Ausbildungsunterlage für die durchgängige Automatisierungslösung Totally Integrated Automation (T I A)

ANHANG VI

Safety Integrated

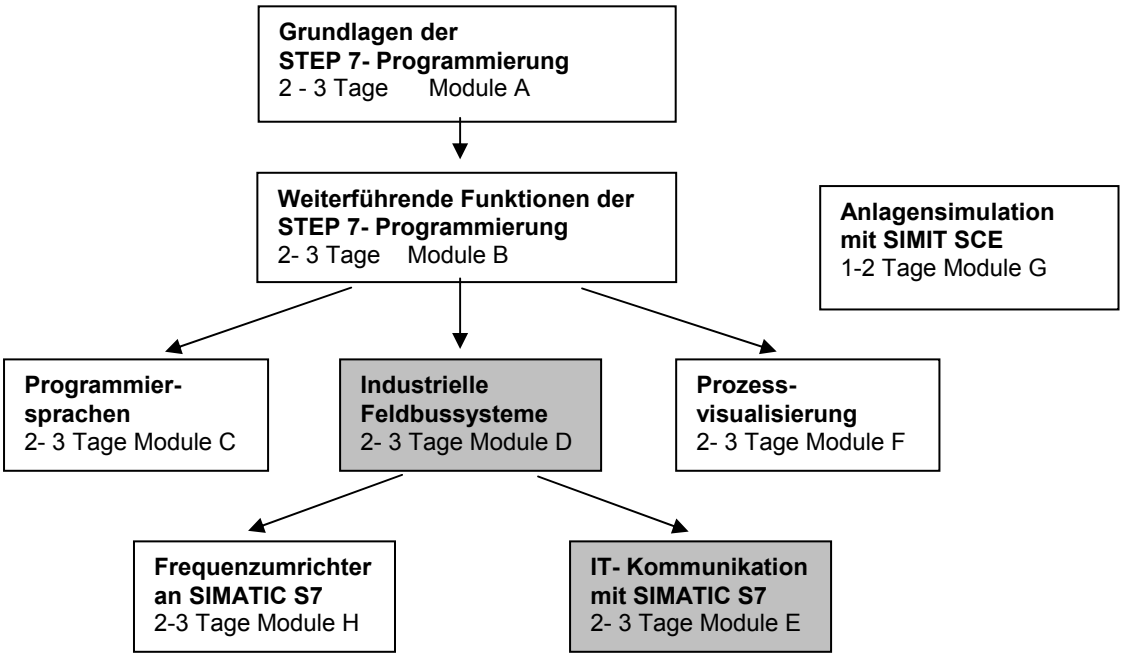
Wir danken der Fa. Michael Dziallas Engineering und den Lehrkräften von beruflichen Schulen sowie weiteren Personen für die Unterstützung bei der Erstellung der Unterlage

SEITE:

1 Vorwort 4
2 Einleitung 5
3 Maschinensicherheit 8
3.1 Allgemeine Begriffsbestimmungen 8
3.2 Vorschriften und Normen in der Europäischen Union (EU) 10
3.3 Sicherheitsbezogene Funktionen in der Maschinensteuerung 13
3.4 Farbkennzeichnung 17
3.4.1 Kennzeichnung von Leuchtmeldern und Drucktastern 17
3.4.2 Kennzeichnung von Leitungen 20
4 Risikobetrachtung und Identifizierung der Gefährdung 22
4.1 Allgemeine Risikobeurteilung / Sicherheitskategorien / Safety Integrity Level (SIL) 22
4.2 Konkrete Risikobeurteilung anhand einer CNC-Maschine 30
4.3 Realisierung der Schutzvorkehrungen 32
5 Safety Integrated mit SIMATIC S7 Safety SPS 37
5.1 Aufbau der SIMATIC S7-300 CPU 315F- 2 PN/DP 37
5.2 Fehlersichere Kommunikation mit PROFIsafe 42
5.3 Peripheriekomponenten für PROFIsafe 54
5.4 Verdrahtungsbeispiele zu den F- Modulen in der ET 200S 56
5.4.1 Powermodul PM-E F pm DC24V PROFIsafe (6ES7 138-4CF0*-0AB0) 56
5.4.2 Digitales Elektronikmodul 4/8 F-DI DC24V PROFIsafe (6ES7 138-4FA0*-0AB0) 67
5.4.3 Digitales Elektronikmodul 4 F-DO DC24V/2A PROFIsafe (6ES7 138-4FB01-0AB0) 79
6 Sicherheitsgerichtete Programmierung 86
6.1 Einführung in die sicherheitsgerichtete Programmierung 86
6.2 Programmstruktur des Sicherheitsprogramms 87
6.3 Fehlersichere Bausteine 89
6.3.1 F-Bausteine einer F-Ablaufgruppe 89
6.3.2 F-Bausteine der F-Bibliothek *Distributed Safety (V1)* 90
6.3.3 Übersicht F-Applikationsbausteine 91
6.4 Programmieren in F-FUP / F-KOP 92
7 Fehlerdiagnose bei Safety Integrated 98
7.1 Diagnose bei den F-Modulen in der ET200S 98
7.2 Diagnosewerkzeuge 100
8 Überprüfung der Wirksamkeit und Erstellen eines Sicherheitsprotokolls 102
8.1 Gesetzliche Vorgaben zur Wirksamkeitsüberprüfung / Validierung 102
8.2 Abnahme einer Anlage 104
8.2.1 Abnahme der Projektierung der F-Peripherie 104
8.2.2 Abnahme eines Sicherheitsprogramms 107

1 Vorwort

Anhang VI stellt eine theoretische Grundlage für die Bearbeitung der Module zur Sicherheitstechnik D13, D14,D15 und E08 dar.



Lernziel:

Der Leser erhält mit diesem Anhang Informationen zur Sicherheitstechnik mit SIMATIC S7.

Voraussetzungen:

Da dies theoretische Grundlagen sind, werden auch keine speziellen Voraussetzungen benötigt.

2 Einleitung

„Das Verhüten von Unfällen darf
nicht als eine Vorschrift des
Gesetzes aufgefasst werden,
sondern als ein Gebot
menschlicher Verpflichtung
und wirtschaftlicher Vernunft.“

Werner von Siemens,
Berlin im Jahr 1880

Zielsetzung der Sicherheitstechnik

Zielsetzung der Sicherheitstechnik ist es, die Gefährdung von Menschen und Umwelt durch technische Einrichtungen so gering wie möglich zu halten, ohne dadurch die Produktion, den Einsatz von Maschinen oder die Herstellung von bestimmten Produkten mehr als unbedingt notwendig einzuschränken.

Durch zum Teil international abgestimmte Regelwerke soll der Schutz von Mensch und Umwelt allen Ländern in gleichem Maße zuteil werden und gleichzeitig sollen Wettbewerbsverzerrungen wegen unterschiedlicher Sicherheitsanforderungen im internationalen Handel vermieden werden.
In den verschiedenen Regionen und Ländern der Welt gibt es unterschiedliche Konzepte und Anforderungen zur Gewährleistung von Sicherheit. Die rechtlichen Konzepte und die Anforderungen wie und wann nachzuweisen ist, ob ausreichende Sicherheit besteht, sind ebenso unterschiedlich wie die Zuordnung der Verantwortlichkeiten. So bestehen z.B. in der EU Anforderungen sowohl an den Hersteller als auch an den Betreiber einer Einrichtung, die durch Richtlinien, Gesetze und Normen geregelt sind.

In USA bestehen dagegen regional und sogar lokal unterschiedliche Anforderungen.
Einheitlich im ganzen Land ist jedoch der Grundsatz, dass ein Arbeitgeber Sicherheit am Arbeitsplatz gewährleisten muss. Im Falle eines Schadens kann, aufgrund der Produkthaftung, der Hersteller für den Schaden, der mit seinem Produkt in Verbindung gebracht werden kann, haftbar gemacht werden.

In anderen Ländern oder Regionen gelten wiederum andere Prinzipien.

Wichtig für Hersteller und Errichter von Maschinen und Anlagen ist, dass immer die Gesetze und Regeln des Ortes gelten, an dem die Maschine oder Anlage betrieben wird. Beispielsweise muss die Steuerung einer Maschine, die in der EU betrieben werden soll, den lokalen Anforderungen genügen, auch wenn der Maschinenhersteller aus der USA stammt.

Elektrische und funktionale Sicherheit

Die Sicherheit ist aus Sicht des zu schützenden Gutes unteilbar. Da die Ursachen von Gefährdungen und damit auch die technischen Maßnahmen zu ihrer Vermeidung aber sehr unterschiedlich sein können, unterscheidet man verschiedene Arten der Sicherheit, z.B. durch Angabe der jeweiligen Ursache möglicher Gefährdungen.

So spricht man von „elektrischer Sicherheit“, wenn der Schutz vor den Gefährdungen durch die Elektrizität zum Ausdruck gebracht werden soll.

Von „funktionaler Sicherheit“ dagegen, wenn die Sicherheit von der korrekten Funktion abhängt.

Diese Unterscheidung hat sich in der neueren Normung in der Art niedergeschlagen, dass es spezielle Normen gibt, die sich mit der funktionalen Sicherheit befassen. Im Bereich der Maschinensicherheit behandelt EN 954 speziell sicherheitsrelevante Teile von Steuerungen und konzentriert sich damit auf die funktionale Sicherheit.
IEC behandelt in der Basis Sicherheitsnorm IEC 61508 funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme unabhängig von einem speziellen Anwendungsgebiet.
Funktionale Sicherheit ist in IEC 61508 definiert als „part of the overall safety relating to the EUC* and the EUC control system which depends on the correct functioning of the E/E/PE** safetyrelated systems, other technology safety-related systems and external risk reduction facilities”.

Um funktionale Sicherheit einer Maschine oder Anlage zu erreichen, ist es notwendig, dass die sicherheitsrelevanten Teile der Schutz und Steuereinrichtungen korrekt funktionieren und sich im Fehlerfall so verhalten, dass die Anlage in einem sicheren Zustand bleibt oder in einen sicheren Zustand gebracht wird. Dazu ist die Verwendung besonders qualifizierter Technik notwendig, die den in den betreffenden Normen beschriebenen Anforderungen genügt. Die Anforderungen zur Erzielung funktionaler Sicherheit basieren auf den grundlegenden Zielen:
• Vermeidung systematischer Fehler,
• Beherrschung systematischer Fehler,
• Beherrschung zufälliger Fehler oder Ausfälle.

Das Maß für die erreichte funktionale Sicherheit ist die Wahrscheinlichkeit gefährlicher Ausfälle, die Fehlertoleranz und die Qualität, durch die die Freiheit von systematischen Fehlern gewährleistet werden soll. Es wird in den Normen durch unterschiedliche Begriffe ausgedrückt. In IEC 61508: „Safety Integrity Level” (SIL), in EN 954: „Kategorien” und in DIN V 19250 und DIN V VDE . 0801: „Anforderungsklassen” (AK).

Anforderungen an die Sicherheitstechnik

Die sicherheitstechnischen Einrichtungen an Maschinen nehmen eine besondere Stellung innerhalb der steuerungs- und installationstechnischen Ausrüstung ein.
Auf der einen Seite stehen dabei die rechtlichen und normativen Anforderungen, die über den Weg der Gefahrenanalyse den Umfang und die Qualität der Sicherheitstechnik durch Gefahrenvermeidung bzw. -reduzierung bestimmen.
Auf der anderen Seite finden sich stetig steigende Leistungskenngrößen heutiger Fertigungssysteme, wie z.B. maximale Achsgeschwindigkeit bzw. –beschleunigung bei Werkzeugmaschinen und die technische Verfügbarkeit, was sich in der Gesamt-Produktivität der betrachteten Maschine (Overall Machine Effectiveness OME) widerspiegelt.
Um die Wirksamkeit der Sicherheitstechnik heutiger Produktionsanlagen zu gewährleisten, d.h. den Anforderungen an einen praxisgerechten Personenschutz zu entsprechen, sind innovative Lösungsprinzipien gefragt. Dabei ist unter innovativer Sicherheitstechnik zu verstehen, dass sie nicht hinter der Steuerungs- und Installationstechnik aus dem Bereich der nicht sicherheitsrelevanten Automatisierungstechnik von Maschinen im Hinblick auf Flexibilität, Diagnostizierbarkeit und Standardisierung zurückbleibt.

Zielsetzung der Vorschriften und Normen zur Maschinensicherheit

Aus der Verantwortung, die Hersteller und Betreiber technischer Einrichtungen und Produkte für die Sicherheit haben, resultiert die Forderung, Anlagen, Maschinen und andere technische Einrichtungen so sicher zu machen, wie es nach dem Stand der Technik möglich ist.
Dazu wird von den Wirtschaftspartnern der Stand der Technik bezüglich aller Aspekte, die für die Sicherheit von Bedeutung sind, in Normen beschrieben.
Durch Einhaltung der jeweils relevanten Normen kann dann sichergestellt werden, dass der Stand der Technik erreicht ist und damit der Errichter einer Anlage oder Hersteller einer Maschine oder eines Gerätes seine Sorgfaltspflicht erfüllt hat.

3 Maschinensicherheit

3.1 Allgemeine Begriffsbestimmungen

(Maschinenrichtlinie (98/37/EG) Anhang I Absatz 1.1.2)
„Durch die Bauart der Maschine muss gewährleistet sein, dass Betrieb, Rüsten und Wartung bei bestimmungsgemäßer Verwendung ohne Gefährdung von Personen erfolgen kann."

Sicherheitsmaßnahmen müssen darauf abzielen, Unfallrisiken während der voraussichtlichen Lebensdauer der Maschine, einschließlich der Zeit, in der die Maschine montiert und demontiert wird, auszuschließen.

Gefahrenbereich:
Der Gefahrenbereich gilt als der Bereich innerhalb und/oder im Umkreis einer Maschine, in dem die Sicherheit oder die Gesundheit einer Person durch den Aufenthalt in diesem Bereich gefährdet wird.

Gefährdete Person:
Als gefährdete Person gilt diejenige Person, die sich ganz oder teilweise in einem Gefahrenbereich befindet.

Bedienungspersonal:
Das Bedienungspersonal ist für Installation, Betrieb, Rüsten, Wartung, Reinigung, Störungsbeseitigung und Transport einer Maschine zuständig.

Sicherheit und Zuverlässigkeit von Steuerungen:
Steuerungen sind so zu konzipieren, dass diese sicher und zuverlässig funktionieren und somit keine gefährlichen Situationen entstehen. Insbesondere müssen sie so konzipiert und gebaut sein, dass sie den zu erwartenden Betriebsbeanspruchungen und Fremdeinflüssen standhalten sowie Fehler in der Logik zu keiner gefährlichen Situation führen.

Die Betriebssicherheits-Verordnung (BetrSichV) schreibt allgemeine Mindestvorschriften für Arbeitsmittel vor:

- Kraftbetriebene Arbeitsmittel müssen mit einer Befehlseinrichtung zum sicheren Stillsetzen des gesamten Arbeitsmittels ausgerüstet sein (Not-Aus).
- Kraftbetriebene Arbeitsmittel müssen mit mindestens einer Not-Befehlseinrichtung versehen sein, mit der gefahrbringende Bewegungen oder Prozesse möglichst schnell stillgesetzt werden, ohne eine zusätzliche Gefährdung zu erzeugen.
- Jeder Arbeitsplatz muss mit Befehlseinrichtungen ausgerüstet sein, mit denen sich entsprechend der Gefahrenlage das gesamte Arbeitsmittel oder bestimmte Teile des Arbeitsmittels in den sicheren Zustand versetzen lassen.
- Arbeitsmittel müssen mit Schutzeinrichtungen ausgestattet sein, die den unbeabsichtigten Zugang zum Gefahrenbereich verhindern oder die beweglichen Teile vor dem Erreichen des Gefahrenbereiches stillsetzen.
- Arbeitsmittel müssen für den Schutz der Beschäftigten gegen direktes oder indirektes Berühren mit elektrischem Strom ausgelegt sein.
- Instandsetzungs- und Wartungsarbeiten müssen bei Stillstand des Arbeitsmittels vorgenommen werden können.
- Befehlseinrichtungen müssen außerhalb des Gefahrenbereiches so angeordnet sein, dass ihre Betätigung keine zusätzliche Gefährdung mit sich bringt.
- Vom Bedienungsstand aus muss sich das Bedienungspersonal vergewissern können, dass sich keine Personen im Gefahrenbereich aufhalten.
- Ist dies nicht möglich, muss dem Ingangsetzen ein sicheres System wie z.B. ein optisches oder ein akustisches Warnsignal vorgeschaltet werden.
- Beschäftige müssen Zeit und Möglichkeit haben, den Gefahrenbereich zu verlassen oder das Ingangsetzen zu verhindern.
- Das Ingangsetzen eines Arbeitsmittels darf durch absichtliche Betätigung einer hierfür vorgesehenen Befehlseinrichtung möglich sein.

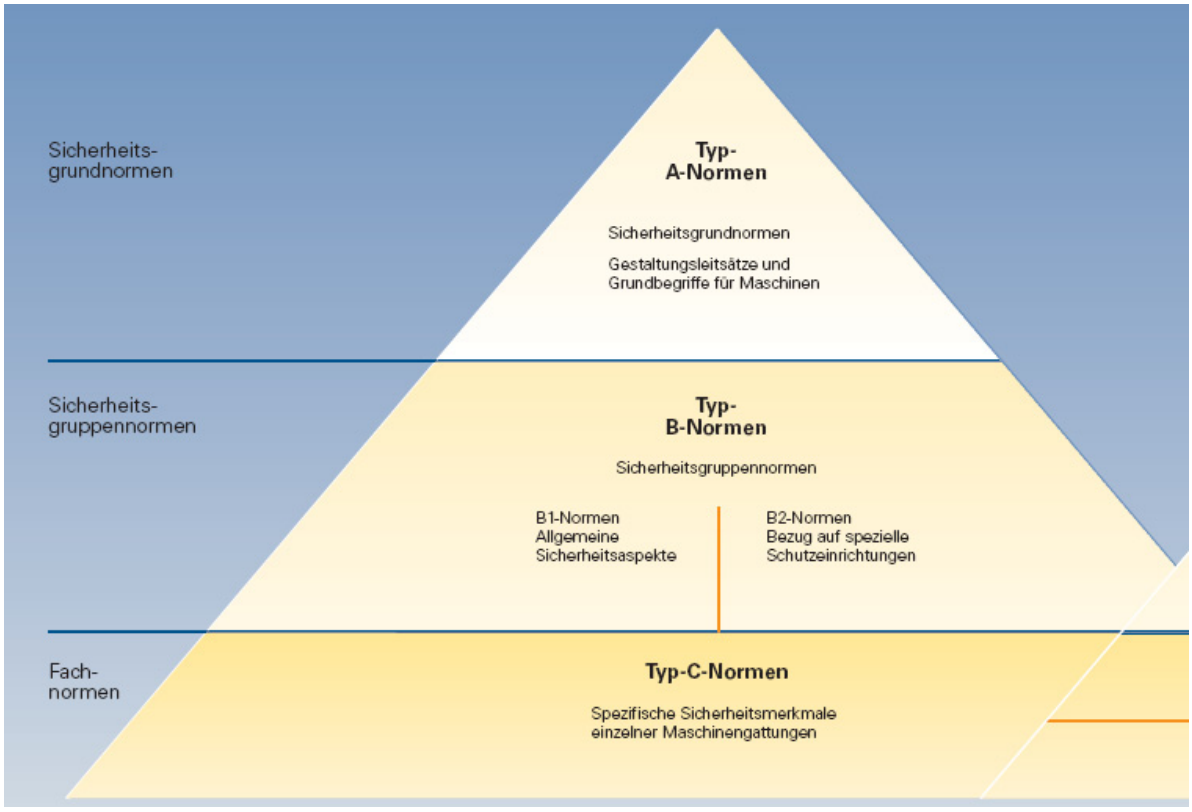
3.2 Vorschriften und Normen in der Europäischen Union (EU)

Um Produkte in den Verkehr bringen oder betreiben zu dürfen, müssen sie den grundlegenden Sicherheitsanforderungen der EU-Richtlinien entsprechen. Zur Erfüllung dieser Sicherheitsanforderungen können Normen sehr hilfreich sein.
Dabei ist in der EU zu unterscheiden zwischen Normen, die unter einer EU-Richtlinie harmonisiert sind und Normen, die zwar ratifiziert, aber nicht unter einer bestimmten Richtlinie harmonisiert sind, sowie sonstigen technischen Regeln, in den Richtlinien auch „nationale Normen“ genannt.
Ratifizierte Normen beschreiben den anerkannten Stand der Technik. D.h. der Hersteller kann durch ihre Anwendung nachweisen, dass er den anerkannten Stand der Technik erfüllt hat.

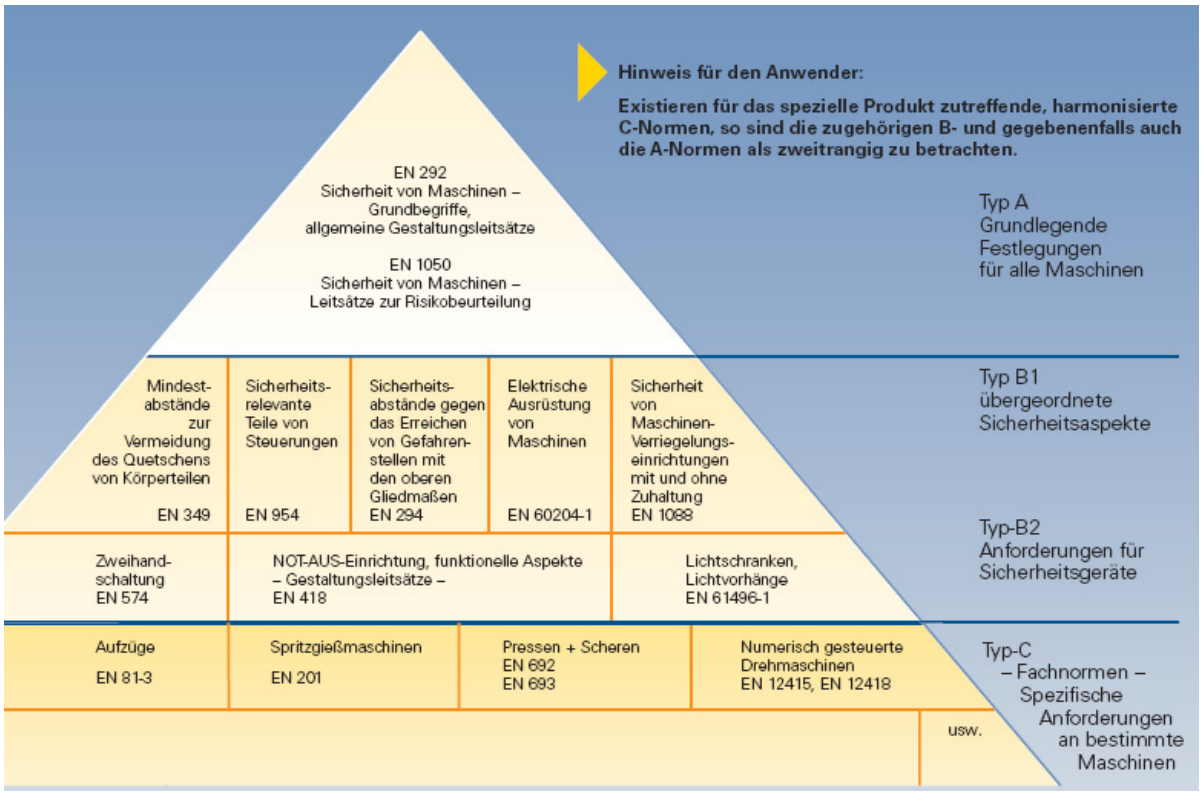
Das europäische Normenwerk für Sicherheit von Maschinen ist hierarchisch aufgebaut,
es gliedert sich in:

- A-Normen, auch Grundnormen genannt.
- B-Normen, auch Gruppennormen genannt.
- C-Normen, auch Produktnormen genannt.

Den Aufbau zeigen die beiden folgenden Darstellungen.



Das europäische Normenwerk für Sicherheit von Maschinen (Übersicht)



Das europäische Normenwerk für Sicherheit von Maschinen (Details)

Zu Typ-A-Normen/Grundnormen

A-Normen enthalten grundlegende Begriffe und Festlegungen für alle Maschinen. Dazu zählt die EN 292 „Sicherheit von Maschinen, Grundbegriffe, allgemeine Gestaltungsleitsätze.“ A-Normen richten sich primär an die Normensetzer von B- und C-Normen. Die dort niedergelegten Verfahren zur Risikominimierung können jedoch auch für den Hersteller hilfreich sein, wenn keine C-Normen vorliegen.

Zu Typ-B-Normen/Gruppennormen
Das sind alle Normen mit sicherheitstechnischen Aussagen, die mehrere Arten von Maschinen betreffen können. Auch die B-Normen richten sich primär an die Normensetzer für C-Normen. Sie können jedoch auch für Hersteller bei Konstruktion und Bau einer Maschine hilfreich sein, wenn keine C-Normen vorliegen.

Es wurde bei den B-Normen eine weitere Unterteilung vorgenommen, und zwar in:

- Typ-B1-Normen

für übergeordnete Sicherheitsaspekte, z.B. ergonomische Grundsätze, Sicherheitsabstände gegen das Erreichen von Gefahrquellen, Mindestabstände zur Vermeidung des Quetschens von Körperteilen.

- Typ-B2-Normen

für Sicherheitseinrichtungen sind bestimmt für verschiedene Maschinenarten, z.B. NOT-AUS-Einrichtungen, Zweihandschaltungen, Verriegelungen, berührungslos wirkende Schutzeinrichtungen, sicherheitsbezogene Teile von Steuerungen.

Zu Typ-C-Normen/Produktnormen
Hierbei handelt es sich um maschinenspezifische Normen z.B. für Werkzeugmaschinen, Holzbearbeitungsmaschinen, Aufzüge, Verpackungsmaschinen, Druckmaschinen u.ä. Das europäische Normenwerk ist so aufgebaut, dass, um Wiederholungen allgemeiner Aussagen zu vermeiden, die in Typ-A- oderTyp-B-Normen bereits enthalten sind, in den Typ- C-Normen soweit wie möglich darauf verwiesen wird.

Produktnormen enthalten maschinenspezifische Anforderungen. Die Anforderungen können unter Umständen von den Grund- und Gruppennormen abweichen. Für den Maschinenbauer hat die Typ-C-Norm/Produktnorm die absolut höhere Priorität. Er darf davon ausgehen, dass er damit die grundlegenden Anforderungen des Anhangs I der Maschinenrichtlinien einhält (automatische Vermutungswirkung).
Liegt für eine Maschine keine Produktnorm vor, so können Typ-B-Normen als Hilfen für den Bau einer Maschine herangezogen werden.

Um ein Mittel der Übereinstimmung mit den grundlegenden Anforderungen der Richtlinie bereitzustellen, werden für Maschinen oder Maschinengruppen nahezu aller Bereiche mit dem Mandat der EG-Komission harmonisierte Normen in technischen Komitees des CEN und CENELEC erarbeitet. An der Erarbeitung sind in erster Linie Vertreter der Hersteller der betreffenden Maschinen, der Aufsichtsbehörden wie Berufsgenossenschaften sowie der Betreiber beteiligt.
Eine Übersicht der wichtigsten Typ-A-, -B- und -C-Normen finden Sie in Teil 8. Eine vollständige Liste aller gelisteten Normen sowie der mandatierten Normungsvorhaben finden Sie im Internet unter:

http://www.NewApproach.org/directiveList.asp

3.3 Sicherheitsbezogene Funktionen in der Maschinensteuerung

Die sicherheitsbezogenen Funktionen umfassen neben den klassischen Funktionen

- Stillsetzen
- Handlungen im Notfall
- Verhindern unbeabsichtigten Anlaufs

inzwischen auch komplexere Funktionen wie

- Zustandsabhängige Verriegelungen
- Geschwindigkeitsbegrenzung
- Positionsbegrenzung
- Geschwindigkeitsabweichung u.ä.

Die klassischen Funktionen sind in EN 60204-1 definiert und wurden bisher im Allgemeinen durch einfache elektromechanische Bauteile realisiert. Sie können aber, ebenso wie komplexere Funktionen, auch durch programmierbare elektronische Systeme realisiert werden, wenn diese die relevanten Normen (IEC 61508, EN 954) erfüllen. Komplexe Funktionen, die z.B. das Verhalten drehzahlveränderbarer Antriebe betreffen, werden in draft IEC 61800- 5-2 beschrieben.

Ingangsetzen und Start: EN 60204 /11.98 Abschnitt 9.2.5.2

Das Ingangsetzen einer Maschine darf nur durch absichtliche Betätigung einer hierfür vorgesehenen Befehlseinrichtung möglich sein, wenn alle Schutzeinrichtungen angebracht und funktionsbereit sind. (Einschalten)
Dies gilt auch für das Wiederingangsetzen nach Stillstand, ungeachtet der Ursache für diesen Stillstand.

Gesteuertes Stillsetzen: EN 60204 /11.98 Abschnitt 3.11

Für das gesteuerte Stillsetzen einer Maschine muss diese mit einer Befehlseinrichtung zum sicheren Stillsetzen der gesamten Maschine ausgerüstet sein. (Ausschalten). Das gesteuerte Stillsetzen erfolgt durch Zurücksetzen des Befehlssignals auf „0“, sobald das Signal von der Steuerung erkannt worden ist. Die Speisespannung für die erforderlichen Maschinenstellglieder bleiben während des Stillsetzvorganges erhalten. Sind die Maschine oder sind ihre gefährlichen Teile stillgesetzt, so muss die Energieversorgung des Antriebs unterbrochen werden.
Der Befehl zum Stillsetzen der Maschine muss den Befehlen zum Ingangsetzen übergeordnet sein.

Ungesteuertes Stillsetzen: EN 60204 /11.98 Abschnitt 3.56

Das ungesteuerte Stillsetzen ist das Stillsetzen einer Maschinenbewegung durch Abschalten der Energie zu den Maschinen-Antriebselementen.

Allgemeine Stopp-Kategorien **FDIS IEC 60204 / 09.02 Abschnitt 9.2**

Zum Stillsetzen einer Maschine sind drei Stopp-Kategorien definiert, die den Steuerablauf für das Stillsetzen unabhängig von einer Notfallsituation beschreiben.

- Stopp-Kategorie 0: Stillsetzen durch sofortiges Ausschalten der Energie zu den Maschinen-Antriebselementen (d.h. ein ungesteuertes Stillsetzen)
- Stopp-Kategorie 1: Ein gesteuertes Stillsetzen, wobei die Energiezufuhr zu den Maschinen-Antriebselementen beibehalten wird, um das Stillsetzen zu erzielen. Die Energie wird erst dann unterbrochen, wenn der Stillstand erreicht ist.

(Zeitverzögerung bis 30 s für Risikokategorie 3, Zeitverzögerung bis 300s für Risikokategorie 1)

- Stopp-Kategorie 2: Ein gesteuertes Stillsetzen, bei dem die Energie zu den Maschinen-Antriebselementen beibehalten wird.

Stopp-Funktionen durch Schutzeinrichtungen: **EN 954-1 Abschnitt 5.2**

Eine durch Schutzeinrichtungen ausgelöste Stopp-Funktion muss die Maschine nach Betätigen dieser Funktion so schnell wie nötig in einen sicheren Zustand überführen. Diese Stopp-Funktion muss funktionellen Vorrang vor einem Betriebsstopp haben. (Überstromauslöser)

Stillsetzen im Notfall und Not-Aus-Funktionen: **EN 954-1 Abschnitt 5.3**

Für das Stillsetzen im Notfall muss jede Maschine mit einer oder mehreren Notbehelfseinrichtungen ausgerüstet sein, durch die jede unmittelbar drohende oder eintretende gefährliche Situation vermieden werden kann.

Bei einem zusammenwirkenden Maschinensystem müssen die sicherheitsbezogenen Teile die Möglichkeit haben, eine Not-Aus-Funktion an alle Teile des zusammenwirkenden Systems zu signalisieren.

Blockieren der Notbefehlseinrichtung:

Wenn die Notbefehlseinrichtung nach Auslösung eines Not-Aus-Befehls nicht mehr betätigt wird, muss dieser Befehl durch die Blockierung der Notbefehlseinrichtung bis zu ihrer Freigabe aufrechterhalten bleiben. (Einrasten)

Freigeben der Notbefehlseinrichtung:

Die Einrichtung darf nur durch eine geeignete Betätigung freigegeben werden. Durch die Freigabe darf die Maschine nicht wieder in Gang gesetzt, sondern nur das Wiederingangsetzen ermöglicht werden. (Quittieren)

Manuelle Rückstellung: **EN 954-1 Abschnitt 5.4**

Nach dem Einleiten eines Stopp-Befehls durch eine Schutzeinrichtung muss der Stopp-Befehl aufrechterhalten bleiben, bis sichere Bedingungen für einen erneuten Start gegeben sind.
Die Rückstellung der Sicherheitsfunktion von der Schutzeinrichtung hebt einen Stopp-Befehl auf. Falls dies in der Risikobeurteilung angezeigt ist, muss das Aufheben des Stopp-Befehls durch eine manuelle, getrennte und absichtliche Betätigung (Manuelle Rückstellung) bestätigt werden.
Die manuelle Rückstellung:

- muss über eine getrennte, handbetriebene Einrichtung der sicherheitsbezogenen Teile der Steuerung vorgenommen werden,
- muss sicherstellen, dass alle Sicherheitsfunktionen und Schutzeinrichtungen betriebsbereit sind; ist das nicht der Fall, darf eine Rückstellung nicht möglich sein,
- darf keine Bewegung oder keinen gefährlichen Zustand verursachen,
- muss durch absichtliche Betätigung erfolgen,
- muss die Steuerung auf die Annahme eines getrennten Anlaufbefehls vorbereiten,
- wird nur akzeptiert durch die Betätigung eines Freigabeschalters.

Start und erneuter Start: **EN 954-1 Abschnitt 5.5**

Wenn eine sicherheitsbezogene Einrichtung einen Befehl für einen Start oder einen erneuten Start erzeugt, hat der Start oder erneute Start nur dann automatisch zu erfolgen, wenn kein gefährlicher Zustand vorliegen kann. Diese Anforderungen für Start und erneuten Start sind auch für Maschinen einzuhalten, die ferngesteuert werden können.

Redundanz: **EN 60204 / 11.98 Abschnitt 3.44**

Redundanz ist die Anwendung von mehr als einem Gerät oder System um sicherzustellen, dass bei Ausfall der Funktion eines Gerätes oder Systems ein anderes verfügbar ist, um diese Funktion zu erfüllen.

Zweihandschaltungen: **EN 60204 / 11.98 Abschnitt 9.2.5.7**

- Typ I: Erfordert die Bereitstellung von zwei Steuergeräten und deren gleichzeitige Betätigung durch beide Hände und deren dauernde gleichzeitige Betätigung während des Gefahr bringenden Zustandes.
- Typ II: Erfordert das Loslassen beider Befehlsgeräte, bevor ein Maschinenbetrieb wieder gestartet werden kann.
- Typ III: Erfordert das gleichzeitige Betätigen beider Befehlsgeräte innerhalb einer Zeit von nicht mehr als 0,5s. Sollte diese Zeit überschritten werden, kann erst nach Loslassen beider Befehlsgeräte erneut gestartet werden.

Trennen von den Energiequellen:

Jede Maschine muss mit Einrichtungen ausgestattet sein, mit denen sie von jeder einzelnen Energiequelle getrennt werden kann (Hauptbefehlseinrichtung)
Diese Einrichtungen sind klar zu kennzeichnen. Sie müssen abschaltbar sein, falls eine Wiedereinschaltung für die gefährdete Person eine Gefahr verursachen kann.

Anforderungen an die Stellteile:
Deutlich sichtbare und zweckmäßig gekennzeichnete Stellteile müssen außerhalb der Gefahrenbereiche so angebracht sein, dass ein sicheres, unbedenkliches, schnelles und eindeutiges Betätigen möglich ist.
Die Stellteile müssen den vorhersehbaren Beanspruchungen standhalten und so gestaltet sein, dass unter Berücksichtigung der ergonomischen Prinzipien ihre Anordnung, ihre Bewegungsrichtung und ihr Widerstand mit der Steuerwirkung kompatibel ist. (Hohe Beanspruchungen beim Betätigen, wenn Schutzausrüstungen getragen werden (Handschuhe, Sicherheitsschuhe, usw.)

