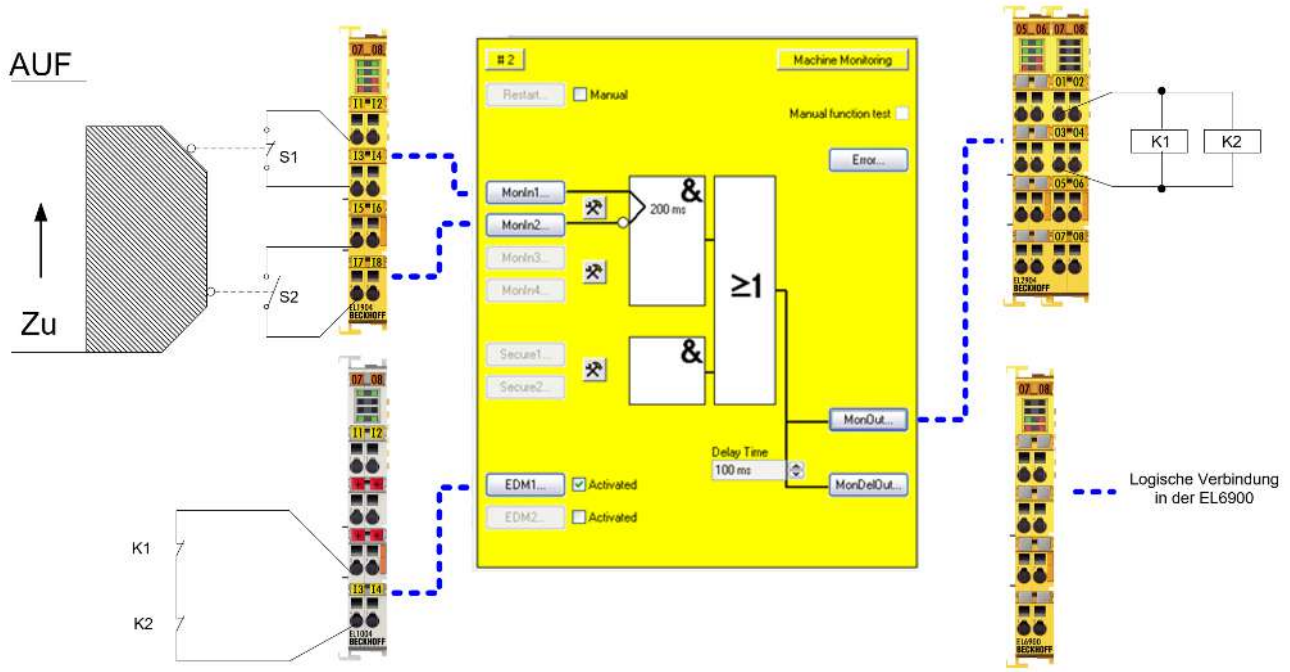
Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4 Zugangsfunktionen

4.1 Schutztür Funktion Variante 1 (Kategorie 3, PL d)

Die Schutztür verwendet eine Kombination von Öffner und Schließer auf sicheren Eingängen einer EL1904. Die Testung der Eingänge ist aktiv und die Signale werden auf Diskrepanz (200 ms) überprüft. Der Rückführkreis wird über einen Standard-Eingang eingelesen und über die Standard-SPS an TwinSAFE übergeben. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



4.1.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

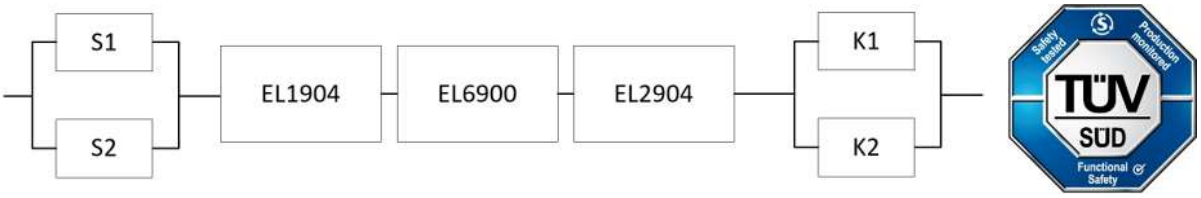
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

4.1.2 Blockbildung und Safety-Loops

4.1.2.1 Sicherheitsfunktion 1



4.1.3 Berechnung

4.1.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.1.3.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
K1/K2 mit Testung und EDM	DC_{avg}=90%

4.1.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

K1/K2:

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

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

und der Annahme, dass S1, S2, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

S2:

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

K1/K2:

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

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da die Anteile $(1-\beta)^2*(PFH_{(S1)}*PFH_{(S2)})*T1$ und $(1-\beta)^2*(PFH_{(K1)}*PFH_{(K2)})*T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

⚠ VORSICHT

Maßnahmen zum Erreichen der Kategorie 3!

Diese Struktur ist durch einen möglichen schlafenden Fehler nur bis maximal Kategorie 3 möglich. Um die Kategorie 3 zu erreichen, müssen in der Standard-Steuerung zur Erwartungshaltung des Rücklesens alle steigenden und fallenden Flanken zusammen mit der Zeitabhängigkeit ausgewertet werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

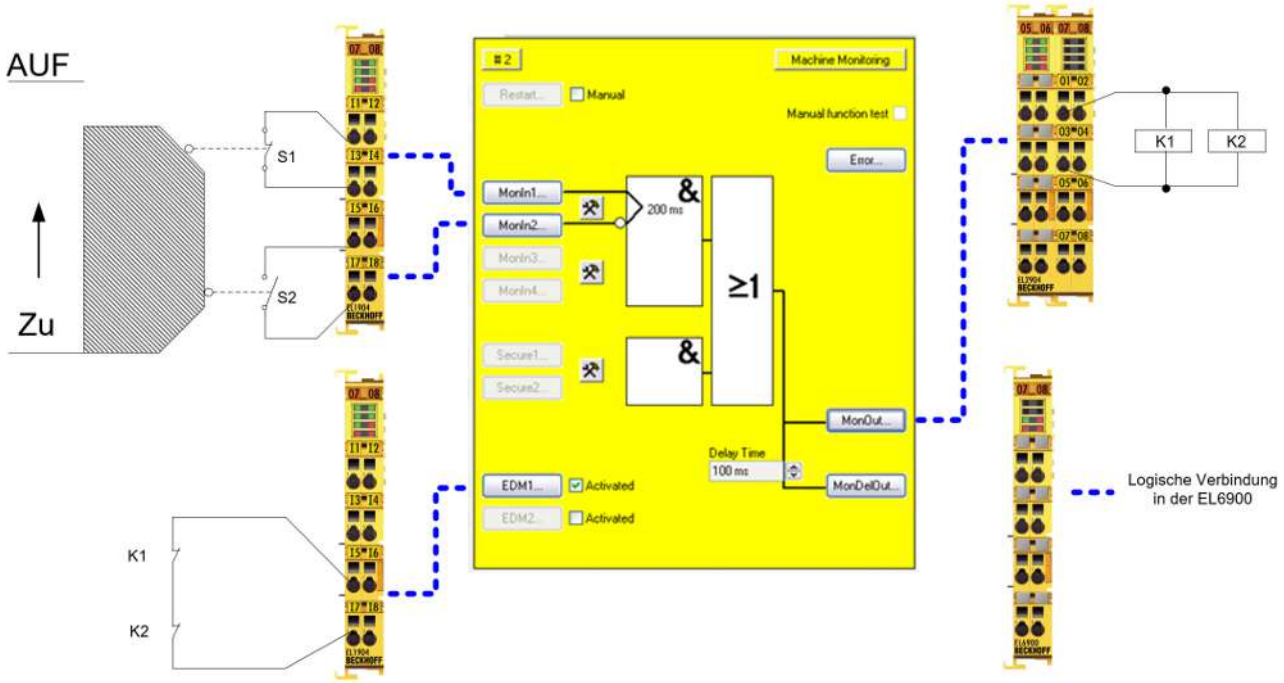
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4.2 Schutztür Funktion Variante 2 (Kategorie 4, PL e)

Die Schutztür verwendet eine Kombination von Öffner und Schließer auf sicheren Eingängen einer EL1904. Die Testung der Eingänge ist aktiv und die Signale werden auf Diskrepanz (200 ms) überprüft. Der Rückführkreis wird über einen sicheren Eingang eingelesen. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



4.2.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

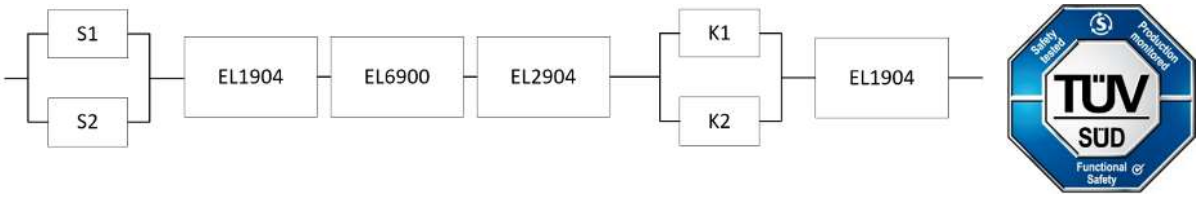
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

4.2.2 Blockbildung und Safety-Loops

4.2.2.1 Sicherheitsfunktion 1



4.2.3 Berechnung

4.2.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.2.3.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
K1/K2 mit Testung und EDM	DC_{avg}=99%

4.2.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_d$-Werte aus den $B10_d$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

K1/K2:

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

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

und der Annahme, dass S1, S2, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

S2:

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

K1/K2:

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

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da die Anteile $(1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ und $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

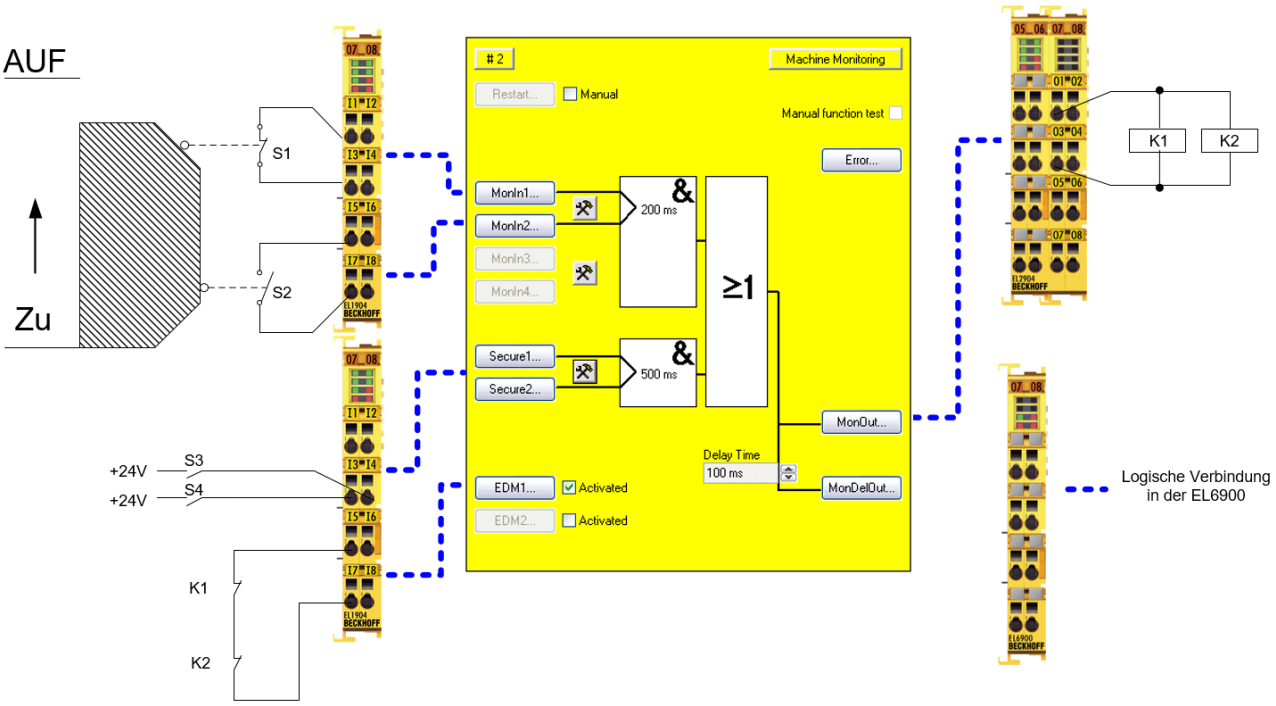
Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

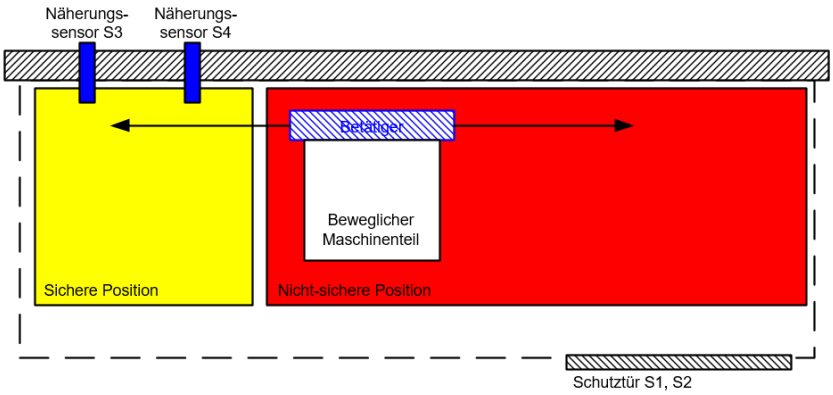
Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4.3 Schutztür Funktion mit Bereichsüberwachung (Kategorie 4, PL e)

Die Schutztür verwendet eine Kombination von Öffner und Schließer auf sicheren Eingängen einer EL1904. Die Testung der Eingänge ist aktiv und die Signale werden auf Diskrepanz (200 ms) überprüft. Der Rückführkreis wird über einen sicheren Eingang eingelesen. Die Näherungssensoren S3 und S4 sind auf sichere Eingänge verdrahtet und stellen fest, dass ein z.B. gefahrbringender Maschinenteil in einer sicheren Position ist, damit die Schutztür bei laufender Maschine geöffnet werden darf. Die Testung dieser Eingänge ist dafür abgeschaltet, damit mit der statischen 24 V Spannung der Sensoren gearbeitet werden kann.

An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.





4.3.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (obere EL1904 in der Zeichnung)

Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja

Parameter	Wert
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL1904 (untere EL1904 in der Zeichnung)

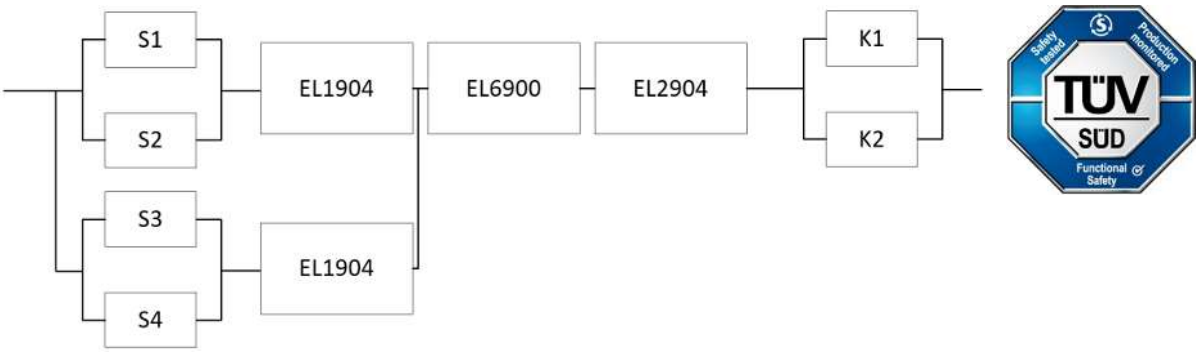
Parameter	Wert
Sensortest Kanal 1 aktiv	Nein
Sensortest Kanal 2 aktiv	Nein
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904 (für alle verwendeten EL2904 gültig)

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

4.3.2 Blockbildung und Safety-Loops

4.3.2.1 Sicherheitsfunktion 1



4.3.3 Berechnung

4.3.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
S3 – $B10_D$	20.000.000
S4 – $B10_D$	20.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16

Komponente	Wert
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.3.3.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
S3/S4 mit ohne Testung/mit Plausibilität	DC_{avg}=90%
K1/K2 mit Testung und EDM	DC_{avg}=99%

4.3.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

S3:

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

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

S4:

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

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

K1/K2:

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

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

und der Annahme, dass S1, S2, S3, S4, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

S2:

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

S3/S4:

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

K1/K2:

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

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Die Näherungssensoren S3/S4 werden auf Plausibilität überwacht (zeitlich/logisch) und sind Typ A-Systeme nach EN 61508 (nicht komplexe Bauteile, deren Verhalten unter Fehlerbedingungen vollständig bekannt ist). Einmal pro Schicht wird die sichere Position angefahren.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da die Anteile $(1-\beta)^2 * (PFH_{(S1/S2/EL1904)} * PFH_{(S3/S4/EL1904)}) * T1$ und $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

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

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich. Die Überwachung der Sensoren S3 und S4 muss zeitlich und logisch programmiert sein.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

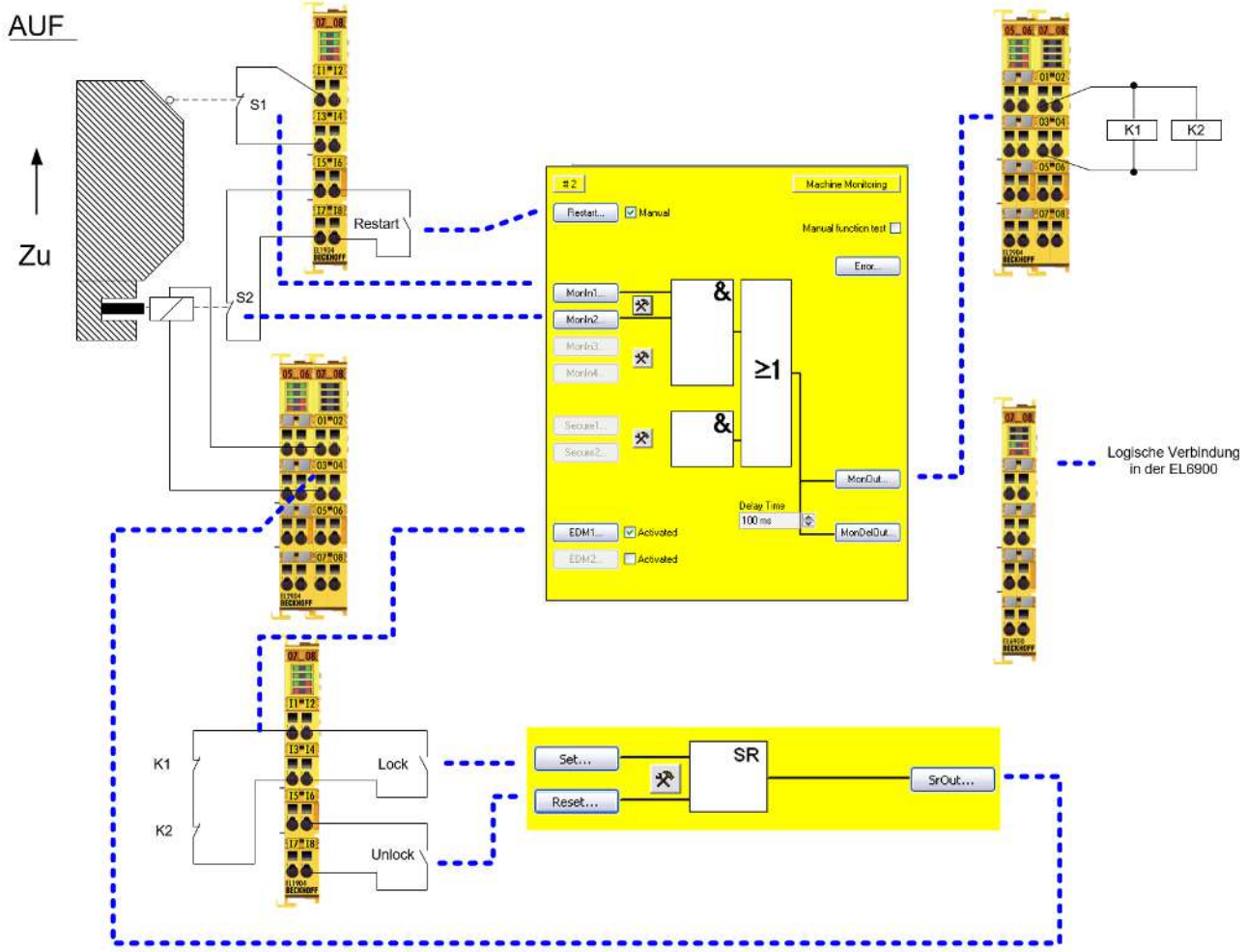
Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4.4 Schutztür Funktion mit Zuhaltung (Kategorie 4, PL e)

Die Schutztür hat zwei Kontakte „Tür geschlossen“ S1 und „Tür geschlossen und verriegelt“ S2, die auf sichere Eingänge einer EL1904 verdrahtet sind. Die Testung der Eingänge ist aktiv. Eine Überprüfung auf Diskrepanz der Signale kann nicht stattfinden, da es keinen zeitlichen Zusammenhang der Signale gibt. Der Rückführkreis und das Restart-Signal werden über einen sicheren Eingang eingelesen. Auch hier ist die Testung der Eingänge aktiv. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.

Die Zuhaltung wird über 2 sichere Eingänge geschaltet bei denen die Testung aktiv ist. Der sichere Ausgang für die Zuhaltung hat die Testung und Strommessung aktiv.



4.4.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

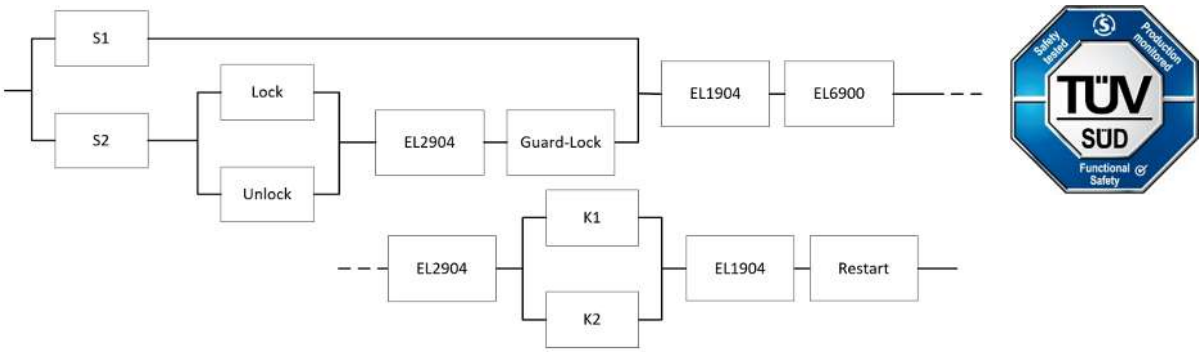
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904 (für alle verwendeten EL2904 gültig)

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

4.4.2 Blockbildung und Safety-Loops

4.4.2.1 Sicherheitsfunktion 1



4.4.3 Berechnung

4.4.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	2.000.000
S2 – $B10_D$	2.000.000
Restart - $B10_D$	10.000.000
Lock – $B10_D$	100.000
Unlock – $B10_D$	100.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Zuhaltung (Guard Lock) - $B10_D$	2.000.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.4.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung	DC_{avg}=90%
S2 mit Testung und Erwartungshaltung	DC_{avg}=99%
Lock/Unlock mit Testung/Plausibilität	DC_{avg}=99%
Restart	DC_{avg}=99%

Komponente	Wert
K1/K2 mit Testung und EDM	DC_{avg}=99%
Zuhaltung	DC_{avg}=99%

4.4.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

Lock/Unlock:

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

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

K1/K2:

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

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

Restart:

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

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

Zuhaltung:

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

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

und der Annahme, dass S1, S2, S3, S4, K1, K2 und die Zuhaltung jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

S2:

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

Lock/Unlock:

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

Restart:

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

K1/K2:

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

Zuhaltung:

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

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 müssen beide betätigt werden. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Die Zuhaltung ist mit dem Schalter S2 mechanisch so verbunden, dass ein Trennen der Kopplung ausgeschlossen werden kann.

Der Restart wird überwacht, dass ein Signalwechsel erst gültig ist, sobald die Tür geschlossen ist.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da die Anteile $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

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

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

$$= 98{,}98\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

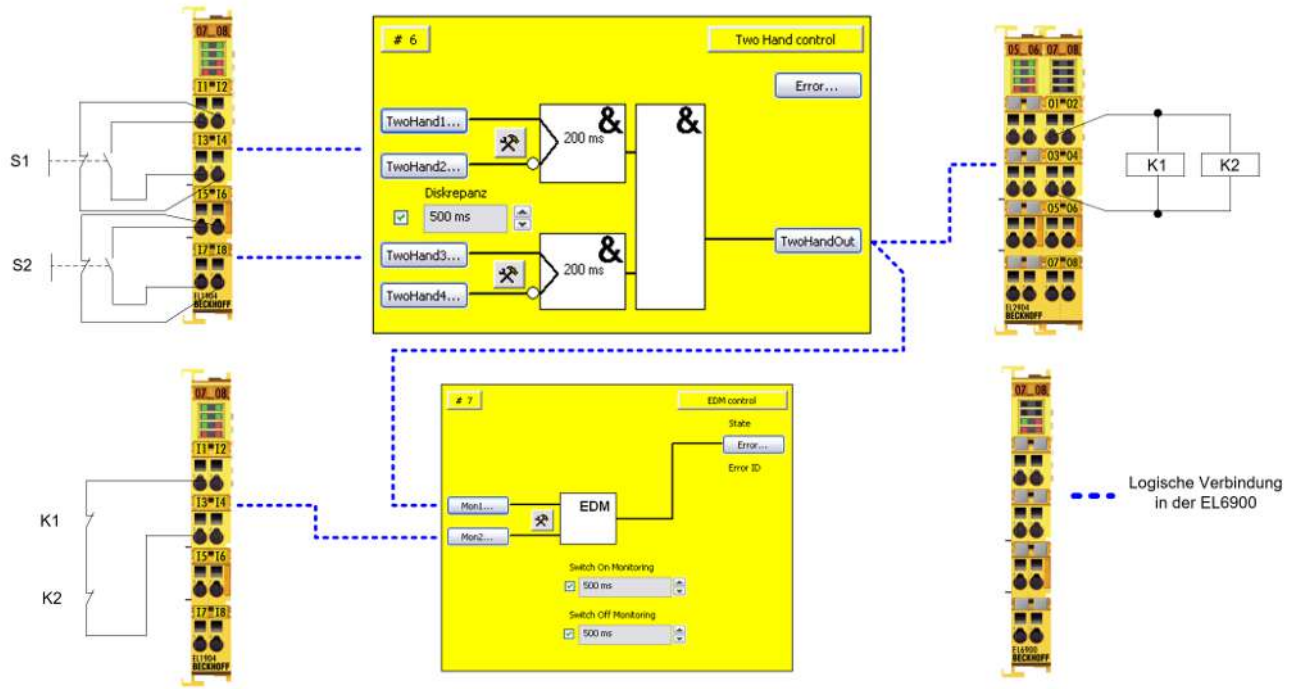
Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4.5 Zweihand-Steuerung (Kategorie 4, PL e)

Die Zweihandtaster bestehen jeweils aus einer Kombination von Öffner und Schließer auf sicheren Eingängen einer EL1904. Die Testung der Eingänge ist aktiv und die Signale werden auf Diskrepanz (200 ms) überprüft. Zusätzlich ist die synchrone Betätigung der beiden Taster aktiviert mit einer Überwachungszeit von 500 ms.

Der Rückführkreis wird über einen sicheren Eingang eingelesen. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



4.5.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

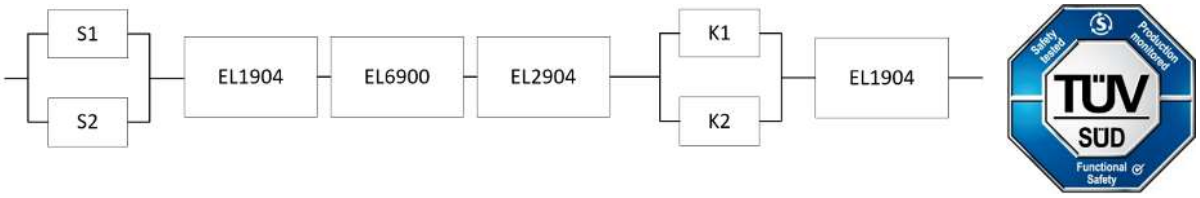
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

4.5.2 Blockbildung und Safety-Loops

4.5.2.1 Sicherheitsfunktion 1



4.5.3 Berechnung

4.5.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	20.000.000
S2 – $B10_D$	20.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	1 (1x pro Minute)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.5.3.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
K1/K2 mit Testung und EDM	DC_{avg}=99%

4.5.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1/S2:

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

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

K1/K2:

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

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

und der Annahme, dass S1, S2, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1/S2:

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

K1/K2:

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da die Anteile $(1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ und $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

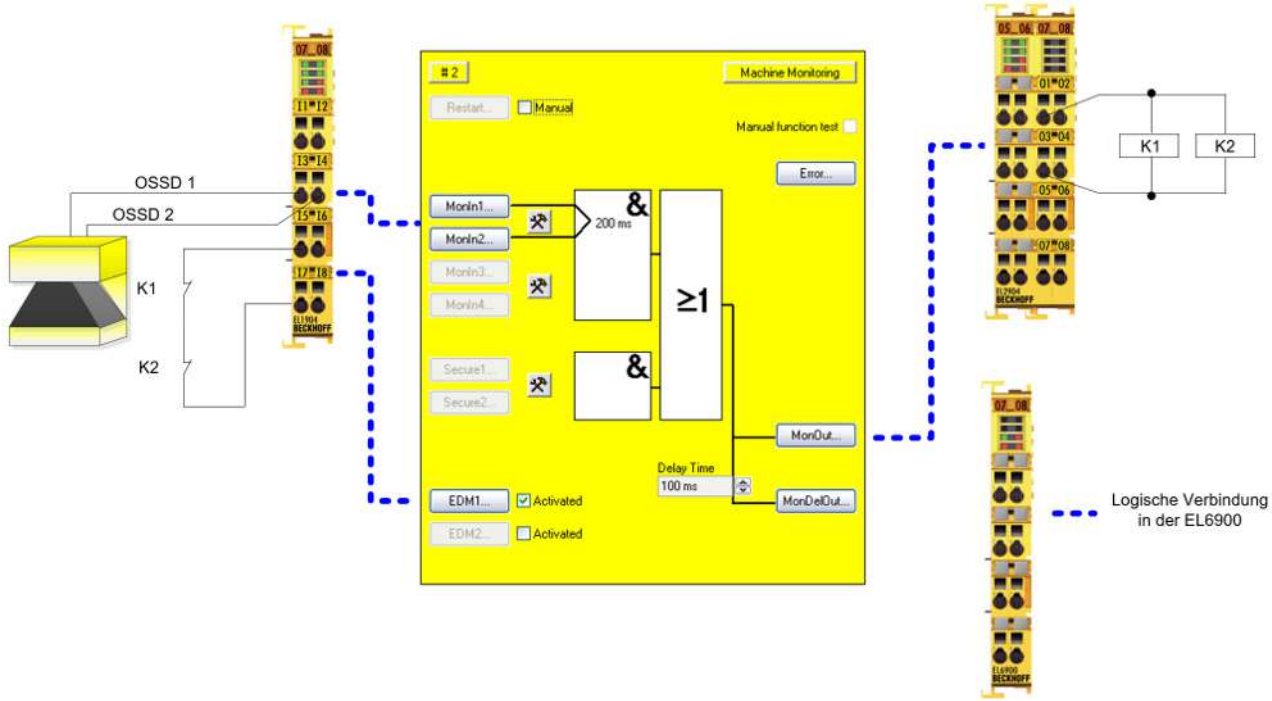
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4.6 Laserscanner (Kategorie 3, PL d)

Der Laser-Scanner hat zwei OSSD-Ausgänge (Output-Signal-Switching-Device), die auf sichere Eingänge einer EL1904 verdrahtet sind. Die Testung der Eingänge ist nicht aktiv, da die OSSD-Ausgänge eine eigene Testung durchführen. Weiterhin werden die Signale auf Diskrepanz (200 ms) überprüft. Der Rückführkreis wird über einen sicheren Eingang eingelesen. Für diesen Eingang ist die Testung aktiv. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



4.6.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

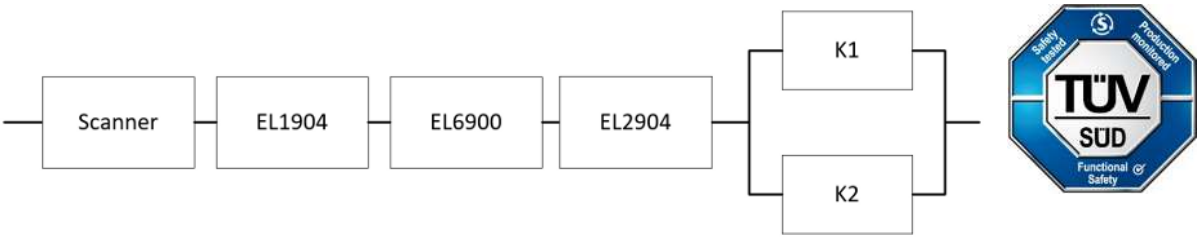
Parameter	Wert
Sensortest Kanal 1 aktiv	Nein
Sensortest Kanal 2 aktiv	Nein
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	OSSD beliebige Pulsarten
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

4.6.2 Blockbildung und Safety-Loops

4.6.2.1 Sicherheitsfunktion 1



4.6.3 Berechnung

4.6.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
Laserscanner – PFH_D	7,67E-08
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10 (6x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.6.3.2 Diagnostic Coverage DC

Komponente	Wert
OSSD1/2 mit Testung(durch Scanner)/Plausibilität	DC_{avg}=90%
K1/K2 mit Testung und EDM	DC_{avg}=99%

4.6.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

K1/K2:

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

Entsprechend der in DIN EN ISO 13849-1 eingeführten Begrenzung der $MTTF_D$ auf 100 Jahre für Komponenten mit einer Kategorie 3 Struktur (für Kategorie 4 liegt die Beschränkung bei 2500 Jahren) wird für die Weiterverarbeitung der $MTTF_D$ des Scanners der Wert auf 100 Jahre begrenzt.

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

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

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

HINWEIS

Kategorie

Diese Struktur ist durch den Einsatz des Typ3 (Kategorie 3) Laserscanners maximal bis Kategorie 3 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

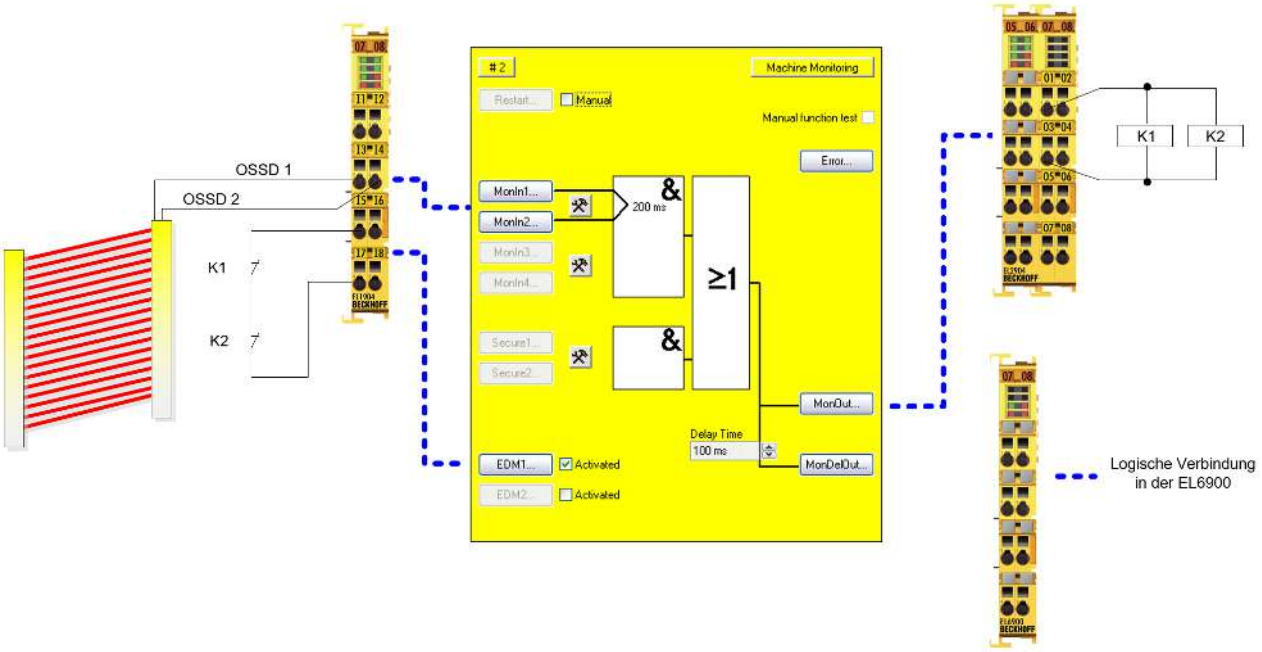
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4.7 Lichtgitter (Kategorie 4, PL e)

Das Lichtgitter hat zwei OSSD-Ausgänge (Output-Signal-Switching-Device), die auf sichere Eingänge einer EL1904 verdrahtet sind. Die Testung der Eingänge ist nicht aktiv, da die OSSD-Ausgänge eine eigene Testung durchführen. Weiterhin werden die Signale auf Diskrepanz (200 ms) überprüft. Der Rückführkreis wird über einen sicheren Eingang eingelesen. Für diesen Eingang ist die Testung aktiv. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



4.7.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904

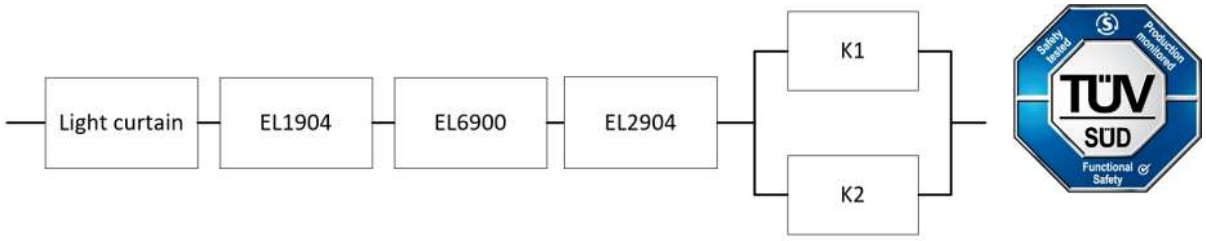
Parameter	Wert
Sensortest Kanal 1 aktiv	Nein
Sensortest Kanal 2 aktiv	Nein
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Asynchrone Auswertung OSSD
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

4.7.2 Blockbildung und Safety-Loops

4.7.2.1 Sicherheitsfunktion 1



4.7.3 Berechnung

4.7.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
Lichtgitter (Light curtain) – PFH_D	1,50E-08
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	5 (12x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.7.3.2 Diagnostic Coverage DC

Komponente	Wert
OSSD1/2 mit Testung(durch Lichtvorhang)/ Plausibilität	DC_{avg}=99%
K1/K2 mit Testung und EDM	DC_{avg}=99%

4.7.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

K1/K2:

$$PFH = \frac{1 - 0{,}99}{294{,}4y * 8760} = 3{,}88E - 09$$

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

$$MTTF_{D(Lightcurtain)} = \frac{(1 - DC_{(Lightcurtain)})}{PFH_{(Lightcurtain)}} = \frac{(1 - 0,99)}{1,50E-08\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,31E-04\frac{1}{y}} = 76,1y$$

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

$$DC_{avg} = \frac{\frac{99\%}{76,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{294,4y} + \frac{99\%}{294,4y}}{\frac{1}{76,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{294,4y} + \frac{1}{294,4y}} = 99,00\%$$

HINWEIS

Kategorie

Diese Struktur ist durch den Einsatz des Typ4 (Kategorie 4) Lichtvorhangs maximal bis Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

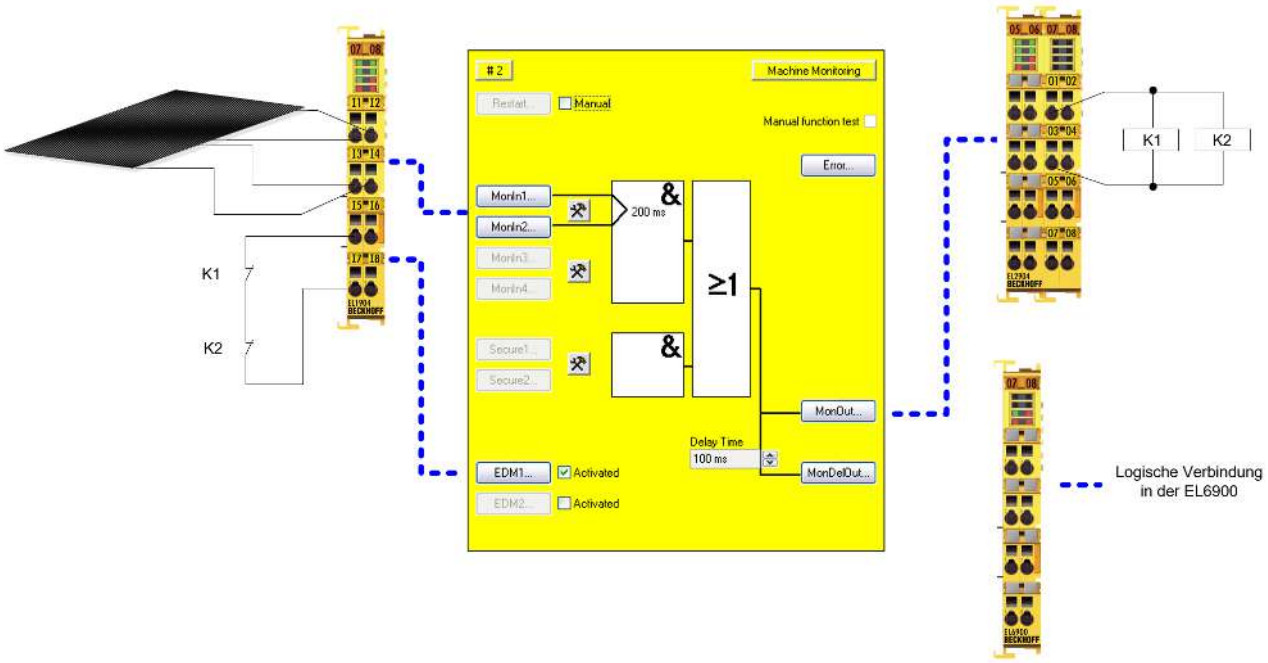
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4.8 Sicherheitsschaltmatte / Safety Bumper (Kategorie 4, PL e)

Sicherheitsschaltmatten oder Safety Bumper arbeiten nach dem Prinzip des Querschlusses. Die Kontaktflächen des Gerätes werden auf sichere Eingänge einer EL1904 verdrahtet. Die Testung der Eingänge ist aktiv und die Signale werden auf Diskrepanz (200 ms) überprüft. Sobald ein Querschluss (Schaltmatte wird betreten) zwischen den Signalen erkannt wird, wird eine logische 0 von der Eingangsklemme EL1904 gemeldet. Ist der Querschluss nicht mehr vorhanden wird eine logische 1 gemeldet. Der Rückführkreis wird über einen sicheren Eingang eingelesen. Auch hier ist die Testung des Einganges aktiv. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



4.8.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

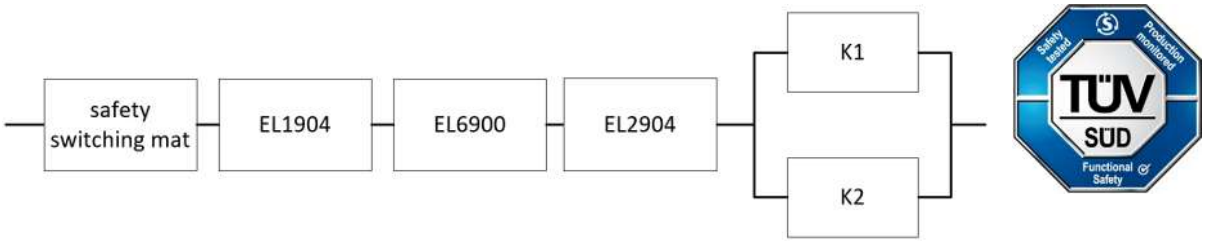
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Querschluss ist kein Modulfehler
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

4.8.2 Blockbildung und Safety-Loops

4.8.2.1 Sicherheitsfunktion 1



4.8.3 Berechnung

4.8.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
Schaltmatte (safety switching mat) – $B10_D$	6,00E06
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	1 (1x pro Minute)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.8.3.2 Diagnostic Coverage DC

Komponente	Wert
Schaltausgänge (Matte) mit Testung/Plausibilität	DC_{avg}=99%
K1/K2 mit Testung und EDM	DC_{avg}=99%

4.8.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_d$-Werte aus den $B10_d$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

K1/K2:

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

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

Schaltmatte:

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

$$MTTF_D = \frac{6{,}00E06}{0{,}1 * 220.800} = 271{,}7y = 2.380.434h$$

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

K1/K2:

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

Schaltmatte:

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

$$DC_{avg} = \frac{\frac{99\%}{271{,}7y} + \frac{99\%}{1028{,}8y} + \frac{99\%}{1108{,}6y} + \frac{99\%}{913{,}2y} + \frac{99\%}{58{,}9y} + \frac{99\%}{58{,}9y}}{\frac{1}{271{,}7y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{58{,}9y} + \frac{1}{58{,}9y}} = 99{,}00\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

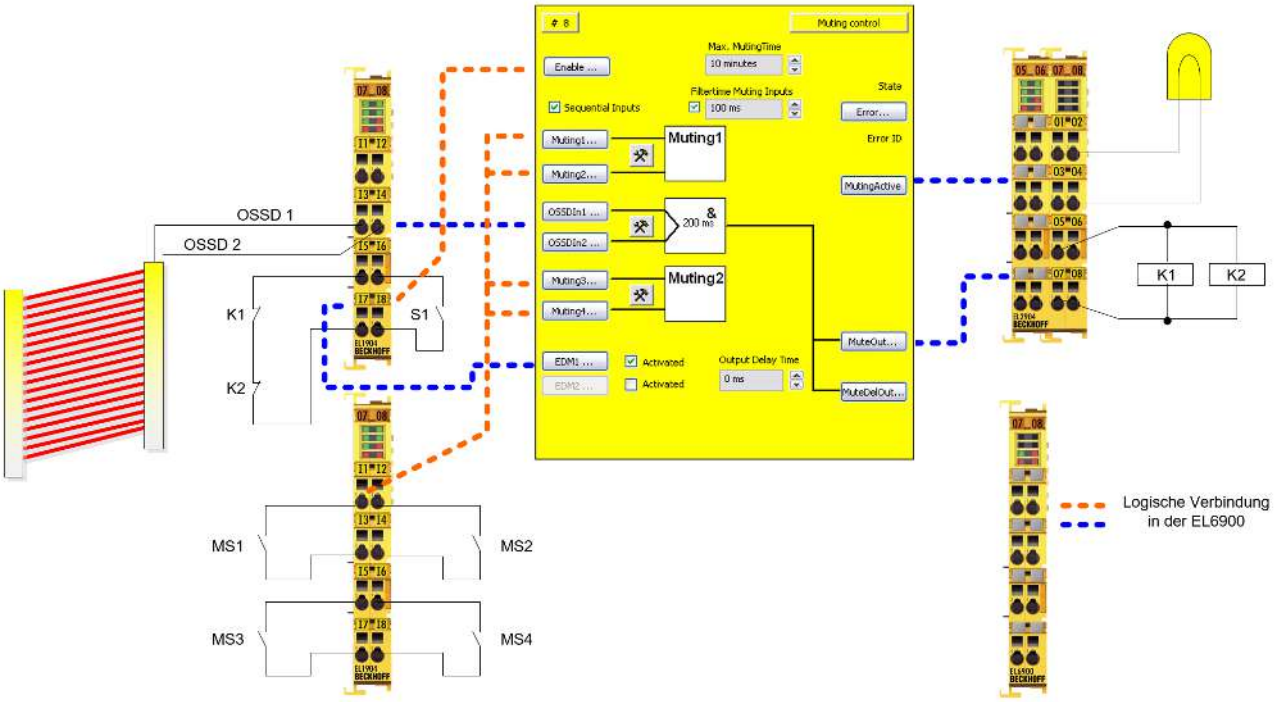
Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4.9 Muting (Kategorie 4, PL e)

Das Lichtgitter hat zwei OSSD Ausgänge (Output-Signal-Switching-Device), die auf sichere Eingänge einer EL1904 verdrahtet sind. Die Testung der Eingänge ist nicht aktiv, da die OSSD Ausgänge eine eigene Testung durchführen. Weiterhin werden die Signale auf Diskrepanz (200 ms) überprüft. Der Rückführkreis wird über einen sicheren Eingang eingelesen. Die Muting-Schalter und der Enable-Schalter sind ebenfalls auf sichere Eingänge verdrahtet. Für diese Eingänge ist die Testung aktiv.
An einem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Die Muting-Lampe ist ebenfalls auf einen sicheren Ausgang verdrahtet. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.



4.9.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (obere Klemme in der Zeichnung)

Parameter	Wert
Sensortest Kanal 1 aktiv	Nein
Sensortest Kanal 2 aktiv	Nein
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Asynchrone Auswertung OSSD
Logik Kanal 3 und 4	Single Logic

EL1904 (untere Klemme in der Zeichnung)

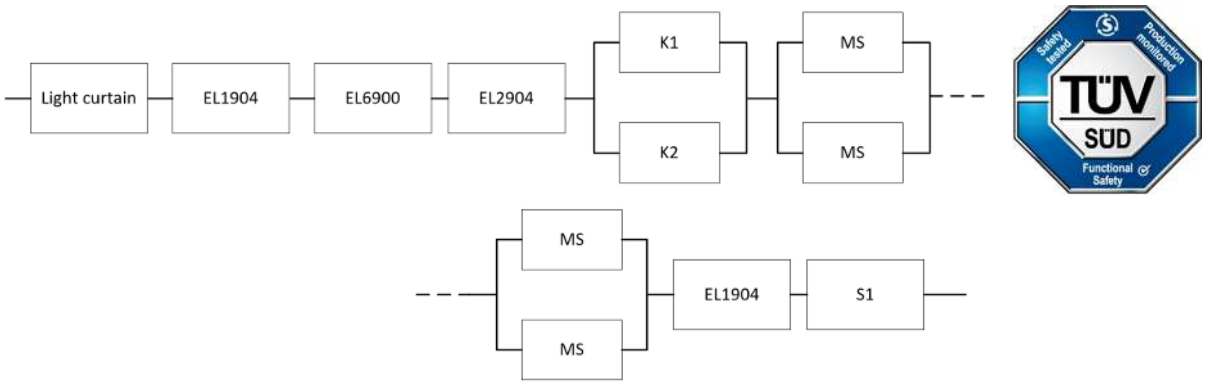
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

4.9.2 Blockbildung und Safety-Loops

4.9.2.1 Sicherheitsfunktion 1



4.9.3 Berechnung

4.9.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	100.000
Lichtvorhang (Light curtain) – PFH_D	1,50E-08
MS1 – $B10_D$	100.000
MS2 – $B10_D$	100.000
MS3 – $B10_D$	100.000
MS4 – $B10_D$	100.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	60 (1x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.9.3.2 Diagnostic Coverage DC

Komponente	Wert
OSSD1/2 mit Testung(durch Lichtvorhang)/ Plausibilität	DC_{avg}=99%

Komponente	Wert
MS1/2/3/4 mit Testung/Plausibilität	DC_{avg}=90%
K1/K2 mit Testung und EDM	DC_{avg}=99%
S1 mit Testung	DC_{avg}=90%

4.9.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

$$n_{op} = \frac{230 * 16 * 60}{60} = 1840$$

$$MTTF_D = \frac{100.000}{0{,}1 * 1840} = 543{,}5y = 4761060h$$

K1/K2:

$$n_{op} = \frac{230 * 16 * 60}{60} = 1840$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 1840} = 7065{,}2y = 61891152h$$

MS1/MS2/MS3/S4:

$$n_{op} = \frac{230 * 16 * 60}{60} = 1840$$

$$MTTF_D = \frac{100.000}{0{,}1 * 1840} = 543{,}5y = 4761060h$$

und der Annahme, dass S1, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

$$PFH = \frac{1 - 0{,}90}{543{,}5 * 8760} = 2{,}10E - 08$$

K1/K2:

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

MS1/MS2/MS3/S4:

$$PFH = \frac{1-0,90}{543,5*8760} = 2,10E-08$$

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da die Anteile $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

$$\begin{aligned}\frac{1}{MTTF_{Dges}} &= \frac{1}{MTTF_{D(Lightcurtain)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} \\ &+ \frac{1}{MTTF_{D(MS1)}} + \frac{1}{MTTF_{D(MS3)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(S1)}}\end{aligned}$$

mit:

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

$$MTTF_{D(Lightcurtain)} = \frac{(1 - DC_{(Lightcurtain)})}{PFH_{(Lightcurtain)}} = \frac{(1 - 0{,}99)}{1{,}50E-08\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}31E-04\frac{1}{y}} = 76{,}1y$$

$$MTTF_{D(MS1/MS3)} = \frac{(1 - DC_{(MS1/MS3)})}{PFH_{(MS1/MS3)}} = \frac{(1 - 0{,}90)}{2{,}10E-08\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}1}{1{,}84E-04\frac{1}{y}} = 543{,}6y$$

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

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

HINWEIS

Kategorie

Diese Struktur ist durch den Einsatz des Typ4 (Kategorie 4) Lichtvorhangs maximal bis Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

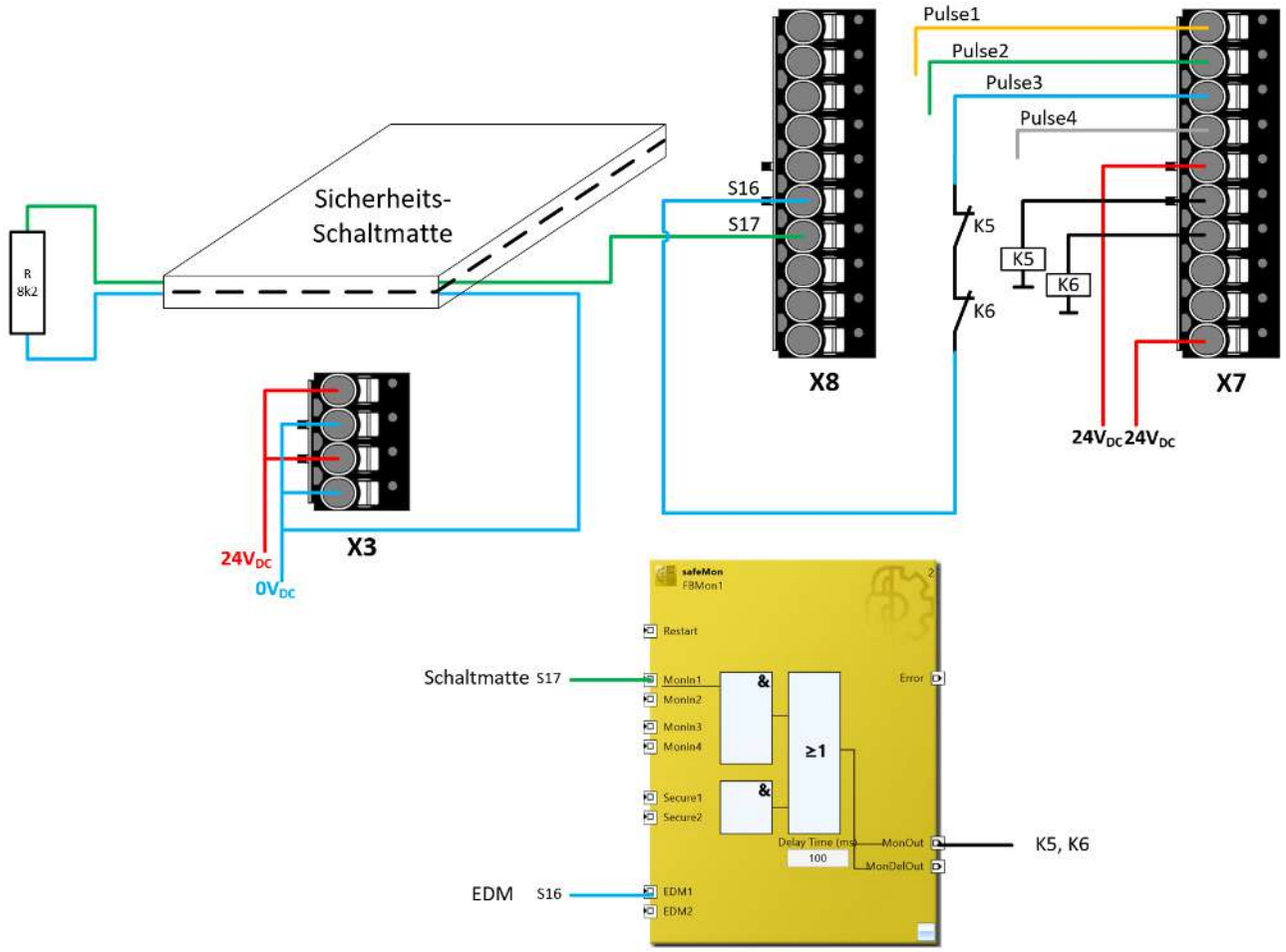
Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

4.10 EK1960 Trittmatten-Eingänge / digitale Ausgänge (Kategorie 2, PL d)

Die Sicherheits-Schaltmatte ist auf den sicheren Eingang S17 (bzw. 8.7) auf dem 10-poligen Stecker X8 verdrahtet. Die erste Ausgangsgruppe auf dem 10-poligen Stecker X7 ist als Taktquelle konfiguriert (bei FSOUT Module 3 ist der Parameter *Diag TestPulse for Inputs active* auf TRUE gesetzt). Für den Eingang S16 ist der Parameter *Channel x.Testpulse Diag Mode* auf die entsprechende Taktquelle konfiguriert.

Die Schütze K5 und K6 sind auf die Ausgänge 7.5 und 7.6 auf dem 2. Ausgangsmodul auf X7 verdrahtet. Der Anschluss A2 der Schütze ist auf die gemeinsame Masse der $24V_{DC}$ Einspeisung des Anschluss X7 verdrahtet. Die Rückführkreise der beiden Schütze sind in Reihe geschaltet von Pulse 3 auf den Eingang S16 (bzw. 8.6) verdrahtet.



⚠ VORSICHT

Verdrahtung Schaltmatte

Es werden nur Schaltmatten unterstützt, die nach dem Prinzip der Widerstandsänderung (Widerstandswert: 8k2) arbeiten. Der Masseanschluss der Schaltmatte muss mit der Masse der EK1960 Versorgungsspannung entsprechend obiger Zeichnung verbunden sein.

4.10.1 Parameter der sicheren Ein- und Ausgangsmodule

EK1960

Parameter	Wert
FSOUT Module 3 (X7.1 – X7.4)	-
8020:01 ModuloDiagTestPulse	0x00

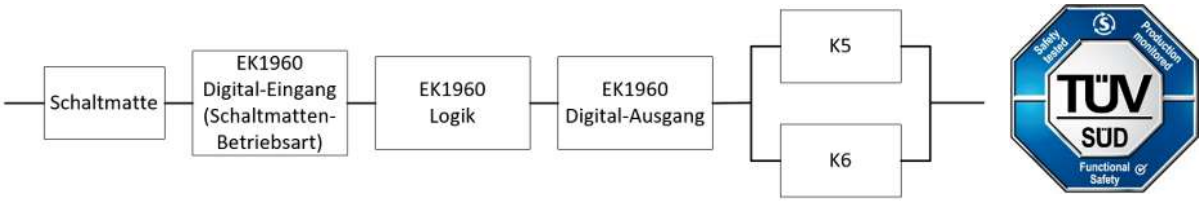
Parameter	Wert
8020:02 MultiplierDiagTestPulse	0x02
8020:03 Standard Outputs active	FALSE
8020:04 Diag Testpulse active	TRUE
8020:05 Diag Testpulse for Inputs active	TRUE
FSOUT Module 4 (X7.5 – X7.8)	**-**
8030:01 ModuloDiagTestPulse	0x00
8030:02 MultiplierDiagTestPulse	0x02
8030:03 Standard Outputs active	FALSE
8030:04 Diag Testpulse active	TRUE
8030:05 Diag Testpulse for Inputs active	FALSE
FSIN Module 8 (X8.5 – X8.6)	**-**
80E1:04 Channel 2.InputFilterTime	0x0014
80E1:05 Channel 2.DiagTestPulseFilterTime	0x0002
80E1:06 Channel 2.Testpulse Diag Mode	(X7.3) Testpulse Detection Output Module 3.Channel 3
FSIN Module 9 (X8.7 – X8.8)	**-**
80F0:03 Input Mode	Bumper Mode Channel 1 (1)
80F1:01 Channel 1.InputFilterTime	0x0014
80F1:02 Channel 1.DiagTestPulseFilterTime	0x0002
80F1:03 Channel 1.Testpulse Diag Mode	External Testpulse (0)

MON FB Parameter

Parameter	Wert
Reset Time (ms) (Port EDM1)	1000

4.10.2 Blockbildung und Safety-Loops

4.10.2.1 Sicherheitsfunktion 1



4.10.3 Berechnung

4.10.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EK1960 Digitaler Eingang – PFH_D	6,40E-11
EK1960 Eingang Trittmatte - PFH_D	8,84E-10
EK1960 Logik – PFH_D	5,18E-09
EK1960 Digitaler Ausgang – PFH_D	1,50E-10
Schaltmatte – $B10_D$	6.000.000
K5 – $B10_D$	1.300.000
K6 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230

Komponente	Wert
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	60 (1x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

Safety-over-EtherCAT Kommunikation

Der PFH_D Wert der Safety-over-EtherCAT (FSoE) Kommunikation ist im PFH_D Wert der EK1960 Logik-Komponente bereits enthalten.

4.10.3.2 Diagnostic Coverage DC

Komponente	Wert
Tritt- bzw. Schaltmatte mit Testung	DC_{avg}=90%
K5/K6 mit EDM-Überwachung (Betätigung 1/Stunde und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) mit Testung	DC_{avg}=99%

4.10.3.3 Berechnung Sicherheitsfunktion 1

Berechnung des Performance Levels nach EN ISO 13849-1:2015:

Berechnung der $MTTF_D$-Werte aus den $B10_D$-Werten.

aus:

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

und:

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

Eingesetzt ergibt das:

Schaltmatte:

$$n_{op} = \frac{230 * 16 * 60}{60} = 3680$$

$$MTTF_{D(SwitchingMat)} = \frac{6.000.000}{0{,}1 * 3680} = 16304y$$

K5/K6:

$$n_{op} = \frac{230 * 16 * 60}{60} = 3680$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 3680} = 3532y$$

Der Gesamt-$MTTF_D$ Wert ergibt sich aus der Formel:

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

als:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(SwitchingMat)}} + \frac{1}{MTTF_{D(EK1960-InputSwitchingMat)}} + \frac{1}{MTTF_{D(EK1960-Logic)}} + \frac{1}{MTTF_{D(EK1960-Output)}} + \frac{1}{MTTF_{D(K5)}}$$

Sind für die EK1960 Komponenten nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EK1960-InputSwitchingMat)} = \frac{(1 - DC_{(EK1960-InputSwitchingMat)})}{PFH_{D(EK1960-InputSwitchingMat)}} = \frac{(1 - 0{,}90)}{8{,}84E-10\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}1}{7{,}74E-06\frac{1}{y}} = 12913y$$

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

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{16304y} + \frac{1}{12913y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{3532y}} = 196y$$

$$DC_{avg} = \frac{\frac{90\%}{16304y} + \frac{90\%}{12913y} + \frac{99\%}{220y} + \frac{99\%}{7610y} + \frac{99\%}{3532y} + \frac{99\%}{3532y}}{\frac{1}{16304y} + \frac{1}{12913y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{3532y} + \frac{1}{3532y}} = 98{,}76\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 2 möglich.

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist **NICHT** Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Berechnung der PFH_D Werte nach EN 62061:

mit der Annahme, dass Schaltmatte, K5 und K6 jeweils einkanalig sind:

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

ergibt sich für

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

Schaltmatte:

$$PFH_D = \frac{1 - 0{,}90}{16304 * 8760} = 7{,}00E - 10$$

K5/K6:

$$PFH_D = \frac{1 - 0{,}99}{3532 * 8760} = 3{,}23E - 10$$

Nun sind folgende Annahmen zu treffen:

Die Relais K5 und K6 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K5 und K6 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

$$PFH_{Dges} = PFH_{D(SwitchingMat)} + PFH_{D(EK1960-InputSwitchingMat)} + PFH_{D(EK1960-Logic)} + PFH_{D(EK1960-Output)} + \beta * \frac{PFH_{D(K5)} + PFH_{D(K6)}}{2} + (1 - \beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$$

Da der Anteil $(1 - \beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$ um Zehnerpotenzen kleiner ist, als der Rest, wird er als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{Dges} = 7{,}00E - 10 + 8{,}84E - 10 + 5{,}18E - 09 + 1{,}50E - 10 + 10\% * \frac{3{,}23E - 10 + 3{,}23E - 10}{2} = 6{,}94E - 09$$

Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	≥ 10-8 bis < 10-7
2	**≥ 10^{-7} bis < 10^{-6}**
1	≥ 10^{-6} bis < 10^{-5}

HINWEIS

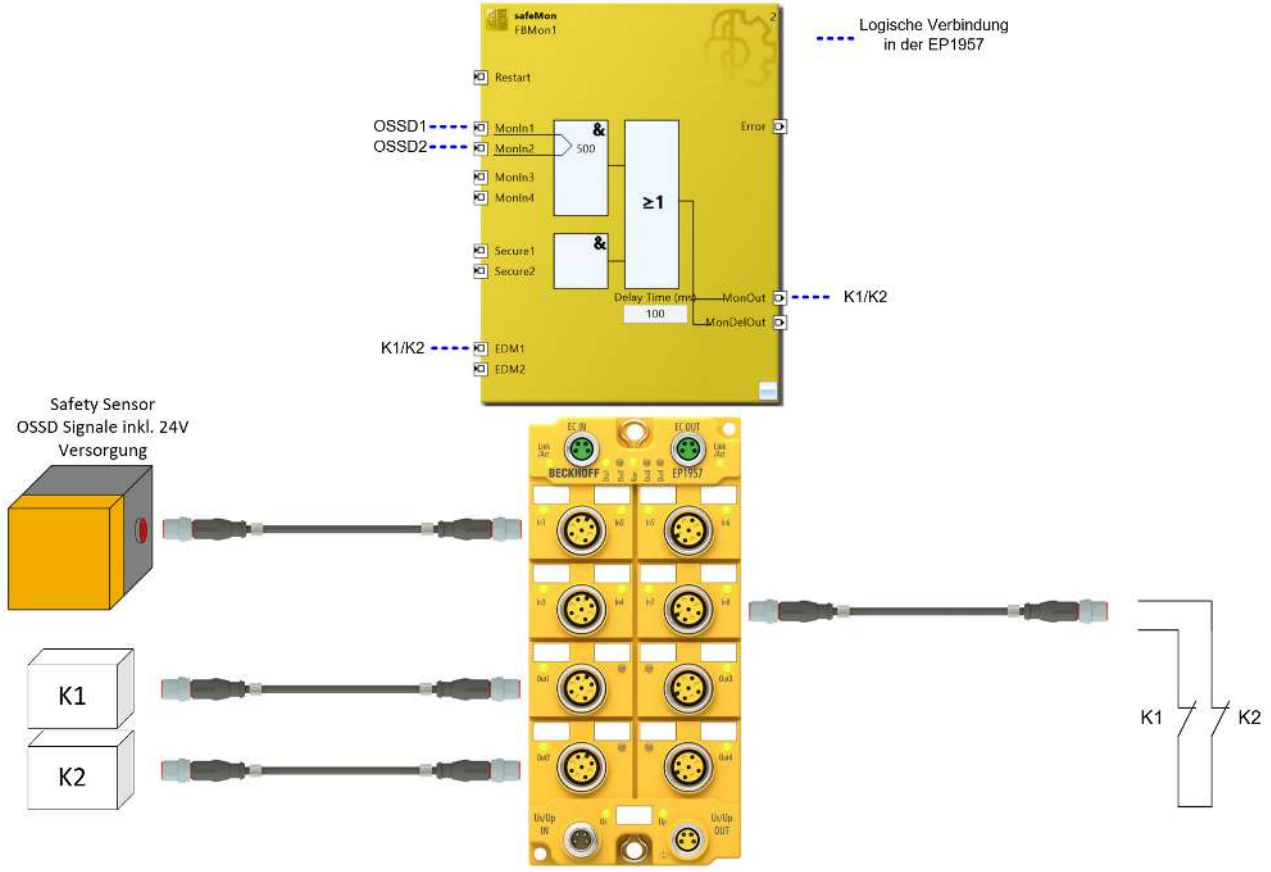
Sicherheits-Integritätslevel

Die Anwendung entspricht einem Sicherheits-Integritätslevel von SIL2 nach EN 62061, da der maximal erreichbare SIL für den Trittmatteneingang auf SIL 2 begrenzt ist.

4.11 EP1957 OSSD Sensor für Schutztür (Kategorie 4, PL e)

Der OSSD Safety Sensor (hier z.B. ein Näherungsschalter mit definiertem Verhalten unter Fehlerbedingungen (PDDB) nach EN 60947-5-3) wird über eine M12 Verbindung an der EP1957 angeschlossen und kann z.B. für eine Schutztür-Anwendung eingesetzt werden. Die Spannungsversorgung liegt auf Pin 1 und 3 des M12 Anschlusses (PowerModeA). Der Sensor prüft die Verdrahtung zwischen Sensor und EP1957 über Testpulse auf den beiden OSSD Kanälen und schaltet im Fehlerfall beide OSSD Signale in den sicheren Zustand. Innerhalb der Logik werden die beiden OSSD Eingänge auf Diskrepanz überwacht.

Entsprechend des Schutztürzustandes werden die beiden Aktoren K1 und K2 geschaltet. Der Rückführkreis der beiden Aktoren wird auf einen sicheren Eingang verdrahtet. Die Testimpulse sind für diesen Eingang eingeschaltet.



