



Berufs Bildung Baden

Fach: Automation

Thema: Speicherprogrammierbare  
Steuerungen

Kapitel: Funktionale Sicherheit von  
Maschinensteuerungen

Quelle: Fachkunde Elektroberufe,  
3. Auflage

Verlag: Bildungsverlag EINS

<b>BBB</b>	Fach: <b>Automation</b>	Thema: <b>Funktionale Sicherheit von Maschinensteuerungen</b>	Beruf: <b>AU3</b>
<b>Inhaltsverzeichnis</b>			
<b>1. Funktionale Sicherheit von Maschinensteuerungen ..... 2</b>			
1.1    Sicherheit von Steuerungen .....			2

<b>BBB</b>	Fach: <b>Automation</b>	Thema: <b>Funktionale Sicherheit von Maschinensteuerungen</b>	Beruf: <b>AU3</b>
------------	----------------------------	--	----------------------

## 1. Funktionale Sicherheit von Maschinensteuerungen

### 1.1 Sicherheit von Steuerungen

#### 13.9.1 Fehlerarten

Unterschieden wird zwischen *aktiven* und *passiven* Fehlern sowie zwischen *gefährlichen* und *ungefährlichen* Fehlern.

- Je nach Aufgabenstellung einer Steuerung können aktive oder passive Fehler gefährliche Auswirkungen haben.

- Bei der Steuerung eines Antriebes führt ein *aktiver Fehler* zu einem unerlaubten Einschalten.
- Bei der Steuerung einer Meldefunktion verhindert ein *passiver Fehler* die Meldung eines gefährlichen Betriebszustandes.

Überall dort, wo auftretende Fehler große Materialschäden oder sogar Personenschäden verursachen können (gefährliche Fehler), müssen Maß-

nahmen getroffen werden, die die Sicherheit der Steuerung erhöhen.  
Hierzu gibt es eindeutige Bestimmungen, die unbedingt zu beachten sind.

### 13.9.2 Sicherheitsmaßnahmen

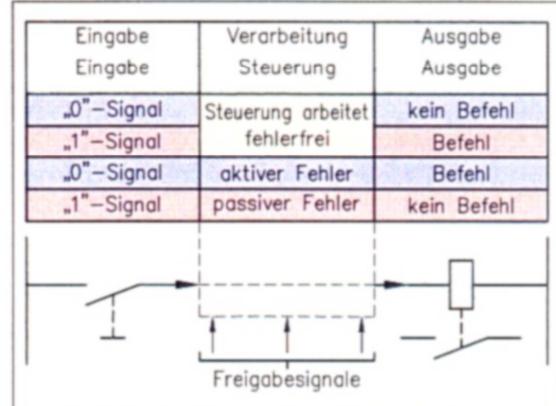
#### Einkanaliger Aufbau

Bei einer *einkanalig* aufgebauten SPS stehen zur Erhöhung der Sicherheit nur begrenzte Maßnahmen zur Verfügung:

- Programme oder Programmteile können mehrfach im Programmspeicher abgelegt und bearbeitet werden.
- Ausgänge können durch eine parallele Rückführung auf die Eingänge des gleichen Gerätes softwaremäßig überwacht werden.
- Diagnosefunktionen innerhalb der SPS, die beim Auftreten eines internen Fehlers die Ausgänge des Gerätes in einen definierten Signalzustand (meist „0“) bringen.
- Programmflussmonitore (Watch-dog-Timer), die in vielen Baugruppen herstellerseitig eingebaut sind. Der Watch-dog ist eine Überwachungseinrichtung für den Prozessablauf.

**Funktionsgruppen dürfen nur durch gleichwertige Funktionsgruppen ersetzt werden. Es dürfen nur unveränderte Programme eingesetzt werden, die nach Inbetriebnahme und Prüfung als sicher erkannt wurden.**

<b>Diagnose</b>	Erkennung, Feststellung von Fehlern
<b>watch dog</b>	engl.: Wachhund



13.123 Fehlerarten bei einer Steuerung, Prinzip

#### Mehrkanaliger Aufbau

Werden die einkanalig aufgebauten Steuerungen den Sicherheitsanforderungen nicht gerecht, müssen die Steuerungen *mehrkanalig* aufgebaut werden. Man spricht dann auch von einem *redundanten* Steuerungsaufbau (Bild 13.124, Seite 440).

