

SIEMENS

Ingenuity for life

24/7

Industry Online Support

Home

Not-Halt bis PL e / SIL 3 mit einer fehlersicheren Steuerung S7-1500

SIMATIC Safety Integrated

<https://support.industry.siemens.com/cs/ww/de/view/21064024>

Siemens
Industry
Online
Support



Gewährleistung und Haftung

Hinweis

Die Anwendungsbeispiele sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit hinsichtlich Konfiguration und Ausstattung sowie jeglicher Eventualitäten. Die Anwendungsbeispiele stellen keine kundenspezifischen Lösungen dar, sondern sollen lediglich Hilfestellung bieten bei typischen Aufgabenstellungen. Sie sind für den sachgemäßen Betrieb der beschriebenen Produkte selbst verantwortlich. Diese Anwendungsbeispiele entheben Sie nicht der Verpflichtung zu sicherem Umgang bei Anwendung, Installation, Betrieb und Wartung. Durch Nutzung dieser Anwendungsbeispiele erkennen Sie an, dass wir über die beschriebene Haftungsregelung hinaus nicht für etwaige Schäden haftbar gemacht werden können. Wir behalten uns das Recht vor, Änderungen an diesen Anwendungsbeispiele jederzeit ohne Ankündigung durchzuführen. Bei Abweichungen zwischen den Vorschlägen in diesem Anwendungsbeispiel und anderen Siemens Publikationen, wie z. B. Katalogen, hat der Inhalt der anderen Dokumentation Vorrang.

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

Unsere Haftung, gleich aus welchem Rechtsgrund, für durch die Verwendung der in diesem Anwendungsbeispiel beschriebenen Beispiele, Hinweise, Programme, Projektierungs- und Leistungsdaten usw. verursachte Schäden ist ausgeschlossen, soweit nicht z. B. nach dem Produkthaftungsgesetz in Fällen des Vorsatzes, der groben Fahrlässigkeit, wegen der Verletzung des Lebens, des Körpers oder der Gesundheit, wegen einer Übernahme der Garantie für die Beschaffenheit einer Sache, wegen des arglistigen Verschweigens eines Mangels oder wegen Verletzung wesentlicher Vertragspflichten zwingend gehaftet wird. Der Schadensersatz wegen Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen, vorhersehbaren Schaden begrenzt, soweit nicht Vorsatz oder grobe Fahrlässigkeit vorliegt oder wegen der Verletzung des Lebens, des Körpers oder der Gesundheit zwingend gehaftet wird. Eine Änderung der Beweislast zu Ihrem Nachteil ist hiermit nicht verbunden.

Weitergabe oder Vervielfältigung dieser Anwendungsbeispiele oder Auszüge daraus sind nicht gestattet, soweit nicht ausdrücklich von der Siemens AG zugestanden.

Security-hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z.B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter <http://www.siemens.com/industrialsecurity>.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter <http://www.siemens.com/industrialsecurity>.

Inhaltsverzeichnis

Gewährleistung und Haftung	2
1 Einführung	4
1.1 Überblick.....	4
1.2 Funktionsweise.....	5
1.2.1 Standard-Anwenderprogramm.....	6
1.2.2 Sicherheitsprogramm.....	7
1.2.3 Datenaustausch zwischen Standard-Anwenderprogramm und Sicherheitsprogramm.....	9
1.3 Verwendete Komponenten.....	10
2 Engineering	11
2.1 Hardware-Aufbau.....	11
2.2 Konfiguration.....	12
2.2.1 Einstellungen der F-DI.....	12
2.2.2 Einstellungen der F-DQ.....	13
2.3 Inbetriebnahme.....	14
2.3.1 Vorbereitung.....	14
2.3.2 S7-Projekt in die CPU S7-1516F laden.....	14
2.3.3 PROFIsafe-Adressen zuweisen.....	16
2.4 Bedienung.....	17
3 Wissenswertes	18
3.1 Grundlagen.....	18
3.1.1 Grundbegriffe.....	18
3.1.2 Funktionale Sicherheit.....	18
3.1.3 Not-Halt.....	19
3.2 Bewertung der Sicherheitsfunktion.....	21
3.2.1 Normen.....	21
3.2.2 Sicherheitsfunktion.....	21
3.2.3 Bewertung nach ISO 13849-1.....	22
Bewertung "Erfassen".....	22
Bewertung "Auswerten".....	23
Bewertung "Reagieren".....	23
Ergebnis der Bewertung nach ISO 13849-1.....	24
3.2.4 Bewertung nach IEC 62061.....	24
Bewertung "Erfassen".....	24
Bewertung "Auswerten".....	25
Bewertung "Reagieren".....	25
Ergebnis der Bewertung nach IEC 62061.....	26
4 Anhang	27
4.1 Service und Support.....	27
4.2 Links und Literatur.....	28
4.3 Änderungsdokumentation.....	28

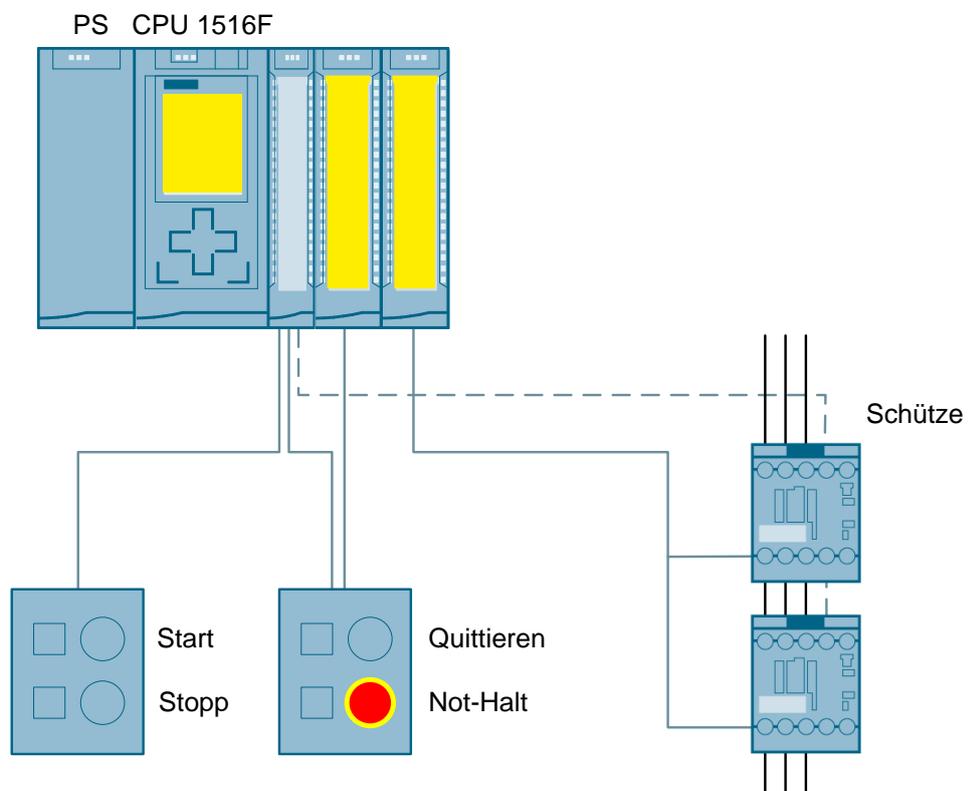
1 Einführung

1.1 Überblick

Um eine Maschine auch im Notfall sicher abschalten zu können, wird ein Not-Halt-Befehlsgerät angebracht und die Aktorik über zwei Schütze gesteuert. Die Sicherheitsfunktion wird bis PL e nach EN ISO 13849-1 bzw. SIL 3 nach IEC 62061 ausgelegt.