4.11.1 Parameter der sicheren Ein- und Ausgangsmodule

EP1957

Parameter	Wert
FSOUT Module 1 Settings Common	-
8000:04 Diag Testpulse active	TRUE
8000:07 Module Fault Link active	TRUE
FSOUT Module 2 Settings Common	-
8010:04 Diag Testpulse active	TRUE
8010:07 Module Fault Link active	TRUE
FSIN Module 1 Settings Common	-
8040:04 Diag Testpulse active	FALSE
8040:05 Module Fault Link active	TRUE
8040:0C Input Power Mode	PowerMode A: Pin1(+) / Pin3(-)
FSIN Module 1 Settings Channel	-

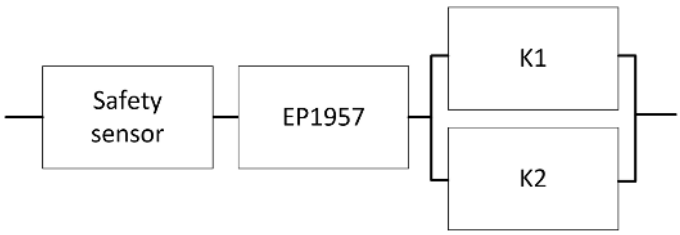
Parameter	Wert
8041:01 Channel 1.InputFilterTime	0x000A (1ms)
8041:02 Channel 1.DiagTestPulseFilterTime	0x0002 (0,2ms)
8041:04 Channel 2.InputFilterTime	0x000A (1ms)
8041:05 Channel 2.DiagTestPulseFilterTime	0x0002 (0,2ms)
FSIN Module 4 Settings Common	**-**
8070:04 Diag Testpulse active	TRUE
8070:05 Module Fault Link active	TRUE
8070:0C Input Power Mode	Diag TestPulse
FSIN Module 4 Settings Channel	**-**
8071:01 Channel 1.InputFilterTime	0x000A (1ms)
8071:02 Channel 1.DiagTestPulseFilterTime	0x0002 (0,2ms)

MON FB Parameter

Parameter	Wert
Reset Time (ms) (Port EDM1)	1000
Discrepancy Time (ms) (Port MonIn1/MonIn2)	500
Safe Inputs After Disc Error	TRUE

4.11.2 Blockbildung und Safety-Loops

4.11.2.1 Sicherheitsfunktion 1



4.11.3 Berechnung

4.11.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EP1957 – PFH_D	6,50E-09
Safety Sensor – PFH_D (zertifiziert nach EN 60947-5-3 und EN ISO 13849)	1,00E-08 (Kat. 4 / PL e)
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

4.11.3.2 Diagnostic Coverage DC

Komponente	Wert
Safety Sensor mit OSSD Ausgängen	DC_{avg}=99%
K1/K2 mit Testung und EDM	DC_{avg}=99%

4.11.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

K1/K2:

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

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

K1/K2

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

Nun sind folgende Annahmen zu treffen:

Die Schütze K1 und K2 sind alle an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Schützes führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Schütz-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

$$PFH_{ges} = PFH_{(SafetySensor)} + PFH_{(EP1957)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{ges} = 1,00E-08 + 6,50E-09 + 10\% * \frac{6,46E-10 + 6,46E-10}{2}$$
$$= 1,66E-08$$

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(SafetySensor)}} + \frac{1}{MTTF_{D(EP1957)}} + \frac{1}{MTTF_{D(K1)}}$$

Sind für EP1957 und Safety Sensor nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EP1957)} = \frac{(1-DC_{(EP1957)})}{PFH_{(EP1957)}} = \frac{(1-0,99)}{6,50E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{5,69E-05\frac{1}{y}} = 175y$$

$$MTTF_{D(SafetySensor)} = \frac{(1-DC_{(SafetySensor)})}{PFH_{(SafetySensor)}} = \frac{(1-0,99)}{1,00E-08\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{8,76E-05\frac{1}{y}} = 114y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{114y} + \frac{1}{175y} + \frac{1}{1766,3y}} = 66y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(SafetySensor)}} + \frac{DC}{MTTF_{D(EP1957)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(SafetySensor)}} + \frac{1}{MTTF_{D(EP1957)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{114y} + \frac{99\%}{175y} + \frac{99\%}{1766,3y} + \frac{99\%}{1766,3y}}{\frac{1}{114y} + \frac{1}{175y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 99,00\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %

DC	
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	**≥ 10^{-8} bis < 10^{-7}**
2	≥ 10^{-7} bis < 10^{-6}
1	≥ 10^{-6} bis < 10^{-5}

HINWEIS

Sicherheits-Integritätslevel

Die Anwendung entspricht einem Sicherheits-Integritätslevel von SIL3 nach EN 62061.

5 Potentialgruppen

5.1 Allpolige Abschaltung einer Potentialgruppe mit nachgeschalteten rückwirkungsfreien Standardklemmen (Kategorie 4, PL e)

Die Schutztür verwendet eine Kombination von Öffner und Schließer auf sicheren Eingängen einer EL1904. Die Testung der Eingänge ist aktiv und die Signale werden auf Diskrepanz (200 ms) überprüft. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.

Die Diagnose Information der KL/EL9110 (24 V liegen an den Powerkontakten an) wird negiert und zusammen mit den Rückführsignalen der Schütze K1, K2, K3 und K4 UND verknüpft auf den EDM-Eingang gelegt.

Mit den Arbeitskontakten der Schütze K1 und K2 wird die Versorgung der Powerkontakte (24 V und auch 0 V) der Potentialgruppe abgeschaltet. Die 0 V Potentiale der verwendeten Last (hier: K3 und K4) müssen immer auf die Potentialgruppe zurückgeführt werden.

HINWEIS

Sicherheitsbetrachtung

Die verwendeten Klemmen EL/KL9110 und EL/KL2xxx sind kein aktiver Teil der Sicherheitssteuerung. Dementsprechend ist der erreichte Sicherheitslevel nur durch die überlagerte Sicherheitssteuerung definiert. Die Standardklemmen werden **nicht** in die Berechnung mit einbezogen.
Die externe Beschaltung der Standardklemmen kann zu Einschränkungen des maximal erreichbaren Sicherheitslevels führen.

HINWEIS

Voraussetzungen Netzteil

Zur Versorgung der Standardklemmen mit 24 V muss ein SELV/PELV-Netzteil mit einer ausgangsseitigen Spannungsbegrenzung auf U_{max} = 60 V im Fehlerfall verwendet werden.

⚠ VORSICHT

Verhinderung der Rückspeisung

Die Rückspeisung kann durch unterschiedliche Maßnahmen verhindert werden (siehe weitere Hinweise untenstehend):

- Kein Schalten von Lasten mit separater Spannungsversorgung
- Masserückführung und allpolige Abschaltung **(hier im Beispiel verwendet)**
  oder
  Fehlerausschluss Leitungskurzschluss (separate Mantelleitung, Verdrahtung nur Schaltschrank-intern, eigene Erdverbindung pro Leiter)

HINWEIS

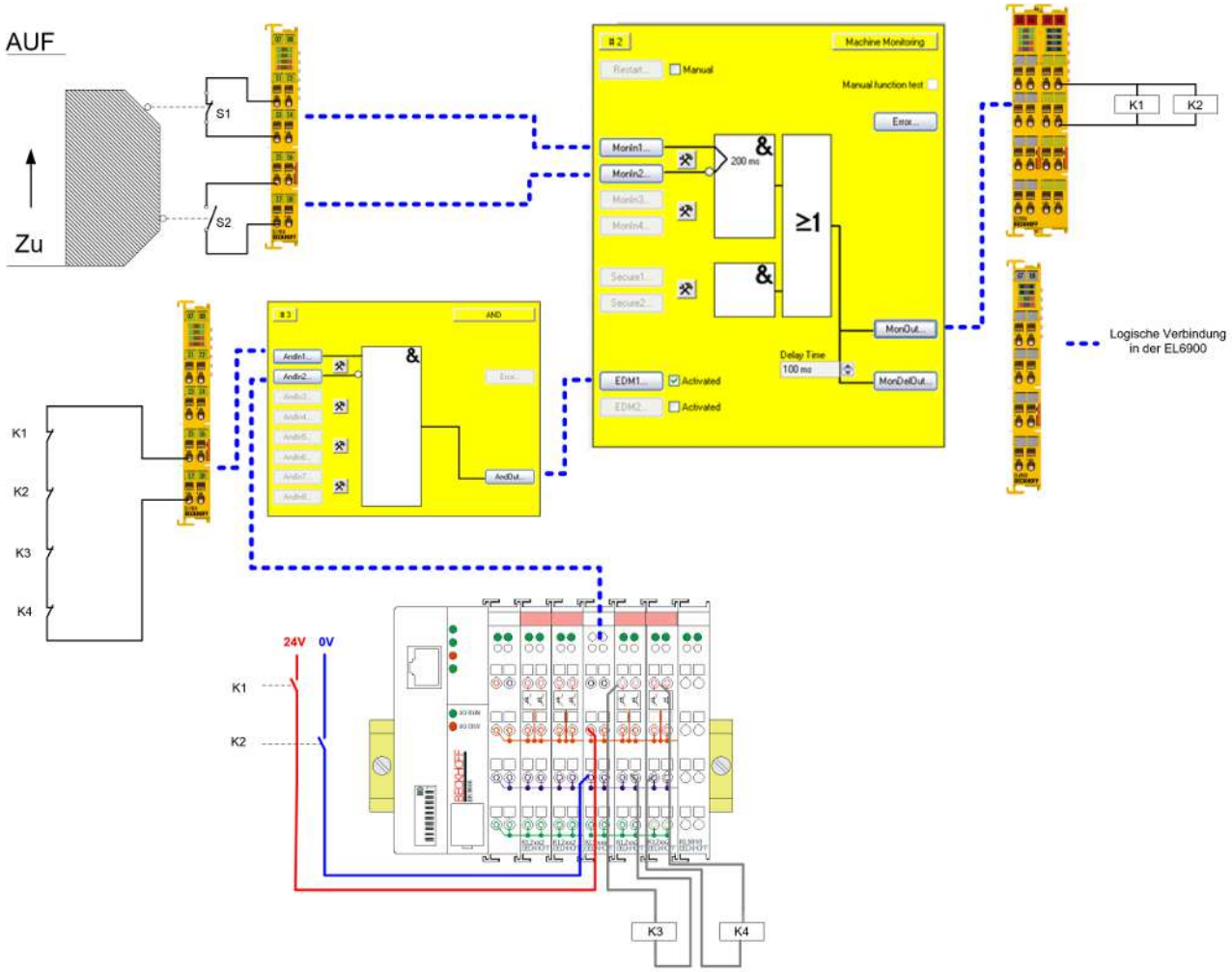
Rückwirkungsfreie Busklemmen

Eine Liste der rückwirkungsfreien Busklemmen finden Sie im Beckhoff Information System unter http://infosys.beckhoff.de.

HINWEIS

Maximal erreichbare Sicherheitslevel

Rückspeisung durch Masserückführung und allpolige Abschaltung vermieden:
DIN EN ISO 13849-1: max. Kat. 4 PL e
IEC 61508: max. SIL3
EN 62061: max. SIL3



⚠ VORSICHT

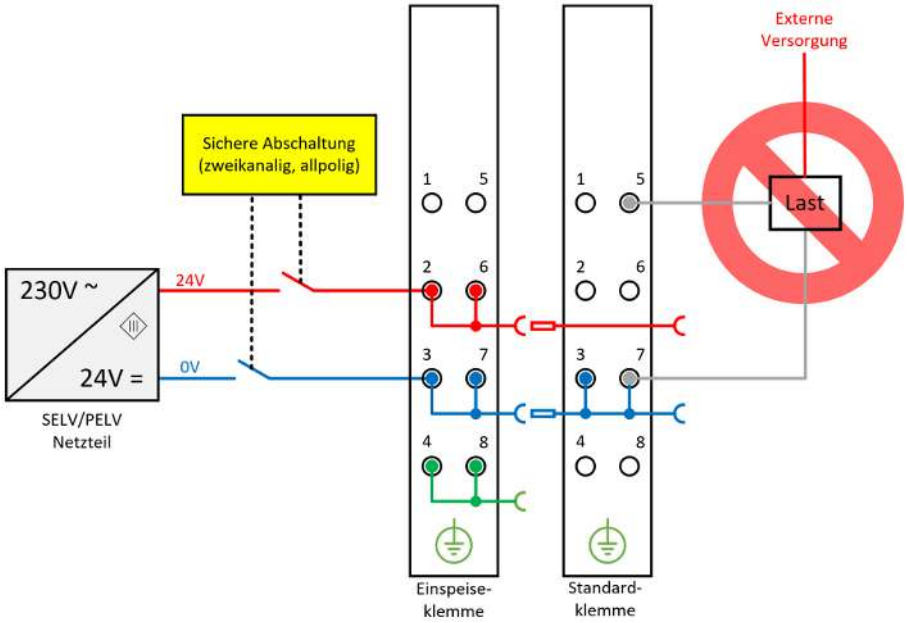
Zeitliche Verzögerung

Durch das Abschalten der Spannungsversorgung der Potentialgruppe, kann sich die Abschaltung der nachgeschalteten Schütze und Aktoren verzögern. Diese Verzögerung ist abhängig von den nachgeschalteten Aktoren, Verbrauchern und Leitungen und ist durch den Anwender in der Sicherheitsbetrachtung zu berücksichtigen.

5.1.1 Hinweise zur Verhinderung der Rückspeisung

5.1.1.1 Kein Schalten von Lasten mit separater Spannungsversorgung

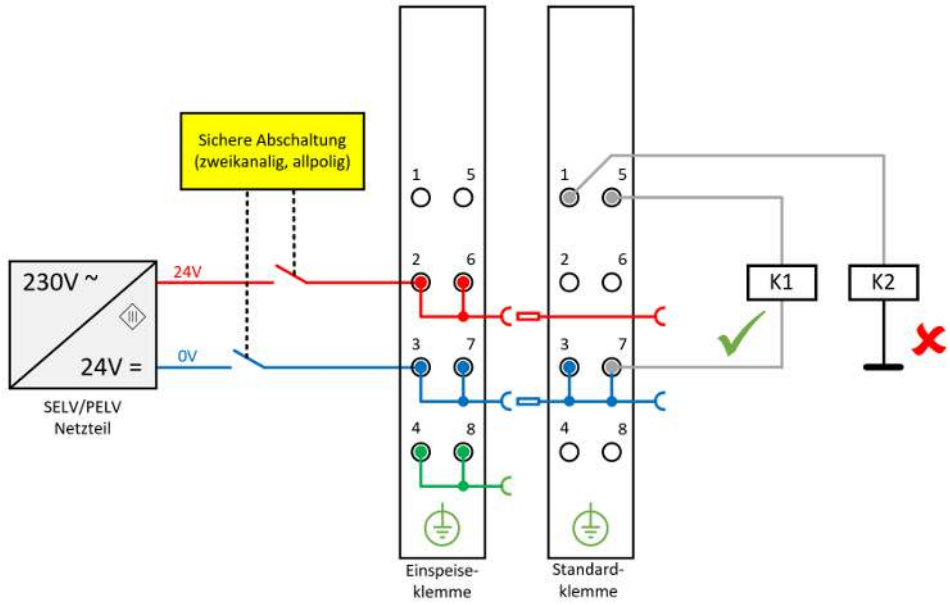
Es dürfen keine Lasten durch Standardklemmen geschaltet werden, die über eine eigene Spannungsversorgung verfügen, da hier eine Rückspeisung durch die Last nicht ausgeschlossen werden kann.



Ausnahmen von der allgemeinen Anforderung sind nur erlaubt, wenn der Hersteller der angeschlossenen Last garantiert, dass es zu keiner Rückspeisung auf den Ansteuerausgang kommen kann.

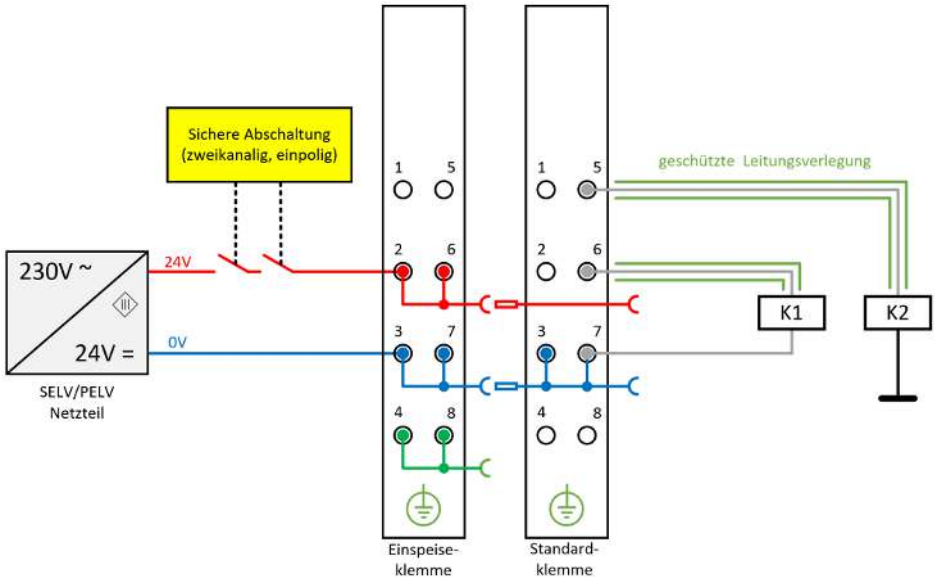
5.1.1.2 Option 1: Masserückführung und allpolige Abschaltung (hier im Beispiel verwendet)

Die Masseverbindung der angeschlossenen Last muss auf die sicher geschaltete Masse der jeweiligen Ausgangsklemme bzw. Potentialgruppe zurückgeführt werden. (Hier: K1 – richtige Verdrahtung, K2 – falsche Verdrahtung)



5.1.1.3 Option 2: Fehlerausschluss Leitungskurzschluss

Ist Option 1 nicht umsetzbar kann auch auf die Masserückführung und allpolige Abschaltung verzichtet werden, wenn die Gefahr der Rückspeisung aufgrund eines Leitungskurzschlusses durch weitere Maßnahmen ausgeschlossen werden kann. Die folgenden Maßnahmen können alternativ umgesetzt werden.



Alternative 1:	Lastanschluss durch separate Mantelleitungen Das nicht sicher geschaltete Potential der Standardklemme darf nicht zusammen mit anderen potentialführenden Leitungen in derselben Mantelleitung geführt werden
Alternative 2:	Verdrahtung nur Schaltschrank-intern Alle an die nicht sicheren Standardklemmen angeschlossenen Lasten müssen sich im selben Schaltschrank wie die Klemmen befinden. Die Leitungsverlegung verbleibt vollkommen innerhalb des Schaltschrankes.
Alternative 3:	Eigene Erdverbindung pro Leiter Alle an die nicht sicheren Standardklemmen angeschlossenen Leiter sind durch eine eigene Erdverbindung geschützt.
Alternative 4:	Verdrahtung dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt Alle an die nicht sicheren Standardklemmen angeschlossenen Leiter sind dauerhaft fest verlegt und z.B. durch einen Kabelkanal oder Panzerrohr gegen äußere Beschädigung geschützt.

⚠ VORSICHT

Fehlerausschluss

Für die korrekte Ausführung und Bewertung der angewendeten Alternativen ist der Maschinenbauer bzw. Anwender allein verantwortlich.

5.1.2 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

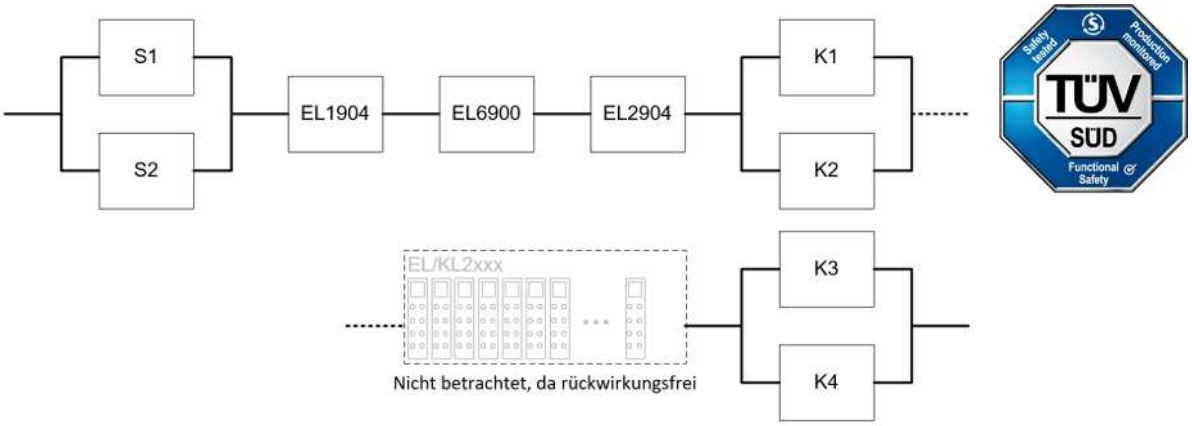
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

5.1.3 Blockbildung und Safety-Loops

5.1.3.1 Sicherheitsfunktion 1



5.1.4 Berechnung

5.1.4.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
K3 – $B10_D$	1.300.000
K4 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

5.1.4.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
K1/K2 mit Testung und EDM	DC_{avg}=99%

Komponente	Wert
K3/K4 mit EDM	DC_{avg}=90%

5.1.4.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7y = 11902212h$$

S2:

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

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4y = 23804424h$$

K1/K2/K3/K4:

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

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

und der Annahme, dass S1, S2, K1, K2, K3 und K4 jeweils einkanalig sind:

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

ergibt sich für

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

S1

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

S2

$$PFH = \frac{1 - 0{,}99}{2717{,}4 * 8760} = 4{,}20E - 10$$

K1/K2

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

K3/K4

$$PFH = \frac{1-0,90}{1766,3*8760} = 6,46E-09$$

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Die Schütze K1, K2, K3 und K4 sind alle an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Schützes führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1, K2, K3 und K4 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Schütz-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1-\beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{ges} = 10\% * \frac{8,40E-10 + 4,20E-10}{2} + 1,11E-09 + 1,03E-09 + 1,25E-09$$
$$+10\% * \frac{6,46E-10 + 6,46E-10}{2} + 10\% * \frac{6,46E-09 + 6,46E-09}{2}$$
$$= 4,16E-09$$

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K3)}}$$

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	**≥ 10^{-8} bis < 10^{-7}**
2	≥ 10^{-7} bis < 10^{-6}
1	≥ 10^{-6} bis < 10^{-5}

5.2 Einpolige Abschaltung einer Potentialgruppe mit nachgeschalteten rückwirkungsfreien Standardklemmen mit Fehlerausschluss (Kategorie 4, PL e)

Die Schutztür verwendet eine Kombination von Öffner und Schließer auf sicheren Eingängen einer EL1904. Die Testung der Eingänge ist aktiv und die Signale werden auf Diskrepanz (hier 200 ms) überprüft. An dem sicheren Ausgang werden die Schütze K1 und K2 parallel angeschlossen. Für diese Beschaltung sind die Strommessung und die Testung des Ausgangs aktiv.
Die Rückführsignale der Schütze K1, K2, K3 und K4 werden auf den EDM-Eingang gelegt.

Mit den Arbeitskontakten der Schütze K1 und K2 wird nur die 24 V Versorgung der Powerkontakte der Potentialgruppe abgeschaltet. Der 0 V Anschluss der Powerkontakte wird direkt auf die 0 V der Spannungsversorgung zurückgeführt.

Die 0 V Potentiale aller verwendeten Lasten und Geräte müssen auf demselben Potential liegen bzw. verbunden sein.

HINWEIS

Sicherheitsbetrachtung

Die verwendeten Klemmen EL/KL9110 und EL/KL2xxx sind kein aktiver Teil der Sicherheitssteuerung. Dementsprechend ist der erreichte Sicherheitslevel nur durch die überlagerte Sicherheitssteuerung definiert. Die Standardklemmen werden **nicht** in die Berechnung mit einbezogen.
Die externe Beschaltung der Standardklemmen kann zu Einschränkungen des maximal erreichbaren Sicherheitslevels führen.

HINWEIS

Voraussetzungen Netzteil

Zur Versorgung der Standardklemmen mit 24 V muss ein SELV/PELV-Netzteil mit einer ausgangsseitigen Spannungsbegrenzung auf U_{max} = 60 V im Fehlerfall verwendet werden.

⚠ VORSICHT

Verhinderung der Rückspeisung

Die Rückspeisung kann durch unterschiedliche Maßnahmen verhindert werden (siehe weitere Hinweise untenstehend):

- Kein Schalten von Lasten mit separater Spannungsversorgung
- Masserückführung und allpolige Abschaltung
  oder
  Fehlerausschluss Leitungskurzschluss (separate Mantelleitung, Verdrahtung nur Schaltschrank-intern, eigene Erdverbindung pro Leiter)
  (hier im Beispiel verwendet)

HINWEIS

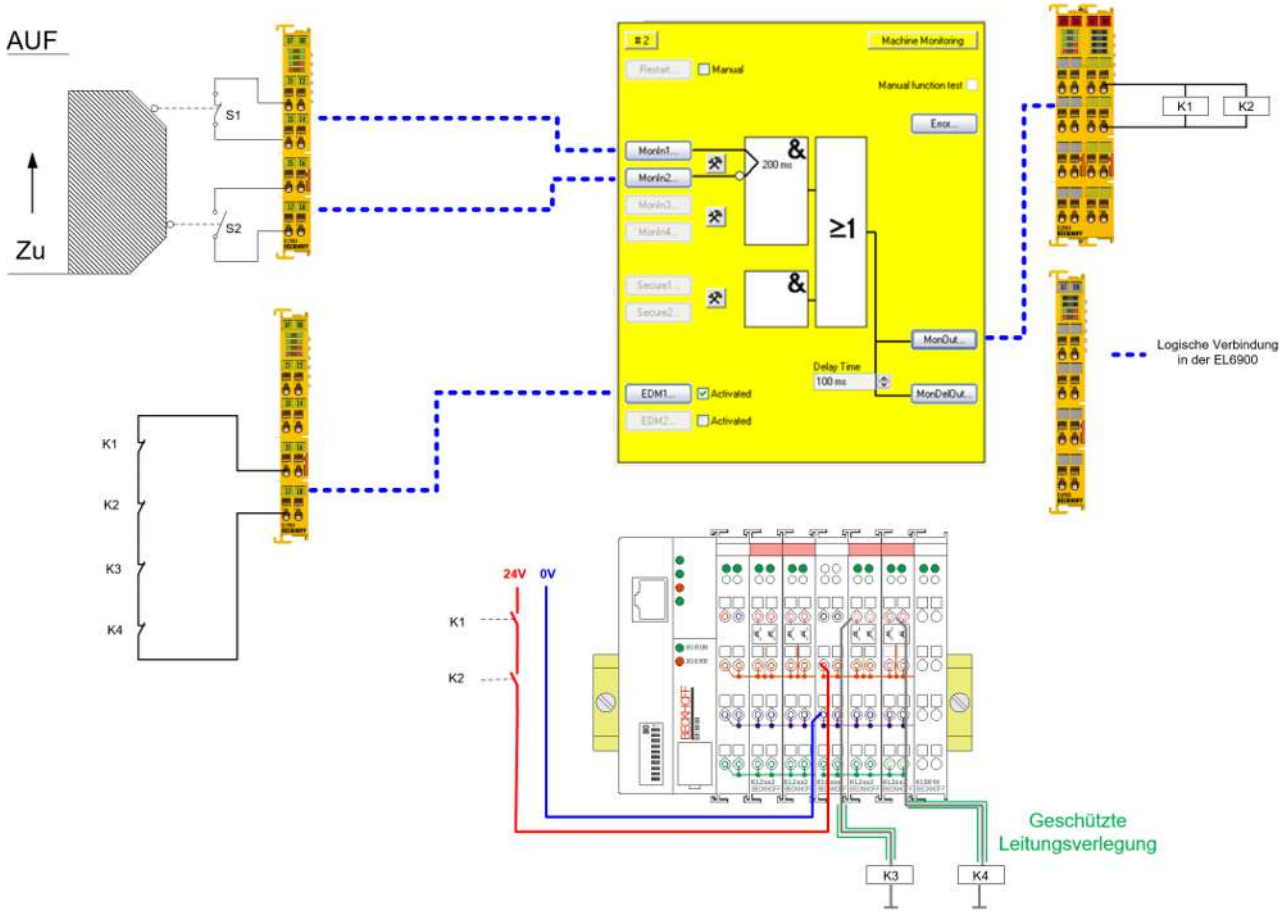
Rückwirkungsfreie Busklemmen

Eine Liste der rückwirkungsfreien Busklemmen finden Sie im Beckhoff Information System unter http://infosys.beckhoff.de.

HINWEIS

Maximal erreichbare Sicherheitslevel

Rückspeisung durch Fehlerausschluss Leitungskurzschluss vermieden:
DIN EN ISO 13849-1: max. Kat. 4 PL e
IEC 61508: max. SIL3
EN 62061: max. SIL2



HINWEIS

Fehlerausschluss

Aufgrund des Fehlerausschlusses „Leitungskurzschluss“ in der Verdrahtung von den rückwirkungsfreien Standard Ausgangsklemmen EL/KL2xxx bis zur Last (hier K3, K4), kann auf eine Einspeiseklemme mit Diagnosefunktion verzichtet werden. Somit können Einspeiseklemmen vom Typ EL/KL9xxx verwendet werden.
Die 0 V Potentiale der Last (hier K3, K4) müssen identisch zum 0 V Potential der Spannungsversorgung der Potentialgruppe sein.

⚠ VORSICHT

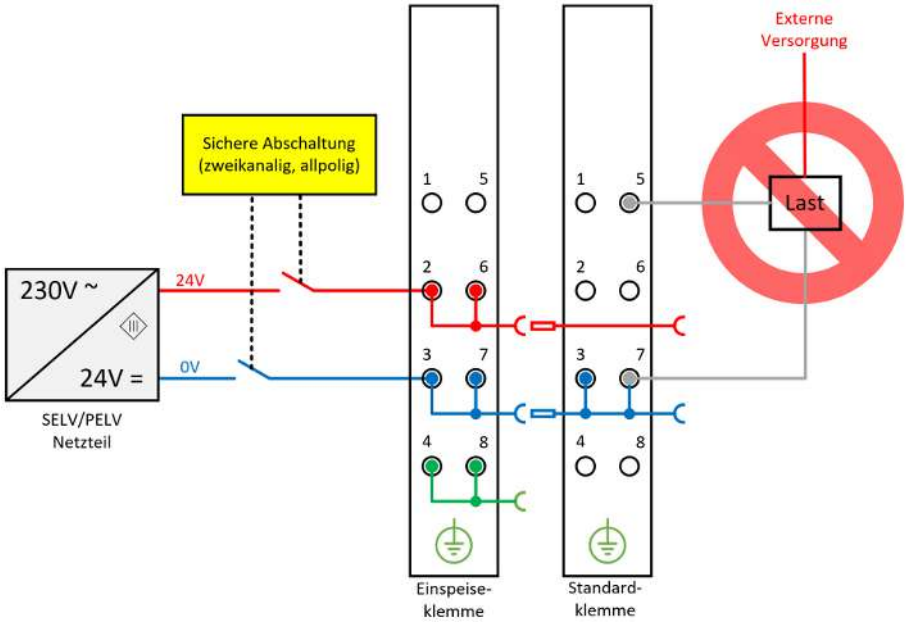
Zeitliche Verzögerung

Durch das Abschalten der Spannungsversorgung der Potentialgruppe, kann sich die Abschaltung der nachgeschalteten Schütze und Aktoren verzögern. Diese Verzögerung ist abhängig von den nachgeschalteten Aktoren, Verbrauchern und Leitungen und ist durch den Anwender in der Sicherheitsbetrachtung zu berücksichtigen.

5.2.1 Hinweise zur Verhinderung der Rückspeisung

5.2.1.1 Kein Schalten von Lasten mit separater Spannungsversorgung

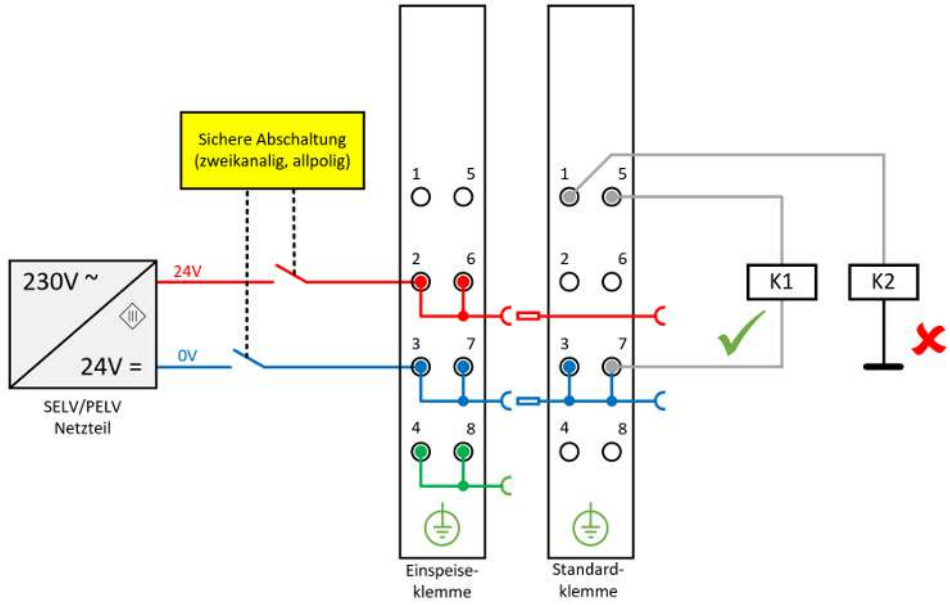
Es dürfen keine Lasten durch Standardklemmen geschaltet werden, die über eine eigene Spannungsversorgung verfügen, da hier eine Rückspeisung durch die Last nicht ausgeschlossen werden kann.



Ausnahmen von der allgemeinen Anforderung sind nur erlaubt, wenn der Hersteller der angeschlossenen Last garantiert, dass es zu keiner Rückspeisung auf den Ansteuereingang kommen kann.

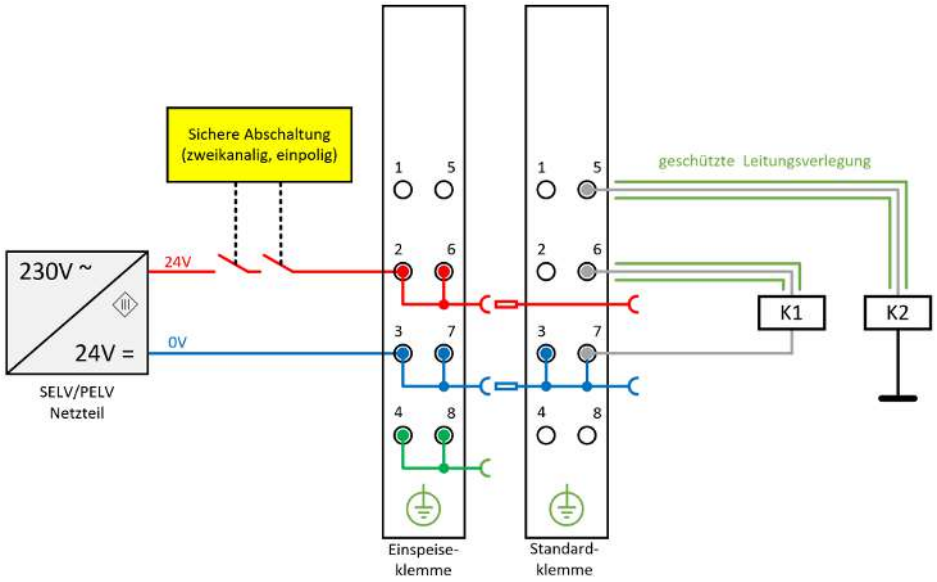
5.2.1.2 Option 1: Masserückführung und allpolige Abschaltung

Die Masseverbindung der angeschlossenen Last muss auf die sicher geschaltete Masse der jeweiligen Ausgangsklemme bzw. Potentialgruppe zurückgeführt werden. (Hier: K1 – richtige Verdrahtung, K2 – falsche Verdrahtung)



5.2.1.3 Option 2: Fehlerausschluss Leitungskurzschluss (hier im Beispiel verwendet)

Ist Option 1 nicht umsetzbar kann auch auf die Masserückführung und allpolige Abschaltung verzichtet werden, wenn die Gefahr der Rückspeisung aufgrund eines Leitungskurzschlusses durch weitere Maßnahmen ausgeschlossen werden kann. Die folgenden Maßnahmen können alternativ umgesetzt werden.



Alternative 1:	Lastanschluss durch separate Mantelleitungen Das nicht sicher geschaltete Potential der Standardklemme darf nicht zusammen mit anderen potentialführenden Leitungen in derselben Mantelleitung geführt werden
Alternative 2:	Verdrahtung nur Schaltschrank-intern Alle an die nicht sicheren Standardklemmen angeschlossenen Lasten müssen sich im selben Schaltschrank wie die Klemmen befinden. Die Leitungsverlegung verbleibt vollkommen innerhalb des Schaltschrankes.
Alternative 3:	Eigene Erdverbindung pro Leiter Alle an die nicht sicheren Standardklemmen angeschlossenen Leiter sind durch eine eigene Erdverbindung geschützt.
Alternative 4:	Verdrahtung dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt Alle an die nicht sicheren Standardklemmen angeschlossenen Leiter sind dauerhaft fest verlegt und z.B. durch einen Kabelkanal oder Panzerrohr gegen äußere Beschädigung geschützt.

⚠ VORSICHT

Fehlerausschluss

Für die korrekte Ausführung und Bewertung der angewendeten Alternativen ist der Maschinenbauer bzw. Anwender allein verantwortlich.

5.2.2 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja

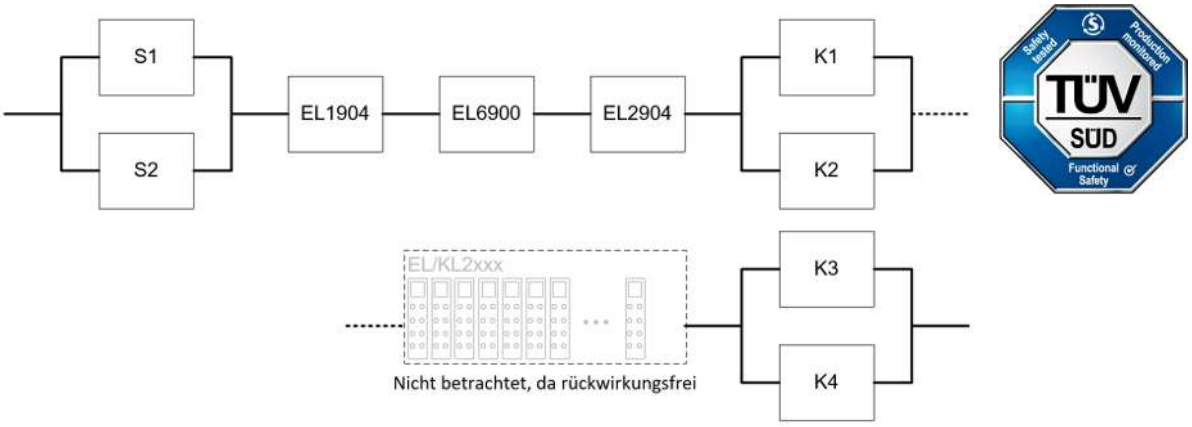
Parameter	Wert
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

5.2.3 Blockbildung und Safety-Loops

5.2.3.1 Sicherheitsfunktion 1



5.2.4 Berechnung

5.2.4.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
K3 – $B10_D$	1.300.000
K4 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

5.2.4.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
K1/K2 mit Testung und EDM	DC_{avg}=99%
K3/K4 mit EDM	DC_{avg}=90%

5.2.4.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7y = 11902212h$$

S2:

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

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4y = 23804424h$$

K1/K2/K3/K4:

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

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

und der Annahme, dass S1, S2, K1, K2, K3 und K4 jeweils einkanalig sind:

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

ergibt sich für

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

S1

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

S2

$$PFH = \frac{1-0,99}{2717,4*8760} = 4,20E-10$$

K1/K2

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

K3/K4

$$PFH = \frac{1-0,90}{1766,3*8760} = 6,46E-09$$

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Die Schütze K1, K2, K3 und K4 sind alle an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Schützes führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1, K2, K3 und K4 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Schütz-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1-\beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{ges} = 10\% * \frac{8,40E-10 + 4,20E-10}{2} + 1,11E-09 + 1,03E-09 + 1,25E-09$$
$$+10\% * \frac{6,46E-10 + 6,46E-10}{2} + 10\% * \frac{6,46E-09 + 6,46E-09}{2}$$
$$= 4,16E-09$$

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K3)}}$$

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2(*)	**≥ 10^{-7} bis < 10^{-6}**
1	≥ 10^{-6} bis < 10^{-5}

(*) Entsprechend der EN 62061 Kapitel 6.7.7.2 ist für ein Teilsystem, das eine HFT von 0 besitzt und für das Fehlerausschlüsse zu Fehlern, die zu einem gefahrbringenden Ausfall führen können, angewendet worden sind, die SILCL in Bezug auf strukturelle Einschränkungen für das Teilsystem auf ein Maximum von SIL2 beschränkt.

5.3 EL2911 Potentialgruppe mit rückwirkungsfreien Standardklemmen (Kategorie 4, PL e)

Die Schutztür verwendet eine Kombination von Öffner und Schließer und wird auf sichere Eingänge der EL2911 verdrahtet. Die Testung der Eingänge ist aktiv und die Signale werden auf Diskrepanz (hier z.B. 500 ms) überprüft. An dem sicheren Ausgang wird die 24 V Versorgung der Powerkontakte der Potentialgruppe abgeschaltet. Der 0 V Anschluss der Powerkontakte wird direkt auf die 0 V der Spannungsversorgung der EL2911 zurückgeführt.

Die EL2911 überwacht eine Rückspeisung auf die 24 V_{DC} der Powerkontakte und geht in einen Modul-Fehler, sobald im ausgeschalteten Zustand eine Spannung höher als 5 V gelesen wird.

Der Rückführkreis der Schütze K3 und K4 wird auf einen sicheren Eingang der EL2911 gelegt.

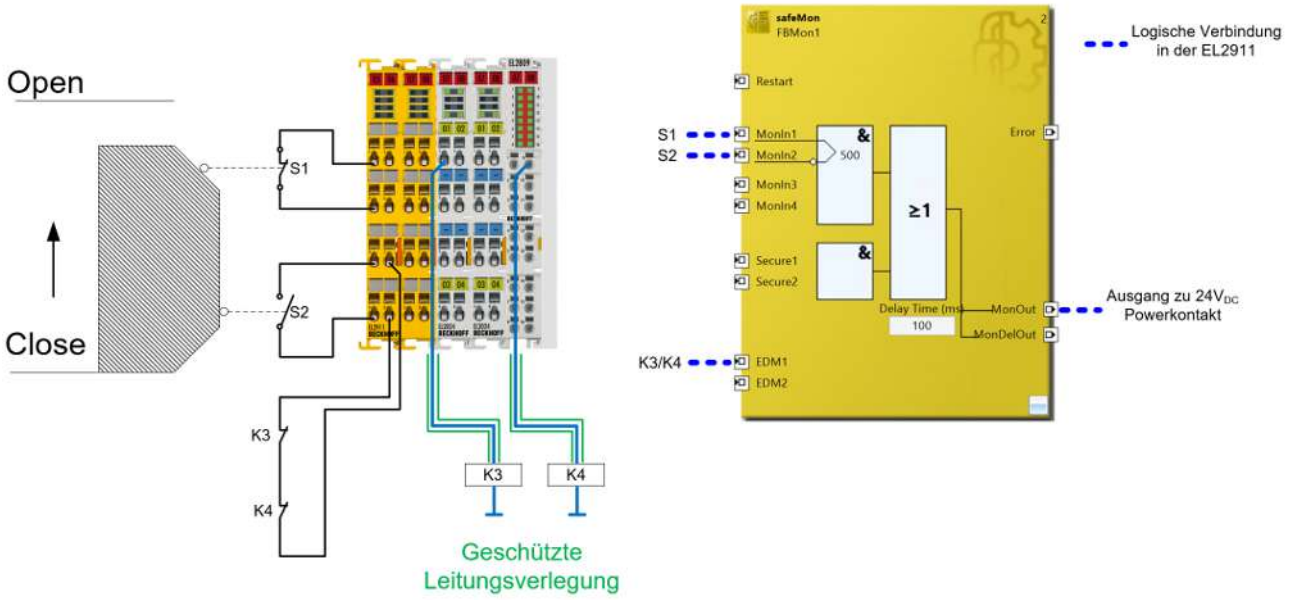
Die 0 V Potentiale aller verwendeten Lasten und Geräte müssen auf demselben Potential liegen bzw. verbunden sein.

HINWEIS

Sicherheitsbetrachtung

Die verwendeten Klemmen EL2xxx sind kein aktiver Teil der Sicherheitssteuerung. Dementsprechend ist der erreichte Sicherheitslevel nur durch die überlagerte Sicherheitssteuerung definiert. Die Standardklemmen werden **nicht** in die Berechnung mit einbezogen, müssen jedoch rückwirkungsfrei sein.

Die externe Beschaltung der Standardklemmen kann zu Einschränkungen des maximal erreichbaren Sicherheitslevels führen.



⚠ VORSICHT

Voraussetzungen Netzteil

Zur Versorgung der Standardklemmen mit 24 V_{DC} muss ein SELV/PELV-Netzteil mit einer ausgangsseitigen Spannungsbegrenzung auf U_{max} = 36 V im Fehlerfall verwendet werden.

⚠ VORSICHT

Verhinderung der Rückspeisung

Die Rückspeisung kann durch unterschiedliche Maßnahmen verhindert werden (siehe weitere Hinweise untenstehend):

- Kein Schalten von Lasten mit separater Spannungsversorgung
- Fehlerausschluss Leitungskurzschluss (separate Mantelleitung, Verdrahtung nur Schaltschrank-intern, eigene Erdverbindung pro Leiter, feste Verlegung)

⚠ VORSICHT

Rückwirkungsfreie EtherCAT-Klemmen

Es dürfen in der durch die EL2911 geschalteten Potentialgruppe nur rückwirkungsfreie Standard-Klemmen verwendet werden. Eine Liste der rückwirkungsfreien EtherCAT-Klemmen finden Sie im Beckhoff Information System unter http://infosys.beckhoff.de.

⚠ VORSICHT

Maximal erreichbare Sicherheitslevel

Rückspeisung durch Fehlerausschluss Leitungskurzschluss vermieden:
DIN EN ISO 13849-1: max. Kat. 4 PL e
IEC 61508: max. SIL3
EN 62061: max. SIL2

⚠ VORSICHT

Potential 0V

Die 0 V Potentiale der Last (hier K3, K4) müssen identisch zum 0 V Potential der Spannungsversorgung der EL2911 sein.

⚠ VORSICHT

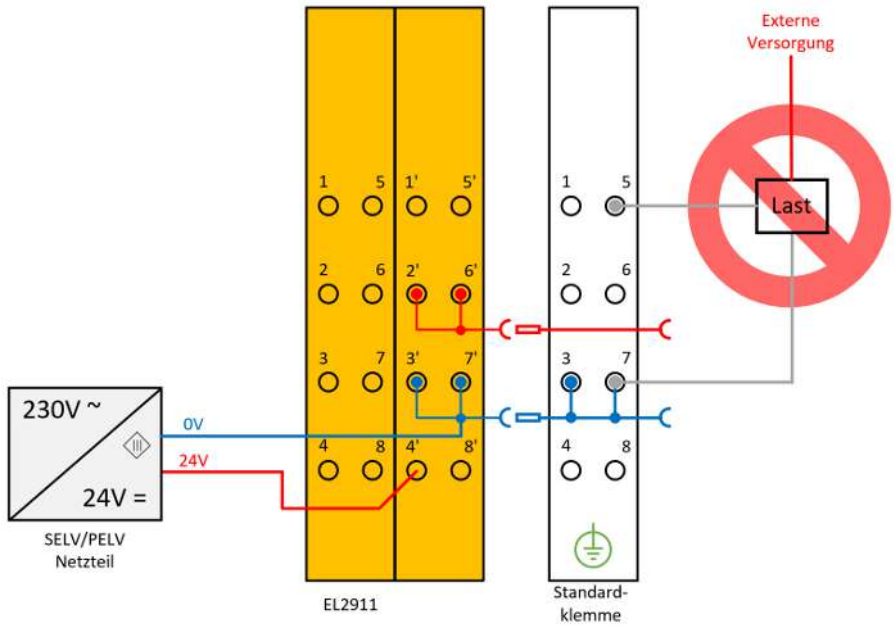
Zeitliche Verzögerung

Durch das Abschalten der Spannungsversorgung der Potentialgruppe, kann sich die Abschaltung der nachgeschalteten Schütze und Aktoren verzögern. Diese Verzögerung ist abhängig von den nachgeschalteten Aktoren, Verbrauchern und Leitungen und ist durch den Anwender in der Sicherheitsbetrachtung zu berücksichtigen.

5.3.1 Hinweise zur Verhinderung der Rückspeisung

5.3.1.1 Kein Schalten von Lasten mit separater Spannungsversorgung

Es dürfen keine Lasten durch Standardklemmen geschaltet werden, die über eine eigene Spannungsversorgung verfügen, da hier eine Rückspeisung durch die Last nicht ausgeschlossen werden kann.



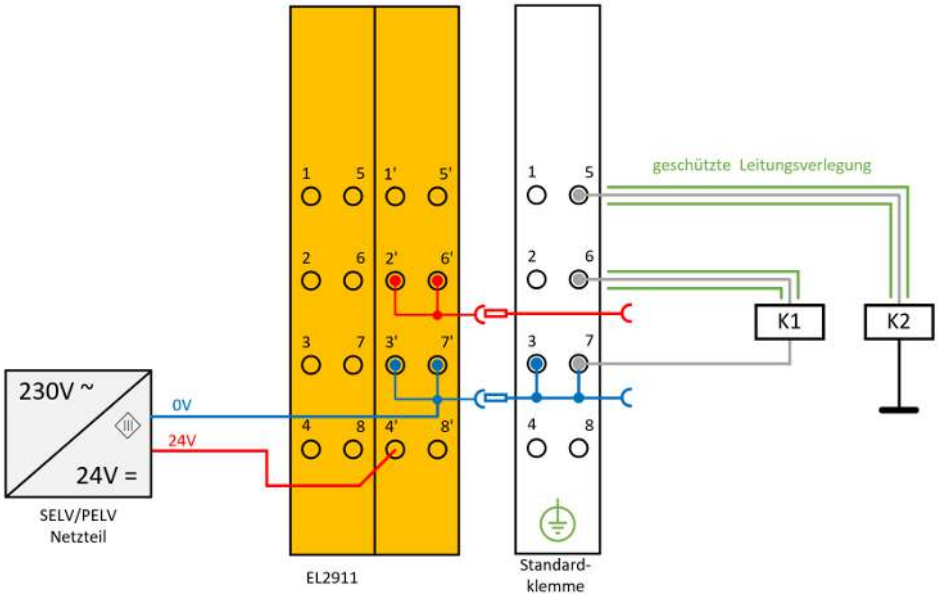
⚠ VORSICHT

Herstellerangabe

Ausnahmen von der allgemeinen Anforderung sind nur erlaubt, wenn der Hersteller der angeschlossenen Last garantiert, dass es zu keiner Rückspeisung auf den Ansteuereingang kommen kann.

5.3.1.2 Fehlerausschluss Leitungskurzschluss

Die Gefahr der Rückspeisung aufgrund eines Leitungskurzschlusses muss durch weitere Maßnahmen ausgeschlossen werden. Die folgenden Maßnahmen können alternativ umgesetzt werden.



Alternative 1: Lastanschluss durch separate Mantelleitungen

Das nicht sicher geschaltete Potential der Standardklemme darf nicht zusammen mit anderen potentialführenden Leitungen in derselben Mantelleitung geführt werden

Alternative 2: Verdrahtung nur Schaltschrank-intern

Alle an die nicht sicheren Standardklemmen angeschlossenen Lasten müssen sich im selben Schaltschrank wie die Klemmen befinden. Die Leitungsverlegung verbleibt vollkommen innerhalb des Schaltschrankes.

Alternative 3: Eigene Erdverbindung pro Leiter

Alle an die nicht sicheren Standardklemmen angeschlossenen Leiter sind durch eine eigene Erdverbindung geschützt.

Alternative 4: Verdrahtung dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt

Alle an die nicht sicheren Standardklemmen angeschlossenen Leiter sind dauerhaft fest verlegt und z.B. durch einen Kabelkanal oder Panzerrohr gegen äußere Beschädigung geschützt.

⚠ VORSICHT

Fehlerausschluss

Für die korrekte Ausführung und Bewertung der angewendeten Alternativen ist der Maschinenbauer bzw. Anwender allein verantwortlich.

5.3.2 Parameter der EL2911

EL2911

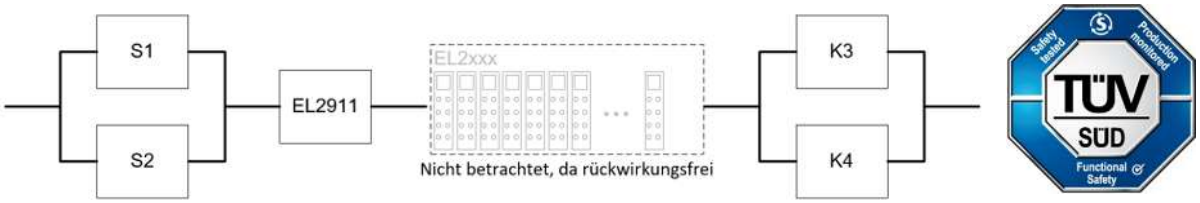
Parameter	Wert
FSOUT Settings Common	-
0x8000:04 – Diag Testpulse active	TRUE
0x8000:12 – Output Cross Circuit Detection Delay	1000 ms
FSIN Settings Common	-
0x8010:02 - MultiplierDiagTestPulse	0x01
0x8010:04 – Diag TestPulse active	TRUE
FSIN Settings Channel	-
0x8011:01 – Channel 1.InputFilterTime	0x0014 (2 ms)
0x8011:02 – Channel 1.DiagTestPulseFilterTime	0x0002 (0,2 ms)
0x8011:04 – Channel 2.InputFilterTime	-
0x8011:05 – Channel 2.DiagTestPulseFilterTime	-
0x8011:07 – Channel 3.InputFilterTime	0x0014 (2 ms)
0x8011:08 – Channel 3.DiagTestPulseFilterTime	0x0002 (0,2 ms)
0x8011:0A – Channel 4.InputFilterTime	0x0014 (2 ms)
0x8011:0B – Channel 4.DiagTestPulseFilterTime	0x0002 (0,2 ms)

FB MON

Parameter	Wert
Reset Time (ms) (Port EDM1)	1000
Discrepancy Time (ms) (Port MonIn1/MonIn2)	500
Safe Inputs After Disc Error	TRUE

5.3.3 Blockbildung und Safety-Loops

5.3.3.1 Sicherheitsfunktion 1



5.3.4 Berechnung

5.3.4.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL2911 – PFH_D	4,50E-09
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
K3 – $B10_D$	1.300.000
K4 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230

Komponente	Wert
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

5.3.4.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
K3/K4 mit EDM	DC_{avg}=90%

5.3.4.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7\,y = 11902212h$$

S2:

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

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4\,y = 23804424h$$

K3/K4:

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

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3\,y = 15472788h$$

und der Annahme, dass S1, S2, K3 und K4 jeweils einkanalig sind:

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

ergibt sich für

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

S1

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

S2

$$PFH = \frac{1-0,99}{2717,4*8760} = 4,20E-10$$

K3/K4

$$PFH = \frac{1-0,90}{1766,3*8760} = 6,46E-09$$

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Die Schütze K3 und K4 sind alle an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Schützes führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K3 und K4 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Schütz-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL2911)}$$
$$+\beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1-\beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{ges} = 10\% * \frac{8,40E-10 + 4,20E-10}{2} + 4,50E-09 + 10\% * \frac{6,46E-09 + 6,46E-09}{2}$$
$$= 5,21E-09$$

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}}$$

Sind für EL2911 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL2911)} = \frac{(1 - DC_{(EL2911)})}{PFH_{(EL2911)}} = \frac{(1 - 0{,}99)}{4{,}50E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{3{,}94E-05\frac{1}{y}} = 253y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358{,}7y} + \frac{1}{253y} + \frac{1}{1766{,}3y}} = 190y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(S2)}} + \frac{DC}{MTTF_{D(EL2911)}} + \frac{DC}{MTTF_{D(K3)}} + \frac{DC}{MTTF_{D(K4)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}} + \frac{1}{MTTF_{D(K4)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{1358{,}7y} + \frac{99\%}{2717{,}4y} + \frac{99\%}{253y} + \frac{90\%}{1766{,}3y} + \frac{90\%}{1766{,}3y}}{\frac{1}{1358{,}7y} + \frac{1}{2717{,}4y} + \frac{1}{253y} + \frac{1}{1766{,}3y} + \frac{1}{1766{,}3y}} = 97{,}35\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2(*)	**≥ 10^{-7} bis < 10^{-6}**
1	≥ 10^{-6} bis < 10^{-5}

(*) Entsprechend der EN 62061 Kapitel 6.7.7.2 ist für ein Teilsystem, das eine HFT von 0 besitzt und für das Fehlerausschlüsse zu Fehlern, die zu einem gefahrbringenden Ausfall führen können, angewendet worden sind, die SILCL in Bezug auf strukturelle Einschränkungen für das Teilsystem auf ein Maximum von SIL2 beschränkt.

5.4 EPP Potentialgruppe mit EPP9022-9060 (Kategorie 4, PL e)

Die Schutztür verwendet eine Kombination von Öffner und Schließer und wird auf sichere Eingänge der ersten EL2911 (1) verdrahtet. Die Testung der Eingänge ist aktiv und die Signale werden auf Diskrepanz (hier z.B. 500 ms) überprüft. An dem sicheren Ausgang der zweiten EL2911 (2) wird die 24 V Versorgung Up der Potentialgruppe abgeschaltet. Der 0 V Anschluss wird direkt auf die 0 V der Spannungsversorgung der EL2911 zurückgeführt. Die 0 V Potentiale der beiden EL2911 liegen auf demselben Potential bzw. sind gebrückt.

Der Rückführkreis der Schütze K3 und K4 wird auf einen sicheren Eingang der EL2911 gelegt.

Die 0 V Potentiale aller verwendeten Lasten und Geräte müssen auf demselben Potential liegen bzw. verbunden sein.

Diagnose

Für die EtherCAT-p-Leitung kann kein Fehlerausschluss herangezogen werden, da Us und Up in einer gemeinsamen Mantelleitung liegen und keine eigene Erdverbindung pro Leiter vorhanden ist.

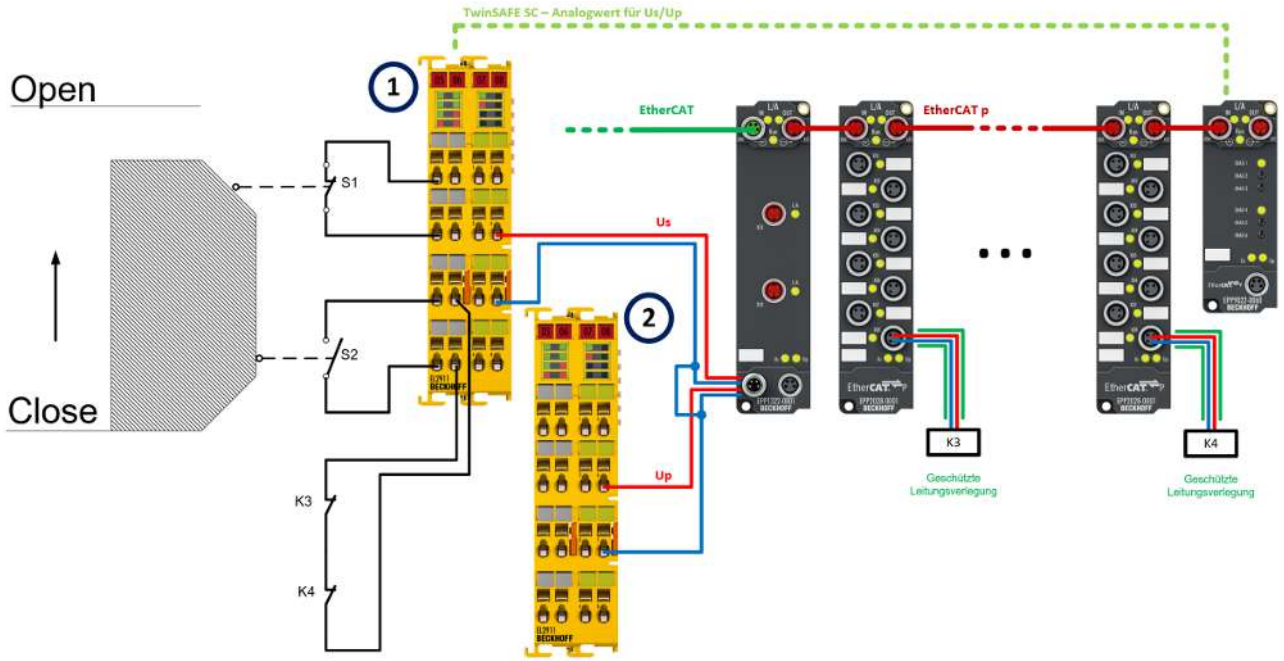
Zur Diagnose, ob eine Rückspeisung oder ein Querschluss auf der EtherCAT-p-Leitung vorliegt, werden zum einen die Spannung Us und Up durch die EtherCAT-p-Box EPP9022-9060 gemessen und als Analogwert per TwinSAFE SC an die EL2911 übermittelt. Damit wird eine Verfälschung der analogen Signale auf dem Kommunikationsweg ausgeschlossen. Zum anderen überwacht die EL2911 eine Rückspeisung auf die 24 V_{DC} des sicheren Ausgangs und geht in einen Modul-Fehler, sobald im ausgeschalteten Zustand eine Spannung höher als 5 V gelesen wird.

HINWEIS

Sicherheitsbetrachtung

Die verwendeten Boxen EPP2xxx sind kein aktiver Teil der Sicherheitssteuerung. Dementsprechend ist der erreichte Sicherheitslevel nur durch die überlagerte Sicherheitssteuerung definiert. Die Standard-Boxen werden **nicht** in die Berechnung mit einbezogen.

Die externe Beschaltung der Standard-Boxen kann zu Einschränkungen des maximal erreichbaren Sicherheitslevels führen (siehe auch Hinweise zur Verhinderung der Rückspeisung [▶ 166]).



⚠ VORSICHT

Voraussetzungen Netzteil

Zur Versorgung der Standardklemmen mit 24 V_{DC} muss ein SELV/PELV-Netzteil mit einer ausgangsseitigen Spannungsbegrenzung auf U_{max} = 36 V im Fehlerfall verwendet werden.

⚠ VORSICHT

Verhinderung der Rückspeisung

Die Rückspeisung kann durch unterschiedliche Maßnahmen verhindert werden (siehe weitere Hinweise untenstehend):

- Kein Schalten von Lasten mit separater Spannungsversorgung
- Fehlerausschluss Leitungskurzschluss (separate Mantelleitung, Verdrahtung nur Schaltschrank-intern, eigene Erdverbindung pro Leiter, feste Verlegung)

⚠ VORSICHT

Maximale Safety-Reaktionszeit

Die maximale Zeit zur Erkennung eines Fehlers (Fault Detection Time) tritt bei der Erkennung eines Fehlers über das Lesen der Rückführkreise der Schütze K3 und K4 auf, da diese Zeit typischerweise sehr viel größer als die Erkennung über das Rücklesen der Spannungen an der EL2911 und der EPP9022-9060 ist. Die Zeit wird in der Safety Logik eingestellt und sollte so groß eingestellt werden, dass eine schnelle Fehlererkennung möglich ist, aber auch eine Verfügbarkeit der Maschine gegeben ist.

Die Fehlerreaktionszeit (Fault Reaction Time) ergibt sich aus der Eingangsfilterzeit der EL2911 (des sicheren Eingangs, an dem der Rückführkreis angeschlossen ist), zweimal der Zykluszeit des auf der EL2911 ausgeführten Logikprogramms (kann aus den CoE-Objekten ausgelesen werden) und der Abfallzeit der Schütze K3 und K4 nachdem die Spannung am Ausgang der EL2911 ausgeschaltet wurde. Diese Zeit hängt stark von der verwendeten Aktorik ab.

Diese beiden Zeiten addiert ergeben die Safety-Reaktionszeit (Safety Response Time).

$$SafetyResponseTime = FaultDetectionTime + FaultReactionTime$$
$$= EDMtime + InputfilterTimeEL2911 + 2 * LogicCycleTime + SwitchOffTimeAktuators$$

Diese Safety-Reaktionszeit muss durch den Anwender bzw. Maschinenbauer für die sicherheitstechnische Bewertung seiner Anwendung herangezogen und geprüft werden.

Safety Applikation

Wird der sichere Ausgang der EL2911 (2) für Up abgeschaltet, muss der über TwinSAFE SC übermittelte Analogwert für Up einen Wert von kleiner 5 V melden. Ist dies nicht der Fall müssen beide EL2911 Ausgänge (1) + (2) abgeschaltet werden. Dies wird z. B. über einen EDM-Baustein realisiert, welcher in einer TwinSAFE-Gruppe mit den Ausgängen Us und Up programmiert wird und im Fehlerfall somit die gesamte Gruppe und alle darin konfigurierten Ausgänge abschaltet.

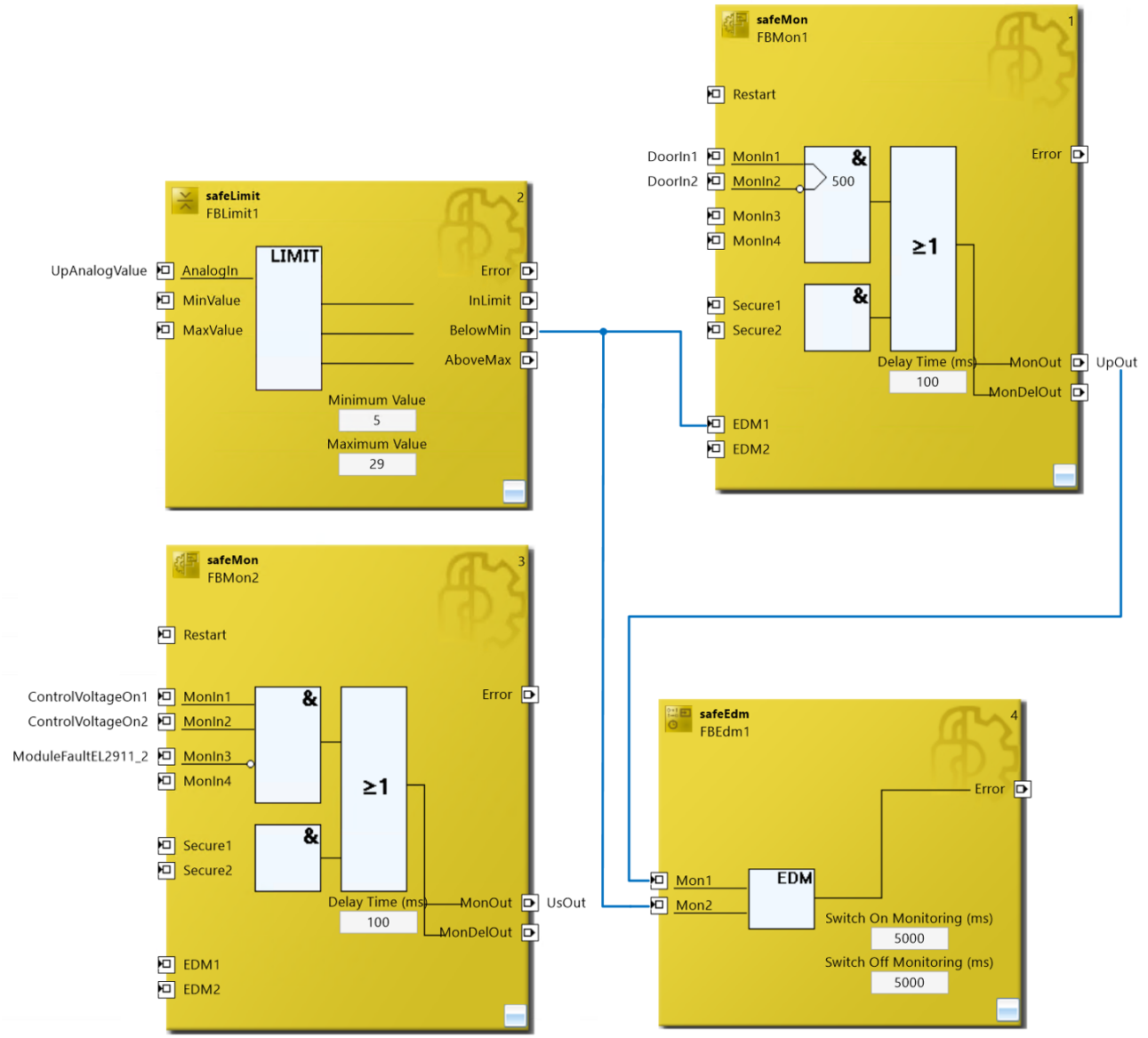
Weiterhin muss im Falle eines Modulfehlers der EL2911 (2) für Up die EL2911 (1) für Us abgeschaltet werden.

⚠ VORSICHT

Umsetzung der Safety-Applikation

Für die korrekte Umsetzung und Prüfung der Safety-Applikation ist der Anwender bzw. Maschinenbauer allein verantwortlich.

Beispiel für eine Safety-Applikation



HINWEIS

Rückführkreis

Der Rückführkreis der Aktoren K3 und K4 ist zur besseren Übersichtlichkeit nicht dargestellt, muss jedoch durch den Anwender berücksichtigt werden.

HINWEIS

Maximal erreichbare Sicherheitslevel

Rückspeisung durch Fehlerausschluss Leitungskurzschluss vermieden:
DIN EN ISO 13849-1: max. Kat. 4 PL e
IEC 61508: max. SIL3
EN 62061: max. SIL2

HINWEIS

Potential 0 V

Die 0 V Potentiale der Last (hier K3, K4) müssen identisch zum 0 V Potential der Spannungsversorgung der beiden EL2911 sein.

⚠ VORSICHT

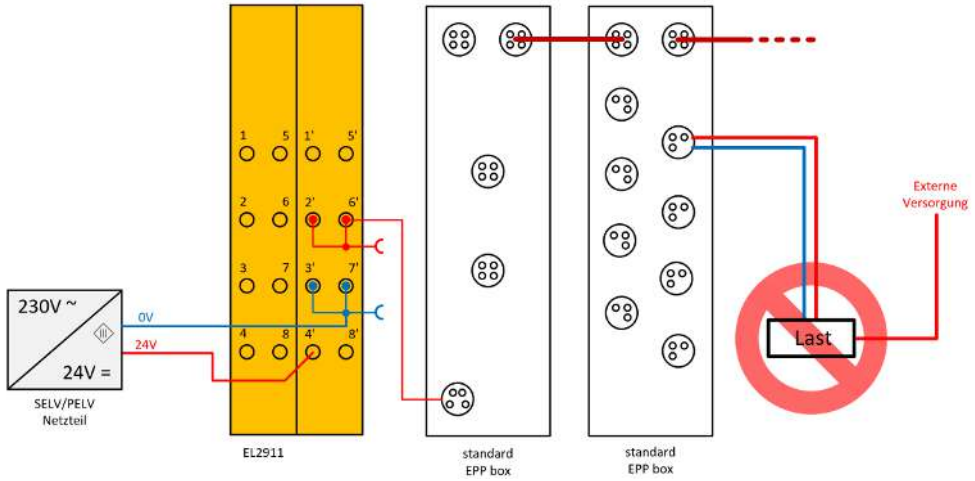
Zeitliche Verzögerung

Durch das Abschalten der Spannungsversorgung der Potentialgruppe, kann sich die Abschaltung der nachgeschalteten Schütze und Aktoren verzögern. Diese Verzögerung ist abhängig von den nachgeschalteten Aktoren, Verbrauchern und Leitungen und ist durch den Anwender in der Sicherheitsbetrachtung zu berücksichtigen.

5.4.1 Hinweise zur Verhinderung der Rückspeisung

5.4.1.1 Kein Schalten von Lasten mit separater Spannungsversorgung

Es dürfen keine Lasten durch Standard-Boxen geschaltet werden, die über eine eigene Spannungsversorgung verfügen, da hier eine Rückspeisung durch die Last nicht ausgeschlossen werden kann.



