SIEMENS

FAQ-04NNGJJ9 • April/2015

Safety Integrity Level (SIL) 3 gemäß EN 62061

SINAMICS S110 / S120, Safety Integrated

https://support.industry.siemens.com/cs/ww/de/view/48336710

Dieser Beitrag stammt aus dem Siemens Industry Online Support. Es gelten die dort genannten Nutzungsbedingungen (www.siemens.com/nutzungsbedingungen).

Security-hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Lösungen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Komponenten in einem ganzheitlichen Industrial Security-Konzept. Die Produkte und Lösungen von Siemens werden unter diesem Gesichtspunkt ständig weiterentwickelt. Siemens empfiehlt, sich unbedingt regelmäßig über Produkt-Updates zu informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Um stets über Produkt-Updates informiert zu sein, melden Sie sich für unseren produktspezifischen Newsletter an. Weitere Informationen hierzu finden Sie unter http://support.industry.siemens.com.

Inhaltsverzeichnis

1 Aufgabenstellung

Die Sicherheitsfunktionen des SINAMICS G120/S110/120 erfüllen im Standard den Safety Integrity Level (SIL) 2. Um auch Anwendungen abdecken zu können, die für die Funktion „Sicheres Abschalten“ (Sicherheitsfunktionen STO bzw. SS1) SIL 3 benötigen, wird in diesem Dokument der Nachweis gemäß IEC 62061 geführt, dass mit einem zusätzlichen Leistungsschütz SIL 3 erreicht werden kann.

2 Beschreibung der Sicherheitsfunktion

Eine Sicherheitsfunktion besteht in der Regel aus den Teilfunktionen „Erfassen“, „Auswerten“ und „Reagieren“. Zu „Erfassen“ gehören die Sicherheitssensoren wie NOT-HALT-Taster, Positionsschalter oder Lichtvorhänge, zu „Auswerten“ gehören Sicherheitsschaltgeräte oder Sicherheitssteuerungen, und zu „Reagieren“ gehören die Sicherheitsaktoren wie Schütze oder Antriebe mit integrierten Sicherheitsfunktionen.

Im Folgenden wird zunächst die Funktionsweise anhand zweier Varianten beschrieben. Dabei liegt der Schwerpunkt auf der Teilfunktion „Reagieren“. Auf die Teilfunktion „Auswerten“ wird nur kurz eingegangen, weil von dort die Sicherheitsfunktionen im Aktor angesteuert werden und die Diagnose erfolgt. Auf die erforderliche Sensorik wird nicht weiter eingegangen.

Das Sicherheitssystem besteht im Folgenden aus dem Teilsystem Sicherheitssteuerung (F-CPU) mit zugehöriger Peripherie und dem Teilsystem Aktor, realisiert mit einem Leistungsschütz und dem Antriebssystemen SINAMICS G120/S110/120 mit integrierten Sicherheitsfunktionen.

2.1 Funktionsweise

Von der Sicherheitssteuerung wird – z. B. nach Ansprechen eines Sicherheitssensors (in den folgenden Abbildungen nicht dargestellt) – der Antrieb stillgesetzt. Hierzu wird über einen sicheren Ausgang der fehlersicheren Peripherie am SINAMICS G120/S110/120 die antriebsintegrierte Sicherheitsfunktion Safe Torque Off (STO), ggf. mit vorangehender Schnellbremsfunktion (SS1), ausgelöst. Ein Rücklesen der Zustandsrückmeldung in die Sicherheitssteuerung ist nicht erforderlich, weil die Diagnose intern realisiert ist (kreuzweiser Datenvergleich der beiden Abschaltpfade und bei Aufdecken eines Fehlers Einleiten einer Fehlerreaktion, die in den sicheren Zustand führt). Allerdings ist eine regelmäßige Zwangsdynamisierung (z. B. alle 8 Stunden) durch Anwahl der Funktion erforderlich.