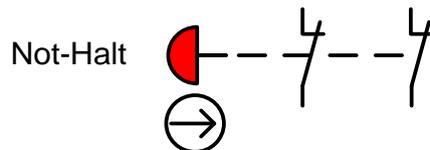
Um die nahtlose Integration in den Automatisierungsprozess zu gewährleisten, wird die fehlersichere Steuerung S7-1516F eingesetzt, in der Standard-Anwenderprogramm und Sicherheitsprogramm koexistent ablaufen.

Abbildung 1-1 Übersicht Hardware-Aufbau



Um den geforderten Sicherheitslevel zu erreichen, wird der Not-Halt zweikanalig ausgelegt und auf Diskrepanz und Querschluss durch die Steuerung überwacht.

Abbildung 1-2: Zweikanaliger Not-Halt



Auch die Aktorik ist zweikanalig ausgelegt, sodass beim Versagen eines Schützes (z. B. Verschweißen der Kontakte) die Maschine dennoch durch das zweite Schütz sicher abgeschaltet wird.

ACHTUNG

PL e / SIL 3 kann nur erreicht werden, wenn die Funktion der Schütze im Rückführkreis überwacht wird.

Weitere Informationen zum Thema "Rückführkreis" finden Sie unter [3](#).

Vorteile

- Integration der Sicherheitsfunktion in die Gesamtapplikation:
 - Status des Not-Halts steht auch im Standard-Anwenderprogramm zur Verfügung und kann dort verarbeitet werden.
 - Erspart die Synchronisation (Extra-Verdrahtung oder Data-Mapping) zwischen Standard- und Safety-Automatisierung.
- Die Diagnose erfolgt kanalgranular auch bei mehreren Not-Halt-Befehlsgeräten:
 - Fehlerlokalisierung wird beschleunigt.
- Diagnosemeldungen können ohne zusätzlichen Aufwand einer Meldungsprojektierung auf
 - einem HMI-Panel,
 - mittels Web-Server oder
 - auf dem Display der CPU angezeigt werden.

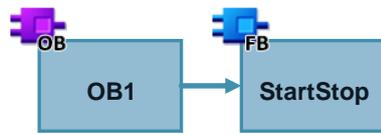
1.2 Funktionsweise

In diesem Anwendungsbeispiel werden folgende Funktionen realisiert:

- Rücksetzen eines sicherheitsgerichteten digitalen Ausgangs (Stopp der Anwendung) nach Betätigung des Not-Halt-Befehlsgeräts.
- Verriegelung gegen ein erneutes Anlaufen der Maschine nach dem Auslösen der Sicherheitsfunktion bis folgende Bedingungen erfüllt sind:
 - Not-Halt ist entriegelt
 - Quittierung ist erfolgt (führt nicht automatisch zum Start der Anwendung)
 - Starttaster wird betätigt
- Überwachung der korrekten Funktion der Schütze.
- Verriegelung gegen ein erneutes Anlaufen der Maschine, wenn ein fehlerhaftes Schütz erkannt wurde.

1.2.1 Standard-Anwenderprogramm

Abbildung 1-3: Überblick Standard-Anwenderprogramm



Funktionsbaustein StartStop

Der Baustein wertet die Start- und Stopptaster aus. Mit einer positiven Flanke am Eingang des Starttasters wird ein Startsignal in den globalen Datenbaustein "DataToSafety" geschrieben. Das Startsignal kann dann im Sicherheitsprogramm ausgewertet werden, wo das Einschalten und Ausschalten der Maschine erfolgt.

Der Baustein wertet aus:

- Starttaster
- Stopptaster
- Fehlermeldung "fault" aus dem Sicherheitsprogramm über den Datenbaustein "DataFromSafety", siehe Kapitel [1.2.3](#).

Wird der Stopptaster betätigt oder ein Fehler über das Signal "fault" vom globalen Datenbaustein "DataFromSafety" erkannt, wird das Startsignal zurückgesetzt.

Abbildung 1-4: Aufruf Funktionsbaustein "StartStop"

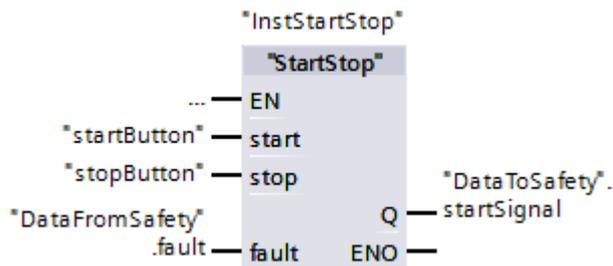
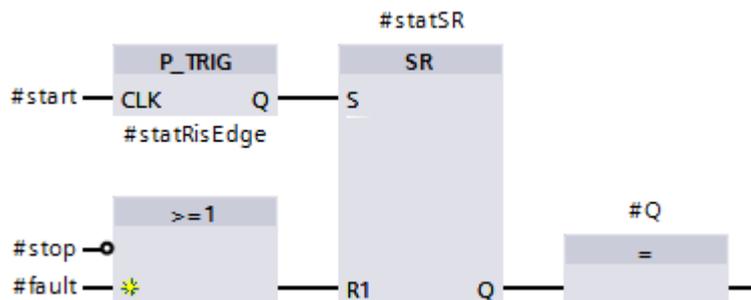
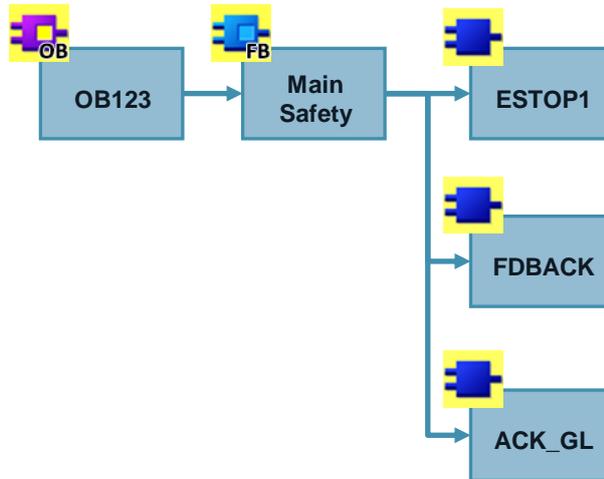


Abbildung 1-5: Funktionsbaustein "StartStop"



1.2.2 Sicherheitsprogramm

Abbildung 1-6: Überblick Sicherheitsprogramm



Anweisung ESTOP1

Die Anweisung ESTOP1 ist in STEP 7 Safety Advanced enthalten. Ist der Not-Halt nicht betätigt, gibt die Anweisung TRUE auf dem Ausgang Q aus. Nach Betätigung des Not-Halts muss dieser entriegelt werden und über den Eingang ACK quittiert werden. Dass eine Quittierung erforderlich ist, wird über den Ausgang ACK_REQ ausgegeben. Der Ausgang Q wird in der temporären Variable #tempEstopQ zwischengespeichert, um einen Zugriff darauf in der nächsten Anweisung zu vereinfachen.