**Redundanz** lat.: Überfluss

#### Zweikanalige Steuerungen

Die beiden „Steuerungskanäle“ überwachen sich gegenseitig. Die Auswertung der Ausgangsfehler erfolgt nach dem „2-von-2-“ oder „1-von-2-Prinzip“. Zwei Automatisierungsgeräte sind gleich programmiert und arbeiten synchron. Durch gegenseitige Überwachung werden Fehler erkannt, die zu entsprechenden Steuerungsreaktionen führen.

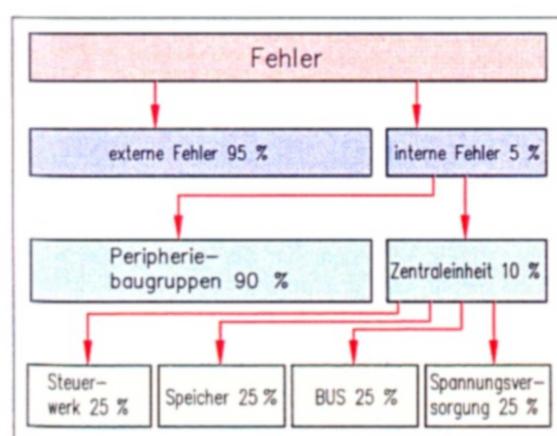
Bei diesem *Parallelbetrieb* werden zwei Möglichkeiten unterschieden:

Die gleiche Steuerungsaufgabe kann mit *unterschiedlicher Hardware* und *unterschiedlicher Software* bearbeitet werden. Diese Lösung wird als besonders sicher angesehen.

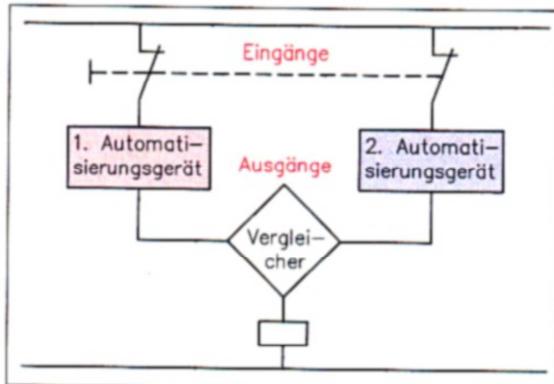
Ebenso kann die Steuerungsaufgabe mit *gleicher Hardware* und *gleicher Software* bearbeitet werden. Dieser Parallelbetrieb wird als weniger sicher betrachtet.

#### Mehrkanalige Steuerungen

Durch Hinzufügen weiterer Kanäle können weitere Auswahlsysteme (z. B. 2-von-3-Auswahl) verwirklicht werden.



13.122 Fehlerverteilung bei SPS-Anlagen



13.124 Parallelbetrieb von Steuerungen

### **Elektromechanische und elektronische Steuerungen**

Schütze und Relais ziehen nur an, wenn an ihrer Spule Spannung anliegt. Daher sind bei ihnen *aktive Fehler* unwahrscheinlicher als *passive Fehler*. In elektronischen Schaltungen treten aktive und passive Fehler in gleichem Maße auf. So kann beispielsweise ein Transistor im Fehlerfall *dauernd leiten* oder *dauernd sperren*.

Bei Kenntnis und Beachtung dieser Eigenschaften kann die Sicherheit von Steuerungen erhöht werden:

- Funktionen, die *keine* sicherheitstechnische Bedeutung haben, werden elektronisch gesteuert.
- Funktionen mit *sicherheitstechnischer Bedeutung* werden mit herkömmlichen elektromechanischen Bauelementen aufgebaut.

#### **Sicherheitsbestimmungen**

- Gefährliche Zustände, durch die Menschen, Maschinen und Material gefährdet bzw. beschädigt werden können, müssen verhindert werden.
- Maschinen dürfen nach Wiederkehr einer zuvor ausgefallenen Spannung *nicht selbsttätig* wieder anlaufen (z. B. nach Entriegelung eines NOT-HALT).
- Fehler im Eingangstromkreis (z. B. Drahtbruch oder Erdschluss) dürfen *Ausschaltfunktionen* nicht verhindern.
- Widersprüchliche Eingangsbefehle (links/rechts usw.) müssen durch *Tasterverriegelung* unterbunden und zusätzlich im SPS-Programm verriegelt werden.
- Widersprüchliche Befehle (links/rechts usw.) müssen auch an den Leistungsschützen *verriegelt* werden.

- Grenztaster dürfen nur *einen Öffner* und *einen Schließer* oder *einen Wechsler* haben. Der Wechsler muss über zwei *getrennte Eingänge* zur SPS geführt werden. Eine programmtechnische Negation des Signals ist in diesem Fall *nicht erlaubt*.