Anforderungen an die Anzeigevorrichtungen:
Jede Maschine muss mit Hinweisen und mit sicherheitsrelevanten Anzeigevorrichtungen (Signalanzeigen, Skalen, Hupe, Sirene, usw.) versehen sein.
Das Bedienungspersonal muss die Anzeigevorrichtungen vom Bedienungsstand aus einsehen können.
Vom Hauptbedienungsstand aus muss sich das Bedienungspersonal vergewissern können, das sich keine gefährdeten Personen in den Gefahrenbereichen aufhalten.

Muting: (Aufhebung) **EN 954-1 Abschnitt 5.9**
Unter Muting versteht man das sichere, automatische und vorübergehende Überbrücken einer berührungslos wirkenden Schutzeinrichtung (BWS), um z.B. Material in einen oder aus einem Gefahrenbereich zu transportieren (z.B. die erwünschte Passage von Paletten durch ein Lichtgitter). Über spezielle Sensoren wird der Muting-Zyklus von der Muting-Steuerung nur dann gestartet, wenn das Material durch das Schutzfeld transportiert wird. Die Anforderung der Sensoren muss so gestaltet sein, dass Personen nicht in der Lage sind, die Muting-Sensoren in dieser Form zu aktivieren. Personen lösen beim Zugang in den Schutzbereich das Abschalten der Gefahr bringenden Bewegung aus.

3.4 Farbkennzeichnung

3.4.1 Kennzeichnung von Leuchtmeldern und Drucktastern

Um Bedienungsfehler an einer Maschine möglichst auszuschließen ist es notwendig dem Bediener einheitliche klar definierte Bedien- und Beobachtungsfunktionen anzubieten.
Das Zusammenwirken zwischen Mensch und Maschine ist so zu erleichtern.
Zu den Maschinenkomponenten, die im Schnittstellenbereich Mensch – Maschine eingesetzt werden, zählen in erster Linie Schalter, Taster und Leuchtmelder. Die durchgängige eindeutige Kennzeichnung dieser Bedienelemente erfolgt durch farbliche Kennzeichnung, die einer konkreten Bedeutung zugeordnet sind. Dadurch ist gewährleistet, dass die Sicherheit des Bedienpersonals erhöht und die Bedienung und Erhaltung der Betriebsmittel / Anlagen erleichtert werden.

Die Farben für Drucktaster, die Bedeutung der Farben sowie Erklärungen und Anwendungsbeispiele werden in folgendem Bild angegeben.

Farbe	Bedeutung	Erklärung	Anwendungsbeispiele
ROT	Notfall	Bei gefährlichem Zustand oder im Notfall betätigen	NOT-AUS, Einleitung von NOT-AUS-Funktionen, bedingt für STOP/AUS
GELB	Anormal	Bei anormalem Zustand betätigen	Eingriff, um anormalen Zustand zu unterdrücken, Eingriff, um einen unterbrochenen automatischen Ablauf wieder zu starten
GRÜN	Sicher	Bei sicherer Bedingung betätigen oder im normalen Zustand vorzubereiten	START/EIN, hierfür jedoch bevorzugt WEISS
BLAU	Zwingend	Bei Zustand betätigen, der zwingende Handlung erfordert	Rückstellfunktion
WEISS	Keine spezielle Bedeutung zugeordnet	Für allgemeine Einleitung von Funktionen außer NOT-AUS (siehe auch Anmerkung)	START/EIN (bevorzugt), STOP/AUS
GRAU			START/EIN, STOP/AUS
SCHWARZ			START/EIN, STOP/AUS (bevorzugt)

Anmerkung: Wird eine zusätzliche Maßnahme der Kennzeichnung (z. B. Struktur, Form, Lage) zum Kennzeichnen von Drucktaster-Bedienteilen verwendet, dürfen dieselben Farben WEISS, GRAU oder SCHWARZ für verschiedene Funktionen verwendet werden, z. B. WEISS für START/EIN- und STOP/AUS-Bedienteile.

Farben für Drucktaster und ihre Bedeutung nach EN 60204-1 (VDE 0113 Teil 1): 06.93

Gemäß DIN EN 60204-1 (VDE 0113 Teil 1) sind folgende Hinweise zu beachten:

- Die bevorzugten Farben für START/EIN- Bedienteile sollten WEISS, GRAU oder SCHWARZ, vorzugsweise WEISS sein. GRÜN darf, ROT darf nicht verwendet werden.
- Die Farbe ROT muss für NOT-AUS-Bedienteile verwendet werden.
- Die Farben für STOP/AUS-Bedienteile sollten SCHWARZ, GRAU oder WEISS, vorzugsweise SCHWARZ sein. ROT ist ebenfalls erlaubt. GRÜN darf nicht benutzt werden.
- WEISS, GRAU und SCHWARZ sind die bevorzugten Farben für Drucktaster- Bedienteile, die wechselweise als START/EIN- und STOP/AUS-Drucktaster wirken. Die Farben ROT, GELB oder GRÜN dürfen nicht verwendet werden.
- WEISS, GRAU und SCHWARZ sind die bevorzugten Farben für Drucktaster- Bedienteile, die einen Arbeitsvorgang bewirken, während sie betätigt sind und den Betrieb beenden, wenn sie losgelassen werden (z. B. Tippen). Die Farben ROT, GELB und GRÜN dürfen nicht verwendet werden.
- Rückstell-Drucktaster müssen BLAU, WEISS, GRAU oder SCHWARZ sein. Falls sie auch als STOP/AUS-Taster wirken, werden die Farben WEISS, GRAU oder SCHWARZ bevorzugt, vorzugsweise SCHWARZ. GRÜN darf nicht benutzt werden.

Im folgenden Bild werden die Farben für Leuchtmelder, ihre Bedeutung in Bezug auf den Zustand der Maschine sowie Handhabung und Anwendungsbeispiele aufgeführt.

Farbe	Bedeutung	Erklärung	Handlung durch den Bediener	Anwendungs-beispiele
ROT	Notfall	Gefährlicher Zustand	Sofortige Handlung, um auf gefährlichen Zustand zu reagieren (z. B. durch Betätigung des NOT-AUS)	Druck/Temperatur außerhalb sicherer Grenzen, Spannungsfall, Spannungszusammenbruch, Überfahren einer Stop-Position
GELB	Anormal	Anormaler Zustand Bevorstehender kritischer Zustand	Überwachen und/ oder Eingreifen (z. B. durch Wiederherstellen der beabsichtigten Funktion)	Druck/Temperatur übersteigt normale Bereiche, Auslösen einer Schutzeinrichtung
GRÜN	Normal	Normaler Zustand	Optional	Druck/Temperatur innerhalb normaler Bereiche, Ermächtigung fortzufahren
BLAU	Zwingend	Anzeige eines Zustandes, der Handlung durch den Bediener erfordert	Zwingende Handlung	Anweisung, vorgegebene Werte einzugeben
WEISS	Neutral	Andere Zustände: darf verwendet werden, wenn Zweifel über die Anwendung von ROT, GELB, GRÜN oder BLAU bestehen	Überwachen	Allgemeine Informationen

Farben für Leuchtmelder und ihre Bedeutung nach EN 60204-1 (VDE 0113 Teil 1): 06.93

- Die Farbe GRÜN ist für Funktionen reserviert, die einen sicheren oder normalen Zustand anzeigen.
- Die Farbe GELB ist für Funktionen reserviert, die eine Warnung oder einen anormalen Zustand anzeigen.
- Die Farbe BLAU ist für Funktionen von zwingender Bedeutung reserviert.

Bei Leuchtdrucktastern gelten die Vorgaben zu Drucktastern und Leuchtmeldern. Bei Problemen mit der Zuordnung geeigneter Farben muss auf die Farbe WEISS zurückgegriffen werden.
Für NOT- AUS- Geräte darf die Farbe ROT nicht von der Beleuchtung abhängen.

3.4.2 Kennzeichnung von Leitungen

Bei der Kennzeichnung von Leitern sind durch die Norm EN 60204 größere Spielräume erlaubt. Sie schreibt nämlich vor, dass die „... Leiter an jeden Anschluss in Übereinstimmung mit der technischen Dokumentation identifizierbar sein müssen ...“.

Die Benummerung von Klemmen in Übereinstimmung mit dem Schaltplan genügt, wenn die Leitung visuell leicht verfolgbar ist. Bei umfangreichen Steuerungen empfiehlt es sich, sowohl den Leiter der Innenverdrahtung als auch den nach außen abgehenden Leiter so zu kennzeichnen, dass man nach dem Lösen später den Draht wieder an die richtige Klemme bringen kann. Es ist auch dort zu empfehlen, wo die Leiter für den Transport aufgetrennt werden müssen.

Mit der Formulierung in IEC 60204-1 1997, Absatz 14.2.1 Aderkennzeichnung, wollte das Normenkomitee folgende Punkte zum Ausdruck bringen:

- 1. Jeder einzelne Leiter muss identifizierbar sein, jedoch in dieser Absolutheit nur im Zusammenhang mit der Dokumentation. Es ist nicht gefordert, dass jeder Leiter für sich, ohne Dokumentation identifizierbar sein muss.
- 2. Die Art der Kennzeichnung und damit auch die Identifizierungsmethode sollte gegebenenfalls zwischen Hersteller und Betreiber vereinbart werden.

Es ist nicht Absicht der Norm, eine bestimmte Kennzeichnungsart zwingend weltweit vorzuschreiben. Aus Sicherheitsgründen können z.B. werksinterne Festlegungen eine höhere Priorität haben, um in Bereichen, die von demselben Personal betreut werden, Verwechslungen vorzubeugen. Diese Festlegungen können wegen des großen Geltungsbereiches der vorliegenden Norm von kleinen Einzelmaschinen (Massenprodukte) bis zu großen komplexen maschinellen Anlagen (Unikate) nicht verallgemeinert werden.
Primär muss die Sicherheit vor Montagefehlern durch entsprechende Prüfungen sichergestellt sein. Statt vieler Farben kann für die Innenverdrahtung eine einheitliche Farbe verwendet werden. Sie sollen wie folgt farblich gekennzeichnet sein:

- Schwarz für Hauptstromkreise für Wechsel- und Gleichstrom
- Rot für Steuerstromkreise für Wechselstrom
- Blau für Steuerstromkreise für Gleichstrom
- Orange für Verriegelungsstromkreise, die von einer externen Stromquelle versorgt werden.

Entschließt man sich zu einer reinen Farbkennzeichnung, so wird die obige Farbzuordnung empfohlen. Bindend vorgeschrieben ist lediglich die Farbe von Schutzleiter und Neutralleiter. Für alle anderen Leiter kann frei zwischen verschiedenen Methoden gewählt werden (Farbe, Ziffern oder Buchstaben; oder eine Kombination aus Farbe und Ziffern oder Farbe und Buchstaben).

Kennzeichnung des Schutzleiters

Der Schutzleiter muss durch Form, Anordnung, Kennzeichnung oder Farbe deutlich zu erkennen sein. Wenn Kennzeichnung nur durch Farbe erfolgt, dann muss es die Zweifarben- Kombination Grün/Gelb sein, die sich über die gesamte Leiterlänge erstrecken muss. Die Farbkennzeichnung Grün/Gelb ist ausschließlich dem Schutzleiter vorbehalten.

Kennzeichnung des Neutralleiters

Enthält ein Stromkreis einen farblich gekennzeichneten Neutralleiter, muss die Farbe Hellblau verwendet werden. Hellblau darf nicht zur Kennzeichnung von anderen Leitern verwendet werden, wenn die Gefahr der Verwechslung besteht. Fehlt ein Neutralleiter, darf ein hellblauer Leiter für andere Zwecke verwendet werden, aber nicht als Schutzleiter.

4 Risikobetrachtung und Identifizierung der Gefährdung

4.1 Allgemeine Risikobeurteilung / Sicherheitskategorien / Safety Integrity Level (SIL)

Die Risikobeurteilung ist eine Folge von Schritten, welche die systematische Untersuchung von Gefährdungen erlauben, die von Maschinen ausgehen. Wo notwendig, folgt einer Risikobeurteilung eine Risikoreduzierung. Bei Wiederholung dieses Vorgangs ergibt sich ein iterativer Prozess, mit dessen Hilfe Gefährdungen so weit wie möglich beseitigt werden können und entsprechende Schutzmaßnahmen getroffen werden können.

Die Risikobeurteilung umfasst die

- **Risikoanalyse**

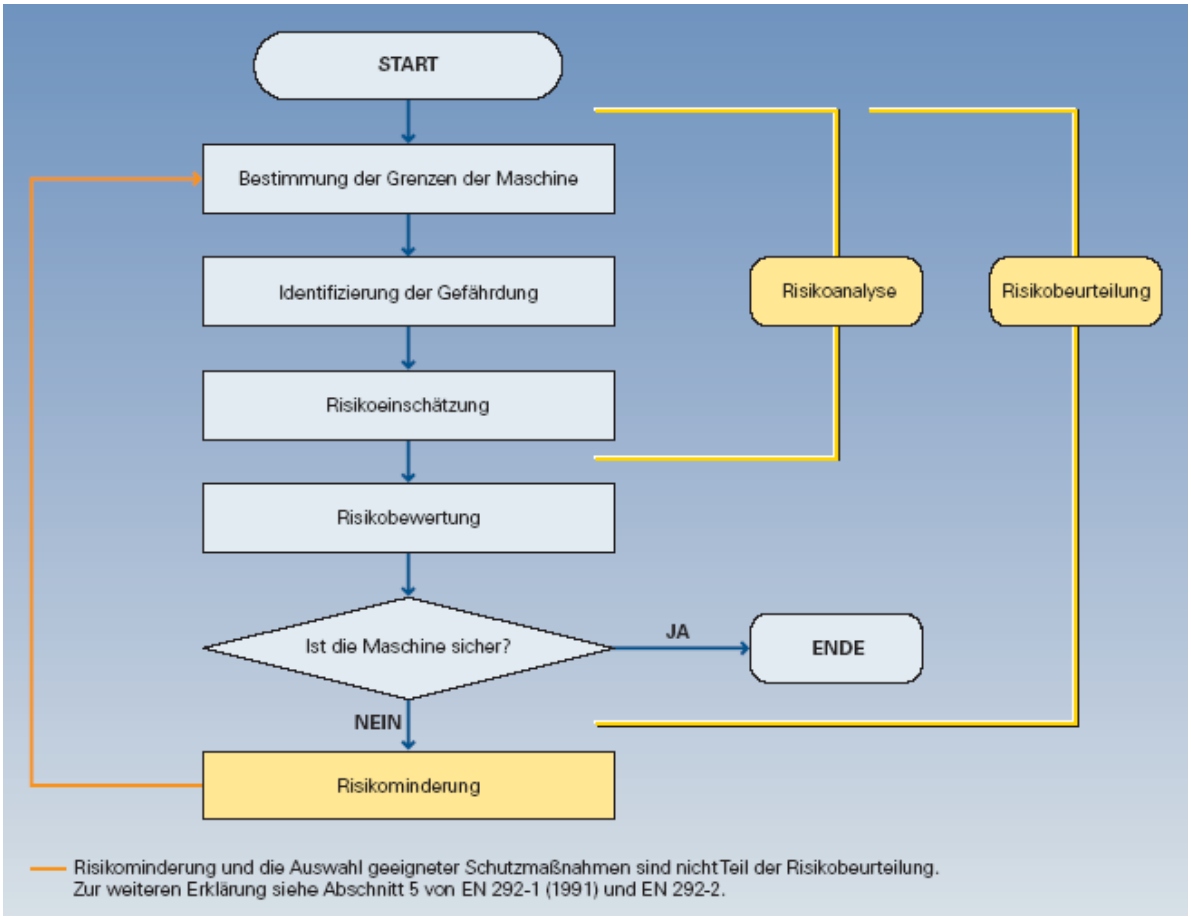
a) Bestimmung der Grenzen der Maschine (EN 292, EN 1050 Abs. 5)
b) Identifizierung der Gefährdungen (EN 292, EN 1050 Abs. 6)
c) Verfahren zur Risikoeinschätzung (EN 1050 Abs. 7)

- **Risikobewertung (EN 1050 Abs. 8)**

Gemäß dem iterativen Prozess zum Erreichen der Sicherheit erfolgt nach der Risikoeinschätzung eine Risikobewertung. Dabei muss entschieden werden, ob eine Risikominderung notwendig ist. Falls das Risiko weiter vermindert werden soll, sind geeignete Schutzmaßnahmen auszuwählen und anzuwenden.

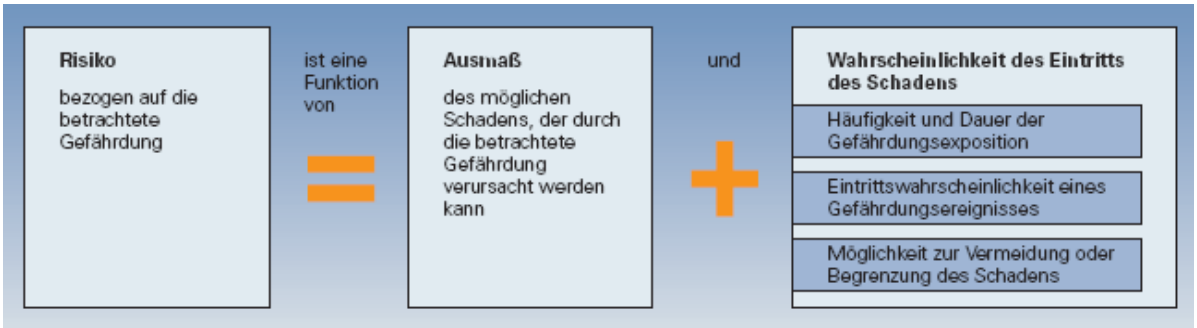
Die Risikobeurteilung ist dann zu wiederholen. Ist die erforderliche Sicherheit noch nicht erreicht, sind Maßnahmen zur Risikominderung erforderlich. Die Risikominderung muss durch geeignete Konzipierung und Realisierung der Maschine erfolgen, z.B. durch für Sicherheitsfunktionen geeignete Steuerung oder Schutzmaßnahmen (siehe dazu Abschnitt „Anforderungen der Maschinenrichtlinie“). Umfassen die Schutzmaßnahmen Verriegelungs- oder Steuerfunktionen, sind diese gemäß EN 954 zu gestalten. Bei Realisierung durch elektronische Steuerungen und Bussysteme ist außerdem IEC / EN 61508 zu erfüllen.

Diesen Vorgang nennt die Norm EN 1050 einen iterativen Prozess zum Erreichen der Sicherheit (siehe Bild unten).



Iterativer Prozess zum Erreichen der Sicherheit nach EN 1050

Als Hilfe zur Risikobewertung sind Risikoelemente definiert. Den Zusammenhang dieser Risikoelemente verdeutlicht die folgende Grafik.



Risikoelemente

Restrisiko (EN 1050)

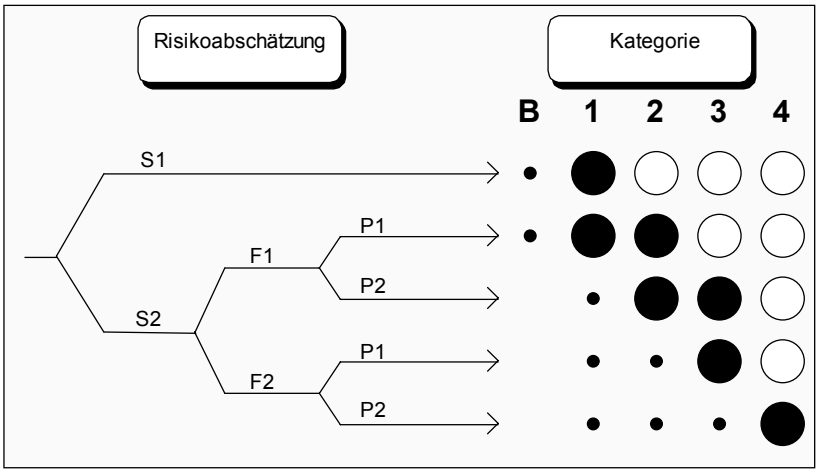
Sicherheit ist ein relativer Begriff unserer technisierten Welt. Sicherheit so zu realisieren, dass unter keinen Umständen etwas passieren kann, sozusagen die „Null-Risiko-Garantie“, ist leider nicht durchführbar. Das verbleibende Restrisiko ist definiert als: Risiko, das nach Ausführung der Schutzmaßnahmen verbleibt. Hierbei sind unter Schutzmaßnahmen alle Maßnahmen zur Risikominderung zu verstehen.

Risikominderung

Die Risikominderung einer Maschine kann, außer durch strukturelle Maßnahmen, auch durch sicherheitsrelevante Steuerungsfunktionen erfolgen. Für die Realisierung dieser Steuerungsfunktionen sind, abgestuft nach der Höhe des Risikos, besondere Anforderungen zu beachten, die in EN 954-1 und, für komplexe Steuerungen mit programmierbarer Elektronik, in IEC 61508 beschrieben sind.

Sicherheitskategorien

Die Anforderungen an sicherheitsrelevante Teile von Steuerungen sind, abgestuft nach der Höhe des Risikos, in Kategorien eingeteilt. In Anhang B der EN 954-1 wird ein Verfahren zur Auswahl der geeigneten Kategorie als Bezugspunkt für die Gestaltung der verschiedenen sicherheitsbezogenen Teile einer Steuerung empfohlen (siehe unten).



S Schwere der Verletzung:
1 : leichte Verletzung
2 : schwere Verletzung einschließlich Tod einer Person

F Aufenthalt im Gefahrenbereich:
1 : selten bis öfters und/oder kurze Dauer
2 : häufig bis dauernd und/oder lange Dauer

P Gefahrenabwendung:
1 : möglich unter bestimmten Bedingungen
2 : kaum möglich

B Kategorien für sicherheitsbezogene Steuerungsteile:
● : bevorzugte Kategorien für die Höhe des Risikos
• : mögliche Kategorien, die zusätzlich Maßnahmen erfordern
○ : überdimensionierte Maßnahmen in Bezug auf das zutreffende Risiko

Risikobewertung nach EN 954-1

Die sicherheitstechnische Anforderung an Steuerungen wird (unabhängig von der verwendeten Technologie) in **fünf** sicherheitstechnische Kategorien eingestuft (B, 1, 2, 3 und 4), die von einfachen Anforderungen (Auswahl der Komponenten) bis aufwendigen (rechtzeitiges Erkennen von Fehlern um Fehleranhäufung zu vermeiden) reichen.

	Kurzfassung der Anforderung	Risikobewertung	Prinzip der Sicherheit
B	Die sicherheitsbezogenen Bauteile der Steuerung müssen entsprechend dem Stand der Technik so ausgewählt werden, dass sie den zu erwartenden Betriebs- und Umgebungsbedingungen standhalten können.	• Wenn ein Fehler auftritt, kann er zum Verlust der Sicherheitsfunktion führen.	Überwiegend durch die Auswahl von Bauteilen.
1	Zusätzlich zu Kategorie "B": Verwendung von sicherheitstechnisch bewährten Komponenten und Prinzipien.	• Wie "B", aber mit einer höheren Zuverlässigkeit der Sicherheitsfunktion.	
2	Zusätzlich zu Kategorie "B und 1": Die Sicherheitsfunktionen müssen in geeigneten Zeitabständen durch die Steuerung geprüft werden.	• Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Prüfungsabständen führen. • Der Fehler wird durch die Prüfung erkannt.	Durch den Aufbau
3	Zusätzlich zu Kategorie "B und 1": Die Steuerungen müssen so gestaltet sein, dass: a) ein einzelner Fehler in der Steuerung nicht zum Verlust der Sicherheitsfunktionen führt (Einfehlersicherheit) und b) ein einzelner Fehler mit geeigneten Mitteln, dem Stand der Technik entsprechend, erkannt wird.	• Wenn ein einzelner Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. • Einige, aber nicht alle Fehler werden erkannt. • Eine Anhäufung unerkannter Fehler kann zum Verlust der Sicherheitsfunktion führen.	
4	Zusätzlich zu Kategorie "B und 1": Die Steuerungen müssen so gestaltet sein, dass: a) ein einzelner Fehler in der Steuerung nicht zum Verlust der Sicherheitsfunktionen führt (Einfehlersicherheit) und b) wann immer möglich, ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird oder wenn „b“ nicht möglich, eine Anhäufung von Fehlern nicht zu einem Verlust der Sicherheitsfunktionen führen darf.	• Wenn Fehler auftreten, bleibt die Sicherheitsfunktion immer erhalten. • Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern.	Durch den Aufbau

Beschreibung der Anforderungen für die Kategorien nach EN 954-1

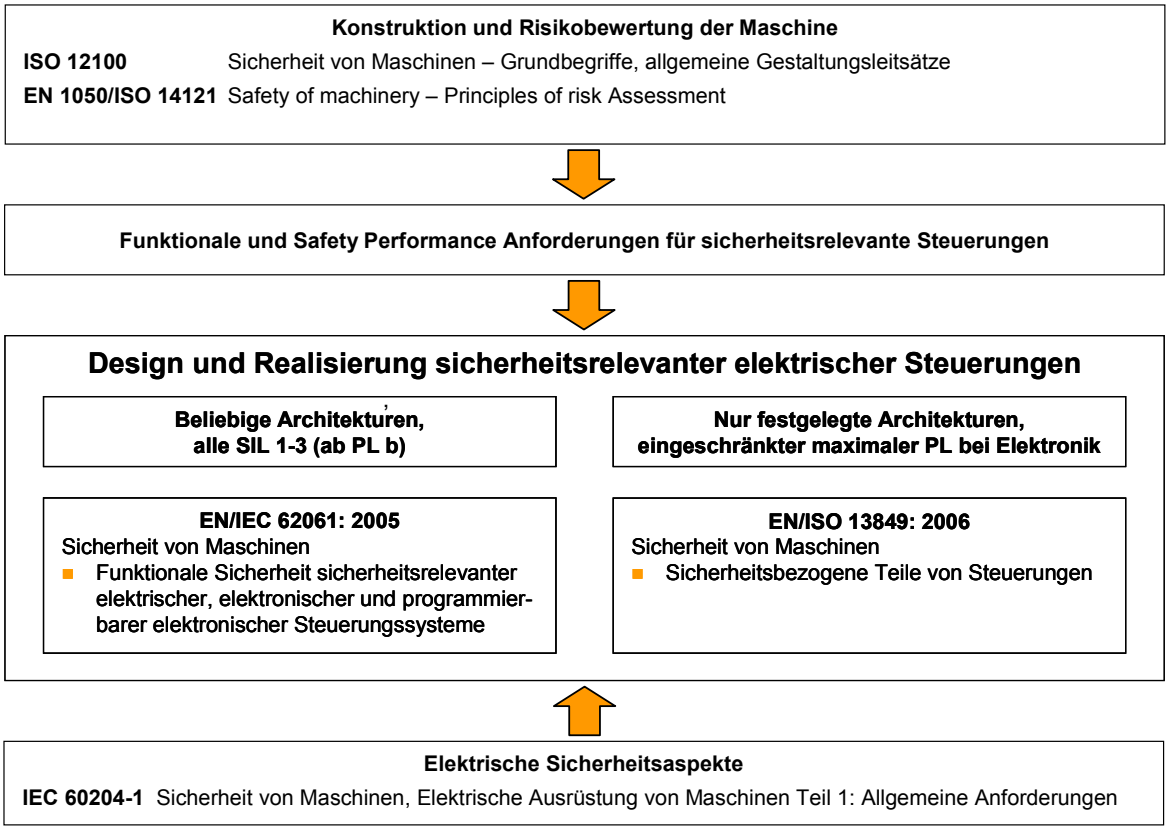
Wichtig ist dabei, dass alle Teile der Steuerung, die an der Ausführung der sicherheitsrelevanten Funktion beteiligt sind, diesen Anforderungen genügen. Nach der Realisierung der Steuerung ist es notwendig zu überprüfen, ob die Anforderungen der ausgewählten Kategorie erfüllt sind. Die Steuerung muss validiert werden. Die Einzelheiten, wie die Validierung durchzuführen ist und was dabei beachtet werden muss, sind im Teil 2 von EN 954 beschrieben.
In den Kategorien sind grundlegende Anforderungen zur Gestaltung von Steuerungen festgelegt, die sie robust gegen Ausfälle der Hardware machen.

Für komplexe Einrichtungen, insbesondere Steuerungen mit programmierbarer Elektronik, Bussysteme oder drehzahlveränderbare Antriebe, sind weitergehende Aspekte zu beachten, damit

- zufällige Ausfälle der Hardware beherrscht,
- systematische Fehler in der Hardware und der Software vermieden und
- systematische Fehler in der Hardware und der Software beherrscht werden, so dass sie ausreichend funktionssicher für sicherheitskritische Aufgaben sind. Die dazu notwendigen

Safety Integrity Level (SIL)

Safety Integrity Level (SIL) ist entstanden aus einer Weiterentwicklung der Basisnormen.



Für die Gültigkeit der neuen Normen gilt:

Die IEC EN 62061 ist seit Ende 2005 unter Maschinenrichtlinie harmonisiert und gelistet.
Diese kann hab heute ohne Verweis auf EN954-1 verwendet werden

Die EN ISO 13849-1 ist seit Oktober 2006 offiziell.

Es wird davon ausgegangen, dass die EN954-1 bis Ende 2009 zurückgezogen sein wird.
Bis dahin bleibt sie weiterhin gültig.

Maß der Safety Performance

Es gilt bei der Maschinensicherheit dass die geforderte sicherheitsbezogene Leistungsfähigkeit (Safety Performance) risikoabhängig ist.

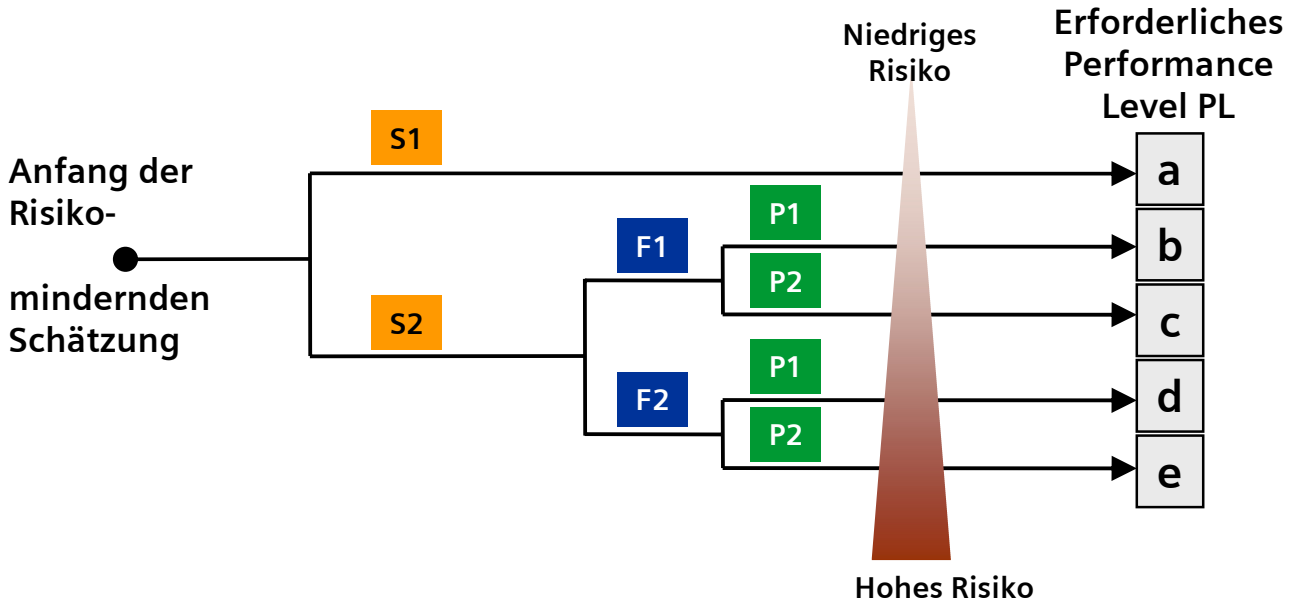
bisher: Kategorie
Diese Einstufung ist Lösungsabhängig ohne eindeutigen Bezug zur Höhe des Risikos

zukünftig: SIL (Safety Integrity level) / PL (Performance Level)
Diese sind Lösungsunabhängig mit eindeutiger Abstufung nach Höhe des Risikos

Performance level (PL)	Average probability of a dangerous failure per hour [1/h]	SIL [EN 61508-1 (IEC 61508-1)] for information
a	≥ 10^{-5} to < 10^{-4}	-
b	≥ 3 x 10^{-6} to < 10^{-5}	SIL 1
c	≥ 10^{-6} to < 3 x 10^{-6}	SIL 1
d	≥ 10^{-7} to < 10^{-6}	SIL 2
e	≥ 10^{-8} to < 10^{-7}	SIL 3

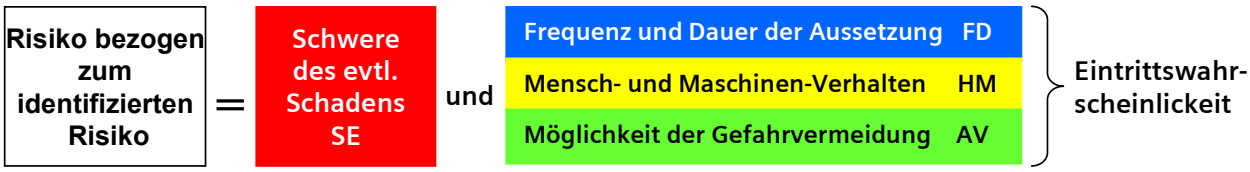
SIL und PL sind aufeinander abbildbar

Risikobeurteilung(II) / Risikograph EN ISO 13849-1: 2006



Risikoparameter:
S = Schwere der Verletzung
F = Häufigkeit und/oder Aufenthaltszeit in der Gefahrenstelle
P= Möglichkeit zur Vermeidung bzw. Begrenzung der Gefahr
a,b,c,d,e = Schätzung der sicherheitsbezogenen Performance Level

Risikobeurteilung(III) SIL assignment in draft IEC 62061, annex A



Auswirkungen	Schadens-ausmaß Se	Klasse Cl 3-4	5-7	8-10	11-13	14-15	Häufigkeit und/oder Aufenthaltsdauer Fr		Eintrittswahrscheinlichkeit des Gefährdungsereignis Pr		Möglichkeit zur Vermeidung Av	
Tod, Verlust von Auge oder Arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 h	5	sehr hoch	5		
Permanent, Verlust von Fingern	3		OM	SIL 1	SIL 2	SIL 3	> 1 h to ≤ 1 day	5	hoch	4		
Reversibel, medizinische Behandlung	2			OM	SIL 1	SIL 2	> 1 day to ≤ 2 weeks	4	möglich	3	unmöglich	5
Reversibel, Erste Hilfe	1				OM	SIL 1	> 2 weeks to ≤ 1 year	3	selten	2	selten	3
							> 1 year	2	unwahrscheinlich	1	möglich	1

Die auf folgender Seite abgebildete Grafik ist für die Risikobeurteilung auszufüllen.

