Kurzeinführung für die praktische Erprobung

SafetySim Erste Schritte

SafetySim

Inhalt

Entwurf und Realisierung sicherheitsbezogener Steuerungen

Normen für Steuerungen: Wiederholung

Zur Erinnerung: In Europa Steuerungen mit sicherheitsrelevanten Funktionen bestimmten Normen entsprechen. Das sind u. a.

- **EN 62061:2005** oder
- **EN ISO 13849-1:2006**.

In beiden Normen ist mit Blick auf die **Zuverlässigkeit** der verwendeten elektrischen und elektronischen Systeme eine **Klassifizierung** vorgesehen.

SafetySim

Normen für Steuerungen: SIL und PL

- In der EN 62061:2005 bezeichnet man die Klassen als **Sicherheits-Integritätslevel 1-4** (häufig werden nur 1-3 genannt), abgekürzt „**SIL**“.
- Gemäß der EN ISO 13849-1:2006 spricht man von **Performance Level a bis e**, abgekürzt „**PL**“.
- Hinsichtlich dieser Level gibt es in weiten Bereichen, wie schon gezeigt, **Übereinstimmungen**.

SafetySim

Normen für Steuerungen: Grundsätze

- Grundsätzlich kann man davon ausgehen, dass sicherheitsbezogene Steuerungen **um so seltener ausfallen**, je höher der Sicherheitsintegritäts- bzw. Performance-Level ist, dem sie entsprechen.
- Das bedeutet aber auch, dass, abhängig vom jeweiligen Sicherheitslevel, **auftretende Fehler mehr oder weniger gut erkannt werden** und entsprechende Reaktionen erfolgen können.

SafetySim

Inhalt

- Entwurf und Realisierung sicherheitsbezogener Steuerungen

Hinweise zur Aufgabenstellung

Grundlegende Aufgabenstellung

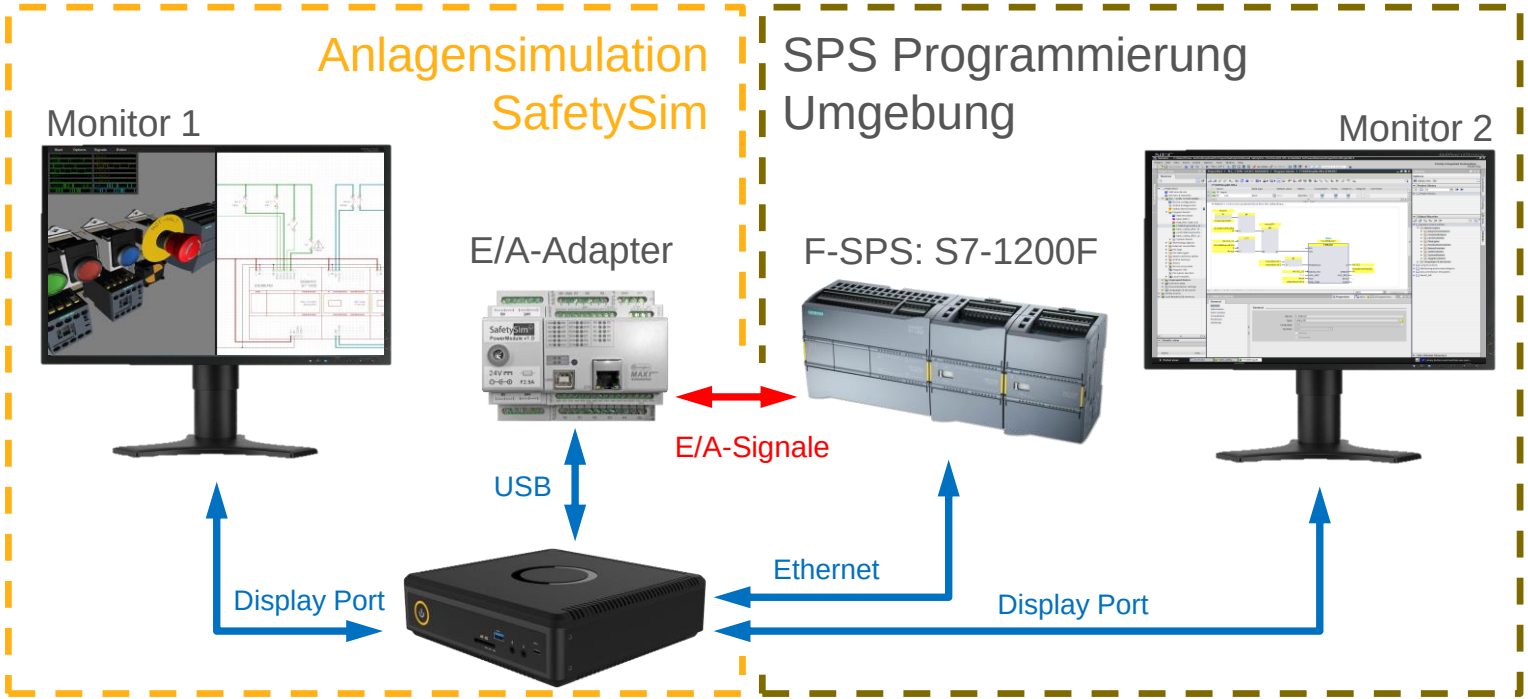
Zur weiteren praktischen Erprobung soll mithilfe