- NOT-HALT-Einrichtungen und Sicherheitsgrenzschalter müssen auch bei Fehlern im Automatisierungsgerät wirksam bleiben und daher *direkt an den Stellgeräten wirken*. Der NOT-HALT muss nach Betätigung *arretieren* und darf nur *vor Ort* durch Lösen der Arretierung wieder einschaltbar sein.

**arretieren** Zustand nach Betätigung beibehalten

- Begrenzte Maschinenbewegungen müssen stets *wegabhängig* (niemals zeitabhängig) gesteuert werden.
- Bei Maschinenbewegungen *ohne mechanischen Anschlag* muss neben dem Grenztaster für Steuerungszwecke noch ein Sicherheitsgrenztaster mit mechanischer Zwangsoffnung vorhanden sein, der *außerhalb* der SPS wirksam ist.

#### **NOT-HALT, NOT-AUS**

Die Bezeichnung NOT-HALT ist i. Allg. besser als die Bezeichnung NOT-AUS, da die Steuerung bei Betätigung dieses Signalgebers in den ungefährlichen Zustand geschaltet werden soll.

Nicht immer ist der ungefährliche Betriebszustand der ausgeschaltete Zustand; so zum Beispiel bei magnetischen Spannvorrichtungen und magnetischen Lasthebevorrichtungen. Die einwandfreie Funktion des NOT-HALT muss besonders sorgfältig geprüft werden.

In der DIN EN 60204-1 (Sicherheit von elektrischen Maschinen) werden folgende Kategorien unterschieden:

##### **Kategorie 0**

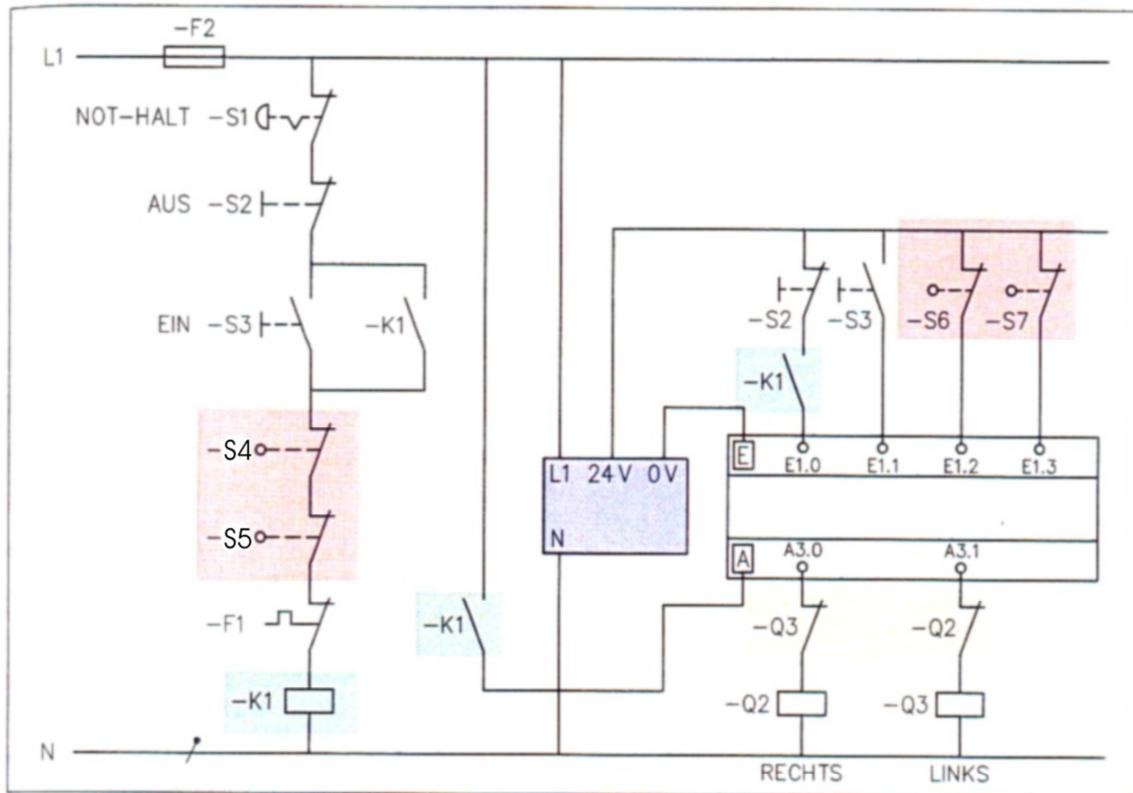
Ungesteuertes Stillsetzen, z. B. durch Hauptschalter