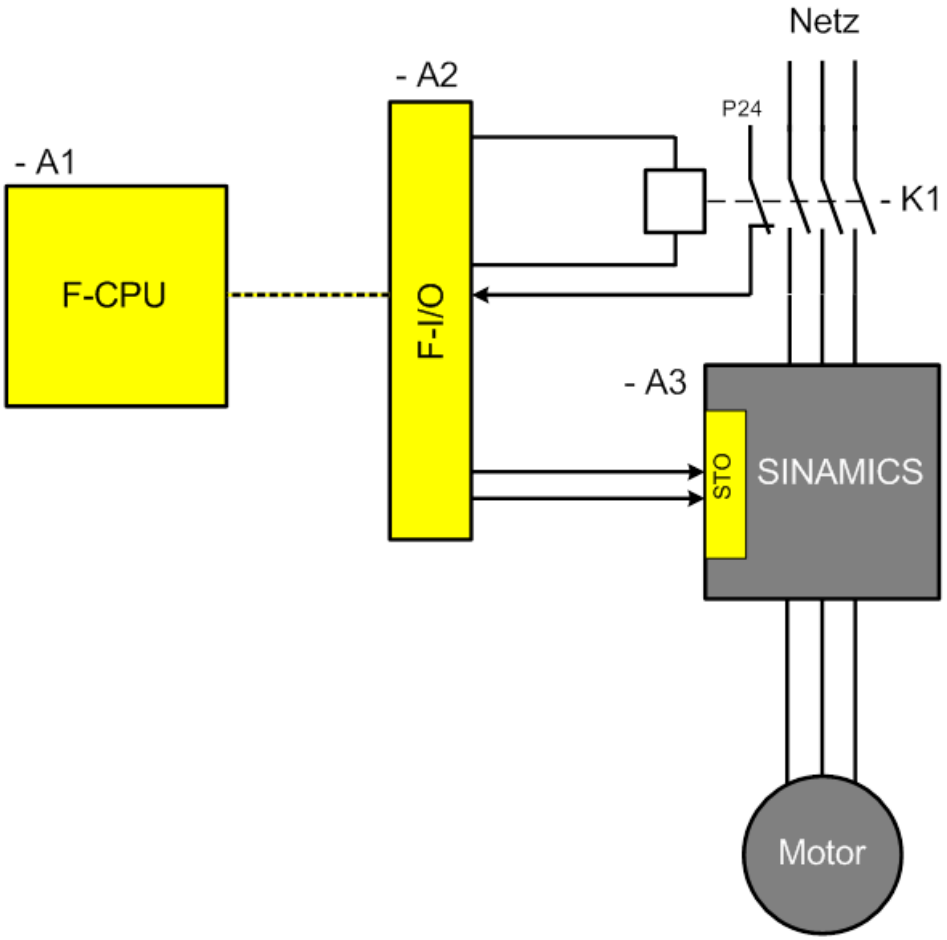
Als zweiter unabhängiger Abschaltkanal wird ein Leistungsschütz zusätzlich zum SINAMICS G120/S110/120 vorgesehen. Dessen zwangsgeführter Hilfskontakt (Öffner) wird in die Peripheriebaugruppe zurück gelesen. Hierfür muss kein sicherer Eingang verwendet werden, allerdings ist auch hier eine regelmäßige Zwangsdynamisierung erforderlich. Um Fehler im zweiten Kanal zu erkennen, kontrolliert die F-Steuerung, ob nach An- und Abwahl der Sicherheitsfunktion die Rückmeldung korrekte Pegel annimmt. Ist das nicht der Fall, muss eine Fehlerreaktion eingeleitet werden, die in einen sicheren Zustand führt. Diese Funktionalität ist im Sicherheitsprogramm der Steuerung in geeigneter Weise zu implementieren.

Mit Aktivieren von STO am SINAMICS G120/S110/120 wird eine Impulssperre im motorseitigen Wechselrichter ausgelöst und damit der Strom unmittelbar elektronisch abgeschaltet. Damit das Schütz stromlos und damit mit weniger Verschleiß schaltet, ist es sinnvoll, dass die Sicherheitssteuerung die Abschaltung des Schützes kurz verzögert. Allerdings muss das Schütz als zweiter unabhängiger Abschaltpfad bei Versagen des ersten Kanals den Laststrom schalten können und ist daher entsprechend auszulegen. Die Verzögerungszeit des Schützes ist bei der Ermittlung der Reaktionszeit der Sicherheitsfunktion zu berücksichtigen.

2.2 Variante 1: Leistungsschütz in der Netzeinspeisung des Umrichters

In der Variante 1 ist das Leistungsschütz in der Netzseite eines SINAMICS G120 bzw. eines SINAMICS S110/S120 Power Module vorgesehen (siehe Abb. 2-1). Diese Variante hat die im Folgenden aufgeführten Eigenschaften:

Abbildung 2-1



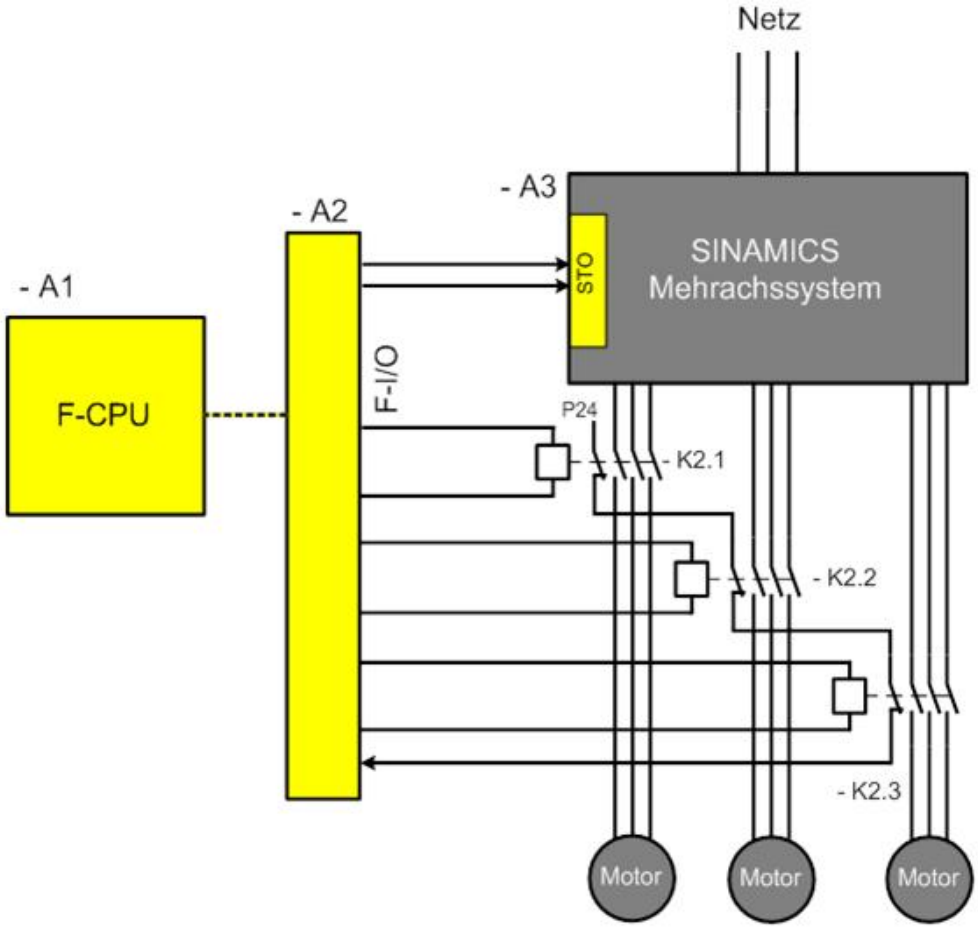
Eigenschaften:

- Das Schütz kann für ohmsche Last (AC1) ausgelegt werden.
- Durch die im Spannungszwischenkreis gespeicherte Energie kann auch nach Abschalten des Netzschützes bei Versagen der antriebsintegrierten Sicherheitsfunktion noch eine Restbewegung stattfinden. Das muss bei der Risikobewertung berücksichtigt werden.
- Das Schütz muss für den thermischen Dauerstrom des Antriebs bzw. der Antriebe ausgelegt werden.
- Nach dem Abschalten werden die Zwischenkreiskondensatoren entladen. Daher muss vor dem Wiedereinschalten des Antriebs die Vorladezeit des Umrichters abgewartet werden.
- Diese Variante ist in der Regel nur für Einzelantriebe geeignet. Bei einem Mehrmotorenantrieb mit gemeinsamer Einspeisung würde mit dem netzseitigen Schütz die Energieversorgung aller angeschlossen Antriebe gemeinsam abgeschaltet werden.

2.3 Variante 2: Leistungsschütz auf der Ausgangsseite zwischen Motor und Umrichter

Die Variante 2 beschreibt einen SINAMICS S120 Mehrachsverband mit ausgangsseitigen Schützen (siehe Abb. 2-2). Diese Variante hat folgende Eigenschaften:

Abbildung 2-2



Eigenschaften:

- Für Einzel- und Mehrmotorenkonstellationen geeignet, da jeder Motor einzeln abgeschaltet werden kann.
- Der Zwischenkreis bleibt am Netz und damit vorgeladen, d. h. keine thermische Belastung der beteiligten Bauelemente und kein Zeitverzug beim Wiedereinschalten.
- Das Schütz muss im Worst Case einen Gleichstrom mit induktiver Last (Motorwicklung) schalten können (bei sehr kleiner Drehzahl bzw. bei Drehzahlsollwert 0 prägt der Wechselrichter einen Strom mit sehr kleiner Frequenz ein, der für das Schütz wie ein Gleichstrom wirkt).
- Das Schütz muss für den thermischen Dauerstrom des Antriebs ausgelegt werden.

3 Berechnung des Safety Integrity Levels für das Teilsystem „Reagieren“

3.1 Kurze Einführung in die IEC 62061

An dieser Stelle wird nur kurz auf die IEC 62061 eingegangen mit dem Ziel, den nachfolgenden Rechenweg für den Nachweis des Safety Integrity Levels (SIL) 3 für das Teilsystem „Reagieren“, bestehend aus einem SINAMICS G120/S110/120 Antriebssystem und einem bzw. mehreren Leistungsschützen, zu erläutern.

Auf die Teilsysteme „Erfassen“ und „Auswerten“ wird ebenfalls nicht weiter eingegangen.

Detaillierte Informationen gibt das Funktionsbeispiel „Praktische Anwendung der IEC 62061“. 23996473

Hat die Risikoanalyse der Maschine ergeben, dass eine Risikoreduzierung erforderlich ist, kann hierfür eine sicherheitsbezogene Steuerungsfunktion (SRCF; Safety-Related Control Function) verwendet werden. Diese hat die Aufgabe, gefährliche Zustände an der Maschine zu verhindern. Die Sicherheitsfunktion muss selbstverständlich in geeigneter Weise realisiert werden. Darüber hinaus ist der Nachweis der erforderlichen Sicherheitsintegrität erforderlich. Sie wird durch den Safety Integrity Level (SIL) ausgedrückt. Welcher SIL für eine Sicherheitsfunktion erforderlich ist, ergibt sich aus der Risikobewertung.

