

Industrielle Schalttechnik

SIRIUS Safety Integrated Application Manual

Applikationshandbuch

Einleitung

1

Sicherheitstechnik
Allgemein

2

Applikationsbeispiele

3

Vorschriften und Normen

4

Spezifikation und Design
sicherheitsrelevanter
Steuerungen für Maschinen

5

Service & Support

6

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

 GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten wird , wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

 WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten kann , wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

 VORSICHT
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

 WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Inhaltsverzeichnis

1	Einleitung	7
1.1	Siemens Industry Online Support	10
1.2	Siemens Industry Online Support App	12
2	Sicherheitstechnik Allgemein	13
2.1	Grundbegriffe	13
2.2	Allgemeines	16
2.2.1	Zielsetzung der Sicherheitstechnik	16
2.2.2	Lokale Gesetze	16
2.2.3	Funktionale Sicherheit	16
2.2.4	Zielsetzung der Normen	17
2.2.5	Sicherheitsbezogene Funktionen	17
2.2.6	Stillsetzen	18
2.2.7	Handlung im Notfall	18
2.2.8	Not-Aus	19
2.2.9	Not-Halt	19
2.2.10	Sicherheitsfunktion	20
2.2.11	Rückstell- und Starteinrichtungen	20
2.2.12	Betriebsartenwahlschalter	22
2.2.13	Anschluss von Aktoren	22
2.2.14	Leistungsschutz als Aktor	25
2.2.15	Reihenschaltung von Sensoren	26
3	Applikationsbeispiele	27
3.1	Einführung	27
3.2	Stillsetzen im Notfall	34
3.2.1	Einleitung	34
3.2.2	Not-Halt-Abschaltung bis SIL 1 bzw. PL c mit einem Sicherheitsschaltgerät 3SK1	35
3.2.3	Not-Halt-Abschaltung bis SIL 1 bzw. PL c mit dem Sicherheitsschaltgerät 3SK2	37
3.2.4	Not-Halt-Abschaltung bis SIL 1 bzw. PL c mit einem Sanftstarter 3RW55 Failsafe	38
3.2.5	Not-Halt-Abschaltung bis SIL 2 bzw. PL c mit einem Schütz mit F-PLC-IN und Sicherheitsschaltgerät 3SK2	40
3.2.6	Not-Halt-Abschaltung bis SIL 2 bzw. PL c mit einem Schütz mit F-PLC-IN und fehlersicherer Steuerung	42
3.2.7	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1	44
3.2.8	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2	46
3.2.9	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicheren Motorstartern und einem Sicherheitsschaltgerät 3SK1	47
3.2.10	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicheren Motorstartern und einem Sicherheitsschaltgerät 3SK2	49
3.2.11	Not-Halt-Abschaltung über AS-i bis SIL 3 bzw. PL e mit einem Modularen Sicherheitssystem	51
3.2.12	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit Schützen mit F-PLC-IN und Sicherheitsschaltgerät 3SK2	53

3.2.13	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit Schützen mit F-PLC-IN und fehlersicherer Steuerung.....	55
3.2.14	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem fehlersicheren Motorstarter im ET 200SP System und Sicherheitsschaltgerät 3SK1	57
3.2.15	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem fehlersicheren Motorstarter im ET 200SP System und Sicherheitsschaltgerät 3SK2	58
3.2.16	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicherem Digitalausgangsmodul und fehlersicheren Motorstartern im ET 200SP System	60
3.2.17	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicherem Powermodul und fehlersicheren Motorstartern im ET 200SP System	62
3.2.18	Not-Halt-Abschaltung bis SIL 3 bzw. PL e über Sicherheitsschaltgerät 3SK2 mit PROFINET-Anbindung und fehlersicheren Motorstartern	64
3.2.19	Not-Halt-Gruppenabschaltung bis SIL 3 bzw. PL e über Sicherheitsschaltgerät 3SK2 mit PROFINET-Anbindung und fehlersicheren Motorstartern	67
3.2.20	Not-Halt-Abschaltung bis SIL3 bzw. PL e mit einem Sanfstarter 3RW55 Failsafe und Sicherheitsschaltgerät 3SK1	71
3.2.21	Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit Koppelrelais 3RQ1 und fehlersicherer Steuerung.....	73
3.3	Schutztürüberwachung.....	76
3.3.1	Einleitung	76
3.3.2	Begriffe aus der Norm	76
3.3.3	Schutztürüberwachung bis SIL 1 bzw. PL c mit einem Sicherheitsschaltgerät 3SK1	84
3.3.4	Schutztürüberwachung bis SIL 1 bzw. PL c mit einem Sicherheitsschaltgerät 3SK2	85
3.3.5	Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1	87
3.3.6	Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2	89
3.3.7	Schutztürüberwachung bis SIL 3 bzw. PL e mit einem fehlersicheren Motorstarter und einem Sicherheitsschaltgerät 3SK1	91
3.3.8	Schutztürüberwachung bis SIL 3 bzw. PL e mit fehlersicheren Motorstarter und einem Sicherheitsschaltgerät 3SK2	93
3.3.9	Schutztürüberwachung über AS-i bis SIL 3 bzw. PL e mit einem Modularen Sicherheitssystem	95
3.3.10	Schutztürüberwachung mittels RFID-Schalter bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1	98
3.3.11	Schutztürüberwachung mittels RFID-Schalter bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2	100
3.3.12	Schutztürüberwachung mit Zuhaltung bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät 3SK2	102
3.3.13	Schutztürüberwachung mit Zuhaltung bis SIL 2 bzw. PL d über ET 200eco PN und F-CPU... ..	104
3.3.14	Schutztürüberwachung mit Zuhaltung mittels RFID-Sicherheitsschalter 3SE64 bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2	106
3.3.15	Schutztürüberwachung mit Zuhaltung mittels RFID-Sicherheitsschalter 3SE64 bis SIL 3 bzw. PL e mit einer fehlersicheren Steuerung.....	109
3.4	Überwachung offener Gefahrenbereiche	112
3.4.1	Einleitung	112
3.4.2	Zugangsüberwachung durch einen Lichtvorhang bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1	112
3.4.3	Zugangsüberwachung durch einen Lichtvorhang bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2	114
3.4.4	Zugangsüberwachung durch eine Schaltmatte bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1	116

3.4.5	Zugangsüberwachung durch eine Schaltmatte bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2	118
3.4.6	Bereichsüberwachung durch einen Laserscanner bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät 3SK1	120
3.4.7	Bereichsüberwachung durch einen Laserscanner bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät 3SK2	122
3.5	Sichere Drehzahl- und Stillstandsüberwachung.....	125
3.5.1	Einleitung	125
3.5.2	Sichere Drehzahlüberwachung bis SIL 3 bzw. PL e mit einem Drehzahlwächter.....	125
3.5.3	Sichere Stillstandsüberwachung inkl. Schutztürzuhaltung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2	128
3.5.4	Sichere Drehzahl-, Schutztür- und Zuhaltungsüberwachung bis SIL 3 bzw. PL e mit einem Drehzahlwächter.....	130
3.6	Sicheres Bedienen.....	132
3.6.1	Einleitung	132
3.6.2	Zweihandbedienung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1	132
3.6.3	Zweihandbedienung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2	134
3.7	Typische Kombinationen mehrerer Sicherheitsfunktionen	137
3.7.1	Einleitung	137
3.7.2	Sichere Temperaturüberwachung bis SIL 1 bzw. PL c mit einem Temperaturüberwachungsrelais 3RS2.....	138
3.7.3	Sichere Temperaturüberwachung und Schutztürüberwachung mit Zuhaltung bis SIL 1 bzw. PL c mit einem Temperaturüberwachungsrelais 3RS2 und Sicherheitsschaltgerät 3SK2.....	140
3.7.4	Sichere Stromüberwachung inkl. Not-Halt-Abschaltung bis PL d mit einem Sicherheitsschaltgerät 3SK2 und zwei Stromüberwachungsrelais	142
3.7.5	Not-Halt- und Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1.....	145
3.7.6	Not-Halt- und Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2.....	147
3.7.7	Zugangsüberwachung durch einen Lichtvorhang mit Zweihandbedienung und Not-Halt bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2.....	149
3.7.8	Kaskadierung von Sicherheitsschaltgeräten 3SK1 bis SIL 3 bzw. PL e	152
3.7.9	Sicherer Querverkehr zwischen mehreren Anlagenteilen bis SIL 3 bzw. PL e über AS-i.....	154
3.7.10	Schutztürüberwachung mittels Magnetschalter und Not-Halt-Abschaltung mittels Seilzugschalter bis SIL3 bzw. PL e über AS-i ET 200SP Master und AS-i SlimLine Compact Module.....	156
3.7.11	Not-Halt-Abschaltung bis SIL 3 bzw. PL e und Schutztürüberwachung bis SIL 2 bzw. PL d mit Zuhaltung über AS-i ET 200SP Master.....	158
3.7.12	Not-Halt-Abschaltung und Schutztürüberwachung bis SIL 3 bzw. PL e über ET 200ecoPN und F-CPU	161
3.7.13	Not-Halt-Abschaltung mehrerer Motoren bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1, Ausgangserweiterung und Koppelrelais 3RQ1.....	163
3.7.14	Schutztürüberwachung mit Zuhaltung mittels RFID-Sicherheitsschalter 3SE64 inklusive Not-Halt-Abschaltung bis SIL 3 bzw. PL e über ET 200AL und F-CPU.....	166
3.7.15	Kaskadierung von Sicherheitsschaltgeräten 3SK2 bis SIL3 bzw. PL e	169
3.8	Weitere Applikationsbeispiele und FAQs	172
3.8.1	Übergreifend	172
3.8.2	Teilsystem Erfassen	172
3.8.3	Teilsystem Auswerten	172

3.8.4	Teilsystem Reagieren.....	173
4	Vorschriften und Normen	175
4.1	Vorschriften und Normen in der Europäischen Union (EU)	175
4.1.1	Maschinensicherheit in Europa.....	175
4.1.1.1	Rechtliche Grundlagen	175
4.1.1.2	CE-Konformitätsprozess	177
4.2	Vorschriften und Normen außerhalb der Europäischen Union (EU).....	183
4.2.1	Vorschriften und Normen außerhalb der Europäischen Union - Übersicht	183
4.2.2	Gesetzliche Anforderungen in den USA	183
4.2.3	Gesetzliche Anforderungen in Brasilien.....	183
4.2.4	Gesetzliche Anforderungen in Australien	185
5	Spezifikation und Design sicherheitsrelevanter Steuerungen für Maschinen	187
5.1	Sicherheitsbezogene Teile für die Maschinensteuerung	187
5.1.1	Vier Risikoelemente	187
5.2	Spezifikation der Sicherheitsanforderungen	191
5.3	Entwurf und Realisierung der (sicherheitsrelevanten) Steuerung nach IEC 62061	192
5.3.1	Philosophie / Theorie.....	192
5.3.2	Entwurfsprozess eines sicherheitsrelevanten Steuerungssystems SRECS.....	194
5.3.3	Systemdesign für eine Sicherheitsfunktion	197
5.3.4	Realisierung des sicherheitsrelevanten Steuerungssystems	198
5.3.4.1	Erreichte Safety Performance	199
5.3.5	Systemintegration für alle Sicherheitsfunktionen.....	200
5.3.6	Entwurf und Realisierung von Subsystemen	201
5.4	Entwurf und Realisierung der sicherheitsbezogenen Teile einer Steuerung nach ISO 13849-1	206
5.4.1	Entwurf und Realisierung von Kategorien	209
6	Service & Support	217
6.1	Service und Support.....	217
	Index	219

Einleitung

Zweck der Dokumentation

Diese Dokumentation gibt Ihnen einen Einblick in die grundlegenden Sicherheitsanforderungen in der Fertigungsindustrie. Die Dokumentation zeigt Ihnen an Hand der SIRIUS Safety Integrated Produkte einfache Schaltungsbeispiele zu Sicherheitsfunktionen aus den Applikationsbereichen:

- Stillsetzen im Notfall
- Schutztürüberwachung
- Drehzahl-/Stillstandsüberwachung
- Überwachung offener Gefahrenbereiche
- Sicheres Bedienen
- Typische Kombinationen von Sicherheitsfunktionen

Im Anschluss an die einfachen Schaltungsbeispiele finden Sie detaillierte Hintergrundinformationen zu Vorschriften und Normen sowie die Spezifikation und das Design von sicherheitsrelevanten Teilen von Steuerungen.

Zielgruppe

Diese Dokumentation enthält Information für folgende Zielgruppen:

- Entscheider
- Technologen
- Projektueure

Erforderliche Kenntnisse

Zum Verständnis dieser Dokumentation sind allgemeine Grundkenntnisse auf folgenden Gebieten erforderlich:

- Niederspannungs-Schalttechnik
- Digitale Schaltungstechnik
- Automatisierungstechnik

Gewährleistung und Haftung

Hinweis

Die Applikationsbeispiele sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit hinsichtlich Konfiguration und Ausstattung sowie jeglicher Eventualitäten. Die Applikationsbeispiele stellen keine kundenspezifischen Lösungen dar, sondern sollen lediglich Hilfestellung bieten bei typischen Aufgabenstellungen. Sie sind für den sachgemäßen Betrieb der beschriebenen Produkte selbst verantwortlich. Diese Applikationsbeispiele entheben Sie nicht der Verpflichtung zu sicherem Umgang bei Anwendung, Installation, Betrieb und Wartung. Wir behalten uns das Recht vor, Änderungen an diesen Applikationsbeispielen jederzeit ohne Ankündigung durchzuführen. Bei Abweichungen zwischen den Vorschlägen in diesem Applikationsbeispiel und anderen Siemens Publikationen, wie z. B. Katalogen, hat der Inhalt der anderen Dokumentation Vorrang.

Für die in diesem Dokument enthaltenen Informationen übernehmen wir keine Gewähr.

Unsere Haftung, gleich aus welchem Rechtsgrund, für durch die Verwendung der in diesem Applikationsbeispiel beschriebenen Beispiele, Hinweise, Programme, Projektierungs- und Leistungsdaten usw. verursachte Schäden ist ausgeschlossen.

Der Ausschluss gilt nicht im Falle einer vorsätzlichen oder fahrlässigen Verletzung von Leben, Körper oder Gesundheit oder bei sonstigen Schäden, sofern sie auf vorsätzlichem oder grob fahrlässigem Fehlverhalten beruhen.

Weitergabe oder Vervielfältigung dieser Applikationsbeispiele oder Auszüge daraus sind nicht gestattet, soweit nicht ausdrücklich von Siemens Industry Sector zugestanden.

Historie

Folgende Ausgaben dieser Dokumentation wurden bisher veröffentlicht. Die Änderungen gelten gegenüber dem vorherigen Ausgabestand:

Ausgabe	Bemerkung/Änderung
09/2013	Erstausgabe
10/2013	Kleine redaktionelle Verbesserungen, defekte Weblinks repariert
03/2014	Einbindung zusätzlicher Applikationsbeispiele, inhaltliche Erweiterungen und Korrekturen
09/2014	Inhaltliche Ergänzungen und Korrekturen
10/2015	Einbindung zusätzlicher Applikationsbeispiele, inhaltliche Erweiterungen und Korrekturen
09/2016	Einbindung zusätzlicher Applikationsbeispiele, inhaltliche Erweiterungen und Korrekturen
08/2017	Einbindung zusätzlicher Applikationsbeispiele, inhaltliche Erweiterungen und Korrekturen
09/2019	Einbindung zusätzlicher Applikationsbeispiele, inhaltliche Erweiterungen und Korrekturen
09/2020	Einbindung zusätzlicher Applikationsbeispiele, inhaltliche Erweiterungen und Korrekturen

Ausgabe	Bemerkung/Änderung
07/2021	Einbindung zusätzlicher Applikationsbeispiele, inhaltliche Erweiterungen und Korrekturen
09/2022	Einbindung zusätzlicher Applikationsbeispiele, inhaltliche Erweiterungen und Korrekturen

1.1 Siemens Industry Online Support

Informationen und Service

Im Siemens Industry Online Support erhalten Sie aktuelle Informationen aus der globalen Support-Datenbank:

- Produkt-Support
- Anwendungsbeispiele
- Forum
- mySupport

Link: Siemens Industry Online Support (<https://support.industry.siemens.com/cs/de/de>)

Produkt-Support

Alle Informationen und umfangreiches Knowhow rund um Ihr Produkt finden Sie hier:

- **FAQs**
Antworten auf häufig gestellte Fragen
- **Handbücher / Betriebsanleitungen**
Online lesen oder downloaden, verfügbar als PDF oder individuell konfigurierbar.
- **Zertifikate**
Übersichtlich sortiert nach Zulassungsstelle, Art und Land.
- **Kennlinien**
Zur Unterstützung bei Planung und Projektierung Ihrer Anlage
- **Produktmitteilungen**
Neueste Informationen und Meldungen für unsere Produkte
- **Downloads**
Für Ihr Produkt finden Sie hier Updates, Servicepacks, HSPs und vieles mehr.
- **Anwendungsbeispiele**
Funktionsbausteine, Hintergrund und Systembeschreibungen, Performance-Aussagen, Vorführrsysteme und Applikationsbeispiele verständlich erklärt und dargestellt
- **Technische Daten**
Technische Produktdaten zur Unterstützung bei der Planung und Umsetzung Ihres Projekts

Link: Produkt-Support (<https://support.industry.siemens.com/cs/de/de/ps>)

mySupport

In Ihrem persönlichen Arbeitsbereich "mySupport" stehen Ihnen folgende Funktionen zur Verfügung:

- **Support Request**
Suchen Sie nach Requestnummer, Produkt oder Betreff
- **Meine Filter**
Mit Filtern grenzen Sie den Inhalt im Online Support auf verschiedene Schwerpunkte ein.

- **Meine Favoriten**
Mit Favoriten setzen Sie Lesezeichen auf Beiträge und Produkte, die Sie häufig benötigen.
- **Meine Benachrichtigungen**
Ihr persönliches Postfach zum Austausch von Informationen und Verwalten Ihrer Kontakte. Mit "Benachrichtigungen" können Sie sich Ihre individuellen Newsletter zusammenstellen.
- **Meine Produkte**
Mit Produktlisten können Sie Ihren Schaltschrank, Ihre Anlage oder Ihr ganzes Automatisierungsprojekt virtuell abbilden.
- **Meine Dokumentation**
Konfigurieren Sie aus verschiedenen Handbüchern Ihre individuelle Dokumentation.
- **CAX-Daten**
Einfacher Zugriff auf CAX-Daten, wie z. B. 3D-Modelle, 2D Maßzeichnungen, EPLAN-Makros, Geräteschaltpläne
- **Meine IBase-Registrierungen**
Registrieren Sie Ihre Produkte, Systeme und Software von Siemens.

1.2 Siemens Industry Online Support App

Siemens Industry Online Support App

Mithilfe der kostenlosen Siemens Industry Online Support App haben Sie Zugriff auf alle gerätespezifischen Informationen, die im Siemens Industry Online Support zu einer Artikelnummer verfügbar sind, z. B. Betriebsanleitungen, Handbücher, Datenblätter, FAQ.

Die Siemens Industry Online Support App ist verfügbar für Android und iOS:



Android



iOS

Sicherheitstechnik Allgemein

2.1 Grundbegriffe

Redundanz

Bei Redundanz werden mehrere Bauteile für die gleiche Funktion eingesetzt, sodass eine fehlerhafte Funktion eines Bauteils durch das andere Bauteil bzw. durch die anderen Bauteile ersetzt wird. Durch den redundanten Aufbau lässt sich die Wahrscheinlichkeit eines Funktionsausfalls aufgrund von einzelnen defekten Bauteilen verringern. Diese Anforderung ist notwendig, um einen Safety Integrity Level SILCL 3 nach IEC 62061, SIL 3 nach IEC 61508 und PL e nach ISO 13849-1 zu erreichen (unter Umständen auch für SIL 2 / PL d notwendig).

Die einfachste Form für die Redundanz ist die Zweikanaligkeit. Durch den zweikanaligen Aufbau wird sichergestellt, dass bei Versagen eines Kreises, die Sicherheitsfunktion weiterhin gewährleistet ist. In einem redundanten Systemaufbau müssen auch die Teilsysteme Erfassen und Reagieren zweikanalig ausgeführt werden.

Hinweis

Alle SIRIUS-Safety-Geräte, die SILCL 3 nach IEC 62061, SIL 3 nach IEC 61508 und PL e nach ISO 13849-1 erfüllen, sind sowohl bezüglich der internen Logik als auch bezüglich der Ausgangskreise redundant aufgebaut.

Querschlusserkennung

Die Querschlusserkennung ist eine Diagnosefunktion eines Auswertegerätes, in dem bei zweikanaligen Erfassen oder Einlesen auch Kurz- und Querschlüsse zwischen den Eingangskanälen (Sensorkreisen) erkannt werden. Ein Querschluss kann beispielsweise durch das Quetschen einer Mantelleitung entstehen, was bei Geräten ohne Querschlusserkennung zur Folge haben kann, dass z. B. eine zweikanalige Not-Halt-Schaltung auch bei nur einem fehlerhaften Öffnerkontakt (Zweitfehler) keine Abschaltung auslöst.

Freigabekreis

Ein Freigabekreis stellt ein sicherheitsgerichtetes Ausgangssignal zur Verfügung. Freigabekreise wirken nach außen meist wie Schließer (funktional aber wird immer das sichere Öffnen betrachtet). Ein einzelner Freigabekreis, der intern im Sicherheitsschaltgerät redundant aufgebaut ist, kann für SIL 3 / PL e eingesetzt werden. Anmerkung: Freigabestrompfade können auch für Meldezwecke eingesetzt werden.

Rückführkreis

Ein Rückführkreis dient der Überwachung angesteuerter Aktoren (z. B. Relais oder Lastschütze) mit zwangsgeführten Kontakten bzw. Spiegelkontakten. Die Freigabekreise können nur bei geschlossenem Rückführkreis aktiviert werden.

2.1 Grundbegriffe

Bei Verwendung eines redundanten Abschaltpfades muss der Rückführkreis beider Aktoren ausgewertet werden. Diese dürfen dafür auch in Reihe geschaltet werden.

Automatischer Start

Bei einem automatischen Start wird das Gerät ohne manuelle Zustimmung, aber nach Prüfung des Eingangsabbildes und positivem Test des Auswertegeräts gestartet. Diese Funktion wird auch als dynamischer Betrieb bezeichnet und ist für Not-Halt-Einrichtungen unzulässig. Schutzeinrichtungen für nicht begehbare Gefahrenzonen (z. B. Positionsschalter, Lichtgitter, Schaltmatte) können mit dem automatischen Start arbeiten, wenn dadurch keine Gefahr entsteht.

Überwachter Start

Bei einem überwachten Start wird die Maschine durch Betätigung des Starttasters, nach Prüfung des Eingangsabbildes und nach positivem Test des Auswertegeräts gestartet. Der überwachte Start wertet den Signalwechsel des Starttasters aus. Somit kann die Bedienung des Starttasters nicht überlistet werden. Für PL e (ISO 13849-1) sowie SIL 3 (IEC 62061) muss bei Not-Halt der überwachte Start eingesetzt werden. Für andere Sicherheitssensoren/-funktionen hängt die Notwendigkeit des überwachten Startbefehls von der Risikobeurteilung ab.

Manueller Start

Bei einem manuellen Start wird das Gerät durch Betätigung des Starttasters, nach Prüfung des Eingangsabbildes und nach positivem Test des Sicherheitsschaltgeräts gestartet. Beim manuellen Start wird der Starttaster nicht auf korrekte Funktion überwacht, es genügt eine positive Flanke des Starttasters um zu starten.

Hinweis

Der manuelle Start ist für Not-Halt-Einrichtungen nicht zulässig.

Zweihandbedienung / Synchronität

Synchrone Sensorbetätigung ist eine spezielle Form der Gleichzeitigkeit von Sensoren. Hier ist es nicht nur erforderlich, dass Sensorkontakt 1 und 2 "in beliebigen zeitlichen Abstand" gemeinsam in den geschlossenen Zustand versetzt werden, sondern hier müssen die Sensorkontakte innerhalb von 0,5 s geschlossen werden. Die Anforderung der Synchronität von Sensoren gibt es insbesondere bei Zweihandsteuerungen an Pressen. Hierdurch soll gewährleistet werden, dass die Presse nur dann aktiv wird, wenn die Sensoren zeitgleich mit beiden Händen betätigt werden. Somit wird das Risiko für den Bediener, versehentlich in die Presse zu greifen, minimiert.

Zwangsöffnung

Zwangsöffnende Schalter sind derart aufgebaut, dass die Betätigung des Schalters zwangsläufig ein Öffnen der Kontakte bewirkt. Verschweißte Kontakte werden durch die Betätigung aufgebrochen (EN 60947-5-1).

Zwangsgeführte Kontakte

Bei einer Komponente mit zwangsgeführten Kontakten ist garantiert, dass die Öffner- und Schließerkontakte niemals gleichzeitig geschlossen sind (EN 60947-5-1).

Spiegelkontakte

Ein Spiegelkontakt ist ein Öffnerkontakt, der garantiert nicht gleichzeitig mit einem Hauptkontakt geschlossen sein kann (EN 60947-4-1).

2.2 Allgemeines

In diesem Kapitel finden Sie allgemeine und übergreifende Informationen zum Thema Sicherheitstechnik.

Details zu Vorschriften und Normen sowie zu Spezifikation und Design von sicherheitsrelevanten Teilen von Steuerungen befinden sich am Ende des Handbuchs.

2.2.1 Zielsetzung der Sicherheitstechnik

Zielsetzung der Sicherheitstechnik ist, die Gefährdung von Menschen und Umwelt durch konstruktive Maßnahmen und technische Einrichtungen so gering wie möglich zu halten, ohne dadurch die industrielle Produktion, den Einsatz von Maschinen oder die Herstellung von chemischen Produkten mehr als unbedingt notwendig einzuschränken. Durch international abgestimmte Regelwerke soll der Schutz von Mensch und Umwelt allen Ländern in gleichem Maße zuteilwerden und gleichzeitig sollen Wettbewerbsverzerrungen wegen unterschiedlicher Sicherheitsanforderungen im internationalen Handel vermieden werden.

2.2.2 Lokale Gesetze

Wichtig für Hersteller von Maschinen und Errichter von 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 USA betrieben werden soll, den dortigen Anforderungen genügen, auch wenn der Maschinenhersteller aus der EU stammt. Auch wenn die technischen Konzepte, mit denen Sicherheit erreicht wird, technischen Gesetzmäßigkeiten unterliegen, ist es trotzdem wichtig zu beachten, ob gesetzliche Regelungen mit bestimmten Vorgaben oder Restriktionen bestehen.

2.2.3 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, oder von "funktionaler Sicherheit", wenn die Sicherheit von der korrekten Funktion abhängt.

Um funktionale Sicherheit einer Maschine oder Anlage zu erreichen, ist es notwendig, dass die sicherheitsrelevanten Teile der Schutzeinrichtungen 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 folgenden 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 62061: "Safety Integrity Level" (SIL)
- In ISO 13849-1: "Performance Level" (PL)

2.2.4 Zielsetzung der Normen

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.

Details zu Vorschriften und Normen befinden sich in Kapitel Vorschriften und Normen (Seite 175).

Hinweis

Kein Anspruch auf Vollständigkeit

Die in diesem Handbuch aufgeführten Normen, Richtlinien und Gesetze sind eine Auswahl, um wesentliche Ziele und Prinzipien zu vermitteln. Die Liste erhebt keinen Anspruch auf Vollständigkeit.

2.2.5 Sicherheitsbezogene Funktionen

Die sicherheitsbezogenen Funktionen umfassen klassische und komplexere Funktionen.

Klassische Funktionen:

- Stillsetzen
- Handlungen im Notfall
- Verhindern unbeabsichtigten Anlaufs

Komplexere Funktionen:

- Zustandsabhängige Verriegelungen
- Geschwindigkeitsbegrenzung
- Positionsbegrenzung
- Kontrolliertes Stillsetzen
- Kontrolliertes Halten u. a.

2.2.6 Stillsetzen

Stillsetzen (Stopp-Kategorien der EN 60204-1)

Zum Stillsetzen einer Maschine sind in EN 60204-1 (VDE 0113 Teil 1) drei Stopp-Kategorien definiert, die den Steuerablauf für das Stillsetzen unabhängig von einer Notfallsituation beschreiben:

Stopp-Kategorie	Bedeutung
0	Ungesteuertes Stillsetzen durch sofortige Abschaltung der Energie zu den Maschinenantriebselementen
1	Gesteuertes Stillsetzen; Energiezufuhr wird erst dann unterbrochen, wenn Stillstand erreicht ist.
2	Gesteuertes Stillsetzen, bei dem die Energiezufuhr im Stillstand erhalten bleibt.

Hinweis

Durch das Abschalten wird nur die Zufuhr der Energie, die eine Bewegung verursachen kann, unterbrochen. Es wird nicht spannungsfrei geschaltet.

2.2.7 Handlung im Notfall

EN 60204-1 / 11.98 hat folgende mögliche Handlungen für Notfälle festgelegt und definiert (EN 60204-1 Anhang D). Die Begriffe in Klammern entsprechen der Ausführung im Schlusssentwurf der Ausgabe 5.0 von IEC 60204-1.

Eine Handlung im Notfall schließt einzeln oder in Kombination ein:

- Stillsetzen im Notfall (Not-Halt)
- Ingangsetzen im Notfall (Not-Start)
- Ausschalten im Notfall (Not-Aus)
- Einschalten im Notfall (Not-Ein)

Diese Funktionen werden nach EN 60204-1 und nach ISO 13850 ausschließlich durch eine bewusste menschliche Handlung ausgelöst. Im Folgenden wird nur auf das "Ausschalten im Notfall" und auf das "Stillsetzen im Notfall" weiter eingegangen. Letzteres entspricht voll dem

gleichnamigen Begriff in der EU-Maschinenrichtlinie (engl. Emergency Stop). Der Einfachheit halber werden im Folgenden die alternativen Begriffe Not-Aus und Not-Halt verwendet.

2.2.8 Not-Aus

Eine Handlung im Notfall, die dazu bestimmt ist, die Versorgung mit elektrischer Energie zu einer ganzen oder zu einem Teil einer Installation abzuschalten, falls ein Risiko für elektrischen Schlag oder ein anderes Risiko elektrischen Ursprungs besteht (aus EN 60204-1 Anhang D).

Funktionale Aspekte zum Ausschalten im Notfall sind in IEC 60364-4-46 (identisch mit HD 384-4-46 und VDE 0100 Teil 460) festgelegt. Ein Ausschalten im Notfall ist vorzusehen, wo

- Schutz gegen direktes Berühren (z. B. mit Schleifleitungen, Schleifringkörpern, Schaltgeräten in elektrischen Betriebsräumen) nur durch Abstand oder Hindernisse erreicht wird;
- Es die Möglichkeit anderer Gefährdungen oder Beschädigungen durch elektrische Energie gibt.

Weiterhin heißt es in 9.2.5.4.3 von EN 60204-1: Ein Ausschalten im Notfall wird durch Abschalten der Maschine von der Versorgung erreicht, mit der Folge eines Stopps der Kategorie 0.

Wenn für eine Maschine der Stopp der Kategorie 0 nicht zulässig ist, kann es notwendig sein, einen anderen Schutz z. B. gegen direktes Berühren vorzusehen, sodass ein Ausschalten im Notfall nicht notwendig ist.

Dies bedeutet, dass Not-Aus dort einzusetzen ist, wo die Risikoanalyse eine Gefährdung durch die elektrische Spannung / Energie ergibt und deshalb ein unverzügliches und umfassendes Abschalten der elektrischen Spannung erfordert.

2.2.9 Not-Halt

Eine Handlung im Notfall, die dazu bestimmt ist, einen Prozess oder eine Bewegung anzuhalten, der (die) Gefahr bringend wurde (aus EN 60204-1 Anhang D). Weiterhin heißt es in 9.2.5.4.2 von EN 60204-1:

Zusätzlich zu den Anforderungen für Stopp (siehe 9.2.5.3 von EN 60204-1) gelten für das Stillsetzen im Notfall folgende Anforderungen:

- Es muss gegenüber allen anderen Funktionen und Betätigungen in allen Betriebsarten Vorrang haben
- Die Energie zu den Maschinen-Antriebselementen, die einen Gefahr bringenden Zustand bzw. Gefahr bringende Zustände verursachen können, muss ohne Erzeugung anderer Gefährdungen so schnell wie möglich abgeschaltet werden (z. B. durch mechanische Anhaltevorrichtungen, die keine externe Versorgung erfordern, durch Gegenstrombremsen bei Stopp-Kategorie 1).
- Das Rücksetzen darf keinen Wiederanlauf einleiten.

Das Stillsetzen im Notfall muss entweder als ein Stopp der Kategorie 0 oder der Kategorie 1 wirken (siehe 9.2.2 von EN 60204-1). Die Kategorie für das Stillsetzen im Notfall muss anhand der Risikobeurteilung für die Maschine festgelegt werden.

Geräte für das Stillsetzen im Notfall müssen an jedem Bedienstand sowie an anderen Orten, wo die Einleitung eines Stillsetzens im Notfall erforderlich sein kann, vorhanden sein.

Um die Schutzziele der EN 60204-1 zu erfüllen, gelten folgende Anforderungen:

- Bei einem Schalten der Kontakte, nur auch bei einer kurzen Betätigung, muss das Befehlsgerät zwangsweise verrasten.
- Es darf nicht möglich sein, dass die Maschine von einem entfernten Hauptbedienstand wieder gestartet wird, ohne dass die Gefahr vorher beseitigt wurde. Die Not-Halt-Einrichtung muss "vor Ort" durch eine bewusste Handlung wieder entriegelt werden.

2.2.10 Sicherheitsfunktion

Eine Sicherheitsfunktion beschreibt die Reaktion einer Maschine / Anlage bei Eintritt eines bestimmten Ereignisses (z. B. Öffnen einer Schutztür). Die Ausführung der Sicherheitsfunktion(en) erfolgt durch ein sicherheitsgerichtetes Steuerungssystem. Dieses besteht in der Regel aus drei Teilsystemen: dem Erfassen, dem Auswerten und dem Reagieren.

Erfassen (Sensoren):

- Das Erkennen einer Sicherheitsanforderung, z. B.: Not-Halt oder ein Sensor zur Überwachung eines gefährlichen Bereichs (Lichtgitter, Laserscanner, etc.) wird betätigt.

Auswerten (Auswerteeinheit):

- Das Erkennen einer Sicherheitsanforderung und das sichere Einleiten der Reaktion, z. B. Abschalten der Freigabekreise.
- Die Überwachung von Sensorik und Aktorik auf korrekte Funktion.
- Das Einleiten einer Reaktion bei erkannten Fehlern.

Reagieren (Aktoren):

- Das Abschalten der Gefährdung gemäß dem Schaltbefehl der Auswerteeinheit.

2.2.11 Rückstell- und Starteinrichtungen

Die Notwendigkeit eine Rückstelleinrichtung (Reset) und eine Starteinrichtung (Start der Maschine) in Sicherheitsfunktion bzw. Maschinensteuerungen zu realisieren ist von mehreren Faktoren abhängig, insbesondere von der Art der Sicherheitsfunktion. Auch die Gestaltung der Befehleinrichtung bietet verschiedene Möglichkeiten.

Abhängigkeit von der Art der Sicherheitsfunktion

Die Notwendigkeit einer Starteinrichtung ergibt sich aus den Anforderungen der EN 60204-1 "Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen".

Im Absatz 9.2.5.2 "Start" wird beschrieben, dass der Start des Betriebes nur dann möglich sein darf, wenn alle entsprechenden Sicherheitsfunktionen und/oder Schutzmaßnahmen in der richtigen Stellung und betriebsbereit sind.

Im Fall von Maschinen, die mehr als eine Bedienstation erfordern, um einen Start einzuleiten, muss jede Bedienstation eine gesonderte, manuell betätigte Starteinrichtung haben. Die Bedingungen um einen Anlauf einzuleiten müssen sein:

- alle erforderlichen Bedingungen für den Maschinenbetrieb müssen erfüllt sein
- alle Starteinrichtungen müssen in Ruhestellung (AUS) sein
- danach müssen alle Starteinrichtungen gleichzeitig betätigt werden.

Dieser Teil der IEC 60204 legt auch die Anforderungen an NOT-HALT-Funktionen fest. Wenn eine aktive Betätigung eines NOT-HALT-Gerätes einen nachfolgenden Steuerbefehl ausgelöst hat, muss die Wirkung dieses Befehls bis zu seiner Rückstellung erhalten bleiben.

"Diese Rückstellung darf nur durch eine manuelle Handlung an dem Ort möglich sein, wo der Befehl eingeleitet wurde. Die Rückstellung des Befehls darf die Maschine nicht wieder in Gang setzen, sondern nur das Wieder-in-Gang-Setzen ermöglichen."

In diesem Fall bedarf es sowohl der Rückstelleinrichtung am Ort des Not-Halt Gerätes, als auch die Start-Einrichtung der Maschine um nach erfolgter Rückstellung diese wieder in Gang zu setzten. (siehe auch EN ISO 13849-1 Absatz 5.2.2 "Manuelle Rückstellung")

In vielen Fällen kann die Rückstellfunktion beim Not-Halt bereits durch die mechanische Entriegelung des Not-Halt Befehlsgerätes vor Ort gewährleistet werden. (siehe EN ISO 13850 Absatz 4.1.4." Rückstellung des Not-Halt-Gerätes")

Eine ähnliche Anforderung für Rückstellfunktionen existiert für trennende Schutzeinrichtung:

"Das (Wieder-) Schließen oder Rückstellen einer verriegelten Schutzeinrichtung darf keinen gefahrbringenden Maschinenbetrieb einleiten.

ANMERKUNG: Anforderungen an trennende Schutzeinrichtungen mit Startfunktion (steuernde trennende Schutzeinrichtung) sind in ISO 12100-2, 5.3.2.5 festgelegt."

Auch hier wird sowohl die Rückstelleinrichtung für die Schutztür beschrieben als auch die Notwendigkeit einer Start-Einrichtung um die Maschine wieder in Gang zu setzen. Eine Ausnahme bilden hier trennende Schutzeinrichtungen, die einen automatischen Wiederanlauf erlauben (z.B. nicht hintertretbare Schutzgitter siehe EN ISO 13849-1) und andere Befehls-einrichtungen mit selbständiger Rückstellung (z.B. Zweihandbedienungen, Tipbetrieb, etc. siehe EN 60204-1). Hier ist keine Rückstell- oder Start-Einrichtung notwendig um nach Auslösen dieser Sicherheitsfunktion die Maschine wieder in Gang zu setzen.

Farbgestaltung der Befehlsgeräte nach Norm

Die Farbgestaltung der Rückstelleinrichtung bzw. Starteinrichtung sind ebenfalls in der EN 60204-1 festgelegt (Kapitel 10.2)

- "Die Farben für START/EIN-Bedienteile sollten WEISS, GRAU, SCHWARZ oder GRÜN, vorzugsweise WEISS sein. ROT darf nicht verwendet werden."
- "Die Farbe ROT muss für NOT-HALT- und NOT-AUS-Bedienteile verwendet werden."
- "Rückstell-Drucktaster müssen BLAU, WEISS, GRAU oder SCHWARZ sein."

Siehe auch

Ausführlicher FAQ zum Thema Rückstell- und Starteinrichtungen (<http://support.automation.siemens.com/WW/view/de/109748231>)

2.2.12 Betriebsartenwahlschalter

Maschinen besitzen häufig mehrere Betriebsarten, die durch einen Betriebsartenwahlschalter umgeschaltet werden. Jede Maschine muss so ausgelegt werden, dass es sich in jeder Betriebsart um eine sichere Maschine handelt. Da der Betriebsartenwahlschalter nur zwischen diesen, durch Sicherheitsfunktionen geschützten, sicheren Betriebsarten wechselt, muss der Betriebsartenwahlschalter nicht sicher ausgelegt oder in die Berechnung dieser Sicherheitsfunktionen einbezogen werden.

Die Betriebsartenwahl darf selbst keinen Maschinenbetrieb auslösen, dieser muss durch eine separate Bedienung erfolgen.

Falls eine Betriebsart das Aufheben einer Sicherheitsfunktion erfordert (z. B. für das Einrichten oder Instandsetzen), muss diese laut EN 60204-1 Kapitel 9.2.4 durch eine andere Sicherheitsfunktion ersetzt werden.

In diesem Fall empfiehlt es sich, den Betriebsartenwahlschalter elektrisch ähnlich des höchsten Sicherheitslevels aller Betriebsarten aufzubauen. Aber auch hier erfolgt kein Einbezug in die Berechnung der Sicherheitsfunktionen.

Zusätzlich gibt es für bestimmte Maschinentypen besondere Anforderungen an die Betriebsartenumschaltung. Diese werden in den C-Normen für diese Maschinentypen erwähnt und müssen angewendet werden.

Siehe auch

Ausführlicher FAQ zum Thema Betriebsartenwahl (<http://support.automation.siemens.com/WW/view/de/89260861>)

2.2.13 Anschluss von Aktoren

Hinweis

Um die in den folgenden Beispielen genannten Performance Level/Safety Integrity Level zu erreichen, müssen die gezeigten Aktoren im Rückführkreis des entsprechenden Sicherheitsschaltgerätes überwacht werden.

Hinweis

Bei kapazitiven und induktiven Verbrauchern empfehlen wir eine geeignete Schutzbeschaltung. Dadurch können elektromagnetische Störungen unterdrückt und die Kontaktlebensdauer erhöht werden.

Aktorbeschtaltung bis zu PL c nach ISO 13849-1 bzw. SIL CL 1 nach IEC 62061

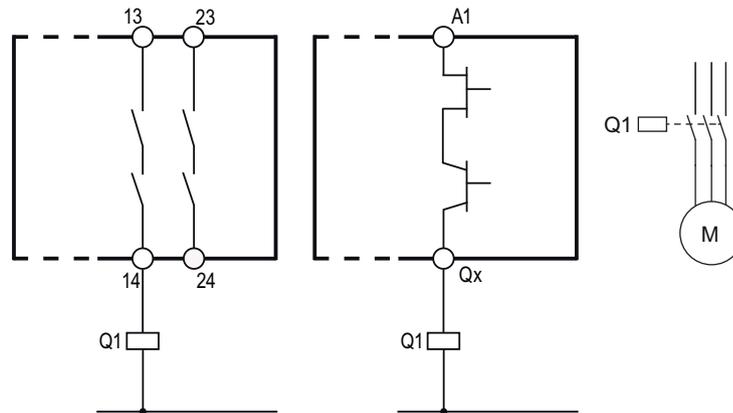


Bild 2-1 PL c nach ISO 13849-1 bzw. SIL CL 1 nach IEC 62061

Aktorbeschtaltung bei geschützter Verlegung bis zu PL e / Kat. 4 nach ISO 13849-1 bzw. SIL CL 3 nach IEC 62061

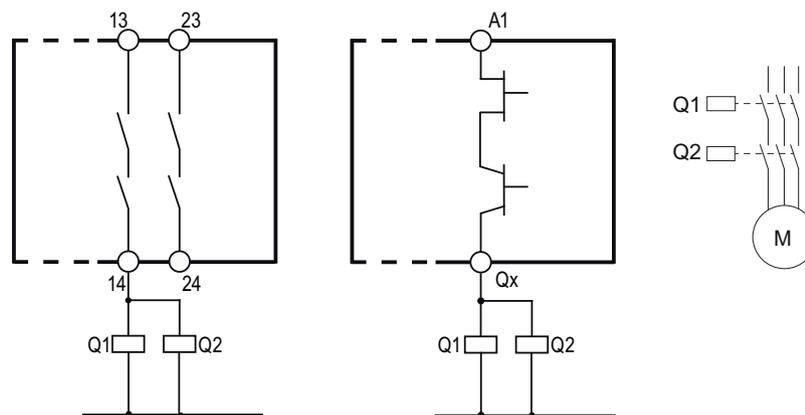


Bild 2-2 PL e nach ISO 13849-1 bzw. SIL CL 3 nach IEC 62061

⚠️ WARNUNG

Verlegung der Steuerleitungen

PL e nach ISO 13849-1 bzw. SIL CL 3 nach IEC 62061 kann nur mit querschluss-/P-Schlussicherer Verlegung der Steuerleitungen vom Schaltgeräte Ausgang (z. B. 14) zu den Steuerrelais/-schützen (Q1 und Q2) erreicht werden (z. B. als separat ummantelte Leitung oder in einem eigenen Kabelkanal).

Einschränkungen bezüglich des erreichbaren Sicherheitslevels bei einzelnen Steuergeräten sind, beachten Sie die Angaben im Handbuch des jeweiligen Geräts.

Aktorbeschaltung bis zu PL e nach ISO 13849-1 bzw. SIL CL 3 nach IEC 62061

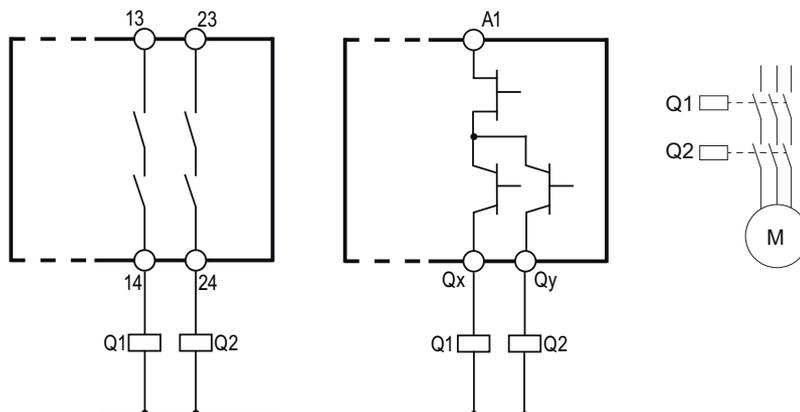


Bild 2-3 PL e nach ISO 13849-1 bzw. SIL CL 3 nach IEC 62061

Überwachung des Rückführkreises

Die Überwachung der Aktorik ist eine Diagnosefunktion und trägt damit erheblich zum erreichten SIL bzw. PL des jeweiligen Teilsystems bei. Bei elektromechanischen Komponenten (z. B. Relais oder Schütze) wird häufig ein zwangsgeführter Hilfskontakt (Spiegelkontakt) der Komponente auf die Steuerung rückgeführt und dort ausgewertet. Hierbei spricht man von der Überwachung des Rückführkreises bzw. dem Rücklesen der Schütze.

Dies ist besonders in einem redundanten Aufbau erforderlich. Verschweißt eines der beiden Schütze unerkannt, würde das zweikanalige System zu einem einkanaligen System werden. Stattdessen wird das Verschweißen erkannt und ein erneutes Einschalten bis zur Behebung des Fehlers verhindert.

Beim Einsatz einer F-PLC als Auswerteeinheit muss das Zurücklesen des NC-Kontaktes nicht zwingend auf einen sicheren Eingang (F-DI) erfolgen – ein Standard-Eingang (DI) ist ebenfalls in den meisten Applikationen ausreichend.

Für den Einsatz eines Sicherheitsschaltgeräts 3SK2 mit PROFINET-Anbindung bedeutet dies, dass das Rückführkreissignal alternativ zum direkten Anschluss an einen F-INx des 3SK2 auch über einen Standard-Eingang (DI) der überlagerten Steuerung eingelesen und über PROFINET an das 3SK2 übertragen werden kann.

In folgenden Fällen kann ein Anschluss des Rückführkreises an eine F-DI sinnvoll bzw. geboten sein:

- Einkanaliger Aufbau der Aktorik aber dennoch Forderung eines hohen Diagnosedeckungsgrads.
- Bestimmte Diagnosefunktionen (z. B. STEP 7-Baustein "FDBACK") sind nicht möglich.
- Einsatz eines fehlersicheren Moduls in der dezentralen Peripherie, um die Sicherheitsmechanismen von PROFIsafe zu nutzen.

Weitere Informationen zur Rückführkreisüberwachung mit einer F-PLC sind folgendem Anwendungsbeispiel (<https://support.industry.siemens.com/cs/ww/de/view/21331098>) zu entnehmen.

2.2.14 Leistungsschütz als Aktor

Schütze sind ein wesentlicher Bestandteil in sicherheitsgerichteten Anwendungen. In vielen sicherheitstechnischen Anwendungen wird ein Leistungsschütz als Aktor verwendet, um bei einer angeforderten Sicherheitsfunktion (z.B. Öffnen einer verriegelten Schutztür) die Maschine in den sicheren Zustand zu versetzen.

In diesem Kapitel wird kurz die sicherheitstechnische Berechnung eines Leistungsschützes erläutert.

Ein separater Anwendungsleitfaden erläutert ausführlich die Möglichkeiten und Anforderungen beim Einsatz von Schützen in sicherheitsgerichteten Anwendungen:

Schütze in Sicherheitsapplikationen – Anwendungsleitfaden (<https://support.industry.siemens.com/cs/de/de/view/109807687>)

Der Fokus liegt maßgeblich auf Anwendungen in der Fertigungsindustrie, ein gesondertes Kapitel erläutert jedoch auch den Einsatz in der Prozessindustrie.

Hierzu werden zunächst die Grundlagen des Einsatzes von Schützen in der funktionalen Sicherheitstechnik anhand der einschlägigen Normen vermittelt. Anschließend wird dem Anwender ein konkreter Leitfaden zur Auswahl des richtigen Schützes für verschiedenste Applikationen zur Verfügung gestellt.

Berechnung der Sicherheitsintegrität

Für die Berechnung der Sicherheitsintegrität werden für diese elektromechanischen Geräte B10-Werte benötigt. Der B10-Wert für verschleißbehaftete Geräte wird in Anzahl Schaltspiele ausgedrückt und spiegelt die Anzahl der Betätigungen wieder, nach denen 10 % der Geräte bei einer Lebensdauerprüfung ausgefallen sind.

Mit Hilfe des B10-Wertes kann der Anwender dann mit einer vereinfachten Formel (siehe Abschnitt 6.7.8.2.1 der DIN EN 62061) die gesamte Ausfallrate einer elektromechanischen Komponente berechnen:

$$\lambda = 0,1 \times C / B10$$

mit C = Betätigungszyklus pro Stunde (Operating Cycle). C ist eine Angabe des Anwenders und für jede Applikation separat zu bestimmen.

Die Ausfallrate setzt sich aus ungefährlichen (λ_S)- und gefahrbringenden (λ_D)-Ausfällen zusammen:

$$\lambda = \lambda_S + \lambda_D$$

oder

$$\lambda_D = [\text{Anteil gefahrbringender Ausfälle in \%}] \times \lambda$$

$$\lambda_S = [\text{Anteil ungefährliche Ausfälle in \%}] \times \lambda$$

Die Ausfallrate der gefahrbringenden Ausfälle λ_D der eingesetzten Komponente wird für die weiteren Berechnungen benötigt.

Der in der DIN EN ISO 13849-1:2008 verwendete B10d-Wert wird wie folgt ermittelt:

$$B10d = B10 / \text{Anteil gefahrbringender Ausfälle}$$

Die Standard-B10-Werte und prozentualen Anteilen gefahrbringender Ausfälle (A_{gA}) für verschleißbehaftete/elektromechanische Komponenten der industriellen Schalttechnik finden sich in den Datenblättern des Produktes. Die Werte sind außerdem in der Safety

Evaluation im TIA Selection Tool hinterlegt und stehen somit bei jeder Berechnung zur Verfügung.

Zu beachten sind insbesondere die Bedingungen unter denen diese Kennwerte gelten. In der Regel wird der B10 Wert eines Leistungsschützes bei 66 % des Bemessungsbetriebsstromes ermittelt. Dies ergibt sich aus der Notwendigkeit der Überdimensionierung als eines der bewährten Sicherheitsprinzipien und muss deshalb auch in der Applikation eingehalten werden.

Betriebsmäßiges Schalten

Sollen die Leistungsschütze auch betriebsmäßig geschaltet werden, so muss beachtet werden, dass dies auch Einfluss auf die Berechnung der Sicherheitsintegrität hat. So muss bei der Berechnung der Ausfallrate als Betätigungszyklus der Wert angenommen werden, der sowohl betriebsmäßiges als auch sicherheitstechnisches Schalten beinhaltet. Die Anforderungen zur zeitlichen Fehleraufdeckung müssen berücksichtigt werden, so dass es nicht grundsätzlich zu einer Fehleranhäufung während des betriebsmäßigen Schaltens kommen kann. Ist dies nicht gegeben, dann muss das betriebsmäßige Schalten anders realisiert werden.

2.2.15 Reihenschaltung von Sensoren

Reihenschaltung von Not-Halt-Befehlsgeräten

Eine Reihenschaltung von Not-Halt-Befehlsgeräten ist bis zum höchsten Sicherheitslevel SILCL 3 nach IEC 62061, SIL 3 nach IEC 61508 und PL e nach ISO 13849-1 möglich, da angenommen wird, dass immer nur ein Not-Halt betätigt wird. Somit ist gewährleistet, dass Fehler / Defekte aufgedeckt werden können. Siehe Kapitel "Stillsetzen im Notfall" - Einleitung (Seite 34).

Reihenschaltung von Positionsschaltern

Grundsätzlich ist es möglich, Positionsschalter in Reihe zu verschalten, wenn ausgeschlossen werden kann, dass mehrere Schutztüren regelmäßig gleichzeitig geöffnet werden (da sonst keine Fehleraufdeckung erfolgen kann)

Für Sicherheitslevel gemäß SILCL 3 nach IEC 62061, SIL 3 nach IEC 61508 und PL e nach ISO 13849-1 dürfen sie jedoch nie in Reihe geschaltet werden, da immer jeder gefährliche Fehler aufgedeckt werden muss (unabhängig vom Bedienpersonal).

Siehe Kapitel "Schutztürüberwachung" - Begriffe aus der Norm (Seite 76).

Reihenschaltung eines Not-Halt-Befehlsgerätes und einer Schutztürüberwachung

Grundsätzlich ist es möglich, ein Not-Halt-Befehlsgerät und Positionsschalter in Reihe zu verschalten, wenn ausgeschlossen werden kann, dass beide regelmäßig gleichzeitig geöffnet/ betätigt werden (da sonst keine Fehleraufdeckung erfolgen kann).

Für Sicherheitslevel gemäß SILCL 3 nach IEC 62061, SIL 3 nach IEC 61508 und PL e nach ISO 13849-1 dürfen sie jedoch nie in Reihe geschaltet werden, da immer jeder gefährliche Fehler aufgedeckt werden muss (unabhängig vom Bedienpersonal).

Siehe Kapitel "Typische Kombinationen von Sicherheitsfunktionen" - Einleitung (Seite 137).

Applikationsbeispiele

3.1 Einführung

Befinden sich Menschen in der Nähe von Maschinen (z. B. in der Fertigungstechnik), müssen diese durch technische Einrichtungen angemessen geschützt werden. Daraus resultiert eine Vielzahl an Sicherheitsfunktionen, die genau diesem Zweck dienen sollen. Die Umsetzung einiger der wesentlichsten Sicherheitsfunktionen wird in den nachfolgenden Kapiteln an Hand leicht verständlicher Applikationsbeispiele gezeigt. Die Beispiele sind aufgeteilt nach der Art der zur realisierenden Sicherheitsfunktion:

- Stillsetzen im Notfall
- Schutztürüberwachung
- Überwachung offener Gefahrenbereiche
- Drehzahl/Stillstandsüberwachung
- Sicheres Bedienen
- Typische Kombinationen von Sicherheitsfunktionen

Applikationsbeispiele pro Auswertegerät

In den folgenden Tabellen sind die Applikationsbeispiele auch noch dem jeweiligen Auswertegerät gruppiert. Auf diese Weise kann zusätzlich zur Kapitelstruktur auch eine gezielte Auswahl von Beispielen zu bestimmten Auswertegeräten (z.b. 3SK2) erfolgen.

