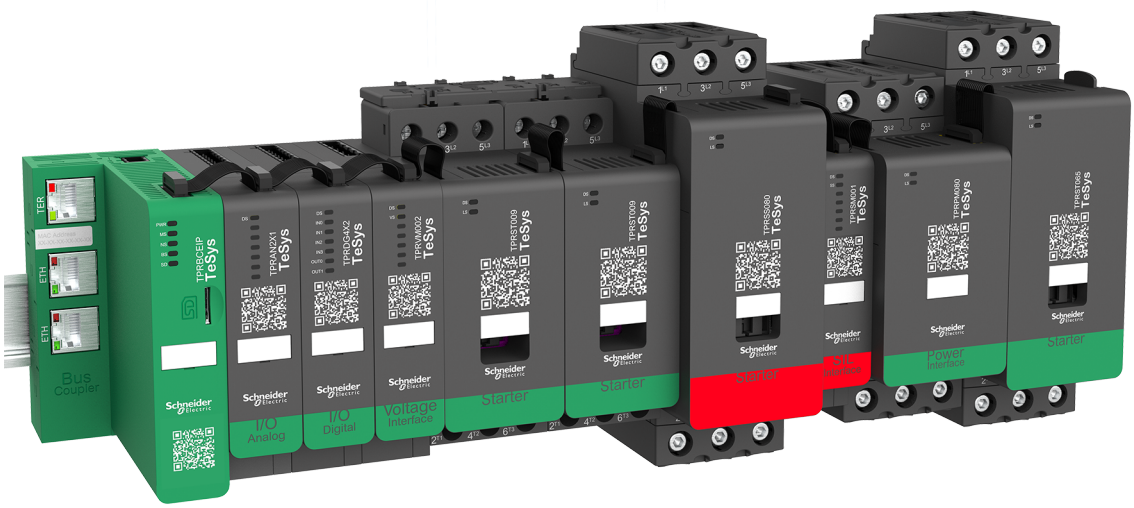
TeSys Active

TeSys™ island – Digitale Motormanagement-Lösung

Handbuch zur Funktionssicherheit

TeSys bietet innovative und vernetzte Lösungen für Motorstarter.

8536IB1904DE-04
08/2023



www.schneider-electric.com

Rechtliche Hinweise

Die in diesem Dokument enthaltenen Informationen umfassen allgemeine Beschreibungen, technische Merkmale und Kenndaten und/oder Empfehlungen in Bezug auf Produkte/Lösungen.

Dieses Dokument ersetzt keinesfalls eine detaillierte Analyse bzw. einen betriebs- und standortspezifischen Entwicklungs- oder Schemaplan. Es darf nicht zur Ermittlung der Eignung oder Zuverlässigkeit von Produkten/Lösungen für spezifische Benutzeranwendungen verwendet werden. Es liegt im Verantwortungsbereich eines jeden Benutzers, selbst eine angemessene und umfassende Risikoanalyse, Risikobewertung und Testreihe für die Produkte/Lösungen in Übereinstimmung mit der jeweils spezifischen Anwendung bzw. Nutzung durchzuführen bzw. von entsprechendem Fachpersonal (Integrator, Spezifikateur oder ähnliche Fachkraft) durchführen zu lassen.

Die Marke Schneider Electric sowie alle anderen in diesem Dokument enthaltenen Markenzeichen von Schneider Electric SE und seinen Tochtergesellschaften sind das Eigentum von Schneider Electric SE oder seinen Tochtergesellschaften. Alle anderen Marken können Markenzeichen ihrer jeweiligen Eigentümer sein.

Schneider Electric gewährt keine Rechte oder Lizenzen für die kommerzielle Nutzung des Dokuments oder dessen Inhalts, mit Ausnahme einer nicht-exklusiven und persönlichen Lizenz, es „wie besehen“ zu konsultieren.

Schneider Electric behält sich das Recht vor, jederzeit ohne entsprechende schriftliche Vorankündigung Änderungen oder Aktualisierungen mit Bezug auf den Inhalt bzw. am Inhalt dieses Dokuments oder dessen Format vorzunehmen.

Soweit nach geltendem Recht zulässig, übernehmen Schneider Electric und seine Tochtergesellschaften keine Verantwortung oder Haftung für Fehler oder Auslassungen im Informationsgehalt dieses Dokuments oder für Folgen, die aus oder infolge der sachgemäßen oder missbräuchlichen Verwendung der hierin enthaltenen Informationen entstehen.

Inhaltsverzeichnis

Sicherheitshinweise

Wichtige Informationen

Lesen Sie sich diese Anweisungen sorgfältig durch und machen Sie sich vor Installation, Betrieb, Bedienung und Wartung mit dem Gerät vertraut. Die nachstehend aufgeführten Warnhinweise sind in der gesamten Dokumentation sowie auf dem Gerät selbst zu finden und weisen auf potenzielle Risiken und Gefahren oder bestimmte Informationen hin, die eine Vorgehensweise verdeutlichen oder vereinfachen.

Der Zusatz eines Symbols zu den Sicherheitshinweisen „Gefahr“ oder „Warnung“ deutet auf eine elektrische Gefahr hin, die zu schweren Verletzungen führen kann, wenn die Anweisungen nicht befolgt werden.

Dieses Symbol steht für eine Sicherheitswarnung. Es macht auf die potenzielle Gefahr eines Personenschadens aufmerksam. Beachten Sie alle Sicherheitshinweise mit diesem Symbol, um schwere oder tödliche Verletzungen zu vermeiden.

⚠ GEFAHR

GEFAHR weist auf eine gefährliche Situation hin, die bei Nichtbeachtung zu schweren bzw. tödlichen Verletzungen **führt**.

⚠ WARNUNG

WARNUNG weist auf eine gefährliche Situation hin, die bei Nichtbeachtung zu schweren bzw. tödlichen Verletzungen **führen kann.**

⚠ ACHTUNG

ACHTUNG weist auf eine gefährliche Situation hin, die bei Nichtbeachtung zu leichten Verletzungen **führen kann**.

HINWEIS

HINWEIS wird verwendet, um Verfahren zu beschreiben, die sich nicht auf eine Verletzungsgefahr beziehen.

Bitte beachten

Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, bedient und gewartet werden. Schneider Electric haftet nicht für Schäden, die durch die Verwendung dieses Materials entstehen.

Als Fachpersonal gelten Mitarbeiter, die über Fähigkeiten und Kenntnisse hinsichtlich der Konstruktion und des Betriebs elektrischer Geräte und deren Installation verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

Zu diesem Dokument

Geltungsbereich des Dokuments

Verwenden Sie dieses Dokument, um mehr über die folgenden TeSys™ island-Funktionssicherheitsmerkmale zu erfahren:

- Allgemeines Verständnis
- Zu beachtende zentrale Aspekte
- Leistungen
- Hardware-Beschreibung
- Typische Konfigurationen
- Musterarchitekturen
- Normenreferenzen

Gültigkeitshinweis

Diese Anleitung ist für alle TeSys island-Konfigurationen gültig. Die Verfügbarkeit einiger Funktionen, die in dieser Anleitung beschrieben sind, hängt vom verwendeten Kommunikationsprotokoll sowie von den im TeSys island installierten physischen Modulen ab.

Informationen zur Produktkonformität mit Umweltrichtlinien, wie z. B. RoHS, REACH, PEP und EOLI, finden Sie auf www.se.com/green-premium.

Informationen zu den technischen Kenndaten der physischen Module, die in dieser Anleitung beschrieben sind, finden Sie auf www.se.com.

Die in diesem Handbuch vorgestellten technischen Merkmale sollten denen entsprechen, die online angezeigt werden. Zur Verbesserung der Klarheit und Genauigkeit werden wir im Lauf der Zeit den Inhalt gegebenenfalls überarbeiten. Wenn Sie einen Unterschied zwischen den Informationen in diesem Handbuch und den Online-Informationen feststellen, verwenden Sie die Online-Informationen.

Zugehörige Dokumente

Dokumenttitel	Beschreibung	Dokumentnummer
TeSys island – System-, Installations- und Betriebshandbuch	Beschreibung der Hauptfunktionen, der mechanischen Installation, der Verdrahtung und der Inbetriebnahme des TeSys island sowie des Betriebs und der Wartung des TeSys island.	DOCA0270DE
TeSys island – EtherNet/IP™ – Kurzanleitung und Handbuch zur Funktionsblockbibliothek	Beschreibung der Integration von TeSys island und der Informationen zur TeSys island-Bibliothek, die in der Rockwell Software® Studio 5000® EtherNet/IP-Umgebung verwendet wird.	DOCA0271DE
TeSys island – Handbuch zur Funktionssicherheit	Beschreibung der funktionalen Sicherheitseinrichtungen von TeSys island.	8536IB1904DE
TeSys island – Handbuch für Drittanbieter-Funktionsblocks	Mit Informationen, die zum Erstellen von Funktionsblocks für Drittanbieter-Hardware erforderlich sind.	8536IB1905DE
TeSys island – DTM-Online-Hilfe	Beschreibung der Installation sowie der Verwendung verschiedener Funktionen der TeSys island-Konfigurationssoftware und der Parameter-Konfiguration für TeSys island.	8536IB1907DE
TeSys island – Produktumweltprofil	Beschreibung der Materialbestandteile und Recyclingfähigkeit sowie Angaben zu den Umweltauswirkungen für das TeSys island.	ENVPEP1904009
TeSys island – Produkt-Entsorgungsanweisungen	Mit Anweisungen für die Entsorgung von TeSys island am Ende seiner Nutzungszeit.	ENVEOLI1904009
TeSys island – Kurzanleitung – Buskoppler, TPRBCEIP	Installationsbeschreibung für den TeSys island-Ethernet/IP-Buskoppler.	MFR44097
TeSys island – Kurzanleitung – Buskoppler, TPRBCPFN	Installationsbeschreibung für den TeSys island-PROFINET-Buskoppler.	MFR44098
TeSys island – Kurzanleitung – Buskoppler, TPRBCPFB	Installationsbeschreibung für den TeSys island-PROFIBUS DP-Buskoppler.	GDE55148
TeSys island – Kurzanleitung – Starter und Leistungsschnittstellenmodule, Größe 1 und 2	Installationsbeschreibung für TeSys island-Starter und -Leistungsschnittstellenmodule der Größen 1 und 2.	MFR77070
TeSys island – Kurzanleitung – Starter und Leistungsschnittstellenmodule, Größe 3	Installationsbeschreibung für TeSys island-Starter und -Leistungsschnittstellenmodule der Größe 3.	MFR77085
TeSys island – Kurzanleitung: Ein-/Ausgangsmodule	Installationsbeschreibung für die TeSys island-Analog- und Digital-E/A-Module.	MFR44099
TeSys island – Kurzanleitung: SIL-Schnittstellen- und Spannungsschnittstellenmodule	Installationsbeschreibung für die TeSys island-Spannungsschnittstellen- und SIL[1]-Schnittstellenmodule.	MFR44100

1. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.

Aus Normen abgeleitete Terminologie

Die technischen Begriffe, die Terminologie und die entsprechenden Beschreibungen in dieser Anleitung entsprechen normalerweise den Begriffen oder Definitionen in den relevanten Normen. Zu den Normen zählen u. a. folgende:

- **EN ISO 13849-1:** Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze
- **EN ISO 13849-2:** Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung
- **IEC 61508:** Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme
- **EN 62061:** Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme
- **IEC 61511:** Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie
- **EN/IEC 60204-1:** Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen
- **IEC 61000-6-7:** Elektromagnetische Verträglichkeit (EMV) – Teil 6-7: Fachgrundnormen – Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind
- **IEC 60664-5:** Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen – Teil 5: Ein umfassendes Verfahren zur Bemessung der Luft- und Kriechstrecken für Abstände gleich oder unter 2 mm
- **IEC 60947-4-1:** Niederspannungsschaltgeräte Teil 4-1: Schütze und Motorstarter – Elektromechanische Schütze und Motorstarter
- **IEC 60947-5-1:** Niederspannungsschaltgeräte Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte
- **IEC 60947-7-1:** Niederspannungsschaltgeräte Teil 7-1: Hilfseinrichtungen – Reihenklemmen für Kupferleiter
- **IEC 60947-7-2:** Niederspannungsschaltgeräte Teil 7-2: Hilfseinrichtungen – Schutzleiter-Reihenklemmen für Kupferleiter
- **EN 50205:** Relais mit (mechanisch) zwangsgeführten Kontakten
- **IEC TR 62380:** Handbuch für Zuverlässigkeitsdaten – Allgemeines Modell für Zuverlässigkeits-Vorhersagen von elektronischen Bauteilen, Leiterplatten und Geräten

Funktionssicherheitsterminologie

ATTENTION

Die Funktionssicherheitsterminologie, die in dieser Anleitung verwendet wird, ist nachstehend definiert:

Begriff	Standard	Definition
Fehlertoleranz	IEC 61511-1	Die Fähigkeit eines Funktionsteils, eine erforderliche Funktion aufrechtzuerhalten, auch wenn Störungen oder Fehler auftreten.
Funktionssicherheit	IEC 61508-4	Teil der Gesamtsicherheit, bezogen auf die überwachte Einrichtung (EUC) und das EUC-Steuerungssystem, der von der korrekten Funktion von elektrischen, elektronischen und programmierbaren elektronischen Systemen (E/E/PE), die eine Sicherheitsfunktion ausführen, und von anderen risikomindernden Maßnahmen abhängt.
Ungefährliche Ausfälle	IEC 61508-4	Ausfall eines Elements, eines Untersystems und/oder eines Systems, das bei der Implementierung der Sicherheitsfunktion eine Rolle spielt, der: 1. zu einer nicht korrekten Wirkweise der Sicherheitsfunktion führt, wodurch die EUC[2] (oder ein Teil davon) in einen sicheren Zustand versetzt bzw. deren sicherer Zustand aufrechterhalten wird – oder 2. die Wahrscheinlichkeit einer nicht korrekten Wirkweise der Sicherheitsfunktion erhöht, wodurch die EUC[2] (oder ein Teil davon) in einen sicheren Zustand versetzt bzw. deren sicherer Zustand aufrechterhalten wird.
Anteil ungefährlicher Ausfälle	IEC 61508-4	Der Anteil der ungefährlichen Ausfälle im Verhältnis zu den Gesamtausfällen des Systems.
Sicherer Zustand	IEC 61511-1	Der Zustand des Verfahrens, wenn die Sicherheit gewährleistet ist.
	IEC 61800-5-2	Zustand der PDS(SR)[3], wenn die Sicherheit gewährleistet ist.
„Safe Stop“	IEC 61800-5-2	Die „Safe Stop“-Funktionen werden folgendermaßen definiert: • **Sicher abgeschaltetes Moment (STO)** ◦ Diese Funktion verhindert, dass dem Motor eine drehmomenterzeugende Kraft zugeführt wird. ◦ Diese *Sicherheitsunterfunktion* entspricht einem ungesteuerten Stillsetzen in Stopp-Kategorie 0 nach IEC 60204-1. • **„Safe Stop“ 1 (SS1)** ◦ „Safe Stop“ 1 mit gesteuerter Verzögerung: SS1-d initiiert und steuert die Motorverzögerungsrate innerhalb ausgewählter Grenzwerte, um den Motor anzuhalten und die STO-Funktion (siehe 4.2.3.2) auszuführen, wenn die Motorgeschwindigkeit unter einen festgelegten Grenzwert fällt; oder ◦ „Safe Stop“ 1 mit Überwachung der Verzögerungsrampe: SS1-r initiiert und überwacht die Motorverzögerungsrate innerhalb ausgewählter Grenzwerte, um den Motor anzuhalten und die STO-Funktion auszuführen, wenn die Motorgeschwindigkeit unter einen festgelegten Grenzwert fällt; oder ◦ „Safe Stop“ 1 mit Zeitsteuerung: SS1-t initiiert die Motorverzögerung und führt die STO-Funktion nach einer anwendungsspezifischen zeitlichen Verzögerung aus.

2. EUC: überwachte Einrichtung
3. Sicherheitsbezogene Antriebssysteme

Begriff	Standard	Definition
Sicherheitsfunktion	IEC 61800-5-2	Eine Funktion, die in Bezug auf ein bestimmtes gefährliches Ereignis von einem sicherheitsbezogenen System oder anderen Risikoverringerungsmaßnahmen implementiert werden muss, mit der ein sicherer Zustand des Geräts oder der Maschine, die vom PDS(SR)[4] angetrieben werden, erreicht bzw. aufrechterhalten werden soll.
Sicherheitsanforderungsstufe (SIL)	IEC 61508	In der Norm IEC 61508 sind vier Sicherheitsanforderungsstufen (SILs) für Sicherheitsfunktionen festgelegt: SIL 1 ist die niedrigste Integritätsstufe und SIL 4 die höchste. Eine Gefahrenanalyse und Risikobeurteilung dienen als Grundlage für die Bestimmung der erforderlichen Sicherheitsanforderungsstufe.
Sicherheitsbezogenes System	IEC 61800-5-2	Festgelegtes System, das sowohl: • die erforderlichen Sicherheitsfunktionen implementiert, die zum Erreichen oder Aufrechterhalten eines sicheren Zustands für das Gerät oder die Maschine, die vom PDS(SR)[5] angetrieben wird, notwendig sind, als auch • die notwendige Sicherheitsintegrität für die erforderlichen Sicherheitsfunktionen, eigenständig oder gemeinsam mit anderen Risikoverringerungsmaßnahmen, erreichen soll
Untersystem	IEC 61800-5-2	Ein Teil der übergeordneten, architektonischen Gestaltung eines sicherheitsbezogenen Systems, dessen Ausfall zum Versagen einer sicherheitsbezogenen Funktion führt.

EG-Konformitätserklärung

Die EG-Konformitätserklärung für TeSys™ island ist auf www.schneider-electric.com erhältlich.

4. Sicherheitsbezogene Antriebssysteme
5. Sicherheitsbezogene Antriebssysteme

Sicherheitsvorkehrungen

Lesen Sie die folgenden Sicherheitsvorkehrungen gründlich durch, bevor Sie ein in dieser Anleitung angegebenes Verfahren ausführen.

⚠⚠GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS, EINER EXPLOSION ODER EINES LICHTBOGENÜBERSCHLAGS

- Dieses Gerät darf nur von qualifizierten Elektrikern installiert und gewartet werden.
- Schalten Sie die Spannungsversorgung ab, bevor Sie Arbeiten an oder in diesem Gerät vornehmen.
- Verwenden Sie nur die angegebene Spannung, wenn Sie dieses Gerät und zugehörige Produkte betreiben.
- Verwenden Sie stets ein genormtes Spannungsprüfgerät, um festzustellen, ob die Spannungsversorgung wirklich abgeschaltet ist.
- Verwenden Sie angemessene Verriegelungen, wenn Personen- bzw. Gerätegefahren vorhanden sind.
- Leitungskreise müssen in Übereinstimmung mit lokalen und nationalen aufsichtsrechtlichen Anforderungen verdrahtet und geschützt werden.
- Tragen Sie eine geeignete persönliche Schutzausrüstung (PSA) und befolgen Sie sichere Arbeitsweisen für die Ausführung von Elektroarbeiten gemäß NFPA 70E, NOM-029-STPS oder CSA Z462 bzw. gemäß den entsprechenden lokalen Bestimmungen.

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

⚠WARNUNG

NICHT BESTIMMUNGSGEMÄßER GERÄTEBETRIEB

- Vollständige Anweisungen zur funktionalen Sicherheit finden Sie im TeSys™ island Funktionssicherheitshandbuch (8536IB1904).
- Sie dürfen dieses Gerät nicht auseinanderbauen, reparieren oder verändern. Es gibt keine vom Benutzer zu wartenden Teile.
- Installieren und betreiben Sie dieses Gerät in einem Gehäuse, das eine angemessene Schutzklasse für die vorgesehene Anwendungsumgebung hat.
- Jede Implementierung dieses Geräts muss vor seiner Inbetriebnahme separat und gründlich auf ordnungsgemäßen Betrieb getestet werden.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠ **WARNUNG:** Dieses Produkt kann chemische Stoffe freisetzen, einschließlich Antimonoxid (Antimontrioxid), das im US-Bundesstaat Kalifornien als krebserregend gilt. Weitere Informationen hierzu finden Sie auf www.P65Warnings.ca.gov.

Qualifiziertes Personal

Nur angemessen geschultes Personal, das den Inhalt dieser Anleitung sowie den von weiteren zugehörigen Produktunterlagen kennen und verstanden hat, darf an und mit diesem Produkt arbeiten.

Das qualifizierte Personal muss in der Lage sein, mögliche Gefahren zu erkennen, die durch Änderungen von Parameterwerten entstehen sowie allgemein Gefahren, die von mechanischen, elektrischen oder elektronischen Geräten ausgehen können. Das qualifizierte Personal muss mit den Normen, Vorschriften und Verordnungen zur Verhütung von Industrieunfällen vertraut sein und diese bei der Gestaltung und Implementierung des Systems einhalten.

Die Nutzung und Anwendung der in dieser Anleitung enthaltenen Informationen erfordert Fachkenntnisse in Bezug auf die Gestaltung und Programmierung von automatisierten Steuersystemen. Nur Sie – der Nutzer, der Maschinenbauer oder der Systemintegrator – können alle Bedingungen und Faktoren kennen, die bei Installation, Einrichtung, Betrieb und Wartung der Maschine oder des Prozesses zutreffen, und Sie sind deshalb in der Lage, die Automatisierungs- und zugehörigen Geräte sowie die entsprechenden Sicherheitseinrichtungen und Verriegelungen zu bestimmen, die effizient und ordnungsgemäß verwendet werden können.

Bei der Auswahl von Automatisierungs- und Steuergeräten sowie von zugehörigen Geräten oder entsprechender Software für eine bestimmte Anwendung, müssen Sie außerdem alle anwendbaren lokalen, regionalen oder nationalen Normen bzw. Bestimmungen berücksichtigen.

Achten Sie besonders darauf, dass Sie die jeweiligen Sicherheitshinweise, elektrischen Anforderungen und normativen Vorgaben einhalten, die für die Verwendung dieses Geräts in Ihrer Maschine oder Ihrem Prozess gelten.

Verwendungszweck

Die in dieser Anleitung beschriebenen Produkte, einschließlich Software, Zubehör und Optionen, sind Starter für Niederspannungslasten, die für industrielle Zwecke gemäß den Anweisungen, Aufforderungen, Beispielen und Sicherheitshinweisen in diesem Dokument und sonstigen Begleitunterlagen vorgesehen sind.

Das Produkt darf ausschließlich in Übereinstimmung mit allen geltenden Sicherheitsbestimmungen und -richtlinien, den angegebenen Anforderungen und den technischen Daten verwendet werden.

Vor der Verwendung des Produkts müssen Sie eine Gefahrenanalyse sowie eine Risikobeurteilung der geplanten Anwendung durchführen. Entsprechend den Ergebnissen sind angemessene Sicherheitsmaßnahmen zu implementieren.

Da das Produkt als Bauteil einer Maschine oder eines Prozesses eingesetzt wird, müssen Sie die Sicherheit der beteiligten Personen durch das Gesamtsystemkonzept sicherstellen.

Betreiben Sie das Produkt ausschließlich mit den angegeben Kabeln und Zubehöroptionen. Verwenden Sie nur Original-Zubehöroptionen und -Ersatzteile.

Eine andere Nutzung als der ausdrücklich gestattete Verwendungszweck ist untersagt. Dabei können unvorhersehbare Gefahren entstehen.

TeSys™ island – Funktionssicherheitsübersicht

Master-Serie: TeSys

TeSys™ ist eine innovative Motorsteuerungs- und -management-Lösung des globalen Marktführers. TeSys bietet verbundene, effiziente Produkte und Lösungen für das Schalten sowie für den Schutz von Motoren und elektrischen Lasten in Übereinstimmung mit allen wichtigen weltweiten elektrischen Normen.

TeSys island-Konzept

TeSys island ist ein modulares, multifunktionales System, das im Rahmen einer Automatisierungsarchitektur integrierte Funktionen bereitstellt und hauptsächlich für die direkte Steuerung und das Management von Niederspannungslasten vorgesehen ist. TeSys island kann nach seiner Installation in einer elektrischen Schalttafel Motoren und andere elektrische Lasten bis zu 80 A (AC1) schalten, schützen und verwalten.