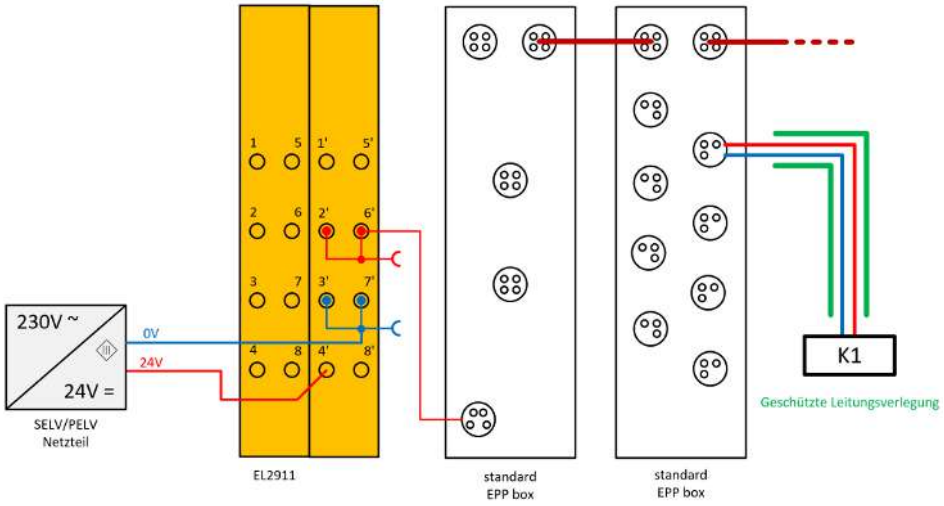
⚠ VORSICHT

Herstellerangabe

Ausnahmen von der allgemeinen Anforderung sind nur erlaubt, wenn der Hersteller der angeschlossenen Last garantiert, dass es zu keiner Rückspeisung auf den Ansteuereingang kommen kann.

5.4.1.2 Fehlerausschluss Leitungskurzschluss

Die Gefahr der Rückspeisung aufgrund eines Leitungskurzschlusses muss durch weitere Maßnahmen ausgeschlossen werden. Die folgenden Maßnahmen können alternativ umgesetzt werden.



Alternative 1: Lastanschluss durch separate Mantelleitungen

Das nicht sicher geschaltete Potential der Standardklemme darf nicht zusammen mit anderen potentialführenden Leitungen in derselben Mantelleitung geführt werden

Alternative 2: Verdrahtung nur Schaltschrank-intern

Alle an die nicht sicheren Standardklemmen angeschlossenen Lasten müssen sich im selben Schaltschrank wie die Klemmen befinden. Die Leitungsverlegung verbleibt vollkommen innerhalb des Schaltschrankes.

Alternative 3: Eigene Erdverbindung pro Leiter

Alle an die nicht sicheren Standardklemmen angeschlossenen Leiter sind durch eine eigene Erdverbindung geschützt.

Alternative 4: Verdrahtung dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt

Alle an die nicht sicheren Standardklemmen angeschlossenen Leiter sind dauerhaft fest verlegt und z.B. durch einen Kabelkanal oder Panzerrohr gegen äußere Beschädigung geschützt.

⚠ VORSICHT

Fehlerausschluss

Für die korrekte Ausführung und Bewertung der angewendeten Alternativen ist der Maschinenbauer bzw. Anwender allein verantwortlich.

5.4.2 Parameter der EL2911

EL2911 (gilt für alle EL2911)

Parameter	Wert
FSOUT Settings Common	-
0x8000:04 – Diag Testpulse active	TRUE
0x8000:12 – Output Cross Circuit Detection Delay	1000 ms
FSIN Settings Common	-
0x8010:02 - MultiplierDiagTestPulse	0x01
0x8010:04 – Diag TestPulse active	TRUE
FSIN Settings Channel	-
0x8011:01 – Channel 1.InputFilterTime	0x0014 (2 ms)

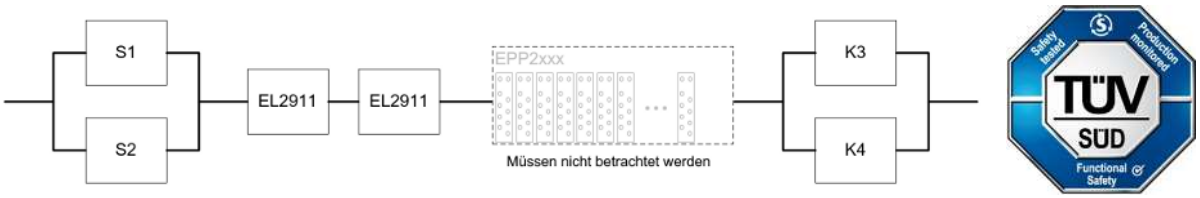
Parameter	Wert
0x8011:02 – Channel 1.DiagTestPulseFilterTime	0x0002 (0,2 ms)
0x8011:04 – Channel 2.InputFilterTime	-
0x8011:05 – Channel 2.DiagTestPulseFilterTime	-
0x8011:07 – Channel 3.InputFilterTime	0x0014 (2 ms)
0x8011:08 – Channel 3.DiagTestPulseFilterTime	0x0002 (0,2 ms)
0x8011:0A – Channel 4.InputFilterTime	0x0014 (2 ms)
0x8011:0B – Channel 4.DiagTestPulseFilterTime	0x0002 (0,2 ms)

FB MON

Parameter	Wert
Reset Time (ms) (Port EDM1)	1000
Discrepancy Time (ms) (Port MonIn1/MonIn2)	500
Safe Inputs After Disc Error	TRUE

5.4.3 Blockbildung und Safety-Loops

5.4.3.1 Sicherheitsfunktion 1



5.4.4 Berechnung

5.4.4.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL2911 – PFH_D	4,50E-09
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
K3 – $B10_D$	1.300.000
K4 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

5.4.4.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
K3/K4 mit EDM	DC_{avg}=90%

5.4.4.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7y = 11902212h$$

S2:

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

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4y = 23804424h$$

K3/K4:

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

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

und der Annahme, dass S1, S2, K3 und K4 jeweils einkanalig sind:

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

ergibt sich für

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

S1

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

S2

$$PFH = \frac{1 - 0{,}99}{2717{,}4 * 8760} = 4{,}20E - 10$$

K3/K4

$$PFH = \frac{1 - 0{,}90}{1766{,}3 * 8760} = 6{,}46E - 09$$

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Die Schütze K3 und K4 sind alle an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Schützes führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K3 und K4 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Schütz-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL2911)} + PFH_{(EL2911)} + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1-\beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{ges} = 10\% * \frac{8,40E-10 + 4,20E-10}{2} + 4,50E-09 + 4,50E-09 + 10\% * \frac{6,46E-09 + 6,46E-09}{2} = 9,71E-09$$

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}}$$

Sind für EL2911 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL2911)} = \frac{(1-DC_{(EL2911)})}{PFH_{(EL2911)}} = \frac{(1-0,99)}{4,50E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{3,94E-05\frac{1}{y}} = 253y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{253y} + \frac{1}{253y} + \frac{1}{1766,3y}} = 108y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(S2)}} + \frac{DC}{MTTF_{D(EL2911)}} + \frac{DC}{MTTF_{D(EL2911)}} + \frac{DC}{MTTF_{D(K3)}} + \frac{DC}{MTTF_{D(K4)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}} + \frac{1}{MTTF_{D(K4)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y} + \frac{99\%}{2717,4y} + \frac{99\%}{253y} + \frac{99\%}{253y} + \frac{90\%}{1766,3y} + \frac{90\%}{1766,3y}}{\frac{1}{1358,7y} + \frac{1}{2717,4y} + \frac{1}{253y} + \frac{1}{253y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 98,00\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2(*)	**≥ 10^{-7} bis < 10^{-6}**
1	≥ 10^{-6} bis < 10^{-5}

(*) Entsprechend der EN 62061 Kapitel 6.7.7.2 ist für ein Teilsystem, das eine HFT von 0 besitzt und für das Fehlerausschlüsse zu Fehlern, die zu einem gefahrbringenden Ausfall führen können, angewendet worden sind, die SILCL in Bezug auf strukturelle Einschränkungen für das Teilsystem auf ein Maximum von SIL2 beschränkt.

6 STO/SS1-Funktionen

6.1 AX8xxx-x1xx STO Funktion (Kategorie 4, PL e)

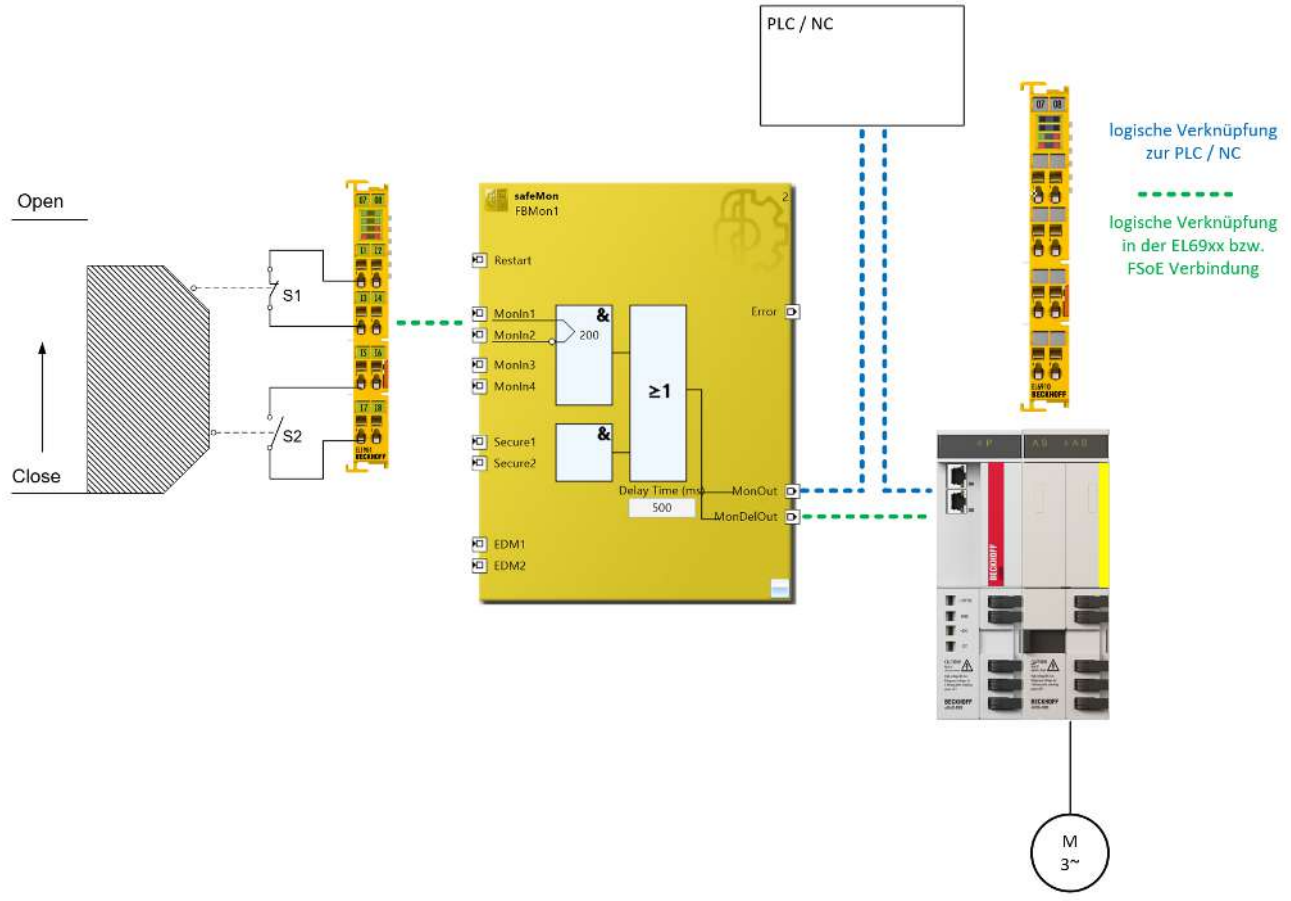
Die Schutztür ist mit einer Öffner-Schließer-Kombination auf sichere Eingänge einer EL1904 verdrahtet. Die Testpulse der Eingänge sind eingeschaltet. Innerhalb der TwinSAFE Logik wird die Schutztür auf einen FB Mon gelegt und der direkt schaltende Ausgang wird verwendet, um der NC-Steuerung mitzuteilen, dass in z.B. 500ms ein STO ausgeführt wird und somit eine Stop-Rampe gefahren werden soll.

Nach z.B. 500ms wird dem AX8xxx-x1xx über den verzögert schaltenden Ausgang mitgeteilt, dass STO aktiviert werden soll.

In diesem Beispiel wird davon ausgegangen, dass mit Öffnen der Tür und dem zeitverzögerten Schalten des AX8xxx-x1xx nach STO die Maschine im sicheren Zustand ist, bevor die Gefahrenstelle vom Anwender erreicht werden kann.

Eine Bewertung der Maschine und der Anwendung muss durch den Maschinenbauer erfolgen.

Soll eine andere Applikation auf dem Antrieb ausgeführt werden, kann dies durch eine kundenspezifische Logik-Applikation auf dem AX8xxx-x1xx realisiert werden.



6.1.1 Parameter der sicheren Ein- und Ausgangsmodule

EL1904

Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	-
Sensortest Kanal 4 aktiv	-

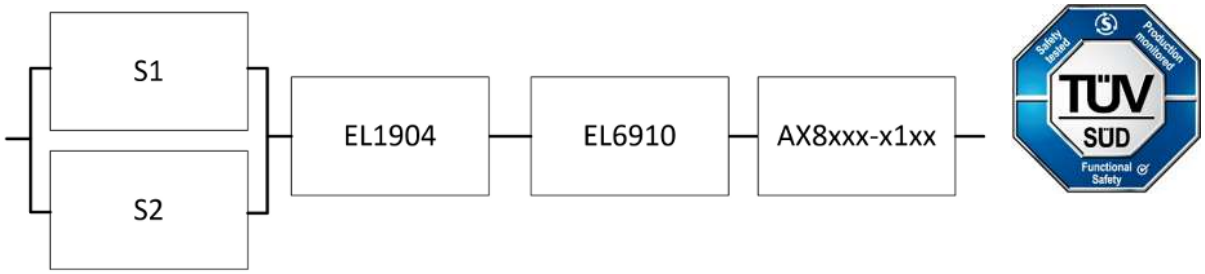
Parameter	Wert
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

MON FB Parameter

Parameter	Wert
Discrepancy Time (ms) (Port MonIn1/MonIn2)	200
Safe Inputs After Disc Error	TRUE
MON Delay Time	500

6.1.2 Blockbildung und Safety-Loops

6.1.2.1 Sicherheitsfunktion 1



6.1.3 Berechnung

6.1.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL6910 – PFH_D	1,79E-09
AX8xxx-x1xx - PFH_D	3,04E-09
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

6.1.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung und Plausibilität	DC_{avg}=99%
AX8xxx-x1xx STO Funktion	DC_{avg}>99%

6.1.3.3 Berechnung Sicherheitsfunktion 1

Berechnung des Performance Levels nach EN ISO 13849-1:2015

Berechnung der $MTTF_D$-Werte aus den $B10_D$-Werten

aus:

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

und:

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

Eingesetzt ergibt das:

S1

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

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

S2

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

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

Der Gesamt-$MTTF_D$ Wert ergibt sich aus der Formel:

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

als:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}$$

Sind für die EL1904, EL6910 und AX8xxx-x1xx nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{15{,}68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(AX8xxx-x1xx)} = \frac{(1 - DC_{(AX8xxx-x1xx)})}{PFH_{D(AX8xxx-x1xx)}} = \frac{(1 - 0{,}99)}{3{,}04E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{2{,}66E-05\frac{1}{y}} = 375y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679y} + \frac{1}{1028y} + \frac{1}{637y} + \frac{1}{375y}} = 149y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(S2)}} + \frac{DC}{MTTF_{D(EL1904)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(AX8xxx-x1xx)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{679y} + \frac{99\%}{1358y} + \frac{99\%}{1028y} + \frac{99\%}{637y} + \frac{99\%}{375y}}{\frac{1}{679y} + \frac{1}{1358y} + \frac{1}{1028y} + \frac{1}{637y} + \frac{1}{375y}} = 99{,}00\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist **NICHT** Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Berechnung der PFH_D Werte nach EN 62061

mit der Annahme, dass S1 und S2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

S2:

$$PFH_D = \frac{1 - 0{,}99}{1358 * 8760} = 8{,}41E - 10$$

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

$$PFH_{Dges} = \beta * \frac{PFH_{D(S1)} + PFH_{D(S2)}}{2} + (1 - \beta)^2 * (PFH_{D(S1)} * PFH_{D(S2)}) * T1 + PFH_{D(EL1904)} + PFH_{D(EL6910)} + PFH_{D(AX8xxx-x1xx)}$$

Da der Anteil $(1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ um Zehnerpotenzen kleiner ist, als der Rest, wird er als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{Dges} = 10\% * \frac{1{,}68E - 09 + 8{,}41E - 10}{2} + 1{,}11E - 09 + 1{,}79E - 09 + 3{,}04E - 09$$
$$= 6{,}07E - 09$$

Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	**≥ 10^{-8} bis < 10^{-7}**
2	≥ 10^{-7} bis < 10^{-6}
1	≥ 10^{-6} bis < 10^{-5}

HINWEIS

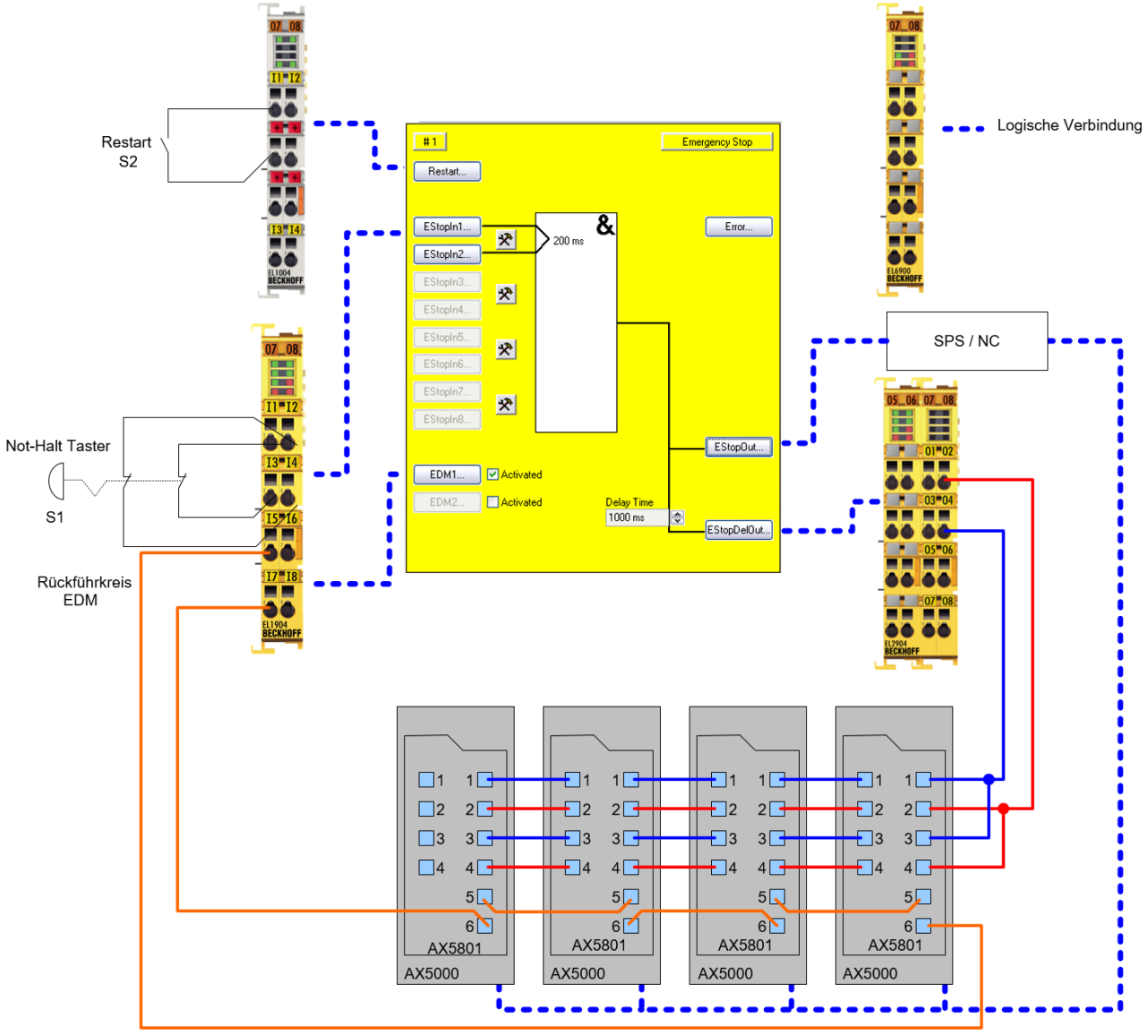
Sicherheits-Integritätslevel

Die Anwendung entspricht einem Sicherheits-Integritätslevel von SIL3 nach EN 62061.

6.2 Antriebsoption AX5801 mit Stopp-Funktion SS1 (Kategorie 4, PL e)

Durch das Betätigen des Not-Halt-Tasters werden die Eingänge EStopIn1 und EStopIn2 vom FB ESTOP in den Zustand „0“ gebracht und dadurch werden die Ausgänge EStopOut vom FB ESTOP in den Zustand „0“ gebracht. Dies hat zur Folge, dass die PLC und damit via EtherCAT der AX5000 den Befehl zum Schnellstopp bekommt. Der Ausgang EStopDelOut vom FB ESTOP sorgt dafür, dass nach Ablauf einer vorgegebenen Verzögerungszeit (hier z.B. 1000 ms) die 24 V Versorgung der Safety-Option AX5801 unterbrochen wird und somit die internen Relais der AX5801 abfallen. Über die internen Abschaltpfade der AX5000 werden beide Kanäle (Motoren) drehmomentfrei geschaltet.

Die Testung und die Prüfung auf Diskrepanz sind für die Eingangssignale eingeschaltet. Die Testung der Ausgänge ist ebenfalls aktiv. Die Relais der 4 AX5801 Optionskarten werden parallel auf einen sicheren Ausgang der EL2904 verdrahtet. Die Rückführkreise werden in Reihe geschaltet auf einen sicheren Eingang verdrahtet. Das Restart-Signal ist auf einen nicht-sicheren Eingang verdrahtet.



6.2.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

Parameter	Wert
Sensortest Kanal 1 aktiv	Ja

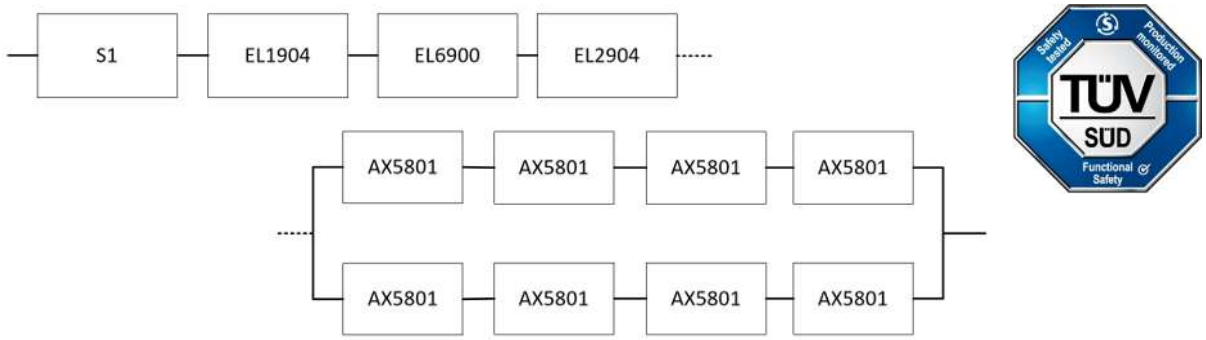
Parameter	Wert
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

6.2.2 Blockbildung und Safety-Loops

6.2.2.1 Sicherheitsfunktion 1



6.2.3 Berechnung

6.2.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
AX5801 – $B10_D$	780.000
S1 – $B10_D$	100.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	60 (1x pro Stunde)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

6.2.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung/Plausibilität	DC_{avg}=99%
AX5801	DC_{avg}=99%

6.2.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

$$MTTF_D = \frac{100.000}{0{,}1 * 1840} = 543{,}5y = 4761060h$$

AX5801:

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

$$MTTF_D = \frac{780.000}{0{,}1 * 1840} = 4239{,}1y = 37134516h$$

$$T_{10D} = \frac{B10_D}{n_{op}} \frac{780.000}{1840\frac{1}{y}} = 423y$$

und der Annahme, dass S1 einkanalig ist:

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

ergibt sich für

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

S1:

$$PFH = \frac{1 - 0{,}99}{543{,}5 * 8760} = 2{,}10E - 09$$

AX5801:

$$PFH = \frac{1 - 0{,}99}{4239{,}1 * 8760} = 2{,}70E - 10$$

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{4 * PFH_{(AX5801)} + 4 * PFH_{(AX5801)}}{2} + 4 * (1-\beta)^2 * (PFH_{(AX5801)} * PFH_{(AX5801)}) * T1$$

Da der Anteil $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}}$$

mit:

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

$$MTTF_{D(AX5801)} = \frac{B10_{D(AX5801)}}{0{,}1 * n_{op}}$$

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

$$DC_{avg} = \frac{\frac{99\%}{543,5y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y} + \frac{99\%}{4239,1y}}{\frac{1}{543,5y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y} + \frac{1}{4239,1y}}$$
$$= 99,00\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

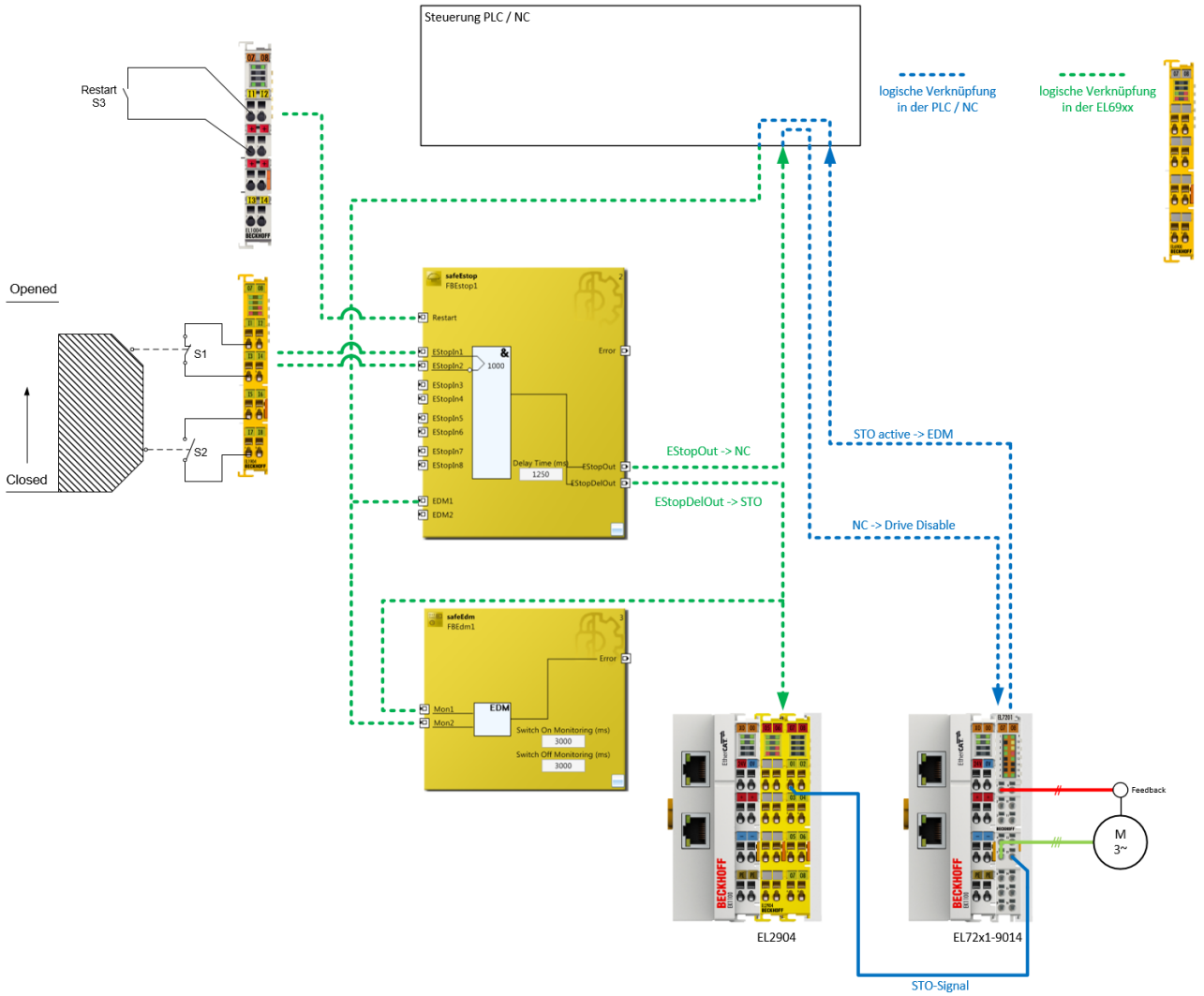
Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

6.3 STO-Funktion mit EL72x1-9014 (Kategorie 3, PL d)

Das folgende Applikationsbeispiel zeigt wie die EL72x1-9014 zusammen mit einer EL2904 beschaltet werden kann, um eine STO Funktion nach EN 61800-5-2 zu realisieren.

Eine Schutztür (S1 und S2) und ein Restart Signal (S3) werden logisch auf einen ESTOP-Baustein verknüpft. Das EStopOut Signal wird an die NC-Steuerung übergeben, mit der z.B. das Enable Signal der EL72x1-9014 geschaltet werden kann. Über den verzögerten Ausgang EStopDelOut wird der STO-Eingang der EL72x1-9014 bedient. Die EL72x1-9014 liefert über die Standard-Steuerung eine Information, dass die STO-Funktion aktiv ist. Diese Information wird an den EDM-Eingang des ESTOP-Bausteins und zusätzlich an den EDM-Baustein übergeben, um eine Erwartungshaltung für dieses Signal zu generieren.



⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

Liefert die Risikoanalyse das Ergebnis, dass ein Wiederanlauf in der Sicherheitssteuerung zu realisieren ist, **muss** der Restart auch auf einen sicheren Eingang gelegt werden.

⚠ WARNUNG

Verdrahtung nur Schaltschrank-intern!

Die Verdrahtung zwischen der EL2904 und dem STO-Eingang der EL72x1-9014 muss sich im selben Schaltschrank befinden, um einen Fehlerausschluss für den Querschluss bzw. Fremdeinspeisung der Verdrahtung zwischen EL2904 und EL72x1-9014 annehmen zu dürfen.

Die Bewertung dieser Verdrahtung und die Bewertung, ob der Fehlerausschluss zulässig ist, muss durch den Maschinenbauer bzw. Anwender erfolgen.

HINWEIS

Berechnung EL72x1-9014

In der Berechnung des Performance Levels nach DIN EN ISO 13849-1 wird die EL72x1-9014 nicht berücksichtigt, da sie sich rückwirkungsfrei gegenüber der Sicherheitsfunktion verhält.

In der Berechnung nach der EN 62061 geht der PFH_D Wert mit einem Wert von 0 ein.

6.3.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904

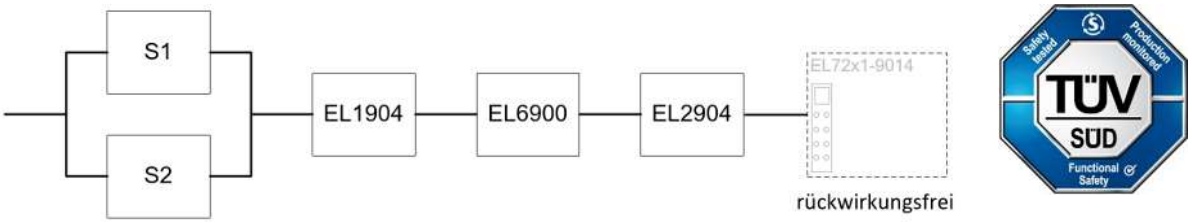
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Ja

6.3.2 Blockbildung und Safety-Loops

6.3.2.1 Sicherheitsfunktion 1



6.3.3 Berechnung

6.3.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09

Komponente	Wert
EL6900 – PFH_D	1,03E-09
EL72x1-9014 - PFH_D	0,00
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

6.3.3.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
EL2904 mit Testung	DC_{avg}=99%

6.3.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D- und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

und der Annahme, dass S1 und S2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

S2:

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

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ um Zehnerpotenzen kleiner ist, als der Rest, wird er als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

Sind für EL1904, EL6900 und EL2904 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

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

⚠ VORSICHT

Kategorie

Diese Struktur ist bis maximal Kategorie 3 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

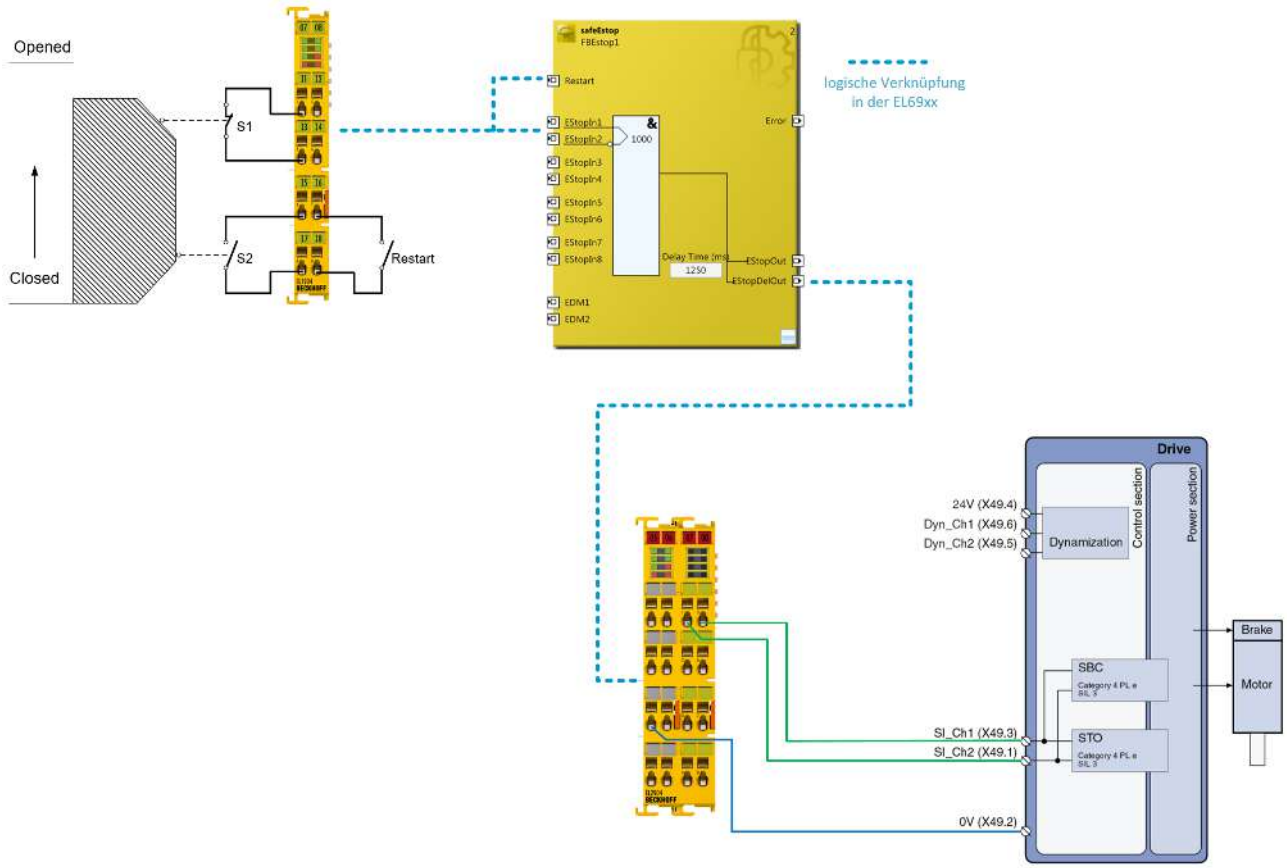
Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

6.4 STO-Funktion mit IndraDrive (Kategorie 4, PL e)

Das folgende Beispiel zeigt die Verwendung der sicheren Ausgänge der EL2904 zusammen mit einem BOSCH Rexroth IndraDrive Antrieb, um eine STO Funktion auf diesem zu realisieren.

Beispielhaft wird eine Schutztür zweikanalig auf einen sicheren Eingang (hier EL1904) zusammen mit einem Restart Signal verdrahtet. Innerhalb der TwinSAFE Logik werden diese Signale an einem ESTOP Baustein verwendet. Der verzögert schaltende Ausgang des ESTOP Bausteins wird für die beiden sicheren Ausgänge der EL2904 verwendet. Der Ausgang EStopOut kann verwendet werden, um über die NC Steuerung den Antrieb elektrisch zu stoppen.

Jeweils ein Ausgang der EL2904 wird auf die STO Eingänge X49.1 und X49.3 des Bosch Rexroth IndraDrive verdrahtet. Der zugehörige GND Anschluss (X49.2) wird hier beispielhaft auf die EL2904 zurückgeführt, um zu zeigen, dass die EL2904 und der IndraDrive identisches Masse-Potential der 24V-Versorgung verwenden.



⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist **NICHT** Teil der Sicherheitskette und muss in der Maschine implementiert werden!

6.4.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904

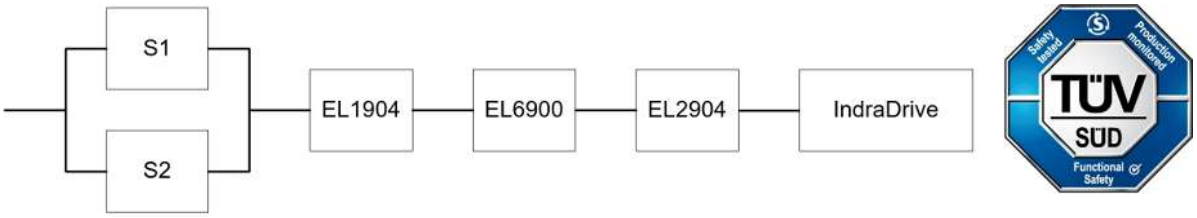
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Ja

6.4.2 Blockbildung und Safety-Loops

6.4.2.1 Sicherheitsfunktion 1



6.4.3 Berechnung

6.4.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
Bosch Rexroth IndraDrive[1)] - PFH_D	0,50E-09
Bosch Rexroth IndraDrive[1)] - $MTTF_D$	> 200 Jahre
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

[1)] Bitte beachten Sie die Informationen der Bosch Rexroth Anwenderdokumentation

6.4.3.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%
EL2904 mit Testung	DC_{avg}=99%
Bosch Rexroth IndraDrive[1)]	DC_{avg}=99%

[1)] Bitte beachten Sie die Informationen der Bosch Rexroth Anwenderdokumentation

6.4.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D- und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

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

S2:

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

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

und der Annahme, dass S1 und S2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

S2:

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

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält Tabellen (Tabelle F.1-Kriterien zur Bestimmung des CCF und Tabelle F.2-Abschätzung des CCF-Faktors(β)), mit der dieser β–Faktor genau bestimmt werden kann.

Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ um Zehnerpotenzen kleiner ist, als der Rest, wird er als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{ges} = 10\% * \frac{1{,}68E - 09 + 8{,}40E - 10}{2} + 1{,}11E - 09 + 1{,}03E - 09 + 1{,}25E - 09 + 0{,}50E - 09 = 4{,}016E - 09$$

HINWEIS

Berechnung nach EN 62061

Gemäß EN 62061 Tab. 3 entspricht dieser Wert einem SIL3.

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

$$MTTF_{D(IndraDrive)} = 200y$$

Sind für EL1904, EL6900 und EL2904 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{679{,}3y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{200y}} = 105{,}9y$$

$$DC_{avg} = \frac{\frac{99\%}{679{,}3y} + \frac{99\%}{1358{,}7y} + \frac{99\%}{1028{,}8y} + \frac{99\%}{1108{,}6y} + \frac{99\%}{913{,}2y} + \frac{99\%}{200y}}{\frac{1}{679{,}3y} + \frac{1}{1358{,}7y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{200y}} = 99{,}00\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**

DC	
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	**≥ 10^{-8} bis < 10^{-7}**
2	≥ 10^{-7} bis < 10^{-6}
1	≥ 10^{-6} bis < 10^{-5}

6.4.4 Technical Note der Firma Bosch Rexroth AG

Rexroth
Bosch Group

Technical Note

Bosch Rexroth AG
Postfach 1357
97803 Lohr am Main
Bgm.-Dr.-Nebel-Str. 2
97816 Lohr am Main
Tel. +49 9352 18-0
Fax +49 9352 18-8400
www.boschrexroth.com

09. März 2017

Sehr geehrte Damen und Herren,

Folgend bestätigen wir Ihnen die Anwendungsbedingungen für die sichere Anwahl von Sicherheitsfunktionen unseres IndraDrive.
Die Anwendungsbedingungen gelten für die IndraDrive Antriebsfamilien Cs, C/M, Mi, ML mit folgenden Sicherheitsoptionen

- L3, L4: Anwahl über Klemme X49 des Steuerteils
- S4, S5: Anwahl über Klemme X41 des Sicherheitszonenmoduls HSZ01

Die Installations- und Projektierungshinweise in der Kundendokumentation sind zu beachten.

Rexroth
Bosch Group

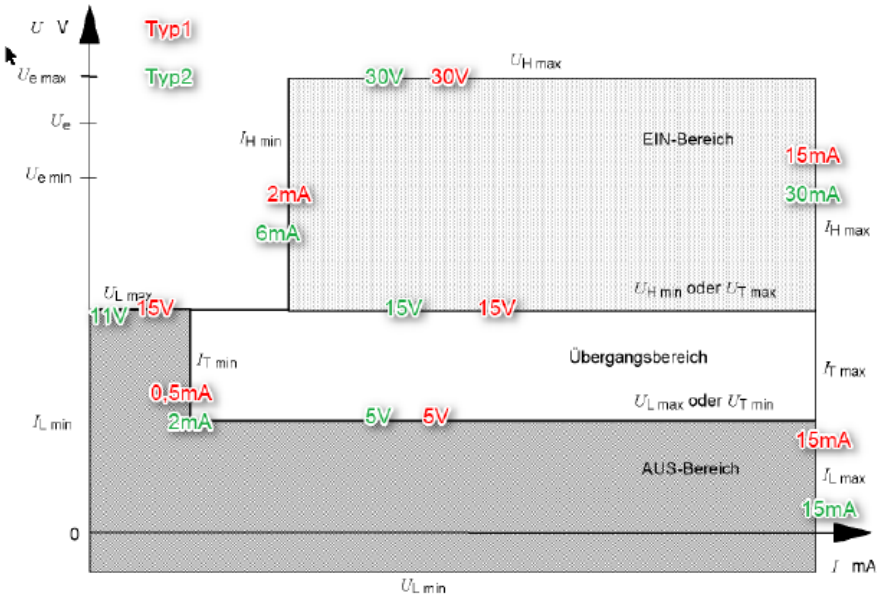
09. März 2017
Seite 2 von 4

1 Safety Anforderungen

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 Ausgangspannung <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

Rexroth
Bosch Group

2 Funktionale Anforderungen an die Anwahl (für Verfügbarkeit)

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_{PLmax}	1 ms	maximale Low-Zeit des Testpulses
t_{PLmin}	20 µs	minimale Low-Zeit des Testpulses
t_{Pmax}	1 h	maximale Periodendauer der Testpulse
t_{Pmin}	500 µs	minimale Periodendauer der Testpulse
t_{Vmax}	1 s	maximale Verzugszeit der Anwahlsignale bei Anwahl oder Abwahl
$t_{Dmin} = t_{PH} / t_P$	90 %	minimales Tastverhältnis der Anwahlsignale
t_{Prell}	400 ms	maximale Prelldauer bei einer An- oder Abwahl
φ	-	Phasenverschiebung der Testpulse auf beiden Kanälen: keine Anforderung

Tab. 5-1: Grenzwerte der Dynamisierungspulse der OSSD-Ausgänge

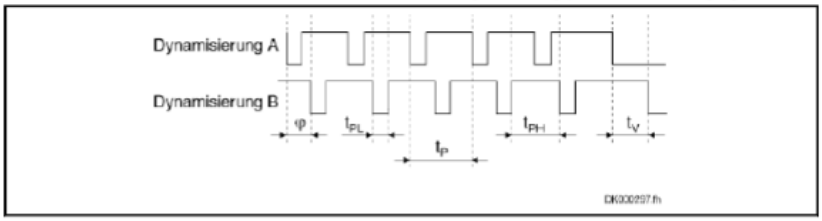
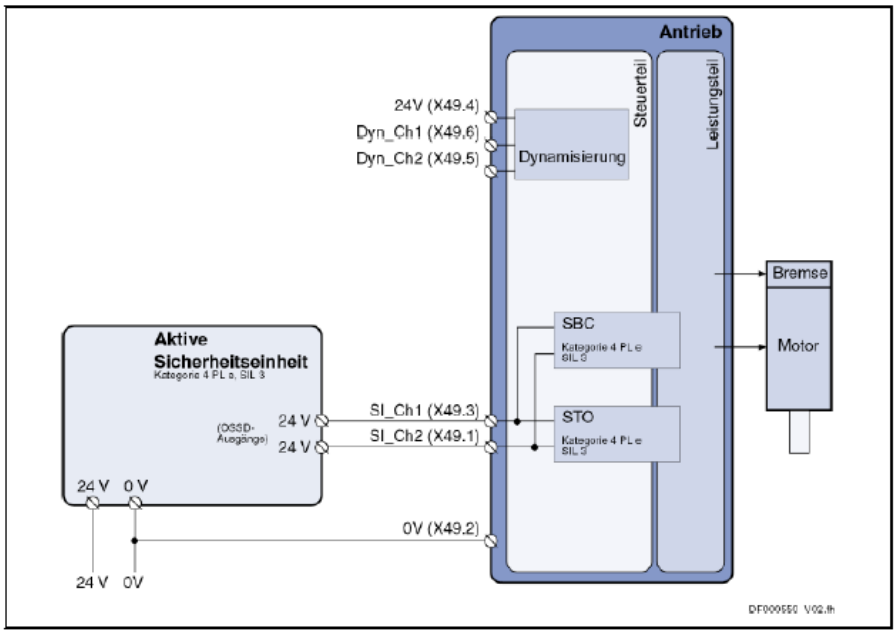


Abb. 5-2: Beispiel für dynamisierte Anwahlsignale



Rexroth
Bosch Group

2.2 Anforderung IndraDrive mit Sicherheitsoption S4, S5

Zweikanalige Anwahl über Klemme X41 des Sicherheitszonenmoduls HSZ01 (Eingang nach IEC 61131-2, Typ 1)

Grenzwert	Erklärung
t_{PLmax} = 1 ms	maximale Low-Zeit des Testpulses
t_{PLmin} = 0 ms	minimale Low-Zeit des Testpulses
t_{Vmax} [1)] = 1 s	maximale Verzugszeit der Anwahlsignale bei Anwahl oder Abwahl
$t_{Dmin} = t_{PH} / t_P$ = 90 %	minimales Tastverhältnis der Anwahlsignale
$t_{Dmax} = t_{PH} / t_P$ = 100 %	maximales Tastverhältnis der Anwahlsignale
t_{Prell} = 400 ms	maximale Prelldauer bei einer An- oder Abwahl
φ [1)] = -	Phasenverschiebung der Testpulse auf beiden Kanälen: keine Anforderung

1) gilt nur bei zweikanaliger Anwahl

Tab. 5-1: Grenzwerte der Dynamisierungspulse der OSSD-Ausgänge

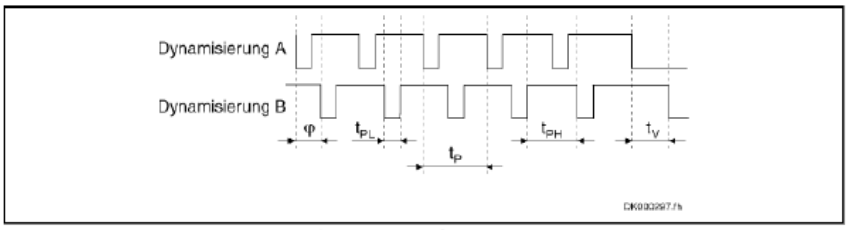


Abb. 5-1: Beispiel für dynamisierte Anwahlsignale

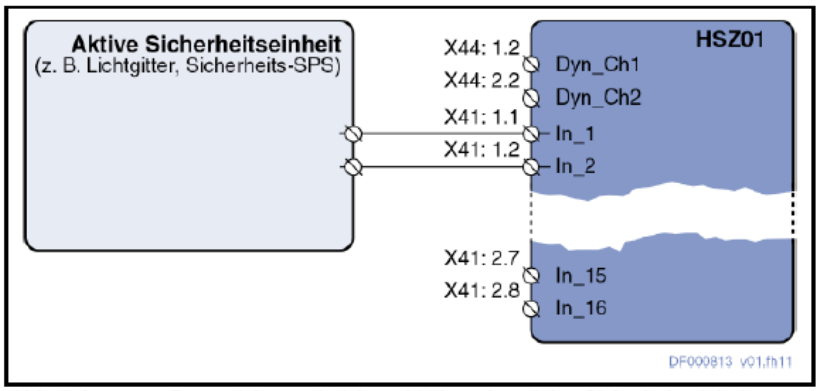


Abb. 5-2: Dynamisierung bei Anwahl über eine aktive Sicherheitseinheit

Diese Bestätigung gilt bis auf Widerruf.

Mit freundlichen Grüßen

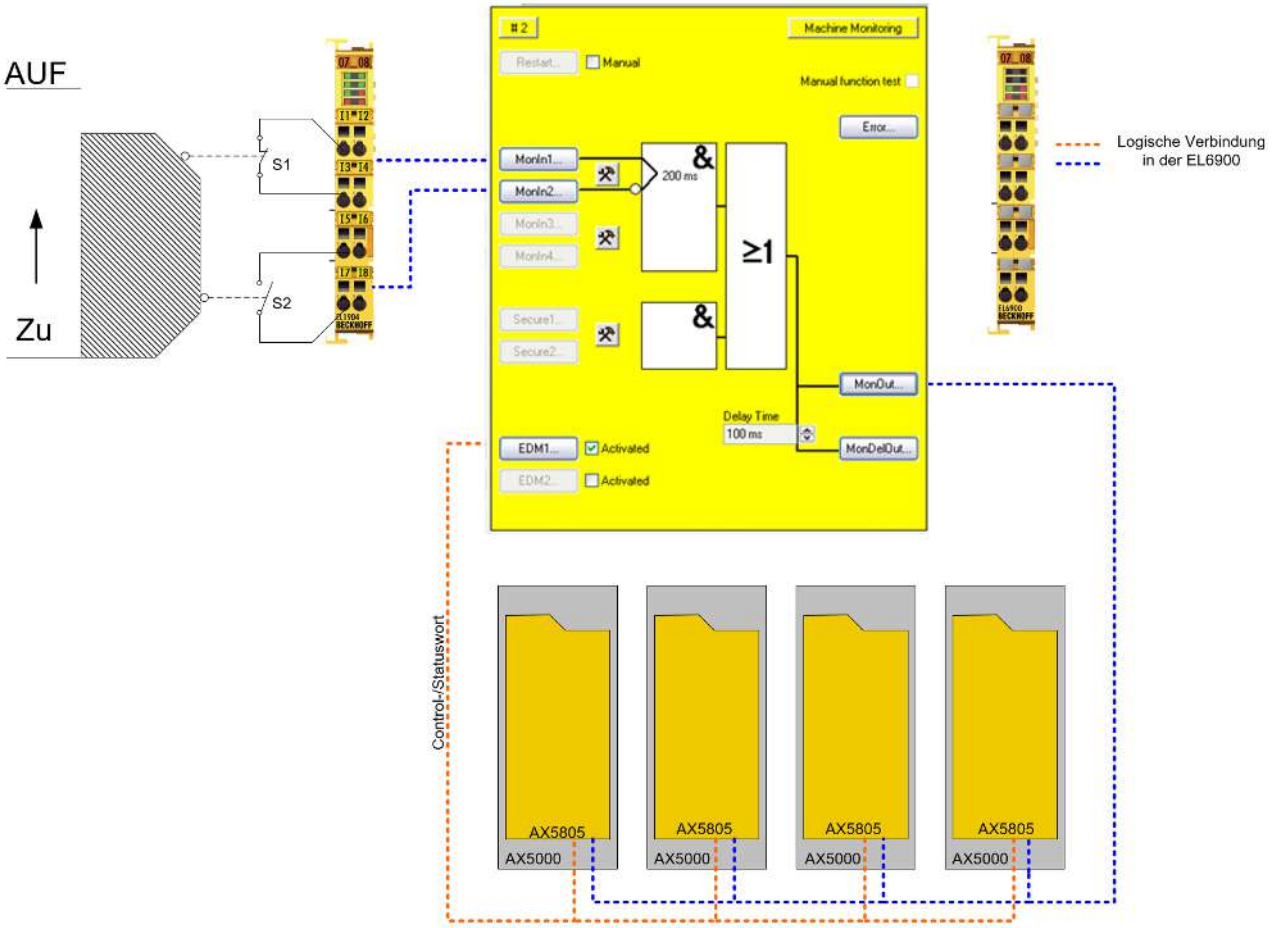
Bosch Rexroth AG (DC-IA/EDY)

7 Safe Motion-Funktionen

7.1 Antriebsoption AX5805 mit Stopp-Funktion SS2 (Kategorie 4, PL e)

Die Schutztür ist mit einer Kombination von Öffner und Schließer auf eine sichere Eingangsklemme EL1904 verbunden. Die Testung und die Prüfung auf Diskrepanz sind für die Eingangssignale eingeschaltet. Der Ausgang ist auf die AX5805 verknüpft.

Die Rückführsignale werden über das von der Antriebsoption zurückgemeldete Control- und Statuswort überprüft.



7.1.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

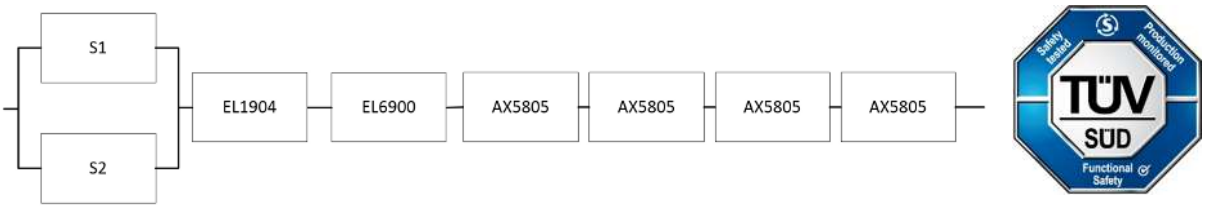
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

AX5805

Parameter	Wert
-	

7.1.2 Blockbildung und Safety-Loops

7.1.2.1 Sicherheitsfunktion 1



7.1.3 Berechnung

7.1.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL6900 – PFH_D	1,03E-09
AX5805 – PFH_D	5,15E-09 (siehe Liste der freigegebenen Motoren)
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	60 (1x pro Stunde)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

7.1.3.2 Diagnostic Coverage DC

Komponente	Wert
S1/S2 mit Testung/Plausibilität	DC_{avg}=99%

7.1.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

$$MTTF_D = \frac{1.000.000}{0{,}1 * 1840} = 5434{,}8y = 47608848h$$

S2:

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

$$MTTF_D = \frac{2.000.000}{0{,}1 * 1840} = 10869{,}6y = 95217696h$$

und der Annahme, dass S1 und S2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

S2:

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

Nun sind folgende Annahmen zu treffen:

Die Türschalter S1/S2 werden immer gegenläufig betätigt. Da die Schalter verschiedene Werte haben, der vollständige Schutztürschalter aber aus einer Kombination von Öffner und Schließer besteht und beide Schalter funktionieren müssen, kann man den schlechteren der beiden Werte (S1) für die Kombination heranziehen!

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(AX5805)}} + \frac{1}{MTTF_{D(AX5805)}} + \frac{1}{MTTF_{D(AX5805)}} + \frac{1}{MTTF_{D(AX5805)}}$$

mit:

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

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

Sind für EL1904, AX5805 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

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

$$DC_{avg} = \frac{\frac{99\%}{5434,8y} + \frac{99\%}{10869,6y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{221,7y} + \frac{99\%}{221,7y} + \frac{99\%}{221,7y} + \frac{99\%}{221,7y}}{\frac{1}{5434,8y} + \frac{1}{10869,6y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y}}$$
$$= 99,00\%$$

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

7.2 AdvPosMon mit integriertem Geber EnDat 3

Einschränkung für bestimmte Motoren

Das in diesem Kapitel beschriebene Applikationsbeispiel funktioniert ausschließlich für Motoren mit einer Maximalgeschwindigkeit von 0,44 Umdrehungen pro ms.

Die TwinSAFE-Drive-Optionskarte AX8911 für den AX8000 kann für Safe-Motion-Funktionen mit einem integrierten Geber die sicherheitstechnischen Kenngrößen SIL2 / PL d Kategorie 3 erreichen. Wenn der integrierte EnDAT-3-Geber genutzt wird, kann durch Zusatzmaßnahmen auch ein SIL3 / PL e Kategorie 4 erreicht werden. Dazu ist die Verwendung des Funktionsbausteins „AdvPosMon“ zwingend erforderlich, um die Position und Geschwindigkeit zusätzlich zu überwachen.

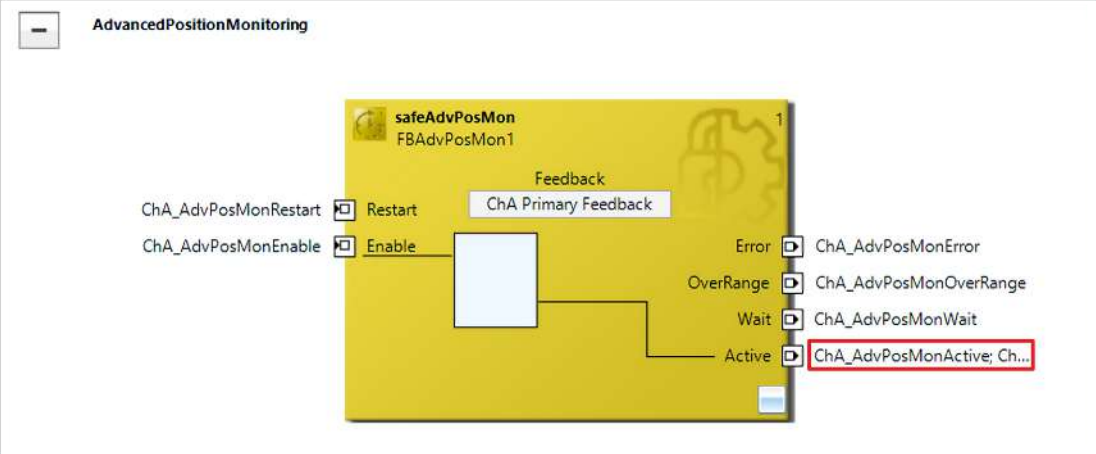
HINWEIS

Integration in Safe-Motion-Funktionen

Sie müssen die Zusatzmaßnahmen in jede Safe-Motion-Funktion integrieren, welche mit SIL3 / PL e Kategorie 4 belastet werden soll.

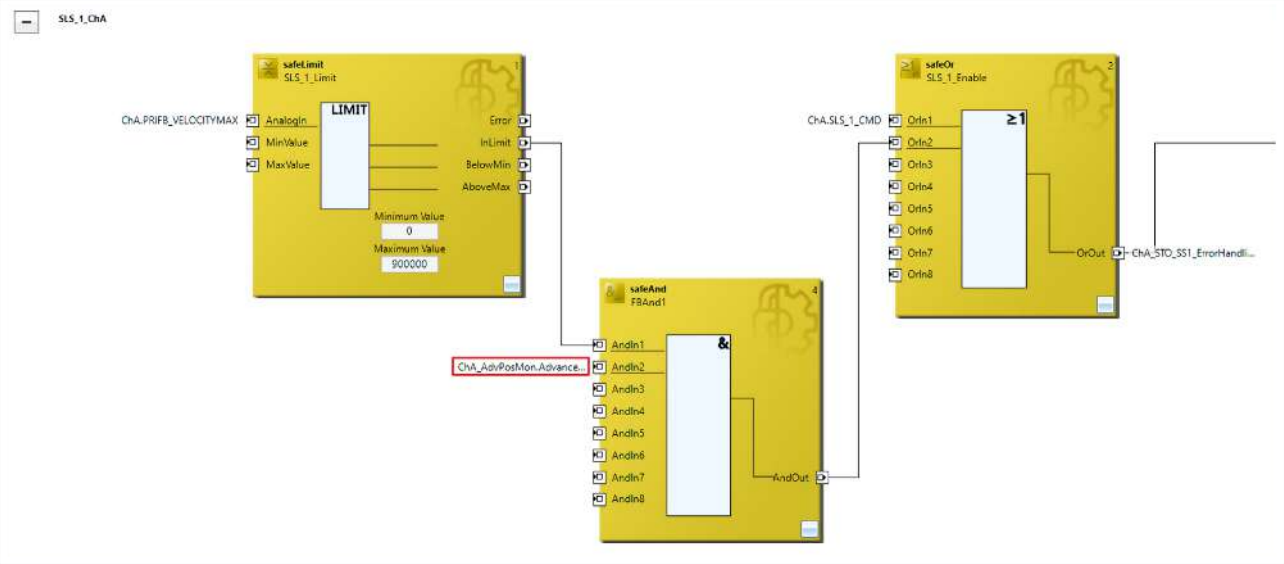
7.2.1 Vorgehensweise

Dieses Kapitel beschreibt die Verwendung des Funktionsbausteins AdvPosMon in einem Safety-Projekt mit einer gewünschten Safe-Motion-Funktion, wie zum Beispiel SLS1.

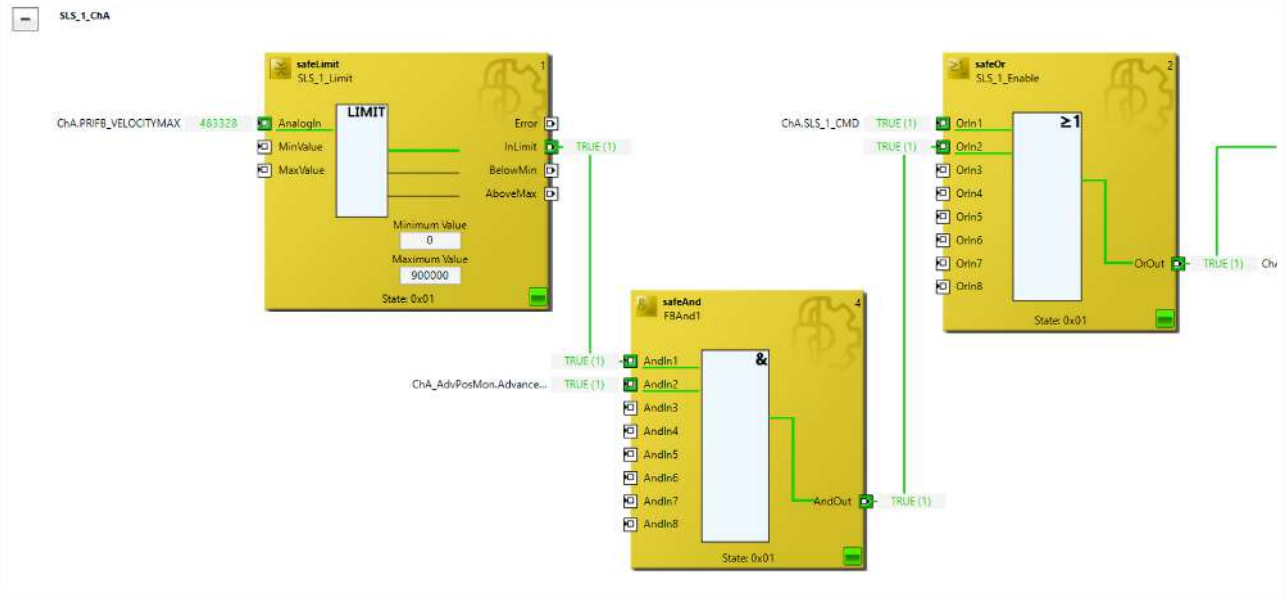


Das Active-Ausgangssignal (rot markiert) des AdvPosMon-Funktionsbausteins zeigt die Aktivität der EnDat-3-SIL3-Zusatzmaßnahmen an. Wenn dieses Signal, wie in diesem Applikationsbeispiel beschrieben, zur Freigabe nachgelagerter Überwachungsfunktionen, wie beispielsweise SLS oder SLP, verwendet wird, dann erreichen diese SIL3/ PL e, Kategorie 4 unter Berücksichtigung der genannten Funktionseinschränkung.

Zur Verwendung des AdvPosMon-Funktionsbausteins muss das Active-Ausgangssignal in die gewünschte Applikation integriert werden. Die Aktivierung und Deaktivierung der erweiterten Überwachung erfolgen über den Enable-Eingang. Falls ein OverRange-Fehler auftritt, kann über Restart der Fehler resettet werden, sofern das Restart-Signal in der Applikation verwendet wird.



Die oben aufgeführte Abbildung zeigt die Integration des Active-Ausgangssignals (rot markiert) in die gewünschte Applikation. Das Active-Ausgangssignal ist mit dem Funktionsbaustein SafeAnd verbunden und so in der SLS1-Konfiguration integriert.



Im Online View des Safety Editors werden die Aktivität des Active-Signals des Funktionsbausteins AdvPosMon sowie der Status der SLS1-Konfiguration angezeigt.

8 Analogwertverarbeitung mit TwinSAFE SC

8.1 Überwachung Drehzahl (Kategorie 3, PL d)

Die Drehzahl eines Antriebes soll überwacht werden. Dieser Antrieb hat eine Sicherheitsfunktion (hier z.B. STO), welcher über einen entsprechenden Eingang aktiviert wird. Dieser Eingang wird über jeweils einen Arbeitskontakt zweier Schütze geführt. Die Positions- und Geschwindigkeitssignale werden über 2 unterschiedliche Kommunikationswege zur TwinSAFE Logik EL6910 übertragen und dort entsprechend der dargestellten Logik verarbeitet. Der Sin/Cos Encoder wird auf eine EL5021-0090 verdrahtet und die Positionsinformation wird über eine TwinSAFE SC Kommunikation über EtherCAT übermittelt. Die Geschwindigkeit des Antriebs wird über die Standard PROFINET-Kommunikation (es ist auch jeder andere Feldbus möglich) und die Standard SPS ebenfalls an die TwinSAFE Logik EL6910 übergeben.

Innerhalb der sicherheitsgerichteten Logik EL6910 wird aus dem Positionswert eine Geschwindigkeit (FB Speed) berechnet. Die Geschwindigkeit des Antriebs wird über den FB Scale skaliert, so dass der Wert zu der berechneten Geschwindigkeit passt. Diese beiden Geschwindigkeitswerte werden über einen FB Compare auf Gleichheit überprüft und über einen FB Limit auf einen Maximalwert überwacht. Da die beiden Geschwindigkeitswerte (einmal direkt und einmal in der sicherheitsgerichteten Logik EL6910 berechnet) zu keiner Zeit eine hundertprozentige Gleichheit aufweisen, muss die Differenz der beiden Geschwindigkeitswerte innerhalb des Toleranzbandes von 10% liegen, um die Bedingung der Gleichheit noch zu erfüllen. Ist der aktuelle Geschwindigkeitswert unterhalb der im FB Limit festgelegten Grenze, wird der STO Ausgang auf logisch 1 gesetzt und der Antrieb kann drehen. Ist die Grenze überschritten oder der Vergleich ungültig, wird der Ausgang auf logisch 0 gesetzt und der Antrieb wird momentenfrei geschaltet bzw. die im Antrieb integrierte Sicherheitsfunktion aktiviert. Die gesamte Berechnung und Skalierung wird in der sicherheitsgerichteten Logik EL6910 auf dem Sicherheitsniveau SIL3 / PL e durchgeführt. Mit dieser Methode wird aus zwei nicht sicherheitsgerichteten Signalen ein sicherheitsgerichtetes Ergebnis erzeugt.

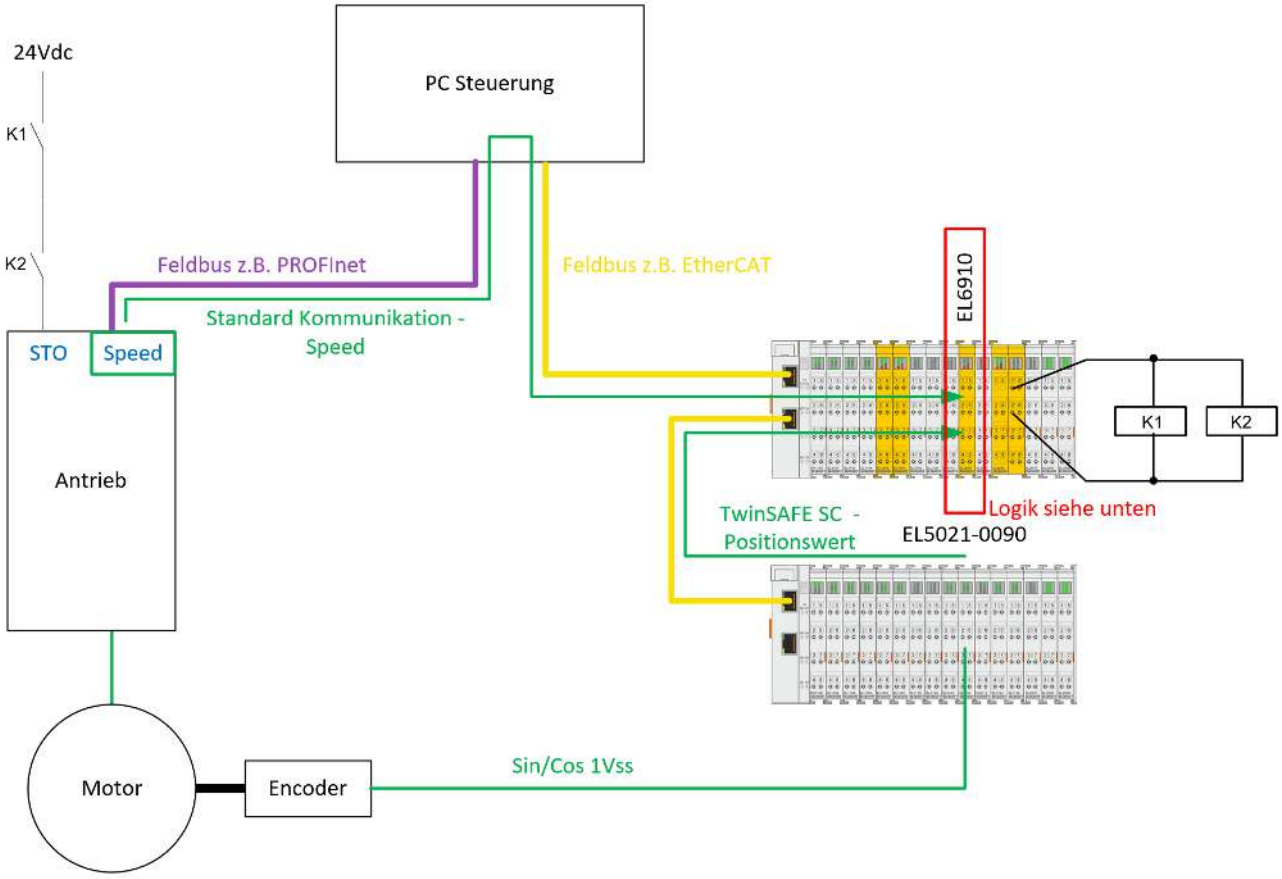
Über einen ESTOP Baustein wird zusätzlich eine Nothalt-Funktion implementiert (der Übersichtlichkeit halber nicht in der Graphik dargestellt), welche den Wiederanlauf verhindert und auch die Schützkontrolle für K1 und K2 übernimmt.