Tabelle 3-1 3SK1

Sicherheits-level		Erfassen						Reagieren			Link
SIL	PL	Not-Halt	Positionsschalter				Sonstiges	Schütz	Motor-starter	Sonstiges	
			Mecha-nisch	RFID	Magne-tisch	Zuhal-tung					
1	c	x	-	-	-	-	-	x	-	-	Kapitel 3.2.2 (Seite 163)
3	e	x	-	-	-	-	-	x	-	-	Kapitel 3.2.7 (Seite 44)
3	e	x	-	-	-	-	-	-	x	3RM1	Kapitel 3.2.9 (Seite 47)
3	e	x	-	-	-	-	-	-	x	ET 200SP	Kapitel 3.2.14 (Seite 57)
3	e	x	-	-	-	-	-	-	-	3RW55	Kapitel 3.2.20 (Seite 71)

3.1 Einführung

Sicherheits-level		Erfassen						Reagieren			Link
SIL	PL	Not-Halt	Positionsschalter				Sonstiges	Schütz	Motorstarter	Sonstiges	
			Mechanisch	RFID	Magnetisch	Zuhal- tung					
1	c	-	x	-	-	-	-	x	-	-	Kapitel 3.3.3 (Seite 84)
3	e	-	x	-	-	-	-	x	-	-	Kapitel 3.3.5 (Seite 87)
3	e	-	x	-	-	-	-	-	x	3RM1	Kapitel 3.3.7 (Seite 91)
3	e	-	-	x	-	-	-	x	-	-	Kapitel 3.3.10 (Seite 98)
3	e	-	-	-	-	-	Licht- vorhang	x	-	-	Kapitel 3.4.2 (Seite 112)
3	e	-	-	-	-	-	Schalt- matte	x	-	-	Kapitel 3.4.4 (Seite 116)
2	d	-	-	-	-	-	Laser- scanner	x	-	-	Kapitel 3.4.6 (Seite 120)
3	e	-	-	-	-	-	Zweihand- bedienung	x	-	-	Kapitel 3.6.2 (Seite 132)
3	e	x	x	-	-	-	-	x	-	-	Kapitel 3.7.5 (Seite 145)
3	e	x	x	-	-	-	Kaskadie- rung	x	-	-	Kapitel 3.7.8 (Seite 152)
3	e	x	-	-	-	-	-	x	-	3RQ1	Kapitel 3.7.13 (Seite 163)

Tabelle 3-2 3SK2

Sicherheits-level		Erfassen						Reagieren			Link
SIL	PL	Not-Halt	Positionsschalter				Sonstiges	Schütz	Motorstarter	Sonstiges	
			Mechanisch	RFID	Magnetisch	Zuhal- tung					
1	c	x	-	-	-	-	-	x	-	-	Kapitel 3.2.3 (Seite 37)
2	c	x	-	-	-	-	-	x	-	F-PLC IN Schütz	Kapitel 3.2.5 (Seite 40)
3	e	x	-	-	-	-	-	x	-	-	Kapitel 3.2.8 (Seite 46)

Sicherheitslevel		Erfassen						Reagieren			Link
SIL	PL	Not-Halt	Positionsschalter				Sonstiges	Schütz	Motorstarter	Sonstiges	
			Mechanisch	RFID	Magnetisch	Zuhalterung					
3	e	x	-	-	-	-	-	-	x	3RM1	Kapitel 3.2.10 (Seite 49)
3	e	x	-	-	-	-	-	x	-	F-PLC IN Schütz	Kapitel 3.2.12 (Seite 53)
3	e	x	-	-	-	-	-	-	x	ET 200SP	Kapitel 3.2.15 (Seite 58)
3	e	x	-	-	-	-	-	-	x	3RM1	Kapitel 3.2.18 (Seite 64)
3	e	x	-	-	-	-	-	-	x	3RM1	Kapitel 3.2.19 (Seite 67)
1	c	-	x	-	-	-	-	x	-	-	Kapitel 3.3.4 (Seite 85)
3	e	-	x	-	-	-	-	x	-	-	Kapitel 3.3.6 (Seite 89)
3	e	-	x	-	-	-	-	-	x	3RM1	Kapitel 3.3.8 (Seite 93)
3	e	-	-	x	-	-	-	x	-	-	Kapitel 3.3.11 (Seite 100)
2	d	-	x	-	-	x	-	x	-	-	Kapitel 3.3.12 (Seite 102)
3	e	-	-	-	-	-	Lichtvorhang	x	-	-	Kapitel 3.4.3 (Seite 114)
3	e	-	-	-	-	-	Schaltmatte	x	-	-	Kapitel 3.4.5 (Seite 118)
2	d	-	-	-	-	-	Laser-scanner	x	-	-	Kapitel 3.4.7 (Seite 122)
3	e	-	x	-	-	x	Stillstandswächter	x	-	-	Kapitel 3.5.3 (Seite 128)
3	e	-	-	-	-	-	Zweihandbedienung	x	-	-	Kapitel 3.6.3 (Seite 134)

3.1 Einführung

Sicherheitslevel		Erfassen					Reagieren			Link	
SIL	PL	Not-Halt	Positionsschalter				Sonstiges	Schütz	Motorstarter		Sonstiges
			Mechanisch	RFID	Magnetisch	Zuhalterung					
2	d	x	-	-	-	-	Stromüberwachung	x	-	-	Kapitel 3.7.4 (Seite 142)
3	e	x	x	-	-	-	-	x	-	-	Kapitel 3.7.6 (Seite 147)
3	e	x	-	-	-	-	Lichtvorhang + Zweihandbedienung	x	-	-	Kapitel 3.7.7 (Seite 149)
3	e	-	-	x	-	x	-	x	-	-	Kapitel 3.3.14 (Seite 106)
3	e	x	x	-	-	x	Lichtvorhang	x	-	-	Kapitel 3.7.15 (Seite 169)

Tabelle 3-3 3RK3 MSS

Sicherheitslevel		Erfassen					Reagieren			Link	
SIL	PL	Not-Halt	Positionsschalter				Sonstiges	Schütz	Motorstarter		Sonstiges
			Mechanisch	RFID	Magnetisch	Zuhalterung					
3	e	x	-	-	-	-	AS-I	x	-	-	Kapitel 3.2.11 (Seite 51)
3	e	-	x	-	-	-	AS-I	x	-	-	Kapitel 3.3.9 (Seite 95)
3	e	x	x	-	-	-	AS-I Querverkehr	x	-	-	Kapitel 3.7.9 (Seite 154)

Tabelle 3-4 F-CPU

Sicherheitslevel		Erfassen						Reagieren			Link
SIL	PL	Not-Halt	Positionsschalter				Sonstiges	Schütz	Motor-starter	Sonstiges	
			Mecha-nisch	RFID	Magne-tisch	Inkl. Zuhaltung					
2	c	x	-	-	-	-	-	x	-	F-PLC IN Schütz	Kapitel 3.2.6 (Seite 42)
3	e	x	-	-	-	-	-	x	-	F-PLC IN Schütz	Kapitel 3.2.13 (Seite 55)
3	e	x	-	-	-	-	-	-	x	ET 200SP	Kapitel 3.2.16 (Seite 60)
3	e	x	-	-	-	-	-	-	x	ET 200SP	Kapitel 3.2.17 (Seite 62)
3	e	x	-	-	-	-	-	x	-	3RQ1	Kapitel 3.2.21 (Seite 73)
3	e	x	-	-	x	-	Seilzug-schalter, AS-I	x	-	-	Kapitel 3.7.10 (Seite 156)
3	e	x	-	-	-	x	AS-I	x	-	-	Kapitel 3.7.11 (Seite 158)
3	e	x	x	-	-	-	ET 200eco PN	x	-	-	Kapitel 3.7.12 (Seite 161)
3	e	-	x	-	-	x	ET 200eco PN	x	-	-	Kapitel 3.3.13 (Seite 104)
3	e	-	-	x	-	x	-	x	-	-	Kapitel 3.3.15 (Seite 109)
3	e	x	-	x	-	x	ET 200AL	x	-	-	Kapitel 3.7.14 (Seite 166)

Handhabung der Applikationsbeispiele

Die Handhabung der Applikationsbeispiele ist durch ihren einheitlichen Aufbau sehr einfach. Zu Beginn jedes Beispiels wird die Anwendung kurz beschrieben. Es folgt der Aufbau der Sicherheitsfunktion an Hand einfacher Übersichtsbilder.

Sensorsignale sowie die Ansteuerung der Aktorik sind durch blaue Linien angedeutet, während der Rückführkreis zur Überwachung der Aktorik durch eine gestrichelte Linie dargestellt wird.

3.1 Einführung

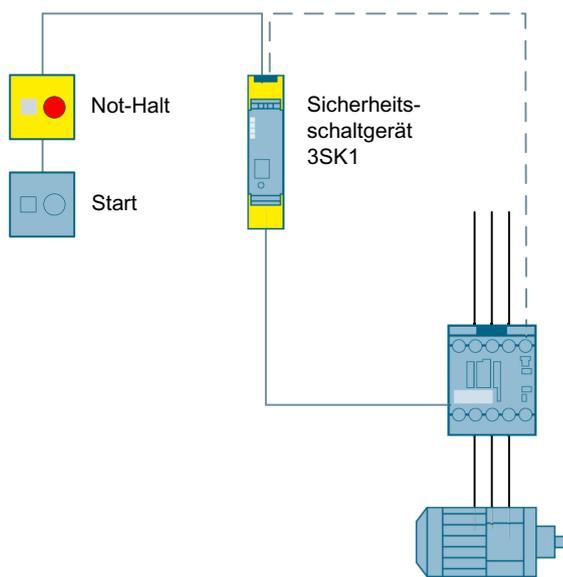


Bild 3-1 Beispieldarstellung: Aufbau einer Sicherheitsfunktion

Die genaue Funktionsweise wird ebenso erläutert wie das maximal erreichbare Sicherheitsniveau in SIL gemäß IEC 62061 sowie in PL gemäß ISO 13849-1.

Darstellung des maximal erreichbaren Sicherheitsniveaus		
Eignung für bis zu SIL 1 / PL c	Eignung für bis zu SIL 2 / PL d	Eignung für bis zu SIL 3 / PL e

Einige Applikationsbeispiele enthalten mehrere Sicherheitsfunktionen. Die Darstellung beschreibt dann das erreichte Sicherheitsniveau der im Titel genannten Sicherheitsfunktion. Das erreichte Sicherheitsniveau der zusätzlichen Sicherheitsfunktionen wird dann textuell erläutert.

Die Applikationsbeispiele werden in der Regel als SIL1 / PLc und als SIL3 / Ple Beispiel ausgelegt. Natürlich kann auch ein SIL2 / PLd erreicht werden. Da die Unterschiede im physikalischen Aufbau zwischen SIL3 / Ple und SIL2 / PLd sehr gering oder nicht vorhanden sind, wird auf dieses Beispiel in der Regel verzichtet. Der Unterschied beider Einstufungen kann auf eine unterschiedliche Qualität der Diagnose zurückgeführt werden. Die notwendigen Diagnosemechanismen sind in Auswertegeräten bereits integriert (Querschussdiagnosen, Diskrepanz,...). Somit ergibt sich in den meisten Fällen kein

unterschiedlicher Aufbau und somit auch keine unterschiedliche Anzahl der verwendeten Komponenten für ein SIL2 / PLd bzw. SIL3 / PLe Beispiel.

Hinweis

Das erreichte Sicherheitsniveau hängt von der jeweiligen Umsetzung der Applikationsbeispiele ab. Insbesondere die getroffenen Annahmen z. B. bezüglich der Schalthäufigkeit oder der Fehlerrückmeldung müssen überprüft bzw. eingehalten werden.

Zum einfachen Nachbau der Applikation werden die verwendeten sicherheitsgerichteten Komponenten aufgeführt.

In der Regel stellen die Safety Applikationsbeispiele nur eine Sicherheitsfunktion an einer Maschine dar. Darüber hinaus gibt es aber häufig eine Vielzahl von Sicherheitsfunktionen, die in einer Maschine vereint sind. Zusätzlich wird an einer Maschine auch betriebliches Schalten der Ausgänge, Motoren etc. durchgeführt. Auch hierfür sind Start-Einrichtungen und Verknüpfungslogiken in der Maschine vorhanden. Diese werden in den Safety Applikationsbeispielen nicht weiter berücksichtigt. Aus diesem Grund wird in der Regel auch darauf verzichtet die Start-Einrichtung der Maschine darzustellen, sondern es wird nur eine Rückstelleinrichtung (Reset oder Start) der Sicherheitsfunktion dargestellt.

Die Funktionalität wurde mit den angegebenen Hardwarekomponenten getestet. Sie können auch ähnliche, von dieser Liste abweichende Produkte, verwenden. Beachten Sie in einem solchen Fall, dass ggf. Änderungen bei der Verdrahtung der Hardwarekomponenten (z. B. andere Anschlussbelegung) notwendig werden.

Am Ende eines jeden Beispiels befindet sich ein Internet-Link, unter dem weiterführende Informationen zum jeweiligen Applikationsbeispiel hinterlegt sind. Dies umfasst z. B.

- Verdrahtungspläne
- Die Projektdateien bei der Verwendung des Modularen Sicherheitssystems oder des Sicherheitsschaltgeräts 3SK2
- CAx-Daten der verwendeten Hardwarekomponenten

Eine detaillierte Sicherheitsberechnung mit allen Kennwerten können Sie der hinterlegten Safety Evaluation Projektdatei entnehmen. Zur Verwendung der Datei benötigen Sie das TIA Selection Tool mit integrierter Safety Evaluation (<http://www.siemens.de/safety-evaluation-tool>).

Mit dem CAx-Download-Link können Sie mit nur wenigen Klicks sämtliche Unterlagen zu den verwendeten Hardwarekomponenten herunterladen (<http://www.siemens.de/cax>). Hierfür ist ein Konto im Siemens Service & Support Portal oder in der Siemens Industry Mall notwendig.

Die Parametrierung der Sicherheitsschaltgeräte erfolgt über DIP-Schalter. Die jeweilige Einstellung entnehmen Sie den hinterlegten Schaltbildern.

Hinweis

Details zu Vorschriften und Normen sowie die Spezifikation und Design von sicherheitsrelevanten Teilen von Steuerungen befinden sich am Ende des Handbuchs.

3.2 Stillsetzen im Notfall

3.2.1 Einleitung

Das Not-Halt-Befehlsgerät stellt eine weit verbreitete Komponente dar, um Menschen, Anlagen und die Umwelt vor Gefahren zu schützen und ein Stillsetzen im Notfall einzuleiten. In diesem Kapitel werden Applikationen mit Sicherheitsfunktionen aus genau diesem Anwendungsbereich beschrieben.

Typische Anwendung

Das Not-Halt-Befehlsgerät mit seinem zwangsöffnenden Kontakt wird hier durch ein Auswertegerät überwacht. Wird der Not-Halt betätigt, schaltet das Auswertegerät über sichere Ausgänge die nachgeschaltete Aktorik gemäß Stoppkategorie 0 nach EN 60204-1 ab. Vor dem Wiedereinschalten bzw. Quittieren der Not-Halt-Abschaltung mittels des Starttasters wird überprüft, ob die Kontakte des Not-Halt-Befehlsgerätes geschlossen sind und die Aktorik abgeschaltet hat.

Hinweis

- Verlegen Sie die Sensorleitungen geschützt; verwenden Sie als Sensoren ausschließlich Sicherheitssensoren mit zwangsöffnenden Kontakten.
 - Einrichtungen, funktionelle Aspekte und Gestaltungsleitsätze zum Not-Halt sind in der EN ISO 13850 hinterlegt. Beachten Sie zusätzlich die Norm EN 60204-1.
 - "Not-Halt" ist kein Mittel zur Risikominderung.
 - "Not-Halt" ist eine "ergänzende Sicherheitsfunktion" (Wenn "Not-Halt" betätigt wird, müssen Sie den Motor ausschalten).
-

Unbeabsichtigte Betätigung

Häufig besteht die Anforderung, ein Not-Halt-Befehlsgerät vor unbeabsichtigter Betätigung zu schützen und so die Anlagenverfügbarkeit zu erhöhen. Der erste Schritt ist die richtige Platzierung des Not-Halt-Befehlsgeräts an der Maschine. Das Not-Halt-Befehlsgerät muss leicht zugänglich, ungehindert erreichbar und gefahrlos zu betätigen sein. Zusätzlich gibt es die Möglichkeit, einen Schutzkragen zum Schutz vor unbeabsichtigter Betätigung zu verwenden. Achten Sie hierbei auch darauf, dass eine ungehinderte Erreichbarkeit gewährleistet ist.

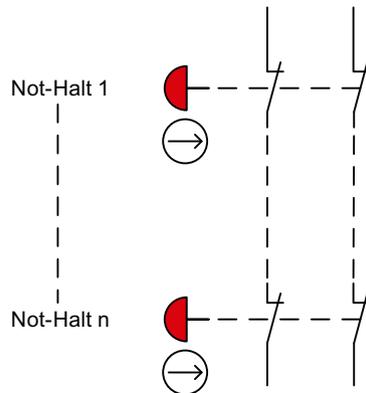
Hinweis

Die SIEMENS SIRIUS Not-Halt-Befehlsgeräte mit Schutzkragen entsprechen den Anforderungen der EN ISO 13850 "Sicherheit von Maschinen - Not-Halt - Gestaltungsleitsätze" und dürfen in Sicherheitsanwendungen eingesetzt werden.

Bedingungen bei Reihenschaltung

Not-Halt-Befehlsgeräte dürfen bis PL e (nach ISO 13849-1) bzw. SIL 3 (nach IEC 62061) nur dann in Reihe geschaltet werden, wenn das Versagen und gleichzeitige Drücken der Not-Halt-Befehlsgeräte ausgeschlossen werden kann.

Wenn mehrere Not-Halt-Befehlsgeräte elektrisch in Reihe geschaltet sind, dann stellt jedes sicherheitsgerichtete Abschalten über ein Not-Halt-Befehlsgerät eine einzelne ergänzende Sicherheitsfunktion dar. Wenn baugleiche Not-Halt-Befehlsgeräte verwendet werden, dann reicht es, exemplarisch eine ergänzende Sicherheitsfunktion stellvertretend für alle ergänzenden Sicherheitsfunktionen zu betrachten.



3.2.2 Not-Halt-Abschaltung bis SIL 1 bzw. PL c mit einem Sicherheitsschaltgerät 3SK1

Anwendung

Einkanalige Not-Halt-Abschaltung eines Motors durch ein Sicherheitsschaltgerät 3SK1 und Leistungsschutz.

Aufbau

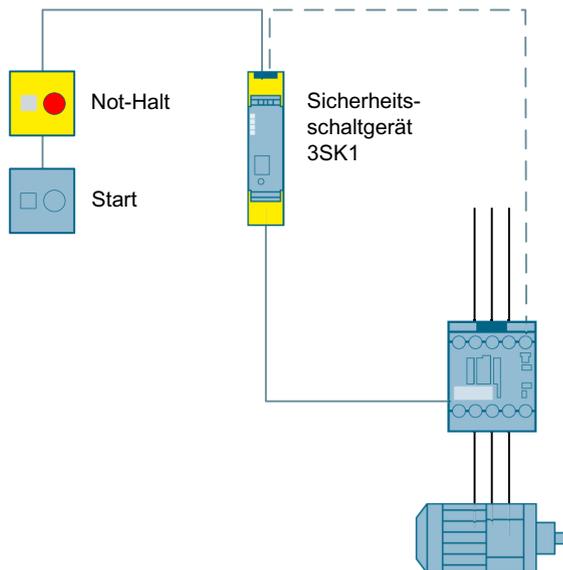
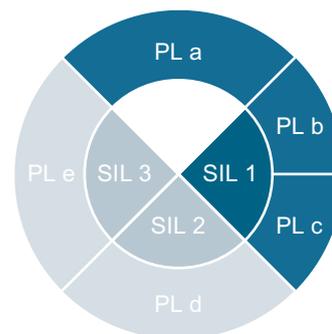


Bild 3-2 Not-Halt-Abschaltung bis SIL 1 bzw. PL c mit einem Sicherheits-schaltgerät 3SK1

Funktionsweise

Das Sicherheits-schaltgerät 3SK1 überwacht das Not-Halt-Befehlsgerät. Bei Betätigen des Not-Halt-Befehlsgeräts öffnet das Sicherheits-schaltgerät die Freigabekreise und schaltet das Leistungsschütz sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheits-schaltgerät	Schütz
3SU1 (http://www.siemens.de/sirius-act)	3SK1 (http://www.siemens.de/safety-relays)	3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/73134129>)

3.2.3 Not-Halt-Abschaltung bis SIL 1 bzw. PL c mit dem Sicherheitsschaltgerät 3SK2

Anwendung

Einkanalige Not-Halt-Abschaltung eines Motors durch ein Sicherheitsschaltgerät 3SK2 und Leistungsschütz.

Aufbau

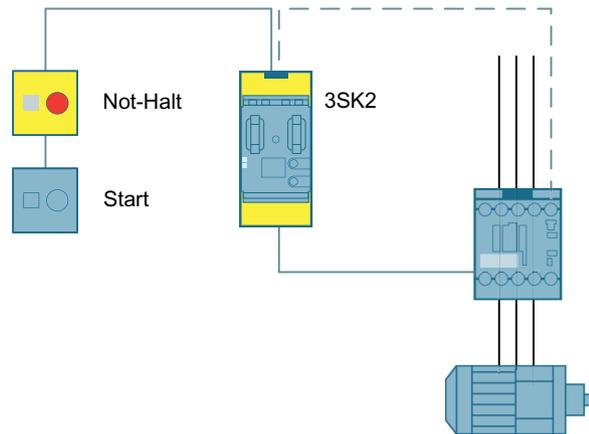
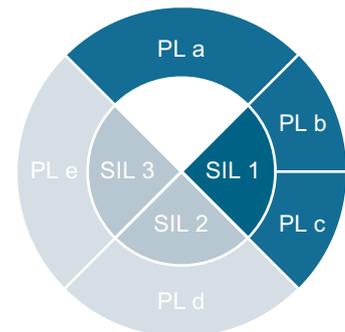


Bild 3-3 Not-Halt-Abschaltung bis SIL 1 bzw. PL c mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Das Sicherheitsschaltgerät 3SK2 überwacht das Not-Halt-Befehlsgerät. Bei Betätigen des Not-Halt-Befehlsgeräts öffnet das Sicherheitsschaltgerät die Freigabekreise und schaltet das Leistungsschütz sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Modulares Sicherheitssystem	Schütz
		
3SU1 (http://www.siemens.de/sirius-act)	3SK2 (http://www.siemens.de/safety-relays)	3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109485642>)

3.2.4 Not-Halt-Abschaltung bis SIL 1 bzw. PL c mit einem Sanftstarter 3RW55 Failsafe

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch einen Sanftstarter 3RW55 Failsafe überwacht. Sowohl das betriebsmäßige Schalten mit Sanftan- und auslauf als auch die sichere Abschaltung erfolgen durch den Sanftstarter 3RW55 Failsafe.

Aufbau

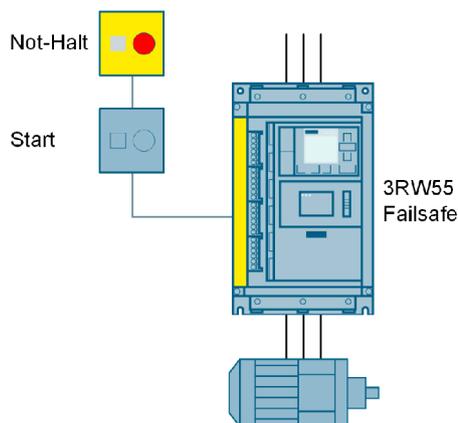


Bild 3-4 Not-Halt-Abschaltung bis SIL 1 bzw. PL c mit einem Sanftstarter 3RW55 Failsafe

Funktionsweise

Der Sanftstarter 3RW55 Failsafe überwacht das Not-Halt-Befehlsgerät. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet der Sanftstarter die Last sicher ab. Ist das Not-Halt-Befehlsgerät entriegelt, kann ein Neustart durch den Knebelschalter S2 eingeleitet werden. Um den Sanftstarter 3RW55 Failsafe nach einer STO-Abschaltung und anschließender Freigabe des Not-Halt-Befehlsgeräts wieder zu starten, ist eine positive Flanke am Starteingang (Default: DI1) notwendig. In dieser Applikation geschieht dies durch Aus- und Einschalten des Knebelschalters S2.

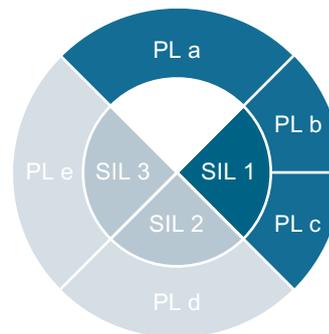
Mit den Sanftstartern 3RW55 Failsafe lassen sich Applikationen mit der Sicherheitsfunktion Safe Torque Off (STO) nach EN 61800-5-2 und Stopp-Kategorie 0 nach EN 60204-1 realisieren.

Der Sanftstarter 3RW55 Failsafe ist so ausgelegt, dass sich STO Applikationen bis zu SIL 1 bzw. PL c realisieren lassen, ohne dass der Anwender weitere Geräte im Abschaltpfad benutzen muss (einkanalige Abschaltung durch den Sanftstarter 3RW55 Failsafe).

Der Abschaltbefehl am fehlersicheren Eingang F-DI des 3RW55 Failsafe kann von einem direkt angeschlossenen Not-Halt Befehlsgerät oder von einem sicheren Ausgang eines übergeordneten Sicherheitsschaltgeräts bzw. einer übergeordneten fehlersicheren Steuerung kommen.

Eine Auswertung des fehlersicheren Meldeausgangs F-RQ (Klemme 41 / 42) ist für Applikationen bis zu SIL 1 bzw. PL c nicht erforderlich. Er kann jedoch auch in diesen Fällen verwendet werden, z.B. um dem Bediener über eine Meldeleuchte einen Fehler am 3RW55 Failsafe zu signalisieren.

Ein Wiederanlauf des Motors ist erst nach Rücksetzen des F-DI Signals und Wechsel der Steuerquelle von AUS nach EIN möglich. Mögliche Steuerquellen sowie detaillierte Informationen zum Sanftstarter 3RW55 Failsafe sind dem Handbuch (<https://support.industry.siemens.com/cs/de/de/view/109753752>) zu entnehmen.



Hinweis

Für die Diagnose ist es zwingend erforderlich, dass der 3RW55 Failsafe immer direkt an der Hauptspannung angeschlossen wird. Zusätzliche Schaltglieder, wie z.B. ein redundantes Schütz, dürfen erst hinter dem 3RW55 Failsafe in Reihegeschaltet werden.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sanftstarter Failsafe
	
<p>3SU1 (http://www.siemens.de/sirius-act)</p>	<p>3RW55 (http://www.siemens.de/sanftstarter)</p>

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109780385>)

Ausführlicher FAQ zum Thema: 3RW Sanftstarter: Sicheres Abschalten nach IEC 62061 (SIL) bzw. ISO 13849-1 (PL) (<https://support.industry.siemens.com/cs/WW/de/view/67474130>)

3.2.5 Not-Halt-Abschaltung bis SIL 2 bzw. PL c mit einem Schütz mit F-PLC-IN und Sicherheitsschaltgerät 3SK2

Anwendung

Einkanalige Not-Halt-Abschaltung eines Motors durch ein Sicherheitsschaltgerät 3SK2 und Leistungsschütz 3RT1 mit fehlersicherer Ansteuerung.

Aufbau

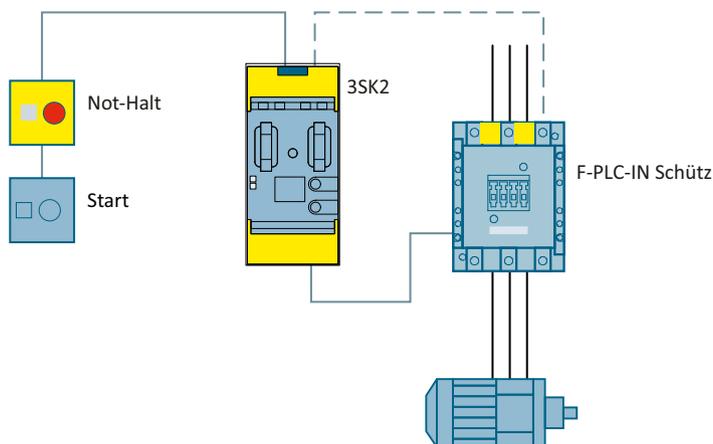
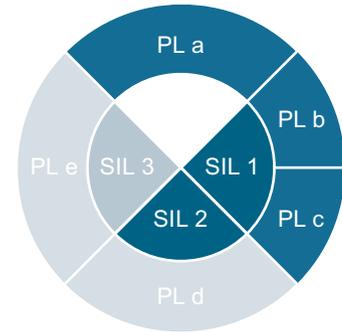


Bild 3-5 Not-Halt-Abschaltung bis SIL 2 bzw. PL c mit einem Schütz mit F-PLC-IN und Sicherheitsschaltgerät 3SK2

Funktionsweise

Das Sicherheitsschaltgerät 3SK2 überwacht das Not-Halt-Befehlsgerät. Bei Betätigen des Not-Halt-Befehlsgeräts öffnet das Sicherheitsschaltgerät die Freigabekreise und schaltet das Leistungsschütz über dessen fehlersicheren Eingang (F-PLC-IN) sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Im hier gezeigten Beispiel kommt exemplarisch ein Schütz mit fehlersicherem Steuereingang in der Baugröße S6 zum Einsatz.

Schütze mit fehlersicherem Steuereingang sind in den Baugrößen S2 bis S12 bis 250 kW verfügbar:

- Schütze 3RT20...-S in Baugrößen S2 und S3
- Schütze 3RT10...-S in Baugrößen S6 bis S12

Hinweis

Für das Erreichen eines PL c genügt bereits ein einkanaliger Aufbau des Not-Halt-Befehlsgerätes. Aufgrund einer einheitlichen Darstellung wurde hier ein zweikanaliger Aufbau gewählt. Dieser ist für eine SIL 2 Applikation notwendig.

Hinweis

Beim Einsatz des Schützes mit F-PLC-IN gemäß IEC 62061 ist zu beachten, dass neben den PFHd-Werten für den SIL auch die Hardwarefehler toleranz (HFT) zu beachten ist. So wird in diesem Beispiel zwar SIL 2 erreicht, durch die HFT von 0 kann jedoch ein Verschweißen der Schützkontakte zum Verlust der Sicherheitsfunktion führen.

Der Spiegelkontakt des Schützes dient der Fehlerdiagnose und muss in der übergeordneten Applikation (Auswerteeinheit) beachtet werden, um in Fehlerfall entsprechende Reaktionen einleiten zu können.

Hier kann beispielsweise als zweiter Abschaltpfad ein Leistungsschalter zum Einsatz kommen. Mehr Informationen hierzu sind folgendem FAQ zu entnehmen:

Welcher Sicherheitslevel kann bei der Verwendung eines Schützes und eines Leistungsschalters erreicht werden (<http://support.automation.siemens.com/WW/view/de/40349715>)

Bei der Überführung dieses Beispiels als Teilsystem in einer Gesamtapplikation nach ISO 13849 muss auch die Architektur des Teilsystems sowie die Ausfälle infolge gemeinsamer Ursache (CCF) mit in Betracht gezogen werden um den entsprechenden PL zu erhalten. Hieraus folgt, dass keine direkte Übertragung des SIL in einen PL möglich ist.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Modulares Sicherheitssystem	Schütz
		
3SU1 (http://www.siemens.de/sirius-act)	3SK2 (http://www.siemens.de/safety-relays)	3RT1 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109747648>)

3.2.6 Not-Halt-Abschaltung bis SIL 2 bzw. PL c mit einem Schütz mit F-PLC-IN und fehlersicherer Steuerung

Anwendung

Einkanalige Not-Halt-Abschaltung eines Motors durch eine fehlersichere Steuerung und Leistungsschütz 3RT1 mit fehlersicherer Ansteuerung.

Aufbau

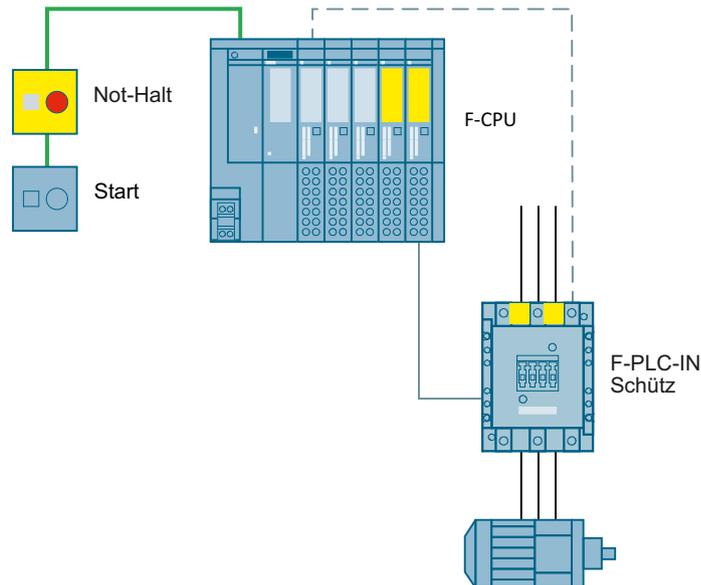
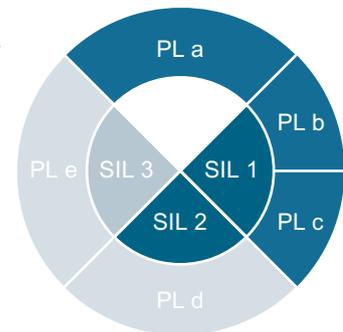


Bild 3-6 Not-Halt-Abschaltung bis SIL 2 bzw. PL c mit einem Schütz mit F-PLC-IN und fehlersicherer Steuerung

Funktionsweise

Die fehlersichere Steuerung überwacht das Not-Halt-Befehlsgerät. Bei Betätigen des Not-Halt-Befehlsgeräts schaltet die fehlersichere Steuerung das Leistungsschütz über dessen fehlersicheren Eingang (F-PLC-IN) sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Im hier gezeigten Beispiel kommt exemplarisch ein Schütz mit fehlersicherem Steuereingang in der Baugröße S6 zum Einsatz.

Schütze mit fehlersicherem Steuereingang sind in den Baugrößen S2 bis S12 bis 250 kW verfügbar:

- Schütze 3RT20...-S in Baugrößen S2 und S3
- Schütze 3RT10...-S in Baugrößen S6 bis S12

Hinweis

Beim Einsatz des Schützes mit F-PLC-IN gemäß IEC 62061 ist zu beachten, dass neben den PFHd-Werten für den SIL auch die Hardwarefehleranzahl (HFT) zu beachten ist. So wird in diesem Beispiel zwar SIL 2 erreicht, durch die HFT von 0 kann jedoch ein Verschweißen der Schützkontakte zum Verlust der Sicherheitsfunktion führen.

Der Spiegelkontakt des Schützes dient der Fehlerdiagnose und muss in der übergeordneten Applikation (Auswerteeinheit) beachtet werden, um in Fehlerfall entsprechende Reaktionen einleiten zu können.

Hier kann beispielsweise als zweiter Abschaltpfad ein Leistungsschalter zum Einsatz kommen. Mehr Informationen hierzu sind folgendem FAQ zu entnehmen:

Welcher Sicherheitslevel kann bei der Verwendung eines Schützes und eines Leistungsschalters erreicht werden (<http://support.automation.siemens.com/WW/view/de/40349715>)

Bei der Überführung dieses Beispiels als Teilsystem in einer Gesamtapplikation nach ISO 13849 muss auch die Architektur des Teilsystems sowie die Ausfälle infolge gemeinsamer Ursache (CCF) mit in Betracht gezogen werden um den entsprechenden PL zu erhalten. Hieraus folgt, dass keine direkte Übertragung des SIL in einen PL möglich ist.

Sicherheitsgerichtete Komponenten

SIRIUS ACT PROFINET Interface-modul	Steuerung Failsafe	Schütz
		
3SU1 (http://www.siemens.de/sirius-act)	S7 F-PLC (http://www.siemens.de/simatic-safety)	3RT1 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, TIA Portal-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109747647>)

3.2.7 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Anwendung

Zweikanalige Not-Halt-Abschaltung eines Motors durch ein Sicherheitsschaltgerät 3SK1 und Leistungsschütze.

Aufbau

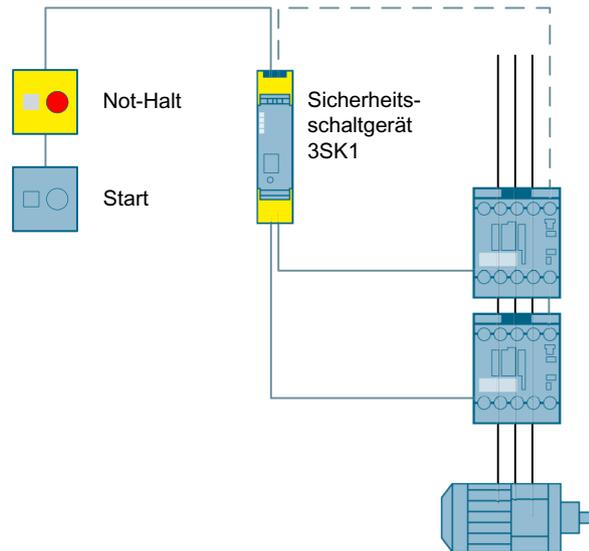
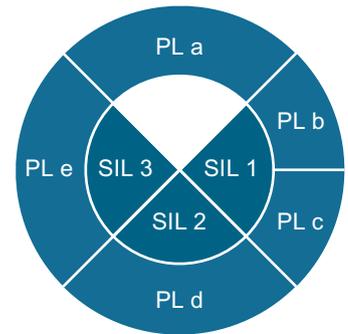


Bild 3-7 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem Sicherheitschaltgerät 3SK1

Funktionsweise

Das Sicherheitschaltgerät überwacht das Not-Halt-Befehlsgerät zweikanalig. Bei Betätigung des Not-Halt-Befehlsgeräts öffnet das Sicherheitschaltgerät die Freigabe- und schaltet die Leistungsschütze sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitschaltgerät	Schütz
		
3SU1 (http://www.siemens.de/sirius-act)	3SK1 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch:

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/73136378>)

Applikation mit Seilzugschalter anstatt Not-Halt (<https://support.industry.siemens.com/cs/ww/de/view/109738710>)

3.2.8 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Anwendung

Zweikanalige Not-Halt-Abschaltung eines Motors durch ein Sicherheitsschaltgerät 3SK2 und Leistungsschütze.

Aufbau

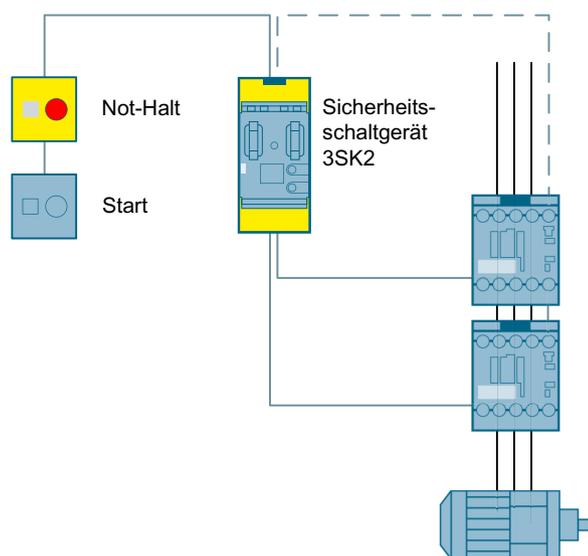
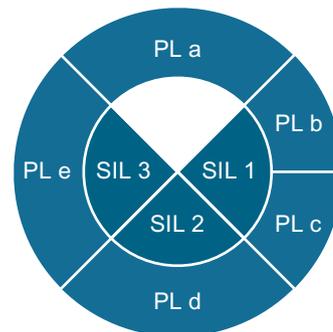


Bild 3-8 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Das Sicherheitsschaltgerät überwacht das Not-Halt-Befehlsgerät zweikanalig. Bei Betätigung des Not-Halt-Befehlsgeräts öffnet das Sicherheitsschaltgerät die Freigabeleiße und schaltet die Leistungsschütze sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschaltgerät	Schütz
		
3SU1 (http://www.siemens.de/sirius-act)	3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch:

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109479271>)

Applikation mit Seilzugschalter anstatt Not-Halt (<https://support.industry.siemens.com/cs/ww/de/view/109738710>)

3.2.9 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicheren Motorstartern und einem Sicherheitsschaltgerät 3SK1

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch ein Sicherheitsschaltgerät 3SK1 überwacht. Das sichere Abschalten erfolgt über fehlersichere Motorstarter.

Aufbau

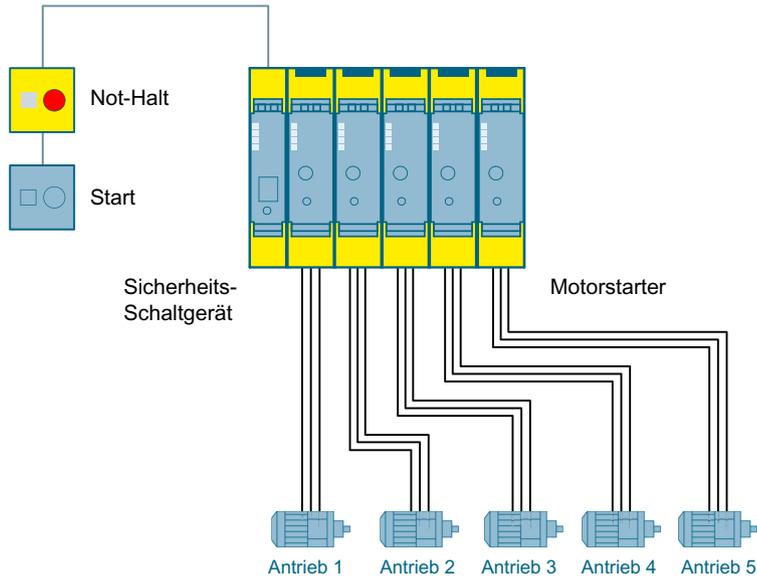
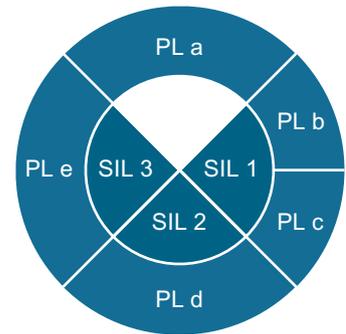


Bild 3-9 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicheren Motorstartern und einem Sicherheitsschaltgerät 3SK1

Funktionsweise

Das Sicherheitsschaltgerät überwacht das Not-Halt-Befehlsgerät. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet das Sicherheitsschaltgerät über die Geräteverbinder die fehlersicheren Motorstarter ab. Die Motorstarter schalten daraufhin die Last sicher ab. Ist das Not-Halt-Befehlsgerät entriegelt, kann durch den Starttaster wieder eingeschaltet werden.



Hinweis

In diesem Beispiel wird davon ausgegangen, dass die Gefährdung nur von jeweils einem der Antriebe ausgeht, jedoch beim Not-Halt eine Gruppe von Antrieben abgeschaltet wird. Aus diesem Grund wird in der Sicherheitsbewertung nur ein einzelner Motorstarter betrachtet und dies exemplarisch verwendet.

Besteht die Gefährdung durch die Bewegung mehrerer Antriebe, so müssen in der Sicherheitsbewertung alle Motorstarter berücksichtigt werden, die an dieser Gefahr beteiligt sind.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschaltgerät	Motorstarter Failsafe
		
3SU1 (http://www.siemens.de/sirius-act)	3SK1 (http://www.siemens.de/safety-relays)	3RM1 (http://www.siemens.de/motorstarter/3rm1)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/88411471>)

Ausführlicher FAQ zum Thema: Sicheres Abschalten mit den Motorstartern 3RM1 (<http://support.automation.siemens.com/WW/view/de/67478946>)

3.2.10 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicheren Motorstartern und einem Sicherheitsschaltgerät 3SK2

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch ein Sicherheitsschaltgerät überwacht. Das sichere Abschalten erfolgt über fehlersichere Motorstarter.

Aufbau

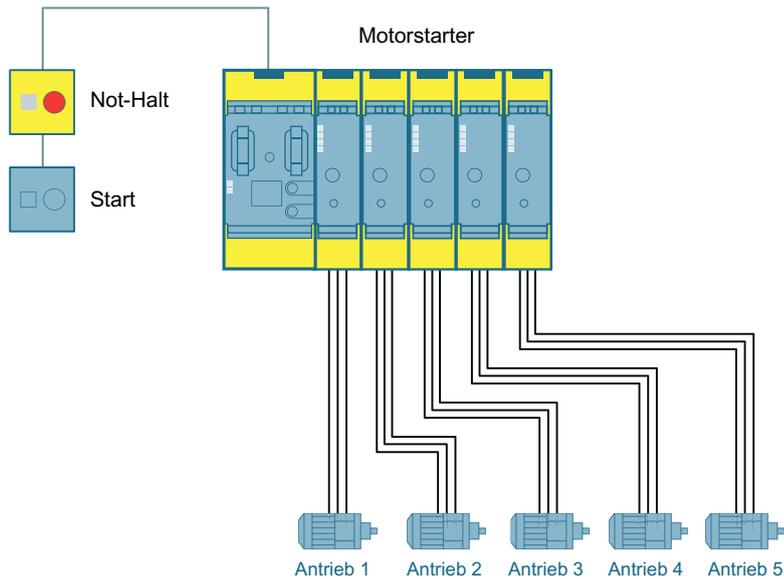
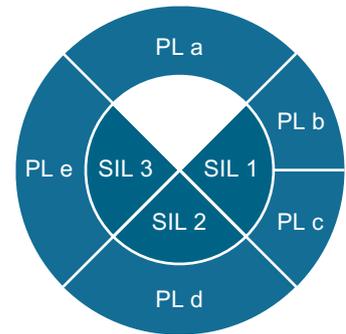


Bild 3-10 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicheren Motorstartern und einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Das Sicherheitsschaltgerät überwacht das Not-Halt-Befehlsgerät. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet das Sicherheitsschaltgerät über die Geräteverbinder die fehlersicheren Motorstarter ab.

Die Motorstarter schalten daraufhin die Last sicher ab. Ist das Not-Halt-Befehlsgerät entriegelt, kann durch den Starttaster wieder eingeschaltet werden.



Hinweis

In diesem Beispiel wird davon ausgegangen, dass die Gefährdung nur von jeweils einem der Antriebe ausgeht, jedoch beim Not-Halt eine Gruppe von Antrieben abgeschaltet wird. Aus diesem Grund wird in der Sicherheitsbewertung nur ein einzelner Motorstarter betrachtet und dies exemplarisch verwendet.

Besteht die Gefährdung durch die Bewegung mehrerer Antriebe, so müssen in der Sicherheitsbewertung alle Motorstarter berücksichtigt werden, die an dieser Gefahr beteiligt sind.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschaltgerät	Motorstarter Failsafe
		
3SU1 (2-kanalig) (http://www.siemens.de/sirius-act)	3SK2 (http://www.siemens.de/safety-relays)	3RM1 (http://www.siemens.de/motorstarter/3rm1)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109485643>)

Ausführlicher FAQ zum Thema: Sicheres Abschalten mit den Motorstartern 3RM1 (<http://support.automation.siemens.com/WW/view/de/67478946>)

3.2.11 Not-Halt-Abschaltung über AS-i bis SIL 3 bzw. PL e mit einem Modularen Sicherheitssystem

Anwendung

Überwachung mehrerer Not-Halt-Befehlsgeräte über AS-i mit einem Modularen Sicherheitssystem 3RK3.

Aufbau

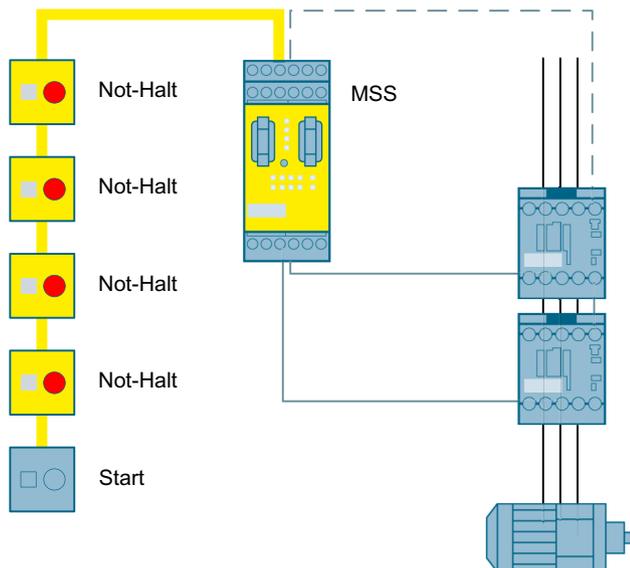
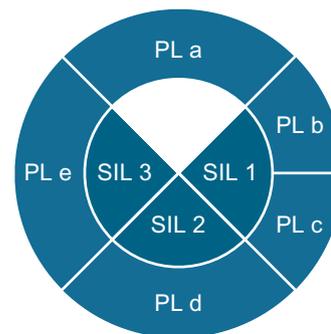


Bild 3-11 Not-Halt-Abschaltung über AS-i bis SIL 3 bzw. PL e mit einem Modulare Sicherheitssystem

Funktionsweise

Das Modulare Sicherheitssystem überwacht jedes der an AS-i angeschlossenen zweikanaligen Not-Halt-Befehlsgeräte. Bei Betätigung eines der Not-Halt-Befehlsgeräte öffnet das Modulare Sicherheitssystem die Freigabekreise und schaltet die Leistungsschütze sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Modulares Sicherheitssystem	Schütz
3SU1 (http://www.siemens.de/sirius-act)	3RK3 (http://www.siemens.de/sirius-monitor)	2x 3RT20 (http://www.siemens.de/sirius-control)

Hinweis

Zusätzlich zu den sicherheitsgerichteten Komponenten werden zum Betrieb eines AS-i-Netzwerks ein AS-i-Master sowie ein AS-i-Netzteil benötigt.

Siehe auch

MSS-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/73133559>)

3.2.12 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit Schützen mit F-PLC-IN und Sicherheitsschaltgerät 3SK2

Anwendung

Zweikanalige Not-Halt-Abschaltung eines Motors durch ein Sicherheitsschaltgerät 3SK2 und Leistungsschütze 3RT1 mit fehlersicherer Ansteuerung.

Aufbau

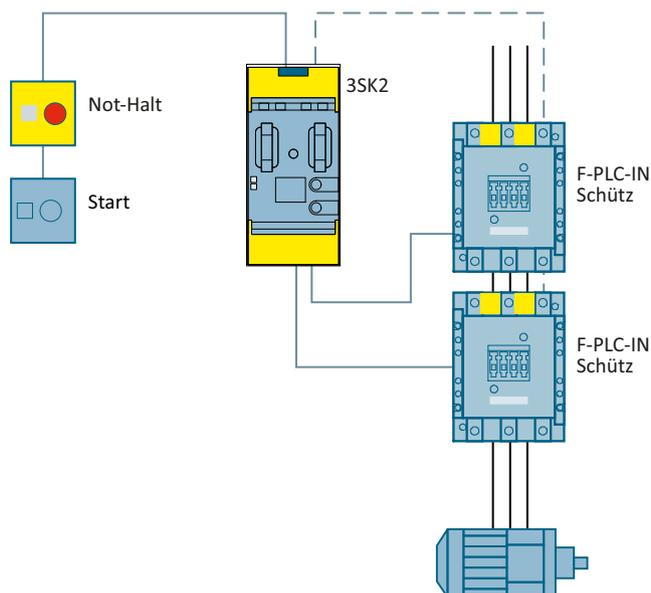
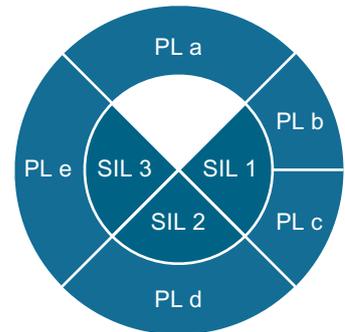


Bild 3-12 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit Schützen mit F-PLC-IN und Sicherheitsschaltgerät 3SK2

Funktionsweise

Das Sicherheitsschaltgerät 3SK2 überwacht das Not-Halt-Befehlsgerät. Bei Betätigen des Not-Halt-Befehlsgeräts öffnet das Sicherheitsschaltgerät die Freigabekreise und schaltet die Leistungsschütze über deren fehlersichere Eingänge (F-PLC-IN) sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Im hier gezeigten Beispiel kommen exemplarisch Schütze mit fehlersicherem Steuereingang in der Baugröße S6 zum Einsatz.

Schütze mit fehlersicherem Steuereingang sind in den Baugrößen S2 bis S12 bis 250 kW verfügbar:

- Schütze 3RT20...S in Baugrößen S2 und S3
- Schütze 3RT10...S in Baugrößen S6 bis S12

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschaltgerät	Schütz
		
3SU1 (http://www.siemens.de/sirius-act)	3SK2 (http://www.siemens.de/safety-relays)	2 x 3RT1 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109747650>)

3.2.13 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit Schützen mit F-PLC-IN und fehlersicherer Steuerung

Anwendung

Zweikanalige Not-Halt-Abschaltung eines Motors durch eine fehlersichere Steuerung und Leistungsschütze 3RT1 mit fehlersicherer Ansteuerung.

Aufbau

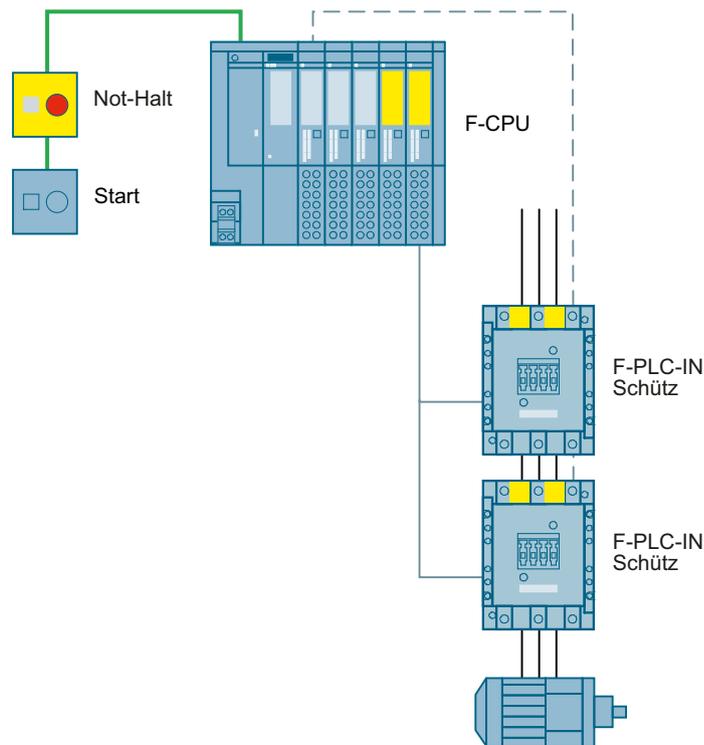
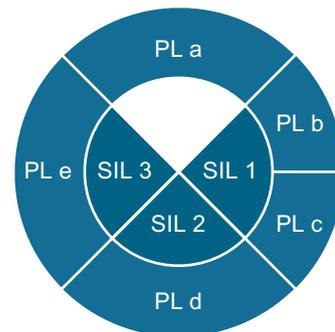


Bild 3-13 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit Schützen mit F-PLC-IN und fehlersicherer Steuerung

Funktionsweise

Die fehlersichere Steuerung überwacht das Not-Halt-Befehlsgerät. Bei Betätigen des Not-Halt-Befehlsgeräts schaltet die fehlersichere Steuerung die Leistungsschütze über deren fehlersichere Eingänge (F-PLC-IN) sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Im hier gezeigten Beispiel kommen exemplarisch Schütze mit fehlersicherem Steuereingang in der Baugröße S6 zum Einsatz.

Schütze mit fehlersicherem Steuereingang sind in den Baugrößen S2 bis S12 bis 250 kW verfügbar:

- Schütze 3RT20...S in Baugrößen S2 und S3
- Schütze 3RT10...S in Baugrößen S6 bis S12

Sicherheitsgerichtete Komponenten

SIRIUS ACT PROFINET Interface-modul	Steuerung Failsafe	Schütz
		
3SU1 (http://www.siemens.de/sirius-act)	S7 F-PLC (http://www.siemens.de/simatic-safety)	2 x 3RT1 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, TIA Portal-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109747649>)

3.2.14 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem fehlersicheren Motorstarter im ET 200SP System und Sicherheitsschaltgerät 3SK1

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch ein Sicherheitsschaltgerät 3SK1 überwacht. Das sichere Abschalten erfolgt über einen fehlersicheren Motorstarter 3RK1.

Aufbau

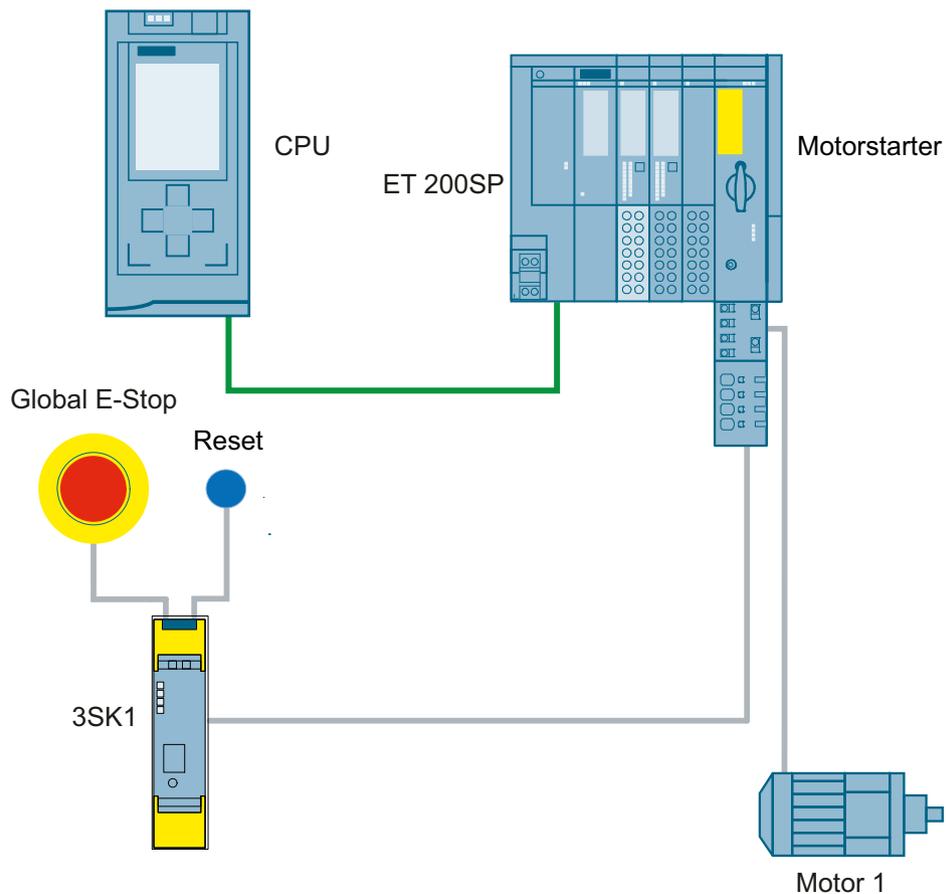
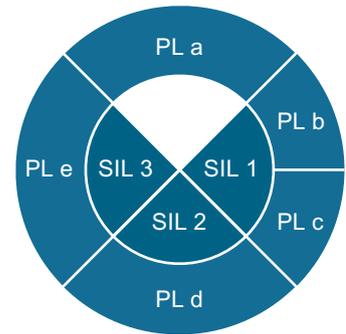


Bild 3-14 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem fehlersicheren Motorstarter im ET 200SP System und Sicherheitsschaltgerät 3SK1

Funktionsweise

Das Sicherheitsschaltgerät 3SK1 überwacht das Not-Halt-Befehlsgerät. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet das Sicherheitsschaltgerät den fehlersicheren Motorstarter über dessen fehlersicheren Eingang (F-DI) ab. Der Motorstarter schaltet daraufhin die Last sicher ab. Ist das Not-Halt-Befehlsgerät entriegelt, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschaltgerät	Motorstarter Failsafe
		
3SU1 (http://www.siemens.de/sirius-act)	3SK1 (http://www.siemens.de/safety-relays)	3RK1 (http://www.siemens.de/et200sp-motorstarter)

Siehe auch

Schaltplan, TIA Portal-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109748128>)

3.2.15 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem fehlersicheren Motorstarter im ET 200SP System und Sicherheitsschaltgerät 3SK2

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch ein Sicherheitsschaltgerät 3SK2 überwacht. Das sichere Abschalten erfolgt über fehlersichere Motorstarter 3RK1.

