SafetySim

HINWEISE ZUM LERNBAUSTEIN FÜR AUSZUBILDENDE

INHALTSVERZEICHNIS

1. Allgemeines

Im Rahmen des Forschungsprojektes SafetySim soll anhand eines ersten Unterrichts der praktische Einsatz des Simulationssystems getestet werden.

2. Generelle Voraussetzungen

Für die praktische Anwendung müssen grundsätzliche Kenntnisse zu Siemens S7-Steuerungen vorhanden sein. Gleiches gilt für den Einsatz und die Nutzung des Totally Integrated Automation Portals (TIA).

3. Zeitplan

Es ist folgender zeitlicher Ablauf vorgesehen:

- 45 Min. Einführung sowie Hinweise zur Maschinenrichtlinie 2006/42/EG
- 180 Min. Praktische Anwendung des Simulationssystems im Labor
- 45 Min. Abschlussbesprechung

4. Aufgabenstellung zur praktischen Anwendung

Mithilfe des Simulationssystems soll ermittelt werden, wie und wodurch ein Sicherheitsgewinn für elektrische Steuerungen zu erreichen ist, wenn diese einem höheren Sicherheitsintegritäts-Level (SIL) entsprechen.

Dazu sind zunächst die sicherheitsrelevanten Funktionen, insbesondere beim Auftreten von Fehlern, einer Motorsteuerung mit Not-Halt-Taster, die SIL 1 entspricht, zu analysieren und zu erproben. Anschließend ist das vorhandene Programm so abzuändern, dass die gesamte Steuerung dem Sicherheits-Integritätslevel SIL 3 entspricht und mithilfe des Simulationssystems dessen Grundfunktionen zu testen. Darüber hinaus sollen anhand der Simulation möglicher Fehler die verbesserten Sicherheitsfunktionen erkannt und bestätigt werden.

5. Motorsteuerung nach SIL 1

Die Steuerung besteht aus realer Hardware (S7-System) und durch SafetySim nachgebildeten und verschalteten Sensoren bzw. Aktoren. Bei Letzteren handelt es sich um die Bedienelemente, das Motorschütz und den Motor.

5.1 Sicherheitsfunktionen entsprechend SIL 1

Diese Funktionen werden hard- und softwareseitig im Wesentlichen durch den Not-Halt-Taster (eStop) und ein Rückmeldesignal des Motorschützes (readbackK1) realisiert. Die generelle Sicherheitsfunktion lautet:

- Bei Drücken des Not-Halts wird der Aktor sicher abgeschaltet.

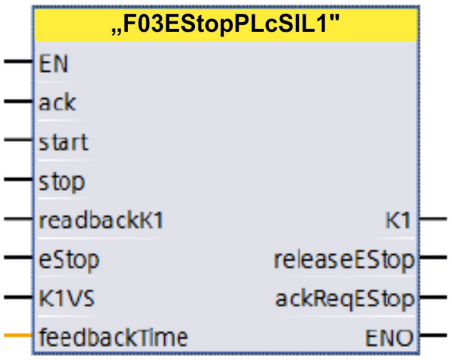
5.2 Funktionsbaustein „F03EStopSIL1PLc“

Wesentliche Elemente zur Erstellung von sicherheitsrelevanten S-SPS-Programmen mit dem Siemens S7-Steuerungssystem sind spezielle F-Anwender-Funktionsbausteine. Für die vorhandene Motorsteuerung ist der Baustein „F03EStopSIL1PLc“ von besonderer Bedeutung.

Um SIL1 zu entsprechen, müssen die beiden Sicherheitselemete „nur“ einkanalig ausgeführt werden.

Dabei handelt es sich um TÜV-zertifizierte Komponenten, die beispielsweise als Kopiervorlagen im Rahmen einer Baustein-Bibliothek zur Verfügung stehen.

Im SafetySim liegt diese Bibliothek unter:
C:\Users\SafetySim\Documents\S7_1200F_LIB_V14_V15.1.



Er verfügt über die links stehenden Ein- sowie die rechts stehenden Ausgänge. Die Eingänge „ack“, „start“, „stop“ und „estop“ stehen über die S7-Eingangsbaugruppe direkt mit den Bedienelementen S1 bis S4 in Verbindung.

Bei „readbackK1“ handelt es sich um eine Rückmeldung über den Schaltzustand von Schütz K1.

An „K1VS“ liegt der sogenannte Wertstatus an. Als „feedbacktime“ ist ein Zeitwert, z. B. 100 ms, angegeben. Der Ausgang „K1“ steht direkt über die Ausgangsbaugruppe mit dem Motorschütz K1 in Verbindung.
„releaseEStop“ stellt intern Informationen über die Entriegelung des Not-Halt-Tasters sowie eine erfolgte Quittierung zur Verfügung. „ackReqEStop“ gibt an, ob eine Quittierung des Not-Halt-Tasters erforderlich ist oder nicht. „ENO“ spielt in der gezeigten Anwendung keine Rolle.