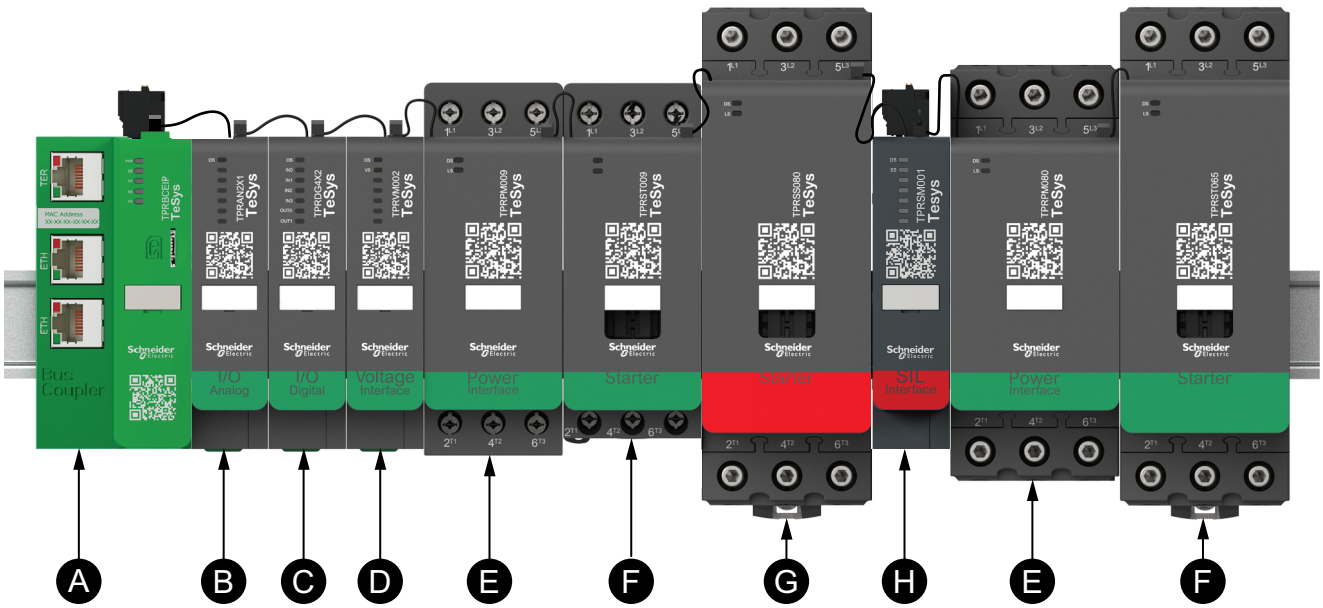
Dieses System wurde basierend auf dem Konzept der TeSys avatars entwickelt. Diese avatars:

- Stellen sowohl die logischen als auch die physischen Aspekte der Automatisierungsfunktionen dar
- Bestimmen die Konfiguration von TeSys island

Die logischen Aspekte des TeSys island werden mit Software-Tools verwaltet, die alle Phasen des Produkt- und Anwendungslebenszyklus abdecken: Entwurf, Konstruktion, Inbetriebnahme, Betrieb und Wartung.

Das physische TeSys island besteht aus einer Reihe von Geräten, die auf einer einzelnen DIN-Schiene installiert und über Flachbandkabel miteinander verbunden sind. Die Flachbandkabel ermöglichen die interne Kommunikation zwischen den Modulen. Die externe Kommunikation mit der Automatisierungsumgebung erfolgt über ein einzelnes Buskoppler-Modul. Das TeSys island wird im Netzwerk als Einzelknoten erfasst. Die anderen Module umfassen Starter, Leistungsschnittstellenmodule, Analog- und Digital-E/A-Module, Spannungsschnittstellenmodule und SIL-Schnittstellenmodule (Sicherheitsanforderungsstufe gemäß IEC 61508), die ein breites Spektrum an Betriebsfunktionen abdecken.

Abbildung 1 - Überblick über TeSys island



A	Buskoppler	E	Leistungsschnittstellenmodul
B	Analog-E/A-Modul	F	Standard-Starter
C	Digital-E/A-Modul	G	SIL-Starter
D	Spannungsschnittstellenmodul	H	SIL-Schnittstellenmodul

Funktionssicherheit von TeSys island

Das TeSys™ island bietet spezielle Avatars und physische Geräte zum Aufbau von Konfigurationen für Funktionen der Stopp-Kategorie 0 und Stopp-Kategorie 1 gemäß EN/IEC 60204-1. TeSys-Avatars sind digitale Repräsentationen der physischen Module auf der Insel. Die TeSys island-Sicherheitsfunktion stützt sich jedoch ausschließlich auf elektromechanische Hardware-Komponenten. Die spezifischen Geräte sind der SIL[6]-Starter und das SIL-Schnittstellenmodul. Ein weiteres wichtiges Konzept ist die SIL-Gruppe: Eine Gruppe von Avatars, die einem SIL-Schnittstellenmodul zugeordnet sind und derselben Sicherheitsfunktion entsprechen. Es können mehrere SIL-Gruppen für eine Insel vorhanden sein.

Das TeSys island muss mit anderen sicherheitsbezogenen Elementen in ein größeres, sicherheitsbezogenes System integriert werden, um die funktionale Sicherheit einer Maschine oder eines Systems/Prozesses sicherzustellen.

6. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.

Funktionssicherheitseigenschaften von TeSys island

TeSys™ island bietet Funktionssicherheitsmerkmale in Übereinstimmung mit diesen spezifischen Bedingungen:

Normen und zertifizierte Eigenschaften

Das TeSys island entspricht diesen Richtlinien und Normen:

- Maschinenrichtlinie 2006/42/EG:
  - EN ISO 13849-1: 2015
  - EN 62061: 2016 oder IEC 62061: 2015 (Ausgabe 1.2)
- Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme: IEC 61508 Ausgabe 2: 2010
- Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie: IEC 61511 Ausgabe 2: 2016
- Die TeSys island-Funktionen der Stopp-Kategorie 0 und Stopp-Kategorie 1 entsprechen der Norm EN/IEC 60204-1.

Bei einem einkanaligen System sind die höchsten Leistungswerte dieser Funktionen folgende:

- Performance-Level „d“ Kategorie 2 in Übereinstimmung mit EN ISO 13849-1
- SIL[7] 2-Kapazität in Übereinstimmung mit IEC 61508 Ausg. 2 und IEC 61511 Ausg. 2
- SIL CL 2-Kapazität in Übereinstimmung mit EN 62061 Ausg. 1

Bei einem zweikanaligen System sind die höchsten Leistungswerte dieser Funktionen folgende:

- Performance-Level „e“ Kategorie 4 in Übereinstimmung mit EN ISO 13849-1
- SIL 3-Kapazität in Übereinstimmung mit IEC 61508 Ausg. 2 und IEC 61511 Ausg. 2
- SIL CL 3-Kapazität in Übereinstimmung mit EN 62061: 2016 oder IEC 62061: 2015 (Ausgabe 1.2)

Das TeSys island ist – je nach seiner Verdrahtungsarchitektur – für die Unterstützung von verschiedenen Funktionssicherheit-Performance-Levels sowie Sicherheitsanforderungsstufen ausgelegt. Es ist mit den Funktionssicherheitseigenschaften konform, die in der folgenden Tabelle beschrieben werden.

Tabelle 1 - Funktionssicherheitseigenschaften

Funktion	Sicherheitsbezogene Stopp-Funktion
Fallback-Position	Offener Schütz
Reaktionszeit (Extremfall)	145 ms
Stopp-Kategorie EN/IEC 60204-1	Kat. 0/Kat. 1
Maschinenrichtlinie	Ja

7. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.

Tabelle 1 - Funktionssicherheitseigenschaften (Fortsetzung)

TeSys island-Systemarchitektur	Einkanalig	Zweikanalig
Performance-Level EN ISO 13849-1	PL c, d	PL c, d, e
Verdrahtungskategorie ISO 13849-1	Kat. 1, 2	Kat. 3, 4
SIL CL EN 62061	SIL CL 2	SIL CL 3
SIL IEC 61508/IEC 61511	SIL 2	SIL 3

Das Zertifikat der funktionalen Sicherheit kann auf www.se.com/tesys/ eingesehen werden.

HINWEIS: Für die Zertifizierung in Bezug auf funktionale Aspekte wird nur ein TeSys island, das sich für den Einsatz in sicherheitsbezogenen Anwendungen eignet, berücksichtigt und nicht das vollständige System, in das es integriert ist, um die funktionale Sicherheit einer Maschine oder eines Systems/ Prozesses sicherzustellen.

Betriebsbedingungen

TeSys island ist für eine dauerhafte Funktion unter den folgenden Bedingungen ausgelegt. Für bestimmte Module können andere Bedingungen gelten, die in ihrem jeweiligen Datenblatt (verfügbar auf www.se.com/tesys-island) angegeben sind:

- 40 °C Umgebungstemperatur
- 400- oder 480-V-Motor
- 50 % Luftfeuchtigkeit
- 80 % Lastwert
- Horizontale Montageausrichtung
- Alle Eingänge aktiviert
- Alle Ausgänge aktiviert
- 24 Stunden/Tag, 365 Tage/Jahr Laufzeit

Einkanalige Architektur (ISO 13849)

Das TeSys island ist anwendbar für einkanalige Architekturen, in denen ein erkannter Fehler zu einem Verlust der Sicherheitsfunktion führen kann.

Zweikanalige Architektur (ISO 13849)

Das TeSys island ist für zweikanalige Architekturen anwendbar, in denen ein einzelner erkannter Fehler (einschließlich Gleichtaktstörungen) zu keinem Verlust der Sicherheitsfunktion führt.

Stopp-Kategorien (EN/IEC 60204-1)

Die Stopp-Kategorie bezieht sich darauf, wie die angetriebene Last deaktiviert wird, und hängt von dem externen sicherheitsbezogenen Untersystem ab, dass die Stopp-Funktion auslöst. Ein externes sicherheitsbezogenes Untersystem kann mit Geräten wie den Preventa™ XPS-Modulen implementiert werden.

Stopp-Kategorie 0

Die Stopp-Kategorie 0 wird definiert als Stillsetzen durch sofortiges Unterbrechen der Energiezufuhr zu den Maschinen-Antriebselementen. Bei Stopp-Kategorie 0 handelt es sich um ein ungesteuertes Stillsetzen.

Stopp-Kategorie 1

Die Stopp-Kategorie 1 wird definiert als Stillsetzen, bei dem die Energiezufuhr zu den Maschinen-Antriebselementen beibehalten wird, um das Stillsetzen zu erzielen. Die Energiezufuhr wird erst dann unterbrochen, wenn der Stillstand erreicht ist. Bei Stopp-Kategorie 1 handelt es sich um ein gesteuertes Stillsetzen.

Verdrahtungskategorien[8]

Die Verdrahtungskategorien beziehen sich darauf, wie das externe Preventa™ XPS-Modul (oder Entsprechung) verdrahtet ist, sowie auf die zugehörige erhöhte Kontrolle über die Sicherheitsfunktion.

Verdrahtungskategorie 1

Ein einzelner erkannter Fehler kann zum Verlust der Sicherheitsfunktion führen. Es ist kein Diagnosedeckungsgrad erforderlich.

Das sicherheitsbezogene Sensorelement kann direkt mit den Eingängen „SIL-Eing.“/„SIL Gemeinsamer“ verdrahtet werden.[9] Die Spiegel-E/A-Eingänge werden nicht verwendet. Weitere Informationen zur Verdrahtung der Eingänge SIL-Eing./ SIL Gemeinsamer finden Sie unter Sicherheitsbezogenes Sensorelement, Seite 24.

Verdrahtungskategorie 2

Das sicherheitsbezogene Sensorelement wird mit einem Preventa XPS-Modul (oder Entsprechung) verdrahtet. Die Ausgänge des Preventa XPS-Moduls (oder Entsprechung) sind mit den Eingängen „SIL-Eing.“/„SIL Gemeinsamer“ des SIL[9]-Schnittstellenmoduls verdrahtet.

Um die Anforderungen von Kategorie 2 zu erfüllen, muss die Spiegelkontakt-Rückkopplung (Spiegel-E/A) von einem Preventa XPS-Modul (oder Entsprechung) überwacht werden, das die externe diagnostische Überwachung des Spiegelkontakts durchführt. Wenn sich der Spiegelkontakt bei Stopp nicht schließt, wird der nächste Neustart für alle SIL-Starter in der SIL-Gruppe verhindert.

Implementierung der indirekten Überwachung für Kategorie 2

Um die Kategorie 2-Anforderungen für den Diagnosedeckungsgrad (DC > 60 %) zu erfüllen, muss eine externe Überwachung des Gruppenstatus implementiert werden, durch die ein sekundärer Mechanismus ausgelöst wird, der die Maschine

8. Verdrahtungskategorien gemäß ISO 13849.
9. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.

anhält (Arbeitsstromauslöser am Leistungsschalter usw.) oder den Zugang zu Gefahrbereichen verhindert (Schutzsperre).

Jede SIL[10]-Gruppe hat fünf Zustände zur Anzeige ihres Betriebszustands. Zustand 0 gibt an, dass sich in diesem Steckplatz keine SIL-Gruppe befindet. Das TeSys island unterstützt bis zu 10 SIL-Gruppen auf der Insel.

SIL-Gruppenstatus für SIL-Stopp-Funktion:

- 0 = SIL-Gruppe nicht in der Systemkonfiguration vorhanden
- 1 = SIL-Gruppe betroffen von Avatar-Geräteereignis
- 2 = Stopp-Befehl empfangen, SIL-Starter noch nicht geöffnet
- 3 = Stopp-Befehl erfolgreich ausgegeben, alle SIL-Starter sind geöffnet
- 4 = Stopp-Befehl nur an einen Eingangskanal des SIL-Schnittstellenmoduls (SIM) ausgegeben (Steckbrücke oder SIM-Eingangsverdrahtung verursacht ein Problem), aber die SIL-Starter wurden erfolgreich geöffnet
- 5 = Normaler Betrieb, die SIL-Starter können geöffnet oder geschlossen sein

Zustand 5 ist der normale Betriebszustand und Zustand 3 ist der normale SIL-Stopp-Zustand. Zustand 1 gibt an, dass ein Firmware- oder Kommunikationsproblem bei einem SIL-Starter vorliegt. Die Zustände 2 und 4 weisen auf SIL-Stopp-bezogene Probleme mit dem SIM, den SIL-Startern oder der SIL-Stopp-Verdrahtung hin. Die indirekte Überwachung muss darauf achten, ob die Zustände 2 oder 4 länger andauern als die Betätigungszeit eines SIL-Stopps, und anhand der Statusinformationen einen sekundären Mechanismus auslösen, der die Maschine anhält (Arbeitsstromauslöser am Leistungsschalter usw.).

Zum Lesen des SIL-Gruppenstatus muss die externe Überwachung den SystemDiagnostics-Funktionsblock verwenden. Jede SIL-Gruppe im System hat an diesem Funktionsblock einen Ausgang für ihren SIL-Gruppenstatus, der auf dem Funktionsblock mit „SILStarterStopMsgGrp *n*“ bezeichnet ist, wobei *n* die SIL-Gruppennummer auf der Insel ist. Der SIL-Gruppenstatus entspricht der vorstehend angegebenen Auflistung.

Diagnostische Überwachung

Da die diagnostische Überwachung auf Anforderung der Sicherheitsfunktion sofort aktiviert wird, sollte die Gesamtzeit von der Erkennung des Fehlers bis zu dem Zeitpunkt, zu dem die Maschine in einen nicht gefährlichen Zustand versetzt wird, kürzer sein, als die Zeit, die man braucht, um den Gefahrenbereich zu erreichen.

Gemäß ISO 13849-2, 9.2.3 für Kategorie 2: Die $MTTF_d$[11] der Überwachungseinrichtung sollte größer als die Hälfte der $MTTF_d$ der Logik sein. Der Beitrag des TeSys island zur $MTTF_d$ der diagnostischen Überwachung ist $MTTF_d$ > 100 Jahre.

Verdrahtungskategorie 3

Bei einem einzelnen Fehler geht die Sicherheitsfunktion nicht verloren. Der einzelne Fehler wird – soweit möglich – bei oder vor der nächsten Anforderung an die Sicherheitsfunktion erkannt.

Um die Anforderungen von Kategorie 3 zu erfüllen, muss die Spiegelkontakt-Rückkopplung (Spiegel-E/A) von einem Preventa XPS-Modul (oder Entsprechung) überwacht werden, das die externe diagnostische Überwachung des SIL[10]-Starter-Spiegelkontakts durchführt. Wenn sich der Spiegelkontakt bei Stopp nicht öffnet, wird der nächste Neustart für alle SIL-Starter in der SIL-Gruppe verhindert. Das sicherheitsbezogene Sensorelement wird mit einem Preventa XPS-Modul (oder Entsprechung) verdrahtet. Die Ausgänge des Preventa XPS-

10. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
11. Mittlere Zeit bis zu einem gefährlichen Ausfall gemäß ISO 13849-1.

Moduls (oder Entsprechung) sind mit den Eingängen SIL-Eing./SIL Gemeinsamer des SIL-Schnittstellenmoduls verdrahtet.

Bei einer indirekten Überwachung muss die externe Überwachung des Gruppenstatus darauf achten, ob die Zustände 2 oder 4 länger andauern als die Betätigungszeit eines SIL-Stopps. Die Statusinformationen sollten genutzt werden, um den nächsten Neustart der SIL-Starter in der Gruppe zu verhindern.

Verdrahtungskategorie 4

Bei einem einzelnen Fehler geht die Sicherheitsfunktion nicht verloren. Der einzelne Fehler wird bei oder vor der nächsten Anforderung an die Sicherheitsfunktion erkannt. Wenn diese Erkennung nicht möglich ist, dann geht die Sicherheitsfunktion bei einer Anhäufung unerkannter Fehler nicht verloren.

Um die Anforderungen von Kategorie 4 zu erfüllen, muss die Spiegelkontakt-Rückkopplung (Spiegel-E/A) von einem Preventa XPS-Modul (oder Entsprechung) überwacht werden, das die externe diagnostische Überwachung des SIL[12]-Starter-Spiegelkontakts durchführt. Wenn sich der Spiegelkontakt bei Stopp nicht öffnet, wird der nächste Neustart für alle SIL-Starter in der SIL-Gruppe verhindert. Das sicherheitsbezogene Sensorelement wird mit einem Preventa XPS-Modul (oder Entsprechung) verdrahtet. Die Ausgänge des Preventa XPS-Moduls (oder Entsprechung) sind mit den Eingängen SIL-Eing./SIL Gemeinsamer des SIL-Schnittstellenmoduls verdrahtet.

Abnahmeprüfung

Der Systemintegrator/Maschinenhersteller muss eine Abnahmeprüfung der Sicherheitsfunktion durchführen, um die korrekte Funktionsweise der Sicherheitsfunktion zu überprüfen und zu dokumentieren. Der Systemintegrator/Maschinenhersteller bescheinigt damit, die Wirksamkeit der verwendeten Sicherheitsfunktionen geprüft zu haben. Die Abnahmeprüfung muss basierend auf einer entsprechenden Gefahrenanalyse und Risikobeurteilung durchgeführt werden. Im Fall einer niedrigen Anforderungsrate in Kategorie 4 muss die Sicherheitsfunktion mindestens einmal pro Monat getestet werden. Alle geltenden Normen und Vorschriften müssen eingehalten werden.

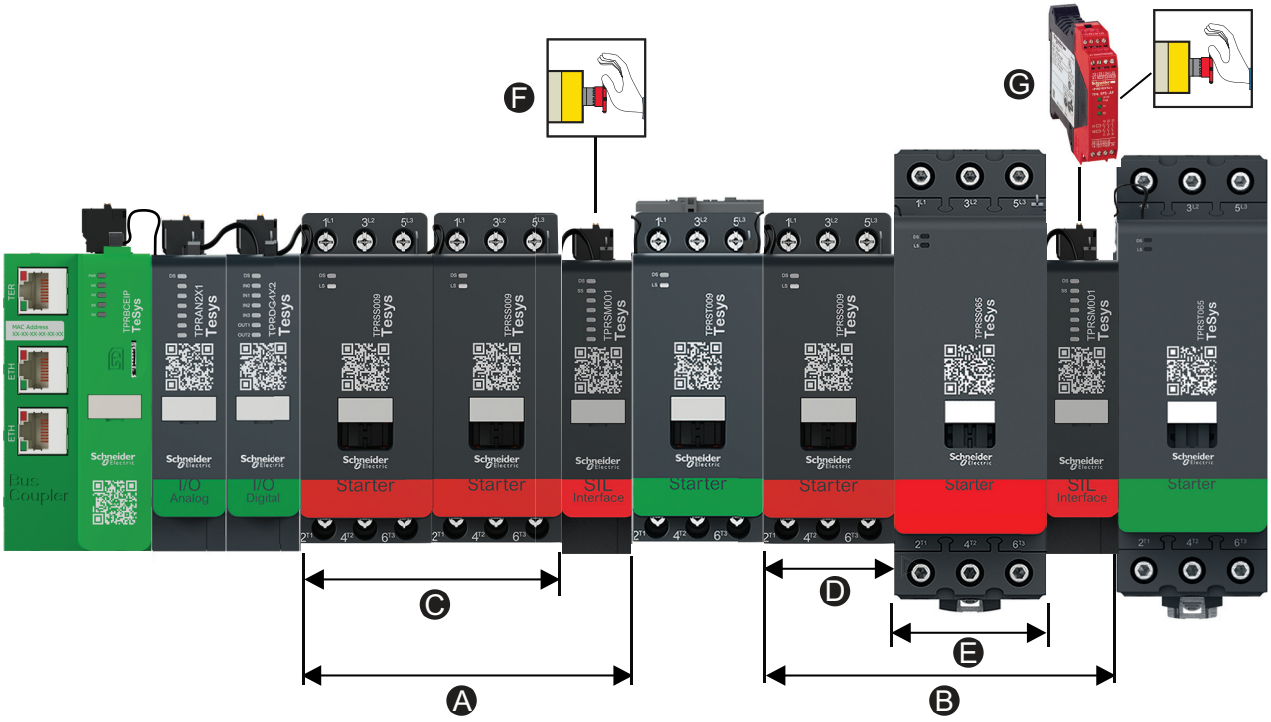
12. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.

Konzepte und Komponenten

Typische TeSys™ island-Struktur

Die nachstehende Abbildung zeigt ein Beispiel für ein TeSys™ island, das aus zwei SIL[13]-Gruppen besteht. Die Zusammensetzung der Insel wird über die digitalen TeSys island-Tools in Übereinstimmung mit den Funktionsanforderungen des Benutzers festgelegt.

Abbildung 2 - TeSys island mit zwei SIL-Gruppen



A	SIL-Gruppe 1	E	Avatar A4
B	SIL-Gruppe 2	F	Verdrahtungskategorie 1, Stopp-Kategorie 0[14]
C	Avatar A1	G	Verdrahtungskategorie 2, Stopp-Kategorie 1[15]
D	Avatar A3		

SIL-Gruppe 1: Enthält einen Avatar, der zwei SIL-Starter umfasst, z. B. einen Avatar „Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2“ (Avatar A1). Der tatsächliche Motor ist mit diesen SIL-Startern verdrahtet und folgt der Avatar-Logik und den operativen Befehlen der SPS, die über den Feldbus gesendet werden. Der SIL-Stopp-Befehl kommt vom Not-Halt-Taster, der mit dem SIL-Schnittstellenmodul verdrahtet ist (Verdrahtungskategorie 1). Er veranlasst die SIL-Starter, die Last zu deaktivieren und in den sicheren Zustand zu wechseln (das Schütz wird geöffnet und der Motor wird deaktiviert).

SIL-Gruppe 2: Enthält zwei Avatars, z. B. einen „Schalter – SIL-Stopp, Verdrahtungskat. 1/2“ (Avatar A3) und einen „Motor – Eine Richtung – SIL-Stopp,

13. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
14. Verdrahtungskategorie 1 gemäß ISO 13849. Stopp-Kategorie 0 gemäß EN/IEC 60204-1.
15. Verdrahtungskategorie 2 gemäß ISO 13849. Stopp-Kategorie 1 gemäß EN/IEC 60204-1.