Das IsValid Signal des Compare-Bausteins muss zur Abschaltung im Fehlerfall verwendet werden.

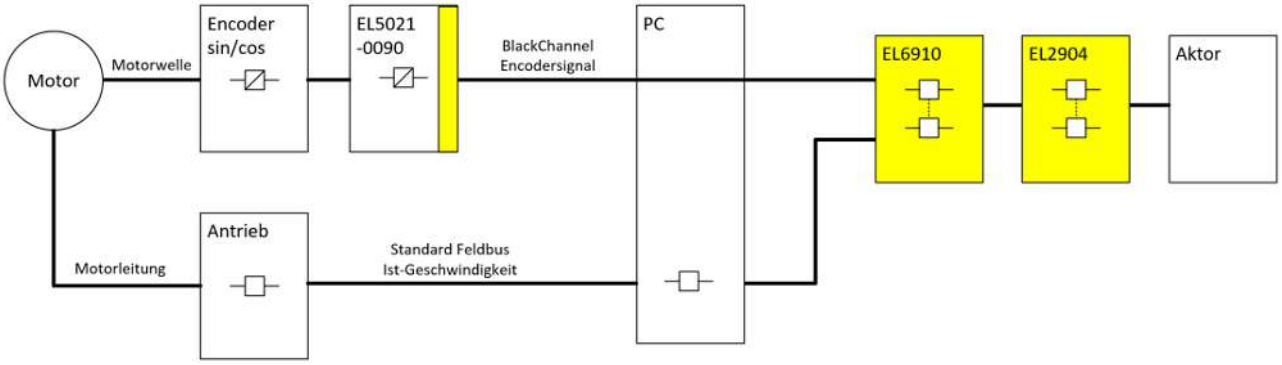
Eine Auswahl an alternativen TwinSAFE SC-Produkten, die für dieses Applikationsbeispiel herangezogen werden können, entnehmen Sie der folgenden Tabelle. Die in diesem Beispiel beschriebenen Annahmen und Argumentationen müssen weiterhin berücksichtigt werden.

Beispiel Drehzahlüberwachung: Antrieb mit Sicherheitsfunktion (z. B. STO) und Sin/Cos-Encoder mit EL5021-0090		
Alternative TwinSAFE SC-Encoder-Klemmen zur Positions- und Geschwindigkeits- bzw. Frequenzübertragung	EL5001-0090	EtherCAT-Klemme, 1-Kanal-Encoder-Interface, SSI, TwinSAFE SC
	EL5101-0090	EtherCAT-Klemme, 1-Kanal-Encoder-Interface, inkremental, 5 V DC (DIFF RS422, TTL), 1 MHz, TwinSAFE SC
	EL5151-0090	EtherCAT-Klemme, 1-Kanal-Encoder-Interface, inkremental, 24 V DC HTL, 100 kHz, TwinSAFE SC
	EL5021-0090	EtherCAT-Klemme, 1-Kanal-Encoder-Interface, SinCos, 1 Vss, TwinSAFE SC
	EL5032-0090	EtherCAT-Klemme, 2-Kanal-Encoder-Interface, EnDat 2.2, TwinSAFE SC

Aufbau



Strukturbild Aufbau



Logik

8.1.1 Struktur und Diagnose

Die eingelesenen Signale vom Antrieb und vom Geber sind Standard Signale, die dynamisch und unterschiedlich sind. Der Antrieb liefert einen Geschwindigkeitswert, der Encoder liefert ein sin/cos Signal, welches von einer Standardklemme ausgewertet wird und in ein sicheres Telegramm (FSoE mit geändertem Polynom - TwinSAFE SC) verpackt und übertragen wird.

Diese Klemme (EL5021-0090) liefert einen Positionswert, der innerhalb der sicheren Logik auf einen Geschwindigkeitswert umgerechnet wird und dann skaliert und mit dem Geschwindigkeitswert des Antriebs verglichen wird. Gleichheit bedeutet in diesem Fall, dass das Differenzsignal in dem Toleranzfenster von 10% liegt.

Die Übermittlung des Encoder Signals über den Standard-Feldbus wird über das Black-Channel Prinzip durchgeführt. Dieser Wert wird mit der Antriebsgeschwindigkeit, die über den Standard-Feldbus übermittelt wird, plausibilisiert. Fehler in einem der beiden Kanäle werden über den Vergleich der beiden diversitären Geschwindigkeits- bzw. Positionssignale innerhalb der sicheren Logik erkannt und führen zur Aktivierung von STO des Antriebs.

8.1.2 FMEA

Fehlerannahme	Erwartungshaltung	Überprüft
Geschwindigkeitswert über z.B. PROFINET selbst friert ein	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt (anderer Feldbus und TwinSAFE SC Kommunikation zwischen EL5021-0090 und EL6910). Zusätzlich sollte für die Drehzahl 0 der Standard-Kommunikations-Watchdog aktiviert sein.	
Geschwindigkeitswert über EtherCAT und TwinSAFE SC Kommunikation friert ein	Wird über den Watchdog innerhalb der TwinSAFE SC Kommunikation erkannt. Plausibilitätsprüfung: Wenn der Motor gestartet wird, werden auch dynamische Geschwindigkeitswerte erwartet.	
Geschwindigkeitswerte werden in der Standard SPS aufeinander kopiert	Ein verfälschter Wert innerhalb der TwinSAFE SC Kommunikation führt zu einer ungültigen CRC innerhalb des Telegramms und damit zur sofortigen Abschaltung der Gruppe und der Ausgänge. Die Datentypen der beiden Geschwindigkeitswerte haben eine unterschiedliche Länge (z.B. 4 Byte und 11 Byte)	
Geschwindigkeitswert über z.B. PROFINET wird verfälscht	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt (anderer Feldbus und TwinSAFE SC Kommunikation zwischen EL5021-0090 und EL6910)	
Verbindung zwischen Motor und Encoder ist nicht mehr gegeben	Wird über die Plausibilisierung mit dem Geschwindigkeitswert des Antriebs innerhalb der EL6910 erkannt. Plausibilitätsprüfung: Wenn der Motor gestartet wird, werden auch dynamische Geschwindigkeitswerte erwartet.	
Encoder liefert falschen Positionswert	Wird über die Plausibilisierung mit dem Geschwindigkeitswert des Antriebs innerhalb der EL6910 erkannt	
Antrieb liefert falschen Geschwindigkeitswert	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt (anderer Feldbus und TwinSAFE SC Kommunikation zwischen EL5021-0090 und EL6910)	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verfälschung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Unbeabsichtigte Wiederholung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt. Zusätzlich sollte für die Drehzahl 0 der Standard-Kommunikations-Watchdog aktiviert sein.	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Falsche Abfolge	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verlust	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Inakzeptable Verzögerung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt. Zusätzlich sollte für die Drehzahl 0 der Standard-Kommunikations-Watchdog aktiviert sein.	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Einfügung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Maskerade	nicht relevant für Standard, sondern nur für Safety Kommunikation.	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Adressierung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler für Standard-Kommunikation: Wiederkehrende Speicherfehler in Switches	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	

8.1.2.1 Anmerkung TwinSAFE SC Kommunikation:

Die TwinSAFE SC Kommunikation verwendet die identischen Mechanismen zur Fehleraufdeckung, wie die Safety-over-EtherCAT Kommunikation mit dem Unterschied, dass zur Berechnung der Prüfsumme eine anderes Polynom verwendet wird, welches hinreichend unabhängig von dem bisher für Safety-over-EtherCAT verwendetem Polynom ist.

Es sind die identischen Mechanismen aktiv, wie z.B. Black-Channel Prinzip (Bitfehlerwahrscheinlichkeit 10^{-2}).

Die Qualität der Datenübertragung ist nicht entscheidend, da letztendlich über den Vergleich in der sicheren Logik alle Übertragungsfehler aufgedeckt werden, da diese zur Ungleichheit führen würden.

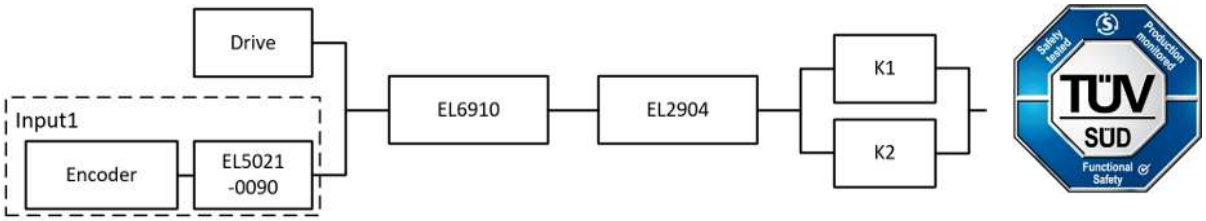
8.1.3 Parameter der sicheren Ausgangsklemme

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

8.1.4 Blockbildung und Safety-Loops

8.1.4.1 Sicherheitsfunktion 1



8.1.5 Berechnung

8.1.5.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6910 – PFH_D	1,79E-09
Antrieb (Drive) – MTBF	516.840 (59a)

Komponente	Wert
Encoder – MTTF	549.149
EL5021-0090 - MTBF	1.205.000
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

8.1.5.2 Diagnostic Coverage DC

Komponente	Wert
Antrieb und Encoder mit EL5021-0090 und Plausibilität innerhalb der Logik	DC_{avg}=90% (Alternativ in Berechnung: 99%)
K1/K2 mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) mit Testung der einzelnen Kanäle	DC_{avg}=99%

8.1.5.3 Berechnung Sicherheitsfunktion 1

Zur Verdeutlichung wird der Sicherheitskennwert sowohl nach EN 62061 als auch nach EN 13849 berechnet. In der Praxis ist die Berechnung nach einer Norm ausreichend.

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den MTBF-Werten:

Anmerkung: Reparaturzeiten können vernachlässigt werden, daher gilt:

$$MTTF_D = 2 * MTBF$$

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

mit

$$\lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

ergibt sich für

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

Eingesetzt ergibt das:

Antrieb

$$MTTF_D = 2 * MTBF = 2 * 59y = 1.033.680h = 118y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.033.680h} = 9,67E - 08$$

Encoder

$$MTTF_D = 2 * MTTF = 2 * 549149h = 1.098.298h = 125y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.098.298h} = 9,10E - 08$$

EL5021-0090

$$MTTF_D = 2 * MTBF = 2 * 1.205.000h = 2.410.000h = 275y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.410.000h} = 4,15E - 08$$

Eingangs-Subsystem 1

$$PFH_{(Input1)} = PFH_{(Encoder)} + PFH_{(EL5021-0090)} = 9,10E - 08 + 4,15E - 08 = 13,25E - 08$$

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

K1/K2: Betätigung 1/Woche und direktes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Die Eingangssignale aus Encoder mit EL5021-0090 und Antrieb haben unterschiedliche Messverfahren, liefern unterschiedlich skalierte Werte und sind beide an der Sicherheitsfunktion beteiligt. Ein Nichtfunktionieren eines Kanals führt nicht zu einer gefährlichen Situation, sondern wird über den Vergleich der beiden Werte in der TwinSAFE Logik erkannt und führt zur Abschaltung.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält Tabellen (Tabelle F.1-Kriterien zur Bestimmung des CCF und Tabelle F.2-Abschätzung des CCF-Faktors(β)), mit der dieser β–Faktor genau bestimmt werden kann. Für das Eingangssubsystem kann bei entsprechender Bearbeitung der Tabelle zur Berechnung des β-Faktors ein Wert von schätzungsweise 2% erreicht werden. In der folgenden Berechnung wird der Worst-Case mit 10% angenommen.

Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Drive)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Drive)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ und $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Antrieb)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

$$PFH_{ges} = 10\% * \frac{13,25E-08 + 9,67E-08}{2} + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 1,45E-08$$

HINWEIS

EN 62061

Entsprechend der EN 62061 wird das Eingangssubsystem mit einer SFF bzw. einem DC von 90% bewertet. Dies schränkt den erreichbaren SIL Wert gemäß Tabelle 5 der EN 62061 auf maximal SIL 2 ein.

Alternative Berechnung des $MTTF_D$-Wertes nach EN 13849 für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

Aus dem Eingangssubsystem, wird der schlechtere Wert genommen (hier Kombination Encoder und EL5021-0090):

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL5021-0090)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

mit:

Sind für EL2904 und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{125y} + \frac{1}{275y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y}} = 69,9y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL5021-0090)}} + \frac{DC}{MTTF_{D(Drive)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL5021-0090)}} + \frac{1}{MTTF_{D(Drive)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{90\%}{125y} + \frac{90\%}{275y} + \frac{90\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{125y} + \frac{1}{275y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 90,78\%$$

Alternativ mit DC=99%

$$DC_{avg} = \frac{\frac{99\%}{125y} + \frac{99\%}{275y} + \frac{99\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{125y} + \frac{1}{275y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99{,}00\%$$

⚠ VORSICHT

Kategorie

Diese Struktur ist bis maximal Kategorie 3 möglich.

⚠ WARNUNG

Stillstand

Im Stillstand des Motors wird ein Fehler, wie z.B. das Einfrieren eines Encoder-Signales erst mit Anforderung einer Bewegung detektiert. Dies muss durch den Maschinenbauer bzw. Anwender berücksichtigt werden.

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Alternative mit DC=99% für das Eingangs-Subsystem:

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2	**≥ 10^{-7} bis < 10^{-6}**
1	≥ 10^{-6} bis < 10^{-5}

8.2 Überwachung Drehzahl (über IO-Link) (Kategorie 3, PL d)

Die Drehzahl eines Antriebes soll überwacht werden. Dieser Antrieb hat eine Sicherheitsfunktion (hier z.B. STO), welche über einen entsprechenden Eingang aktiviert wird. Dieser Eingang wird über jeweils einen Arbeitskontakt zweier Schütze geführt.

Die Geschwindigkeitssignale werden über 2 unterschiedliche Arten zur TwinSAFE Logik EL6910 übertragen und dort entsprechend der dargestellten Logik verarbeitet. Der IO-Link Encoder wird auf eine EL6224-0090 verdrahtet und die Geschwindigkeitsinformation wird über eine TwinSAFE SC Kommunikation übermittelt. Die Geschwindigkeit des Antriebs wird über die Standard PROFINET Kommunikation (es ist auch jeder andere Feldbus möglich) und die Standard SPS ebenfalls an die TwinSAFE Logik EL6910 übergeben.

Innerhalb der sicherheitsgerichteten Logik EL6910 werden die beiden Geschwindigkeiten über den FB Scale skaliert, so dass die Werte zueinander passen. Diese beiden Geschwindigkeitswerte werden über einen FB Compare auf Gleichheit überprüft und über einen FB Limit auf einen Maximalwert überwacht. Da die beiden Geschwindigkeitswerte zu keiner Zeit eine 100 prozentige Gleichheit aufweisen, muss die Differenz der beiden Geschwindigkeitswerte innerhalb des Toleranzbandes von 10% liegen, um die Bedingung der Gleichheit noch zu erfüllen. Ist der aktuelle Geschwindigkeitswert unterhalb der im FB Limit festgelegten Grenze, wird der STO Ausgang auf logisch 1 gesetzt und der Antrieb kann drehen. Ist die Grenze überschritten oder der Vergleich ungültig, wird der Ausgang auf logisch 0 gesetzt und der Antrieb wird momentenfrei geschaltet bzw. die im Antrieb integrierte Sicherheitsfunktion aktiviert. Die gesamte Berechnung und Skalierung wird in der sicherheitsgerichteten Logik EL6910 auf dem Sicherheitsniveau SIL3 / PL e durchgeführt. Mit dieser Methode wird aus zwei nicht sicherheitsgerichteten Signalen ein sicherheitsgerichtetes Ergebnis erzeugt.

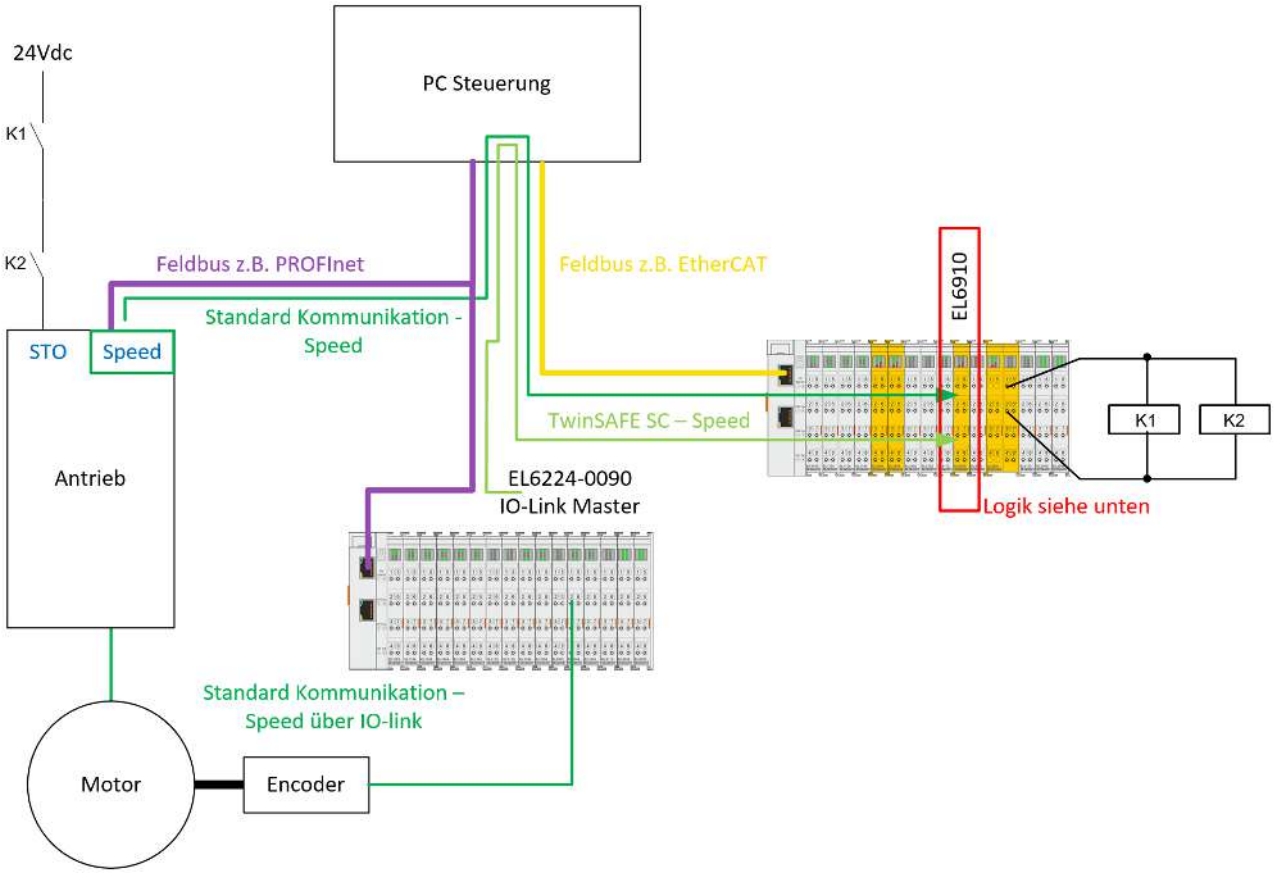
Über einen ESTOP Baustein wird zusätzlich eine Nothalt-Funktion implementiert (der Übersichtlichkeit halber nicht in der Graphik dargestellt), welche den Wiederanlauf verhindert und auch die Schützkontrolle für K1 und K2 übernimmt.

Das IsValid Signal des Compare-Bausteins muss zur Abschaltung im Fehlerfall verwendet werden.

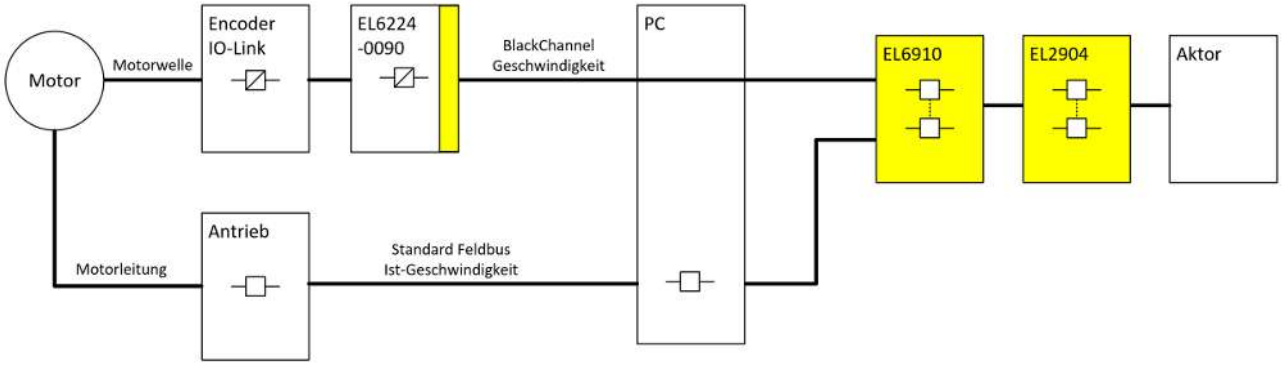
Eine Auswahl an alternativen TwinSAFE SC-Produkten, die für dieses Applikationsbeispiel herangezogen werden können, entnehmen Sie der folgenden Tabelle. Die in diesem Beispiel beschriebenen Annahmen und Argumentationen müssen weiterhin berücksichtigt werden.

Beispiel Drehzahlüberwachung: Antrieb mit Sicherheitsfunktion (z. B. STO) und IO-Link-Encoder mit EL6224-0090		
Alternative TwinSAFE SC-Encoder-Klemmen zur Positions- und Geschwindigkeits- bzw. Frequenzübertragung	EL5001-0090	EtherCAT-Klemme, 1-Kanal-Encoder-Interface, SSI, TwinSAFE SC
	EL5101-0090	EtherCAT-Klemme, 1-Kanal-Encoder-Interface, inkremental, 5 V DC (DIFF RS422, TTL), 1 MHz, TwinSAFE SC
	EL5151-0090	EtherCAT-Klemme, 1-Kanal-Encoder-Interface, inkremental, 24 V DC HTL, 100 kHz, TwinSAFE SC
	EL5021-0090	EtherCAT-Klemme, 1-Kanal-Encoder-Interface, SinCos, 1 Vss, TwinSAFE SC
	EL5032-0090	EtherCAT-Klemme, 2-Kanal-Encoder-Interface, EnDat 2.2, TwinSAFE SC

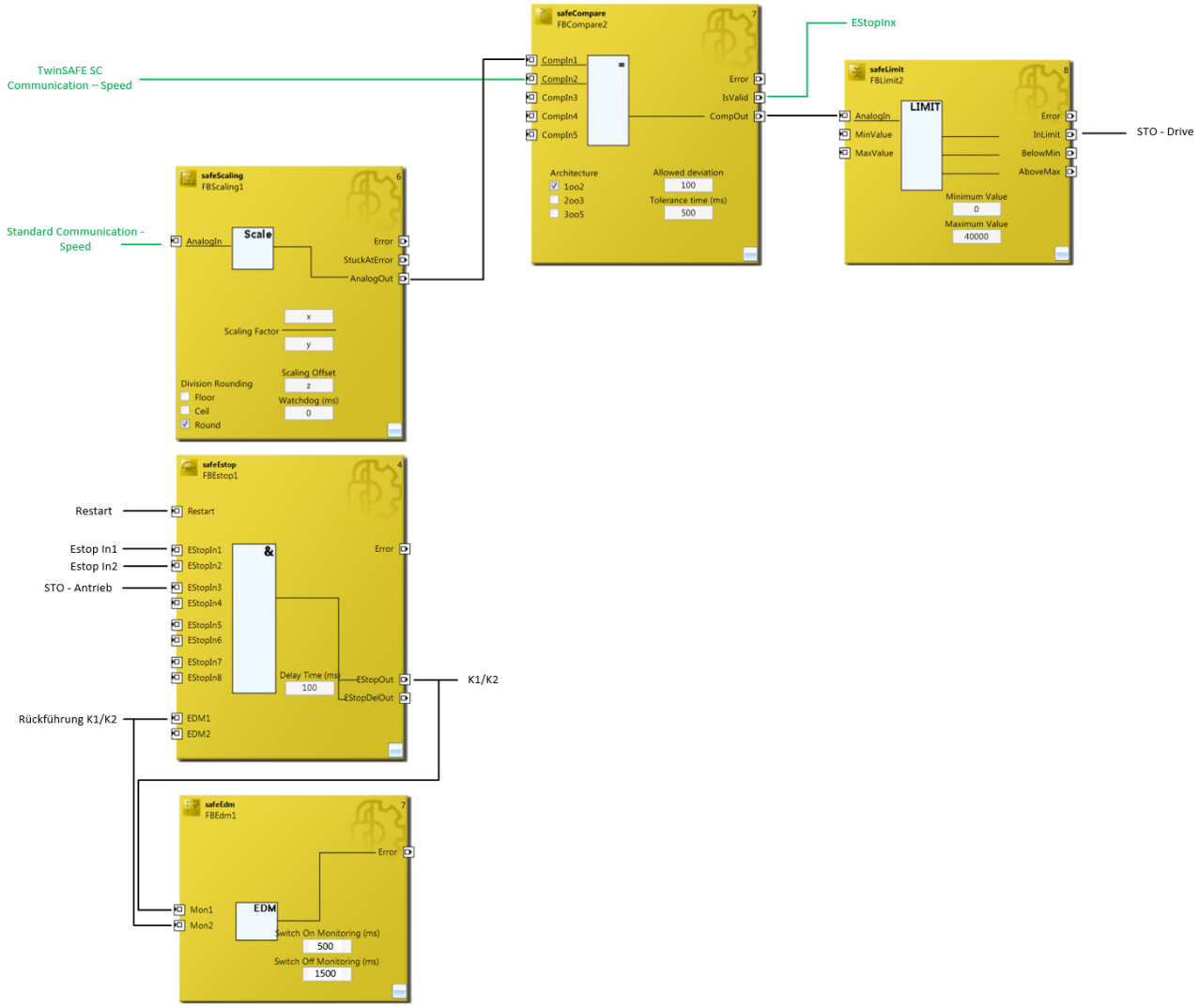
Aufbau IO-Link



Strukturbild Aufbau



Logik



8.2.1 Struktur und Diagnose

Die eingelesenen Signale vom Antrieb und vom Geber sind Standard Signale, die jedoch sehr unterschiedlich sind. Der Antrieb liefert einen Geschwindigkeitswert, der Encoder liefert ein IO-Link Signal, welches von einer Standardklemme ausgewertet wird und in ein sicheres Telegramm (FSoE mit geändertem Polynom - TwinSAFE SC) verpackt und übertragen wird. Diese Klemme (EL6224-0090) liefert einen Geschwindigkeitswert, der innerhalb der sicheren Logik skaliert wird und mit dem Geschwindigkeitswert des Antriebs verglichen wird. Gleichheit bedeutet in diesem Fall, dass das Differenzsignal in dem Toleranzfenster von 10% liegt.

Die Übermittlung des IO-Link Encoder Signals über den Standard-Feldbus wird über das Black-Channel Prinzip durchgeführt. Dieser Wert wird mit der Antriebsgeschwindigkeit, die über den Standard-Feldbus übermittelt wird, plausibilisiert. Fehler in einem der beiden Kanäle werden über den Vergleich der beiden diversitären Geschwindigkeitssignale innerhalb der sicheren Logik erkannt und führen zur Aktivierung von STO des Antriebs.

8.2.2 FMEA

Fehlerannahme	Erwartungshaltung	Überprüft
Geschwindigkeitswert z.B. über PROFINET selbst friert ein	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt (TwinSAFE SC Kommunikation zwischen EL6224-0090 und EL6910).	

Fehlerannahme	Erwartungshaltung	Überprüft
	Zusätzlich sollte für die Drehzahl 0 der Standard-Kommunikations-Watchdog aktiviert sein.	
Geschwindigkeitswert über EtherCAT und TwinSAFE SC Kommunikation friert ein	Wird über den Watchdog innerhalb der TwinSAFE SC Kommunikation erkannt. Plausibilitätsprüfung: Wenn der Motor gestartet wird, werden auch dynamische Geschwindigkeitswerte erwartet.	
Geschwindigkeitswerte werden in der Standard SPS aufeinander kopiert	Ein verfälschter Wert innerhalb der TwinSAFE SC Kommunikation führt zu einer ungültigen CRC innerhalb des Telegramms und damit zur sofortigen Abschaltung der Gruppe und der Ausgänge Die Datentypen der beiden Geschwindigkeitswerte haben eine unterschiedliche Länge (z.B. 4 Byte und 11 Byte)	
Geschwindigkeitswert über z.B. PROFINET wird verfälscht	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt (TwinSAFE SC Kommunikation zwischen EL6224-0090 und EL6910)	
Verbindung zwischen Motor und Encoder ist nicht mehr gegeben	Wird über die Plausibilisierung mit dem Geschwindigkeitswert des Antriebs innerhalb der EL6910 erkannt Plausibilitätsprüfung: Wenn der Motor gestartet wird, werden auch dynamische Geschwindigkeitswerte erwartet.	
Encoder liefert falschen Positionswert	Wird über die Plausibilisierung mit dem Geschwindigkeitswert des Antriebs innerhalb der EL6910 erkannt	
Antrieb liefert falschen Geschwindigkeitswert	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt (TwinSAFE SC Kommunikation zwischen EL6224-0090 und EL6910)	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verfälschung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Unbeabsichtigte Wiederholung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt. Zusätzlich sollte für die Drehzahl 0 der Standard-Kommunikations-Watchdog aktiviert sein.	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Falsche Abfolge	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verlust	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Inakzeptable Verzögerung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt. Zusätzlich sollte für die Drehzahl 0 der Standard-Kommunikations-Watchdog aktiviert sein.	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Einfügung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Maskerade	nicht relevant für Standard-, sondern nur für Safety-Kommunikation.	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Adressierung	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler für Standard-Kommunikation: Wiederkehrende Speicherfehler in Switches	Wird über die Plausibilisierung der Geschwindigkeitswerte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	

8.2.2.1 Anmerkung TwinSAFE SC Kommunikation:

Die TwinSAFE SC Kommunikation verwendet die identischen Mechanismen zur Fehleraufdeckung, wie die Safety-over-EtherCAT Kommunikation mit dem Unterschied, dass zur Berechnung der Prüfsumme eine anderes Polynom verwendet wird, welches hinreichend unabhängig von dem bisher für Safety-over-EtherCAT verwendetem Polynom ist.

Es sind die identischen Mechanismen aktiv, wie z.B. Black-Channel Prinzip (Bitfehlerwahrscheinlichkeit 10^{-2}).

Die Qualität der Datenübertragung ist nicht entscheidend, da letztendlich über den Vergleich in der sicheren Logik alle Übertragungsfehler aufgedeckt werden, da diese zur Ungleichheit führen würden.

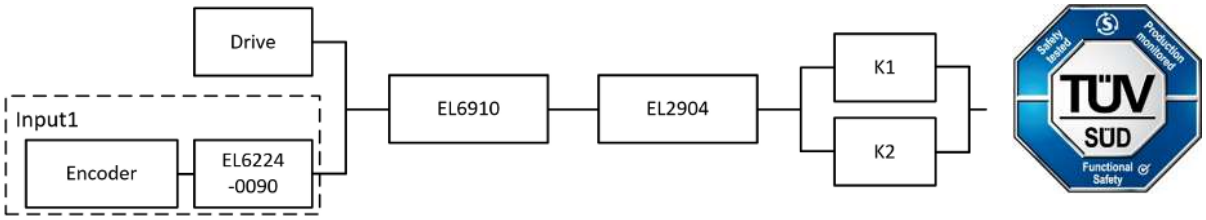
8.2.3 Parameter der sicheren Ausgangsklemme

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

8.2.4 Blockbildung und Safety-Loops

8.2.4.1 Sicherheitsfunktion 1



8.2.5 Berechnung

8.2.5.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6910 – PFH_D	1,79E-09
Antrieb (Drive) – MTBF	516.840 (59y)
Encoder – MTTF	1.208.880 (138y)
EL6224-0090 - MTBF	1.200.000
K1 – $B10_D$	1.300.000

Komponente	Wert
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

8.2.5.2 Diagnostic Coverage DC

Komponente	Wert
Antrieb und Encoder mit EL6224-0090 und Plausibilität innerhalb der Logik	DC_{avg}=90% (Alternativ in Berechnung: 99%)
K1/K2 mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) mit Testung der einzelnen Kanäle	DC_{avg}=99%

8.2.5.3 Berechnung Sicherheitsfunktion 1

Zur Verdeutlichung wird der Sicherheitskennwert sowohl nach EN 62061 als auch nach EN 13849 berechnet. In der Praxis ist die Berechnung nach einer Norm ausreichend.

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den MTBF-Werten:

Anmerkung: Reparaturzeiten können vernachlässigt werden, daher gilt:

$$MTTF_D = 2 * MTBF$$

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

mit

$$\lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

ergibt sich für

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

Eingesetzt ergibt das:

Antrieb

$$MTTF_D = 2 * MTBF = 2 * 59y = 1.033.680h = 118y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.033.680h} = 9{,}67E - 08$$

Encoder

$$MTTF_D = 2 * MTTF = 2 * 1.208.880h = 2.417.760h = 276y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.417.760h} = 4,13E - 08$$

EL6224-0090

$$MTTF_D = 2 * MTBF = 2 * 1.200.000h = 2.400.000h = 273y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.400.000h} = 4,17E - 08$$

Eingangssystem 1

$$PFH_{(Input1)} = PFH_{(Encoder)} + PFH_{(EL6224-0090)} = 4,13E - 08 + 4,17E - 08 = 8,30E - 08$$

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

K1/K2: Betätigung 1/Woche und direktes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Die Eingangssignale aus Encoder mit EL6224-0090 und Antrieb haben unterschiedliche Messverfahren, liefern unterschiedlich skalierte Werte und sind beide an der Sicherheitsfunktion beteiligt. Ein-Nichtfunktionieren eines Kanals führt nicht zu einer gefährlichen Situation, sondern wird über den Vergleich der beiden Werte in der TwinSAFE Logik erkannt und führt zur Abschaltung.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält Tabellen (Tabelle F.1-Kriterien zur Bestimmung des CCF und Tabelle F.2-Abschätzung des CCF-Faktors(β)), mit der dieser β–Faktor genau bestimmt werden kann. Für das Eingangssubsystem kann bei entsprechender Bearbeitung der Tabelle zur Berechnung des β-Faktors ein Wert von schätzungsweise 2% erreicht werden. In der folgenden Berechnung wird der Worst-Case mit 10% angenommen.
Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Drive)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Drive)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+ \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ und $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Antrieb)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

$$PFH_{ges} = 10\% * \frac{8,30E-08 + 9,67E-08}{2} + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 1,2E-08$$

HINWEIS

EN 62061

Entsprechend der EN 62061 wird das Eingangssubsystem mit einer SFF bzw. einem DC von 90% bewertet. Dies schränkt den erreichbaren SIL Wert gemäß Tabelle 5 der EN 62061 auf maximal SIL 2 ein.

Alternative Berechnung des $MTTF_D$-Wertes nach EN 13849 für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

Aus dem Eingangssubsystem, wird der schlechtere Wert genommen (hier der Antrieb):

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Antrieb)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

mit:

Sind für EL2904 und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y}} = 89,7y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL6244-0090)}} + \frac{DC}{MTTF_{D(Antrieb)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6224-0090)}} + \frac{1}{MTTF_{D(Antrieb)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{90\%}{276y} + \frac{90\%}{273y} + \frac{90\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{276y} + \frac{1}{273y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91,30\%$$

Alternativ mit DC=99%

$$DC_{avg} = \frac{\frac{99\%}{276y} + \frac{99\%}{273y} + \frac{99\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{276y} + \frac{1}{273y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99,00\%$$

⚠ VORSICHT

Kategorie

Diese Struktur ist bis maximal Kategorie 3 möglich.

⚠ WARNUNG

Stillstand

Im Stillstand des Motors wird ein Fehler, wie z.B. das Einfrieren eines Encoder-Signales erst mit Anforderung einer Bewegung detektiert. Dies muss durch den Maschinenbauer bzw. Anwender berücksichtigt werden.

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Alternative mit DC=99 % für das Eingangs-Subsystem:

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**

$MTTF_D$	
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

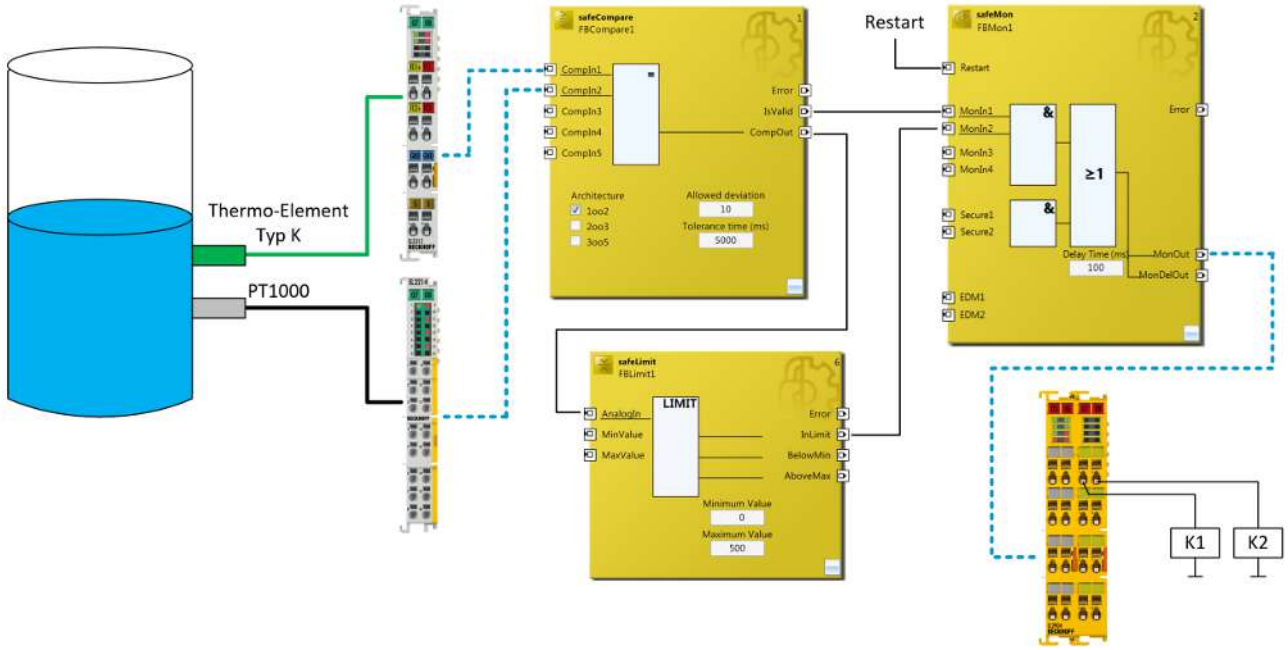
Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2	**≥ 10^{-7} bis < 10^{-6}**
1	≥ 10^{-6} bis < 10^{-5}

8.3 Temperaturmessung mit TwinSAFE SC (Kategorie 3, PL d)

In diesem Beispiel soll gezeigt werden, wie eine Temperaturmessung mit der TwinSAFE SC Technologie realisiert werden kann. Hierzu werden zwei Messstellen mit Temperatursensoren ausgestattet, zum einen mit einem Thermoelement vom Typ K, welches auf eine Standard EtherCAT-Klemme EL3312 verdrahtet ist und zum anderen ein PT1000 - Messwiderstand, der auf eine TwinSAFE SC EtherCAT Klemme EL3214-0090 verdrahtet ist.

Innerhalb der sicheren TwinSAFE-Logik EL6910 werden diese beiden Signale mittels Compare-Baustein verglichen bzw. plausibilisiert. Anschließend wird das Signal über den FB *Limit* überprüft. Das Ergebnis des FB *Limit* und der Ausgang *IsValid* des Compare-Bausteins wird zur Abschaltung der Schütze K1 und K2 über den Baustein *Mon* verwendet.

Die Schützkontrolle wird in diesem Beispiel der Übersichtlichkeit halber nicht dargestellt, ist jedoch durch den Anwender zu berücksichtigen.



⚠ VORSICHT

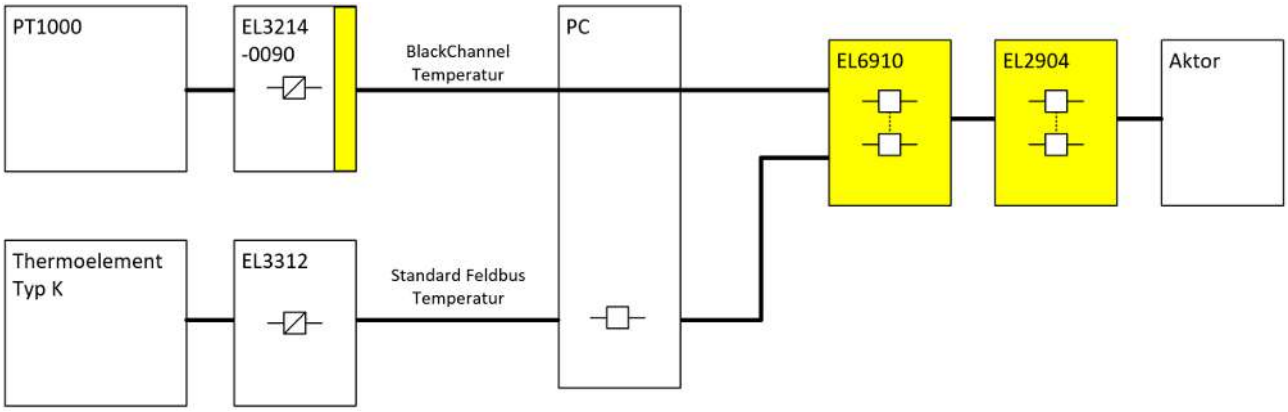
Nothalt / Schützkontrolle!

Neben der oben gezeigten Funktion, muss eine Schützkontrolle, z.B. über einen EDM-Baustein für K1 und K2 und ggf. eine Nothalt-Funktion durch den Anwender realisiert werden!

Eine Auswahl an alternativen TwinSAFE SC-Produkten, die für dieses Applikationsbeispiel herangezogen werden können, entnehmen Sie der folgenden Tabelle. Die in diesem Beispiel beschriebenen Annahmen und Argumentationen müssen weiterhin berücksichtigt werden.

Beispiel Temperaturmessung: Thermoelement Typ K mit EL3312 und Pt100-Messwiderstand mit EL3214-0090
Kein alternatives TwinSAFE SC-Produkt vorhanden.

8.3.1 Strukturbild des Aufbaus



8.3.2 Struktur und Diagnose

Die eingelesenen Signale von den beiden Messstellen sind Standard Signale, die eine unterschiedliche Technologie verwenden. Mindestens ein Signal wird über die TwinSAFE SC Technologie an die sichere TwinSAFE Logik übermittelt, so dass Verfälschungen dieses Signals im PC oder auf dem Übertragungsweg erkannt werden. Die Prüfung auf Gleichheit dieser beiden Signale, innerhalb der zulässigen Toleranzen, wird in der sicheren TwinSAFE Logik durchgeführt.

Die einzelnen Fehlerannahmen und zugehörigen Erwartungshaltungen werden in folgender FMEA Tabelle aufgelistet.

8.3.3 FMEA

Fehlerannahme	Erwartungshaltung	Überprüft
Temperaturwert über den Standard-Feldbus friert ein	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt.	
Temperaturwert über die TwinSAFE SC Kommunikation friert ein	Wird über den Watchdog innerhalb der TwinSAFE SC Kommunikation und über die Plausibilisierung in der EL6910 erkannt.	
Temperaturwerte werden in der Standard SPS aufeinander kopiert	Ein verfälschter Wert innerhalb der TwinSAFE SC Kommunikation führt zu einer ungültigen CRC innerhalb des Telegramms und damit zur sofortigen Abschaltung der Gruppe und der Ausgänge.	
Temperaturwert über den Standard-Feldbus wird verfälscht	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt.	
Verbindung zwischen Sensor und EtherCAT-Klemme ist nicht mehr gegeben	Wird über die Plausibilisierung mit dem zweiten Temperaturwert innerhalb der EL6910 erkannt.	
PT1000 liefert falschen Temperaturwert	Wird über die Plausibilisierung mit dem zweiten Temperaturwert innerhalb der EL6910 erkannt.	
Thermoelement liefert falschen Temperaturwert	Wird über die Plausibilisierung mit dem zweiten Temperaturwert innerhalb der EL6910 erkannt.	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verfälschung	Wird über die Plausibilisierung der Temperaturwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Unbeabsichtigte Wiederholung	Wird über die Plausibilisierung der Temperaturwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Falsche Abfolge	Wird über die Plausibilisierung der Temperaturwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verlust	Wird über die Plausibilisierung der Temperaturwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Inakzeptable Verzögerung	Wird über die Plausibilisierung der Temperaturwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Einfügung	Wird über die Plausibilisierung der Temperaturwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Maskerade	nicht relevant für Standard, sondern nur für Safety Kommunikation.	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Adressierung	Wird über die Plausibilisierung der Temperaturwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler für Standard-Kommunikation: Wiederkehrende Speicherfehler in Switches	Wird über die Plausibilisierung der Temperaturwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	

8.3.3.1 Anmerkung TwinSAFE SC Kommunikation:

Die TwinSAFE SC Kommunikation verwendet die identischen Mechanismen zur Fehleraufdeckung, wie die Safety-over-EtherCAT Kommunikation mit dem Unterschied, dass zur Berechnung der Prüfsumme eine anderes Polynom verwendet wird, welches hinreichend unabhängig von dem bisher für Safety-over-EtherCAT verwendetem Polynom ist.

Es sind die identischen Mechanismen aktiv, wie z.B. Black-Channel Prinzip (Bitfehlerwahrscheinlichkeit 10^{-2}).

Die Qualität der Datenübertragung ist nicht entscheidend, da letztendlich über den Vergleich in der sicheren TwinSAFE Logik alle Übertragungsfehler aufgedeckt werden, da diese zur Ungleichheit führen würden.

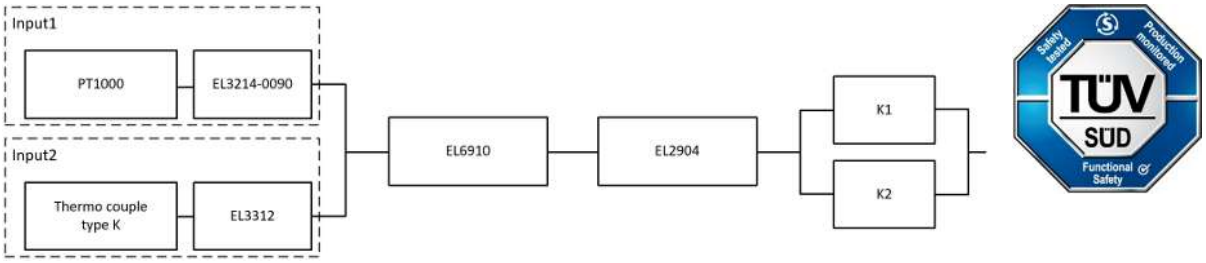
8.3.4 Parameter der sicheren Ausgangsklemme

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Ja

8.3.5 Blockbildung und Safety-Loops

8.3.5.1 Sicherheitsfunktion 1



8.3.6 Berechnung

8.3.6.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL2904 – PFH_D	1,25E-09
EL6910 – PFH_D	1,79E-09
PT1000 – $MTTF_D$	7.618 a (nach Tabelle C.5 EN ISO 13849-1:2023)
Thermoelement Type K – FIT	1900 (Fehleranzahl in 10^9 Stunden)
EL3214-0090 - MTBF	890.000
EL3312 - MTBF	1.661.253
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

8.3.6.2 Diagnostic Coverage DC

Komponente	Wert
Temperaturwerte über TwinSAFE SC und Plausibilität innerhalb der Logik	DC_{avg}=90% (Alternativ in Berechnung: 99%)
K1/K2 mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) mit Testung der einzelnen Kanäle	DC_{avg}=99%

8.3.6.3 Berechnung Sicherheitsfunktion 1

Zur Verdeutlichung wird der Sicherheitskennwert sowohl nach EN 62061 als auch nach EN 13849 berechnet. In der Praxis ist die Berechnung nach einer Norm ausreichend.

Berechnung der PFH_D- und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Berechnung der PFH_D- und $MTTF_D$-Werte aus den MTBF-Werten:

Anmerkung: Reparaturzeiten können vernachlässigt werden, daher gilt:

$$MTTF_D = 2 * MTBF$$

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

mit

$$\lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

ergibt sich für

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

Eingesetzt ergibt das:

PT1000

$$MTTF_D = 7618y = 66.733.680h$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{66.733.680h} = 1{,}50E - 09$$

EL3214-0090

$$MTTF_D = 2 * MTBF = 2 * 890.000h = 1.780.000h = 203y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.780.000h} = 5{,}62E - 08$$

Eingangssystem 1

$$PFH_{(Input1)} = PFH_{(PT1000)} + PFH_{(EL3214-0090)} = 1{,}50E - 09 + 5{,}62E - 08 = 5{,}77E - 08$$

Thermoelement

$$MTTF_D = \frac{1}{\lambda_D} = \frac{1}{1900FIT} * 10^9 h = 526.315h = 60y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{526.315h} = 19{,}0E - 08$$

EL3312

$$MTTF_D = 2 * MTBF = 2 * 1.661.253h = 3.322.506h = 379y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{3.322.506h} = 3{,}0E - 08$$

Eingangssystem 2

$$PFH_{(Input2)} = PFH_{(ThermoCouple)} + PFH_{(EL3312)} = 19{,}0E - 08 + 3{,}0E - 08 = 22{,}0E - 08$$

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

K1/K2: Betätigung 1/Woche und direktes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Die Eingangssignale aus PT1000 mit EL3214-0090 und Thermoelement mit EL3312 haben unterschiedliche Messverfahren, liefern beide einen Temperaturwert und sind beide an der Sicherheitsfunktion beteiligt. Ein-Nichtfunktionieren eines Kanals führt nicht zu einer gefährlichen Situation, sondern wird über den Vergleich der beiden Werte in der TwinSAFE Logik erkannt und führt zur Abschaltung.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält Tabellen (Tabelle F.1-Kriterien zur Bestimmung des CCF und Tabelle F.2-Abschätzung des CCF-Faktors(β)), mit der dieser β–Faktor genau bestimmt werden kann. Für das Eingangssubsystem kann bei entsprechender Bearbeitung der Tabelle zur Berechnung des β-Faktors ein Wert von schätzungsweise 2% erreicht werden. In der folgenden Berechnung wird der Worst-Case mit 10% angenommen.

Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ und $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{ges} = 10\% * \frac{5{,}77E-08 + 22{,}0E-08}{2} + 1{,}79E-09 + 1{,}25E-09 + 10\% * \frac{1{,}92E-12 + 1{,}92E-12}{2}$$
$$= 1{,}693E-08$$

HINWEIS

EN 62061

Entsprechend der EN 62061 wird das Eingangssubsystem mit einer SFF bzw. einem DC von 90% bewertet. Dies schränkt den erreichbaren SIL Wert gemäß Tabelle 5 der EN 62061 auf maximal SIL 2 ein.

Alternative Berechnung des $MTTF_D$-Wertes nach EN 13849 für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit

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

Aus dem Eingangssubsystem, wird der schlechtere Wert genommen:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(ThermoCouple)}} + \frac{1}{MTTF_{D(EL3312)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

Sind für die EL2904 und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{15{,}68E-06\frac{1}{y}} = 637y$$

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{60y} + \frac{1}{379y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 45{,}5y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(PT1000)}} + \frac{DC}{MTTF_{D(EL3214)}} + \frac{DC}{MTTF_{D(Thermocouple)}} + \frac{DC}{MTTF_{D(EL3312)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(PT1000)}} + \frac{1}{MTTF_{D(EL3214)}} + \frac{1}{MTTF_{D(Thermocouple)}} + \frac{1}{MTTF_{D(EL3312)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

Eingesetzt mit DC=90%

$$DC_{avg} = \frac{\frac{90\%}{7618y} + \frac{90\%}{203y} + \frac{90\%}{60y} + \frac{90\%}{379y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{7618y} + \frac{1}{203y} + \frac{1}{60y} + \frac{1}{379y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91{,}11\%$$

Alternativ mit DC=99%

$$DC_{avg} = \frac{\frac{99\%}{7618y} + \frac{99\%}{203y} + \frac{99\%}{60y} + \frac{99\%}{379y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{7618y} + \frac{1}{203y} + \frac{1}{60y} + \frac{1}{379y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99{,}00\%$$

⚠ VORSICHT

Kategorie

Diese Struktur ist bis maximal Kategorie 3 möglich.

DC=90% für das Eingangs-Subsystem

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Alternative mit DC=99% für das Eingangs-Subsystem

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

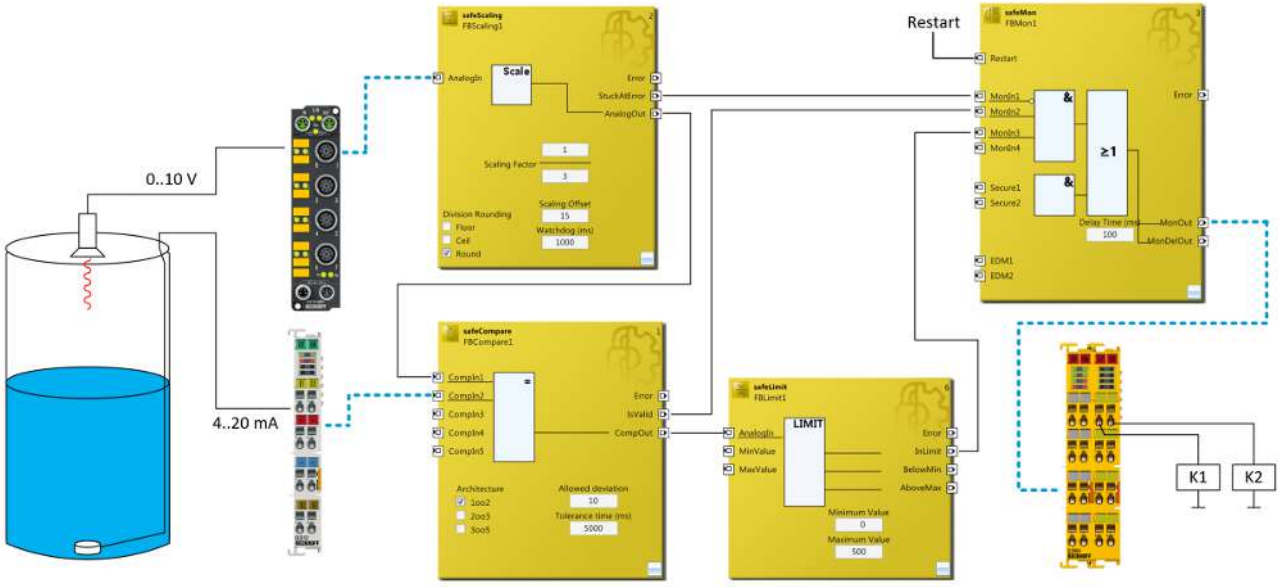
Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2	**≥ 10^{-7} bis < 10^{-6}**
1	≥ 10^{-6} bis < 10^{-5}

8.4 Füllstandsmessung mit TwinSAFE SC (Kategorie 3, PL d)

In diesem Beispiel soll gezeigt werden, wie eine Füllstandsmessung eines Behälters mit der TwinSAFE SC Technologie realisiert werden kann. Hierzu werden zwei unterschiedliche Mess-Methoden verwendet. Zum einen wird ein Ultraschall-Sensor mit einer 0 - 10 V Schnittstelle, welcher auf eine TwinSAFE SC EtherCAT-Box EP3174-0092 verdrahtet ist, verwendet und zum anderen eine Pegelsonde mit einer 4-20 mA Schnittstelle, die auf eine Standard EtherCAT Klemme EL3152 verdrahtet ist.

Innerhalb der sicheren TwinSAFE-Logik EL6910 werden diese beiden Signale mittels Compare-Baustein verglichen bzw. plausibilisiert. Das Signal von der EP3174-0092 wird vorher noch über den Scale-Baustein skaliert, so dass die beiden Signale einen identischen Wertebereich haben. Anschließend wird das Signal über den FB *Limit* überprüft. Das Ergebnis des FB *Limit* und der Ausgang *IsValid* des Compare-Bausteins wird zur Abschaltung der Schütze K1 und K2 über den Baustein *Mon* verwendet. Zusätzlich kann auch noch der StuckAtError Ausgang des Scale-Bausteins auf einen Mon-Eingang gelegt werden. Damit kann ein Einfrieren des Signals erkannt werden.

Die Schützkontrolle wird in diesem Beispiel der Übersichtlichkeit halber nicht dargestellt, ist jedoch durch den Anwender zu berücksichtigen.



⚠ VORSICHT

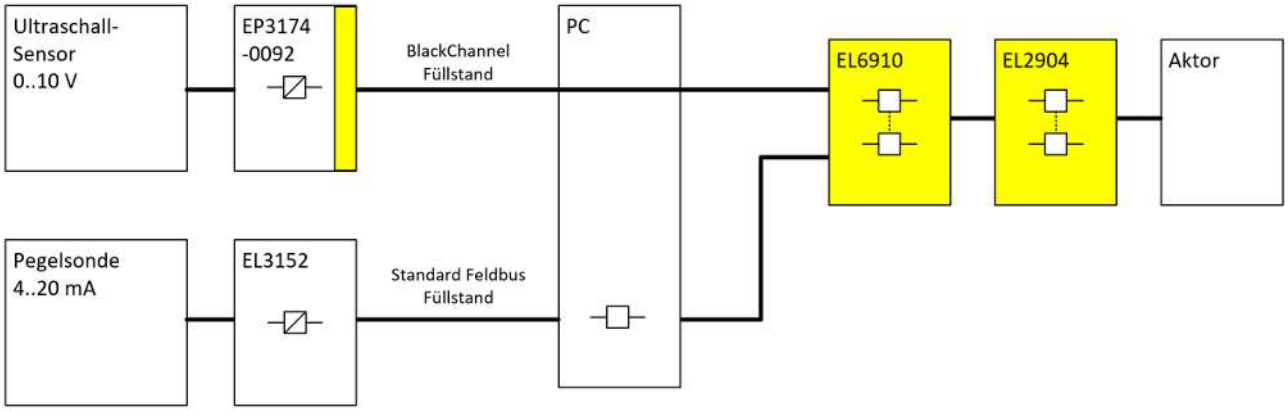
Nothalt / Schützkontrolle

Neben der oben gezeigten Funktion, muss eine Schützkontrolle, z.B. über einen EDM-Baustein für K1 und K2 und ggf. eine Nothalt-Funktion durch den Anwender realisiert werden!

Eine Auswahl an alternativen TwinSAFE SC-Produkten, die für dieses Applikationsbeispiel herangezogen werden können, entnehmen Sie der folgenden Tabelle. Die in diesem Beispiel beschriebenen Annahmen und Argumentationen müssen weiterhin berücksichtigt werden.

Beispiel Füllstandsmessung: Ultraschall-Sensor (0 – 10 V) mit EP3174-0092 und Pegelsonde (4 - 20 mA) mit EL3152		
Alternative TwinSAFE SC-Produkte mit 0 – 10 V und/oder +/- 10-V Analog-Eingang bzw. Sensoren mit IO-Link-Interface	EL3174-0090	EtherCAT-Klemme, 4-Kanal-Analog-Eingang, Multifunktion, ±10 V, ±20 mA, 16 Bit, TwinSAFE SC
	EL6224-0090	EtherCAT-Klemme, 4-Kanal-Kommunikations-Interface, IO-Link, Master, TwinSAFE SC
	EJ6224-0090	EtherCAT-Steckmodul, 4-Kanal-Kommunikations-Interface, IO-Link, Master, TwinSAFE SC
	EP6224-0092	EtherCAT Box, 4-Kanal-Kommunikations-Interface + 4-Kanal-Digital-Eingang, IO-Link, Master, Class A, M12, TwinSAFE SC

8.4.1 Strukturbild des Aufbaus



8.4.2 Struktur und Diagnose

Die eingelesenen Signale von den beiden Messstellen sind Standard Signale, die eine unterschiedliche Technologie verwenden. Mindestens ein Signal wird über die TwinSAFE SC Technologie an die sichere TwinSAFE Logik übermittelt, so dass Verfälschungen dieses Signals im PC oder auf dem Übertragungsweg erkannt werden. Die Prüfung auf Gleichheit dieser beiden Signale, innerhalb der zulässigen Toleranzen, wird in der sicheren TwinSAFE Logik durchgeführt.

Die einzelnen Fehlerannahmen und zugehörigen Erwartungshaltungen werden in folgender FMEA Tabelle aufgelistet.

8.4.3 FMEA

Fehlerannahme	Erwartungshaltung	Überprüft
Füllstandswert über den Standard-Feldbus friert ein	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt.	
Füllstandswert über die TwinSAFE SC Kommunikation friert ein	Wird über den Watchdog innerhalb der TwinSAFE SC Kommunikation und über die Plausibilisierung in der EL6910 erkannt.	
Füllstandswerte werden in der Standard SPS aufeinander kopiert	Ein verfälschter Wert innerhalb der TwinSAFE SC Kommunikation führt zu einer ungültigen CRC innerhalb des Telegramms und damit zur sofortigen Abschaltung der Gruppe und der Ausgänge.	
Füllstandswert über den Standard-Feldbus wird verfälscht	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt.	
Verbindung zwischen Sensor und EtherCAT-Klemme ist nicht mehr gegeben	Wird über die Plausibilisierung mit dem zweiten Füllstandswert innerhalb der EL6910 erkannt.	
Ultraschallsensor liefert falschen Füllstandswert	Wird über die Plausibilisierung mit dem zweiten Füllstandswert innerhalb der EL6910 erkannt.	
Pegelsonde liefert falschen Füllstandswert	Wird über die Plausibilisierung mit dem zweiten Füllstandswert innerhalb der EL6910 erkannt.	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verfälschung	Wird über die Plausibilisierung der Füllstandswerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Unbeabsichtigte Wiederholung	Wird über die Plausibilisierung der Füllstandswerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Falsche Abfolge	Wird über die Plausibilisierung der Füllstandswerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verlust	Wird über die Plausibilisierung der Füllstandswerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Inakzeptable Verzögerung	Wird über die Plausibilisierung der Füllstandswerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Einfügung	Wird über die Plausibilisierung der Füllstandswerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Maskerade	nicht relevant für Standard, sondern nur für Safety Kommunikation.	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Adressierung	Wird über die Plausibilisierung der Füllstandswerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler für Standard-Kommunikation: Wiederkehrende Speicherfehler in Switches	Wird über die Plausibilisierung der Füllstandswerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	

8.4.3.1 Anmerkung TwinSAFE SC Kommunikation:

Die TwinSAFE SC Kommunikation verwendet die identischen Mechanismen zur Fehleraufdeckung, wie die Safety-over-EtherCAT Kommunikation mit dem Unterschied, dass zur Berechnung der Prüfsumme eine anderes Polynom verwendet wird, welches hinreichend unabhängig von dem bisher für Safety-over-EtherCAT verwendetem Polynom ist.

Es sind die identischen Mechanismen aktiv, wie z.B. Black-Channel Prinzip (Bitfehlerwahrscheinlichkeit 10^{-2}).

Die Qualität der Datenübertragung ist nicht entscheidend, da letztendlich über den Vergleich in der sicheren TwinSAFE Logik alle Übertragungsfehler aufgedeckt werden, da diese zur Ungleichheit führen würden.

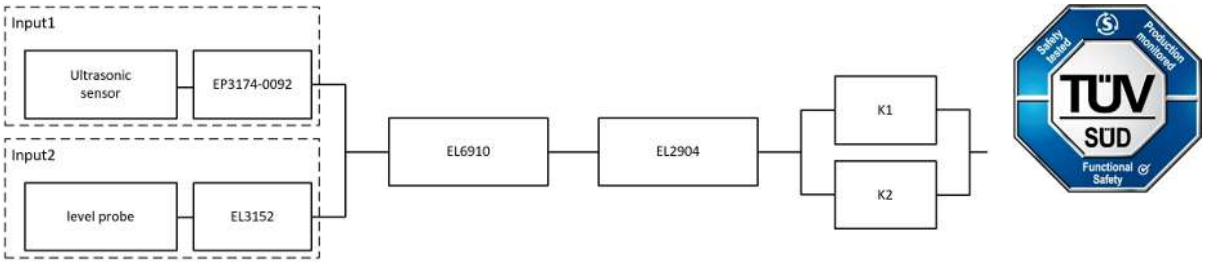
8.4.4 Parameter der sicheren Ausgangsklemme

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Ja

8.4.5 Blockbildung und Safety-Loops

8.4.5.1 Sicherheitsfunktion 1



8.4.6 Berechnung

8.4.6.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL2904 – PFH_D	1,25E-09
EL6910 – PFH_D	1,79E-09
Ultraschallsensor (Ultrasonic Sensor) – MTBF	195 a (1.708.200 h)
Pegelsonde (Level probe) – MTTF	732 a (6.412.320 h)
EP3174-0092 - MTBF	600.000 h
EL3152 - MTBF	2.507.303 h
K1 – $B10_D$	1.300.000 h
K2 – $B10_D$	1.300.000 h
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

8.4.6.2 Diagnostic Coverage DC

Komponente	Wert
Füllstandswerte über TwinSAFE SC und Plausibilität innerhalb der Logik	DC_{avg}=90% (Alternativ in Berechnung: 99%)
K1/K2 mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) mit Testung der einzelnen Kanäle	DC_{avg}=99%

8.4.6.3 Berechnung Sicherheitsfunktion 1

Zur Verdeutlichung wird der Sicherheitskennwert sowohl nach EN 62061 als auch nach EN 13849 berechnet. In der Praxis ist die Berechnung nach einer Norm ausreichend.

Berechnung der PFH_D- und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Berechnung der PFH_D- und $MTTF_D$-Werte aus den MTBF-Werten:

Anmerkung: Reparaturzeiten können vernachlässigt werden, daher gilt:

$$MTTF_D = 2 * MTBF$$

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

mit

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

ergibt sich für

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

Eingesetzt ergibt das:

Ultraschallsensor

$$MTTF_D = 2 * MTBF = 2 * 195y = 390y = 3.416.400h$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.416.400h} = 2,93E - 08$$

EP3174-0092

$$MTTF_D = 2 * MTBF = 2 * 600.000h = 1.200.000h = 136y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.200.000h} = 8,33E - 08$$

Eingangssystem 1

$$PFH_{(Input1)} = PFH_{(Ultrasonic)} + PFH_{(EP3174-0092)} = 2,93E - 08 + 8,33E - 08 = 11,26E - 08$$

Pegelsonde

$$MTTF_D = 2 * MTTF = 2 * 732y = 1.464y = 12.824.640h$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{12.824.640h} = 7,79E - 09$$

EL3152

$$MTTF_D = 2 * MTBF = 2 * 2.507.303h = 5.014.606h = 572y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{5.014.606h} = 1,99E - 08$$

Eingangssystem 2

$$PFH_{(Input2)} = PFH_{(Level\,Probe)} + PFH_{(EL3152)} = 7,79E - 09 + 1,99E - 08 = 2,77E - 08$$

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

K1/K2: Betätigung 1/Woche und direktes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Die Eingangssignale aus Ultraschallsensor mit EP3174-0092 und Pegelsonde mit EL3152 haben unterschiedliche Messverfahren, liefern beide einen Füllstand und sind beide an der Sicherheitsfunktion beteiligt. Ein-Nichtfunktionieren eines Kanals führt nicht zu einer gefährlichen Situation, sondern wird über den Vergleich der beiden Werte in der TwinSAFE Logik erkannt und führt zur Abschaltung.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält Tabellen (Tabelle F.1-Kriterien zur Bestimmung des CCF und Tabelle F.2-Abschätzung des CCF-Faktors(β)), mit der dieser β–Faktor genau bestimmt werden kann. Für das Eingangssubsystem kann bei entsprechender Bearbeitung der Tabelle zur Berechnung des β-Faktors ein Wert von schätzungsweise 2% erreicht werden. In der folgenden Berechnung wird der Worst-Case mit 10% angenommen.

Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ und $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{ges} = 10\% * \frac{11,26E-08 + 2,77E-08}{2} + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 1,005E-08$$

HINWEIS

EN 62061

Entsprechend der EN 62061 wird das Eingangssubsystem mit einer SFF bzw. einem DC von 90% bewertet. Dies schränkt den erreichbaren SIL Wert gemäß Tabelle 5 der EN 62061 auf maximal SIL 2 ein.

Alternative Berechnung des $MTTF_D$-Wertes nach EN 13849 für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit

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

Aus dem Eingangssubsystem, wird der schlechtere Wert genommen:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(UltraSonicSensor)}} + \frac{1}{MTTF_{D(EP3174-0092)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

Sind für die EL2904 und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{15{,}68E-06\frac{1}{y}} = 637y$$

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{390y} + \frac{1}{136y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 79{,}46y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(UltraSonic)}} + \frac{DC}{MTTF_{D(EP3174-0092)}} + \frac{DC}{MTTF_{D(Level\,Probe)}} + \frac{DC}{MTTF_{D(EL3152)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(UltraSonic)}} + \frac{1}{MTTF_{D(EP3174-0092)}} + \frac{1}{MTTF_{D(Level\,Probe)}} + \frac{1}{MTTF_{D(EL3152)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

Eingesetzt mit DC=90%

$$DC_{avg} = \frac{\frac{90\%}{390y} + \frac{90\%}{136y} + \frac{90\%}{1464y} + \frac{90\%}{572y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{390y} + \frac{1}{136y} + \frac{1}{1464y} + \frac{1}{572y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91{,}33\%$$

Alternativ mit DC=99%

$$DC_{avg} = \frac{\frac{99\%}{390y} + \frac{99\%}{136y} + \frac{99\%}{1464y} + \frac{99\%}{572y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{390y} + \frac{1}{136y} + \frac{1}{1464y} + \frac{1}{572y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99{,}00\%$$

⚠ VORSICHT

Kategorie

Diese Struktur ist bis maximal Kategorie 3 möglich.