5.3 Simulation der Motorsteuerung mittels SafetySim

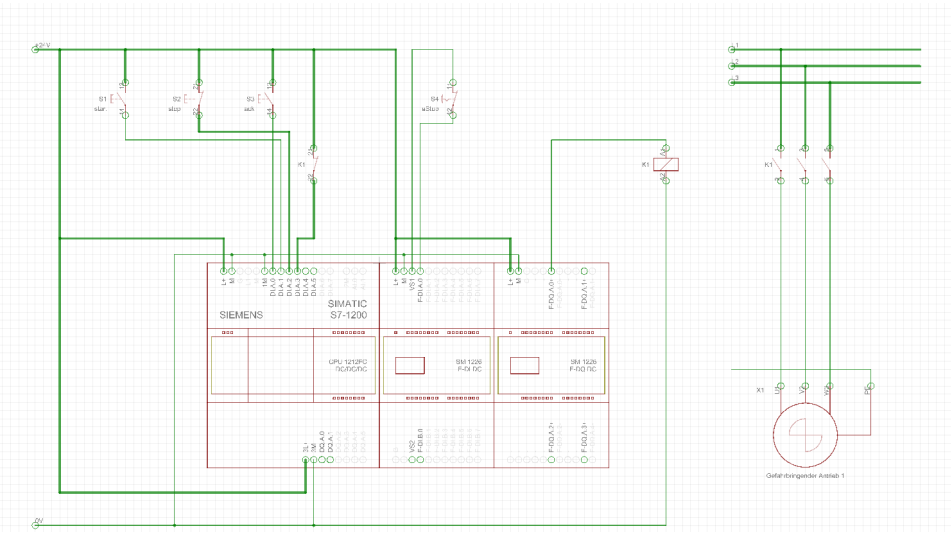
5.3.1 Voraussetzungen

Um die Simulation durchführen zu können, müssen folgende Bedingungen gegeben sein:

- Das Simulationssystem SafetySim wurde gestartet und die Scene „NOT-Halt in PL c/SIL 1“ aufgerufen.
- Das Programm „ProjectSIL1_V15.1“ befindet sich in der S-SPS.

5.3.2 Schaltplan

Mit dem Start obiger Scene in SafetySim erscheint der zugehörige Schaltplan:



Die dargestellten Sensoren (S1 bis S4) lassen sich hier mithilfe der Maus „bedienen“.

Der Not-Halt-Taster (S4) rastet nach einer Betätigung ein und muss durch erneute Betätigung gezielt wieder zurückgesetzt werden. Der Eingang „ack“ (Taster S3) dient dazu, eine Not-Halt-Auslösung (S4) oder einen möglichen Rücklesefehler der Schütz-Hilfskontakte zu quittieren.

readbackK1: Mithilfe dieser Meldung kann steuerungsintern überprüft werden, ob das Schütz auch tatsächlich den vorgegebenen Ansteuerungssignalen folgt. Auf diese Weise ist es u. U. möglich, auftretende Fehler zu erkennen. Da es sich bei dem Kontakt um einen Öffner handelt, kann das abgefallenen Schütz, das heißt ein nicht eingeschalteter Motor, sicher erkannt werden.

Der Wertstatus bezieht sich auf den Ausgang K1 und ist gleich „0“ im Falle eines Fehlers.
feedbacktime: Innerhalb der Zeit muss nach Ansteuerung des Schützes K1 über „readbackK1“ eine positive Rückmeldung gegeben werden, das heißt, dass kontrolliert wird, ob das Schütz auch tatsächlich angezogen hat.

releaseEStop: Das Ausgangssignal ist 1, wenn der Not-Halt-Taster entriegelt ist und eine Quittierung („ack“) durchgeführt wurde.

ackReqEStop: Der Ausgang ist 1, wenn eine Quittierung über S3 notwendig ist. Das ist immer dann der Fall, wenn zuvor der Not-Halt-Taster betätigt wurde oder ein anderer Fehler vorlag.

Es ist wichtig, dass hier der „EN“-Eingang nicht beschaltet werden darf!

5.3.3 Betriebszustände

Um den Motor erstmalig einschalten zu können, müssen
- der Not-Halt- und der Stop-Taster sowie der Rückmeldekontakt des Schützes K1 geschlossen sein,
- der Quittier-Taster (S3) kurzzeitig geschlossen und
- der Start-Taster kurz betätigt werden.

Sind die Einschaltbedingungen erfüllt, schließen die Haupt-Kontakte des Schützes K1 dauerhaft und der Motor beginnt sich zu drehen. Gleichzeitig wird der Hilfskontakt des Schützes geöffnet.

Der Motor kann stillgesetzt werden durch die Betätigung
- des Stop-Tasters (Betriebsstopp) oder
- des Not-Halt-Tasters (Not-Halt).

Nach einem regulären Betriebsstopp lässt sich der Motor mithilfe des Start-Tasters sofort wieder einschalten. Nach einem Not-Halt ist zuvor der Not-Halt-Taster zu entriegeln und der Quittier-Taster kurzzeitig zu betätigen.

5.3.4 Fehlfunktionen simulieren

Die Wirksamkeit von Sicherheitsfunktionen kann man am besten beurteilen, wenn Fehler auftreten. Von daher sollen für obige Steuerung drei gängige Probleme betrachtet werden.

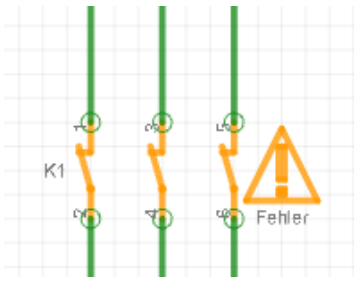
5.3.4.1 Verschweißung

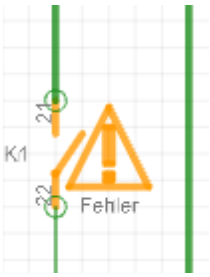
Um im SafetySim einen solchen Fehler zu simulieren, muss man mit dem Mauszeiger auf die Schützkontakte gehen und einen kurzen Klick mit der rechten Maustaste durchführen. Jetzt erscheint rechts oben auf dem Bildschirm ein Auswahlmenü.

Das enthält drei Möglichkeiten:
- Verschweißung
- Unterbrechung
- Fehleraufhebung (None)

Eine **Kontaktverschweißung** kann u. a. bei Schützen auftreten, z. B. wenn über die Kontakte ein zu hoher Strom fließt. Es soll hier davon ausgegangen werden, dass alle Kontakte gleichzeitig betroffen sind. Das heißt, die Motorkontakte bleiben geschlossen und der Hilfskontakt geöffnet.