Aufbau

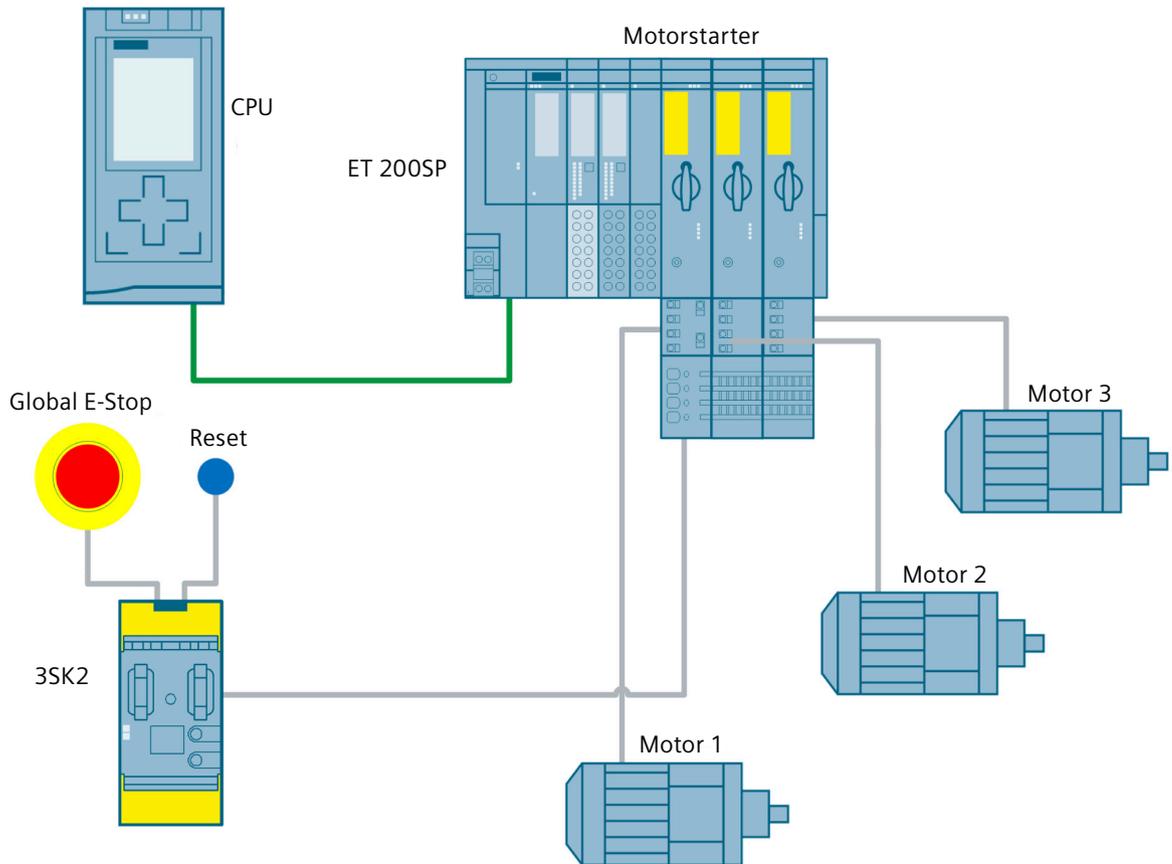
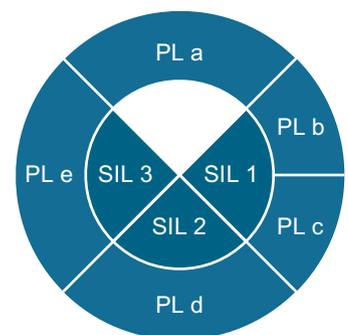


Bild 3-15 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicheren Motorstartern im ET 200SP System und Sicherheitschaltgerät 3SK2

Funktionsweise

Das Sicherheitschaltgerät 3SK2 überwacht das Not-Halt-Befehlsgerät. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet das Sicherheitschaltgerät den ersten Motorstarter über dessen fehlersicheren Eingang (F-DI) ab. Der zweite bzw. alle weiteren Motorstarter sind über ihre gebrückte Base Unit mit diesem F-DI verbunden und werden dadurch auch abgeschaltet. Die Motorstarter schalten daraufhin die Last sicher ab. Ist das Not-Halt-Befehlsgerät entriegelt, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschaltgerät	Motorstarter Failsafe
		
3SU1 (http://www.siemens.de/sirius-act)	3SK2 (http://www.siemens.de/safety-relays)	3RK1 (http://www.siemens.de/et200sp-motorstarter)

Siehe auch

Schaltplan, Safety Evaluation, TIA Portal- und 3SK2-Projekt (<http://support.automation.siemens.com/WW/view/de/109748128>)

3.2.16 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicherem Digitalausgangsmodul und fehlersicheren Motorstartern im ET 200SP System

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch eine fehlersichere Steuerung überwacht. Das sichere Abschalten erfolgt über ein fehlersicheres Digitalausgangsmodul F-DQ und fehlersichere Motorstarter 3RK1.

Aufbau

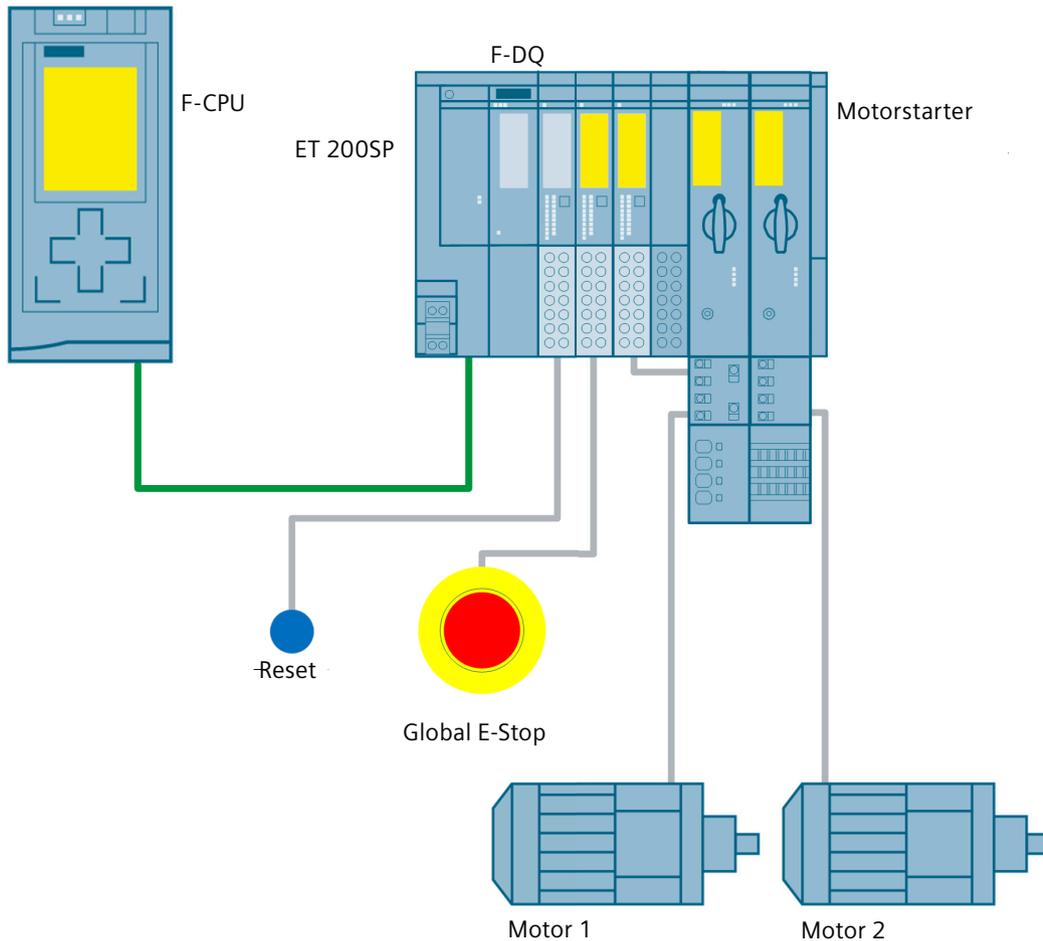
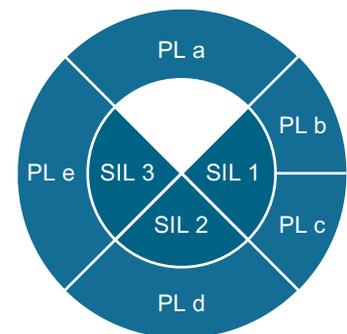


Bild 3-16 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicherem Digitalausgangsmodul und fehlersicheren Motorstartern im ET 200SP System

Funktionsweise

Die fehlersichere Steuerung überwacht das Not-Halt-Befehlsgerät. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet die fehlersichere Steuerung (über die F-DQ-Baugruppe) den ersten Motorstarter über dessen fehlersicheren Eingang (F-DI) ab. Der zweite bzw. alle weiteren Motorstarter sind über ihre gebrückte Base Unit mit diesem F-DI verbunden und werden dadurch auch abgeschaltet. Die Motorstarter schalten daraufhin die Last sicher ab. Ist das Not-Halt-Befehlsgerät entriegelt, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Steuerung Failsafe	Motorstarter Failsafe
		
<p>3SU1 (http://www.siemens.de/sirius-act)</p>	<p>S7-1500 (http://www.siemens.de/simatic-safety)</p>	<p>3RK1 (http://www.siemens.de/et200sp-motorstarter)</p>

Siehe auch

Schaltplan, TIA Portal-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109748128>)

3.2.17 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicherem Powermodul und fehlersicheren Motorstartern im ET 200SP System

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch eine fehlersichere Steuerung überwacht. Das sichere Abschalten erfolgt über ein fehlersicheres Powermodul F-PM-E und fehlersichere Motorstarter 3RK1.

Aufbau

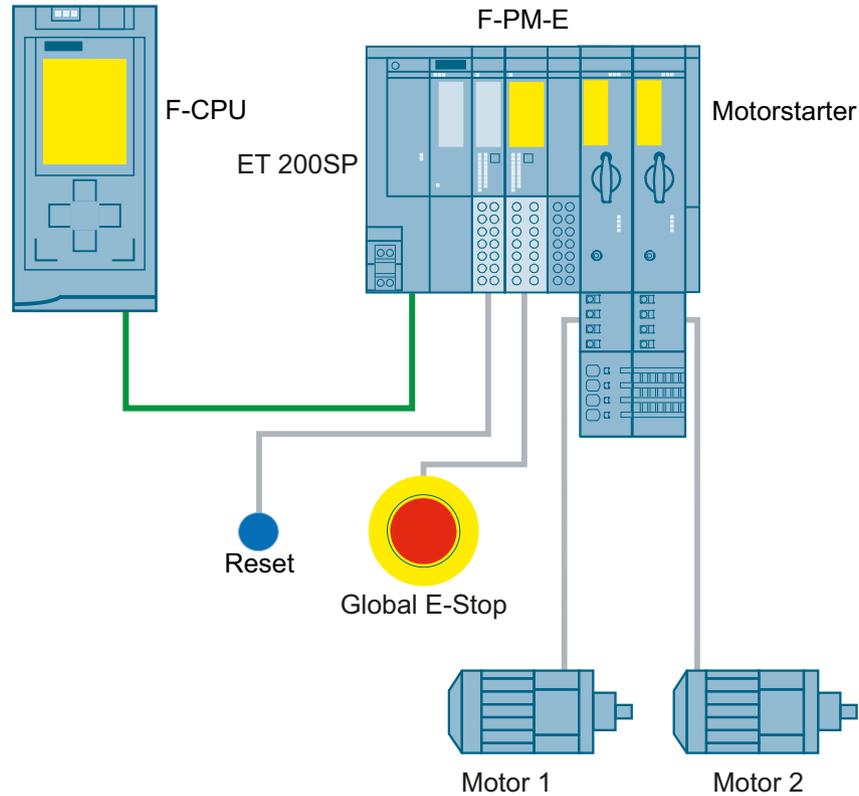
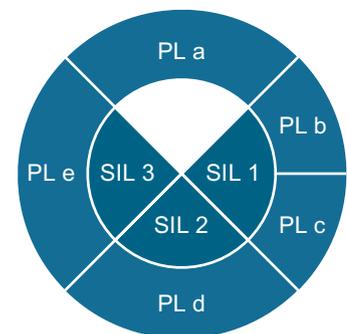


Bild 3-17 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit fehlersicherem Powermodul und fehlersicheren Motorstartern im ET 200SP System

Funktionsweise

Die fehlersichere Steuerung überwacht das Not-Halt-Befehlsgerät. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet die fehlersichere Steuerung das fehlersichere Powermodul F-PM-E und somit die fehlersicheren Motorstarter ab. Der Motorstarter schaltet daraufhin die Last sicher ab. Ist das Not-Halt-Befehlsgerät entriegelt, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Steuerung Failsafe	Motorstarter Failsafe
		
3SU1 (http://www.siemens.de/sirius-act)	S7-1500 (http://www.siemens.de/simatic-safety)	3RK1 (http://www.siemens.de/et200sp-motorstarter)

Siehe auch

Schaltplan, TIA Portal-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109748128>)

3.2.18 Not-Halt-Abschaltung bis SIL 3 bzw. PL e über Sicherheitsschaltgerät 3SK2 mit PROFINET-Anbindung und fehlersicheren Motorstartern

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch ein Sicherheitsschaltgerät 3SK2 überwacht. Die sichere Einzelabschaltung und das betriebsmäßige Schalten der fehlersicheren Motorstarter 3RM1 erfolgen lokal über Einzelverdrahtung zwischen Motorstarter 3RM1 und Sicherheitsschaltgerät 3SK2. Das Signal zum betriebsmäßigen Schalten wird von der übergeordneten Steuerung über PROFINET an das Sicherheitsschaltgerät übertragen.

Aufbau

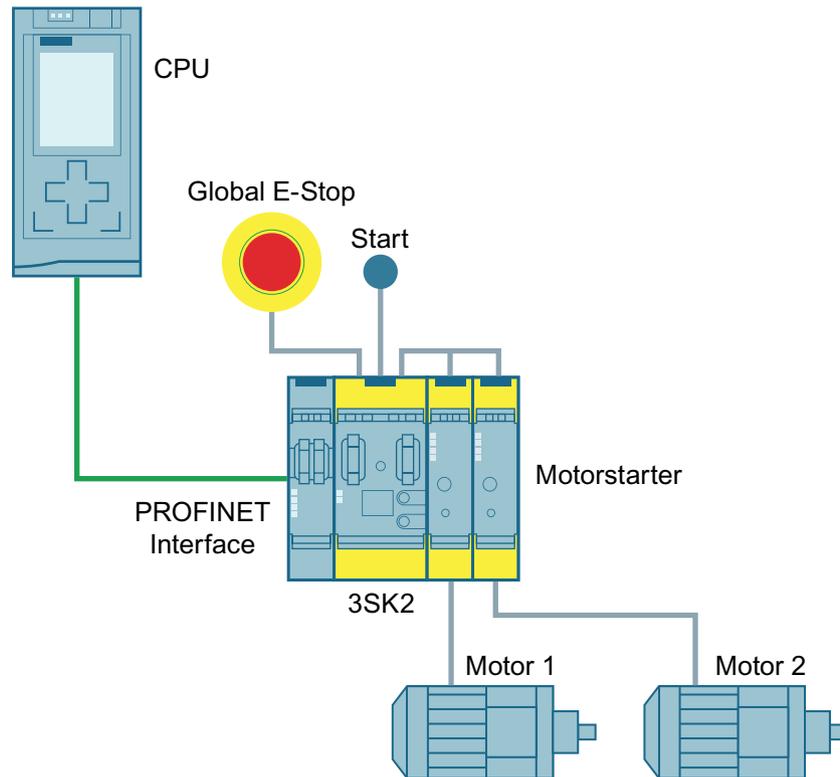


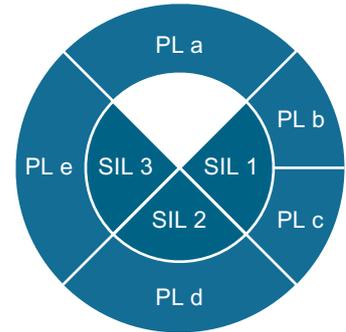
Bild 3-18 Not-Halt-Abschaltung bis SIL 3 bzw. PL e über Sicherheitsschaltgerät 3SK2 mit PROFINET-Anbindung und fehlersicheren Motorstartern

Funktionsweise

Das Sicherheitsschaltgerät 3SK2 überwacht das Not-Halt-Befehlsgerät. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet das Sicherheitsschaltgerät die fehlersicheren Motorstarter ab. Die Motorstarter schalten daraufhin die Last sicher ab. Ist das Not-Halt-Befehlsgerät entriegelt, kann durch den Starttaster wieder eingeschaltet werden.

Die Steuerung ist über das PROFINET Interfacemodul mit dem Sicherheitsschaltgerät verbunden. Im Anwenderprogramm der Steuerung wird das betriebliche Schalten der Motorstarter realisiert und über PROFINET an das 3SK2 übermittelt. Das 3SK2 leitet diese Steuersignale – verknüpft mit dem Not-Halt-Signal – über seine fehlersicheren Ausgänge an die Steuereingänge der Motorstarter (IN1 bei Direktstarter bzw. IN1 und IN2 bei Wendestarter) weiter. Somit werden das betriebsmäßige Schalten und die sichere Abschaltung bei Betätigung der Sicherheitsfunktion über dasselbe Signal realisiert.

Die Rückmeldung des 3SK2, in welchem Zustand die Sicherheitsfunktion sich aktuell befindet, wird über PROFINET an die Steuerung geschickt. Es ist möglich den Starttaster für das Wiedereinschalten, anstatt direkt am 3SK2, auch über Eingangsbaugruppen der Steuerung einzulesen und das Signal ebenfalls über PROFINET an das Sicherheitsschaltgerät zu übertragen.



Hinweis

In diesem Beispiel wird davon ausgegangen, dass die Gefährdung nur von jeweils einem der Antriebe ausgeht, jedoch beim Not-Halt eine Gruppe von Antrieben abgeschaltet wird. Aus diesem Grund wird in der Sicherheitsbewertung nur ein einzelner Motorstarter betrachtet und dies exemplarisch verwendet. Besteht die Gefährdung durch die Bewegung mehrerer Antriebe, so müssen in der Sicherheitsbewertung alle Motorstarter berücksichtigt werden, die an dieser Gefahr beteiligt sind.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschaltgerät mit PROFINET-Interfacemodul	Motorstarter Failsafe
		
3SU1 (http://www.siemens.de/sirius-act)	3SK2 (http://www.siemens.de/safety-relays)	3RM1 (http://www.siemens.de/motorstarter/3rm1)

Siehe auch

Schaltplan, Safety Evaluation, TIA Portal- und 3SK2-Projekt (<http://support.automation.siemens.com/WW/view/de/109769504>)

3.2.19 Not-Halt-Gruppenabschaltung bis SIL 3 bzw. PL e über Sicherheitsschaltgerät 3SK2 mit PROFINET-Anbindung und fehlersicheren Motorstartern

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch ein Sicherheitsschaltgerät 3SK2 überwacht. Die sichere Gruppenabschaltung der fehlersicheren Motorstarter 3RM1 erfolgt lokal über Geräteverbinder durch das Sicherheitsschaltgerät. Die übergeordnete Steuerung schaltet die Motorstarter betriebsmäßig über PROFINET.

Aufbau

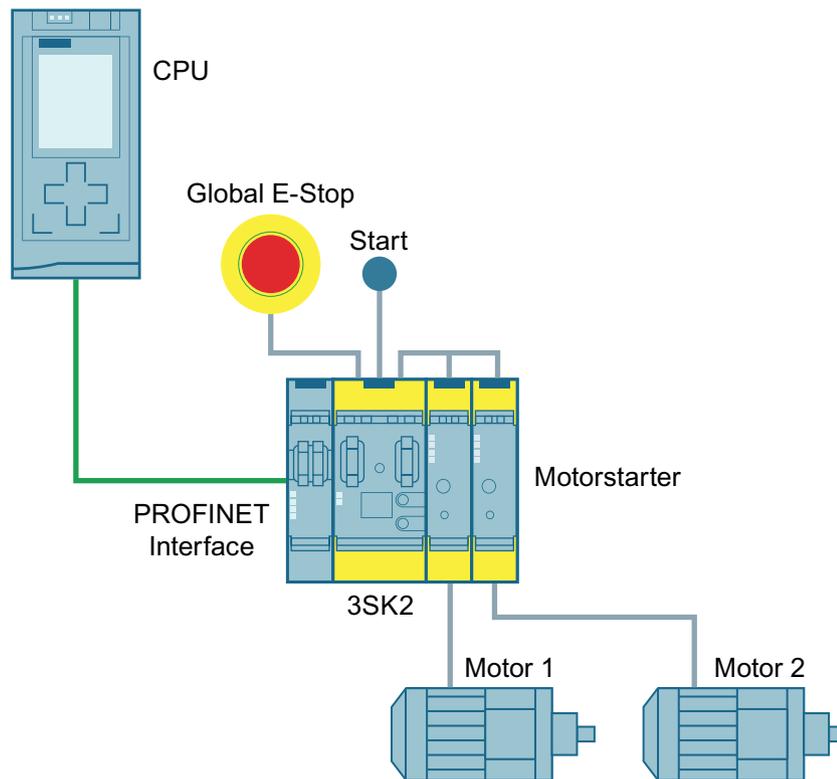


Bild 3-19 Not-Halt-Gruppenabschaltung bis SIL 3 bzw. PL e über Sicherheitsschaltgerät 3SK2 mit PROFINET-Anbindung und fehlersicheren Motorstartern

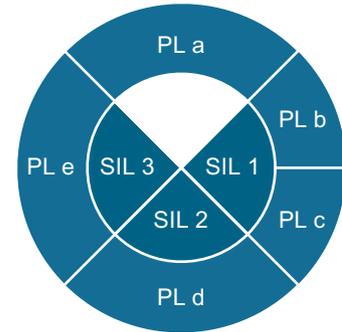
Funktionsweise

Das Sicherheitsschaltgerät 3SK2 überwacht das Not-Halt-Befehlsgerät. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet das Sicherheitsschaltgerät über die Geräteverbinder die fehlersicheren Motorstarter ab. Die Motorstarter schalten daraufhin die Last sicher ab. Ist das Not-Halt-Befehlsgerät entriegelt, kann durch den Starttaster wieder eingeschaltet werden.

Die Steuerung ist über das PROFINET Interfacemodul mit dem Sicherheitsschaltgerät verbunden. Im Anwenderprogramm der Steuerung wird das betriebliche Schalten der Motorstarter realisiert und über PROFINET an das 3SK2 übermittelt. Das 3SK2 leitet diese Steuersignale über seine Ausgänge (F-DQ oder QM) an die Steuereingänge der Motorstarter (IN1 bei Direktstarter bzw. IN1 und IN2 bei Wendestarter) weiter.

Die Rückmeldung, in welchem Zustand die Sicherheitsfunktion sich aktuell befindet, wird über PROFINET vom 3SK2 an die Steuerung geschickt. Es ist möglich den Starttaster für das Wiedereinschalten, anstatt direkt am 3SK2, auch über Eingangsbaugruppen der Steuerung einzulesen und das Signal ebenfalls über PROFINET an das Sicherheitsschaltgerät zu übertragen.

Zudem kann über das PROFINET Interfacemodul ein Fernreset der Motorstarter durch die Steuerung angestoßen werden um beispielsweise einen Fehler eines oder mehrerer Motorstarter zu beheben. Hierbei werden die Motorstarter über die Geräteverbinder abgeschaltet und anschließend wieder eingeschaltet. So können auf einfache Weise Sammelfehler des 3RM1 quittiert werden, ohne den Reset-Taster am Gerät betätigen zu müssen. Das Abschaltsignal muss hierbei länger als eine 1s anliegen. Bitte beachten Sie, dass nur Sammelfehler quittiert werden können. Gerätefehler oder ein Auslösen des Motor- oder Relaischutzes bedingt eine Quittierung mittels Reset-Taster am Gerät. Weitere Hinweise finden Sie im 3RM1 Gerätehandbuch (<https://support.industry.siemens.com/cs/ww/de/view/66295730>).



Hinweis

In diesem Beispiel wird davon ausgegangen, dass die Gefährdung nur von jeweils einem der Antriebe ausgeht, jedoch beim Not-Halt eine Gruppe von Antrieben abgeschaltet wird.

Aus diesem Grund wird in der Sicherheitsbewertung nur ein einzelner Motorstarter betrachtet und dies exemplarisch verwendet. Besteht die Gefährdung durch die Bewegung mehrerer Antriebe,

so müssen in der Sicherheitsbewertung alle Motorstarter berücksichtigt werden, die an dieser Gefahr beteiligt sind.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitschaltgerät mit PROFINET-Interfacemodul	Motorstarter Failsafe
		
<p>3SU1 (http://www.siemens.de/sirius-act)</p>	<p>3SK2 (http://www.siemens.de/safety-relays)</p>	<p>3RM1 (http://www.siemens.de/motorstarter/3rm1)</p>

Siehe auch

Schaltplan, Safety Evaluation, TIA Portal- und 3SK2-Projekt (<http://support.automation.siemens.com/WW/view/de/109769503>)

3.2.20 Not-Halt-Abschaltung bis SIL3 bzw. PL e mit einem Sanftstarter 3RW55 Failsafe und Sicherheitsschaltgerät 3SK1

Anwendung

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und durch ein Sicherheitsschaltgerät 3SK1 überwacht. Sowohl das betriebsmäßige Schalten mit Sanftan- und auslauf als auch die sichere Abschaltung erfolgen durch den Sanftstarter 3RW55 Failsafe.

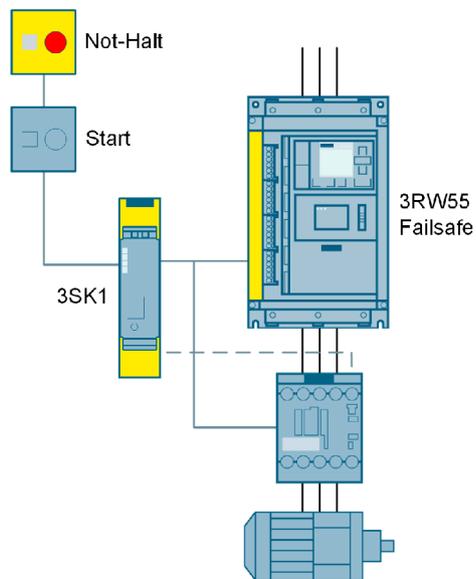


Bild 3-20 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit einem Sanftstarter 3RW55 Failsafe und Sicherheitsschaltgerät 3SK1

Funktionsweise

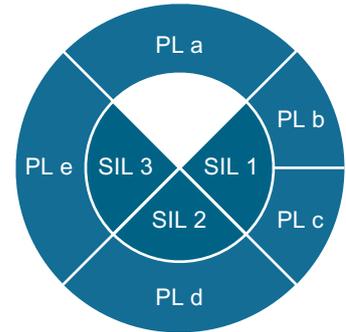
Das Sicherheitsschaltgerät 3SK1 überwacht das Not-Halt-Befehlsgerät. Bei Betätigen des Not-Halt-Befehlsgeräts öffnet das Sicherheitsschaltgerät die Freigabekreise und den Sanftstarter 3RW55 Failsafe über dessen STO-Eingang (F-DI) sowie das nachgeschaltete Leistungsschütz sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt, der Rückführkreis des Leistungsschützes geschlossen und meldet der Sanftstarter seinen fehlerfreien Zustand über dessen Ausgang F-RQ, kann durch den Starttaster wieder eingeschaltet werden.

In Verbindung mit einem zusätzlichen, redundanten Motorschütz, das zwischen Sanftstarter 3RW55 Failsafe und Motor geschaltet wird, können mit dem 3RW55 Failsafe zweikanalige Safe Torque Off (STO) Applikationen bis SIL 3 bzw. PL e realisiert werden (zweikanalige Abschaltung mit Verwendung des Sanftstarters 3RW55 Failsafe in einem der beiden Kanäle).

Die Überwachung des sicheren Meldeausgangs F-RQ (Klemme 41/42) des 3RW55 Failsafe und der Hilfskontakte des Schützes erfolgt durch ein übergeordnetes Sicherheitsschaltgerät 3SK1. Die Überwachung kann außerdem alternativ von einer fehlersicheren Steuerung übernommen werden. In diesem Beispiel kommen die Steuerbefehle am fehlersicheren Eingang F-DI des 3RW55 Failsafe und am Schütz von zwei sicheren Ausgängen des übergeordneten Sicherheitsschaltgeräts.

Da bei Applikationen bis SIL 3 bzw. PL e der sichere Meldeausgang F-RQ überwacht werden muss, kann aus dem Portfolio der Sicherheitsschaltgeräte 3SK1 nur die Variante „3SK1 Advanced“ – mit integriertem Kaskadiereingang INK – eingesetzt werden.

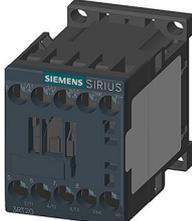
Ist die Steuerquelle des 3RW55 Failsafe auf EIN, wird nach einer STO Anforderung am 3SK1 mit Freigabe des F-DI Signals über den Start-Taster am 3SK1 automatisch auch gleich wieder der Motor über den 3RW55 Failsafe gestartet, ohne dass eine weitere Freigabeaktion über eine Steuerquelle am 3RW55 Failsafe erforderlich ist. Mögliche Steuerquellen, ein Beispiel ohne Kopplung des Digitaleingangs DI mit dem fehlersicheren Digitaleingang F-DI sowie detaillierte Informationen zum Sanftstarter 3RW55 Failsafe sind dem Handbuch (<https://support.industry.siemens.com/cs/de/de/view/109753752>) zu entnehmen.



Hinweis

Für die Diagnose ist es zwingend erforderlich, dass der 3RW55 Failsafe immer direkt an der Hauptspannung angeschlossen wird. Zusätzliche Schaltglieder, wiez.B. ein redundantes Schütz, dürfen erst hinter dem 3RW55 Failsafe in Reihengeschaltet werden.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sanftstarter Failsafe	Schütz
		
3SU1 (http://www.siemens.de/sirius-act)	3RW55 (http://www.siemens.de/sanftstarter)	3RT20 (http://www.siemens.de/sirius-control)

Siehe auch:

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109780386>)

Ausführlicher FAQ zum Thema: 3RW Sanftstarter: Sicheres Abschalten nach IEC 62061 (SIL) bzw. ISO 13849-1 (PL) (<https://support.industry.siemens.com/cs/WW/de/view/67474130>)

3.2.21 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit Koppelrelais 3RQ1 und fehlersicherer Steuerung

Anwendung

Zweikanalige Not-Halt-Abschaltung eines Motors durch eine fehlersichere Steuerung, einem zwangsgeführten Koppelrelais 3RQ1 und einem Leistungsschütze 3RT2.

Aufbau

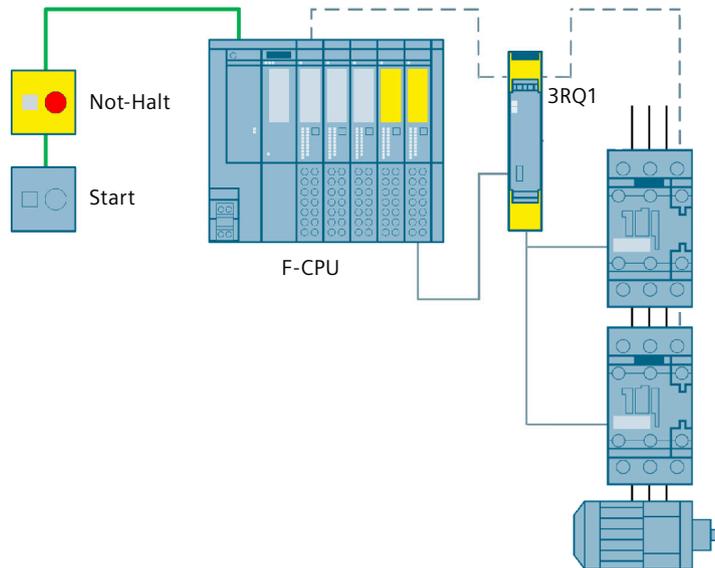


Bild 3-21 Not-Halt-Abschaltung bis SIL 3 bzw. PL e mit Koppelrelais 3RQ1 und fehlersicherer Steuerung

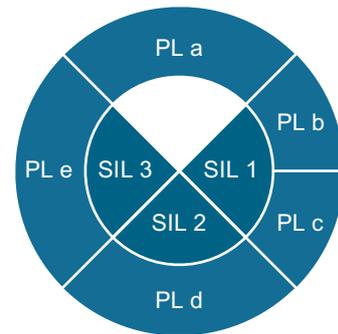
Funktionsweise

Die fehlersichere Steuerung überwacht das Not-Halt-Befehlsgerät zweikanalig. Bei Betätigen des Not-Halt-Befehlsgeräts schaltet die fehlersichere Steuerung das Koppelrelais sicherheitsgerichtet ab. Dieses wiederum schaltet über seine zwangsgeführten Kontakte die Leistungsschütz sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Eine direkte Anschaltung eines Schützes der Baugröße S2 (Leistung > 18,5 kW) ist mit den Halbleiterausgängen der F-DQ-Baugruppe (z.B. ET 200SP F-DQ 8x 24VDC/0.5A PP) aufgrund der zu hohen Halteleistung nicht möglich. In diesem Beispiel wird gezeigt, wie dieses Problem durch die Nutzung eines Koppelrelais 3RQ1 umgangen werden kann. Die Kombination aus der hier verwendeten Variante des Koppelrelais 3RQ12 und Schütz ist bis SIL 3 bzw. PL e ausgelegt.

Für Anwendungen mit geringeren Anforderungen an die funktionale Sicherheit bieten sich auch die zwangsgeführten Koppelrelais 3RQ10 an. Diese können in fehlersicheren Applikationen bis SIL 2 bzw. PL c eingesetzt werden. Um dieses Sicherheitslevel zu erreichen muss allerdings zusätzlich auf eine entsprechende Auslegung des Schützes geachtet werden (z.B. redundanter Aufbau).

Das Koppelrelais 3RQ1 eignet sich ebenfalls zur Kontakterweiterung einer fehlersicheren Steuerung. Hierdurch können die Ausgänge der fehlersicheren Steuerung vervielfacht bzw. deren Schaltvermögen erweitert werden.



Sicherheitsgerichtete Komponenten

SIRIUS ACT PROFINET Interfacemodul	Steuerung Failsafe	Koppelrelais	Schütz
			
3SU1 (http://www.siemens.de/sirius-act)	S7 F-PLC (http://www.siemens.de/simatic-safety)	3RQ1 (http://www.siemens.de/relais)	3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, TIA Portal-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109769502>)

Ausführlicher FAQ zum Thema: Kontakterweiterung einer fehlersicheren Steuerung mit 3SK1 und 3RQ1 (<https://support.industry.siemens.com/cs/de/de/view/76676971>)

3.3 Schutztürüberwachung

3.3.1 Einleitung

Dieses Kapitel beschreibt Applikationen mit trennenden Schutzeinrichtungen in Form einer Schutztür. Die am häufigsten eingesetzte Lösung im Bereich von Anlagen und Maschinen ist die Absicherung von Gefahrenbereichen mit mechanisch trennenden Schutzeinrichtungen oder Zugangsklappen. Hier gilt es das unbefugte Betreten von Anlagenbereichen zu überwachen, sowie eine Gefahr bringende Maschinenfunktion zu verhindern, wenn die Schutzeinrichtung nicht geschlossen ist. Die Überwachung der Schutzeinrichtung kann sowohl mit mechanischen Positions- bzw. Sicherheitsschaltern erfolgen, als auch mit berührungslosen Sicherheitsschaltern auf magnetischer oder RFID-Basis.

Häufig wird im Zusammenhang eine Schutztürüberwachung auch eine Zuhaltung der Schutztür realisiert. Verriegelungseinrichtungen mit Zuhaltung dienen dazu, Gefahrenbereiche vor ungewolltem Betreten zu sichern. Das hat meistens zwei Gründe:

1. Zum Schutz des Menschen vor nachlaufenden gefährlichen Maschinenbewegungen, hohen Temperaturen etc. Hier gibt die ISO 14119 Leitsätze zur Gestaltung und Auswahl von Verriegelungseinrichtungen. In dieser Norm wird gefordert, dass erst nach dem Stoppen der gefährlichen Maschinenbewegung der Gefahrenbereich zugänglich sein darf.
2. Eine Zuhaltung kann aus Gründen der Prozesssicherheit sinnvoll sein. Dieser Fall tritt ein, wenn die Gefahr nach dem Öffnen der Schutzeinrichtung gestoppt wird, aber dadurch Schäden an der Maschine oder dem Werkstück entstehen können. Hier wird erst die Maschine in eine geordnete Halteposition gefahren, bevor der Zugang frei gegeben wird.

3.3.2 Begriffe aus der Norm

Die ISO 14119 "Leitsätze zur Gestaltung und Auswahl von Verriegelungseinrichtungen" definiert verschiedene Bauarten von Verriegelungseinrichtungen. Diese unterscheiden sich im Wesentlichen durch ihr Betätigungsprinzip und damit auch in ihrer Kodierung, um ein einfaches Umgehen zu verhindern.

Die Eigenschaften der Bauarten 1 bis 4 entnehmen Sie der folgenden Tabelle:

Bauart	Betätigungsprinzip		Beispiele für Betätiger	
Bauart 1	mechanisch	Kontakt, Kraft	unkodiert	Kurvenscheibe
				lineare Nocken
				Scharnier
Bauart 2			kodiert	Zunge (geformter Betätiger)
				Schlüsseltransfersystem

Bauart	Betätigungsprinzip		Beispiele für Betätiger	
Bauart 3	berührungslos	induktiv	unkodiert	geeignetes Eisenmetall
		magnetisch		Magnet, Elektromagnet
		kapazitiv		jedes geeignete Objekt
		Ultraschall		
		optisch		
Bauart 4		magnetisch	kodiert	kodierter Magnet
		RFID		kodierter RFID-Transponder
		optisch		optisch kodierter Transponder

Manipulationsschutz:

Ein weiterer wesentlicher Aspekt aus der Norm ist der Manipulationsschutz. Jede Maschine muss so gestaltet sein, dass Anreize zum Umgehen der Verriegelungseinrichtung auf ein Minimum herabgesetzt werden. Die Norm beschreibt in Kapitel 7 einen Ablauf, wie dieses Ziel erreichbar ist.

1. Anwendung grundlegender Maßnahmen zur Anordnung und Befestigung
2. Überprüfung, ob Anreiz zur Umgehung besteht (Leitfaden zur Beurteilung in Anhang H der Norm)
3. Minimierung der Anreize durch konstruktive Maßnahmen/Betriebsarten
4. Falls weiterhin Anreiz besteht → zusätzliche Maßnahmen erforderlich

Die zusätzlichen Maßnahmen zur Anreizminimierung sind ebenfalls in der Norm aufgeführt:

Verhindern der Zugänglichkeit zu den Elementen der Verriegelungseinrichtung:

1. Anbringen außer Reichweite
2. Hindernisse oder Abschirmung
3. Anbringung an verdeckter Position

Verhindern einer Ersatzbetätigung der Verriegelungseinrichtung durch leicht verfügbare Gegenstände:

1. Kodierter Betätiger mit geringer Kodierungsstufe (1-9 Kodierstufen)
2. Kodierter Betätiger mit mittlerer Kodierungsstufe (10-1000 Kodierstufen)
3. Kodierter Betätiger mit hoher Kodierungsstufe (>1000 Kodierstufen)

Verhindern der Demontage oder Lageänderung von Elementen der Verriegelungseinrichtung durch nicht lösbare Befestigungen (z. B. Schweißen, Kleben, Einwegschrauben, Nieten).

Verhindern eines Umgehens:

1. Integration einer Umgehungsüberwachung in die Steuerung durch:
 - Zustandsüberwachung
 - Periodische Prüfungen
2. Plausibilitätsprüfung mithilfe einer zusätzlichen Verriegelungseinrichtung, wobei ein Umgehen nur durch eine zusätzliche Handlung möglich ist

Maßnahmen:

Welche Maßnahmen in Abhängigkeit der Bauart der Verriegelungseinrichtung Sie verwenden können bzw. müssen, entnehmen Sie der folgenden Tabelle:

Grundsätze und Maßnahmen	Bauart 1 (ohne Scharnier) und Bauart 3	Bauart 1 (Scharnier)	Bauart 2 und Bauart 4 (geringe oder mittlere Kodierstufe)	Bauart 2 und Bauart 4 (hohe Kodierstufe)
Anbringen außer Reichweite	①		①	
Hindernis/ Abschirmung				
Anbringen in verdeckter Position				
Zustandsüberwachung oder periodische Prüfung				
Nicht-lösbare Befestigung des Positionsschalter und Betätigers				
Nicht-lösbare Befestigung des Positionsschalters		②		
Nicht-lösbare Befestigung des Betätigers			②	②
Zusätzliche Verriegelungseinrichtung und Plausibilitätsprüfung	③		③	

- ① Mindestens eine dieser Maßnahme ist anzuwenden
- ② Anzuwendende Maßnahme
- ③ Empfohlene Maßnahme (zusätzlich)

Positionsschalter

Die Positionsschalter werden normalerweise als zwangsbetätigter Schalter an Schutztüren eingesetzt. Wird die Schutztür geöffnet, so wird der Positionsschalter betätigt und der Schalter wird zuverlässig geöffnet (siehe Grundbegriffe: Zwangsöffnung (Seite 13)). Positionsschalter entsprechen einer Bauart 1 der ISO 14119 und sind unkodiert.

Mechanische Sicherheitsschalter (mit getrenntem Betätiger)

Im Gegensatz zu den Positionsschaltern können Sicherheitsschalter nicht einfach überlistet werden. Der Sicherheitsschalter lässt sich nur mit dem zugehörigen codierten Betätiger schalten. Sicherheitsschalter entsprechen einer Bauart 2 der ISO 14119 und sind kodiert.

Mechanische Sicherheitsschalter (Scharnierschalter)

Die Scharnierschalter werden dort eingesetzt, wo aus Sicherheitsgründen die Stellung von schwenkbaren Schutzeinrichtungen wie Türen und Klappen überwacht werden müssen. Scharnierschalter entsprechen einer Bauart 1 der ISO 14119 und sind unkodiert.

Mechanische Sicherheitsschalter (mit Zuhaltung)

Die Sicherheitsschalter mit Zuhaltung sind besondere sicherheitstechnische Geräte, die ein zufälliges oder absichtliches Öffnen von Schutztüren, Schutzgittern oder anderen Abdeckungen verhindert, solange noch ein gefährlicher Zustand besteht. (z. B. Nachlauf der Maschine). Unabhängig von der Zuhaltung wird auch eine Positionserfassung mithilfe eines getrennten Betätigers durch diese Art von Schaltern ausgeführt. Sicherheitsschalter entsprechen einer Bauart 2 der ISO 14119 und sind kodiert.

Berührungslose Sicherheitsschalter (Magnetschalter)

Magnetschalter bestehen aus einem codierten Schaltmagnet und einem Schaltelement. Sie sind zum Anbau an bewegliche Schutzeinrichtungen vorgesehen und sind durch ihre geschlossene Bauform besonders geeignet für Bereiche, die durch hohe Verschmutzung, Reinigungs- oder Desinfektionsmittel belastet sind. Sicherheitsmagnetschalter entsprechen einer Bauart 4 der ISO 14119 sind kodiert.

Berührungslose Sicherheitsschalter (RFID)

Die RFID-Sicherheitsschalter bestehen aus einem codierten RFID-Schalter und einem baugleichen RFID-Betätiger und sind vielfältig einsetzbar, besonders für Bereiche mit extremen Umweltbedingungen. Dank des elektronischen Wirkprinzips sind die Schalter auch ideal für Metall verarbeitende Maschinen. Die Schalter haben einen größeren Schaltabstand gegenüber mechanischen Schaltern und bieten eine bessere Montagetoleranz sowie umfangreiche Diagnosemöglichkeiten. Sie bieten außerdem einen maximalen Manipulationsschutz durch individuelle Codierung von Schalter und Betätiger. RFID-Sicherheitsschalter entsprechen einer Bauart 4 der ISO 14119 und sind hoch kodiert.

Typische Anwendung

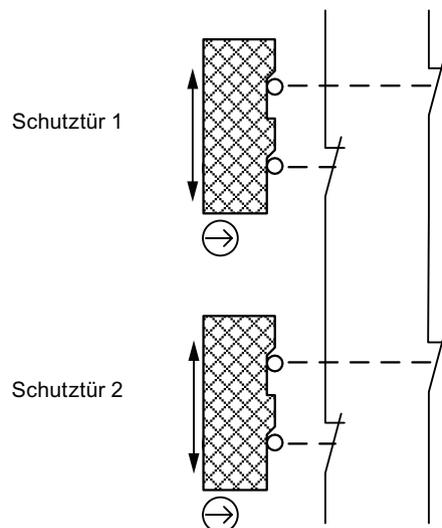
Die Schutztür wird mit SIRIUS Positionsschaltern mit zwangsöffnenden Kontakten durch ein Auswertegerät überwacht. Wird diese Schutztür geöffnet, schaltet das Auswertegerät über sichere Ausgänge die nachgeschalteten Aktoren gemäß Stoppkategorie 0 nach EN 60204-1 ab. Wird die Schutztür geschlossen, erfolgt beim automatischen Start nach Überprüfung der Positionsschalter und der nachgeschalteten Aktoren das Wiedereinschalten. Beim manuellen Start geschieht dies erst nach Betätigen des Starttasters.

Hinweis

- Ordnen Sie Positionsschalter so an, dass die Positionsschalter beim An- und Überfahren nicht beschädigt werden. Deshalb dürfen Sie Positionsschalter nicht als mechanischen Anschlag verwenden.
- Verlegen Sie Sensorleitungen geschützt; verwenden Sie als Sensoren ausschließlich Sicherheitssensoren mit zwangsöffnenden Kontakten.
- Die Zuhaltung stellt eine einzelne, separate Sicherheitsfunktion neben der Sicherheitsfunktion der Überwachung der Schutztür mittels Positionsschalter dar. Die Ansteuerung kann eine geforderte Sicherheitsintegrität haben, die um eine Stufe niedriger ist, als die Risikobewertung für die Überwachung der Schutztür ergeben hat. (Begründung: Die Wahrscheinlichkeit, dass beide Sicherheitsfunktionen zum gleichen Zeitpunkt versagen, kann quasi ausgeschlossen werden.
Beispiel: Die Schutztürüberwachung wird in PL d bzw. SIL 2 gefordert, die Ansteuerung der Zuhaltung kann in PL c bzw. SIL 1 realisiert werden.

Bedingungen bei Reihenschaltung

Eine Reihenschaltung von Positionsschaltern kann bis zu PLd (nach ISO 13849-1) bzw. bis zu SIL 2 (nach IEC 62061) eingesetzt werden. Das erreichbare Sicherheitslevel ist abhängig von der möglichen Fehlerdiagnose, der Anzahl verwendeter Türen und der Häufigkeit der Türbetätigungen. Eine Abschätzung der erreichbaren Diagnose und damit des Sicherheitslevel kann dem Technischen Report ISO /TR 24119 entnommen werden. Eine Reihenschaltung in PL e (nach ISO 13849-1) bzw. SIL 3 (nach IEC62061) ist nicht möglich.



Mögliche Kombination zur Positionserfassung und erreichbare Sicherheitslevel

Die Applikationsbeispiele in diesem Kapitel können nur einen Bruchteil der möglichen Kombination von Erfassungsgeräten zur Positionserfassung abdecken. Die nachfolgenden Tabellen zeigen auf einfache Art und Weise, welches Sicherheitslevel durch welche Art der Positionserfassung maximal erreichbar ist.

Tabelle 3-5 Sichere Positionsüberwachung mit mechanischen Schaltern

Auswertegeräte		Positionsschalter	Sicherheits-schalter Schar-nierschalter	Sicherheits-schalter mit ge-trenntem Betäti-ger	Sicherheits-schalter mit opti-onaler Zuhal-tungsfunktion
					
Erreichbarer Sicher-heitslevel mit EINEM Position-schalter	Überwachung eines Öffner-kontakts	SIL 1 / PL c	SIL 1 / PL c	SIL 1 / PL c	SIL 1 / PL c
	Überwachung von 2 Öffner-kontakten oder 1 Öffner- + 1 Schließer-Kon-takt	SIL 1 / PL c	SIL 2 / PL d	SIL 2 / PL d	SIL 2 / PL d
Erreichbarer Sicher-heitslevel mit ZWEI Positionsschaltern	Positionsschal-ter 	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e
	Sicherheits-schalter Schar-nierschalter 	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e
	Sicherheits-schalter mit ge-trenntem Betäti-ger 	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e
	Sicherheits-schalter mit opti-onaler Zuhal-tungsfunktion 	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e	SIL 3 / PL e

Beispiel 1:

Durch die Kombination zweier mechanischer Sicherheitsschalter (mit getrenntem Betätiger) kann ein Sicherheitslevel von bis zu PL e bzw. SIL 3 erreicht werden.

Beispiel 2:

Bei der Verwendung eines mechanischen Sicherheitsschalters (Scharnierschalter) kann ein Sicherheitslevel von bis zu PL d bzw. SIL 2 erreicht werden.

Tabelle 3-6 Sichere Schutztürzuhaltung

Sichere Auswertegeräte	Sicherheitsschalter	
	Sicherheitsschalter mit Zuhaltung	Sicherheitsschalter mit Zuhaltung
	 Sicherheitsschaltgerät 3SK2	 SIL 2 / PL d

Hinweis

Generell muss zur Verwendung dieser Positionsschalter eine zwangsläufige Betätigung durch die Konstruktion der Schutzeinrichtung sichergestellt werden. Nur unter dieser Bedingung sind die in der Tabelle genannten Werte zulässig.

Hinweis

Unter Berücksichtigung von gewissen Fehlerausschlüssen (z. B. Bruch des Betätigers), ist der Einsatz nur eines Scharnierschalters oder eines Schalters mit getrenntem Betätiger bis zu SIL 2 bzw. PL d, wie in der Tabelle beschrieben, möglich. Da der Maschinenhersteller den Beweis des Fehlerausschlusses erbringen muss, kann seitens des Komponentenherstellers keine endgültige Bewertung der getroffenen Maßnahmen erfolgen.

Weitere Informationen entnehmen Sie dem Schreiben unter folgendem Link: (<http://support.automation.siemens.com/WW/view/de/35443942>)

Hinweis

Bei einem zweikanaligen Aufbau mit elektromechanischen Sensoren kann SIL 3 bzw. PL e nur bei Versorgung der Sensoren durch die Auswerteeinheit erreicht werden. Nur dadurch ist eine ausreichende Diagnose möglich.

Tabelle 3-7 Sichere Positionsüberwachung mit berührungslosen Sicherheitsschaltern

Sichere Auswertegeräte	Erfassungsgeräte Berührungslose Sicherheitsschalter	
		Magnetschalter 3SE66/3SE67  1S + 1Ö; 2Ö
 Sicherheitsschaltgerät 3SK	SIL 3 / PL e*	SIL 3 / PL e

* Mit den Sicherheitsschaltgeräten 3SK1111 und 3SK1112 (3SK1 Standard) ist eine Auswertung von 1 NO + 1 NC nicht möglich. Hierfür müssen 3SK112 (3SK1 Advanced) verwendet werden.

Hinweis

Die erreichbaren Sicherheitslevels hängen auch von der Art des verwendeten Sicherheits-Auswertegeräts ab (insbesondere dessen Diagnosefähigkeit).

Hinweis

Bei der Verwendung von Magnetschaltern kann es bedingt durch kapazitive Effekte zum Verschweißen der Magnetkontakte kommen. Der Grund dafür ist, dass beim Schalten dieser Lasten (z. B. auch Kabelkapazitäten) ein hoher Spitzenstrom auftreten kann. Es ist eine entsprechende Absicherung mit dem Nennstrom des Magnetschalters vorzusehen, wenn die Geräte- / Sensorkombinationen nicht explizit freigegeben sind. Weitere Details entnehmen Sie bitte der Dokumentation des Magnetschalters.

Siehe auch:

Erreichbare Sicherheitslevel unter Einsatz nur eines SIRIUS Positionsschalter mit oder ohne Zuhaltung (<http://support.automation.siemens.com/WW/view/de/35443942>)

3.3.3 Schutztürüberwachung bis SIL 1 bzw. PL c mit einem Sicherheitsschaltgerät 3SK1

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet.

Aufbau

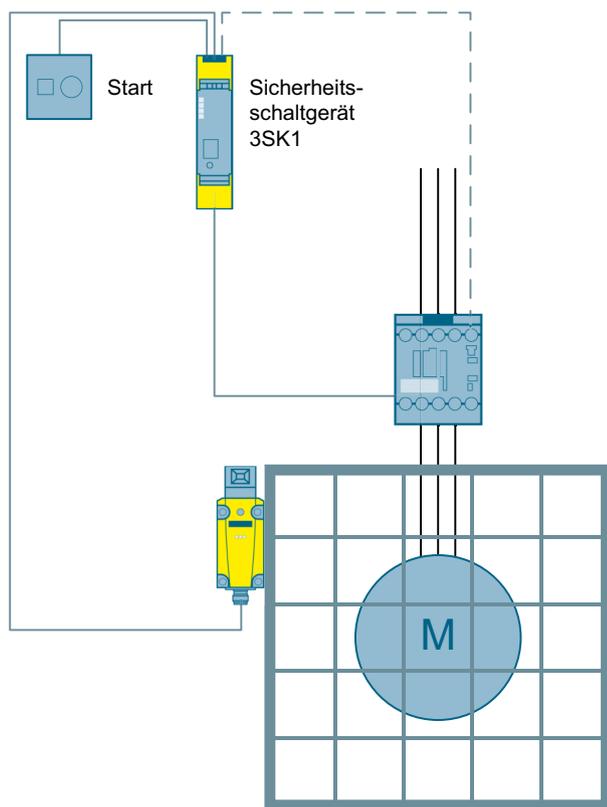
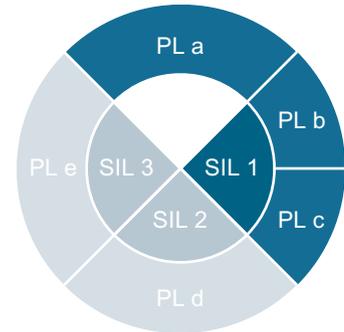


Bild 3-22 Schutztürüberwachung bis SIL 1 bzw. PL c mit einem Sicherheitsschaltgerät 3SK1

Funktionsweise

Über den Kontakt des Sicherheitsschalters wird die Stellung einer Schutztür überwacht. Beim Öffnen der überwachten Tür löst das Sicherheitsschaltgerät aus und öffnet die Freigabekreise, wodurch das Leistungsschütz sicherheitsgerichtet abgeschaltet wird. Ist die Tür geschlossen und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Sicherheitsschalter	Sicherheitsschaltgerät	Schütz
		
3SE5 (http://www.siemens.de/sirius-erfassen)	3SK1 (http://www.siemens.de/safety-relays)	3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/73135973>)

3.3.4 Schutztürüberwachung bis SIL 1 bzw. PL c mit einem Sicherheitsschaltgerät 3SK2

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet.

Aufbau

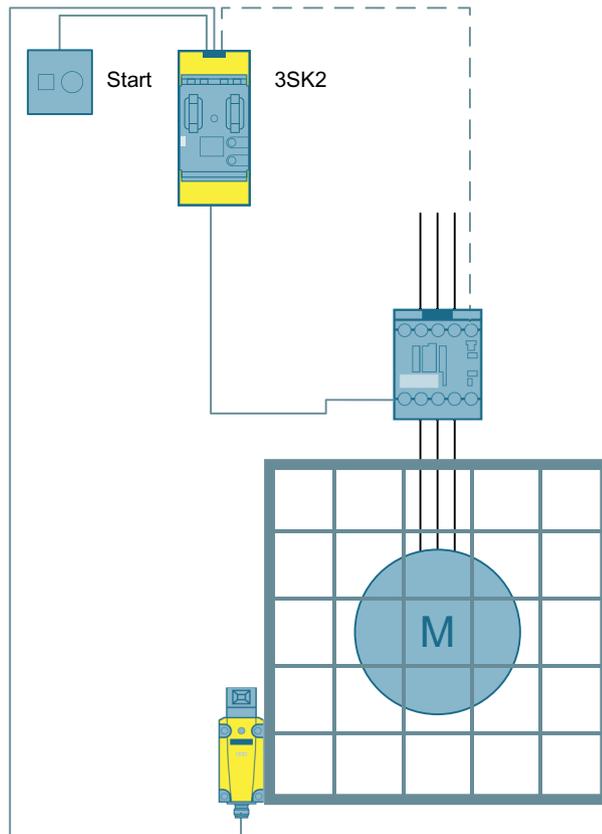
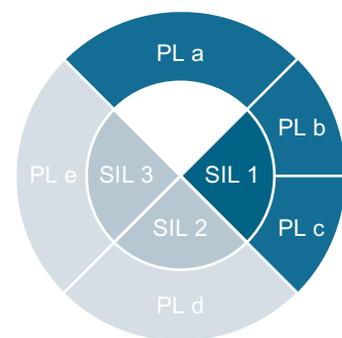


Bild 3-23 Schutztürüberwachung bis SIL 1 bzw. PL c mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Über den Kontakt des Sicherheitsschalters wird die Stellung einer Schutztür überwacht. Beim Öffnen der überwachten Tür löst das Sicherheitsschaltgerät aus und öffnet die Freigabekreise, wodurch das Leistungsschütz sicherheitsgerichtet abgeschaltet wird. Ist die Tür geschlossen und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Sicherheitsschalter	Modulares Sicherheitssystem	Schütz
		
3SE5 (http://www.siemens.de/sirius-erfassen)	3SK2 (http://www.siemens.de/safety-relays)	3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109485644>)

3.3.5 Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet.

Aufbau

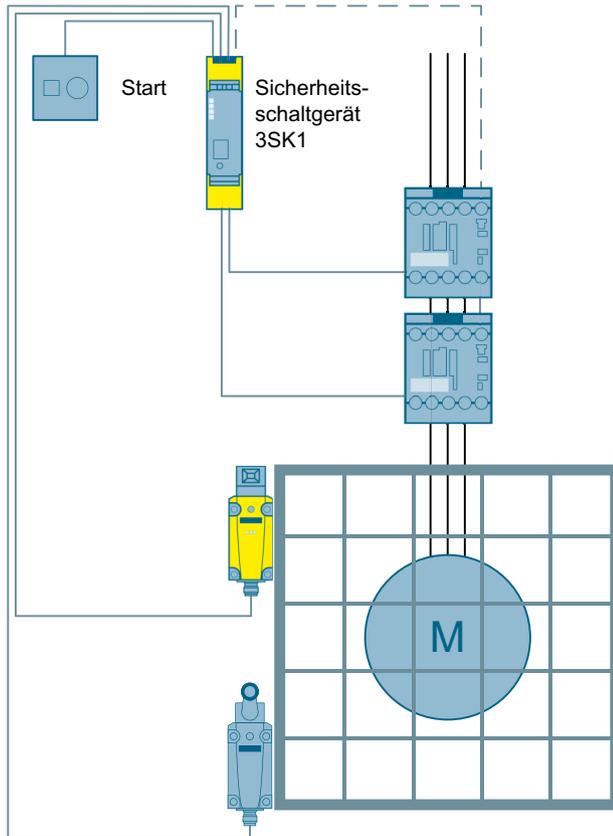
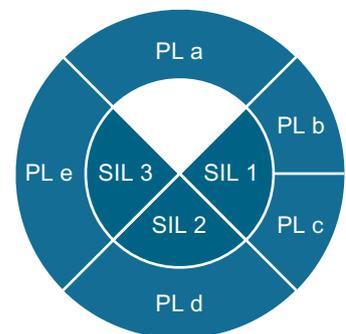


Bild 3-24 Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Funktionsweise

Über zwei Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Beim Öffnen der überwachten Tür löst das Sicherheitsschaltgerät aus und öffnet die Freigabe- und Rückführkreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist die Tür geschlossen und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Positionsschalter		Sicherheitschaltgerät	Schütz
			
2x 3SE5 (http://www.siemens.de/sirius-erfassen)		3SK1 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/73135309>)

3.3.6 Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitschaltgerät 3SK2

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet.