DC=90% für das Eingangs-Subsystem

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Alternative mit DC=99% für das Eingangs-Subsystem

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

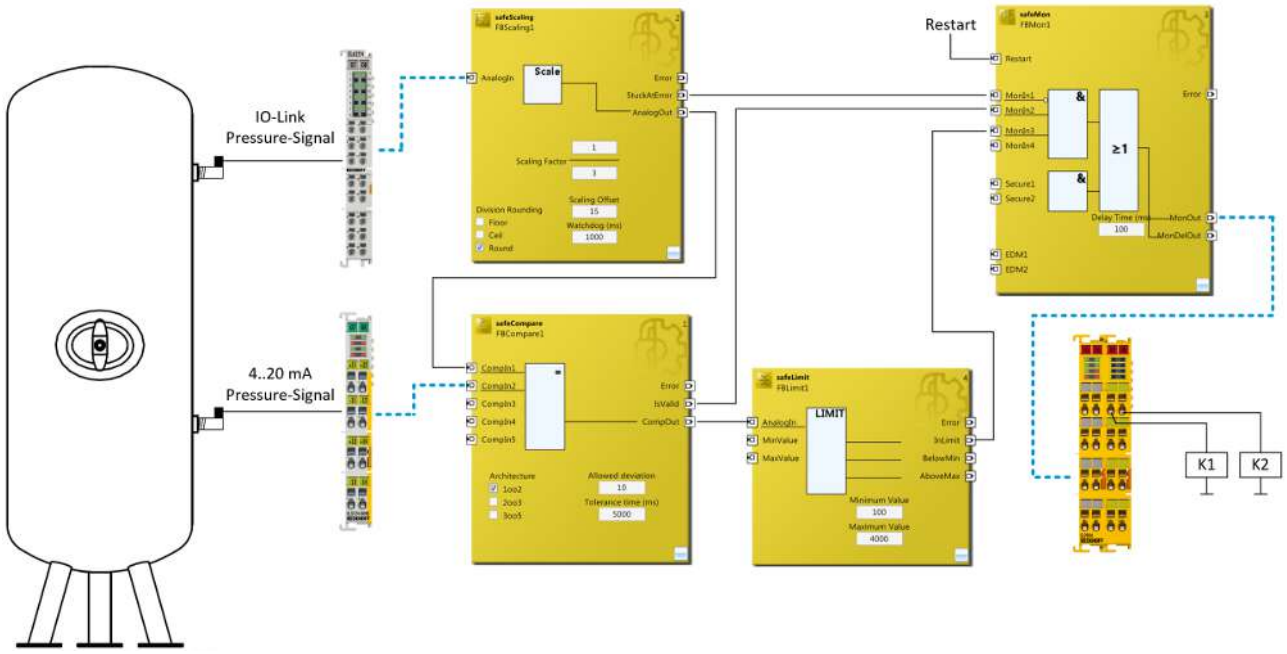
Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2	**≥ 10^{-7} bis < 10^{-6}**
1	≥ 10^{-6} bis < 10^{-5}

8.5 Druckmessung mit TwinSAFE SC (Kategorie 3, PL d)

In diesem Beispiel soll gezeigt werden, wie eine Druckmessung eines Behälters mit der TwinSAFE SC Technologie realisiert werden kann. Hierzu werden zwei Messstellen mit Drucksensoren ausgestattet, zum einen mit einem Drucksensor mit IO-Link Schnittstelle, welcher auf eine Standard EtherCAT-Klemme EL6224 verdrahtet ist und zum anderen ein Drucksensor mit 4-20 mA Schnittstelle, der auf eine TwinSAFE SC EtherCAT Klemme EL3124-0090 verdrahtet ist.

Innerhalb der sicheren TwinSAFE-Logik EL6910 werden diese beiden Signale mittels Compare-Baustein verglichen bzw. plausibilisiert. Das Signal von der EL6224 wird vorher noch über den Scale-Baustein skaliert, so dass die beiden Signale einen identischen Wertebereich haben. Anschließend wird das Signal über den FB *Limit* überprüft. Das Ergebnis des FB *Limit* und der Ausgang *IsValid* des Compare-Bausteins wird zur Abschaltung der Schütze K1 und K2 über den Baustein *Mon* verwendet. Zusätzlich kann auch noch der StuckAtError-Ausgang des Scale-Bausteins auf einen Mon-Eingang gelegt werden. Damit kann ein Einfrieren des Signals erkannt werden.

Die Schützkontrolle wird in diesem Beispiel der Übersichtlichkeit halber nicht dargestellt, ist jedoch durch den Anwender zu berücksichtigen.



⚠ WARNUNG

Sicherheitsventil (PSV - Pressure Safety Valve)!

Die oben gezeigte Applikation kann nicht als Ersatz für ein Sicherheitsventil entsprechend der EG Druckgeräterichtlinie verwendet werden.

⚠ VORSICHT

Nothalt / Schützkontrolle!

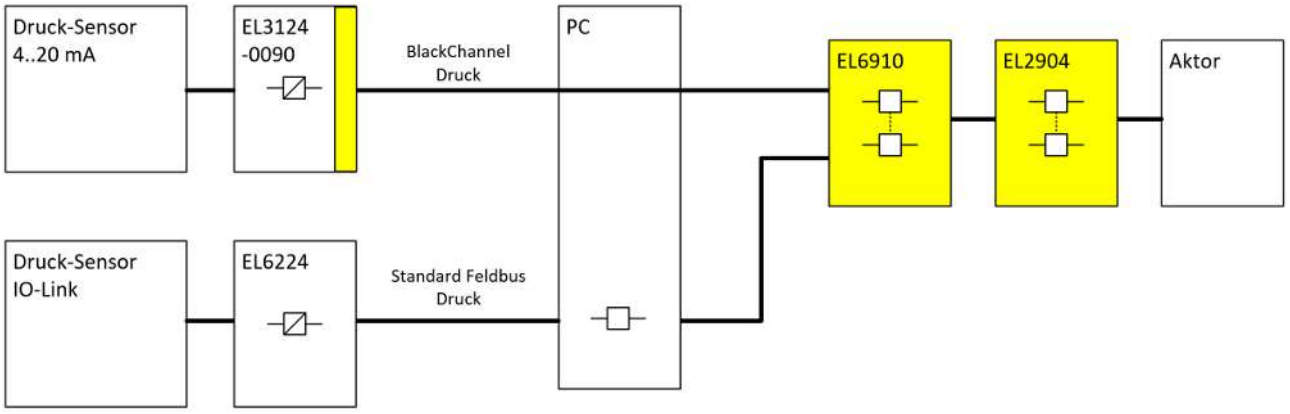
Neben der oben gezeigten Funktion, muss eine Schützkontrolle, z.B. über einen EDM-Baustein für K1 und K2 und ggf. eine Nothalt-Funktion durch den Anwender realisiert werden!

Eine Auswahl an alternativen TwinSAFE SC-Produkten, die für dieses Applikationsbeispiel herangezogen werden können, entnehmen Sie der folgenden Tabelle. Die in diesem Beispiel beschriebenen Annahmen und Argumentationen müssen weiterhin berücksichtigt werden.

Beispiel Druckmessung: Drucksensor (IO-Link-Schnittstelle) mit EL6224 und ein Drucksensor (4 – 20 mA) mit EL3124-0090		
Alternative TwinSAFE SC-Produkte mit 4 - 20mA Analog-Eingang	EL3174-0090	EtherCAT-Klemme, 4-Kanal-Analog-Eingang, Multifunktion, ±10 V, ±20 mA, 16 Bit, TwinSAFE SC

Beispiel Druckmessung: Drucksensor (IO-Link-Schnittstelle) mit EL6224 und ein Drucksensor (4 – 20 mA) mit EL3124-0090		
	EP3174-0092	EtherCAT Box, 4-Kanal-Analog-Eingang, Multifunktion, ±10 V, 0/4…20 mA, 16 Bit, differentiell, M12, TwinSAFE SC

8.5.1 Strukturbild des Aufbaus



8.5.2 Struktur und Diagnose

Die eingelesenen Signale von den beiden Messstellen sind Standard Signale, die eine unterschiedliche Technologie verwenden. Mindestens ein Signal wird über die TwinSAFE SC Technologie an die sichere TwinSAFE Logik übermittelt, so dass Verfälschungen dieses Signals im PC oder auf dem Übertragungsweg erkannt werden. Die Prüfung auf Gleichheit dieser beiden Signale, innerhalb der zulässigen Toleranzen, wird in der sicheren TwinSAFE Logik durchgeführt.

Die einzelnen Fehlerannahmen und zugehörigen Erwartungshaltungen werden in folgender FMEA Tabelle aufgelistet.

8.5.3 FMEA

Fehlerannahme	Erwartungshaltung	Überprüft
Druckwert über den Standard-Feldbus friert ein	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt.	
Druckwert über die TwinSAFE SC Kommunikation friert ein	Wird über den Watchdog innerhalb der TwinSAFE SC Kommunikation und über die Plausibilisierung in der EL6910 erkannt.	
Druckwerte werden in der Standard SPS aufeinander kopiert	Ein verfälschter Wert innerhalb der TwinSAFE SC Kommunikation führt zu einer ungültigen CRC innerhalb des Telegramms und damit zur sofortigen Abschaltung der Gruppe und der Ausgänge.	
Druckwert über den Standard-Feldbus wird verfälscht	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt.	
Verbindung zwischen Sensor und EtherCAT-Klemme ist nicht mehr gegeben	Wird über die Plausibilisierung mit dem zweiten Druckwert innerhalb der EL6910 erkannt.	
Drucksensor (4..20mA) liefert falschen Druckwert	Wird über die Plausibilisierung mit dem zweiten Druckwert innerhalb der EL6910 erkannt.	
Drucksensor (IO-Link) liefert falschen Druckwert	Wird über die Plausibilisierung mit dem zweiten Druckwert innerhalb der EL6910 erkannt.	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verfälschung	Wird über die Plausibilisierung der Druckwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Unbeabsichtigte Wiederholung	Wird über die Plausibilisierung der Druckwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Falsche Abfolge	Wird über die Plausibilisierung der Druckwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verlust	Wird über die Plausibilisierung der Druckwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Inakzeptable Verzögerung	Wird über die Plausibilisierung der Druckwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Einfügung	Wird über die Plausibilisierung der Druckwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Maskerade	nicht relevant für Standard, sondern nur für Safety Kommunikation.	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Adressierung	Wird über die Plausibilisierung der Druckwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler für Standard-Kommunikation: Wiederkehrende Speicherfehler in Switches	Wird über die Plausibilisierung der Druckwerte und über die TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	

8.5.3.1 Anmerkung TwinSAFE SC Kommunikation:

Die TwinSAFE SC Kommunikation verwendet die identischen Mechanismen zur Fehleraufdeckung, wie die Safety-over-EtherCAT Kommunikation mit dem Unterschied, dass zur Berechnung der Prüfsumme eine anderes Polynom verwendet wird, welches hinreichend unabhängig von dem bisher für Safety-over-EtherCAT verwendetem Polynom ist.

Es sind die identischen Mechanismen aktiv, wie z.B. Black-Channel Prinzip (Bitfehlerwahrscheinlichkeit 10^{-2}).

Die Qualität der Datenübertragung ist nicht entscheidend, da letztendlich über den Vergleich in der sicheren TwinSAFE Logik alle Übertragungsfehler aufgedeckt werden, da diese zur Ungleichheit führen würden.

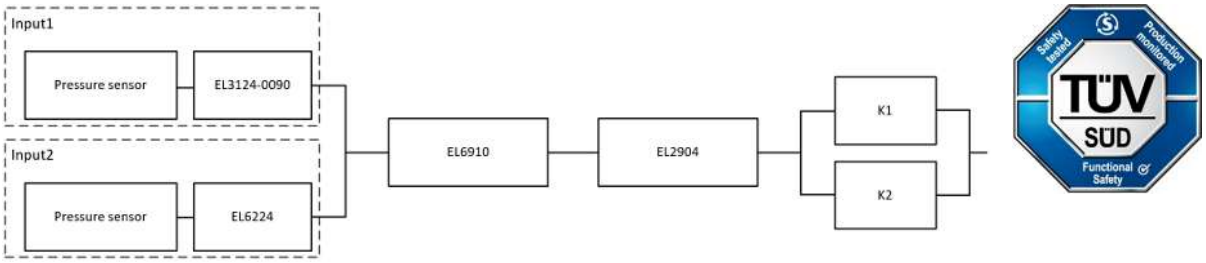
8.5.4 Parameter der sicheren Ausgangsklemme

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Ja

8.5.5 Blockbildung und Safety-Loops

8.5.5.1 Sicherheitsfunktion 1



8.5.6 Berechnung

8.5.6.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL2904 – PFH_D	1,25E-09
EL6910 – PFH_D	1,79E-09
Drucksensor 1 (4-20 mA) – MTTF	124 a (1.086.240 h)
Drucksensor 2 IO-Link – MTTF	201 a (1.760.760 h)
EL3124-0090 - MTBF	950.000 h
EL6224 - MTBF	1.607.919 h
K1 – $B10_D$	1.300.000 h
K2 – $B10_D$	1.300.000 h
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

8.5.6.2 Diagnostic Coverage DC

Komponente	Wert
Druckwerte über TwinSAFE SC und Plausibilität innerhalb der Logik	DC_{avg}=90% (Alternativ in Berechnung: 99%)
K1/K2 mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) mit Testung der einzelnen Kanäle	DC_{avg}=99%

8.5.6.3 Berechnung Sicherheitsfunktion 1

Zur Verdeutlichung wird der Sicherheitskennwert sowohl nach EN 62061 als auch nach EN 13849 berechnet. In der Praxis ist die Berechnung nach einer Norm ausreichend.

Berechnung der PFH_D- und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Berechnung der PFH_D- und $MTTF_D$-Werte aus den MTBF-Werten:

Anmerkung: Reparaturzeiten können vernachlässigt werden, daher gilt:

$$MTTF_D = 2 * MTBF$$

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

mit

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

ergibt sich für

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

Eingesetzt ergibt das:

Drucksensor 1 (4-20mA)

$$MTTF_D = 2 * MTTF = 2 * 124y = 248y = 2.172.480h$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.172.480h} = 4,60E - 08$$

EL3124-0090

$$MTTF_D = 2 * MTBF = 2 * 950.000h = 1.900.000h = 216y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.900.000h} = 5,26E - 08$$

Eingangssystem 1

$$PFH_{(Input1)} = PFH_{(PressureSensor1)} + PFH_{(EL3124-0090)} = 4,60E - 08 + 5,26E - 08 = 9,86E - 08$$

Drucksensor 2 (IO-Link)

$$MTTF_D = 2 * MTBF = 2 * 1.760.760h = 3.521.520h = 402y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.521.520h} = 2,84E - 08$$

EL6224

$$MTTF_D = 2 * MTBF = 2 * 1.607.919h = 3.215.838h = 367y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{3.215.838h} = 3,11E - 08$$

Eingangssystem 2

$$PFH_{(Input2)} = PFH_{(PressureSensor2)} + PFH_{(EL6224)} = 2,84E - 08 + 3,11E - 08 = 5,95E - 08$$

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

K1/K2: Betätigung 1/Woche und direktes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Die Eingangssignale aus Drucksensor 1 mit EL3124-0090 und Drucksensor 2 mit EL6224 haben unterschiedliche Messverfahren, liefern beide einen Druckwert und sind beide an der Sicherheitsfunktion beteiligt. Ein-Nichtfunktionieren eines Kanals führt nicht zu einer gefährlichen Situation, sondern wird über den Vergleich der beiden Werte in der TwinSAFE Logik erkannt und führt zur Abschaltung.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält Tabellen (Tabelle F.1-Kriterien zur Bestimmung des CCF und Tabelle F.2-Abschätzung des CCF-Faktors(β)), mit der dieser β–Faktor genau bestimmt werden kann. Für das Eingangssubsystem kann bei entsprechender Bearbeitung der Tabelle zur Berechnung des β-Faktors ein Wert von schätzungsweise 2% erreicht werden. In der folgenden Berechnung wird der Worst-Case mit 10% angenommen.

Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ und $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

$$PFH_{ges} = 10\% * \frac{9,86E-08 + 5,95E-08}{2} + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 1,094E-08$$

HINWEIS

EN 62061

Entsprechend der EN 62061 wird das Eingangssubsystem mit einer SFF bzw. einem DC von 90% bewertet. Dies schränkt den erreichbaren SIL Wert gemäß Tabelle 5 der EN 62061 auf maximal SIL 2 ein.

Alternative Berechnung des $MTTF_D$-Wertes nach EN 13849 für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit

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

Aus dem Eingangssubsystem, wird der schlechtere Wert genommen:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(PressureSensor)}} + \frac{1}{MTTF_{D(EL3124-0090)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

Sind für die EL2904 und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{15{,}68E-06\frac{1}{y}} = 637y$$

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{248y} + \frac{1}{216y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 88{,}27y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Pressure1)}} + \frac{DC}{MTTF_{D(EL3124-0090)}} + \frac{DC}{MTTF_{D(Pressure2)}} + \frac{DC}{MTTF_{D(EL6224)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Pressure1)}} + \frac{1}{MTTF_{D(EL3124-0090)}} + \frac{1}{MTTF_{D(Pressure2)}} + \frac{1}{MTTF_{D(EL6224)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

Eingesetzt mit DC=90%

$$DC_{avg} = \frac{\frac{90\%}{248y} + \frac{90\%}{216y} + \frac{90\%}{402y} + \frac{90\%}{367y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{248y} + \frac{1}{216y} + \frac{1}{402y} + \frac{1}{367y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91{,}41\%$$

Alternativ mit DC=99%

$$DC_{avg} = \frac{\frac{99\%}{248y} + \frac{99\%}{216y} + \frac{99\%}{402y} + \frac{99\%}{367y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{248y} + \frac{1}{216y} + \frac{1}{402y} + \frac{1}{367y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99{,}00\%$$

⚠ VORSICHT

Kategorie

Diese Struktur ist bis maximal Kategorie 3 möglich.

DC=90% für das Eingangs-Subsystem

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Alternative mit DC=99% für das Eingangs-Subsystem

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

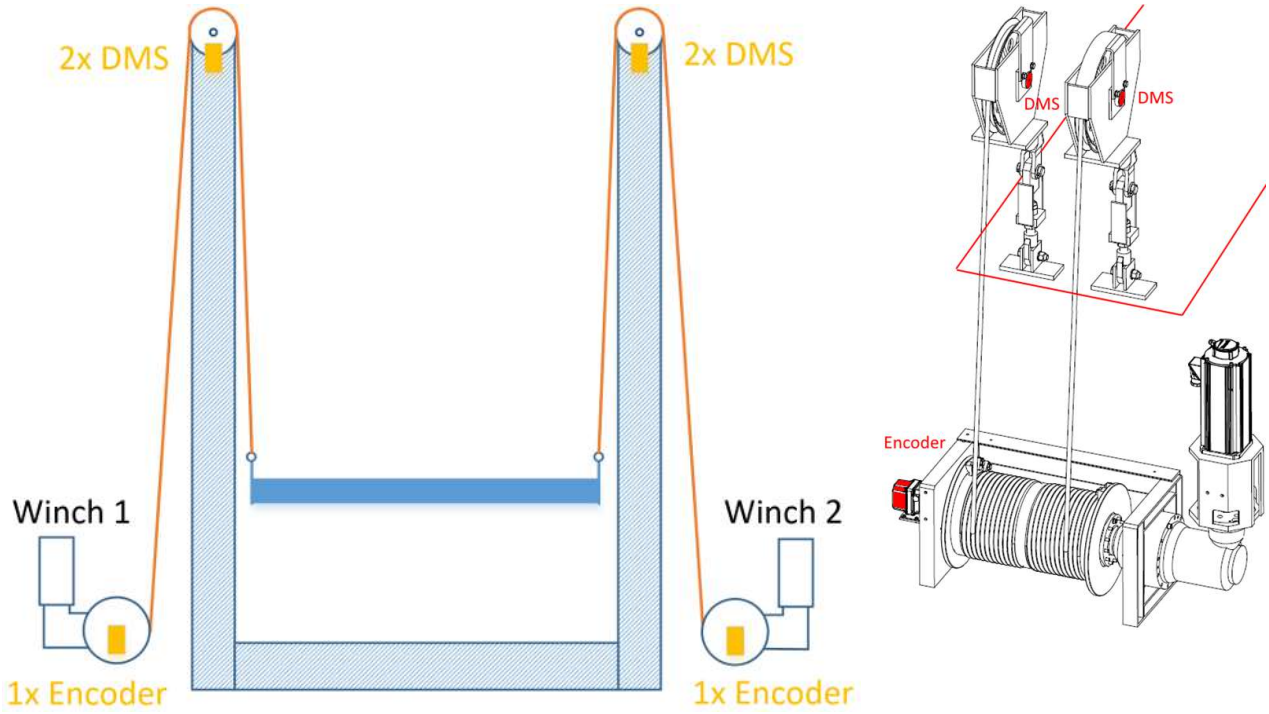
Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Sicherheits-Integritätslevel entspr. Tab. 3 EN62061	
Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2	**≥ 10^{-7} bis < 10^{-6}**
1	≥ 10^{-6} bis < 10^{-5}

8.6 Überwachung Hubgerät (Kategorie 3, PL d)

Ein Hubgerät, bestehend aus 2 Windwerken (Winch) mit Umlenkrollen zur Bewegung eines Hubtisches, soll sicherheitstechnisch überwacht werden. Dabei sollen die Funktionen Schlaffseil-Erkennung und Überlast realisiert werden. Es gibt oben an den Pfosten auf jeder Seite jeweils 2 Umlenkrollen mit jeweils einem DMS Sensor, somit in Summe 4 DMS Sensoren. Einer dieser beiden Sensoren einer Seite wird mit einer TwinSAFE SC Klemme EL3356-0090 eingelesen. Der jeweils andere DMS Sensor wird auf eine EL3751 verdrahtet. Diese liefert ein DMS mV/V Signal, welches in der sicheren Logik in einen Gewichtswert umgerechnet werden muss, damit er mit dem Wert der EL3356-0090 verglichen werden kann.



Sicherheitsfunktion 1 - Überlast

Für das Hubgerät ist eine maximal zulässige Zuladung spezifiziert. Diese muss überwacht werden. Dazu wird nach der Plausibilisierung der Signale der EL3751 und EL3356-0090 eine Limitierung des Ergebnisses mit dem Limit Baustein in der EL6910 vorgenommen.

Laut der Risiko- und Gefährdungsanalyse des Kunden ist diese Sicherheitsfunktion mit PL c nach EN 13849-1:2023 zu bewerten.

Die Sicherheitsfunktion wird in einer Kategorie 3 Struktur aufgebaut.

Sicherheitsfunktion 2 - Schlaffseil-Erkennung

Eine Schlaffseil-Erkennung dient zur Erkennung, ob der Hubschlitten irgendwo mechanisch hängen geblieben ist, oder auf dem Boden aufsteht. In beiden Fällen muss sofort abgeschaltet werden. Zusätzlich wird darüber auch erkannt, ob ein Seil gerissen ist.

Laut der Risiko- und Gefährdungsanalyse des Kunden ist diese Sicherheitsfunktion mit PL c nach EN 13849-1:2023 zu bewerten.

Die Sicherheitsfunktion wird in einer Kategorie 3 Struktur aufgebaut.

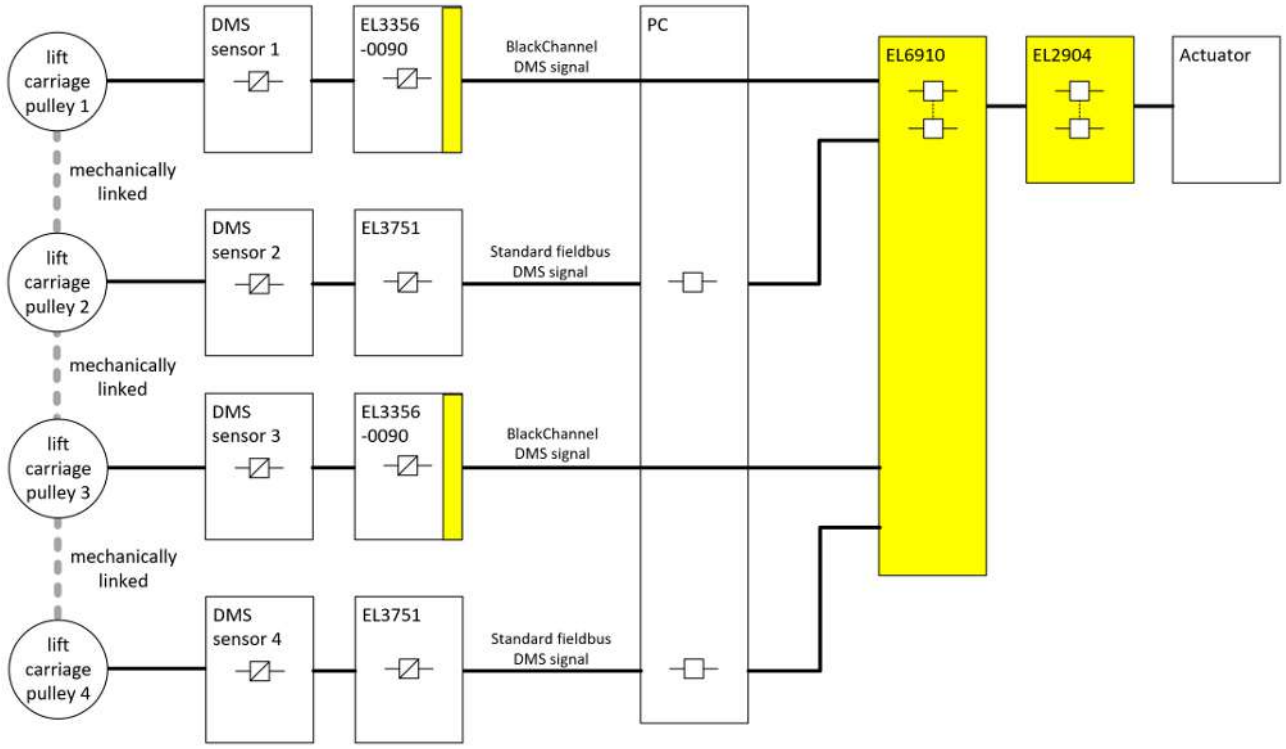
Zusatzfunktion - ohne sicherheitstechnische Anforderungen

Durch inkrementellen Vergleich der Geberwerte von Windwerk 1 und 2 kann ein Gleichlauf überprüft werden. Damit wird ein Schrägziehen des Hubschlitten durch die beiden Windwerke frühzeitig verhindert.

Eine Auswahl an alternativen TwinSAFE SC-Produkten, die für dieses Applikationsbeispiel herangezogen werden können, entnehmen Sie der folgenden Tabelle. Die in diesem Beispiel beschriebenen Annahmen und Argumentationen müssen weiterhin berücksichtigt werden.

Beispiel: Überwachung von Hubgeräten, Schlaffseil-Erkennung und Überlast: DMS-Sensoren an den Umlenkrollen (EL3356-0090 und EL3751)
Kein alternatives TwinSAFE SC-Produkt vorhanden.

8.6.1 Strukturbild Aufbau



8.6.2 Struktur und Diagnose

Die eingelesenen Signale der DMS Sensoren sind Standard Signale, die pro Seite unterschiedlich erfasst werden. Der erste DMS Sensor wird auf eine DMS Klemme EL3356-0090 verdrahtet, die den ermittelten Gewichtswert in ein sicheres Telegramm (FSoE mit geändertem Polynom - TwinSAFE SC) verpackt und an die EL6910 überträgt. Der zweite DMS Sensor wird auf eine Klemme EL3751 verdrahtet, die eine DMS mV/V Messung durchführt. Dieses Signal wird über den Standard Kommunikationsweg an die EL6910 gesendet. Dieses Signal wird vor der Plausibilisierung innerhalb der sicheren Logik in einen Gewichtswert umgerechnet.

Für die zweite Seite des Hubwerks mit DMS Sensor 3 und 4 wird identisch vorgegangen. Für die TwinSAFE SC Kommunikation der zweiten EL3356-0090 wird ein, verglichen zur ersten Seite, unterschiedliches Polynom verwendet. Dadurch wird ein aufeinander kopieren der Daten der beiden TwinSAFE SC Verbindungen erkannt.

8.6.3 FMEA

Fehlerannahme	Erwartungshaltung	Überprüft
DMS Signal über den Standard Feldbus friert ein	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt (TwinSAFE SC Kommunikation zwischen EL3356-0090 und EL6910).	
DMS Signal über TwinSAFE SC Kommunikation friert ein	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 und über den Watchdog innerhalb der TwinSAFE SC Kommunikation erkannt.	

Fehlerannahme	Erwartungshaltung	Überprüft
DMS Werte werden in der Standard SPS aufeinander kopiert	Ein verfälschter Wert innerhalb der TwinSAFE SC Kommunikation führt zu einer ungültigen CRC innerhalb des Telegramms und damit zur sofortigen Abschaltung der Gruppe und der Ausgänge. Die Datentypen der beiden DMS Werte haben eine unterschiedliche Länge, da einer der beiden in das TwinSAFE SC Telegramm verpackt ist (z.B. 4 Byte und 11 Byte)	
DMS Signal über den Standard Feldbus wird verfälscht	Wird über den zweiten Wert und die Plausibilisierung in der EL6910 erkannt (TwinSAFE SC Kommunikation zwischen EL3356-0090 und EL6910)	
Mechanische Verbindung zwischen Hubschlitten und Windwerk ist nicht mehr gegeben	Wird über die Plausibilisierung mit dem zweiten DMS Signal innerhalb der EL6910 erkannt.	
EL3356-0090 liefert falschen DMS-Wert	Wird über die Plausibilisierung mit dem DMS Wert der EL3751 innerhalb der EL6910 erkannt	
EL3751 liefert falschen DMS-Wert	Wird über die Plausibilisierung mit dem DMS Wert der EL3356-0090 innerhalb der EL6910 erkannt	

Fehlerannahme	Erwartungshaltung	Überprüft
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verfälschung	Wird über die Plausibilisierung der DMS Werte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Unbeabsichtigte Wiederholung	Wird über die Plausibilisierung der DMS Werte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Falsche Abfolge	Wird über die Plausibilisierung der DMS Werte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Verlust	Wird über die Plausibilisierung der DMS Werte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Inakzeptable Verzögerung	Wird über die Plausibilisierung der DMS Werte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Einfügung	Wird über die Plausibilisierung der DMS Werte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Maskerade	nicht relevant für Standard, sondern nur für Safety Kommunikation.	
Kommunikationsfehler 61784-3 für Standard-Kommunikation: Adressierung	Wird über die Plausibilisierung der DMS Werte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	
Kommunikationsfehler für Standard-Kommunikation: Wiederkehrende Speicherfehler in Switches	Wird über die Plausibilisierung der DMS Werte zusammen mit der TwinSAFE SC Kommunikation innerhalb der EL6910 erkannt	

8.6.3.1 Anmerkung TwinSAFE SC Kommunikation:

Die TwinSAFE SC Kommunikation verwendet die identischen Mechanismen zur Fehleraufdeckung, wie die Safety-over-EtherCAT Kommunikation mit dem Unterschied, dass zur Berechnung der Prüfsumme eine anderes Polynom verwendet wird, welches hinreichend unabhängig von dem bisher für Safety-over-EtherCAT verwendetem Polynom ist.

Es sind die identischen Mechanismen aktiv, wie z.B. Black-Channel Prinzip (Bitfehlerwahrscheinlichkeit 10^{-2}).

Die Qualität der Datenübertragung ist nicht entscheidend, da letztendlich über den Vergleich in der sicheren Logik alle Übertragungsfehler aufgedeckt werden, da diese zur Ungleichheit führen würden.

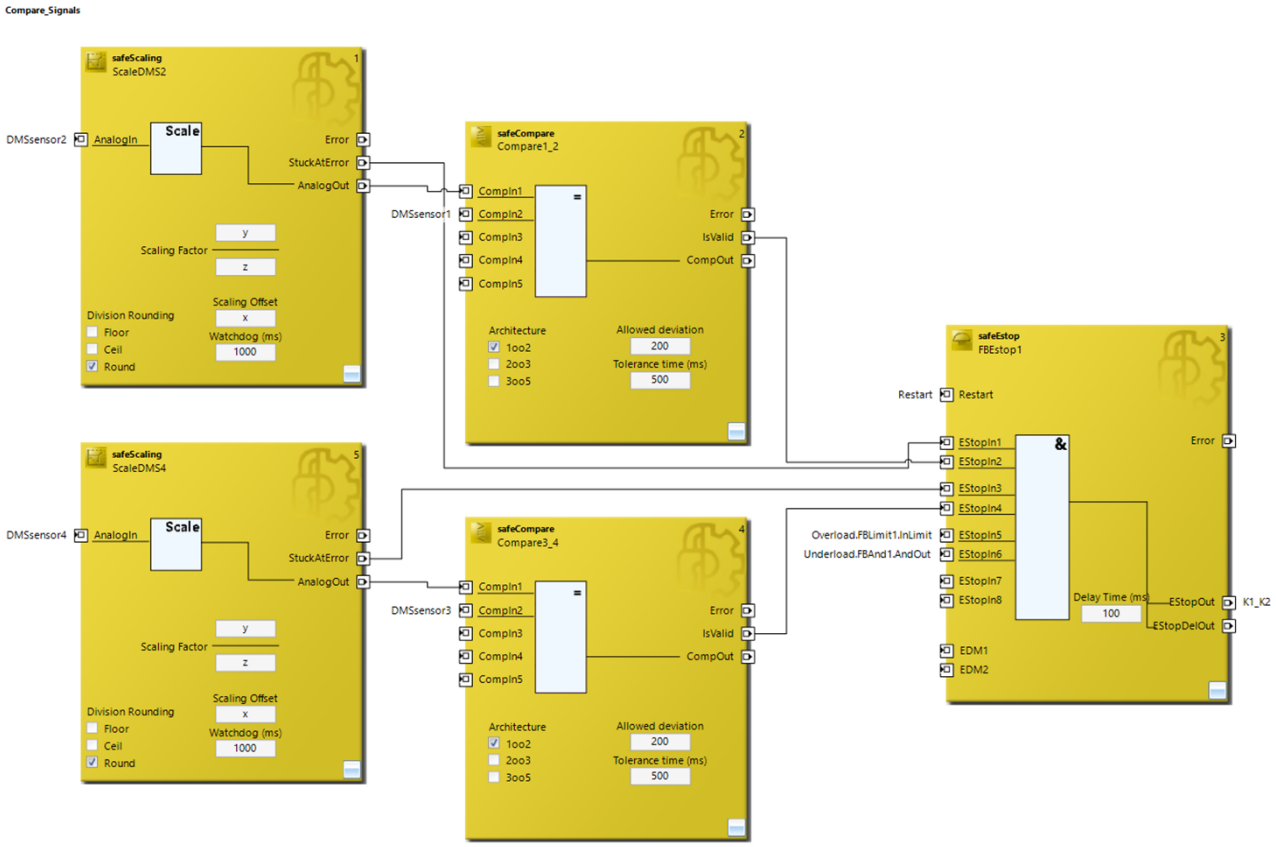
8.6.4 Aufbau innerhalb der Logik

Die Logik in der EL6910 ist in 3 Teile aufgeteilt. Im ersten Abschnitt werden die DMS Werte skaliert und plausibilisiert. Es ist auch die Wiederanlaufsperre und die Abschaltung der Schütze K1 und K2 über einen ESTOP Baustein enthalten.

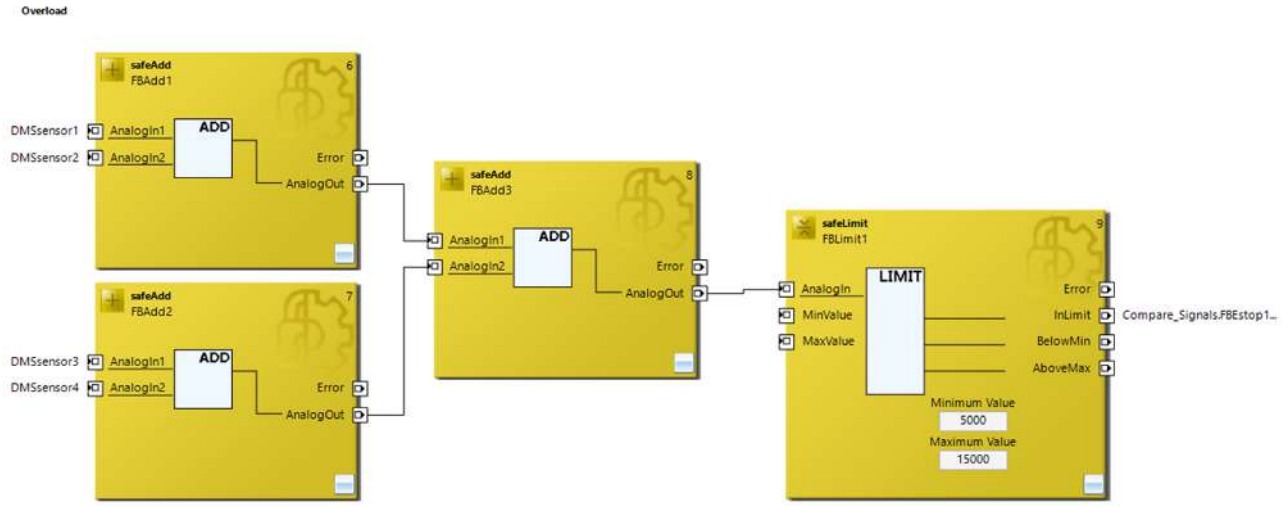
Im zweiten Abschnitt wird die Gesamtlast ermittelt und über einen Limitbaustein auf ein Maximum und Minimum überwacht. Das Ergebnis wird auf den ESTOP Baustein des ersten Abschnitts geführt.

Im dritten Abschnitt wird jedes einzelne Signal auf einen minimalen Wert überwacht. Diese 4 Signale werden UND verknüpft auf den ESTOP Baustein des ersten Abschnitts verknüpft.

Abschnitt 1



Abschnitt 2


Overload
safeAdd
FBAdd1
6
DMSsensor1
AnalogIn1
ADD
DMSsensor2
AnalogIn2
Error
AnalogOut
safeAdd
FBAdd2
7
DMSsensor3
AnalogIn1
ADD
DMSsensor4
AnalogIn2
Error
AnalogOut
safeAdd
FBAdd3
8
AnalogIn1
ADD
AnalogIn2
Error
AnalogOut
safeLimit
FBLimit1
9
AnalogIn
LIMIT
MinValue
MaxValue
Error
InLimit
BelowMin
AboveMax
Compare_Signals.FBEstop1...
Minimum Value
5000
Maximum Value
15000

Abschnitt 3

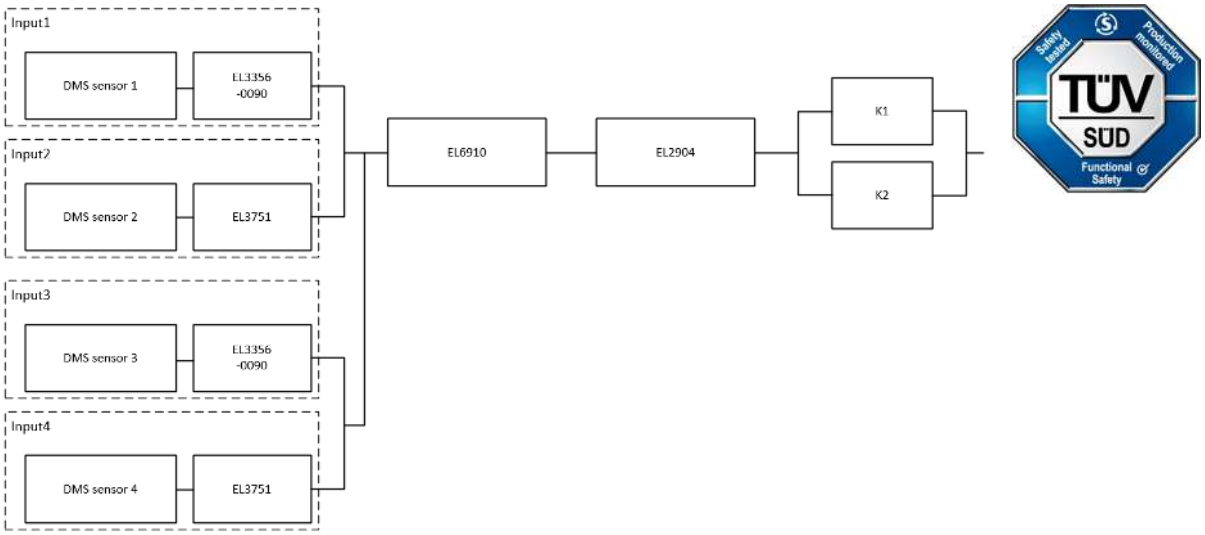
8.6.5 Parameter der sicheren Ausgangsklemme

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Ja

8.6.6 Blockbildung und Safety-Loops

8.6.6.1 Sicherheitsfunktion 1/2



8.6.7 Berechnung

8.6.7.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL2904 – PFH_D	1,25E-09
EL6910 – PFH_D	1,79E-09
DMS Sensor 1-4 – $MTTF_D$ (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 – $B10_D$	1.300.000 h
K2 – $B10_D$	1.300.000 h
Encoder MTBF	107,5 y (914.700 h)
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

8.6.7.2 Diagnostic Coverage DC

Komponente	Wert
DMS Werte über TwinSAFE SC und Plausibilität innerhalb der Logik	DC_{avg}=90% (Alternativ in Berechnung: 99%)
K1/K2 mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) mit Testung der einzelnen Kanäle	DC_{avg}=99%

8.6.7.3 Berechnung Sicherheitsfunktion 1/2

Zur Verdeutlichung wird der Sicherheitskennwert sowohl nach EN 62061 als auch nach EN 13849 berechnet. In der Praxis ist die Berechnung nach einer Norm ausreichend.

Berechnung der PFH_D- und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Berechnung der PFH_D- und $MTTF_D$-Werte aus den MTBF-Werten:

Anmerkung: Reparaturzeiten können vernachlässigt werden, daher gilt:

$$MTTF_D = 2 * MTBF$$

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

mit

$$\lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

ergibt sich für

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

Eingesetzt ergibt das:

DMS Sensor 1

$$MTTF_D = 1.401.600h = 160y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.401.600h} = 7{,}13E - 08$$

EL3356-0090

$$MTTF_D = 2 * MTBF = 2 * 780.733h = 1.561.466h = 178y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.561.466h} = 6{,}40E - 08$$

Eingangssystem 1

$$PFH_{(Input1)} = PFH_{(DMS1)} + PFH_{(EL3356-0090)} = 7{,}13E - 08 + 6{,}40E - 08 = 13{,}53E - 08$$

DMS Sensor 2

$$MTTF_D = 1.401.600h = 160y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.401.600h} = 7{,}13E - 08$$

EL3751

$$MTTF_D = 2 * MTBF = 2 * 513.333h = 1.026.666h = 117y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{1.026.666h} = 9,74E-08$$

Eingangssystem 2

$$PFH_{(Input2)} = PFH_{(DMS2)} + PFH_{(EL3751)} = 7,13E-08 + 9,74E-08 = 16,87E-08$$

Für Eingangssystem 3 gelten die Werte, wie für Eingangssystem 1 berechnet. Für Eingangssystem 4 gelten die Werte, wie für Eingangssystem 2 berechnet.

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

K1/K2: Betätigung 1/Woche und direktes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Die Eingangssignale aus DMS Sensor 1 mit EL3356-0090 und DMS Sensor 2 mit EL3751 haben einen unterschiedlichen internen Aufbau, liefern unterschiedliche Werte (Gewichtswert und mV/V Wert) und sind beide an der Sicherheitsfunktion beteiligt. Ein-Nichtfunktionieren eines Kanals führt nicht zu einer gefährlichen Situation, sondern wird über den Vergleich der beiden Werte in der TwinSAFE Logik erkannt und führt zur Abschaltung. Ein identischer Aufbau ist für DMS Sensor 3 und 4 verwendet. Die Summe aus den 4 Sensoren liefert den Gewichtswert für die Überlast-Abschaltung. Ein Unterschreiten der Minimallast eines DMS Sensors führt zur Schlaffseil-Abschaltung.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält Tabellen (Tabelle F.1-Kriterien zur Bestimmung des CCF und Tabelle F.2-Abschätzung des CCF-Faktors(β)), mit der dieser β–Faktor genau bestimmt werden kann. Für das Eingangssubsystem kann bei entsprechender Bearbeitung der Tabelle zur Berechnung des β-Faktors ein Wert von schätzungsweise 2% erreicht werden. In der folgenden Berechnung wird der Worst-Case mit 10% angenommen.

Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1 / 2

$$PFH_{(DMS1/2)} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$$
$$= 10\% * \frac{13,53E-08 + 16,87E-08}{2} = 1,52E-08$$

$$PFH_{(DMS3/4)} = \beta * \frac{PFH_{(Input3)} + PFH_{(Input4)}}{2} + (1-\beta)^2 * (PFH_{(Input3)} * PFH_{(Input4)}) * T1$$
$$= 10\% * \frac{13,53E-08 + 16,87E-08}{2} = 1,52E-08$$

$$PFH_{(K1/K2)} = \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$
$$= 10\% * \frac{1,92E-12 + 1,92E-12}{2} = 1,92E-13$$

Da die Anteile $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ um mindestens eine Zehnerpotenz kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

$$PFH_{ges} = PFH_{(DMS1/2)} + PFH_{(DMS3/4)} + PFH_{(EL6910)} + PFH_{(EL2904)} + PFH_{(K1/K2)}$$
$$= 1,52E-08 + 1,52E-08 + 1,79E-09 + 1,25E-09 + 1,92E-13$$
$$= 3,344E-08$$

HINWEIS

EN 62061

Entsprechend der EN 62061 wird das Eingangssubsystem mit einer SFF bzw. einem DC von 90% bewertet. Dies schränkt den erreichbaren SIL Wert gemäß Tabelle 5 der EN 62061 auf maximal SIL 2 ein.

Alternative Berechnung des $MTTF_D$-Wertes nach EN 13849 für Sicherheitsfunktion 1 / 2 (unter der gleichen Annahme) berechnet sich mit

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

Aus dem Eingangssubsystem, wird der schlechtere Wert genommen:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(DMSsensor2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

Sind für die EL2904 und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{160y} + \frac{1}{117y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 57,26y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(DMS1)}} + \frac{DC}{MTTF_{D(EL3356)}} + \frac{DC}{MTTF_{D(DMS2)}} + \frac{DC}{MTTF_{D(EL3751)}} + \frac{DC}{MTTF_{D(DMS1)}} + \frac{DC}{MTTF_{D(EL3356)}} + \frac{DC}{MTTF_{D(DMS2)}} + \frac{DC}{MTTF_{D(EL3751)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(DMS1)}} + \frac{1}{MTTF_{D(EL3356)}} + \frac{1}{MTTF_{D(DMS2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(DMS1)}} + \frac{1}{MTTF_{D(EL3356)}} + \frac{1}{MTTF_{D(DMS2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

Eingesetzt mit DC=90%

$$DC_{avg} = \frac{\frac{90\%}{160y} + \frac{90\%}{178y} + \frac{90\%}{160y} + \frac{90\%}{117y} + \frac{90\%}{160y} + \frac{90\%}{178y} + \frac{90\%}{160y} + \frac{90\%}{117y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 90,42\%$$

Alternativ mit DC=99%

$$DC_{avg} = \frac{\frac{99\%}{160y} + \frac{99\%}{178y} + \frac{99\%}{160y} + \frac{99\%}{117y} + \frac{99\%}{160y} + \frac{99\%}{178y} + \frac{99\%}{160y} + \frac{99\%}{117y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99,00\%$$

⚠ VORSICHT

Kategorie

Diese Struktur ist bis maximal Kategorie 3 möglich.

DC=90% für das Eingangs-Subsystem

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

Alternative mit DC=99% für das Eingangs-Subsystem

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5% angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

HINWEIS

Ergebnis

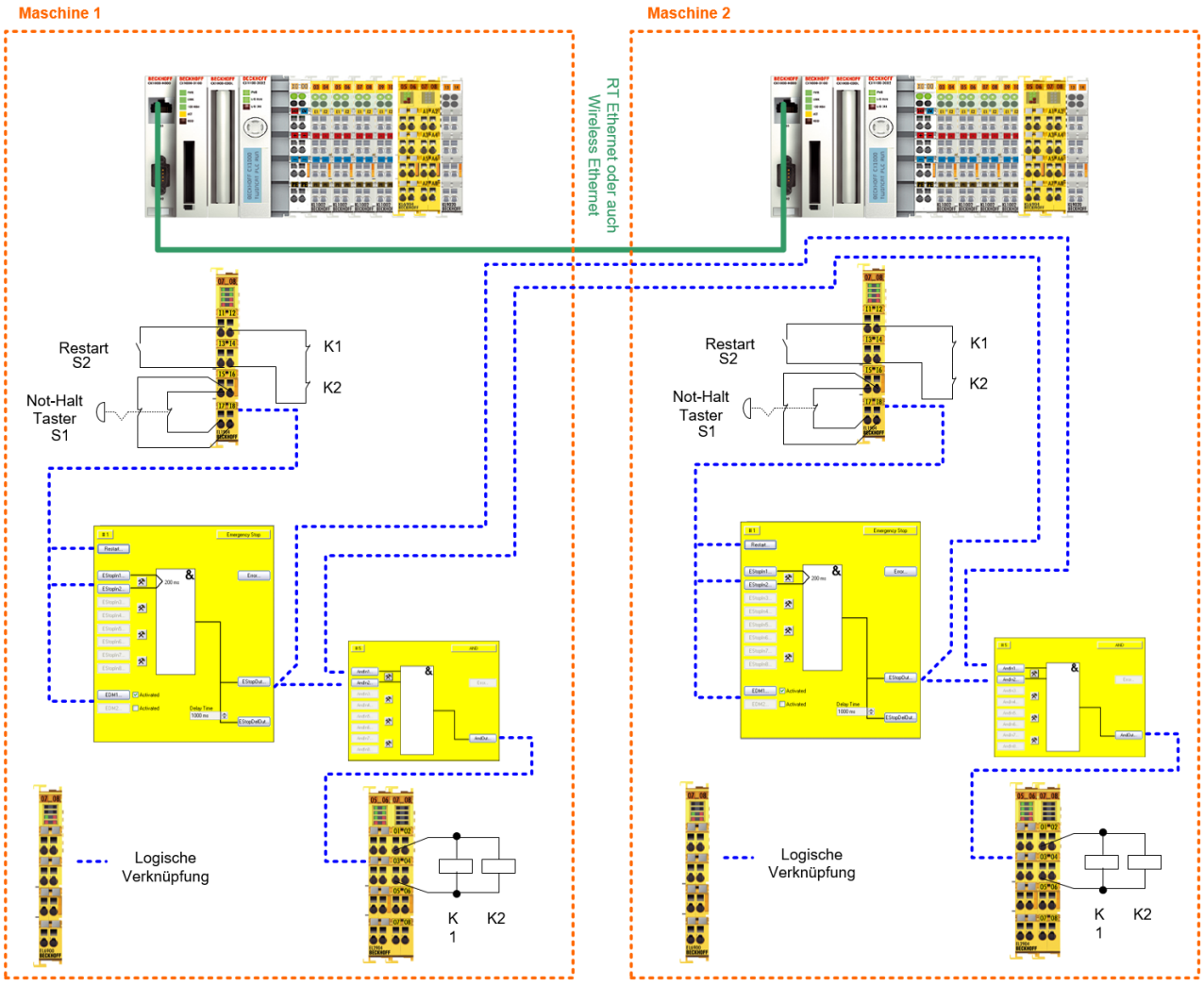
Das Ergebnis mit Kategorie 3, PL d erfüllt bzw. übertrifft die Anforderung der Risiko- und Gefährdungsanalyse (PL c).

9 Anwendungsspezifische Szenarien

9.1 Vernetzte Anlage (Kategorie 4, PL e)

Hier werden 2 Anlagen über Ethernet verbunden. Die Strecke kann auch durch eine Wireless Ethernet Verbindung realisiert sein. Jede Station schaltet die Ausgänge K1 / K2 nur ein, wenn auch die zweite Maschine keinen Not-Halt meldet. Die Signale des Not-Halt-Tasters, des Restart und des Rückführkreises sind auf sichere Eingänge verdrahtet. Der Ausgang des ESTOP-Bausteins wird auf einen UND Baustein verknüpft und zusätzlich über das Netzwerk der anderen Maschine mitgeteilt. Der ESTOP-Ausgang der jeweils anderen Maschine wird auf den UND Baustein verknüpft und der Ausgang des UND schaltet dann die Schütze auf der sicheren Ausgangsklemme.

Die Testung und die Prüfung auf Diskrepanz sind für die Eingangssignale eingeschaltet. Die Testung der Ausgänge ist ebenfalls aktiv.



HINWEIS

Start / Wiederanlauf

Wo eine Maschine mehr als eine Bedienstation hat, müssen Maßnahmen vorgesehen werden, um sicherzustellen, dass die Einleitung von Kommandos von verschiedenen Bedienstationen nicht zu einer Gefährdungssituation führt.

HINWEIS

Schützüberwachung

Sollte das Ergebnis der Risiko- und Gefährdungsanalyse ergeben, dass beim Schalten der Schütze der jeweils entfernten Steuerung eine Schützkontrolle notwendig ist, ist diese über die Verwendung eines EDM-Bausteins zu realisieren.

9.1.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904 (für alle verwendeten EL1904 gültig)

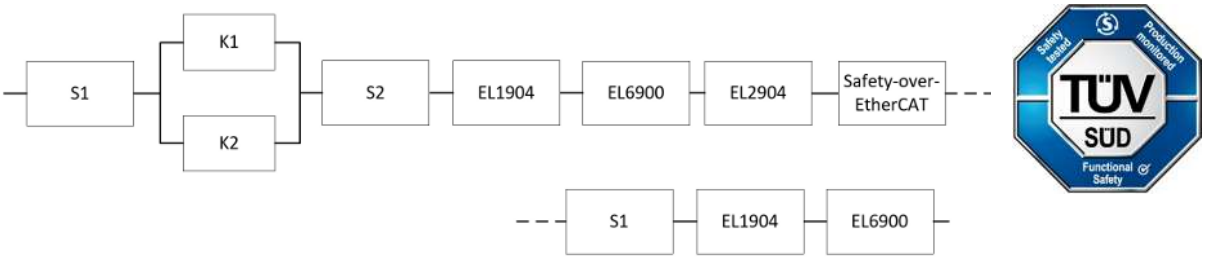
Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

9.1.2 Blockbildung und Safety-Loops

9.1.2.1 Sicherheitsfunktion 1



9.1.3 Berechnung

9.1.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
EL6900 – PFH_D	1,03E-09
Safety-over-EtherCAT (FSoE) – PFH_D	1,00E-09
S1 – $B10_D$	1.000.000
S2 – $B10_D$	2.000.000
K1 – $B10_D$	1.300.000

Komponente	Wert
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	15 (4x pro Stunde)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

9.1.3.2 Diagnostic Coverage DC

Komponente	Wert
S1 mit Testung/Plausibilität	DC_{avg}=99%
S2 mit Plausibilität	DC_{avg}=90%
K1/K2 mit Testung und EDM (Betätigung 1/Schicht)	DC_{avg}=99%

9.1.3.3 Berechnung Sicherheitsfunktion 1

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

Eingesetzt ergibt das:

S1:

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

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7y = 11902212h$$

S2:

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

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4y = 23804424h$$

K1/K2:

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

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

und der Annahme, dass S1, S2, K1 und K2 jeweils einkanalig sind:

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

ergibt sich für

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

S1:

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

S2:

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

K1/K2: Betätigung 1/Schicht und direktes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Der Sicherheitsschalter S1: Laut BGIA-Report 2/2008 ist ein Fehlerausschluss bis 100 000 Zyklen möglich, sofern eine Herstellerbestätigung vorliegt. Liegt dieser nicht vor, geht S1 wie folgt in die Rechnung ein.

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die Zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

Da der Anteil $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

mit:

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

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

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

Sind für EL1904, EL2904 und EL6900 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

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

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

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

$$MTTF_{D(FSoE)} = \frac{(1 - DC_{(FSoE)})}{PFH_{(FSoE)}} = \frac{(1 - 0,99)}{1,00E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{8,76E-06\frac{1}{y}} = 1141,6y$$

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 4 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

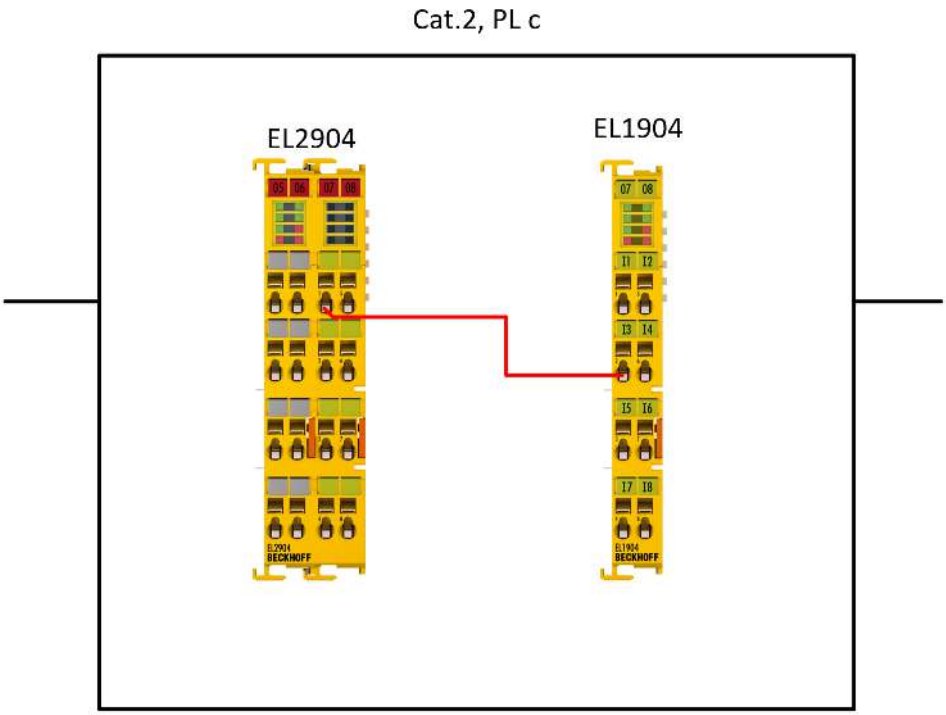
Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

9.2 Direktes Verdrahten der TwinSAFE-Ausgänge auf TwinSAFE-Eingänge (1-kanalig) (Kategorie 2, PL c)

Der Ausgang einer EL2904 wird direkt auf einen sicheren Eingang EL1904 verdrahtet, dabei werden die Testpulse und Strommessung der Ausgänge und der Sensortest der Eingänge abgeschaltet. Somit sind keine zyklischen Prüfungen für Querschluss und Fremdeinspeisung auf der Leitung möglich.

Die EL2904 und EL1904 sind aufgrund ihrer hohen internen Diagnose als einzelne Komponente mit Kategorie 2, SIL2 und PL d zu bewerten, da extern nur eine einkanalige Struktur verwendet wird. Der Gesamtperformance Level von Ausgang und Eingang ist aufgrund von Kapitel 6.2.5 DIN EN ISO 13849-1:2016-06 mit maximal PL c zu bewerten.

Die für Kategorie 2 erforderliche Testeinrichtung ist in der EL2904 integriert. Beim Einschalten des Ausgangs der EL2904 wird überprüft, ob auch tatsächlich 24 V zurückgelesen werden. Beim Ausschalten wird überprüft, dass auch tatsächlich 0 V zurückgelesen werden. Wird dabei ein Fehler festgestellt, geht die EL2904 in den Zustand Fehler, der auch an die überlagerte Sicherheitssteuerung gemeldet wird. Dieser Modulfehler der EL2904 muss in der Maschinensteuerung ausgewertet werden. Hierzu ist für die Connection zu der EL2904 der Parameter *ModuleFault is ComError* einzuschalten, was dazu führt, dass die TwinSAFE Gruppe bei einem Modulfehler in den sicheren Zustand wechselt und einen ComError meldet.



9.2.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904

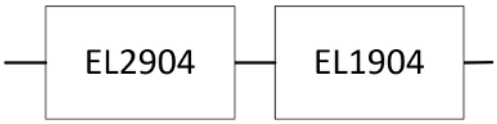
Parameter	Wert
Sensortest Kanal 1 aktiv	Nein
Sensortest Kanal 2 aktiv	Nein
Sensortest Kanal 3 aktiv	Nein
Sensortest Kanal 4 aktiv	Nein
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Nein

9.2.2 Blockbildung und Safety-Loops

9.2.2.1 Sicherheitsfunktion 1



9.2.3 Berechnung

9.2.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	60 (1x pro Stunde)
Lebenszeit (T1)	20 Jahre = 175200 Stunden

9.2.3.2 Diagnostic Coverage DC

Komponente	Wert
EL1904/EL2904 Aufgrund der internen Diagnose der Klemmen (wie Überwachung der Feldspannung, Temperatur usw.) und der Prüfung der EL2904 auf die Korrektheit des geschalteten Ausgangs jeweils beim Wechsel des Signalzustands	DC_{avg}=60%

9.2.3.3 Berechnung Sicherheitsfunktion 1

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 berechnet sich mit:

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

als:

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

Sind für EL1904 und EL2904 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0{,}60)}{1{,}11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}4}{9{,}72E-06\frac{1}{y}} = 41152y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0{,}60)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}4}{1{,}1E-05\frac{1}{y}} = 36364y$$

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 2 möglich.

⚠ VORSICHT

Erlangung des Sicherheitslevels

Zur Erlangung des Sicherheitslevels muss der Anwender sicherstellen, dass eine Testung der Verdrahtung in seiner Applikation realisiert wird und 100 Mal häufiger durchgeführt wird, als die Sicherheitsfunktion angefordert wird.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	**60 % ≤ DC < 90 %**
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

9.3 Direktes Verdrahten der TwinSAFE-Ausgänge auf TwinSAFE-Eingänge (2-kanalig) (Kategorie 3, PL d)

Zwei Ausgänge einer EL2904 werden direkt auf zwei sichere Eingänge einer EL1904 verdrahtet, dabei werden die Testpulse und Strommessung der Ausgänge und der Sensortest der Eingänge abgeschaltet. Auf der Eingangsseite werden die beiden Signale auf Diskrepanz innerhalb der TwinSAFE Logik überprüft. Es werden somit die beiden Signale auf ihren Wert überprüft, jedoch sind keine Testungen auf der Leitung aktiv, sodass mögliche Fremdeinspeisungen beim Schalten der Ausgänge detektiert werden.

9.3.1 Parameter der sicheren Ein- und Ausgangsklemmen

EL1904

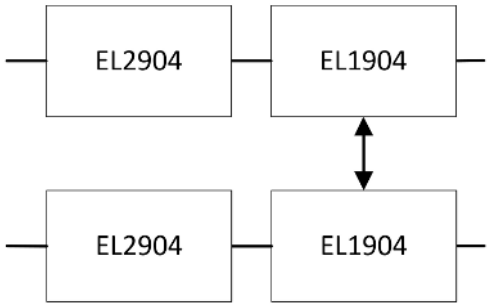
Parameter	Wert
Sensortest Kanal 1 aktiv	Nein
Sensortest Kanal 2 aktiv	Nein
Sensortest Kanal 3 aktiv	Nein
Sensortest Kanal 4 aktiv	Nein
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

EL2904

Parameter	Wert
Strommessung aktiv	Nein
Testpulse des Ausgangs aktiv	Nein

9.3.2 Blockbildung und Safety-Loops

9.3.2.1 Sicherheitsfunktion 1



9.3.3 Berechnung

9.3.3.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
EL1904 – PFH_D	1,11E-09
EL2904 – PFH_D	1,25E-09
Arbeitstage (d_{op})	230

Komponente	Wert
Arbeitsstunden / Tag (h_{op})	8
Zykluszeit (Minuten) (T_{zyklus})	60 (1x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

9.3.3.2 Diagnostic Coverage DC

Komponente	Wert
EL1904/EL2904	DC_{avg}=90%

9.3.3.3 Berechnung Sicherheitsfunktion 1

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1:

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

zu:

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

Die Berechnung des $MTTF_D$-Wertes für Sicherheitsfunktion 1 (unter der gleichen Annahme) berechnet sich mit:

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

als:

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

Sind für EL1904 und EL2904 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

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

Somit:

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0{,}90)}{1{,}11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}1}{9{,}72E-06\frac{1}{y}} = 10288{,}1y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0{,}90)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}1}{1{,}1E-05\frac{1}{y}} = 9090{,}9y$$

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

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

HINWEIS

Kategorie

Diese Struktur ist bis maximal Kategorie 3 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

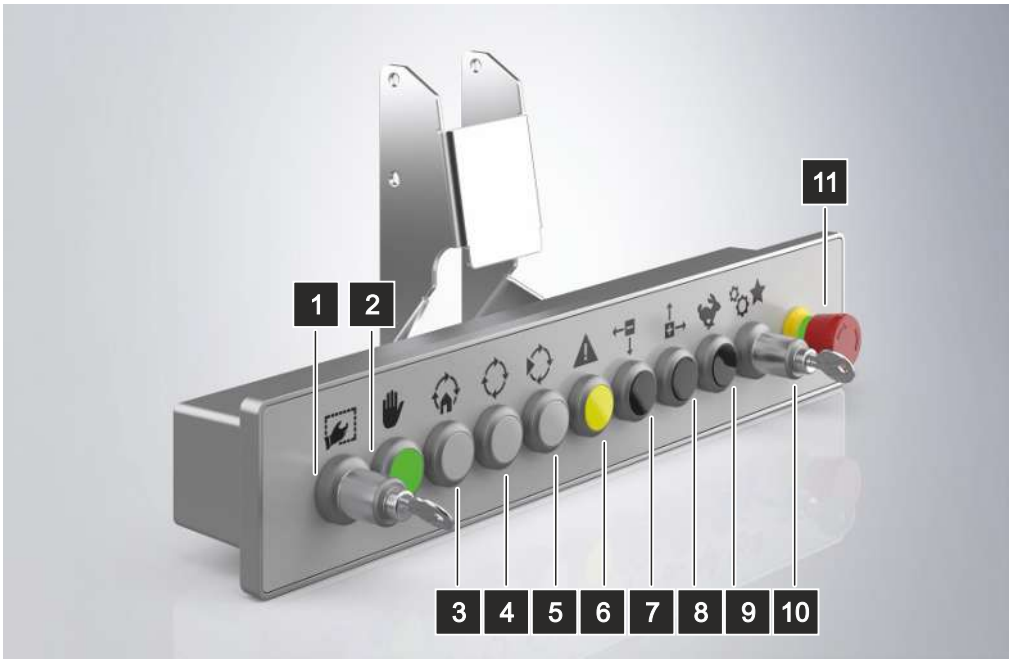
Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

9.4 Applikationsbeispiel C9900-M800

9.4.1 Beschreibung C9900-M800

Das Produkt C9900-M800 ist eine Taster-Erweiterung für ControlPanels aus dem Hause Beckhoff. Die relevanten Taster (siehe Tabelle unten) werden mit einer Safety-Komponente (FB6901-1918 siehe Z10 62386 037 Rev. 1) eingelesen. Diese Signale werden dann von der Safety-Komponente FB6901-1918 in ein PROFIsafe Telegramm verpackt und durch die Standard-Steuerung auf der Taster-Erweiterung an die PROFINET Schnittstelle übergeben.



Taster	Beschreibung	PROFIsafe Signale	Signale FB6901-1918
1 (SW700)	Standard	-	-
2 (SW701)	Standard	-	-
3 (SW702)	Standard	-	-
4 (SW703)	Standard	-	-
5 (SW704)	Standard	-	-
6 (SW705.2)	Leuchtdrucktaster gelb (1x Schließer-Kontakt)	PROFIsafe_2B[0].4	SW705_SafeIn2
7 (SW706)	Standard	-	-
8 (SW707)	Standard	-	-
9 (SW708)	Standard	-	-
10 (SW709.1/.2)	Schlüsselschalter SSG10, links tastend, rechts rastend (2x Schließer-Kontakte)	PROFIsafe_2B[0].2 PROFIsafe_2B[0].3	SW709_SafeIn4 SW709_SafeIn3
11 (SW710.1/.2)	Not-Halt Taster (2x Öffner-Kontakte)	PROFIsafe_2B[0].0 PROFIsafe_2B[0].1	SW710_SafeIn1 SW710_SafeIn5

	Weitere PROFIsafe Signale		
	ModuleFault_SafeIn1_2	PROFIsafe_2B[0].5	FSIN Module1.Module Fault
	ModuleFault_SafeIn3_4	PROFIsafe_2B[0].6	FSIN Module2.Module Fault
	ModuleFault_SafeIn5	PROFIsafe_2B[0].7	FSIN Module3.Module Fault
	ModuleFault_ErrAck	PROFIsafe_1B[0].0	FSIN Module1.Err Ack FSIN Module2.Err Ack

	Weitere PROFIsafe Signale		
			FSIN Module3.Err Ack

9.4.2 Berechnung

9.4.2.1 Allgemein

Die Taster- und Schalter-Signale werden von der FB6901-1918 als einkanalige Signale eingelesen, innerhalb der SIL3-zertifizierten FB6901-1918 verarbeitet und an das PROFIsafe Telegramm übergeben. Die Berechnung der sicherheitstechnischen Kenngrößen erfolgt somit von dem Taster bis zur Übergabe an das sichere Protokoll. Für die weitere Auswertung auf der überlagerten Sicherheitssteuerung werden Annahmen getroffen und daraus Alternativ-Berechnungen erstellt. Somit sind bis auf Sicherheits-Teilfunktion 3 alle Beispiele Kat.2 Funktionen.

9.4.2.2 Kenngrößen FB6901-1918

Kenngröße	Wert
Lifetime [a]	20
Prooftest Intervall [a]	Nicht erforderlich
PFHD	3,4 E-09
PFDavg	5,1E-05
MTTFD	1780 a
DC	97,5% (CAT4)
Performance Level	PL e
Kategorie	4
SFF	>99%
HFT	1
Klassifizierung Element	Typ B
Restfehlerrate Bus Communication	1E-09

Die Restfehlerrate der Bus Kommunikation von 1E-09 (1% vom SIL3) ist bereits in den Kenngrößen der FB6901-1918 berücksichtigt und muss daher nicht nochmal in die folgenden Berechnungen einfließen.

9.4.2.3 Kenngrößen Taster SW710

Kenngröße	Bedienelement	Schaltelement
Lifetime	50.000 Zyklen	1.000.000 Zyklen
B10	65.000 Zyklen	1.300.000 Zyklen
$B10_D$	130.000 Zyklen	2.600.000 Zyklen
Betätigungen / [a] (n_{op})	12	
Ausführung	2x Öffner-Kontakte	

Die Kennzahlen des Schaltelements sind sehr viel größer als die Kennzahlen des Bedienelements, daher werden hier die schlechteren Werte für die Berechnung verwendet.

⚠ WARNUNG

Wert verifizieren

Die Anzahl der Betätigungen ist eine Annahme seitens des Kunden. Dieser Wert muss im Zuge der finalen Berechnung der Sicherheitsfunktion durch den Kunden verifiziert und ggf. angepasst werden.

9.4.2.4 Kenngrößen Taster SW709

Kenngröße	Bedienelement	Schaltelement
Lifetime	50.000 Zyklen	1.000.000 Zyklen
B10	71.660 Zyklen	1.300.000 Zyklen
$B10_D$	-	-
Betätigungen / [a] (n_{op})	52	
Ausführung	2x Schließer-Kontakte	

Die Kennzahlen des Schaltelements sind sehr viel größer als die Kennzahlen des Bedienelements, daher werden hier die schlechteren Werte für die Berechnung verwendet.

⚠ WARNUNG

Wert verifizieren

Die Anzahl der Betätigungen ist eine Annahme seitens des Kunden. Dieser Wert muss im Zuge der finalen Berechnung der Sicherheitsfunktion durch den Kunden verifiziert und ggf. angepasst werden.

9.4.2.5 Kenngrößen Taster SW705

Kenngröße	Bedienelement	Schaltelement
Lifetime	1.000.000 Zyklen	1.000.000 Zyklen
B10	1.300.000 Zyklen	1.300.000 Zyklen
$B10_D$	-	-
Betätigungen / [a] (n_{op})	8760	
Ausführung	1x Schließer-Kontakt	

Die Kennzahlen des Schaltelements sind identisch, somit ist es nicht relevant welcher der Werte verwendet wird.

⚠ WARNUNG

Wert verifizieren

Die Anzahl der Betätigungen ist eine Annahme seitens des Kunden. Dieser Wert muss im Zuge der finalen Berechnung der Sicherheitsfunktion durch den Kunden verifiziert und ggf. angepasst werden.