Mithilfe der Maus auf „Verschweißung“ gehen und einmal klicken. Eine solche „Verschweißung“ betrifft automatisch immer das gesamte Schütz und nicht nur ein einzelnes Kontaktpaar. Zur besseren Kenntlichmachung werden die Motor-Kontakte gelb eingefärbt. Sie bleiben geschlossen und es wird ein Hinweis auf einen Fehler gegeben. Ähnlich sieht es bei dem Hilfskontakt aus. Er bleibt geöffnet.





Man stellt fest, dass trotz des Fehlers der Motor weiterläuft und nicht mehr abschaltbar ist, weder durch den Not-Halt- noch den Stop-Taster. Ein Stillstand des Antriebs wäre nur durch eine generelle Spannungsabschaltung (Hauptschalter) erreichbar. Würde dann die Spannung, ohne den Fehler zu beseitigen, wieder eingeschaltet, so würde der Motor sofort wieder anlaufen. Die Aufhebung des erzeugten Fehlers wird dadurch erreicht, dass man mit der Maus erneut auf die entsprechenden Kontakte geht, mit der rechten Maustast klickt, damit das Fehlermenü aufruft und dort auf „None“ klickt. Die gelbe Einfärbung wird zurückgenommen, das Fehlersymbol verschwindet und das Schütz ist wieder im Normalzustand.

5.3.4.2 Unterbrechung

Um im SafetySim einen solchen Fehler zu simulieren, beispielsweise am Not-Halt-Taster, muss man, ähnlich wie oben beschrieben, mit dem Mauszeiger auf die Tasterkontakte gehen und einen kurzen Klick mit der rechten Maustaste durchführen. Im erscheinenden Menü ist natürlich „Unterbrechung“ zu wählen. Das Schütz fällt sofort ab und der Motor bleibt stehen. Ein Wiedereinschalten ist nicht mehr möglich. Zur Beseitigung des Fehlers ist wie oben beschrieben vorzugehen.

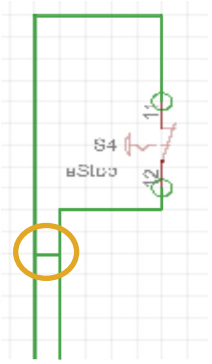
5.3.4.3 Kurzschluss

Um einen derartigen Fehler im SafetySim zu erzeugen, beispielsweise zwischen den beiden Anschlusspunkten (S4, 11/12) des Not-Halt-Tasters, muss man

- den Editor mithilfe der Maus anwählen

- einmal klicken
- in dem rechts oben erscheinenden Auswahlmenü auf den grünen Winkel gehen und einmal klicken

- mit der Maustaste zu der Stelle gehen, von der aus die Verbindung (Kurzschluss) erfolgen soll
- dort einmal klicken
- danach die Maus zu der Stelle führen, zu der die Verbindung (Kurz- bzw. Querschluss) hergestellt werden soll
- dort einmal klicken
- die Verbindung ist hergestellt.



Derartige Fehler können in der Praxis auf unterschiedlichste Weise zustande kommen.
Ein typisches Beispiel ist das Abbrechen eines Drahtes unmittelbar hinter einer Kontaktstelle, wenn z. B. beim Abisolieren die Adern verletzt wurden. Ähnliche Effekte sind möglich, wenn die Befestigungsschrauben für die Anschlussdrähte nicht oder nicht ordnungsgemäß angezogen wurden.

Kurz- oder Querschlüsse können in der Realität beispielsweise durch defekte Isolierungen in den Kabeln zustandekommen. Es ist aber bei der Verwendung von flexiblen Leitungen auch möglich, dass sie durch Aderreste, die aus unsachgemäßem Abisolieren resultieren, entstehen.

Wenn das Motorschütz angezogen war, d. h. der Motor läuft, fällt es sofort ab. Ein Wiedereinschalten ist nicht möglich. Das Problem wird steuerungsseitig intern in der S7-Eingangsbaugruppe erkannt und an die CPU weitergemeldet.

Zur Aufhebung dieses Fehlers muss man
- im Editor-Menü den Papierkorb anwählen (einmal klicken)
- mit der Maus zu der zu beseitigenden Stelle gehen (einmal klicken)
- die Verbindung bzw. der Kurzschluss ist wieder beseitigt

Vor einem möglichen Neustart muss zunächst der Editor durch Anwählen und einmaliges Klicken geschlossen werden.

5.4 Zusammenfassung

Eine Steuerung, die den Anforderungen nach SIL 1 bzw. PL c genügt, ist weniger zuverlässig als eine, die z. B. SIL 3 entspricht. Im vorliegenden Falle lässt sich das besonders gut daran erkennen, dass bei einer Verschweißung der Schütz-Kontakte der Motor trotz des Fehlers weiterläuft. Das darf bei einem höheren Sicherheitslevel nicht vorkommen.

6. Motorsteuerung nach SIL 3

6.1 Allgemeines

Ein wesentlicher Teil der Aufgabenstellung besteht darin, die Zuverlässigkeit der oben besprochenen Motorsteuerung zu erhöhen und diese in eine, die den Sicherheitsanforderungen von Level SIL 3 entspricht, umzuwandeln.

6.2 Änderung im Bereich der S7-S-SPS

Um den Sicherheits-Integritätslevel anzuheben, müssen im Bereich der S-SPS die Gerätekonfiguration sowie das Programm angepasst werden. Letzteres erfolgt im Wesentlichen durch den Einsatz eines speziellen F-Anwender-Funktionsbausteins.