Risikobeurteilung und Sicherheitsmaßnahmen

Dokument Nr.:
Teil:

Produkt: _____
Ausgestellt von: _____
Datum: _____

☐ Vorab Risibobeurteilung
☐ Zwischenriskobeurteilung
☐ Folgerisikobeurteilung

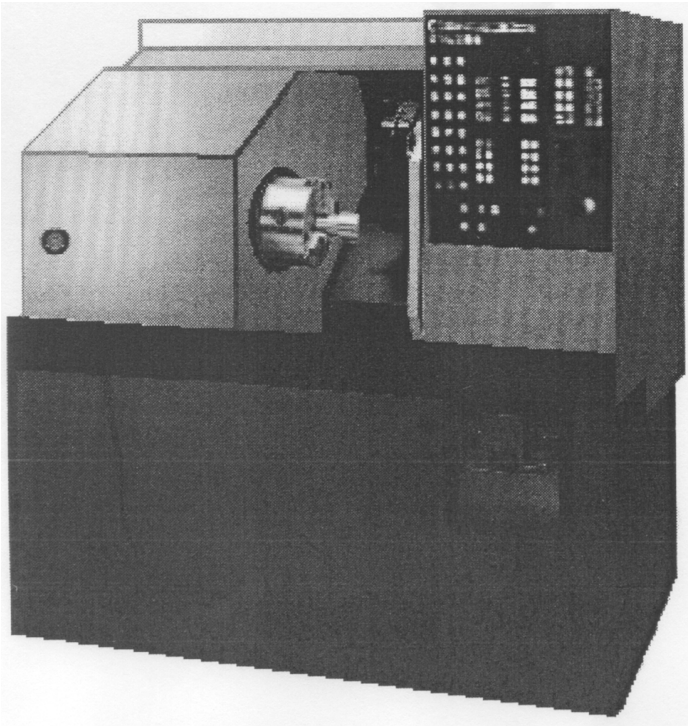
Auswirkungen	Schadens-ausmaß **Se**	Klasse **Cl** 3-4	5-7	8-10	11-13	14-15	Häufigkeit und/oder Aufenthaltsdauer **Fr**		Eintrittswahrscheinlichkeit des Gefährdungsereignis **Pr**				Möglichkeit zur Vermeidung **Av**	
Tod, Verlust von Auge oder Arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 h	5	sehr hoch	5				
Permanent, Verlust von Fingern	3		OM	SIL 1	SIL 2	SIL 3	> 1 h to ≤ 1 day	5	hoch	4				
Reversibel, medizinische Behandlung	2			OM	SIL 1	SIL 2	> 1 day to ≤ 2 weeks	4	möglich	3			unmöglich	5
Reversibel, Erste Hilfe	1				OM	SIL 1	> 2 weeks to ≤ 1 year	3	selten	2			selten	3
							> 1 year	2	unwahrscheinlich	1			möglich	1

Ser. Nr.	Gefahr Nr.	**Gefährdung**	**Se**	**Fr**	**Pr**	**Av**	**Cl**	**Sicherheitsmaßnahmen**	**Sicher**

Kommentare

4.2 Konkrete Risikobeurteilung anhand einer CNC-Maschine

Im folgenden Beispiel soll für eine Beispielapplikation CNC-Maschine eine Risikobeurteilung durchgeführt werden.



Das zu bearbeitende Werkstück wird vor jedem Arbeitsgang von Hand in die Spannzange eingelegt. Dann wird der Arbeitsvorgang gestartet und nach Ablauf des Bearbeitungsvorganges wird das Werkstück wieder von Hand entnommen.

Von folgenden Aspekten gehen Gefährdungen aus:

- Es entstehen scharfe Kanten am Werkstück
- Es entstehen scharfe Stahlspäne
- Es ist mit hohen Umdrehungsgeschwindigkeiten zu rechnen
- Beim vorzeitigen Griff auf das Werkstück können Kleidungsstücke erfasst werden
- Durch fliegende, heiße Späne kann es zu Augenverletzungen kommen

Bewertung der Schwere der Verletzung S1 oder S2:
Es ist mit irreversiblen Verletzungen zu rechnen: S2

S1: leichte (üblicherweise reversible) wieder verheilende Verletzungen
S2: schwere (üblicherweise irreversible) nicht wieder verheilende Verletzungen, einschließlich Tod

Bewertung der Häufigkeit und Dauer der Gefährdungsexposition F1 oder F2:
Es ist ein zyklischer Betrieb gegeben, die CNC-Maschine wird von Hand bestückt: F2

F1: der Zugang in den Gefahrenbereich ist selten oder nur von Zeit zu Zeit erforderlich
F2: der Zugang in den Gefahrenbereich ist aufgrund des zyklischen Betriebes häufig bis dauernd erforderlich

Bewertung der Möglichkeit zur Vermeidung der Gefährdung P1 oder P2:
Die Gefahrenstelle ist offen und auch während des Fertigungsprozesses zugänglich. Es ist immer mit einem Unfall zu rechnen: P2

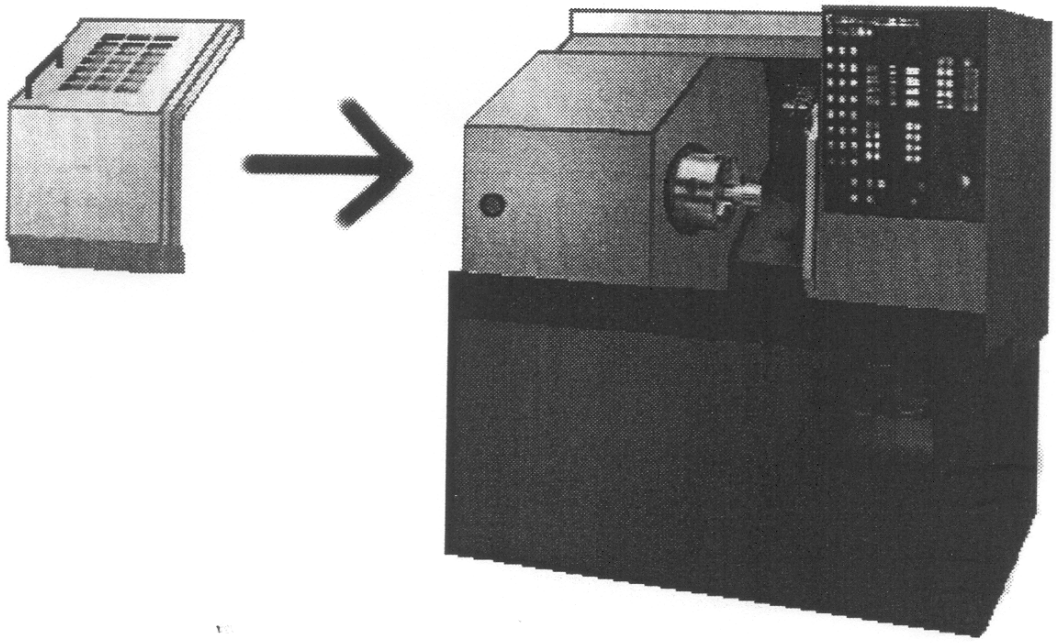
P1: eine Vermeidung ist unter bestimmten Bedingungen gegeben
P2: eine Vermeidung der Gefährdung ist kaum möglich

Das Ergebnis der Risikobeurteilung liefert die Risikokategorie B4.

4.3 Realisierung der Schutzvorkehrungen

Werden keine Sicherheitsvorrichtungen angebracht, bleibt das Unfallrisiko sehr hoch. Bei gleichmäßigen eintönigen Arbeiten ist schnell ein Flüchtigkeitsfehler zu erwarten. Statistisch ist beim Menschen jede tausendste Handlung eine Fehlhandlung. (z. B. Stolpern, Danebengreifen, Übersehen, falsches Einschätzen, usw.) Solche Fehlhandlungen werden aus Gewohnheit selbst nicht mehr registriert. Unter Berücksichtigung dieser Fakten kann ausgerechnet werden, wie lange es dauert, bis es zu einem Unfall kommt.

Nach dem Produkthaftungsgesetz wird dem Hersteller oder Betreiber einer Maschine nach einem Arbeitsunfall ein Verschulden unterstellt.



Hier besteht Handlungsbedarf für eine Schutzvorrichtung! Möglichkeiten sind:

Schutz durch feste Verdeckungen = Schutzgitter:
Durch Schutzgitter werden Bereiche abgegrenzt. Ein Zugang in den gefahrbringenden Bereich wird verhindert.

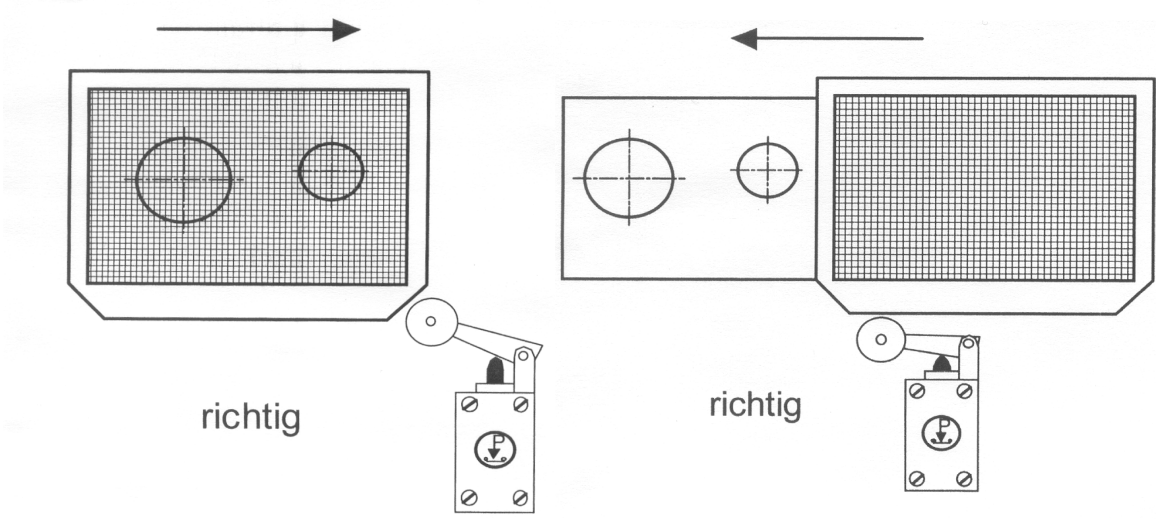
Schutz durch bewegliche Verdeckungen = Schutztür:
Eine Schutztür bietet abhängig vom Arbeitsablauf einen Zugang in einen gefahrbringenden Bereich. Erforderlich ist die Stellungs-Überwachung der Schutztür. EN 1088

Schutz durch berührungslose Verdeckung = Lichtgitter:
Ein Lichtgitter toleriert über die Muting- Funktion normale Arbeitsabläufe, verhindert aber gefahrbringende Situationen für Personen. Erforderlich ist ein konkreter Abstand zur Gefahrenquelle, der die Nachlaufzeit des Antriebs und die Personengeschwindigkeit berücksichtigt.

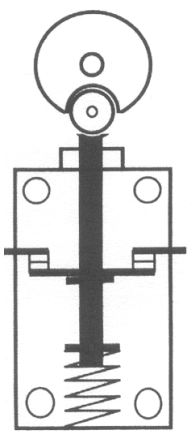
Schutz durch bewegliche Verdeckung überwacht durch sicherheitsgerechte Positionstaster in den Kategorien B1 und B2:
Es wird ein Positionstaster an der Verdeckung installiert

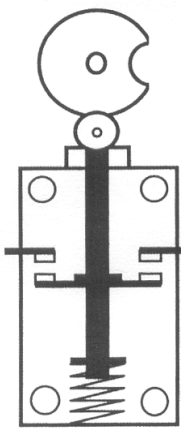
Tasterpositionen und Tasterfunktionen bei beweglichen Verdeckungen:

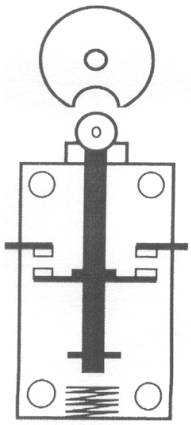
Ein Positionsschalter ist zur Überwachung der beweglichen Verdeckung angebracht. Ist die Gefahrenquelle nicht abgedeckt, muss der Positionsschalter betätigt sein!

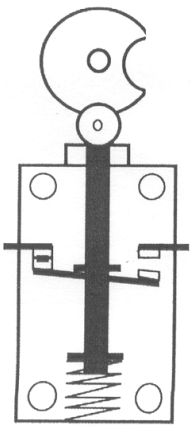


Zwangsbetätigter Öffnerkontakt:
Der Kontakt des Positionsschalters muss eine Öffnerfunktion mit Zwangsbetätigung haben:





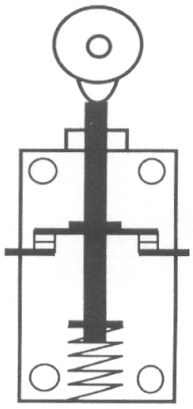


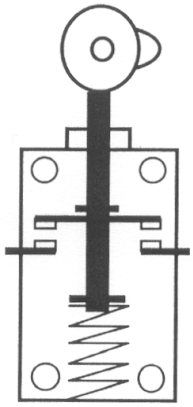


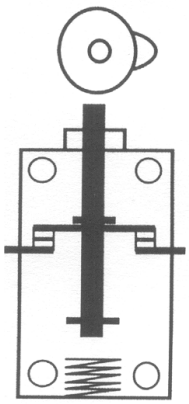
Zwangsbetätigter Öffnerkontakt:
Der Kontakt wird durch Betätigung geöffnet

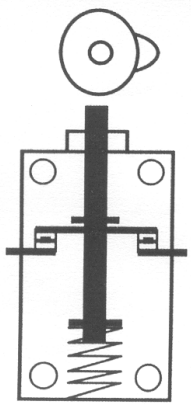
Öffnerfunktion auch bei Federbruch, oder bei Verschweißen

Normaler Schließerkontakt:
Die normale Schließerfunktion ist nicht zwangsbetätigt:





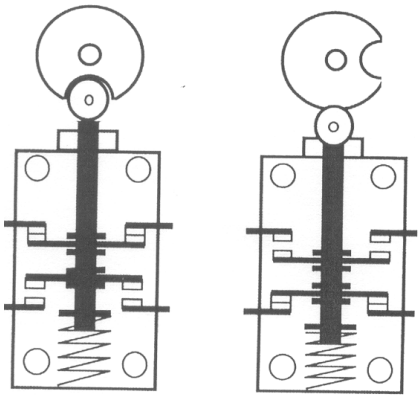




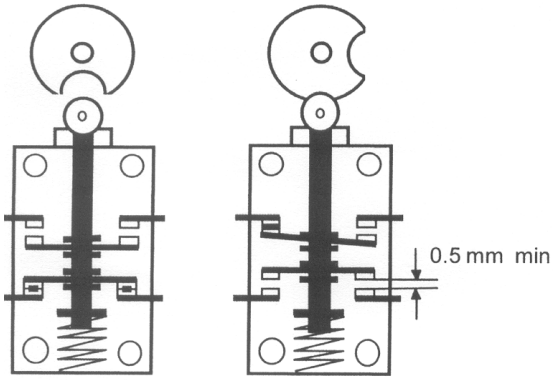
Normaler Schließerkontakt:
Kontakt wird durch Federkraft geöffnet

Kontakt bleibt bei Federbruch und bei Verschweißen geschlossen

Zwangsgeführter Positionstaster mit Öffner- und Schließerkontakt:
Ist der Positionstaster mit Öffner- und Schließerkontakt bestückt, kann der Schließerkontakt als Stellungsüberwachung des Öffnerkontakts verwendet werden. Es ist sicherzustellen, dass im Fehlerfall Öffner und Schließer zu keinem Zeitpunkt gleichzeitig geschlossen sind.



Öffner und Schließer in Ruhe- und in zwangsgeführter Position



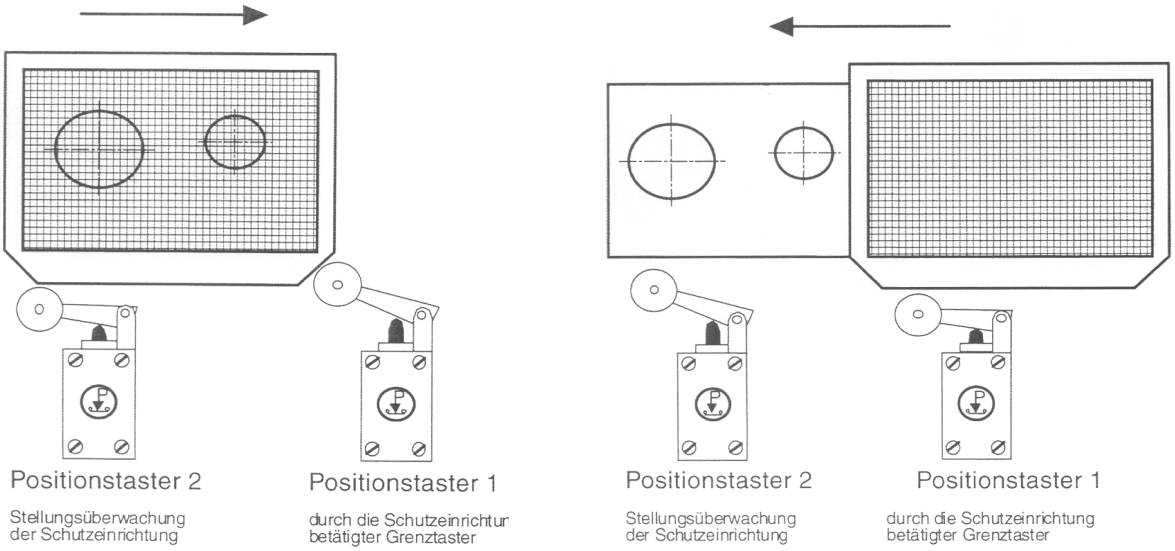
Nach Verschweißen des Schließerkontaktes bleibt der Öffnerkontakt offen
Nach Verschweißen des Öffnerkontaktes wird dieser zwangsgeöffnet und der Schließer bleibt offen

Kennzeichen sicherheitsgerechter Positionstaster:

Sicherheitsgerechter Positionstaster

Zwangsgeführter Kontakt

Schutz durch sicherheitsgerechte Positionstaster in den Kategorien B3 und B4:
In den Risikokategorien B3 und B4 müssen zwei mechanisch betätigte Positionstaster an der Verdeckung installiert werden. Ein einzelner Fehler darf nicht zum Verlust der Sicherheitsfunktion führen.



Für die Kategorie B3 ist eine einkanalige Ausführung erforderlich:
Positionstaster 1 wird zwangsläufig betätigt und beinhaltet einen zwangsbetätigten Öffner.
Positionstaster 2 wird nicht zwangsläufig betätigt und beinhaltet einen Schließerkontakt.

Für die Kategorie B4 ist eine zweikanalige Ausführung erforderlich:
Positionstaster 1 wird zwangsläufig betätigt und beinhaltet einen zwangsöffnenden Kontakt und einen Schließerkontakt zur Stellungsüberwachung des Positionstasters.
Positionstaster 2 wird nicht zwangsläufig betätigt und dient der Stellungsüberwachung der Schutztür. Ist auch dieser mit einem Öffner- und Schließerkontakt bestückt, so wird nicht nur die Schutztür, sondern auch der Positionstaster auf Stellungssicherheit überwacht.

5 Safety Integrated mit SIMATIC S7 Safety SPS

5.1 Aufbau der SIMATIC S7-300 CPU 315F- 2 PN/DP

Die CPU 315F basiert auf einer Standard- CPU (F steht hier für fehlersicher), deren Betriebssystem um verschiedene Schutzmechanismen erweitert wurde, um die Abarbeitung sicherheitsgerichteter Anwenderprogramme zu ermöglichen.
Dies wird für den Aufbau eines fehlersicheren Automatisierungssystems in Anlagen mit erhöhten Sicherheitsanforderungen benötigt. Einsatzbereich ist vorrangig in der Fertigungstechnik.
Die dezentralen Peripheriegeräte ET 200S PROFIsafe mit fehlersicheren Peripheriebaugruppen sind sowohl an die integrierten PROFIBUS DP / PROFINET- Schnittstellen als auch über externe PROFIBUS/PROFINET- CPs anschließbar. Die sicherheitsgerichtete Kommunikation erfolgt über PROFIBUS DP /PROFINET mit *PROFI*safe- Profil.

Technische Daten der CPU 315F-2 PN/DP:

- Die CPU 315F-2 PN/DP ist eine CPU die mit 2 integrierten Schnittstellen ausgeliefert wird.
- Die erste Schnittstelle ist eine kombinierte MPI/PROFIBUS-DP– Schnittstelle, die am PROFIBUS DP als Master oder Slave für den Anschluss von dezentraler Peripherie/Feldgeräten mit sehr schnellen Reaktionszeiten eingesetzt werden kann. Des weiteren kann Die CPU hier über MPI oder auch über PROFIBUS DP programmiert werden
- Die zweite Schnittstelle ist eine integrierten PROFINET- Schnittstelle. Diese ermöglicht den Einsatz der CPU als PROFINET IO- Controller für den Betrieb von dezentraler Peripherie an PROFINET. Über diese Schnittstelle kann die CPU ebenfalls programmiert werden!
- An beiden Schnittstellen können auch fehlersichere Peripheriegeräte mit *PROFI*safe- Profil eingesetzt werden.
- 1-Bus-Konzept, Übertragung von F-Signalen und Standard-Signalen über ein Busmedium (PROFIBUS DP oder PROFINET)
- Fehlersichere Peripheriebaugruppen der ET 200M/S/eco dezentral anschließbar
- Gemischter Aufbau von F-Baugruppen und Standardbaugruppen in einer Station
- Anschluss von Feldgeräten anderer Hersteller möglich.
- Standard-Baugruppen für nicht sicherheitsgerichtete Anwendungen sowohl zentral wie dezentral betreibbar
- Erfüllt Sicherheitsanforderungen bis SIL 3 nach IEC 61508, AK 6 nach DIN V 19250 und Kat. 4 nach EN 954-1
- Standard- als auch sicherheitsrelevante Aufgaben mit nur einer CPU lösbar

Sicherheitskonzept

Die Sicherheitsfunktionen der CPU 315F sind im F-Programm der CPU und in den fehlersicheren Signalbaugruppen enthalten. Die fehlersicheren Baugruppen können in den dezentralen Peripheriesystemen ET 200M und ET 200S verwendet werden

Die fehlersicheren Signalbaugruppen überwachen Ausgangs- und Eingangssignale durch Diskrepanzanalysen und Testsignalaufschaltungen.
Die CPU überprüft den ordnungsgemäßen Betrieb der Steuerung durch regelmäßige Selbsttests, Befehlstests sowie logische und zeitliche Programmlaufkontrolle. Zusätzlich wird die Peripherie durch Anforderung von Lebenszeichen kontrolliert.
Wird ein Fehler im System diagnostiziert, wird dieses in einen sicheren Zustand gefahren.
Zum Betrieb der CPU 315F ist keine F- Runtime Lizenz erforderlich.

Zusätzlich können, neben den fehlersicheren Baugruppen, auch Standard-Baugruppen eingesetzt werden.
Dadurch ist es möglich, ein vollintegriertes Steuerungssystem für eine Anlage aufzubauen, in der neben sicherheitsgerichteten auch Standard- Bereiche existieren.
Die gesamte Anlage wird mit den gleichen Standard- Werkzeugen projektiert und programmiert.

Der SIMATIC S7-300F erschließen sich damit auch Automatisierungsbereiche, die noch vor wenigen Jahren ausschließlich konventioneller elektromechanischer Steuerungstechnik vorbehalten waren, z.B. Automobilrohbau mit Pressen und Robotern, Feuerungstechnik, Personentransport in Seilbahnen und nicht zuletzt die Prozessautomatisierung.
Die CPU 315F-2 PN/DP erfüllt folgende Sicherheitsanforderungen:

- Sicherheitsanforderungsklasse: SIL 1 bis SIL 3 nach IEC 61508
- Kategorie: 2 bis 4 nach EN 954-1
- Anforderungsklasse: AK 1 bis AK 6 nach DIN V 19250/DIN V VDE 0801

Reaktionszeiten

Worst- Case- Reaktionszeiten lassen sich über eine mitgelieferte Excel-Tabelle (s7cotia.xls) während der Projektierungsphase abhängig von der Anzahl der fehlersicheren Signale und des Programmumfangs berechnen.
In dieser Tabelle befinden sich genaue Angaben zu Befehl-Bearbeitungszeiten sowie weitere F-relevante Informationen.

Diagnose- und Meldekonzept

Die CPU 315F-2 PN/DP bietet die gleichen Diagnose- und Meldefunktionen wie eine Standard-SIMATIC- SPS. Dabei bestehen hinsichtlich Diagnose keine Einschränkungen bei der Auswahl der Geräte.

Programmierung

Die Programmierung der CPU 315F erfolgt wie bei den anderen SIMATIC S7-Systemen. Das Anwenderprogramm für nicht fehlersichere Anlagenteile wird mit den bewährten Programmierwerkzeugen von STEP 7, erstellt.
Für die Programmierung der sicherheitsgerichteten Programme ist das Softwarepaket “S7 Distributed Safety V5.4” unerlässlich. Es enthält alle Elemente, die Sie zum Engineering benötigen.

Die Programmierung für die CPU 416F-2 erfolgt mit den STEP 7-Sprachen F-KOP und F-FUP. Hier können Sicherheitsfunktionen wie:

- frei programmierbare sichere Verknüpfung von Sensoren mit Aktoren
- selektive sichere Abschaltung von Aktoren

realisiert werden

Der Funktionsumfang bezüglich Operationen und Datentypen ist dabei eingeschränkt.
Durch eine spezielle Vorgabe bei der Kompilierung wird ein sicherheitsgerichtetes, passwortgeschütztes Programm erzeugt. Neben dem fehlersicheren Programm kann auf einer CPU parallel auch ein Standardprogramm ablaufen (Koexistenz), das keinen Einschränkungen unterliegt.

Zusätzlicher Bestandteil dieses Softwarepakets ist die F-Bibliothek mit vorgefertigten und vom TÜV abgenommenen Programmierbeispielen für sicherheitsgerichtete Funktionen. Diese Programmierbeispiele können vom Anwender verändert werden; die Änderungen müssen dann aber neu zertifiziert werden.

Optionspaket S7 Distributed Safety

Das Paket enthält alle erforderlichen Funktionen und Bausteine zur Erstellung des F-Programms.
Damit **„S7 Distributed Safety V5.4“** abläuft, muss **STEP 7 ab V5.3+SP3** auf dem PG/PC geladen sein
Das F-Programm mit den Sicherheitsfunktionen wird in F-FUP oder F-KOP oder mit speziellen Funktionsbausteinen aus der F-Bibliothek verschaltet. Die Verwendung von F-FUP oder F-KOP vereinfacht die Projektierung und Programmierung der Anlage und, durch die anlagenübergreifende, einheitliche Darstellung, auch die Abnahme. Der Programmierer kann sich ganz auf die Projektierung der sicherheitsgerichteten Anwendung konzentrieren, ohne zusätzliche Werkzeuge einsetzen zu müssen.

Kommunikation

Die CPU 315F-2 PN/DP besitzt 2 Schnittstellen. Eine davon kann am PROFIBUS DP als Master konfiguriert werden, die andere am PROFINET als Controller. Dies ermöglicht einen dezentralen Automatisierungsaufbau mit hoher Geschwindigkeit bei der Datenübertragung.
Die dezentrale Peripherie wird aus Anwendersicht wie zentrale Peripherie behandelt (gleiche Projektierung, Adressierung und Programmierung).

Die Kommunikation zwischen dezentralen Peripheriegeräten ET 200S / ET 200M mit fehlersicheren Peripheriebaugruppen und CPU erfolgt über die Profile PROFIBUS DP oder PROFINET.

Das speziell entwickelte PROFIBUS- Profil *PROFI*safe erlaubt die Übertragung von Nutzdaten der Sicherheitsfunktion innerhalb des Standard-Datentelegramms. Zusätzliche Hardware-Komponenten, z.B. spezielle Sicherheitsbusse, sind nicht erforderlich. Die notwendige Software wird entweder in den Hardware-Komponenten als Erweiterung des Betriebssystems integriert oder als zertifizierter Software-Baustein in die CPU nachgeladen.
Die Daten werden gemäß dem PROFIsafe Profil verkapselt, so dass diese Daten unbeeinflusst von anderen nicht sicherheitsgerichteten Teilnehmern am Bus über den Standardfeldbus übertragen werden können.

Für den Einsatz von Standard-Baugruppen für nicht sicherheitsgerichtete Anwendungen sowohl zentral
wie dezentral bestehen keinerlei Einschränkungen.

Generische Treiber ermöglichen den direkten Anschluss von Feldgeräten anderer Hersteller an den PROFIBUS sowie auch an das PROFINET.

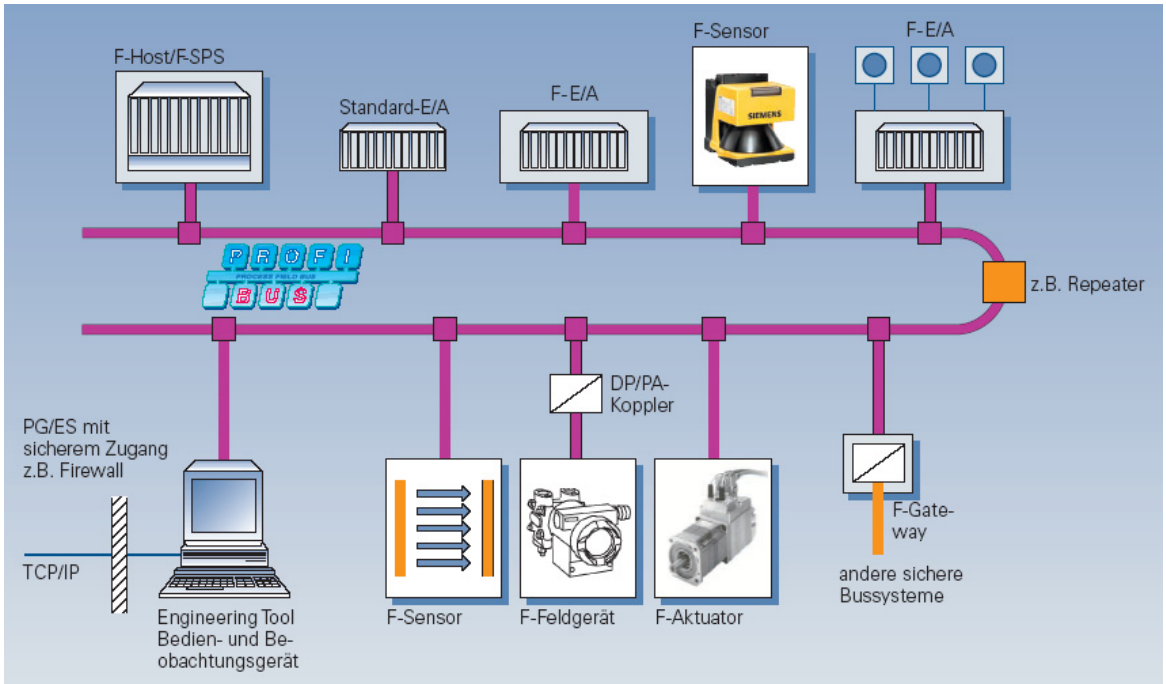
5.2 Fehlersichere Kommunikation mit PROFIsafe

Mit PROFIsafe sicher kommunizieren über PROFIBUS-DP / PROFINET

Die PROFIBUS- Nutzerorganisation (PNO) hat bereits im Frühjahr 1999, als Ergebnis eines Arbeitskreises, Richtlinien für die sichere Kommunikation auf dem Standard- PROFIBUS unter dem geschützten Markennamen PROFIsafe veröffentlicht, die von BIA (Berufsgenossenschaftliches Institut für Arbeitssicherheit) und TÜV durch positive technische Berichte bestätigt wurden.
Ziel des Arbeitskreises war es von Anfang an, möglichst viele Partner an der Definition und der Lösungsfindung zu beteiligen und die Ergebnisse in einer offenen Weise zur Verfügung zu stellen. So sind, neben Herstellern von Sicherheitssystemen, mehr als 25 namhafte nationale und internationale Hersteller von sicheren Sensoren und Aktoren, Werkzeugmaschinenfabriken, Endanwender und Universitätsinstitute vertreten.
Zwischen- und Endergebnisse wurden ständig mit dem TÜV und dem BIA abgestimmt. Bedeutende Beiträge kamen vom Verein Deutscher Werkzeugmaschinenfirmen (VDW), der im DESINA- Projekt die Entwicklung der Sicherheitstechnik konzeptionell beeinflusst. Über die gemeinsame Betrachtung von Sicherheitsszenarien ist quasi ein „normiertes“ vollständiges Anforderungsprofil für dezentrale Sicherheitstechnik entstanden, an dem das PROFIsafe- Konzept stets gemessen werden konnte.

Koexistenz von PROFIsafe und PROFIBUS- Teilnehmern am gleichen Kabel

Die hauptsächliche Vorgabe bei der Definition des PROFIsafe- Profils war die rückwirkungsfreie Koexistenz der sicherheitsgerichteten und der Standardkommunikation auf ein und demselben Buskabel.



Koexistenz von PROFIsafe- und PROFIBUS-Teilnehmern am gleichen Kabel

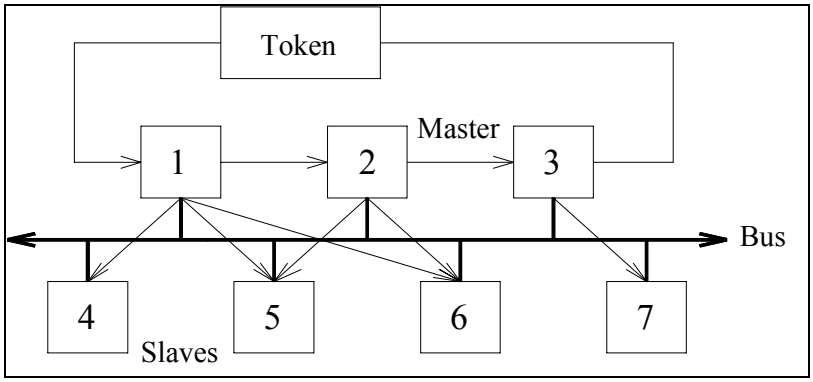
Weiterhin sollte die erforderliche Sicherheit auf einem 1-kanaligen Kommunikationssystem möglich sein, jedoch der optionale Weg zu erhöhter Verfügbarkeit, durch Redundanz der Nachrichtenkanäle, nicht verbaut werden. PROFIsafe setzt daher auf den eingeführten Standard-Kommunikationskomponenten wie Kabeln, ASICs und Softwarepaketen auf.

Grundsätzlich bestehen auch keine neuen Einschränkungen hinsichtlich Baudrate, Zahl der Busteilnehmer oder der Übertragungstechnik, sofern die geforderten Reaktionszeiten der Automatisierungsaufgabe dies jeweils zulassen. Es gelten die technischen von PROFIBUS DP.

Die folgenden Parameter sind für den PROFIBUS DP festgelegt:

PROFIBUS DP ist ein Multimastersystem bei dem die Buszuteilung nach dem Verfahren 'Token-Passing mit unterlagertem Master- Slave' erfolgt.

Die Sendeberechtigung wird hier durch ein „hybrides" Buszugriffsverfahren geregelt.
Hier kommen zwei Verfahren zur Anwendung, das **Token- Passing**- und das **Master/ Slave**-Verfahren.
Beim Master/Slave- Verfahren besitzt der alleinige Master das Recht des Buszugriffes. Die passiven Slaves dürfen nur auf Befehl des Masters antworten.
Anders ist dies beim Token- Passing- Verfahren. Hier wird das Zugriffsrecht über den „Token" zugewiesen und den einzelnen aktiven Teilnehmern nacheinander zugeteilt. Nur der Master, der den Token besitzt , kann auf den Bus zugreifen und mit den anderen aktiven und passiven Teilnehmern kommunizieren.



Darstellung des hybriden Zugriffverfahrens

So werden zwei wichtige Forderungen an den Bus realisiert:

- Automatisierungsgeräte mit Eigenintelligenz bekommen genug Zeit um ihre Kommunikationsaufgaben durchzuführen (durch Token- Passing- Verfahren).
- Der Datenaustausch zwischen den Automatisierungsgeräten mit der einfachen Prozessperipherie (E/A-Ebene) wird unter Echtzeitbedingungen realisiert (durch Master/Slave- Verfahren).

Typische Zykluszeiten werden mit 5 -10 ms angegeben.

Maximal 127 Teilnehmer mit einer Telegrammlänge von 0 - 246 Byte Nutzdaten können angeschlossen werden.