9.4.2.6 Parameter der FB6910-1918

Index	Beschreibung	Wert
80x0:01	ModuloDiagTestPulse	0x00
80x0:02	MultiplierDiagTestPulse	0x01
80x0:04	Diag Testpulse active	TRUE
80x0:05	Module Fault Link active	TRUE
80x1:01	Channel 1.InputFilterTime	0x0014 (20) x 0.1 msec
80x1:02	Channel 1.DiagTestPulseFilterTime	0x0002 (2) x 0.1 msec
80x1:04	Channel 2.InputFilterTime	0x0014 (20) x 0.1 msec
80x1:05	Channel 2.DiagTestPulseFilterTime	0x0002 (2) x 0.1 msec

Die Parameter der FB6901-1918 sind auf den Default-Einstellungen belassen worden.

Die Testpulse aller Kanäle sind eingeschaltet und über den Parameter Module Fault Link active werden alle Eingangsmodule im Fehlerfall in den Zustand ModuleFault gesetzt.

9.4.2.7 Annahmen für den Diagnostic Coverage DC

Komponente	DC-Wert
SW710.1 Einkanalige Auswertung des Not-Halt Signals mit Testpulsen (Kategorie 2 Struktur) Der Not-Halt-Taster ist als Öffner-Kontakt ausgeführt und wird somit durch zyklische Tests überprüft. Die Testrate ist somit mehr als 100-mal höher als die Anforderung der Sicherheitsfunktion.	90%
SW710.2 Einkanalige Auswertung des Not-Halt Signals mit Testpulsen (Kategorie 2 Struktur) Begründung siehe SW710.1	90%

Alternative für Not-Halt-Taster	DC-Wert
Für SW710.1 und SW710.2 wird in der überlagerten Sicherheitssteuerung eine zweikanalige Auswertung mit Prüfung auf Plausibilität durchgeführt (Kategorie 4 Struktur)	99%

Einkanalige Komponenten	DC-Wert
SW709.1 Einkanalige Auswertung des Schlüsselschalter (Position 1) mit Testpulsen (Kategorie 2 Struktur) Die Verdrahtung des Schließer-Kontaktes wird nur im betätigten Zustand mit Testpulsen überprüft. Die Verbindung zwischen Schalter und sicherem Eingang ist innerhalb des Gehäuses realisiert, somit können keine Kurzschlüsse durch externe Einflüsse entstehen. Durch die hohe Diagnose der FB6901-1918 werden Umgebungsbedingungen, wie z.B. Spannung, Temperatur, usw. überwacht und somit kann für den DC ein Wert von 60% angenommen werden. **WARNUNG Die Sicherheitsfunktion muss durch den Anwender so festgelegt werden, dass der NICHT-geschaltete Zustand der sichere Zustand ist.**	60%
SW709.2 Einkanalige Auswertung des Schlüsselschalter (Position 2) mit Testpulsen (Kategorie 2 Struktur) Begründung und Warnung siehe SW709.1	60%
SW705.2 Einkanalige Auswertung des Reset-Tasters mit Testpulsen (Kategorie 2 Struktur) Begründung und Warnung siehe SW709.1 **Hinweis Wenn in der überlagerten Steuerung die steigende und fallende Flanke und das zeitliche Verhalten des Reset-Tasters überwacht werden (im Bereich von 0,5s – 5s zwischen steigender und fallender Flanke), kann statt eines DC von 60 % ein DC von 90% angenommen werden.**	60%

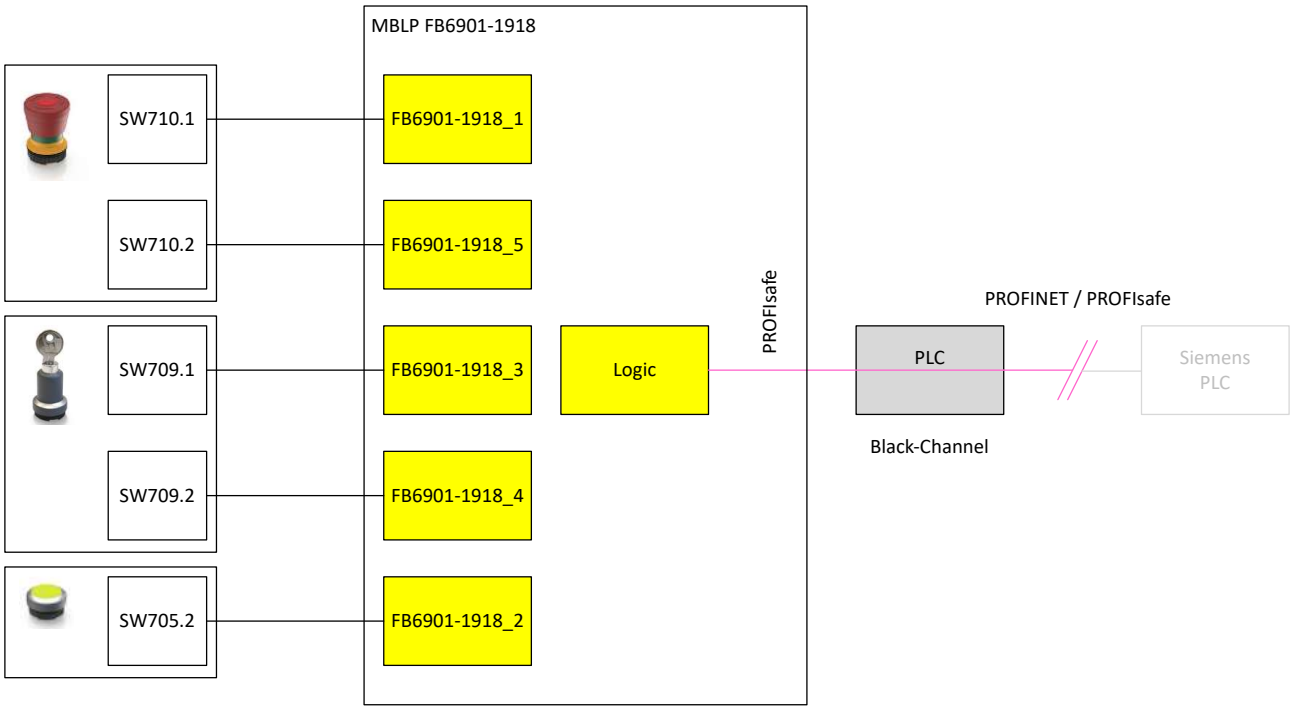
⚠ WARNUNG

Plausibilitätsprüfung und Kreuzvergleich durchführen

Für die alternative Berechnung des Not-Halt-Tasters mit der Annahme eines DC von 99% muss zwingend eine Plausibilitätsprüfung / Kreuzvergleich der beiden Signale des Schalters SW710 in der überlagerten Sicherheitssteuerung erfolgen.

9.4.2.8 Blockblildung und Safety-Loops

9.4.2.8.1 Übersicht



9.4.2.8.2 Allgemeine Formeln zur Berechnung von MTTFD und PFHD

Abschätzung, wenn nur ein B10-Wert zur Verfügung steht (siehe Tabelle C.1 DIN EN ISO 13849-1):

$$B10_D = 2 * B10$$

Betätigungen pro Jahr:

$$n_{op} = Betätigungen\ pro\ Jahr$$

Herleitung MTTFD aus B10D:

$$MTTF_D = \frac{1}{\lambda_D}\ mit\ \lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

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

Berechnung Gesamt MTTFD:

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

$$MTTF_D = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}}$$

Berechnung Gesamt-DC:

$$DC_{avg} = \frac{\frac{DC_{SW7xx}}{MTTF_{D(SW7xx)}} + \frac{DC_{FB6901-1918}}{MTTF_{D(FB6901-1918)}}}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}}$$

Berechnung PFHD aus MTTFD und DC:

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

Berechnung Gesamt-PFHD (für einkanalige Strukturen):

$$PFH_{Dges} = PFH_{D(SW7xx)} + PFH_{D(FB6901-1918)}$$

Berechnung Gesamt-PFHD (für zweikanalige Strukturen):

$$PFH_{Dges} = \beta * \frac{PFH_{D(SW710.1)} + PFH_{D(SW710.2)}}{2} + (1-\beta)^2 * \left(PFH_{D(SW710.1)} * PFH_{D(SW710.2)}\right) * T_1 + PFH_{D(FB6901-1918)}$$

9.4.2.8.3 Sicherheits-Teilfunktionen 1/2 (SW710.1 / SW710.2)

Die Sicherheits-Teilfunktion 1/2 besteht aus einem Kanal des Nothalt-Tasters (hier SW710.1 bzw. SW710.2), zusammen mit der FB6901-1918 und dem Signal im PROFIsafe-Telegramm.

Die Berechnung für die beiden Einzelkanäle ist identisch, daher wird diese hier nur einmal berechnet.

⚠ WARNUNG

Maßnahmen durchführen

Die Erweiterung dieses Blockschaltbildes um die überlagerte Steuerung und die geschaltete Aktorik zusammen mit der Überwachung des Rückführkreises und der Implementierung der Wiederanlaufsperre muss durch den Kunden erfolgen.

Berechnung der PFH_D und $MTTF_D$ Werte aus den $B10_D$-Werten:

Berechnung MTTFD und DC:

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}} = \frac{130.000}{0{,}1 * 12} = 108.000\ a$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}} = \frac{1}{\frac{1}{108.000} + \frac{1}{1.780}} = 1.751\ a$$

$$DC_{avg} = \frac{\frac{0{,}9}{108.000} + \frac{0{,}975}{1.780}}{\frac{1}{108.000} + \frac{1}{1.780}} = 0{,}973 = 97{,}3\%$$

Berechnung PFH:

$$PFH_D = \frac{(1 - DC)}{MTTF_D} = \frac{1 - 0{,}9}{108.000} = 9{,}26E - 07$$

$$PFH_{Dges} = PFH_{D(SW7xx)} + PFH_{D(FB6901-1918)} = 9{,}26E - 07 + 3{,}4E - 09 = 9{,}30E - 07$$

⚠ WARNUNG

In Kategorie 2 einsetzen

Diese Struktur der Sicherheits-Teilfunktion kann in Kategorie 2 eingesetzt werden.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC_{avg}	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

9.4.2.8.4 Sicherheits-Teilfunktion 3 (SW710.1 und SW710.2)

Die Sicherheits-Teilfunktion 3 besteht aus zwei Kanälen des Nothalt-Tasters (hier SW710.1 und SW710.2), zusammen mit der FB6901-1918 und den 2 Signalen im PROFIsafe-Telegramm.

⚠ WARNUNG

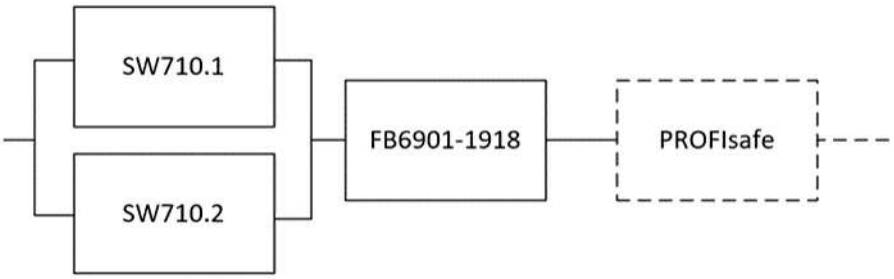
Plausibilitätsprüfung durchführen und Wiederanlaufsperre einrichten

In der überlagerten Sicherheitssteuerung muss eine Plausibilitätsprüfung der beiden Signale durchgeführt und auch die Wiederanlaufsperre durch den Kunden implementiert werden

⚠ WARNUNG

Maßnahmen durchführen

Die Erweiterung dieses Blockschaltbildes um die überlagerte Steuerung und die geschaltete Aktorik zusammen mit der Überwachung des Rückführkreises und der Implementierung der Wiederanlaufsperre muss durch den Kunden erfolgen.



Die beiden Kanäle des Not-Halt-Tasters sind als Öffner-Kontakte ausgeführt und werden über Testpulse getestet. In der überlagerten Steuerung wird die Prüfung der beiden Signale auf Plausibilität durchgeführt. Um die Berechnung zu vereinfachen, kann man den schlechteren der beiden Werte für die Kombination heranziehen (siehe auch D.2 der DIN EN ISO 13849-1:2016). Hier in diesem Fall sind die Werte identisch.

Berechnung der PFH_D und $MTTF_D$ Werte aus den $B10_D$-Werten:

Berechnung MTTFD und DC:

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}} = \frac{130.000}{0{,}1 * 12} = 108.000\ a$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}} = \frac{1}{\frac{1}{108.000} + \frac{1}{1.780}} = 1.751\ a$$

$$DC_{avg} = \frac{\frac{0{,}99}{108.000} + \frac{0{,}975}{1.780}}{\frac{1}{108.000} + \frac{1}{1.780}} = 0{,}975 = 97{,}5\%$$

Berechnung PFH:

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-Case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält eine Tabelle, mit der dieser β–Faktor genau bestimmt werden kann. Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

$$PFH_{D(SW710.1)} = \frac{(1 - DC)}{MTTF_D} = \frac{1 - 0{,}99}{108.000} = 9{,}26E - 08$$

$$PFH_{D(SW710.2)} = \frac{(1 - DC)}{MTTF_D} = \frac{1 - 0{,}99}{108.000} = 9{,}26E - 08$$

$$PFH_{Dges} = \beta * \frac{PFH_{D(SW710.1)} + PFH_{D(SW710.2)}}{2} + (1 - \beta)^2 * \left(PFH_{D(SW710.1)} * PFH_{D(SW710.2)}\right) * T_1 + PFH_{D(FB6901-1918)}$$

Da der Anteil $(1 - \beta)^2 * \left(PFH_{D(SW710.1)} * PFH_{D(SW710.2)}\right) * T_1$ um Zehnerpotenzen kleiner ist, als der Rest, wird dieser als Vereinfachung in dieser Berechnung nicht berücksichtigt.

$$PFH_{Dges} = \beta * \frac{PFH_{D(SW710.1)} + PFH_{D(SW710.2)}}{2} + PFH_{D(FB6901-1918)}$$

$$PFH_{Dges} = 10\% * \frac{9{,}26E - 08 + 9{,}26E - 08}{2} + 3{,}4E - 09 = 12{,}66E - 09 = 1{,}27E - 08$$

⚠ WARNUNG

Bis höchstens Kategorie 4 einsetzen

Diese Struktur der Sicherheits-Teilfunktion kann in Kategorie 4 eingesetzt werden.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC_{avg}	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

9.4.2.8.5 Sicherheits-Teilfunktionen 4/5 (SW709.1 und SW709.2)

Die Sicherheits-Teilfunktionen 4 und 5 bestehen aus einem Kanal des Schlüsselschalters (hier SW709.1 bzw. SW709.2), zusammen mit der FB6901-1918 und dem Signal im PROFIsafe-Telegramm.

Die Berechnung für die beiden Einzelkanäle ist identisch, daher wird diese hier nur einmal berechnet.

⚠ WARNUNG

Maßnahmen durchführen

Die Erweiterung dieses Blockschaltbildes um die überlagerte Steuerung und die geschaltete Aktorik zusammen mit der Überwachung des Rückführkreises und der Implementierung der Wiederanlaufsperre muss durch den Kunden erfolgen.

⚠ WARNUNG

Sicheren Zustand einhalten

Die Sicherheitsfunktion muss durch den Anwender so festgelegt werden, dass der NICHT-geschaltete Zustand der sichere Zustand ist.

Berechnung der PFH_D und $MTTF_D$ Werte aus den $B10_D$-Werten:

Berechnung B10D:

$$B10_D = 2 * B10 = 2 * 71.660 = 143.320$$

Berechnung MTTFD und DC:

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}} = \frac{143.320}{0{,}1 * 52} = 27.561\ a$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}} = \frac{1}{\frac{1}{27.561} + \frac{1}{1.780}} = 1.672\ a$$

$$DC_{avg} = \frac{\frac{0{,}6}{27.561} + \frac{0{,}975}{1.780}}{\frac{1}{27.561} + \frac{1}{1.780}} = 0{,}9523 = 95{,}2\%$$

Berechnung PFH:

$$PFH_D = \frac{(1 - DC)}{MTTF_D} = \frac{1 - 0{,}6}{27.561} = 1{,}45E-05$$

$$PFH_{Dges} = PFH_{D(SW7xx)} + PFH_{D(FB6901-1918)} = 1{,}45E-05 + 3{,}4E-09 = 1{,}45E-05$$

⚠ WARNUNG

In Kategorie 2 einsetzen

Diese Struktur der Sicherheits-Teilfunktion kann in Kategorie 2 eingesetzt werden.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC_{avg}	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

9.4.2.8.6 Sicherheits-Teilfunktion 6 (SW705.2)

Die Sicherheits-Teilfunktion 6 besteht aus einem Kanal des Reset-Tasters (hier SW705.2), zusammen mit der FB6901-1918 und dem Signal im PROFIsafe-Telegramm.

⚠ WARNUNG

Maßnahmen durchführen

Die Erweiterung dieses Blockschaltbildes um die überlagerte Steuerung und die geschaltete Aktorik zusammen mit der Überwachung des Rückführkreises und der Implementierung der Wiederanlaufsperre muss durch den Kunden erfolgen.

Berechnung der PFH_D und $MTTF_D$ Werte aus den $B10_D$-Werten:

Berechnung B10D:

$$B10_D = 2 * B10 = 2 * 1.300.000 = 2.600.000$$

Berechnung MTTFD und DC:

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}} = \frac{2.600.000}{0{,}1 * 8760} = 2.968\ a$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}} = \frac{1}{\frac{1}{2.968} + \frac{1}{1.780}} = 1.112\ a$$

HINWEIS

DC-Wert

Wenn in der überlagerten Steuerung die steigende und fallende Flanke und das zeitliche Verhalten des Reset-Tasters überwacht werden (im Bereich von 0,5 s – 5 s zwischen steigender und fallender Flanke), kann statt eines DC von 60 % ein DC von 90% angenommen werden.

$$DC_{avg} = \frac{\frac{0{,}6}{1.112} + \frac{0{,}975}{1.780}}{\frac{1}{1.112} + \frac{1}{1.780}} = 0{,}744 = 74{,}4\%$$

Berechnung PFH:

$$PFH_D = \frac{(1 - DC)}{MTTF_D} = \frac{1 - 0{,}6}{1.112} = 3{,}60E-04$$

$$PFH_{Dges} = PFH_{D(SW7xx)} + PFH_{D(FB6901-1918)} = 3{,}60E-04 + 3{,}4E-09 = 3{,}60E-04$$

⚠ WARNUNG

In Kategorie 2 einsetzen

Diese Struktur der Sicherheits-Teilfunktion kann in Kategorie 2 eingesetzt werden.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC_{avg}	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	**60 % ≤ DC < 90 %**
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	kein	kein	niedrig	mittel	niedrig	mittel	hoch
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

10 Anbindung von PROFIsafe

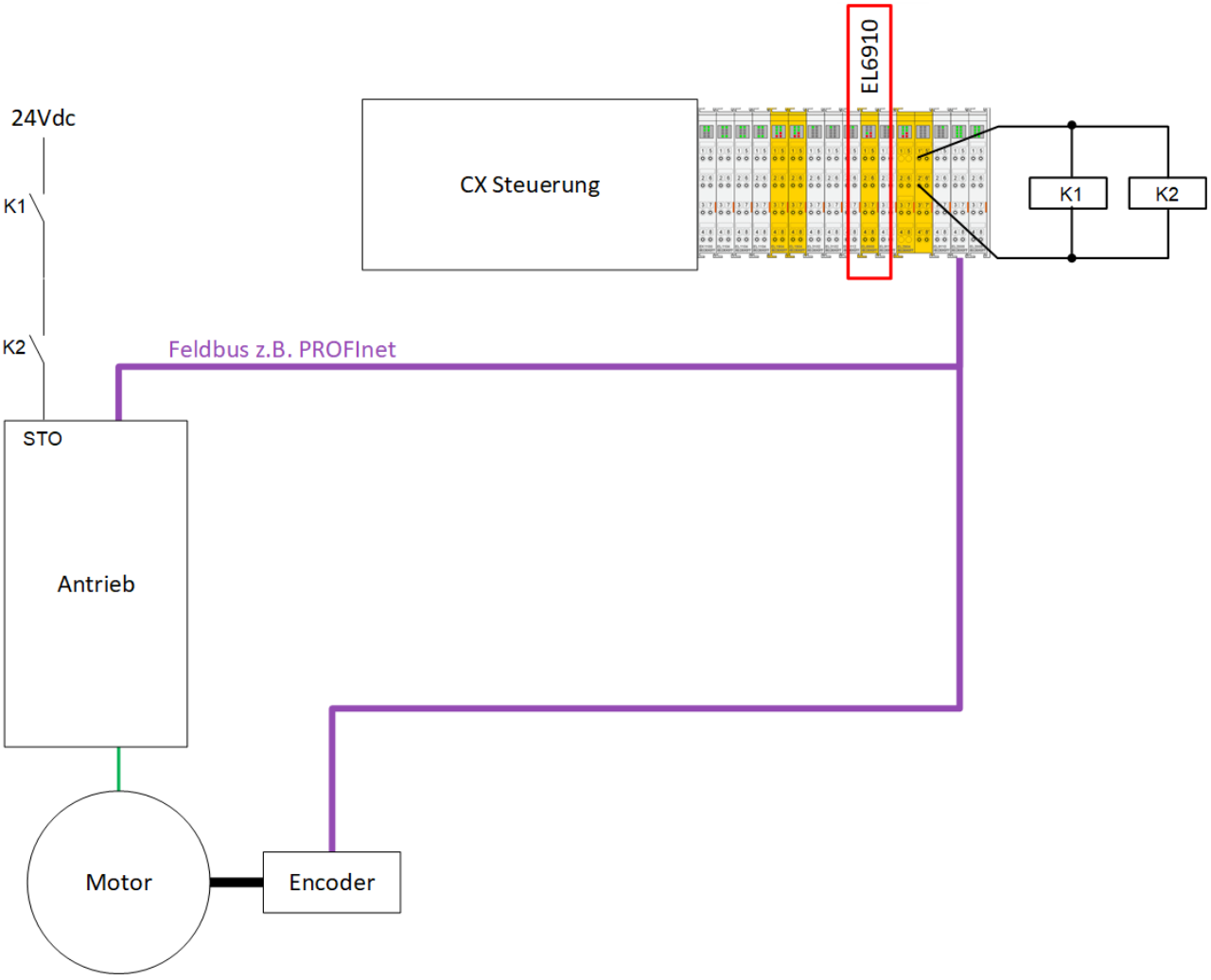
10.1 Sichere Geschwindigkeitsüberwachung mit PROFIsafe-Encoder (Kategorie 4, PL e)

Die Geschwindigkeit eines Antriebes soll überwacht werden. Dieser Antrieb hat eine Sicherheitsfunktion (hier z.B. STO), welche über einen entsprechenden Eingang aktiviert wird. Dieser Eingang/Eingänge wird über jeweils einen Arbeitskontakt zweier Schütze geführt. Zur sicheren Aufnahme der Geschwindigkeit wird ein sicherer Absolutdrehgeber der Firma TR-Electronic genutzt. Dieser ist für Anwendungen bis Performance Level e zertifiziert. Die sicherheitsrelevanten Daten werden mit Hilfe von PROFIsafe über PROFInet übertragen. Die Geschwindigkeitsdaten werden über das sicherheitsrelevante Protokoll PROFIsafe an die EL6910 als PROFIsafe-Master übertragen und dort mit Hilfe der verfügbaren vorzertifizierten Funktionsbausteine für Analogwertverarbeitung überwacht.

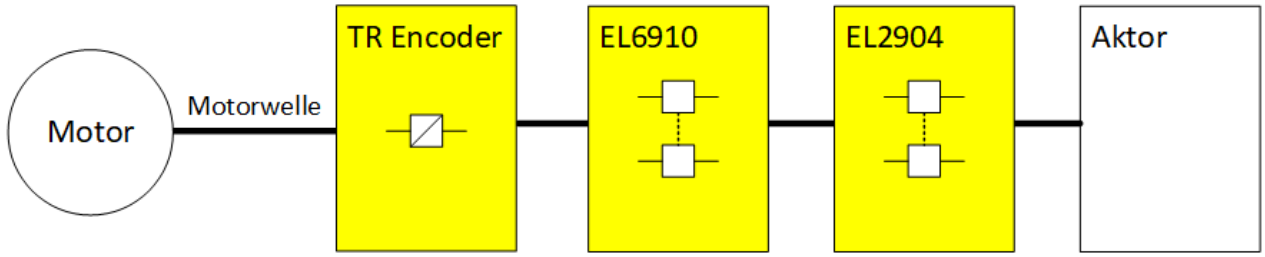
Ist der aktuelle Geschwindigkeitswert unterhalb der im FB Limit festgelegten Grenze, wird der STO Ausgang auf logisch 1 gesetzt und der Antrieb kann drehen. Ist die Grenze überschritten, wird der Ausgang auf logisch 0 gesetzt und der Antrieb wird momentenfrei geschaltet bzw. die im Antrieb integrierte Sicherheitsfunktion aktiviert. Die gesamte Berechnung und Skalierung wird in der sicherheitsgerichteten Logik EL6910 auf dem Sicherheitsniveau SIL3 / PL e durchgeführt.

Über einen ESTOP Baustein wird zusätzlich eine Nothalt-Funktion implementiert (zur Reduktion der Komplexität nicht in der Graphik dargestellt), welche den Wiederanlauf verhindert und auch die Schützkontrolle für K1 und K2 übernimmt.

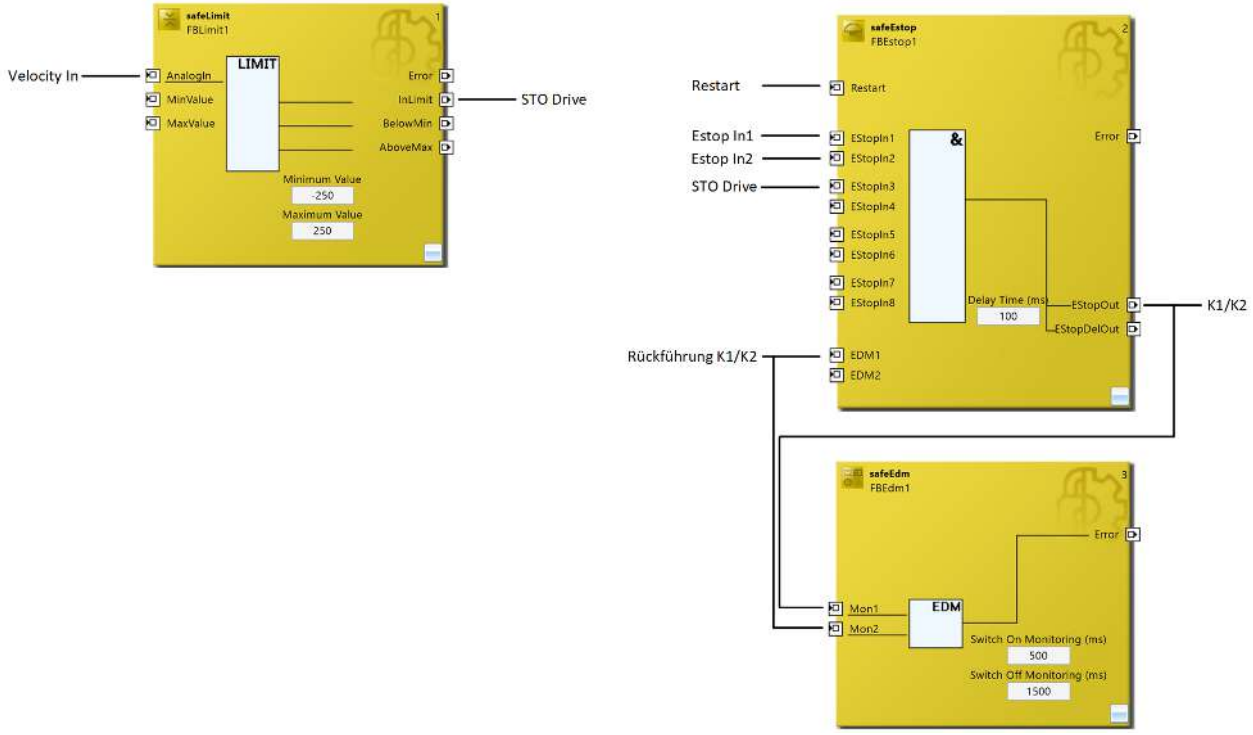
Aufbau



Strukturbild Aufbau



Logik



Korrekte Konfiguration Gesamtsystem

Bei der Übertragung von PROFIsafe innerhalb EtherCAT gibt es folgende Einschränkungen.

PROFIsafe-Telegramm nur über E-Bus und PROFINET/PROFIBUS

Die Verwendung von PROFIsafe ist es aufgrund der PROFIsafe Policy nur über die Feldbusse PROFIBUS und PROFINET oder über einen Rückwandbus, hier z.B. der E-Bus zulässig. Eine Nutzung von PROFIsafe über andere Feldbusse ist aus patentrechtlichen Gründen nicht zulässig. Dies muss durch Verwendung der Segment-Abschluss-Klemme EL9930 sichergestellt werden.

Folgende Patente der Siemens AG sind entsprechend des PROFIsafe Profils relevant:
- EP1267270-A2 Method for data transfer
- WO00/045562-A1 Method and device for determining the reliability of data carriers
- WO99/049373-A1 Shortened data message of an automation system
- EP1686732 Method and system for transmitting protocol data units
- EP1802019 Identification of errors in data transmission
- EP1921525-A1 Method for operation of a safety-related system
- EP13172092.2 Method and system for detection of errors

Je nach Architektur der Anwendung müssen also entsprechende Maßnahmen getroffen werden. Details zur korrekten Konfiguration des Gesamtsystems bezüglich PROFIsafe sind in den Dokumentationen der EL6910 und EL9930 zu finden.

Einsatz externer sicherer Geber

Bei dem Einsatz eines externen Gebers sind weitere Anforderungen zu beachten.

⚠ VORSICHT

Einsatz externer sicherer Geber

Beim Einsatz eines externen sicheren Gebers ist stets die aktuelle Version der Dokumentation zu beachten. Hier finden sich alle Anforderungen bezüglich Montage, Betrieb, Instandsetzung, welche zwingend erfüllt werden müssen, damit der Geber in einer sicherheitsrelevanten Applikation korrekt genutzt werden kann.

10.1.1 FMEA

Fehlerannahme	Erwartungshaltung	Überprüft
Geschwindigkeitswert friert ein	Die Geschwindigkeit im Encoder wird sicher ermittelt (Performance Level e) und über PROFIsafe sicher übertragen. Ein Einfrieren des Telegrammes wird über den Watchdog des sicheren Kommunikationsprotokolls detektiert.	
Geschwindigkeitswert wird verfälscht	Die Geschwindigkeit im Encoder wird sicher ermittelt (Performance Level e) und über PROFIsafe sicher übertragen. Eine Verfälschung des Telegrammes wird über das sichere Kommunikationsprotokoll detektiert.	
Verbindung zwischen Motor und Encoder ist nicht mehr gegeben	Kann detektiert werden über eine Plausibilisierung mit einem Standardsignal des Antriebs. So kann sowohl die Standard-Geschwindigkeit des Antriebs zur Plausibilisierung genutzt werden als auch eine Boolesche Information, ob der Antrieb drehen soll. Alternativ kann das Positionssignal des sicheren Telegramms als Eingangssignal des Funktionsblocks safeScaling genutzt werden, um mit Hilfe des Ausgangs *StuckAtError* diesen Fehlerfall detektieren zu können (z. B. in Kombination mit der Auswertung der Information ob der Antrieb aktiv gebremst wird). Plausibilitätsprüfung: Wenn der Motor gestartet wird, werden auch dynamische Geschwindigkeitswerte erwartet.	

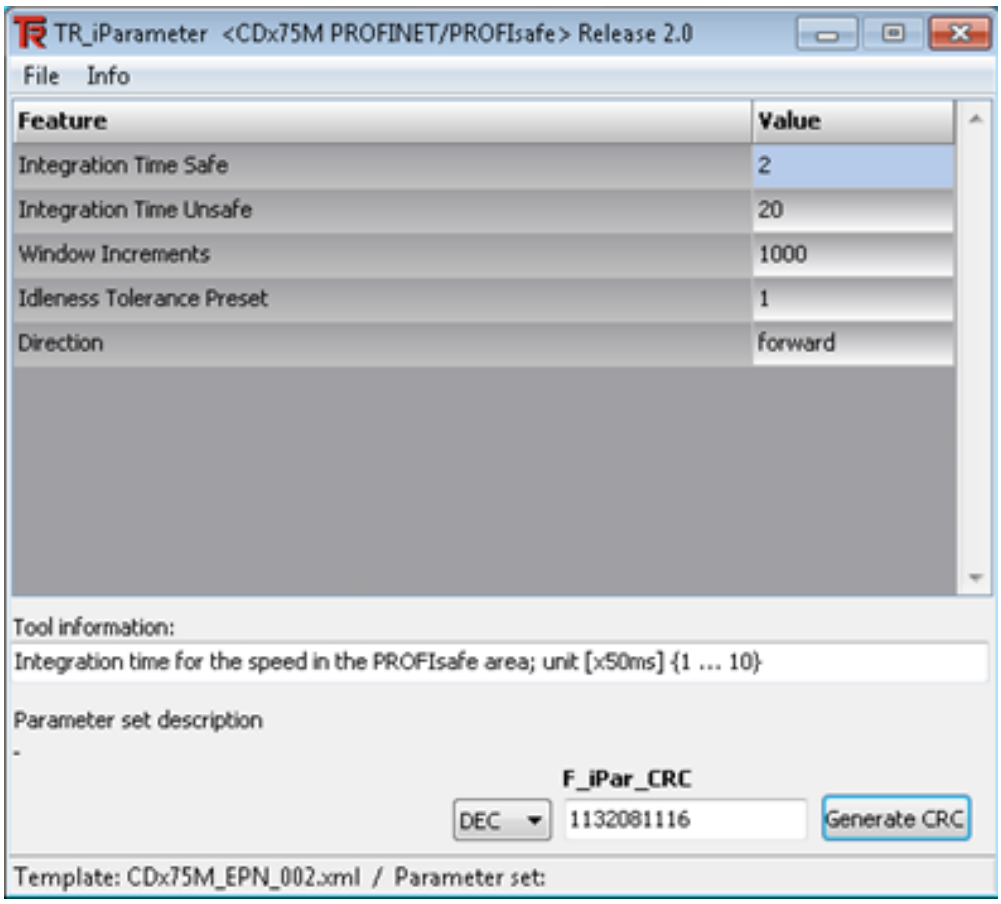
10.1.2 Konfiguration in Engineeringumgebung

Im Rahmen des vorliegenden Applikationsbeispiels wird neben der Anbindung von TwinSAFE-Komponenten die zusätzliche Anbindung eines Encoders über PROFIsafe/PROFInet betrachtet. Im Folgenden werden im Detail alle nötigen Konfigurationsschritte zur Realisierung beschrieben.

Für die Konfiguration der sicherheitsrelevanten Parameter des Encoders ist eine zusätzliche Anwendung erforderlich, um die Parametrierung des Geräts vorzunehmen und die CRC Prüfsumme der iParameter zu ermitteln, welche letztlich innerhalb TwinCAT zusätzlich konfiguriert werden muss.

10.1.2.1 Konfiguration Encoder

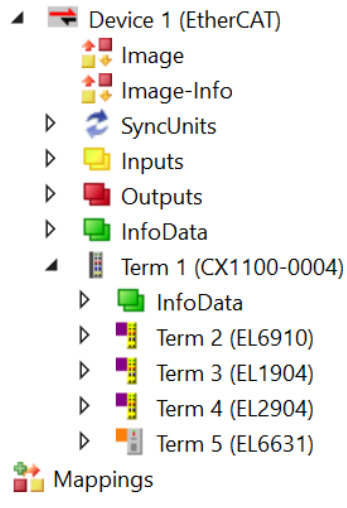
Zur Parametrierung des Encoders ist eine zusätzliche Anwendung notwendig. Die aktuelle Version kann von der Webseite des Herstellers bezogen werden.



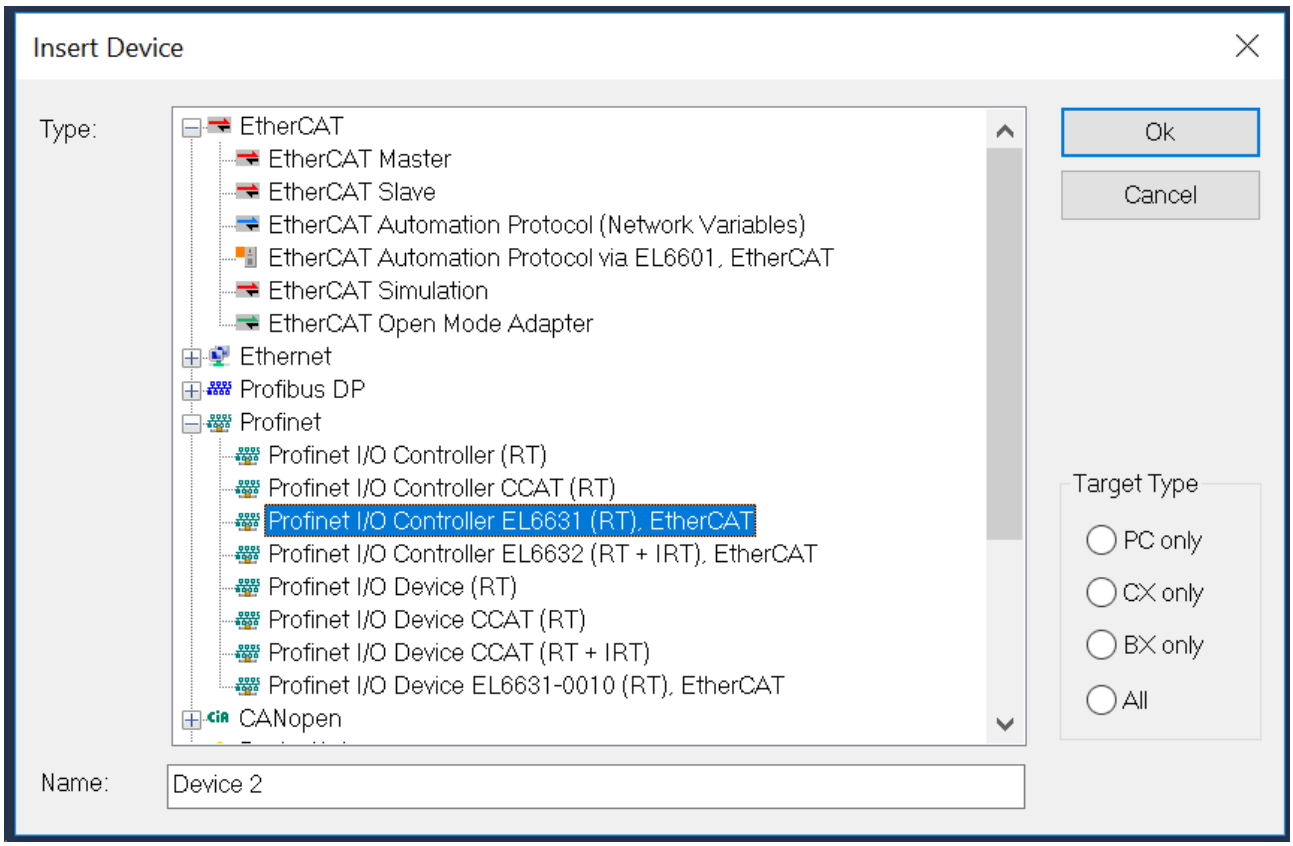
Hier müssen entsprechend der Applikation die notwendigen Parameter konfiguriert werden, damit die CRC Prüfsumme korrekt berechnet werden kann (im Bild **F_iPar_CRC**).

10.1.2.2 Konfiguration TwinCAT I/O

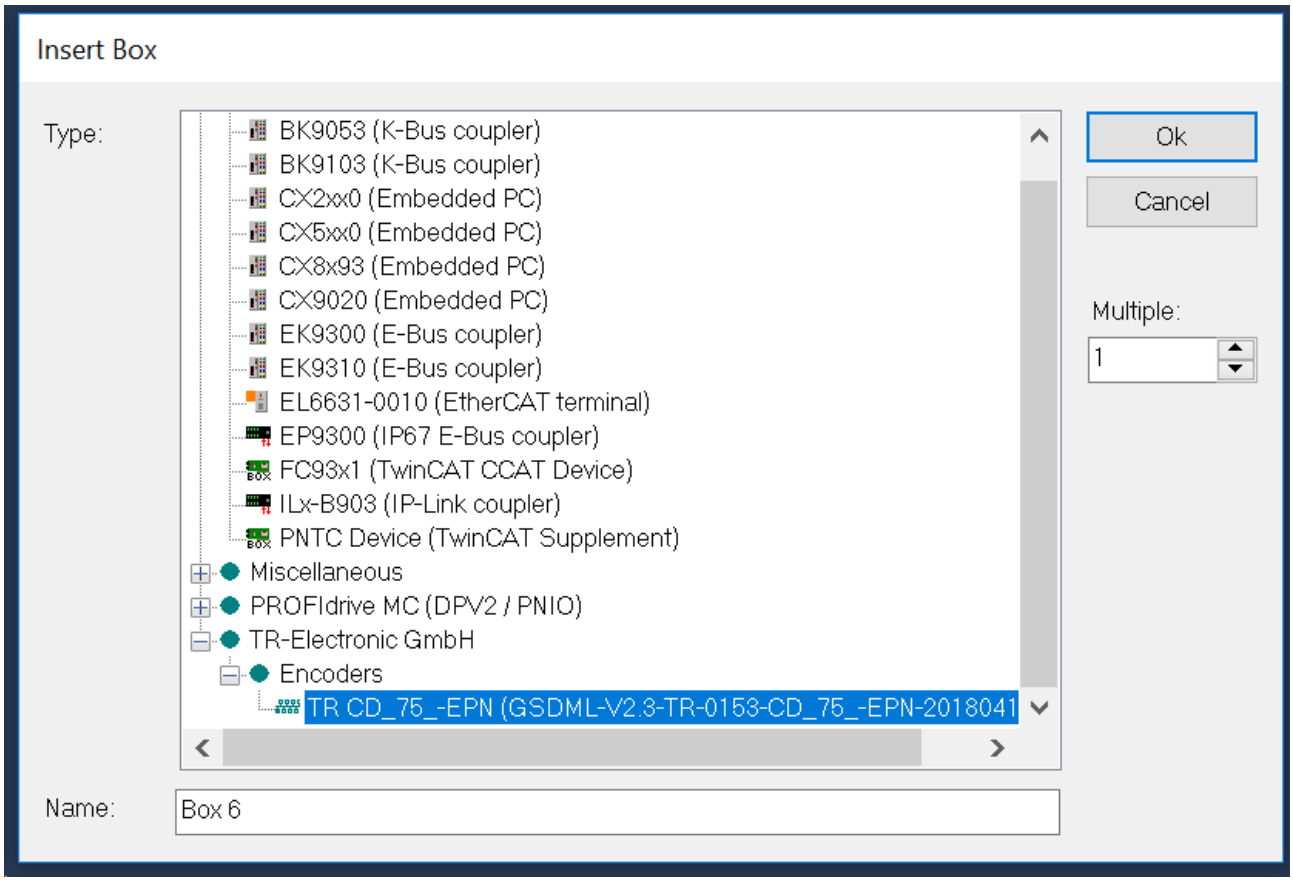
Zunächst wird eine neues TwinCAT Projekt angelegt und der EtherCAT-Strang konfiguriert.



Zusätzlich wird die Konfiguration des PROFInet-Strangs durch Hinzufügen eines PROFInet-I/O-Controllers erzeugt.



Analog zur Konfiguration des EtherCAT-Strangs kann auch im Falle des PROFInet-Controllers ein automatischer Scan angestoßen oder die Konfiguration manuell erzeugt werden. So kann auch der Encoder manuell hinzugefügt werden.



Für die erfolgreiche Nutzung des Encoders über PROFIsafe sind folgende Informationen zu beachten.

⚠ VORSICHT

Datentyp WORD!

Bei Verwendung von WORD-Datentypen innerhalb des Prozessabbildes muss unter Umständen eine zusätzliche Konfiguration erfolgen.

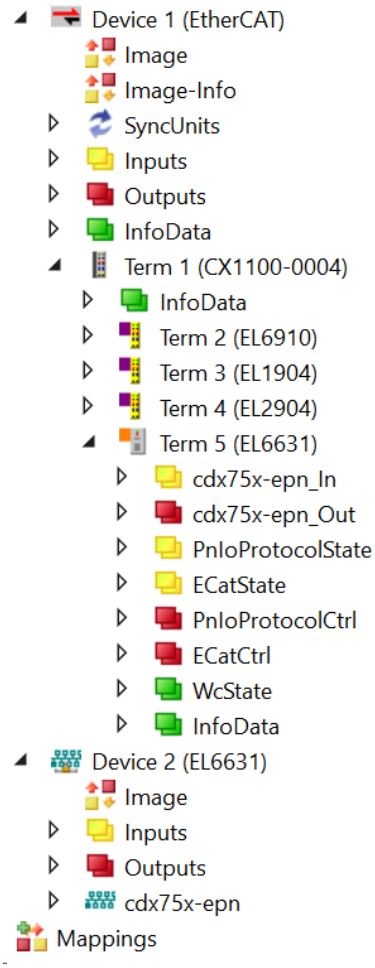
Wird innerhalb der Konfiguration keine EL9930 zur Begrenzung des PROFIsafe-Segments eingesetzt, so muss im Rahmen der I/O-Konfiguration des PROFIsafe-Gerätes für die im Prozessabbild enthaltenen Signale mit WORD-Datentyp des Tauschen des High und Low Byte-Anteiles konfiguriert werden. Dies erfolgt durch Auswahl der Checkbox *Tausche LOBYTE und HIBYTE* direkt auf den Datenwerten (unter dem Reiter *Flags*).

⚠ VORSICHT

iParamater

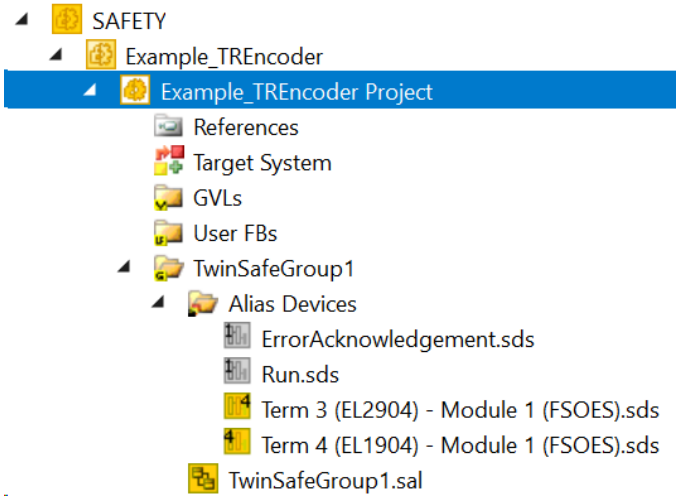
Auf dem PROFIsafe I/O-Gerät müssen die identischen iParameter wie auf dem *Alias Device* konfiguriert sein, damit die Kommunikation korrekt starten kann.

Anschließend kann mit der Konfiguration des Safety Projekts fortgefahren werden. Dabei wird an dieser Stelle von folgender Ausgangslage ausgegangen.

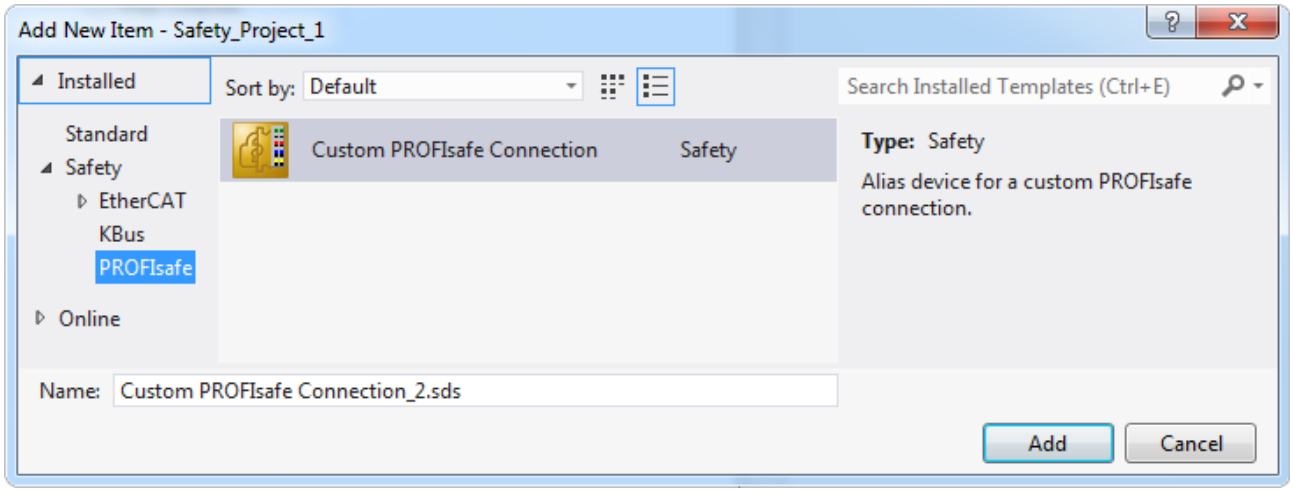


10.1.2.3 Konfiguration Verbindungen TwinCAT Safety Projekt

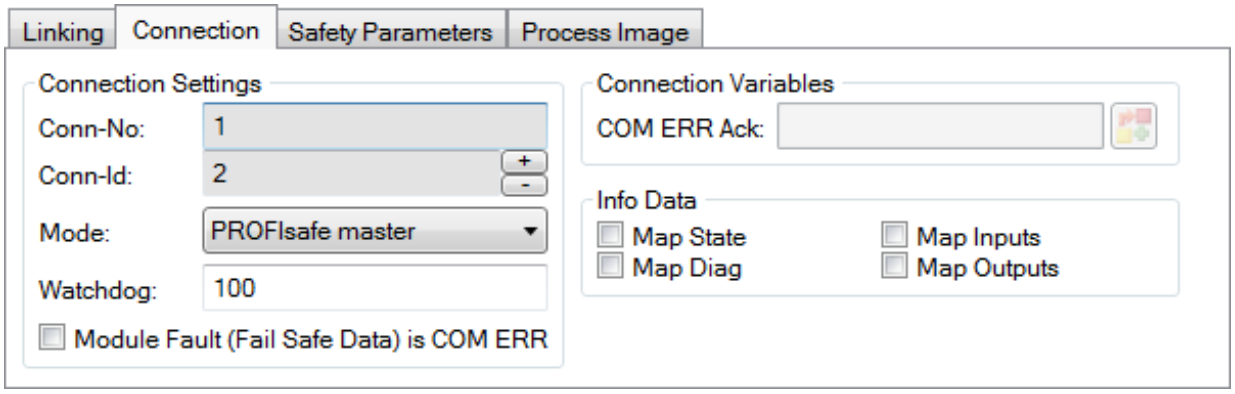
Vor der Konfiguration der PROFIsafe-Verbindung wird zunächst ein Safety Projekt angelegt und die benötigten Alias Devices für die verfügbaren EtherCAT-Komponenten importiert. Zusätzlich wird das Zielsystem auf die EL6910 des EtherCAT-Strangs gemappt (über den Knoten *Target System*).



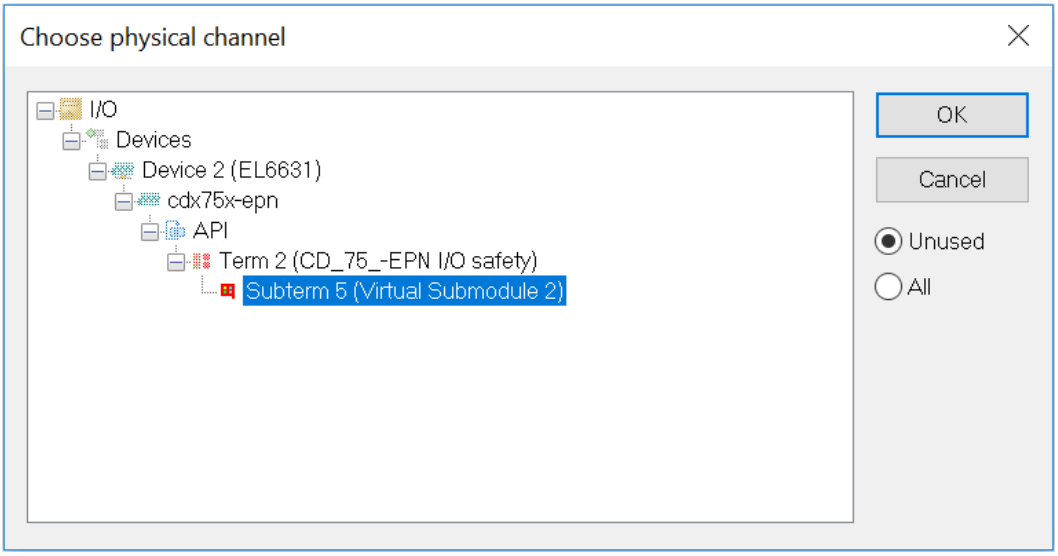
Anschließend kann mit der Konfiguration der PROFIsafe-Verbindung zum TR Encoder fortgefahren werden. Diese Verbindung wird wie üblich über ein *Alias Device* realisiert. Über das Kontextmenu des Knotens *Alias Devices* und durch Auswahl von *Add* und *New item…* kann eine Custom PROFIsafe Connection angelegt werden.



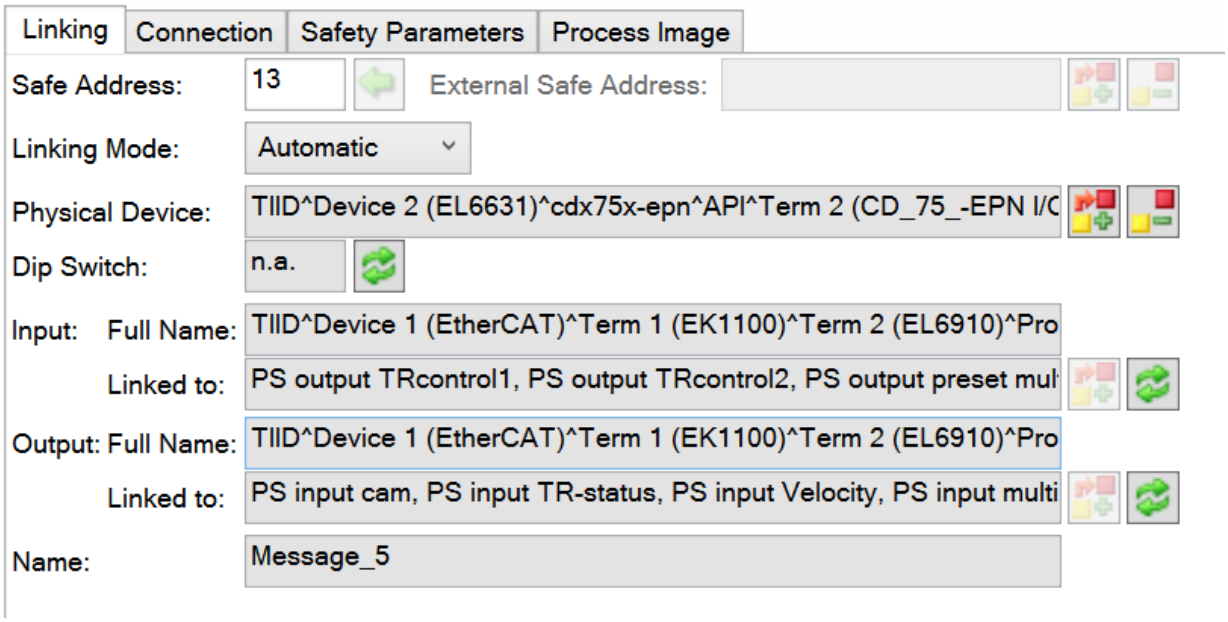
Nach dem Öffnen des Alias Devices muss zunächst über den Reiter *Connection* als Modus der Verbindung *PROFIsafe-Master* gewählt werden.



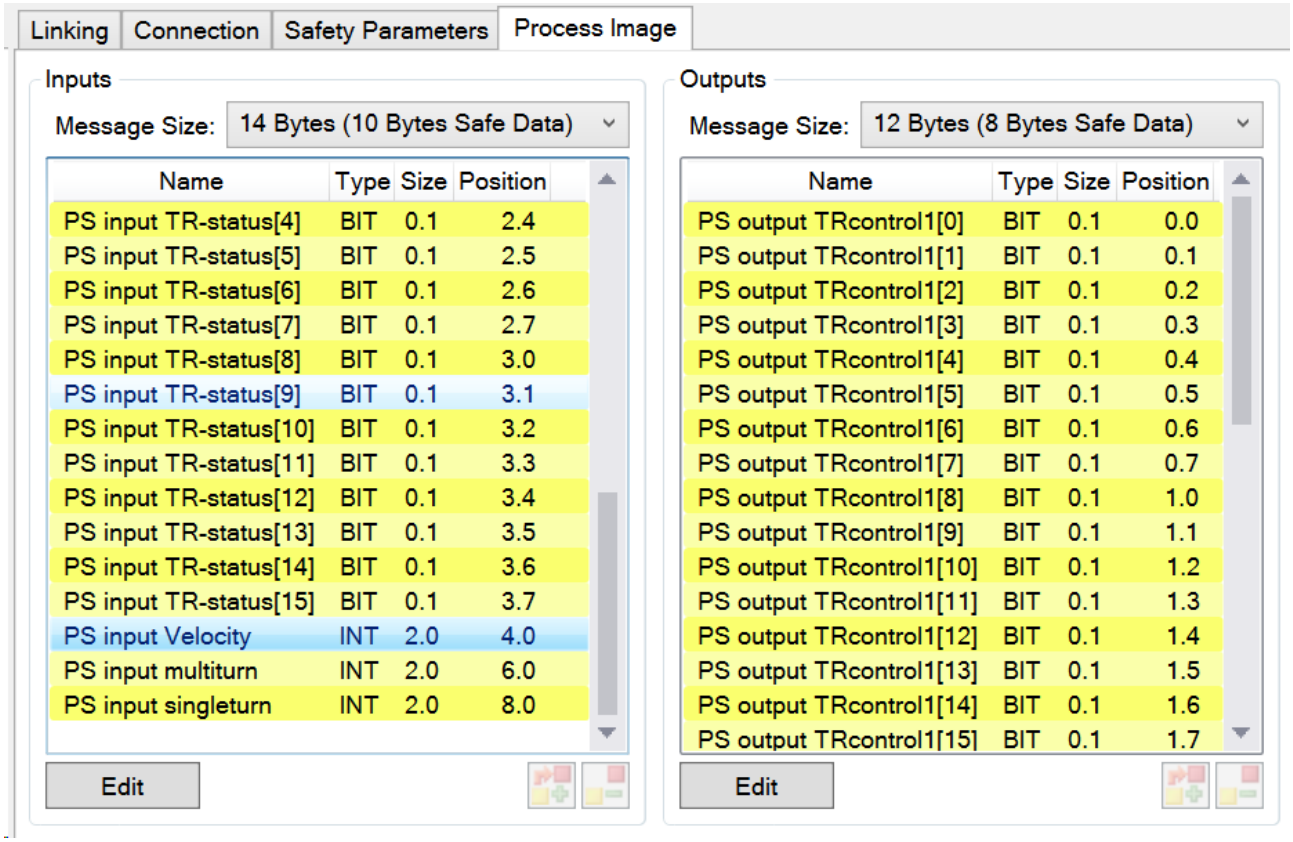
Auf dem Reiter *Linking* muss der Linking Mode auf *Automatic* eingestellt werden, damit über den Button *Map to Physical Device* der hier betrachtete TR Encoder ausgewählt werden kann.



Neben dem Mapping zum physikalischen Device muss auf dem Reiter *Linking* auch die sichere Adresse des Gebers eingetragen werden (in diesem Beispiel 13).



Wurden alle Einstellungen korrekt vorgenommen, kann auf dem Reiter *Process Image* das sichere Prozessabbild des Encoders eingesehen werden (mit dem in diesem Beispiel relevanten Eintrag *Velocity*).



Der Reiter *Safety Parameters* stellt die Parameter für die PROFIsafe-Master-Verbindung zur Verfügung.

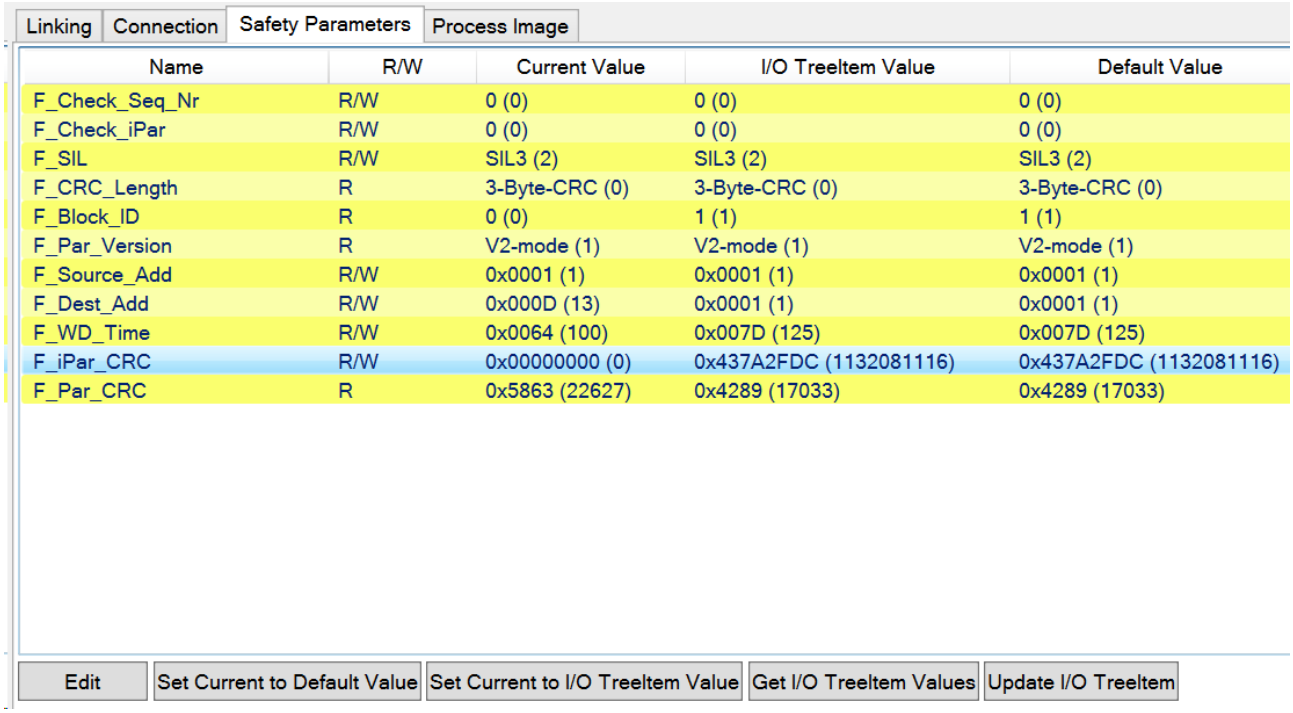


Abb. 1: Safety Parameter Encoder

Hier müssen alle Parameter für die PROFIsafe-Verbindung korrekt eingestellt werden. Darunter zählen unter anderem die beiden Adressen F_Source_Add (Zielsystem) und F_Dest_Add (sichere Adresse PROFIsafe-Gerät). Darüber hinaus muss die CRC der *iParameter* konfiguriert werden. Diese kann der zusätzlichen Applikation zur Konfiguration des Encoders entnommen werden (siehe Abschnitt *Konfiguration Encoder*)

Die Parameter müssen im Falle eines PROFIsafe-Geräts sowohl innerhalb des Alias Devices als auch direkt für das Device in der I/O-Konfiguration vorgenommen werden. Das Auslesen der Daten aus dem I/O-Device und das Übertragen an das I/O-Device kann über die entsprechenden Schaltflächen auf dem Reiter *Safety Parameters* angestoßen werden. Beide Daten müssen übereinstimmen, damit eine PROFIsafe-Verbindung erfolgreich aufgebaut werden kann.

Parameter	Beschreibung
F_Check_Seq_Nr	Einstellung (0/1), ob die Sequenz-Nummer der Verbindung geprüft werden soll.
F_Check_iPar	Einstellung (0/1), ob die Parametrierung über einen iPar Server erfolgt.
F_SIL	Auswahl des erforderlichen SIL Levels (SIL1, SIL2, SIL3, NoSIL)
F_CRC_Length	Anzeige der CRC - Länge
F_Block_ID	immer 0
F_Par_Version	Verwendete Version PROFIsafe (typischerweise V2-Mode)
F_Source_Add	Einstellung der PROFIsafe-Source-Adresse
F_Dest_Add	Einstellung der PROFIsafe-Ziel-Adresse
F_WD_Time	Einstellung der Watchdogzeit
F_iPar_CRC	i-Parameter für den PROFIsafe Slave
F_Par_CRC	Berechnete CRC über die gesamten Parameter

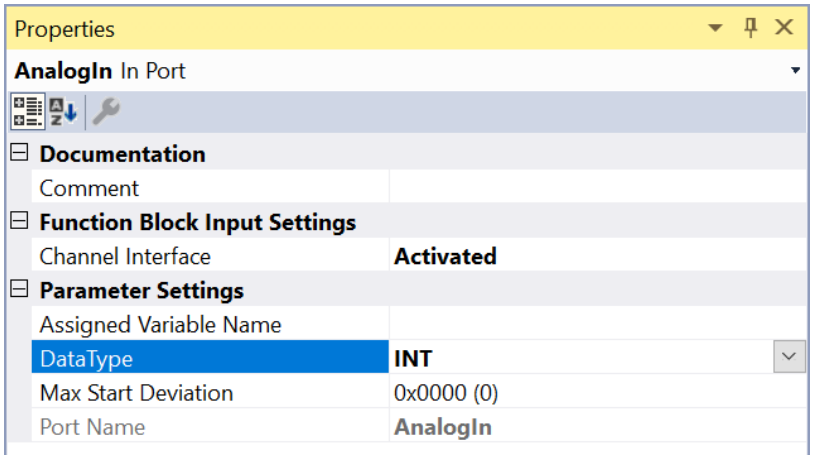
Nach Fertigstellung der Konfiguration der Parameter müssen diese durch Klick auf den Button *Update IO TreeItem* final an die I/O-Konfiguration übertragen werden.

Nach Beendigung der Konfiguration der Verbindungen kann mit der Implementierung der eigentlichen Sicherheitsfunktion fortgefahren werden.

10.1.2.4 Implementierung TwinCAT Safety Projekt

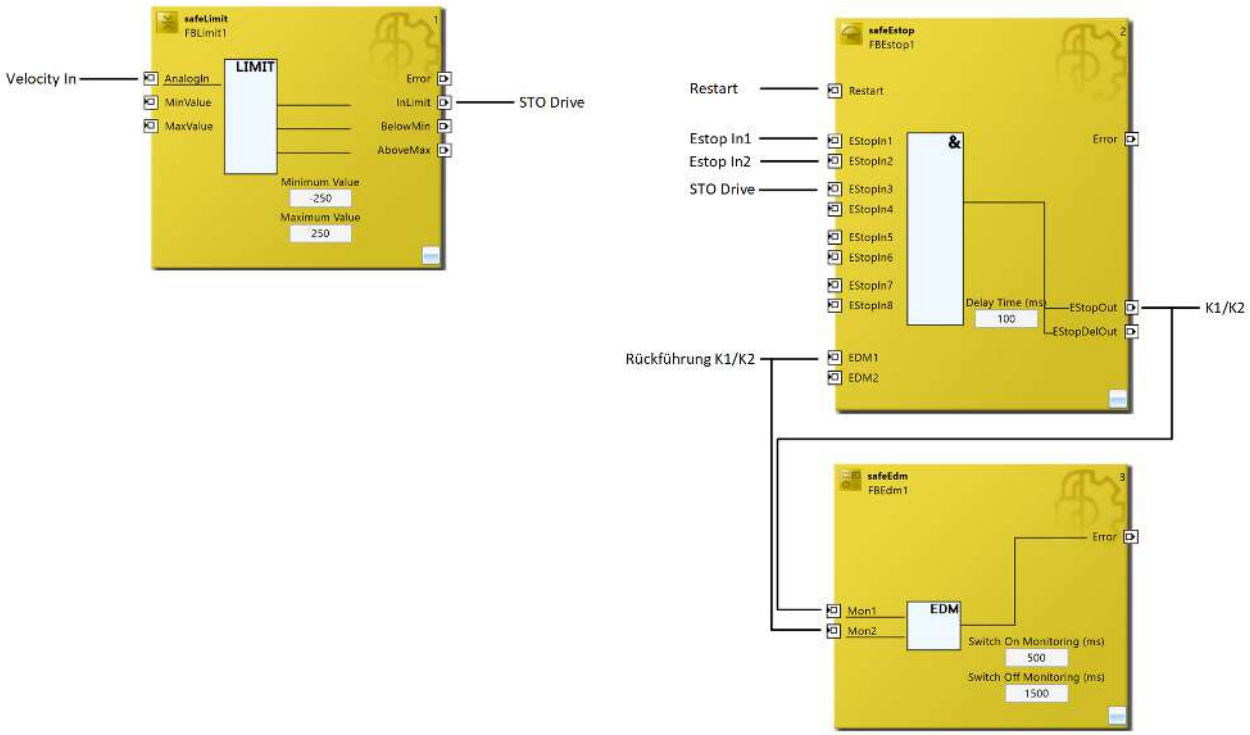
Im Rahmen der in diesem Beispiel betrachteten Sicherheitsfunktion zur Überwachung der Geschwindigkeit eines Antriebs wird der über PROFIsafe empfangene sichere Geschwindigkeitswert genutzt, um diesen gegen einen vorgegebenen Grenzwert zu prüfen und bei Überschreitung dieses Grenzwertes adäquat zu reagieren.

Zur Überprüfung des Geschwindigkeitswertes wird ein Funktionsblock *safeLimit* genutzt. Bei dem Geschwindigkeitswert, welcher über PROFIsafe empfangen wird, handelt es sich um einen 16 Bit Integerwert (siehe Reiter *Process Image* des *Alias Devices* für die PROFIsafe-Verbindung). Entsprechend muss für den eingefügten Funktionsblock safeLimit der Datentyp des Eingangs *AnalogIn* auf den Typ *INT* konfiguriert werden.



Anschließend kann der Eingang mit dem Signal *Velocity* der PROFIsafe-Verbindung verknüpft werden.

Das aus dem Funktionsblock safeLimit resultiertende Signal *InLimit* gibt an, ob die Geschwindigkeit unterhalb der konfigurierten Maximalgrenze liegt. Es kann weiter genutzt werden, um mit einem Funktionsblock *safeEstop* zum Beispiel einen evtl. vorliegenden Notausschalter zusätzlich auszuwerten.



Wie die Abbildung zeigt werden über den Ausgang *EstopOut* des Funktionsblocks *safeEstop* die beiden Schütze *K1* und *K2* geschaltet, welche wiederum die Sicherheitsfunktion *STO* des Antriebs ansteuern. Die Rückführung der Schütze wird als *EDM*-Eingang des Funktionsblocks safeEstop genutzt.

Zusätzlich zu den bereits beschriebenen Funktionsblöcken wird ein Funktionsblock *safeEdm* genutzt, um das korrekte Verhalten der Schütze K1 und K2 zu prüfen. Hier werden entsprechend der verwendeten Schütze die Zeiten für die An- und Abschaltüberprüfung konfiguriert.