6.2.1 Voraussetzungen

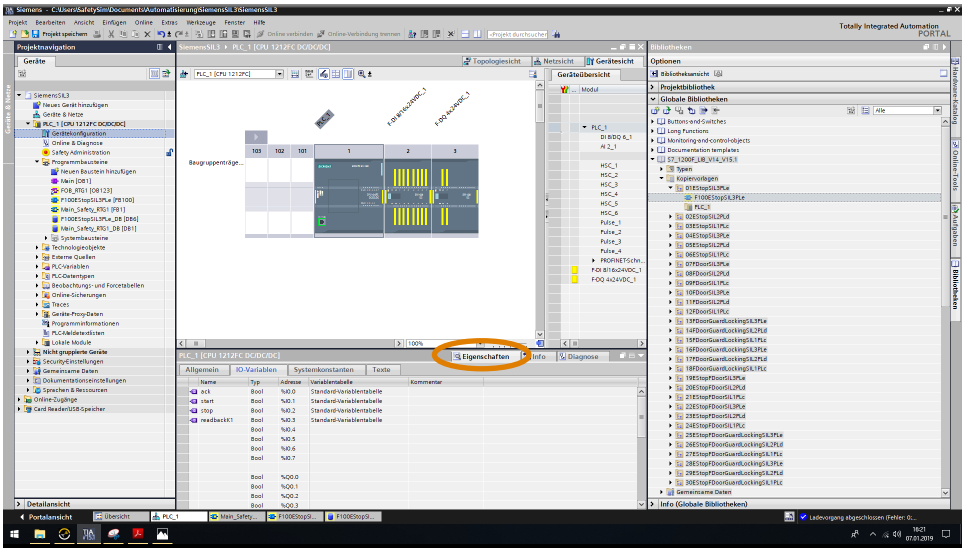
Zur Änderung müssen
- das TIA-Portal geöffnet,
- das Projekt „Siemens SIL1.ap15_1“ markiert,
- die Projektansicht gewählt,
- die CPU „PLC_1“ markiert und
- die Gerätekonfiguration geöffnet sein.

Elektrische und elektronische Systeme, die Sicherheitsfunktionen beinhalten, werden hinsichtlich deren Zuverlässigkeit in unterschiedliche Klassen eingeteilt. Je nach Ausgangsnorm unterscheidet man zwischen Performance Level PL und Sicherheits-Integritätslevel SIL. Letztere reichen von 1 bis 4 und die PL von a bis e. Dabei ist zum Beispiel SIL 3 vergleichbar mit PL e und SIL1 mit PL b bzw. PL c.

6.2.2 Gerätekonfiguration anpassen

Zur Erreichung des Sicherheitslevels SIL 3 sind u. a. zwei Motorschütze und ein zweikanaliger Not-Halt-Taster erforderlich. Von daher muss für die CPU zunächst der Rückmeldekontakt des zweiten Motorschützes ergänzt werden. Des Weiteren ist der zweite Kanal des Tasters an die Eingangsbaugruppe anzuschließen.

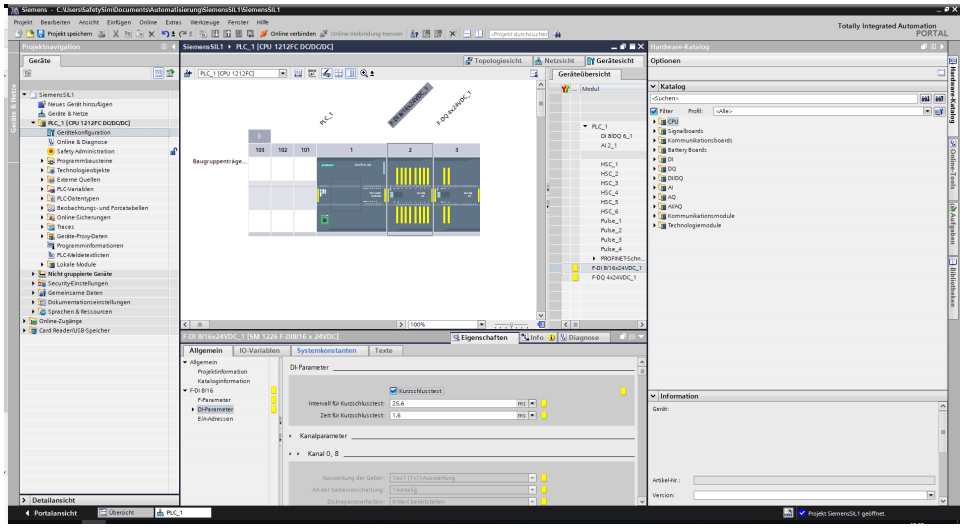
Wenn die obigen Voraussetzungen bezüglich des TIA-Portals korrekt erfüllt sind, sieht man den folgenden Bildschirm:



Das mittlere obere Fenster zeigt eine Abbildung des vorhandenen Steuerungssystems, in dem die CPU markiert ist. Nun muss im unteren mittleren Fenster der Reiter „Eigenschaften“ gewählt werden und in der nächst tieferen Ebene „IO-Variablen“. Dort ist bei Adresse „%IO.4“ „readbackK2“ einzutragen.

Anschließend ist die Konfiguration für den Eingangsbaustein zu ändern. Dazu muss dieser in der Gerätedarstellung angewählt werden. Eine mögliche Abfrage nach dem **Passwort für das Sicherheitsprogramm** ist grundsätzlich mit „siemens“ und „OK“ zu beantworten. Diese Frage kommt immer dann, wenn etwas geändert werden soll und das „Schloss“ im Bereich des Menüs links außen optisch noch geschlossen ist. Nach korrekter Beantwortung ist es geöffnet und zeigt an, dass Änderungen möglich sind.

Nach Anwahl des Eingangsbausteins ist es erforderlich, im unteren mittleren Fenster „Allgemein“ und dort „DI-Parameter“ zu wählen sowie da durch ein Häkchen den „Kurzschlusstest“ zu aktivieren.

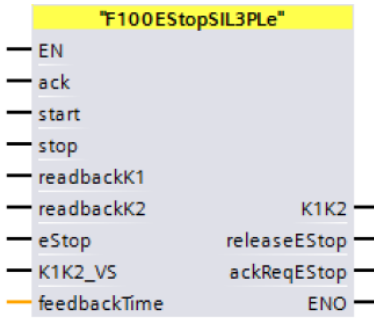


readbackK2: Mithilfe dieser Meldung kann steuerungsintern überprüft werden, ob das 2. Schütz auch tatsächlich den vorgegebenen Ansteuerungssignalen folgt. Auf diese Weise ist es u. U. möglich, auftretende Fehler zu erkennen. Da es sich bei dem Kontakt um einen Öffner handelt, kann das abgefallenen Schütz, das heißt ein nicht eingeschalteter Motor, sicher erkannt werden.