Abbildung 1-7: Aufruf Anweisung ESTOP1



Hinweis

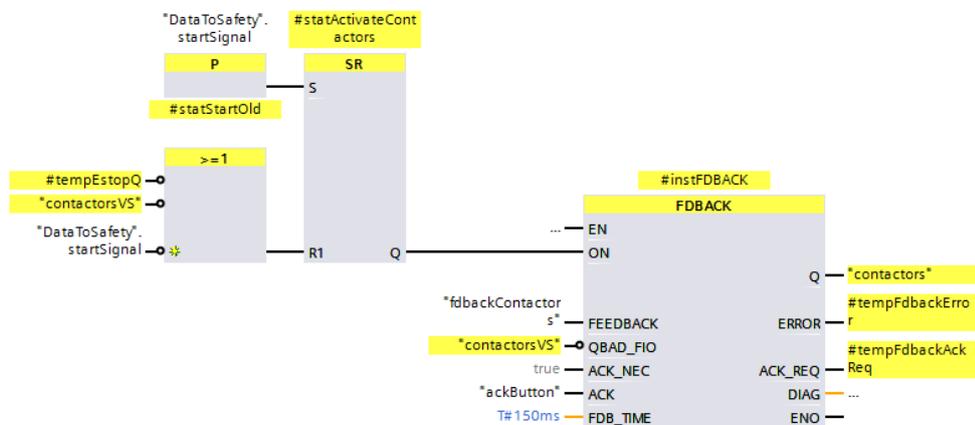
Die beiden Kanäle des Not-Halts werden durch das F-DI-Modul auf Diskrepanz und Querschloss überwacht. Im Anwenderprogramm steht dann ein verarbeitetes Signal für beide Kanäle zur Verfügung. Auf die einzelnen Kanäle kann nicht zugegriffen werden.

Anweisung FDBACK

Die Anweisung FDBACK ist in STEP 7 Safety Advanced enthalten. Sie schaltet die Aktorik (in diesem Beispiel die beiden Schütze) und überwacht über den Rückführkreis deren korrekte Funktion.

Wird ein Startbefehl aus dem Standard-Anwenderprogramm empfangen (siehe Kapitel [1.2.1](#)), das Freigabesignal der Anweisung ESTOP1 liegt an und es liegt kein Fehler im Sicherheitsprogramm vor, werden die Schütze eingeschaltet. Innerhalb der parametrisierten Zeit FDB_TIME muss das Signal am Eingang FEEDBACK invers zum Ausgangssignal Q schalten. Ist dies nicht der Fall, werden die Schütze wieder abgeschaltet. Danach muss über den Eingang ACK quittiert werden. Dass eine Quittierung erforderlich ist, wird über den Ausgang ACK_REQ ausgegeben.

Abbildung 1-8: Aufruf Anweisung FDBACK



Hinweis

Bei neuen Steuerungen S7-1200 und S7-1500 wird das kanalgranulare QBAD-Bit durch den Wertstatus ersetzt. Für den Wertstatus (engl. "Value status") gilt folgende Konvention:

FALSE: Es werden Ersatzwerte ausgegeben.

TRUE: Es werden Prozesswerte ausgegeben.

Der Wertstatus verhält sich invers zum QBAD-Bit und wird in das Prozessabbild der Eingänge (PAE) eingetragen.

Mehr Informationen zum Wertstatus finden Sie hier [\5](#).

Anweisung ACK_GL

Die Anweisung ACK_GL ist in STEP 7 Safety Advanced enthalten. Sie erzeugt eine Quittierung zur gleichzeitigen Wiedereingliederung aller F-Peripherien/Kanäle der F-Peripherie einer F-Ablaufgruppe nach Kommunikationsfehlern bzw. F-Peripherie-/Kanalfehlern.

Abbildung 1-9: Aufruf Anweisung ACK_GL



Beispiele für Ereignisse, die zur Passivierung führen:

- Drahtbruch an der F-DQ
- Fehlende Spannungsversorgung an der F-DI

Hinweis

Tritt ein Fehler in der Hardware auf, kann es ein paar Sekunden dauern, bis die Baugruppe erkennt, dass der Fehler beseitigt wurde (z. B. Beseitigung eines Drahtbruchs). Erst danach hat die Betätigung des Quittiertasters Auswirkung.

1.2.3 Datenaustausch zwischen Standard-Anwenderprogramm und Sicherheitsprogramm

Um Daten zwischen dem Standard-Anwenderprogramm und dem Sicherheitsprogramm auszutauschen, werden zwei globale Datenbausteine verwendet:

- DataToSafety
- DataFromSafety

Der Datenbaustein DataToSafety wird vom Standard-Anwenderprogramm geschrieben und vom Sicherheitsprogramm gelesen. Der Datenbaustein DataFromSafety wird vom Sicherheitsprogramm geschrieben und vom Standard-Anwenderprogramm gelesen.

Vom Standard-Anwenderprogramm wird das verarbeitete Startsignal "StartSignal" an das Sicherheitsprogramm übertragen. Das Sicherheitsprogramm meldet ein fehlersicheres Abschalten oder Fehler im Sicherheitsprogramm über die Variable "fault" an das Standard-Anwenderprogramm.

Hinweis

Mehr Informationen zu dem Austausch von Daten zwischen dem Standard-Anwenderprogramm und dem Sicherheitsprogramm finden Sie unter [5](#).

1.3 Verwendete Komponenten

Dieses Anwendungsbeispiel wurde mit diesen Hard- und Softwarekomponenten erstellt:

Tabelle 1-1: Hardware- und Software-Komponenten

Komponente	Anz.	Artikelnummer	Hinweis
Stromversorgung	1	6EP1332-4BA00	PM 190 W
Fehlersichere S7-CPU	1	6ES7516-3FN01-0AB0	CPU 1516F-3 PN/DP FW 2.0
SIMATIC Memory Card	1	6ES7954-8LF01-0AA0	SMC 24MB
Digitales Eingabe-/Ausgabemodul	1	6ES7523-1BL00-0AA0	DI 16/DQ 16x24VDC
Fehlersicheres digitales Eingabemodul	1	6ES7526-1BH00-0AB0	
Fehlersicheres digitales Ausgabemodul	1	6ES7526-2BF00-0AB0	
Profilschiene S7-1500	1	6ES7590-1AE80-0AA0	Länge: 482 mm
Not-Halt	1	3SU1851-0NB00-2AA2	Pilzdrucktaster 2Ö
Drucktaster	3	3SU1	2S, 1Ö
Schütz	2	3RT2015-1BB42	S00, DC24V, 1Ö
STEP 7 Professional	1	6ES7822-1AA04-0YA5	V14 Update 1
STEP 7 Safety Advanced	1	6ES7833-1FA14-0YA5	V14 Update 1

Dieses Anwendungsbeispiel besteht aus folgenden Komponenten:

Tabelle 1-2: Beispieldateien und Projekte

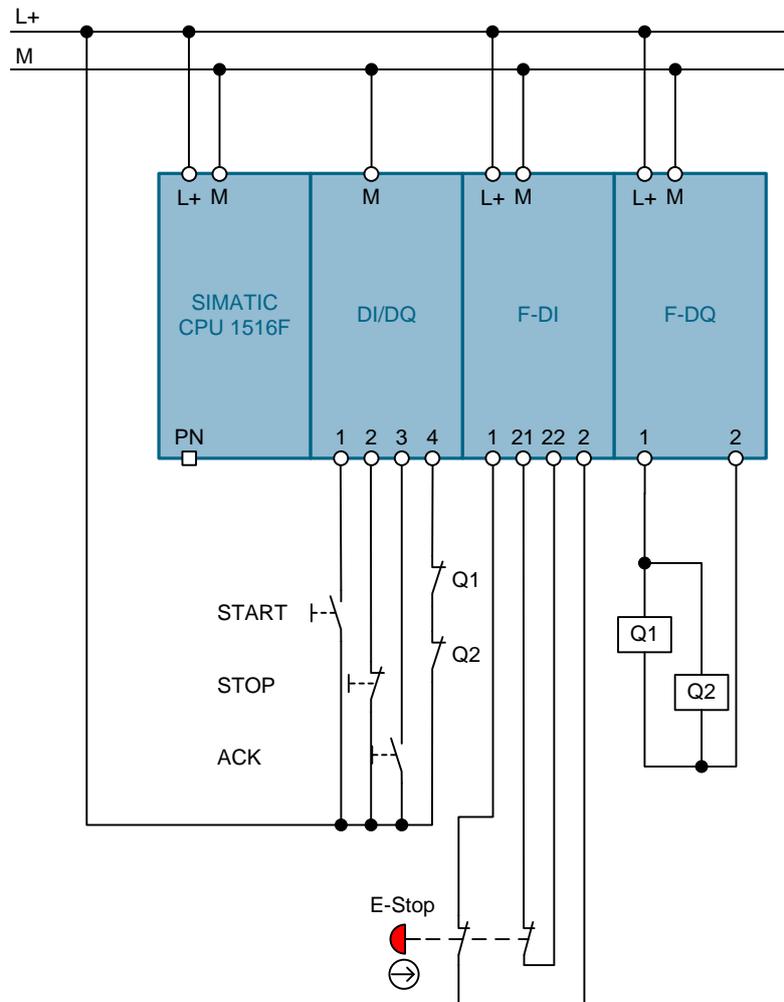
Komponente	Hinweis
21064024_ESTOP_SIL3_1500F_DOC_V50_de.pdf	Dieses Dokument
21064024_ESTOP_SIL3_1500F_PROJ_V50.zip	Diese gepackte Datei enthält das TIA Portal-Projekt
21064024_ESTOP_SIL3_1500F_SET_V50.zip	Bewertung der Sicherheitsfunktionen als SET-Projekt

2 Engineering

2.1 Hardware-Aufbau

Zum Nachstellen dieses Anwendungsbeispiels verdrahten Sie die Hardware-Komponenten wie nachfolgend gezeigt.

Abbildung 2-1: Verdrahtung der Hardware-Komponenten



2.2 Konfiguration

Das mitgelieferte Projekt bedarf keiner weiteren Konfiguration. Sollten Sie das Anwendungsbeispiel mit anderen Komponenten nachbauen, werden in diesem Kapitel die wichtigsten Einstellungen gezeigt.

ACHTUNG Die nachfolgend gezeigten Einstellungen tragen mit dazu bei, PL e / SIL 3 zu erfüllen. Änderungen an den Einstellungen können zu einem Verlust der Sicherheitsfunktion führen.

ACHTUNG Die in den Beispielprojekten verwendeten Default-Werte können gegebenenfalls von Ihren individuellen Anforderungen abweichen.

2.2.1 Einstellungen der F-DI

Kurzschlussstest

Die Kurzschlussstests für die verwendeten Kanäle 0 und 8 sind aktiviert.

Abbildung 2-2: Kurzschlussstests für Geberversorgung 0 aktivieren

> > Sensor supply 0

Supplied channels: Channels [0...3]

Short-circuit test activated

Time for short-circuit test: 4.2 ms

Startup time of sensor after short-circuit test: 4.2 ms

Abbildung 2-3: Kurzschlussstests für Geberversorgung 2 aktivieren

> > Sensor supply 2

Supplied channels: Channels [8...11]

Short-circuit test activated

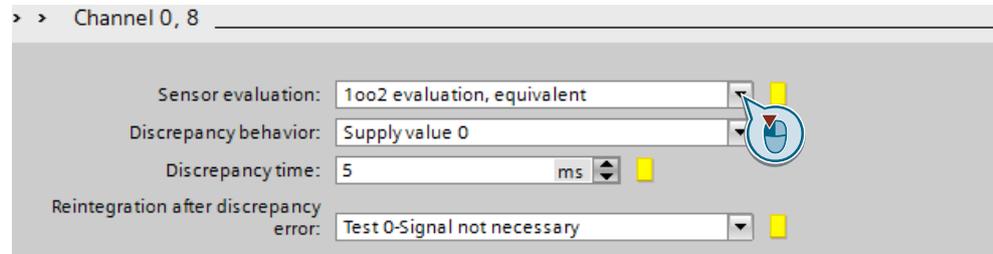
Time for short-circuit test: 4.2 ms

Startup time of sensor after short-circuit test: 4.2 ms

Kanalparameter

Die Überwachung des Not-Halts erfolgt über das Kanalpaar 0, 8. Um Diskrepanzen zwischen den beiden Kanälen zu erkennen und somit den geforderten Sicherheitslevel zu erreichen, müssen Sie die Auswertung der Geber auf "1oo2 (2v2)-Auswertung, äquivalent" ("1oo2 evaluation, equivalent") stellen.

Abbildung 2-4: Kanalparameter Not-Halt



Hinweis

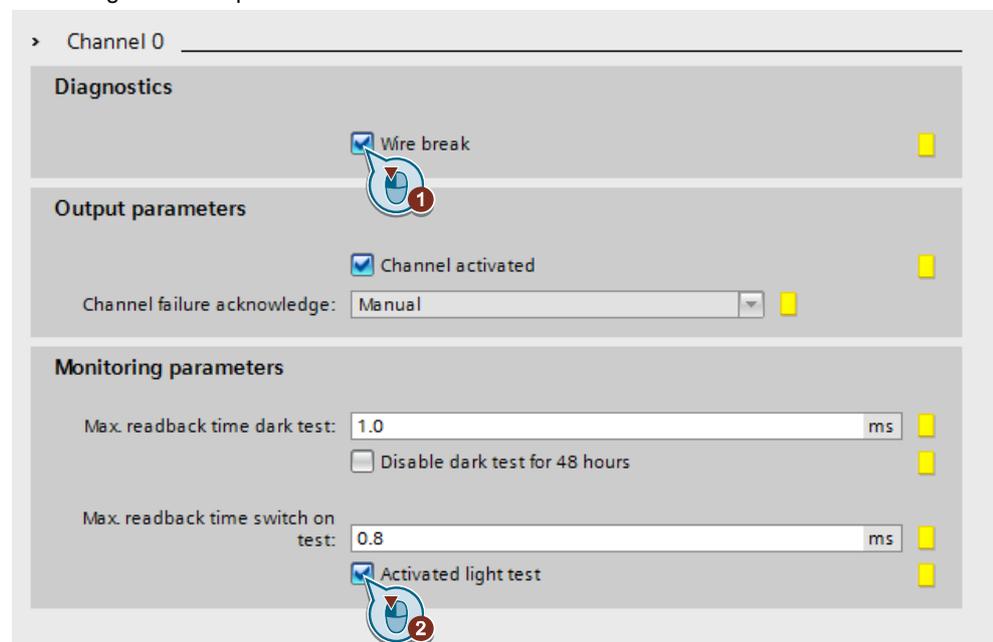
Setzen Sie die Diskrepanzzeit so kurz wie möglich, sodass im fehlerfreien Betrieb des Not-Halt-Befehlsgeräts kein Diskrepanzfehler ausgelöst wird.