Aufbau

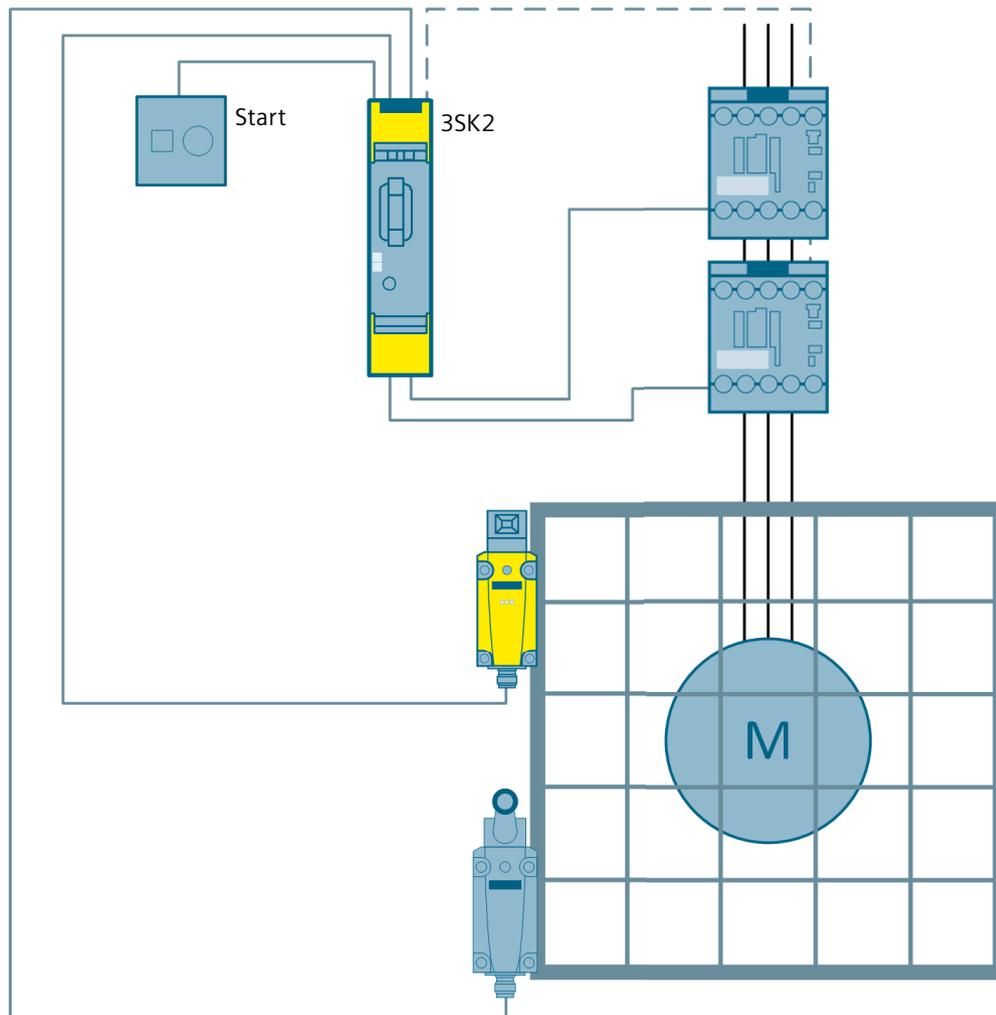
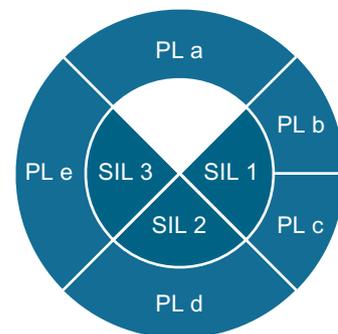


Bild 3-25 Schutztürüberwachung bis SIL 3 bzw. PL e mit fehlersicheren Motorstarter und einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Über zwei Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Beim Öffnen der überwachten Tür löst das Sicherheitsschaltgerät aus und öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist die Tür geschlossen und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Positionsschalter		Sicherheitsschaltgerät	Schütz
			
2x 3SE5 (http://www.siemens.de/sirius-erfassen)		3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109479275>)

3.3.7 Schutztürüberwachung bis SIL 3 bzw. PL e mit einem fehlersicheren Motorstarter und einem Sicherheitsschaltgerät 3SK1

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet.

Aufbau

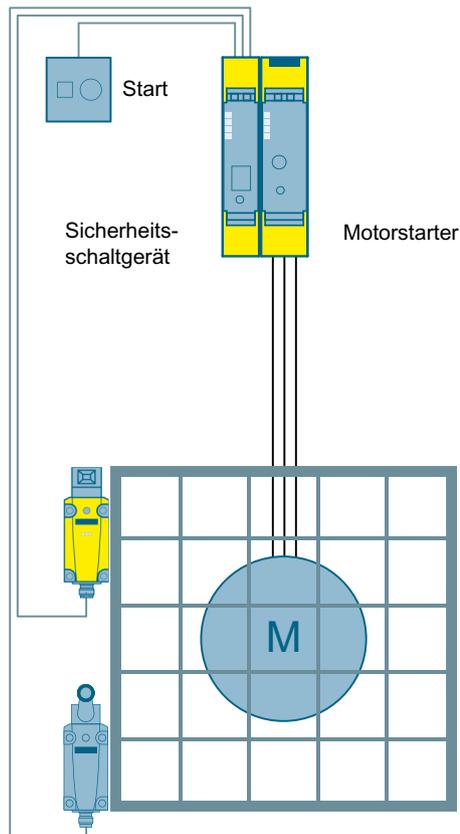
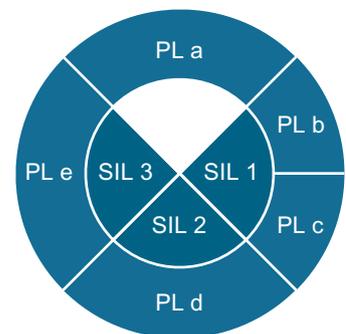


Bild 3-26 Schutztürüberwachung bis SIL 3 bzw. PL e mit einem fehlersicheren Motorstarter und einem Sicherheitsschaltgerät 3SK1

Funktionsweise

Über den Kontakt des Sicherheitsschalters wird die Stellung einer Schutztür überwacht. Beim Öffnen der überwachten Tür löst das Sicherheitsschaltgerät aus und schaltet über den Geräteverbinder den fehlersicheren Motorstarter ab. Der Motorstarter schaltet daraufhin die Last sicher ab. Ist die Tür geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Sicherheitsschalter		Sicherheitsschaltgerät	Motorstarter Failsafe
			
2x 3SE5 (http://www.siemens.de/sirius-erfassen)		3SK1 (http://www.siemens.de/safety-relays)	3RM1 (http://www.siemens.de/motorstarter/3rm1)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/88822953>)

Ausführlicher FAQ zum Thema: Sicheres Abschalten mit den Motorstartern 3RM1 (<http://support.automation.siemens.com/WW/view/de/67478946>)

3.3.8 Schutztürüberwachung bis SIL 3 bzw. PL e mit fehlersicheren Motorstarter und einem Sicherheitsschaltgerät 3SK2

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet.

Aufbau

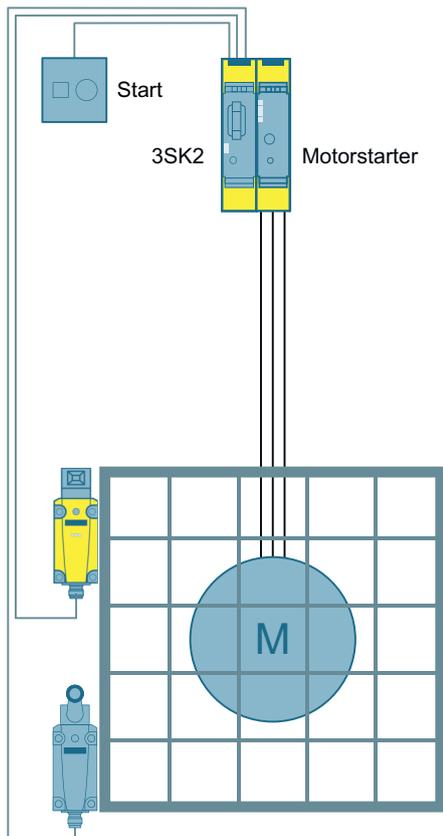
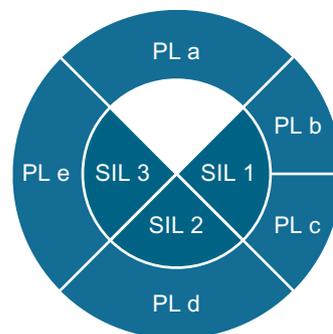


Bild 3-27 Schutztürüberwachung bis SIL 3 bzw. PL e mit fehlersicheren Motorstarter und einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Über den Kontakt des Sicherheitsschalters wird die Stellung einer Schutztür überwacht. Beim Öffnen der überwachten Tür löst das Sicherheitsschaltgerät aus und schaltet über den Geräteverbinder den fehlersicheren Motorstarter ab. Der Motorstarter schaltet daraufhin die Last sicher ab. Ist die Tür geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Sicherheitsschalter		Sicherheitsschaltgerät	Motorstarter Failsafe
			
2x 3SE5 (http://www.siemens.de/sirius-erfassen)		3SK2 (http://www.siemens.de/safety-relays)	3RM1 (http://www.siemens.de/motorstarter/3rm1)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109485645>)

Ausführlicher FAQ zum Thema: Sicheres Abschalten mit den Motorstartern 3RM1 (<http://support.automation.siemens.com/WW/view/de/67478946>)

3.3.9 Schutztürüberwachung über AS-i bis SIL 3 bzw. PL e mit einem Modularen Sicherheitssystem

Anwendung

Überwachung mehrerer Schutztüren und Ansteuerung der Aktorik über AS-i mit einem Modularen Sicherheitssystem.

Aufbau

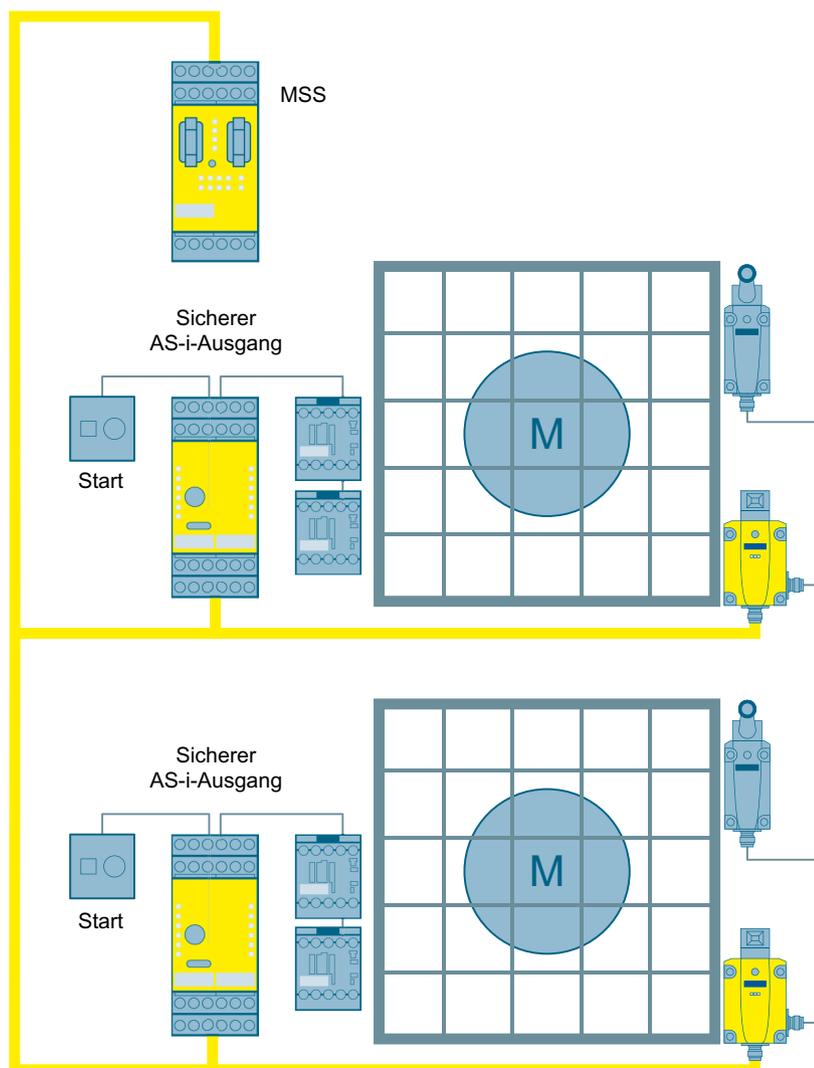
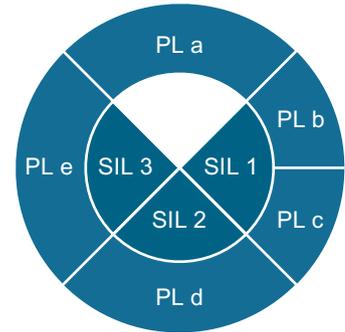


Bild 3-28 Schutztürüberwachung über AS-i bis SIL 3 bzw. PL e mit einem Modulare Sicherheitssystem

Funktionsweise

Das Modulare Sicherheitssystem überwacht die am AS-i angeschlossenen Sicherheitsschalter und sendet Statussignale in Form von simulierten AS-i Slaves über den AS-i Bus. Diese simulierten Slaves werden von den sicheren AS-i Ausgängen überwacht. Beim Öffnen einer der Schutztüren unterbricht das Modulare Sicherheitssystem das jeweilige Statussignal. Der sichere AS-i Ausgang öffnet daraufhin die Freigabekreise und die Leistungsschütze schalten sicherheitsgerichtet ab.

Die Signale vom Starttaster und den Hilfskontakten der Schütze werden vom sicheren AS-i Ausgang über den AS-i Bus an das Modulare Sicherheitssystem geschickt und dort ausgewertet. Ist die jeweilige Schutztür geschlossen und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Positionsschalter		Modulares Sicherheitssystem	Sicherer AS-i Ausgang	Schütz
				
2x 3SE5 (http://www.siemens.de/sirius-erfassen)		3RK3 (http://www.siemens.de/sirius-monitor)	3RK1405 (http://www.siemens.de/as-interface)	2x 3RT20 (http://www.siemens.de/sirius-control)

Hinweis

Zusätzlich zu den sicherheitsgerichteten Komponenten werden zum Betrieb eines AS-i-Netzwerks ein AS-i-Master sowie ein AS-i-Netzteil benötigt.

Siehe auch

Schaltplan, MSS-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/73135311>)

3.3.10 Schutztürüberwachung mittels RFID-Schalter bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet.

Aufbau

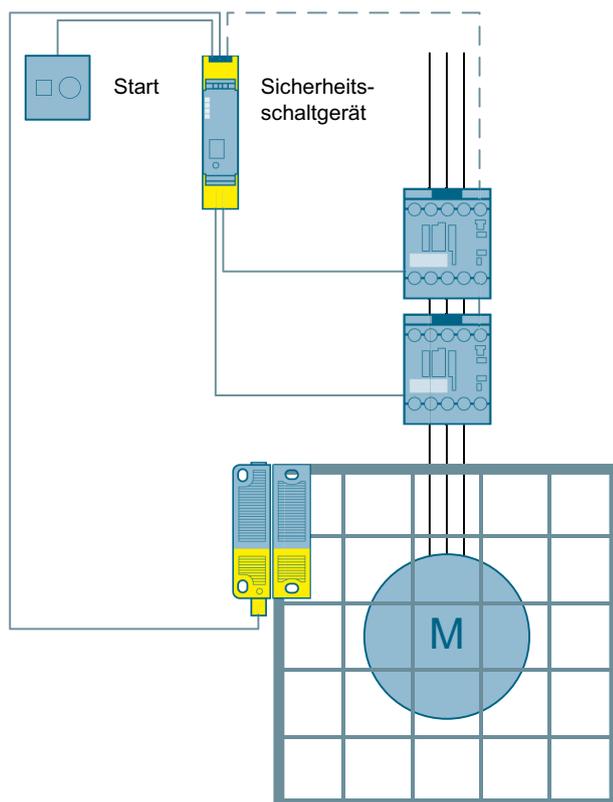


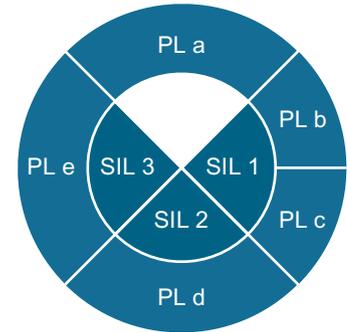
Bild 3-29 Schutztürüberwachung mittels RFID-Schalter bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Funktionsweise

Über den berührungslosen Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Beim Öffnen der überwachten Tür löst das Sicherheitsschaltgerät aus und öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist die Tür geschlossen und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Der berührungslose Sicherheitsschalter 3SE6315 ist intern zweikanalig aufgebaut und verfügt über eine eigene Diagnosefähigkeit. Deshalb und aufgrund seiner auf RFID-Technik basierenden, manipulationsfreien Beschaffenheit wird kein redundanter Sicherheitsschalter benötigt, um bis zu PL e nach ISO 13849-1 bzw. SIL 3 nach IEC 62061 zu erreichen.

Als Alternative zu den hier gezeigten RFID-Schaltern können auch die ebenfalls berührungslosen und bis PL e bzw. SIL 3 einsetzbaren Magnetschalter 3SE66 bzw. 3SE67 verwendet werden.



Sicherheitsgerichtete Komponenten

Berührungsloser Sicherheitsschalter	Sicherheitsschaltgerät	Schütz
		
3SE6315 (http://www.siemens.de/sirius-erfassen)	3SK1 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/73134150>)

3.3.11 Schutztürüberwachung mittels RFID-Schalter bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet.

Aufbau

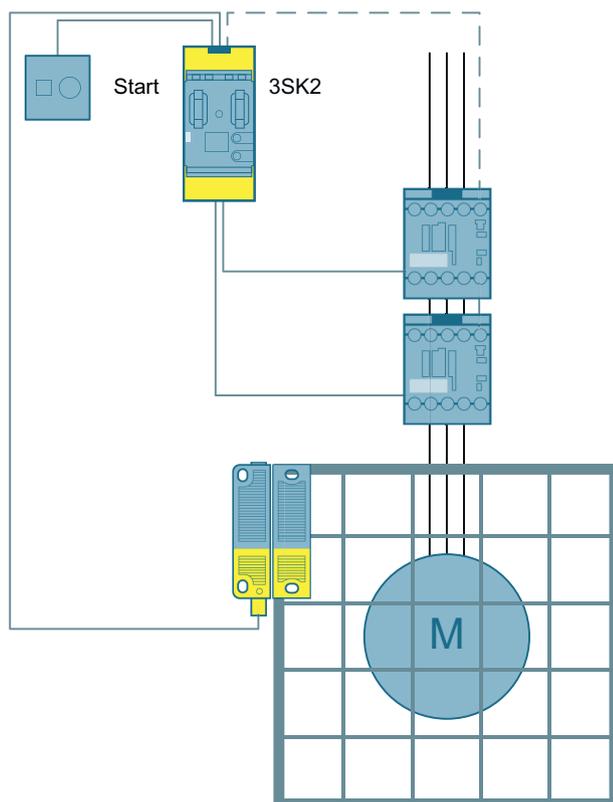


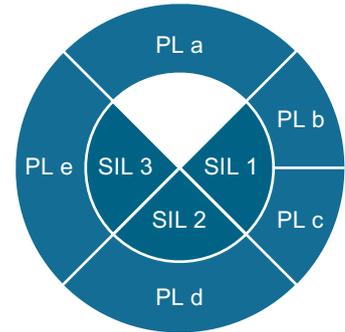
Bild 3-30 Schutztürüberwachung mittels RFID-Schalter bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Über den berührungslosen Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Beim Öffnen der überwachten Tür löst das Sicherheitsschaltgerät aus und öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist die Tür geschlossen und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Der berührungslose Sicherheitsschalter 3SE6315 ist intern zweikanalig aufgebaut und verfügt über eine eigene Diagnosefähigkeit. Deshalb und aufgrund seiner auf RFID-Technik basierenden, manipulationsfreien Beschaffenheit wird kein redundanter Sicherheitsschalter benötigt, um bis zu PL e nach ISO 13849-1 bzw. SIL 3 nach IEC 62061 zu erreichen.

Als Alternative zu den hier gezeigten RFID-Schaltern können auch die ebenfalls berührungslosen und bis PL e bzw. SIL 3 einsetzbaren Magnetschalter 3SE66 bzw. 3SE67 verwendet werden.



Sicherheitsgerichtete Komponenten

Berührungsloser Sicherheitsschalter	Sicherheitsschaltgerät	Schütz
		
3SE6315 (http://www.siemens.de/sirius-erfassen)	3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109485646>)

3.3.12 Schutztürüberwachung mit Zuhaltung bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät 3SK2

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet. Geht von der Maschine auch nach Abschaltung für eine gewisse Zeit noch eine Gefahr aus, kann der Zugang durch eine Zuhaltung solange verhindert werden.

Aufbau

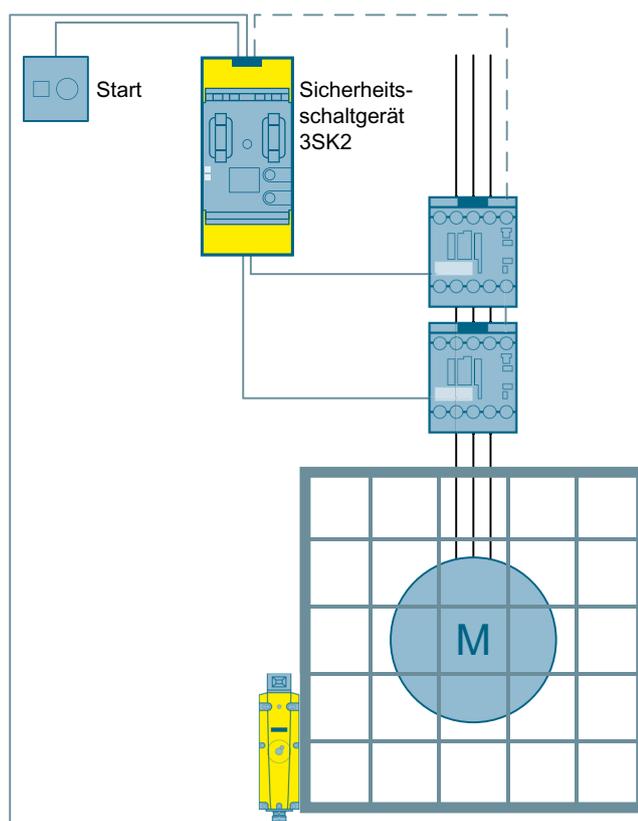
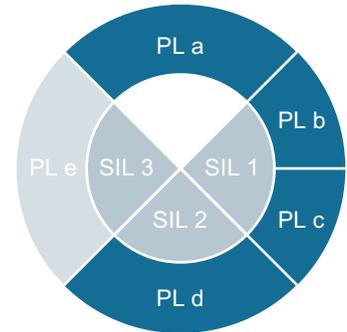


Bild 3-31 Schutztürüberwachung mit Zuhaltung bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Über einen Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Zusätzlich wird über den Sicherheitsschalter die Tür verriegelt. Wird der Befehl zum Entriegeln der Tür gegeben, löst das Sicherheitsschaltgerät aus und öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Nach Ablauf einer eingestellten Zeit wird die Zuhaltung entriegelt. Ist die Tür geschlossen und verriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sowohl die Sicherheitsfunktion „Schutztürüberwachung“ als auch die Sicherheitsfunktion "Schutztürzuhaltung" sind bis SIL 2 bzw. PL d ausgelegt.

Bei diesem Beispiel kommt ein Sicherheitsschalter mit Federkraftverriegelung zum Einsatz. Dies bedeutet, dass aktiv Spannung angelegt werden muss, um die Zuhaltung der Schutztür aufzuheben.

Im Gegensatz dazu stehen auch Sicherheitsschalter mit Magnetkraftverriegelung zur Verfügung, mit welchen sich allerdings für die Sicherheitsfunktion "Schutztürzuhaltung" kein SIL bzw. PL umsetzen lässt.

Unter Berücksichtigung von Fehlerausschlüssen ist der Einsatz von nur einem Sicherheitsschalter mit oder ohne Zuhaltung bis SIL 2 bzw. PL d zulässig. Weitere Informationen entnehmen Sie dem unten aufgeführten Schreiben.

Sicherheitsgerichtete Komponenten

Sicherheitsschalter mit Zuhaltung	Sicherheitsschaltgerät	Schütz
		
3SE5 (http://www.siemens.de/sirius-erfassen)	3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109479276>)

Schreiben zum Einsatz von Sicherheitsschaltern bis SIL 2 bzw. PL d (<http://support.automation.siemens.com/WW/view/de/35443942>)

3.3.13 Schutztürüberwachung mit Zuhaltung bis SIL 2 bzw. PL d über ET 20eco PN und F-CPU

Anwendung

Um den Zutritt zu dem Gefahrenbereich einer Maschine während des Betriebs zu verhindern, wird eine Schutztür installiert. Geht von der Maschine auch nach Abschaltung für eine gewisse Zeit noch eine Gefahr aus, kann der Zugang durch eine Zuhaltung solange verhindert werden.

Aufbau

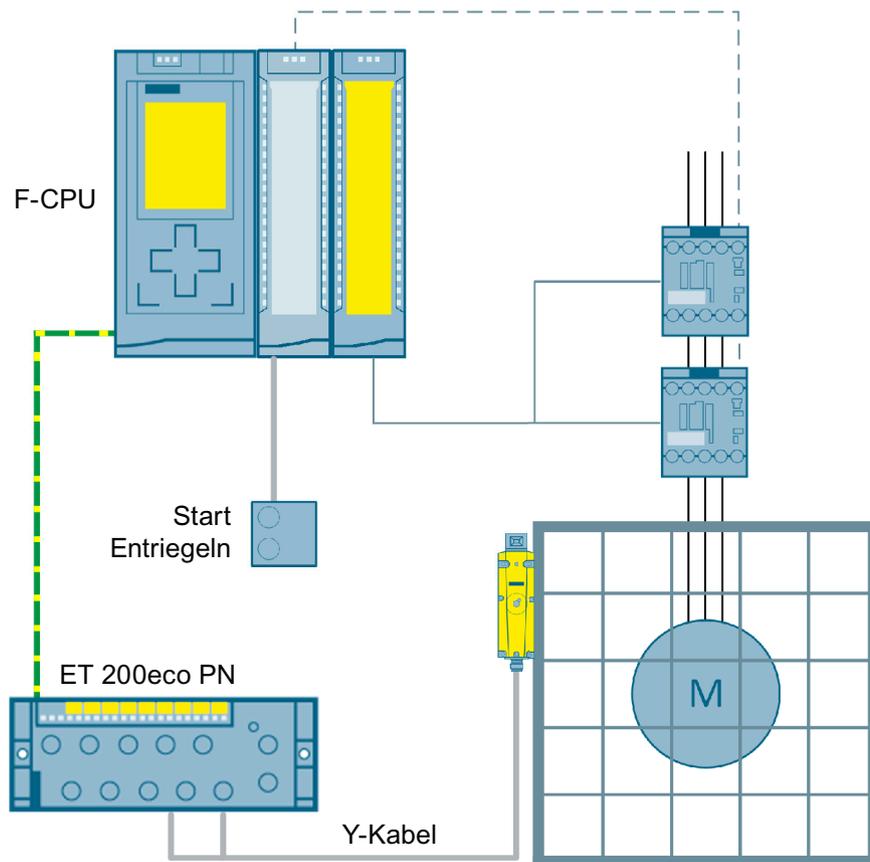


Bild 3-32 Schutztürüberwachung mit Zuhaltung bis SIL 2 bzw. PL d e über ET 20eco PN und F-CPU

Funktionsweise

Über einen Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Zusätzlich wird über den Sicherheitsschalter die Tür verriegelt. Wird der Befehl zum Entriegeln der Tür gegeben, schaltet die fehlersichere Steuerung die Leistungsschütze sicherheitsgerichtet ab. Nach Ablauf einer eingestellten Zeit wird die Zuhaltung entriegelt. Ist die Tür geschlossen und verriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Die Signale des Positionsschalters werden via M12-Stecker an das fehlersichere Peripheriemodul ET 200eco PN-F übertragen. Da sowohl Ausgangs- als auch Eingangssignale übergeben werden, ist ein Y-Kabel nötig.

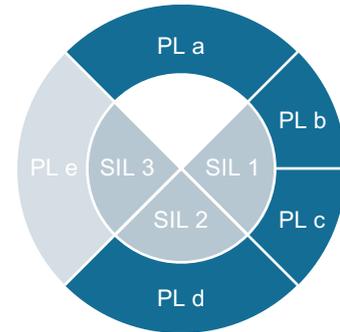
Da der Positionsschalter mehr Kontakte hat als an einem F-DI Port eingelesen werden können, existieren 2 Varianten des Positionsschalters, die sich in der Pinbelegung unterscheiden. Eine detaillierte Dokumentation ist dem unten aufgeführten Industry Online Support Beitrag zu entnehmen.

Sowohl die Sicherheitsfunktion "Schutztürüberwachung" als auch die Sicherheitsfunktion "Schutztürzuhaltung" sind bis SIL 2 bzw. PL d ausgelegt.

Bei diesem Beispiel kommt ein Sicherheitsschalter mit Federkraftverriegelung zum Einsatz. Dies bedeutet, dass aktiv Spannung angelegt werden muss, um die Zuhaltung der Schutztür aufzuheben.

Im Gegensatz dazu stehen auch Sicherheitsschalter mit Magnetkraftverriegelung zur Verfügung, mit welchen sich allerdings für die Sicherheitsfunktion "Schutztürzuhaltung" kein SIL bzw. PL umsetzen lässt.

Unter Berücksichtigung von Fehlerausschlüssen ist der Einsatz von nur einem Sicherheitsschalter mit oder ohne Zuhaltung bis SIL 2 bzw. PL d zulässig. Weitere Informationen entnehmen Sie dem unten aufgeführten Schreiben.



Sicherheitsgerichtete Komponenten

Sicherheitsschalter mit Zuhaltung	Dezentrale Peripherie IP67	Verbindungskabel
		
3SE5 (http://www.siemens.de/sirius-erfassen)	ET 200eco PN (http://www.siemens.de/simatic-safety)	Y-Kabel für ET 200eco PN (http://www.siemens.de/simatic-safety)

Steuerung Failsafe	Schütz
	
<p>S7 F-PLC (http://www.siemens.de/simatic-safety)</p>	<p>2x 3RT20 (http://www.siemens.de/sirius-control)</p>

Siehe auch

Ausführliche Dokumentation, TIA Portal-Projekt und Safety Evaluation (<https://support.industry.siemens.com/cs/ww/de/view/109778289>)

Schreiben zum Einsatz von Sicherheitsschaltern bis SIL 2 bzw. PL d (<https://support.industry.siemens.com/cs/ww/de/view/35443942>)

3.3.14 Schutztürüberwachung mit Zuhaltung mittels RFID-Sicherheitsschalter 3SE64 bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet. Geht von der Maschine auch nach Abschaltung für eine gewisse Zeit noch eine Gefahr aus, kann der Zugang durch eine Zuhaltung so lange verhindert werden.

Aufbau

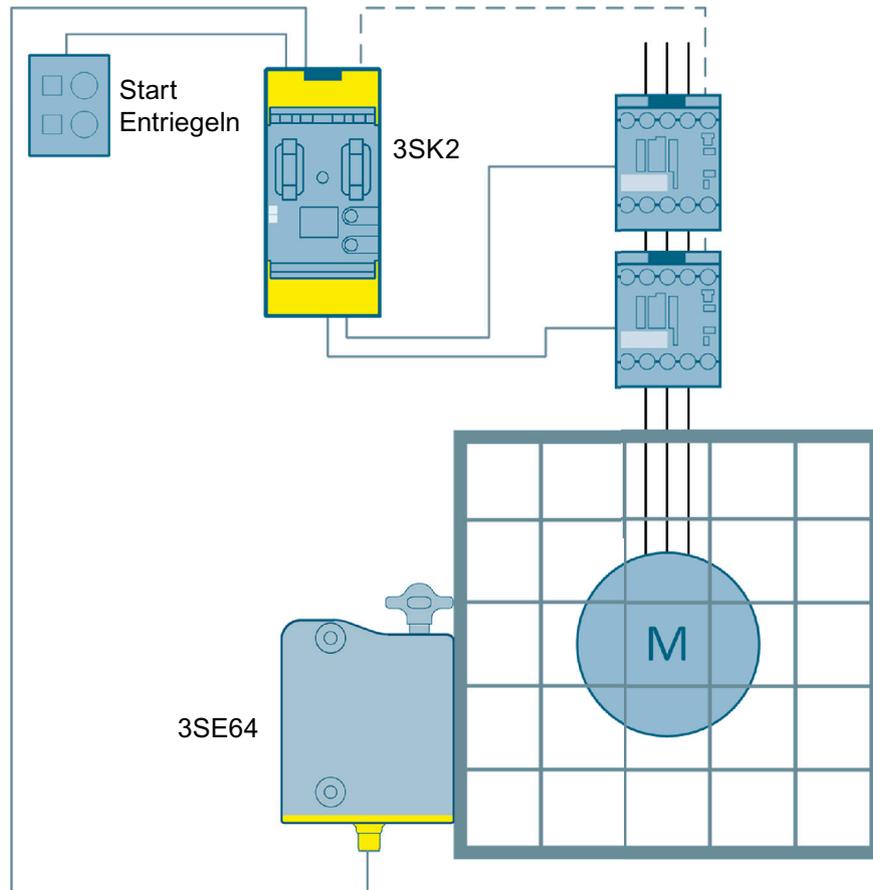


Bild 3-33 Schutztürüberwachung mit Zuhaltung mittels RFID-Sicherheitsschalter 3SE64 bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Funktionshinweise

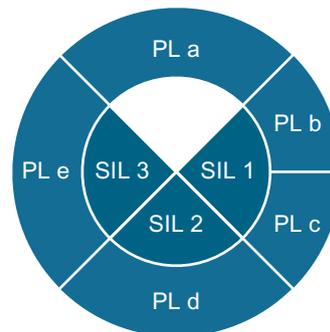
Über einen Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Zusätzlich wird über den Sicherheitsschalter die Tür verriegelt. Wird der Befehl zum Entriegeln der Tür gegeben, löst das Sicherheitsschaltgerät aus und öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Nach Ablauf einer eingestellten Zeit wird die Zuhaltung entriegelt. Ist die Tür geschlossen und verriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Der RFID-Sicherheitsschalter 3SE64 mit Zuhaltung ist in zwei Varianten verfügbar, welche sich im Ansteuerprinzip der Zuhaltfunktion unterscheiden (Arbeits-/Ruhestromprinzip).

Bei beiden Varianten ist für die Sicherheitsfunktion „Schutztürüberwachung“ SIL 3 bzw. PL e möglich. Während bei Variante 1 (Ruhestromprinzip) SIL 2 bzw. PL d für die Sicherheitsfunktion „Schutztürzuhaltung“ erreicht werden kann, ist bei Variante 2 (Arbeitsstromprinzip) für die Zuhaltung kein SIL / PL möglich – in dieser Variante dient die Zuhaltung ausschließlich dem Prozessschutz.

In diesem Applikationsbeispiel kommt Variante 1 zum Einsatz, da SIL 2 bzw. PL d für die Sicherheitsfunktion "Schutztürzuhaltung" gefordert wird.

Bei Variante 1 wird die RFID-Rückmeldung (OSSD-Ausgänge des 3SE64) erst aktiv, sobald die Zuhaltung ordnungsmäßig ausgeführt wurde. Hierbei wird auch die Zuhaltung überwacht und im Anwenderprogramm kann ausgewertet werden, ob die Tür tatsächlich verriegelt ist oder nicht, wodurch den Anforderungen an die Diagnose bei SIL 2 bzw. PL d Rechnung getragen wird.



Sicherheitsgerichtete Komponenten

RFID-Sicherheitsschalter mit Zuhaltung	Sicherheitsschaltgerät	Schütz
		
3SE64 (http://www.siemens.de/sirius-erfassen)	3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<https://support.industry.siemens.com/cs/ww/de/view/109811081>)

3.3.15 Schutztürüberwachung mit Zuhaltung mittels RFID-Sicherheitsschalter 3SE64 bis SIL 3 bzw. PL e mit einer fehlersicheren Steuerung

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet. Geht von der Maschine auch nach Abschaltung für eine gewisse Zeit noch eine Gefahr aus, kann der Zugang durch eine Zuhaltung solange verhindert werden.

Aufbau

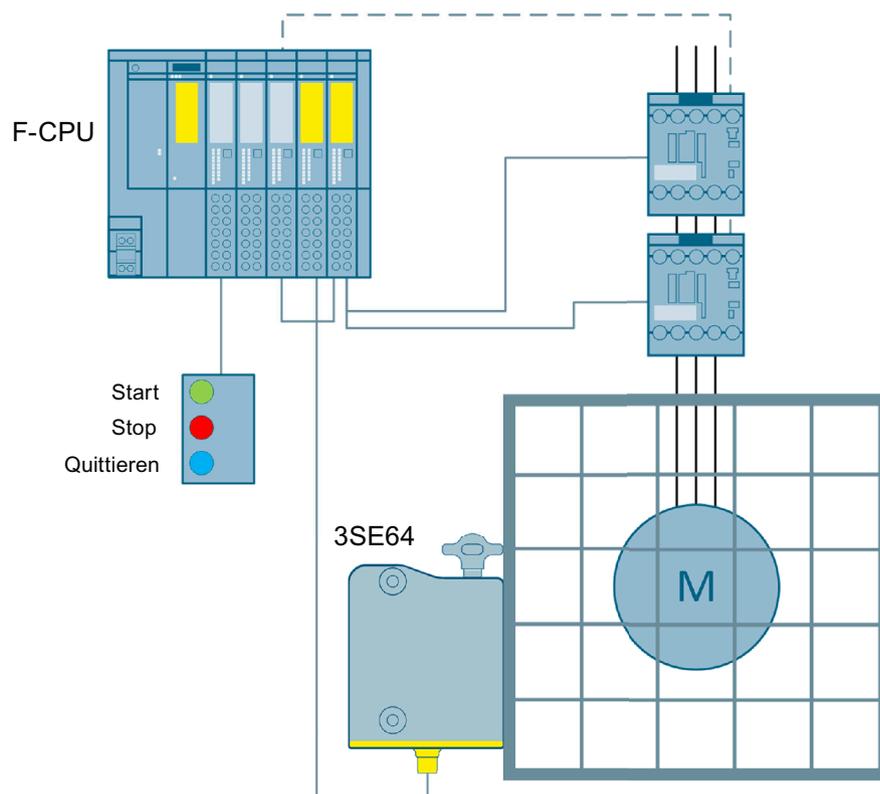


Bild 3-34 Schutztürüberwachung mit Zuhaltung mittels RFID-Sicherheitsschalter 3SE64 bis SIL 3 bzw. PL e mit einer fehlersicheren Steuerung

Funktionsweise

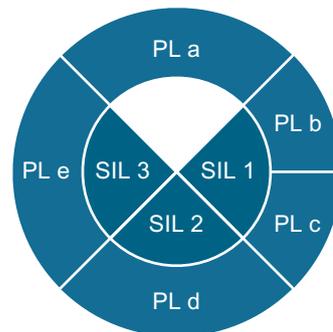
Über einen Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Zusätzlich wird über den Sicherheitsschalter die Tür verriegelt. Wird der Befehl zum Entriegeln der Tür gegeben, schaltet die fehlersichere Steuerung die Leistungsschütze sicherheitsgerichtet ab. Nach Ablauf einer eingestellten Zeit wird die Zuhaltung entriegelt. Ist die Tür geschlossen und verriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Der RFID-Sicherheitsschalter 3SE64 mit Zuhaltung ist in zwei Varianten verfügbar, welche sich im Ansteuerprinzip der Zuhaltfunktion unterscheiden (Arbeits-/Ruhestromprinzip).

Bei beiden Varianten ist für die Sicherheitsfunktion „Schutztürüberwachung“ SIL 3 bzw. PL e möglich. Während bei Variante 1 (Ruhestromprinzip) SIL 2 bzw. PL d für die Sicherheitsfunktion „Schutztürzuhaltung“ erreicht werden kann, ist bei Variante 2 (Arbeitsstromprinzip) für die Zuhaltung kein SIL / PL möglich – in dieser Variante dient die Zuhaltung ausschließlich dem Prozessschutz.

In diesem Applikationsbeispiel kommt Variante 1 zum Einsatz, da SIL 2 bzw. PL d für die Sicherheitsfunktion "Schutztürzuhaltung" gefordert wird.

Bei Variante 1 wird die RFID-Rückmeldung (OSSD-Ausgänge des 3SE64) erst aktiv, sobald die Zuhaltung ordnungsmäßig ausgeführt wurde. Hierbei wird auch die Zuhaltung überwacht und im Anwenderprogramm kann ausgewertet werden, ob die Tür tatsächlich verriegelt ist oder nicht, wodurch den Anforderungen an die Diagnose bei SIL 2 bzw. PL d Rechnung getragen wird.



Sicherheitsgerichtete Komponenten

RFID-Sicherheitsschalter mit Zuhaltung	Steuerung Failsafe	Schütz
		
3SE64 (http://www.siemens.de/sirius-erfassen)	S7 F-PLC (http://www.siemens.de/simatic-safety)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, TIA-Portal-Projekt und Safety Evaluation (<https://support.industry.siemens.com/cs/ww/de/view/109811981>)

3.4 Überwachung offener Gefahrenbereiche

3.4.1 Einleitung

Innerhalb eines industriellen Betriebs existieren oftmals Bereiche, die für Menschen aufgrund der hohen Gefährdung, für bestimmte Zeiten nicht zugänglich sein dürfen. So dürfen sich beispielsweise keine Körperteile im Innenraum einer Presse während der Abwärtsbewegung befinden. Solche Überwachungen werden oftmals mit Lichtvorhängen realisiert.

Zu bestimmten Zeiten kann eine beabsichtigte Unterdrückung der Schutzfunktion gefordert sein. Muting ist eine beabsichtigte, temporäre Unterdrückung der Schutzfunktion. Dieser sogenannte Mutingbetrieb wird von Mutingsensoren ausgelöst (z. B. während des Materialtransports in den Gefahrenbereich).

Hinweis

Lichtvorhänge können ihre Schutzwirkung nur erfüllen, wenn sie mit ausreichendem Sicherheitsabstand montiert werden. Die Berechnungsformeln für den Sicherheitsabstand sind abhängig von der Art der Absicherung. Anbausituationen und Berechnungsformeln finden sich in der Norm EN 13855 ("Anordnung von Schutzeinrichtungen in Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen").

3.4.2 Zugangsüberwachung durch einen Lichtvorhang bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Anwendung

Um den Zugang zu einem offenen Gefahrenbereich zu überwachen, können sogenannte berührungslos wirkende Schutzeinrichtungen, wie zum Beispiel ein Lichtvorhang, eingesetzt werden. Bei Unterbrechung des Lichtwegs wird ein Abschaltsignal ausgelöst.

Aufbau

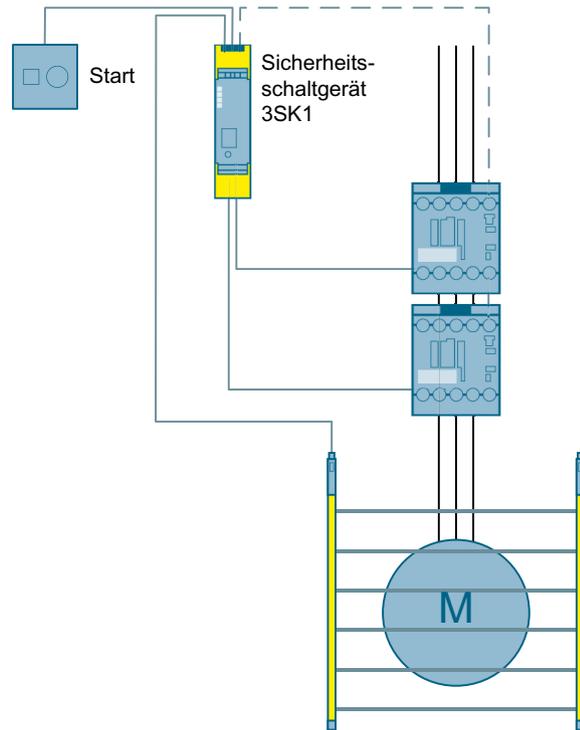
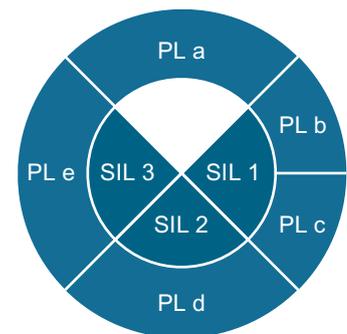


Bild 3-35 Zugangsüberwachung durch einen Lichtvorhang bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Funktionsweise

Der Lichtvorhang besteht aus einer Sende- und einer Empfangseinheit. Zwischen den beiden liegt das Schutzfeld. Ist der Lichtweg nicht unterbrochen, führen die Ausgänge OSSD1 und OSSD2 Spannung und werden von dem Sicherheitsschaltgerät ausgewertet. Bei einer Unterbrechung des Lichtwegs schalten die beiden Ausgänge ab und das Sicherheitsschaltgerät öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist der Lichtweg ununterbrochen und der Rückführkreis geschlossen, kann wieder eingeschaltet werden. Abhängig von der Applikation kann dies automatisch oder durch einen Starttaster geschehen.



Sicherheitsgerichtete Komponenten

Lichtvorhang	Sicherheitsschaltgerät	Schütz
		
SICK C4000	3SK1 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/73136329>)

3.4.3 Zugangsüberwachung durch einen Lichtvorhang bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Anwendung

Um den Zugang zu einem offenen Gefahrenbereich zu überwachen, können sogenannte berührungslos wirkende Schutzeinrichtungen, wie zum Beispiel ein Lichtvorhang, eingesetzt werden. Bei Unterbrechung des Lichtwegs wird ein Abschaltsignal ausgelöst.

Aufbau

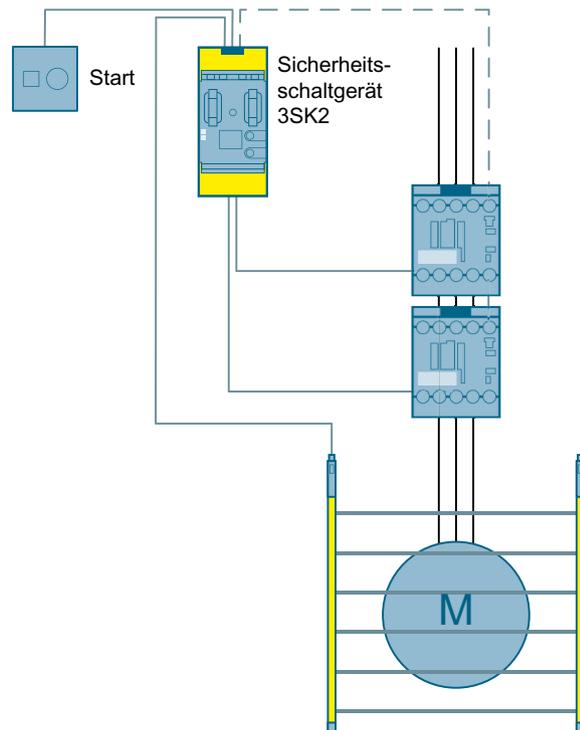
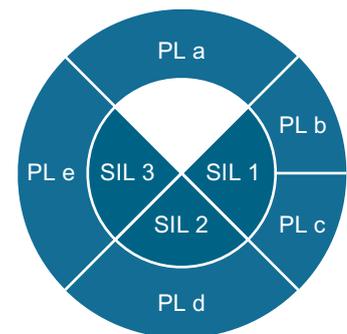


Bild 3-36 Zugangsüberwachung durch einen Lichtvorhang bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Der Lichtvorhang besteht aus einer Sende- und einer Empfangseinheit. Zwischen den beiden liegt das Schutzfeld. Ist der Lichtweg nicht unterbrochen, führen die Ausgänge OSSD1 und OSSD2 Spannung und werden von dem Sicherheitsschaltgerät ausgewertet. Bei einer Unterbrechung des Lichtwegs schalten die beiden Ausgänge ab und das Sicherheitsschaltgerät öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist der Lichtweg ununterbrochen und der Rückführkreis geschlossen, kann wieder eingeschaltet werden. Abhängig von der Applikation kann dies automatisch oder durch einen Starttaster geschehen.



Sicherheitsgerichtete Komponenten

Lichtvorhang	Sicherheitsschaltgerät	Schütz
		
SICK C4000	3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109479277>)

3.4.4 Zugangsüberwachung durch eine Schaltmatte bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Anwendung

Um den Zugang zu einem offenen Gefahrenbereich zu überwachen, können Schaltmatten eingesetzt werden, die bei Betreten ein Abschaltsignal auslösen.

Aufbau

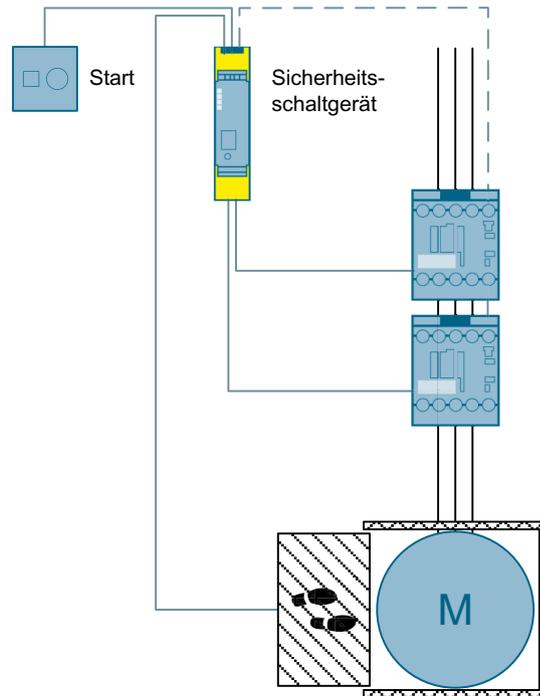
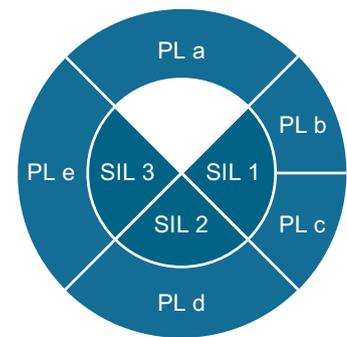


Bild 3-37 Zugangsüberwachung durch eine Schaltmatte bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Funktionsweise

Mit dem Sicherheitsschaltgerät 3SK1 können Schaltmatten beruhend auf dem Öffnerprinzip (bzw. Öffner-Schließer) ausgewertet werden. Bei diesem Prinzip wird der zweikanalige Sensorkreis bei Betreten unterbrochen. Das Sicherheitsschaltgerät öffnet daraufhin die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist die Schaltmatte frei und der Rückführkreis geschlossen, kann wieder eingeschaltet werden. Abhängig von der Applikation kann dies automatisch oder durch einen Starttaster geschehen.



Sicherheitsgerichtete Komponenten

Schaltmatte	Sicherheitsschaltgerät	Schütz
		
	3SK1 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/77262359>)

3.4.5 Zugangsüberwachung durch eine Schaltmatte bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Anwendung

Um den Zugang zu einem offenen Gefahrenbereich zu überwachen, können Schaltmatten eingesetzt werden, die bei Betreten ein Abschaltsignal auslösen.

Aufbau

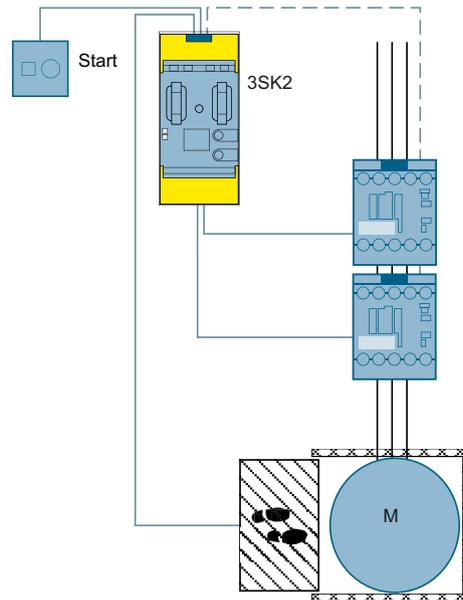
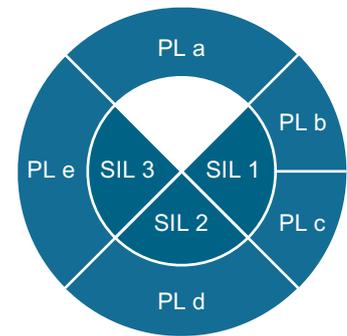


Bild 3-38 Zugangsüberwachung durch eine Schaltmatte bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Schaltmatten können entweder auf dem Öffnerprinzip oder dem Querschlussprinzip beruhen. Beim Öffnerprinzip wird der zweikanalige Sensorkreis bei Betreten unterbrochen. Hingegen wird beim Querschlussprinzip ein Querschluss zwischen den beiden Sensorkreisen beim Betreten ausgelöst. In beiden Fällen wird das Signal vom Sicherheitsschaltgerät 3SK2 ausgewertet. Das Sicherheitsschaltgerät öffnet daraufhin die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist die Schaltmatte frei und der Rückführkreis geschlossen, kann wieder eingeschaltet werden. Abhängig von der Applikation kann dies automatisch oder durch einen Starttaster geschehen.



Sicherheitsgerichtete Komponenten

Schaltmatte	Sicherheitsschaltgerät	Schütz
		
	3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109747651>)

3.4.6 Bereichsüberwachung durch einen Laserscanner bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät 3SK1

Anwendung

Um ganze Bereiche auf unbefugten Zutritt zu überwachen, werden häufig Laserscanner eingesetzt. Diese überwachen großflächig einen Gefahrenbereich und lösen bei Erkennung von Objekten ein Abschaltsignal aus.

Aufbau

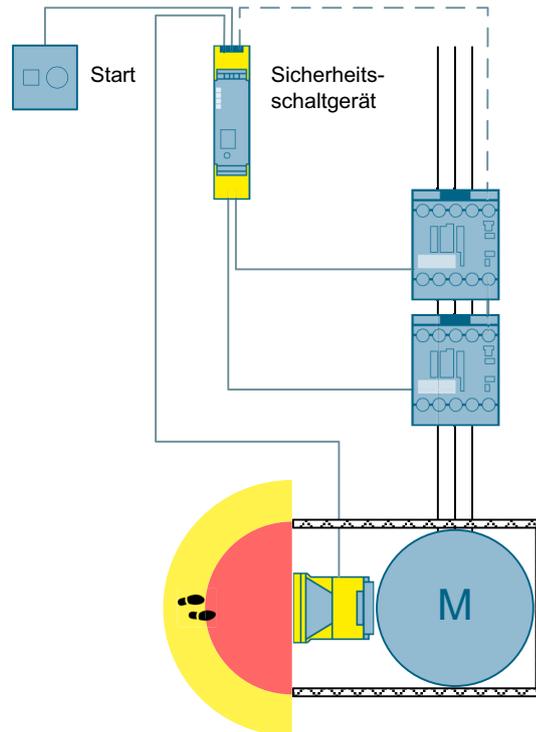
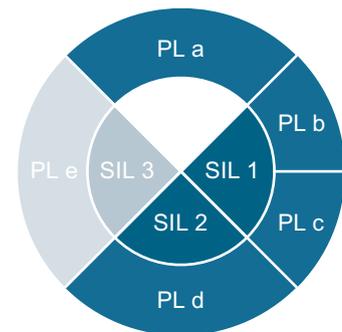


Bild 3-39 Bereichsüberwachung durch einen Laserscanner bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät 3SK1

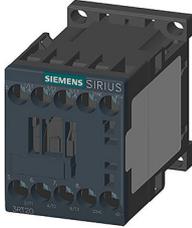
Funktionsweise

Der Laserscanner überwacht großflächig einen Sicherheitsbereich. Dieser kann in der Regel in einen Warnbereich und einen Gefahrenbereich eingeteilt werden. Bei Eintritt in den Warnbereich wird eine Warnung zum Beispiel durch eine Meldeleuchte ausgegeben. Hingegen wird bei Eintritt in den Sicherheitsbereich die Maschine abgeschaltet.

Dabei führen während des Betriebs die Ausgänge OSSD1 und OSSD2 Spannung und werden von dem Sicherheitsschaltgerät ausgewertet. Bei einer Unterbrechung des Lichtwegs schalten die beiden Ausgänge ab und das Sicherheitsschaltgerät öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist der Lichtweg ununterbrochen und der Rückführkreis geschlossen, kann wieder eingeschaltet werden. Abhängig von der Applikation kann dies automatisch oder durch einen Starttaster geschehen.



Sicherheitsgerichtete Komponenten

Laserscanner	Sicherheitsschaltgerät	Schütz
		
SICK S3000	3SK1 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/77262367>)

3.4.7 Bereichsüberwachung durch einen Laserscanner bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät 3SK2

Anwendung

Um ganze Bereiche auf unbefugten Zutritt zu überwachen, werden häufig Laserscanner eingesetzt. Diese überwachen großflächig einen Gefahrenbereich und lösen bei Erkennung von Objekten ein Abschaltsignal aus.

Aufbau

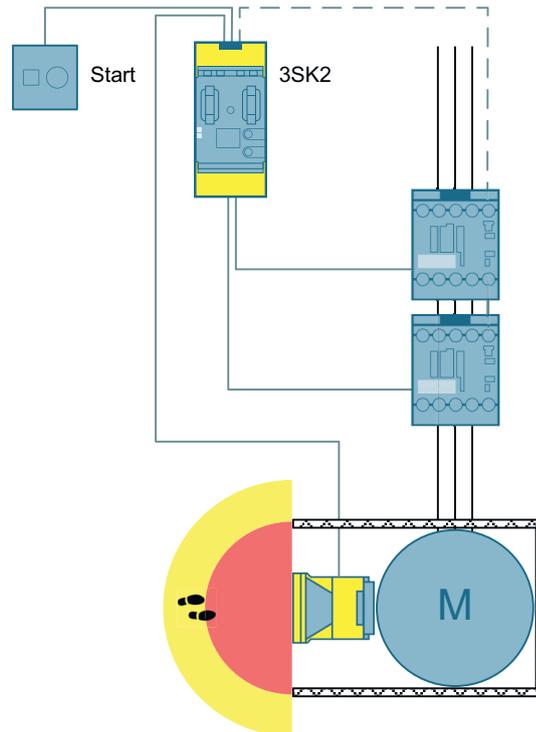
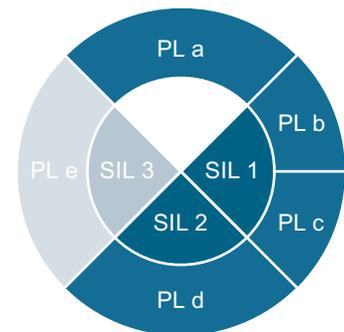


Bild 3-40 Bereichsüberwachung durch einen Laserscanner bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Der Laserscanner überwacht großflächig einen Sicherheitsbereich. Dieser kann in der Regel in einen Warnbereich und einen Gefahrenbereich eingeteilt werden. Bei Eintritt in den Warnbereich wird eine Warnung zum Beispiel durch eine Meldeleuchte ausgegeben. Hingegen wird bei Eintritt in den Sicherheitsbereich die Maschine abgeschaltet.

Dabei führen während des Betriebs die Ausgänge OSSD1 und OSSD2 Spannung und werden von dem Sicherheitsschaltgerät ausgewertet. Bei einer Unterbrechung des Lichtwegs schalten die beiden Ausgänge ab und das Sicherheitsschaltgerät öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden. Ist der Lichtweg ununterbrochen und der Rückführkreis geschlossen, kann wieder eingeschaltet werden. Abhängig von der Applikation kann dies automatisch oder durch einen Starttaster geschehen.