Verdrahtungskat. 1/2“ (Avatar A4). Beide Avatars umfassen einen einzelnen SIL-Starter. Beide Avatars folgen der Avatar-Logik und den operativen Befehlen der SPS, die über den Feldbus gesendet werden. Der SIL-Stopp-Befehl kommt vom externen Preventa™ XPS-Modul (oder Entsprechung), das mit dem SIL-Schnittstellenmodul verdrahtet ist. Er veranlasst die SIL-Starter, die Last zu deaktivieren und in den sicheren Zustand zu wechseln (Verdrahtungskategorie 2).

SIL-Gruppe

Eine SIL[16]-Gruppe besteht aus einem oder mehreren SIL-Avatars, die alle einem einzigen SIL-Schnittstellenmodul zugewiesen sind. Alle SIL-Avatars in der SIL-Gruppe reagieren auf einen einzigen SIL-Stopp-Befehl. Das SIL-Schnittstellenmodul ist immer rechts vom letzten SIL-Starter der SIL-Gruppe installiert (der vom Buskoppler abgewandten Seite).

Eine Insel kann mehrere SIL-Gruppen umfassen.

SIL-Avatars

Die für die SIL-Stopp-Funktionen verfügbaren SIL[17]-Avatars sind folgende:

- Schalter – SIL-Stopp, Verdrahtungskat. 1/2
- Schalter – SIL-Stopp, Verdrahtungskat. 3/4
- Motor – Eine Richtung – SIL-Stopp, Verdrahtungskat. 1/2
- Motor – Eine Richtung – SIL-Stopp, Verdrahtungskat. 3/4
- Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2
- Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 3/4
- Motor – Zwei Geschwindigkeiten – SIL-Stopp, Verdrahtungskat. 1/2
- Motor – Zwei Geschwindigkeiten – SIL-Stopp, Verdrahtungskat. 3/4
- Motor – Zwei Geschwindigkeiten/Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2
- Motor – Zwei Geschwindigkeiten/Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 3/4
- Förderband – Eine Richtung – SIL-Stopp, Verdrahtungskat. 1/2
- Förderband – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 3/4

SIL-Avatars bestehen aus bestimmten Hardware-Geräten, einschließlich SIL-Startern, Standard-Startern und dem erforderlichen SIL-Schnittstellenmodul, das die SIL-Gruppe verwaltet, der die SIL-Avatars zugewiesen sind.

HINWEIS: SIL-Avatars sind für Anwendungen mit einer geringen Häufigkeit von operativen Befehlen konzipiert, d. h. für einen Jahresdurchschnitt von weniger als 15 Start/Stopp-Zyklen pro Stunde.

16. Sicherheitsanforderungsstufe gemäß IEC 61508.
17. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.

SIL-Starter **Standard-Starter** **SIL-Schnittstellenmodul**

SIL-Schnittstellenmodul

Das TeSys™ island-SIL[18]-Schnittstellenmodul (SIM) ist ein Zubehörmodul, das für die Aktivierung des Funktionssicherheitsmerkmals der Insel erforderlich ist.

Die SIL-Stopp-Funktion wird durch rein elektromechanische Mittel erzielt, ohne digitale Kommunikation oder Buskoppler-Beteiligung.

Das SIM:

- Dient als Schnittstelle zum externen Preventa™ XPS-Modul (oder Entsprechung)
- Steuert die Stopp-Funktion seiner SIL-Gruppe
- Tauscht Betriebsdaten mit dem Buskoppler aus
- Meldet Betriebsinformationen über die LEDs auf der Vorderseite

SIL-Starter-Kontaktstatus

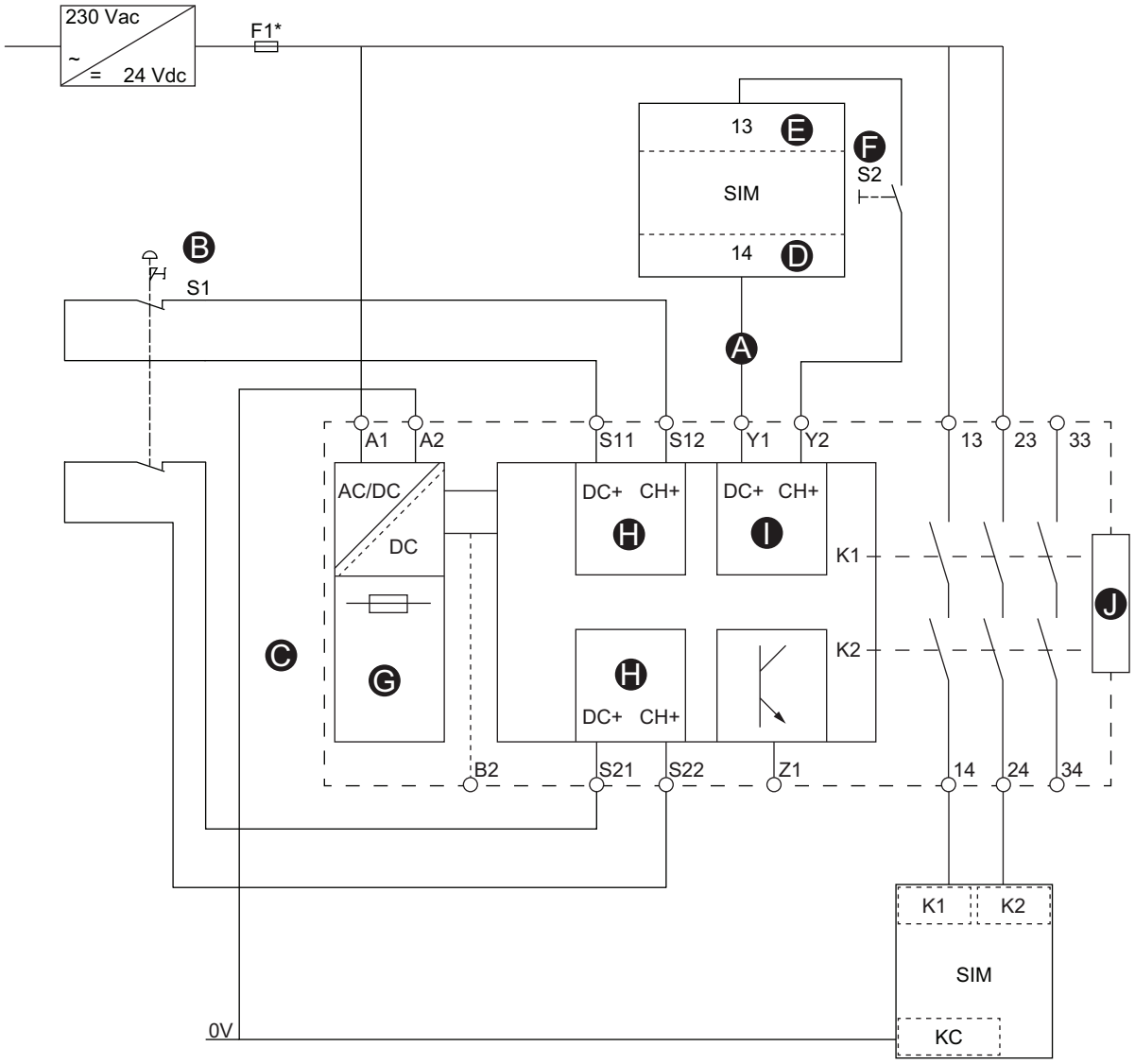
Der Status der SIL[18]-Starter, die zu einer SIL-Gruppe gehören, wird über die SIM-Spiegel-E/A-Anschlüsse gemeldet. Das ermöglicht die Implementierung von Architekturen der Verdrahtungskategorie 2[19], bei der die Spiegelkontakte an das Preventa XPS-Modul (oder Entsprechung) angeschlossen werden. Diese Konfigurationen bieten Möglichkeiten zur direkten Überwachung von elektromechanischen Geräten durch ein mechanisch verbundenes Kontaktelement, das einen Diagnosedeckungsgrad von bis zu 99 % ermöglicht. Siehe EN ISO 13849-1, Tabelle E.1 – Abschätzungen des Diagnosedeckungsgrades (DC).

Tabelle 2 - SIL-Starter-Kontaktstatus

SIL-Gruppenstatus	Spiegel-E/A-Status
Alle SIL-Starter sind offen	Spiegel-E/A-Kontakt ist geschlossen
Mindestens ein SIL-Starter ist geschlossen	Spiegel-E/A-Kontakt ist offen
Das TeSys island ist stromlos oder die Sicherheitsfunktion hat einen Fehler erkannt	Spiegel-E/A-Kontakt ist offen

18. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
19. Verdrahtungskategorie 2 gemäß ISO 13849.

Abbildung 3 - Verdrahtung von SIM und Preventa-Modul XPS-AF



A	Externe Startbedingungen (ESC)	F	Startknopf (S2)
B	Not-Halt-Taster (S1)	G	Spannungsversorgung
C	Preventa XPS-UAF-Modul	H	Eingang
D	SIM-Spiegel-Ausg.	I	Start
E	SIM-Spiegel-Eing.	J	Erweiterung

Sicherheitsbezogenes Sensorelement

Das SIM-Modul wird vorgeschaltet angeschlossen:

- An die 24-V DC-Quelle
- An das sicherheitsbezogene Sensorelement oder an ein Preventa XPS-Modul (oder Entsprechung)

Das SIM-Modul ist mit zwei Eingangskanälen für zweikanalige sicherheitsbezogene Sensorelemente ausgestattet. Für ein höheres Fehlertoleranzniveau wird die zweikanalige Architektur empfohlen.

Für die nachstehenden Schaltpläne siehe die Legende für SIM-Kanal-Schaltpläne, Seite 24.

Abbildung 4 - SIM – einkanalige Verdrahtung

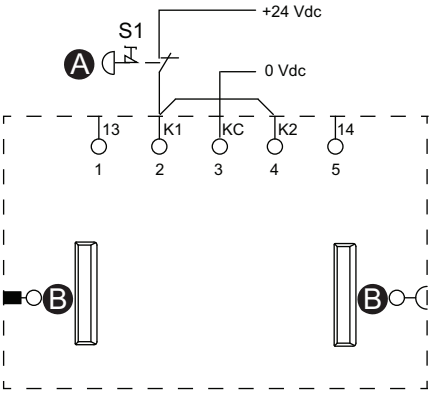


Abbildung 5 - SIM – zweikanalige Verdrahtung

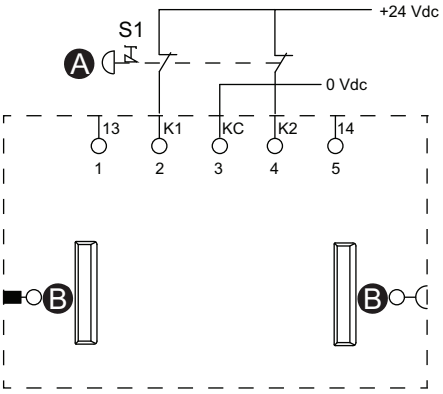


Tabelle 3 - Legende für SIM-Kanal-Schaltpläne

A	Not-Halt-Taster (S1)
B	Flachbandkabel

SIL-Starter

⚠WARNUNG

NICHT VORGESEHENER GERÄTEBETRIEB

Vollständige Anweisungen zur funktionalen Sicherheit finden Sie im TeSys™ island Funktionssicherheitshandbuch (8536IB1904).

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

SIL[20]-Starter bieten mit Standardstartern vergleichbare Funktionen, sind jedoch einem SIL-Schnittstellenmodul zugeordnet.

Die Hauptfunktionen der SIL-Starter sind:

- Bietet Funktionalität der Stoppkategorie 0 und Stoppkategorie 1[21]
- Betriebssteuerung für Lasten
- Messung der elektrischen Daten zur Last
- Bereitstellung von Energieüberwachungsdaten, wenn ein Spannungsschnittstellenmodul im TeSys island installiert ist

Für eine einzige TeSys avatar-Funktion sind gegebenenfalls mehrere SIL-Starter erforderlich. Der avatar „Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2“[22] zum Beispiel verfügt über zwei SIL-Starter. Darüber hinaus verfügen avatars, die SIL-Starter verwenden, immer über ein SIL-Schnittstellenmodul.

Die SIL-Starter sind folgendermaßen verbunden:

- Vorgeschaltet mit einem Leistungsschalter
- Nachgeschaltet mit der Last

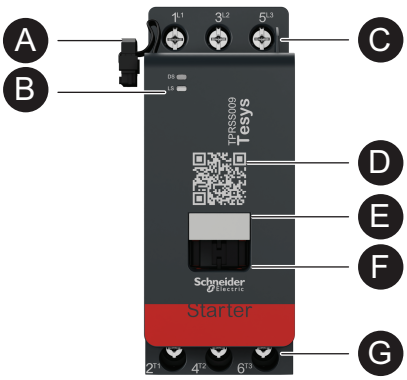
Die SIL-Starter kommunizieren mit dem Buskoppler, senden Betriebsdaten und empfangen Befehle.

Tabelle 4 - SIL-Starter-Nennwerte

Leistungsnennwerte		Stromstärke	Bestellnummer
kW	PS		
4	5	0,18–9	TPRSS009
11	15	0,5–25	TPRSS025
18,5	20	0,76–38	TPRSS038
30	40	3,25–65	TPRSS065
37	40	4–80	TPRSS080

20. Sicherheitsanforderungsstufe gemäß IEC 61508.
21. Stoppkategorie 0 und Stoppkategorie 1 gemäß EN/IEC 60204-1.
22. Verdrahtungskategorie 1 und 2 gemäß ISO 13849.

Abbildung 6 - SIL-Starter-Funktionen



A	Flachbandkabel (für die Verbindung mit dem Modul links)	E	Namens-Tag
B	LED-Statusanzeigen	F	Mobile Brücke
C	Vorgeschaltete Spannungsversorgungsanschlüsse	G	Nachgeschaltete Spannungsversorgungsanschlüsse
D	QR-Code		

Externes sicherheitsbezogenes Element

Das TeSys™ island muss mit anderen sicherheitsbezogenen Elementen in ein größeres, sicherheitsbezogenes System integriert werden, um die funktionale Sicherheit einer Maschine oder eines Systems/Prozesses sicherzustellen.

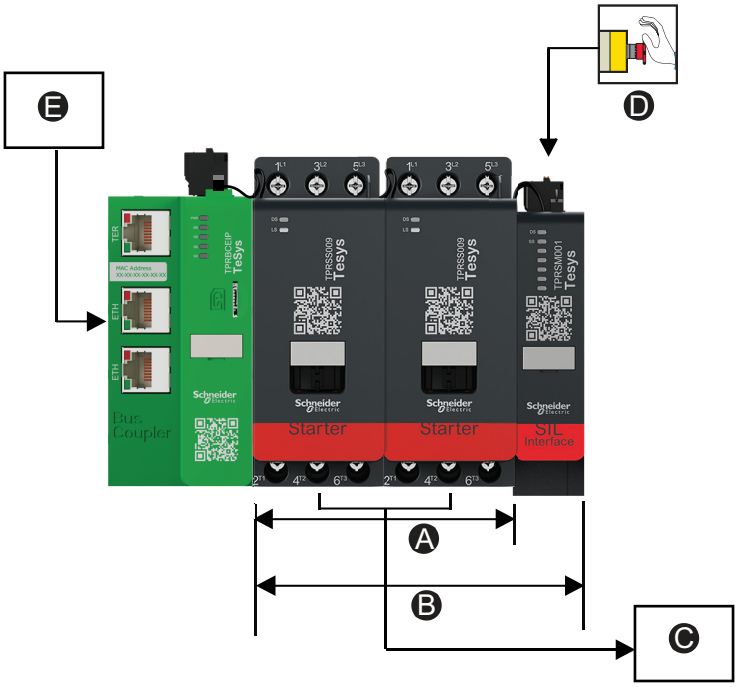
Die folgenden Konfigurationen zeigen typische Geräte.

Konfiguration SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 1

HINWEIS: Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 1 gemäß ISO 13849. Stopp-Kategorie 0 gemäß EN/IEC 60204-1.

Der SIL-Stopp des Motors wird direkt durch das Öffnen des Not-Halt-Taster-Kontakts gesteuert.

Abbildung 7 - SIL-Stopp



A	Avatar A1	D	Verdrahtungskategorie 1, Stopp-Kategorie 0
B	SIL-Gruppe 1	E	SPS
C	Motor		

Konfiguration SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 2

HINWEIS: Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 2 gemäß ISO 13849. Stopp-Kategorie 0 gemäß EN/IEC 60204-1.

Abbildung 8 - Beispiel: Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2 – Konfiguration Stopp-Kategorie 0, Verdrahtungskategorie 2 (indirekte Überwachung)

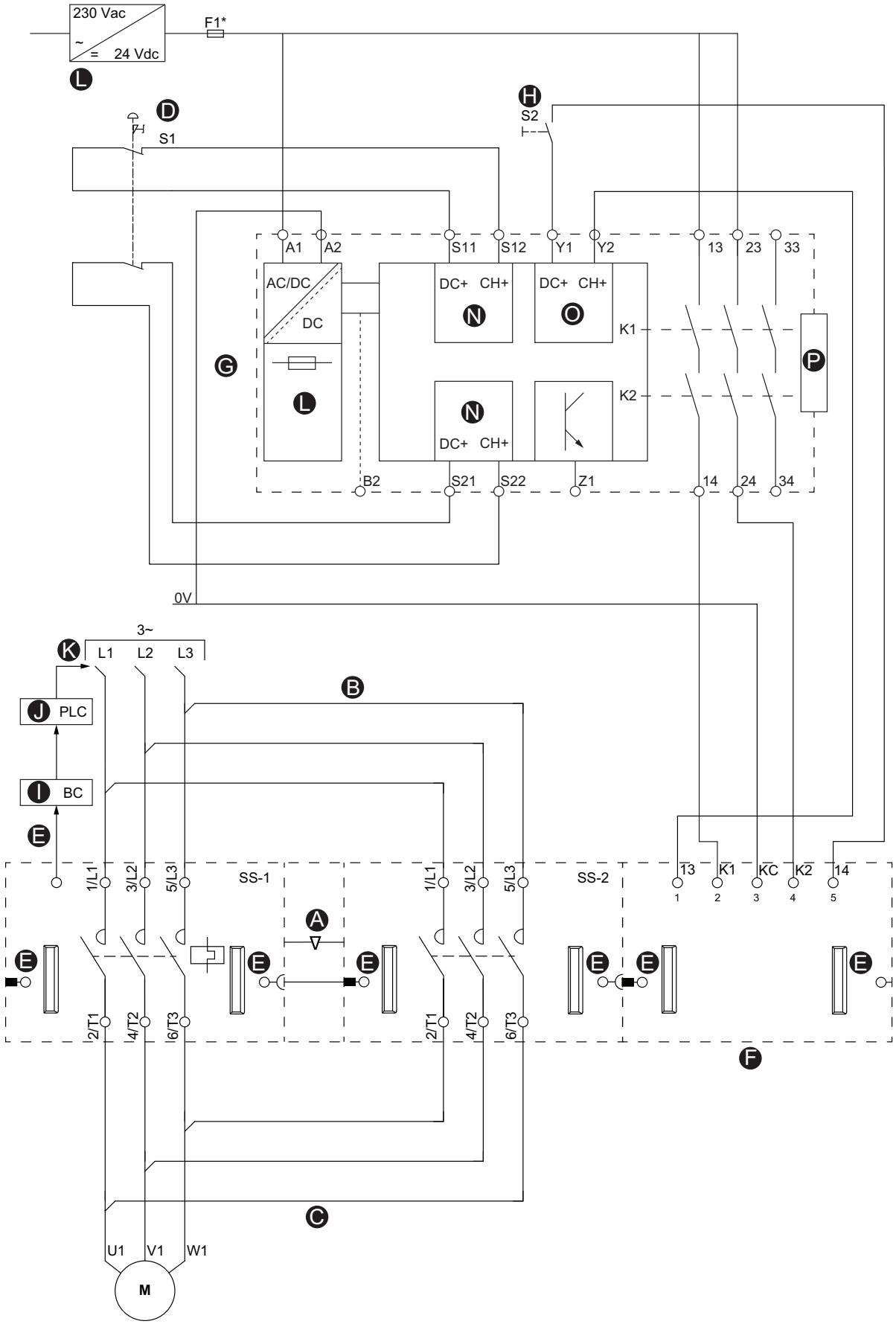
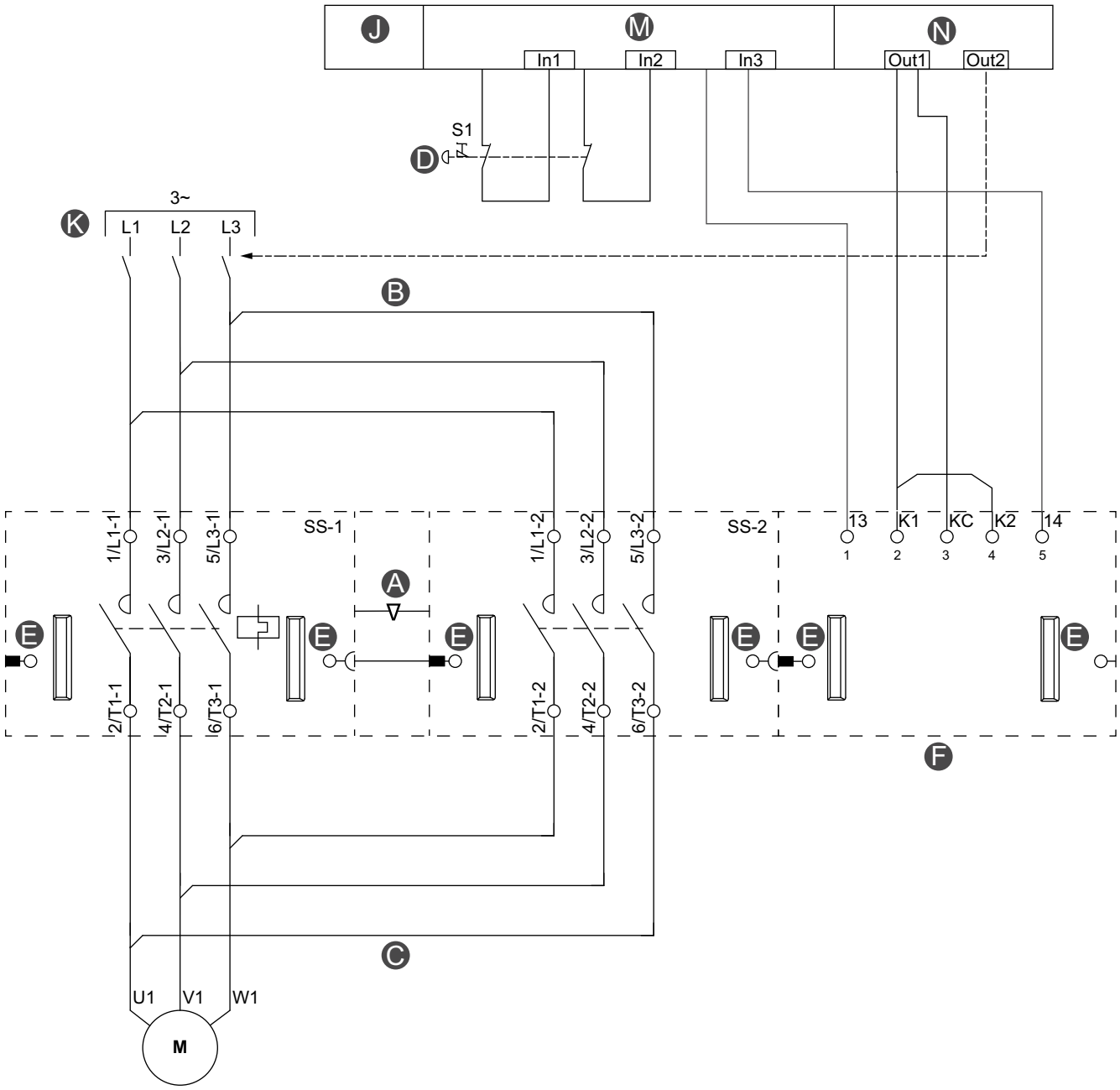


Tabelle 5 - Legende für Beispiel: Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2 – Konfiguration Stopp-Kategorie 0, Verdrahtungskategorie 2 (indirekte Überwachung), Seite 28

A	Mechanische Verriegelung	I	Buskoppler
B	Parallelbrücke	J	SPS
C	Reversierbrücke	K	Vorgeschalteter Leistungsschalter
D	Not-Halt-Taster (S1)	L	Spannungsversorgung
E	Flachbandkabel	N	Eingang
F	SIL-Schnittstellenmodul (SIM)	O	Start
G	Preventa XPS-UAF-Modul	P	Erweiterung
H	Startknopf (S2)		

Abbildung 9 - Beispiel: Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2 – Konfiguration Stopp-Kategorie 0, Verdrahtungskategorie 2 (direkte Überwachung)



A	Mechanische Verriegelung	F	SIL-Schnittstellenmodul (SIM)
B	Parallelbrücke	J	Sicherheitsfunktions-SPS
C	Reversierbrücke	K	Vorgeschalteter Leistungsschalter
D	Not-Halt-Taster (S1)	M	Digitaleingang
E	Flachbandkabel	N	Digitalausgang

Konfiguration SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 2

HINWEIS: Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 2 gemäß ISO 13849. Stopp-Kategorie 1 gemäß EN/IEC 60204-1.