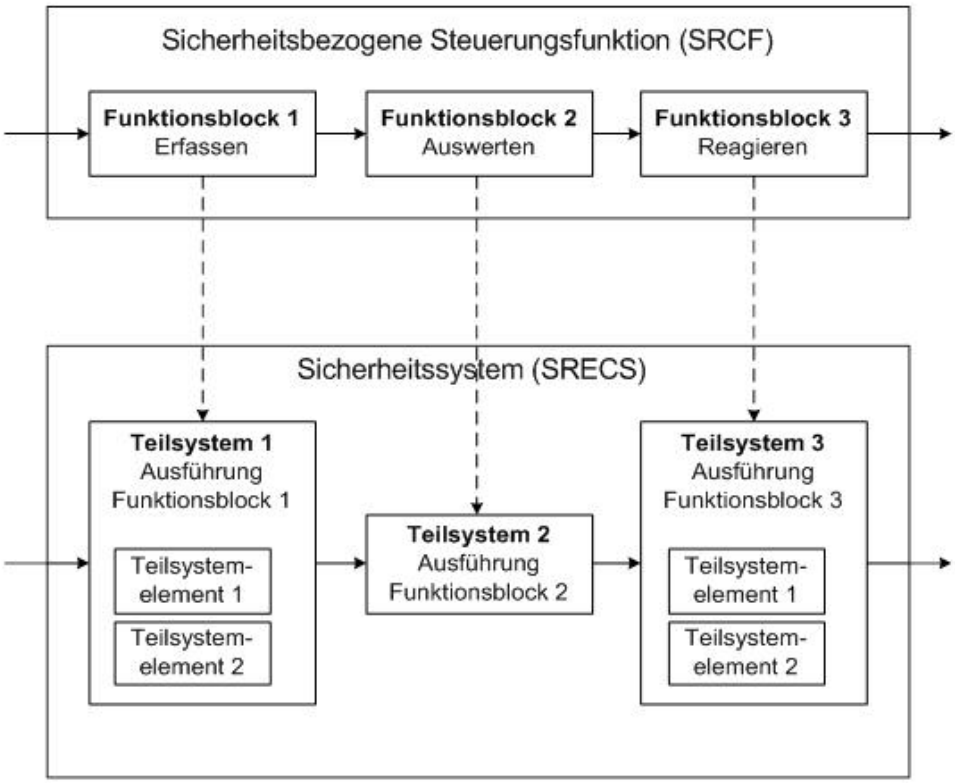
Zur Realisierung einer Sicherheitsfunktion wird ein Sicherheitssystem (SRECS; Safety-Related Electrical Control System) eingesetzt.

Eine sicherheitsbezogene Steuerungsfunktion besteht in aller Regel aus den Teilfunktionen

- Erfassen
- Auswerten
- Reagieren.

Diese finden sich im Sicherheitssystem wieder, das in der Regel aus den entsprechenden Teilsystemen besteht (siehe Abb. 3-1).

Abbildung 3-1



Abhängig vom erforderlichen SIL leiten sich unterschiedliche Anforderungen an das Sicherheitssystem (SRECS) ab, nämlich

- Anforderungen an die Struktur des (Teil-) Systems,
- die Wahrscheinlichkeit eines gefahrbringenden Ausfalls der Hardware (PFH_D),
- die „Robustheit“ gegen systematische Fehler,
- die Erkennung gefahrbringender Fehler (Diagnose) und der daraus abgeleiteten Fehlerreaktion,
- an die sicherheitsbezogene Anwendersoftware.

Alle Teilsysteme, die an der Ausführung einer SRCF beteiligt sind, müssen einen SIL Claim Limit (SIL CL) aufweisen, der mindestens gleich dem geforderten SIL der SRCF ist.

Die IEC 62061 sieht bei der Auswahl eines SRECS zwei Möglichkeiten vor:

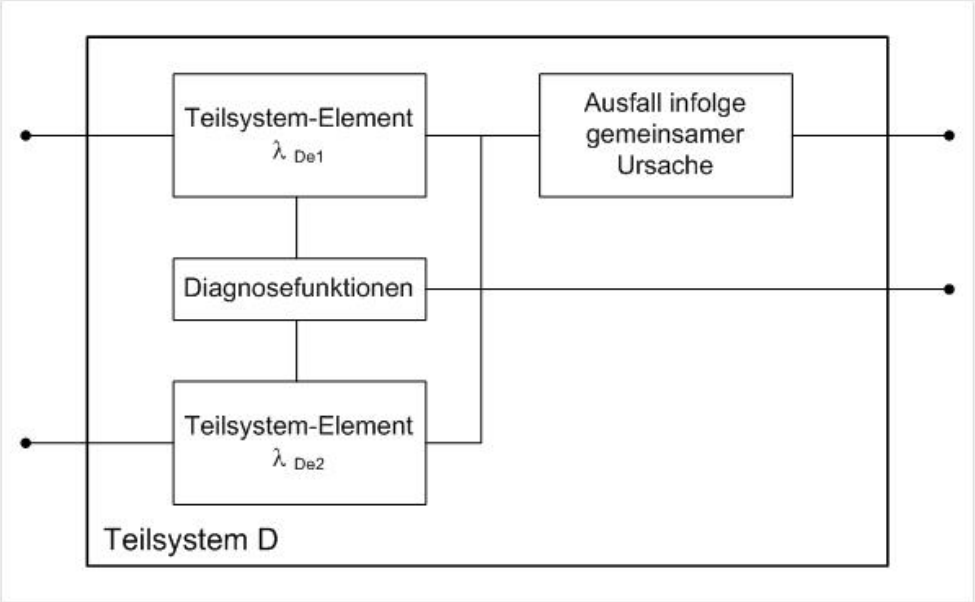
- Einsatz eines fertigen SRECS eines Herstellers, das die Anforderung bereits erfüllt,
- Entwurf und Entwicklung eines SRECS Teilsystems aus Teilsystemelementen.

Da das Antriebssystem SINAMICS G120/S110/120 im Standard nur SIL CL 2 erfüllt, kann es ohne Zusatzmaßnahmen nicht in einer Sicherheitsfunktion, die SIL 3 erfordert, eingesetzt werden. Deshalb kommt ein entworfenes Teilsystem zum Einsatz. Die IEC 62061 definiert hierfür vier Basis-Teilsystemarchitekturen und gibt einen Rechenweg an, wie die Ausfallrate dieser Basis-Teilsystemarchitekturen berechnet werden kann.