Sicherheitsgerichtete Komponenten

Laserscanner	Sicherheitsschaltgerät	Schütz
		
<p>SICK S3000</p>	<p>3SK2 (http://www.siemens.de/safety-relays)</p>	<p>2x 3RT20 (http://www.siemens.de/sirius-control)</p>

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109485647>)

3.5 Sichere Drehzahl- und Stillstandsüberwachung

3.5.1 Einleitung

In Maschinen, bei denen die Maschinenbewegung bzw. die sich bewegenden Teile eine Gefährdung für Mensch und Maschine ausgehen kann, wird häufig eine Drehzahl- oder Stillstandsüberwachung eingesetzt.

Oftmals sind diese Applikationen in Verbindung mit trennenden Schutzeinrichtungen (Schutztür) und Schutztürzuhaltung realisiert.

Verriegelungseinrichtungen mit Zuhaltung dienen dazu, Gefahrenbereiche vor ungewolltem Betreten zu sichern. Das hat meistens zwei Gründe:

1. Zum Schutz des Menschen vor nachlaufenden gefährlichen Maschinenbewegungen, hohen Temperaturen etc. Hier gibt die ISO 14119 bzw. EN 1088 Leitsätze zur Gestaltung und Auswahl von Verriegelungseinrichtungen. In dieser Norm wird gefordert, dass erst nach dem Stoppen der gefährlichen Maschinenbewegung der Gefahrenbereich zugänglich sein darf.
2. Eine Zuhaltung kann aus Gründen der Prozesssicherheit sinnvoll sein. Dieser Fall tritt ein, wenn die Gefahr nach dem Öffnen der Schutzeinrichtung gestoppt wird, aber dadurch Schäden an der Maschine oder dem Werkstück entstehen können. Hier wird erst die Maschine in eine geordnete Halteposition gefahren, bevor der Zugang frei gegeben wird.

Bei der Drehzahlüberwachung wird eine Schutztürzuhaltung z. B. erst dann entriegelt, wenn das sich bewegende Teil zum Stillstand gekommen ist, oder bei einer sicheren Drehzahl läuft.

Im Gegensatz zur Drehzahlüberwachung wird bei der Stillstandsüberwachung z. B. die Schutztürzuhaltung nur dann entriegelt, wenn der Stillstand erreicht wurde.

3.5.2 Sichere Drehzahlüberwachung bis SIL 3 bzw. PL e mit einem Drehzahlwächter

Anwendung

Um sicherzustellen, dass selbst im Falle eines Fehlers, die Drehzahl eines Motors begrenzt und somit der Menschen vor möglichen abfallenden Werkzeugteilen geschützt wird, wird die Drehzahl mithilfe eines Drehzahlwächters überwacht.

Aufbau

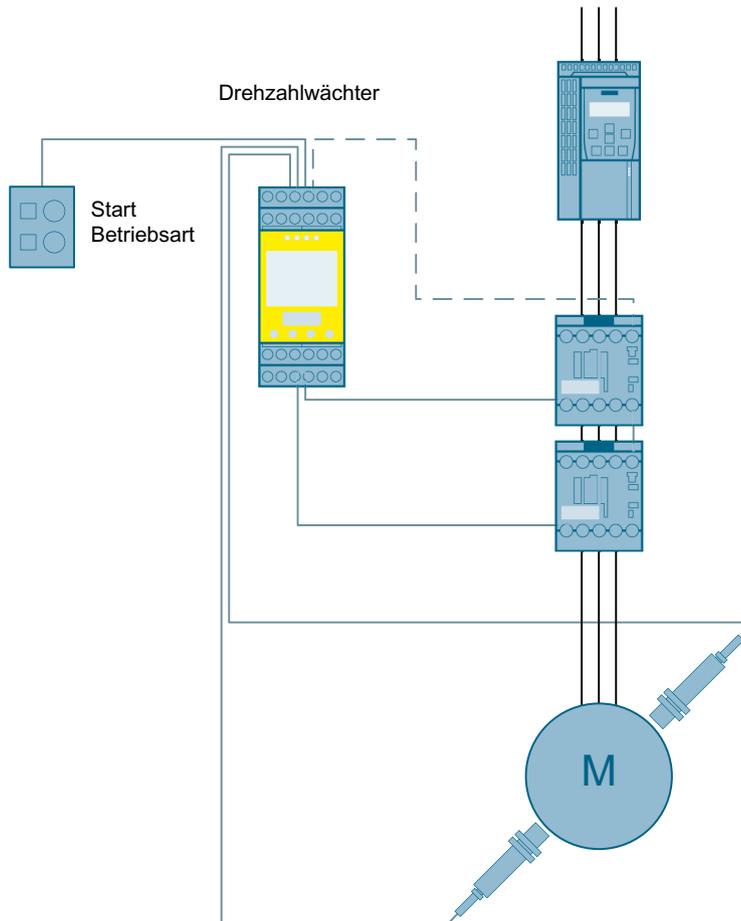


Bild 3-41 Sichere Drehzahlüberwachung bis SIL 3 bzw. PL e mit einem Drehzahlwächter

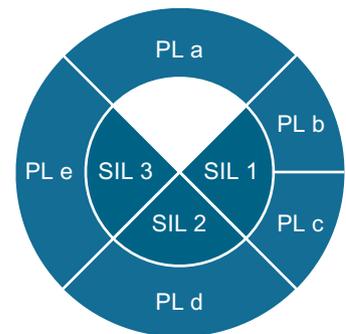
Funktionsweise

Am Drehzahlwächter wird eine bestimmte Drehzahlgrenze bzw. ein bestimmter Drehzahlbereich (Ober- und Untergrenze) eingestellt.

Über einen Betriebsartenschalter kann zwischen Einricht- und Automatikbetrieb mit individuellen Drehzahlbereichen gewechselt werden.

Bei Über- oder Unterschreitung des jeweiligen Drehzahlfensters werden die Leistungsschütze sicherheitsgerichtet abgeschaltet.

Sobald die Aktorik abgeschaltet hat und der Rückführkreis geschlossen ist, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Drehzahlwächter	Schütz
	
3TK2810-1 (http://www.siemens.de/sirius-monitor)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/69065043>)

3.5.3 Sichere Stillstandsüberwachung inkl. Schutzürzuhaltung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Anwendung

Das Sicherheitssystem überwacht eine Schutztür. Der Stillstandswächter stellt sicher, dass während des Betriebs des Motors kein Zugang zu den sich bewegenden, gefahrbringenden Maschinenteilen, gestattet wird.

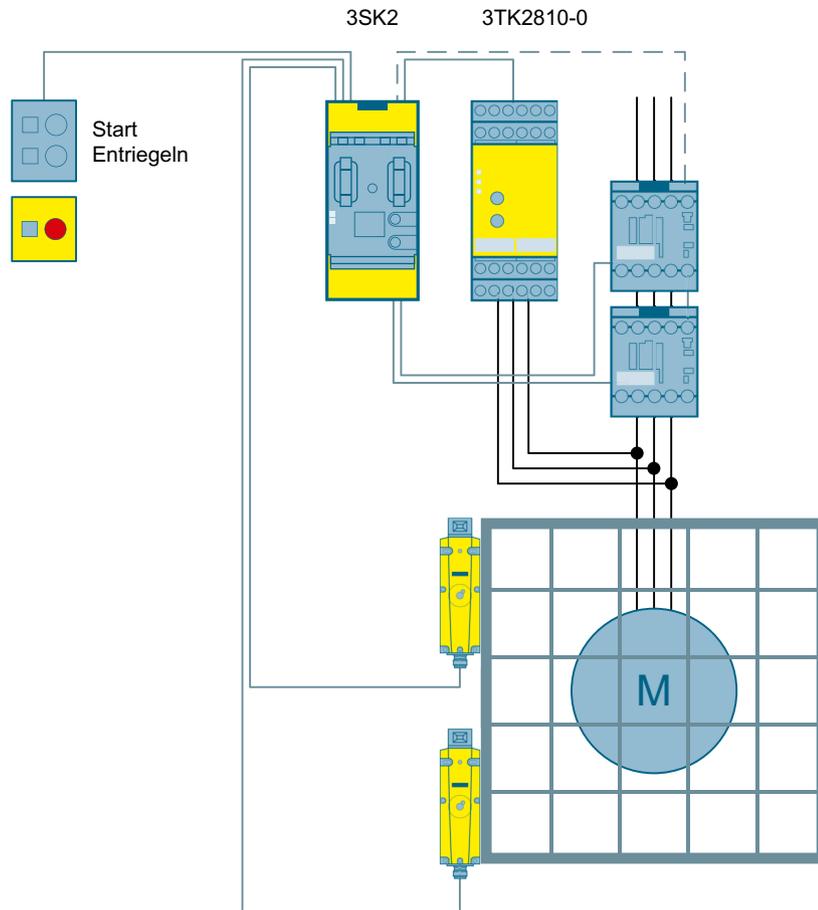


Bild 3-42 Sichere Stillstandsüberwachung inkl. Schutzürzuhaltung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Der sichere Stillstandswächter 3TK2810-0 misst eine durch Restmagnetisierung induzierte Spannung des auslaufenden Motors an drei Klemmen der Ständerwicklung. Geht die Induktionsspannung gegen 0, bedeutet dies für das Gerät Motorstillstand und die Ausgangsrelais werden aktiviert.

Das Modulare Sicherheitssystem überwacht dieses Signal vom Stillstandswächter sowie die beiden Sicherheitsschalter.

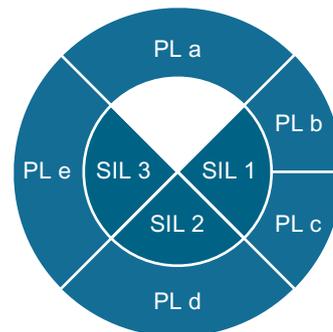
Wird Motorstillstand erkannt und der Taster zum Entriegeln betätigt, wird die Zuhaltung entriegelt und die Schutztür kann geöffnet werden. Gleichzeitig werden die Schütze sicherheitsgerichtet abgeschaltet und somit ein unerwarteter Wiederanlauf des Motors verhindert.

Ist die Tür verriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Der Not-Halt stellt eine zusätzliche Sicherheitsfunktion dar, die hier nicht weiter betrachtet wird.

Bei diesem Beispiel kommen Sicherheitsschalter mit Federkraftverriegelung zum Einsatz. Dies bedeutet, dass aktiv Spannung angelegt werden muss, um die Zuhaltung der Schutztür aufzuheben.

Im Gegensatz dazu stehen auch Sicherheitsschalter mit Magnetkraftverriegelung zur Verfügung, mit welchen sich allerdings für die Sicherheitsfunktion "Schutztürzuhaltung" kein SIL bzw. PL umsetzen lässt.



Sicherheitsgerichtete Komponenten

Sicherheitsschalter mit Zuhaltung	Stillstandswächter	Sicherheitsschaltgerät	Schütz
			
2x 3SE5 (http://www.siemens.de/sirius-erfassen)	3TK2810-0 (http://www.siemens.de/sirius-monitor)	3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109479278>)

3.5.4 Sichere Drehzahl-, Schutztür- und Zuhaltungsüberwachung bis SIL 3 bzw. PL e mit einem Drehzahlwächter

Anwendung

Der Drehzahlwächter stellt sicher, dass ab einer einstellbaren Drehzahl, kein Zugang zu den sich bewegenden, gefahrbringenden Maschinenteilen, gestattet wird.

Aufbau

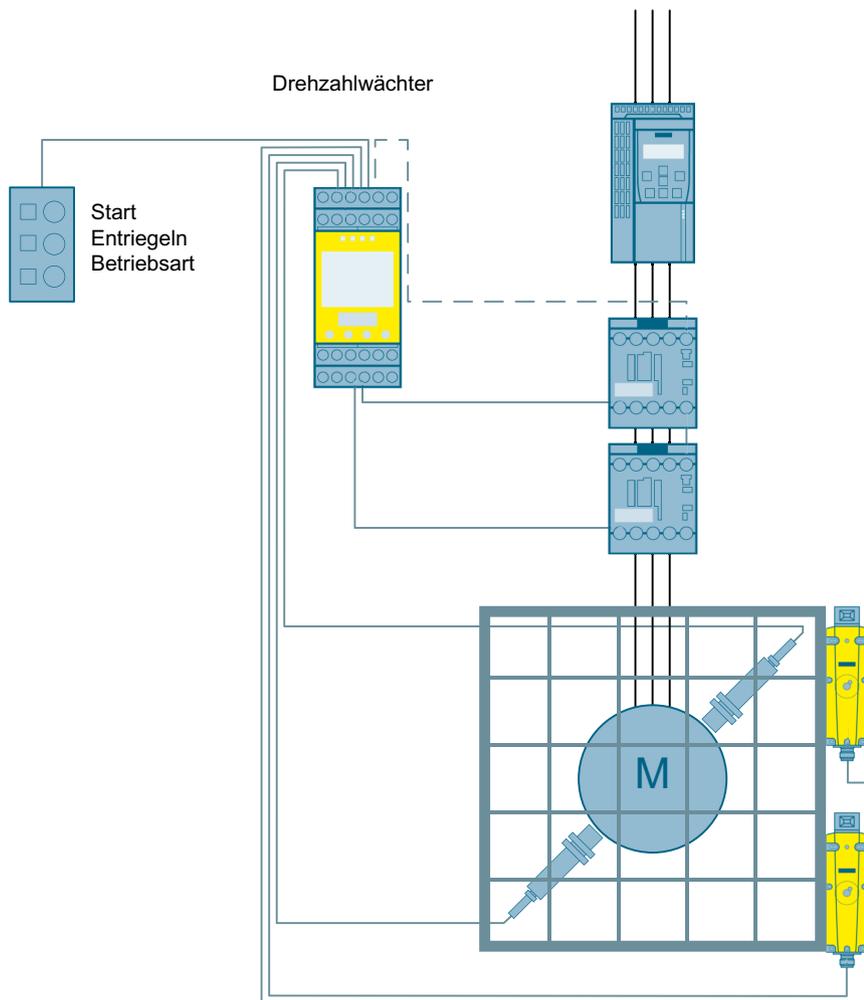
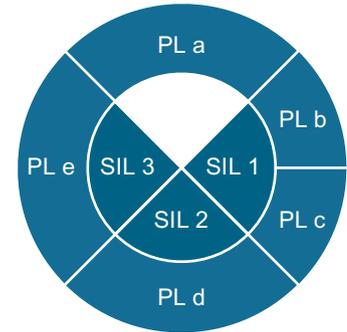


Bild 3-43 Sichere Drehzahl-, Schutztür- und Zuhaltungsüberwachung bis SIL 3 bzw. PL e mit einem Drehzahlwächter

Funktionsweise

Am Drehzahlwächter wird ein sicheres Drehzahlfenster eingestellt. Solange sich die Drehzahl außerhalb dieses sicheren Drehzahlfensters befindet, wird der Zugang zu den sich bewegenden, gefahrbringenden Maschinenteilen durch eine Schutztür mit Zuhaltung verhindert. Gleichzeitig überwacht der Drehzahlwächter die Stellung der Schutztür.

Über einen Betriebsartenschalter kann zwischen Einricht- und Automatikbetrieb mit individuellen Drehzahlfenstern gewechselt werden. Über zwei Relaisausgänge werden ein erkannter Stillstand und das Einhalten des eingestellten Drehzahlfensters ausgegeben.



Im Automatikbetrieb bleibt die Schutztür verriegelt, solange kein Stillstand erkannt wird. Bei Über- oder Unterschreitung des Automatik-Drehzahlfensters werden die Leistungsschütze sicherheitsgerichtet abgeschaltet.

Im Einrichtbetrieb ist die Schutztür dauerhaft freigegeben. Bei Über- oder Unterschreitung des Einricht-Drehzahlfensters werden die Leistungsschütze abgeschaltet.

Bei geöffneter Schutztür stellt der Drehzahlwächter sicher, dass der Motor nicht eingeschaltet werden kann. Ist die Tür geschlossen und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Sicherheitsgerichtete Komponenten

Sicherheitsschalter mit Zuhaltung	Drehzahlwächter	Schütz
		
2x 3SE5 (http://www.siemens.de/sirius-erfassen)	3TK2810-1 (http://www.siemens.de/sirius-monitor)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/77284316>)

3.6 Sicheres Bedienen

3.6.1 Einleitung

Muss ein Bediener in einem gefährlichen Bereich einer Maschine hantieren, z. B. beim Einlegen oder Entnehmen von Werkstücken bei Pressen, Stanzen oder ähnlichen Maschinen, müssen Sicherheitsfunktionen für das sichere Bedienen der Maschine umgesetzt werden. Das Starten der gefahrbringenden Bewegung darf z. B. erst erfolgen, wenn sich kein Körperteil des Bedieners im Gefahrenbereich aufhält. Eine Möglichkeit, dies zu gewährleisten, ist der Einsatz einer Zweihandbedienung. Hier muss der Bediener mit beiden Händen jeweils einen Taster annähernd gleichzeitig betätigen, um die Maschine bzw. die gefahrbringende Bewegung zu starten. Das Loslassen der Taster führt zum Stopp der Maschine bzw. der Bewegung.

Das folgende Kapitel enthält Applikationsbeispiele mit Zweihandbedienung zum sicheren Bedienen einer Maschine.

Hinweis

Die Auswahl einer Zweihandschaltung als eine geeignete Sicherheitseinrichtung hängt von der Risikobeurteilung ab.

Für bestimmte Anwendungsfälle kann eine Zweihandbedienung ungeeignet sein, weil die Bedienung per Hand nicht möglich ist. Hier bieten sich als Lösung die einpedaligen Sicherheits-Fußschalter 3SE2924-3AA20 an. Die Schalter haben eine Verriegelungsfunktion nach EN ISO 13850 und sind mit einer Schutzhaube gegen unbeabsichtigtes Betätigen geschützt. Die Schalter sind mit zwei Schaltelementen mit je einem Schließer und einem Öffner ausgestattet.

Der normale Arbeitsablauf wird durch Herunterdrücken des Pedals bis zum Druckpunkt eingeleitet, wobei die beiden Schließer schließen und z.B. der Motor zu laufen beginnt. Wird das Pedal im Gefahrenfall über den Widerstand des Druckpunktes hinaus betätigt, werden die zwangsöffnenden Öffnerkontakte geöffnet und der Motor gestoppt. Gleichzeitig tritt die selbstständige Rastung in Kraft und hält die Öffnerkontakte in geöffneter Stellung fest. Hierdurch wird ein unkontrolliertes Weiterlaufen oder ein neuer Start beweglicher Maschinenteile verhindert. Nach Beseitigung der Gefahr ist ein Wiederanlauf der Maschine erst nach einer manuellen Entriegelung über einen Drucktaster an der Oberseite des Gehäuses möglich. Die Kontakte werden dabei wieder freigegeben und gehen in ihren Ausgangszustand zurück.

3.6.2 Zweihandbedienung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Anwendung

Zweihandbedienpulte bestehen aus zwei Tastern, die simultan betätigt werden müssen, um eine Maschine zu betreiben. Dadurch wird verhindert, dass der Bediener während des Betriebs in den Gefahrenbereich greifen kann.

Aufbau

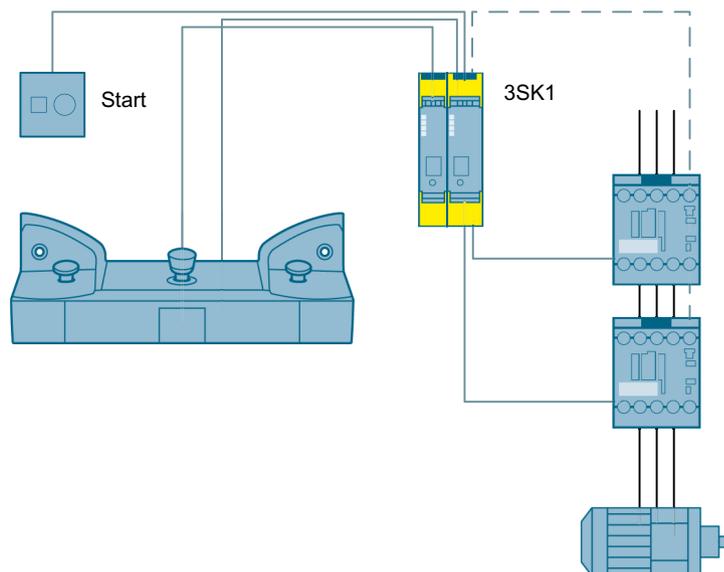


Bild 3-44 Zweihandbedienung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

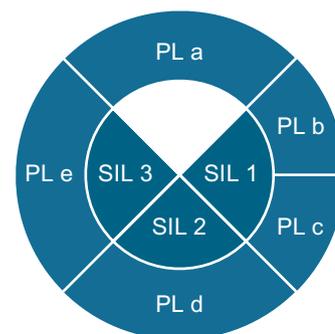
Funktionsweise

Durch die Bedingung der simultanen Betätigung beider Taststellen ist der Bediener an das Zweihandbedienpult gebunden und kann so nicht in den Gefahrenbereich greifen. Das Sicherheitsschaltgerät 3SK1 schaltet die Freigabekreise nur, wenn beide Signale innerhalb von 500 ms anliegen und der Rückführkreis geschlossen ist.

Bei Loslassen einer der beiden Taster schaltet das Sicherheitsschaltgerät 3SK1 die Maschine sofort sicherheitsgerichtet ab.

Nach Betätigung des Not-Halts muss durch den Starttaster wieder eingeschaltet werden.

Die hier gezeigte Beschaltung (mit jeweils nur einem Schließer pro Schaltgeber) entspricht den Anforderungen des Typs IIIB nach EN574 bzw. EN ISO 13851. Durch Anwendung von entsprechend zugelassenen Schaltern und querschluss sicherer Leitungsverlegung können mit den 3SK1 Sicherheitsschaltgeräten Applikationen bis Typ IIIC gem. EN 574 bzw. EN ISO 13851 aufgebaut werden. Details sind dem 3SK1 Gerätehandbuch (<https://support.industry.siemens.com/cs/at/de/view/67585885>) zu entnehmen.



Sicherheitsgerichtete Komponenten

Zweihandbedienpult	Sicherheitschaltgerät	Eingangserweiterung	Schütz
			
3SU18 (http://www.siemens.de/sirius-command)	3SK1 (http://www.siemens.de/safety-relays)	3SK1 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/74562494>)

Einsatz des Sensortasters im Zweihandbedienpult (<http://support.automation.siemens.com/WW/view/de/109479531>)

3.6.3 Zweihandbedienung bis SIL 3 bzw. PL e mit einem Sicherheitschaltgerät 3SK2

Anwendung

Zweihandbedienpulte bestehen aus zwei Tastern, die simultan betätigt werden müssen, um eine Maschine zu betreiben. Dadurch wird verhindert, dass der Bediener während des Betriebs in den Gefahrenbereich greifen kann.

Aufbau

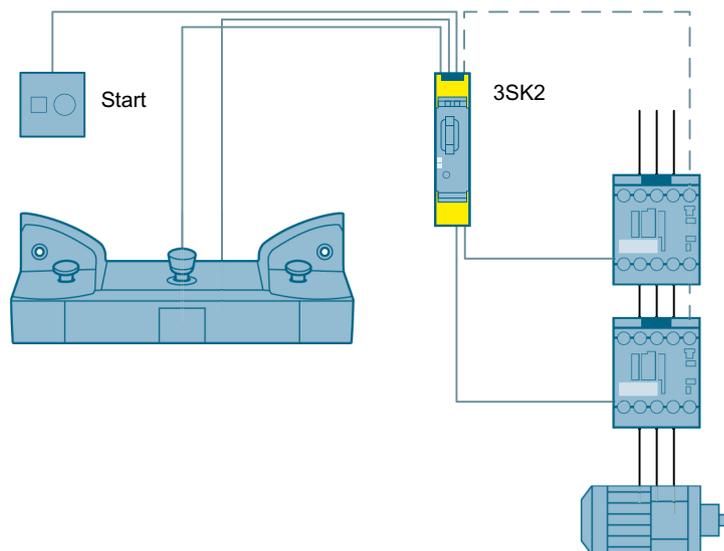


Bild 3-45 Zweihandbedienung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

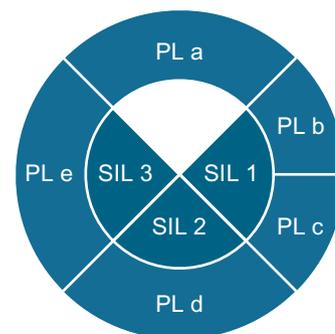
Durch die Bedingung der simultanen Betätigung beider Taststellen ist der Bediener an das Zweihandbedienpult gebunden und kann so nicht in den Gefahrenbereich greifen. Das Sicherheitsschaltgerät 3SK2 schaltet die Freigabekeine nur, wenn beide Signale innerhalb von 500 ms anliegen und der Rückführkreis geschlossen ist.

Bei Loslassen einer der beiden Taster schaltet das Sicherheitsschaltgerät 3SK2 die Maschine sofort sicherheitsgerichtet ab.

Durch einen vierkanaligen Aufbau im Zweihandbedienpult wird sichergestellt, dass ein mögliches Verschweißen einer der Kontakte unmittelbar erkannt wird.

Nach Betätigung des Not-Halts muss durch den Starttaster wieder eingeschaltet werden.

Die hier gezeigte Beschaltung entspricht den Anforderungen des Typs IIIC nach EN574 bzw. EN ISO 13851.



Sicherheitsgerichtete Komponenten

Zweihandbedienpult	Sicherheitsschaltgerät	Schütz
		
3SU18 (http://www.siemens.de/sirius-command)	3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109479279>)

Einsatz des Sensortasters im Zweihandbedienpult (<http://support.automation.siemens.com/WW/view/de/109479531>)

3.7 Typische Kombinationen mehrerer Sicherheitsfunktionen

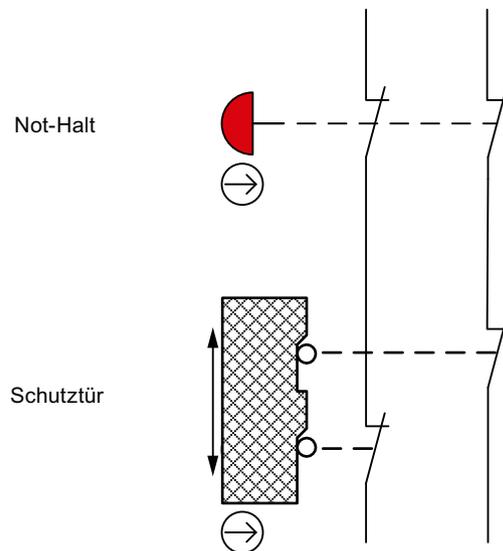
3.7.1 Einleitung

In den seltensten Fällen genügt es, an einer Maschine nur eine Sicherheitsfunktion umzusetzen. Häufig werden verschiedene Sicherheitsfunktionen aus den vorangegangenen Kapiteln gleichzeitig an einer Maschine umgesetzt, um das nötige Maß an Sicherheit zu erreichen.

Im folgenden Kapitel werden Applikationsbeispiele gezeigt, die typische Kombinationen von Sicherheitsfunktionen beinhalten.

Bedingungen bei Reihenschaltung von Not-Halt-Befehlsgeräten und Schutztürüberwachung mit Positionsschaltern

Not-Halt-Befehlsgeräte und Positionsschalter dürfen bis PL d (nach ISO 13849) bzw. SIL 2 (nach IEC 62061) in Reihe geschaltet werden, wenn ausgeschlossen werden kann, dass nicht das Not-Halt-Befehlsgerät und die Schutztür gleichzeitig betätigt werden (da sonst keine Fehleraufdeckung erfolgen kann).



Kopplung bzw. Kaskadierung von Sicherheitsfunktionen

Sollen zwei oder mehrere Anlagenteile miteinander gekoppelt werden, d. h. die Anforderung einer Sicherheitsfunktion in einem Anlagenteil löst die Anforderung einer Sicherheitsfunktion im anderen Anlagenteil aus, muss die Übertragung des Signals denselben Anforderungen an die Sicherheitsfunktion im betroffenen Anlagenteil genügen.

Beispiel:

In beiden Anlagenteilen wird ein Not-Halt-Befehlsgerät überwacht. Die Not-Halt-Funktion in Anlagenteil 1 ist nach SIL 3 bzw. PL e ausgelegt und die in Anlagenteil 2 nach SIL 2 bzw. PL d.

3.7 Typische Kombinationen mehrerer Sicherheitsfunktionen

Während sich ein Not-Halt-Befehl, ausgelöst im Anlagenteil 2, nur auf diesen Anlagenteil auswirkt, soll ein Not-Halt-Befehl, ausgelöst im Anlagenteil 1, beide Anlagenteile sicher stillsetzen.

Da die Risikobeurteilung für Anlagenteil 2 ein SIL 2 bzw. PL d fordert, muss die Signalübertragung des Not-Halt-Befehls aus Anlagenteil 1 mindestens diesem Sicherheitslevel entsprechen. Die Signalleitungen müssen demnach querschlussicher verlegt oder das Signal über eine sichere Kommunikation (zum Beispiel ASIsafe) übertragen werden.

Grundsätzlich gilt, dass der Gefahrenbereich von der Position, von der der Start-/Wiederanlaufbefehl erfolgt, gut einsehbar sein muss. Ob nun jeder Anlagenteil einen eigenen Starttaster benötigt, ist abhängig von der Anlage und der Risikobeurteilung.

Hinweis

Die Kopplung innerhalb eines Schaltschranks darf 1-kanalig realisiert werden, was selbst bis SIL 3 bzw. PL e zulässig ist, da die Kabelverlegung innerhalb eines Schaltschranks als P-Schlussicher/kurzschlussicher gilt (Fehlerrückmeldung gemäß ISO 13849-2).

3.7.2 Sichere Temperaturüberwachung bis SIL 1 bzw. PL c mit einem Temperaturüberwachungsrelais 3RS2

Anwendung

Die Temperatur von Körpern, die eine entsprechende Wärme entwickeln können und frei zugänglich sind, muss überwacht werden. Das 3RS2 schaltet bei Überschreitung eines definierten Temperaturgrenzwertes über ein Schütz den überhitzten Motor sicherheitsgerichtet ab.

Aufbau

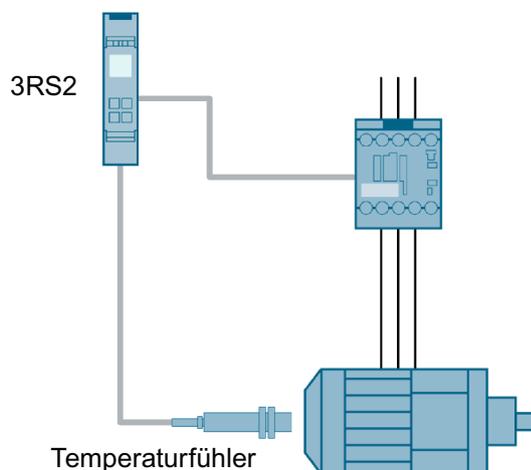


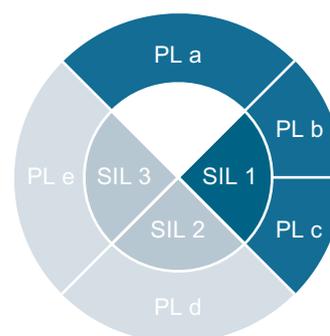
Bild 3-46 Sichere Temperaturüberwachung bis SIL 1 bzw. PL c mit einem Temperaturüberwachungsrelais 3RS2

Funktionsweise

Laut EN ISO 12100, Anhang B, besteht die mögliche Gefährdung „Verbrennung durch Kontakt mit Material hoher Temperatur“, die während der Risikobeurteilung bewertet und gegebenenfalls reduziert werden muss. Die Temperatur von Körpern, die eine entsprechende Wärme entwickeln können und frei zugänglich sind, muss überwacht werden. Das 3RS2 schaltet bei Überschreitung eines definierten Temperaturgrenzwertes direkt über ein Schütz den überhitzten Motor sicherheitsgerichtet bis SIL 1 / PL c ab, ohne dass ein zwischengeschaltetes Sicherheitsschaltgerät benötigt wird.

Bei dem hier verwendeten Temperaturüberwachungsrelais handelt es sich um ein 3RS26 oder 3RS28 der 3RS2-Reihe. Diese beiden Gerätetypen können in Safety Applikationen bis SIL 1 / PL c eingesetzt werden.

Weitere Informationen zur Parametrierung der Temperaturüberwachungsrelais 3RS2 sind dem Handbuch (<https://support.industry.siemens.com/cs/de/de/view/109772132>) zu entnehmen.



Sicherheitsgerichtete Komponenten

Temperaturüberwachungsrelais	Schütz
	
<p>3RS2 (http://www.siemens.de/relais)</p>	<p>3RT20 (http://www.siemens.de/sirius-control)</p>

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109780387>)

3.7.3 Sichere Temperaturüberwachung und Schutztürüberwachung mit Zuhaltung bis SIL 1 bzw. PL c mit einem Temperaturüberwachungsrelais 3RS2 und Sicherheitsschaltgerät 3SK2

Anwendung

Der Zugang zu einem Bereich mit Körpern, die eine entsprechende Wärme entwickeln können, wird durch eine Umhausung mit Schutztür verhindert. Das 3SK2 überwacht die Stellung der Schutztür und schaltet bei einer Zugangsanforderung den Motor sicherheitsgerichtet ab. Die Zuhaltung der Schutztür wird durch das 3SK2 solange aufrechterhalten, bis das 3RS2 die Unterschreitung eines definierten Temperaturgrenzwertes an das 3SK2 meldet.

Aufbau

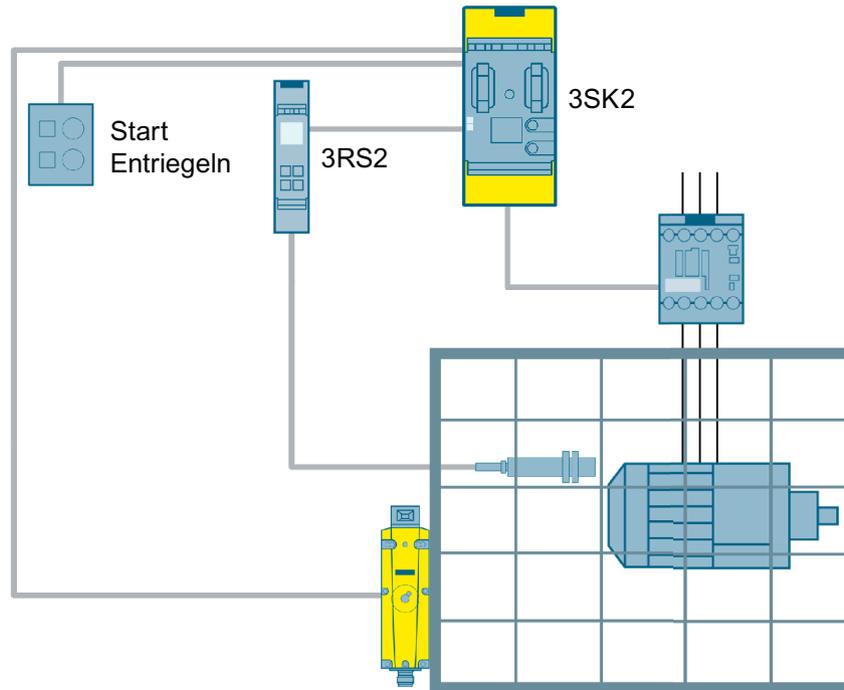


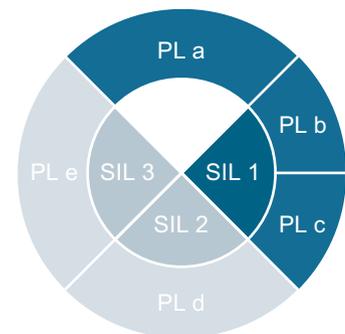
Bild 3-47 Sichere Temperaturüberwachung und Schutztürüberwachung mit Zuhaltung bis SIL 1 bzw. PL c mit einem Temperaturüberwachungsrelais 3RS2 und Sicherheitschaltgerät 3SK2

Funktionsweise

Laut EN ISO 12100, Anhang B, besteht die mögliche Gefährdung „Verbrennung durch Kontakt mit Material hoher Temperatur“, die während der Risikobeurteilung bewertet und gegebenenfalls reduziert werden muss. Körper, die eine entsprechende Wärme entwickeln können, werden eingehaust. Z.B. zu Servicearbeiten muss der Bereich allerdings über eine Schutztür zugänglich sein. Bei einer Zugangsanforderung schaltet das Sicherheitschaltgerät 3SK2 den Motor über ein Schütz sicherheitsgerichtet ab. Das 3RS2 meldet die Unterschreitung eines definierten Temperaturgrenzwertes an das 3SK2 sicherheitsgerichtet bis SIL 1 / PL c. Das 3SK2 schaltet anschließend die Schutztür frei und der Bereich kann vom Servicepersonal betreten werden.

Bei dem hier verwendeten Temperaturüberwachungsrelais handelt es sich um ein 3RS26 oder 3RS28 der 3RS2-Reihe. Diese beiden Gerätetypen können in Safety Applikationen bis SIL 1 / PL c eingesetzt werden

Weitere Informationen zur Parametrierung der Temperaturüberwachungsrelais 3RS2 sind dem Handbuch (<https://support.industry.siemens.com/cs/de/de/view/109772132>) zu entnehmen.



Sicherheitsgerichtete Komponenten

Sicherheitsschalter mit Zuhaltung	Temperaturüberwachungsrelais	Sicherheitsschaltgerät	Schütz
			
2x 3SE5 (http://www.siemens.de/sirius-erfassen)	3RS2 (http://www.siemens.de/relais)	3SK2 (http://www.siemens.de/safety-relays)	3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109780388>)

3.7.4 Sichere Stromüberwachung inkl. Not-Halt-Abschaltung bis PL d mit einem Sicherheitsschaltgerät 3SK2 und zwei Stromüberwachungsrelais

Anwendung

Die Stromaufnahme z. B. eines Lüftermotors steigt mit zunehmender Verstopfung des Filters. Es gilt beim Überschreiten eines eingestellten Grenzwertes den Antrieb sicher abzuschalten. Die Stromaufnahme wird mithilfe von zwei Stromüberwachungsrelais mit diversitären Technologien (3UG4 und 3RR2) und einem Sicherheitsschaltgerät 3SK2 überwacht. Zusätzlich wird zum Abschalten des Motors im Notfall ein Not-Halt-Befehlsgerät überwacht.

Aufbau

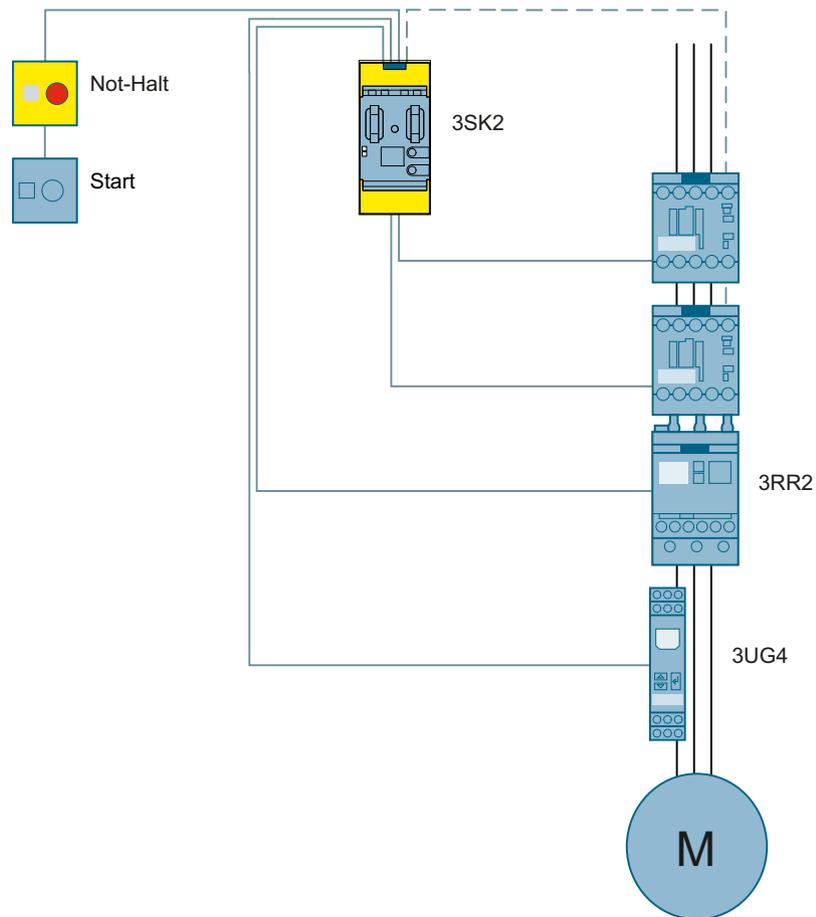


Bild 3-48 Sichere Stromüberwachung inkl. Not-Halt-Abschaltung bis PL d mit einem Sicherheitsschaltgerät 3SK2 und zwei Stromüberwachungsrelais

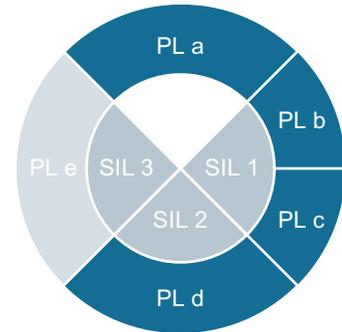
Funktionsweise

Durch den redundanten Einsatz von zwei Standard-Stromüberwachungsrelais mit diversitären Technologien ist es möglich bis zu PL d zu erreichen. Dabei wird an den beiden Stromüberwachungsrelais 3UG4 und 3RR2 eine bestimmte Stromgrenze bzw. ein bestimmter Strombereich (Ober- und Untergrenze) eingestellt. Diese überwachen die Stromaufnahme des Motors kontinuierlich und geben das Einhalten bzw. Überschreiten der Grenze bzw. des Bereichs über Relaiskontakte aus.

Das Sicherheitsschaltgerät wiederum überwacht die Signale der Stromüberwachungsrelais sowie die beiden Not-Halt-Kontakte auf Diskrepanz sowie Querschluss. Überschreitet die Stromaufnahme des Motors die Stromgrenze bzw. verlässt den Strombereich oder wird das Not-Halt-Befehlsgerät betätigt, wird der Motor sofort sicherheitsgerichtet abgeschaltet.

Ist die Stromaufnahme des Motors wieder unter die Stromgrenze gefallen bzw. befindet sich innerhalb des Strombereichs, ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Dieses Beispiel wurde mit PL d nach ISO 13849-1 bewertet. Diese Bewertung ist nicht direkt in einen SIL nach IEC 62061 übertragbar.



Hinweis

Werden zwei redundante Überwachungsrelais im Sensorkreis zur Erfassung von Prozessgrößen verwendet, kann es gegebenenfalls dazu führen, dass ein Überwachungsrelais eine Grenzwertüberschreitung vor dem Anderen erkennt. Ursächlich dafür können Einstell- und Messabweichungen der Geräte sein.

In dem oben aufgeführten Beispiel könnte bei einem kontinuierlichen Anstieg des Stromes ein Überwachungsrelais die Grenzwertüberschreitung kurz vor dem Zweiten erkennen. In diesem Fall wird die Energieversorgung des Antriebs abgeschaltet. Aufgrund des notwendigen Kreuzvergleichs der Eingänge in der sicherheitsgerichteten Auswertung bleibt ein Diskrepanzfehler anstehen. Ein Wiedereinschalten der Applikation ist erst nach einem Null-Durchgang beider Kanäle möglich. In diesem Fall müssen die Überwachungsrelais überprüft und manuell zurückgesetzt werden.

Dieses Verhalten kann bei der Überwachung von langsam ansteigenden Prozessgrößen auftreten. Eine Möglichkeit zur Vermeidung eines Diskrepanzfehlers ist z. B. eine empirische Ermittlung der Einstellparameter zur Synchronisation der Überwachungsrelais.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Stromüberwachungsrelais		Sicherheitschaltgerät	Schütz
				
3SU1 (http://www.siemens.de/sirius-act)	3UG4 und 3RR2 (http://www.siemens.de/sirius-monitor)		3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109747652>)

Schreiben zum Einsatz von Überwachungsrelais in Sicherheitsanwendungen (<http://support.automation.siemens.com/WW/view/de/39863898>)

3.7.5 Not-Halt- und Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitschaltgerät 3SK1

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet. Zusätzlich wird zum Abschalten der Maschine im Notfall ein Not-Halt-Befehlsgerät überwacht.

Aufbau

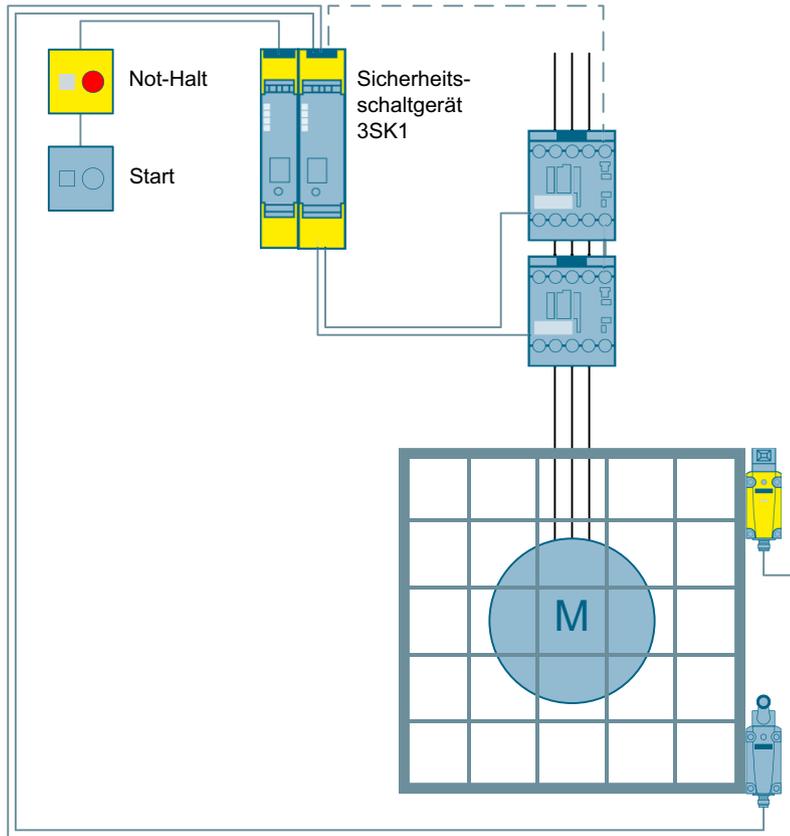
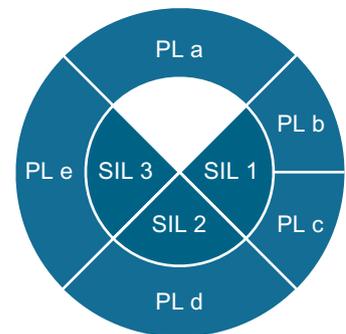


Bild 3-49 Not-Halt- und Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Funktionsweise

Das Sicherheitsschaltgerät überwacht die beiden Sicherheitsschalter sowie die beiden Not-Halt-Kontakte über eine zusätzliche Eingangserweiterung. Bei Betätigung des Not-Halt-Befehlsgerätes oder Öffnen der Schutztür öffnet das Sicherheitsschaltgerät die Freigabekreise und schaltet die Leistungsschütze sicherheitsgerichtet ab.

Ist die Tür geschlossen, das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehls- gerät	Positionsschalter		Sicherheitschalt- gerät	Eingangserweite- rung	Schütz
					
3SU1 (http://www.siemens.de/sirius-act)	2x 3SE5 (http://www.siemens.de/sirius-erfassen)		3SK1 (http://www.siemens.de/safety-relays)	3SK1 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/74562495>)

3.7.6 Not-Halt- und Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitschaltgerät 3SK2

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet. Zusätzlich wird zum Abschalten der Maschine im Notfall ein Not-Halt-Befehlsgerät überwacht.

Aufbau

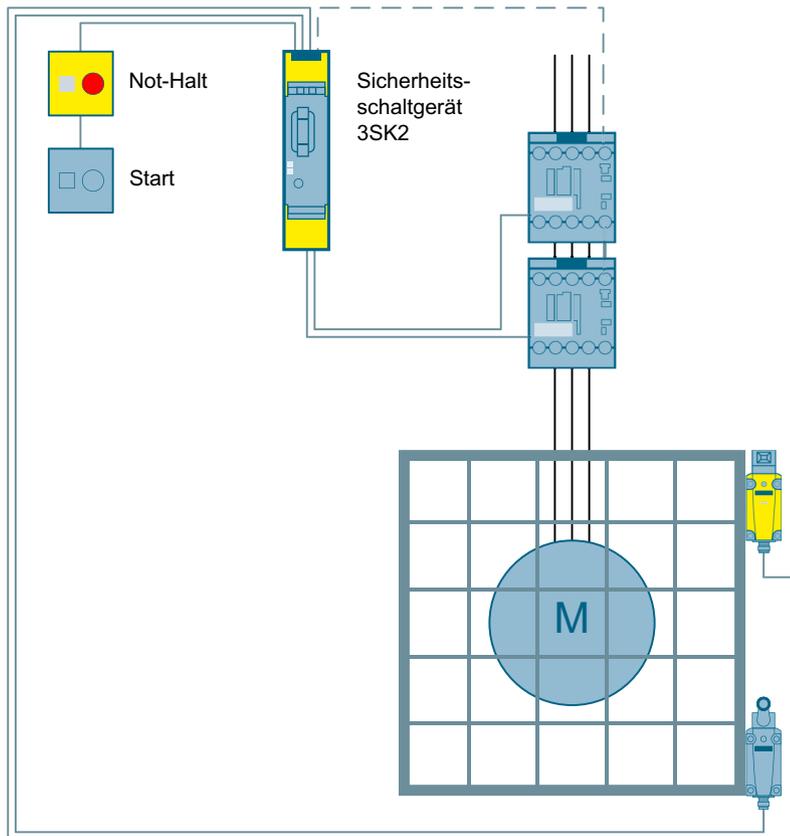
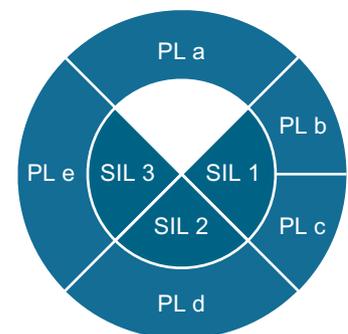


Bild 3-50 Not-Halt- und Schutztürüberwachung bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

Das Sicherheitsschaltgerät überwacht die beiden Sicherheitsschalter sowie das Not-Halt-Befehlsgerät zweikanalig. Bei Betätigung des Not-Halt-Befehlsgerätes oder Öffnen der Schutztür öffnet das Sicherheitsschaltgerät die Freigabekreise und schaltet die Leistungsschütze sicherheitsgerichtet ab.

Ist die Tür geschlossen, das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Positionsschalter		Sicherheitschaltgerät	Schütz
				
3SU1 (http://www.siemens.de/sirius-act)	2x 3SE5 (http://www.siemens.de/sirius-erfassen)		3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109479280>)

3.7.7 Zugangüberwachung durch einen Lichtvorhang mit Zweihandbedienung und Not-Halt bis SIL 3 bzw. PL e mit einem Sicherheitschaltgerät 3SK2

Anwendung

Um den Zugang zu einem offenen Gefahrenbereich zu überwachen, können sogenannte berührungslos wirkende Schutzzeineinrichtungen, wie zum Beispiel ein Lichtvorhang, eingesetzt werden. Bei Unterbrechung des Lichtwegs wird ein Abschaltsignal ausgelöst.

Um den Aktor sicher verfahren zu können, kommt eine Zweihandbedienung zum Einsatz. Dadurch wird verhindert, dass der Bediener während des Betriebs in den Gefahrenbereich greifen kann.

Aufbau

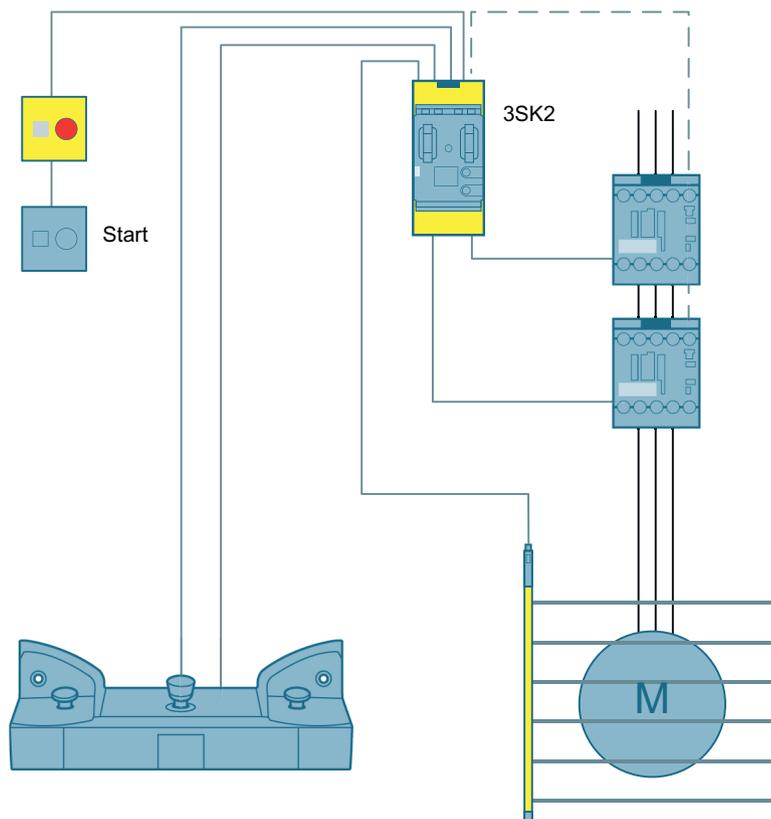


Bild 3-51 Zugangüberwachung durch einen Lichtvorhang mit Zweihandbedienung und Not-Halt bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK2

Funktionsweise

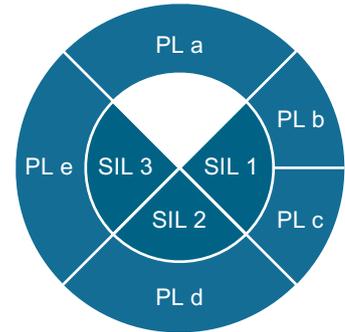
Der Lichtvorhang besteht aus einer Sende- und einer Empfangseinheit. Zwischen den beiden liegt das Schutzfeld. Ist der Lichtweg nicht unterbrochen, führen die Ausgänge OSSD1 und OSSD2 Spannung und werden von dem Sicherheitsschaltgerät ausgewertet. Bei einer Unterbrechung des Lichtwegs schalten die beiden Ausgänge ab und das Sicherheitsschaltgerät öffnet die Freigabekreise, wodurch die Leistungsschütze sicherheitsgerichtet abgeschaltet werden.

Zusätzlich wird durch die Bedienung der simultanen Betätigung am Zweihandbedienpult das Hineingreifen in den Gefahrenbereich untersagt. Das Sicherheitsschaltgerät 3SK2 schaltet die Freigabekreise nur wenn beide Signale innerhalb von 500ms anliegen, der Lichtweg des Lichtvorhangs ununterbrochen und der Rückführkreis geschlossen ist.

Bei Loslassen einer der beiden Taster schaltet das Sicherheitsschaltgerät 3SK2 die Maschine sofort sicherheitsgerichtet ab.

Durch einen vierkanaligen Aufbau im Zweihandbedienpult wird sichergestellt, dass ein mögliches Verschweißen einer der Kontakte unmittelbar erkannt wird.

Ebenso wird nach Betätigung beider Not-Halt-Befehlsgeräte die Anlage sicherheitsgerichtet abgeschaltet.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Lichtvorhang	Zweihandbedienpult	Sicherheitsschaltgerät	Schütz
				
3SU1 (2-kanalig) (http://www.siemens.de/sirius-act)	SICK C4000	3SU18 (http://www.siemens.de/sirius-command)	3SK2 (http://www.siemens.de/safety-relays)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109485648>)

3.7.8 Kaskadierung von Sicherheitsschaltgeräten 3SK1 bis SIL 3 bzw. PL e

Anwendung

Die Kaskadierung von Sicherheitsschaltgeräten dient dazu, mehrere Sicherheitsschaltgeräte in Reihe zu schalten. Somit können mehrere Sicherheitsfunktionen mit gemeinsamem Abschaltpfad logisch verknüpft werden. Gleichzeitig können für eine selektive Abschaltung von Antriebselementen mehrere Freigabekreise erzeugt werden.

Aufbau

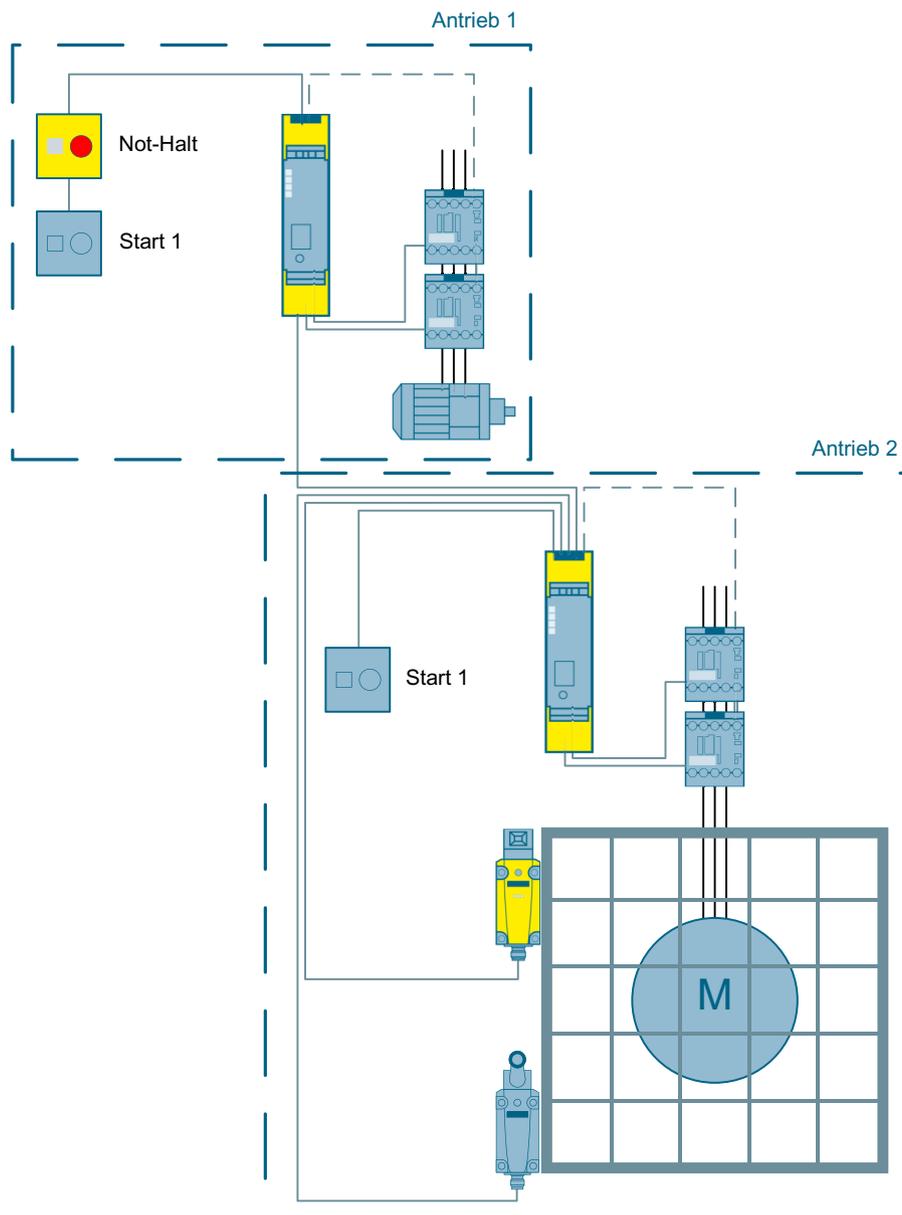
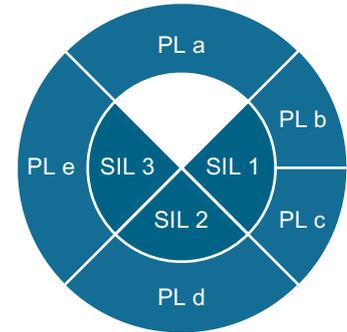


Bild 3-52 Kaskadierung von Sicherheitsschaltgeräten 3SK1 bis SIL 3 bzw. PL e

Funktionsweise

Die beiden dargestellten Sicherheitsschaltgeräte sind über den Kaskadiereingang miteinander verknüpft. Wird der Not-Halt am ersten Sicherheitsschaltgerät ausgelöst, schalten daraufhin beide Sicherheitsschaltgeräte ihre Aktoren ab. Hingegen wird bei Öffnen der dargestellten Schutzhaube zum Beispiel nur die dahinterliegende Aktorik abgeschaltet.