##### **Kategorie 1**

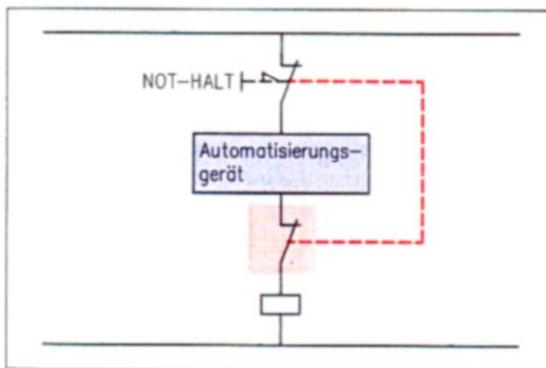
Gesteuertes Stillsetzen; rotierende bzw. bewegte Teile durch Bremsung zum Stillstand bringen und Energiezufuhr sicher abschalten. Direkte Stillstandabfrage erforderlich.

##### **Kategorie 2**

Vorgabe des Sollwertes Null (über Tastatur). Eine sichere Abschaltung der Energiezufuhr ist hierbei nicht vorgesehen. Diese Kategorie ist für den NOT-AUS-Vorgang nicht zulässig.



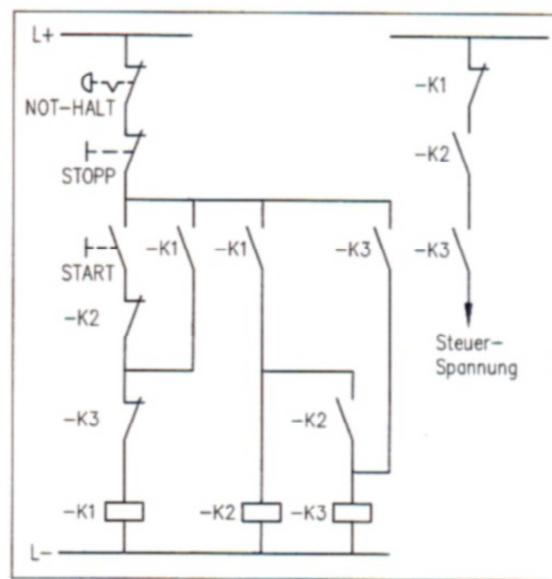
### 13.125 Beschaltung einer SPS, vereinfachtes Beispiel



### 13.126 Übergeordnete Sicherheitsschaltung

- Bei Betätigung des NOT-HALT muss die Spannungsversorgung der Ausgänge unterbrochen werden, (Bild 13.127: das Schütz K1 und die Lastschütze fallen ab)
  - Das Gleiche gilt für die beiden Sicherheitsgrentaster S4, S5, den Austaster S2 sowie den thermischen Überstromauslöser E1

Beachten Sie besonders den Schließer K1 vor dem Eingang E1.0 in Bild 13.125. Da das Prozess-



### 13.127 Sicherheitsstromkreis (NOT-HALT)

abbild der Ausgänge z. B. bei Betätigung des NOTHALT erhalten bleibt, hat der Abfall von K1 die glei-



Fach:  
**Automation**

Thema:  
**Funktionale Sicherheit von Maschinensteuerungen**

Beruf:  
**AU3**

che Wirkung für das *Steuerungsprogramm* wie eine Betätigung des Austasters S2.

Damit ist ein selbsttätiger Wiederanlauf nach Wiederkehr der Ausgangsspannung auch programmtechnisch ausgeschlossen. Die Sicherheitsgrenztaster S4, S5 und die Grenztaster S6, S7 haben die gleiche Aufgabe.

Die Grenztaster S6 und S7 wirken allerdings ausschließlich softwaremäßig, d. h. im Steuerungsprogramm des Automatisierungsgerätes. Bei *übergeordneten Sicherheitsschaltungen* werden die Ausgangssignale vor ihrem Wirksamwerden kontakttechnisch verriegelt.

Bild 13.126, Seite 441 zeigt eine solche Schaltung am Beispiel eines NOT-HALT. Der NOT-HALT wird einmal auf den Eingang des Automatisierungsgerätes, zum anderen unmittelbar auf das Lastschütz, das an die Ausgabe-Ebene angeschlossen ist, gegeben.

In Bild 13.127, Seite 441 ist ein oftmals angewandter NOT-HALT-Steuerstromkreis dargestellt. Hierbei werden die drei Schütze bei jedem Start- und Stoppvorgang zumindest einmal automatisch überprüft. Man spricht dann von einem *selbstkontrollierenden Stromkreis*.