3.2 Berechnung des PFH_D anhand der Basis-Teilsystemarchitektur D

In den hier behandelten Beispielen kommt für das Teilsystem 3 (Aktor) die Basis-Teilsystemarchitektur D zur Anwendung, denn es handelt sich um ein redundantes System mit Diagnose. Die logische Darstellung der Basis-Teilsystemarchitektur D zeigt Abb. 3-2.

Abbildung 3-2



Zur Berechnung des PFH_D sind verschiedene Parameter erforderlich, die im Folgenden ermittelt werden.

3.2.1 Strukturelle Anforderungen

In den Abbildungen 2-1 und 2-2 ist ein Leistungsschütz in Reihe zum SINAMICS G120/S110/120 geschaltet. Dieses stellt einen zusätzlichen Abschaltpfad dar und bietet damit die erforderliche redundante Struktur.

Im Strukturbild Abb. 3-1 ist das durch die beiden parallelen Teilsystemelemente im Teilsystem 3 dargestellt. Gemäß IEC 62061, Tabelle 5, ist zum Erreichen eines SIL CL = 3 bei einer Hardwarefehlertoleranz (HFT) von 1 eine Safe Failure Fraction (SFF) von 90 % erforderlich. Diese wird in beiden Teilsystemelementen durch die implementierte Diagnose erreicht.

Beim SINAMICS wird kein Diagnosedeckungsgrad (DC) ausgewiesen. Deshalb wird in der folgenden Rechnung der DC für das Teilsystemelement 2 gleich Null angenommen. Durch interne Maßnahmen ist allerdings sichergestellt, dass die Anforderung gemäß Tabelle 5 (SFF ≥ 90 %) erfüllt ist.

Beim Schütz erfolgt die Diagnose, indem die Zustände des zwangsgeführten Rückmeldekontakts in der Steuerung überwacht werden. Gemäß IEC 61508-2, Anhang A, kann mit diesem Prinzip ein hoher Diagnosedeckungsgrad (DC = 99 % bzw. SFF ≥ 99%) erreicht werden. Wenn in der Applikation das Schütz oder der SINAMICS nur selten abgeschaltet werden, ist eine Zwangsdynamisierung der Abschaltfunktion erforderlich, z. B. alle 8 Stunden.

3.2.2 Bestimmung der Ausfallraten

Gemäß IEC 62061 müssen im ersten Schritt die Ausfallraten der beiden Teilsystemelemente bestimmt werden.

Ausfallrate des Teilsystemelements 1 (Schütz)

Die Ausfallrate ☐ eines elektromechanischen Bauelements berechnet sich nach folgender Formel:

$$\lambda = \frac{0{,}1 \times \mathrm{C}}{B10}$$

Hierbei ist:

C Anzahl der Betätigungen des Teilsystemelement pro Stunde

B10 Anzahl der Schaltspiele, nach denen statistisch 10% der Bauelemente ausgefallen sind (Herstellerangabe).

In der folgenden Berechnung wird beispielhaft von zehn Betätigungen pro Tag (8 Betriebsstunden) ausgegangen:

C = 1,25 / h.

Der B10-Wert beträgt laut Hersteller 1.000.000.

Es folgt

$$\lambda = \frac{0{,}1 \times 1{,}25/\mathrm{h}}{1000000} = 1{,}25 \times 10^{-7} / h$$

Den Einfluss der Anzahl der Betätigungen auf die Ausfallrate des Schützes zeigt die folgende Tabelle:

Tabelle 3-1

Betätigungen		B10	C	λ
1		1.000.000	0,042	4,17 x 10^{-09}
10	pro Tag (24 h)	1.000.000	0,417	4,17 x 10^{-08}
100		1.000.000	4,167	4,17 x 10^{-07}
1		1.000.000	0,125	1,25 x 10^{-08}
10	pro Tag (8 h)	1.000.000	1,25	1,25 x 10^{-07}
100		1.000.000	12,5	1,25 x 10^{-06}
1		1.000.000	1	1,00 x 10^{-07}
10	pro Stunde	1.000.000	10	1,00 x 10^{-06}
100		1.000.000	100	1,00 x 10^{-05}
1		1.000.000	60	6,00 x 10^{-06}
10	pro Minute	1.000.000	600	6,00 x 10^{-05}
100		1.000.000	6000	6,00 x 10^{-04}

Im nächsten Schritt wird die Rate der gefahrbringenden Ausfälle des Teilsystemelements berechnet. Laut Herstellerangabe sind das bei einem Schütz 75% der Ausfälle.