Wurde ein Not-Halt durch das übergeordnete Sicherheitsschaltgerät ausgelöst, muss das untergeordnete Sicherheitsschaltgerät manuell durch den Starttaster wieder eingeschaltet werden. Ein globaler Starttaster ist nur dann möglich, wenn alle Gefahrenbereiche von diesem Starttaster einsehbar sind.



Hinweis

Dieses Beispiel gilt für den Aufbau innerhalb eines Schaltschranks. Befinden sich die beiden Sicherheitsschaltgeräte nicht im selben Schaltschrank, sind weitere Vorkehrungen zu treffen, wie zum Beispiel eine querschluss sichere Verlegung des Kaskadiersignals.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschalter	Sicherheitsschaltgerät	Schütz
			
3SU1 (http://www.siemens.de/sirius-act)	2x 3SE5 (http://www.siemens.de/sirius-erfassen)	2x 3SK1 (http://www.siemens.de/safety-relays)	4x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/77282496>)

3.7.9 Sicherer Querverkehr zwischen mehreren Anlagenteilen bis SIL 3 bzw. PL e über AS-i

Anwendung

Um mehrere Anlagenteile logisch miteinander zu verknüpfen, wird ein Querverkehr benötigt. Dieser soll fehlersicher ausgelegt werden, um auch sichere Abschaltsignale zu übertragen. Das Modulare Sicherheitssystem bietet mit AS-i eine solche Möglichkeit.

Aufbau

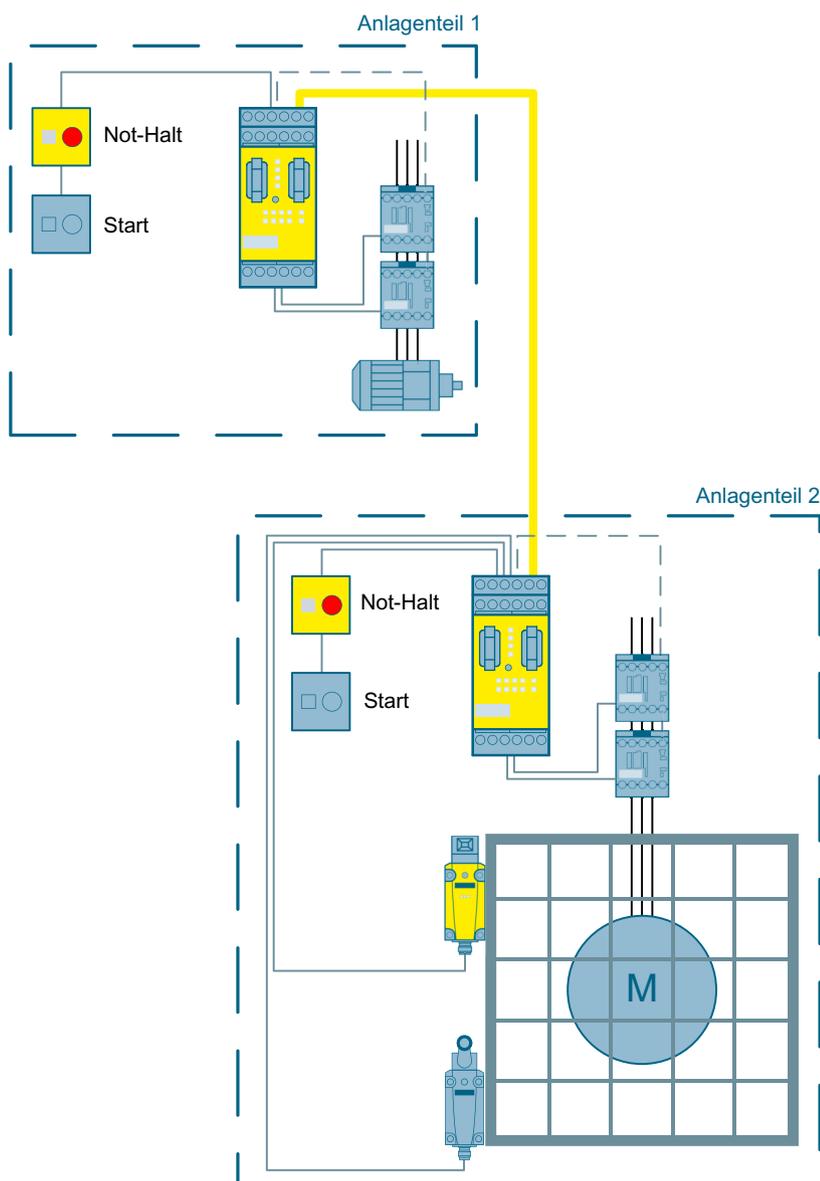
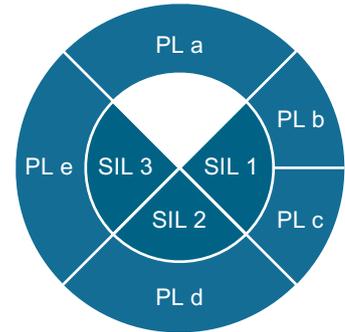


Bild 3-53 Sicherer Querverkehr zwischen mehreren Anlagenteilen bis SIL 3 bzw. PL e über AS-i

Funktionsweise

Die beiden Anlagenteile sind aufgrund des Prozesses voneinander abhängig. Wird in einem der beiden Anlagenteile ein Abschalten der Maschine eingeleitet, wird dieser Abschaltbefehl über den sicheren Querverkehr mittels AS-i an das Modulare Sicherheitssystem im anderen Anlagenteil weitergeleitet.

Zusätzlich können auch Diagnoseinformationen und Meldesignale zwischen den beiden Anlagenteilen ausgetauscht werden.



Hinweis

Ob mit einem Starttaster beide Anlagenteile wieder eingeschaltet werden können oder für jeden Anlagenteil ein eigener Starttaster notwendig ist, ist abhängig von der Anlage und der Risikobeurteilung.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschalter	Modulares Sicherheitssystem	Schütz
			
2x 3SU1 (http://www.siemens.de/sirius-act)	2x 3SE5 (http://www.siemens.de/sirius-erfassen)	2x 3RK3 (http://www.siemens.de/sirius-monitor)	4x 3RT20 (http://www.siemens.de/sirius-control)

Hinweis

Zusätzlich zu den sicherheitsgerichteten Komponenten werden zum Betrieb eines AS-i-Netzwerks ein AS-i-Master sowie ein AS-i-Netzteil benötigt.

Siehe auch

MSS-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/88823146>)

Ausführlicher FAQ zum Thema: Sicherer Querverkehr (<http://support.automation.siemens.com/WW/view/de/58512565>)

3.7.10 Schutztürüberwachung mittels Magnetschalter und Not-Halt-Abschaltung mittels Seilzugschalter bis SIL3 bzw. PL e über AS-i ET 200SP Master und AS-i SlimLine Compact Module

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden mittels Magnetschalter 3SE6 auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet. Zusätzlich wird zum Abschalten der Maschine im Notfall ein Seilzugschalter 3SE7 überwacht. Zur Anbindung an die fehlersichere Steuerung werden AS-Interface SlimLine Compact Module sowie CM AS-i Master und F-CM AS-i Safety eingesetzt.

Aufbau

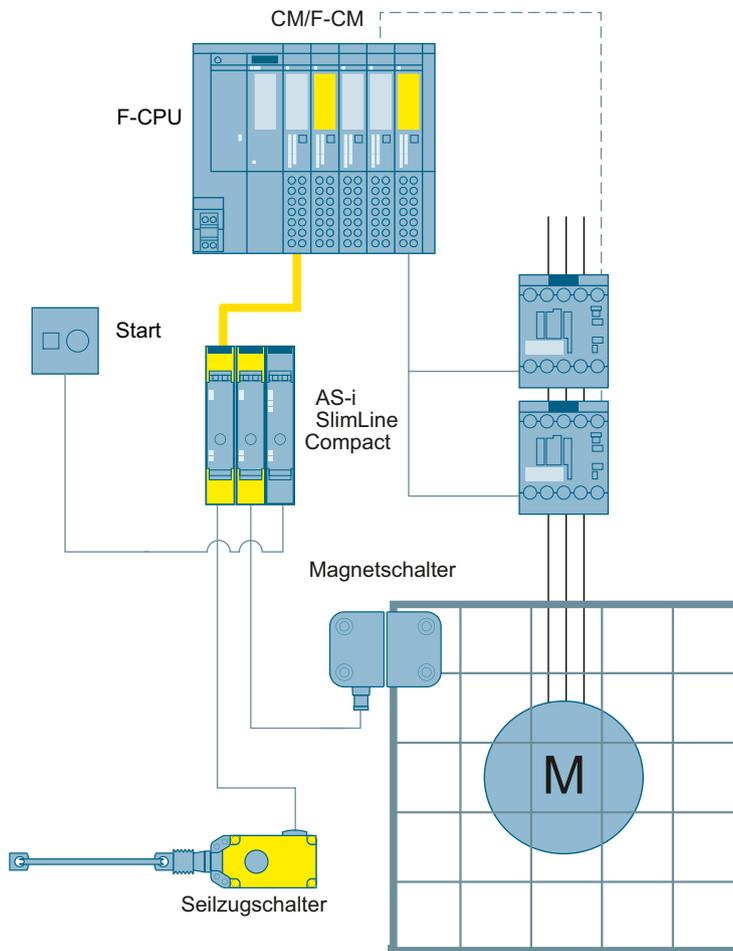
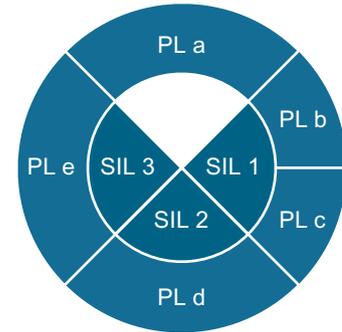


Bild 3-54 Schutztürüberwachung mittels Magnetschalter und Not-Halt-Abschaltung mittels Seilzugschalter bis SIL 3 bzw. PL e über AS-i ET 200SP Master und AS-i SlimLine Compact Module

Funktionsweise

Die fehlersichere Steuerung überwacht den zweikanaligen Magnetschalter sowie den zweikanaligen Seilzugschalter. Beide Signale werden über das ASIsafe SlimLine Compact Modul eingelesen. Anschließend werden sie mit Hilfe des CM AS-i Master und des F-CM AS-i Safety Moduls (Module der ET 200SP Station) an die fehlersichere Steuerung übergeben. Bei Betätigung des Seilzugschalters oder Öffnen der Schutztür schaltet die fehlersichere Steuerung die Leistungsschütze sicherheitsgerichtet ab. Ist die Tür geschlossen, der Seilzugschalter rückgestellt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden. Der Starttaster wird ebenfalls über ein AS-i SlimLine Compact Modul eingelesen. Die drei AS-i SlimLine Compact Modul sind über Geräteverbinder miteinander verbunden, so dass das AS-i Flachbandkabel nur einmal angeschlossen werden muss.



Sicherheitsgerichtete Komponenten

Sicherheitsschalter	Magnetschalter	AS-i SlimLine Compact	
			
3SE7 (http://www.siemens.de/sirius-command)	3SE6 (http://www.siemens.de/sirius-erfassen)	3x AS-i Modul (http://www.siemens.de/as-interface)	

Steuerung Failsafe	ET 200SP AS-i Master		Schütz
			
S7 F-PLC (http://www.siemens.de/simatic-safety)	CM AS-i Master und F-CM (http://www.siemens.de/as-interface)		2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, TIA Portal-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109747653>)

Schreiben zum Einsatz von Seilzugschaltern in Sicherheitsfunktionen (<https://support.industry.siemens.com/cs/ww/de/view/69778886>)

3.7.11 Not-Halt-Abschaltung bis SIL 3 bzw. PL e und Schutztürüberwachung bis SIL 2 bzw. PL d mit Zuhaltung über AS-i ET 200SP Master

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet. Zur Sicherstellung des Produktionsprozesses kann der Zugang durch eine Zuhaltung solange verhindert werden. Zusätzlich wird zum Abschalten der Maschine im Notfall ein Not-Halt-Befehlsgerät überwacht. Zur Anbindung an die fehlersichere Steuerung werden CM AS-i Master und F-CM AS-i Safety eingesetzt.

Aufbau

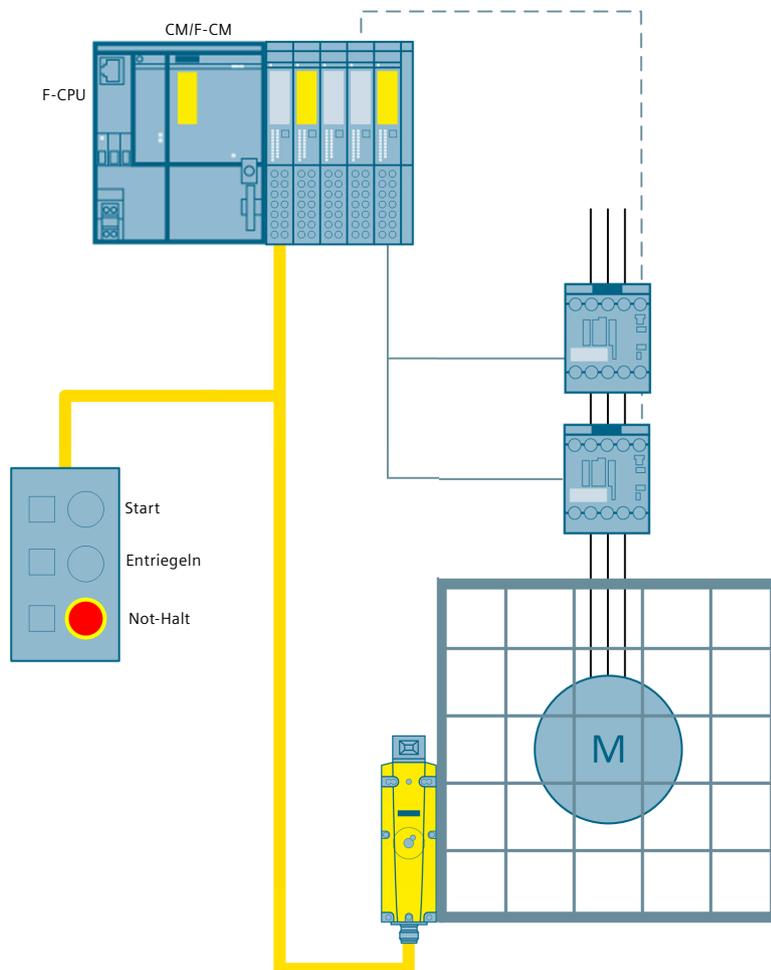
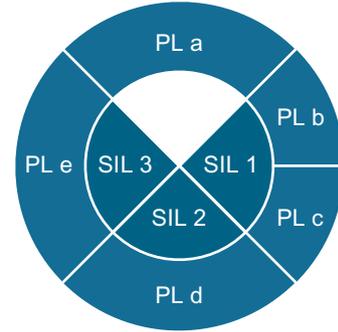


Bild 3-55 Not-Halt-Abschaltung bis SIL 3 bzw. PL e und Schutztürüberwachung bis SIL 2 bzw. PL d mit Zuhaltung über AS-i ET 200SP Master

Funktionsweise

Die fehlersichere Steuerung überwacht das Not-Halt-Befehlsgerät sowie den Sicherheitsschalter zweikanalig. Beide Geräte besitzen einen integrierten AS-i Slave und sind dadurch an das AS-Interface angebunden. Die beiden Signale werden mit Hilfe der Kombination aus CM AS-i Master und F-CM AS-i Safety (Module der ET 200SP Station) an die fehlersichere Steuerung übergeben. Über einen Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Zusätzlich wird über eine im Sicherheitsschalter integrierte Zuhaltung die Tür verriegelt. Wird der Befehl zur Türfreigabe über einen Knebelschalter gegeben, schaltet die fehlersichere Steuerung die Leistungsschütze sicherheitsgerichtet ab. Nach Ablauf einer eingestellten Zeit wird die Zuhaltung entriegelt und der Zugang zur Maschine freigegeben. Nachdem die Tür wieder geschlossen und verriegelt wurde und der Rückführkreis geschlossen ist, kann durch den Starttaster wieder eingeschaltet werden. Bei Betätigung des Not-Halt-Befehlsgerätes schaltet die fehlersichere Steuerung die Leistungsschütze ebenfalls sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät rückgestellt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden. Starttaster und Knebelschalter werden ebenfalls über AS-Interface eingelesen.



Die Sicherheitsfunktion "Stillsetzen im Notfall" ist bis SIL 3 bzw. PL e ausgelegt. Die Sicherheitsfunktion „Schutztürüberwachung“ ist bis SIL 2 bzw. PL d ausgelegt. Die Schutztürzuhaltung ist keine Sicherheitsfunktion (nicht sichere Ansteuerung des Magneten). Sie ist einsetzbar zur Sicherstellung des Produktionsprozesses.

Unter Berücksichtigung von Fehlerausschlüssen ist der Einsatz von nur einem Sicherheitsschalter mit oder ohne Zuhaltung bis SIL 2 bzw. PL d zulässig. Weitere Informationen entnehmen Sie dem unten aufgeführten Schreiben.

Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Positionsschalter	Steuerung Failsafe
		
3SU1 (http://www.siemens.de/sirius-act)	3SF1 (http://www.siemens.de/sirius-erfassen)	S7 F-PLC (http://www.siemens.de/simatic-safety)

ET 200SP AS-i Master		Schütz
		
CM AS-i Master und F-CM (http://www.siemens.de/as-interface)		2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, TIA Portal-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109769506>)

Schreiben zum Einsatz von Sicherheitsschaltern bis SIL 2 bzw. PL d (<http://support.automation.siemens.com/WW/view/de/35443942>)

3.7.12 Not-Halt-Abschaltung und Schutztürüberwachung bis SIL 3 bzw. PL e über ET 200ecoPN und F-CPU

Anwendung

Zur Abgrenzung von Gefahrenbereichen werden häufig Schutztüren eingesetzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem die Gefahr ausgeht, abgeschaltet. Zusätzlich wird zum Abschalten der Maschine im Notfall ein Not-Halt-Befehlsgerät überwacht. Zum Erfassen dieser beiden Sicherheitsfunktionen im IP67-Umfeld kommt eine ET 200eco PN in fehlersicherer Ausführung zum Einsatz.

Aufbau

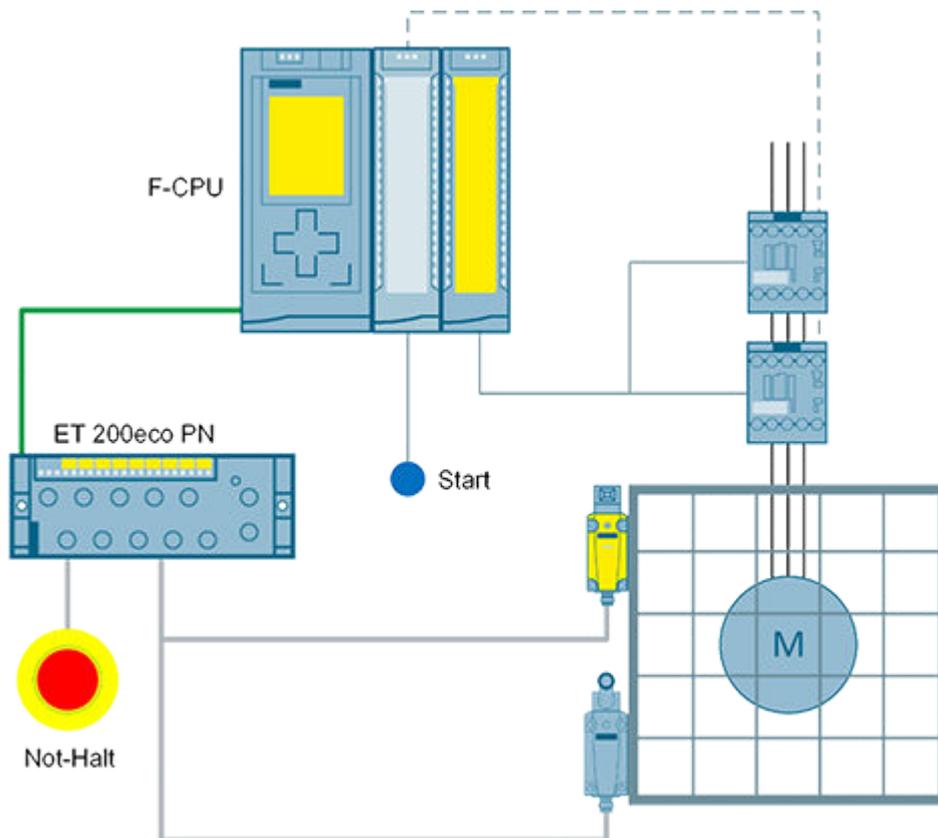
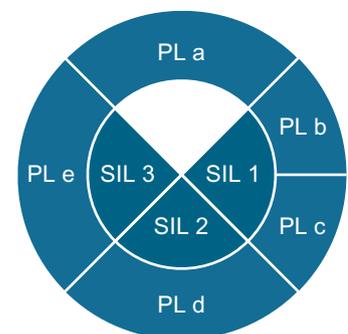


Bild 3-56 Not-Halt-Abschaltung und Schutztürüberwachung bis SIL 3 bzw. PL e über ET 200ecoPN und F-CPU

Funktionsweise

Das Not-Halt-Befehlsgerät wird direkt über ein M12-Kabel mit einer fehlersicheren Eingangsbuchse (F-DI) der ET 200eco PN verbunden. Die beiden Positionsschalter werden über ein spezielles M12-Y-Kabel zusammengeführt und ebenfalls direkt mit einer einzelnen F-DI der ET 200eco PN verbunden. Die fehlersichere Steuerung (F-CPU) überwacht die beiden Sicherheitsschalter sowie das Not-Halt-Befehlsgerät zweikanalig. Bei Betätigung des Not-Halt-Befehlsgerätes oder Öffnen der Schutztür schaltet die fehlersichere Steuerung die Leistungsschütze sicherheitsgerichtet ab. Ist die Tür geschlossen, das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Positionsschalter		Steuerung Failsafe
			
3SU1 (http://www.siemens.de/sirius-act)	2x3SE5 (http://www.siemens.de/sirius-erfassen)		ET 200eco PN (http://www.siemens.de/simatic-safety)

Verbindungskabel	Steuerung Failsafe	Schütz
		
Y-Kabel für ET 200eco PN (http://www.siemens.de/simatic-safety)	S7 F-PLC (http://www.siemens.de/simatic-safety)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, TIA Portal-Projekt und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/109769505>)

3.7.13 Not-Halt-Abschaltung mehrerer Motoren bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1, Ausgangserweiterung und Koppelrelais 3RQ1

Anwendung

Sollen aufgrund einer Sicherheitsanforderung mehrere Antriebe gleichzeitig abgeschaltet werden (z. B. Werkzeugschlitten, Maschinenwerkzeug, Absaugvorrichtung usw.), kann dies mithilfe von Ausgangserweiterungen oder Koppelrelais mit zusätzlichen Freigabekreisen erfolgen.

Aufbau

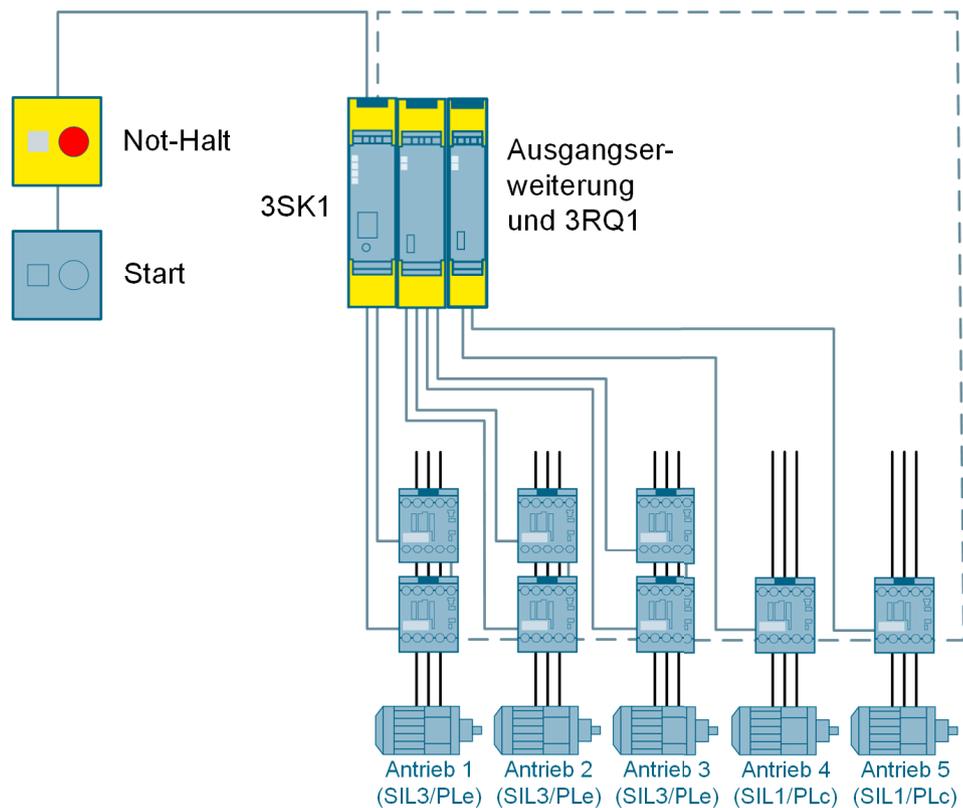


Bild 3-57 Not-Halt-Abschaltung mehrerer Motoren bis SIL 3 bzw. PL e mit einem Sicherheitsschaltgerät 3SK1

Funktionsweise

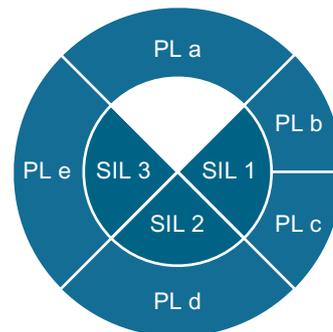
Das Sicherheitsschaltgerät überwacht das Not-Halt-Befehlsgerät zweikanalig. Bei Betätigung des Not-Halt-Befehlsgerätes öffnen das Sicherheitsschaltgerät, die 3SK1 Ausgangserweiterung und das Koppelrelais die Freigabekei-
 reise und schalten die Leistungsschütze sicherheitsgerichtet ab. Ist das Not-Halt-Befehlsgerät entriegelt und der Rückführkreis aller Aktoren geschlossen, kann durch den Starttaster wieder eingeschaltet werden.

Das Abschalten der einzelnen Antriebe stellt jeweils eine eigene Sicherheitsfunktion dar, auch wenn der Abschaltbefehl von demselben Not-Halt-Befehlsgerät und Sicherheitsschaltgerät stammt.

Die sicherheitsgerichtete Abschaltung der Antriebe 1, 2 und 3 direkt über das Sicherheitsschaltgerät 3SK1 bzw. über dessen Ausgangserweiterung und jeweils zwei redundante Schütze ist bis SIL 3 bzw. PL e ausgelegt. Eine Rückführkreisüberwachung der Schütze ist zur Erreichung dieser Sicherheitsintegrität obligatorisch.

Die sicherheitsgerichtete Abschaltung der Antriebe 4 und 5 über das Koppelrelais 3RQ1 und jeweils ein Schütz ist bis SIL 1 bzw. PL c ausgelegt. Das Koppelrelais 3RQ10 allein ist bis SIL 2 bzw. PL c zugelassen. Um diese Sicherheitslevel zu erreichen, muss allerdings zusätzlich auf eine entsprechende Auslegung des Schützes geachtet werden (z.B. redundanter Aufbau).

Das Koppelrelais 3RQ1 ist auch als Variante 3RQ12 verfügbar, die bis SIL 3 bzw. PL e zertifiziert ist.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Sicherheitsschaltgerät	Ausgangserweiterung	Koppelrelais	Schütz
				
3SU1 (2-kanalig) (http://www.siemens.de/sirius-act)	3SK1 (http://www.siemens.de/safety-relays)	3SK1 (http://www.siemens.de/safety-relays)	3RQ1 (http://www.siemens.de/relais)	3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan und Safety Evaluation (<http://support.automation.siemens.com/WW/view/de/74563681>)

Kontakterweiterung einer fehlersicheren Steuerung mit 3SK1 und 3RQ1 (<https://support.industry.siemens.com/cs/de/de/view/76676971>)

3.7.14 Schutztürüberwachung mit Zuhaltung mittels RFID-Sicherheitsschalter 3SE64 inklusive Not-Halt-Abschaltung bis SIL 3 bzw. PL e über ET 200AL und F-CPU

Anwendung

Gefahrenbereiche werden häufig durch Schutztüren abgegrenzt. Diese werden auf ihre Stellung überwacht und gegebenenfalls der Bereich, von dem eine Gefahr ausgeht, abgeschaltet. Soll der Maschinenprozess nicht unterbrochen und erst zu Ende gefahren werden, kann der Zugang durch die Zuhaltung des RFID-Sicherheitsschalters 3SE64 so lange verhindert werden. Für die Anwendung direkt an der Maschine mit kleinem dezentralem Aufbau ist die ET 200AL eine geeignete Wahl.

Aufbau

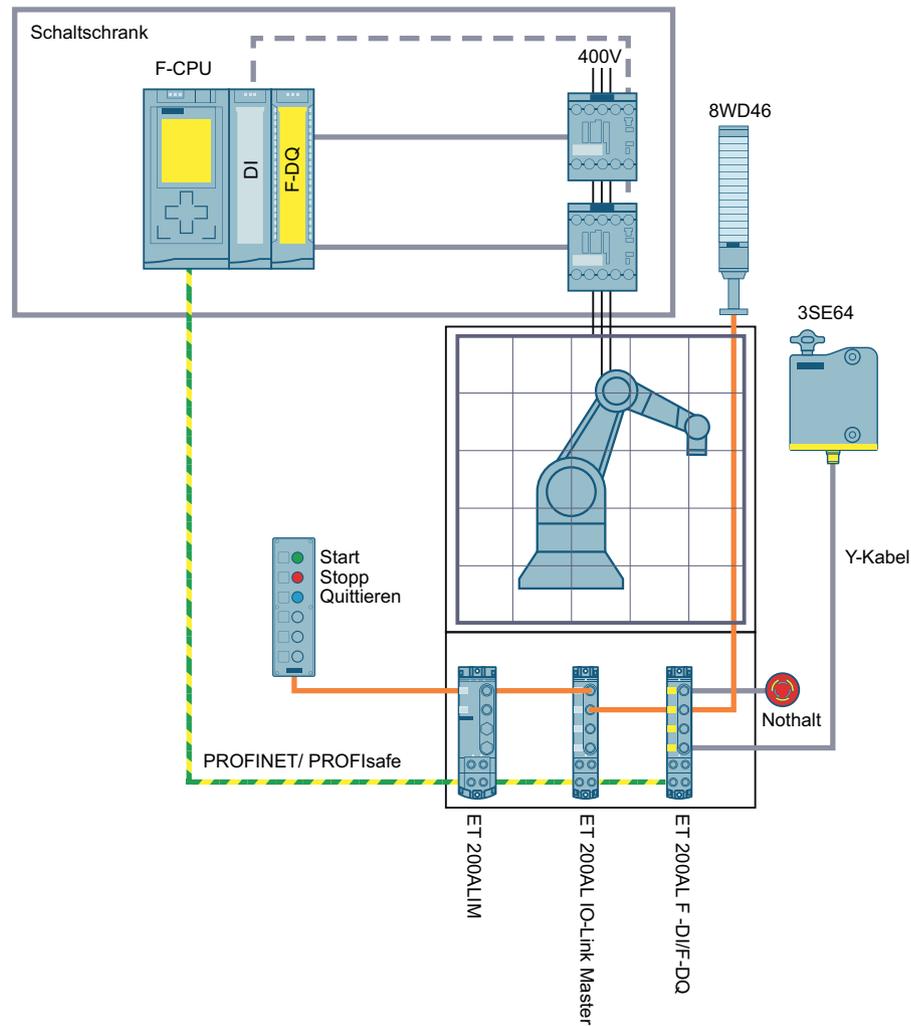
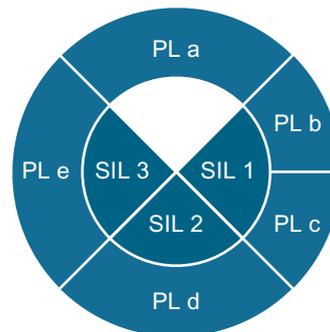


Bild 3-58 Schutztürüberwachung mit Zuhaltung mittels RFID-Sicherheitsschalter 3SE64 inklusive Not-Halt-Abschaltung bis SIL 3 bzw. PL e über ET 200AL und F-CPU

Funktionsweise

Über einen Sicherheitsschalter wird die Stellung einer Schutztür überwacht. Zusätzlich wird über den Sicherheitsschalter die Tür verriegelt. Wird der Befehl zum Entriegeln der Tür gegeben, schaltet die fehlersichere Steuerung die Leistungsschütze sicherheitsgerichtet ab. Nach Ablauf einer eingestellten Zeit und der Beendigung des Maschinenprozesses wird die Zuhaltung entriegelt. Ist die Tür geschlossen und verriegelt und der Rückführkreis geschlossen, kann durch den Starttaster wieder eingeschaltet werden. Der RFID-Sicherheitsschalter 3SE64 mit Zuhaltung ist in zwei Varianten verfügbar, welche sich im Ansteuerprinzip der Zuhaltfunktion unterscheiden (Arbeits-/Ruhestromprinzip). Bei beiden Varianten ist für die Sicherheitsfunktion „Schutztürüberwachung“ SIL 3 bzw. PL e möglich. Während bei Variante 1 (Ruhestromprinzip) SIL 2 bzw. PL d für die Sicherheitsfunktion „Schutztürzuhaltung“ erreicht werden kann, ist bei Variante 2 (Arbeitsstromprinzip) hierfür kein SIL/PL möglich. In dieser Variante dient die Zuhaltung ausschließlich dem Prozessschutz. In diesem Applikationsbeispiel kommt Variante 2 zum Einsatz, da kein SIL bzw. PL für die Sicherheitsfunktion "Schutztürzuhaltung" gefordert wird.



Bei Variante 2 werden beide OSSD-Ausgänge des Sicherheitsschalters 3SE64 bereits bei geschlossener Schutztür aktiv. Daher kann im Anwenderprogramm nicht ausgewertet werden, ob die Tür tatsächlich verriegelt ist oder nicht. Im Arbeitsstromprinzip (Variante 2) ist jedoch auch keine Diagnose der Zuhaltung notwendig, da die Art der Verriegelung jeglichen SIL/PL verhindert. In dieser Variante dient die Zuhaltung ausschließlich dem Prozessschutz. Ausführliche Informationen dazu befinden sich unter unten angegebenem Link.

Die Anbindung eines Not-Halts an einen freien Port der F-Baugruppe der AL wird zusätzlich gezeigt, da diese Konstellation einen Großteil der Maschinen sicherheitsgerichtet abdecken kann.

Das Bedienpanel wird via IO-Link angebunden, um Verdrahtungsaufwand zu reduzieren. Hier wäre eine Anbindung über eine Standard-eingangskarte der ET 200AL ebenso möglich. Das Meldekonzept wird mittels IO-Link Variante der 8WD46 gelöst.

Sicherheitsgerichtete Komponenten

RFID-Sicherheitsschalter mit Zuhaltung	Not-Halt-Befehlsgerät	Dezentrale Peripherie IP67
		
3SE64 (http://www.siemens.de/sirius-erfassen)	3SU1 (http://www.siemens.de/sirius-act)	ET 200AL (http://www.siemens.de/simatic-safety)

Steuerung Failsafe	Schütz
	
S7 F-PLC (http://www.siemens.de/simatic-safety)	2x 3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Ausführliche Dokumentation, Schaltplan, TIA-Portal-Projekt und Safety Evaluation (<https://support.industry.siemens.com/cs/de/de/view/109818115>)

3.7.15 Kaskadierung von Sicherheitsschaltgeräten 3SK2 bis SIL3 bzw. PL e**Anwendung**

Die Kaskadierung von Sicherheitsschaltgeräten dient dazu, verschiedene Anlagenteile und deren Sicherheitsfunktionen miteinander zu verknüpfen.

Darüber hinaus bietet die Kaskadierung eine Implementierungsmöglichkeit, wenn das Mengengerüst eines einzelnen 3SK2 Sicherheitsschaltgeräts nicht für die Applikation ausreicht und weitere Ein- bzw. Ausgänge benötigt werden.

Aufbau

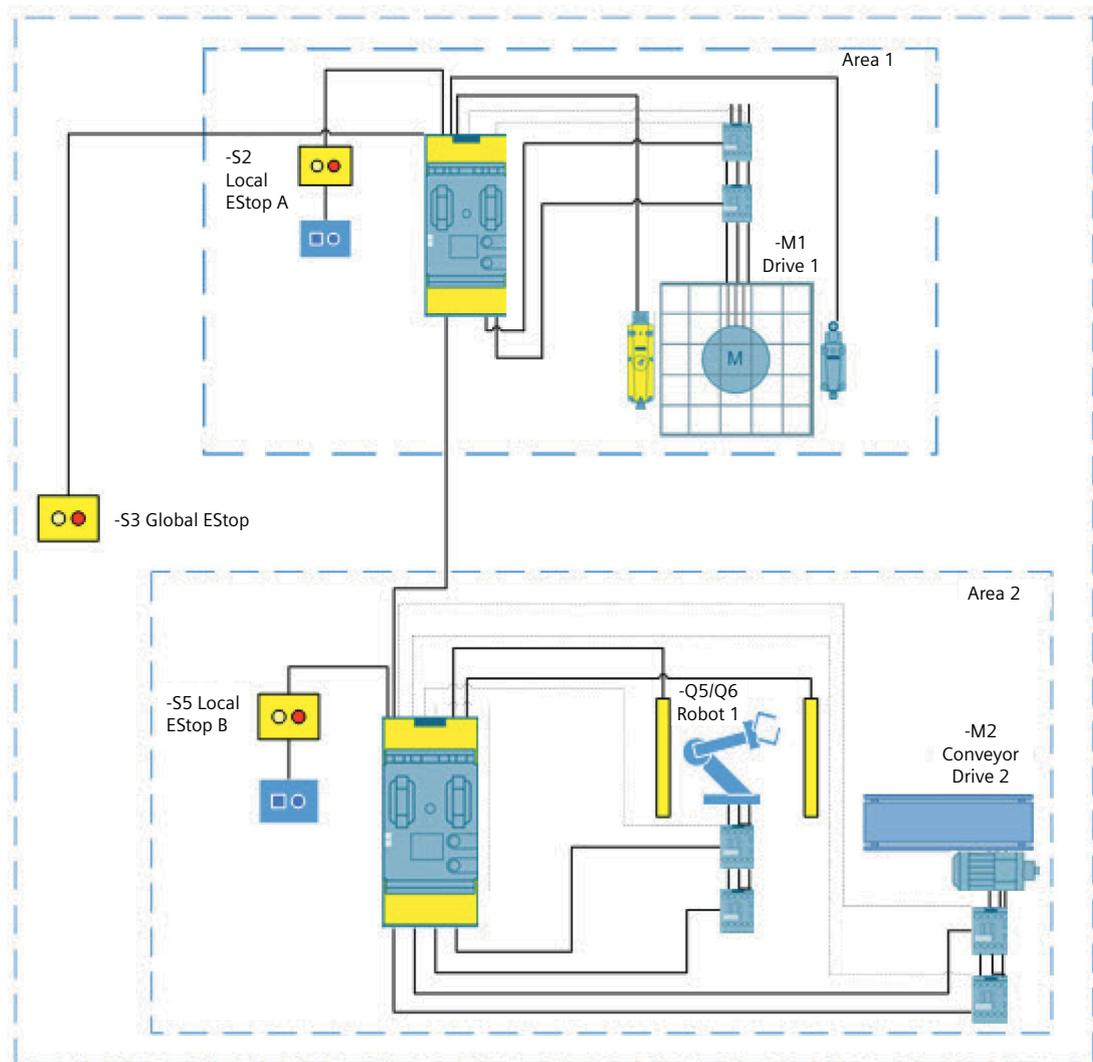


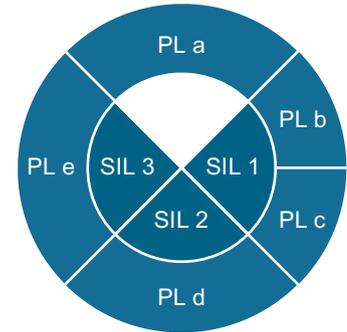
Bild 3-59 Kaskadierung von Sicherheitsschaltgeräten 3SK2 bis SIL 3 bzw. PL e

Funktionsweise

Die beiden Sicherheitsschaltgeräte sind über eine Kaskadierung miteinander verknüpft. Zur besseren Darstellung wurde für jedes Sicherheitsschaltgerät ein Bereich definiert, welcher die jeweiligen Sensoren und Aktoren beinhaltet. Bei Auslösen des Not-Halts A wird nur der Antrieb 1 abgeschaltet. Bei Auslösen des Not-Halts B wird der Roboter und Antrieb 2 abgeschaltet. Bei Auslösen des Globalen Not-Halts werden alle Aktoren sicherheitsgerichtet abgeschaltet. Der globale Not-Halt wird hier auf das 3SK2 im Bereich 1 verdrahtet. Über einen fehlersicheren Ausgang wird das Not-Halt-Signal an das 3SK2 im Bereich 2 übertragen.

Nach einem Not-Halt muss ein manueller Startbefehl im jeweiligen Sicherheitsschaltgerät über den Starttaster ausgeführt werden. Beim Öffnen der Schutztür wird nur die dahinter liegende Aktorik abgeschaltet. Bei Detektion des Lichtvorhangs wird der Roboter sicherheitsgerichtet stillgesetzt.

Grundlage für die Auslegung der Sicherheitsfunktionen und Programmierung in den beiden 3SK2 Sicherheitsschaltgeräten bildet eine Cause-Effect-Matrix. Durch die Verknüpfung von Ursachen und Wirkungen kann leichter bestimmt werden, welche Sicherheitsfunktionen in welchem 3SK2 Gerät realisiert werden und dementsprechend das Sicherheitsprogramm entworfen werden.



Sicherheitsgerichtete Komponenten

Not-Halt-Befehlsgerät	Positionsschalter	Sicherheitsschaltgerät	Schütz
			
3SU1 (http://www.siemens.de/sirius-act)	3SE5 (http://www.siemens.de/sirius-erfassen)	3SK2 (http://www.siemens.de/safety-relays)	3RT20 (http://www.siemens.de/sirius-control)

Siehe auch

Schaltplan, 3SK2-Projekt und Safety Evaluation (<https://support.industry.siemens.com/cs/de/de/view/109818869>)

3.8 Weitere Applikationsbeispiele und FAQs

Auf den Seiten des Industry Online Supports finden Sie sehr viele Anwendungsbeispiele zum Thema Safety in der Automatisierungstechnik. Der Safety Selektor erlaubt Ihnen durch Vorgabe von Kategorien schnell die passenden Safety Anwendungsbeispiele im Industry Online Support (<https://support.industry.siemens.com/cs/de/de/view/109773295>) zu finden.

3.8.1 Übergreifend

- Sicherheitstechnische Kenngrößen - Standard-B10-Werte / Ausfallraten elektromechanischer SIRIUS- und SENTRON-Produkte (<https://support.industry.siemens.com/cs/ww/de/view/109739348>)
- Schütze in Sicherheitsapplikationen – Anwendungsleitfaden (<https://support.industry.siemens.com/cs/de/de/view/109807687>)
- Not-Halt-Abschaltung bis SIL 2 bzw. PL d mit einem Sicherheitsschaltgerät SIRIUS 3SK1 und Leistungsschalter (<https://support.industry.siemens.com/cs/ww/de/view/38472027>)
- Schutztür mit Zuhaltung durch Federkraft an einer S7-1500 (<https://support.industry.siemens.com/cs/ww/de/view/21063946>)

3.8.2 Teilsystem Erfassen

- Was ist bei der Betriebsartenwahl in Verbindung mit funktionaler Sicherheit zu beachten? (<https://support.industry.siemens.com/cs/de/de/view/89260861>)
- Sichere Betriebsartenwahl mit IO-Link ID-Schlüsselschalter (<https://support.industry.siemens.com/cs/de/de/view/109778665>)
- Anwendungsbeispiel: Betriebsartenwahl in Verbindung mit funktionaler Sicherheit (<https://support.industry.siemens.com/cs/ww/de/view/109757316>)

3.8.3 Teilsystem Auswerten

- Automatischer Wiederanlauf nach Netzausfall mit 3SK1 und Zeitrelais (<https://support.industry.siemens.com/cs/ww/de/view/109758052>)
- Kontakterweiterung einer fehlersicheren Steuerung mit 3SK1 und 3RQ1 (<https://support.industry.siemens.com/cs/ww/de/view/76676971>)
- Wie kann ein 3SK2 Sicherheitsschaltgerät mit PROFINET in Betrieb genommen werden? (<https://support.industry.siemens.com/cs/ww/de/view/109778581>)
- Sichere Nachlaufwegprüfung linearer Achsen mit 3SK2 (<https://support.industry.siemens.com/cs/ww/de/view/109782767>)
- Auslesen der Diagnosedaten aus dem Sicherheitsschaltgerät SIRIUS 3SK2 oder 3RK3 (MSS) mittels einer SIMATIC S7- CPU (<https://support.industry.siemens.com/cs/ww/de/view/109747831>)

3.8.4 Teilsystem Reagieren

- Welcher Sicherheitslevel kann bei der Verwendung eines Schützes und eines Leistungsschalters erreicht werden? (<https://support.industry.siemens.com/cs/ww/de/view/40349715>)
- IEC 62061 / ISO 13849-1 – Erläuterungen zur Anwendung Welche Sicherheitsintegrität ist bei Verwendung von zwei Leistungsschaltern erreichbar? (<https://support.industry.siemens.com/cs/de/de/view/109483115>)
- Was ist der Unterschied zwischen zwangsgeführten Kontaktelementen von Hilfsschützen und Spiegelkontakte von Leistungsschützen? (<https://support.industry.siemens.com/cs/ww/de/view/109758261>)
- 3RW Sanftstarter: Sicheres Abschalten nach IEC 62061 (SIL) bzw. ISO 13849-1 (PL) (<https://support.industry.siemens.com/cs/ww/de/view/67474130>)
- SINAMICS S120/S110, SIMOTION D: Anschluss von F-DIs an F-Dos (u.a. 3SK) (<https://support.industry.siemens.com/cs/ww/de/view/39700013>)

Vorschriften und Normen

4.1 Vorschriften und Normen in der Europäischen Union (EU)

4.1.1 Maschinensicherheit in Europa

4.1.1.1 Rechtliche Grundlagen

Maschinenrichtlinie (2006 / 42 / EG)

Mit der Einführung des einheitlichen europäischen Binnenmarktes wurde beschlossen, dass die nationalen Normen und Vorschriften aller EG-Mitgliedsstaaten, die die technische Realisierung von Maschinen betreffen, harmonisiert werden. Dies hatte zur Folge, dass die Maschinenrichtlinie als eine Binnenmarktrichtlinie von den einzelnen Mitgliedsstaaten inhaltlich in nationales Recht umgesetzt werden musste. In Deutschland wurde der Inhalt der Maschinenrichtlinie als 9. Verordnung zum Produktsicherheitsgesetz (9. ProdSV) umgesetzt. Dies geschah bei der Maschinenrichtlinie vor dem Hintergrund einheitlicher Schutzziele mit dem Zweck, technische Handelshemmnisse abzubauen. Der Anwendungsbereich der Maschinenrichtlinie ist entsprechend ihrer Definition "Maschine ist eine Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist" sehr weit gefasst. Der Anwendungsbereich erstreckt sich außerdem über auswechselbare Ausrüstungen, Sicherheitsbauteile, Lastaufnahmemittel, Ketten, Gurte, Seile, abnehmbare Gelenkwellen und unvollständige Maschinen.

Als "Maschine" wird auch eine Gesamtheit von Maschinen bezeichnet, die, damit sie zusammenwirken, so angeordnet sind und betätigt werden, dass sie als Gesamtheit funktionieren.

Der Anwendungsbereich der Maschinenrichtlinie erstreckt sich somit von einer einfachen Maschine bis hin zu einer Anlage.

Die Erfüllung der grundlegenden Sicherheitsanforderungen und Gesundheitsanforderungen in Anhang I der Richtlinie ist für die Sicherheit von Maschinen zwingend notwendig. Der Hersteller muss die in Anhang I Absatz 1.1.2 genannten Grundsätze für die Integration der Sicherheit beachten.

Die Schutzziele müssen verantwortungsbewusst umgesetzt werden, um die Forderung nach Konformität mit der Richtlinie zu erfüllen. Der Hersteller einer Maschine muss den Nachweis über die Übereinstimmung mit den grundlegenden Anforderungen erbringen. Dieser Nachweis wird durch die Anwendung harmonisierter Normen erleichtert. Bei Maschinen nach Anhang IV der Maschinenrichtlinie, die ein größeres Gefahrenpotenzial darstellen, wird ein Bescheinigungsverfahren verlangt. (Empfehlung: Auch Maschinen, die nicht in Anhang IV aufgeführt sind, können ein großes Gefahrenpotenzial darstellen und sollten entsprechend behandelt werden.)

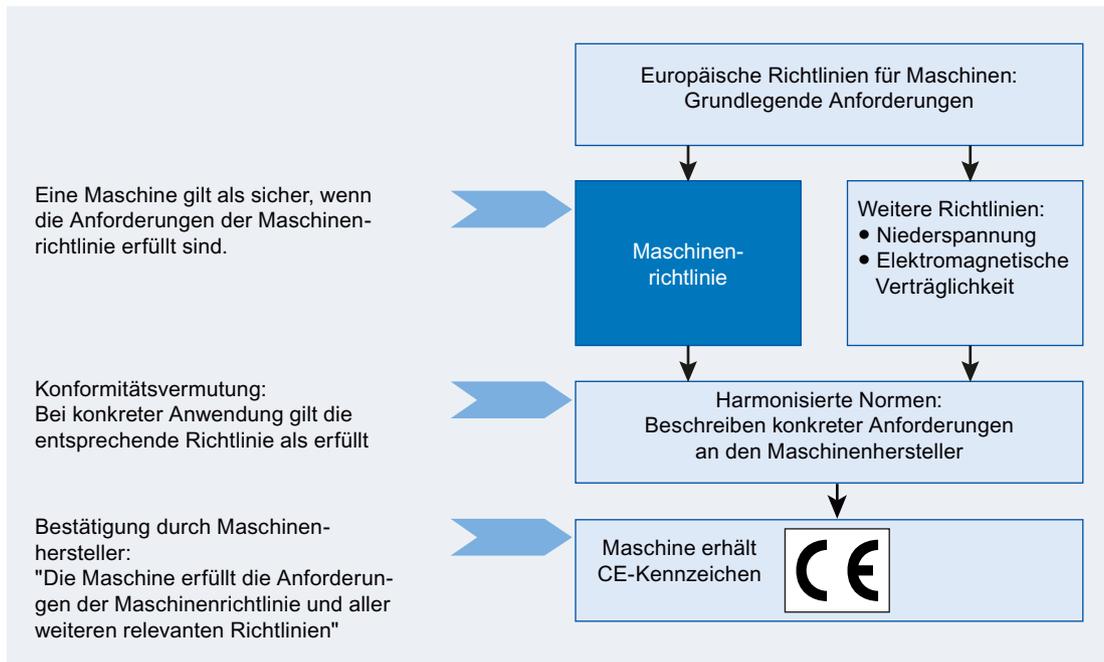


Bild 4-1 Europäische Richtlinien für Maschinen

Normen

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.

Grundsätzlich müssen alle Normen, die als Europannormen ratifiziert sind, in die nationalen Normenwerke der Mitgliedsstaaten unverändert übernommen werden, unabhängig davon, ob die Normen unter einer Richtlinie harmonisiert sind oder nicht. Bestehende nationale Normen zum gleichen Thema müssen dann zurückgezogen werden. So soll im Laufe der Zeit in Europa ein einheitliches (widerspruchsfreies) Normenwerk geschaffen werden.

Harmonisierte Europannormen

Harmonisierte Europannormen (EN-Normen) werden im Amtsblatt der Europäischen Gemeinschaften veröffentlicht und sind danach ohne Änderungen in nationale Normen zu übernehmen.

Sie dienen zur Erfüllung der grundlegenden Sicherheitsanforderungen und Gesundheitsanforderungen und der im Anhang I der Maschinenrichtlinie genannten Schutzziele.

Durch Einhaltung der harmonisierten Normen ergibt sich eine "automatische Vermutungswirkung" der Erfüllung der Richtlinie, d. h., der Hersteller darf darauf vertrauen,

dass er die Sicherheitsaspekte der Richtlinie erfüllt hat, soweit sie in der jeweiligen Norm behandelt sind. Allerdings ist nicht jede Europannorm in diesem Sinne harmonisiert. Entscheidend ist die Listung im europäischen Amtsblatt. Diese Listen sind stets aktuell im Internet (<http://www.newapproach.org/>) abrufbar.

4.1.1.2 CE-Konformitätsprozess

CE-Konformitätsprozess

Phasen im CE-Konformitätsprozess

Der CE-Konformitätsprozess gliedert sich in verschiedene Phasen, die während des kompletten Lebenszyklus (Planung, Konstruktion, Installation, Betrieb und Wartung) durchgeführt werden müssen.

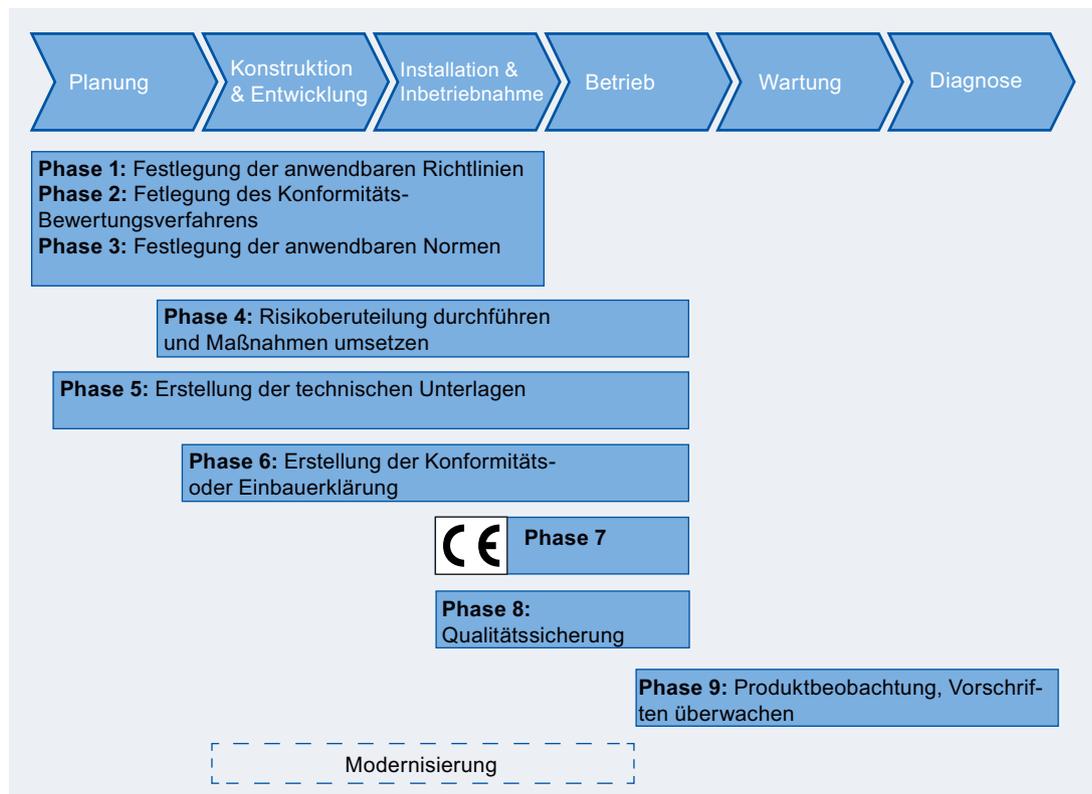


Bild 4-2 CE-Konformitätsprozess für Maschinen und Anlagen

Bereits während der Planung müssen in Phase 1 die anwendbaren Richtlinien festgelegt werden. Dies kann keine, eine, oder mehrere Richtlinien umfassen. (z.B. Maschinenrichtlinie siehe Kapitel 2.2.1)

In Phase 2 wird das Konformitäts-Bewertungsverfahren entsprechend der anzuwendenden Richtlinien aus Phase 1 festgelegt.

In Phase 3 folgt die Festlegung der anwendbaren Normen.

Die sich anschließende Phase 4 besteht aus der Risikobeurteilung der Maschine, der Risikoreduzierung und Validierung. Auch die Bewertung der sicherheitsbezogenen Teile der Maschinensteuerung gehören zu dieser Phase. Die einzelnen Schritte der Phase 4 werden in den nachfolgenden Abschnitten erläutert.

Begleitend während der gesamten Planung, Entwicklung und Inbetriebnahme findet die Erstellung der technischen Unterlagen statt, dies wird auch Phase 5 genannt. Die technischen Unterlagen müssen mit Bereitstellung der Maschine vollständig vorliegen. Hierzu zählen technische Dokumentation (siehe Anh. VII der Maschinenrichtlinie), Konformitätsbescheinigung, gegebenenfalls Abnahmeprotokolle, Transportunterlagen, etc.