- eines **rechnergestützten Simulationssystems (SafetySim)** sowie
- einer **realen fehlersicheren SPS** der Firma Siemens

eine Motorsteuerung unter sicherheitstechnischen Aspekten untersucht bzw. angepasst werden.

Grundlegende Aufgabenstellung

SafetySim Systemübersicht



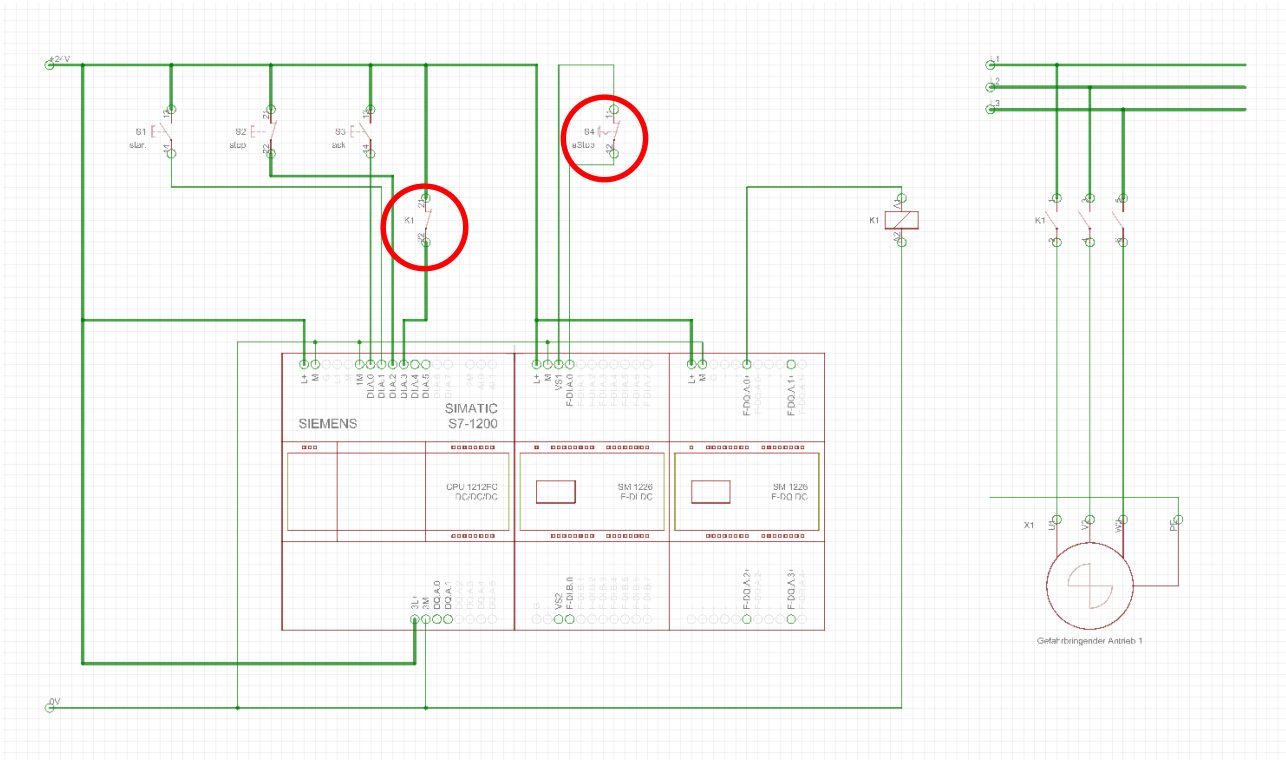
Motorsteuerung nach SIL 1

Eine vorhandene Motorsteuerung besteht aus:

- **realer sicherheitsgerichteter Speicherprogrammierbarer Steuerung** (S7, Safety Integrated);
- entsprechender **Software**;
- durch SafetySim **nachgebildeten Sensoren bzw. Aktoren** (Bedienelemente und ein Motorschütz mit angeschlossenem Motor).

Insgesamt entspricht die Steuerung dem **Sicherheitsintegritäts-Level SIL 1**.

Stromlaufplan SIL 1



Stromlaufplan SIL 1

SIL 1: Betriebszustände

Mithilfe der Bedienelemente kann

- der Motor **ein- oder ausgeschaltet sowie**
- **im Notfall gestoppt** werden.

Für letzteren Fall ist zusätzlich eine Fehlerquittierung vorgesehen.

SIL 1: Fehlfunktionen

- Unter Sicherheitsaspekten ist es besonders wichtig zu wissen, **wie sich eine Steuerung im Falle auftretender Fehler verhält**.
- Deshalb ist auch vorgesehen, dass im Weiteren in obiger Steuerung **bestimmte Fehler simuliert** werden.
- Dabei stellt man fest, dass **einige nicht erkannt** werden!