$$\lambda_{De1} = (Anteil\_gefahrbringender\_Ausfälle) \times \lambda = 0{,}75 \times 1{,}25 \times 10^{-7} / h$$

$$\lambda_{De1} = 9{,}375 \times 10^{-8} / h$$

Ausfallrate des Teilsystemelements 1 (Schütz) für Variante 1

In der Variante 1 (Abb. 2-1) besteht das Antriebssystem aus einem Antrieb mit einem Schütz. Daher kann für die Ausfallrate des Teilsystemelements der oben berechnete Wert angesetzt werden:

$$\lambda_{De1\_V1} = 9{,}375 \times 10^{-8} / h$$

Ausfallrate des Teilsystemelements 1 (Schütz) für Variante 2

In der Variante 2 (Abb. 2-2) besteht das Antriebssystem aus drei Antrieben mit jeweils einem Schütz. Die Schütze werden von der F-Steuerung zeitgleich angesteuert. In Anlehnung an die Basis-Teilsystemarchitektur A ist das eine Reihenschaltung von drei Teilsystemelementen. Zur Ermittlung der Ausfallrate des gesamten Teilsystemelements werden die einzelnen Ausfallraten addiert:

$$\lambda_{De1\_V2} = \lambda_{De1\_1} + \lambda_{De1\_2} + \lambda_{De1\_3} = 3 \times 9{,}375 \times 10^{-8} / h$$

$$\lambda_{De1\_V2} = 2{,}8125 \times 10^{-7} / h$$

Ausfallrate des Teilsystemelements 2 (SINAMICS)

Für das Antriebssystem SINAMICS liegen PFH_D-Werte der sicherheitsrelevanten Komponenten vor.

Aus der Beziehung

$$PFH_D = \lambda_D \times 1h$$

können so die Ausfallraten bestimmt werden.

$$\lambda_D = \sum PFH_D / h$$

Ausfallrate des Teilsystemelements 2 für Variante 1

Für den in Variante 1 (siehe Abb. 2-1) dargestellten Einachsantrieb wird im Folgenden ein SINAMICS S110 mit Power Module PM340 und Control Unit CU305 betrachtet. Als antriebsintegrierte Sicherheitsfunktion kommt Safe Torque Off (STO), aktiviert über Klemmen auf der CU305, zum Einsatz. Alternativ kann die Funktion auch über die sichere Kommunikation PROFIsafe angesteuert werden. Dies hat keinen Einfluss auf den PFH_D-Wert des SINAMICS. STO gehört zu den sog. Basic Functions. Für diese ist kein Geber erforderlich.

Die PFH_D-Werte der beiden SINAMICS-Komponenten sind

- 18×10^{-9} (Power Module M340) und
- 10×10^{-9} (Control Unit CU305);

der Summen-PFH_D beträgt somit

$$\sum PFH_D = 28 \times 10^{-9}$$

Mit der o. g. Formel ergibt sich somit

$$\lambda_{De2\_V1} = 28 \times 10^{-9} / h$$

Alternativ zum SINAMICS S110 kann hier auch ein SINAMICS G120 zum Einsatz kommen. Beim SINAMICS G120 gibt es keine separaten PFH-Werte für einzelne Komponenten, sondern es gibt einen Gesamt-PHF-Wert für das komplette Gerät:

- 50 x 10^{-9} (SINAMICS G120).

Es ergibt sich

$$\lambda_{De2\_V1} = 50 \times 10^{-9} / h$$

Hinweis Dieser Wert gilt auch für die Ausprägungen G120D und G120C

Ausfallrate des Teilsystemelements 2 (SINAMICS S120) für Variante 2

In der Variante 2 (Abb. 2-2) besteht das Antriebssystem aus drei SINAMICS S120 Antrieben. Auch hier wird für alle Antriebe die Sicherheitsfunktion STO, angesteuert über Onboard-Klemmen oder PROFIsafe, eingesetzt.

Die PFH_D-Werte der verwendeten Komponenten sind

- 10 x 10^{-9} (Control Unit CU320),
- 10 x 10^{-9} (Single Motor Module, Bauform Booksize),
- 14 x 10^{-9} (Single Motor Module, Bauform Chassis),
- 18 x 10^{-9} (Power Module Bauform Blocksize, an die CU320 über CUA32 angekoppelt).

Der Summen-PFH_D des Antriebssystems beträgt somit

$$\sum PFH_D = 52 \times 10^{-9}$$

(Das Line Module hat keinen Einfluss auf die funktionale Sicherheit des Systems und bringt daher keinen PFH_D -Beitrag.)

Es ergibt sich

$$\lambda_{De2\_V2} = 52 \times 10^{-9} / h$$

Gebrauchsdauer / Proof-Test-Intervall

Für die Berechnung der Ausfallraten für die Basis-Teilsystemarchitektur D wird weiterhin die Zeit T1 benötigt. Gemäß IEC 62061 ist T1 definiert als das Minimum aus Gebrauchsdauer und Proof-Test-Intervall. Ein Proof-Test, d. h. eine vollständige manuelle Überprüfung und Wartung des Systems mit dem Ziel, dass es sich anschließend in einem „wie neu Zustand“ befindet, wird bei elektronischen

Komponenten in der Regel nicht durchgeführt. Daher entspricht hier T1 der Gebrauchsdauer (Mission Time).

Für die verwendeten Teilsystemelemente „Schütz“ und „SINAMICS“ ist

T11 = T12 = 20 Jahre,

bzw.

T11 = T12 = 175.200 h.

Hinweis Beim verschleißbehafteten Schütz gilt T1 = 20 Jahre nur, wenn innerhalb dieser Zeit die mit dem B10-Wert angegebenen maximale Anzahl von Schaltspielen nicht überschritten wird. Ansonsten ist die Gebrauchsdauer entsprechend zu reduzieren.

3.2.3 CCF-Faktor

Bei redundanten Teilsystemen muss betrachtet werden, ob Fehler auftreten können, die beide Teilsysteme gleichzeitig ausfallen lassen. Man spricht hier von „Ausfällen in Folge gemeinsamer Ursache“ oder englisch „Common Cause Failure (CCF)“. Als Symbol wird β verwendet.