10.1.3 Parameter der sicheren Ausgangsklemme

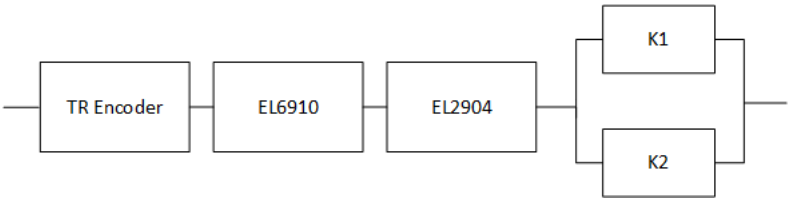
EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

10.1.4 Blockbildung und Safety-Loops

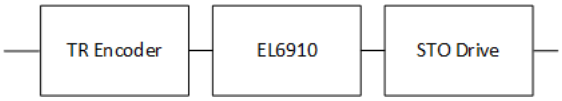
10.1.4.1 Sicherheitsfunktion 1 (ohne Antrieb)

Sicherheitsfunktion 1 betrachtet für das bisher beschriebene Anwendungsbeispiel den Safety Loop ausgehend vom TR Encoder bis hin zu den Schützen K1/K2. Die nachgeschalteten STO-Eingänge werden in dieser Sicherheitsfunktion nicht betrachtet.



10.1.4.2 Sicherheitsfunktion 2 (mit Antrieb)

Sicherheitsfunktion 2 betrachtet für das bisher beschriebene Anwendungsbeispiel den Safety Loop ausgehend vom TR Encoder. Die STO-Funktionalität wird über eine sichere Kommunikation angesteuert. Dafür wird im Rahmen der Berechnung ein Antrieb mit entsprechenden sicherheitstechnischen Kennwerten angenommen.



10.1.5 Berechnung Sicherheitsfunktion 1 (ohne Antrieb)

10.1.5.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
TR Encoder[1)] – PFH_D	1,46E-09
EL2904 – PFH_D	1,25E-09
EL6910 – PFH_D	1,79E-09
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

[1)] Bitte beachten Sie die Informationen der aktuellen Anwenderdokumentation

10.1.5.2 Diagnostic Coverage DC

Komponente	Wert
TR Encoder[1)]	DC_{avg}=95%
K1/K2 mit EDM-Überwachung (Betätigung 1/Woche und Auswertung aller steigenden und fallenden Flanken mit zeitlicher Überwachung) mit Testung der einzelnen Kanäle	DC_{avg}=99%

[1)] Bitte beachten Sie die Informationen der aktuellen Anwenderdokumentation

10.1.5.3 Berechnung Sicherheitsfunktion 1

Zur Verdeutlichung wird der Sicherheitskennwert sowohl nach EN 62061 als auch nach EN ISO 13849-1 berechnet. In der Praxis ist die Berechnung nach einer Norm ausreichend.

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

ergibt sich für

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

Eingesetzt ergibt das:

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

K1/K2: Betätigung 1/Woche und direktes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält Tabellen (Tabelle F.1-Kriterien zur Bestimmung des CCF und Tabelle F.2-Abschätzung des CCF-Faktors(β)), mit der dieser β–Faktor genau bestimmt werden kann. Für das Ausgangssubsystem kann bei entsprechender Bearbeitung der Tabelle zur Berechnung des β-Faktors ein Wert von schätzungsweise 2% erreicht werden. In der folgenden Berechnung wird der Worst-Case mit 10% angenommen.

Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1

$$PFH_{ges} = PFH_{(Encoder)} + PFH_{(EL6910)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Da die Anteile $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

$$PFH_{ges} = 1{,}46E - 09 + 1{,}79E - 09 + 1{,}25E - 09 + 10\% * \frac{1{,}94E - 09 + 1{,}94E - 09}{2}$$

$$PFH_{ges} = 4{,}69E - 09$$

Der $MTTF_D$-Wert nach EN 13849 für Sicherheitsfunktion 1 berechnet sich mit:

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

zu:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTFD_{(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

mit:

Sind für EL2904 und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

$$MTTF_{d(x)} = \frac{(1 - DC(x))}{PFH(x)}$$

Somit:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{15{,}68E-06\frac{1}{y}} = 637y$$

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

Der Wert des Encoders kann der aktuellen Anwenderdokumentation entnommen werden:

$$MTTF_{d(Encoder)} = 421y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{421y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y}} = 198y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{95\%}{421} + \frac{99\%}{637} + \frac{99\%}{913} + \frac{99\%}{593607} + \frac{99\%}{593607}}{\frac{1}{421} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = 97{,}12\%$$

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	B	1	2	2	3	3	4
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

10.1.6 Berechnung Sicherheitsfunktion 2 (mit Antrieb)

10.1.6.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
TR Encoder[1)] – PFH_D	1,46E-09
EL2904 – PFH_D	1,25E-09
EL6910 – PFH_D	1,79E-09
AX8xxx-x1xx – PFH_D	3,04E-09
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

[1)] Bitte beachten Sie die Informationen der aktuellen Anwenderdokumentation

10.1.6.2 Diagnostic Coverage DC

Komponente	Wert
TR Encoder[1)]	DC_{avg}=95%
AX8xxx-x1xx STO-Funktion	DC_{avg}>99%

[1)] Bitte beachten Sie die Informationen der aktuellen Anwenderdokumentation

10.1.6.3 Berechnung Sicherheitsfunktion 2

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 2:

$$PFH_{ges} = PFH_{(Encoder)} + PFH_{(EL6910)} + PFH_{(AX8xxx-x1xx)}$$

$$PFH_{ges} = 1,46E-09 + 1,79E-09 + 3,04E-09$$
$$PFH_{ges} = 6,29E-09$$

Der $MTTF_D$-Wert nach EN 13849 für Sicherheitsfunktion 1 berechnet sich mit:

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

zu:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTFD_{(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}$$

mit:

Sind für AX8xxx-x1xx und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

$$MTTF_{d(x)} = \frac{(1-DC(x))}{PFH(x)}$$

Somit:

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(AX8xxx-x1xx)} = \frac{(1-DC_{(AX8xxx-x1xx)})}{PFH_{D(AX8xxx-x1xx)}} = \frac{(1-0,99)}{3,04E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{2,66E-05\frac{1}{y}} = 375y$$

Abb. 2:

Der Wert des Encoders kann der aktuellen Anwenderdokumentation entnommen werden:

$$MTTF_{d(Encoder)} = 421y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{421y} + \frac{1}{637y} + \frac{1}{375y}} = 151y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(AX8xxx-x1xx)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}}$$

$$DC_{avg} = \frac{\frac{95\%}{421} + \frac{99\%}{637} + \frac{99\%}{375}}{\frac{1}{421} + \frac{1}{637} + \frac{1}{375}} = 97{,}56\%$$

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	**99 % ≤ DC**

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / **$MTTF_D$**	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

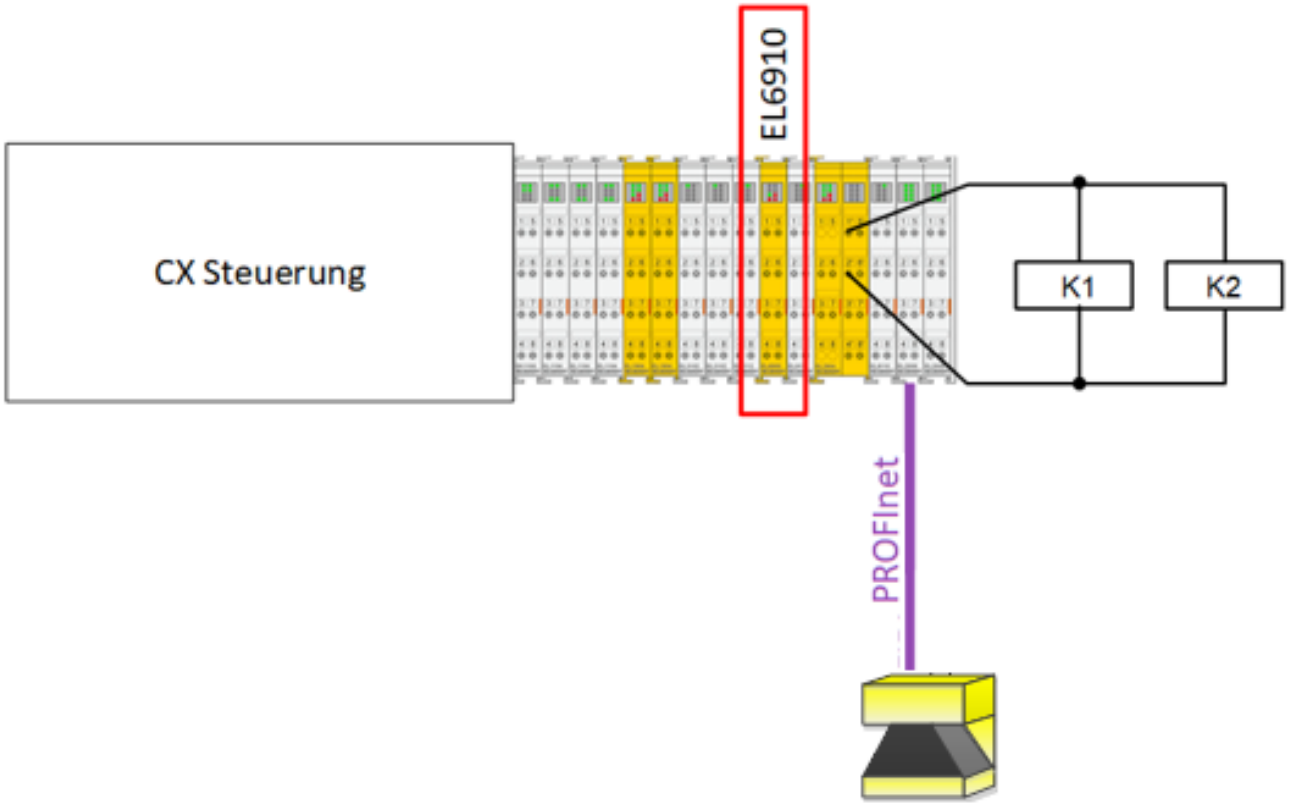
10.2 Sichere Bereichsüberwachung mit PROFIsafe-Laserscanner (Kategorie 3, PL d)

Der Gefahrenbereich einer Maschine soll mittels Sicherheits-Laserscanner überwacht werden. Diese Gefahr kann über zwei Schütze abgeschaltet werden. Die Schütze werden an einem Ausgang einer EL2904 angeschlossen. Zur sicheren Bereichsüberwachung wird ein Sicherheits-Laserscanner microScan3 der Firma SICK genutzt. Dieser ist für Anwendungen bis Performance Level d zertifiziert. Die relevanten Daten werden über das sicherheitsrelevante Protokoll PROFIsafe an die EL6910 als PROFIsafe-Master übertragen und dort mit Hilfe der verfügbaren vorzertifizierten Funktionsbausteine überwacht.

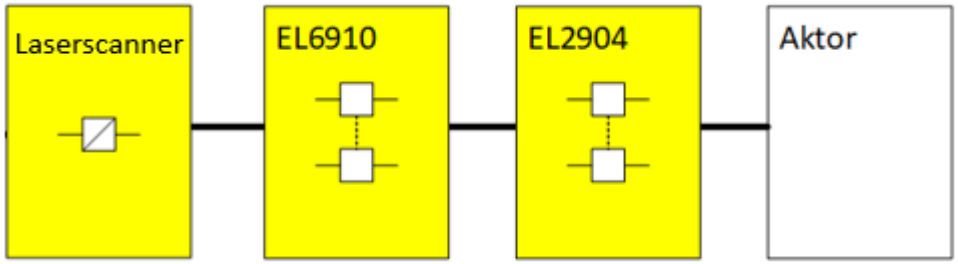
Wenn die beiden Abschaltpfade (2 Signale innerhalb des PROFIsafe-Protokolls) des eingestellten Überwachungsfalles logisch 1 melden, dann ist das Schutzfeld frei und die zwei Schütze werden eingeschaltet. Ist das Schutzfeld belegt, melden die beiden Abschaltpfade logisch 0 und die Schütze werden abgeschaltet. Die gesamte Auswertung wird in der sicherheitsgerichteten Logik EL6910 auf dem Sicherheitsniveau SIL3 / PL e durchgeführt.

Eine eventuell notwendige Wiederanlaufsperre kann über den Reset-Eingang des fbMon realisiert werden. Der Rückführkreis wird über einen sicheren Eingang eingelesen. Für diesen Eingang ist die Testung aktiv.

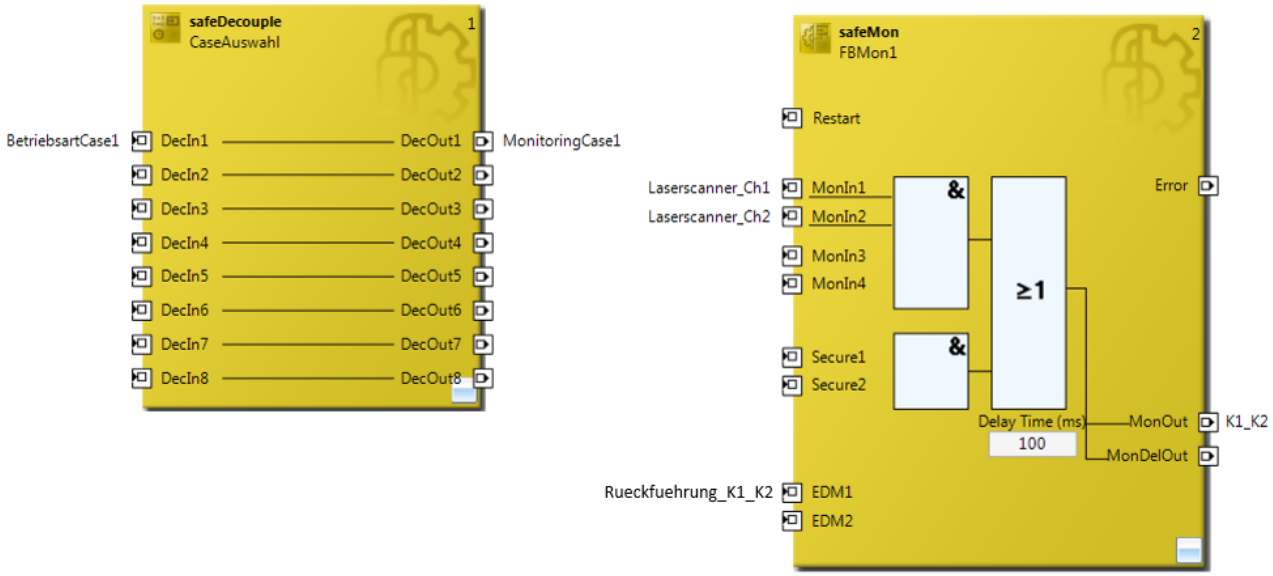
Aufbau



Strukturbild Aufbau



Logik



Korrekte Konfiguration Gesamtsystem

Bei der Übertragung von PROFIsafe innerhalb EtherCAT gibt es folgende Einschränkungen.

PROFIsafe-Telegramm nur über E-Bus und PROFINET/PROFIBUS

Die Verwendung von PROFIsafe ist es aufgrund der PROFIsafe Policy nur über die Feldbusse PROFIBUS und PROFINET oder über einen Rückwandbus, hier z.B. der E-Bus zulässig. Eine Nutzung von PROFIsafe über andere Feldbusse ist aus patentrechtlichen Gründen nicht zulässig. Dies muss durch Verwendung der Segment-Abschluss-Klemme EL9930 sichergestellt werden.

Folgende Patente der Siemens AG sind entsprechend des PROFIsafe Profils relevant:
- EP1267270-A2 Method for data transfer
- WO00/045562-A1 Method and device for determining the reliability of data carriers
- WO99/049373-A1 Shortened data message of an automation system
- EP1686732 Method and system for transmitting protocol data units
- EP1802019 Identification of errors in data transmission
- EP1921525-A1 Method for operation of a safety-related system
- EP13172092.2 Method and system for detection of errors

Je nach Architektur der Anwendung müssen also entsprechende Maßnahmen getroffen werden. Details zur korrekten Konfiguration des Gesamtsystems bezüglich PROFIsafe sind in den Dokumentationen der EL6910 und EL9930 zu finden.

Einsatz externer sicherer Sensoren

Bei dem Einsatz eines externen sicheren Sensors sind weitere Anforderungen zu beachten.

⚠ VORSICHT

Einsatz externer sicherer Sensoren

Beim Einsatz eines externen sicheren Sensors ist stets die aktuelle Version der Dokumentation zu beachten. Hier finden sich alle Anforderungen bezüglich Montage, Betrieb, Instandsetzung, welche zwingend erfüllt werden müssen, damit der Sensor in einer sicherheitsrelevanten Applikation korrekt genutzt werden kann.

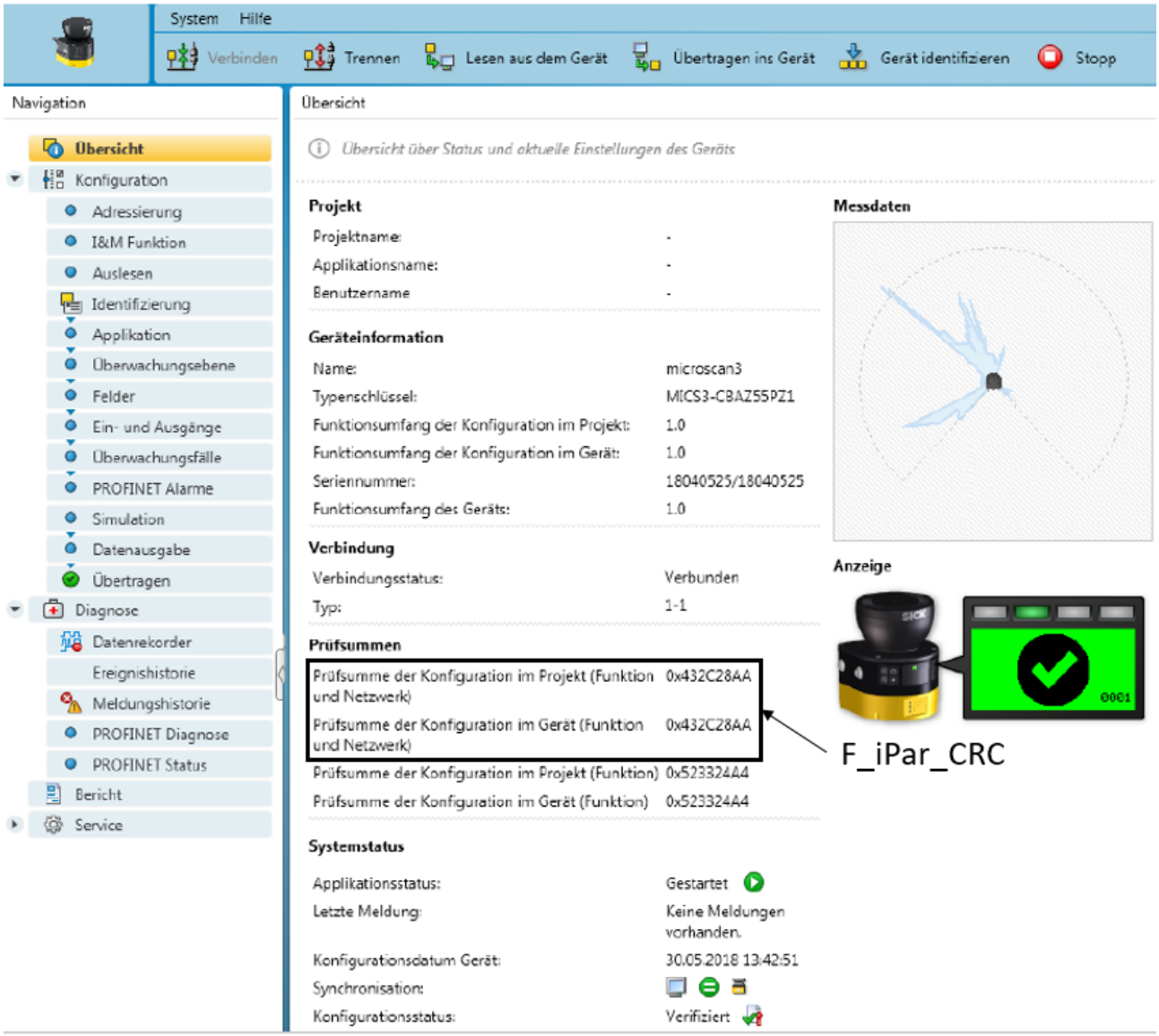
10.2.1 Konfiguration in Engineeringumgebung

Im Rahmen des vorliegenden Applikationsbeispiels wird neben der Anbindung von TwinSAFE-Komponenten die zusätzliche Anbindung eines Sicherheits- Laserscanners über PROFIsafe/PROFInet betrachtet. Im Folgenden werden im Detail alle nötigen Konfigurationsschritte zur Realisierung beschrieben.

Für die Konfiguration des Sicherheits-Laserscanners ist eine zusätzliche Anwendung erforderlich. Damit wird der Funktionsumfang des Sicherheits-Laserscanners, die Kommunikationseinstellungen im PROFInet/ PROFIsafe und die CRC Prüfsumme der iParameter ermittelt, welche letztlich innerhalb TwinCAT zusätzlich konfiguriert werden muss.

10.2.1.1 Konfiguration Sicherheits-Laserscanner

Zur Konfiguration des Sicherheits-Laserscanners ist eine zusätzliche Anwendung notwendig. Die aktuelle Version kann von der Webseite des Herstellers bezogen werden.

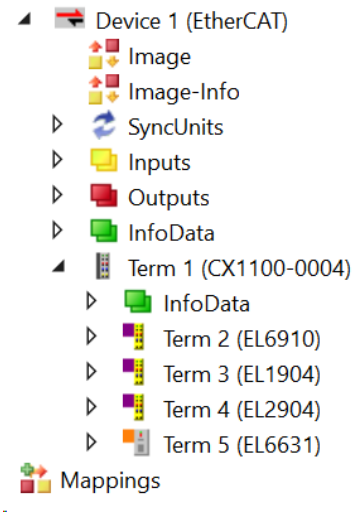


Hier müssen entsprechend der Applikation die notwendigen Funktionen und Parameter konfiguriert werden, damit die CRC Prüfsumme korrekt berechnet werden kann (im Bild **F_iPar_CRC**).

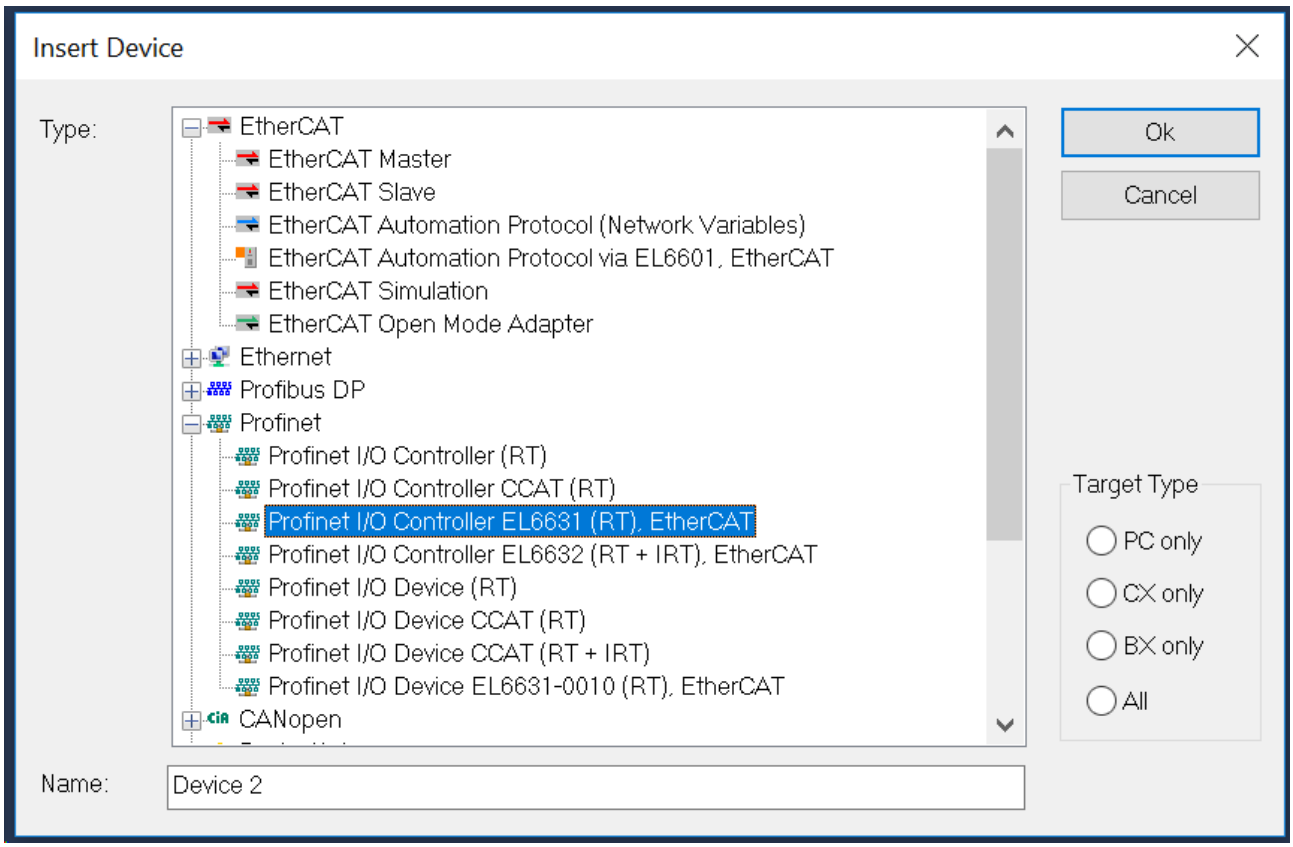
10.2.1.2 Konfiguration TwinCAT I/O

Die aktuelle GSDML-Datei des Sicherheits-Laserscanners muss vor Beginn der TwinCAT- Konfiguration in das Profinet- Geräteverzeichnis unter \TwinCAT\3.1\Config\Io\Profinet eingefügt werden.

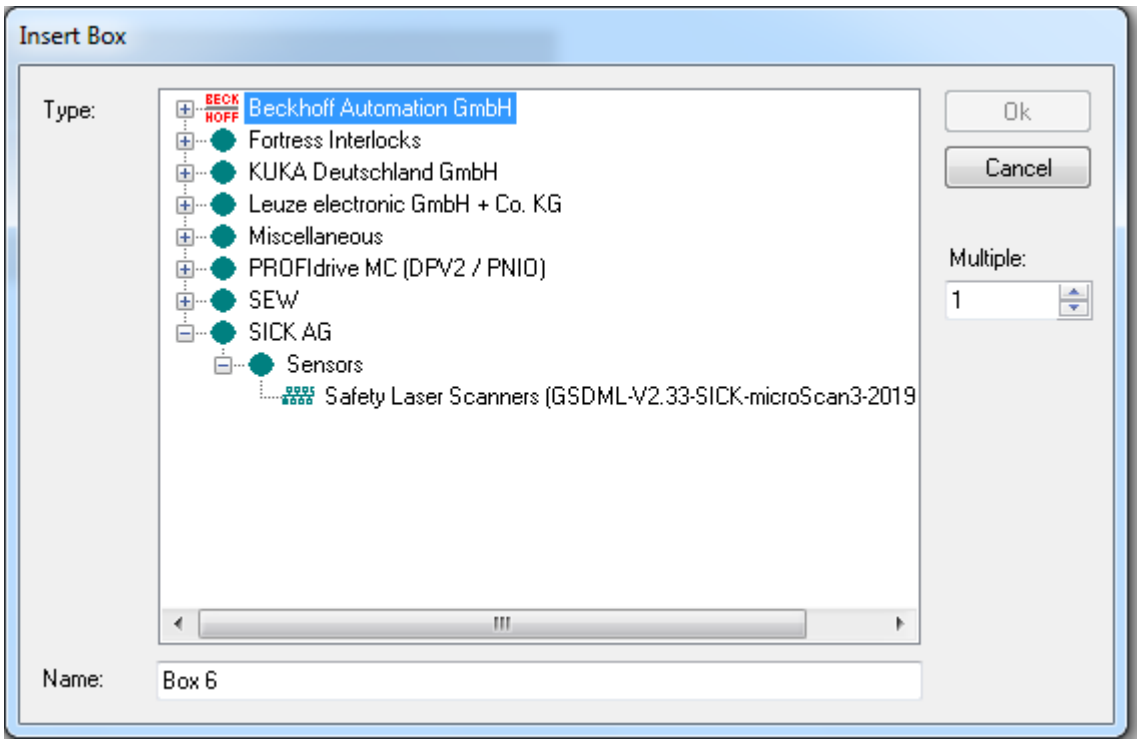
Im Anschluss wird ein neues TwinCAT Projekt angelegt und der EtherCAT-Strang konfiguriert.



Zusätzlich wird die Konfiguration des PROFInet-Strangs durch Hinzufügen eines PROFInet-I/O-Controllers erzeugt.



Analog zur Konfiguration des EtherCAT-Strangs kann auch im Falle des PROFInet-Controllers ein automatischer Scan angestoßen oder die Konfiguration manuell erzeugt werden. So kann auch der Sick Laserscanner manuell hinzugefügt werden.



Für die erfolgreiche Nutzung des Sick Laserscanners über PROFIsafe sind folgende Informationen zu beachten.

⚠ VORSICHT

Datentyp WORD!

Bei Verwendung von WORD-Datentypen innerhalb des Prozessabbildes muss unter Umständen eine zusätzliche Konfiguration erfolgen.

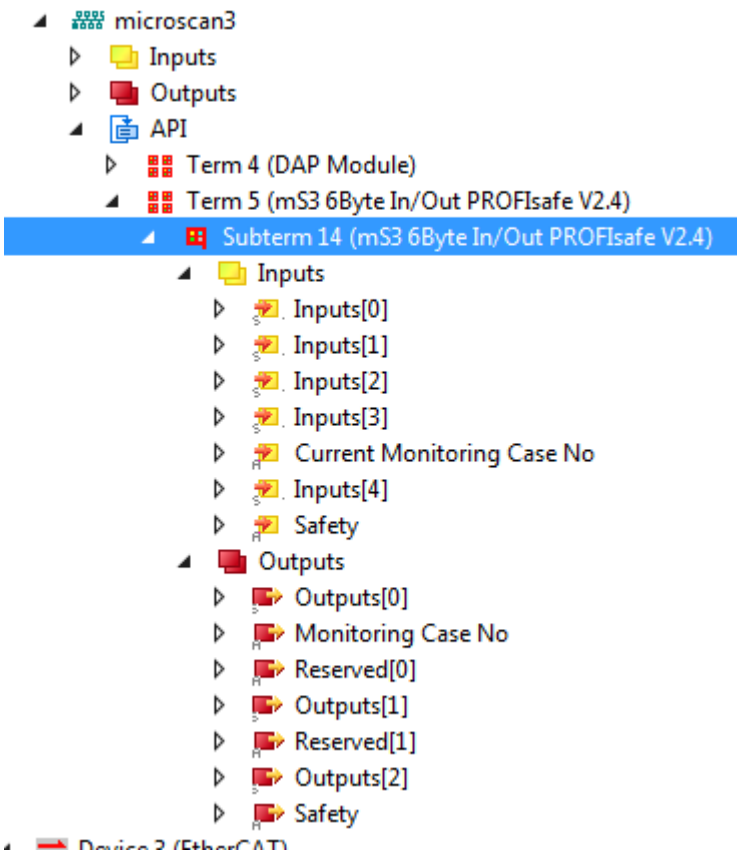
Wird innerhalb der Konfiguration keine EL9930 zur Begrenzung des PROFIsafe-Segments eingesetzt, so muss im Rahmen der I/O-Konfiguration des PROFIsafe-Gerätes für die im Prozessabbild enthaltenen Signale mit WORD-Datentyp des Tauschen des High und Low Byte-Anteiles konfiguriert werden. Dies erfolgt durch Auswahl der Checkbox *Tausche LOBYTE und HIBYTE* direkt auf den Datenwerten (unter dem Reiter *Flags*).

⚠ VORSICHT

iParameter

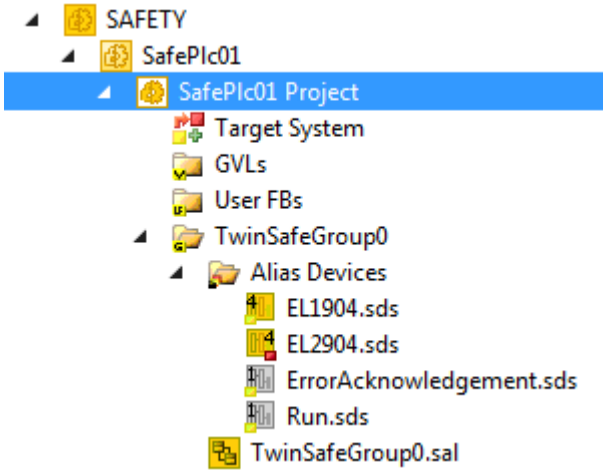
Auf dem PROFIsafe I/O-Gerät müssen die identischen iParameter wie auf dem *Alias Device* konfiguriert sein, damit die Kommunikation korrekt starten kann.

Anschließend kann mit der Konfiguration des Safety Projekts fortgefahren werden. Dabei wird an dieser Stelle von folgender Ausgangslage ausgegangen.

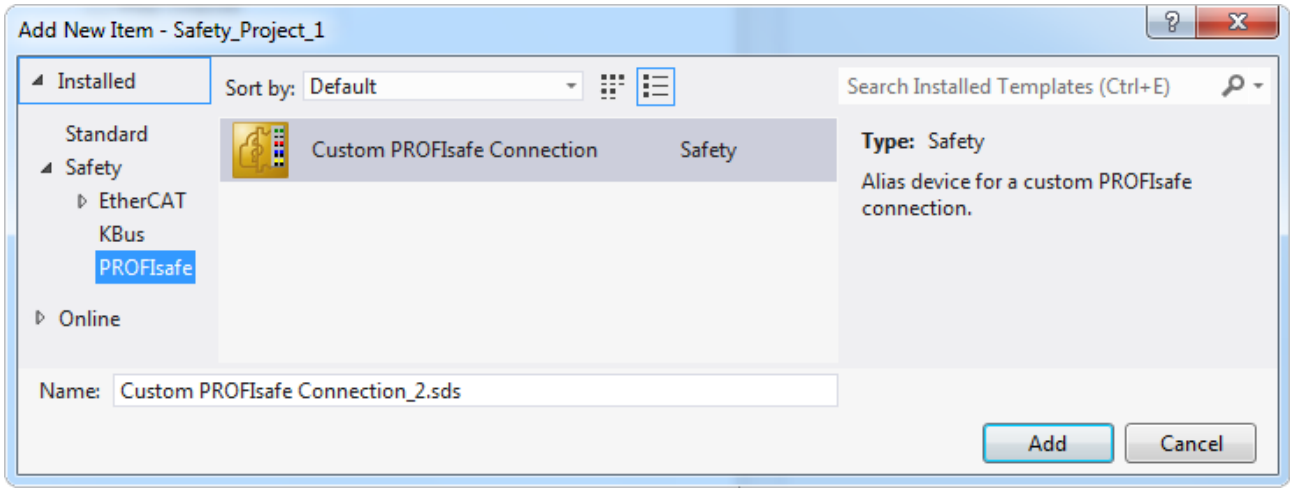


10.2.1.3 Konfiguration Verbindungen TwinCAT Safety Projekt

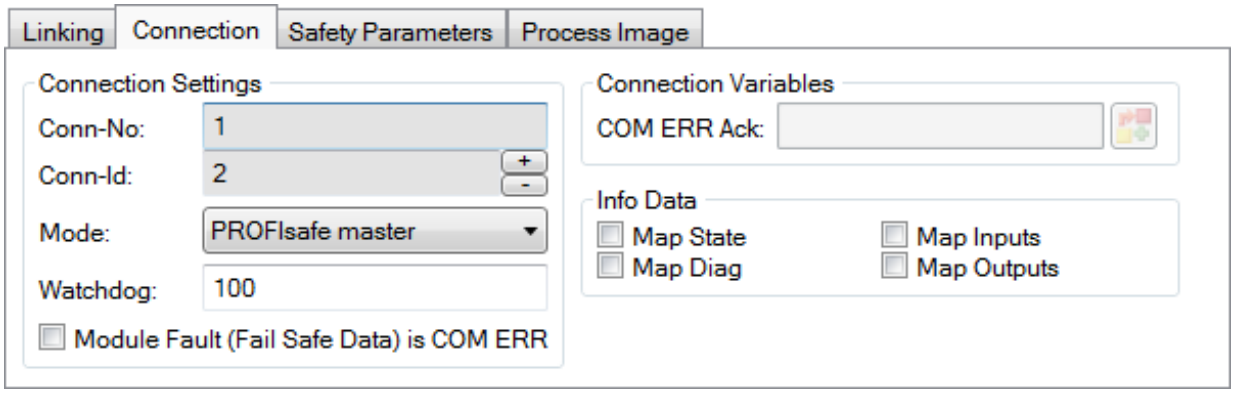
Vor der Konfiguration der PROFIsafe-Verbindung wird zunächst ein Safety Projekt angelegt und die benötigten Alias Devices für die verfügbaren EtherCAT-Komponenten importiert. Zusätzlich wird das Zielsystem auf die EL6910 des EtherCAT-Strangs gemappt (über den Knoten *Target System*).



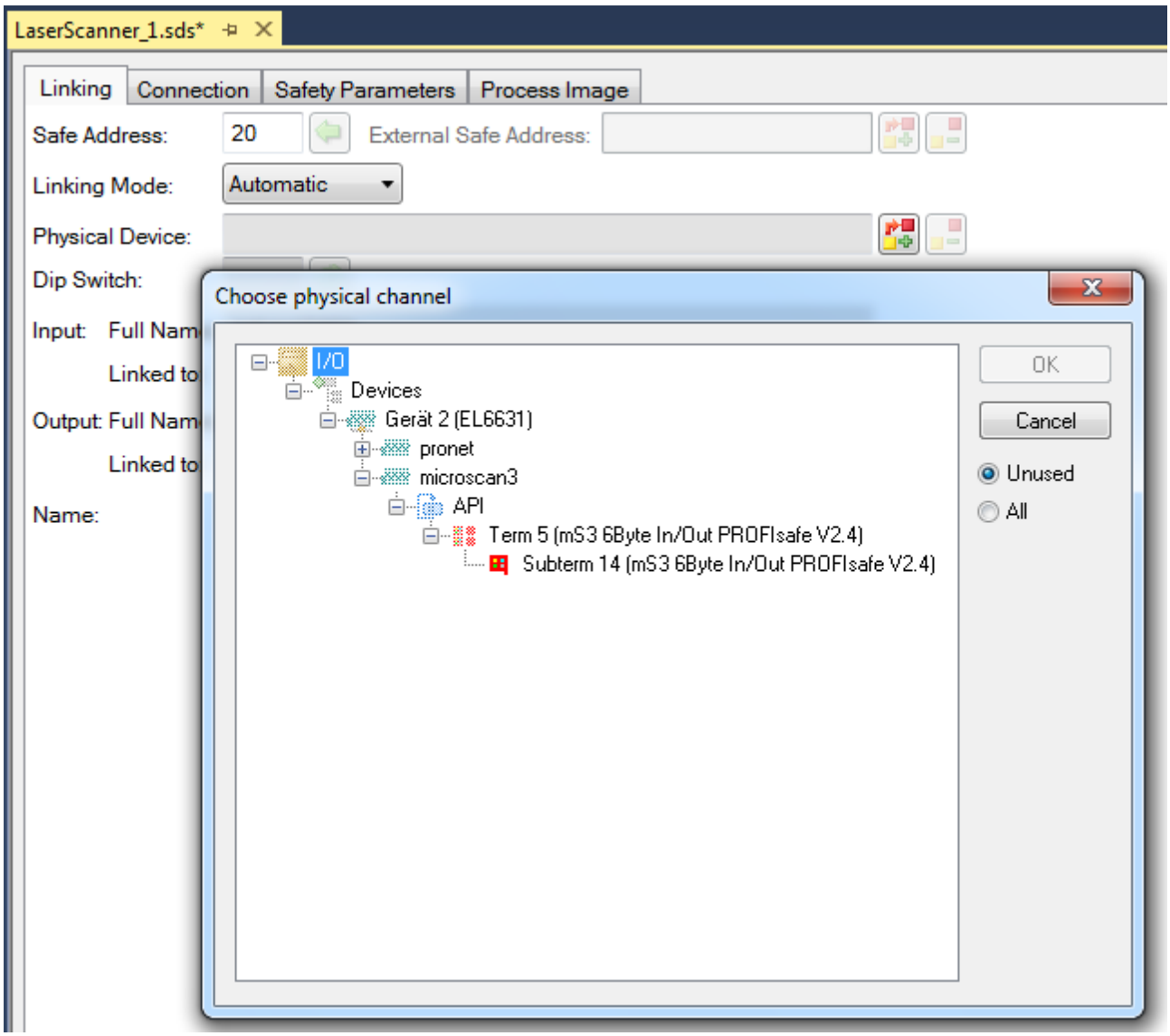
Anschließend kann mit der Konfiguration der PROFIsafe-Verbindung zum Sicherheits-Laserscanner fortgefahren werden. Diese Verbindung wird wie üblich über ein *Alias Device* realisiert. Über das Kontextmenu des Knotens *Alias Devices* und durch Auswahl von *Add* und *New item…* kann eine Custom PROFIsafe Connection angelegt werden.



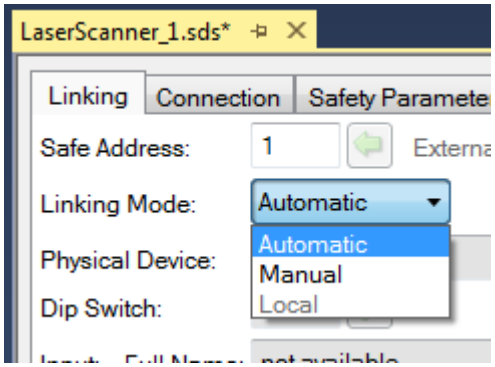
Nach dem Öffnen des Alias Devices muss zunächst über den Reiter *Connection* als Modus der Verbindung *PROFIsafe-Master* gewählt werden.



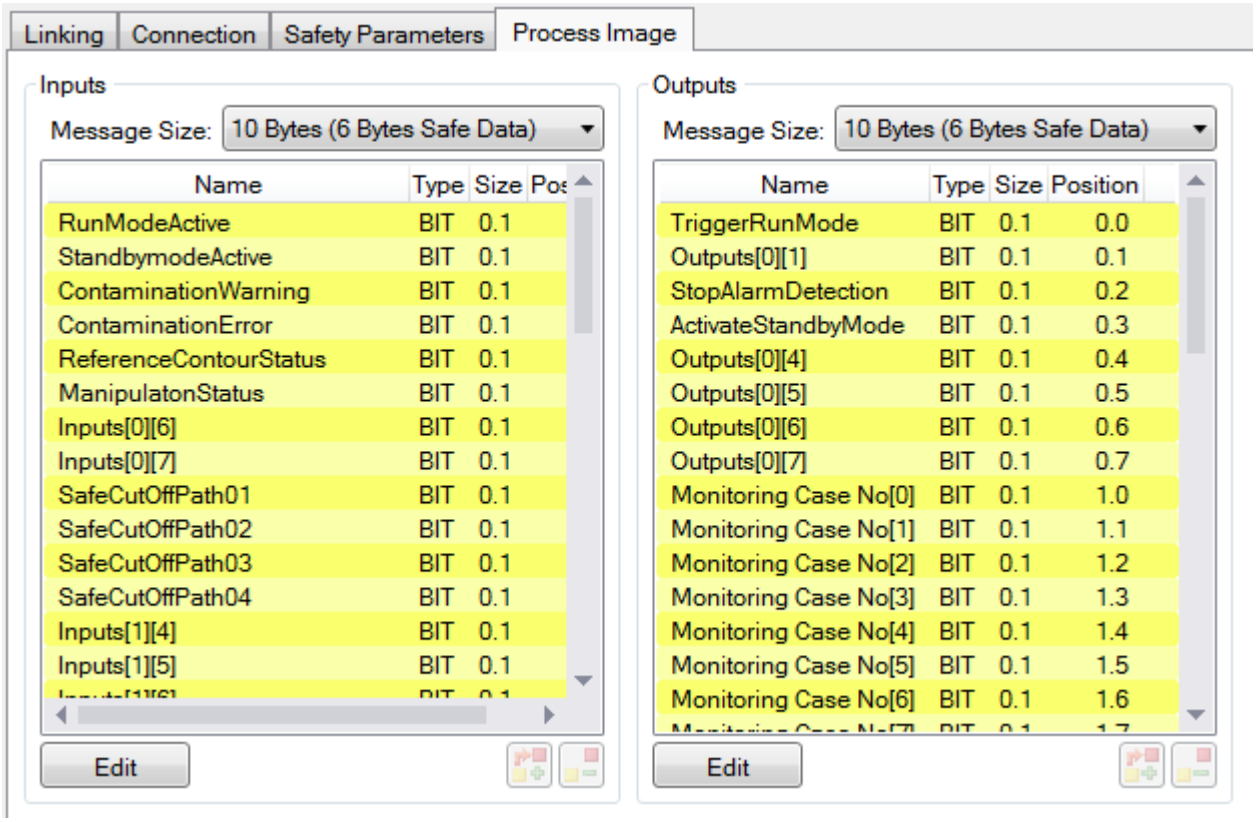
Auf dem Reiter *Linking* muss der Linking Mode auf *Automatic* eingestellt werden, damit über den Button *Map to Physical Device* der hier betrachtete Sick Sicherheits-Laserscanner ausgewählt werden kann.



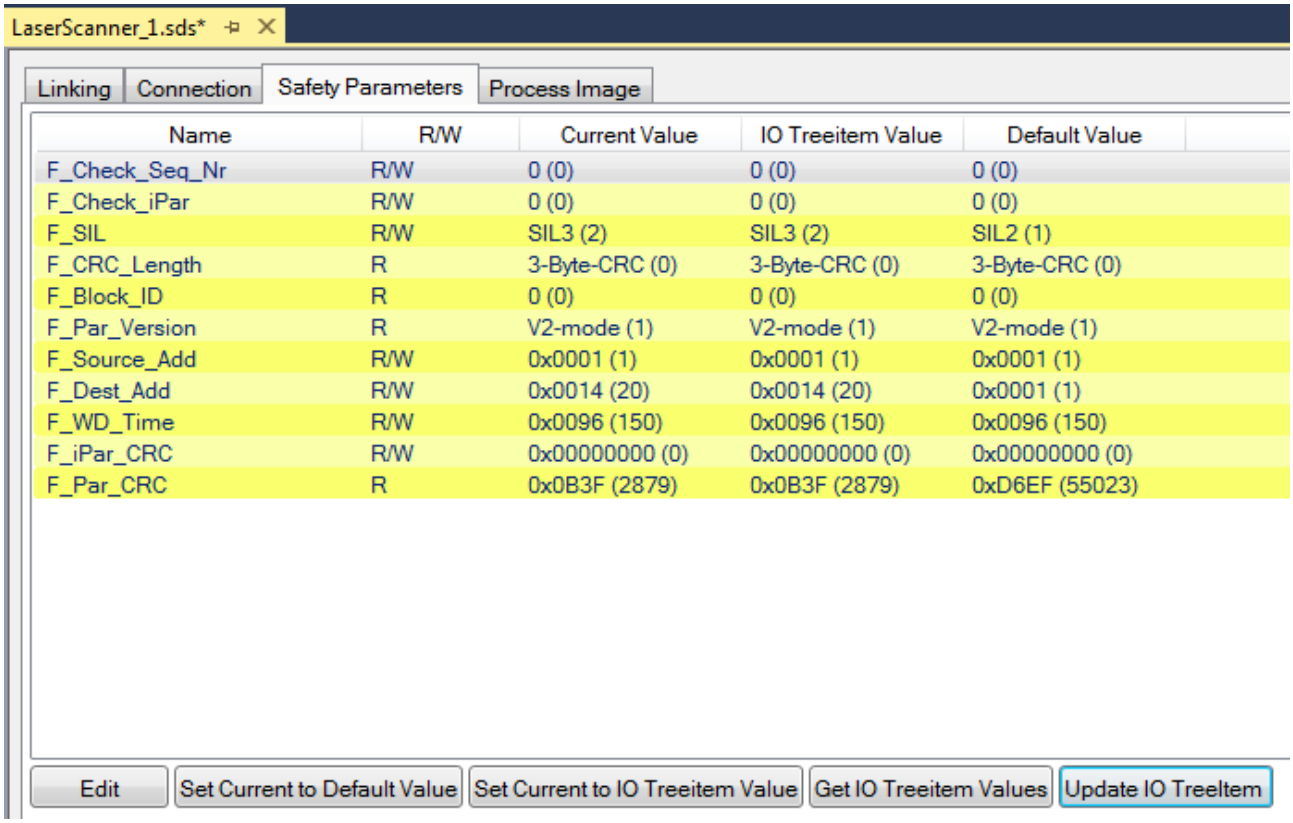
Neben dem Mapping zum physikalischen Device muss auf dem Reiter *Linking* auch die sichere Adresse des Sicherheits-Laserscanners eingetragen werden (in diesem Beispiel 20).



Wurden alle Einstellungen korrekt vorgenommen, kann auf dem Reiter *Process Image* das sichere Prozessabbild des Sicherheits-Laserscanners eingesehen werden. Anpassung der Namen können über den Button Edit vorgenommen werden. Die Belegung der Schnittstelle sowie die Beschreibung der einzelnen Signale müssen Sie der aktuellen Dokumentation des Herstellers entnehmen.



Der Reiter *Safety Parameters* stellt die Parameter für die PROFIsafe-Master-Verbindung zur Verfügung.



Hier müssen alle Parameter für die PROFIsafe-Verbindung korrekt eingestellt werden. Darunter zählen unter anderem die beiden Adressen F_Source_Add (Zielsystem) und F_Dest_Add (sichere Adresse PROFIsafe-Gerät). Darüber hinaus muss die CRC der *iParameter* konfiguriert werden. Diese kann der zusätzlichen Applikation zur Konfiguration des Sicherheits-Laserscanners entnommen werden (siehe Abschnitt *Konfiguration Encoder*).

Die Parameter müssen im Falle eines PROFIsafe-Geräts sowohl innerhalb des Alias Devices als auch direkt für das Device in der I/O-Konfiguration vorgenommen werden. Das Auslesen der Daten aus dem I/O-Device und das Übertragen an das I/O-Device kann über die entsprechenden Schaltflächen auf dem Reiter *Safety Parameters* angestoßen werden. Beide Daten müssen übereinstimmen, damit eine PROFIsafe-Verbindung erfolgreich aufgebaut werden kann.

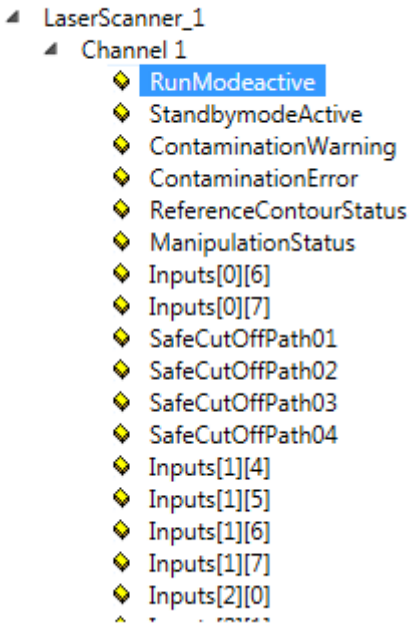
Parameter	Beschreibung
F_Check_Seq_Nr	Einstellung (0/1), ob die Sequenz-Nummer der Verbindung geprüft werden soll.
F_Check_iPar	Einstellung (0/1), ob die Parametrierung über einen iPar Server erfolgt.
F_SIL	Auswahl des erforderlichen SIL Levels (SIL1, SIL2, SIL3, NoSIL)
F_CRC_Length	Anzeige der CRC - Länge
F_Block_ID	immer 0
F_Par_Version	Verwendete Version PROFIsafe (typischerweise V2-Mode)
F_Source_Add	Einstellung der PROFIsafe-Source-Adresse
F_Dest_Add	Einstellung der PROFIsafe-Ziel-Adresse
F_WD_Time	Einstellung der Watchdogzeit
F_iPar_CRC	i-Parameter für den PROFIsafe Slave
F_Par_CRC	Berechnete CRC über die gesamten Parameter

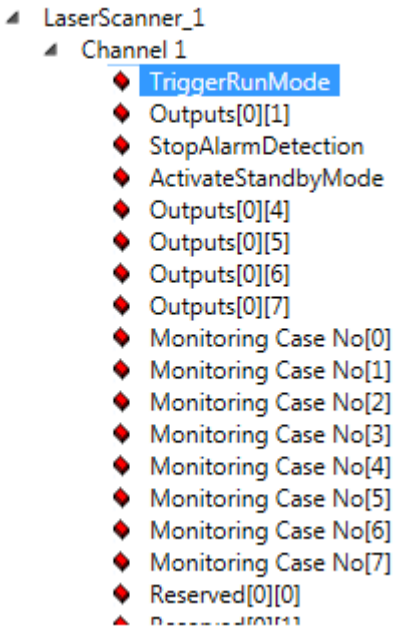
Nach Fertigstellung der Konfiguration der Parameter müssen diese durch Klick auf den Button *Update IO TreeItem* final an die I/O-Konfiguration übertragen werden.

Nach Beendigung der Konfiguration der Verbindungen kann mit der Implementierung der eigentlichen Sicherheitsfunktion fortgefahren werden.

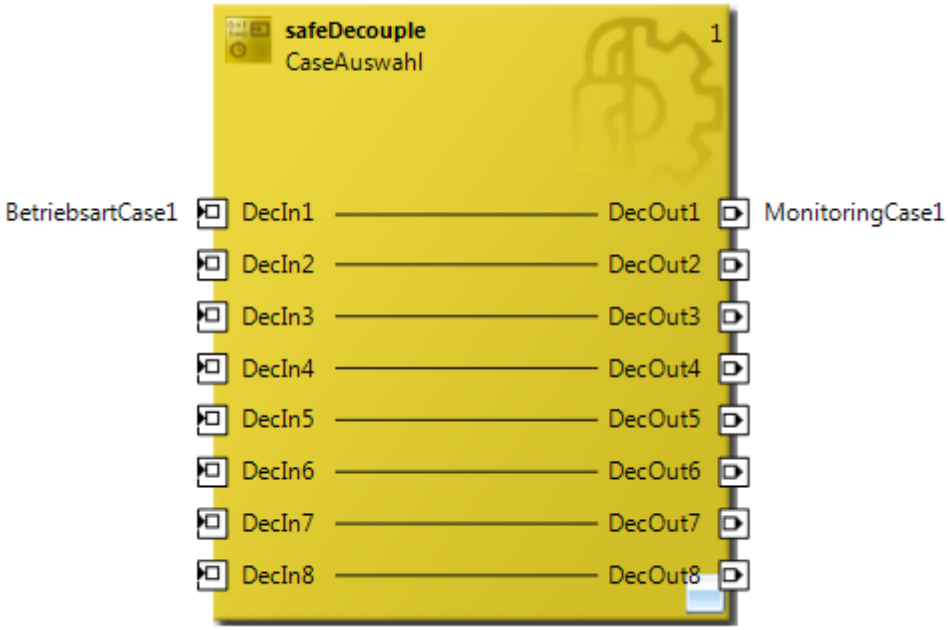
10.2.1.4 Implementierung TwinCAT Safety Projekt

Im Rahmen der in diesem Beispiel betrachteten Sicherheitsfunktion zur Bereichsüberwachung mittels Sicherheits-Laserscanner wird das über PROFIsafe empfangene sichere Prozessabbild genutzt. Die zwingend notwendig auszuwertenden Eingänge sowie zu beschaltenden Ausgänge ergeben sich aus der Konfiguration des Sicherheits-Laserscanners.

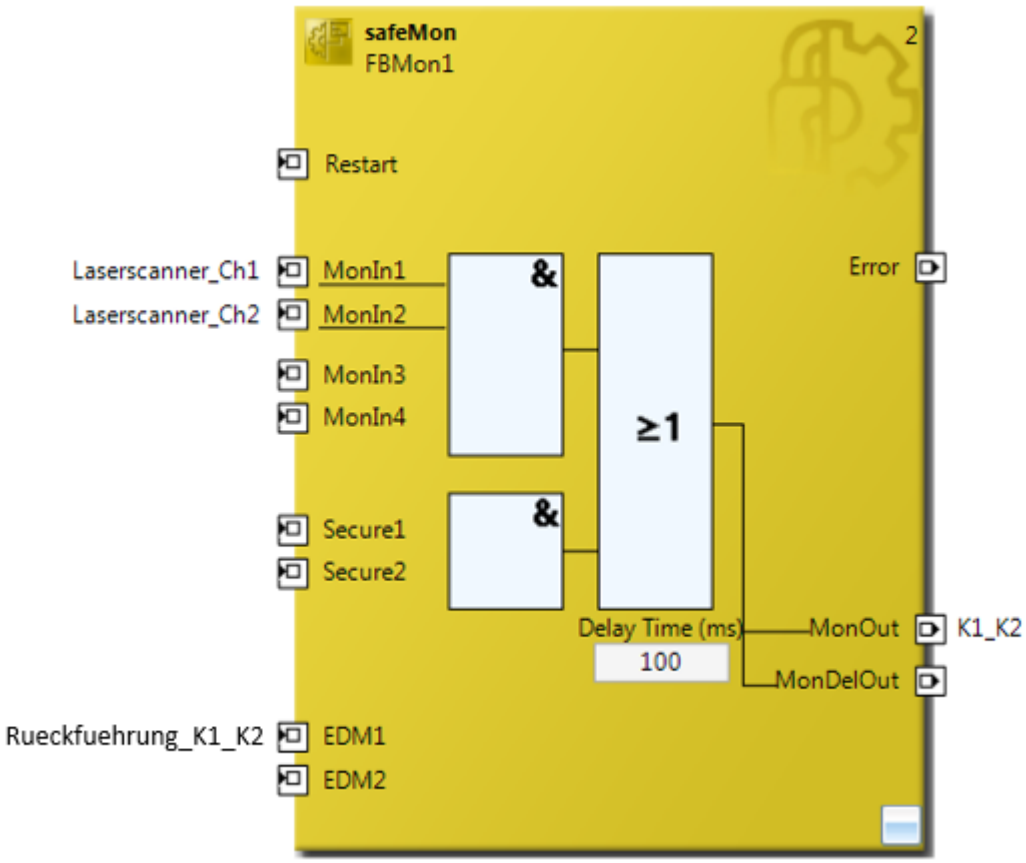




In diesem Beispiel wird ohne weitere Bedingung der Überwachungsfall 1 eingeschaltet mittels Funktionsblock *safeDecoupler*.



Der Sicherheits-Laserscanner überwacht den im Gerät parametrierten Gefahrenbereich und sendet in den Signalen Abschaltpfade 01 und 02 das Ergebnis der Überwachung. Diese beiden Signale werden mittels Funktionsblock *safeMon* ausgewertet. Die Abschaltpfade sind logisch 1, wenn der Gefahrenbereich frei und sicherheitsgerichtet überwacht wird.



Wie die Abbildung zeigt werden bei logisch 1 an den Eingängen *MonIn1* und *MonIn2* und *EDM1* über den Ausgang *MonOut* des Funktionsblocks *safeMon* die beiden Schütze *K1* und *K2* geschaltet, welche die Sicherheitsfunktion ausführen. Die Rückführung der Schütze wird als *EDM1*-Eingang des Funktionsblocks *safeMon* genutzt.

Eine eventuell notwendige Wiederanlaufsperre kann über den Reset- Eingang des Funktionsblocks *safeMon* realisiert werden.

10.2.2 Parameter der sicheren Ein- und Ausgangsklemme

EL2904

Parameter	Wert
Strommessung aktiv	Ja
Testpulse des Ausgangs aktiv	Ja

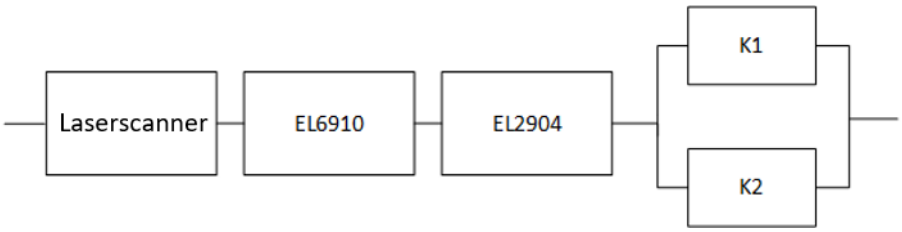
EL1904

Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

10.2.3 Blockbildung und Safety-Loops

10.2.3.1 Sicherheitsfunktion 1

Sicherheitsfunktion 1 betrachtet für das bisher beschriebene Anwendungsbeispiel den Safety Loop ausgehend vom Sicherheits-Laserscanner bis hin zu den Schützen K1/K2.



10.2.4 Berechnung Sicherheitsfunktion 1

10.2.4.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
Laserscanner[1] – PFH_D, SIL, Kat, PL	8E-08, SIL 2, Kat. 3, PL d
EL2904 – PFH_D	1,25E-09
EL6910 – PFH_D	1,79E-09
K1 – $B10_D$	1.300.000
K2 – $B10_D$	1.300.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10 (6x pro Stunde)
Lebenszeit (T1)	20Jahre = 175200 Stunden

[1] Bitte beachten Sie die Informationen der aktuellen Anwenderdokumentation

10.2.4.2 Diagnostic Coverage DC

Komponente	Wert
Laserscanner mit Testung (durch Scanner)[1]	DC_{avg}=90%
K1/K2 mit EDM-Überwachung mit Testung der einzelnen Kanäle	DC_{avg}=99%

[1] Bitte beachten Sie die Informationen der aktuellen Anwenderdokumentation

10.2.4.3 Berechnung Sicherheitsfunktion 1

Zur Verdeutlichung wird der Sicherheitskennwert sowohl nach EN 62061 als auch nach EN ISO 13849-1 berechnet. In der Praxis ist die Berechnung nach einer Norm ausreichend.

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

ergibt sich für

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

Eingesetzt ergibt das:

K1/K2:

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

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

und der Annahme, dass K1 und K2 jeweils einkanalig sind:

K1/K2: Betätigung 10/Sunde und direktes zurücklesen

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

Nun sind folgende Annahmen zu treffen:

Die Relais K1 und K2 sind beide an der Sicherheitsfunktion angeschlossen. Ein Nicht-Funktionieren eines Relais führt nicht zu einer gefährlichen Situation, wird aber durch die Rücklesung aufgedeckt. Weiterhin sind die $B10_D$-Werte für K1 und K2 identisch.

Es gibt einen Kopplungsfaktor zwischen den Komponenten, die zweikanalig verschaltet sind. Beispiele sind Temperatur, EMV, Spannungsspitzen oder Signale zwischen diesen Komponenten. Dieser wird als Worst-case-Abschätzung mit β =10% angenommen. Die EN 62061 enthält Tabellen (Tabelle F.1-Kriterien zur Bestimmung des CCF und Tabelle F.2-Abschätzung des CCF-Faktors(β)), mit der dieser β–Faktor genau bestimmt werden kann. Für das Ausgangssubsystem kann bei entsprechender Bearbeitung der Tabelle zur Berechnung des β-Faktors ein Wert von schätzungsweise 2% erreicht werden. In der folgenden Berechnung wird der Worst-Case mit 10% angenommen.

Weiterhin wird angenommen, dass alle üblichen Maßnahmen getroffen werden, um zu verhindern, dass beide Kanäle gleichzeitig durch einen Fehler (wie z.B. Überstrom durch Relais-Kontakte, Übertemperatur im Schaltschrank) unsicher ausfallen.

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1

$$PFH_{ges} = PFH_{(Scanner)} + PFH_{(EL6910)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

Da die Anteile $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ um Zehnerpotenzen kleiner sind, als der Rest, werden sie als Vereinfachung in dieser und allen weiteren Berechnungen nicht berücksichtigt.

$$PFH_{ges} = 8E - 08 + 1{,}79E - 09 + 1{,}25E - 09 + 10\% * \frac{1{,}94E - 09 + 1{,}94E - 09}{2} = 8{,}32E - 08$$

Der $MTTF_D$-Wert nach EN 13849 für Sicherheitsfunktion 1 berechnet sich mit:

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

zu:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Scanner)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

mit:

Sind für Scanner, EL2904 und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

$$MTTF_{d(x)} = \frac{(1 - DC(x))}{PFH(x)}$$

Somit:

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{15{,}68E-06\frac{1}{y}} = 637y$$

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

$$MTTF_{D(Scanner)} = \frac{(1-DC_{(Scanner)})}{PFH_{(Scanner)}} = \frac{(1-0{,}90)}{8E-08\frac{1}{h} * 8760\frac{h}{y}} = 142y$$

Entsprechend der in DIN EN ISO 13849-1 eingeführten Begrenzung der $MTTF_D$ auf 100 Jahre für Komponenten mit einer Kategorie 3 Struktur (für Kategorie 4 liegt die Beschränkung bei 2500 Jahren) wird für die Weiterverarbeitung der $MTTF_D$ des Scanners der Wert auf 100 Jahre begrenzt.

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

$$MTTF_{Dges} = \frac{1}{\frac{1}{100y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{588y}} = 69{,}6y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Scanner)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Scanner)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{90\%}{100} + \frac{99\%}{637} + \frac{99\%}{913} + \frac{99\%}{588} + \frac{99\%}{588}}{\frac{1}{100} + \frac{1}{637} + \frac{1}{913} + \frac{1}{588} + \frac{1}{588}} = 93{,}4\%$$

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

HINWEIS

Kategorie

Diese Struktur ist durch den Einsatz des Typ3 (Kategorie 3) Laserscanners maximal bis Kategorie 3 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

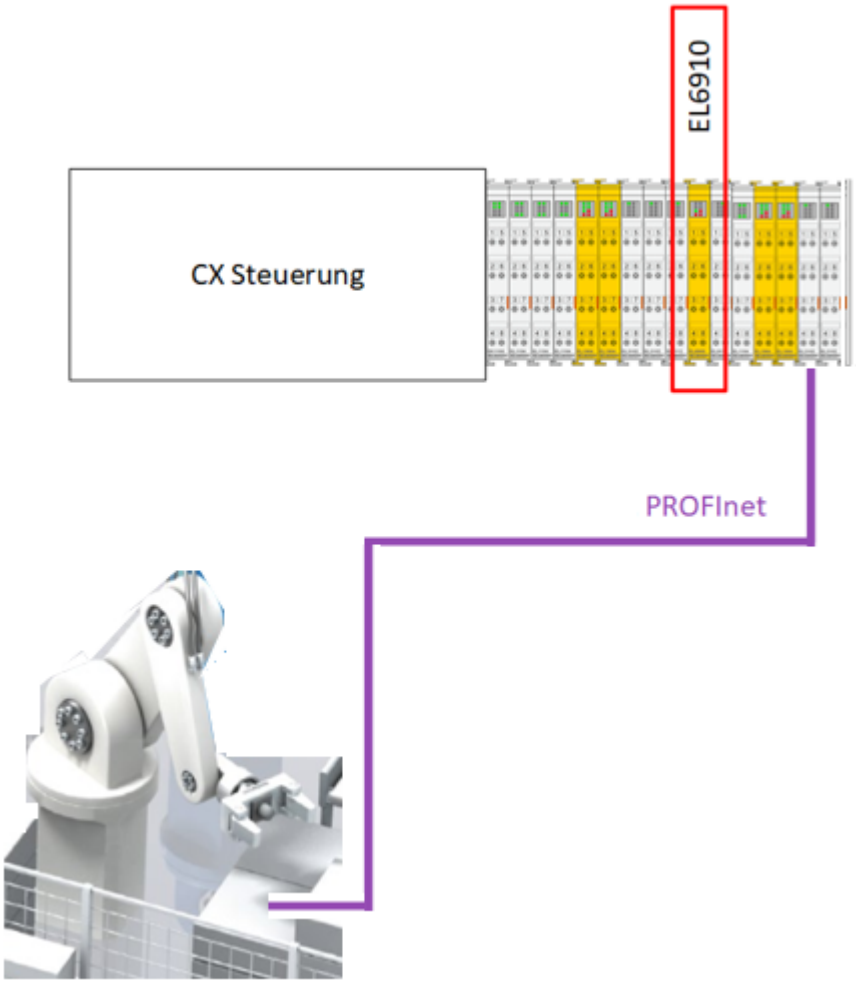
Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

10.3 Sichere Ansteuerung eines ABB-Roboters über PROFIsafe (Kategorie 3, PL d)

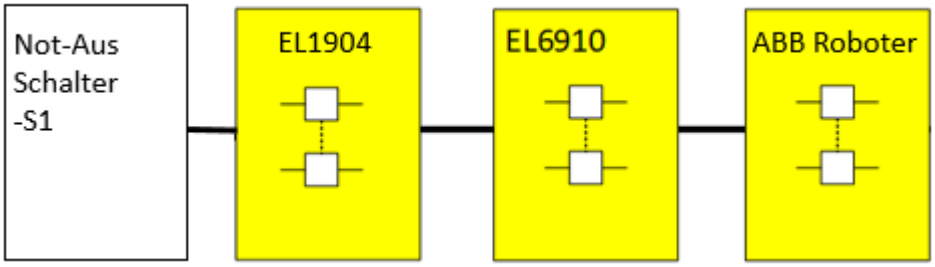
Ein ABB Roboter wird als PROFIsafe-Gerät an eine TwinSAFE-Steuerung angebunden. Der ABB Roboter mit der Funktionalität *SafeMove* ist für Anwendungen bis Performance Level d zertifiziert. Die sicherheitsrelevanten Daten werden mit Hilfe von PROFIsafe über PROFInet übertragen. Der Not-Aus wird von der EL6910 als PROFIsafe-Master über das sicherheitsrelevante Protokoll PROFIsafe an den Roboter übertragen. Der Roboter ist so konfiguriert, dass er einen Stopp der Kategorie 0 ausführt. Der sichere Zustand wird über die PROFIsafe-Verbindung an die EL6910 zurückgemeldet und dort mit den verfügbaren vorzertifizierten Funktionsbausteinen weiterverarbeitet.

Das Beispiel betrachtet die Sicherheitsfunktion Not-Halt. Der Not-Halt-Schalter ist mit 2 Öffnerkontakten 2-kanalig auf eine EL1904 verdrahtet. Die Testung der Signale ist eingeschaltet. Die Eingangssignale werden auf Diskrepanz überwacht. Die gesamte Auswertung wird in der sicherheitsgerichteten Logik EL6910 auf dem Sicherheitsniveau SIL 3/ PL e durchgeführt.