Ist die Validierung erfolgreich durchlaufen worden, so kann in Phase 6 die Konformitäts- oder Einbauerklärung erstellt werden und in Phase 7 die CE Kennzeichnung an der Maschine angebracht werden.

Jeder Hersteller ist verpflichtet, sein Produkt nach dem Inverkehrbringen hinsichtlich eventuell versteckter Mängel zu beobachten. Dies wird durch die Phase 8 der Qualitätssicherung und Phase 9 der Produktbeobachtung abgedeckt. So sind beispielsweise Informationen darüber zu sammeln, ob das Produkt tatsächlich so verwendet wird, wie ursprünglich vorgesehen und wie es sich im Verlauf seines Lebenszyklus verhält.

Insbesondere sind gefährliche Mängel sowie missbräuchliche Verwendungen oder falsche Handhabung am Produkt durch entsprechende Maßnahmen abzustellen. Werden versteckte Mängel entdeckt, muss der Anwender informiert werden.

Risikobeurteilung

Maschinen und Anlagen beinhalten, aufgrund ihres Aufbaus und ihrer Funktionalität, Risiken. Deshalb verlangt die Maschinenrichtlinie für jede Maschine eine Risikobeurteilung und gegebenenfalls eine Risikominderung, bis das Restrisiko kleiner als das tolerierbare Risiko ist. Für die Verfahren der Bewertung dieser Risiken ist die Norm EN ISO 12100 "Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung" (03 / 2011) anzuwenden.

Schwerpunktmäßig beschreibt EN ISO 12100 die zu betrachtenden Risiken und Gestaltungsleitsätze und den iterativen Prozess mit Risikobeurteilung und Risikominderung zum Erreichen der Sicherheit.

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 der iterative Prozess, mit dessen Hilfe Gefährdungen so weit wie möglich beseitigt werden können und entsprechende Schutzmaßnahmen getroffen werden können.

Die Risikobeurteilung umfasst die folgenden Schritte:

- Risikoanalyse
 - Bestimmung der Grenzen der Maschine
 - Identifizierung der Gefährdungen
 - Risikoeinschätzung
- Risikobewertung

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.

Die Risikominderung muss durch geeignete Konzipierung und Realisierung der Maschine erfolgen, z. B. durch für Sicherheitsfunktionen geeignete Steuerung oder Schutzmaßnahmen.

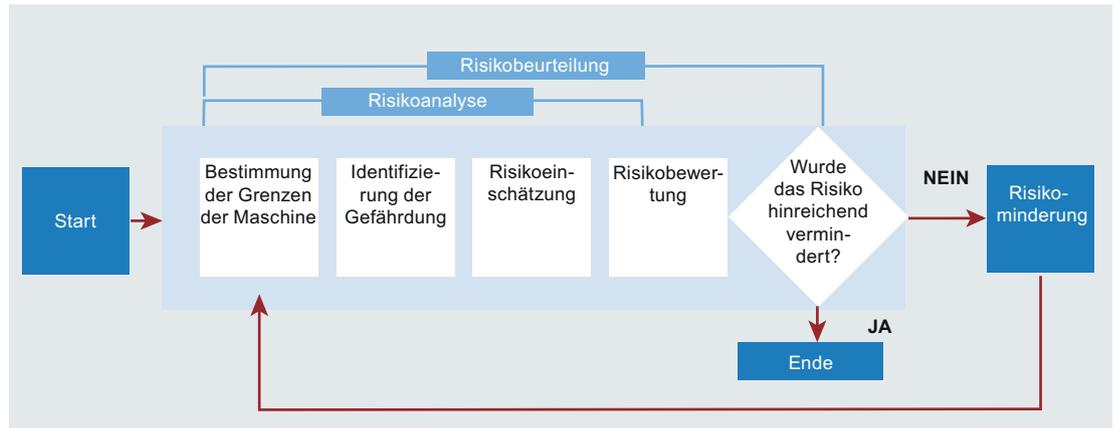


Bild 4-3 Iteratives Verfahren zur Risikobeurteilung nach EN ISO 12100

Risikoreduzierung

Falls das abgeschätzte Risiko zu hoch erscheint, muss es vermindert werden, bis das verbleibende Restrisiko geringer als das tolerierbare Risiko ist. Dazu muss zuerst durch Konstruktionsänderung versucht werden, die Maschine sicher zu machen. Falls das nicht möglich ist, muss durch geeignete Schutzmaßnahmen eine Risikominderung erreicht werden.

- Die Schwere eines möglichen Schadens kann z. B. dadurch verringert werden, dass während der Anwesenheit von Personen die Bewegungsgeschwindigkeiten oder Kräfte der Maschinenteile verringert werden.
- Durch Absperrrichtungen kann die Häufigkeit, mit der Personen im Gefahrenbereich sind, verringert werden.
- Es besteht immer eine gewisse Wahrscheinlichkeit, dass sich eine Maschine nicht bestimmungsgemäß verhält oder Schutzeinrichtungen versagen. Dies kann durch Fehler in beliebigen Teilen der Maschine verursacht werden. Eine Minderung dieses Risikofaktors kann durch geeignete Konstruktion der sicherheitsrelevanten Teile erreicht werden. Zu den sicherheitsrelevanten Teilen gehört auch die Steuerung der Maschine, wenn durch deren Versagen eine Gefährdung entstehen kann. Durch Realisierung der Steuerung gemäß IEC 62061 bzw. ISO 13849-1 kann das Risiko, das durch Fehler der Steuerung verursacht wird, vermindert werden.
- Die Möglichkeit einen Schaden zu vermeiden kann u. a. dadurch vergrößert werden, dass Gefahrenzustände rechtzeitig erkennbar sind, z. B. durch Signallampen.

Ein gemeinsamer Parameter all dieser Elemente ist die Wahrscheinlichkeit des Eintretens eines unerwünschten Ereignisses. Durch Vermindern dieser Wahrscheinlichkeit kann eine Verminderung des Risikos erreicht werden.

Folgende Schritte sind zur Risikominderung durchzuführen:

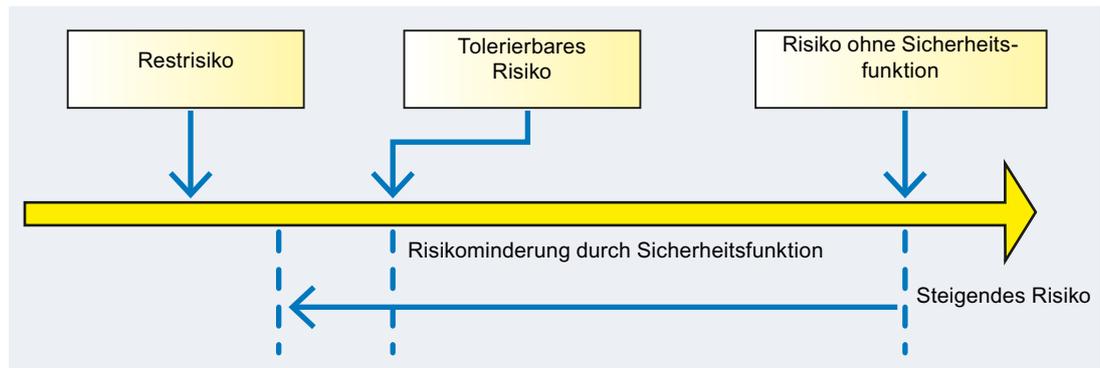


Bild 4-4 Risikominderung

Schritt 1: inhärent sichere Konstruktion

Inhärent sichere Konstruktion beseitigt Gefährdungen oder vermindert die damit verbundenen Risiken durch eine geeignete Auswahl von Konstruktionsmerkmalen der Maschine selbst und / oder Wechselwirkungen zwischen den gefährdeten Personen und der Maschine.

Eine sichere Konstruktion lässt sich beispielsweise durch Integration der Sicherheit in die Maschine (Abdeckungen, Zäune etc.) erzielen. Diese Maßnahmen haben im Rahmen der Risikominderung oberste Priorität. Sie sollen:

- Quetschstellen vermeiden
- Elektrischen Schlag vermeiden
- Konzepte für ein Stillsetzen im Notfall beinhalten
- Konzepte für Bedienung und Wartung beinhalten

Schritt 2: technische Schutzmaßnahmen und/oder ergänzende Schutzmaßnahmen

Unter Berücksichtigung der bestimmungsgemäßen Verwendung und der vernünftigerweise vorhersehbaren Fehlanwendung können in geeigneter Weise ausgewählte technische und ergänzende Schutzmaßnahmen angewendet werden, um das Risiko zu mindern, wenn sich die Beseitigung einer Gefährdung als nicht durchführbar erweist oder das damit verbundene Risiko nicht in hinreichendem Maße durch eine inhärent sichere Konstruktion vermindert werden kann.

Unter Schritt 2 fallen auch alle sicherheitsrelevanten Steuerungsfunktionen einer Maschine. Für diese gelten spezielle Anforderungen, deren Erfüllung geprüft werden muss.

Beispielaufbau einer sicherheitsrelevanten Steuerungsfunktion:

- Erfassen (Positionsschalter, Not-Halt, Lichtvorhang etc.)
- Auswerten (Fehlersichere Steuerung, Sicherheitsschaltgerät etc.)
- Reagieren (Schütz, Frequenzumrichter etc.)

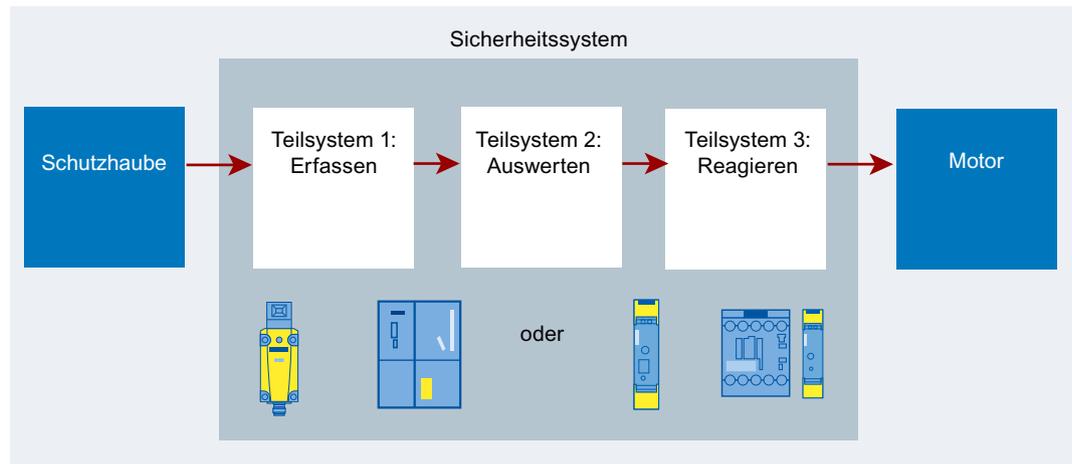


Bild 4-5 Sicherheitssystem für die Sicherheitsfunktion

Schritt 3: Benutzerinformation

Falls trotz inhärent sicherer Konstruktion und dem Einsatz technischer und ergänzender Schutzmaßnahmen Risiken verbleiben, muss die Benutzerinformation auf jegliche Restrisiken hinweisen.

Zu diesen Benutzerinformationen zählen beispielsweise:

- Warnhinweise in der Betriebsanleitung
- Spezielle Arbeitsanweisungen
- Piktogramme
- Hinweis zur Verwendung von persönlicher Schutzausrüstung

Die Anforderungen an sicherheitsrelevante Teile von Steuerungen sind nach der Höhe des Risikos bzw. der notwendigen Risikominderung abgestuft. Die EN ISO 13849-1 verwendet den hierarchisch abgestuften Performance Level (PL) zur Bewertung. Die IEC 62061 verwendet den Safety Integrity Level (SIL) zur Abstufung. Beides ist ein Maß für die sicherheitsbezogene Leistungsfähigkeit einer Steuerungsfunktion.

Wichtig ist in jedem Fall, unabhängig davon, welche Norm angewendet wird, dass alle Teile der Steuerung der Maschine, die an der Ausführung der sicherheitsrelevanten Funktionen beteiligt sind, diesen Anforderungen genügen.

Hinweis

Zur Steuerung einer Maschine gehören auch die Laststromkreise der Antriebe und Motoren.

Beim Entwurf und der Realisierung der Steuerung ist es notwendig zu überprüfen, ob die Anforderungen der ausgewählten PL bzw. des SIL erfüllt sind. Da die Anforderungen zur Erzielung der notwendigen Safety Performance in EN ISO 13849 und IEC 62061 unterschiedlich strukturiert sind, sind auch die Anforderungen zur Überprüfung unterschiedlich strukturiert. Für ein Design gemäß EN ISO 13849 sind die Einzelheiten für die Validierung und was dabei zu beachten ist, im Teil 2 (EN ISO 13849-2) beschrieben. Die Anforderungen zur Validierung eines Designs gemäß IEC 62061 sind in der Norm selbst beschrieben.

Validierung

Validierung bedeutet eine bewertende Überprüfung der angestrebten Sicherheitsfunktionalität. Ihr Zweck 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 weiterhin aufzeigen, dass jedes sicherheitsbezogene Teil die Anforderungen der relevanten Norm erfüllt. Dabei sind die folgenden Aspekte beschrieben:

- Fehlerlisten
- Validierung der Sicherheitsfunktionen
- Validierung der geforderten und der erreichten Safety Performance (Kategorie, Safety Integrity Level oder Performance level)
- Validierung der Umgebungsanforderungen
- Validierung der Instandhaltungsanforderungen

In einem Validierungsplan müssen die Anforderungen für die Durchführung der Validierung für die festgelegten Sicherheitsfunktionen beschrieben werden.

Ziel der Validierung:

Feststellung der Konformität mit den Anforderungen

- der europäischen Richtlinien.
- die sich aus dem Kundenauftrag, dem Einsatz der Maschine und ggf. weiteren länderspezifischen Forderungen, die für die Maschine gelten, ergeben.

Bei der Bereitstellung der Maschine müssen alle maschinenrelevanten Informationen vorliegen. Hierzu zählen: Kundenauftrag, technische Dokumentation (siehe auch Anh. VII der Maschinenrichtlinie), Konformitätsbescheinigung, ggf. Abnahmeprotokoll, Transportunterlagen etc.

4.2 Vorschriften und Normen außerhalb der Europäischen Union (EU)

4.2.1 Vorschriften und Normen außerhalb der Europäischen Union - Übersicht

Die folgende Beschreibung soll einen Überblick über die Vorschriften einiger Länder außerhalb der Europäischen Union vermitteln. Sie darf nicht als vollständige Beschreibung betrachtet werden. Die genauen Anforderungen sowie nationalen und lokalen Regeln für eine spezielle Anwendung müssen in jedem Einzelfall detailliert geprüft werden. Für weitere Informationen bezüglich der Vorgaben zur Sicherheitstechnik in anderen Ländern kontaktieren Sie die jeweiligen Zulassungsbehörden vor Ort.

4.2.2 Gesetzliche Anforderungen in den USA

Ein wesentlicher Unterschied bei den gesetzlichen Anforderungen zur Sicherheit am Arbeitsplatz zwischen den USA und Europa ist, dass es in den USA keine einheitliche Bundesgesetzgebung zur Maschinensicherheit gibt, welche die Verantwortlichkeit des Herstellers/Lieferanten abdeckt. Vielmehr besteht die generelle Anforderung, dass der Arbeitgeber einen sicheren Arbeitsplatz bieten muss. Dies ist mit dem Occupational Safety and Health Act (OSHA) geregelt. Die für Arbeitssicherheit relevanten Regeln der OSHA sind in OSHA 29 CFR 1910.xxx ("OSHA Regulations (29 CFR) PART 1910 Occupational Safety and Health") beschrieben. (CFR: Code of Federal Regulations).

Neben den OSHA Regeln, ist es wichtig die aktuellen Standards von Organisationen wie NFPA und ANSI sowie die in USA bestehende umfassende Produkthaftung zu beachten. Zwei besonders wichtige Standards für Sicherheit in der Industrie sind NFPA 70 (bekannt als National Electric Code (NEC)) und NFPA 79 (Electrical Standard for industrial Machinery). Beide beschreiben die grundlegenden Anforderungen an die Eigenschaften und die Ausführung der elektrischen Ausrüstung. Der National Electric Code (NFPA70) gilt vorrangig für Gebäude aber auch für die elektrischen Verbindungen von Maschinen und Teilmaschinen. NFPA 79 gilt für Maschinen. Damit besteht ein Graubereich in der Abgrenzung zwischen beiden Standards bei großen Maschinen, die aus Teilmaschinen bestehen. Z.B. große Fördersysteme können als Teil des Gebäudes betrachtet werden, so dass NFPA 70 und/oder NFPA 79 anzuwenden sind.

4.2.3 Gesetzliche Anforderungen in Brasilien

Das brasilianische Ministerium für Arbeit und Beschäftigung, das für die Regelung von Aktivitäten in den Bereichen Gesundheit und Arbeitssicherheit verantwortlich ist, veröffentlichte im Dezember 2010 die neue Version der Rechtsverordnung Nr. 12. An Artikel 137 der EU-Richtlinien angelehnt, ist diese Regelung auf Bestands- und Neuanlagen anwendbar und gewährleistet die Sicherheit im Umgang mit Maschinen nach dem aktuellen Stand der Technik. Basierend auf internationalen Normen berücksichtigt diese brasilianische Regelung auch den Gesamtlebenszyklus einer Maschine, beginnend mit der Konstruktionsphase, über die Etappen der Kommerzialisierung, Transport, über den Betrieb und Instandhaltung bis zur schlussendlichen Entsorgung.

Obwohl die neue Version von NR 12 auf dem europäischen Modell basiert, bei dem die Gesetzgebung durch internationale Normen unterstützt wird, unterscheidet sie sich hinsichtlich der Rechtsinstrumente zur Konformitätsbewertung und bei der Verwendung von harmonisierten Normen. Anstelle von Überprüfungen durch Kontrollbehörden inspiziert die Regierung selbst am Betriebsort Maschinen und Installationen mittels nominierter Behörden. Dafür werden lediglich die spezifischen Anforderungen berücksichtigt, die in der Regelung beschrieben werden. Aus diesem Grund enthält die NR 12 zusätzliche technische Beschreibungen für bestimmte Maschinen.

NR 12 weist strukturelle Ähnlichkeiten mit den Sicherheitsnormen auf. Sie besitzt allgemeine Anforderungen, die anhand einer Risikoanalyse angelehnt an Typ A Normen wie die ISO 12100, erfüllt werden können, technische Anforderungen in Einklang mit einigen Normen vom Typ B und spezifischen Anforderungen für bestimmte Maschinen, ähnlich den Normen vom Typ C.

Die Anhänge der NR 12 sind nicht mit Normen vom Typ C harmonisiert, aber die Mehrheit wurde auf Grundlage von Normen vom Typ C erstellt oder sind stark von ihnen beeinflusst, um international etablierte Standards einzuhalten. Obwohl die Konformitätsvermutung mit NR 12 nicht möglich ist, bedeutet dies, dass trotzdem die Mehrzahl der Anforderungen der Norm durch Anwendung der Normen vom Typ C erreicht werden können.

Eine kurze Zusammenfassung der NR 12 erhalten Sie im Folgenden:

12.1 bis 12.5: Allgemeine Prinzipien und Umfang der Normen.

12.6 bis 12.13: Anordnung, Anlagen und Umgebungsbedingungen der Maschinen.

12.14 bis 12.23: Elektrische Ausrüstungen – Anwendung konventioneller technischer Anforderungen für elektrische Ausrüstungen, Steuerungseinheiten und Bedienelemente (Referenzen aus EN 60204). Dieser Abschnitt der NR 12 nimmt Bezug auf andere Rechtsverordnungen hinsichtlich elektrischer Ausrüstungen (NR 10).

12.24 bis 12.37: Steuerungssysteme – Anwendung von Konzepten, die in der Norm ISO 12100 zu Steuerungen klar festgelegt sind: Anordnung und Art der Steuerung (Zweihandschaltgerät gemäß EN 574), Auswahlmodi, Verhinderung von unerwartetem Anlauf, Manipulation, Verwendung bewährter Komponenten u.a.

12.38 bis 12.55: Sicherheitssteuerungssysteme – allgemeine Anforderungen, Verhalten bei Störung, Design auf Grundlage von Kategorien (NRB 14153 oder EN 954) gemäß Risikoanalysen (ISO 12100). Dieser Abschnitt enthält ebenfalls Anforderungen für trennende und verriegelnde Schutzeinrichtungen (EN 953, EN 1088).

12.56 bis 12.63: Notausschaltungssysteme – spezifische Anforderungen (ähnlich ISO 13850).

12.64 bis 12.76: Ortsfeste Zugänge zu Maschinenteilen

12.77 bis 12.84: Drucksysteme

12.85 bis 12.93: Fördersysteme und Ausrüstung für das Heben von Lasten

12.94 bis 12.105: Ergonomische Gesichtspunkte

12.106 bis 12.110: Zusätzliche Risiken

12.111 bis 12.115: Instandhaltung, Kontrolle und Einstellung von Maschinen

12.116 bis 12.124: Zeichen

12.125 bis 12.129: Informationen zur Verwendung, Handbücher, Verfahren

12.130 bis 12.134: Sicherheitsverfahren

12.135 bis 12.147: Ausbildung und Qualifizierung

12.148 bis 12.156: Zusätzliche Anforderungen

ANHANG I: Sicherheitsabstände gegen das Erreichen von Gefahrstellen (ISO 13852, ISO 13853, ISO 13854 und ISO 13855)

ANHANG II: Ausbildung

ANHANG III: Ortsfeste Zugänge (EN 14122)

ANHANG IV: Begriffe und Definitionen

ANHANG V: Motorsägen

ANHANG VI: Süßwaren- und Konditoreimaschinen

ANHANG VII: Metzgerei - und Lebensmittelmaschinen

ANHANG VIII: Mechanische (EN 692), hydraulische (EN 693) und ähnliche Pressen

ANHANG IX: Kunststoffspritzgießmaschinen (EN 201)

ANHANG X: Maschinen zur Schuhherstellung u.a.

ANHANG XI: Maschinen und Geräte zur Landwirtschaftlichen und Forstwirtschaftlichen Nutzung

HINWEIS: NR 12 wird gegenwärtig überprüft, es können nachträglich neue Anhänge hinzugefügt werden.

4.2.4 Gesetzliche Anforderungen in Australien

Der Gesundheitsschutz am Arbeitsplatz spielt auch in Australien eine wesentliche Rolle. Durch die im Januar 2013 neu überarbeiteten Richtlinien ergeben sich auch für Maschinen neue Anforderungen. So spielen hier die Richtlinien "Work Health and Safety Act 2012" und die "Work Health and Safety Regulations 2012" in Zusammenhang mit den entsprechenden Anwendungsregeln (Codes of Practice) eine entscheidende Rolle. In den Richtlinien werden Maßnahmen für bestimmte Gefährdungen definiert (wie z.B. Schutzzäune) um einen sicheren Arbeitsplatz zu gewährleisten. Die Anwendungsregeln (Codes of Practice) enthalten zusätzlich praktische Umsetzungen und Hilfen zur Anwendung der Richtlinien, sind selbst aber nicht verbindlich.

Spezifikation und Design sicherheitsrelevanter Steuerungen für Maschinen

5

5.1 Sicherheitsbezogene Teile für die Maschinensteuerung

5.1.1 Vier Risikoelemente

Vier Risikoelemente

Die Risikobeurteilung erlaubt die Bestimmung des Risikos mittels der vier Risikoelemente:

- Schwere des möglichen Schadens
- Häufigkeit mit der sich Personen im Gefahrenbereich aufhalten
- Wahrscheinlichkeit, dass das gefährliche Ereignis eintritt
- Möglichkeit den Schaden zu vermeiden oder zu mindern

Diese Risikoelemente wiederum bilden die Eingangsparameter zur Realisierung einer sicherheitsrelevanten Steuerungsfunktion: Sie ermöglichen erst die Zuordnung des Risikos an die Anforderungen der sicherheitsgerichteten Steuerung. Deshalb bietet die IEC 62061 Verfahren zur Bewertung der Risikoelemente und Einstufung der Safety Performance an.

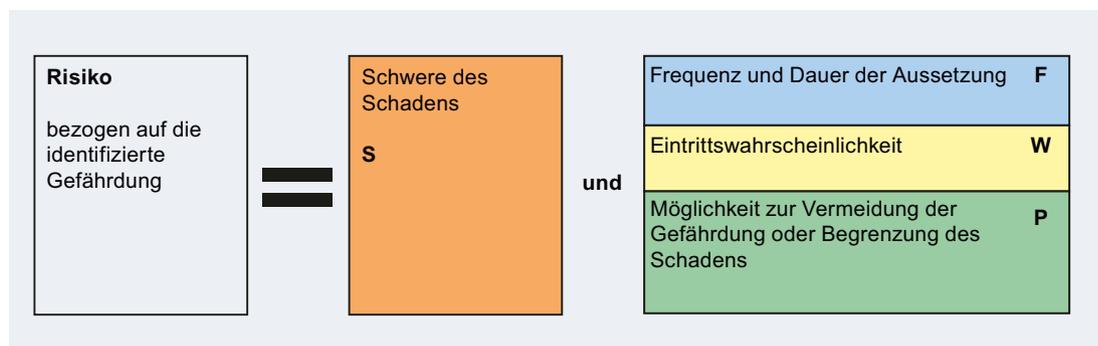


Bild 5-1 Risiko bezogen auf die identifizierte Gefährdung

Ermittlung der notwendigen Safety Performance (Safety Integrity)

Wurde bei der Risikountersuchung festgestellt, dass Funktionsfehler der Steuerung oder das Versagen von Schutzeinrichtungen zu einem zu hohen Risiko führen können, dann muss deren Wahrscheinlichkeit soweit verringert werden, bis das verbleibende Risiko tolerierbar ist. D. h., die Steuerung muss eine ausreichende "Safety Performance" erreichen.

Mit IEC 62061 gibt es ein Verfahren, das eine an Wahrscheinlichkeiten orientierte quantifizierte und damit hierarchische Abstufung der Safety Performance verwendet. Das Ergebnis der Risikoanalyse ist dann der Safety Integrity Level (SIL) für die betreffenden Sicherheitsfunktionen.

5.1 Sicherheitsbezogene Teile für die Maschinensteuerung

In der ISO 13849-1 gibt es eine ähnliche quantifizierte und damit hierarchische Abstufung der Safety Performance. Das dort als Performance Level (PL) bezeichnete Maß korreliert über die zugeordneten Ausfallwahrscheinlichkeiten mit den SILs der IEC 62061.

Konformität mit der neuen Maschinenrichtlinie und somit Exportfähigkeit und Haftungssicherheit erreichen Maschinenhersteller durch Anwendung der Normen EN ISO 13849-1 und IEC 62061. Diese haben neben qualitativen Betrachtungen auch quantitative Aspekte eingeführt. Aus dem Prozess der Risikobewertung leiten sich Schutzmaßnahmen zur Risikominderung ab, die durch Sicherheitsfunktionen beschrieben werden. Anschließend wird die Lösung der Sicherheitsfunktion mit Hardware- und gegebenenfalls Softwarekomponenten überprüft und bewertet, bis die in der Risikobeurteilung geforderte Sicherheitsintegrität erreicht wird.

Hinweis

Falls für den betrachteten Maschinentyp eine C-Norm existiert, sind vorrangig die dort beschriebenen Schutzmaßnahmen zu realisieren. Die Vorgaben sollten aber auf ihre Aktualität bezüglich neuerer technischer Entwicklungen geprüft werden.

Risikograph nach ISO 13849-1

Ziel ist es einen geforderten Performance Level PL, also die Wahrscheinlichkeit gefahrbringender Ausfälle des Systems, durch die Risikoelemente zu ermitteln.

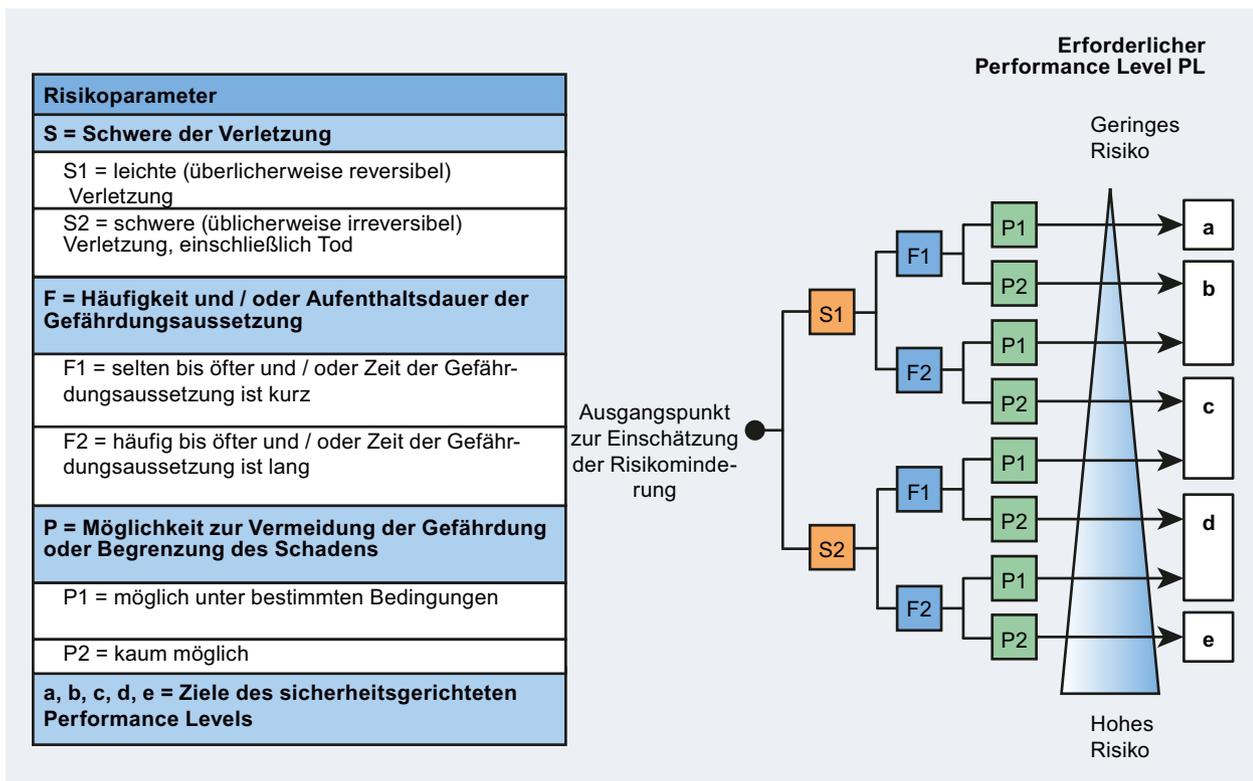


Bild 5-2 Risikograph nach ISO 13849-1 zur Bestimmung der erforderlichen Performance Level

Zur Bestimmung des notwendigen Performance Levels werden die Parameter **S** (Schwere der Verletzung), **F** (Häufigkeit/Dauer der Gefährdungsexposition) und **P** (Möglichkeit der Vermeidung) verwendet.

Die Schwere der Verletzung (S) wird unterschieden nach reversibel (z.B. Quetschungen oder Fleischwunden) und irreversibel (Amputation, Tod).

Für die Häufigkeit und Dauer der Gefährdungsexposition (F) gibt es keine allgemeingültigen Zeiträume. Wird eine Person häufiger als einmal pro Stunde der Gefährdung ausgesetzt (z.B. um Werkstücke zuzuführen) sollte F2 (häufig bis andauernd) gewählt werden. Es ist auch unerheblich, ob dieselbe oder unterschiedliche Personen der Gefährdung ausgesetzt werden. Ist ein Zugang nur von Zeit zu Zeit notwendig, kann F1 (selten bis weniger häufig) gewählt werden.

Wenn die Häufigkeit höher als einmal je 15 Minuten ist und keine andere Rechtfertigung vorliegt, sollte F2 gewählt werden. F1 darf gewählt werden, wenn die gesamte Expositionsdauer 1/20 der gesamten Betriebsdauer nicht überschreitet und die Häufigkeit nicht höher als einmal je 15 Minuten ist.

Die Möglichkeit zur Vermeidung (P) wird durch verschiedene Aspekte beeinflusst. Hier ist die Ausbildung und der Wissensstand der Bediener zu betrachten, sowie die Möglichkeiten der Vermeidung durch z. B. Flucht als auch Betrieb unter Aufsicht oder ohne Beaufsichtigung. Der Parameter **P1** (möglich unter bestimmten Bedingungen) sollte nur gewählt werden, wenn tatsächlich die Möglichkeit besteht, einen Unfall zu vermeiden oder sein Schadensausmaß erheblich zu reduzieren.

Wenn die Eintrittswahrscheinlichkeit des Gefährdungsereignisses als niedrig bewertet werden kann, darf der notwendige Performance Level (PL) um eine Stufe verringert werden.

Die Performance Level (PL) sind ein quantitatives Maß für die Safety Performance genauso wie die Safety Integrity Level (SIL) in IEC 61508 und IEC 62061.

Safety Performance für Realisierung der Steuerung nach IEC 62061

Das in IEC 62061 im Anhang A beschriebene Verfahren verwendet ein tabellarisches Verfahren, das direkt zur Dokumentation der durchgeführten Risikobewertung und SIL-Zuweisung verwendet werden kann.

Für die einzelnen Risikoparameter ist anhand der im Kopf der Tabelle vorgegebenen Werte die zugehörige Gewichtung auszuwählen. Die Summe der Gewichte aller Parameter ergibt die Wahrscheinlichkeitsklasse des Schadens.

$$K = F + W + P$$

Die Häufigkeit und Dauer des Aufenthaltes wird durch den Parameter "F" ausgedrückt. Die Notwendigkeit des Zugangs zum Gefahrenbereich kann in einzelnen Betriebsarten unterschiedlich sein (Automatikbetrieb, Wartungsbetrieb, ...), auch die Art des Zugangs (Werkzeugeinstellungen, Materialzuführung,...) spielt eine Rolle und muss unter diesem Aspekt betrachtet werden. Die zutreffende Häufigkeit und Dauer wird aus der zugehörigen Tabelle ausgewählt. Wenn die Aufenthaltsdauer kleiner als 10 Minuten beträgt, kann der Wert auf die nächste Stufe verringert werden. Jedoch darf der Wert für Häufigkeit ≤ 1 h nie verringert werden.

Die Eintrittswahrscheinlichkeit des Gefährdungsereignisses wird durch den Parameter "W" ausgedrückt. Dieser muss unabhängig von den anderen Parametern abgeschätzt werden. Hierbei muss auch das menschliche Verhalten (bedingt durch z. B. Zeitdruck,

5.1 Sicherheitsbezogene Teile für die Maschinensteuerung

fehlendes Bewusstsein für die Gefahr,...) berücksichtigt werden. Unter normalen Produktionsbedingungen und unter Betrachtung des Worst-Case ist die Wahrscheinlichkeit "sehr hoch". Bei Verwendung eines niedrigen Wertes muss eine detaillierte Begründung vorliegen (z. B. Fähigkeiten der Bediener auf hohem Niveau).

Die Möglichkeit der Vermeidung oder Begrenzung des Schadens wird durch den Parameter "P" ausgedrückt. Hierbei sind Aspekte zu berücksichtigen, die sowohl die Maschine betreffen (z. B. Möglichkeit, sich der Gefährdung zu entziehen) als auch der Möglichkeit, die Gefährdung zu erkennen (z.B. laute Umgebungsgeräusche machen Erkennen unmöglich). Die Einstufung erfolgt entsprechend der Tabelle (wahrscheinlich, möglich, unmöglich).

Mit Hilfe dieser Wahrscheinlichkeitsklasse und der möglichen Schadensschwere der betrachteten Gefährdung kann dann aus der Tabelle der notwendige SIL für die zugehörige Sicherheitsfunktion abgelesen werden.

Ziel ist es einen geforderten Sicherheits-Integritätslevel SIL des Systems durch die Risikoelemente zu ermitteln.

Häufigkeit und / oder Aufenthaltsdauer		Eintrittswahrscheinlichkeit des Gefährdungereignisses		Möglichkeit der Vermeidung	
F		W		P	
≤ 1 Std.	5	häufig	5		
> 1 Std. bis ≤ 1 Tag	5	wahrscheinlich	4		
> 1 Tag bis ≤ 2 Wo.	4	möglich	3	unmöglich	5
> 2 Wo. bis ≤ 1 Jahr	3	selten	2	möglich	3
> 1 Jahr	2	vernachlässigbar	1	wahrscheinlich	1

Auswirkungen	Schadensausmaß	Klasse K = F + W + P				
		3-4	5-7	8-10	11-13	14-15
Tod, Verlust von Auge oder Arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, Verlust von Fingern	3	andere Maßnahmen			SIL 2	SIL 3
Reversibel, medizinische Behandlung	2	andere Maßnahmen			SIL 1	SIL 2
Reversibel, Erste Hilfe	1	andere Maßnahmen			SIL 1	

Bild 5-3 Bestimmung des erforderlichen SIL

5.2 Spezifikation der Sicherheitsanforderungen

Spezifikation der Sicherheitsanforderungen

Wurden Steuerungsfunktionen als sicherheitsrelevant identifiziert oder sollen Schutzmaßnahmen mit Mitteln der Steuerung realisiert werden, sind die genauen Anforderungen für diese "Sicherheitsfunktionen" ("sicherheitsrelevanten Steuerungsfunktionen") in der Spezifikation der Sicherheitsanforderungen ("safety requirements specification") festzulegen. Diese Spezifikation beschreibt für jede sicherheitsrelevante Funktion u. a.:

- deren Funktionalität, d. h. alle erforderlichen Eingangsinformationen, deren Verknüpfung und die zugehörigen Ausgangszustände oder Aktionen, sowie die Benutzungshäufigkeit
- die notwendigen Reaktionszeiten
- die geforderte Safety Performance

Die Spezifikation der Sicherheitsanforderungen enthält alle Information, die für den Entwurf und die Implementierung der Steuerung notwendig ist. Sie ist die Schnittstelle zwischen Maschinenkonstrukteur und Hersteller / Integrator der Steuerung und kann so auch zur Abgrenzung von Verantwortlichkeiten dienen.

5.3 Entwurf und Realisierung der (sicherheitsrelevanten) Steuerung nach IEC 62061

5.3.1 Philosophie / Theorie

Strukturierungsprinzip für ein sicherheitsrelevantes Steuerungssystem

Wesentliche Voraussetzung für das korrekte und bestimmungsgemäße Funktionieren einer Steuerung ist deren korrekte Konstruktion. Um dieses Ziel zu erreichen hat IEC 62061 einen systematischen top down Entwurfsprozess definiert:

Ein sicherheitsrelevantes elektrisches Steuerungssystem (Safety related electrical control system, SRECS) umfasst alle Komponenten von der Informationserfassung über die Informationsverknüpfung bis einschließlich der Ausführung von Aktionen. Um eine einfache systematische Vorgehensweise für den Entwurf, die sicherheitstechnische Bewertung und die Realisierung eines SRECS, das die Anforderungen von IEC 61508 erfüllen soll, zu ermöglichen, verwendet IEC 62061 ein Strukturierungsprinzip, das auf folgenden Architekturelementen beruht (siehe folgendes Bild).

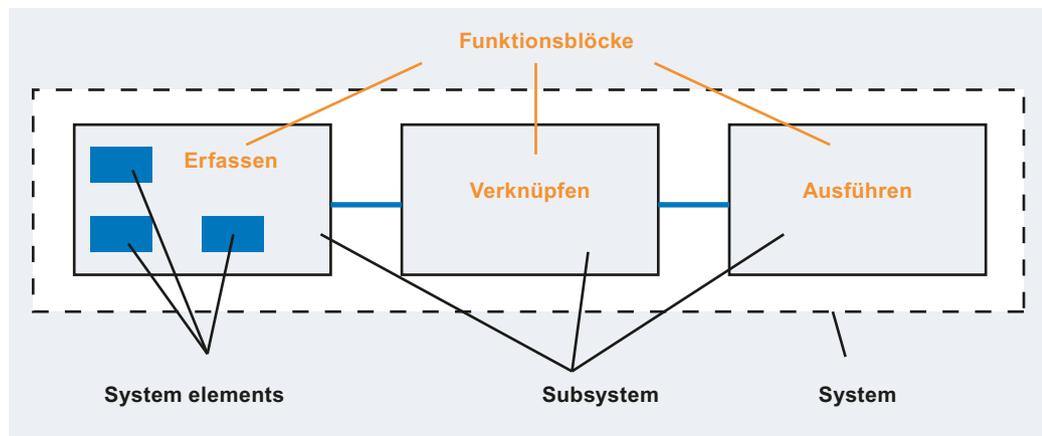


Bild 5-4 Strukturierungselemente der Systemarchitektur

Zunächst wird zwischen einer "virtuellen (d. h. funktionalen) Sicht" und der "realen (d. h. System-) Sicht" unterschieden. Die funktionale Sicht betrachtet nur die funktionalen Aspekte, unabhängig von der Realisierung durch Hard- und Software. In der virtuellen Sicht wird z.B. nur betrachtet, welche Information zu erfassen ist, wie diese zu verknüpfen ist und welche Aktion daraus resultieren soll. Es wird aber noch keine Aussage darüber gemacht, ob z.B. zur Erfassung der Informationen redundante Sensoren erforderlich sind oder wie die Aktoren realisiert werden. Erst mit der "realen Sicht" wird die Realisierung durch das SRECS betrachtet. Hier muss dann entschieden werden, ob z.B. zur Realisierung der Erfassung einer bestimmten Information ein oder zwei Sensoren notwendig sind, um die geforderte Safety Performance zu erreichen. Es werden die folgenden Begriffe definiert.

Begriffe für die Strukturierung der Funktionen (funktionale Sicht)

- **Funktionsblock**
Kleinste Einheit einer sicherheitsbezogenen Steuerungsfunktion (SRCF), deren Ausfall zum Ausfall der sicherheitsbezogenen Steuerungsfunktion führt.
Anmerkung: In IEC 62061 wird eine SRCF (F) als logische "und" Verknüpfung der Funktionsblöcke (FB) betrachtet, z. B. $F = FB1 \ \& \ FB2 \ \& \ \dots \ \& \ FBn$. Die Definition eines Funktionsblocks unterscheidet sich von den in IEC 61131 und anderen Normen verwendeten.
- **Funktionsblock-Element**
Teil eines Funktionsblocks.

Begriffe für die Strukturierung des realen Systems (Systemsicht)

- **Sicherheitsbezogenes elektrisches Steuerungssystem**
Elektrisches Steuerungssystem einer Maschine, dessen Ausfall zu einer unmittelbaren Erhöhung des Risikos führen kann.
Anmerkung: Ein SRECS umfasst alle Teile eines elektrischen Steuerungssystems, deren Ausfall zu einer Reduzierung oder dem Verlust der funktionalen Sicherheit führen kann. Dies kann beides, Energie- und Steuerkreise, umfassen.
- **Subsystem**
Teil des Architekturdesigns des SRECS auf oberster Ebene, wobei ein Ausfall irgendeines Subsystems zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führt.
Anmerkung: Im Unterschied zum allgemeinen Sprachgebrauch, in dem "Subsystem" irgendeine unterteilte Einheit bedeuten kann, wird der Begriff "Subsystem" in IEC 62061 in einer streng definierten Hierarchie der Terminologie verwendet. "Subsystem" bedeutet die Unterteilung auf oberster Ebene. Die Teile, die aus einer weiteren Unterteilung eines Subsystems hervorgehen, werden "Subsystem-Elemente" genannt
- **Subsystem-Element**
Teil eines Subsystems, das eine einzelne Komponente oder eine Gruppe von Komponenten umfasst. Mit diesen Strukturierungselementen können Steuerungsfunktionen nach einem eindeutigen Verfahren so strukturiert werden, dass definierte Teile der Funktion (Funktionsblöcke) bestimmten Hardwarekomponenten, den Subsystemen, zugeordnet werden können. Für die einzelnen Subsysteme ergeben sich dadurch klar definierte Anforderungen, sodass sie unabhängig voneinander entworfen und realisiert werden können. Die Architektur zur Realisierung des vollständigen Steuerungssystems ergibt sich, indem die Subsysteme untereinander so angeordnet werden wie die Funktionsblöcke innerhalb der Funktion (logisch) angeordnet sind.

5.3.2 Entwurfsprozess eines sicherheitsrelevanten Steuerungssystems SRECS

Entwurfsprozess

Wenn die Spezifikation der Sicherheitsanforderungen vorliegt, kann das vorgesehene Steuerungssystem entworfen und implementiert werden. Ein Steuerungssystem, das den spezifischen Anforderungen einer bestimmten Anwendung genügt, kann im allgemeinen nicht fertig gekauft werden, sondern muss aus verfügbaren Geräten individuell für die betreffende Maschine entworfen und aufgebaut werden.

Im Entwurfsprozess wird schrittweise zunächst für jede Sicherheitsfunktion eine geeignete Architektur des Steuerungssystems entworfen. Anschließend können die Architekturen aller Sicherheitsfunktionen der betreffenden Maschine zu einem Steuerungssystem integriert werden.

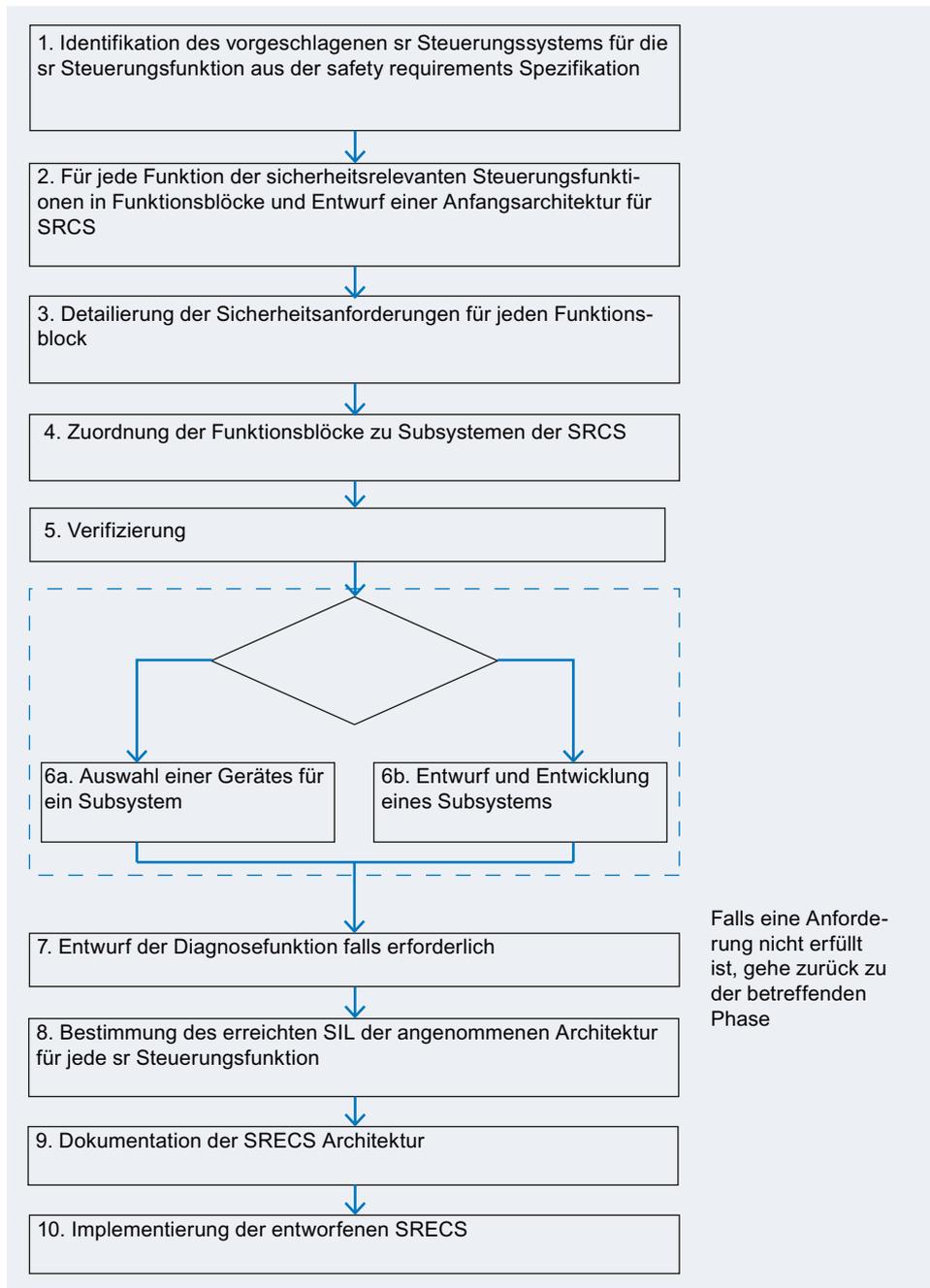


Bild 5-5 Designprozess eines sicherheitsrelevanten Steuerungssystems

Strukturierung der Sicherheitsfunktion

Das Grundprinzip des strukturierten Entwurfs besteht darin, jede Steuerungsfunktion in (gedachte) Funktionsblöcke so zu unterteilen, dass diese bestimmten Subsystemen zugeordnet werden können. Die Abgrenzung der einzelnen Funktionsblöcke wird dabei so gewählt, dass sie vollständig von bestimmten Subsystemen ausgeführt werden können. Wichtig ist dabei, dass jeder Funktionsblock eine logische Einheit darstellt, die korrekt ausgeführt werden muss, damit die gesamte Sicherheitsfunktion korrekt ausgeführt wird.

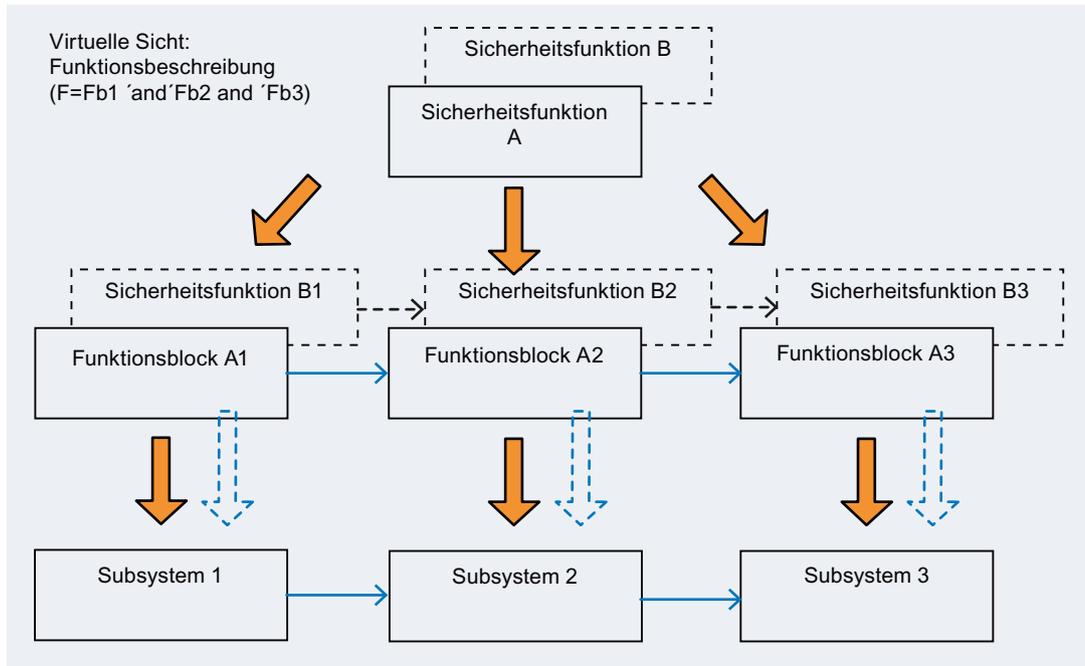


Bild 5-6 Aufteilung einer Sicherheitsfunktion in Funktionsblöcke und Zuordnung zu Subsystemen

Safety Performance eines Subsystems nach IEC 62061

Die "Safety Integrity" nach IEC 62061 erfordert die Erfüllung der drei Grundanforderungen, die entsprechend dem SIL abgestuft sind:

1. Systematische Integrität,
2. Strukturelle Einschränkungen, d.h. Fehlertoleranz und
3. Begrenzte Wahrscheinlichkeit gefährlicher zufälliger (Hardware) Ausfälle (PFH₀).

Die für die ganze Funktion geforderte systematische Integrität (1) des Systems sowie die strukturellen Einschränkungen (2) gelten für die einzelnen Subsysteme genauso wie für das System. D. h. wenn jedes einzelne Subsystem die geforderte systematische Integrität und die strukturellen Einschränkungen eines bestimmten SIL erfüllt, dann erfüllt sie das System auch. Erfüllt jedoch ein Subsystem nur die geringeren Anforderungen eines niedrigeren SIL, dann begrenzt das den SIL, den das System erreichen kann. Man spricht deshalb vom "SIL claim limit" (SIL CL) eines Subsystems.

- Systematische Integrität: $SIL_{SYS} \leq SIL_{CL_{lowest}}$
- Strukturelle Einschränkungen: $SIL_{SYS} \leq SIL_{CL_{lowest}}$

Die Begrenzung der Wahrscheinlichkeit gefahrbringender zufälliger Fehler (3) gilt für die gesamte Funktion, d. h. sie darf von allen Subsystemen zusammen nicht überschritten werden. Es gilt somit:

$$PFH_D = PFH_{D1} + \dots + PFH_{Dn}$$

5.3.3 Systemdesign für eine Sicherheitsfunktion

Architekturentwurf

Die Architektur eines Steuerungssystems für eine bestimmte Sicherheitsfunktion entspricht in ihrer logischen Struktur der zuvor ermittelten Struktur der Sicherheitsfunktion. Zur Festlegung der realen Systemstruktur werden die Funktionsblöcke der Sicherheitsfunktion bestimmten Subsystemen zugeordnet. Die Subsysteme werden dann so miteinander verschaltet, dass die durch die Funktionsstruktur vorgegebenen Verbindungen hergestellt werden. Die physikalische Verschaltung erfolgt entsprechend den Eigenschaften der gewählten Technik, z. B. durch Einzelverdrahtung (Punkt zu Punkt) oder durch Busverbindung.

Für weitere Sicherheitsfunktionen der Maschine oder Anlage wird ebenso verfahren. Dabei können aber Funktionsblöcke, die denjenigen anderer Sicherheitsfunktionen entsprechen, denselben Subsystemen zugeordnet werden. Wenn also z. B. für zwei verschiedene Funktionen dieselbe Information erfasst werden muss (z. B. Position derselben Schutztür), dann können dazu dieselben Sensoren verwendet werden.

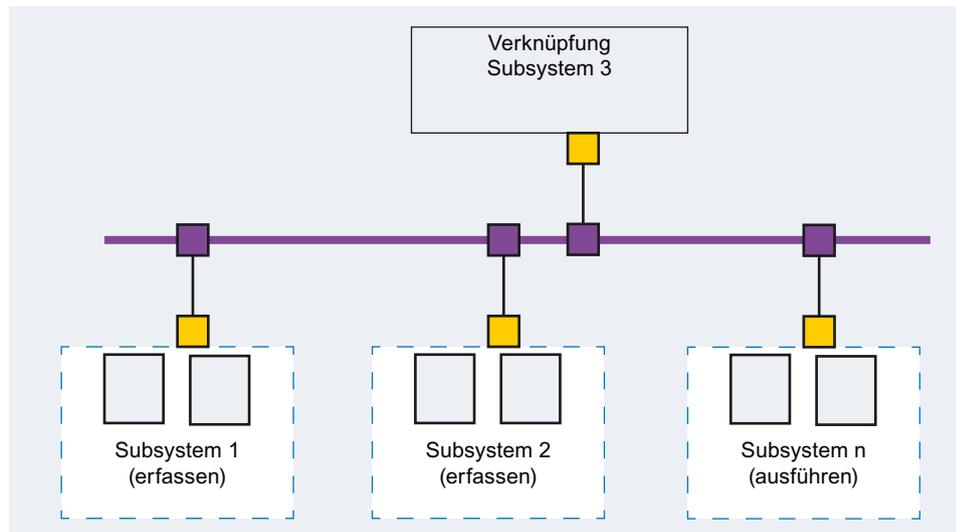


Bild 5-7 Beispiel einer Systemarchitektur für eine Sicherheitsfunktion

Auswahl geeigneter Geräte (Subsysteme)

Ein Subsystem, das zur Implementierung einer Sicherheitsfunktion eingesetzt werden soll, muss die geforderte Funktionalität haben und den betreffenden Anforderungen von IEC 62061 genügen. Mikroprozessorbasierte Subsysteme müssen IEC 61508 für den entsprechenden SIL erfüllen.

Die einzelnen Subsysteme müssen die in der Spezifikation geforderten Sicherheitsparameter (SIL CL und PFH_D) erfüllen.

In vielen Fällen benötigen Geräte noch zusätzliche Fehleraufdeckungsmaßnahmen (Diagnose), um die für ihre Verwendung als Subsystem angegebene Safety Performance tatsächlich zu erreichen. Diese Fehleraufdeckung kann z. B. durch Zusatzgeräte (z. B. Sicherheitsschaltgeräte SIRIUS 3SK1) oder entsprechende Software-Diagnosebausteine in der Logikverarbeitung erfolgen. Für diesen Fall muss die Beschreibung des Gerätes entsprechende Informationen enthalten.

Wenn kein geeignetes Gerät zur Verfügung steht, das den Anforderungen eines so spezifizierten Subsystems genügt, muss es aus verfügbaren Geräten zusammengesetzt werden. Das erfordert einen nächsten Entwurfsschritt. Siehe dazu Abschnitt "Entwurf und Realisierung von Subsystemen (Seite 201)".

5.3.4 Realisierung des sicherheitsrelevanten Steuerungssystems

Ein sicherheitsrelevantes Steuerungssystem muss so realisiert werden, dass es alle Anforderungen entsprechend dem verlangten SIL erfüllt. Ziel ist es, die Wahrscheinlichkeit sowohl systematischer als auch zufälliger Fehler, die zu gefährlichem Versagen der Sicherheitsfunktion führen können, ausreichend klein zu machen. Folgende Aspekte sind zu beachten:

- Hardwareintegrität, d. h. Architectureinschränkungen, (Fehlertoleranz) und begrenzte Versagenswahrscheinlichkeit,
- Systematische Integrität, d. h. Anforderungen zur Vermeidung und Beherrschung von Fehlern,
- Verhalten bei Aufdecken eines Fehlers und Softwaredesign / Softwareentwicklung

Hardwareintegrität

Jedes Subsystem muss eine für den SIL des Systems ausreichende Fehlertoleranz haben. Diese ist abhängig davon, wie groß der Anteil der Fehler, die in eine sichere Richtung gehen, bezogen auf die Wahrscheinlichkeit aller möglichen Fehler des Subsystems ist. Potentiell gefährliche Fehler eines Subsystems, die durch Diagnose rechtzeitig aufgedeckt werden, gehören dabei zu den Fehlern, die in eine sichere Richtung gehen.

Die erlaubte Wahrscheinlichkeit des Versagens einer Sicherheitsfunktion ist durch den in der Spezifikation festgelegten SIL begrenzt.

Systematische Integrität

Es sind Maßnahmen sowohl zur Vermeidung systematischer Fehler als auch zur Beherrschung im System verbliebener Fehler anzuwenden.