Als Standard-Übertragungsgeschwindigkeiten sind 9,6 KBaud / 19,2 KBaud / 93,75 KBaud / 187,5 KBaud / 500 KBaud / 1,5 MBaud / 3 MBaud / 6 MBaud / 12 MBaud definiert.

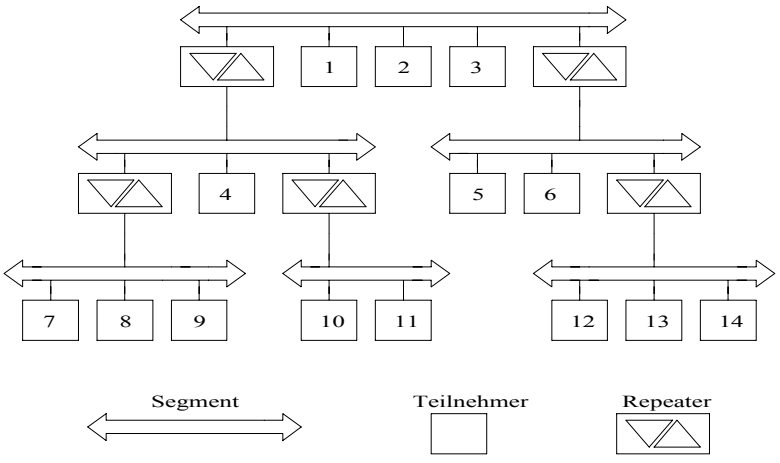
Die Buskonfiguration ist modular ausbaubar wobei die Peripherie- und Feldgeräte während des Betriebes an- und abkoppelbar sind.

Die Datenübertragung erfolgt entweder über Zweidrahtleitung mit RS-485-Schnittstelle oder über Lichtwellenleiter. Wobei wir uns hier im wesentlichen auf die Zweidrahtleitung beschränken.

Die geschirmte und verdrillte Zweidrahtleitung (Twisted Pair) hat einen Mindestquerschnitt von 0,22 mm², und muss an den Enden mit dem Wellenwiderstand abgeschlossen werden.

Eine Flächendeckende Vernetzung erfolgt beim PROFIBUS DP durch Aufteilung des Bussystems in Bussegmente, die wiederum über Repeater verbunden werden können.

Die Topologie der einzelnen Bussegmente ist die Linienstruktur mit kurzen Stichleitungen. Mit Hilfe von Repeatern kann auch eine Baumstruktur wie hier dargestellt aufgebaut werden.



Die maximale Anzahl der Teilnehmer je Bussegment bzw. Linie beträgt 32. Mehrere Linien können untereinander durch Leistungsverstärker (Repeater) verbunden werden. Insgesamt sind maximal 127 Teilnehmer anschließbar (über alle Bussegmente).

Es können 10 Bussegmente in Reihe geschaltet werden (9 Repeater)

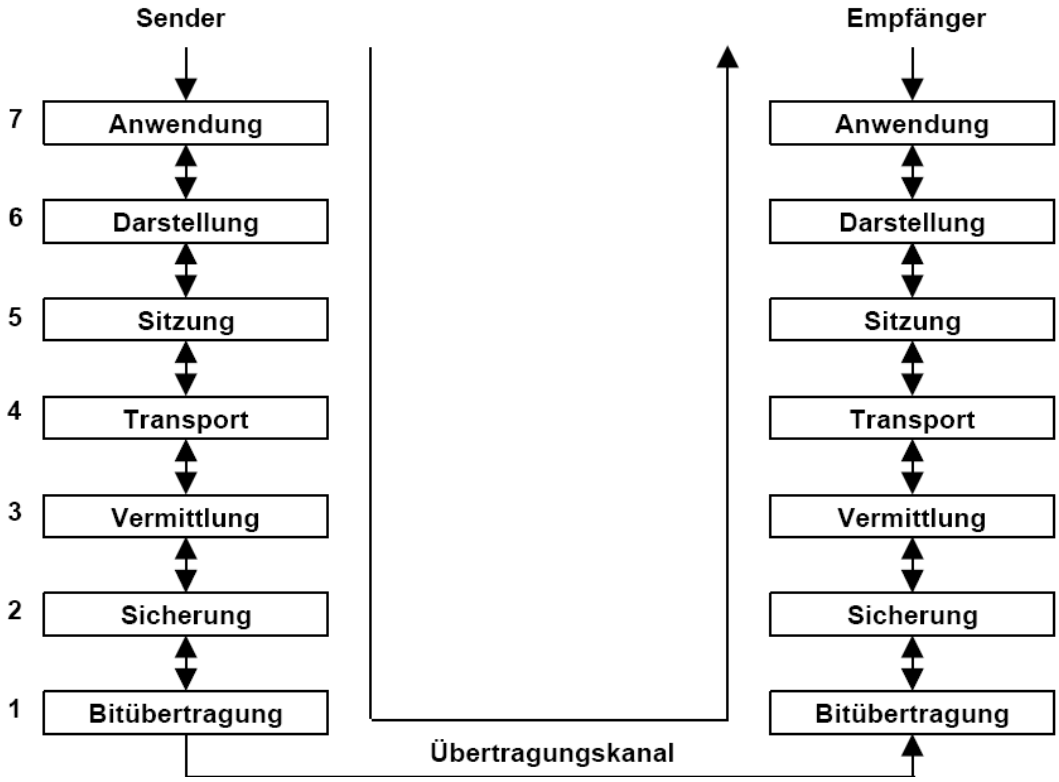
Übertragungsstrecken bei elektrischen Aufbau bis 12 km, bei optischen Aufbau bis 23,8 km möglich. Die Strecken sind wie in hier angegeben von der Übertragungsrate abhängig (elektrischer Aufbau).

Übertragungsrate in KBaud	9,6	45,45	19,2	93,75	187,5	500	1500	3000	6000	12000
Länge pro Segment in m	1200	1200	1200	1200	1000	400	200	100	100	100
max. Länge in m	12000	12000	12000	12000	10000	4000	2000	1000	1000	1000
bei Anzahl Bus-Segmente:	10	10	10	10	10	10	10	10	10	10

Beim PROFIBUS DP bestehen mit Hilfe von Softwaretools umfangreiche Diagnosemöglichkeiten.

ISO-OSI- SCHICHTENMODELL FÜR KOMMUNIKATIONSNETZE

Die Kommunikationsmechanismen zwischen unterschiedlichen Systemen sind in der Regel sehr komplex und unübersichtlich. Daher wurden einzelne logische Bereiche der Kommunikation in überschaubare Teilsysteme aufgeteilt. Diese Aufteilung erfolgte in einzelne hierarchisch angeordnete Schichten mit klar definierten Aufgaben. Dabei stützt sich eine Schicht auf die Funktionalität der jeweils darunter liegenden Schicht.
Die folgende Abbildung stellt das ISO-OSI- Schichtenmodell dar, welches durch die „International Standards Organisation“ definiert wurde. OSI steht dabei für „Open Systems Interconnection”



Wie in der Abbildung zu sehen ist, sind die einzelnen Schichten symmetrisch angelegt, d.h. zu jeder Schicht beim Sender gibt es eine korrespondierende Schicht beim Empfänger.
Die einzelnen Schichten bieten dabei die folgende Funktionalität:

- Schicht 1: Bitübertragung (physical layer)

Diese Schicht dient dazu die rohen Bitdaten der Kommunikation über den entsprechenden Kanal zu übertragen. Dazu werden unter anderem Übertragungsmedien, Signalpegel oder auch Kommunikationsrichtungen festgelegt.

- Schicht 2: Sicherungsschicht (data link layer)

Diese Schicht bietet Sicherungsmechanismen um fehlerhaft übertragene Daten durch Koderedundanz zu erkennen und entsprechend darauf zu reagieren. Im Fehlerfall könnten beispielsweise die übertragenen Daten erneut angefordert werden.

- Schicht 3: Vermittlungsschicht (network layer)

Die Aufgabe dieser Schicht ist es, einen Weg vom Ursprungs- zum Bestimmungsort zu ermitteln und auszuwählen.

- Schicht 4: Transportschicht (transport layer)

In dieser Schicht werden die Daten für die Vermittlungsschicht aufbereitet. Im wesentlichen werden die zu übertragenen Daten in kleine Pakete aufgeteilt bzw. auf der anderen Seite wieder zusammengesetzt.

- Schicht 5: Sitzungsschicht (session layer)

Diese Schicht stellt gehobenere Dienste für die Datenkommunikation bereit. Dazu zählen zum Beispiel die Zugangsmechanismen oder Zugriffssynchronisation.

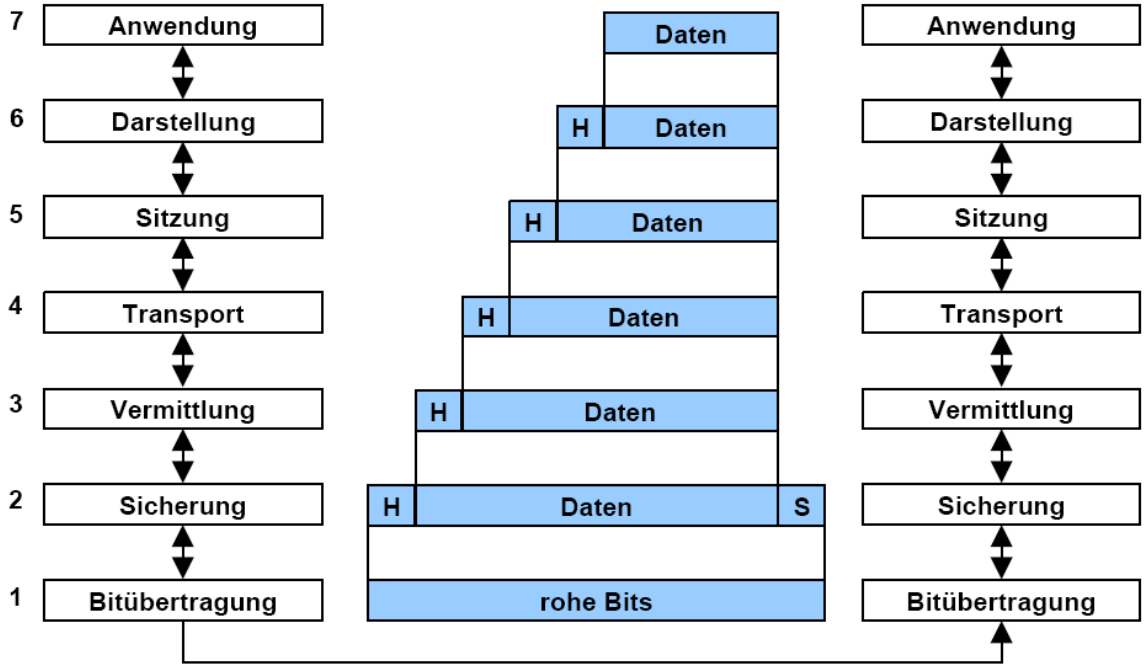
- Schicht 6: Darstellungsschicht (presentation layer)

In dieser Schicht werden die Datenstrukturen entsprechend dem Protokoll oder Zielsystem umgewandelt. Dies können beispielsweise Konvertierungen von Zeichensätzen oder auch kryptographische Verschlüsselungen sein.

- Schicht 7: Anwendungsschicht (application layer)

Diese Schicht stellt dem Anwender die entsprechende Dienste bereit. Dazu zählen unter anderem Dateiübertragung / -verwaltung oder auch E-Mail. In der Anwendungsschicht wird das eigentliche Ziel des Systems erfüllt.

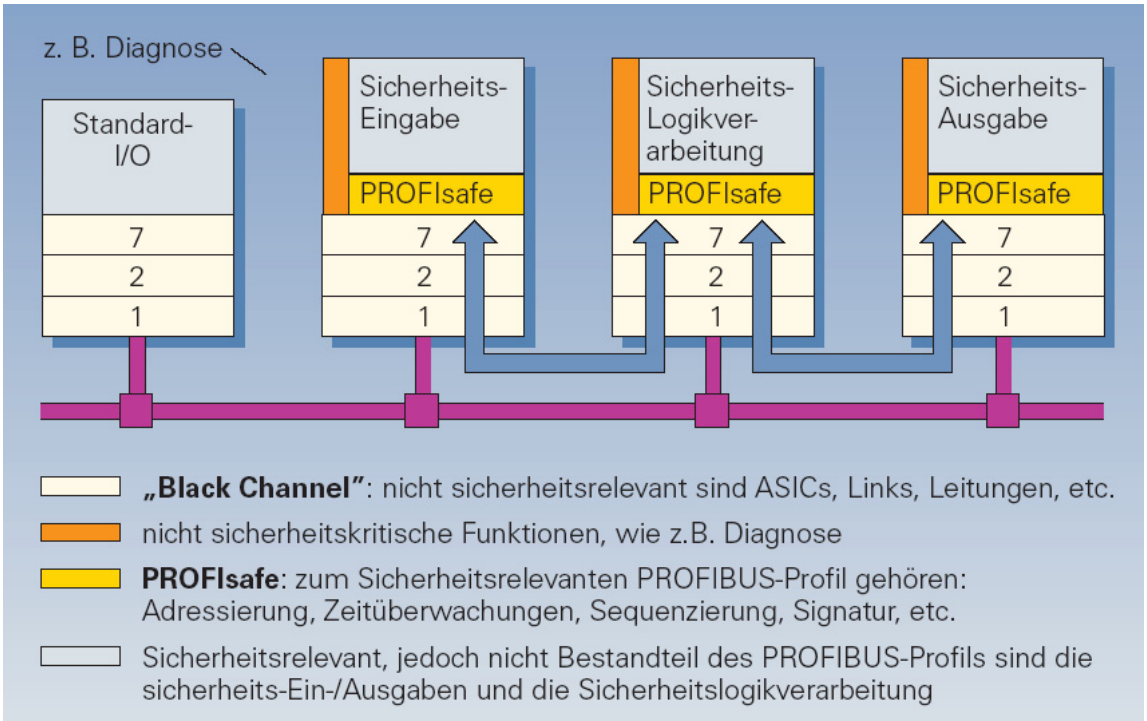
Die folgende Abbildung zeigt, wie die Daten gemeinsam mit einer Kopfinformation (Header... H) in eine sogenannte Protokoll-Daten-Einheit (Protocol Data Unit...PDU) verpackt werden, um sie der jeweils darunter liegenden Schicht zu übergeben. Der Dateninhalt interessiert dabei die jeweils tiefere Schicht nicht, sondern diese entnimmt ihre Steuerinformation der Kopfinformation. Die Information wird so immer weiter verpackt und auf der Empfängerseite wieder ausgepackt. So kommt jede Schicht wieder zu der für sie bestimmten Kopfinformation. Es ist dann so, als ob die Schichten miteinander kommunizieren würden.



In der Sicherungsschicht wird noch eine Sicherungsinformation, z.B. eine Prüfsumme angehängt, um beim Empfänger eine Prüfung zu ermöglichen, ob die rohen Bits auch richtig über das Kommunikationsmedium übertragen wurden.

Sicherheitsmaßnahmen bei PROFIsafe

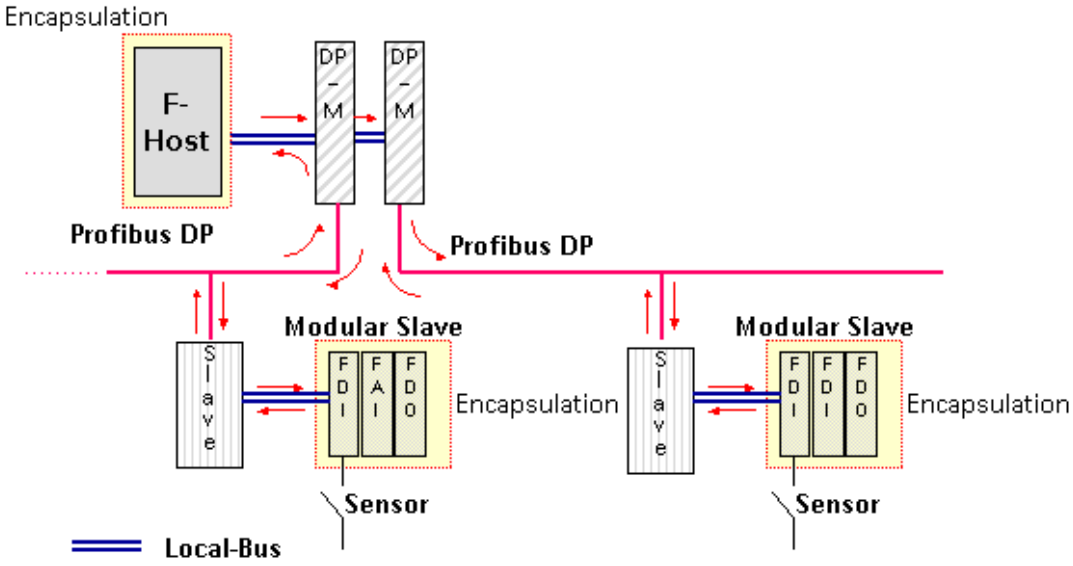
Die Sicherheitsmaßnahmen beim PROFIsafe- Profil befinden sich über der Schicht 7 des ISO/OSI-Kommunikationsmodells. Hierzu bedarf es einer weiteren Schicht, die sich sicherheitsgerichtet um die Beschaffung und Aufbereitung der Nutzdaten kümmert.



PROFIsafe Safety-Layer oberhalb des OSI-Models

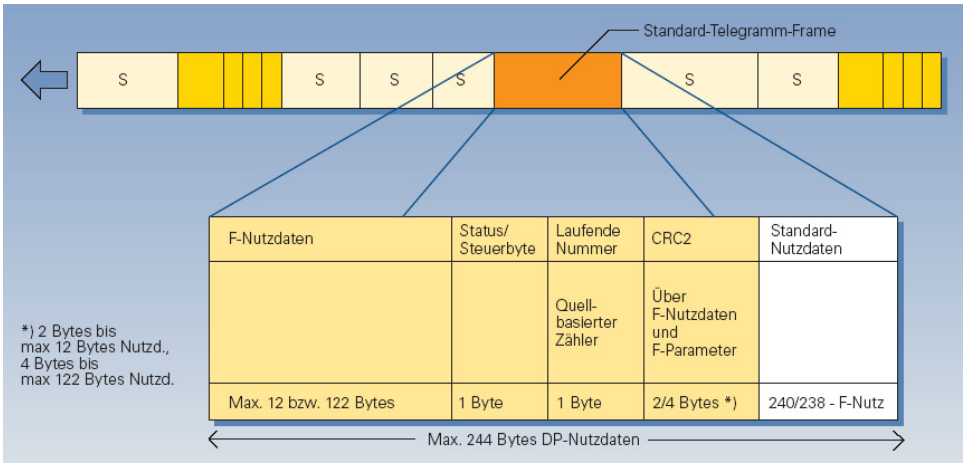
Die Entwicklung der PROFIsafe- Richtlinie wurde nach der neuen Norm IEC 61508 durchgeführt. Die erreichten Sicherheitsstufen sind Safety Integrity Level 3 (IEC 61508), Kat. 4 (EN 954-1) und AK6 (DIN V 19250).

Die Sicherheitsmaßnahmen sind in den sicherheitsgerichteten Kommunikationsendteilnehmern gekapselt.



Kapselung der Sichheitsmaßnahmen

In einem sicheren Feldgerät kann diese Funktion z.B. durch dessen Technologie-Firmware wahrgenommen werden. Wie im Standardbetrieb auch, werden die Prozesssignale bzw. Prozesswerte in entsprechende Nutztelegramme verpackt. Sie werden bei sicheren Daten lediglich um Sicherheitsinformationen ergänzt. Für den Versand der sicherheitsgerichteten Telegramme wird der Standardmechanismus „Master-Slave- Betrieb“ von PROFIBUS genutzt. Ein Master, der in der Regel einer CPU zugeordnet ist, tauscht zyklisch mit allen seinen konfigurierten Slaves Telegramme aus.



PROFIsafe- Telegramme einfach in Standardtelegramme verpackt

Beim Versand von Telegrammen können eine Reihe von Fehlern auftreten. Telegramme können verloren gehen, wiederholt auftreten, zusätzlich eingefügt werden, in falscher Reihenfolge oder verzögert auftauchen und Datenverfälschungen aufweisen.
Im Sicherheitsfall kommt noch fehlerhafte Adressierung hinzu, das heißt, ein Standard-Telegramm erscheint irrtümlich bei einem Sicherheitsteilnehmer und gibt sich als Sicherheitstelegramm aus (Maskerade).

Maßnahme: / Fehler:	Laufende Nummer (Lebenszeichen)	Zeiterwartung mit Quit-tierung	Kennung für Sender und Empfänger	Daten-sicherung
Wiederholung	x			
Verlust	x	x		
Einfügung	x	x	x	
Falsche Abfolge	x			
Verfälschung von Nutzdaten				x
Verzögerung		x		
Kopplung von sicher-heitsrelevanten und Standard-Nachrichten (Maskerade), einschließ-lich Falsch- und Doppel-adressierung		x	x	x
FIFO Fehler innerhalb des Routers		x		

Mögliche Kommunikationsfehler und PROFIsafe- Maßnahmen zur Aufdeckung

In der obigen Matrix sind die möglichen Fehlerursachen und die bei PROFIsafe gewählten Abhilfemaßnahmen eingetragen.
Zu diesen zählen:

- Fortlaufende Nummerierung der Sicherheitstelegramme
- Zeiterwartung mit Quittierung
- Kennung zwischen Sender und Empfänger („Losungswort“) und
- Zusätzliche Datensicherung (CRC – cyclic redundancy check).

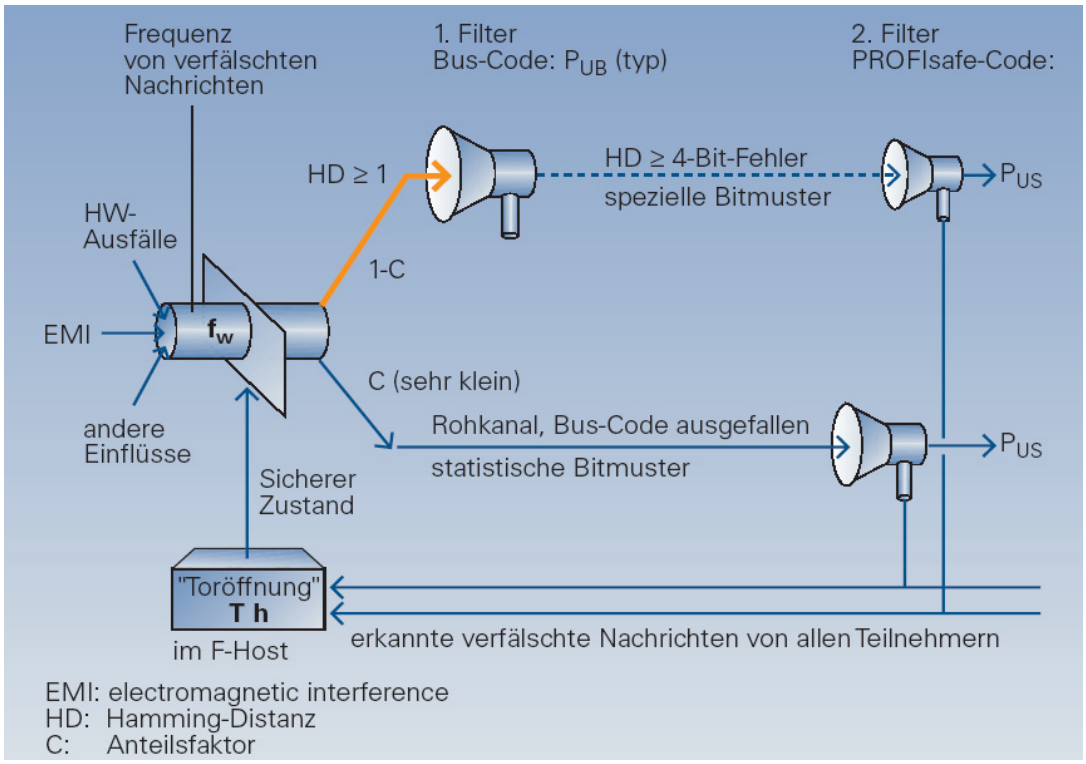
Anhand der fortlaufenden Nummer kann ein Empfänger erkennen, ob er sämtliche Telegramme in der korrekten Reihenfolge empfangen hat. In der Sicherheitstechnik kommt es nicht allein darauf an, dass ein Telegramm die richtigen Prozesssignale oder Werte überträgt, sondern diese müssen auch innerhalb einer Fehlertoleranzzeit eintreffen, so dass der jeweilige Teilnehmer gegebenenfalls Sicherheitsreaktionen automatisch vor Ort einleiten kann.

Hierzu verfügen die Teilnehmer über eine einstellbare Zeitüberwachung (Time-out), die nach dem Eintreffen eines Sicherheitstelegramms neu „aufgezogen“ wird. Die 1:1-Beziehung zwischen Master und einem Slave erleichtert die Erkennung von fehlgeleiteten Telegrammen. Beide müssen lediglich über eine im Netzwerk eindeutige Kennung ("Losungswort") verfügen, an Hand derer sie die Authentizität eines Telegramms überprüfen können. Eine Schlüsselrolle spielt die Datensicherung über CRC. Ihr kommt zusätzlich die Verantwortung zu, neben der Datenintegrität der transportierten Nutzdaten auch die Integrität der im jeweiligen Endgerät deponierten Parameter sicherzustellen.

Da die Datensicherungsmaßnahmen und die Zuverlässigkeit des Standard- PROFIBUS für den Sicherheitsnachweis nicht herangezogen wurden, war dieser Sicherheitsnachweis für PROFIsafe zwar etwas aufwendiger, hat aber den Vorteil, dass der Anwenderhinsichtlich Buskabel, Schirmung, Buskoppler usw. für PROFIsafe keine besondere Maßnahme treffen muss.

In der EN 50159-1 ist ein Markov- Modell angegeben, welches in geringfügig erweiterter Form für die Berechnung der Restfehlerwahrscheinlichkeiten von Sicherheitskreisen eingesetzt werden konnte. Es geht von drei wesentlichen Einflüssen für die Verfälschung von Nachrichten aus, die allesamt von den beiden Datensicherungseinrichtungen erkannt werden müssen: Ausfälle in ASICs und Treibern, elektromagnetische Störungen und der spezielle Fall, dass lediglich die Sicherungseinrichtung im Bus- ASIC ausgefallen ist.

Ohne besondere Maßnahmen hätte sonst für jede Buskonfiguration ein gesonderter Nachweis erbracht werden müssen. Für einen offenen Standard-Feldbus wie den PROFIBUS wäre dies eine gravierende Einschränkung. Es wurde daher eine Einrichtung geschaffen, die die Einhaltung von SIL- Stufen über die Lebenszeit einer dezentralen sicheren Automatisierungslösung, unabhängig von den eingesetzten Komponenten und der Konfiguration, gewährleistet: ein patentierter SIL-Monitor.



Patentierter SIL- Monitor überwacht laufend die funktionale Sicherheit des PROFIsafe

Der SIL- Monitor ist in Software realisiert. Er berücksichtigt alle vorstellbaren Fehlereinflüsse und löst eine Reaktion aus, wenn die Anzahl der Störungen oder Fehler ein bestimmtes Maß pro Zeiteinheit übersteigt. Die Zahl der zulässigen Fehler pro Zeiteinheit ist abhängig von der eingestellten SIL Stufe.

Anschluss von komplexen Endgeräten an PROFIsafe

Den Arbeitskreis-Mitgliedern war schnell klar geworden, dass eine reine Profilbeschreibung für die schnelle Umsetzung in eine Vielzahl von „PROFIsafe- Produkten“ nicht ausreichen würde. Insbesondere die optische Sicherheitstechnik, mit z.B. Laserscannern und Lichtvorhängen, benötigt große Mengen von Parametern, deren Einlernphasen eine spezielle Bedienung erfordern. Hierfür hat der Arbeitskreis in den Richtlinien Lösungen beschrieben, die auch für weitere komplexe Geräte angewandt werden können.

Parametrierung und Diagnose von PROFIsafe- Komponenten können, wie bei PROFIBUS üblich, über einen direkt am PROFIBUS angeschlossenen PC erfolgen.

Um das Projektieren von Sicherheitskreisen optimal zu vereinfachen, stehen den Engineering- Tools alle notwendigen Parameter zur Verfügung. Insbesondere für die Berechnung von Gesamtreaktionszeiten der Sicherheitskette müssen von den Herstellern in den GSD (Gerätestammdaten)- Datenblättern die Bearbeitungszeiten von Sensoren und Aktoren angegeben werden.

5.3 Peripheriekomponenten für PROFIsafe

Das fehlersichere Steuerungssystem beinhaltet fehlersichere Steuerungen und fehlersichere, dezentrale Peripheriebaugruppen. Die Anbindung der Peripherie an die CPU erfolgt durch PROFIBUS DP oder PROFINET mit PROFIsafe-Profil.
Dank der feinmodularen F-Peripherie (F steht für fehlersicher) muss die Sicherheitstechnik nur dort eingesetzt werden, wo sie notwendig ist. Ohne Probleme können auch Fremdsysteme angeschlossen werden. Die Lösung ersetzt herkömmliche elektromechanische Komponenten und zeichnen sich durch folgende Eigenschaften aus:

- frei programmierbare sichere Verknüpfung von Sensoren mit Aktoren
- selektive sichere Abschaltung von Aktoren
- gemischter Aufbau von F-Baugruppen (F steht für fehlersicher) und Standardbaugruppen in einer Station
- 1-Bus-Konzept, Übertragung von F-Signalen und Standard-Signalen über ein Busmedium (PROFIBUS DP)
- Peripheriebaugruppen stehen in ET 200S / ET 200M-Aufbautechnik zur Verfügung.

Fehlersichere Peripherie ET 200S

Die SIMATIC ET 200S ist ein feinmodular aufgebautes, dezentrales Peripheriegerät. Es kann mit unterschiedlichen Interfacemodulen betrieben werden:

IM 151-1 BASIC, IM 151-1 STANDARD und IM 151-1 FO STANDARD zum Anschluss von max. 63 Peripheriemodulen (alle Typen, außer PROFIsafe) an den PROFIBUS DP; alternativ Busanschluss mit RS 485 Sub-D-Stecker oder über integrierten Lichtleiteranschluss

IM 151-1 HIGH-FEATURE zum Anschluss von max. 63 Peripheriemodulen (alle Typen, auch taktsynchroner Betrieb für PROFIsafe) an den PROFIBUS-DP; Busanschluss mit RS485 Sub-D-Stecker

IM 151-3 PN zum Anschluss von max. 63 Peripheriemodulen (alle Typen, auch taktsynchroner Betrieb für PROFIsafe) an PROFINET IO-Controller; Busanschluss über RJ45 Stecker

IM 151-7/F-CPU, IM 151-7/CPU bzw. IM 151-7/CPU FO zum Anschluss von max. 63 Peripheriemodulen (alle Typen, PROFIsafe nur mit IM151-7/F-CPU) an den PROFIBUS DP; alternativ Busanschluss mit RS 485 Sub-D-Stecker oder über integrierten Lichtleiteranschluss. Mit integrierter CPU 314 der SIMATIC S7-300 zur Vorverarbeitung der Prozessdaten.

Die folgenden Peripheriemodule können hier eingesetzt werden:

Powermodule zur individuellen Gruppierung von Last- und Geberversorgungsspannungen und deren Überwachung

Digitale Elektronikmodule zum Anschluss digitaler Sensoren und Aktoren

Analoge Elektronikmodule zum Anschluss analoger Sensoren und Aktoren

Sensormodul zum Anschluss von IQ-Sense-Sensoren

Technologiemodule Elektronikmodule mit integrierten technologischen Funktionen z.B. Zählen, Positionieren, Datenaustausch usw.

Frequenzumrichter- und Motorstartermodule

Für den Schuleinsatz hat man so ein durchgängiges System an dem eine Vielzahl an Technologien gelehrt werden können

F-Baugruppen der ET 200S umfassen fehlersichere Ein und Ausgangsbaugruppen und fehlersichere Motorstarter:

- **Fehlersichere Eingangsbaugruppen** erfassen die Informationen der Sensoren.
- **Fehlersichere Ausgangsbaugruppen** steuern die Aktoren.
- **Fehlersichere Motorstarter** steuern und überwachen Antriebe.

Alle F-Baugruppen können interne und externe Fehler diagnostizieren und sind intern redundant aufgebaut, verfügen über eigene Selbsttests und entsprechen den notwendigen Sicherheitsanforderungen.

Die Elektronikmodule der ET 200S sind 30 mm breit, durch einen gelben Beschriftungsstreifen gekennzeichnet und intern zweikanalig aufgebaut. Sie können während des Betriebs unter Spannung gezogen und gesteckt werden.

Folgende fehlersicheren ET 200S Module stehen zur Verfügung:

- **4/8 F-DI** DC 24 V, Fehlersichere Digitaleingabe mit 4 Eingängen bei 2-kanaligen SIL 3-Sensoren (Kat. 4) oder 8 Eingängen bei 1-kanaligen SIL 2-Sensoren (Kat. 3) für 24 V
- **4 F-DO** DC 24 V/2 A, Fehlersichere Digitalausgabe mit 4 Ausgängen für 24 V und 2 A (bis SIL 3/Kat. 4)
- **PM-E F** DC 24 V, Powermodul mit 2 (SIL 3, Kat. 4) Ausgängen für 24 V/2 A und einem weiteren Relais-Ausgang (max. 10 A, SIL 3, Kat. 4), der an 2 Klemmen zur Verfügung steht und außerdem die Laststromversorgung für die nachfolgenden Baugruppen (SIL 2, Kat. 3) übernimmt
- **PM-D F**, Fehlersicheres Powermodul PROFIsafe mit 6 integrierten sicheren Abschaltschienen (SIL 3), 24 V und 3 A zur sicheren Abschaltung von nachgeordneten fehlersicheren Motorstartern/Kontaktvervielfachern, bei interner Ansteuerung über PROFIsafe
- **PM-D F X1**, Powermodul (Einspeiseklemmenmodul) mit 6 integrierten sicheren Abschaltschienen (SIL 3), 24 V und 2 A zur sicheren Abschaltung von nachgeordneten fehlersicheren Motorstartern/Kontaktvervielfachern, bei Abschaltung durch externe Sicherheitsschaltgeräte mit potenzialfreien Kontakten (z.B. 3TK28, Monitor von AS-Interface *Safety at Work*). Eine PROFIsafe Anbindung ist hier nicht erforderlich.
- **F-CM**, Fehlersicherer Kontaktvervielfacher mit 2 (SIL 3) Ausgängen für 24 V und 2 A
- **F-MS**, Fehlersichere Direkt- und Reversierstarter bis 7,5 kW Schaltleistung, mit redundanter galvanischer Trennung

5.4 Verdrahtungsbeispiele zu den F- Modulen in der ET 200S

5.4.1 Powermodul PM-E F pm DC24V PROFIsafe (6ES7 138-4CF0*-0AB0)

Eigenschaften

Das Powermodul PM-E F pm DC24V PROFIsafe verfügt über folgende Eigenschaften:

- 2 Relais zum Schalten der Potenzialschienen P1 und P2, Ausgangsstrom 10 A
- 2 fehlersichere Digitalausgänge, P-/M-schaltend, Ausgangsstrom 2 A
- Lastnennspannung DC 24 V
- geeignet für Magnetventile, Gleichstromschütze und Meldeleuchten
- Sammelfehleranzeige (SF; rote LED)
- Statusanzeige pro Ausgang (grüne LED)
- Statusanzeige für Laststromversorgung (PWR; grüne LED)
- parametrierbare Diagnose
- erreichbare Sicherheitsklassen siehe folgende Tabelle

PM-E F pm DC24V PROFIsafe			**erreichbare Sicherheitsklasse**
Relais-Ausgänge P1 und P2	ohne Standard-DO-Module	Signal wechselt täglich oder öfter	AK6/SIL3/Kat.4
		Signal wechselt seltener als einmal pro Tag	AK4/SIL2/Kat.3
	mit Standard-DO Modulen		AK4/SIL2/Kat.3
Elektronische Ausgänge DO 0 und DO 1	ohne Standard-DO-Module an P1 und P2		AK6/SIL3/Kat.4
	mit Standard-DO-Modulen an P1 und P2		AK4/SIL2/Kat.3

Übersicht erreichbare Sicherheitsklassen mit PM-E F pm DC24V PROFIsafe

Schalten der Potenzialschienen P1 und P2

Das Powermodul kann die Potenzialschienen P1 und P2 über Relaiskontakte fehlersicher schalten nach AK4/SIL2/Kat.3.