2.2.2 Einstellungen der F-DQ

Kanalparameter

Aktivieren Sie die Drahtbruch-Erkennung und den Helltest.

Abbildung 2-5: Kanalparameter Schütze



2.3 Inbetriebnahme

2.3.1 Vorbereitung

1. Laden Sie sich die Projektdatei "21064024_ESTOP_SIL3_1500F_PROJ_V50.zip" runter. Den Downloadlink finden Sie unter [\](#).
2. Speichern Sie die zip-Datei in einem beliebigen Verzeichnis auf Ihrem Computer und entpacken Sie diese.
3. Stellen Sie die IP-Adresse des PG/PCs ein, sodass sich das PG/PC im selben Subnetz wie die CPU befindet.
4. Verbinden Sie mit einem Ethernet-Kabel das PG/PC mit der Ethernet-Schnittstelle der CPU S7-1516F.

Für dieses Anwendungsbeispiel wurde folgende IP-Adresse verwendet:

CPU S7-1516F

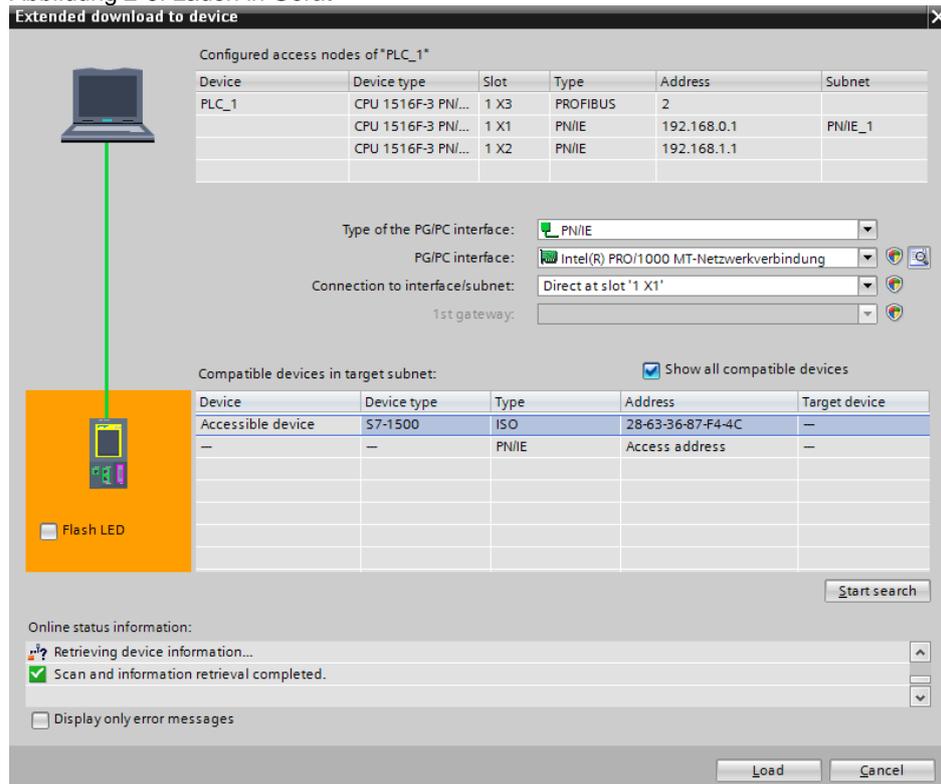
IP-Adresse: 192.168.0.30

Subnetz-Maske: 255.255.255.0

2.3.2 S7-Projekt in die CPU S7-1516F laden

1. Öffnen Sie "TIA Portal V14".
2. Wechseln Sie in die Projektansicht.
3. Klicken Sie in der Menüleiste im TIA Portal auf "Projekt > Öffnen" ("Project > Open").
4. Klicken Sie "Durchsuchen" ("Browse") und öffnen Sie das entpackte Projekt.
5. Stellen Sie die CPU S7-1516F auf STOP.
6. Klicken Sie mit der rechten Maustaste im Projektbaum auf "PLC_1 [CPU1516F-3 PN/DP]" und dann auf "Laden in Gerät > Hardware und Software (nur Änderungen)" ("Download to device > Hardware and Software (only changes)").
7. Wählen Sie die jeweilige Schnittstelle aus und klicken Sie auf "Suche starten" ("Start search").

Abbildung 2-6: Laden in Gerät



- Wählen Sie die CPU anhand der Adresse aus und klicken Sie anschließend auf "Laden" ("Load").

Hinweis

Die IP-Adresse und der Gerätenamen werden beim Laden des Projekts in die CPU automatisch zugewiesen.

- Bestätigen Sie den nächsten Dialog, indem Sie auf "Laden" ("Load") klicken.
- Klicken Sie auf "Fertig" ("Finish"), wenn der Ladevorgang abgeschlossen ist.

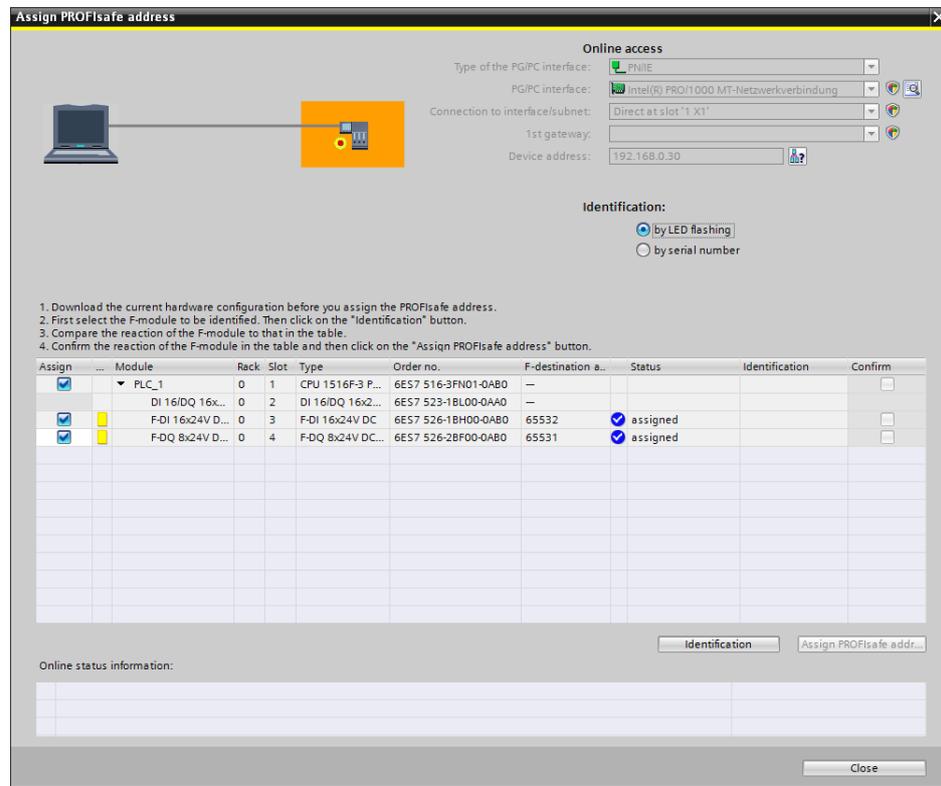
2.3.3 PROFIsafe-Adressen zuweisen

Um die sichere Kommunikation zwischen der F-CPU und den fehlersicheren Modulen zu realisieren, müssen den Modulen noch PROFIsafe-Adressen zugewiesen werden.