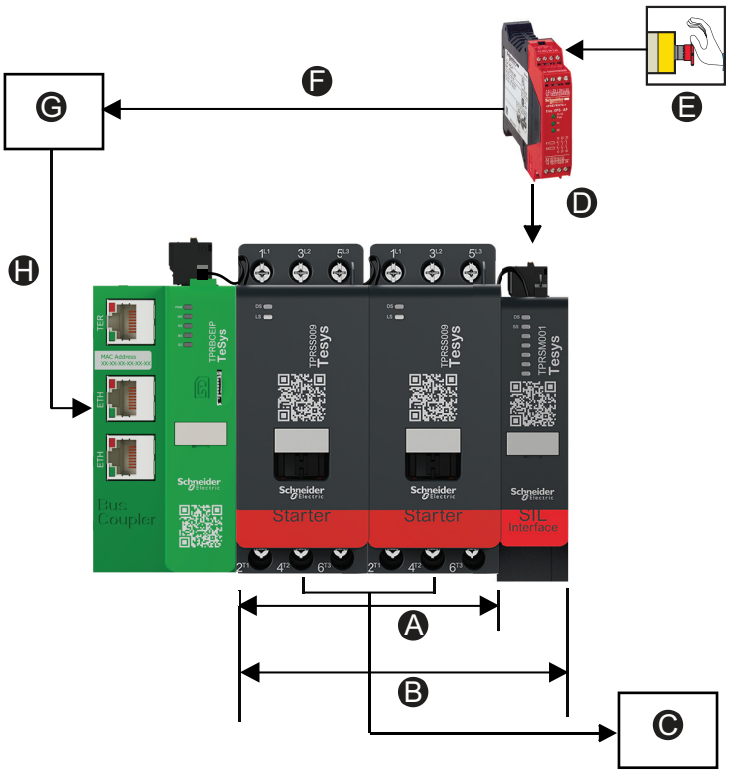
Die Stopp-Kategorie 1 ist definiert als „gesteuertes Stillsetzen, wobei die Energiezufuhr zu den Maschinen-Antriebselementen beibehalten wird, um das Stillsetzen zu erzielen. Die Energiezufuhr wird erst dann unterbrochen, wenn der Stillstand erreicht ist“.

Wenn der Not-Halt ausgelöst wird, wird der Stopp-Befehl zuerst an ein externes Gerät gesendet (z. B. an eine SPS oder einen Umrichter). Anstatt durch eine sofortige Unterbrechung der Energiezufuhr wird der Prozess auf diese Weise kontrolliert gestoppt. Nach einer vordefinierten Zeit wird der SIL-Stopp-Befehl an das SIM gesendet, um die Lasten auf den SIL-Avatars in der zugehörigen SIL-Gruppe zu deaktivieren.

Die empfohlene Konfiguration umfasst eine SPS, mit der sichergestellt wird, dass der Prozess korrekt angehalten wird, bevor der SIL-Stopp eintritt.

Der Stopp-Befehl kann direkt an einen SPS-Digitaleingang bzw. an einen Digitaleingang eines TeSys™ island-Digital-E/A-Modul-Avatars geleitet werden, der von der SPS gelesen wird. Nach dem Empfang des Stopp-Befehl-Eingangs initiiert die SPS ein gesteuertes Stillsetzen, indem sie einen operativen Befehl „Sicherer Betriebshalt“ an den betreffenden TeSys island-Avatar sendet.

Abbildung 10 - Stopp-Befehl



A	Avatar A1	E	Verdrahtungskategorie 2, Stopp-Kategorie 1
B	SIL-Gruppe 1	F	Befehl „Gesteuertes Stillsetzen“ Stopp-Kategorie 1

C	Motor	G	SPS
D	Ungesteuertes Stillsetzen	H	Operativer Stopp-Befehl

Abbildung 11 - Beispiel: Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2 – Konfiguration Stopp-Kategorie 1, Verdrahtungskategorie 2

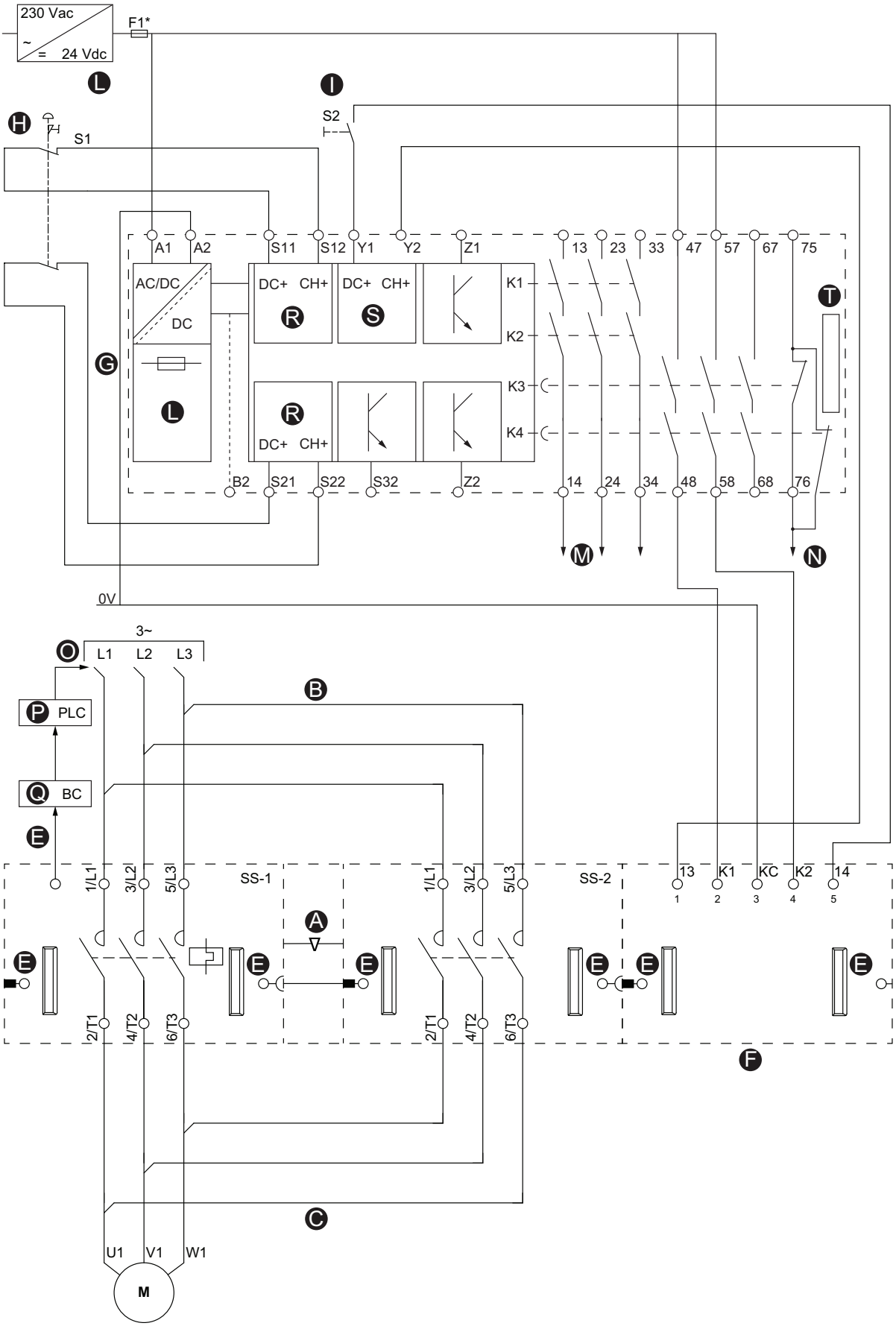


Tabelle 6 - Legende für Beispiel: Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2 – Konfiguration Stopp-Kategorie 1, Verdrahtungskategorie 2, Seite 33

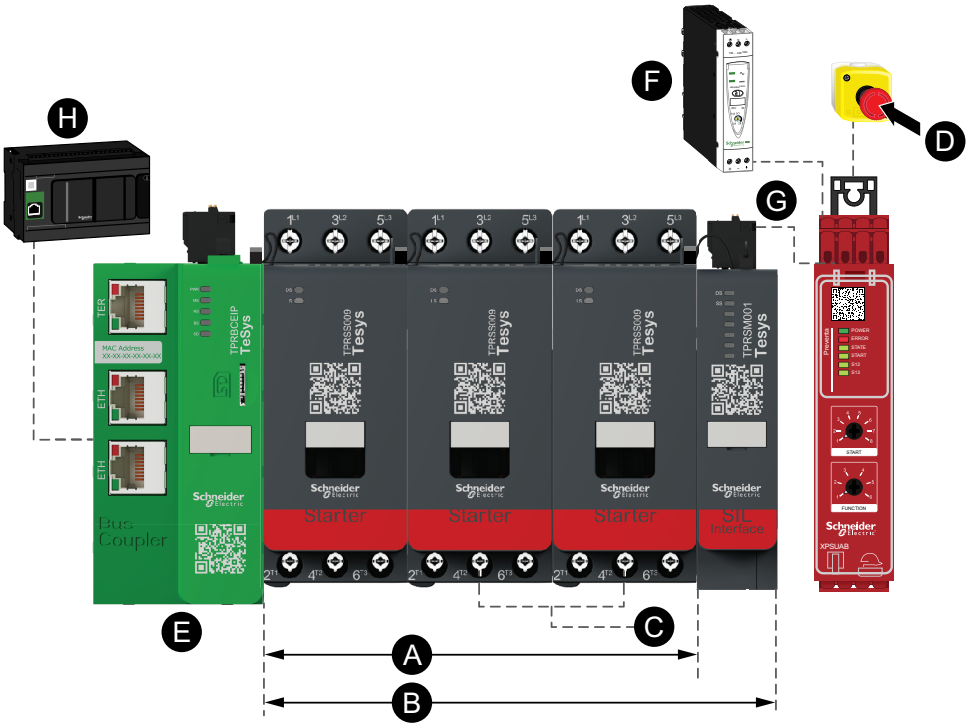
A	Mechanische Verriegelung	M	Gesteuertes Stillsetzen
B	Parallelbrücke	N	Stopp-Kategorie 1
C	Reversierbrücke	O	Vorgeschalteter Leistungsschalter
E	Flachbandkabel	P	SPS
F	SIL-Schnittstellenmodul (SIM)	Q	Buskoppler
G	Preventa XPS-UAF-Modul	R	Eingang
H	Not-Halt-Taster	S	Start
I	S2-Startknopf	T	Erweiterung
L	Spannungsversorgung		

SIL-Stopp, Stopp-Kategorie 0, Konfiguration Verdrahtungskategorie 3/4

HINWEIS: Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 3/4 gemäß ISO 13849. Stopp-Kategorie 0 gemäß EN/IEC 60204-1.

Der SIL-Stopp des Motors wird direkt durch das Öffnen des Not-Halt-Taster-Kontakts gesteuert.

Abbildung 12 - SIL-Stopp, Verdrahtungskategorie 3/4



A	Avatar A1	E	Buskoppler
B	SIL-Gruppe 1	F	24 VDC
C	Motor	G	Preventa XPS-UAF-Modul
D	Verdrahtungskategorie 3/4, Stopp-Kategorie 0	H	SPS

Abbildung 13 - Beispiel: Motor – Eine Richtung – SIL-Stopp, Verdrahtungskat. 3/4 – Konfiguration Stopp-Kategorie 0, Verdrahtungskategorie 3/4

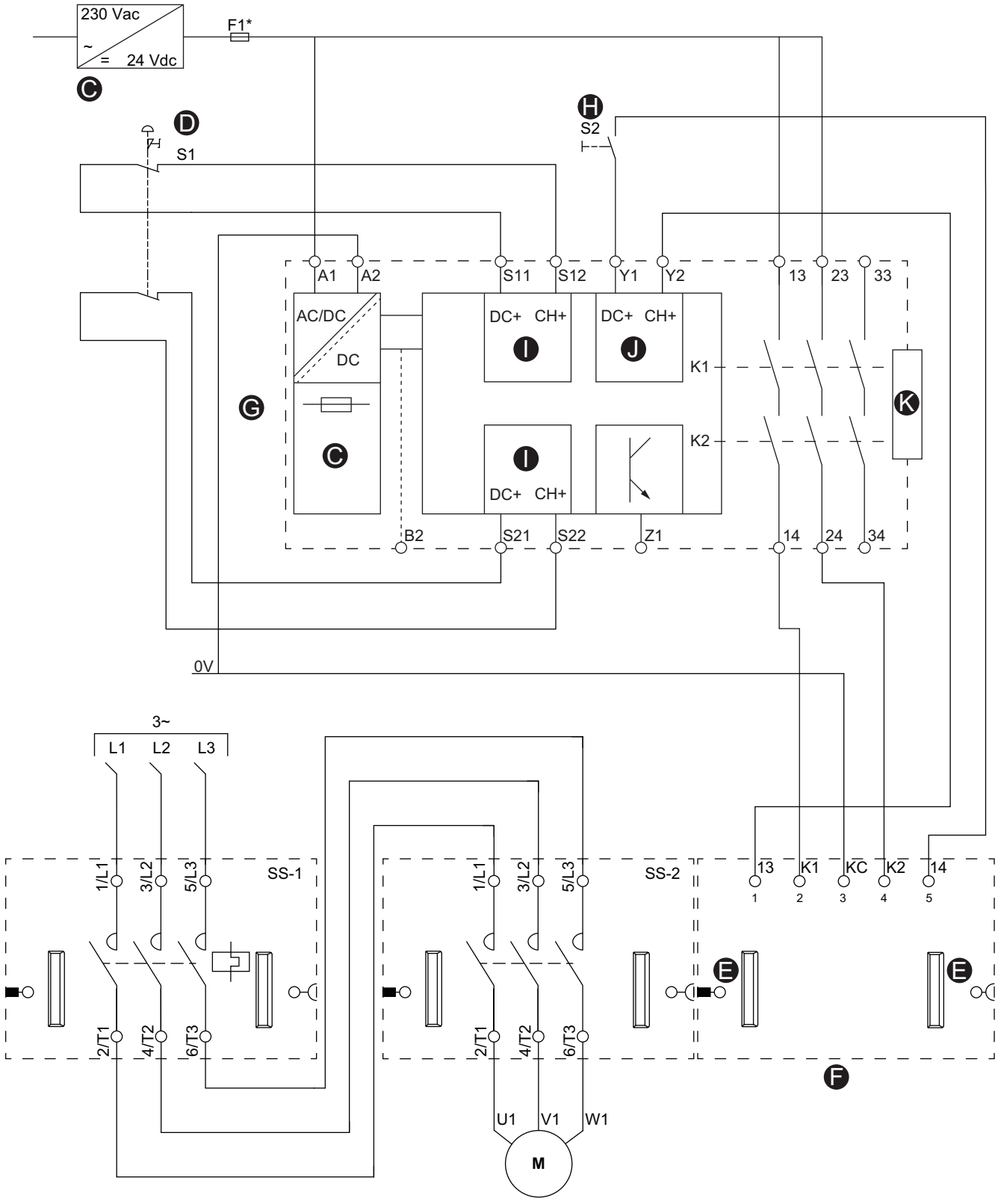


Tabelle 7 - Legende für Beispiel: Motor – Eine Richtung – SIL-Stopp, Verdrahtungskat. 3/4 – Konfiguration Stopp-Kategorie 0, Verdrahtungskategorie 3/4, Seite 36

C	Spannungsversorgung	H	Startknopf (S2)
D	Not-Halt-Taster (S1)	I	Eingang
E	Flachbandkabel	J	Start
F	SIL-Schnittstellenmodul (SIM)	K	Erweiterung
G	Preventa XPS-UAF-Modul		

SIL-Stopp, Stopp-Kategorie 1, Konfiguration Verdrahtungskategorie 3/4

HINWEIS: Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 3/4 gemäß ISO 13849. Stopp-Kategorie 1 gemäß EN/IEC 60204.

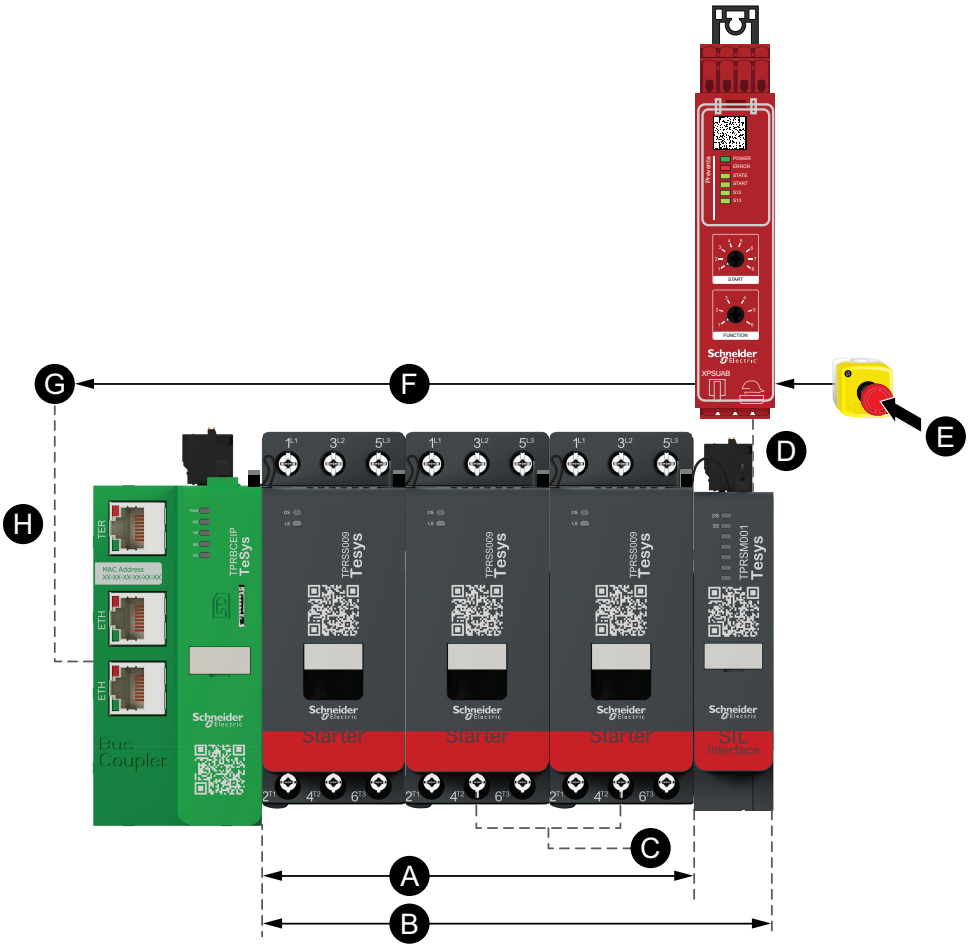
Die Stopp-Kategorie 1 ist definiert als „gesteuertes Stillsetzen, wobei die Energiezufuhr zu den Maschinen-Antriebselementen beibehalten wird, um das Stillsetzen zu erzielen. Die Energiezufuhr wird erst dann unterbrochen, wenn der Stillstand erreicht ist“.

Wenn der Not-Halt ausgelöst wird, wird der Stopp-Befehl zuerst an ein externes Gerät gesendet (z. B. an eine SPS oder einen Umrichter). Anstatt durch eine sofortige Unterbrechung der Energiezufuhr wird der Prozess auf diese Weise kontrolliert gestoppt. Nach einer vordefinierten Zeit wird der SIL-Stopp-Befehl an das SIM gesendet, um die Lasten auf den SIL-Avatars in der zugehörigen SIL-Gruppe zu deaktivieren.

Für die Einrichtung wird eine SPS empfohlen, mit der sichergestellt wird, dass der Prozess korrekt angehalten wird, bevor der SIL-Stopp eintritt.

Der Stopp-Befehl kann direkt an einen SPS-Digitaleingang bzw. an einen Digitaleingang eines TeSys™ island-Digital-E/A-Modul-Avatars geleitet werden, der von der SPS gelesen wird. Nach dem Empfang des Stopp-Befehl-Eingangs initiiert die SPS ein gesteuertes Stillsetzen, indem sie einen operativen Befehl „Sicherer Betriebshalt“ an den betreffenden TeSys island-Avatar sendet.

Abbildung 14 - Stopp-Befehl, Verdrahtungskategorie 3/4



A	Avatar A1	E	Verdrahtungskategorie 3/4, Stopp-Kategorie 1
B	SIL-Gruppe 1	F	Befehl „Gesteuertes Stillsetzen“ Stopp-Kategorie 1
C	Motor	G	SPS
D	Ungesteuertes Stillsetzen	H	Operativer Stopp-Befehl

Abbildung 15 - Beispiel: Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 3/4 – Konfiguration Stopp-Kategorie 1, Verdrahtungskategorie 3/4

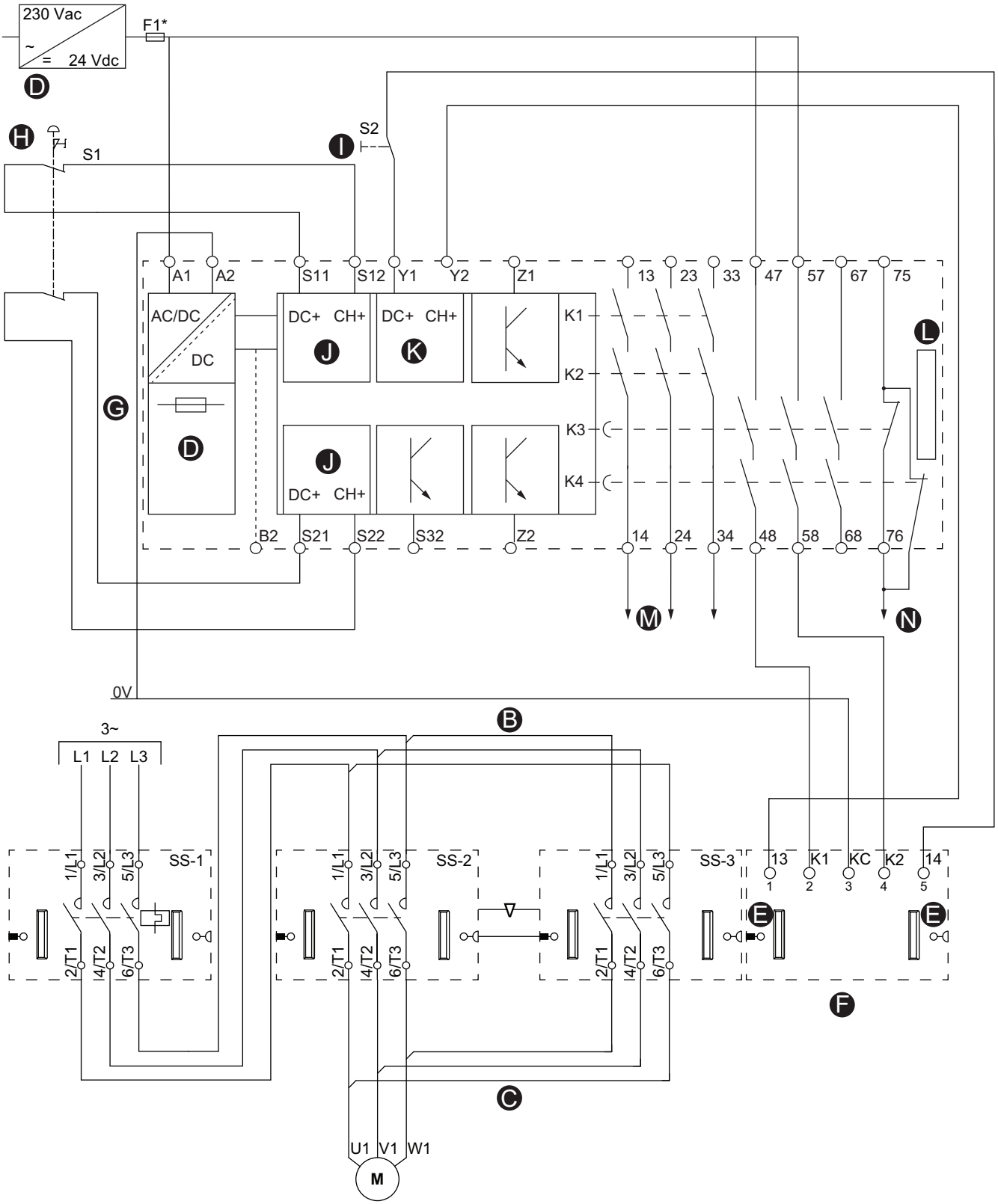


Tabelle 8 - Legende für Beispiel: Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 3/4 – Konfiguration Stopp-Kategorie 1, Verdrahtungskategorie 3/4, Seite 39

B	Parallelbrücke	I	S2-Startknopf
C	Reversierbrücke	J	Eingang
D	Spannungsversorgung	K	Start
E	Flachbandkabel	L	Erweiterung
F	SIL-Schnittstellenmodul (SIM)	M	Gesteuertes Stillsetzen
G	Preventa XPS-UAF-Modul	N	Stopp-Kategorie 1
H	Not-Halt-Taster (S1)		

Geschützte Kabelisolierung

⚠ GEFAHR

NICHT BESTIMMUNGSGEMÄSSER GERÄTEBETRIEB

Vergewissern Sie sich, dass die Kabel des sicherheitsbezogenen Systems gemäß ISO 13849-2 installiert werden.