Jetzt muss der Kanal 8 ebenfalls aktiviert werden (zweiter Kanal des Not-Halt-Tasters). Anschließend ist in dem bereits benutzten Fenster nach oben zu scrollen zu „Kanal 0, 8“ und dort bei „Auswertung der Geber“ anstelle von „1oo1 (1v1)-Auswertung“ „1oo2 (2v2) Auswertung“ zu wählen. Dann im gleichen Fenster bei „Wiedereingliederung nach Diskrepanzfehler“ „Test 0-Signal erforderlich“ einstellen. Zum Schluss ist zu Kanal 0 zu scrollen und dort „Kanalfehler-Quittierung“ „Automatisch“ anstelle von „Manuell“ zu wählen. Die Einstellung auf „automatisch“ bedeutet, dass intern ein Kanalfehler, wenn er nicht mehr existent ist, selbstständig zurückgestellt wird. Die Anpassung der Gerätekonfiguration ist nun abgeschlossen.

6.2.3 Funktionsbaustein „F100EStopSIL3PLe“

Um den sicherheitsgerichteten Programmteil auf den Level SIL 3 zu bringen, spielt dieser Baustein neben der angepassten Gerätekonfiguration eine ganz entscheidende Rolle. Im Wesentlichen verfügt er über die gleichen Ein- und Ausgänge wie der oben bereits beschriebene „FB F03EStopSIL1PLc“. Um aber die für den Sicherheitslevel SIL 3 erforderliche zweikanalige Rückmeldung der Motorschütze realisieren zu können, besitzt er einen zweiten „readback“-Eingang, nämlich den für das Schütz K2 („readbackK2“).



6.2.4 Funktionsbaustein einbauen

Der Baustein steht als Kopiervorlage im Bereich der Globalen Bibliotheken in der Safety-Basic-Bibliothek. Man findet ihn, indem man einige Bibliotheks-Dateien öffnet
- Bibliotheken
- globalen Bibliotheken
- „S7_1200F_LIB_V14_V15.1“
- Kopiervorlagen
- „01EStopSIL3PLe“ (Bausteine für SIL 3)

Von dort ist er zu den Programmbausteinen der PLC_1 (Geräte) zu kopieren. Anschließend den Baustein in das mittlere Fenster (Netzwerk1) ziehen bzw. kopieren.

Die Frage nach der „Aufrufoption“ muss mit
- „automatisch“ und
- „OK“

beantwortet werden.

Jetzt muss er eingangs- und ausgangsseitig angeschlossen werden. Zu belegen sind zunächst „ack“, „start“, „stop“, „readbackK1“, „readbackK2“ „estop“, „K1K2_VS“ und „K1K2“. Dazu ist für den jeweiligen Anschluss
- auf „false“ zu klicken (doppelt),
- das erscheinende Listensymbol anzuwählen (Doppelklick),
- in der erscheinenden Liste den jeweils passenden Anschluss durch Doppelklick aussuchen (lilafarben, DI).

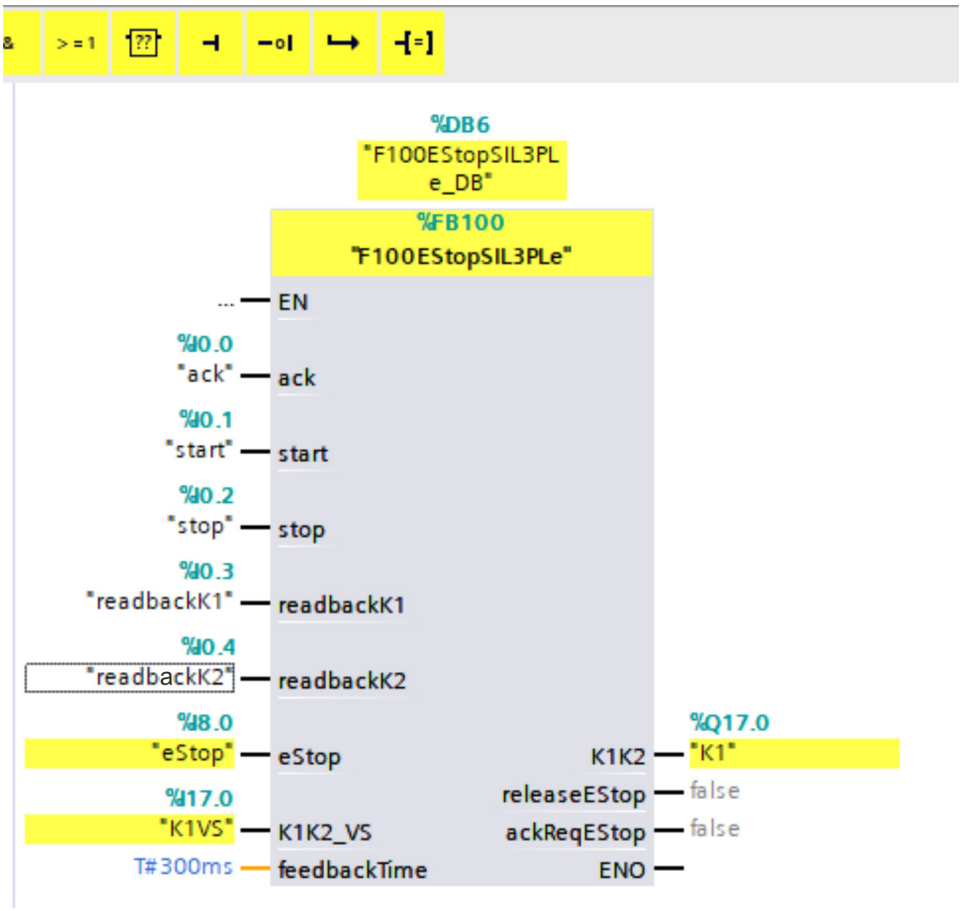
Danach erscheinen an dem gewählten Ein- bzw. Ausgang die ausgewählten Namen und Adressen.
In dieser Weise ist mit allen oben benannten Eingängen sowie dem Ausgang zu verfahren.