Die IEC 62061 gibt im Anhang F Bewertungskriterien zur Ermittlung des CCF an.

In der hier behandelten beispielhaften Sicherheitsfunktion werden folgende Maßnahmen ergriffen:

- Signalkabel werden in getrennten Kabelkanälen verlegt (5 Punkte),
- Signal- und Leistungskabel sind schon aus EMV-Gründen getrennt verlegt und sind geschützt, weil alle Komponenten in einem Schaltschrank aufgebaut sind (5 Punkte),
- Die beiden Teilsystem-Elemente Schütz und SINAMICS haben jeweils eigene Gehäuse und sind somit als physikalisch getrennte Einheiten zu betrachten (5 Punkte),
- Diversität durch verschiedene Technologien liegt vor (konventionelles Schütz und elektronische Sicherheitsfunktion im SINAMICS; 8 Punkte),
- Beide Teilsystemelemente funktionieren nach verschiedenen physikalischen Prinzipien (elektromechanische Schützkontakte und mikroprozessorgesteuerter Umrichter mit Leistungshalbleitern als „Schaltelemente“; 10 Punkte),
- Sowohl das bzw. die Schütze und der SINAMICS sind in einem Schaltschrank in einer für die Aufstellbedingungen ausreichenden Schutzart aufgebaut, so dass negative Einflüsse aufgrund der Umgebungsbedingungen ausgeschlossen werden können (9 Punkte).

Es ergibt sich eine Summe von 42 Punkten. Laut Tabelle F.2 im Anhang F der IEC 62061 kann für eine Gesamtpunktzahl von 35 bis 65 ein CCF von 5 % angesetzt werden.

Es gilt somit $\beta = 0{,}05$.

3.2.4 Diagnose-Testintervall

Zur Fehleraufdeckung durch Diagnose müssen die Sicherheitsfunktionen der Teilssystemelemente Schütz und SINAMICS vom Teilsystem 2 (Sicherheitssteuerung) in regelmäßigen Abständen angewählt werden. Beim SINAMICS wird hiermit die interne Diagnose angestoßen. Beim Schütz erfolgt die Diagnose in der Sicherheitssteuerung, indem die Rückmeldung auf Plausibilität überprüft wird. Das Zeitintervall zwischen zwei solcher Prüfungen wird mit Diagnose-Testintervall T2 bezeichnet. Um die Gefahr durch einen temporär unentdeckten Ausfall zu begrenzen, sollte die Zeit T2 nicht zu groß gewählt werden. Welche Zeit in der Praxis vorgesehen wird, hängt von der Risikoanalyse der Maschine, aber auch von den zulässigen Betriebszuständen, die einen Diagnosetest zulassen, ab. Bei Produktions- und Werkzeugmaschinen bietet sich der Schichtwechsel, d. h. alle 8 Stunden, an.

Bei Maschinen, deren Sicherheitsfunktionen betriebsmäßig immer wieder angefordert werden, z. B. für die Befüllung mit Material oder die Entnahme fertiger Produkte, reduziert sich T2 entsprechend. Im Kap. „Ausfallrate des Teilsystemelements 1 (Schütz)“ wurde für C der Wert 1,25 / h angenommen. Da mit jeder Betätigung der Testzyklus angestoßen wird, korreliert C mit T2:

Es gilt hier:

T2 = 2/C.

T2 = 1,6 h.

3.2.5 Berechnung der PFH_D-Werte

Gemäß IEC 62061 berechnet sich die Ausfallrate für die Basis-Teilsystemarchitektur D wie folgt:

$$PFH_D = (1-\beta)^2 \times \left[\{\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2)\} \times \frac{T_2}{2} + \{\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2))\} \times \frac{T_1}{2} \right] + \beta \times \frac{(\lambda_{De1} + \lambda_{De2})}{2}$$

Berechnung des PFH_D - Wertes für Variante 1

In den vorigen Kapiteln wurden folgende Parameter ermittelt:

Teilsystemelement 1

λ_{De1_V1} = 9,375 x 10^{-8} / h

DC_1 = 0,99

Teilsystemelement 2

λ_{De2_V1} = 2,8 x 10^{-8} / h

DC_2 = 0

T2 = 1,6 h

T1 = 175.200 h

β = 0,05

Es ergibt sich schließlich

PFH_{DssD_V1} = 3,25 x 10^{-9}.

Soll ein Teilsystem SIL CL 3 erfüllen, so muss der zugehörige PFH_D folgende Bedingung erfüllen:

$PFH_D < 1 \times 10^{-7}$.

Das ist hier gegeben.

Für den SINAMICS G120 ergibt sich ein unterschiedlicher λ – Wert. Die übrigen Werte gelten auch für das SINAMICS G120 – Beispiel.

Es ergibt sich hier

$PFH_{DssD\_V1} = 3{,}97 \times 10^{-9}$.

Auch dieser Wert erfüllt die Bedingungen für SIL CL 3.

Berechnung des PFH_D - Wertes für Variante 2

In den vorigen Kapiteln wurden folgende Parameter ermittelt:

Teilsystemelement 1

$\lambda_{De1\_V2} = 2{,}8125 \times 10^{-7}$ / h

DC1 = 0,99

Teilsystemelement 2

$\lambda_{De2\_V2} = 5{,}2 \times 10^{-8}$ / h

DC2 = 0

T2 = 1,6 h

T1 = 175.200 h

$\beta = 0{,}05$

Es ergibt sich:

$PFH_{DssD\_V2} = 9{,}5 \times 10^{-9}$.