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

Wenn in den Kabeln des sicherheitsbezogenen Systems Kurz- und Querschlüsse auftreten können und diese von den vorgeschalteten Geräten nicht erkannt werden, ist eine geschützte Kabelinstallation gemäß ISO 13849-2 erforderlich.

Bei einer ungeschützten Kabelinstallation dürfen die zwei Signale (beide Kanäle) einer Sicherheitsfunktion in einem Kurzschluss-Zustand an eine externe Spannung angeschlossen werden, wenn ein Kabel beschädigt ist. In diesem Fall ist die Sicherheitsfunktion nicht mehr wirksam.

Architektur mit geringer/hoher Schalthäufigkeit

Die Informationen in diesem Abschnitt können verwendet werden, um festzustellen, ob Sie mit einer Architektur mit geringer oder hoher Schalthäufigkeit arbeiten.

Der elektromechanische Teil des SIL[23]-Starters hat einen B10d-Wert.

Für die Berechnung der $MTTF_d$ (gemäß ISO 13849-1) oder von λd (gemäß IEC 62061) gilt die folgende Formel:

$$MTTF_d = B10d / (0,1 * Nop)$$

mit $\lambda d = 1 / MTTF_d$

Nop: Mittlere Anzahl der Schaltspiele pro Jahr

Gemäß ISO 13849 ist die Betriebszeit einer elektromechanischen Komponente auf T10d begrenzt (mittlere Zeit, bis 10 % der Komponenten gefährlich ausgefallen sind[24]).

Deshalb ist die Betriebszeit eines SIL-Starters auf Folgendes begrenzt:

$$T10d = B10d / Nop$$

Der B10d-Wert des SIL-Starters ist B10d = 1.369.863 und setzt einen T10d-Wert von 10 Jahren voraus. Die Anzahl der Schaltspiele für einen TeSys island-SIL-Starter ist auf Nop = B10d/T10 = 131.400/Jahr (oder Jahresdurchschnitt von 15 Schaltspielen/h) begrenzt.

Wenn für die Anwendung ein geringerer Nop-Wert als dieser erforderlich ist, fällt sie in die Kategorie „Geringe Schalthäufigkeit“ (dann können SIL-Avatars unverändert genutzt werden). Anderenfalls fällt sie in die Kategorie „Hohe Schalthäufigkeit“ (hier muss die Sicherheitsfunktion wie nachstehend beschrieben mit einem speziellen SIL-Avatar implementiert werden).

23. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
24. Gefährlich ausgefallen gemäß ISO 13849

Geringe Schalthäufigkeit (< 15 Schaltspiele pro Stunde)

Bei einer geringen Schalthäufigkeit können die SIL[25] -Stopp- sowie die operativen Ein-/Aus-Steuerungsfunktionen mit einem SIL-Avatar realisiert werden.

Abbildung 16 - Beispiel-Avatar mit SIL-Starter

Tabelle 9 - Geringe Schalthäufigkeit – Betriebs- und Sicherheitsfunktionen

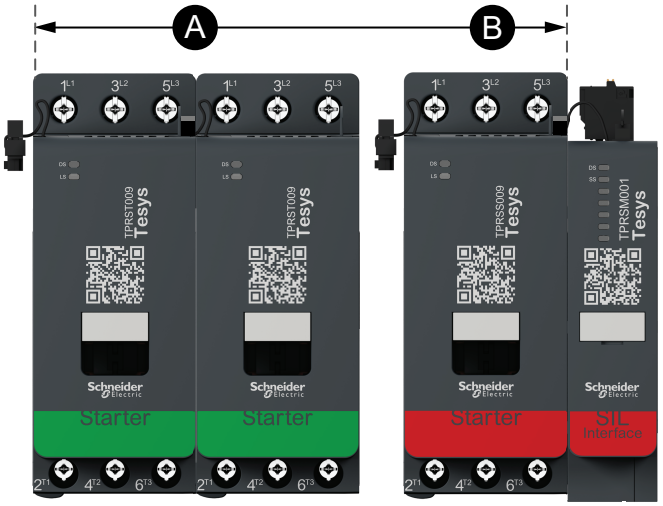
SIL-Avatar	Modul 1	Modul 2	Modul 3	Modul 4	Modul 5
Schalter – SIL-Stopp, Verdrahtungskat. 1/2[26]	SIL-Starter	SIM	—	—	—
Schalter – SIL-Stopp, Verdrahtungskat. 3/4[27]	SIL-Starter	SIL-Starter	SIM	—	—
Motor – Eine Richtung – SIL-Stopp, Verdrahtungskat. 1/2	SIL-Starter	SIM		—	—
Motor – Eine Richtung – SIL-Stopp, Verdrahtungskat. 3/4	SIL-Starter	SIL-Starter	SIM	—	—
Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2	SIL-Starter	SIL-Starter	SIM	—	—
Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 3/4	SIL-Starter	SIL-Starter	SIL-Starter	SIM	—
Motor – Zwei Geschwindigkeiten – SIL-Stopp, Verdrahtungskat. 1/2	SIL-Starter	SIL-Starter	SIM	—	—
Motor – Zwei Geschwindigkeiten – SIL-Stopp, Verdrahtungskat. 3/4	SIL-Starter	SIL-Starter	SIL-Starter	SIM	—
Motor – Zwei Geschwindigkeiten/Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	Standard-Starter	SIL-Starter	SIL-Starter	SIM
Motor – Zwei Geschwindigkeiten/Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 3/4	SIL-Starter	SIL-Starter	SIL-Starter	SIL-Starter	SIM
Förderband – Eine Richtung – SIL-Stopp, Verdrahtungskat. 1/2	SIL-Starter	SIM	—	—	—
Förderband – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2	SIL-Starter	SIL-Starter	SIM	—	—

25. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
26. Verdrahtungskategorie 1 und 2 gemäß ISO 13849.
27. Verdrahtungskategorie 3 und 4 gemäß ISO 13849.

Hohe Schalthäufigkeit (≥ 15 Schaltspiele pro Stunde)

Bei einer hohen Schalthäufigkeit muss die Sicherheitsfunktion von der Betriebsfunktion isoliert werden, indem ein SIL[28]-Avatar für die Sicherheitsfunktion und ein Standard-Avatar für die Betriebsfunktion verwendet wird. Die Standard-Starter werden dann – den SIL-Startern nachgeschaltet – in Reihe verdrahtet. Die Tabelle „Hohe Schalthäufigkeit - Betriebs- und Sicherheitsfunktionen“ enthält Beispiele für Standard-Avatars, die nachgeschaltet zu den SIL-Startern für Architekturen des Typs SIL-Stopp, Verdrahtungskat. 1/2[29] und SIL-Stopp, Verdrahtungskat. 3/4[30] verwendet werden.

Abbildung 17 - Standard-Avatar für Betriebsfunktion und SIL-Avatar für Sicherheitsfunktion – SIL-Stopp, Verdrahtungskat. 1/2



A	Standard-Avatar
B	SIL-Avatar

Tabelle 10 - Hohe Schalthäufigkeit – SIL-Stopp, Verdrahtungskat. 1/2 – Betriebs- und Sicherheitsfunktionen

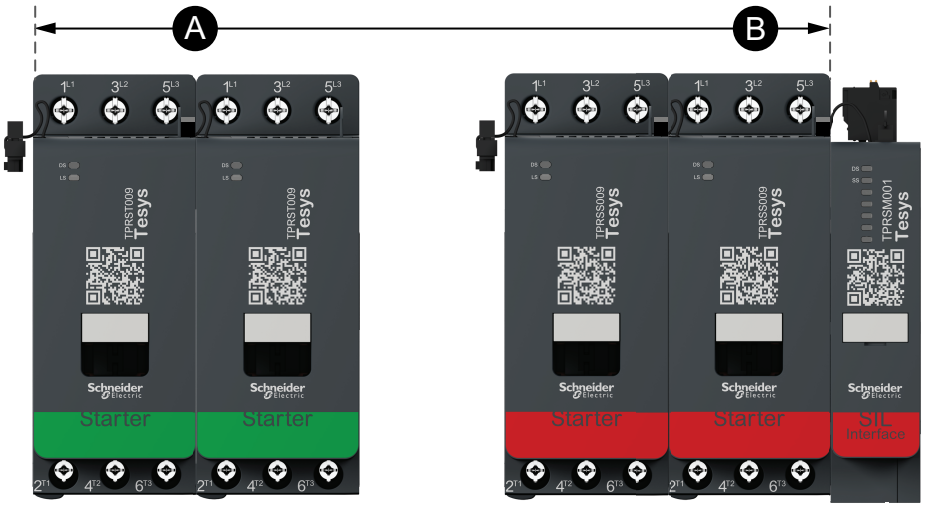
Standard-Avatar	SIL-Avatar	Modul 1	Modul 2	Modul 3	Modul 4	Modul 5	Modul 6
Schalter	Schalter – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	SIL-Starter	SIM	—	—	—
Motor – Eine Richtung	Schalter – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	SIL-Starter	SIM	—	—	—
Motor – Zwei Richtungen	Schalter – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	Standard-Starter	SIL-Starter	SIM	—	—
Motor – Zwei Geschwindigkeiten	Schalter – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	Standard-Starter	SIL-Starter	SIM	—	—
Motor – Zwei Geschwindigkeiten/Zwei Richtungen	Schalter – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	Standard-Starter	Standard-Starter	Standard-Starter	SIL-Starter	SIM
Förderband – Eine Richtung	Schalter – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	SIL-Starter	SIM	—	—	—
Förderband – Zwei Richtungen	Schalter – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	Standard-Starter	SIL-Starter	SIM	—	—

28. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
29. Verdrahtungskategorie 1 und 2 gemäß ISO 13849.
30. Verdrahtungskategorie 3 und 4 gemäß ISO 13849.

Tabelle 10 - Hohe Schalthäufigkeit – SIL-Stopp, Verdrahtungskat. 1/2 – Betriebs- und Sicherheitsfunktionen (Fortsetzung)

Standard-Avatar	SIL-Avatar	Modul 1	Modul 2	Modul 3	Modul 4	Modul 5	Modul 6
Motor Y/D – Eine Richtung	Schalter – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	Standard-Starter	Standard-Starter	SIL-Starter	SIM	—
Motor Y/D – Zwei Richtungen	Schalter – SIL-Stopp, Verdrahtungskat. 1/2	Standard-Starter	Standard-Starter	Standard-Starter	Standard-Starter	SIL-Starter	SIM

Abbildung 18 - Standard-Avatar für Betriebsfunktion und SIL-Avatar für Sicherheitsfunktion – SIL-Stopp, Verdrahtungskat. 3/4



A	Standard-Avatar
B	SIL-Avatar

Tabelle 11 - Hohe Schalthäufigkeit – SIL-Stopp, Verdrahtungskat. 3/4 – Betriebs- und Sicherheitsfunktionen

Standard-Avatar	SIL-Avatar	Modul 1	Modul 2	Modul 3	Modul 4	Modul 5	Modul 6	Modul 7
Schalter	Schalter – SIL-Stopp, Verdrahtungskat. 3/4	Standard-Starter	SIL-Starter	SIL-Starter	SIM	—	—	—
Motor – Eine Richtung	Schalter – SIL-Stopp, Verdrahtungskat. 3/4	Standard-Starter	SIL-Starter	SIL-Starter	SIM	—	—	—
Motor – Zwei Richtungen	Schalter – SIL-Stopp, Verdrahtungskat. 3/4	Standard-Starter	Standard-Starter	SIL-Starter	SIL-Starter	SIM	—	—
Motor – Zwei Geschwin-digkeiten	Schalter – SIL-Stopp, Verdrahtungskat. 3/4	Standard-Starter	Standard-Starter	SIL-Starter	SIL-Starter	SIM	—	—
Motor – Zwei Geschwin-digkeiten/ Zwei Richtungen	Schalter – SIL-Stopp, Verdrahtungskat. 3/4	Standard-Starter	Standard-Starter	Standard-Starter	Standard-Starter	SIL-Starter	SIL-Starter	SIM
Motor Y/D – Eine Richtung	Schalter – SIL-Stopp, Verdrahtungskat. 3/4	Standard-Starter	Standard-Starter	Standard-Starter	Standard-Starter	SIL-Starter	SIL-Starter	SIM
Motor Y/D – Zwei Richtungen	Schalter – SIL-Stopp, Verdrahtungskat. 3/4	Standard-Starter	Standard-Starter	Standard-Starter	Standard-Starter	SIL-Starter	SIL-Starter	SIM

Musterarchitekturen

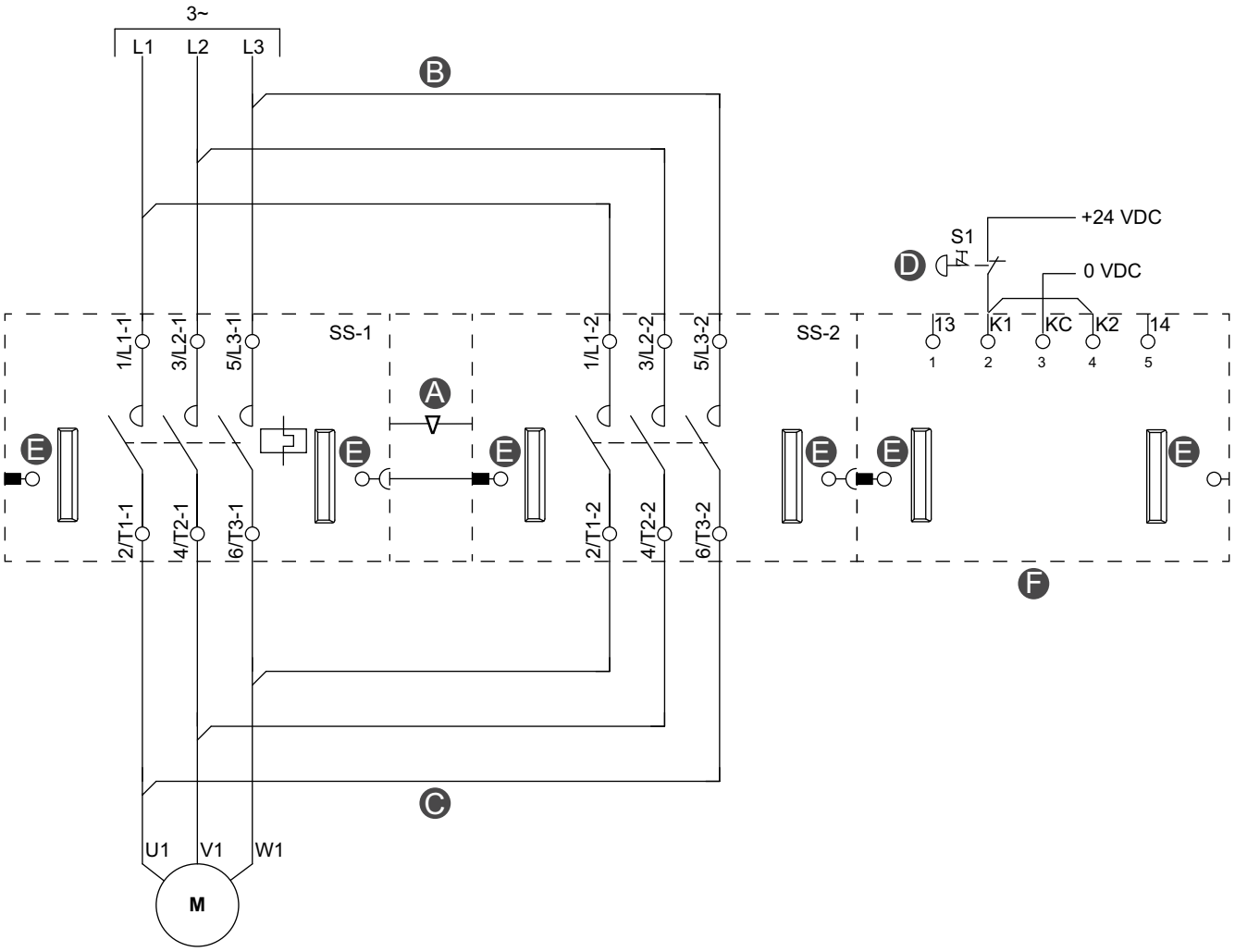
Die folgenden Architekturen sind für die TeSys™ island-Funktionssicherheit erhältlich:

- SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 1[31]
- SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 2
- SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 2
- SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 3/4
- SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 3/4

31. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 1, Kategorie 2 und Kategorie 3/4 gemäß ISO 13849. Stopp-Kategorie 0 und Kategorie 1 gemäß EN/IEC 60204-1.

SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 1

Abbildung 19 - Beispiel: SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 1[32]

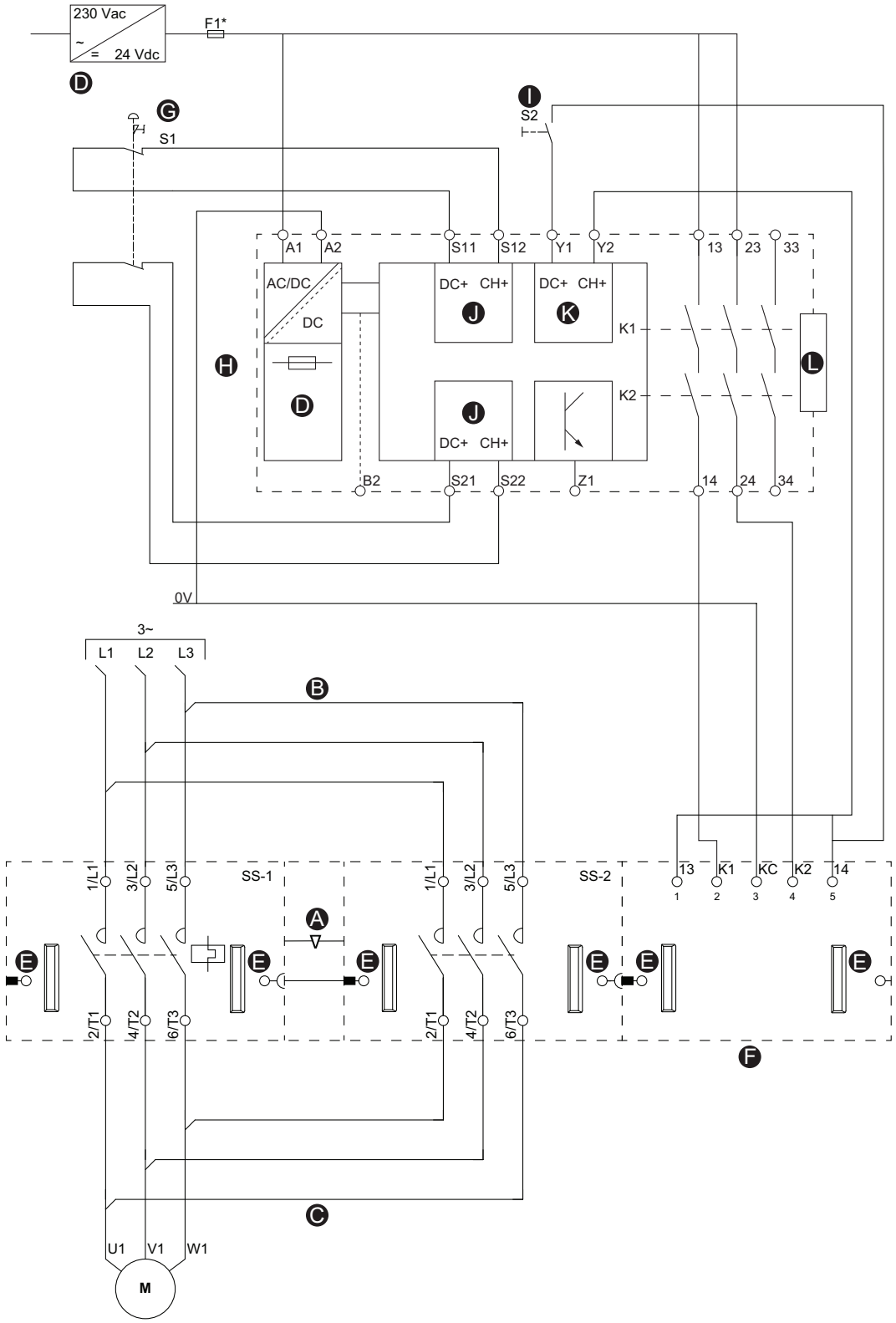


A	Mechanische Verriegelung	D	Not-Halt-Taster (S1)
B	Parallelbrücke	E	Flachbandkabel
C	Reversierbrücke	F	SIL-Schnittstellenmodul (SIM)

32. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 1 gemäß ISO 13849. Stopp-Kategorie 0 gemäß EN/IEC 60204-1.

SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 2

Abbildung 20 - Beispiel: SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 2[33]



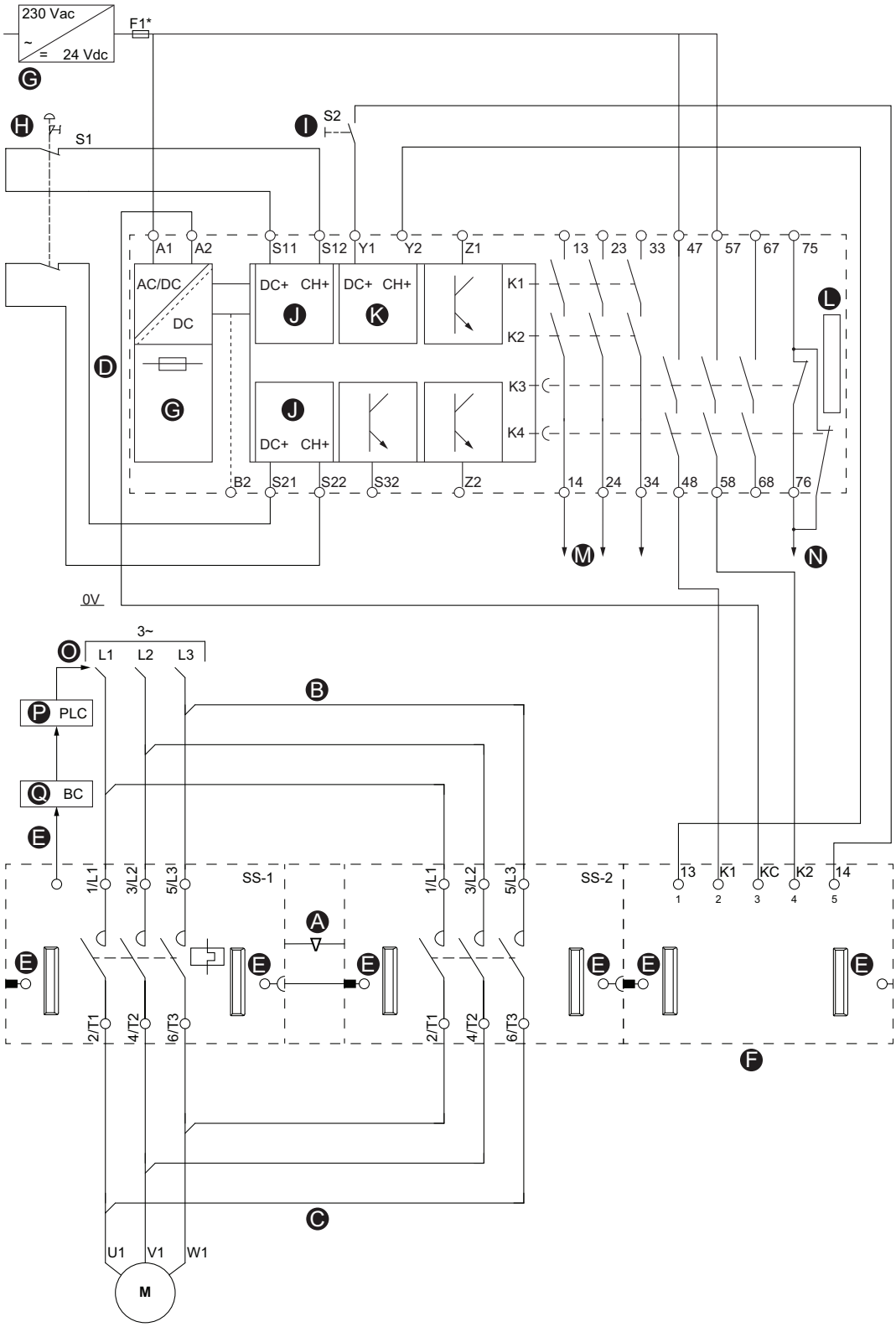
33. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 2 gemäß ISO 13849. Stopp-Kategorie 0 gemäß EN/IEC 60204-1.