Vermeidung systematischer Fehler:

- Das System ist gemäß Sicherheitsplan zu installieren
- Die Herstellerangaben der verwendeten Geräte sind zu befolgen
- Die elektrische Installation gemäß IEC 60204-1 (7.2, 9.1.1 und 9.4.3) auszuführen
- Das Design auf seine Eignung und Korrektheit überprüfen
- Verwendung eines rechnergestützten Tools, das vorkonfigurierte und erprobte Elemente benutzt.

Beherrschung systematischer Fehler:

- Verwendung des Prinzips der Energieabschaltung
- Maßnahmen zur Beherrschung temporärer Subsystemausfälle oder -störungen, z. B. wegen Spannungsunterbrechungen
- Bei Verbindung der Subsysteme durch einen Bus sind die Anforderungen von IEC 61508-2 an die Datenkommunikation zu erfüllen (z. B. PROFIsafe und ASIsafe)
- Fehler in der Verbindung (Verdrahtung) und den Schnittstellen der Subsysteme müssen erkannt und geeignete Reaktionen veranlasst werden. Für die systematische Behandlung werden die Schnittstellen und die Verdrahtung als Bestandteil des betreffenden Subsystems betrachtet.

Details siehe IEC 62061 6.4

Verhalten beim Aufdecken eines Fehlers

Wenn Fehler eines Subsystems zu einem gefährlichen Versagen einer Sicherheitsfunktion führen können, müssen diese rechtzeitig aufgedeckt und eine geeignete Reaktion veranlasst werden, um eine Gefahr zu vermeiden. In welchem Maße automatische Fehleraufdeckung (Diagnose) notwendig ist, hängt von den Ausfallraten der verwendeten Geräte und dem zu erreichenden SIL des Systems (bzw. der geforderten PFH des Subsystems) ab.

Wie sich das System bzw. Subsystem bei Erkennen eines Fehlers verhalten muss, ist abhängig von der Fehlertoleranz des betreffenden Subsystems. Führt der erkannte Fehler nicht direkt zum Versagen der Sicherheitsfunktion, d. h. Fehlertoleranz > 0 , ist eine Fehlerreaktion nicht sofort notwendig, sondern erst wenn die Wahrscheinlichkeit für das Auftreten eines zweiten Fehlers zu groß wird (in der Regel sind das Stunden oder Tage). Führt der erkannte Fehler direkt zum Versagen der Sicherheitsfunktion, d. h. Fehlertoleranz $= 0$, ist eine Fehlerreaktion sofort, d. h. bevor eine Gefahr eintritt, notwendig.

5.3.4.1 Erreichte Safety Performance

Erreichte Safety Performance

Für jede Sicherheitsfunktion ist in ihrer Spezifikation festgelegt, welche Safety Performance sie benötigt. Diese muss von dem sicherheitsrelevanten Steuerungssystem erfüllt werden.

Welche Safety Performance ein System erreicht, muss für jede Sicherheitsfunktion ermittelt werden. Dies erfolgt anhand der Architektur des Systems und der Sicherheitsparameter der Subsysteme, die an der Ausführung der betrachteten Sicherheitsfunktion beteiligt sind.

Design nach IEC 62061

Der erreichte SIL wird begrenzt durch die "SIL-Eignung" seiner Subsysteme. Der niedrigste Wert der eingesetzten Subsysteme begrenzt den SIL des Systems auf diesen Wert (Das schwächste Glied einer Kette bestimmt deren Festigkeit.).

- Systematische Integrität: $SIL_{SYS} \leq SIL_{CL_{lowest}}$
- Strukturelle Einschränkungen: $SIL_{SYS} \leq SIL_{CL_{lowest}}$

Für die Verbindung der Subsysteme untereinander müssen die gleichen Anforderungen erfüllt werden. Dazu werden Einzelverdrahtungen als Bestandteil jeweils eines der beiden verbundenen Subsysteme betrachtet. Bei Busverbindung sind Sende- und Empfangshardware und -software Bestandteile der Subsysteme.

Außer dieser prinzipiellen Eignung muss außerdem die Wahrscheinlichkeit gefährlichen Versagens jeder Sicherheitsfunktion betrachtet werden. Dieser Wert ergibt sich durch einfache Addition der Versagenswahrscheinlichkeiten der an der Funktion beteiligten Subsysteme:

$$PFH_D = PFH_{D1} + \dots + PFH_{Dn}$$

Bei Busverbindungen muss zusätzlich noch die Wahrscheinlichkeit möglicher Datenübertragungsfehler (PTE) addiert werden.

Der für eine bestimmte Sicherheitsfunktion so ermittelte Wert muss kleiner (oder gleich) sein als der durch den zugehörigen SIL festgelegte Wert.

Tabelle 5-1 Grenzwerte der Wahrscheinlichkeiten gefahrbringender Fehler einer Sicherheitsfunktion

Wahrscheinlichkeit eines gefahrbringenden Fehlers pro Stunde (PFH _D)			
	SIL 1	SIL 2	SIL3
PFH _D	< 10 ⁻⁵	< 10 ⁻⁶	< 10 ⁻⁷

5.3.5 Systemintegration für alle Sicherheitsfunktionen

Nachdem die Architekturen für alle Sicherheitsfunktionen entworfen sind, folgt als nächster Schritt die Integration dieser funktionspezifischen Architekturen zu dem vollständigen sicherheitsrelevanten Steuerungssystem.

Dort, wo mehrere Sicherheitsfunktionen identische Funktionsblöcke haben, können für deren Realisierung gemeinsame Subsysteme verwendet werden:

- Z. B. braucht man nur eine Sicherheits-SPS zur Implementierung der Logik aller Sicherheitsfunktionen.
- Wenn zur Beseitigung unterschiedlicher Gefährdungen (d. h. unterschiedliche Sicherheitsfunktionen) der Zustand derselben Schutztür erfasst werden muss, braucht der notwendige Sensor an dieser Tür nur einmal installiert zu werden.

Auf die Safety Integrity, die für die einzelnen Funktionen bereits bestimmt wurde, hat dies keinen Einfluss. Lediglich bei den elektromechanischen (verschleißbehafteten) Geräten muss das bei der Bestimmung ihrer Schalthäufigkeit berücksichtigt werden.

5.3.6 Entwurf und Realisierung von Subsystemen

Als Alternative zur Auswahl eines vorhandenen Subsystems kann ein Subsystem auch aus Geräten, die alleine nicht die Sicherheitsanforderungen erfüllen, so zusammengesetzt werden, dass das Subsystem dann die notwendige Safety Performance erreicht. Das ist bezüglich der systematischen Integrität und der strukturellen Einschränkungen das durch den SIL der Sicherheitsfunktion vorgegebene SIL claim limit (SIL CL). Für die Wahrscheinlichkeit gefahrbringender zufälliger Fehler (PFH_D) wurden beim Entwurf der Systemarchitektur die maximalen PFH Werte für die einzelnen Subsysteme festgelegt.

Zumindest für SIL 2 und SIL 3 wird im Allgemeinen Redundanz benötigt. Sei es, um die notwendige Fehlertoleranz zu erreichen, oder um Fehleraufdeckung (Diagnose) zu ermöglichen. Die Kombination zweier Geräte zu einem Subsystem kann aber auch erforderlich sein, um die Wahrscheinlichkeit eines gefährlichen Versagens zu verringern.

Die genauen Anforderungen für Entwurf und Realisierung von Subsystemen sind in IEC 62061 Abschnitt 6.7 und 6.8 beschrieben. Die folgende Beschreibung vermittelt einen Überblick.

Subsystem Architekturentwurf

Eine spezielle Subsystemarchitektur ist immer dann zu entwerfen, wenn mit den für eine bestimmte Aufgabe (Teilfunktion, "Funktionsblock") vorgesehenen Geräten die notwendige Safety Integrity (Safety Performance) nicht direkt erreicht wird. Im Allgemeinen können die sicherheitstechnischen Eigenschaften

- Geringe Versagenswahrscheinlichkeit
- Fehlertoleranz, Fehlerbeherrschung
- Fehleraufdeckung

nur durch besondere Architekturmaßnahmen erreicht werden. In welchem Umfang bestimmte Maßnahmen notwendig sind, ist abhängig von der geforderten Safety Performance (Safety Integrity).

Dem Subsystem ist eine bestimmte (Teil-)Funktion, der Funktionsblock, zugeordnet (z. B. Zuhalten einer Tür). Dieser Funktionsblock wird zunächst (gedanklich) in einzelne Elemente (Funktionsblockelemente) unterteilt, die dann bestimmten Geräten, den Subsystemelementen, zugeordnet werden können. Im Allgemeinen kann die gleiche Funktion zwei Funktionsblockelementen zugeteilt werden (die Funktion wurde praktisch verdoppelt). Wenn diese Funktionsblockelemente dann durch jeweils eigene Geräte realisiert werden, hat das Subsystem eine einfache Fehlertoleranz (einfache Redundanz).

Fehleraufdeckung eines Subsystems (Diagnose)

Bei einem Subsystem ohne Fehlertoleranz führt jeder Fehler zum Verlust der Funktion. Das Versagen der Funktion kann, abhängig von der Art des Fehlers, zu einem gefährlichen oder sicheren Zustand der Maschine führen. Kritisch sind die Fehler, die einen gefährlichen Zustand der Maschine zur Folge haben. Sie werden als "gefahrbringende Fehler" bezeichnet. Um zu vermeiden, dass ein gefahrbringender Fehler tatsächlich zu einer Gefährdung führt, kann man bestimmte Fehler durch Diagnose aufdecken und die Maschine in einen sicheren Zustand bringen, bevor die Gefährdung entsteht. Ein durch die Diagnose aufgedeckter gefahrbringender Fehler kann so in einen "sicheren Fehler" umgewandelt werden.

Bei einem redundanten Subsystem führt der erste Fehler noch nicht zum Versagen seiner Funktion. Erst ein weiterer Fehler kann den Verlust der Funktion verursachen. Um das Versagen des Subsystems zu vermeiden, muss also der erste Fehler aufgedeckt werden bevor ein zweiter Fehler auftritt. Die Fehleraufdeckung muss natürlich mit einer geeigneten Systemreaktion verbunden sein. Im einfachsten Fall wird z. B. die Maschine angehalten, um sie in einen sicheren Zustand zu bringen, der die (fehlerhafte) Sicherheitsfunktion nicht benötigt.

Durch die Fehleraufdeckung (Diagnose) verbunden mit einer geeigneten Fehlerreaktion wird in beiden Fällen die Wahrscheinlichkeit eines gefährlichen Versagens der betreffenden Sicherheitsfunktion verringert. In welchem Maße die Wahrscheinlichkeit verringert wird hängt u. a. davon ab, wie viele der möglichen gefährlichen Fehler erkannt werden. Das Maß dafür ist der Diagnosedeckungsgrad (diagnostic coverage DC).

Die Fehleraufdeckung eines Subsystems kann im betreffenden Subsystem selber oder durch ein anderes Gerät, z. B. die Sicherheits-SPS erfolgen.

Systematische Integrität eines Subsystems

Bei Design und Implementierung eines Subsystems müssen Maßnahmen sowohl zur Vermeidung als auch zur Beherrschung systematischer Fehler getroffen werden, z. B.:

- Die eingesetzten Geräte müssen die entsprechenden internationalen Normen erfüllen.
- Die vom Hersteller angegebenen Anwendungsbedingungen müssen eingehalten werden.
- Das Design und die verwendeten Materialien müssen so sein, dass sie allen zu erwartenden Umgebungsbedingungen standhalten.
- Das Verhalten aufgrund von Umgebungseinflüssen muss vorherbestimmt sein, sodass ein sicherer Zustand der Maschine erhalten werden kann.
- Online Fehleraufdeckung
- Zwangsbetätigung zur Initiierung einer Schutzmaßnahme

Die in IEC 62061 beschriebenen Anforderungen betreffen nur das Design elektrischer Subsysteme geringer Komplexität, also keine Subsysteme mit Mikroprozessoren. Die geforderten Maßnahmen gelten für alle SIL gleichermaßen.

Ausfallwahrscheinlichkeit (PFH_D) eines Subsystems

Die möglichen Ausfälle werden unterschieden in "sichere" oder "gefährbringende" Ausfälle. Dabei sind die gefährbringenden Ausfälle eines Subsystems wie folgt definiert.

Gefährbringender Ausfall

Ausfall eines SRECS, eines Subsystems oder Subsystemelements mit dem Potenzial, eine Gefährdung oder funktionsunfähigen Zustand zu verursachen.

Anmerkung: Ob ein solcher Zustand eintritt oder nicht, kann von der Systemarchitektur abhängen; in Systemen mit mehrfachen Kanälen zur Verbesserung der Sicherheit führt ein gefährbringender Hardwareausfall mit geringerer Wahrscheinlichkeit zum gefährbringenden Gesamtzustand oder zu einem Funktionsausfall.

Das bedeutet z. B.: Bei einem redundanten Subsystem (d. h. Fehlertoleranz 1) wird ein Fehler eines Kanals als gefährbringend bezeichnet, wenn er potenziell gefährbringend ist, d. h. bei nicht vorhandenem zweiten Kanal zu einem gefährlichen Zustand der Maschine führen kann.

Für die Sicherheitsanforderungen ist nur die Wahrscheinlichkeit gefährbringender Ausfälle maßgebend. Die so genannten "sicheren Fehler" verschlechtern zwar die Verfügbarkeit des Systems, verursachen aber keine Gefährdung.

Die Ausfallwahrscheinlichkeit eines Subsystems ist abhängig von den Ausfallraten der Geräte aus denen das Subsystem aufgebaut ist, der Architektur und den Diagnosemaßnahmen. Für die beiden gebräuchlichsten Architekturen sind die Formeln in der IEC 62061 angegeben.

Struktur ohne Fehlertoleranz mit Diagnose

Bei dieser Struktur (siehe folgendes Bild) versagt das Subsystem, wenn ein beliebiges seiner Elemente versagt, d. h. ein einzelner Fehler führt zum Versagen der eigentlichen Sicherheitsfunktion. Dies bedeutet aber noch nicht zwingend einen gefährlichen Verlust der Sicherheitsfunktion. Abhängig von der Art des Fehlers kann die Maschine in einen sicheren oder einen gefährlichen Zustand gehen, d. h. das Subsystem hat einen "sicheren" oder einen "gefährlichen" Fehler. Ist die Wahrscheinlichkeit gefährlicher Fehler (PFHd) größer als in der Spezifikation vorgegeben, müssen diese Fehler durch Diagnose aufgedeckt und eine Fehlerreaktion veranlasst werden bevor eine Gefahr entsteht. Dadurch werden gefährliche Fehler zu sicheren Fehlern und folglich die Wahrscheinlichkeit eines gefährlichen Versagens des Subsystems verringert, sodass evtl. die in der Spezifikation erlaubte Versagenswahrscheinlichkeit erreicht wird.

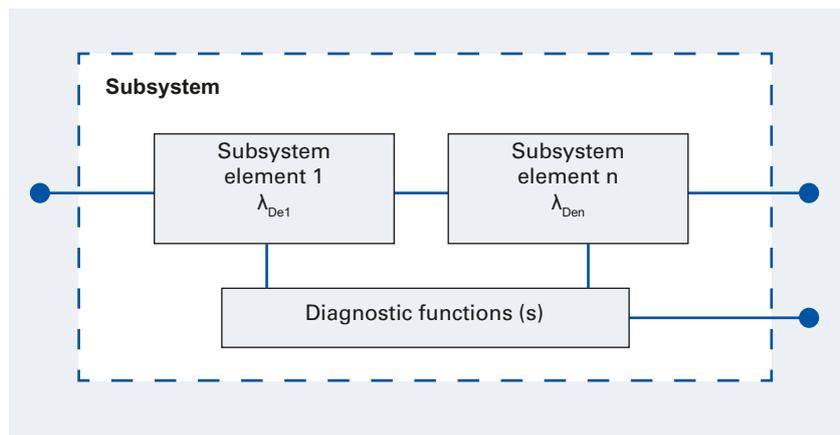


Bild 5-8 Logische Struktur eines Subsystems ohne Fehlertoleranz mit Diagnose

Struktur mit einfacher Fehlertoleranz und mit Diagnose

Bei dieser Struktur (siehe folgendes Bild) führt der erste Fehler noch nicht zum Versagen der Funktion. Der Fehler muss aber aufgedeckt werden, bevor die Wahrscheinlichkeit für das Auftreten eines zweiten Fehlers, d. h. des Versagens des Subsystems, die in der Spezifikation gegebene Grenze überschreitet.

Außer den unabhängigen, zufälligen Fehlern ist bei redundanten Subsystemen noch die Möglichkeit von Fehlern gemeinsamer Ursache (common cause failure) zu beachten. Gegen solche Fehler hilft homogene Redundanz nicht. Beim Entwurf müssen deshalb systematische Maßnahmen getroffen werden, die ihre Wahrscheinlichkeit ausreichend gering machen.

Da common cause Fehler nie ganz ausgeschlossen werden können, müssen sie bei der Berechnung der Ausfallwahrscheinlichkeit des Subsystems berücksichtigt werden. Dies erfolgt mit Hilfe des Common Cause Faktors (β), mit dem die Wirksamkeit der getroffenen Maßnahmen bewertet wird. In Annex F von IEC 62061 befindet sich eine Tabelle zur Bestimmung des erreichten Common Cause Faktors.

Bei dieser Struktur führt ein einzelner Ausfall eines beliebigen Subsystemelements nicht zum Ausfall der sicherheitsrelevanten Steuerungsfunktion.

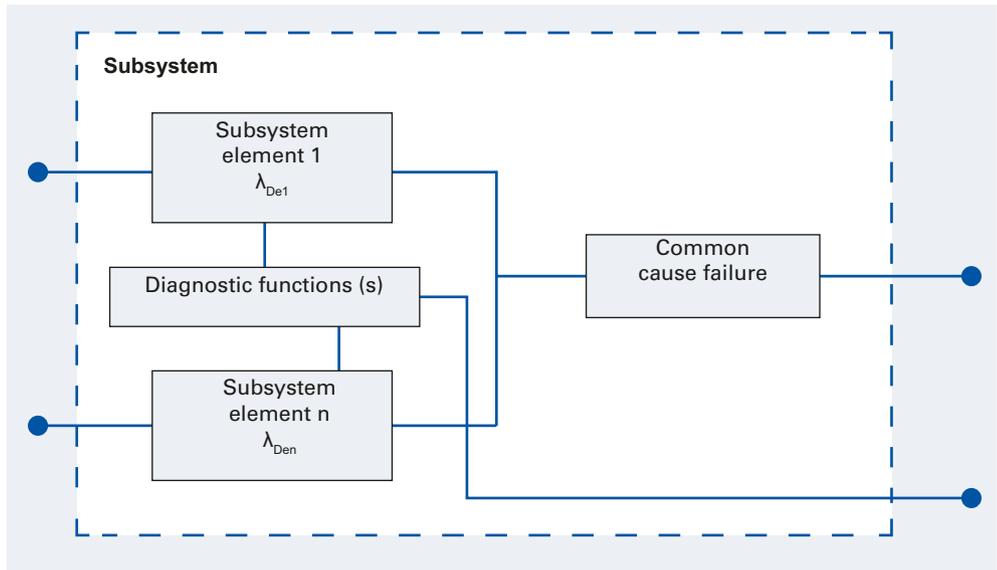


Bild 5-9 Logische Struktur eines Subsystems mit einfacher Fehlertoleranz mit Diagnose

Strukturelle Einschränkungen eines Subsystems

Die strukturellen Einschränkungen fordern ein Minimum an Fehlertoleranz abhängig von der Art der möglichen Fehler des Subsystems. Je größer der Anteil "sicherer" Fehler, desto kleiner ist die geforderte Fehlertoleranz für einen bestimmten SIL.

Folgende Tabelle zeigt die entsprechenden Grenzen. "Sichere Fehler" in diesem Zusammenhang sind auch die potenziell gefährlichen Fehler, die durch Diagnose aufgedeckt werden.

Tabelle 5-2 Strukturelle Einschränkungen eines Subsystems

Anteil sicherer Fehler	Hardwarefehlertoleranz	
	0	1
< 60 %	Nicht erlaubt (Ausnahmen siehe Norm)	SIL 1
60 % bis < 90 %	SIL 1	SIL 2
90 % bis < 99 %	SIL 2	SIL 3
$\geq 99 %$	SIL 3	SIL 3

Anmerkung: Eine Hardwarefehlertoleranz von N bedeutet, dass N+1 Fehler zum Verlust der Funktion führen können.

So ist z.B. für ein Subsystem, das für SIL 2 eingesetzt werden soll, keine Fehlertoleranz gefordert ($FT = 0$) wenn der Anteil seiner Fehler, die in eine sichere Richtung gehen, mehr als 90 % beträgt. Die meisten Geräte erreichen diesen Wert von sich aus nicht. Man kann aber den Anteil der gefährlichen Fehler verringern, indem man die Fehler durch Diagnose aufdeckt und rechtzeitig eine geeignete Reaktion veranlasst.

Die safe failure fraction eines Subsystems ist der prozentuale Anteil der Fehler, die zu einem sicheren Zustand der Maschine führen, an der Menge aller Fehler des Subsystems gewichtet nach deren Auftretenswahrscheinlichkeit.

5.4 Entwurf und Realisierung der sicherheitsbezogenen Teile einer Steuerung nach ISO 13849-1

Zielsetzung

Ein sicherheitsrelevantes (Steuerungs-) System muss eine Sicherheitsfunktion korrekt ausführen. Auch im Fehlerfall muss sie sich so verhalten, dass die Maschine oder Anlage in einem sicheren Zustand bleibt oder gebracht wird.

Ermittlung der notwendigen Safety Performance (Safety Integrity)

Durch den Prozess der Risikobeurteilung (siehe Kapitel "Sicherheitsbezogene Teile für die Maschinensteuerung (Seite 187)") wurden die Anforderungen an die Sicherheitsfunktion ermittelt.

Die ISO 13849-1 schreibt einen erforderlichen Performance Level PL_r vor. Siehe dazu Kapitel "Sicherheitsbezogene Teile für die Maschinensteuerung (Seite 187)".

Entwurfsprozess der sicherheitsbezogenen Teile einer Steuerung

Die Kategorien nach ISO 13849-1 beziehen sich gleichermaßen auf das System (Sicherheitsfunktion) und seine Teilsysteme. Bei der Realisierung nach ISO 13849-1 kann das gleiche Prinzip der Strukturierung des sicherheitsrelevanten Systems angewendet werden wie in der IEC 62061 beschrieben. Jedes so abgegrenzte Teilsystem muss dann den Performance Level erreichen, der für die Schutzfunktion verlangt wird. Die Anforderungen der betreffenden Kategorie gelten auch für die Verdrahtung der Teilsysteme untereinander.

In der ISO 13849-1 wird beim Entwurf neben den Kategorien zusätzlich der Performance Level PL_r als die quantitative Größe für die Ausfallwahrscheinlichkeit eingeführt.

Das folgende Bild zeigt den iterativen Prozess für die Gestaltung der sicherheitsbezogenen Teile von Steuerungen (SRP / CS):

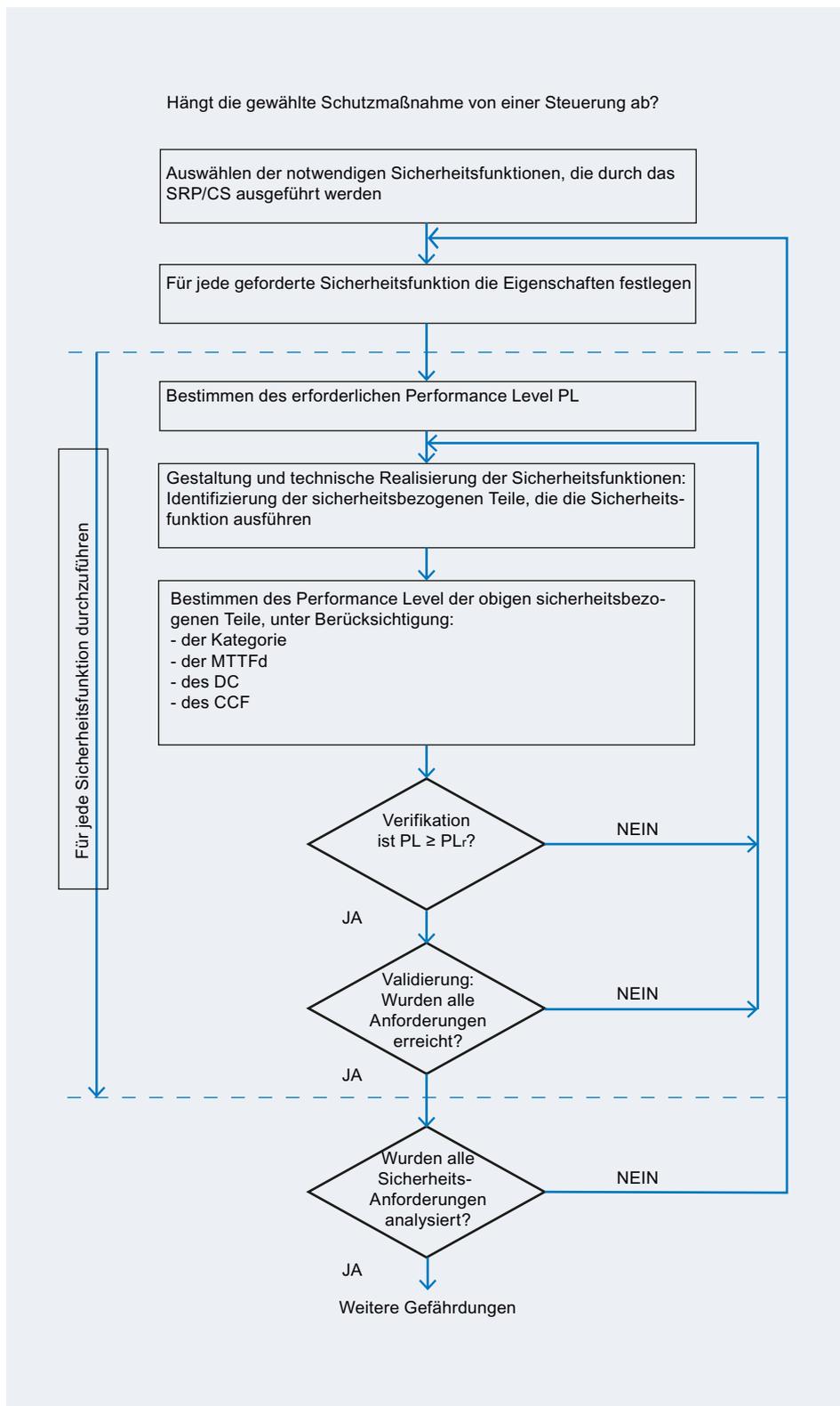


Bild 5-10 Iterativer Prozess für die Gestaltung der sicherheitsbezogenen Teile von Steuerungen

Entwurf nach ISO 13849-1

Der Architekturentwurf richtet sich nach dem erforderlichen Performance Level PL_r .

Das Entwurfskonzept von ISO 13849-1 basiert auf speziellen vordefinierten Architekturen der sicherheitsrelevanten Teile der Steuerung.

Eine Sicherheitsfunktion kann aus einem oder mehreren sicherheitsbezogenen Teilen einer Steuerung (SRP / CS) bestehen.

Eine Sicherheitsfunktion kann auch eine Betriebsfunktion sein, wie z. B. eine Zweihandschaltung zur Einleitung eines Prozesses.

Eine typische Sicherheitsfunktion besteht aus folgenden sicherheitsbezogenen Teilen einer Steuerung:

- Eingang (SRP/CS_a)
- Logik / Bearbeitung (SRP/CS_b)
- Ausgang / Energieübertragungselement (SRP/CS_c)
- Verbindungen (i_{ab} , i_{ac}) (z. B. elektrisch, optisch)

Anmerkung: Sicherheitsbezogene Teile bestehen aus einer oder mehreren Komponenten; Komponenten können aus einem oder mehreren Elementen bestehen.

Alle Verbindungselemente sind in den sicherheitsbezogenen Teilen enthalten.

Wurden die Sicherheitsfunktionen der Steuerung bestimmt, müssen die sicherheitsbezogenen Teile der Steuerung identifiziert werden. Ebenso muss deren Beitrag zu dem Prozess der Risikominderung (ISO 12100) beurteilt werden.

Performance Level PL

Bei der Anwendung der ISO 13849 wird die Fähigkeit sicherheitsbezogener Teile eine Sicherheitsfunktion auszuführen, durch die Bestimmung eines Performance Levels ausgedrückt.

Für jedes gewählte SRP/CS und/oder der Kombination von SRP/CS, die eine Sicherheitsfunktion ausführt, muss eine Abschätzung des PL durchgeführt werden.

Der PL der SRP/CS muss durch die Abschätzung folgender Aspekte bestimmt werden:

- $MTTF_d$ (mittlere Zeit zum gefahrbringenden Ausfall)
- DC (Diagnosedeckungsgrad)
- CCF (Ausfall auf Grund gemeinsamer Ursachen)
- Struktur
- Verhalten der Sicherheitsfunktion unter Fehlerbedingung(en)
- Sicherheitsbezogene Software
- Systematische Ausfälle

Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF_d)

Der Wert der MTTF_d jedes Kanals wird in drei Stufen angegeben und muss für jeden Kanal individuell berücksichtigt werden (z. B. einzelner Kanal oder jeder Kanal eines redundanten Systems). In Bezug auf die MTTF_d kann ein maximaler Wert von 100 Jahren angesetzt werden. Eine Ausnahme bilden Kanäle mit PL e, hier ist die MTTF_d auf 2500 Jahre begrenzt.

MTTF _d	
Niedrig	3 Jahre ≤ MTTF _d < 10 Jahre
Mittel	10 Jahre ≤ MTTF _d < 30 Jahre
Hoch	30 Jahre ≤ MTTF _d ≤ 100 Jahre

Diagnosedeckungsgrad (DC)

Der Wert für den DC wird in vier Stufen angegeben. Zur Abschätzung des DC kann in den meisten Fällen die Ausfallarten- und Effektanalyse (FMEA) oder ähnliche Verfahren verwendet werden. In diesem Fall sollten alle relevanten Fehler und/oder Ausfallarten berücksichtigt werden, und der PL der Kombination des SRP/CS, die die Sicherheitsfunktion ausführen sollte, gegen den erforderlichen Performance Level (PL_r) geprüft werden. Für einen vereinfachten Ansatz zur Abschätzung des DC, siehe ISO 13849-1 Anhang E.

Diagnosedeckungsgrad (DC)	
Kein	DC < 60 %
Niedrig	60 % ≤ DC < 90 %
Mittel	90 % ≤ DC < 99 %
Hoch	99 % ≤ DC

5.4.1 Entwurf und Realisierung von Kategorien

Kategorie B

Zum Erreichen einer Kategorie B müssen die sicherheitsgerichteten Teile der Steuerung die folgenden Anforderungen erfüllen und nach diesen gestaltet, ausgewählt und kombiniert sein.

- Anwendung der grundlegenden Sicherheitsprinzipien
- Standhaltung gegenüber den zu erwartenden Betriebsbeanspruchungen, dazu gehört das Schaltvermögen bzw. die Schalthäufigkeit der Komponenten
- Robustheit gegenüber den Einflüssen des bearbeiteten Materials und Umgebungsbedingungen, dazu gehören z. B. auftretende Stoffe wie Öle, Reinigungsmittel, Salznebel
- Robustheit gegenüber anderen relevanten äußeren Einflüssen, dazu gehören mechanische Schwingungen, elektromagnetische Störungen, Unterbrechungen oder Störungen der Energieversorgung.

In einem Kategorie B System kann der MTTF_d jedes Kanals niedrig bis mittel sein. Einen Diagnosedeckungsgrad gibt es nicht (DC avg = kein). Da die Struktur üblicherweise einkanalig ist, wird eine CCF Betrachtung in dieser Kategorie nicht angewendet, da dies nicht

relevant ist. Der maximal erreichbare Performance Level eines Kategorie B Systems ist $PL = b$. Durch den einkanaligen Aufbau kann ein Fehler zum Verlust der Sicherheitsfunktion führen.

Beispiel einer vorgesehenen Architektur Kategorie B:

- I1: Sensor 1 (z. B. ein Positionsschalter)
- L1: Logikeinheit 1 (z. B. ein Sicherheitsschaltgerät)
- O1: Aktor 1 (z. B. ein Schütz)

Die strukturellen Eigenschaften sind:

- Einkanaliger Aufbau

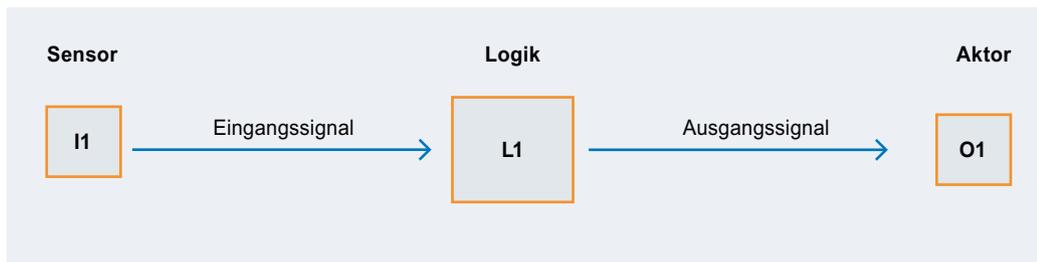


Bild 5-11 Vorgesehene Architektur für Kategorie B

Kategorie 1

Zum Erreichen einer Kategorie 1 müssen die Anforderungen wie für Kategorie B erfüllt sein. Zusätzlich müssen noch die folgenden Anforderungen umgesetzt werden:

Für die sicherheitsgerichteten Teile der Steuerung müssen bewährte Bauteile verwendet werden und bewährte Sicherheitsprinzipien eingehalten werden (siehe ISO 13849-2).

In einem Kategorie 1 System muss der $MTTFd$ jedes Kanals hoch sein.

Der maximal erreichbare Performance Level ist $PL = c$.

Beispiel einer vorgesehenen Architektur Kategorie 1:

- I1: Sensor 1 (z. B. ein Positionsschalter)
- L1: Logikeinheit 1 (z. B. ein Sicherheitsschaltgerät)
- O1: Aktor 1 (z. B. ein Schütz)

Die strukturellen Eigenschaften sind:

- Einkanaliger Aufbau
- Einsatz bewährter Bauteile

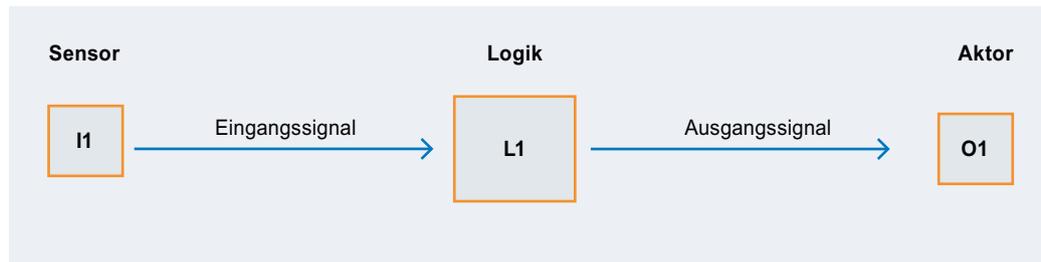


Bild 5-12 Vorgesehene Architektur für Kategorie 1

Kategorie 2

Zum Erreichen einer Kategorie 2 müssen die Anforderungen wie für die Kategorie B erfüllt sein. Es müssen ebenfalls die bewährten Sicherheitsprinzipien eingehalten werden. Zusätzlich gelten die folgenden Anforderungen:

Die sicherheitsbezogenen Teile der Steuerung eines Kategorie 2 Systems müssen in angemessenen Zeitabständen durch die Maschinensteuerung getestet werden. Dieser Test der Sicherheitsfunktion durch die Maschinensteuerung muss durchgeführt werden:

- Bei Maschinenanlauf, sowie
- Vor jedem Einleiten einer Gefährdungssituation, z. B. bei Beginn eines neuen Maschinenzklus, Einleitung anderer Bewegungen, etc.

Als Ergebnis des Tests durch die Testeinrichtung

- muss bei einem erkannten Fehler eine geeignete Fehlerreaktion erfolgen
- darf bei keinem erkannten Fehler der Betrieb zugelassen werden

Die Fehlerreaktion muss wenn immer möglich einen sicheren Zustand einleiten. Erst wenn der Fehler behoben wurde, darf der normale Betrieb fortgesetzt werden. Ist das Erreichen des sicheren Zustandes nicht möglich (z. B. bei verschweißten Kontakten), so muss eine Warnung vor der Gefährdung bereitgestellt werden.

In einem Kategorie 2 System muss der MTTFd jedes Kanals in Abhängigkeit des erforderlichen PLr, niedrig bis hoch sein. Die sicherheitsbezogenen Teile des Steuerungssystems müssen einen niedrigen bis mittleren Diagnosedegrad aufweisen. Gleichzeitig müssen CCF Maßnahmen angewendet werden (siehe ISO 13849-1 Anhang F).

Zusätzlich darf es durch den Test selbst zu keinen weiteren Gefährdungen kommen. Die Testeinrichtung darf ein Bestandteil der sicherheitsbezogenen Teile des Steuerungssystems sein oder aber auch getrennt davon umgesetzt werden.

Der maximal erreichbare Performance Level eines Kategorie 2 Systems ist PL = d.

Hinweis

Bei der Kategorie 2 handelt es sich im Sinne des vereinfachten Verfahrens der ISO 13849-1 um ein einkanaliges getestetes System: wenn ein gefahrbringender Fehler auftritt, dann ist die Fehlererkennung nur dann (sinnvoll) effektiv, wenn der Fehler aufdeckende Test vor der nächsten Anforderung der Sicherheitsfunktion stattfindet. Mit diesem Hintergrund wird eine Testrate gefordert, die 100 Mal größer ist als die Anforderungsrate der Sicherheitsfunktion.

Beispiel einer vorgesehenen Architektur Kategorie 2

- I1: Sensor 1 (z. B. ein Positionsschalter)
- L1: Logikeinheit 1 (z. B. ein Sicherheitsschaltgerät)
- O1: Aktor 1 (z. B. ein Schütz)
- TE: Testeinrichtung

Die strukturellen Eigenschaften sind:

- Einkanaliger Aufbau
- Überwachung durch Testeinrichtung

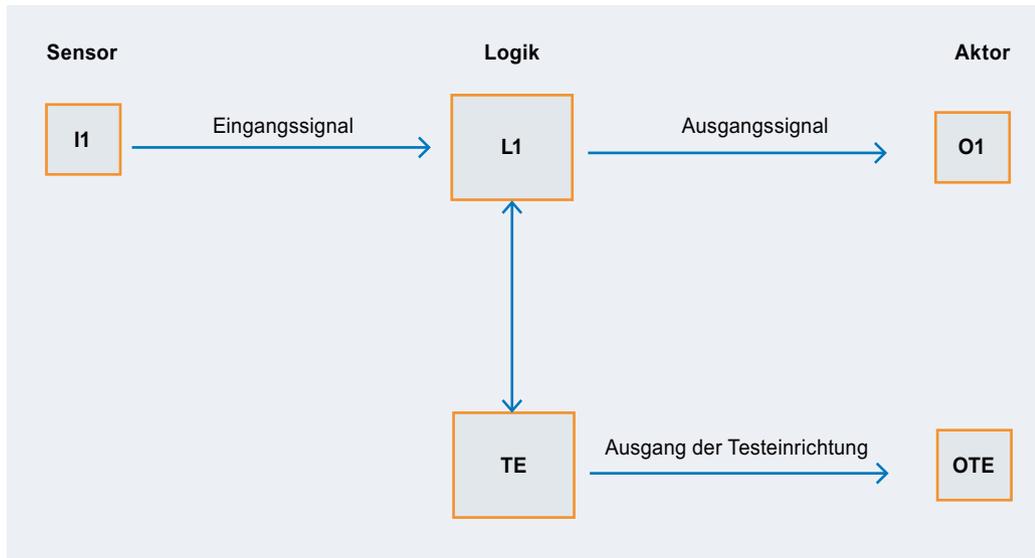


Bild 5-13 Vorgesehene Architektur für Kategorie 2

Kategorie 3

Zum Erreichen einer Kategorie 3 müssen die Anforderungen wie für die Kategorie B erfüllt sein. Es müssen ebenfalls die bewährten Sicherheitsprinzipien eingehalten werden. Zusätzlich gelten die folgenden Anforderungen:

Die sicherheitsbezogenen Teile des Steuerungssystems der Kategorie 3 müssen so ausgelegt werden, dass es bei Auftreten eines einzelnen Fehlers nicht zum Verlust der Sicherheitsfunktion kommt. Der einzelne Fehler muss, wenn immer möglich, bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.

In einem Kategorie 3 System muss der MTTFd jedes redundanten Kanals in Abhängigkeit des erforderlichen PLr, niedrig bis hoch sein. Die sicherheitsbezogenen Teile des Steuerungssystems müssen einen niedrigen bis mittleren Diagnosedeckungsgrad aufweisen. Gleichzeitig müssen CCF Maßnahmen angewendet werden (siehe ISO 13849-1 Anhang F).

Beispiel einer vorgesehenen Architektur Kategorie 3:

- I1 und I2: Sensor 1 und 2 (z. B. zwei Positionsschalter mit zwangsöffnenden Kontakten)
- L1 und L2: Logikeinheit 1 und 2 (ein Sicherheitsschaltgerät z. B. beinhaltet bereits diese beiden Einheiten)
- O1 und O2: Aktor 1 und 2 (z. B. zwei Schütze)

Die strukturellen Eigenschaften sind:

- Redundanter Aufbau
- Überwachung der Sensoren (Diskrepanzüberwachung)
- Überwachung der Freigabekreise (Überwachung, vergleichbar mit den Rückführkreisen heute)

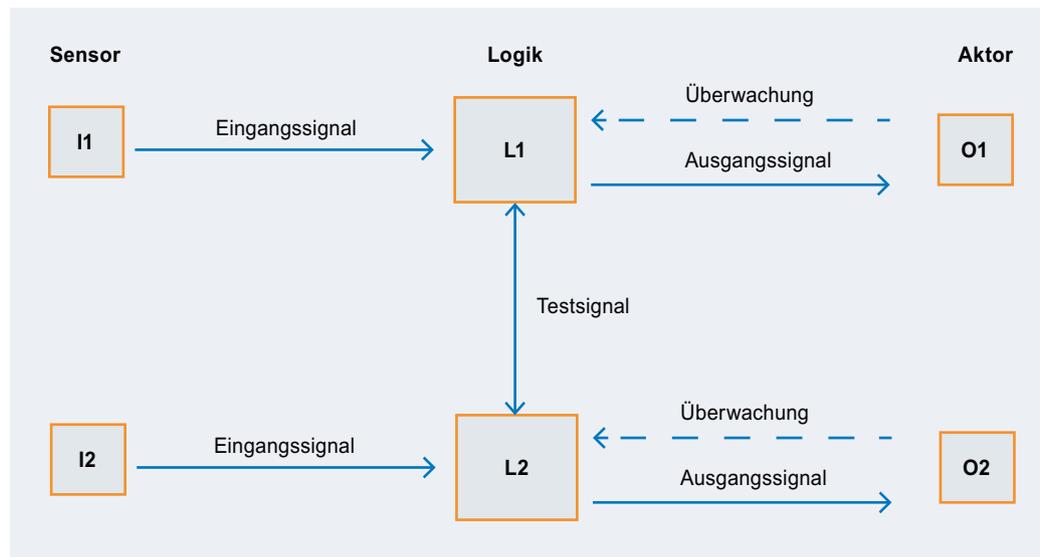


Bild 5-14 Vorgesehene Architektur für Kategorie 3

Kategorie 4

Zum Erreichen einer Kategorie 4 müssen die Anforderungen wie für die Kategorie B erfüllt sein. Es müssen ebenfalls die bewährten Sicherheitsprinzipien eingehalten werden. Zusätzlich gelten die folgenden Anforderungen:

Die sicherheitsbezogenen Teile des Steuerungssystems der Kategorie 4 müssen so ausgelegt werden, dass es bei Auftreten eines einzelnen Fehlers nicht zum Verlust der Sicherheitsfunktion kommt. Der einzelne Fehler muss bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden. Kann ein Fehler nicht erkannt werden, dann darf eine Anhäufung dieser Fehler nicht zum Verlust der Sicherheitsfunktion führen.

In einem Kategorie 4 System muss der MTTFd jedes redundanten Kanals hoch sein. Die sicherheitsbezogenen Teile des Steuerungssystems müssen einen hohen Diagnosedegrad aufweisen. Gleichzeitig müssen CCF Maßnahmen angewendet werden (siehe ISO 13849-1 Anhang F).

Beispiel einer vorgesehenen Architektur Kategorie 4:

- I1 und I2: Sensor 1 und 2 (z. B. zwei Positionsschalter mit zwangsöffnenden Kontakten)
- L1 und L2: Logikeinheit 1 und 2 (ein Sicherheitsschaltgerät z. B. beinhaltet bereits diese beiden Einheiten)
- O1 und O2: Aktor 1 und 2 (z. B. zwei Schütze)

Die strukturellen Eigenschaften sind:

- Redundanter Aufbau
- Überwachung der Sensoren (Diskrepanzüberwachung)
- Überwachung der Freigabekreise (Überwachung, vergleichbar mit den Rückführkreisen)
- Hoher Diagnosedeckungsgrad in allen Teilsystemen

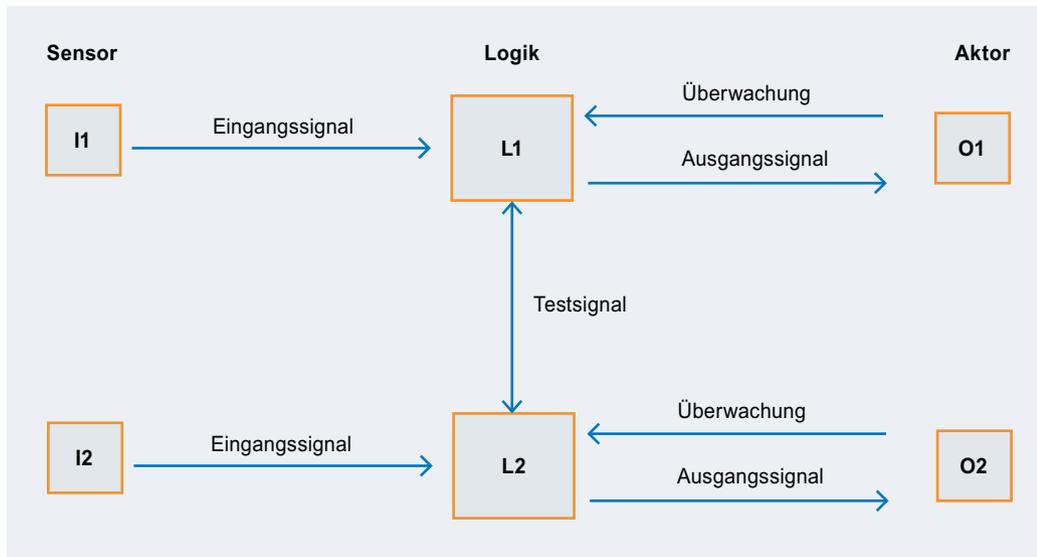


Bild 5-15 Vorgesehene Architektur für Kategorie 4

Bewertung der Sicherheitsfunktionen

Jede vorgesehene Sicherheitsfunktion, deren Umsetzung sowie Bewertung muss entsprechend den Vorgaben der Norm dokumentiert werden.

Bei der Bewertung von Sicherheitsfunktionen an Maschinen und Anlagen bietet Ihnen die schnelle und einfache Handhabung der Safety Evaluation im TIA Selection Tool wertvolle Unterstützung.

Das Offline-Tool führt den Anwender schrittweise von der Festlegung der Struktur des Sicherheitssystems, über die Auswahl der Komponenten zur Ermittlung der erreichten Sicherheitsintegrität gemäß ISO 13849-1 und IEC 62061.

Hierbei unterstützen Sie auch die integrierten umfangreichen Bibliotheken. Als Ergebnis erhält der Benutzer einen normenkonformen Report, der als Sicherheitsnachweis in die Dokumentation integriert werden kann.

Sie können die Aktualität der sicherheitstechnischen Daten von Siemens durch die Durchführung von regelmäßigen Updates des TIA Selection Tools erreichen. Dadurch ist sichergestellt, dass die Berechnungen immer mit der aktuellen Normenlage durchgeführt werden und dass stets auf die aktuellen technischen Daten aller sicherheitsrelevanten Komponenten von SIEMENS zugegriffen wird.

Die Safety Evaluation im TIA Selection Tool finden Sie im Internet (<http://www.siemens.de/safety-evaluation-tool>).

Service & Support

6.1 Service und Support

Safety Integrated im Internet

Aktuelle Informationen rund um die Sicherheitstechnik bietet Ihnen unser Online-Auftritt. Sie finden dort hilfreiche Dokumente, Links, Filme und Tools zu Safety-Integrated-Produkten und -Lösungen sowie zur Anwendung der Normen.

Safety Integrated im Internet (<http://www.siemens.de/safety-integrated>)

Safety Consulting

Maschinensicherheit ist ein komplexes, sensibles und kostenintensives Thema. Mit der Beratungsleistung Safety Consulting bieten wir maßgeschneiderte Antworten auf Ihre Fragen und führen Sie routiniert durch den Prozess, an dessen Ende eines steht: die Sicherheit Ihrer Maschine.

Safety Consulting im Internet (<http://www.siemens.com/safety-consulting>)

SITRAIN Training für Safety Integrated

Risikobeurteilung, Normen, CE-Kennzeichnung, Produkttraining: Alles Wissenswerte rund um unser umfangreiches Trainingsprogramm SITRAIN finden Sie im Internet.

SITRAIN Training für Safety Integrated im Internet (<http://www.siemens.de/sitrain>)

Kataloge und Infomaterial

Im Informations- und Download-Center finden Sie alle aktuellen Kataloge, Kundenzeitschriften, Broschüren, Demosoftware und Aktionspakete zum Download. Unter anderem unseren Katalog "Safety Integrated".

Information und Download Center (<http://www.siemens.de/safety-infomaterial>)

Funktionsbeispiele

Im Internet finden Sie weitere praxisnahe Funktionsbeispiele, die typischen Anforderungen innerhalb der industriellen Sicherheitstechnik abdecken. Sie enthalten typische Anwendungen mit Produktbeispielen inklusive Verdrahtungsplan, Programmiercode und Bewertung nach EN 62061 und EN ISO 13849.

Funktionsbeispiele im Internet (<http://www.siemens.de/safety-functional-examples>)

Safety Integrated Newsletter

Aktuelle Informationen rund um die Sicherheitstechnik bietet Ihnen unser regelmäßiger Newsletter.

Safety Integrated Newsletter (<http://www.siemens.de/safety-integrated>)

Vor-Ort-Service

Siemens unterstützt seine Kunden weltweit mit produkt-, system- und applikationsnahen Services über den gesamten Lebenszyklus einer Anlage. Von der Planung und Entwicklung über den Betrieb bis hin zur Modernisierung profitieren Kunden durch den Service auch vom umfangreichen Technologie- und Produktwissen und der Branchenkompetenz der Siemens-Experten.

Industry Services (<http://www.siemens.com/services>)

Konfiguratoren

Stellen Sie Produkte und Systeme einfach mithilfe unserer Konfiguratoren zusammen.

Industry Mall

Anschließend online bestellen in der Industry Mall – so einfach geht das.

Industry Mall (<http://www.siemens.com/industrymall/DE>)

Beratung

Um den wachsenden Anforderungen im Bereich der Sicherheitstechnik gerecht zu werden, setzt Siemens neben den eigenen Safety-Experten auch auf ausgewählte Siemens Solution Partner Automation. Diese hoch qualifizierten Partnerunternehmen bieten professionelle Beratung und tatkräftige Unterstützung für alle relevanten Sicherheitsaspekte Ihrer Automatisierungsprojekte.

Solution Partner Internet (<http://www.siemens.com/solutionpartner>)

Index

A

Aktoren, 20
ANSI, 183
Applikationsbeispiele
 Handhabung, 31
Architektur
 Steuerungssystem, 194
Architektur Kategorie 2, 212
Architektur Kategorie 3, 213
Architektur Kategorie 4, 214
Architektur Kategorie B, 210
Architektorentwurf, 208
 Subsystem, 201
Ausfallwahrscheinlichkeit, 188, 203
Ausfallwahrscheinlichkeit (PFHD), 202
Australien, 185
Auswerteeinheit, 20
Auswertegeräte
 sichere, 82
Auswerten, 20
Automatischer Start, 14

B

Benutzerinformation, 181
Bereichsüberwachung, 121, 123
Berührungslose Sicherheitsschalter, 79

C

CAX-Daten, 33
CE-Konformitätsprozess, 177

D

Diagnose, 203, 204
Diagnosedeckungsgrad, 202, 209
Diagnostic coverage DC, 202
Dokumentation
 Erforderliche Kenntnisse, 7
 Historie, 8
 Zielgruppe, 7
Drehzahlüberwachung, 125, 126
Drehzahlwächter, 126, 130

E

EN 60204-1, 18
EN ISO 12100, 178
EN 60204-1, 19
EN ISO 13849-1, 181
Entwurfskonzept, 208
Entwurfsprozess, 194, 206
Erfassen, 20
Erforderliche Kenntnisse, 7
EU-Richtlinien, 176
Europannormen
 harmonisierte, 176

F

Fehlanwendung, 180
Fehler, 201
 gefährbringende, 201
 systematischer, 198
Fehleraufdeckung, 198, 199, 201
Fehlerreaktion, 199
Fehlertoleranz, 198, 199, 201, 203, 204
Freigabekreis, 13
Funktionsbeispiele, 217
Funktionsblock, 193
Funktionsblock-Element, 193

G

Gefährbringende Fehler, 201
Gefährbringender Ausfall, 202
Gefährdungsereignis, 190
Gewährleistung, 8

H

Haftung, 8
Hardwareintegrität, 198
Harmonisierte Europannormen, 176
Historie, 8

I

IEC 62061, 32, 187
IEC 61508, 192

IEC 62061, 17, 181, 187, 189, 196
Industry Mall, 218
Infomaterial, 217
ISO 13849-1, 32
ISO 13849-1, 17, 188, 208
 Kategorien, 206

K

Kaskadierung
 Sicherheitsschaltgeräte, 152
Kataloge, 217
Kategorie 1, 210
Kategorie 2, 211
Kategorie 3, 212
Kategorie 4, 213
Kategorie B, 209
Kombination zur Positionserfassung, 81
Kombinationen von Sicherheitsfunktionen, 137
Konfiguratoren, 218

L

Laserscanner, 121, 123
Lebenszyklus, 177
Lichtvorhang, 113, 115
Lichtvorhänge, 112

M

Magnetschalter, 79
Manueller Start, 14
Maschinenrichtlinie, 175
Maschinensicherheitsrichtlinie
 Brasilien, 185
Mechanische Sicherheitsschalter, 78
Muting, 112
Mutingbetrieb, 112

N

National Electric Code (NEC), 183
NFPA, 183
NFPA 70, 183
NFPA 79, 183
Normen, 176
Not-Aus, 18
Not-Ein, 18
Not-Halt, 18, 143, 146, 148

Not-Halt-Abschaltung, 35, 37, 40, 42, 44, 46, 52, 164
Not-Start, 18

O

Offener Gefahrenbereich, 112, 114, 116, 118
OSHA Regulations, 183

P

Performance Level, 17, 181, 188, 208
PL, 181
PL c, 32
PL d, 32
PL e, 32
Positionserfassung, 81
Positionsschalter, 78
Positionsüberwachung, 81
Produkthaftung, 183
Produktsicherheitsgesetz, 175

Q

Querschlusserkennung, 13

R

Reagieren, 20
Redundanz, 13
Reihenschaltung, 35, 80, 137
Restrisiko, 178, 179
Risiko, 179
Risikoanalyse, 178
Risikobeurteilung, 178, 187, 206, 217
Risikobewertung, 178, 188
Risikoelemente, 187, 188, 190
Risikograph, 188
Risikominderung, 179, 188
Risikoparameter, 189
Risikoreduzierung, 179
Rückführkreis, 13

S

Safety Evaluation, 33, 215
Safety Integrated, 217
Safety Integrity, 206
Safety Integrity Level, 17, 181
Safety Integrity Level (SIL), 187

- Safety Performance, 187, 189, 196, 206
 - Safety related electrical control system, SRECS, 192
 - Schadensschwere, 190
 - Schaltmatte, 116, 118
 - Scharnierschalter, 79
 - Schutzfunktion
 - Unterdrückung, 112
 - Schutzmaßnahme, 188
 - Schutzmaßnahmen, 179, 180
 - Schutztür, 131, 145, 147
 - Schutztüren, 84, 85, 87, 89, 91, 93, 95, 98, 100, 102
 - Schutztürüberwachung, 76, 84, 86, 88, 96, 98, 100, 102, 146, 148, 157
 - Schutztürzuhaltung, 128, 157
 - Schutzziele, 175
 - Sensoren, 20
 - Sichere Drehzahlüberwachung, 126
 - Sichere Fehler, 204
 - Sichere Stillstandsüberwachung, 128
 - Sicheres Bedienen, 132
 - Sicherheitsanforderungen
 - Spezifikation, 191
 - Sicherheitsberechnung, 33
 - Sicherheitsfunktion, 197, 199, 208
 - Bewertung, 214
 - Strukturierung, 196
 - Sicherheitsfunktionen
 - Kombinationen, 137
 - Validierung, 182
 - Sicherheitsintegrität, 214
 - Sicherheits-Integritätslevel, 190
 - Sicherheitslevel, 81
 - Sicherheitsniveau, 32
 - Sicherheitsschalter
 - berührungslose, 79
 - SIL, 181, 189
 - SIL 1, 32
 - SIL 2, 32
 - SIL 3, 32
 - SIL claim limit, 196, 201
 - SITRAIN, 217
 - Sorgfaltspflicht, 17
 - Spezifikation
 - Sicherheitsanforderungen, 191
 - SRCF, 193
 - SRECS, 192, 202
 - Steuerungsfunktion, 193
 - Steuerungssystem, 193, 194
 - Architekturentwurf, 197
 - Stillsetzen, 18
 - gesteuertes, 18
 - ungesteuertes, 18
 - Stillsetzen im Notfall, 20, 34
 - Stillstandsüberwachung, 125, 128
 - Stillstandswächter, 128
 - Stopp-Kategorien, 18
 - Strukturelle Einschränkungen, 204
 - Strukturierungselemente, 192
 - Strukturierungsprinzip, 192
 - Subsystem, 193, 198, 201, 202
 - Auswahl, 198
 - Design, 202
 - Subsystem-Element, 193
 - Synchronität, 14
 - Systemarchitektur, 192, 197
 - Systematische Integrität, 196, 198, 202
 - Systematischer Fehler, 17, 198
- U**
- Überwachter Start, 14
 - USA, 183
- V**
- Validierung, 182
 - Verriegelungseinrichtungen, 76, 125
 - Vorschriften, 17
- Z**
- Zielgruppe, 7
 - Zugangsüberwachung, 113, 115, 117, 119
 - Lichtvorhang, 149
 - Zuhaltung, 79, 125
 - Zuhaltungsüberwachung, 130
 - Zweihandbedienpult, 132, 134
 - Zweihandbedienung, 14
 - Zweihandschaltung, 132