Die Bezeichnung „1oo1“ bedeutet sinngemäß, dass es sich um eine einkanalige Verarbeitung des Not-Halt-Tasters handelt. „1oo2“ steht für eine zweikanalige Ausführung mit redundanter Auswertung. Letztere ist zur Erreichung von SIL 3 erforderlich.

Wiedereingliederung nach Diskrepanzfehler: Das bedeutet, dass nach einem Diskrepanzfehler abgefragt wird, ob der Quittiertaster nicht bereits betätigt ist.

Bei „feedbackTime“ auf „T#0ms“ doppelklicken und in das Fenster den Wert „300“ eingeben.

Wenn der Baustein vollständig und korrekt angeschlossen wurde, muss sich folgendes Bild ergeben:



Jetzt kann der „alte“ Sicherheitsbaustein „F03EStopSIL1PLc (FB3)“ komplett entfernt werden. Dazu ist unter „Programmbausteine“ „Main_Safety_RTG (FB1)“ anzuwählen. Er erscheint im mittleren Fenster. Dann den Sicherheitsbaustein „F03EStopSIL1PLc (FB3)“ durch Rechtsklick anklicken. Es wird ein Bearbeitungsmenü sichtbar. Dort „Löschen“ betätigen. Falls der Baustein nicht direkt zu sehen ist, mittels scrollen den Fensterinhalt solange verschieben, bis das der Fall ist.

Anschließend müssen die Netzwerke des Bausteins „F100EStopSIL3PLe“ aktualisiert werden. Dazu ist dieser mittels Doppelklick zu markieren (links außen). „ESTOP1“ (Netzwerk1, mittleres Fenster) aktualisieren (Rechtsklick) und Abfrage bestätigen. „FDBACK“ (Netzwerk2) anwählen und bei „ACK_NEC“ „true“ eintragen. Danach Baustein aktualisieren. Im Netzwerk 5 den Baustein „ACK_GL“ ebenfalls aktualisieren.

Nochmals ins Netzwerk 1 scrollen und dort auf den roten Namen des Bausteins „E-STOP“ doppelklicken. Es erscheint ein kleines Eingabefeld mit rechts einem Listensymbol. In der Auswahlliste den Datenbaustein „ESTOP_DB“ wählen. In ähnlicher Weise im Netzwerk 2 mit dem Baustein“FDBACK“ vorgehen und dort „FDBACK_DB“ anklicken. Jetzt ist der Baustein „F03EStopSIL1Plc (FB3)“ aus der Liste der Programmbausteine im linken Fenster zu löschen. In gleicher Weise ist mit dem Baustein „instF03StopSIL1Plc“ zu verfahren und dieser ebenfalls zu löschen.

6.2.5 Programm in CPU laden

Das Programm ist nun komplett geändert und muss in die CPU übertragen und diese wieder gestartet werden. Danach blinkt die LED „RUN7/STOP“ in der Zentraleinheit gelb und geht nach kurzer Zeit in grünes Dauerlicht über. Das Programm befindet sich jetzt in der Zentraleinheit und wird bei jedem Neustart ausgeführt.

6.3 Test des geänderten Programms und Simulation der Motorsteuerung mittels SafetySim

Ob die Programmänderung komplett und erfolgreich war, lässt sich durch entsprechende Tests überprüfen.

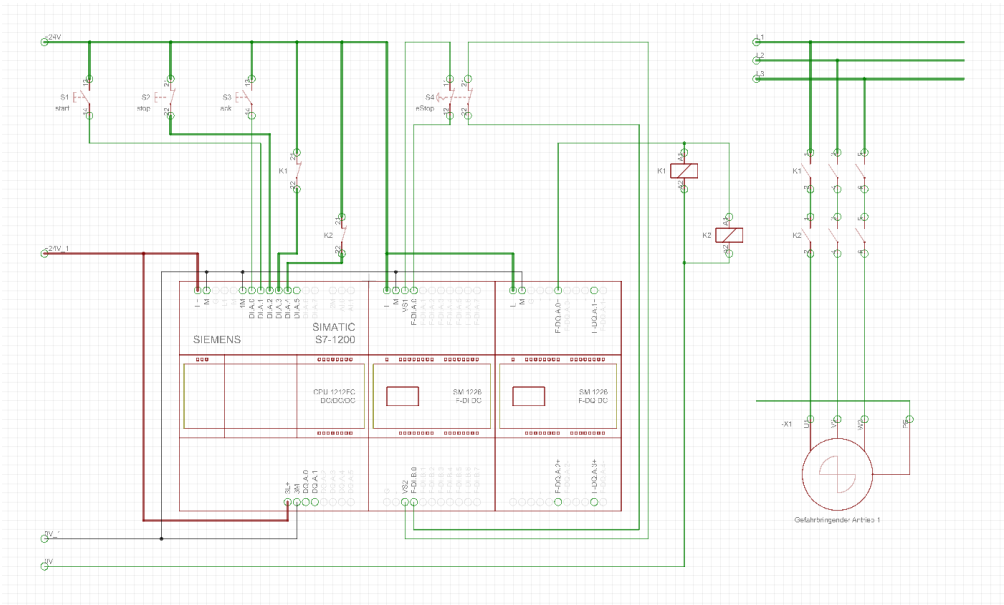
6.3.1 Anpassung der „Hardware“

Passend zu den erfolgten Programmänderungen muss auch eine abgewandelte „Hardware“ bzw. Steuerung, die den Anforderungen des Sicherheitsintegrations-Levels 3 entspricht, zum Einsatz kommen. Diese muss im Gegensatz zu der bisher verwendeten u. a. zwei Motorschütze, zwei Rückmeldekontakte und einen zweikanaligen Not-Halt-Taster aufweisen.