2 fehlersichere Digitalausgänge

Zusätzlich zu den Potenzialschienen P1 und P2 hat das Powermodul zwei fehlersichere Digitalausgänge DO 0 und DO 1. Mit diesen Ausgängen kann AK6/SIL3/Kat.4 erreicht werden, sofern keine Standard- DO- Module an P1 und P2 angeschlossen sind.

Bedingungen für das Erreichen der Sicherheitsklasse
In der folgenden Tabelle sind die Bedingungen für das Erreichen der jeweiligen Sicherheitsklasse zusammengefasst.

Bedingung	erreichbare AK/SIL/Kat.
Versorgung von ET 200S-Standardmodulen über P1 und P2	AK4/SIL2/Kat.3 an P1 und P2 sowie an DO 0 und DO 1
Nutzung von DO 0 und DO 1 und keine Versorgung von Modulen über P1 und P2	AK6/SIL3/Kat.4 an DO 0 und DO 1

PM-E F pm DC24V PROFIsafe: Bedingungen für AK/SIL/Kat.

Warnung für Versorgung der Standard- ET 200S-Module durch Powermodul:

- Schließen Sie die DC 24 V-Versorgung für die Standard- ET 200S-Module immer am PM-E F pm DC24V PROFIsafe an. Andernfalls ist ein sicherheitskritisches Verhalten an den Ausgängen von DO- Modulen nicht auszuschließen!
- Bei der Versorgung von Standard- DO- Modulen müssen die Aktoren immer über die Terminalmodule dieser Module versorgt werden (Aktorrückführung am DO- Modul). Andernfalls wird ein Kurzschluss von dem Powermodul gemeldet und die Lastspannung dieser Potenzialgruppe wird abgeschaltet.

Warnung für sicherheitsgerichtete Abschaltung von Standard-DO-Modulen:

- Das digitale Elektronikmodul 4DO DC24V/0,5A (Bestell-Nr. 6ES7 132-4BD00- 0AA0) ist das einzige Standard-ET 200S-Modul, das für die sicherheitsgerichtete Abschaltung gemäß SIL2 freigegeben ist.
- Die Ausgänge von Standard- DO- Modulen können nicht sicherheitsgerichtet geschaltet, sondern nur sicherheitsgerichtet **ab**geschaltet werden. Deshalb müssen Sie die folgenden möglichen
Auswirkungen berücksichtigen: Im worst case- Fall müssen Sie mit allen denkbaren Fehlern der Standard- DO- Module und des sie steuernden Programms rechnen, für die es auch keine direkte Fehleraufdeckung gibt. Z. B. erkennt das PM-E F pm DC24V PROFIsafe keine externen Kurzschlüsse nach L+ an den Ausgängen von Standard- DO- Modulen. Alle Fehler der Standard- DO- Module wirken über Stellglieder auf den Prozess. Der Prozess muss über Geber und ein entsprechendes Sicherheitsprogramm der F-CPU bekannt gemacht werden. Das Sicherheitsprogramm muss auf unerwünschte oder potenziell gefährliche Zustände des Prozesses über das PM-E F pm DC24V PROFIsafe und fehlersichere Ausgabemodule sicherheitsgerichtet und logisch angemessen reagieren.

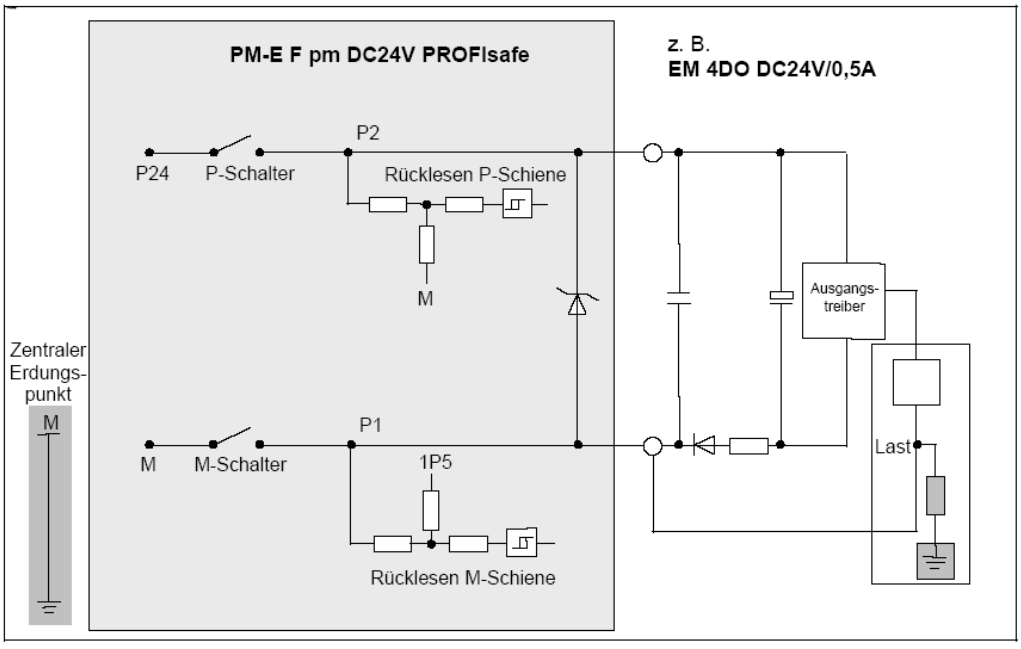
Wenn Sie die oben beschriebenen Fehler gänzlich vermeiden wollen, dann empfehlen wir Ihnen, anstelle von Standard- DO- Modulen den Einsatz der P-/M-schaltenden fehlersicheren Elektronikmodule 4 F-DO DC24V/2A PROFIsafe mit Standard- ET 200S-Powermodulen.

Eigenschaft der sicherheitsgerichteten Abschaltung von Standard- DO- Modulen durch das PM-E F pm DC24V PROFIsafe:
Bei dieser kostengünstigen Lösung erfolgt bei der Aufdeckung eines Fehlers im Prozess oder am PM-E F pm DC24V PROFIsafe ein umfassendes und zeitgleiches Abschalten aller betroffenen Ausgänge.

Eigenschaft der individuellen Abschaltung von F-Modulen mit fehlersicheren Ausgängen:
Bei der Aufdeckung eines Fehlers erfolgt ein Abschalten in minimalem Umfang. Außerdem kann auf kritische Prozess-Zustände zeitlich gestaffelt reagiert bzw. können Ausgänge einzeln und sicherheitsgerichtet abgeschaltet werden.
Diese Lösung bringt im Vergleich zur sicherheitsgerichteten Abschaltung durch das PM-E F pm DC24V PROFIsafe höhere Kosten mit sich.

Schalten von Lasten, die nicht erdfrei aufgebaut sind
Wenn vom PM-E F pm DC24V PROFIsafe Lasten geschaltet werden, die eine Verbindung zwischen Masse und Erde aufweisen (z. B. zur Verbesserung der EMV- Eigenschaften) **und** wenn beim versorgenden Netzteil Masse und Erde verbunden sind, dann wird .Kurzschluss. erkannt. Aus Sicht des F-Moduls wird durch die Masse-Erde-Verbindung der M-Schalter überbrückt (siehe folgendes Bild als Beispiel für ein PM-E F pm DC24V PROFIsafe).

Abhilfe:
- Einsatz des PM-E F pp DC24V PROFIsafe
- der lastseitige Widerstandswert zwischen Masse und Erde muss größer 100 kΩ sein



Schalten von nicht erdfreien Lasten (Widerstand zwischen Masse und Erde vorhanden)

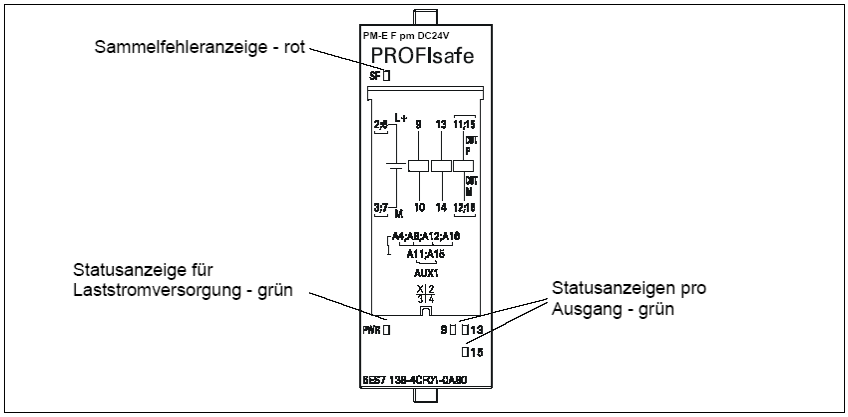
Kapazitives Übersprechen von digitalen Ein-/Ausgangssignalen
Bei der gemeinsamen Führung von fehlersicheren digitalen Ausgangssignalen und fehlersicheren digitalen Eingangssignalen in einem Kabel kann es zu Rücklesefehlern bei dem Powermodul PM E-F pm DC24V PROFIsafe bzw. Den F- DO- Modulen kommen. Die Baugruppe meldet dann einen Kurzschluss.

Ursache
Während des Geberversorgungstests des Moduls 4/8 F-DI DC24V PROFIsafe kann die steile Schaltflanke der Ausgangstreiber aufgrund der Koppelkapazität der Leitung zu einem Übersprechen auf andere, nicht eingeschaltete Ausgangskanäle führen, z. B. am Powermodul PM E F pm DC24V PROFIsafe. In diesen Kanälen kann es dann zu einem Ansprechen der Rückleseschaltung kommen. Es wird ein Querschluss erkannt, was zu einer sicherheitsgerichteten Abschaltung führt.

Abhilfe
- getrennte Kabel für F- DI- Module und F- DO- Module bzw. Standard- DO- Module, die von einem PM-E F pm DC24V PROFIsafe angesteuert werden
- Koppelrelais oder Dioden in den Ausgängen
- Test der Geberversorgung ausschalten, sofern dies die geforderte Sicherheitsklasse erlaubt.

Einspeisung der DC 24 V-Versorgung für Elektronikmodule mit Technologiefunktionen
Abhängig davon, ob in den Elektronikmodulen mit Technologiefunktionen (Positionieren, Zählen) eine Potenzialtrennung zwischen der Elektronik- und der Laststromversorgung vorhanden ist, müssen Sie folgende Verdrahtungsvorschriften einhalten:
- wenn Potenzialtrennung vorhanden ist, kann die DC 24 V-Zuführung für das Elektronikmodul von extern erfolgen
- wenn keine Potenzialtrennung vorhanden ist, muss das Elektronikmodul von der Potenzialschiene P1 des PM-E F pm DC24V PROFIsafe versorgt werden. In beiden Fällen ist AK4/SIL2/Kat.3 erreichbar.

Frontansicht



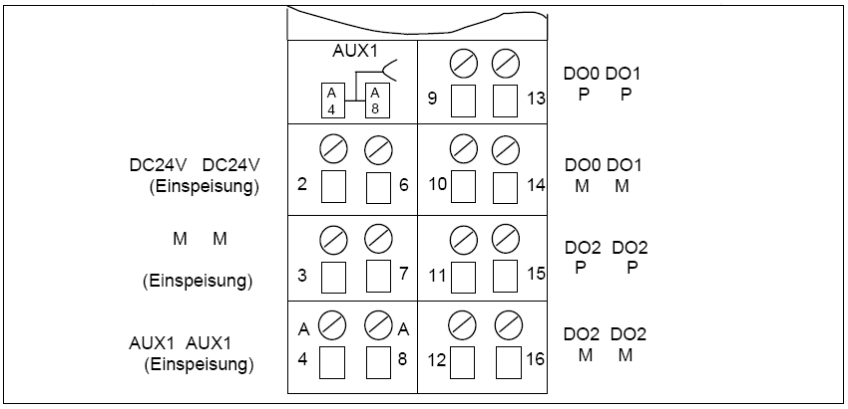
Frontansicht PM-E F pm DC24V PROFIsafe

Warnung

Die SF-LED und die Statusanzeigen der Ausgänge dürfen nicht für sicherheitsgerichtete Aktivitäten ausgewertet werden.

Anschlussbelegung

Im folgenden Bild und in der nachfolgenden Tabelle finden Sie die Anschlussbelegung des PM-E F pm DC 24V PROFIsafe für die einsetzbaren Terminalmodule TM-P30S44-A0 bzw. TM-P30C44-A0.



Anschlussbelegung TM-P30S44-A0 bzw. TM-P30C44-A0 für PM-E F pm DC 24V PROFIsafe

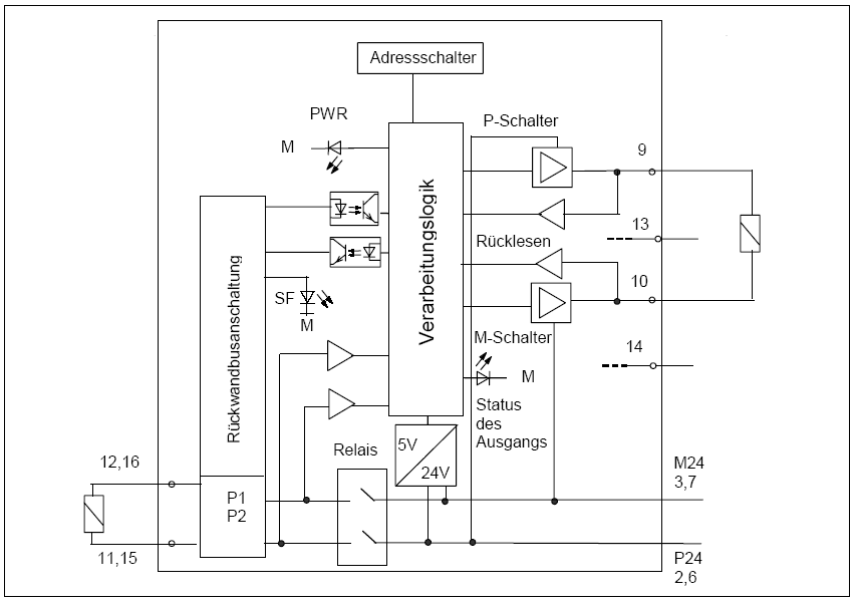
Klemme		Bezeichnung
2	DC 24 V	Lastnennspannung DC 24 V für: • gestecktes Powermodul, • zugehörige Potenzialgruppe, • DO 0 und DO 1 und • Potenzialschienen P1 und P2
3	M	Masse
A 4	AUX 1	Beliebiger Anschluss für PE oder Potenzialschiene bis zur maximalen Lastnennspannung des Moduls
6	DC 24 V	Lastnennspannung DC 24 V für: • gestecktes Powermodul, • zugehörige Potenzialgruppe, • DO 0 und DO 1 • und Potenzialschienen P1 und P2
7	M	Masse
A 8	AUX 1	Beliebiger Anschluss für PE oder Potenzialschiene bis zur maximalen Lastnennspannung des Moduls
9	DO 0 P	Anschlüsse für fehlersicheren Digitalausgang 0 (P-/M-schaltend)
10	DO 0 M	
11	DO 2 P	Anschlüsse (Relaiskontakte) für fehlersicheres Schalten der Potenzialschienen P1 und P2 P1 und P2 können zusätzlich als DO 2 M und DO 2 P genutzt werden
12	DO 2 M	
13	DO 1 P	Anschlüsse für fehlersicheren Digitalausgang 1 (P-/M-schaltend)
14	DO 1 M	
15	DO 2 P	Anschlüsse (Relaiskontakte) für fehlersicheres Schalten der Potenzialschienen P1 und P2 P1 und P2 können zusätzlich als DO 2 M und DO 2 P genutzt werden
16	DO 2 M	

Anschlussbelegung des TM-P30S44-A0 bzw. TM-P30C44-A0

Vorsicht

Wenn an DO 2 P und DO 2 M hohe Ströme auftreten können, müssen Sie jeweils die Klemmen 11 und 15 (DO 2 P) und 12 und 16 (DO 2 M) parallel verdrahten. Andernfalls ist durch die Strombelastung eine Erwärmung der Klemmen nicht auszuschließen.

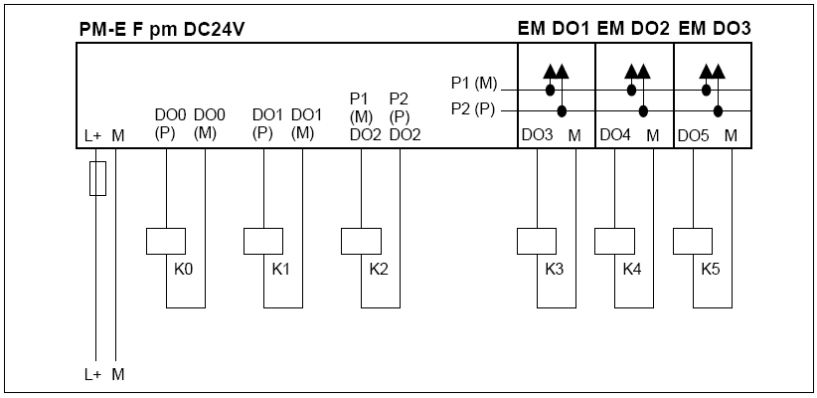
Prinzipschaltbild



Prinzipschaltbild des PM-E F pm DC24V PROFIsafe

Verdrahtungsschema

Jeder der 3 Digitalausgänge besteht aus einem P-Schalter DOx P und einem M-Schalter DOx M. Sie schließen die Last zwischen P- und M-Schalter an. Damit Spannung an der Last anliegt, werden immer beide Schalter angesteuert. Die Verdrahtung nehmen Sie am speziellen Terminalmodul für das PM vor.



Verdrahtungsschema des PM-E F pm DC24V PROFIsafe

Warnung

Bitte verwenden Sie generell zur Absicherung der Relaiskontakte vor Überlast eine externe Sicherung für L+ am PM-E F pm mit folgenden Eigenschaften: Leistungsschalter der Charakteristik B nach IEC 947-5-1, 10 A.

Relaisausgang DO 2

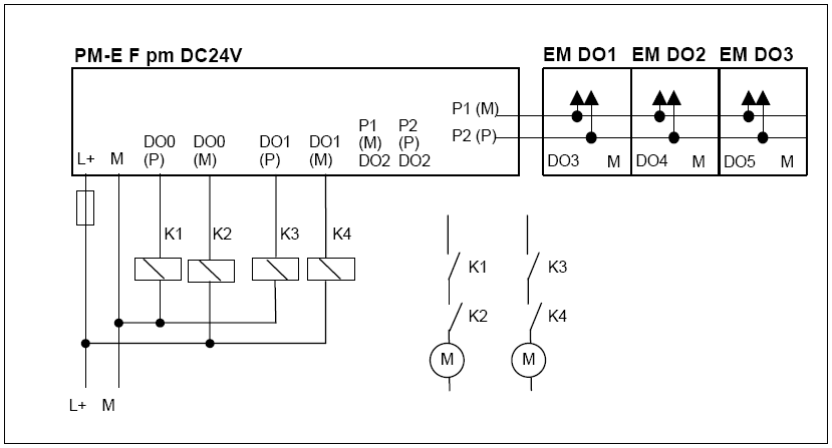
Der Relaisausgang DO 2 schaltet die Spannung L+ und M über je einen Relaiskontakt. Die Spannung wird nach außen auf das Terminalmodul und auf die internen Potenzialschienen P1 und P2 geführt. Damit ergeben sich zwei Anschlussmöglichkeiten, die Sie auch gleichzeitig nutzen können:

- Eine Last kann direkt am Terminalmodul angeschlossen werden (K2 im *Bild*).
- Über die internen Potenzialschienen P1 und P2 können Elektronikmodule gespeist werden. An diesen können wiederum Lasten angeschlossen werden (K3, K4, K5 im *Bild*).

Anschluss von 2 Relais an 1 Digitalausgang

Sie können 2 Relais mit einem fehlersicheren Digitalausgang schalten. Beachten Sie bitte die folgenden Bedingungen:

- L+ und M der Relais müssen mit L+ und M des PM-E F pm verbunden werden (gleiches Bezugspotenzial ist notwendig).
- Die Arbeitskontakte der beiden Relais müssen in Reihe geschaltet werden. Dieser Anschluss ist nur an den Digitalausgängen DO 0 und DO 1 möglich (nicht an DO 2). Sie erreichen mit dieser Schaltung:
- AK6/SIL3/Kat.4 ohne Standard- DO- Module an P1 und P2
- AK4/SIL2/Kat.3 mit Standard- DO- Modulen an P1 und P2



Verdrahtungsschema je 2 Relais an DO 0 und DO 1 des PM-E F pm DC24V PROFIsafe

Warnung

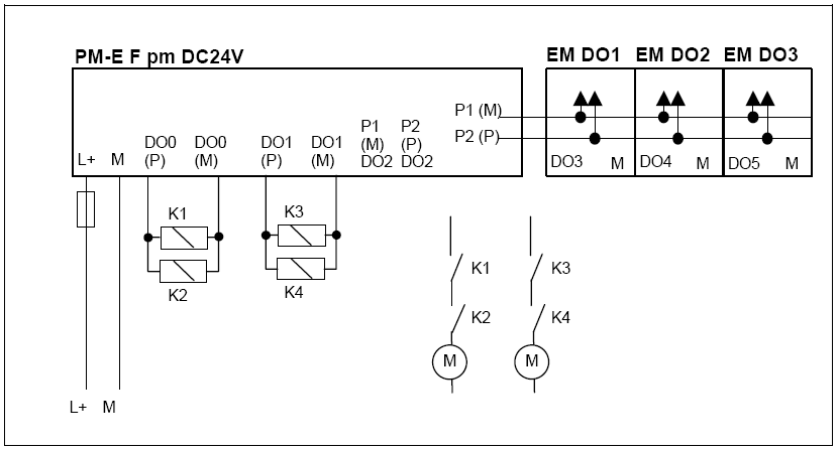
Beim Anschluss von 2 Relais an einem Digitalausgang (wie im Bild oben) werden die Fehler „Drahtbruch“ und „Überlast“ nur am P-Schalter des Ausgangs erkannt (nicht am M-Schalter).
Bei einem Querschluss zwischen P- und M-Schalter des Ausgangs wird der angesteuerte Aktor nicht mehr abgeschaltet.

Warnung

Um Querschlüsse zwischen P- und M-Schalter eines fehlersicheren Digitalausgangs zu vermeiden, müssen Sie die Leitungen für den Anschluss der Relais am P- und M-Schalter querschlusssicher verlegen (z. B. als separat ummantelte Leitungen oder in eigenen Kabelkanälen).

Vermeidung/Beherrschung von Querschlüssen

Um Querschlüsse zwischen P- und M-Schalter eines fehlersicheren Digitalausgangs zu beherrschen, empfehlen wir Ihnen die folgende Verdrahtungsvariante:



Verdrahtungsschema je 2 Relais parallel an DO 0 und DO 1 des PM-E F pm DC24V PROFIsafe

Hinweis

Beim parallelen Anschluss von 2 Relais an einem Digitalausgang (wie im Bild oben) wird der Fehler „Drahtbruch“ nur erkannt, wenn durch den Drahtbruch beide Relais von P oder M getrennt werden. Diese Diagnose ist nicht sicherheitsrelevant.

Parameter in *STEP 7*

In der folgenden Tabelle finden Sie die Parameter, die Sie für das PM-E F pm DC24V PROFIsafe einstellen können.

Parameter	Wertebereich	Voreinstellung	Art des Parameters	Wirkungsbereich
F-Parameter:				
F_Ziel_Adresse	1 bis 1022	wird von STEP 7 vergeben	statisch	Modul
F-Überwachungszeit	10 bis 10000 ms	150 ms	statisch	Modul
Baugruppenparameter:				
DO-Kanal 0	aktiviert/deaktiviert	aktiviert	statisch	Kanal
Rücklesezeit	1 bis 400 ms	1 ms	statisch	Kanal
Diagnose: Drahtbruch	aktiviert/deaktiviert	deaktiviert	statisch	Kanal
DO-Kanal 1	aktiviert/deaktiviert	aktiviert	statisch	Kanal
Rücklesezeit	1 bis 400 ms	1 ms	statisch	Kanal
Diagnose: Drahtbruch	aktiviert/deaktiviert	deaktiviert	statisch	Kanal

Parameter des PM-E F pm DC24V PROFIsafe

Rücklesezeit

Jeder Ausgangskanal verfügt über eine eigene parametrierbare Rücklesezeit. Diese Zeit legt die maximale Dauer des Ausschalttests für den entsprechenden Kanal und somit auch die Rücklesezeit für den Ausschaltvorgang des Kanals fest. Folgende Rücklesezeiten sind parametrierbar: 1 ms, 5 ms, 10 ms, 50 ms, 100 ms, 200 ms und 400 ms.

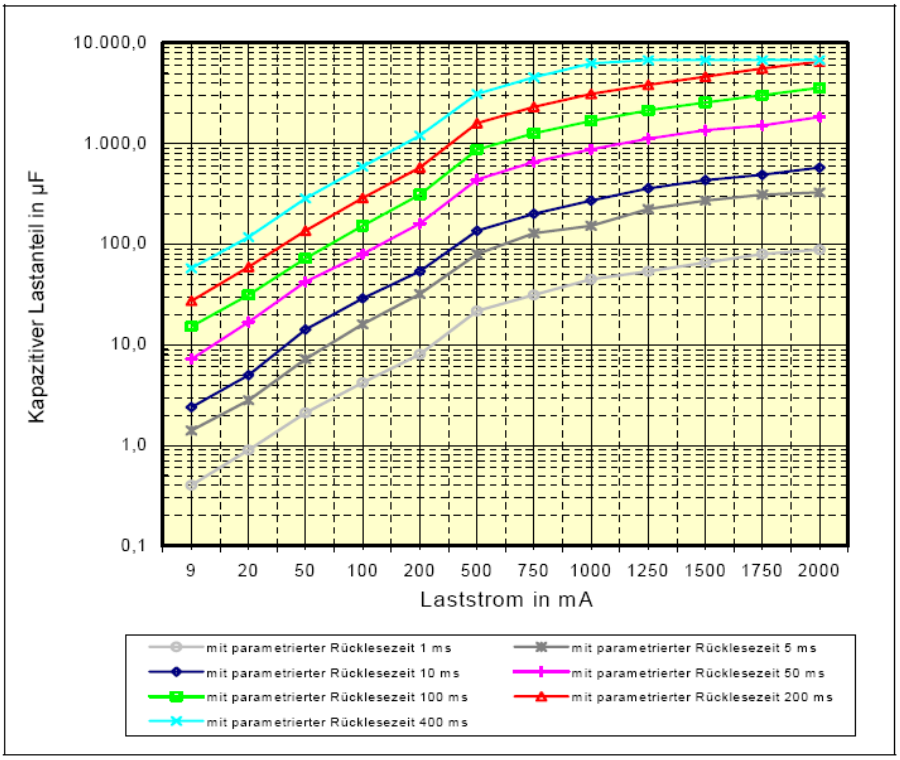
Sie sollten die Rücklesezeit hinreichend groß einstellen, wenn der betroffene Kanal große kapazitive Lasten schaltet. Ist die Rücklesezeit für eine angesteuerte kapazitive Last zu klein eingestellt, wird der Ausgangskanal passiviert, weil die Entladung der Kapazität nicht innerhalb des Ausschalttests erfolgt.

Bei falschen Rücklesesignalen wird die parametrierte Rücklesezeit abgewartet, bevor der Fehler „Kurzschluss" zur Passivierung des Ausgangskanals führt.

Schalten von kapazitiven Lasten

Wenn die elektronischen Ausgänge des PM-E F pm DC24V PROFIsafe mit Lasten verschaltet werden, die wenig Strom verbrauchen und eine Kapazität aufweisen, dann kann es zu der Fehlermeldung „Kurzschluss" kommen. Grund: Während der parametrierten Rücklesezeit beim Selbsttest werden die Kapazitäten nicht genügend entladen.

Das folgende Bild zeigt zu den parametrierbaren Rücklesezeiten typische Kurven für den Zusammenhang zwischen Lastwiderstand und schaltbarer Lastkapazität.



Zusammenhang zwischen Lastwiderstand und schaltbarer Lastkapazität für PM-E F pm DC24V PROFIsafe

Abhilfe:

1. Bestimmen Sie den Laststrom und die Kapazität der Last.
2. Bestimmen Sie den Arbeitspunkt im obigen Bild.
3. Wenn der Arbeitspunkt oberhalb der Kurve liegt, dann müssen Sie durch Parallelschalten eines Widerstandes den Laststrom so weit erhöhen, dass der neue Arbeitspunkt unterhalb der Kurve liegt.

5.4.2 Digitales Elektronikmodul 4/8 F-DI DC24V PROFIsafe (6ES7 138-4FA0*-0AB0)

Eigenschaften

Das digitale Elektronikmodul 4/8 F-DI DC24V PROFIsafe verfügt über folgende Eigenschaften:

- 8 Eingänge (AK4/SIL2/Kat.3) oder 4 Eingänge (AK6/SIL3/Kat.3 bzw. Kat.4)
- Eingangsnennspannung DC 24 V
- geeignet für Schalter und 3-/4-Draht-Näherungsschalter (BEROs)
- 2 kurzschlussfeste Geberversorgungen für jeweils 4 Eingänge
- externe Geberversorgung möglich
- Sammelfehleranzeige (SF; rote LED)
- Statusanzeige pro Eingang (grüne LED)
- eine Fehleranzeige für jede Geberversorgung (1VsF und 2VsF; rote LED)
- parametrierbare Diagnose

Einsetzbare Powermodule für SIL2 oder SIL3

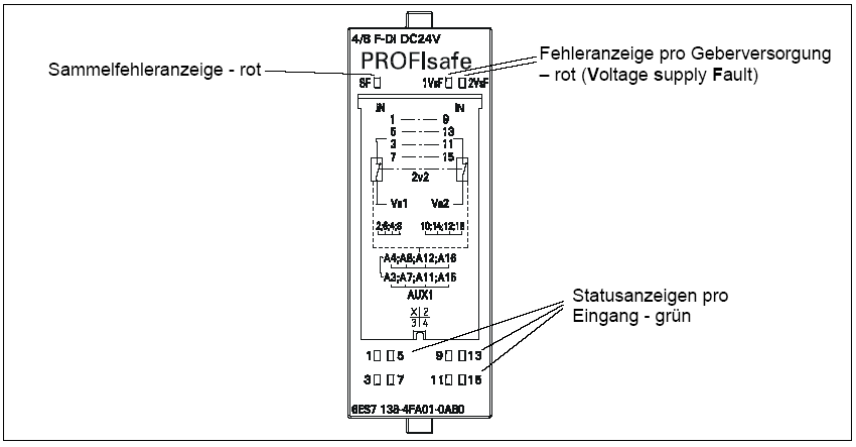
Powermodul	erreichbare AK/SIL/Kat.
Versorgung durch PM-E DC24V	bei 1v1-Auswertung der Geber (8 F-DI) AK4/SIL2/Kat.3
Versorgung durch PM-E DC24..48V/AC24..230V	bei 1v1-Auswertung der Geber (8 F-DI) AK4/SIL2/Kat.3 bei 2v2-Auswertung der Geber (4 F-DI) AK6/SIL3/Kat.4
Versorgung durch PM-E DC24..48V	bei 1v1-Auswertung der Geber (8 F-DI) AK4/SIL2/Kat.3 bei 2v2-Auswertung der Geber (4 F-DI) AK6/SIL3/Kat.4

EM 4/8 F-DI DC24V PROFIsafe: Powermodule für AK/SIL/Kat.

Kapazitives Übersprechen von digitalen Ein-/Ausgangssignalen

siehe *Kapitel 4.4.1*

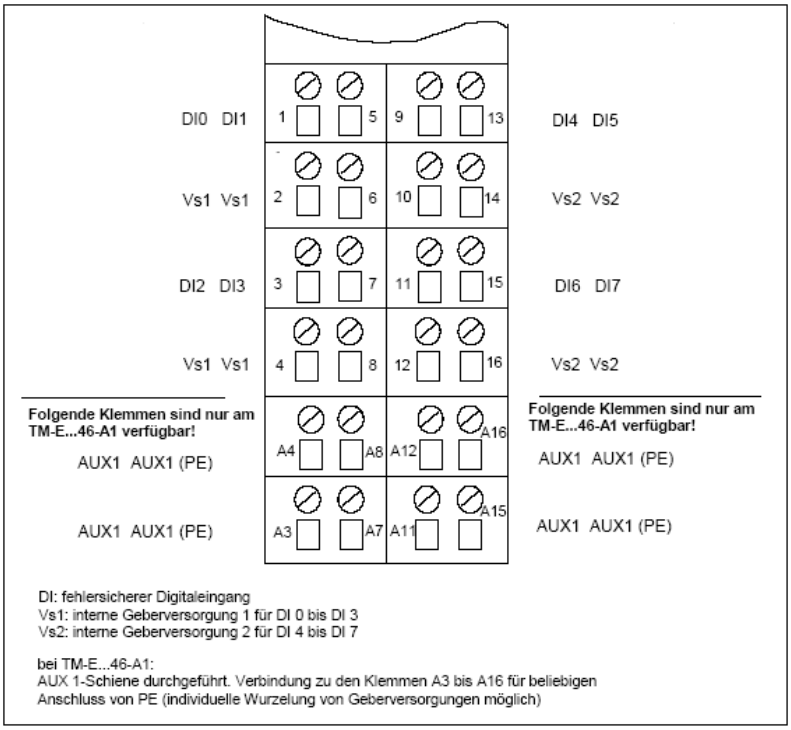
Frontansicht



Frontansicht EM 4/8 F-DI DC24V PROFIsafe

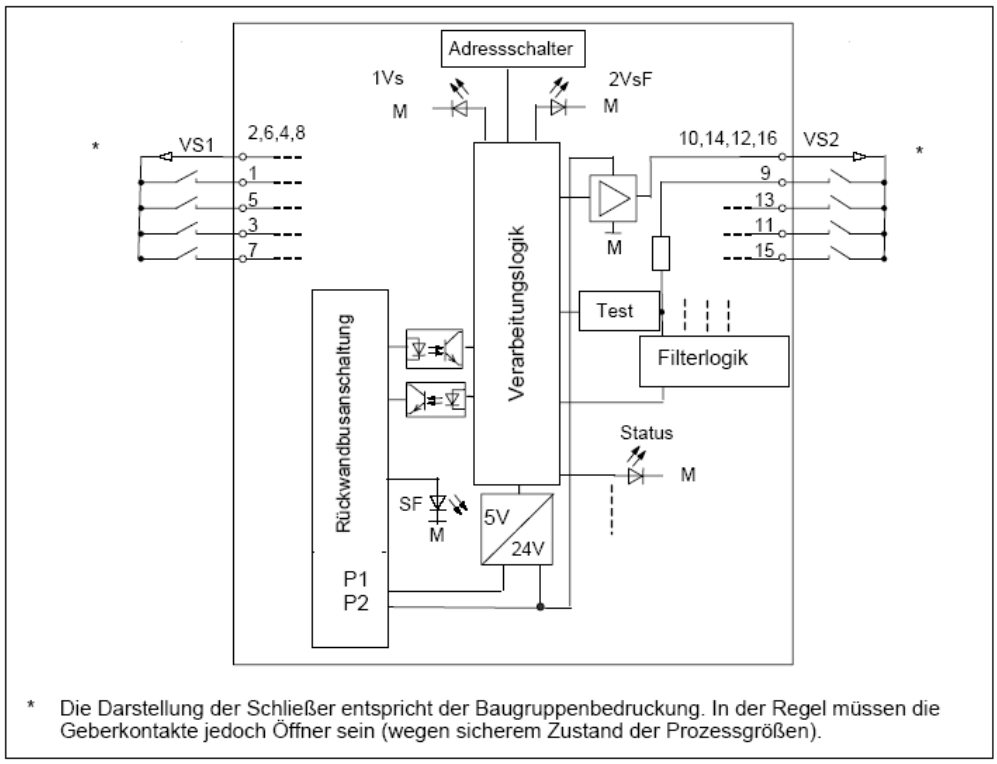
Anschlussbelegung

Im folgenden Bild finden Sie die Anschlussbelegung des EM 4/8 F-DI DC24V PROFIsafe für die einsetzbaren Terminalmodule TM-E30S44-01, TM-E30C44-01, TM-E30S46-A1 und TM-E30C46-A1.