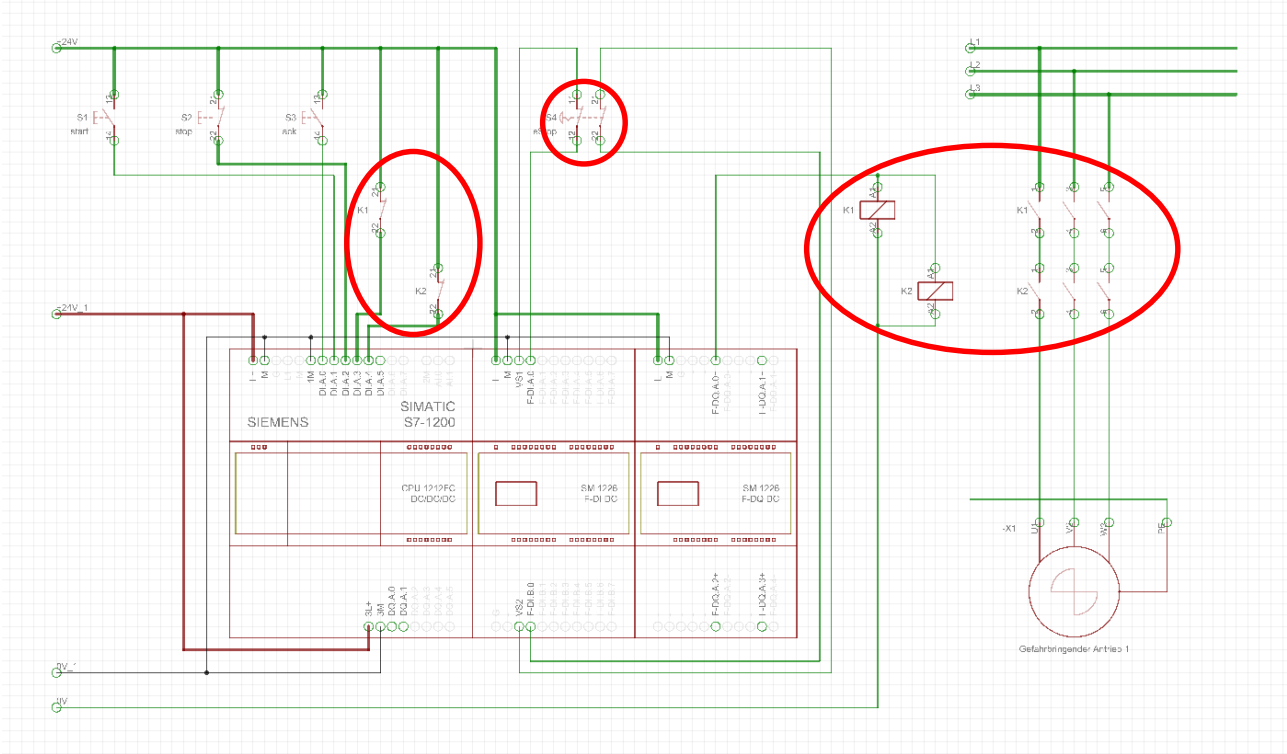
SafetySim

Motorsteuerung nach SIL 3

- Zum Vergleich soll deshalb die oben beschriebene Steuerung **auf den Sicherheitsintegrations-Level 3 gebracht** werden.
- Um den höheren Sicherheitslevel (SIL 3) zu erreichen, müssen die **relevanten Komponenten entsprechend angepasst** werden.
- Insbesondere bedeutet das: Die Sicherheitselemente müssen **zweikanalig ausgeführt** werden.

SafetySim

Stromlaufplan SIL 3



Stromlaufplan SIL3

Änderungen an der S-SPS

Zur Auswertung der Hardwareänderungen muss Einiges **an der Simatic-Steuerung (S7) geändert** werden. Zum einen müssen

- die **Eingänge angeschlossen** und zum anderen
- diese **intern im Programm verarbeitet**

werden.

Letzteres erfolgt durch Eingriffe in die S-SPS-Software, insbesondere den **Austausch eines sicherheitsgerichteten Funktionsbausteins**.

Beide Modifikationen werden mithilfe des **TIA-Portals** durchgeführt.

Fehlfunktionen

Bei kompletter richtiger Überarbeitung und entsprechenden Tests stellt man fest, dass jetzt

- die **Fehlfunktionen erkannt** werden und
- die **Sicherheit** der Steuerung dadurch erheblich **gestiegen** ist.

Erkenntnisse aus der Übung

- Eine Steuerung, die dem **Sicherheitsintegritäts-Level 1** entspricht, beinhaltet in der Regel zwar gewisse sicherheitsrelevante Funktionen, kann aber **bestimmte Fehler nicht erkennen**.
- Entspricht diese Steuerung hingegen dem **Sicherheitsintegritäts-Level 3**, so kann sie auch die **oben nicht erkannten Fehler feststellen** und darauf entsprechend reagieren.
- Bei der Entwicklung einer Steuerung muss man das vorhandene **Restrisiko sehr genau abschätzen** und dementsprechend den erforderlichen **Sicherheitslevel festlegen**.

SafetySim

Vielen Dank!

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Bundesinstitut
für Berufsbildung
BIBB

- Forschen
- Beraten
- Zukunft gestalten

Gefördert durch die

DGUV
Deutsche Gesetzliche
Unfallversicherung
Spitzenverband

DEKRA Media
GmbH

SafetySim