Es sind

- **das SafetySim zu aktivieren,**
- **SafetySim-Simulation anzuwählen und**
- **dort in den verfügbaren Szenen „Not-Halt in PL d, e/SIL 2, 3“ aufzurufen.**

Der entsprechende Stromlaufplan wird auf dem Monitor dargestellt.



Alternatives Vorgehen: Sie können die Motorsteuerung nach SIL 1 erneut testen. Dazu gehen Sie vor wie unter 5.3 bis 5.4 beschrieben. Beachten Sie dazu aber auch Punkt 7, Vergleich der beiden Sicherheitslevel.

6.3.2 Betriebszustände

Wie unter Punkt 5.3.3 beschrieben können die Betriebszustände entsprechend getestet werden. Lassen sich diese problemlos realisieren, kann man das Verhalten der Steuerung im Fehlerfalle ermitteln.

6.3.3 Fehlfunktionen simulieren

Anhand der Erkennung von Fehlfunktionen lassen sich die Unterschiede bzw. der Sicherheitsgewinn bei SIL 3 gegenüber SIL 1 erkennen.

6.3.3.1 Verschweißung

Diese Defekte lassen sich, wie unter 5.3.4.1 beschrieben, erzeugen.
Im Gegensatz zu der Steuerungen nach SIL 1 kann hier (SIL 3) der Motor trotz der Kontaktverschweißung in einem Schütz nach wie vor betriebsmäßig oder über den Not-Halt-Taster gestoppt werden. Ein Wiederanlauf ist, solange der Fehler besteht, nicht möglich. Hier zeigt sich der deutliche sicherheitstechnische Vorteil von SIL 3 gegenüber SIL 1. Die Verschweißung kann wie oben (5.3.4.1) erklärt, wieder aufgehoben werden.

Dieser Vorteil wird im Wesentlichen durch den Einsatz von zwei Motorschützen incl. der Rückmeldungen sowie natürlich der auswertenden Software erreicht.

6.3.3.2 Unterbrechung

Um derartige Fehler zu erzeugen ist, wie unter 5.3.4.2 ausgeführt, vorzugehen. Die Effekte in der geänderten Steuerung sind die gleichen wie die oben bereits beschrieben. Eine Unterbrechung in einem der Anschlüsse, beispielsweise des Not-Halt-Tasters oder des Rückmeldekontaktes, wird sofort erkannt und gegebenenfalls der Motor abgeschaltet. Zwischen den beiden Steuerungen (SIL 1 und SIL 3) besteht in dieser Hinsicht kein wesentlicher Unterschied bzw. ist kein zusätzlicher Sicherheitsgewinn zu verzeichnen. Die Aufhebung des Problems erfolgt, wie in 5.3.4.2 beschrieben.

6.3.3.3 Kurz- bzw. Querschluss

Für den Sicherheitsintegrations-Level 3 wird die sogenannte Querschlusssicherheit gefordert. Diese bezieht sich im vorliegenden Fall hauptsächlich auf den Not-Halt-Taster. Das heißt, dass beispielsweise eine Verbindung zwischen den beiden Anschlüssen eines Kontaktes obigen Tasters besteht. Zur Erzeugung sowie der Aufhebung eines solchen Fehlers ist, wie im Punkt 5.3.4.3 erläutert, vorzugehen.
Wenn das Motorschütz angezogen hat, d. h. der Motor läuft, fällt es beim Auftreten des Querschlusses sofort ab. Ein Widereinschalten ist nicht möglich. Das Problem wird steuerungsseitig in der S7-Eingangsbaugruppe (SM 1226 F-DI DC) und vor allem durch die Verwendung der internen Geberversorgung erkannt.

6.4 Zusammenfassung

Man kann davon ausgehen, dass Steuerungen, die einem höheren Sicherheits-Level entsprechen, im Falle eines auftretenden Fehlers, besseren Schutz für die Maschinen, vor allem aber die damit umgehenden Menschen, bieten. Ein typisches Beispiel ist bei den beiden vorliegenden Steuerungsvarianten die Tatsache, dass auf eine Kontaktverschweißung des Motorschützes bei SIL 1 gar nicht reagiert werden kann, bei SIL 3 sie aber sicher erkannt wird und notwendige Maßnahmen ergriffen werden. Ähnlich sieht es aus, wenn in einer SIL 1-Steuerung keine besondere Geberversorgung bzw. eine entsprechende Auswertung für den Not-Halt-Taster verwendet wird. Dann kann nämlich ein Querschluss in dem Taster nicht erkannt werden und dieser ist dann in seiner Funktion wirkungslos.

Elektrische und elektronische Systeme, die Sicherheitsfunktionen beinhalten, werden hinsichtlich deren Zuverlässigkeit in unterschiedliche Klassen eingeteilt. Je nach Ausgangsnorm unterscheidet man zwischen Performance Level PL und Sicherheits-Integritätslevel SIL. Letztere reichen von 1 bis 4 und die PL von a bis e. Es ist zum Beispiel SIL 3 vergleichbar mit PL e und SIL1 mit PL b bzw. PL c.

7. Vergleich der beiden Sicherheits-Level SIL 1 und SIL 3

In der nachfolgenden Tabelle sind einige der wesentlichen Merkmale zu den beiden Motorsteuerungen und ihren unterschiedlichen Sicherheitsintegritäts-Leveln aufgelistet.