Hinweis Da die PROFIsafe-Adresse in dem elektronischen Kodierelement gespeichert wird, sind die nachfolgenden Schritte nur dann notwendig, wenn dem Kodierelement zuvor noch keine oder eine andere PROFIsafe-Adressen zugewiesen wurde.

1. Öffnen Sie "Geräte & Netze" ("Devices & networks") aus dem Projektbaum.
2. Klicken Sie mit der rechten Maustaste auf die F-CPU und wählen Sie die Aktion "PROFIsafe-Adresse zuweisen" ("Assign PROFIsafe address").
3. Aktivieren Sie das Kontrollkästchen des ersten fehlersicheren Moduls und klicken Sie auf die Schaltfläche "Identifikation" ("Identification").
4. Wenn die LEDs der F-DI gleichzeitig im Sekundentakt grün blinken, aktivieren Sie das Kontrollkästchen "Bestätigen" ("Confirm").
5. Klicken Sie anschließend auf die Schaltfläche "PROFIsafe-Adresse zuweisen" ("Assign PROFIsafe address") und bestätigen Sie den Dialog mit "Ja".

Abbildung 2-7: PROFIsafe-Adressen zuweisen



6. Wiederholen Sie die Schritte für die weiteren fehlersicheren Module.
7. Anschließend können Sie das Fenster schließen.

Hinweis Alle roten LEDs der F-Baugruppen sollten nach der Zuweisung der PROFIsafe-Adresse erlöschen. Ist dies nicht der Fall, liegt womöglich ein Fehler in der Verdrahtung vor.

8. Stellen Sie die CPU S7-1516F nun auf RUN.

2.4 Bedienung

Nachfolgende Tabelle demonstriert die Funktionsweise:

Tabelle 2-1: Bedienungsanleitung

	Aktion	Ergebnis / Hinweis
1.	Drücken Sie den Quittiertaster	Quittierung
2.	Drücken Sie den Starttaster	Schütze schalten ein
3.	Drücken Sie den Stopptaster	Schütze schalten ab
4.	Drücken Sie den Starttaster	Schütze schalten ein
5.	Drücken Sie den Not-Halt	Schütze schalten ab
6.	Entriegeln Sie den Not-Halt	
7.	Wiederholen sie die Aktionen 1 und 2	Schütze schalten ein

3 Wissenswertes

3.1 Grundlagen

3.1.1 Grundbegriffe

Querschluss

Die Querschlusserkennung ist eine Diagnosefunktion eines Auswertegerätes, wodurch Kurz- bzw. Querschlüsse zwischen zwei Eingangskanälen (Sensorkreisen) erkannt werden.

Ein Querschluss kann beispielsweise durch das Quetschen einer Mantelleitung entstehen. Ohne Querschlusserkennung würde dies zur Folge haben, dass z. B. eine zweikanalige Not-Halt-Schaltung auch bei nur einem fehlerhaften Öffnerkontakt (Zweitfehler) keine Abschaltung auslöst.

Rückführkreis

Ein Rückführkreis dient der Überwachung angesteuerter Aktoren (z. B. Relais oder Lastschütze) mit zwangsgeführten Kontakten bzw. Spiegelkontakten. Die Ausgänge können nur bei geschlossenem Rückführkreis aktiviert werden. Bei Verwendung eines redundanten Abschaltpfades muss der Rückführkreis beider Aktoren ausgewertet werden. Diese dürfen dafür auch in Reihe geschaltet werden.

Zwangsöffnung

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

Zwangsgeführte Kontakte

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

3.1.2 Funktionale Sicherheit

Die Sicherheit ist aus Sicht des zu schützenden Gutes unteilbar. Da die Ursachen von Gefährdungen und damit auch die technischen Maßnahmen zu ihrer Vermeidung aber sehr unterschiedlich sein können, unterscheidet man verschiedene Arten der Sicherheit, z. B. durch Angabe der jeweiligen Ursache möglicher Gefährdungen. So spricht man von "elektrischer Sicherheit", wenn der Schutz vor den Gefährdungen durch die Elektrizität zum Ausdruck gebracht werden soll, oder von "funktionaler Sicherheit", wenn die Sicherheit von der korrekten Funktion abhängt.

Um funktionale Sicherheit einer Maschine oder Anlage zu erreichen, ist es notwendig, dass die sicherheitsrelevanten Teile der Schutzeinrichtungen und Steuereinrichtungen korrekt funktionieren und sich im Fehlerfall so verhalten, dass die Anlage in einem sicheren Zustand bleibt oder in einen sicheren Zustand gebracht wird.

Dazu ist die Verwendung besonders qualifizierter Technik notwendig, die den in den betreffenden Normen beschriebenen Anforderungen genügt. Die Anforderungen zur Erzielung funktionaler Sicherheit basieren auf den folgenden grundlegenden Zielen:

- Vermeidung systematischer Fehler
- Beherrschung systematischer Fehler
- Beherrschung zufälliger Fehler oder Ausfälle

Das Maß für die erreichte funktionale Sicherheit ist die Wahrscheinlichkeit gefährlicher Ausfälle, die Fehlertoleranz und die Qualität, durch die die Freiheit von systematischen Fehlern gewährleistet werden soll. Es wird in den Normen durch unterschiedliche Begriffe ausgedrückt:

- In IEC 62061: "Safety Integrity Level" (SIL)
- In ISO 13849-1: "Performance Level" (PL)

Mehr Informationen zu Funktionaler Sicherheit finden Sie unter [\8\](#).

3.1.3 Not-Halt

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

Einrichtungen, funktionelle Aspekte und Gestaltungsleitsätze zum Not-Halt sind in der EN ISO 13850 hinterlegt. Zusätzlich ist noch die Norm EN 60204-1 zu beachten.

Typische Anwendung

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

Hinweis

Not-Halt ist kein Mittel zur Risikominderung. Not-Halt ist eine "ergänzende Sicherheitsfunktion" (Wenn "Not-Halt" betätigt wird, muss der Motor ausgeschaltet werden).

Unbeabsichtigte Betätigung

Häufig besteht die Anforderung, ein Not-Halt-Befehlsgerät vor unbeabsichtigter Betätigung zu schützen und so die Anlagenverfügbarkeit zu erhöhen. Der erste Schritt ist die richtige Platzierung des Not-Halt-Befehlsgeräts an der Maschine. Das Not-Halt-Befehlsgerät muss leicht zugänglich, ungehindert erreichbar und gefahrlos zu betätigen sein.

Zusätzlich gibt es die Möglichkeit, einen Schutzkragen zum Schutz vor unbeabsichtigter Betätigung zu verwenden. Auch hierbei ist darauf zu achten, dass eine ungehinderte Erreichbarkeit gewährleistet ist.

Hinweis

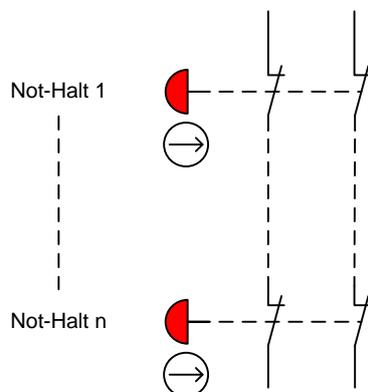
Die SIEMENS SIRIUS Not-Halt-Befehlsgeräte mit Schutzkragen entsprechen den Anforderungen der EN ISO 13850 "Sicherheit von Maschinen - Not-Halt - Gestaltungsleitsätze".