Anschlussbelegung TM-E...44-01/TM-E...46-A1 für EM 4/8 F-DI DC24V PROFIsafe

Prinzipschaltbild



Prinzipschaltbild des EM 4/8 F-DI DC24V PROFIsafe

Parameter in *STEP 7*

In der folgenden Tabelle finden Sie die Parameter, die Sie für das EM 4/8 F-DI DC24V PROFIsafe einstellen können.

Parameter	Wertebereich	Voreinstellung	Art des Parameters	Wirkungsbereich
F-Parameter:				
F_Ziel_Adresse	1 bis 1022	wird von STEP 7 vergeben	statisch	Modul
F-Überwachungszeit	10 bis 10000 ms	150 ms	statisch	Modul
Baugruppenparameter:				
Eingangsverzögerung	0,5; 3; 15 ms	3 ms	statisch	Modul
Kurzschlusstest	zyklisch/sperren	zyklisch	statisch	Modul
Kanal n, n+4	aktiviert/deaktiviert	aktiviert	statisch	Kanalgruppe
Auswertung der Geber	2v2-Auswertung/ 1v1-Auswertung	2v2-Auswertung	statisch	Kanalgruppe
Art der Geberverschaltung	1-kanalig; 2-kanalig äquivalent; 2-kanalig antivalent	2-kanalig äquivalent	statisch	Kanalgruppe
Diskrepanzverhalten	letzten gültigen Wert bereitstellen; 0-Wert bereitstellen	0-Wert bereitstellen	statisch	Kanalgruppe
Diskrepanzzeit	10 bis 30000 ms	10 ms	statisch	Kanalgruppe

Parameter des EM 4/8 F-DI DC24V PROFIsafe

Hinweis Eingangsverzögerung

Zur Vermeidung einer Sicherheitsabschaltung bei einer parametrierten Eingangsverzögerung von **0,5 ms** oder **3 ms** müssen Sie für die fehlersicheren Digitaleingänge und die Geberversorgung **geschirmte** Leitungen verwenden. Als Alternative können Sie eine Eingangsverzögerung von 15 ms parametrieren.

Parameter Kurzschlusstest

Mit dem Parameter Kurzschlusstest wird der zyklische Kurzschlusstest aktiviert/deaktiviert. Der Kurzschlusstest ist nur sinnvoll beim Einsatz von einfachen Schaltern, die keine eigene Stromversorgung haben. Wenn Sie den Kurzschlusstest aktiviert haben, dann müssen Sie die internen Geberversorgungen verwenden.

Parameter Diskrepanzverhalten

Als .Diskrepanzverhalten. parametrieren Sie den Wert, der während der Diskrepanz zwischen den beiden betroffenen Eingangskanälen, d. h. bei laufender Diskrepanzzeit, dem Sicherheitsprogramm in der F-CPU zur Verfügung gestellt wird. Das Diskrepanzverhalten parametrieren Sie wie folgt:

- „letzten gültigen Wert bereitstellen“ oder
- „0-Wert bereitstellen“

Voraussetzungen

Sie haben Folgendes parametriert:

- Auswertung der Geber: .2v2-Auswertung. und
- Art der Geberverschaltung: „2-kanalig äquivalent“ oder „2-kanalig antivalent“

„Letzten gültigen Wert bereitstellen“

Der letzte, vor dem Auftreten der Diskrepanz gültige Wert (Altwert) wird dem Sicherheitsprogramm in der F-CPU zur Verfügung gestellt, sobald eine Diskrepanz zwischen den Signalen der beiden betroffenen Eingangskanäle festgestellt wird.

Dieser Wert wird solange bereitgestellt, bis die Diskrepanz verschwunden ist bzw. bis die Diskrepanzzeit abgelaufen ist und ein Diskrepanzfehler erkannt wird. Die Geber- Aktor-Reaktionszeit verlängert sich entsprechend um diese Zeit.

Daraus ergibt sich, dass die Diskrepanzzeit 2-kanalig angeschlossener Geber für Schnellreaktionen auf kurze Reaktionszeiten abgestimmt sein muss. So macht es z. B. keinen Sinn, wenn von 2-kanalig angeschlossenen Gebern mit einer Diskrepanzzeit von 500 ms eine zeitkritische Abschaltung angestoßen wird. Für den schlechtesten aller denkbaren Fälle verlängert sich die Geber- Aktor- Reaktionszeit etwa um die Diskrepanzzeit:

- Wählen Sie daher eine möglichst **diskrepanzarme** Anordnung der Geber im Prozess.
- Wählen Sie dann eine **möglichst kleine** Diskrepanzzeit, die andererseits hinreichende Reserve besitzt gegen Fehlauslösungen von Diskrepanzfehlern.

„0-Wert bereitstellen"

Der Wert „0" wird dem Sicherheitsprogramm in der F-CPU zur Verfügung gestellt, sobald eine Diskrepanz zwischen den Signalen der beiden betroffenen Eingangskanälen festgestellt wird.

Wenn Sie „0-Wert bereitstellen" parametriert haben, wird die Geber-Aktor-Reaktionszeit durch die Diskrepanzzeit nicht beeinflusst.

Diskrepanzzeit

Sie können hier für jedes Kanalpaar die Diskrepanzzeit festlegen. Der eingegebene Wert wird auf ganze Vielfache von 10 ms gerundet.

Voraussetzungen

Sie haben Folgendes parametriert:

- Auswertung der Geber: „2v2-Auswertung“ und
- Art der Geberverschaltung: „2-kanalig äquivalent“ oder „2-kanalig antivalent“

Diskrepanzanalyse und Diskrepanzzeit

Wenn Sie einen zweikanaligen, einen antivalenten oder zwei einkanalige Geber einsetzen, die dieselbe physikalische Prozessgröße erfassen, so werden die Geber beispielsweise aufgrund der begrenzten Genauigkeit ihrer Anordnung zueinander verzögert ansprechen.

Die Diskrepanzanalyse auf Äquivalenz/Antivalenz wird bei fehlersicheren Eingaben benutzt, um aus dem zeitlichen Verlauf zweier Signale gleicher Funktionalität auf Fehler zu schließen. Die Diskrepanzanalyse wird gestartet, wenn bei zwei zusammengehörigen Eingangssignalen unterschiedliche Pegel (bei Prüfung auf Antivalenz: gleiche Pegel) festgestellt werden. Es wird geprüft, ob nach Ablauf einer parametrierbaren Zeitspanne, der sogenannten Diskrepanzzeit, der Unterschied (bei Prüfung auf Antivalenz: die Übereinstimmung) verschwunden ist. Wenn nicht, liegt ein Diskrepanzfehler vor.

In den meisten Fällen wird die Diskrepanzzeit gestartet ohne vollständig abzulaufen, da die Signalunterschiede nach kurzer Zeit wieder ausgeglichen sind. Wählen Sie die Diskrepanzzeit so groß, dass im fehlerfreien Fall der Unterschied der beiden Signale (bei Prüfung auf Antivalenz: die Übereinstimmung der Signale) in jedem Fall verschwunden ist, bevor die Diskrepanzzeit abgelaufen ist.

Verhalten bei laufender Diskrepanzzeit

Während des modulinternen Ablaufs der parametrierten Diskrepanzzeit wird, in Abhängigkeit von der Parametrierung des Diskrepanzverhaltens, entweder der **letzte gültige Wert** oder **.0.** von den betroffenen Eingangskanälen dem Sicherheitsprogramm in der F-CPU zur Verfügung gestellt.

Verhalten nach Ablauf der Diskrepanzzeit

Falls nach Ablauf der parametrierten Diskrepanzzeit keine Übereinstimmung (bei Prüfung auf Antivalenz: Ungleichheit) der Eingangssignale vorliegt, z. B. durch Drahtbruch auf einer Geberleitung, wird ein Diskrepanzfehler erkannt und die Diagnosemeldung .Diskrepanzfehler" im Diagnosepuffer des F-Peripheriemoduls mit Angabe der fehlerhaften Kanäle generiert.

Bedingungen für das Erreichen der AK/SIL/Kat.

In der folgenden Tabelle sind die Bedingungen dargestellt, um die entsprechenden Sicherheitsanforderungen zu erreichen.

Anwendungsfall	Geber	Auswertung der Geber	Geberversorgung	erreichbare AK/SIL/Kat.
1	1-kanalig	1v1	intern, mit Kurzschlusstest	4 / 2 / 3
			intern, ohne Kurzschlusstest	
			extern	
2.1	1-kanalig	2v2	intern, mit Kurzschlusstest	6 / 3 / 3
			intern, ohne Kurzschlusstest	
			extern	
2.2	2-kanalig äquivalent	2v2	intern, ohne Kurzschlusstest	
			extern	
2.3	2-kanalig antivalent	2v2	intern, ohne Kurzschlusstest	
			extern	
3.1	2-kanalig äquivalent	2v2	intern, mit Kurzschlusstest	6 / 3 / 4
3.2	2-kanalig antivalent			

EM 4/8 F-DI DC24V PROFIsafe: Bedingungen für Erreichen der AK/SIL/Kat.

Hinweis

Sie können die verschiedenen Eingänge eines F-DI-Moduls gleichzeitig in AK4/SIL2/Kat.3 **und** in AK6/SIL3/Kat.3 bzw. Kat.4 betreiben. Sie müssen nur die Eingänge verschalten und parametrieren, wie in den folgenden Kapiteln gezeigt.

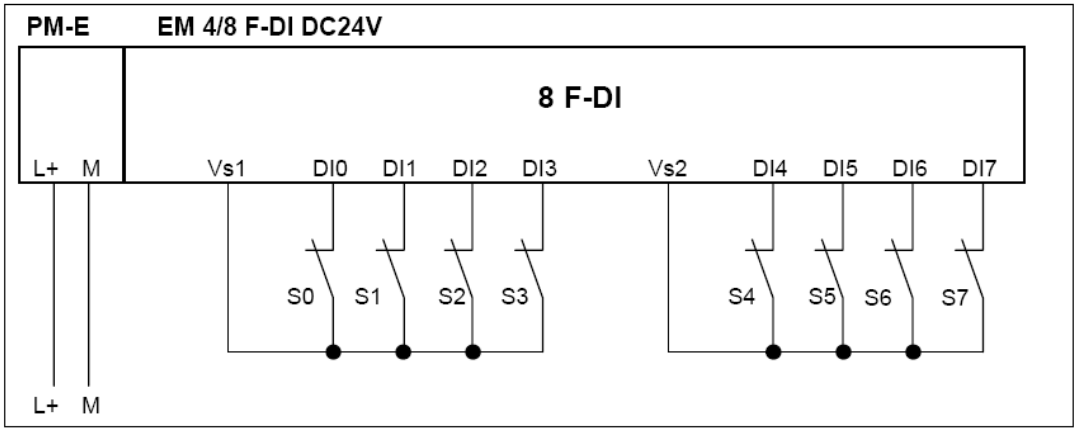
Anwendungsbeispiel 1: Sicherheitsbetrieb AK4/SIL2/Kat.3

Geberversorgung

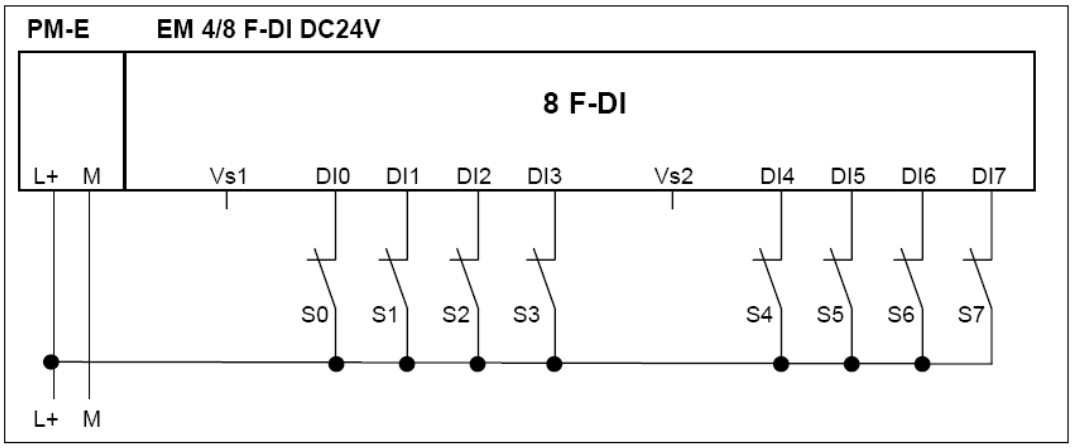
Das EM 4/8 F-DI DC24V PROFIsafe stellt für die Eingänge 0 bis 3 die Geberversorgung Vs1 und für die Eingänge 4 bis 7 die Geberversorgung Vs2 zur Verfügung. Die Geberversorgung kann von intern oder von extern erfolgen.

Verdrahtungsschema zum Anwendungsbeispiel 1 . einen Geber 1-kanalig anschließen

Pro Prozesssignal wird ein Geber 1-kanalig (1v1-Auswertung) angeschlossen. Die Verdrahtung nehmen Sie am passenden Terminalmodul vor.



Verdrahtungsschema EM 4/8 F-DI DC24V PROFIsafe . ein Geber 1-kanalig angeschlossen, interne GV



Verdrahtungsschema EM 4/8 F-DI DC24V PROFIsafe . ein Geber 1-kanalig angeschlossen, externe GV

Einstellbare Parameter zum Anwendungsbeispiel 1

Stellen Sie für den entsprechenden Eingang den Parameter .Auswertung der Geber. auf .1v1-Auswertung. Sie können den Parameter .Kurzschlusstest. aktivieren oder deaktivieren. Sobald jedoch mindestens ein fehlersicherer Digitaleingang **von extern** versorgt wird, müssen Sie den Kurzschlusstest deaktivieren. Andernfalls wird ggf. die Diagnose .Kurzschluss. gemeldet.

Besonderheiten bei der Fehlererkennung (Anwendungsbeispiel 1)

In der folgenden Tabelle ist die Fehlererkennung in Abhängigkeit von der Geberversorgung und der Parametrierung des Kurzschlusstests dargestellt:

Fehler, Beispiel	Fehlererkennung bei ...		
	interner GV und KS-Test aktiviert	interner GV u. KS-Test deaktiviert	externer GV
Kurzschluss DI 0 mit DI 1	nein	nein	nein
Kurzschluss DI 0 mit DI 4	ja*	nein	nein
P-Schluss DI 0	ja	nein	nein
M-Schluss DI 0	ja*	ja*	nein
Diskrepanzfehler	-	-	-
P-Schluss GV 1	ja	nein	nein
M-Schluss GV 1 oder GV 2 defekt	ja	ja	ja
Kurzschluss GV 1 mit GV 2	ja	nein	nein
Fehler in der Lese-/ Prüfschaltung	ja	ja	ja
Versorgungsspannungs-fehler	ja	ja	ja

* Die Fehlererkennung erfolgt nur bei einer Signalverfälschung. D. h., das gelesene Signal unterscheidet sich gegenüber dem Gebersignal. Wenn sich keine Signalverfälschung gegenüber dem Gebersignal ergibt, ist keine Fehlererkennung möglich und sicherheitstechnisch auch nicht erforderlich.

EM 4/8 F-DI DC24V PROFIsafe: Fehlererkennung (Anwendungsbeispiel 1)

Anwendungsbeispiel 2: Sicherheitsbetrieb AK6/SIL3/Kat.3

Zuordnung der Eingänge zueinander

Das EM 4/8 F-DI DC24V PROFIsafe hat 8 fehlersichere Eingänge DI 0 bis DI 7 (SIL2). Je zwei dieser Eingänge können als ein Eingang (SIL3) verwendet werden. Dabei gilt folgende Zuordnung:

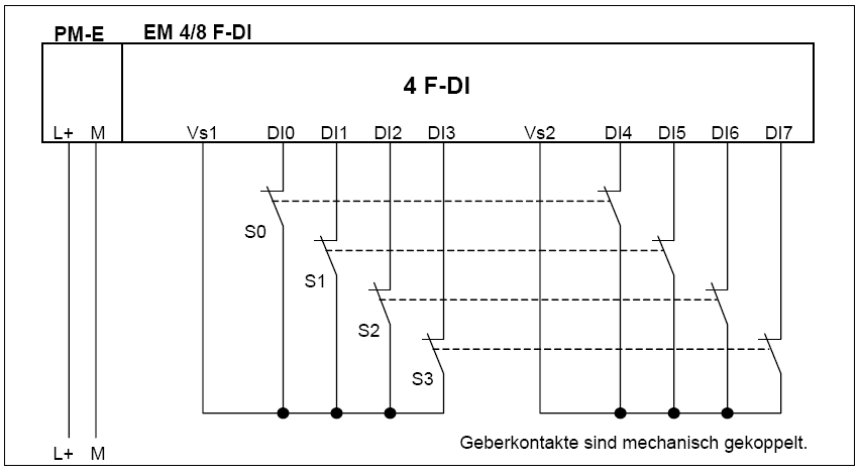
- DI 0 mit DI 4
- DI 1 mit DI 5
- DI 2 mit DI 6
- DI 3 mit DI 7

Geberversorgung

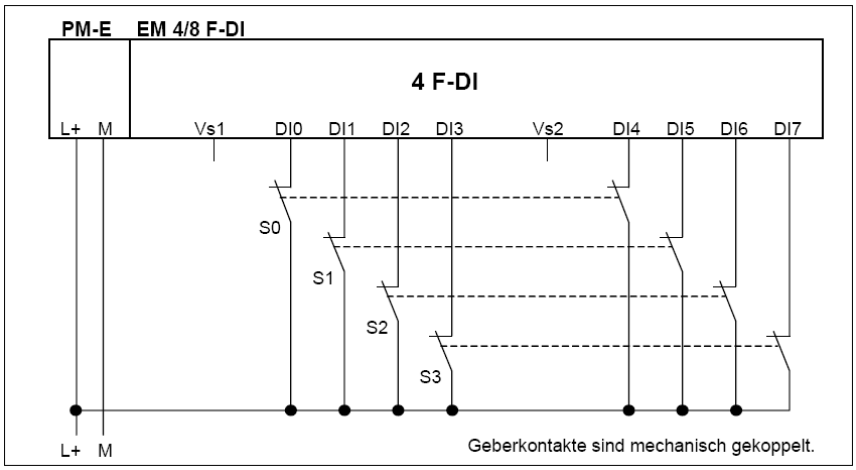
Das EM 4/8 F-DI DC24V PROFIsafe stellt für die Eingänge 0 bis 3 die Geberversorgung Vs1 und für die Eingänge 4 bis 7 die Geberversorgung Vs2 zur Verfügung. Die Geberversorgung kann von intern oder auch von extern erfolgen.

Verdrahtungsschema zum Anwendungsbeispiel 2 . einen zweikanaligen Geber 2-kanalig anschließen

Pro Prozesssignal wird ein zweikanaliger Geber 2-kanalig an zwei Eingänge des F-Moduls angeschlossen (2v2-Auswertung). Die Verdrahtung nehmen Sie am passenden Terminalmodul vor.



Verdrahtungsschema EM 4/8 F-DI DC24V . ein zweikanaliger Geber 2-kanalig angeschlossen, interne GV



Verdrahtungsschema EM 4/8 F-DI DC24V . ein zweikanaliger Geber 2-kanalig angeschlossen, externe GV

Warnung
Um mit dieser Verdrahtung AK6/SIL3/Kat.3 zu erreichen, ist ein entsprechend qualifizierter Geber erforderlich.

Einstellbare Parameter zum Anwendungsbeispiel 2
Stellen Sie für den entsprechenden Eingang den Parameter „Auswertung der Geber“ auf „2v2-Auswertung“ und den Parameter „Art der Geberverschaltung“ Auf „2-kanalig äquivalent“. Deaktivieren Sie den Parameter „Kurzschlusstest“.

Besonderheiten bei der Fehlererkennung (Anwendungsbeispiel 2)

In der folgenden Tabelle ist die Fehlererkennung in Abhängigkeit von der Geberversorgung und der Parametrierung des Kurzschlusstests dargestellt:

Fehler, Beispiel	Fehlererkennung bei ...	
	interner GV u. KS-Test deaktiviert	externer GV
Kurzschluss DI 0 mit DI 1	ja*	ja*
Kurzschluss DI 0 mit DI 4	nein	nein
Kurzschluss DI 0 mit DI 5	ja*	ja*
P-Schluss DI 0	ja*	ja*
M-Schluss DI 0	ja*	ja*
Diskrepanzfehler	ja	ja
P-Schluss GV 1	nein	nein
M-Schluss GV 1 oder GV 2 defekt	ja	ja
Kurzschluss GV 1 mit GV 2	nein	nein
Fehler in der Lese-/Prüfschaltung	ja	ja
Versorgungsspannungsfehler	ja	ja

* Die Fehlererkennung erfolgt nur bei einer Signalverfälschung. D. h., das gelesene Signal unterscheidet sich gegenüber dem Gebersignal (Diskrepanzfehler). Wenn sich keine Signalverfälschung gegenüber dem Gebersignal ergibt, ist keine Fehlererkennung möglich und sicherheitstechnisch auch nicht erforderlich.

EM 4/8 F-DI DC24V PROFIsafe: Fehlererkennung (Anwendungsbeispiel 2)

5.4.3 Digitales Elektronikmodul 4 F-DO DC24V/2A PROFIsafe (6ES7 138-4FB01-0AB0)

Eigenschaften

Das digitale Elektronikmodul 4 F-DO DC24V/2A PROFIsafe verfügt über folgende Eigenschaften:

- 4 Ausgänge, P-/M-schaltend
- Ausgangsstrom 2 A
- Lastnennspannung DC 24 V
- geeignet für Magnetventile, Gleichstromschütze und Meldeleuchten
- Sammelfehleranzeige (SF; rote LED)
- Statusanzeige pro Ausgang (grüne LED)
- parametrierbare Diagnose
- erreichbare Sicherheitsklasse SIL3

Einsetzbare Powermodule für SIL2 oder SIL3

Powermodul	erreichbare AK/SIL/Kat.
Versorgung durch PM-E DC24V	AK4/SIL2/Kat.3
Versorgung durch PM-E DC24V/AC120/230V	AK6/SIL3/Kat.4
Versorgung durch PM-E DC24..48V	AK6/SIL3/Kat.4

EM 4 F-DO DC24V/2A PROFIsafe: Powermodule für AK/SIL/Kat.

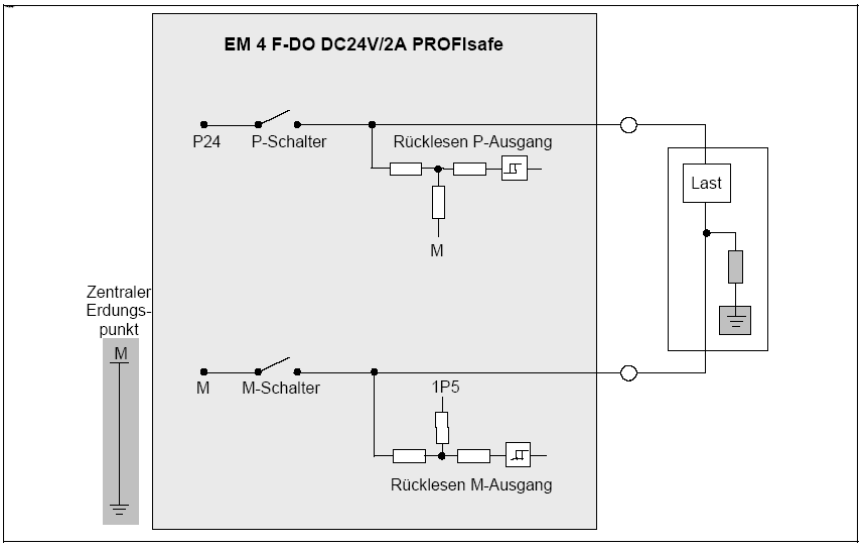
Schalten von Lasten, die nicht erdfrei aufgebaut sind

Wenn vom EM 4 F-DO DC24V/2A PROFIsafe Lasten geschaltet werden, die eine Verbindung zwischen Masse und Erde aufweisen (z. B. zur Verbesserung der EMV- Eigenschaften) **und** wenn beim versorgenden Netzteil Masse und Erde verbunden sind, dann wird .Kurzschluss. erkannt.

Aus Sicht des F-Moduls wird durch die Masse-Erde-Verbindung der M-Schalter überbrückt (siehe folgendes Bild als Beispiel für ein EM 4 F-DO DC24V/2A PROFIsafe).

Abhilfe:

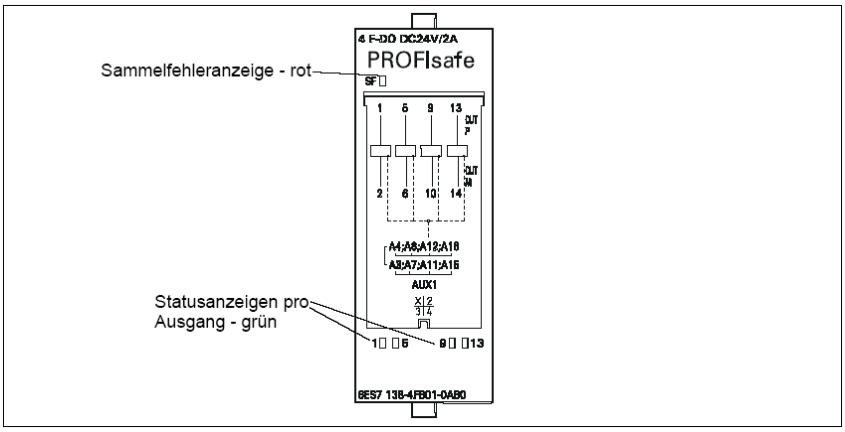
- Einsatz des PM-E F pp DC24V PROFIsafe
- der lastseitige Widerstandswert zwischen Masse und Erde muss größer 100 kΩ sein



Schalten von nicht erdfreien Lasten (Widerstand zwischen Masse und Erde vorhanden)

Kapazitives Übersprechen von digitalen Ein-/Ausgangssignalen
siehe *Kapitel 4.4.1*

Frontansicht

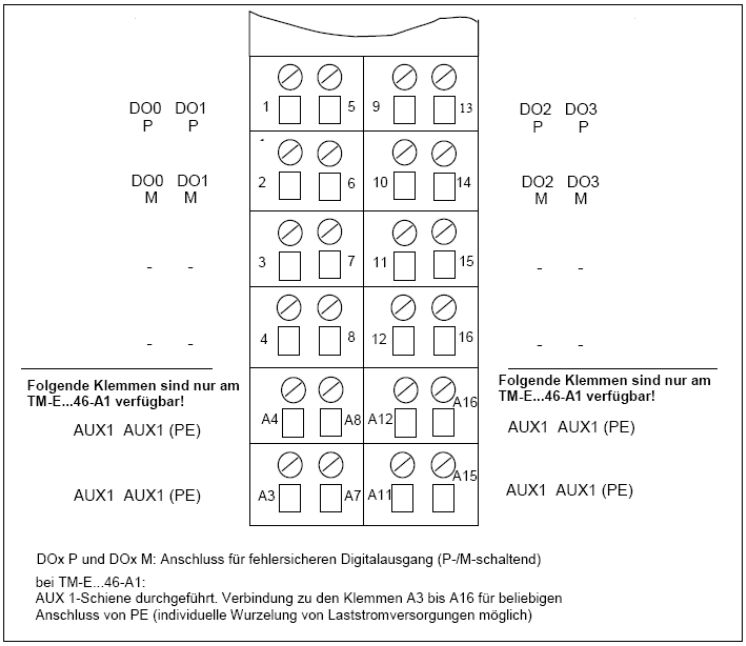


Frontansicht EM 4 F-DO DC24V/2A PROFIsafe

Warnung
Die SF-LED und die Statusanzeigen der Ausgänge dürfen nicht fürsicherheitsgerichtete Aktivitäten ausgewertet werden.

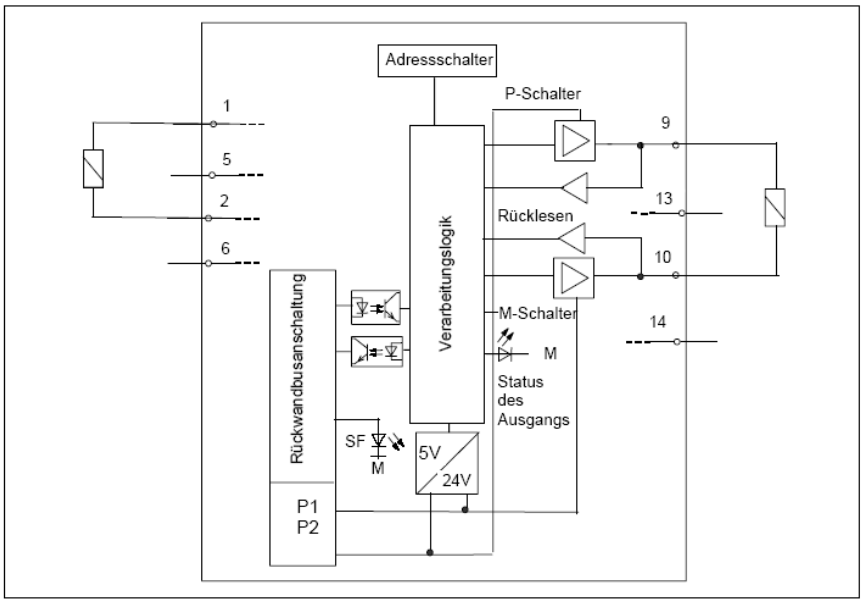
Anschlussbelegung

Im folgenden Bild finden Sie die Anschlussbelegung des EM 4 F-DO DC24V/2APROFIsafe für die einsetzbaren Terminalmodule TM-E30S44-01, TM-E30C44-01,TM-E30S46-A1 und TM-E30C46-A1.



Anschlussbelegung TM-E...44-01/TM-E...46-A1 für EM 4 F-DO DC24V/2A PROFIsafe

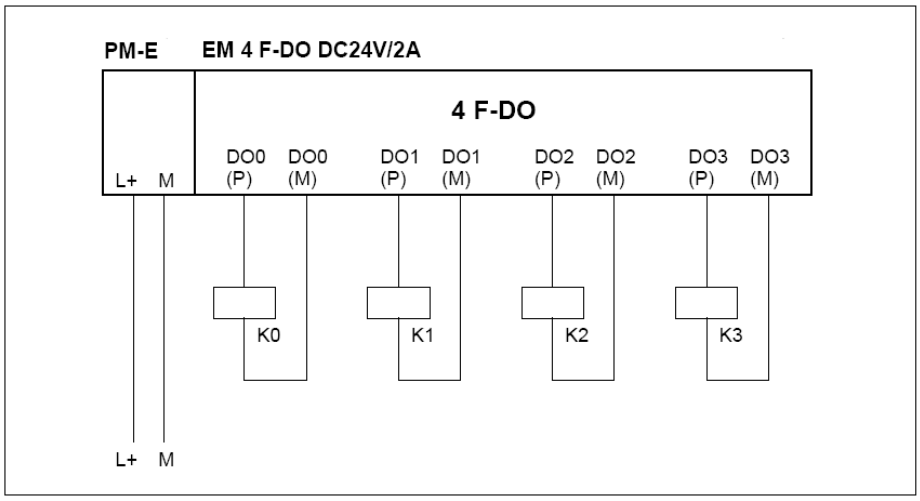
Prinzipschaltbild



Prinzipschaltbild des EM 4 F-DO DC24V/2A PROFIsafe

Verdrahtungsschema

Jeder der 4 fehlersicheren Digitalausgänge besteht aus einem P-Schalter DOx P und einem M-Schalter DOx M. Sie schließen die Last zwischen P- und M-Schalter an. Damit Spannung an der Last anliegt, werden immer beide Schalter angesteuert. Die Verdrahtung nehmen Sie an einem passenden Terminalmodul vor.



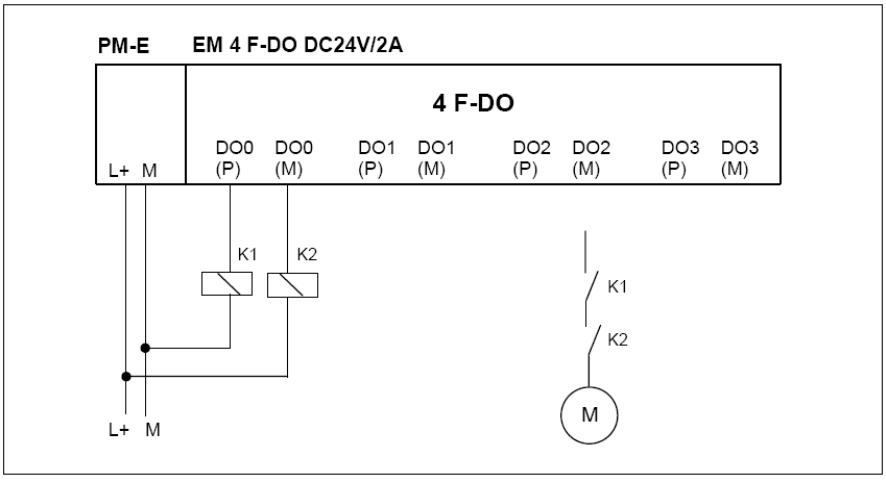
Verdrahtungsschema des EM 4 F-DO DC24V/2A PROFIsafe

Anschluss von 2 Relais an 1 Digitalausgang

Sie können 2 Relais mit einem fehlersicheren Digitalausgang schalten. Beachten
Sie bitte die folgenden Bedingungen:

- L+ und M der Relais müssen mit L+ und M des F-DO-Moduls verbunden werden (gleiches Bezugspotenzial ist notwendig).
- Die Arbeitskontakte der beiden Relais müssen in Reihe geschaltet werden. Der Anschluss ist an

jedem der 4 Digitalausgänge möglich. Im folgenden Bild finden Sie als Beispiel den Anschluss an DO 0. Sie erreichen mit dieser Schaltung AK6/SIL3/Kat.4.

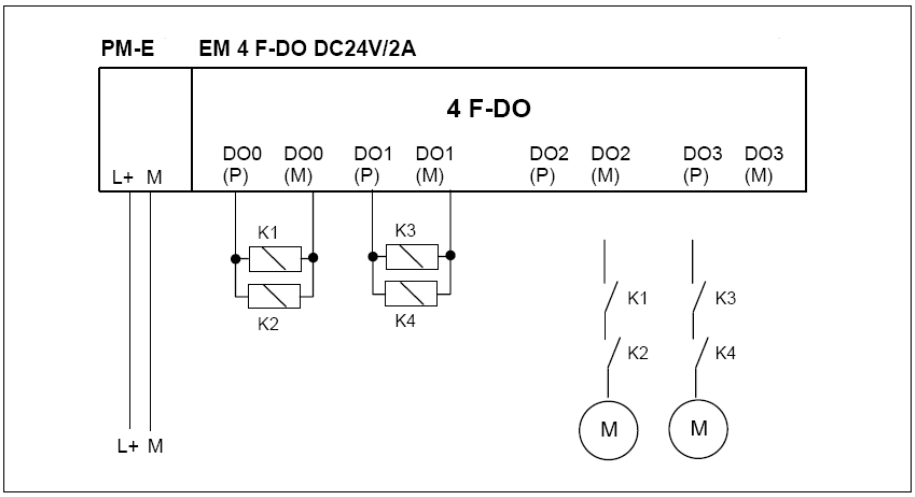


Verdrahtungsschema je 2 Relais an 1 F-DO des EM 4 F-DO DC24V/2A PROFIsafe

Warnung
Beim Anschluss von 2 Relais an einem Digitalausgang (wie im Bild oben) werden die Fehler „Drahtbruch“ und „Überlast“ nur am P-Schalter des Ausgangs erkannt (nicht am M-Schalter). Bei einem Querschluss zwischen P- und M-Schalter des Ausgangs wird der angesteuerte Aktor nicht mehr abgeschaltet.