Tabelle 12 - Legende für Beispiel: SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 2, Seite 48

A	Mechanische Verriegelung	G	Not-Halt-Taster (S1)
B	Parallelbrücke	H	Preventa XPS-UAF-Modul
C	Reversierbrücke	I	Startknopf (S2)
D	Spannungsversorgung	J	Eingang
E	Flachbandkabel	K	Start
F	SIL-Schnittstellenmodul (SIM)	L	Erweiterung

SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 2

Abbildung 21 - Beispiel: SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 2[34]



34. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 2 gemäß ISO 13849. Stopp-Kategorie 1 gemäß EN/IEC 60204-1.

Tabelle 13 - Legende für Beispiel: SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 2, Seite 50

A	Mechanische Verriegelung	J	Eingang
B	Parallelbrücke	K	Start
C	Reversierbrücke	L	Erweiterung
E	Flachbandkabel	M	Gesteuertes Stillsetzen
F	SIL-Schnittstellenmodul (SIM)	N	Stopp-Kategorie 1
G	Spannungsversorgung	O	Vorgeschalteter Leistungsschalter
H	Not-Halt-Taster (S1)	P	SPS
I	S2-Startknopf	Q	Buskoppler

SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 3/4

Abbildung 22 - Beispiel: SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 3/4[35]

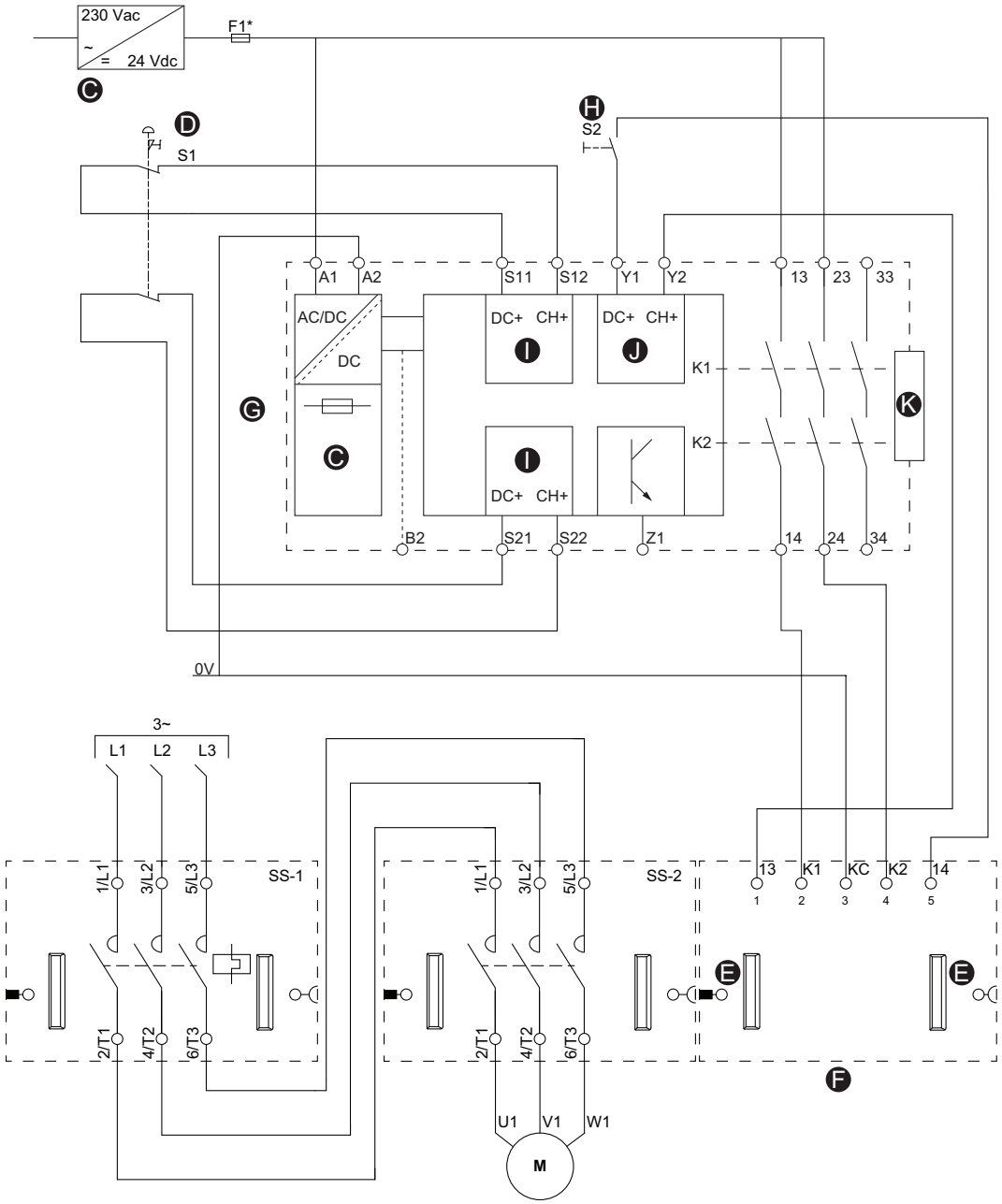


Tabelle 14 - Legende für Beispiel: SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 3/4, Seite 52

C	Spannungsversorgung	H	Startknopf (S2)
D	Not-Halt-Taster (S1)	I	Eingang
E	Flachbandkabel	J	Start

35. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 3/4 gemäß ISO 13849. Stopp-Kategorie 0 gemäß EN/IEC 60204-1.

Tabelle 14 - Legende für Beispiel: SIL-Stopp, Stopp-Kategorie 0, Verdrahtungskategorie 3/4 (Fortsetzung)

F	SIL-Schnittstellenmodul (SIM)	K	Erweiterung
G	Preventa XPS-UAF-Modul		

SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 3/4

Abbildung 23 - Beispiel: SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 3/4[36]

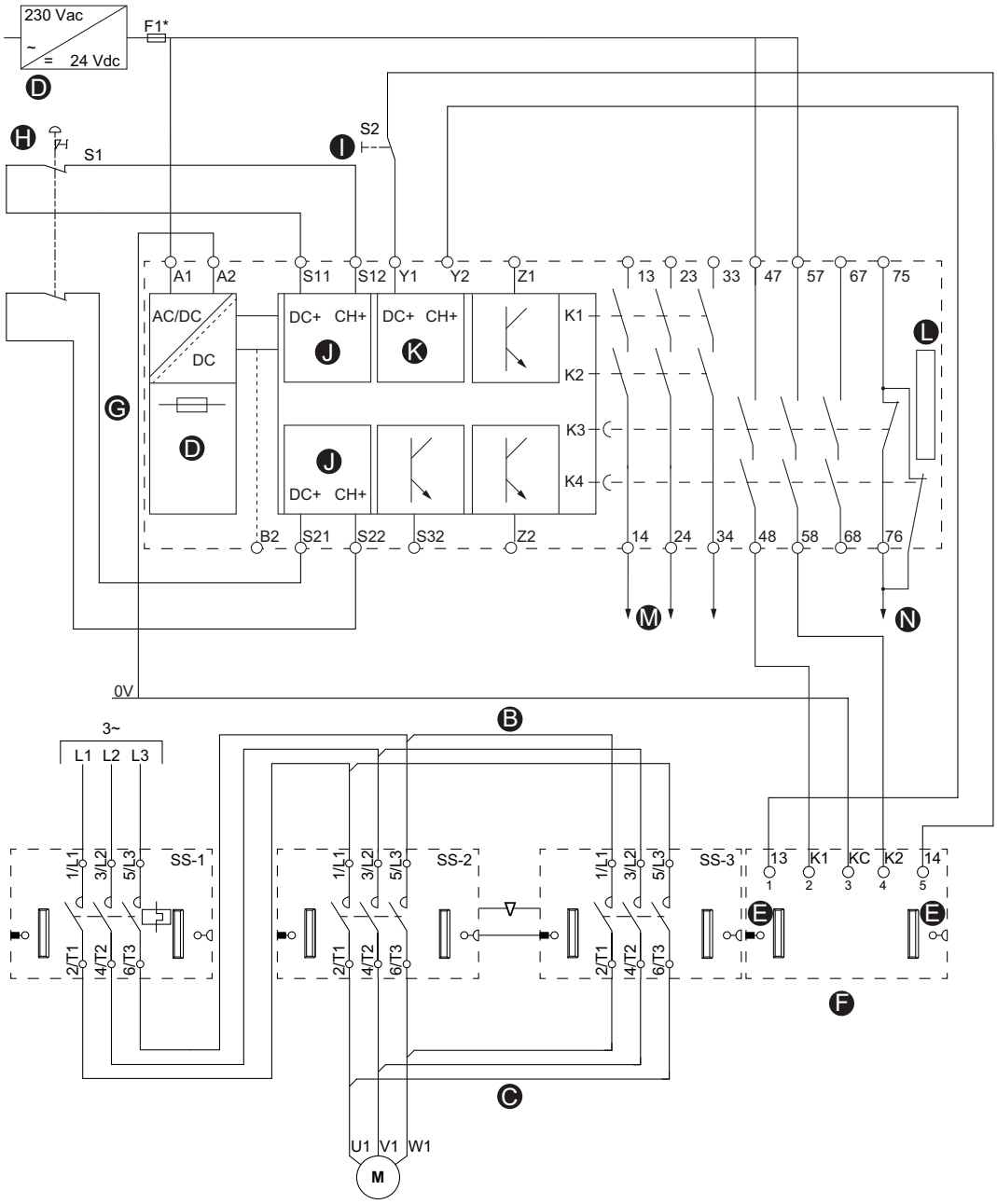


Tabelle 15 - Legende für Beispiel: SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 3/4, Seite 54

B	Parallelbrücke	I	S2-Startknopf
C	Reversierbrücke	J	Eingang
D	Spannungsversorgung	K	Start
E	Flachbandkabel	L	Erweiterung

36. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508. Verdrahtungskategorie 3/4 gemäß ISO 13849. Stopp-Kategorie 1 gemäß EN/IEC 60204-1.

Tabelle 15 - Legende für Beispiel: SIL-Stopp, Stopp-Kategorie 1, Verdrahtungskategorie 3/4 (Fortsetzung)

F	SIL-Schnittstellenmodul (SIM)	M	Gesteuertes Stillsetzen
G	Preventa XPS-UAF-Modul	N	Stopp-Kategorie 1
H	Not-Halt-Taster (S1)		

Technische Daten

SIL-Schnittstellenmodul

Tabelle 16 - Berechnete Werte des SIL[37]- Schnittstellenmoduls (SIM)

Architektur	SIM					
	PFH[38]	PFD[39]	SFF[40]	HFT[41]	$MTTF_d$ (Jahre)	DC[42]
Verdrahtungs-kategorie 1[43]	$2{,}10^{-10}$	$2{,}10^{-5}$	> 90 %	1	17.459	Nicht relevant
Verdrahtungs-kategorie 2			> 99%			90%
Verdrahtungs-kategorie 3			> 99%			90%
Verdrahtungs-kategorie 4			99%			99%

HINWEIS: Die PFD- und PFH-Werte werden folgendermaßen berechnet:

- Testintervall = 20 Jahre
- MTTR[44] = MRT[45] = 24 Stunden

Die architektonischen Anforderungen gemäß IEC 61508-2 Tabelle 3 und EN 62061 Tabelle 5 werden bis zu Stufe SIL 3 erfüllt.

SIL-Starter

Mit den folgenden Daten kann der Performance-Level von SIL[37]-Startern bestimmt werden.

B10: **1.000.000**

% gefährliche Ausfälle[46]: **73%**

$B10_d$: **1.369.863**

Vorausgesetzt wird eine Anzahl an Vorgängen = 131.400 Schaltspiele/Jahr (Durchschnitt von 15 Schaltspiele/Stunde)

Die berechneten Werte des SIL-Starters sind in den nachstehenden Tabellen angegeben:

Tabelle 17 - SIL-Starter – einkanalig

Verdrahtungskategorie[43]	SFF	HFT	$MTTF_d$ (Jahre)	Gleichspan-nung
Kategorie 1	27%	0	100 Jahre	Nicht relevant
Kategorie 2 – Direktüberwachung	90%	0	100 Jahre	≥ 90%

37. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
38. Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [h-1] gemäß der Norm IEC 61508-4
39. Wahrscheinlichkeit eines gefährlichen Ausfalls bei Anforderung gemäß der Norm IEC 61509-4.
40. Anteil ungefährlicher Ausfälle gemäß der Norm IEC 61509-4.
41. Hardware-Fehlertoleranz gemäß der Norm IEC 61509-4.
42. Diagnosedeckungsgrad gemäß der Norm IEC 61509-4.
43. Verdrahtungskategorien 1, 2, 3 und 4 gemäß ISO 13849.
44. Durchschnittliche Reparaturzeit gemäß der Norm IEC 61509-4
45. Mittlere Reparaturdauer gemäß der Norm IEC 61509-4
46. Gefährliche Ausfälle gemäß der Norm IEC 61508-4

Tabelle 18 - SIL-Starter – zweikanalig

Verdrahtungs-kategorie	SFF	HFT	$MTTF_d$ (Jahre)	Gleichspan-nung
Kategorie 3	27%	0	100 Jahre	≥ 90%
Kategorie 4	90%	0	100 Jahre	≥ 99 %

Die Beziehung zwischen den Werten PFH_d und PFD der SIL-Starter in Abhängigkeit der Architektur und des Testintervalls ist in der nachstehenden Tabelle angegeben:

Tabelle 19 - SIL-Starter – PFH_d und PFD

Verdrahtungskategorie	PFH (IEC 61508)	PFD (IEC 61508) Ti = 10 Jahre[47]	PFD (IEC 61508) Ti = 5 Jahre[47]
Kategorie 1	1.10E-06	4.80E-02	4.82E-03
Kategorie 2 – Direktüberwachung	1.10E-06	4.82E-03	5.06E-04
Kategorie 3	4.5E-09	—	1.30E-04
Kategorie 4	2.5E-10	—	2.5E-06

Die architektonischen Anforderungen gemäß IEC 61508-2 Tabelle 3 und EN 62061 Tabelle 5 werden bis zu Stufe SIL 2 erfüllt.

Eine Kategorie 2-Architektur wird zur Erfüllung von architektonischen Auflagen für SIL 2 benötigt (was mit dem Einsatz der direkten Überwachung Spiegel-E/A erreicht wird).

HINWEIS: Die Fehlererkennung und die angegebene Fehlerreaktion müssen erfolgen, bevor die Gefahrensituation, der mit der sicherheitsbezogenen Steuerungsfunktion entgegengewirkt wird, eintreten kann.

47. Testintervall

Zuverlässigkeitsdaten

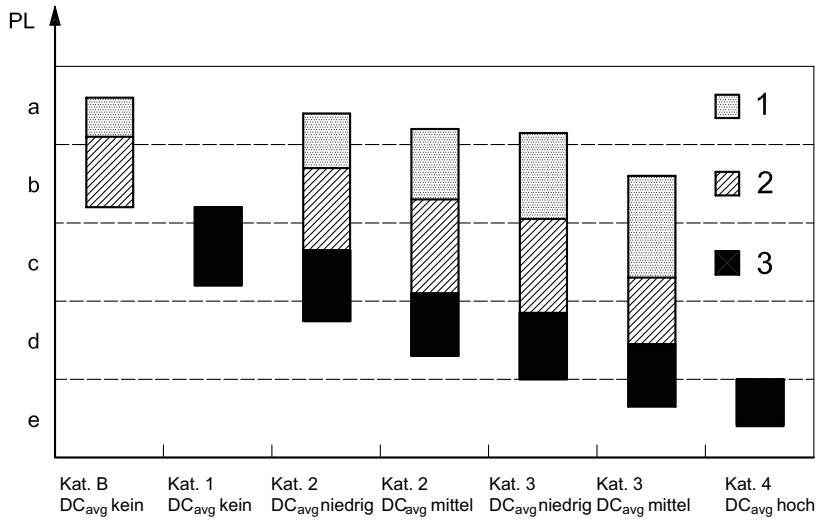
Sicherheitsfunktionsnormenreferenz

Die SIL[48] -Stopp-Funktion hat eine höhere Priorität als ein Stopp, der aus operativen Gründen ausgelöst wurde (EN ISO 13849-1, 5.2.1).

Der Performance-Level hängt von der Verdrahtungskategorie[49], der $MTTF_d$ und dem DC_{avg} ab.

Im folgenden Diagramm wird die Position des TeSys™ island gemäß der jeweiligen Kategorieanforderung gezeigt.

Abbildung 24 - TeSys island-Position gemäß Kategorieanforderung



Legende

PL – Performance Level

1 $MTTF_d$ für jeden Kanal = niedrig

2 $MTTF_d$ für jeden Kanal = mittel

3 $MTTF_d$ für jeden Kanal = hoch

Tabelle 20 - Vereinfachtes Verfahren zur Beurteilung des erreichten PL der sicherheitsbezogenen Teile von Steuerungen (SRP/CS)

Kategorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**Keine**	**Keine**	**Niedrig**	**Mittel**	**Niedrig**	**Mittel**	**Hoch**
$MTTF_d$ für jeden Kanal							
Niedrig	a	Nicht abgedeckt	a	b	b	c	Nicht abgedeckt
Mittel	b	Nicht abgedeckt	b	c	c	d	Nicht abgedeckt
Hoch	Nicht abgedeckt	c	v	d	d	d	e

Gemäß der TeSys island-Architektur und -Verdrahtungskategorie stimmen die Schlüsselindikatoren (DC_{avg}, $MTTF_d$, PL) für TeSys island mit den in der nachstehenden Tabelle aufgeführten Werten überein.

48. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
49. Verdrahtungskategorien gemäß ISO 13849.

Tabelle 21 - Werte der Schlüsselindikatoren für ein- und zweikanalige Architekturen

TeSys island-Systemarchitektur	Kategorie	Einfehlersicherheit[50]	DC_{avg}	$MTTF_d$ für jeden Kanal	Angestrebter PL
Einkanalig	1	Nein	Keine	Hoch (≥ 30 Jahre)	c
	2	Nein	Niedrig (≥ 60 %) bis mittel (≥ 90 %)	Niedrig (≥ 3 Jahre) bis hoch (≥ 30 Jahre)	c, d
Zweikanalig	3	Ja			c, d, e
	4	Ja	Hoch (≥ 99 %)	Hoch (≥ 30 Jahre)	e

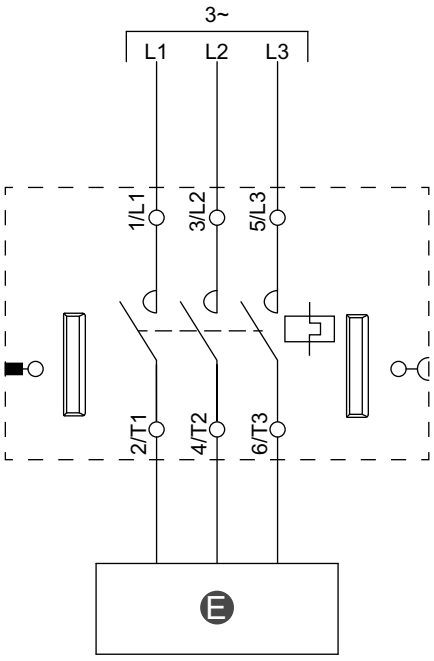
SIL-Avatar-Verdrahtung

Die Schaltpläne in diesem Abschnitt beziehen sich auf die SIL[51]-Avatars. Die folgende Tabelle ist eine Legende für die Diagramme in diesem Abschnitt.

Tabelle 22 - Legende für Schaltpläne

A	Mechanische Verriegelung
B	Parallelbrücke
C	Reversierbrücke
E	Stromkreis

Abbildung 25 - Schalter – SIL-Stopp, Verdrahtungskat. 1/2[52]



50. Einfehlersicherheit bedeutet, dass ein einzelner Fehler (einschließlich Gleichtaktereignisse) nicht zum Verlust der Sicherheitsfunktion führen darf.
51. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
52. Verdrahtungskategorie 1 und 2 gemäß ISO 13849.