Soll ein Teilsystem SIL CL 3 erfüllen, so muss der zugehörige PFH_D folgende Bedingung erfüllen:

$PFH_D < 1 \times 10^{-7}$.

Das ist hier ebenfalls gegeben.

4 Bestimmung des SIL eines Sicherheitssystems

Im Kapitel 3 wurden SIL CL und PFH_D des Teilsystems „Reagieren“ bestimmt. Zu einem Sicherheitssystem (SRECS) gehören in der Regel weitere Teilsysteme, z. B. die in Abb. 2-1 und 2-2 dargestellte F-CPU mit den zugehörigen F-I/O-Modulen.

Für eine Sicherheitsfunktion (SRCF), die SIL 3 erfüllen muss, müssen diese Teilsysteme ebenfalls mindestens SIL CL 3 aufweisen.

Weiterhin ergibt sich der PFH_D der SRCF aus der Summe der einzelnen PFH_D - Werte. Soll die Sicherheitsfunktion SIL 3 erfüllen, darf die Summe aller PFH_D - Werte den Grenzwert 1 x 10-7 nicht überschreiten.

5 Hinweise für den Anwender

Das vorliegende Dokument beschreibt zwei Konstellationen mit SINAMICS G120/S110/120 Antriebskomponenten und den Nachweis des erreichten SIL.

Es kann als Anleitung verwendet werden, um für konkrete Applikationen den erreichten SIL zu bestimmen. Hierbei sind die Parameter der konkreten Applikation zu berücksichtigen, z. B.

- die jeweiligen PFH_D- und T1-Werte der verwendeten SINAMICS Komponenten,
- B10- und T1-Wert der verwendeten Schütze und die Anzahl der Schaltzyklen,
- Das Diagnosetestintervall T2,
- die ergriffenen Maßnahmen gegen Fehler gemeinsamer Ursache (CCF).

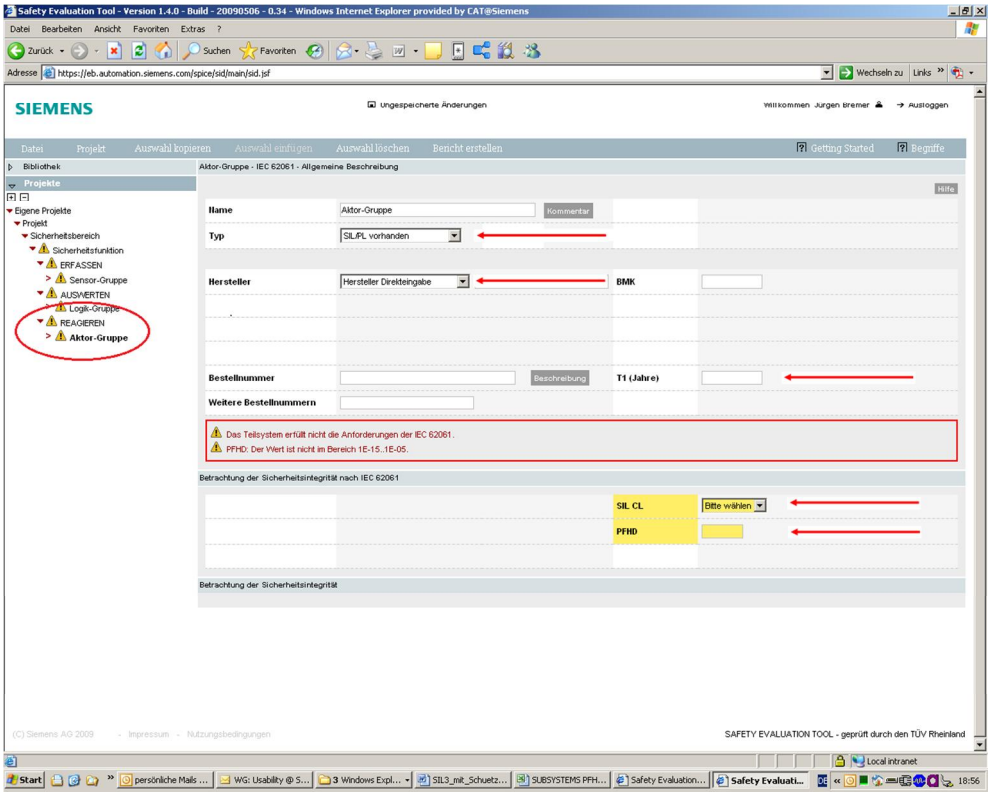
Für die Berechnung des Gesamtsystems kann das Siemens „Safety Evaluation Tool“ eingesetzt werden.

Hierbei können für das Teilsystem „Reagieren“ die Parameter

- SIL CL
- PFH_D
- T1,

die gemäß Kapitel 3 bestimmt worden sind, über die Auswahl „Hersteller Direkteingabe“ eingegeben werden.

Abbildung 5-1



Das Tool unterstützt bei der Auswahl der weiteren Sicherheitsbauteile für die Funktionen „Erfassen“ und „Auswerten“ und berechnet die Sicherheitsintegrität der gesamten Sicherheitsfunktion. Als Abschluss kann ein Report ausgedruckt und der Maschinendokumentation beigelegt werden.