Warnung
Um Querschlüsse zwischen P- und M-Schalter eines fehlersicheren Digitalausgangs zu vermeiden, müssen Sie die Leitungen für den Anschluss der Relais am P- und M-Schalter querschlusssicher verlegen (z. B. als separat ummantelte Leitungen oder in eigenen Kabelkanälen).

Vermeidung/Beherrschung von Querschlüssen
Um Querschlüsse zwischen P- und M-Schalter eines fehlersicheren Digitalausgangs zu beherrschen, empfehlen wir Ihnen die folgende Verdrahtungsvariante:



Verdrahtungsschema je 2 Relais parallel an 1 F-DO des EM 4 F-DO DC24V/2A PROFIsafe

Hinweis
Beim parallelen Anschluss von 2 Relais an einem Digitalausgang (wie im Bild oben) wird der Fehler „Drahtbruch“ nur erkannt, wenn durch den Drahtbruch beide Relais von P oder M getrennt werden. Diese Diagnose ist nicht sicherheitsrelevant.

Parameter in *STEP 7*

In der folgenden Tabelle finden Sie die Parameter, die Sie für das F-DO-Modul einstellen können.

Parameter	Wertebereich	Voreinstellung	Art des Parameters	Wirkungsbereich
F-Parameter:				
F_Ziel_Adresse	1 bis 1022	wird von STEP 7 vergeben	statisch	Modul
F-Überwachungszeit	10 bis 10000 ms	150 ms	statisch	Modul
Baugruppenparameter:				
DO-Kanal n	aktiviert/deaktiviert	aktiviert	statisch	Kanal
Rücklesezeit	1 bis 400 ms	1 ms	statisch	Kanal
Diagnose: Drahtbruch	aktiviert/deaktiviert	deaktiviert	statisch	Kanal

Parameter des F-DO- Moduls

Rücklesezeit

Jeder Ausgangskanal verfügt über eine eigene parametrierbare Rücklesezeit. Diese Zeit legt die maximale Dauer des Ausschalttests für den entsprechenden Kanal und somit auch die Rücklesezeit für den Ausschaltvorgang des Kanals fest.

Folgende Rücklesezeiten sind parametrierbar: 1 ms, 5 ms, 10 ms, 50 ms, 100 ms, 200 ms und 400 ms.

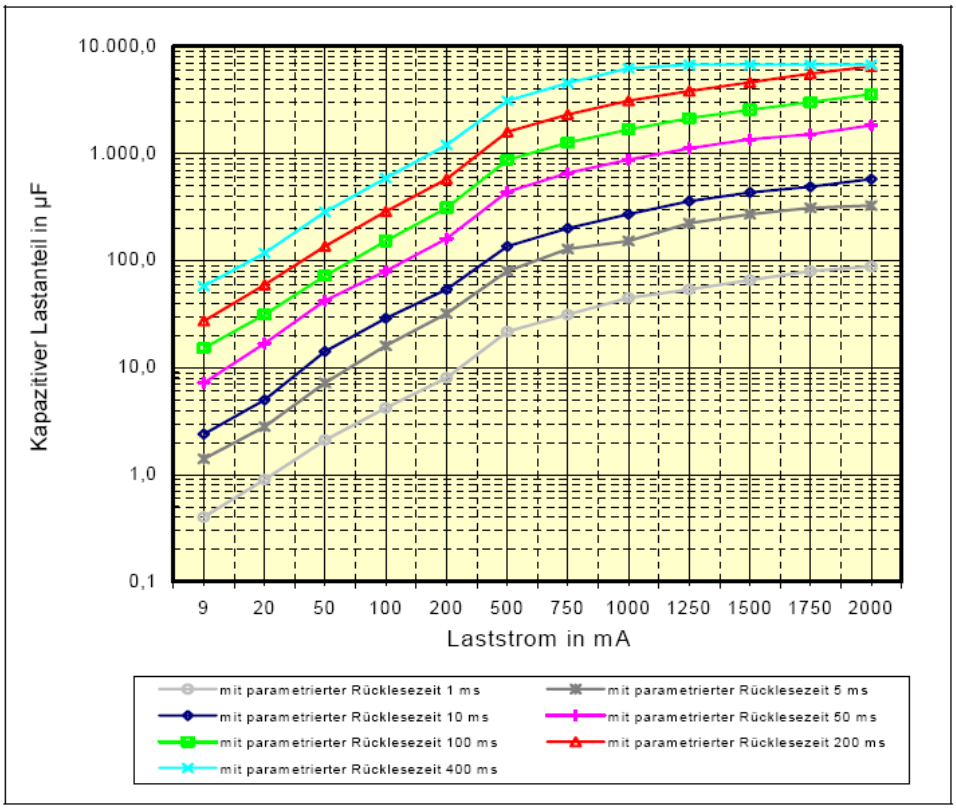
Sie sollten die Rücklesezeit hinreichend groß einstellen, wenn der betroffene Kanal große kapazitive Lasten schaltet. Ist die Rücklesezeit für eine angesteuerte kapazitive Last zu klein eingestellt, wird der Ausgangskanal passiviert, weil die Entladung der Kapazität nicht innerhalb des Ausschalttests erfolgt.

Bei falschen Rücklesesignalen wird die parametrierte Rücklesezeit abgewartet, bevor der Fehler „Kurzschluss" zur Passivierung des Ausgangskanals führt. **Schalten von kapazitiven Lasten**

Wenn die elektronischen Ausgänge des EM 4 F-DO DC24V/2A PROFIsafe mit Lasten verschaltet werden, die wenig Strom verbrauchen und eine Kapazität aufweisen, dann kann es zu der Fehlermeldung „Kurzschluss" kommen. Grund:

Während der parametrierten Rücklesezeit beim Selbsttest werden die Kapazitäten nicht genügend entladen.

Das folgende Bild zeigt zu den parametrierbaren Rücklesezeiten typische Kurven für den Zusammenhang zwischen Lastwiderstand und schaltbarer Lastkapazität.



Zusammenhang zwischen Lastwiderstand und schaltbarer Lastkapazität für EM 4 F-DO DC24V/2A PROFIsafe

Abhilfe:

1. Bestimmen Sie den Laststrom und die Kapazität der Last.
2. Bestimmen Sie den Arbeitspunkt im obigen Bild.
3. Wenn der Arbeitspunkt oberhalb der Kurve liegt, dann müssen Sie durch Parallelschalten eines Widerstandes den Laststrom so weit erhöhen, dass der neue Arbeitspunkt unterhalb der Kurve liegt.

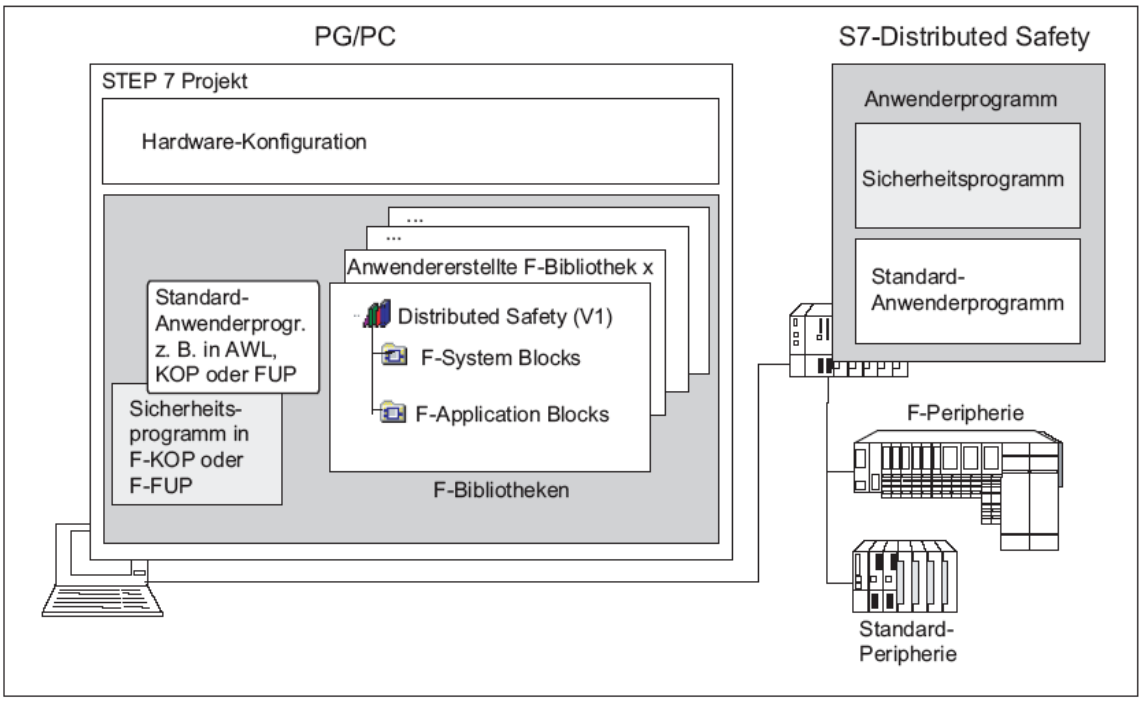
6 Sicherheitsgerichtete Programmierung

6.1 Einführung in die sicherheitsgerichtete Programmierung

Ein Sicherheitsprogramm besteht aus F-Bausteinen, die Sie mit der Programmiersprache F-FUP oder F-KOP erstellen oder aus einer F-Bibliothek auswählen, und F-Bausteinen, die beim Generieren des Sicherheitsprogramms automatisch ergänzt werden. Damit wird das von Ihnen erstellte Sicherheitsprogramm automatisch um Fehlerbeherrschungsmaßnahmen ergänzt und es werden zusätzliche sicherheitsrelevante Überprüfungen durchgeführt.

Aufbau eines Projekts mit Standard-Anwenderprogramm und Sicherheitsprogramm

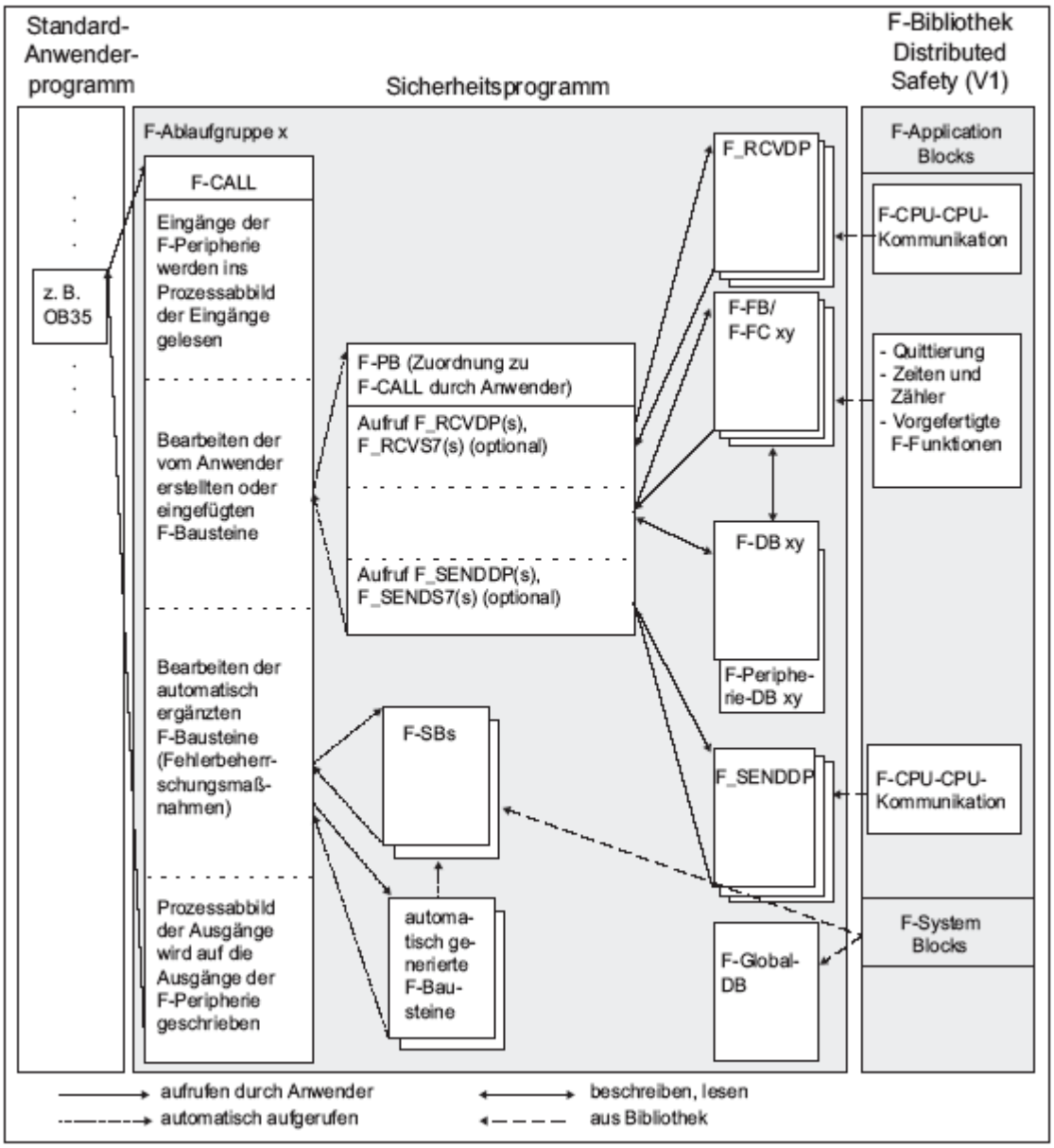
Im folgenden Bild ist der schematische Aufbau eines *STEP 7*-Projekts mit Standard-Anwenderprogramm und Sicherheitsprogramm für S7 Distributed Safety dargestellt.
Für die Programmierung des Sicherheitsprogramms wird mit dem Optionspaket *S7 Distributed Safety* die F-Baustein-Bibliothek *Distributed Safety* (V1) mitgeliefert. Die F-Bibliothek befindet sich im Verzeichnis *step7/s7libs*.



6.2 Programmstruktur des Sicherheitsprogramms

Das folgende Bild zeigt den schematischen Aufbau eines Sicherheitsprogramms für S7 Distributed Safety. Ein Sicherheitsprogramm besteht zur Strukturierung aus einer oder zwei F-Ablaufgruppen. Jede F-Ablaufgruppe enthält:

- F-Bausteine, die von Ihnen erstellt, aus der F-Bibliothek *Distributed Safety* (V1) oder einer anwendererstellten F-Bibliothek ausgewählt werden und
- F-Bausteine, die automatisch ergänzt werden (F-Systembausteine F-SBs, automatisch generierte F-Bausteine und der F-Global-DB)



Erläuterung der Programmstruktur

Der Einstieg in das Sicherheitsprogramm erfolgt mit dem Aufruf des F-CALL aus dem Standard-Anwenderprogramm heraus. Rufen Sie den F-CALL direkt in einem OB auf, am Besten in einem Weckalarm- OB (z. B. OB 35).
Weckalarm- OBs haben den Vorteil, dass sie die zyklische Programmbearbeitung im OB 1 des Standard-Anwenderprogramms in festen zeitlichen Abständen unterbrechen, d. h. in einem Weckalarm- OB wird das Sicherheitsprogramm in festen zeitlichen Abständen aufgerufen und durchlaufen.
Nach der Abarbeitung des Sicherheitsprogramms wird das Standard- Anwenderprogramm weiterbearbeitet.

F-Ablaufgruppen
Zur besseren Hantierbarkeit besteht ein Sicherheitsprogramm aus einer oder zwei "F-Ablaufgruppen". Bei einer F-Ablaufgruppe handelt es sich um ein logisches Konstrukt aus mehreren zusammengehörigen F-Bausteinen, das intern vom F-System gebildet wird.
Eine F-Ablaufgruppe besteht aus:

- einem F-Aufrufbaustein F-CALL
- einem F-Programmbaustein F-PB (das ist ein F-FB/F-FC, den Sie dem F-CALL zuweisen)
- ggf. weiteren F- FBs/F- FCs, die Sie mit F-FUP/F-KOP programmieren
- ggf. einem oder mehreren F- DBs
- F- Peripherie- DBs
- F-Bausteinen der F-Bibliothek *Distributed Safety* (V1)
- F-Bausteinen aus anwendererstellten F-Bibliotheken
- F-Systembausteinen F- SBs
- automatisch generierten F-Bausteinen

Strukturierung des Sicherheitsprogramms in zwei F-Ablaufgruppen
Ab *S7 Distributed Safety* V 5.3 können Sie Ihr Sicherheitsprogramm in zwei F-Ablaufgruppen aufteilen. Wenn Sie Teile des Sicherheitsprogramms (eine F-Ablaufgruppe) in einer schnelleren Ablaufebene ablaufen lassen, erreichen Sie schnellere Sicherheitskreise mit kurzen Reaktionszeiten.

6.3 Fehlersichere Bausteine

6.3.1 F-Bausteine einer F-Ablaufgruppe

In einer F-Ablaufgruppe verwenden Sie die folgenden F-Bausteine :

- F-CALL (Erstellsprache F-CALL)

F-Baustein für den Aufruf der F-Ablaufgruppe aus dem Standard- Anwenderprogramm heraus. Der F-CALL enthält den Aufruf für den F-Programmbaustein und die Aufrufe für die automatisch ergänzten F-Bausteine der F-Ablaufgruppe.
Der F-CALL wird von Ihnen angelegt, kann aber von Ihnen nicht editiert werden.

- F-FB/F-FC/F-PB (Erstellsprache F-FUP/F-KOP)

Die eigentliche Sicherheitsfunktion programmieren Sie mit Hilfe von F-FUP
oder F-KOP. Einstieg in die F-Programmierung ist der F-Programmbaustein.
Der F-PB ist ein F-FC oder F-FB (mit Instanz-DB), der durch die Zuordnung zum F-CALL zum F-PB wird. Im F-PB können Sie:

- das Sicherheitsprogramm mit F-FUP oder F-KOP programmieren
- weitere erstellte F-FBs/F-FCs zur Strukturierung des Sicherheitsprogramms aufrufen
- F-Bausteine des Bausteincontainers *F-Application Blocks* (FApplikationsbausteine) aus der F-Bibliothek *Distributed Safety* (V1) einfügen
- F-Bausteine aus "anwendererstellten F-Bibliotheken" einfügen

Innerhalb des F-PB bestimmen Sie die Aufrufreihenfolge der F-Bausteine.

- F-DB (Erstellsprache F-DB)

Von Ihnen optional einsetzbare fehlersichere Datenbausteine, auf die innerhalb des gesamten Sicherheitsprogramms lesend und schreibend zugegriffen werden kann.

- F-Peripherie-DB

Zu jeder F-Peripherie wird beim Übersetzen in *HW Konfig* automatisch ein F-Peripherie-DB erzeugt. Auf die Variablen des F-Peripherie-DB können oder müssen Sie im Zusammenhang mit F-Peripheriezugriffen zugreifen

6.3.2 F-Bausteine der F-Bibliothek *Distributed Safety (V1)*

In der F-Bibliothek *Distributed Safety* (V1) finden Sie:

- den Bausteincontainer *F-Application Blocks* und
- den Bausteincontainer *F-System Blocks*

F-Application Blocks
enthält die F-Applikationsbausteine, die von Ihnen im F-PB/F-FBs/F-FCs aufgerufen werden können. Dabei gibt es Bausteine für die folgenden Anwendungsfälle:

- Sicherheitsgerichtete CPU-CPU- Kommunikation

F_SENDDP, F_RCVDP, F_SENDS7 und F_RCVS zum Senden und Empfangen von Daten bei sicherheitsgerichteter CPU-CPU-Kommunikation

- Quittierung

F_ACK_OP für eine fehlersichere Quittierung über ein Bedien- und Beobachtungssystem

- Zeiten und Zähler

F-Applikationsbausteine F_TP, F_TON, F_TOF;
F-Applikationsbausteine F_CTU, F_CTD, F_CTUD

- Vorgefertigte F-Funktionen

F-Applikationsbausteine für z. B. Zweihandüberwachung, Muting, NOT-AUS, Schutztürüberwachung, Rückführkreisüberwachung

- Datenkonvertierung und Skalierung

F-Applikationsbausteine F_SCA_I, F_BO_W, F_W_BO

- Kopieren F-Applikationsbausteine F_INT_WR, F_INT_RD
- Schiebeoperationen F-Applikationsbausteine F_SHL_W, F_SHR_W

F-System Blocks
enthält die F-Systembausteine (F-SBs) und den F-Global-DB enthält, die automatisch im Sicherheitsprogramm eingefügt werden

- Die F-Systembausteine (F-SBs) werden von *S7 Distributed Safety* beim Generieren des Sicherheitsprogramms automatisch eingefügt, um aus dem von Ihnen programmierten Sicherheitsprogramm ein ablauffähiges Sicherheitsprogramm zu erzeugen.
Sie dürfen F-Systembausteine aus dem Bausteincontainer *F-System Blocks* nicht in einen F-PB/F-FB/F-FC einfügen und weder in der F-Bibliothek *Distributed Safety* (V1) noch in dem Bausteincontainer Ihres Anwenderprojekts verändern (umbenennen) oder löschen!

- F-Global-DB Fehlersicherer Datenbaustein, der alle globalen Daten

des Sicherheitsprogramms und zusätzliche Informationen enthält, die das F-System benötigt.
Der F-Global-DB wird beim Speichern und Übersetzen der Hardware-Konfiguration automatisch eingefügt und erweitert. Über seinen symbolischen Namen F_GLOBDB können Sie bestimmte Daten des Sicherheitsprogramms im Standard-Anwenderprogramm auswerten.

6.3.3 Übersicht F-Applikationsbausteine

Bausteinnummer	Bausteinname	Funktion
FB179	F_SCA_I	Werte vom Datentyp INT skalieren
FB181	F_CTU	Vorwärtszählen
FB182	F_CTD	Rückwärtszählen
FB183	F_CTUD	Vor- und Rückwärtszählen
FB184	F_TP	Erzeugen eines Impulses
FB185	F_TON	Erzeugen einer Einschaltverzögerung
FB186	F_TOF	Erzeugen einer Ausschaltverzögerung
FB187	F_ACK_OP	Fehlersichere Quittierung
FB188	F_2HAND	Zweihandüberwachung
FB189	F_MUTING	Muting
FB 190	F_1oo2DI	2v2-Auswertung mit Diskrepanzanalyse
FB 211	F_2H_EN	Zweihandüberwachung mit Freigabe
FB 212	F_MUT_P	Paralleles Muting
FB 215	F_ESTOP1	NOT-AUS bis Stop-Kategorie 1
FB 216	F_FDBBACK	Rückführkreisüberwachung
FB 217	F_SFDOOR	Schutztürüberwachung
FB223	F_SENDDP	Senden von Daten (16 BOOL, 2 INT) über PROFIBUS DP
FB224	F_RCVDP	Empfangen von Daten (16 BOOL, 2 INT) über PROFIBUS DP
FB 225	F_SENDS7	Für CPUs 4xxF: Senden von Daten (aus F-DB) über S7-Verbindungen
FB 226	F_RCVS7	Für CPUs 4xxF: Empfangen von Daten (aus F-DB) über S7-Verbindungen
FC 174	F_SHL_W	16 Bit links schieben
FC 175	F_SHR_W	16 Bit rechts schieben
FC 176	F_BO_W	16 Daten vom Datentyp BOOL in Datum vom Datentyp WORD konvertieren
FC 177	F_W_BO	Datum vom Datentyp WORD in 16 Daten vom Datentyp BOOL konvertieren
FC 178	F_INT_WR	Wert vom Datentyp INT indirekt in einen F-DB schreiben
FC 179	F_INT_RD	Wert vom Datentyp INT indirekt aus einem F-DB lesen

Weitere Detailinformation erhalten Sie aus der Online-Hilfe.

6.4 Programmieren in F-FUP / F-KOP

Die Programmiersprachen F-FUP und F-KOP entsprechen grundsätzlich dem Standard- FUP/KOP. Zur Programmierung wird der Standard- *FUP/KOP-Editor* in *STEP 7* verwendet.
F-FUP und F-KOP unterscheiden sich vom Standard im Wesentlichen durch Einschränkungen im Operationsvorrat und bei den verwendbaren Datentypen und Operandenbereichen.

Unterstützte Daten- und Parametertypen
In F-FUP/F-KOP werden die folgenden elementaren Datentypen unterstützt:

- BOOL
- INT
- WORD
- TIME

Nicht zulässige Daten- und Parametertypen

- oben nicht aufgeführte elementare Datentypen (z. B. BYTE, DWORD, DINT, REAL)
- zusammengesetzte Datentypen (z. B. STRING, ARRAY, STRUCT, UDT)
- Parametertypen (z. B. BLOCK_FB, BLOCK_DB, ANY)

Unterstützte Operandenbereiche
Der Systemspeicher einer F-CPU ist in dieselben Operandenbereiche aufgeteilt wie der einer Standard- CPU. Im Sicherheitsprogramm können Sie auf die in der nachfolgenden Tabelle aufgeführten Operandenbereiche zugreifen. Beachten Sie dabei, dass Sie in F-FUP/F-KOP auf

- Daten vom Datentyp BOOL nur bitweise
- Daten vom Datentyp INT nur wortweise
- Daten vom Datentyp WORD nur wortweise
- Daten vom Datentyp TIME nur doppelwortweise zugreifen können.

Beispiel: Auf Eingangskanäle vom Datentyp BOOL im Prozessabbild der Eingänge von F-Peripherie können Sie nur über die Einheit "Eingang (Bit)" zugreifen.
Diese Einschränkung besteht nicht beim Zugriff auf Daten aus dem Standard- Anwenderprogramm (Merker oder Prozessabbild von Standard-Peripherie), wenn für diese in der Symboltabelle kein Datentyp deklariert wurde.
Auf diese Daten können Sie jedoch immer nur über dieselbe Einheit zugreifen. Beispiel: Wenn Sie auf M0.0 zugreifen, können Sie nicht auch auf MW0 zugreifen.
In einem Sicherheitsprogramm sollten Sie aus Gründen der Übersichtlichkeit immer über symbolische Namen auf die Operandenbereiche zugreifen.

Prozessabbild der Eingänge von F-Peripherie

Zu Beginn der F-Ablaufgruppe (F-CALL) liest die F-CPU die Eingänge aus der F-Peripherie und speichert die Werte in das Prozessabbild der Eingänge. Auf Eingangskanäle kann nur lesend zugegriffen werden. Deshalb ist auch keine Übergabe an Durchgangs-(IN_OUT-)Parameter eines F-FB oder F-FC zulässig.

- Kanäle vom Datentyp BOOL, z. B. digitale Kanäle

Auf Eingangskanäle vom Datentyp BOOL kann nur bitweise lesend über die Einheit "Eingang (E)" zugegriffen werden. Ein Zugriff z. B. mit der Einheit "Eingangswort" ist nicht zulässig.

- Kanäle vom Datentyp INT (WORD), z. B. analoge Kanäle

Auf Eingangskanäle vom Datentyp INT (WORD) kann nur lesend über die Einheit "Eingangswort (EW)" zugegriffen werden. Ein Zugriff auf einzelne Bits über die Einheit "Eingang (E)" ist nicht zulässig.

Prozessabbild der Eingänge von Standard-Peripherie

Zu Beginn jedes OB 1-Zyklus liest die F-CPU die Eingänge aus der Standard-Peripherie und speichert die Werte in das Prozessabbild der Eingänge. Beachten Sie bei S7-400 ggf. auch die Aktualisierungszeitpunkte bei Verwendung von Teilprozessabbildern.

Auf Eingangskanäle von Standard-Peripherie kann nur lesend über die Einheiten "Eingang (E)" und "Eingangswort (EW)" zugegriffen werden.
Deshalb ist auch keine Übergabe an Durchgangs-(IN_OUT-)Parameter eines F-FB
oder F-FC zulässig.
Zusätzlich ist eine prozessspezifische Plausibilitätskontrolle erforderlich
.

Prozessabbild der Ausgänge von F-Peripherie

Im F-PB berechnet das Sicherheitsprogramm die Werte für die Ausgänge der F-Peripherie und legt sie im Prozessabbild der Ausgänge ab. Am Ende der F-Ablaufgruppe (F-CALL) schreibt die F-CPU die errechneten Ausgangswerte auf die Ausgänge der F-Peripherie. Auf Ausgangskanäle kann nur schreibend zugegriffen werden.
Deshalb ist auch keine Übergabe an Durchgangs-(IN_OUT-)Parameter eines F-FB oder F-FC zulässig.

- Kanäle vom Datentyp BOOL, z. B. digitale Kanäle

Auf Ausgangskanäle vom Datentyp BOOL kann nur bitweise schreibend über die Einheit "Ausgang (A)" zugegriffen werden. Ein Zugriff z. B. mit der Einheit "Ausgangswort" ist nicht zulässig.

- Kanäle vom Datentyp INT (WORD), z. B. analoge Kanäle

Auf Ausgangskanäle vom Datentyp INT (WORD) kann nur schreibend über die Einheit "Ausgangswort (AW)" zugegriffen werden. Ein Zugriff auf einzelne Bits über die Einheit "Ausgang (A)" ist nicht zulässig.

Prozessabbild der Ausgänge von Standard-Peripherie

Im F-PB berechnet das Sicherheitsprogramm ggf. auch Werte für die Ausgänge der Standard-Peripherie und legt sie im Prozessabbild der Ausgänge ab. Am Anfang des nächsten OB 1- Zyklus schreibt die F-CPU die errechneten Ausgangswerte auf die Ausgänge der Standard- Peripherie
Beachten Sie bei S7-400 ggf. auch die Aktualisierungszeitpunkte bei Verwendung von Teilprozessabbildern.
Auf Ausgangskanäle von Standard-Peripherie kann nur schreibend über die Einheiten "Ausgang (A)" und "Ausgangswort (AW)" zugegriffen werden. Deshalb ist auch keine Übergabe an Durchgangs-(IN_OUT-)Parameter eines F-FB oder F-FC zulässig.

Merker

Dieser Bereich dient zum Datenaustausch mit dem Standard-Anwenderprogramm.
Auf Merker kann nur über die aufgeführten Einheiten Merker(M) und Merkerwort (MW) zugegriffen werden.
Bei einem lesenden Zugriff ist zusätzlich eine prozessspezifische Plausibilitätskontrolle erforderlich.
Für einen Merker sind im Sicherheitsprogramm entweder schreibende oder lesende Zugriffe möglich.
Deshalb ist auch keine Übergabe an Durchgangs-(IN_OUT-)Parameter eines F-FB oder F-FC zulässig.
Bitte beachten Sie, dass Merker nur für die Kopplung zwischen Standard- Anwenderprogramm und Sicherheitsprogramm erlaubt sind, als Zwischenspeicher für F-Daten dürfen Merker nicht verwendet werden.

Datenbaustein

Datenbausteine speichern Informationen für das Programm. Sie können entweder so definiert sein, dass alle F-FB/F-FC/F-PB auf sie zugreifen können (F-DBs), oder sie sind einem bestimmten F-FB/F-PB zugeordnet (Instanz-DB). Die Datenbausteine müssen mit der Erstellsprache "F-DB" oder als Instanz-DB eines F-FB/F-PB angelegt werden.

Lokaldaten

Dieser Speicherbereich nimmt die temporären Daten eines (F-)Bausteins für die Dauer der Bearbeitung dieses (F-)Bausteins auf. Der Lstack stellt auch Speicher zum Übertragen von Bausteinparametern und zum Speichern von Zwischenergebnissen zur Verfügung.
Anmerkung: Das Übertragen von Bausteinparametern kann auch durch einen vollqualifizierten Zugriff ersetzt werden: *"Name Instanz-DB".Parametername*.
Auf Lokaldaten kann nur über Einheiten zugegriffen werden, die dem Datentyp in der Deklarationstabelle entsprechen. Möglich sind:
Lokaldatenbit (L), Lokaldatenwort (LW) und Lokaldatendoppelwort (LD)

Nicht zulässige Operandenbereiche

Nicht zulässig ist der Zugriff über nicht in obiger Tabelle aufgeführte Einheiten sowie der Zugriff auf nicht aufgeführte Operandenbereiche, insbesondere auf:

- Zähler (fehlersichere Zähler werden über F-Applikationsbausteine aus der F-Bibliothek *Distributed Safety* (V1) realisiert: F_CTU, F_CTD, F_CTUD)
- Zeiten (fehlersichere Zeiten werden über F-Applikationsbausteine aus der F-Bibliothek *Distributed Safety* (V1) realisiert: F_TP, F_TON, F_TOF)
- Datenbausteine des Standard-Anwenderprogramms
- Datenbausteine (F-DBs) über "OPN DI"
- Datenbausteine, die automatisch ergänzt wurden (- Ausnahme: bestimmte Daten im F-Peripherie-DB und im F-Global-DB des Sicherheitsprogramms)
- Peripheriebereich: Eingänge
- Peripheriebereich: Ausgänge

Boolesche Konstanten "0" und "1"

Wenn Sie in Ihrem Sicherheitsprogramm zur Versorgung von Parametern bei Bausteinaufrufen die booleschen Konstanten "0" und "1" benötigen, dann können Sie auf die Variablen "VKE0" und "VKE1" im F-Global-DB über einen vollqualifizierten DB-Zugriff zugreifen ("F_GLOBDB".VKE0 bzw. "F_GLOBDB".VKE1).

Unterstützte Operationen

Im Sicherheitsprogramm können Sie die in der nachfolgenden Tabelle aufgeführten Operationen verwenden:

Operation		Funktion	Beschreibung
F-FUP	**F-KOP**		
>=1	-	Bitverknüpfung	ODER-Verknüpfung
&	-	Bitverknüpfung	UND-Verknüpfung
XOR	-	Bitverknüpfung	EXKLUSIV-ODER-Verknüpfung
---|	-	Bitverknüpfung	Binären Eingang einfügen
---o|	-	Bitverknüpfung	Binären Eingang negieren
=	-	Bitverknüpfung	Zuweisung
-	---| |---	Bitverknüpfung	Schließerkontakt
-	---| / |---	Bitverknüpfung	Öffnerkontakt
-	---|NOT|---	Bitverknüpfung	Verknüpfungsergebnis invertieren
-	---( )	Bitverknüpfung	Relaisspule, Ausgang
#	---(#)---	Bitverknüpfung	Konnektor
S	---(S)	Bitverknüpfung	Ausgang setzen
R	---(R)	Bitverknüpfung	Ausgang rücksetzen
SR	SR	Bitverknüpfung	Flipflop setzen rücksetzen
RS	RS	Bitverknüpfung	Flipflop rücksetzen setzen
N	---(N)---	Bitverknüpfung	Flanke 1 -> 0 abfragen
NEG	NEG	Bitverknüpfung	Signalflanke 1 -> 0 abfragen
P	---(P)---	Bitverknüpfung	Flanke 0 -> 1 abfragen
POS	POS	Bitverknüpfung	Signalflanke 0 -> 1 abfragen
WAND_W	WAND_W	Wortverknüpfung	16 Bit UND verknüpfen
WOR_W	WOR_W	Wortverknüpfung	16 Bit ODER verknüpfen
WXOR_W	WXOR_W	Wortverknüpfung	16 Bit EXKLUSIV ODER verknüpfen
ADD_I	ADD_I	Festpunkt-Funktion	Ganze Zahlen addieren (16 Bit)
DIV_I	DIV_I	Festpunkt-Funktion	Ganze Zahlen dividieren (16 Bit)
MUL_I	MUL_I	Festpunkt-Funktion	Ganze Zahlen multiplizieren (16 Bit)
SUB_I	SUB_I	Festpunkt-Funktion	Ganze Zahlen subtrahieren (16 Bit)
CMP ? I	CMP ? I	Vergleicher	Ganze Zahlen vergleichen (16 Bit) (CMP==I, CMP<>I, CMP>I, CMP<I, CMP>=I, CMP<=I)
NEG_I	NEG_I	Umwandler	Zweier-Komplement zu Ganzzahl (16 Bit) erzeugen
OPN	---(OPN)	DB-Aufruf	Datenbaustein öffnen
MOVE	MOVE	Verschieben	Wert übertragen
CALL_FC (FC als Box aufrufen)	CALL_FC (FC als Box aufrufen)	Programmsteuerung	F-FCs unbedingt aufrufen (EN = 1, keine Verschaltung von EN!)