Abbildung 26 - Motor – Eine Richtung – SIL-Stopp, Verdrahtungskat. 1/2

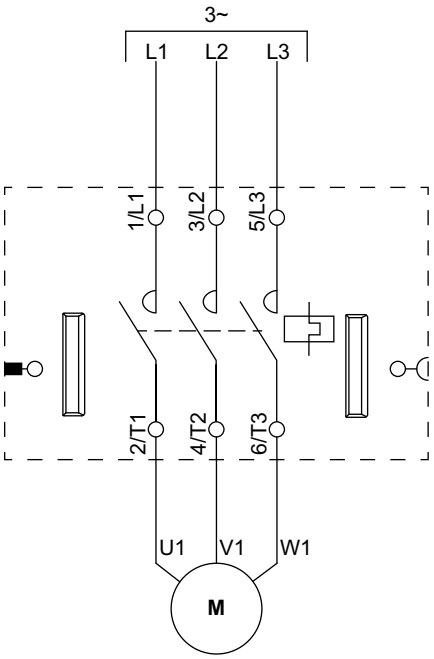


Abbildung 27 - Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2

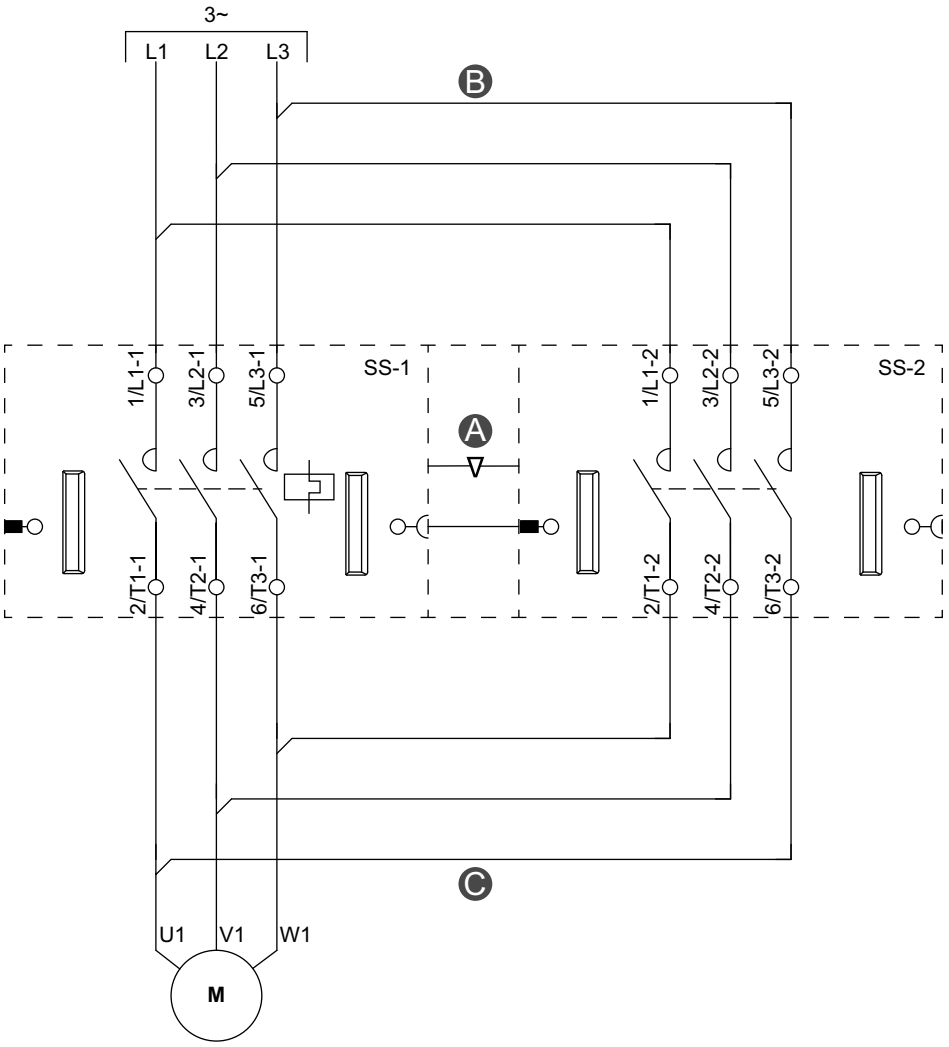


Abbildung 28 - Motor – Zwei Geschwindigkeiten – SIL-Stopp, Verdrahtungskat. 1/2

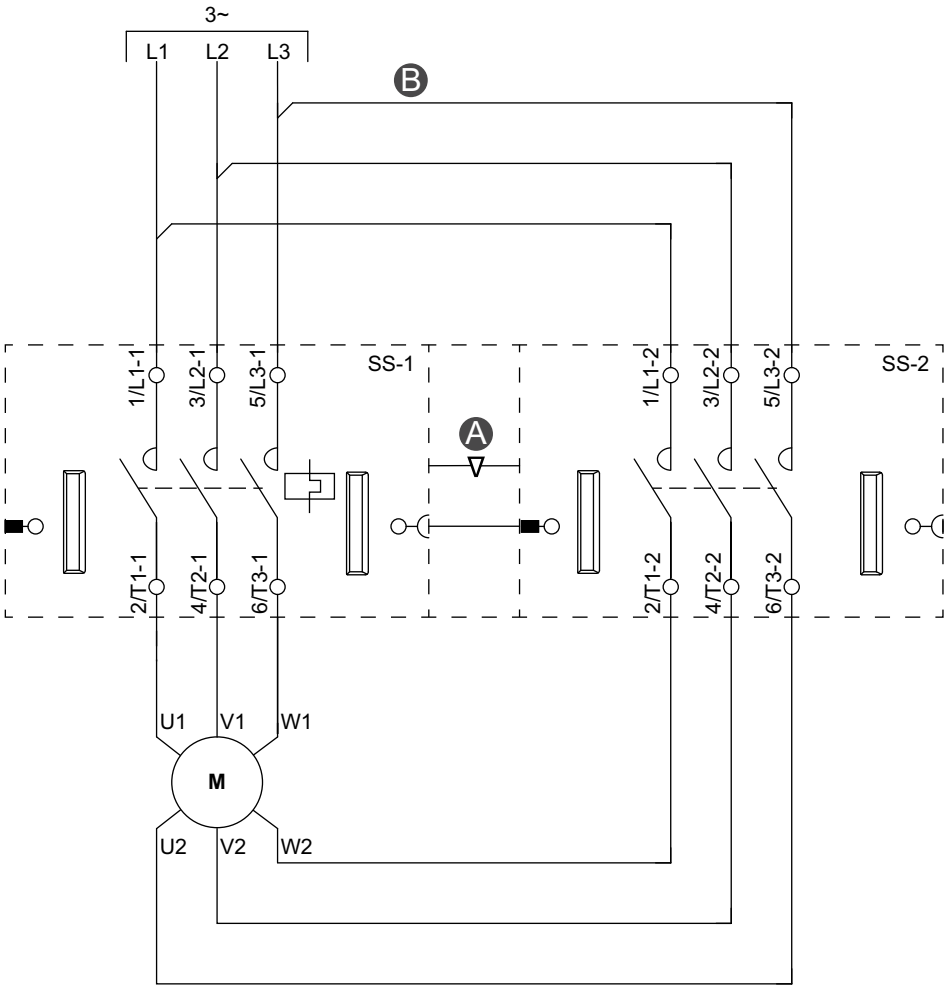


Abbildung 29 - Motor – Zwei Geschwindigkeiten/Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2

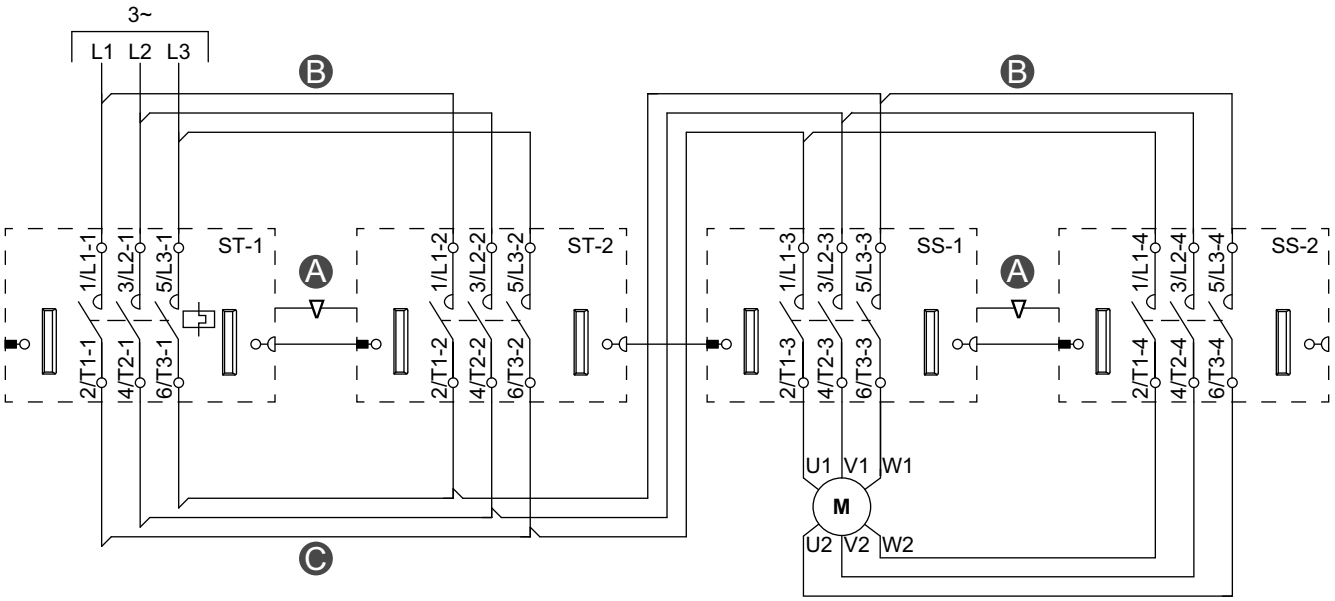


Abbildung 30 - Schalter – SIL-Stopp, Verdrahtungskat. 3/4[53]

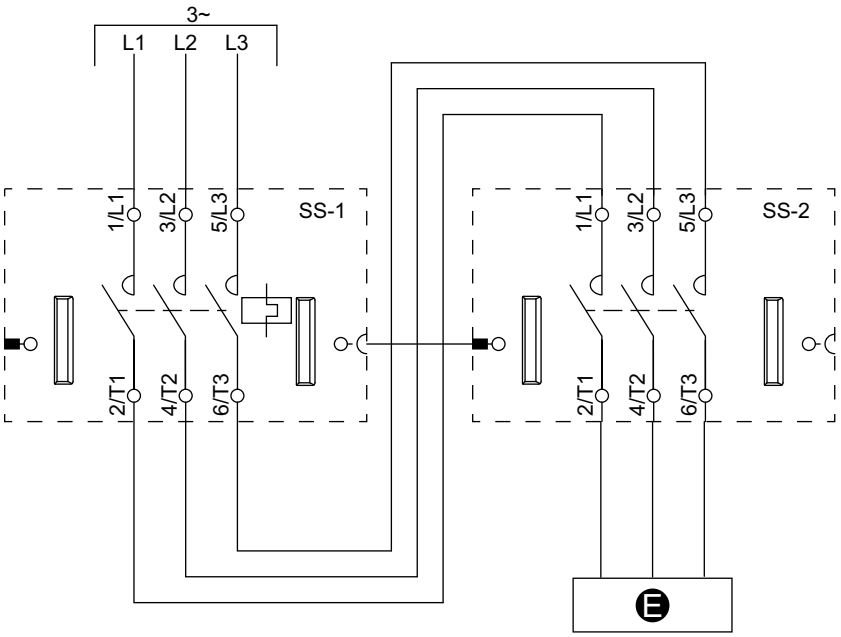
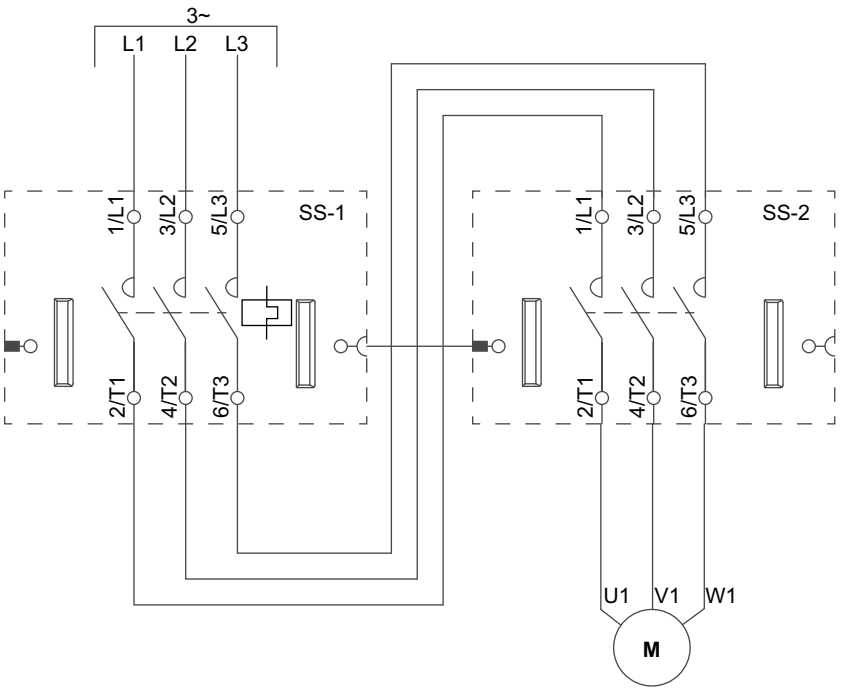


Abbildung 31 - Motor – Eine Richtung – SIL-Stopp, Verdrahtungskat. 3/4



53. Verdrahtungskategorie 3 und 4 gemäß ISO 13849.

Abbildung 32 - Motor – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 3/4

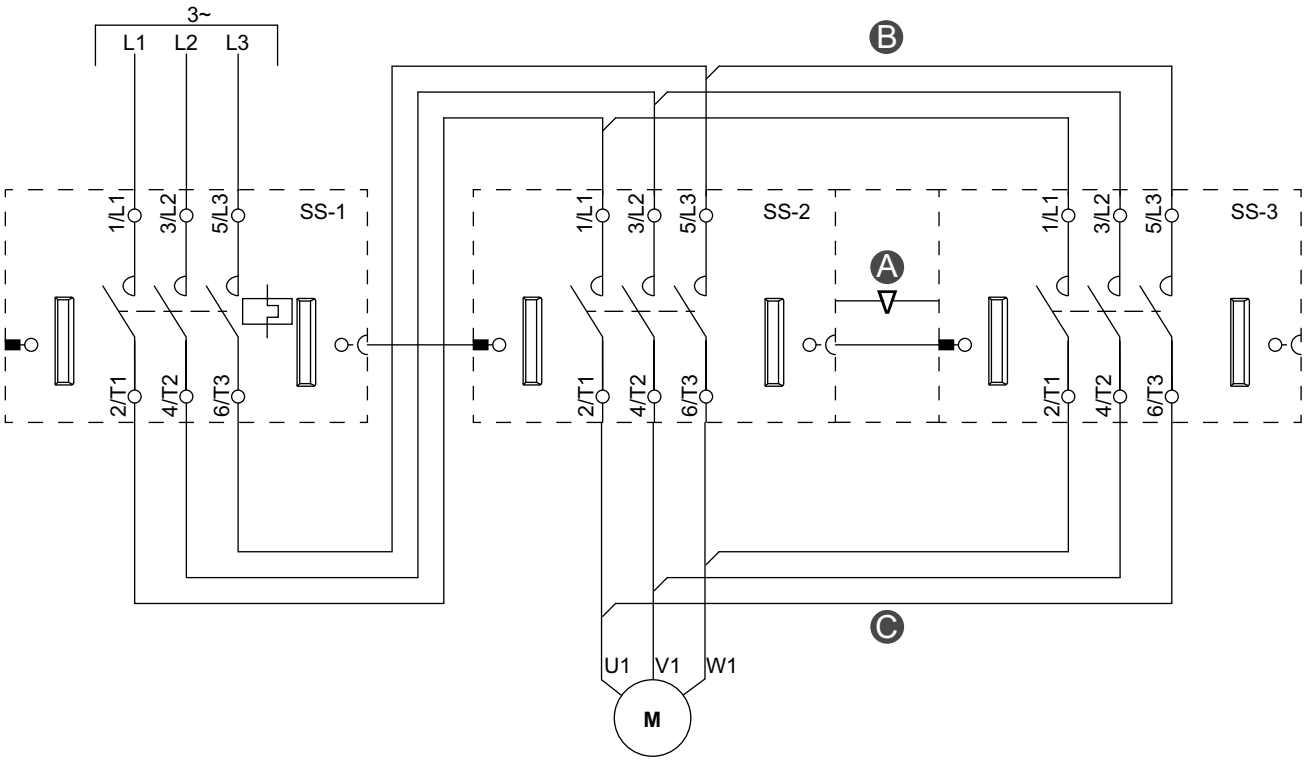


Abbildung 33 - Motor – Zwei Geschwindigkeiten – SIL-Stopp, Verdrahtungskat. 3/4

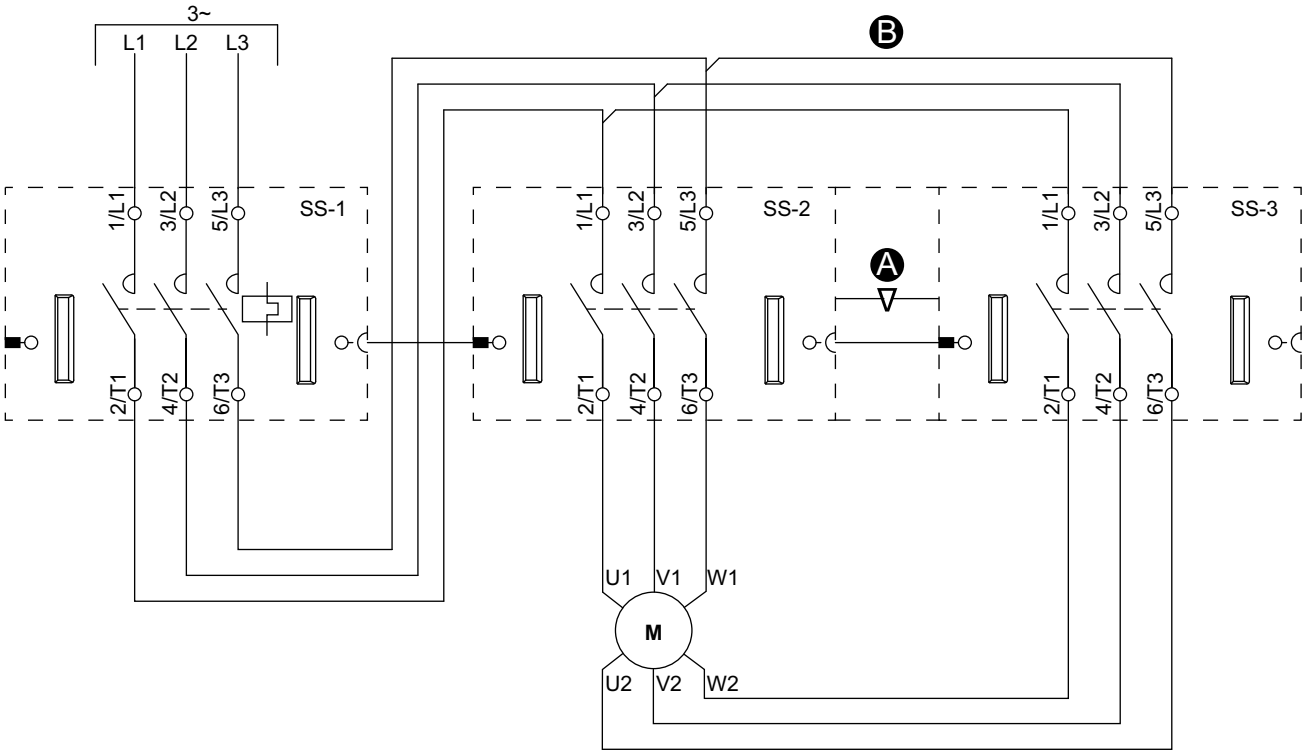


Abbildung 34 - Motor – Zwei Geschwindigkeiten/Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 3/4

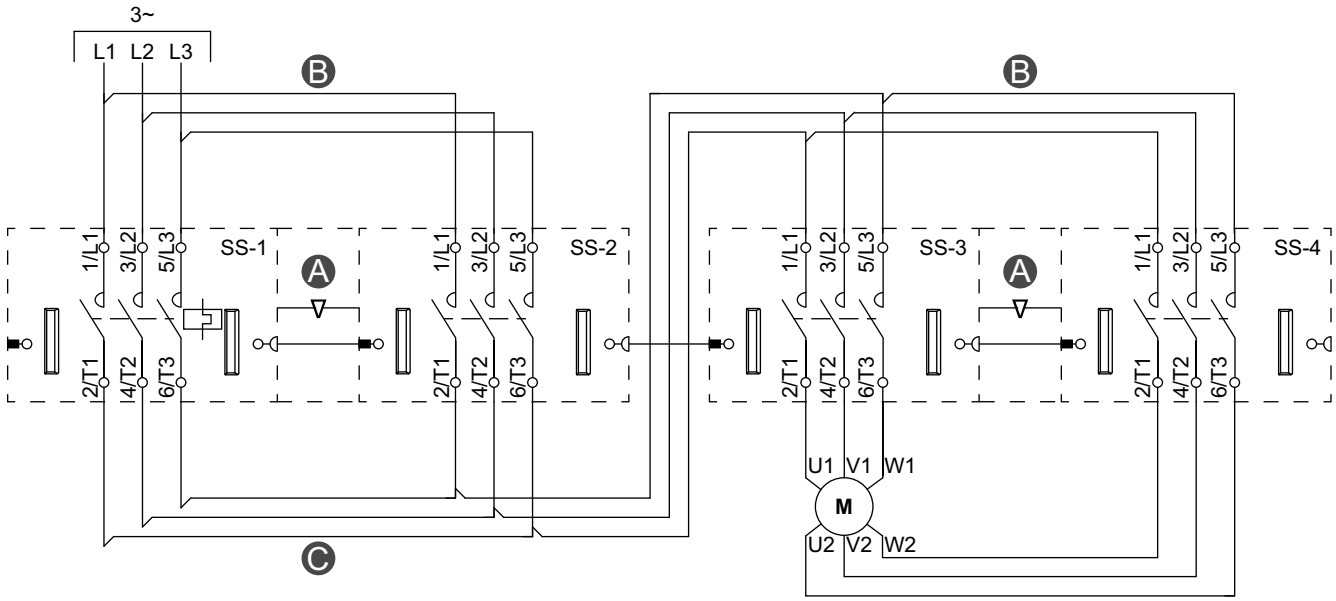


Abbildung 35 - Förderband – Eine Richtung – SIL-Stopp, Verdrahtungskat. 1/2

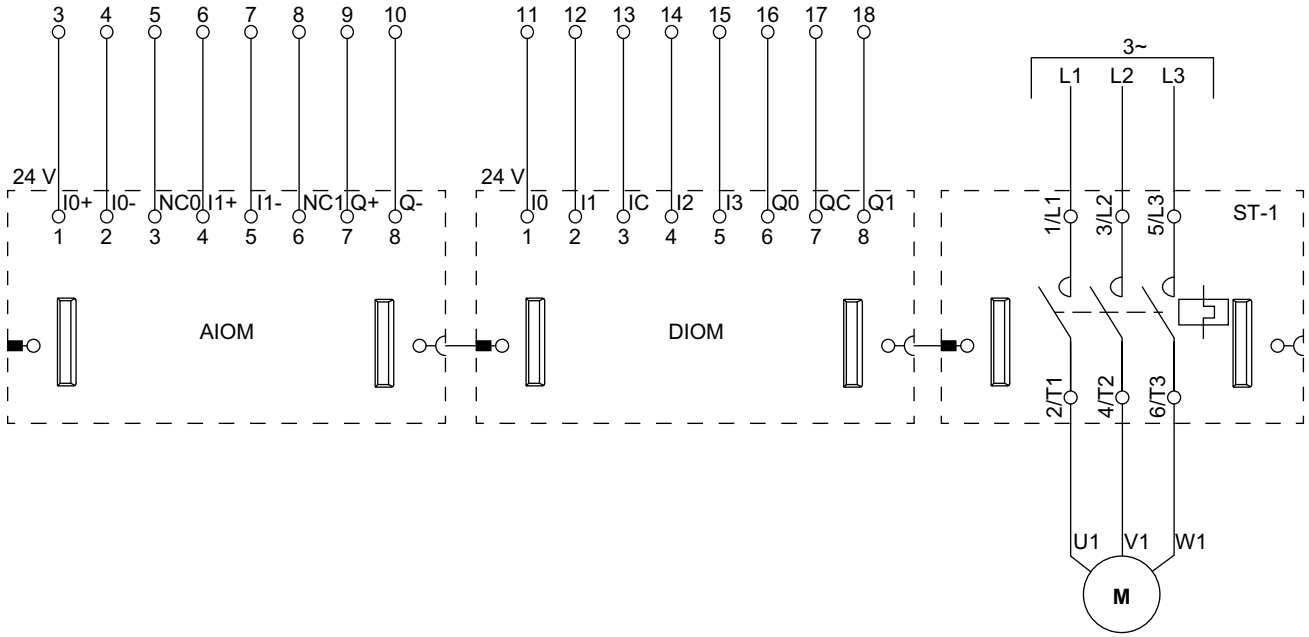
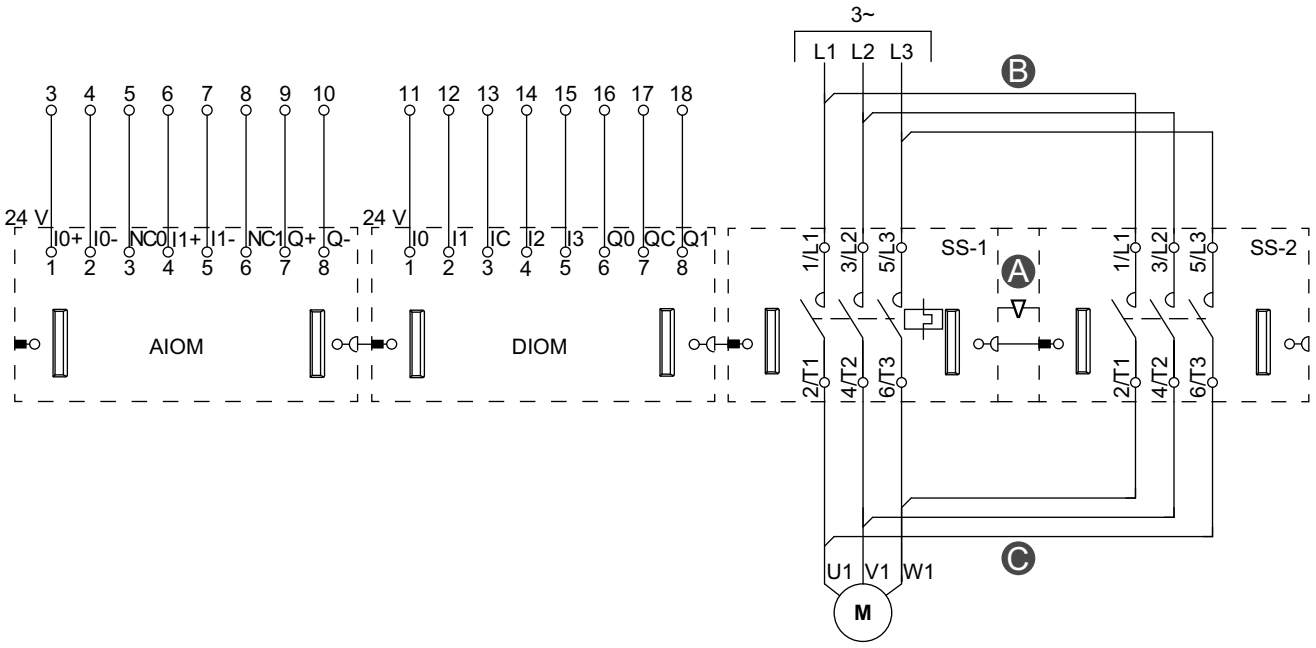


Abbildung 36 - Förderband – Zwei Richtungen – SIL-Stopp, Verdrahtungskat. 1/2



Inbetriebnahme der Sicherheitsfunktion

Verwenden Sie dieses Verfahren, um die Sicherheitsfunktion in Betrieb zu nehmen. Das Verfahren umfasst zwei Schritte:

- Installationstests
- Abnahmeprüfungen der Sicherheitsfunktion[54]

Installationstests

Führen Sie die Schritte in der folgenden Tabelle aus, um die Installation der Sicherheitsfunktion zu überprüfen.