Spezielle Anforderungen an Schutzkragen existieren bisher noch nicht, da diese in keiner Norm zur Funktionalen Sicherheit explizit erwähnt werden. Es liegt häufig im Ermessen des Gutachters diese für eine bestimmte Maschine zu akzeptieren.

Bedingungen bei Reihenschaltung

Not-Halt-Befehlsgeräte dürfen bis PL e (nach ISO 13849-1) bzw. SIL 3 (nach IEC 62061) nur dann in Reihe geschaltet werden, wenn das Versagen und gleichzeitige Drücken der Not-Halt-Befehlsgeräte ausgeschlossen werden kann. Weitere Informationen hierzu finden Sie unter [19](#).

Abbildung 3-1: Reihenschaltung von Not-Halt-Befehlsgeräten



Wenn mehrere Not-Halt-Befehlsgeräte elektrisch in Reihe geschaltet sind, dann stellt jedes sicherheitsgerichtete Abschalten über ein Not-Halt-Befehlsgerät eine einzelne ergänzende Sicherheitsfunktion dar. Wenn baugleiche Not-Halt-Befehlsgeräte verwendet werden, dann reicht es, exemplarisch eine ergänzende Sicherheitsfunktion stellvertretend für alle ergänzenden Sicherheitsfunktionen zu betrachten. Weitere Informationen hierzu finden Sie unter [16](#).

3.2 Bewertung der Sicherheitsfunktion

3.2.1 Normen

Zur Bewertung der Sicherheitsfunktion wurden folgende Fassungen der Normen herangezogen:

Tabelle 3-1: Normen

Fassung	Nachfolgend genannt
EN ISO 13849-1:2015	ISO 13849-1
EN ISO 13849-2:2012	ISO 13849-2
EN 62061:2005/A2:2015	IEC 62061

3.2.2 Sicherheitsfunktion

Vorbemerkung

- Not-Halt ist kein Mittel zur Risikominderung.
- Not-Halt ist eine "ergänzende Sicherheitsfunktion".

Ergänzende Sicherheitsfunktion

Für die folgenden Betrachtungen wird die folgende ergänzende Sicherheitsfunktion zu Grunde gelegt:

Tabelle 3-2: Beschreibung der Sicherheitsfunktion

Sicherheitsfunktion	Beschreibung
SF1	Wenn der Not-Halt betätigt wird, muss die Maschine sicher abschalten.

Im Folgenden wird die Sicherheitsfunktion SF1 nach den Normen ISO 13849-1, ISO 13849-2 und IEC 62061 bewertet.

3.2.3 Bewertung nach ISO 13849-1

Nachfolgend wird eine Bewertung nach ISO 13849-1 mit dem Safety Evaluation Tool (SET) durchgeführt. Den Link zum SET finden Sie im Internet unter [4](#).

Bewertung "Erfassen"

Die zur Bewertung relevanten Parameter werden vom Hersteller geliefert und vom Anwender festgelegt.

Tabelle 3-3: Parameter Teilsystem "Erfassen"

Parameter	Wert	Begründung	Festlegung
B10 B10-Wert Not-Halt Befehlsgerät	100.000	Herstellerangabe	SIEMENS AG
Anteil gefährbringender Ausfälle Not-Halt Befehlsgerät	0,2 (20%)	Herstellerangabe	
T1 Gebrauchsdauer	175.200 h (20 Jahre)	Herstellerangabe	
Architektur	Kategorie 4	2 Kanäle, 1 Komponente	Anwender
Betätigungen/ Testintervall	1/Woche	Annahme	
CCF-Maßnahmen (Punkte) Anfälligkeit gegenüber Ausfällen in Folge gemeinsamer Ursache	≥ 65	Ausreichende Maßnahmen gegen CCF nach ISO 13849-1 Tabelle F.1 müssen getroffen werden	
DC Diagnosendeckungsgrad	≥ 0,99 (99%)	Kreuzvergleich in F-DI	

Tabelle 3-4: Ergebnis Teilsystem "Erfassen"

PFH _D	Erreichter PL
$2,47 \cdot 10^{-8}$	PL e

Bewertung "Auswerten"

Die zur Bewertung relevanten Parameter werden vom Hersteller geliefert und sind im SET verfügbar:

Tabelle 3-5: Berechnung Teilsystem "Auswerten"

Komponente	PFH _b	PL	Festlegung
CPU 1516F-3PN/DP inkl. PROFIsafe	$2,00 \cdot 10^{-9}$	PL e	SIEMENS AG
ET 200MP F-DI	$1,00 \cdot 10^{-9}$	PL e	
ET 200MP F-DQ	$2,00 \cdot 10^{-9}$	PL e	
Gesamt	$5,00 \cdot 10^{-9}$	PL e	

Bewertung "Reagieren"

Die zur Bewertung relevanten Parameter der Schütze werden vom Hersteller geliefert und vom Anwender festgelegt.

Tabelle 3-6: Parameter Teilsystem "Reagieren"

Parameter	Wert	Begründung	Festlegung
B10 B10-Wert Schütz	1.000.000	Herstellerangabe	SIEMENS AG
Anteil gefährdender Ausfälle Schütz	0,73 (73%)	Herstellerangabe	
T1 Gebrauchsdauer	175.000 h (20 Jahre)	Herstellerangabe	
Architektur	Kategorie 4	2 Kanäle, 2 Komponenten	Anwender
Betätigungen/ Testintervall	1/h	Annahme	
CCF-Maßnahmen (Punkte) Anfälligkeit gegenüber Ausfällen in Folge gemeinsamer Ursache	≥ 65	Ausreichende Maßnahmen gegen CCF nach ISO 13849-1 Tabelle F.1 müssen getroffen werden	
DC Diagnosedeckungsgrad	≥ 0,99 (99%)	Redundanter Abschaltpfad und dynamische Überwachung der Schütze	

Tabelle 3-7: Ergebnis Teilsystem "Reagieren"

PFH _b	Erreichter PL
$2,47 \cdot 10^{-8}$	PL e

Ergebnis der Bewertung nach ISO 13849-1

Tabelle 3-8: Ergebnis der Bewertung nach ISO 13849-1

Teilsystem	PFH _D	Erreichter PL
Erfassen	$2,47 \cdot 10^{-8}$	PL e
Auswerten	$5,00 \cdot 10^{-9}$	PL e
Reagieren	$2,47 \cdot 10^{-8}$	PL e
Gesamt	$5,44 \cdot 10^{-8}$	PL e
		PL e

3.2.4 Bewertung nach IEC 62061

Nachfolgend wird eine Bewertung nach IEC 62061 mit dem Safety Evaluation Tool (SET) durchgeführt. Den Link zum SET finden Sie im Internet unter [4](#).

Bewertung "Erfassen"

Die zur Bewertung relevanten Parameter werden vom Hersteller geliefert und vom Anwender festgelegt.