Operation		Funktion	Beschreibung
CALL_FB (FB als Box aufrufen)	CALL_FB (FB als Box aufrufen)	Programmsteuerung	F-FBs unbedingt aufrufen (EN = 1, keine Verschaltung von EN!)
RET	---(RET)	Programmsteuerung	Springe zurück (Baustein verlassen)
Multiinstanzen aufrufen	Multiinstanzen aufrufen	Programmsteuerung	Multiinstanzen aufrufen
JMP	---(JMP)	Sprungoperation	Springe im Baustein absolut Springe im Baustein wenn 1 (bedingt)
JMPN	---(JMPN)	Sprungoperation	Springe im Baustein wenn 0 (bedingt)
OV	OV ---| |---	Statusbit	Störungsbit Überlauf auswerten (OV-Bit im Statuswort)

Weitere Detailinformation erhalten Sie aus der Online-Hilfe.

Nicht zulässige Operationen

Nicht zulässig sind alle nicht in obiger Tabelle aufgeführten Operationen, insbesondere:

- Zähloperationen (fehlersichere Zähler werden über F-Applikationsbausteine aus der F-Bibliothek *Distributed Safety* (V1) realisiert: F_CTU, F_CTD, F_CTUD)
- Zeitoperationen (fehlersichere Zeiten werden über F-Applikationsbausteine aus der F-Bibliothek *Distributed Safety* (V1) realisiert: F_TP, F_TON, F_TOF)
- Schiebe- und Rotieroperationen (Schiebeoperationen werden über F-Applikationsbausteine aus der F-Bibliothek *Distributed Safety* (V1) realisiert: F_SHL_W, F_SHR_W)
- folgende Programmsteuerungsoperationen:

- Standard-Bausteine (FBs, FCs) aufrufen
- CALL: FC/SFC ohne Parameter aufrufen
- F-FBs, F-FCs bedingt aufrufen (Verschaltung von EN bzw. EN = 0)
- SFBs, SFCs aufrufen

Hinweis

Den Freigabeeingang EN und den Freigabeausgang ENO dürfen Sie bei der fehlersicheren Programmierung nicht verschalten, mit "0" versorgen oder auswerten!

7 Fehlerdiagnose bei Safety Integrated

7.1 Diagnose bei den F-Modulen in der ET200S

Sicherer Zustand (Sicherheitskonzept)
Grundlage des Sicherheitskonzeptes ist es, dass für alle Prozessgrößen ein sicherer Zustand existiert. Bei digitalen F-Modulen ist das z. B. der Wert .0.. Dies gilt für Geber wie für Aktoren.

Reaktionen auf Fehler und Anlauf des F-Systems
Die Sicherheitsfunktion bedingt, dass für ein fehlersicheres Modul in folgenden Fällen statt der Prozesswerte Ersatzwerte (sicherer Zustand) verwendet werden

Passivierung des fehlersicheren Moduls:

- beim Anlauf des F-Systems
- bei Fehlern in der sicherheitsgerichteten Kommunikation zwischen F-CPU und F-Modul über das Sicherheitsprotokoll gemäß PROFIsafe (Kommunikationsfehler)
- bei F-Peripherie-/Kanalfehlern (z. B. Drahtbruch, Kurzschluss, Diskrepanzfehler) Erkannte Fehler werden in den Diagnosepuffer der F-CPU eingetragen und dem Sicherheitsprogramm in der F-CPU mitgeteilt.

F-Module können Fehler nicht remanent speichern. Nach einem NETZ AUS . NETZ EIN wird im Anlauf ein weiterhin bestehender Fehler wieder erkannt. Die Fehlerspeicherung können Sie jedoch in Ihrem Sicherheitsprogramm vornehmen.

Warnung
Für Kanäle, die Sie in *STEP 7* als .deaktiviert. parametriert haben, erfolgt bei einem Kanalfehler keine Diagnosereaktion und Fehlerbehandlung; auch dann nicht, wenn ein solcher Kanal indirekt durch einen Kanalgruppenfehler betroffen ist (Parameter .Kanal aktiviert/deaktiviert.).

Ersatzwertausgabe für fehlersichere Module

Bei F-DI-Modulen werden vom F-System bei einer Passivierung statt der an den fehlersicheren Eingängen anstehenden Prozesswerte Ersatzwerte für das Sicherheitsprogramm bereitgestellt:

- Bei F-DI-Modulen ist das immer der Ersatzwert (0).

Bei F-DO-Modulen und PM-E F pm DC24V PROFIsafe werden vom F-System bei einer Passivierung statt der vom Sicherheitsprogramm bereitgestellten Ausgabewerte Ersatzwerte (0) zu den fehlersicheren Ausgängen übertragen. Die Ausgabekanäle werden in den strom- und spannungslosen Zustand gebracht. Das gilt auch beim STOP der F-CPU. Eine Parametrierung von Ersatzwerten ist nicht möglich.
Abhängig vom eingesetzten F-System und von der Art des aufgetretenen Fehlers (F-Peripherie-, Kanal- oder Kommunikationsfehler) erfolgt die Verwendung der Ersatzwerte entweder nur für den betroffenen Kanal oder für alle Kanäle des betroffenen fehlersicheren Moduls. In F-Systemen S7 Distributed Safety wird bei Kanalfehlern das gesamte F-Modul
passiviert.

Wiedereingliederung eines fehlersicheren Moduls

Die Umschaltung von Ersatzwerten auf Prozesswerte (Wiedereingliederung eines F-Moduls) erfolgt automatisch oder erst nach einer Anwenderquittierung im Sicherheitsprogramm. Bei Kanalfehlern wird ggf. das Ziehen und Stecken des F-Moduls notwendig. Nach einer Wiedereingliederung:

- werden bei einem fehlersicheren DI-Modul wieder die an den fehlersicheren Eingängen anstehenden Prozesswerte für das Sicherheitsprogramm bereitgestellt
- werden bei einem fehlersicheren DO-Modul wieder die im Sicherheitsprogramm bereitgestellten Ausgabewerte zu den fehlersicheren Ausgängen übertragen

Verhalten des F-DI-Moduls bei Kommunikationsstörung

Das F-DI-Modul verhält sich bei einer Kommunikationsstörung anders, als bei anderen Fehlern. Im Falle einer Kommunikationsstörung bleiben die aktuellen Prozesswerte an den Eingängen des F-DI-Moduls bestehen; es erfolgt keine Passivierung der Kanäle. Die aktuellen Prozesswerte werden zur F-CPU gesendet und in der F-CPU passiviert.

Diagnose von Fehlern

Über Diagnose können Sie ermitteln, ob die Signalerfassung der fehlersicheren Module fehlerfrei erfolgt. Die Diagnoseinformationen sind entweder einem Kanal oder dem gesamten F-Modul zugeordnet.

Diagnosefunktionen sind nicht sicherheitskritisch

Alle Diagnosefunktionen (Anzeigen und Meldungen) sind nicht sicherheitskritisch und somit nicht sicherheitsgerichtet realisiert, d. h., die Diagnosefunktionen werden intern nicht getestet.

Diagnosemöglichkeiten für fehlersichere Module in ET 200S

Folgende Diagnosemöglichkeiten stehen Ihnen für die fehlersicheren Module zur Verfügung:

- LED-Anzeige auf der Modul-Frontseite
- Diagnosefunktionen der F-Module (Slave- Diagnose nach PROFIBUS- Norm)

Nichtparametrierbare Diagnosefunktionen

Die fehlersicheren Elektronik- und Powermodule stellen nichtparametrierbare Diagnosefunktionen zur Verfügung. D. h., die Diagnose ist immer aktiv geschaltet und wird im Fehlerfall automatisch vom F-Modul in *STEP 7* zur Verfügung gestellt und an die F-CPU weitergeleitet.

Parametrierbare Diagnosefunktionen

Einige Diagnosefunktionen können Sie in *STEP 7* parametrieren (freischalten):

- für das F-DO-Modul und das PM-E F pm die Drahtbrucherkennung
- für das F-DI-Modul die Kurzschlussüberwachung

Warnung

Das Zu- oder Abschalten von Diagnosefunktionen muss in Abstimmung mit der Anwendung erfolgen.

Diagnose durch LED-Anzeige

Jedes fehlersichere Power- und Elektronikmodul zeigt Ihnen Fehler über seine SFLED (Sammelfehler-LED) an. Die SF-LED leuchtet, sobald eine Diagnosefunktion vom F-Modul ausgelöst wird. Sie erlischt, wenn alle Fehler behoben sind. Das Powermodul verfügt zusätzlich über eine PWR-LED, die die Lastspannungsversorgung der Potenzialgruppe anzeigt.
Das Elektronikmodul 4/8 F-DI DC24V PROFIsafe verfügt zusätzlich über zwei Fehler-LEDs (1VsF und 2VsF), die die Fehler der beiden internen Geberversorgungen anzeigen.

Slave-Diagnose

Die Slave-Diagnose verhält sich nach Norm IEC 61784-1:2002 ED1 CP 3/1. Die fehlersicheren Elektronik- und Powermodule unterstützen die Slave-Diagnose genauso wie die Standard-ET 200S-Module.
Nachfolgend finden Sie als Ergänzung die kanalbezogene Diagnose für die fehlersicheren Module.

Kanalbezogene Diagnose

Es stehen wie bei ET 200S ab Byte 35 jeweils 3 Byte für eine kanalbezogene Diagnose zur Verfügung. Pro Station sind maximal 9 kanalbezogene Diagnosemeldungen möglich.

7.2 Diagnosewerkzeuge

In diesem Kapitel finden Sie eine Zusammenstellung der Diagnosemöglichkeiten, die Sie im Fehlerfall für Ihr F-System auswerten können. Die meisten Diagnosemöglichkeiten unterscheiden sich nicht von denen in Standard- Automatisierungssystemen.

LEDs an der Hardware auswerten (F-CPU, F-Peripherie):

- BUSF-LED der F-CPU: blinkt bei einem Kommunikationsfehler am PROFIBUS DP;

leuchtet, wenn OB 85 und OB 121 programmiert sind, bei einem Programmierfehler (z. B. Instanz-DB nicht geladen)

- STP-LED der F-CPU: leuchtet, wenn F-CPU im Betriebszustand STOP ist
- Fehler- LEDs der F-Peripherie: z. B. SF-LED (Sammelfehler- LED) leuchtet, wenn ein beliebiger

Fehler in der speziellen F-Peripherie aufgetreten ist

Diagnosepuffer in *STEP 7* auswerten:

in *HW Konfig* über den Menübefehl **Zielsystem > Baugruppenzustand** die Diagnosepuffer der Baugruppen (F-CPU, F-Peripherie) auslesen

Stacks in *STEP 7* auswerten:

wenn sich die F-CPU im Betriebszustand STOP befindet, in
HW Konfig über den Menübefehl **Zielsystem > Baugruppenzustand** nacheinander auslesen:

- B-Stack: überprüfen, ob der STOP der F-CPU durch einen F-Baustein des

Sicherheitsprogramms ausgelöst wurde

- U-Stack
- L-Stack

Diagnosevariable des F-Peripherie-DB über Test- und Inbetriebsetzungsfunktionen oder im Standard- Anwenderprogramm auswerten:
im F-Peripherie-DB die Variable DIAG auswerten

Diagnoseparameter der Instanz-DBs von F-Applikationsbausteinen über Test- und Inbetriebsetzungsfunktionen oder im Standard- Anwenderprogramm auswerten:

- Für F_MUTING, F_1oo2DI, F_2H_EN, F_MUT_P, F_ESTOP1, F_FDBBACK, F_SFDOOR im zugeordneten Instanz-DB auswerten:

- Parameter DIAG

- Für F_SENDDP bzw. F_RCVDP im zugeordneten Instanz-DB auswerten:

- Parameter RETVAL14
- Parameter RETVAL15
- Parameter DIAG

- Für F_SENDS7 bzw. F_RCVS7 im zugeordneten Instanz- DB auswerten:

- Parameter STAT_RCV
- Parameter STAT_SND
- Parameter DIAG

Tipp zu RETVAL14 und 15
Die Diagnoseinformationen der Parameter RETVAL14 und RETVAL15 entsprechen denen der SFCs 14 und 15. Die Beschreibung finden Sie deshalb in der *Onlinehilfe STEP 7* zu den SFCs 14 und 15.

Tipp zu STAT_RCV und STAT_SND
Die Diagnoseinformation des Parameters STAT_RCV entspricht der Diagnoseinformation des Parameters STATUS des SFB 9/FB 9. Die Diagnoseinformation des Parameters STAT_SND entspricht der Diagnoseinformation des Parameters STATUS des SFB 8/FB 8. Die Beschreibung finden Sie deshalb in der *Onlinehilfe STEP 7* zu den SFBs 8 und 9.

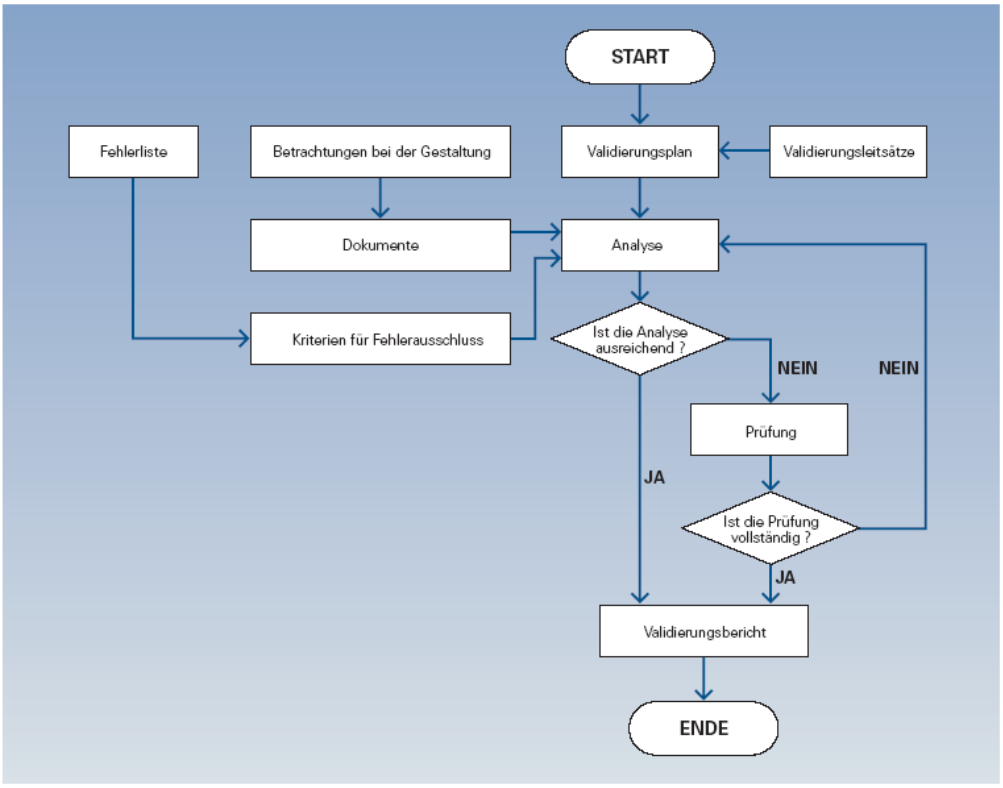
8 Überprüfung der Wirksamkeit und Erstellen eines Sicherheitsprotokolls

8.1 Gesetzliche Vorgaben zur Wirksamkeitsüberprüfung / Validierung

In dem Normentwurf prEN954-2 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“ wird der Themenkomplex „Validierung“ behandelt. Validierung bedeutet eine bewertende Überprüfung der angestrebten Sicherheitsfunktionalität. Die Norm entspricht dem Status einer B1-Sicherheitsgruppennorm (allgemeine Sicherheitsaspekte). Zweck der Validierung ist, die Festlegungen und das Niveau der
Konformität der sicherheitsbezogenen Teile der Steuerung innerhalb der Gesamtfestlegung für Sicherheitsanforderungen an der Maschine zu bestätigen. Die Validierung muss aufzeigen, dass jedes sicherheitsbezogene Teil die Anforderung von EN 954- 1 erfüllt. Dabei sind die folgenden Aspekte beschrieben:

- Validierung durch Analyse
- Validierung durch Prüfen
- Fehlerlisten
- Validierung der Sicherheitsfunktionen
- Validierung der Kategorien
- Validierung der Umgebungsanforderungen
- Validierung der Instandhaltungsanforderungen

Das folgende Bild gibt einen Überblick über das Validierungsverfahren gemäß EN 954-2.



Übersicht über den Validierungsprozess (aus prEN 954-2)

Der Validierungsplan muss die Anforderungen für die Durchführung des Validierungsverfahrens für die festgelegten Sicherheitsfunktionen und ihrer Kategorien identifizieren und beschreiben. Wo angemessen, muss er sie auch dokumentieren.
Die Anforderungen an die Dokumentation entsprechend den Kategorien sieht wie folgt aus.

Anforderungen an die Dokumentation	Kategorie, für die eine Dokumentation erfordlich ist				
	B	1	2	3	4
Grundlegende Sicherheitsprinzipien	X	X	X	X	X
Zu erwartende Betriebsbeanspruchungen	X	X	X	X	X
Einfluss des zu verarbeitenden Materials	X	X	X	X	X
Leistungsfähigkeit während anderer relevanter externer Einflüsse	X	X	X	X	X
Bewährte Bauteile	–	X	–	–	–
Bewährte Sicherheitsprinzipien	–	X	X	X	X
Das Prüfverfahren für die Sicherheitsfunktion(en)	–	–	X	–	–
Festgelegte Prüfintervalle	–	–	X	–	–
Bei der Gestaltung berücksichtigte, vorhersehbare Einzelfehler und das angewendete Erkennungsverfahren	–	–	X	X	X
Alle identifizierte Fehler gemeinsamer Ursache und wie sie verhindert werden	–	–	–	X	X
Wie die Sicherheitsfunktion bei jedem Fehler aufrechterhalten bleibt	–	–	–	X	X
Fehler, die zu erkennen sind	–	–	X	X	X
Verschiedene Fehleranhäufungen, die bei der Gestaltung zu berücksichtigen sind	–	–	–	X	X
Wie die Sicherheitsfunktion bei allen Fehlerkombinationen aufrechterhalten bleibt	–	–	–	–	X

Anforderungen an die Dokumentation (aus prEN 954-2)

Die in EN 954-1 beschriebenen Anforderungen sind für Systeme mit programmierbarer Elektronik nicht ausreichend. Deshalb verlangt EN 954-2 für deren Validierung die Anwendung weiterer Normen, z.B.die IEC 61508 oder, bei berührungslos wirkenden Schutzeinrichtungen, IEC 61496 anzuwenden.

Diese umfangreichen Anforderungen beziehen sich auf die Entwicklung und Implementierung von Steuerungen, nicht auf die Anwendung und Parametrierung zertifizierter Systeme wie z.B. Simatic S7-300F, Sinumerik Safety Integrated, Siguard Laser Scanner und Lichtvorhänge, PROFIsafe oder AS-i *Safety at Work*.

8.2 Abnahme einer Anlage

Bei der Abnahme der Anlage müssen alle relevanten anwendungsspezifischen Normen und das nachfolgende Verfahren eingehalten werden. Dies gilt auch für nicht "abnahmepflichtige" Anlagen.

8.2.1 Abnahme der Projektierung der F-Peripherie

Nach Abschluss der Hardware-Konfigurierung und Parametrierung der F-Peripherie können Sie eine erste Abnahme der Projektierung der F-Peripherie durchführen.

Die Hardware-Konfigurationsdaten müssen dazu ausgedruckt, überprüft und zusammen mit dem gesamten *STEP 7*-Projekt gesichert werden.

Hardware-Konfigurationsdaten drucken

1. Wählen Sie die richtige F-CPU bzw. das ihr zugeordnete S7-Programm.

2. Wählen Sie im *SIMATIC Manager* den Menübefehl **Extras >Sicherheitsprogramm bearbeiten**. Der Dialog "Sicherheitsprogramm" erscheint.

3. Aktivieren Sie die Schaltfläche "Drucken" und wählen Sie im Folgedialog "Sicherheitsprogramm drucken" die Option "Hardware-Konfiguration".

4. Wählen Sie als Druckbereich "Alles". Damit werden die "Baugruppenbeschreibung" und die "Adressliste" mit ausgedruckt. Markieren Sie die Option "Mit Parameterbeschreibung", damit auch Ihre
Parameterbeschreibungen ausgedruckt werden.

Hardware-Konfigurationsdaten überprüfen

1. Überprüfen Sie die sicherheitsrelevanten Parameter der F-Peripherie im Ausdruck.
Diese sicherheitsrelevanten Parameter sind im Ausdruck der jeweiligen F-Peripherie zu finden. Der Aufbau der Daten unterscheidet sich je nach F-Peripherie:

SM 326; DI 24 DC 24 V (Best.-Nr. 6ES7326-1BK00-0AB0), SM 326; DI 8 Namur, SM 326 DO 10 DC 24V/2A und SM 336; AI 6 13 Bit

- Die PROFIsafe- Quelladresse ist immer "1" und erscheint nicht im Ausdruck.
- Die PROFIsafe- Zieladresse ermitteln Sie aus dem Adresswert unter "Adressen – Eingänge – Anfang". Teilen Sie diesen Adresswert durch "8".
- Die sicherheitsrelevanten Parameter finden Sie unter "Parameter – Grundeinstellungen" bzw. unter "Parameter – Ein-/Ausgang x".

Fehlersichere Module ET200S, ET 200eco, SM 326; DI 24 DC 24 V (ab Best.-Nr. 6ES7326-1BK01-0AB0) und SM 326; DO 8 DC 24V/2A PM

- Die PROFIsafe-Quelladresse finden Sie unter "Parameter – F-Parameter – F_Quell_Adresse.
- Die PROFIsafe-Zieladresse finden Sie unter "Parameter – F-Parameter – F_Ziel_Adresse".
- Die sicherheitsrelevanten Parameter finden Sie unter "Parameter – F-Parameter" und unter "Parameter – Baugruppenparameter".

Fehlersichere DP-Normslaves

- Die PROFIsafe-Quelladresse finden Sie unter "PROFIsafe – F_Source_Add".
- Die PROFIsafe-Zieladresse finden Sie unter "PROFIsafe – F_Dest_Add".
- Die sicherheitsrelevanten Parameter finden Sie unter "PROFIsafe".

Die Handhabung eventueller technologischer sicherheitsrelevanter Parameter ist in der Dokumentation des jeweiligen DP-Normslave nachzulesen.

Parameter der F-CPU

Für den Sicherheitsbetrieb muss Schutzstufe "1" und "Durch Passwort aufhebbar" eingestellt sein. Des Weiteren muss die Option "CPU enthält Sicherheitsprogramm" aktiviert sein. Im Ausdruck wird ausgegeben: "Schutzstufe: Kein Schutz CPU enthält Sicherheitsprogramm"

2. Nach der Überprüfung der sicherheitsrelevanten Parameter einer F-Peripherie genügen für die weitere Abnahme als Referenz die Parameter-CRCs im Ausdruck. Diese sehen folgendermaßen aus (Adresse/F-Adresse = PROFIsafe- Adresse):

Fehlersichere Signalbaugruppen S7-300 (SM 326; DI 24 DC 24 V, mit Bestell-Nr. 6ES7326-1BK00-0AB0; SM 326; DI 8 NAMUR; SM 326; DO 10 DC 24V/2A; SM 336; AI 6 13Bit)

- Parameter-CRC (inkl. Adresse): 12345
- Parameter-CRC (ohne Adresse): 54321

Fehlersichere Module ET200S, ET 200eco und Fehlersichere Signalbaugruppen S7-300 (SM 326; DI 24 DC 24 V, ab Bestell-Nr. 6ES7326-1BK01-0AB0; SM 326; DO 8 DC 24V/2A PM)

- Parameter-CRC: 12345
- Parameter- CRC (ohne F-Adressen): 54321

Fehlersichere DP-Normslaves

- F_Par_CRC: 12345
- F_Par_CRC (ohne F-Adressen): 54321

F-Peripherien, die dieselben sicherheitsrelevanten Parameter erhalten sollen, können bei der Projektierung kopiert werden. Bei ihnen müssen nicht mehr alle sicherheitsrelevanten Parameter einzeln überprüft werden: Es genügt ein Vergleich der jeweiligen zweiten CRC (z. B. "Parameter-CRC (ohne Adresse)") der kopierten F-Peripherie mit der entsprechenden CRC der bereits überprüften
F-Peripherie und eine Überprüfung der PROFIsafe- Quell- und Zieladressen.

3. Überprüfen Sie die Eindeutigkeit der PROFIsafe- Adressen.

Warnung
Die Schalterstellung am Adressschalter der F-Peripherie, d. h. deren PROFIsafe- Zieladresse muss netz*- und stationsweit** (systemweit) eindeutig sein. In einem System dürfen Sie maximal 1022 PROFIsafe- Zieladressen vergeben, d. h. es sind maximal 1022 F-Peripherien über PROFIsafe ansprechbar.

Ausnahme: In verschiedenen I-Slaves dürfen F-Peripherien die gleiche PROFIsafe- Zieladresse haben, da sie nur stationsweit, d. h. von der F-CPU im I-Slave angesprochen werden.
Die folgende Einschränkung gilt nur für F-Module ET 200S oder fehlersichere DP- Normslaves, deren voreingestellte PROFIsafe- Adressen in *HW Konfig* **nicht änderbar** sind:
Wenn Sie F-Module ET 200S oder fehlersichere DP- Normslaves an einem PROFIBUS- Netz einsetzen, deren PROFIsafe- Adressen nicht in *HW Konfig* änderbar sind, dürfen Sie nur **einen DP-Master mit F-CPU** an diesem Netz betreiben, sonst ist die systemweite Eindeutigkeit der PROFIsafe-Adressen nicht gewährleistet.

* Ein Netz besteht aus einem oder mehreren Subnetzen. "Netzweit" bedeutet, über
PROFIBUS- Subnetz- Grenzen hinweg.
** "Stationsweit" bedeutet, für eine Station in *HW Konfig* (z. B. eine S7-300-Station oder auch einen I-Slave)

Zur Ermittlung der PROFIsafe-Adressen der einzelnen F-Peripherien siehe Schritt 1.

8.2.2 Abnahme eines Sicherheitsprogramms

Prinzipielle Vorgehensweise bei der Abnahme eines Sicherheitsprogramms

1. Erstellen Sie die HW-Konfiguration und das Sicherheitsprogramm. Generieren Sie das Sicherheitsprogramm und sichern Sie das gesamte *STEP 7*-Projekt.

2. Drucken Sie das Sicherheitsprogramm:

- Wählen Sie die richtige F-CPU bzw. das ihr zugeordnete S7-Programm.
- Wählen Sie im *SIMATIC Manager* den **Menübefehl Extras > Sicherheitsprogramm bearbeiten**. Der Dialog "Sicherheitsprogramm" erscheint.
- Aktivieren Sie die Schaltfläche "Offline", da die Signatur der Symbole nur bei Ausdruck des Offline- Sicherheitsprogramms in der Fußzeile mitgedruckt wird.
- Aktivieren Sie die Schaltfläche "Drucken" und wählen Sie im Folgedialog "Sicherheitsprogramm drucken" die Optionen

- "Hardware-Konfiguration"
- "Funktionsplan/Kontaktplan"
- "Sicherheitsprogramm"
- "Symboltabelle"

- Wählen Sie bei der "Hardware-Konfiguration" den Druckbereich "Alles". Damit werden die "Baugruppenbeschreibung" und die "Adressliste" mit ausgedruckt. Markieren Sie die Option "Mit Parameterbeschreibung", damit auch Ihre Parameterbeschreibungen ausgedruckt werden.

3. Überprüfen Sie die Ausdrucke. Überprüfen Sie insbesondere auch Folgendes:
Die beiden Gesamtsignaturen in der Fußzeile des Ausdrucks (Gesamtsignatur aller F-Bausteine mit F-Attribut des Bausteincontainers und Signatur der Symbole) müssen in allen 4 Ausdrucken übereinstimmen. Überprüfen Sie in der Fußzeile des Ausdrucks die Angabe für die Symbolik.

Hinweis
Wenn "Symbolik nicht aktuell" ausgegeben wird, wurden Zuordnungen für globale oder lokale Symbole geändert (z. B. Änderungen in der Symboltabelle oder von Parameternamen von F-DBs oder F-FBs), ohne dass die Änderungen in allen betroffenen F-FBs/F-FCs nachgezogen wurden.
Um dies zu beheben, verwenden Sie die Funktion "Bausteinkonsistenz prüfen" (siehe Onlinehilfe *STEP 7*). Ggf. müssen Sie das Sicherheitsprogramm neu generieren. Im Ausdruck des Sicherheitsprogramm müssen die Gesamtsignatur aller F-Bausteine mit F-Attribut des Bausteincontainers und die Gesamtsignatur des Sicherheitsprogramms übereinstimmen.

Die Signaturen und Anfangswertsignaturen aller F-Applikationsbausteine und F-Systembausteine sowie die Version von *S7 Distributed Safety* müssen denen im Annex 1 zum Bericht zum Zertifikat entsprechen.

Überprüfen Sie, ob Sie bei der sicherheitsgerichteten Master-Master-, Master- I-Slave- und I-Slave-I-Slave- Kommunikation den Parameter DP_DP_ID netzweit für alle sicherheitsgerichteten Kommunikationsverbindungen eindeutig vergeben haben.
Überprüfen Sie, ob Sie bei der sicherheitsgerichteten Kommunikation über S7-Verbindungen den Parameter R_ID netzweit für alle sicherheitsgerichteten Kommunikationsverbindungen eindeutig vergeben haben.
Überprüfen Sie, ob Sie bei allen Daten aus dem Standard- Anwenderprogramm im Sicherheitsprogramm eine Plausibilitätskontrolle programmiert haben. Überprüfen Sie die Anzahl der F-Ablaufgruppen im Sicherheitsprogramm (max. 2) und den Aufbau der F-Ablaufgruppen (ob alle notwendigen Bausteine in der F-Ablaufgruppe vorhanden sind).
Sie müssen im Ausdruck "Sicherheitsprogramm" bei einigen Werten überprüfen, ob sie den von Ihnen projektierten oder programmierten Werten entsprechen:

- Ablaufgruppeninformation für jede F-Ablaufgruppe:

- Nummer des F-CALL;
- Nummer des aufgerufenen F-Programmbausteins
- ggf. Nummer des zugehörigen Instanz- DB
- maximale Zykluszeit der F-Ablaufgruppe
- ggf. Nummer des DB für F-Ablaufgruppenkommunikation

- Für jede in der F-Ablaufgruppe angesprochene F-Peripherie:

- Der im Sicherheitsprogramm verwendete symbolische Name und die verwendete Nummer des F-Peripherie- DB müssen zur Anfangsadresse der richtigen Baugruppe gehören.
- Der Wert der F_Überwachungszeit muss mit dem entsprechenden Wert der F-Peripherie mit derselben Anfangsadresse im Ausdruck "Hardware- Konfiguration" übereinstimmen. Dort heißt der entsprechende Parameter bei fehlersicheren Signalbaugruppen S7-300 "Überwachungszeit" und bei fehlersicheren DP- Normslaves "F_WD_Time". Sollten bei diesen Überprüfungen Abweichungen bzw. Fehler auftreten, so generieren Sie das Sicherheitsprogramm neu und beginnen Sie wieder bei Schritt 1 der Abnahme.

4. Laden Sie das Sicherheitsprogramm in die F-CPU (falls noch nicht geschehen). Das letzte Laden von F-Bausteinen vor der Abnahme muss mit dem Dialog "Sicherheitsprogramm" erfolgen. Überpüfen Sie nach dem Laden des Sicherheitsprogramms in die F-CPU Folgendes:
Die Online-Gesamtsignatur aller F-Bausteine mit F-Attribut des Bausteincontainers muss mit derjenigen im abgenommenen Offline- Ausdruck übereinstimmen und im Online-Sicherheitsprogramm darf kein unbenutzter F-CALL vorhanden sein. Es dürfen maximal 2 F-CALL-Bausteine in der F-CPU
vorhanden sein. Ist dies nicht der Fall, so überprüfen Sie, ob Sie das Sicherheitsprogramm in die richtige F-CPU geladen haben und ggf. wiederholen Sie diesen Schritt. Besteht
das Problem weiterhin, so generieren Sie das Sicherheitsprogramm neu und
beginnen Sie wieder bei Schritt 1 der Abnahme.

5. Führen Sie einen vollständigen Funktionstest des Sicherheitsprogramms durch

6. Um bei wiederkehrenden Prüfungen festzustellen, ob sich das richtige Sicherheitsprogramm in der F-CPU befindet, vergleichen Sie die Online- Gesamtsignatur aller F-Bausteine mit F-Attribut des Bausteincontainers mit derjenigen im abgenommenen Offline- Ausdruck.
Sollte für wiederkehrende Prüfungen kein PG/PC mit *S7 Distributed Safety* V5.3 zur Verfügung stehen, können Sie die Gesamtsignatur des Sicherheitsprogramms aus dem F-Global-DB über ein Bedien- und Beobachtungssystem auslesen. Die Adresse, unter der im F-Global-DB die Gesamtsignatur des Sicherheitsprogramms steht (Variable "F_PROG_SIG"), können Sie dem Ausdruck des Sicherheitsprogramms entnehmen. Diese Variante sollten Sie nur verwenden, wenn Sie nicht mit einer Manipulation rechnen müssen.

Abnahme von Änderungen des Sicherheitsprogramms
Bei der Abnahme von Änderungen des Sicherheitsprogramms müssen Sie wie bei der Abnahme des Sicherheitsprogramms verfahren, mit dem Unterschied, dass nur ein Funktionstest der Änderungen erforderlich ist.

Vorgehensweise zur Feststellung der Änderungen im Sicherheitsprogramm
1. Durch einen Vergleich der beiden Gesamtsignaturen im Ausdruck des zu überprüfenden Sicherheitsprogramms mit denen im Ausdruck des abgenommenen Sicherheitsprogramms erkennen Sie, ob eine sicherheitsrelevante Änderung vorliegt.
2. Falls eine sicherheitsrelevante Änderung vorliegt, vergleichen Sie das geänderte Sicherheitsprogramm offline mit dem gesicherten abgenommenen Sicherheitsprogramm über die Schaltfläche "Vergleichen..." im Dialog "Sicherheitsprogramm".
Dadurch können Sie erkennen, welche F-Bausteine geändert wurden. Detaillierte Angaben zu den Änderungen im F-Baustein erhalten Sie durch einen Vergleich der Ausdrucke. Änderungen in der Parametrierung der F-Peripherie können Sie indirekt im Ausdruck des Sicherheitsprogramms an der Angabe "Parameter-CRC" des zugehörigen F-Peripherie-DB erkennen. Änderungen der Anfangsadresse können Sie indirekt im Ausdruck an der Angabe "Anfangsadresse" des zugehörigen F-Peripherie-DB erkennen.

Einsatz von Software-Paketen mit Standard-Anwenderprogramm
Bei Software-Paketen, die für den Standard und parallel zum Sicherheitsprogramm eingesetzt werden können (z.B. SW-Redundancy), können sich Randbedingungen ergeben, die Sie beachten müssen:

Hinweis
Belegt das Sicherheitsprogramm Bausteinnummern (für FBs, DBs und FCs), die das Softwarepaket zwingend benötigt, kann beim nachträglichen Einsatz des Softwarepaketes eine Änderung des Sicherheitsprogramms zur Freigabe der Bausteinnummern erforderlich sein. Damit müssen Sie die Änderungen des Sicherheitsprogramms erneut abnehmen.