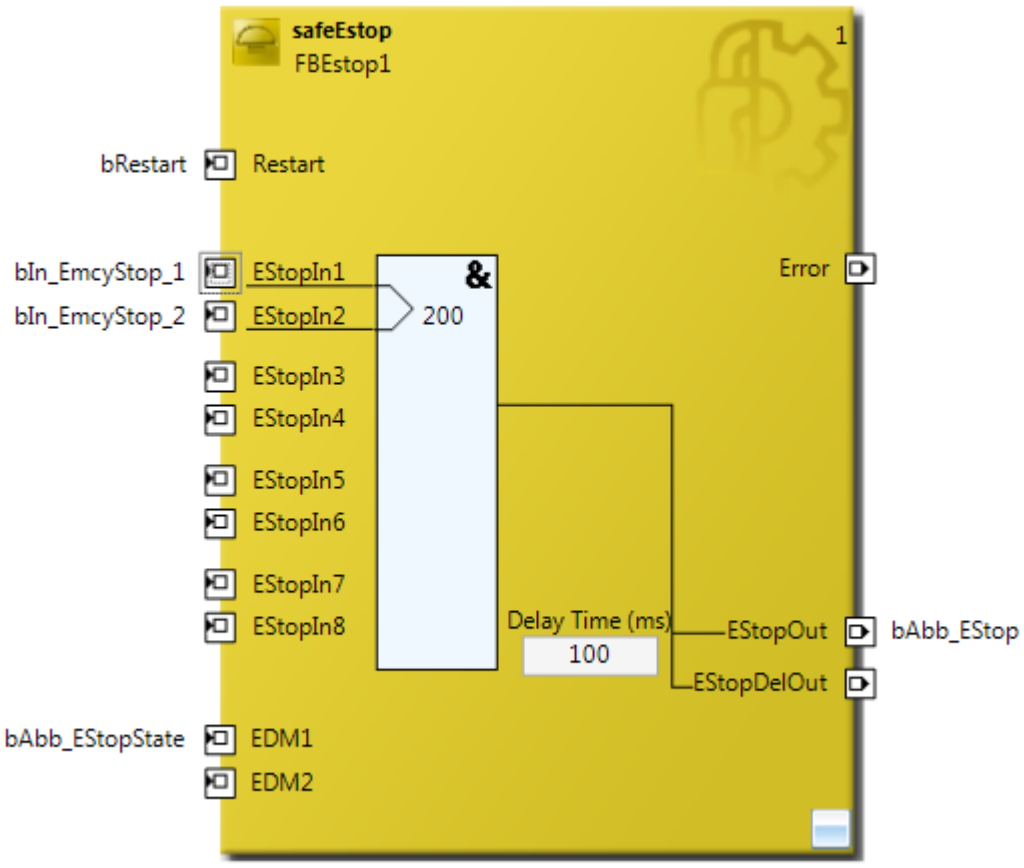
Aufbau



Strukturbild Aufbau



Logik



Korrekte Konfiguration Gesamtsystem

Bei der Übertragung von PROFIsafe innerhalb EtherCAT gibt es folgende Einschränkungen.

PROFIsafe-Telegramm nur über E-Bus und PROFINET/PROFIBUS

Die Verwendung von PROFIsafe ist es aufgrund der PROFIsafe Policy nur über die Feldbusse PROFIBUS und PROFINET oder über einen Rückwandbus, hier z.B. der E-Bus zulässig. Eine Nutzung von PROFIsafe über andere Feldbusse ist aus patentrechtlichen Gründen nicht zulässig. Dies muss durch Verwendung der Segment-Abschluss-Klemme EL9930 sichergestellt werden.

Folgende Patente der Siemens AG sind entsprechend des PROFIsafe Profils relevant:
- EP1267270-A2 Method for data transfer
- WO00/045562-A1 Method and device for determining the reliability of data carriers
- WO99/049373-A1 Shortened data message of an automation system
- EP1686732 Method and system for transmitting protocol data units
- EP1802019 Identification of errors in data transmission
- EP1921525-A1 Method for operation of a safety-related system
- EP13172092.2 Method and system for detection of errors

Je nach Architektur der Anwendung müssen also entsprechende Maßnahmen getroffen werden. Details zur korrekten Konfiguration des Gesamtsystems bezüglich PROFIsafe sind in den Dokumentationen der EL6910 und EL9930 zu finden.

Einsatz externer PROFIsafe Roboter

Bei dem Einsatz eines externen PROFIsafe Roboters sind weitere Anforderungen zu beachten.

⚠ VORSICHT

Einsatz externer PROFIsafe Roboter

Beim Einsatz eines externen PROFIsafe Roboters ist stets die aktuelle Version der Dokumentation zu beachten. Hier finden sich alle Anforderungen bezüglich Montage, Betrieb, Instandsetzung, welche zwingend erfüllt werden müssen, damit der Roboter in einer sicherheitsrelevanten Applikation korrekt genutzt werden kann.

10.3.1 FMEA

Einsatz externer PROFIsafe Roboter

Bei dem Einsatz eines externen PROFIsafe Roboters sind weitere Anforderungen auch hinsichtlich FMEA zu beachten.

⚠ VORSICHT

Einsatz externer PROFIsafe Roboter

Beim Einsatz eines externen PROFIsafe Roboters ist stets die aktuelle Version der Dokumentation zu beachten. Hier finden sich alle Anforderungen bezüglich Montage, Betrieb, Instandsetzung, welche zwingend erfüllt werden müssen, damit der Roboter in einer sicherheitsrelevanten Applikation korrekt genutzt werden kann.

10.3.2 Konfiguration in Engineeringumgebung

Im Rahmen des vorliegenden Applikationsbeispiels wird neben der Anbindung von TwinSAFE-Komponenten die zusätzliche Anbindung eines Encoders über PROFIsafe/PROFInet betrachtet. Im Folgenden werden im Detail alle nötigen Konfigurationsschritte zur Realisierung beschrieben.

Für die Konfiguration der sicherheitsrelevanten Parameter des Encoders ist eine zusätzliche Anwendung erforderlich, um die Parametrierung des Geräts vorzunehmen und die CRC Prüfsumme der iParameter zu ermitteln, welche letztlich innerhalb TwinCAT zusätzlich konfiguriert werden muss.

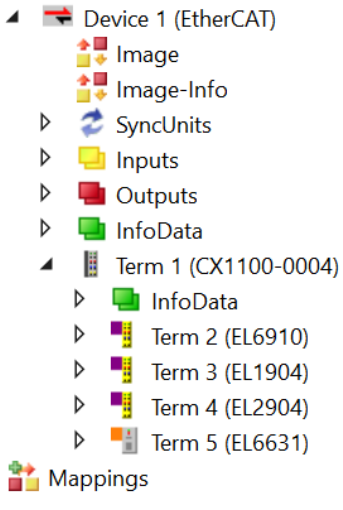
10.3.2.1 Konfiguration Roboter

Zur Konfiguration des Roboters ist eine zusätzliche Anwendung notwendig. Die aktuelle Version kann von der Webseite des Herstellers bezogen werden.

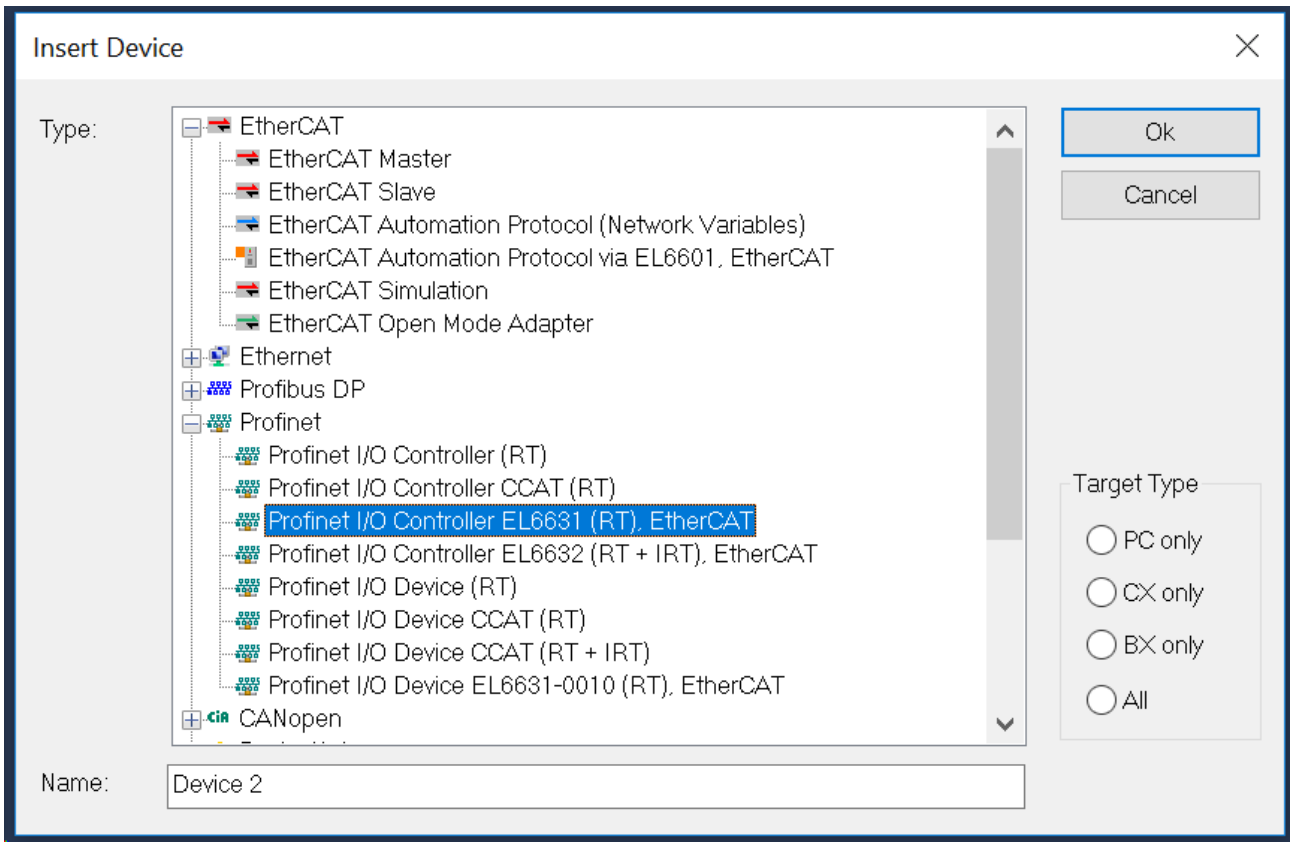
Hier müssen entsprechend der Applikation die notwendigen Funktionen und Parameter konfiguriert werden, damit z.B. die CRC Prüfsumme korrekt berechnet werden kann. Nur wenn die Einstellungen der sicheren Prozessabbilder übereinstimmen, ist die sicherheitsgerichtete Kommunikation möglich.

10.3.2.2 Konfiguration TwinCAT I/O

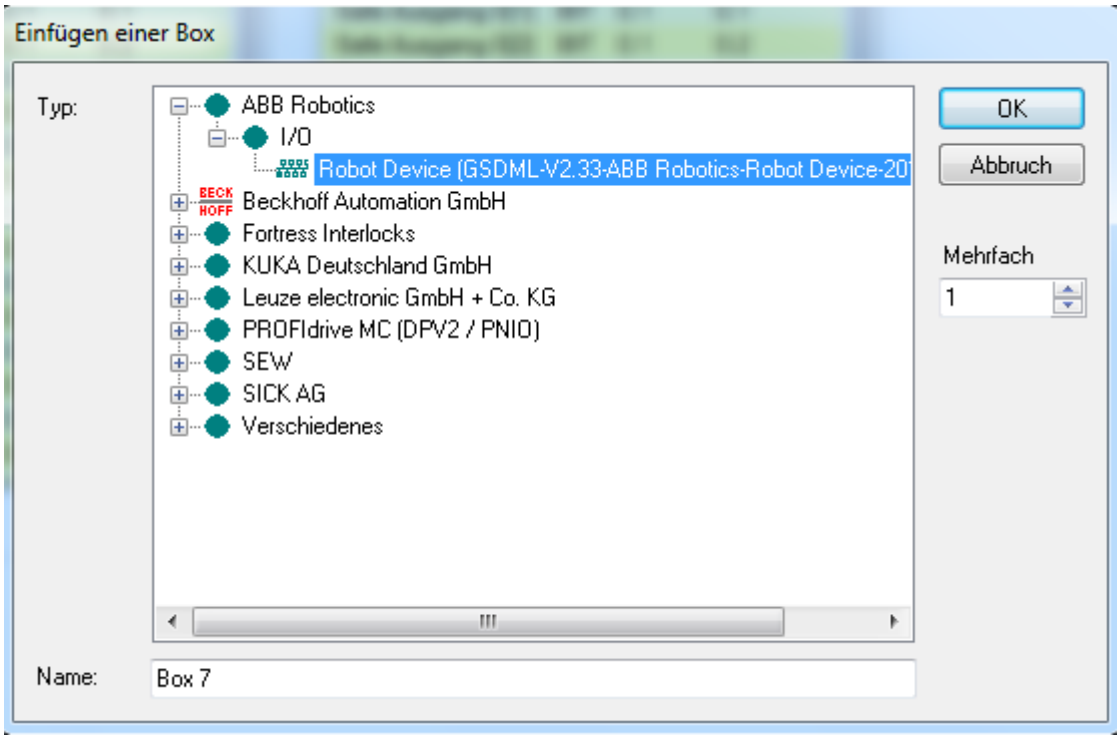
Zunächst wird eine neues TwinCAT Projekt angelegt und der EtherCAT-Strang konfiguriert.



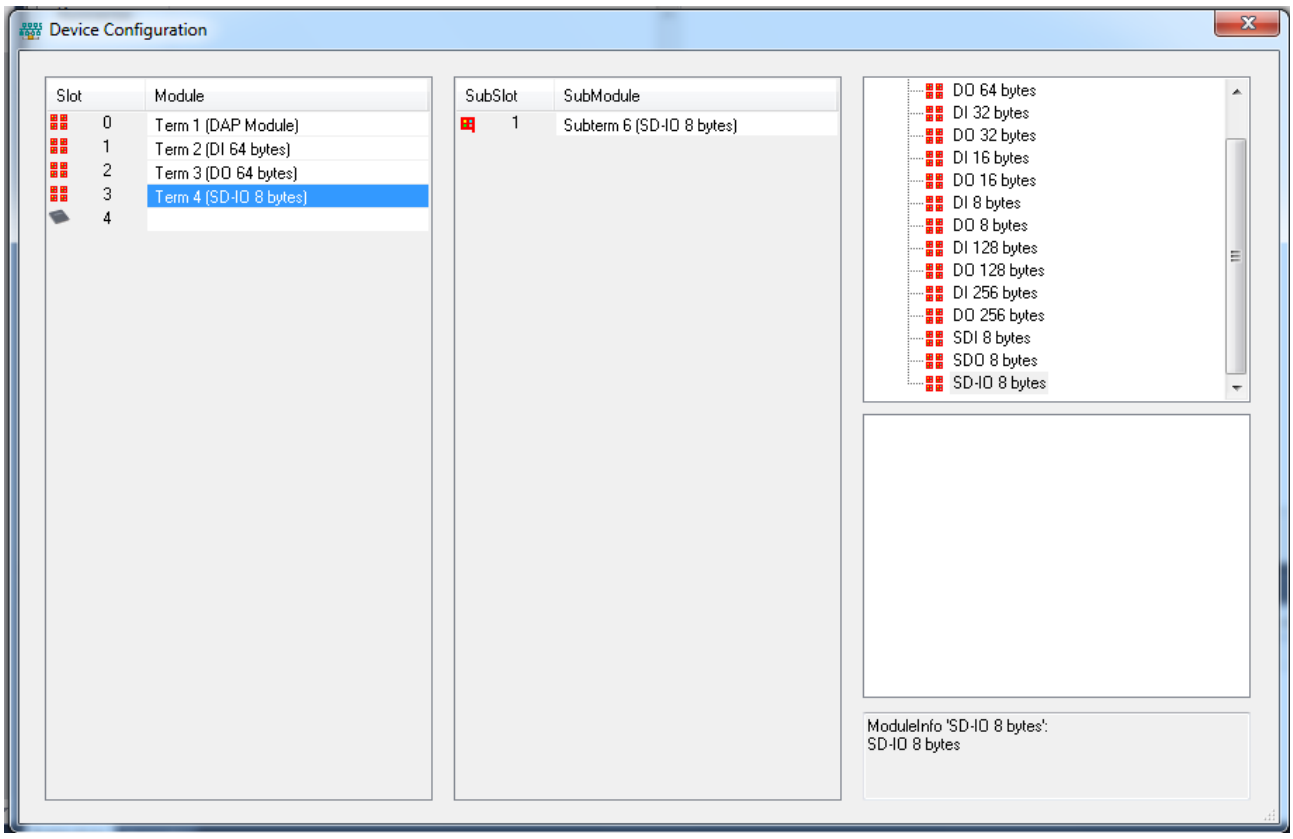
Zusätzlich wird die Konfiguration des PROFInet-Strangs durch Hinzufügen eines PROFInet-I/O-Controllers erzeugt.



Analog zur Konfiguration des EtherCAT-Strangs kann auch im Falle des PROFInet-Controllers ein automatischer Scan angestoßen oder die Konfiguration manuell erzeugt werden. So kann auch der ABB Roboter manuell hinzugefügt werden.



Die Device Konfiguration muss um das PROFIsafe- Safetymodul erweitert werden.



Für die erfolgreiche Nutzung des ABB Roboters über PROFIsafe sind folgende Informationen zu beachten.

⚠ VORSICHT

Datentyp WORD!

Bei Verwendung von WORD-Datentypen innerhalb des Prozessabbildes muss unter Umständen eine zusätzliche Konfiguration erfolgen.

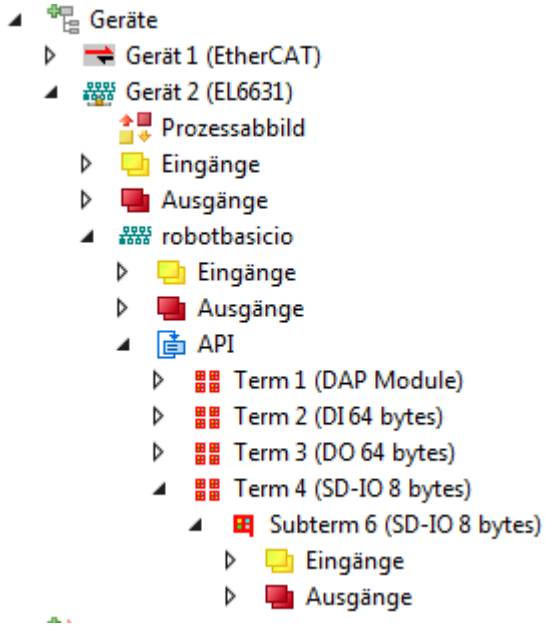
Wird innerhalb der Konfiguration keine EL9930 zur Begrenzung des PROFIsafe-Segments eingesetzt, so muss im Rahmen der I/O-Konfiguration des PROFIsafe-Gerätes für die im Prozessabbild enthaltenen Signale mit WORD-Datentyp des Tauschen des High und Low Byte-Anteiles konfiguriert werden. Dies erfolgt durch Auswahl der Checkbox *Tausche LOBYTE und HIBYTE* direkt auf den Datenwerten (unter dem Reiter *Flags*).

⚠ VORSICHT

iParamater

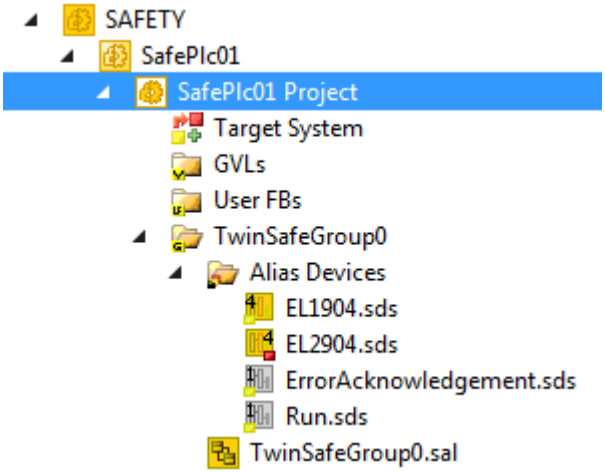
Auf dem PROFIsafe I/O-Gerät müssen die identischen iParameter wie auf dem *Alias Device* konfiguriert sein, damit die Kommunikation korrekt starten kann.

Anschließend kann mit der Konfiguration des Safety Projekts fortgefahren werden. Dabei wird an dieser Stelle von folgender Ausgangslage ausgegangen.

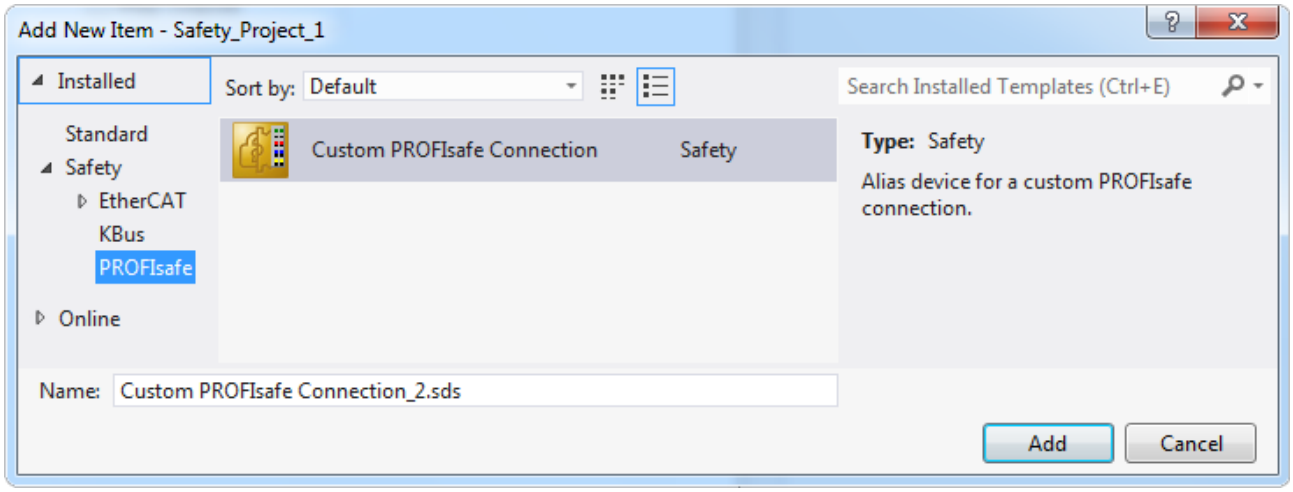


10.3.2.3 Konfiguration Verbindungen TwinCAT Safety Projekt

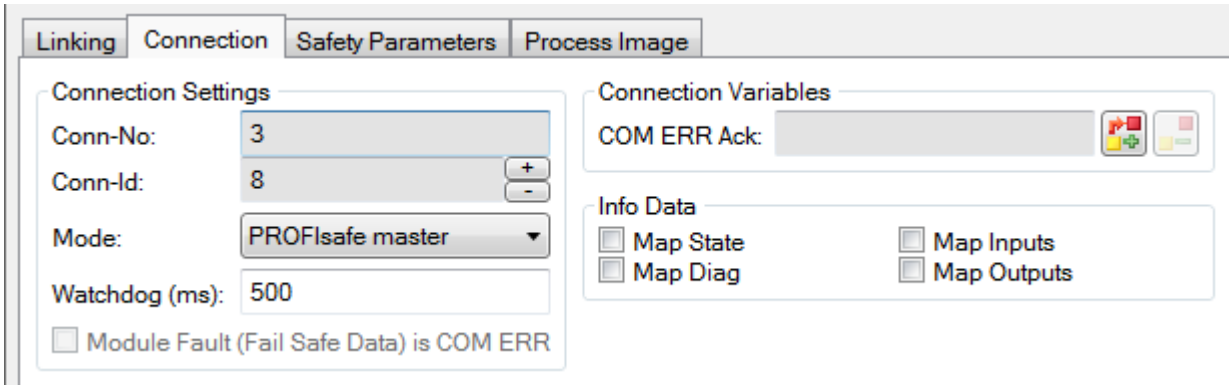
Vor der Konfiguration der PROFIsafe-Verbindung wird zunächst ein Safety Projekt angelegt und die benötigten Alias Devices für die verfügbaren EtherCAT-Komponenten importiert. Zusätzlich wird das Zielsystem auf die EL6910 des EtherCAT-Strangs gemappt (über den Knoten *Target System*).



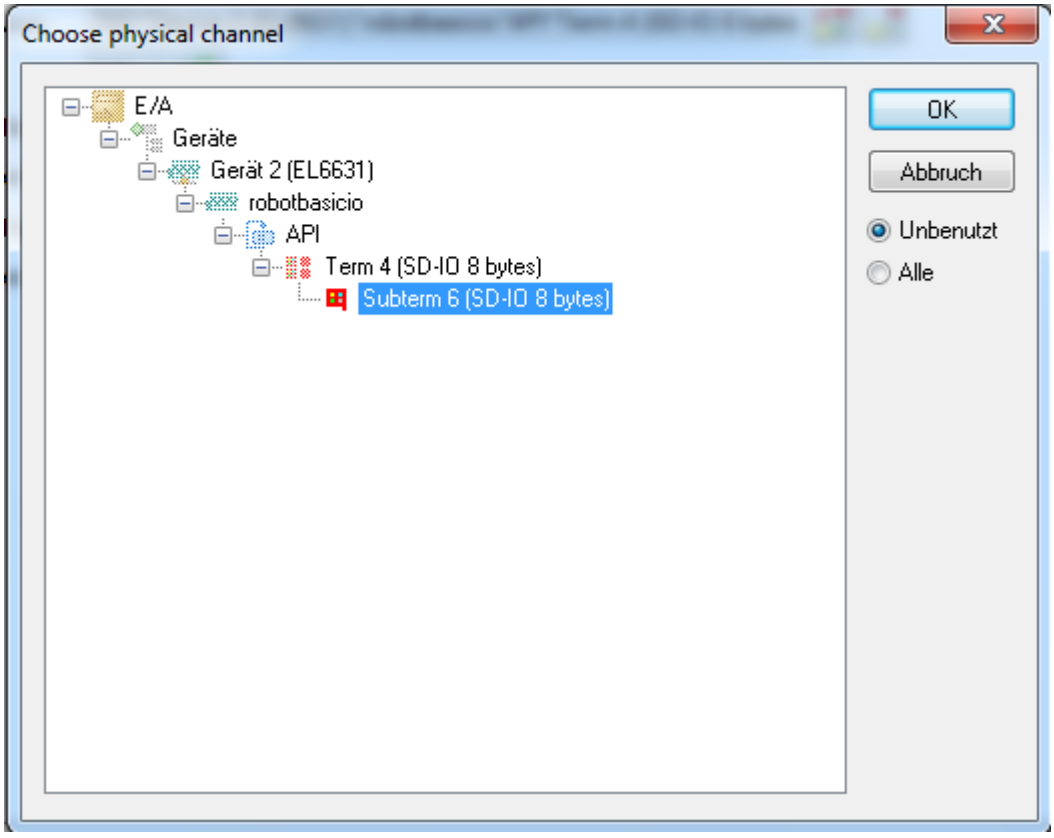
Anschließend kann mit der Konfiguration der PROFIsafe-Verbindung zum ABB Roboter fortgefahren werden. Diese Verbindung wird wie üblich über ein *Alias Device* realisiert. Über das Kontextmenu des Knotens *Alias Devices* und durch Auswahl von *Add* und *New item…* kann eine Custom PROFIsafe Connection angelegt werden.



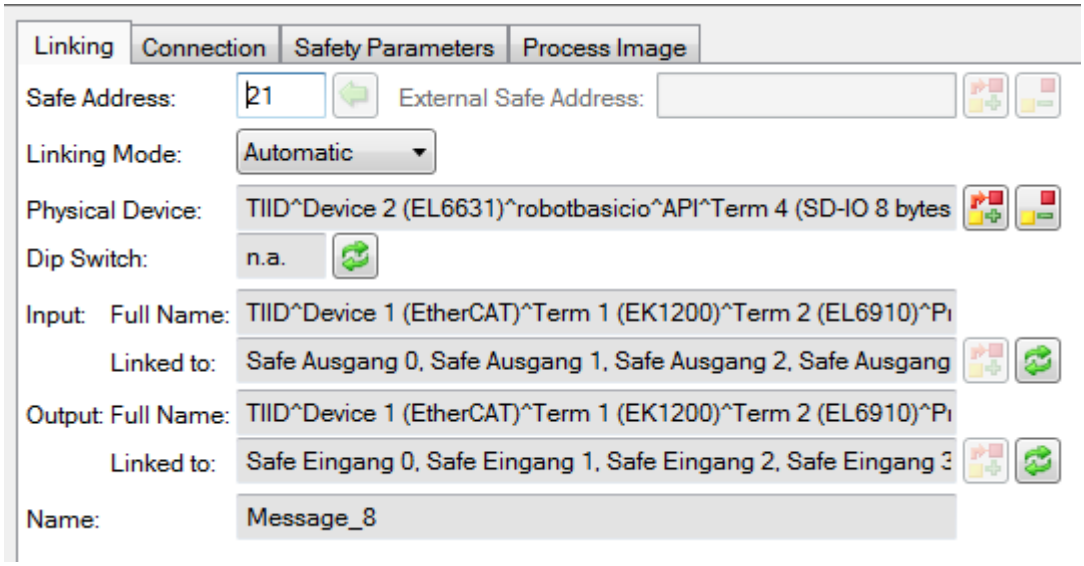
Nach dem Öffnen des Alias Devices muss zunächst über den Reiter *Connection* als Modus der Verbindung *PROFIsafe-Master* gewählt werden und der Watchdog für die Kommunikation.



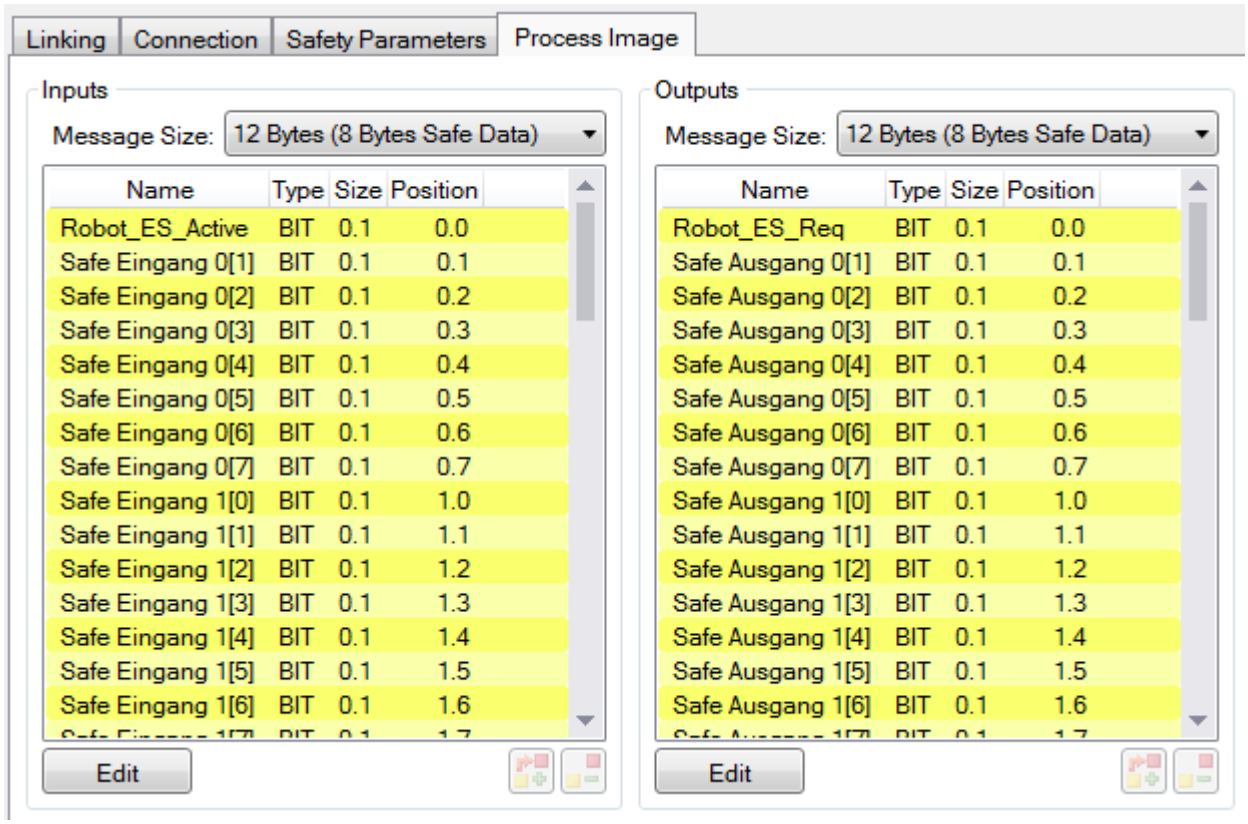
Auf dem Reiter *Linking* muss der Linking Mode auf *Automatic* eingestellt werden, damit über den Button *Map to Physical Device* der hier betrachtete ABB Roboter ausgewählt werden kann.



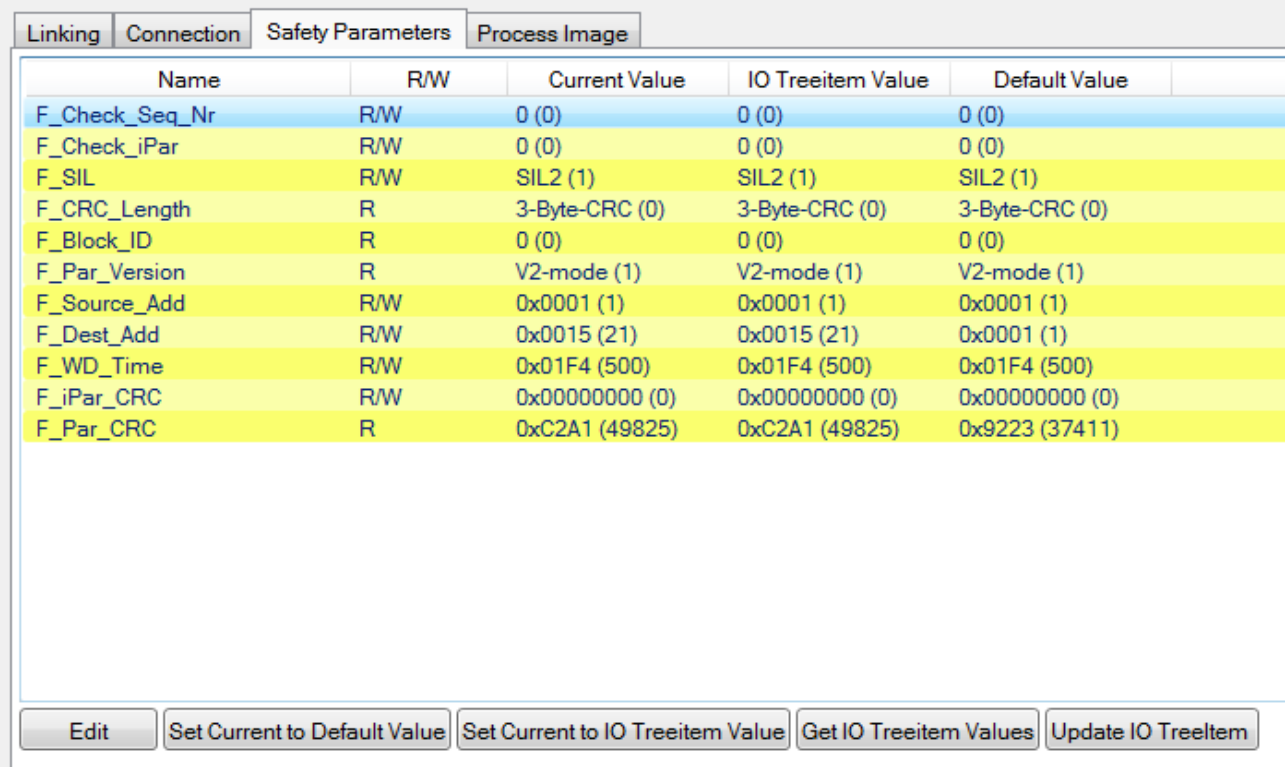
Neben dem Mapping zum physikalischen Device muss auf dem Reiter *Linking* auch die sichere Adresse des Gebers eingetragen werden (in diesem Beispiel 21).



Wurden alle Einstellungen korrekt vorgenommen, kann auf dem Reiter *Process Image* das sichere Prozessabbild des ABB Roboters eingestellt werden und entsprechend den Einstellung aus dem Applikationstool des Roboters editiert werden.



Der Reiter *Safety Parameters* stellt die Parameter für die PROFIsafe-Master-Verbindung zur Verfügung. Die Werte müssen gegebenfalls mit Hilfe des Buttons Edit an die Applikation angepasst werden.



Hier müssen alle Parameter für die PROFIsafe-Verbindung korrekt eingestellt werden. Darunter zählen unter anderem die beiden Adressen F_Source_Add (Zielsystem) und F_Dest_Add (sichere Adresse PROFIsafe-Gerät). Darüber hinaus muss die CRC der *iParameter* konfiguriert werden. Diese kann der zusätzlichen Applikation zur Konfiguration des Roboters entnommen werden (siehe Abschnitt *Konfiguration Roboter*)

Die Parameter müssen im Falle eines PROFIsafe-Geräts sowohl innerhalb des Alias Devices als auch direkt für das Device in der I/O-Konfiguration vorgenommen werden. Das Auslesen der Daten aus dem I/O-Device und das Übertragen an das I/O-Device kann über die entsprechenden Schaltflächen auf dem Reiter *Safety Parameters* angestoßen werden. Beide Daten müssen übereinstimmen, damit eine PROFIsafe-Verbindung erfolgreich aufgebaut werden kann.

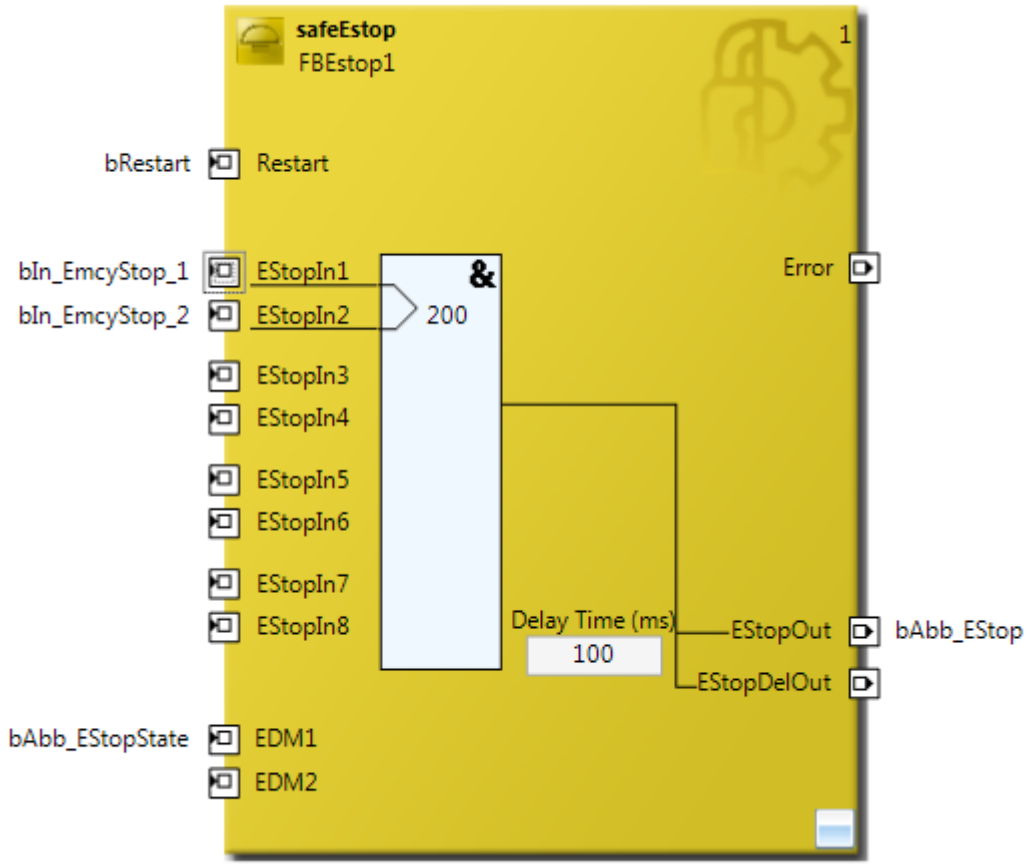
Parameter	Beschreibung
F_Check_Seq_Nr	Einstellung (0/1), ob die Sequenz-Nummer der Verbindung geprüft werden soll.
F_Check_iPar	Einstellung (0/1), ob die Parametrierung über einen iPar Server erfolgt.
F_SIL	Auswahl des erforderlichen SIL Levels (SIL1, SIL2, SIL3, NoSIL)
F_CRC_Length	Anzeige der CRC - Länge
F_Block_ID	immer 0
F_Par_Version	Verwendete Version PROFIsafe (typischerweise V2-Mode)
F_Source_Add	Einstellung der PROFIsafe-Source-Adresse
F_Dest_Add	Einstellung der PROFIsafe-Ziel-Adresse
F_WD_Time	Einstellung der Watchdogzeit
F_iPar_CRC	i-Parameter für den PROFIsafe Slave
F_Par_CRC	Berechnete CRC über die gesamten Parameter

Nach Fertigstellung der Konfiguration der Parameter müssen diese durch Klick auf den Button *Update IO TreeItem* final an die I/O-Konfiguration übertragen werden.

Nach Beendigung der Konfiguration der Verbindungen kann mit der Implementierung der eigentlichen Sicherheitsfunktion fortgefahren werden.

10.3.2.4 Implementierung TwinCAT Safety Projekt

Im Rahmen der in diesem Beispiel betrachteten Sicherheitsfunktion wird ein Not-Aus-Schalter mit 2 Öffnerkontakten über EL1904 2-kanalig sicher eingelesen. Die Testung der Eingänge ist aktiviert. Die Auswertung der Eingänge erfolgt über den Funktionsblock safeEstop mit aktivierter Diskrepanzüberwachung.



Wie die Abbildung zeigt werden über den Ausgang *EStopOut* des Funktionsblocks *safeEstop* das Signal für die Ansteuerung des ABB Roboters über PROFIsafe geschaltet. Die Rückführung des ABB Roboters wird als *EDM*-Eingang des Funktionsblocks safeEstop genutzt.

10.3.3 Parameter der sicheren Eingangsklemme

EL1904

Parameter	Wert
Sensortest Kanal 1 aktiv	Ja
Sensortest Kanal 2 aktiv	Ja
Sensortest Kanal 3 aktiv	Ja
Sensortest Kanal 4 aktiv	Ja
Logik Kanal 1 und 2	Single Logic
Logik Kanal 3 und 4	Single Logic

10.3.4 Blockbildung und Safety-Loops

10.3.4.1 Sicherheitsfunktion 1

Sicherheitsfunktion 1 betrachtet für das bisher beschriebene Anwendungsbeispiel den Safety Loop ausgehend vom Not-Aus Schalter S1 bis hin zu dem ABB Roboter.

10.3.5 Berechnung Sicherheitsfunktion 1

10.3.5.1 PFHD / MTTFD / B10D – Werte

Komponente	Wert
ABB Roboter, SafeMove Funktion[1] – PFH_D, PL, $MTTF_D$, DC_{avg}	1,19E-07, PL d, 52y, mittel
EL1904 – PFH_D	1,11E-09
EL6910 – PFH_D	1,79E-09
S1 – $B10_D$	100.000
Arbeitstage (d_{op})	230
Arbeitsstunden / Tag (h_{op})	16
Zykluszeit (Minuten) (T_{zyklus})	10080 (1x pro Woche)
Lebenszeit (T1)	20Jahre = 175200 Stunden

[1] Bitte beachten Sie die Informationen der aktuellen Anwenderdokumentation

10.3.5.2 Diagnostic Coverage DC

Komponente	Wert
ABB Roboter, SAFEMove Funktion[1]	DC_{avg}=90%
S1 mit Testung/ Plausibilität	DC_{avg}=99%

[1] Bitte beachten Sie die Informationen der aktuellen Anwenderdokumentation

10.3.5.3 Berechnung Sicherheitsfunktion 1

Zur Verdeutlichung wird der Sicherheitskennwert sowohl nach EN 62061 als auch nach EN ISO 13849-1 berechnet. In der Praxis ist die Berechnung nach einer Norm ausreichend.

Berechnung der PFH_D-/ und $MTTF_D$-Werte aus den $B10_D$-Werten:

Aus:

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

und:

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

ergibt sich für

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

Eingesetzt ergibt das:

S1:

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

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

und der Annahme, dass S1 einkanalig ist:

S1: Betätigung 1/Woche und direktes zurücklesen

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

Daraus folgt für die Berechnung des PFH_D-Wertes für Sicherheitsfunktion 1

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6910)} + PFH_{(Roboter)}$$

$$PFH_{ges} = 2,5E-11+1,11E-9+1,79E-9+1,19E-7 = 1,22E-7$$

Der $MTTF_D$-Wert nach EN 13849 für Sicherheitsfunktion 1 berechnet sich mit:

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

zu:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(Roboter)}}$$

mit:

Sind für EL1904 und EL6910 nur PFH_D Werte vorhanden, gilt folgende Abschätzung:

$$MTTF_{d(x)} = \frac{(1-DC(x))}{PFH(x)}$$

Somit:

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

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

Der Wert des Roboters kann der aktuellen Anwenderdokumentation entnommen werden:

$$MTTF_{D(Roboter)} = 52y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{637y} + \frac{1}{52y}} = 45,88y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(EL1904)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(Roboter)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(Roboter)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{637y} + \frac{90\%}{52y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{637y} + \frac{1}{52y}} = 91\%$$

⚠ VORSICHT

Wiederanlaufsperre in der Maschine implementieren!

Die Wiederanlaufsperre ist NICHT Teil der Sicherheitskette und muss in der Maschine implementiert werden!

HINWEIS

Kategorie

Diese Struktur ist durch die Sicherheitsdaten des eingesetzten Roboters maximal bis Kategorie 3 möglich.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	**30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre**

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	**90 % ≤ DC < 99 %**
hoch	99 % ≤ DC

HINWEIS

Diagnosedeckungsgrad

Für die praktische Anwendbarkeit wurde die Zahl der Bereiche auf vier beschränkt. Für die gezeigten Grenzwerte dieser Tabelle wird eine Genauigkeit von 5 % angenommen.

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC / $MTTF_D$	**kein**	**kein**	**niedrig**	**mittel**	**niedrig**	**mittel**	**hoch**
niedrig	a	-	a	b	b	c	-
mittel	b	-	b	c	c	d	-
hoch	-	c	c	d	d	d	e

11 Projektierung eines Safety-Projektes mit TwinSAFE-Komponenten

Dieses Kapitel gibt einen Überblick über den generellen Ablauf einer Projektierung eines Sicherheitsprojektes, bei denen TwinSAFE-Komponenten zum Einsatz kommen.

⚠ VORSICHT

Maschinenrichtlinie

Diese Beschreibung gilt nur für Maschinen im Sinne der Maschinenrichtlinie.

⚠ VORSICHT

Normen

Die relevanten Normen müssen dem Anwender vorliegen. Die folgende Beschreibung kann die Norm nicht ersetzen. Typischerweise sollten mindestens die EN ISO 13849-1 und die EN ISO 13849-2 oder die EN 62061 in dem jeweils aktuellen Stand vorliegen. Weitere hilfreiche Informationen finden sich auch im IFA-Report 2/2017.

HINWEIS

Typ-C Norm

Bevor mit dem folgenden Prozess begonnen wird, sollten Sie klären, ob für ihre Maschine eine Typ-C Norm vorliegt. Liegt diese vor, befolgen Sie bitte die Schritte und Vorgaben die dort aufgeführt sind. Liegt keine Typ-C Norm vor, können Sie den im Folgenden beschriebenen Prozess als Leitfaden für die durchzuführenden Prozessschritte nehmen.

11.1 Identifizieren der Risiken und Gefährdungen

Die DIN EN ISO 12100 definiert einen *iterativen Prozess zur Risikominimierung* zur Beseitigung von Gefährdungen oder zur Minderung des Risikos an Maschinen. Darin wird der Prozess der Risikominimierung in einer 3-Stufen-Methode beschrieben. Im ersten Schritt soll die Maschine inhärent sicher konstruiert werden, ist dies nicht möglich können technische Schutzmaßnahmen ergriffen werden, um das Risiko zu minimieren und im letzten Schritt kann eine Benutzerinformation über das Restrisiko erfolgen.

Im ersten Schritt müssen also die Risiken und Gefährdungen und somit die Sicherheitsfunktionen identifiziert werden. Hierbei benötigt der Maschinenbauer genaue Kenntnis der Funktionsweise seiner Maschine, um Risiken und Gefährdungen zu identifizieren. Hierbei hilft unter anderem auch ein Blick in den Anhang B der EN ISO 12100:2010.

Diese Risiko- und Gefährdungsanalyse sollte von Personen mit Kenntnissen aus unterschiedlichen Bereichen durchgeführt werden (Mechanik, Elektrik, Hydraulik, Software, Wartung, ...). Es müssen alle Betriebsarten bzw. -zustände berücksichtigt werden, wie z.B. die Inbetriebnahme, die Instandhaltung/ Wartung, der normale Betrieb und die Außerbetriebnahme. Die Gründe für oder gegen eine Entscheidung sollen ebenfalls festgehalten werden. Achten Sie dabei auf die Nachvollziehbarkeit und Schlüssigkeit Ihrer Argumente und Rechtfertigungen.

Hierbei ist besonders zu beachten, dass zur Bewertung des Risikos noch keine Sicherheitsmaßnahmen berücksichtigt werden dürfen.

Wenn alle beteiligten Personen dem Ergebnis der Analyse zustimmen, sollte diese von allen Beteiligten unterzeichnet werden.

11.2 Bestimmung des PLr / SIL

Für jede in der Risiko- und Gefährdungsanalyse identifizierte Sicherheitsfunktion (SF) der Maschine muss der Maschinenbauer bzw. Anwender eine Bestimmung des erforderlichen Performance Level oder SIL Levels durchführen.
Der SIL Level wird anhand der Beschreibung im Anhang A der EN 62061 ermittelt
Anhand des Risikograph zur Bestimmung des PL_r der EN ISO 13849-1 wird der Performance Level ermittelt.
Informationen zum Risikograph finden Sie im Anhang A der EN ISO 13849-1:2015.

11.3 Spezifikation der Sicherheitsfunktionen

Für jede identifizierte Sicherheitsfunktion muss spezifiziert werden, auf welche Art und Weise das Risiko entsprechend der EN ISO 12100 *Strategie zur Risikominderung* reduziert werden soll.

Risiken und Gefährdungen, deren Restrisiko durch inhärent sichere Konstruktion oder durch Benutzerinformation reduziert werden soll, müssen spezifiziert werden, sind jedoch nicht Teil dieser Beschreibung.
Die folgenden Ausführungen beziehen sich nur auf Sicherheitsfunktionen, deren Restrisiko durch technische Schutzmaßnahmen reduziert werden soll.

Für diese Sicherheitsfunktionen wird der *iterative Prozess der Gestaltung der sicherheitsbezogenen Teile der Steuerung (SRP/CS)* entsprechend der EN ISO 13849-1:2015 durchgeführt.

11.4 Spezifikation der Maßnahmen

Zu jeder identifizierten Sicherheitsfunktion (SF), deren Restrisiko über technische Schutzmaßnahmen reduziert werden soll, wird eine detaillierte Beschreibung durch den Maschinenbauer erstellt. Diese Beschreibung enthält Informationen über die Gefährdung, die Art und Weise der Maßnahmen zur Reduzierung der Gefährdung und den erforderlichen Performance Level bzw. SIL Level für diese Sicherheitsfunktion.

Die Beschreibung der Maßnahmen muss für jede SF unter anderem die Kategorie nach EN ISO 13849-1 und die zu verwendenden Komponenten mit ihren sicherheitstechnischen Kenngrößen ($MTTF_D$, DC, CCF, SFF) enthalten.

Informationen über die Betriebszustände und -charakteristika werden benötigt. Dies sind u.a. die Betriebsarten, die Zykluszeit, erforderliche Reaktionszeiten bzw. die Prozess-Sicherheitszeit, Umgebungsbedingungen, Häufigkeit der Ausführung, Betriebszeiten, Verhalten der Maschine bei Energieverlust und weitere. Detaillierte Informationen dazu finden Sie unter anderem im Kapitel 5.2 der EN 62061 und Kapitel 5 der EN ISO 13849-1:2015.

Die Beschreibung des sicherheitsgerichteten Programmes für die TwinSAFE Logic muss durch den Maschinenbauer spezifiziert und dokumentiert werden, da dies die Basis für die Realisierung ist. Neben der Auswahl der TwinSAFE Komponenten, der zu verwendenden Funktionsblöcke und der Sensorik und Aktorik, muss auch die Parametrierung der Komponenten festgelegt werden, da dies den maximal erreichbaren Performance Level beeinflussen kann.

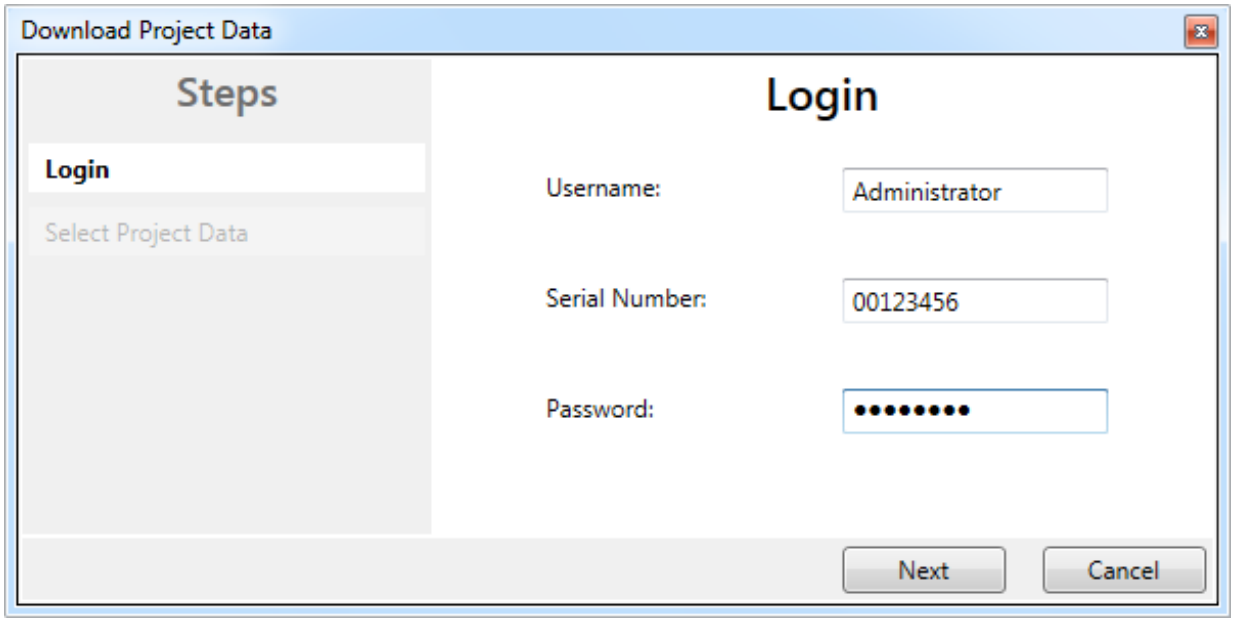
Beispiele zur Implementation von Sicherheitsfunktionen und der Parametrierung der TwinSAFE Komponenten finden Sie in diesem Handbuch.

11.5 Realisierung der Sicherheitsfunktionen

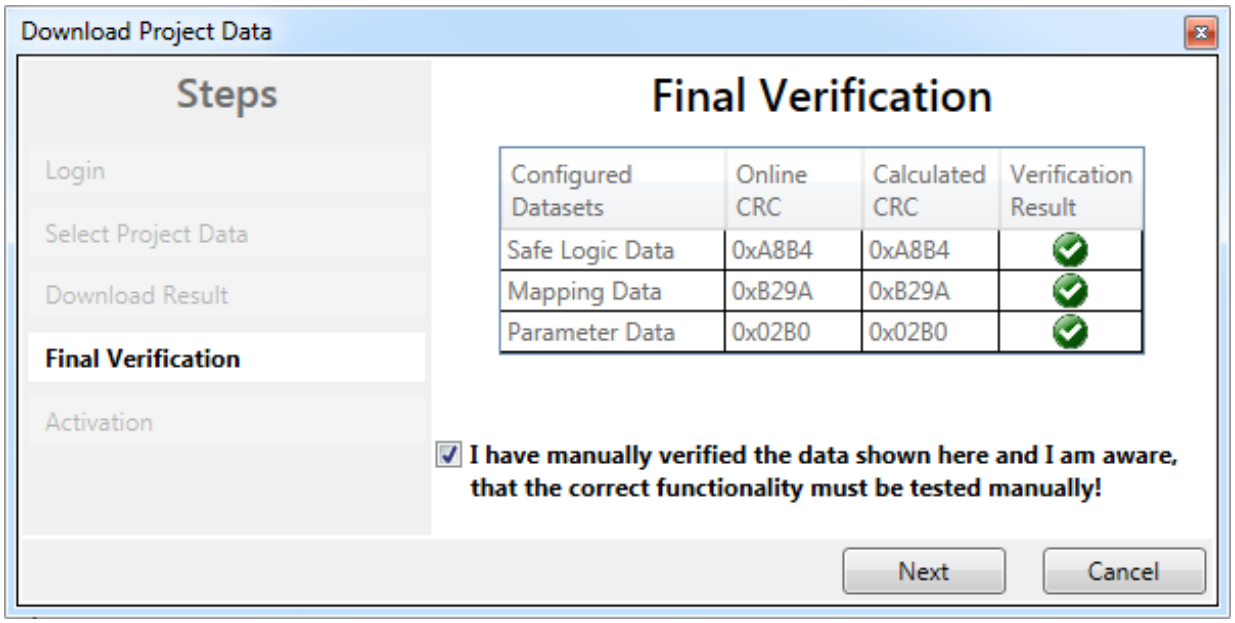
Anhand der spezifizierten Sicherheitsfunktionen werden die Funktionsbausteine in TwinCAT entsprechend projektiert. Für die typischen Sicherheitsfunktionen gibt es vordefinierte Bausteine, die in einem freigrafischen Editor miteinander verschaltet werden können. Sichere Ein- und Ausgangs-Komponenten stellen die Schnittstelle zur Sensorik und Aktorik sicher.

Nachdem die gesamte Sicherheitslogik und die Parametrierung der sicheren Ein- und Ausgänge implementiert ist, kann ein Download auf die TwinSAFE-Logic erfolgen.

Für den Download muss ein gültiger Benutzername und Passwort zusammen mit der Seriennummer des Gerätes angegeben werden.



Die Prüfung auf einen korrekten Download des Safety Programmes erfolgt über einen CRC Vergleich zwischen der CRC des geladenen Projektes (Online-CRC) und der berechneten CRC aus dem Safety Editor (Offline-CRC). Der Vergleich wird zum einen durch TwinCAT und zum anderen von dem Anwender durchgeführt. Dieser bestätigt den Vergleich mit Setzen der Checkbox und erneuter Eingabe des Passwortes.



Über die Safety CRC Toolbar in TwinCAT kann jederzeit durch den Anwender überprüft werden, ob die Online CRC zur Offline CRC passt, d.h. ob Daten im Editor oder auf der TwinSAFE-Logic verändert wurden. Folgende Tabelle ist der EL6910 Dokumentation entnommen.

Icon	Name	Beschreibung
CRCs:	CRC Toolbar	Durch einen linken Mausklick auf die Toolbar kann eine Aktualisierung der CRCs durch den Anwender gestartet werden. Rotes Icon: CRCs unterschiedlich
CRCs:	CRC Toolbar	Grünes Icon: Alle CRCs sind gleich
0x9135 | 0x9135 | 0x9135	Online CRC	CRC des Safety-Projektes auf EL6910/EJ6910. Dieser Wert wird online von EL6910/EJ6910 gelesen. Besteht keine ADS-Verbindung zu EL6910/EJ6910 wird dieser Wert mit 0x---- angezeigt.
0x9135 | 0x9135 | 0x9135	Downloaded CRC	CRC des zuletzt geladenen Safety-Projektes. Wurde nach dem Öffnen des TwinCAT-Projektes noch kein Safety-Projekt geladen, wird der Wert mit 0x---- angezeigt.
0x9135 | 0x9135 | 0x9135	Offline CRC	CRC des aktuellen Safety-Projektes, wie es im Safety-Editor gespeichert ist. Eine CRC wird angezeigt, wenn das gespeicherte Projekt gültig ist. Ist das Projekt nicht gültig, wird 0x---- als CRC angezeigt.

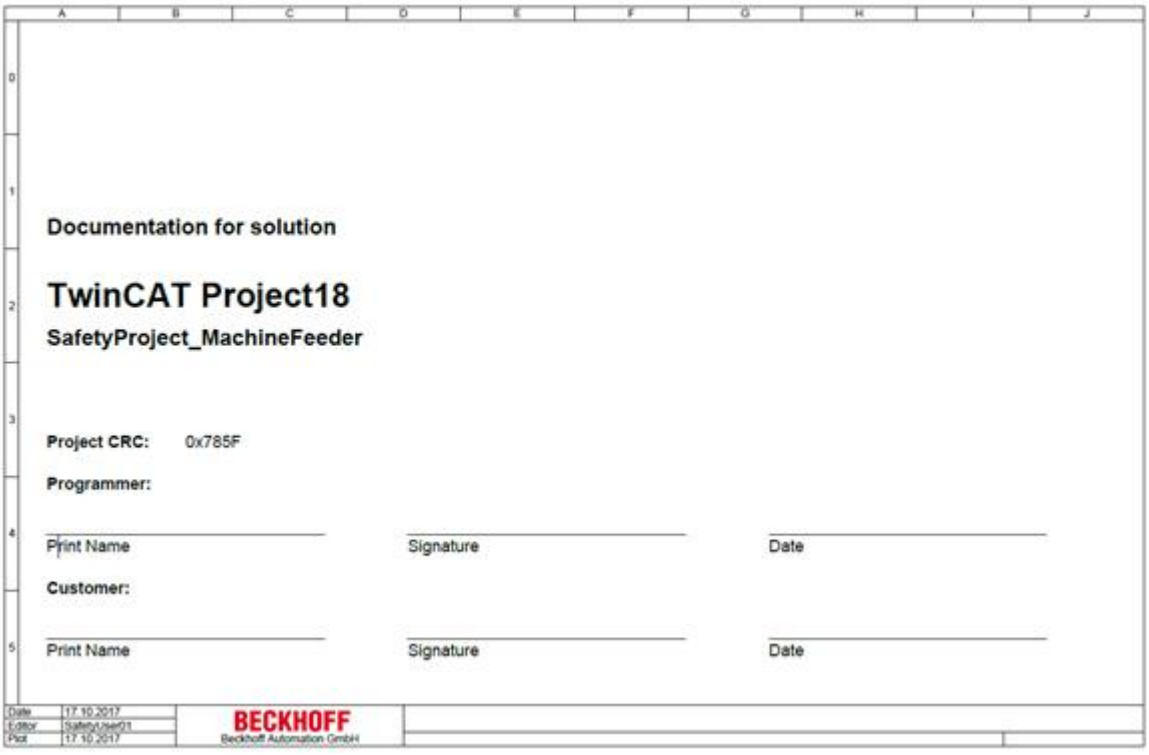
⚠ VORSICHT

Kontrolle der Prüfsummen

Der Anwender hat zu prüfen, dass die Online-CRC und die Offline-CRC übereinstimmen. Nur so kann sichergestellt werden, dass nach Erstellung des Projektes oder Änderungen des Projektes auch ein Download erfolgt ist.

Nachdem alle spezifizierten Sicherheitsfunktionen in der TwinSAFE-Logic umgesetzt sind, erfolgt ein Ausdruck der realisierten Logik.

Der Ausdruck enthält neben der gesamten Logik, den Parametern und Safety Adressen aller verwendeten Safety Komponenten auch die berechnete Projekt-Prüfsumme. Diese wird schon auf dem Deckblatt angezeigt. Auf dem Deckblatt können der Programmierer und der Kunde die Abnahme der Sicherheitsfunktionen mit Datum und Unterschrift dokumentieren.



11.6 Nachweis über das Erreichen des Performance Levels

Nach der Realisierung des Safety Projektes für die identifizierten Sicherheitsfunktionen (SF) erfolgt der rechnerische Nachweis über den erreichten Performance Level für diese SF. Beispiele, wie solche Berechnungen und Nachweise durchgeführt werden finden sich in diesem Handbuch in Kapitel 2.

11.7 Validierung der Sicherheitsfunktionen

Auszug aus der EN ISO 13849-2:2013, Kapitel 4.1 Validierungsleitsätze.

Die referenzierten Kapitel sind bereits auf die Kapitelnummern der EN ISO 13849-1:2015 umgesetzt, obwohl in der EN ISO 13849-2:2013 noch die EN ISO 13849-1:2006 referenziert wird.

Der Zweck des Validierungsverfahrens ist es, zu bestätigen, dass die Gestaltung der sicherheitsbezogenen Teile der Steuerung (SRP/CS) die Spezifikation der Sicherheitsanforderungen der Maschinen unterstützt.

Die Validierung muss aufzeigen, dass jedes SRP/CS die Anforderungen von EN ISO 13849-1:2015 erfüllt, insbesondere bei

a) den festgelegten Sicherheitseigenschaften der Sicherheitsfunktionen, wie diese bei der sinnvollen Gestaltung vorgesehen wurde;

b) den Anforderungen für den festgelegte Performance Level (siehe EN ISO 13849-1:2015, 4.5):
   1. den Anforderungen für die festgelegte Kategorie (siehe EN ISO 13849-1:2015, 6.2),
   2. den Maßnahmen zur Beherrschung und zur Vermeidung systematischer Ausfälle (siehe EN ISO 13849-1:2015, Anhang G),
   3. den Anforderungen an die Software, falls vorhanden (siehe EN ISO 13849-1:2015, 4.6), und
   4. der Fähigkeit, eine Sicherheitsfunktion unter den erwarteten Umgebungsbedingungen zu leisten;

c) der ergonomischen Gestaltung der Benutzerschnittstelle, z. B. damit der Benutzer nicht verleitet wird, in einer gefährlichen Weise zu handeln, indem er z. B. die SRP/CS umgeht (siehe EN ISO 13849-1:2015, 4.8).

Die Validierung sollte von Personen durchgeführt werden, die unabhängig von der Gestaltung der SRP/CS sind.

ANMERKUNG „Unabhängige Person“ bedeutet nicht unbedingt, dass eine Prüfung durch Dritte erforderlich ist.

Weitere Informationen zur Validierung finden Sie in der EN ISO 13849-2:2013 z.B. unter Bild 1 *Übersicht über das Validierungsverfahren* und in der EN ISO 13849-1:2015.

11.8 Hinweise für das Testen der SF

Alle implementierten Sicherheitsfunktionen (SF) müssen auf ihre Korrektheit überprüft werden. Dies umfasst sowohl den Normalbetrieb, als auch die Funktion im Fehlerfall. Ein Teil der Testfälle sind aus der definierten Sicherheitsfunktion mit ihren beschriebenen Maßnahmen zur Risikominimierung ablesbar. Zu jeder Funktion müssen die möglichen Fehlerfälle definiert und entsprechend überprüft werden. Diese Informationen müssen in einer Testspezifikation bzw. einem Abnahmeprotokoll festgehalten werden.

- Folgende Auflistung zeigt einige zu berücksichtigende Fehlerfälle:
- Diskrepanzfehler zweier sicherer Eingänge
- Leitungsunterbrechung des verwendeten Feldbusses
- Feedback (EDM) Fehler der Aktorik
- Ausfall der Spannungsversorgung
- Querschluss / Fremdeinspeisung / Leitungsunterbrechung in der Verdrahtung
- Verletzung eines definierten Limits z.B. Geschwindigkeitsgrenze bei Achsfunktionen und Überprüfen des definierten Fehlerverhaltens

- ...

Weiterhin muss auch überprüft werden, dass alle seitens der Risikobeurteilung identifizierten Gefahren auch durch Maßnahmen abgedeckt sind und diese auch tatsächlich umgesetzt sind.

Dies gilt vor allem auch für die Lebensphasen Installation/Montage und Instandhaltung. Es muss sichergestellt werden, dass erforderliche Änderungen oder Erweiterungen des Safety Projektes erst nach Rückmeldung an den Konstrukteur (Maschinenbauer) und Änderung der Sicherheits-Spezifikation durch diesen erfolgen. Eine Prüfung, ob eine Erweiterung der Testspezifikation notwendig ist, muss ebenfalls erfolgen. Dies gilt besonders für Maschinen, die beim Endkunden vor Ort aufgebaut und in Betrieb gesetzt werden.

Folgende Punkte muss der Test mindestens umfassen:

- I/O Check der sicheren Ein- und Ausgänge
- Prüfung der Parametrierung aller Safety Komponenten (Watchdogzeiten, Sensortests, FSoE-Adresse usw.)
- Überprüfung der Sicherheitsfunktionen im Normalbetrieb
- Überprüfung der Sicherheitsfunktionen im Fehlerfall
- Überprüfung der sicheren Antriebsfunktionen im Normalbetrieb
- Überprüfung der sicheren Antriebsfunktionen außerhalb der definierten Sicherheitsgrenzen
- Überprüfung der sicheren Antriebsfunktionen bei Spannungsausfall
- ...

11.9 Abnahme

Folgende Liste enthält Punkte, die zur Abnahme des Safety Projektes erforderlich sind. Diese Liste erhebt nicht den Anspruch auf Vollständigkeit. Diese Punkte sind nach der Erstinbetriebnahme, sowie nach jeder Softwareänderungen des TwinSAFE Projektes durchzuführen.

- Implementierung bzw. Änderungen nur durch qualifiziertes Personal
- Ausdruck des TwinSAFE Projektes
- Überprüfung des gesamten Safety Projektes auf Korrektheit entsprechend des vorherigen Kapitels
- Vergleich der Online CRC des TwinSAFE Projektes mit der Offline-CRC, um sicherzustellen, dass nach den Änderungen am Safety Projekt auch ein Download erfolgt ist
- Durchführung und Ausdruck des Abnahmeprotokolls
- Unterschrift durch Programmierer und Kunden
- Hinzufügen dieser Informationen zur Maschinen-Dokumentation
- ...

12 Technischer Bericht TÜV SÜD

KONFORMITÄTSBESTÄTIGUNG
LETTER OF CONFIRMATION

BV89987T

Rail

Applikationshandbuch TwinSAFE
(Application guide TwinSAFE)

Hersteller: Manufacturer:	**Prüfstelle:** Test body:
Beckhoff Automation GmbH & Co. KG	TÜV SÜD RAIL GmbH Rail Automation
Huelshorstweg 20 D-33415 Verl	Barthstr. 16 D-80339 München

1. Allgemein / General

Das **"Applikationshandbuch TwinSAFE"** zeigt die Berechnungen der sicherheitsrelevanten Kennwerte bezüglich der Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle (MTTFd und PFH) nach EN 61508 bzw. EN ISO 13849-1.

The **"Application guide TwinSAFE"** shows calculations of the safety relevant parameters of the probability of dangerous random hardware failures (MTTFd and PFH) according to EN 61508 respectively EN ISO 13849-1.

2. Prüfgrundlagen / Test bases

Berechnung des $MTTF_d$ und DC entsprechend EN ISO 13849-1:2015 Calculation of $MTTF_d$ and DC in accordance with EN ISO 13849-1:2015
Berechnung des PFH entsprechend EN 61508:2010 Calculation of PFH in accordance with EN 61508:2010
Applikationshandbuch TwinSAFE Version 3.2.0 Application guide TwinSAFE version 3.2.0

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
2022-06-14

Digital signiert von Claudio Gregorio
Datum: 2022.06.14 14:59:03 +02'00'

C. Gregorio
Technical Certifier

Digital unterschrieben von Thomas Kreten
Datum: 2022.06.14 14:46:03 +02'00'

T. Kreten
Project Leader

Diese Bestätigung wurde auf Grundlage einer TÜV-internen technischen Beurteilung erstellt.
Diese enthält das Ergebnis einer einmaligen Untersuchung an dem zur Prüfung vorgelegten Erzeugnis.

This confirmation was created on basis of a TÜV internal technical review report.
It includes the result of a one-time examination of the product submitted for examination.

Mehr Informationen:
www.beckhoff.de/TwinSAFE

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Deutschland
Telefon: +49 5246 9630
info@beckhoff.com
www.beckhoff.com