Tabelle 3-9: Parameter Teilsystem "Erfassen"

Parameter	Wert	Begründung	Festlegung
B10 B10-Wert Not-Halt Befehlsgerät	100.000	Herstellerangabe	SIEMENS AG
Anteil gefährbringender Ausfälle Not-Halt Befehlsgerät	0,2 (20%)	Herstellerangabe	
T1 Gebrauchsdauer	175.200 h (20 Jahre)	Herstellerangabe	
Teilsystemarchitektur	D	2 Kanäle, 1 Komponente: Einfehlertoleranz mit Diagnosefunktion	Anwender
Betätigungen/ Testintervall	1/Woche	Annahme	
β (CCF-Faktor) Anfälligkeit gegenüber Ausfällen in Folge gemeinsamer Ursache	0,1 (10%)	Bei Installation nach IEC 62061 wird ein CCF- Faktor von 0,1 (10%) erreicht.	
DC Diagnosedeckungsgrad	≥ 0,99 (99%)	Kreuzvergleich in F-DI	

Ergebnis "Erfassen"

Tabelle 3-10: Ergebnis Teilsystem "Erfassen"

PFH _D	Erreichter SILCL
$1,19 \cdot 10^{-10}$	SILCL 3

Bewertung "Auswerten"

Die zur Bewertung relevanten Parameter werden vom Hersteller geliefert und sind im SET verfügbar:

Tabelle 3-11: Berechnung Teilsystem "Auswerten"

Komponente	PFH _D	SILCL	Festlegung
CPU 1516F-3PN/DP inkl. PROFI-safe	$2,00 \cdot 10^{-9}$	SILCL 3	SIEMENS AG
ET 200MP F-DI	$1,00 \cdot 10^{-9}$	SILCL 3	
ET 200MP F-DQ	$2,00 \cdot 10^{-9}$	SILCL 3	
Gesamt	$5,00 \cdot 10^{-9}$	SILCL 3	

Bewertung "Reagieren"

Die zur Bewertung relevanten Parameter der Schütze werden vom Hersteller geliefert und vom Anwender festgelegt.

Tabelle 3-12: Parameter Teilsystem "Reagieren"

Parameter	Wert	Begründung	Festlegung
B10 B10-Wert Schütz	1.000.000	Herstellerangabe	SIEMENS AG
Anteil gefährbringender Ausfälle Schütz	0,73 (73%)	Herstellerangabe	
T1 Gebrauchsdauer	175.000 h (20 Jahre)	Herstellerangabe	
Teilsystemarchitektur	D	2 Kanäle, 2 Komponenten: Einfehlertolanz mit Diagnosefunktion	Anwender
Betätigungen/ Testintervall	1/h	Annahme	
β (CCF-Faktor) Anfälligkeit gegenüber Ausfällen in Folge gemeinsamer Ursache	0,1 (10%)	Bei Installation nach IEC 62061 wird ein CCF- Faktor von 0,1 (10%) erreicht.	
DC Diagnosedeckungsgrad	≥ 0,99 (99%)	Redundanter Abschaltpfad und dynamische Überwachung der Schütze	

Tabelle 3-13: Erebnis Teilsystem "Reagieren"

PFH _D	Erreichter SILCL
$7,30 \cdot 10^{-9}$	SILCL 3

Ergebnis der Bewertung nach IEC 62061

Tabelle 3-14: Ergebnis der Bewertung nach IEC 62061

Teilsystem	PFH _D	Erreichter SIL
Erfassen	$1,19 \cdot 10^{-10}$	SILCL 3
Auswerten	$5,00 \cdot 10^{-9}$	SILCL 3
Reagieren	$7,30 \cdot 10^{-9}$	SILCL 3
Gesamt	$1,24 \cdot 10^{-8}$	SILCL 3
		SIL 3

4 Anhang

4.1 Service und Support

Industry Online Support

Sie haben Fragen oder brauchen Unterstützung?

Über den Industry Online Support greifen Sie rund um die Uhr auf das gesamte Service und Support Know-how sowie auf unsere Dienstleistungen zu.

Der Industry Online Support ist die zentrale Adresse für Informationen zu unseren Produkten, Lösungen und Services.

Produktinformationen, Handbücher, Downloads, FAQs und Anwendungsbeispiele – alle Informationen sind mit wenigen Mausklicks erreichbar:

<https://support.industry.siemens.com/>

Technical Support

Der Technical Support von Siemens Industry unterstützt Sie schnell und kompetent bei allen technischen Anfragen mit einer Vielzahl maßgeschneiderter Angebote – von der Basisunterstützung bis hin zu individuellen Supportverträgen.

Anfragen an den Technical Support stellen Sie per Web-Formular:

www.siemens.de/industry/supportrequest

Serviceangebot

Unser Serviceangebot umfasst u. a. folgende Services:

- Produkttrainings
- Plant Data Services
- Ersatzteilservices
- Reparaturservices
- Vor-Ort und Instandhaltungsservices
- Retrofit- und Modernisierungsservices
- Serviceprogramme und Verträge

Ausführliche Informationen zu unserem Serviceangebot finden Sie im Servicekatalog:

<https://support.industry.siemens.com/cs/sc>

Industry Online Support App

Mit der App "Siemens Industry Online Support" erhalten Sie auch unterwegs die optimale Unterstützung. Die App ist für Apple iOS, Android und Windows Phone verfügbar.

<https://support.industry.siemens.com/cs/ww/de/sc/2067>

4.2 Links und Literatur

Tabelle 4-1

	Thema
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link auf den Beitrag https://support.industry.siemens.com/cs/ww/de/view/21064024
\3\	Anwendungsbeispiel "Rückführkreis" https://support.industry.siemens.com/cs/ww/de/view/21331098
\4\	Safety Evaluation Tool (SET) http://siemens.com/safety-evaluation-tool
\5\	SIMATIC Safety - Projektieren und Programmieren https://support.industry.siemens.com/cs/ww/de/view/54110126
\6\	Reihenschaltung mehrerer Not-Halt-Befehlsgeräte https://support.industry.siemens.com/cs/ww/de/view/35444028
\7\	Migration eines Sicherheitsprogramms auf TIA Portal https://support.industry.siemens.com/cs/ww/de/view/109475826
\8\	Funktionale Sicherheit bei Siemens www.siemens.de/safety-integrated
\9\	Festzulegender Diagnosedeckungsgrad für Teilsysteme mit elektronischen Komponenten https://support.industry.siemens.com/cs/ww/de/view/35444114

4.3 Änderungsdokumentation

Tabelle 4-2

Version	Datum	Änderung
V1.0	02/2005	Erste Ausgabe
V2.0	09/2007	Aktualisierung der Inhalte bezüglich: <ul style="list-style-type: none"> • Hardware und Software • Leistungsdaten • Screenshots
		Neues Kapitel: <ul style="list-style-type: none"> • Bewertung des Funktionsbeispiels nach den neuen Normen EN 62061 und EN ISO 13849-1:2006.
V3.0	01/2015	Migration von STEP 7 V5.4 mit Distributed Safety auf TIA Portal (STEP 7 Professional V13 mit STEP 7 Safety V13)
V4.0	07/2015	<ul style="list-style-type: none"> • Veröffentlichung der Migrationsanleitung als eigenes Anwendungsbeispiel • Austausch des Leuchtmelders zur Simulation der Aktorik gegen zwei Schütze • Ergänzung der Bewertung der Sicherheitsfunktion um das Teilsystem "Reagieren"
V5.0	01/2017	<ul style="list-style-type: none"> • Hochrüsten auf TIA Portal V14 • Austausch der dezentralen Peripherie durch zentrale Baugruppen