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="2">Sicherheitsintegrations-Level</th><th rowspan="2">Hinweise</th></tr>
<tr><th>SIL 1</th><th>SIL 3</th></tr>
<tr><td colspan="2">Allgemeine Sicherheitsfunktion</td><td colspan="2">Bei Drücken des Not-Halts wird der Aktor sicher abgeschaltet.</td><td>Aufgrund der Rückführung der Meldekontakte der Motorschütze wird die Sicherheit der Steuerungen erheblich erhöht.</td></tr>
<tr><td rowspan="4">Reaktion auf Fehler</td><td>Verschweißung der Kontakte eines Schützes</td><td>Trotz der Betätigung von Stop- oder Not-Halt-Taster läuft der Motor weiter! Er kann allein durch Betätigung des Haupt- bzw. Haupt-Not-Aus-Schalters gestoppt werden (Spannungsabschaltung). Nach der Fehlerbeseitigung ist ein Wiedereinschalten nur durch vorherige Quittierung möglich.</td><td>Bei jedem Ausschalten fällt das nicht betroffene Schütz ab, der Motor bleibt stehen und lässt sich nicht mehr starten. Auch nach der Fehlerbeseitigung ist ein Wiedereinschalten nur nach erfolgter Quittierung möglich.</td><td>In beiden Steuerungen wird zwar ein sogenannter Rücklesefehler beim Abschalten erkannt, aber nur bei SIL 3 kann aufgrund der vorhandenen Zweikanaligkeit bzw. der Verwendung von zwei Schützen der Motor sicher angehalten werden! Hier zeigt sich der deutliche sicherheitstechnische Vorteil von SIL 3 gegenüber SIL 1.</td></tr>
<tr><td rowspan="2">Kurz- bzw. Querschluss</td><td>Querschlusssicherheit nicht gefordert</td><td>Querschlusssicherheit gefordert</td><td rowspan="2">Bei Steuerungen des Levels SIL 1 wird in der Regel ein Kurz- bzw. Querschluss nicht erkannt. Für SIL 3 ist die überwachte Geberversorgung zwingend vorgeschrieben. Nur durch diese ist eine Querschlusserkennung sicher möglich.</td></tr>
<tr><td colspan="2">Aufgrund der Tatsache, dass in der vorliegenden Steuerung die interne Geberversorgung der S-SPS-Eingangsbaugruppe (F-DI DC) benutzt wird, kann ein Kurz- bzw. Querschluss im Not-Halt-Taster sicher erkannt werden.</td></tr>
<tr><td>Unterbrechung</td><td colspan="2">Eine Unterbrechung in einem der Anschlüsse des Not-Halt-Tasters oder des Rückmeldekontaktes wird sofort erkannt und gegebenenfalls der Motor abgeschaltet.</td><td>Es können in beiden Steuerungen keine unerkannten, sicherheitsrelevanten und kritische Probleme auftreten.</td></tr>
</table>

		Sicherheitsintegrations-Level		Hinweise
		SIL 1	SIL 3	
Sicherheitsrelevante Software	Basis-Sicherheits-Software	STEP 7 Safety Basic V15		Sicherheits-Engineering- Software für SIMATIC S 7; Im (Funktionsbaustein „FDBACK") erfolgt eine Diskrepanzanalyse zwischen dem Ansteuersignal der Schützspule und den Rückmeldekontakten des Schützes. Innerhalb einer einstellbaren Zeit müssen die beiden Signale korrelieren. Ansonsten erfolgt eine Abschaltung des Ausganges.
	Bibliothek für F-Anwender-FBs	S7_1200F_LIB_V14_V15.1		Diese Baustein-Bibliothek befindet sich im Bereich der Globalen Bibliotheken. Der Zusatz „V14" steht nur hier, weil für das vorhandene System eine Versionsanpassung von V14 auf V15.1 stattgefunden hat.
	eingesetzte F-Anwender-Funktionsbausteine	F03EStopSIL1PLc	F100EStopSIL3PLe	Bei diesen Bausteinen handelt es sich um sicherheitsgerichtete und TÜV-zertifizierte Kopiervorlagen.
	Diskrepanzanalyse der Not-Halt-Kontakte	nein	ja	Diese Auswertung findet in der fehlersicheren Eingangsbaugruppe (F-DI) statt. Eine Zeitüberschreitung wirkt wie ein Drücken des NOT-Halt-Tasters. Zusätzlich erfolgt eine Signalweitergabe an die CPU.

		Sicherheitsintegrations-Level		Hinweise
		SIL 1	SIL 3	
Sicherheitsrelevante Hardware	CPU 1212 FC, DC/DC/DC	Fehlersicheres S-SPS-System aus der S7-Familie von Siemens, insbesondere geeignet für Safety Anwendungen		Mithilfe dieses Steuerungssystems können Standard- sowie fehlersichere Automatisierungsaufgaben kleineren Projektumfanges gelöst werden. Es ist nach EN DIN 61508 für funktionale Sicherheit zertifiziert. Für den Einsatz in sicherheitsgerichteten Applika-tionen bis SIL 3 nach IEC 62061:2005 + A1:2012 + A2:2015 und PL e nach EN ISO 13849-1:2015 ist es ebenfalls geeignet und zugelassen.
	Digitaleingabe SM 1226 F-DI DC			
	Digitalausgabe SM 1226 F-DO DC			
	Not-Halt-Taster (verriegelnd)	1-kanalig zulässig	2-kanalig gefordert	Der PFH-Wert gibt die „durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde" (Probability of a Dangerous Failure per Hour) an. Man spricht häufig auch einfach von der Ausfallwahrscheinlichkeit.
		Ausfallwahrscheinlich-keit: $10^{-6} \leq PFHD < 3 \times 10^{-5}$	Ausfallwahrscheinlich-keit: $10^{-8} \leq PFHD < 10^{-7}$	
		Geberversorgung kann intern über die S-SPS-Eingangsbau-gruppe (F-DI DC) oder extern erfolgen.	Geberversorgung muss intern (F-DI DC) erfolgen.	Nur durch Nutzung der internen Geber-versorgung an der (F-DI DC) kann ein Querschluss zwischen den NOT-Halt-Kanälen sicher erkannt werden.
	Anzahl der Rück-meldekontakte	1	2	Hilfskontakte der Motorschütze