Tabelle 23 - Installationstest

1	Überprüfen Sie im Bereich **DIAGNOSE** des TeSys™ island-DTM, ob die physische Topologie mit der logischen Topologie übereinstimmt.
2	Überprüfen Sie im Bereich **MEIN AVATAR** des TeSys island-DTM, ob unter **AVATAR-PARAMETER** die SIL[55]-Avatars der richtigen SIL-Gruppe zugewiesen wurden.

Abnahmeprüfung der Sicherheitsfunktion

Die Abnahmeprüfung der Sicherheitsfunktion wird für jede SIL[55]-Gruppe auf der Insel durchgeführt. Eine SIL-Gruppe kann mehrere SIL-Avatars umfassen, die von einem SIL-Schnittstellenmodul (SIM) verwaltet werden.

Die Abnahmeprüfung der Sicherheitsfunktion ist erfolgreich, wenn bei Aktivierung der Not-Halt-Einrichtung, die zu einer SIL-Gruppe gehört, alle SIL-Starter dieser SIL-Gruppe in den sicheren Zustand wechseln (die Last wird deaktiviert).

HINWEIS: Bei Stopp-Kategorie 0 (ungesteuertes Stillsetzen) sollte das Stillsetzen unmittelbar erfolgen. Bei Stopp-Kategorie 1 (gesteuertes Stillsetzen) wird das Stillsetzen nach einer Verzögerung wirksam.[56]

Führen Sie die Schritte in der nachstehenden Tabelle für jede SIL-Gruppe auf der Insel aus, um die Abnahmeprüfung der Sicherheitsfunktion durchzuführen.

54. Abnahmeprüfung gemäß IEC 62061
55. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
56. Stopp-Kategorie 0 und 1 gemäß EN/IEC 60204-1.

Tabelle 24 - Abnahmeprüfung der Sicherheitsfunktion

1	Aktivieren Sie die Not-Halt-Einrichtung, die zu der SIL-Gruppe gehört, und überprüfen Sie, ob alle SIL-Starter dieser SIL-Gruppe in den sicheren Zustand wechseln (die Last wird deaktiviert). **HINWEIS:** Die Gerätestatus-LED (DS) an den SIL-Startern blinkt rot als Hinweis auf ein geringfügiges Geräteereignis. Bei nicht bestandener Prüfung: • Die Not-Halt-Einrichtung ist möglicherweise mit dem falschen SIM verbunden. Überprüfen Sie diese Verbindungen. • Die Not-Halt-Einrichtung ist möglicherweise nicht korrekt mit dem SIM verdrahtet. Überprüfen Sie diese Verbindungen. • Einige SIL-Avatars wurden möglicherweise nicht der erwarteten SIL-Gruppe zugewiesen. Überprüfen Sie die Konfiguration.
2	Kontrollieren Sie den **STATUS** und die **EREIGNISPROTOKOLLE** im Bereich **AVATARS** des Abschnitts **DIAGNOSE** im TeSys™ island-DTM oder -OMT, um zu überprüfen, ob der Wert für **SIL-Gruppenstatus** gleich **Stopp-Befehl** ist. Der Eintrag im Ereignisprotokoll lautet „SIL Group Stop cmd, Safe State achieved“ (SIL-Gruppen-Stopp-Befehl, sicherer Zustand erreicht). Bei nicht bestandener Prüfung: • Einige SIL-Avatars wurden möglicherweise nicht der erwarteten SIL-Gruppe zugewiesen. Überprüfen Sie die Konfiguration.
3	Überprüfen Sie im Abschnitt **GERÄTE** des Bereichs **DIAGNOSE**, ob der Wert für **SIL-Schnittstellenmodul-Status (SIM)** gleich **Stopp-Befehl** ist. Der Eintrag im Ereignisprotokoll lautet „SIL Group Stop cmd, Safe State achieved“ (SIL-Gruppen-Stopp-Befehl, sicherer Zustand erreicht). Bei nicht bestandener Prüfung: • Die Not-Halt-Einrichtung ist möglicherweise mit dem falschen SIM verbunden. Überprüfen Sie diese Verbindungen. • Die Not-Halt-Einrichtung ist möglicherweise nicht korrekt mit dem SIM verdrahtet. Überprüfen Sie diese Verbindungen.
4	Geben Sie einen Start-Befehl an einen SIL-Avatar der SIL-Gruppe aus und überprüfen Sie, ob der Start fehlschlägt. Die Starter müssen offen bleiben und der Start-Befehl muss ignoriert werden, bis die Not-Halt-Einrichtung zurückgesetzt wurde. Bei nicht bestandener Prüfung: • Einige SIL-Avatars wurden möglicherweise nicht der erwarteten SIL-Gruppe zugewiesen. Überprüfen Sie die Konfiguration. Wenn einer dieser Tests trotz korrektiver Maßnahmen fortlaufend fehlschlägt, dürfen Sie die Insel nicht weiter nutzen. Tauschen Sie die Geräte, die die Tests nicht bestehen, aus.
5	Wenn die Abnahmeprüfung der Sicherheitsfunktion abgeschlossen ist, setzen Sie die Not-Halt-Einrichtung zurück und überprüfen Sie, ob sich alle SIL-Starter und SIL-Schnittstellenmodule im Bereit-Zustand befinden (die DS-LED zeigt grünes Dauerlicht).

Wartungsanforderungen der Sicherheitsfunktion

In diesem Abschnitt werden die Routine-Wartungsarbeiten beschrieben, die für die Aufrechterhaltung der funktionalen Sicherheit Ihres TeSys™ island erforderlich sind.

Wartungsplan

Die Wartungsintervalle sind vom Schalthäufigkeitsmodus abhängig.

- Führen Sie für den Modus mit geringer Schalthäufigkeit (der Jahresdurchschnitt der Schützzyklen ist kleiner als 15 Schaltspiele/Stunde) alle 12 Monate Wartungsarbeiten durch.
- Führen Sie für den Modus mit hoher Schalthäufigkeit (der Jahresdurchschnitt der Schützzyklen ist größer als 15 Schaltspiele/Stunde oder 136.986 Schaltspiele/Jahr) Wartungsarbeiten in Intervallen durch, die 1/10 der geschätzten Gerätelebensdauer betragen.

Die geschätzte Lebensdauer (Jahre) = B10d (= 1.369.863) / Jahresdurchschnitt der Schützzyklen

Wartungskontrollen

Gerätenutzungskontrollen

Führen Sie die in der nachstehenden Tabelle aufgeführten Kontrollen durch, um zu überprüfen, ob sich die SIL[57]-Starter-Schützzyklen innerhalb zulässiger Lebensdauerwerte befinden.

1	Verwenden Sie die Gerätefunktion **DIAGNOSE** des TeSys™ island-DTM oder OMT, um die Geräte-Asset-Daten für jeden SIL-Starter abzurufen.
2	Wenn der Wert **Anzahl Schützzyklen** größer als B10d (= 1.369.863) ist, dann tauschen Sie den SIL-Starter aus.
3	Ist das nicht der Fall, dann verwenden Sie den Wert **Anzahl Schützzyklen**, um die nächste Wartung zu planen. Siehe Wartungsplan, Seite 68.

Abnahmeprüfung der Sicherheitsfunktion

Führen Sie die Abnahmeprüfung der Sicherheitsfunktion für jede SIL[57] -Gruppe durch. Siehe Abnahmeprüfung der Sicherheitsfunktion, Seite 66.

57. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.

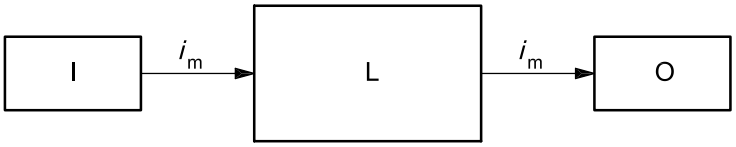
Anhang: Einkanalige Architektur

Diese einkanalige Architektur umfasst die Verdrahtungskategorien 1 und 2.

Architektonische Anforderungen der Verdrahtungskategorie 1

Die vorgesehene Architektur für **Kategorie 1** ist in EN ISO 13849-1, 6.2.4 definiert.

Abbildung 37 - Vorgesehene Architektur für Kategorie 1 (EN ISO 13849-1)



I: Eingabegerät

L: Logik

O: Ausgabegerät

^{i}**m**: Verbindungseinrichtung

Die SRP/CS (die sicherheitsbezogenen Teile der Steuerung) für Verdrahtungskategorie 1 müssen mit **bewährten Komponenten** konzipiert und konstruiert werden.

Eine „bewährte Komponente” für eine sicherheitsbezogene Anwendung ist eine Komponente, auf die eine der folgenden Aussagen zutrifft:

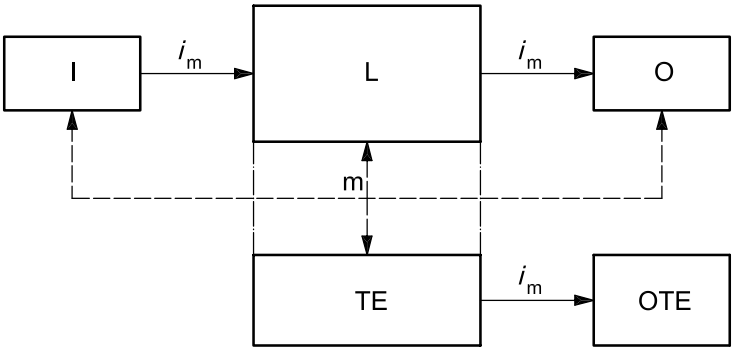
- Sie wurde in der Vergangenheit mit guten Ergebnissen in ähnlichen Anwendungen eingesetzt oder
- Sie wurde anhand von Grundsätzen gefertigt und geprüft, die ihre Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen belegen

Es gibt **keinen Diagnosedeckungsgrad** (DC_{avg} = keiner) in Kategorie 1-Systemen.

Architektonische Anforderungen der Verdrahtungskategorie 2

Die vorgesehene Architektur für **Kategorie 2** ist in EN ISO 13849-1, 6.2.5 definiert.

Abbildung 38 - Vorgesehene Architektur für Kategorie 2 (EN ISO 13849-1)



I: Eingabegerät

L: Logik

O: Ausgabegerät

^{i}**m**: Verbindungseinrichtung

m: Überwachung

TE: Prüfvorrichtung

OTE: Ausgabe an TE

Die SRP/CS (die sicherheitsbezogenen Teile der Steuerung) für Verdrahtungskategorie 2 müssen so konzipiert sein, dass ihre Funktionen in geeigneten Intervallen von der Maschinensteuerung kontrolliert werden.

In einer einkanaligen Architektur ist ein SIM mit einem SIL[58]-Starter verknüpft.

Speziell für Verdrahtungskategorie 2 ist der Spiegelkontakt an das Preventa™ XPS-Modul (oder Entsprechung) angeschlossen. Wenn der Zustand der Spiegelkontakt-Rückkopplungsleitung nicht dem Ausgangszustand des Preventa XPS-Moduls (oder Entsprechung) entspricht, blockiert das Preventa XPS-Modul (oder Entsprechung) einen zweiten Start.

HINWEIS: Die Spiegelkontakt-Rückkopplung übermittelt ausschließlich Diagnoseinformationen.

58. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.

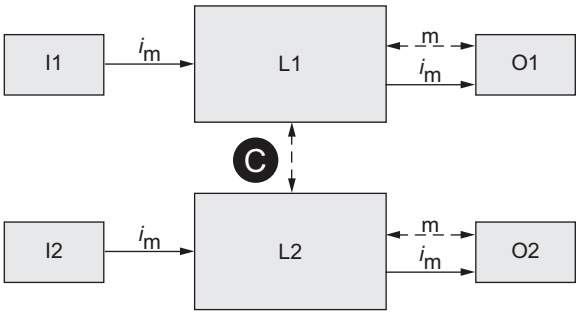
Anhang: Zweikanalige Architektur

Diese zweikanalige Architektur umfasst die Verdrahtungskategorien 3 und 4.

Architektonische Anforderungen der Verdrahtungskategorie 3

Die für Kategorie 3 vorgesehene Architektur ist in EN ISO 13849-1, 6.2.6 definiert.

Abbildung 39 - Vorgesehene Architektur für Kategorie 3 (EN ISO 13849-1)



im: Verbindungseinrichtung

c: Querschlusserkennung

I1, I2: Eingabegerät, z. B. Sensor

L1, L2: Logik

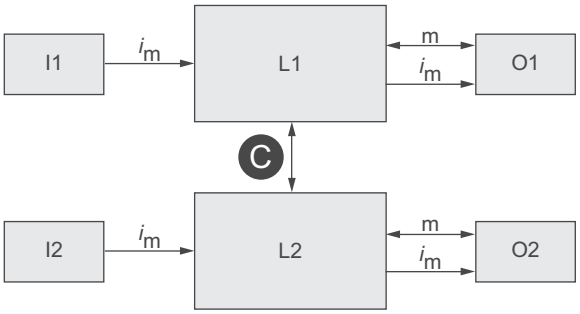
m: Überwachung

O1, O2: Ausgabegerät, z. B. Hauptschütz

Architektonische Anforderungen der Verdrahtungskategorie 4

Die für Kategorie 4 vorgesehene Architektur ist in EN ISO 13849-1, 6.2.7 definiert.

Abbildung 40 - Vorgesehene Architektur für Kategorie 4 (EN ISO 13849-1)



im: Verbindungseinrichtung

c: Querschlusserkennung

I1, I2: Eingabegerät, z. B. Sensor

L1, L2: Logik

m: Überwachung

O1, O2: Ausgabegerät, z. B. Hauptschütz

Durchgezogene Linien bei der Überwachung stellen einen Diagnosedeckungsgrad dar, der höher ist als in der für Kategorie 3 vorgesehenen Architektur.

Glossar

A

Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls [h^{-1}] (PFH). (Gefährliche Ausfälle gemäß der Norm IEC 61508-4)

Um die Sicherheitsfunktion aufrechtzuerhalten, erfordert die Norm IEC 61508 Maßnahmen auf verschiedenen Ebenen zur Vermeidung und Steuerung erkannter Fehler – je nach erforderlichem SIL[59]-Wert.

Alle Komponenten einer Sicherheitsfunktion müssen einer Wahrscheinlichkeitseinschätzung unterzogen werden, um die Wirksamkeit der für die Steuerung von erkannten Fehlern implementierten Maßnahmen zu beurteilen.

Mit dieser Beurteilung wird der PFH-Wert (durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls[60] [h^{-1}]) für ein sicherheitsbezogenes System bestimmt. Das ist die Wahrscheinlichkeit bezogen auf eine Stunde, dass ein sicherheitsbezogenes System auf gefährliche Weise ausfällt und die Sicherheitsfunktion nicht korrekt ausgeführt werden kann.

Je nach SIL darf der PFH bestimmte Werte für das gesamte sicherheitsbezogene System nicht überschreiten.

Die einzelnen PFH-Werte in einer Funktionskette werden addiert. Das Ergebnis darf den in der Norm angegebenen Höchstwert nicht überschreiten.

Sicherheitsanforderungsstufe	**Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls[60] [h^{-1}] (PFH) bei hoher Anforderungsrate oder kontinuierlicher Anforderung**
4	$10^{-9} \leq — < 10^{-8}$
3	$10^{-8} \leq — < 10^{-7}$
2	$10^{-7} \leq — < 10^{-6}$
1	$10^{-6} \leq — < 10^{-5}$

E

EN ISO 13849 (Norm)

In dieser europäischen Norm ist das Validierungsverfahren, einschließlich Gefahrenanalyse, Risikobeurteilung und Prüfung, für die Sicherheitsfunktionen und -kategorien der sicherheitsbezogenen Teile von Steuerungen festgelegt. Die Beschreibungen der Sicherheitsfunktionen sowie die Anforderungen der Kategorien sind in ISO 13849-1 aufgeführt, die die allgemeinen Gestaltungsleitsätze abdeckt. Einige der Validierungsanforderungen sind allgemeiner Natur und andere abhängig von der verwendeten Technologie. In EN ISO 13849-2 sind auch die Bedingungen festgelegt, unter welchen die Validierung beim Prüfen der sicherheitsbezogenen Teile von Steuerungen durchgeführt werden sollte.

EN/IEC 60204-1 (Norm)

Die Stopp-Kategorie 0 wird definiert als „Stillsetzen durch sofortiges Unterbrechen der Energiezufuhr zu den Maschinen-Antriebselementen (d. h. ein ungesteuertes Stillsetzen)“.

59. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.
60. Gefährliche Ausfälle gemäß der Norm IEC 61508-4

Die Stopp-Kategorie 1 ist definiert als „gesteuertes Stillsetzen, wobei die Energiezufuhr zu den Maschinen-Antriebselementen beibehalten wird, um das Stillsetzen zu erzielen. Die Energiezufuhr wird erst dann unterbrochen, wenn der Stillstand erreicht ist“.

F

Fehlervermeidende Maßnahmen

Systematische Fehler in den Spezifikationen sowie in der Hardware und in der Software, Anwenderfehler und Wartungsfehler im sicherheitsbezogenen System müssen im größtmöglichen Umfang vermieden werden. Für die Erfüllung dieser Anforderungen ist in der Norm IEC 61508 eine Reihe von Maßnahmen zur Fehlervermeidung aufgeführt, die in Abhängigkeit des erforderlichen SIL[61]-Werts implementiert werden müssen. Diese fehlervermeidenden Maßnahmen müssen den gesamten Lebenszyklus des sicherheitsbezogenen Systems abdecken, d. h. vom Entwurf bis zur Außerbetriebnahme des Systems.

Funktionssicherheit

Automatisierungs- und Funktionssicherheitstechnik sind zwei Bereiche, die in der Vergangenheit vollkommen voneinander getrennt waren, in letzter Zeit aber immer enger miteinander verknüpft werden.

Entwicklung und Installation von komplexen Automatisierungslösungen werden durch die Integration von Sicherheitsfunktionen vereinfacht.

Die technischen Anforderungen an die funktionale Sicherheit sind normalerweise von der Anwendung abhängig.

Das Anforderungsniveau ergibt sich aus dem Risiko- und Gefahrenpotenzial, das die jeweilige Anwendung mit sich bringt.

H

Hardware-Fehlertoleranz (HFT) und Anteil ungefährlicher Ausfälle (SFF)

Je nach SIL[61]-Wert des sicherheitsbezogenen Systems ist gemäß Norm IEC 61508 ein bestimmter HFT-Wert (Hardware-Fehlertoleranz) in Verbindung mit einem bestimmten Prozentsatz von ungefährlichen Ausfällen, bekannt als SFF-Wert (Anteil ungefährlicher Ausfälle), erforderlich.

Der HFT-Wert beschreibt die Fähigkeit eines Systems, die erforderliche Sicherheitsfunktion trotz der Gegenwart von einem oder mehreren Hardware-Fehlern auszuführen.

Der SFF-Wert eines Systems ist definiert als der Anteil der ungefährlichen Ausfälle im Verhältnis zu den Gesamtausfällen des Systems.

Gemäß IEC 61508 wird der maximal erreichbare SIL-Wert eines Systems zum Teil vom HFT- und SFF-Wert des Systems bestimmt.

Diese Typen werden auf der Grundlage von Kriterien spezifiziert, die in der Norm für die sicherheitsbezogenen Elemente definiert sind.

SFF	**HFT für Untersystem Typ A**			**HFT für Untersystem Typ B**		
	0	1	2	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3	—	SIL 1	SIL 2
60 % – < 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3

61. Sicherheitsanforderungsstufe gemäß der Norm IEC 61508.

SFF	HFT für Untersystem Typ A			HFT für Untersystem Typ B		
90% – < 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

I

IEC 61508 (Norm)

Die Norm IEC 61508 beschreibt die funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme.

Anstelle einer einzelnen Komponente wird eine ganze Funktionskette (z. B. von einem Sensor über die logischen Verarbeitungseinheiten bis zum Stellglied) als Einheit betrachtet.

Diese Funktionskette muss die Anforderungen der jeweiligen Sicherheitsanforderungsstufe in ihrer Gesamtheit erfüllen.

L

Niedrige/Hohe Anforderungsrate

IEC 61508 beschreibt die Anforderungsrate von Sicherheitsfunktionen:

- Hohe Anforderungsrate oder kontinuierliche Anforderung (PFH)
- Niedrige Anforderungsrate (PFDavg, PTI)

M

Mittlere Zeit bis zu einem gefährlichen Ausfall ($MTTF_d$)

Nach Norm ISO 13849-1 wird die $MTTF_d$ als die erwartete mittlere Zeit bis zu einem gefährlichen Ausfall definiert.

P

Performance-Level (PL)

In der Norm IEC 13849-1 sind fünf Performance-Levels (PL) für Sicherheitsfunktionen festgelegt.

„Level a“ ist der niedrigste Level und „e“ ist der höchste.

Fünf Levels (a, b, c, d und e) entsprechen verschiedenen Werten der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls[62] pro Stunde.

Performance-Level	Wahrscheinlichkeit eines gefährlichen Ausfalls[62] pro Stunde
e	≥ 10^{-8} bis < 10^{-7}
d	≥ 10^{-7} bis < 10^{-6}
c	≥ 10^{-6} bis < 3 x 10^{-6}
b	≥ 3 x 10^{-6} bis < 10^{-5}
a	≥ 10^{-5} bis < 10^{-4}

62. Gefährliche Ausfälle gemäß der Norm IEC 61508-4

S

Sicherheitsanforderungsstufe (SIL)

In der Norm IEC 61508 sind vier Sicherheitsanforderungsstufen (SIL) für Sicherheitsfunktionen festgelegt.

SIL 1 ist die niedrigste Integritätsstufe und SIL 4 die höchste.

Eine Gefahrenanalyse und Risikobeurteilung dienen als Grundlage für die Bestimmung der erforderlichen Sicherheitsanforderungsstufe.

Diese wird verwendet, um zu entscheiden, ob die relevante Funktionskette als Sicherheitsfunktion gilt und welches Gefahrenpotenzial sie abdecken muss.

Schneider Electric
800 Federal Street
01810 Andover, MA
USA

https://www.schneider-electric.com/en/work/support/

www.schneider-electric.com

Da Normen, Spezifikationen und Bauweisen sich von Zeit zu Zeit ändern, sollten Sie um Bestätigung der in dieser Veröffentlichung gegebenen Informationen nachsuchen.

8536IB1904DE-04