Zu „Sicherheit“: Übung ASA 12

Zur Durchsprache in der Vorlesung:

12.1 Sichere Abschaltung

Eine Heizanlage soll bei Überdruck und Übertemperatur „sicherheitsgerichtet" abgeschaltet werden, d.h. im Zweifelsfall (bei Drahtbruch, Erdschluss, Spannungsausfall) abschalten. Signale dieser Kriterien gehen innerhalb der Steuerung an ein ODER – Gatter, wo sie mit log. "1" abschalten.
Für die Druckmessung steht ein Druckwächter mit einem Wechselkontakt zur Verfügung (als Schließer oder Öffner verwendbar). Die Temperatur wird analog gemessen (Eingabegerät für Widerstandsthermometer).
Die zugehörigen Eingabegeräte liefern der CPU Pegel "0" wenn am Eingang keine Spannung ansteht, haben aber keine Eingangskreisüberwachung.

a) ***Erstellen Sie eine Skizze*** für die Überdruckabschaltung, aus der erkennbar ist, welchen Kontakt Sie benutzen (Schließer oder Öffner), welchen physikalischen Zustand die gezeichnete Kontaktstellung bedeutet und bei welchem Signal vom Eingabegerät ("1" oder "0") die Steuerung abschalten müsste um sicherheitsgerichtet zu arbeiten.

b) ***Erstellen Sie eine Skizze*** für die Abschaltung über die Temperatur. Stellen Sie dar, wie Sie das notwendige Binärsignal erzeugen und sicherstellen, dass auch im Fehlerfall (Unterbrechung oder Erdschluss im Eingangskreis) abgeschaltet wird.

c) Die Schaltung für a) soll sicher sein, hat dann aber geringe Verfügbarkeit. Wie könnte man die Abschaltung durch den Überdruck zwar nicht sicherheitsgerichtet aber relativ sicher und verfügbar ausführen, wenn ein zweiter Druckwächter zur Verfügung stünde? ***Skizzieren Sie die Lösung***.

12.2 Ausfallwahrscheinlichkeit

Die gesamte Überdruckabschaltung aus **12.1** soll SIL2 erreichen, sie ist für „kontinuierliche Anforderung“ auszulegen. Für Verarbeitung + Befehlsausgabe wurde ermittelt, dass alle $2 * 10^6$ Stunden ein Fehler auftreten kann, bei dem nicht abgeschaltet wird und der nicht erkannt wird. Alle $1 * 10^6$ Std. tritt ein gefährlicher Fehler auf, der entdeckt wird, und alle $4 * 10^5$ Std. ein ungefährlicher Fehler.

a) ***Welche Ausfallwahrscheinlichkeit*** darf die Kombination aus Druckwächter und Eingabegerät haben?

b) ***Gibt es sonstige Einschränkungen***, wenn 1 Kanal verwendet wird (N=0), das Ausfallverhalten gut definiert und vollständig ermittelbar ist und Erfahrungswerte vorliegen?

12.3 Fehlersicherheit

Eine einkanalige Maschinensteuerung besitzt Diagnosefunktionen und ist so ausgelegt, dass bei Auftreten eines Fehlers die Maschine abgeschaltet wird.

a) ***Welchem Auslegungsziel*** (Verfügbarkeit oder Sicherheit) ***dient das?***

b) ***Wie verhält sich diese Steuerung im Sinne der Fehlertoleranz*** (integer / stetig)?

c) ***Wie würde sie nach IEC 61508*** (Fehlertoleranz) ***bezeichnet / klassifiziert?***

Als zusätzliche Übung mit Lösung: *(Empfehlung: zuerst zu lösen versuchen, dann nachsehen!)*

12.4 Sicherheitsabschaltung

Von einer sicherheitsrelevanten Temperaturbegrenzung in einer Heizungsanlage, die nur ganz selten einzugreifen hat (voraussichtlich alle 2 Jahre), wird SIL 2 verlangt. Sie besteht aus einer Temperaturmessung mit einem Wechslerkontakt, der bei „Temp. zu hoch“ umschaltet, sowie einem Magnetventil zur Unterbrechung der Ölzufuhr an den Brenner. Dieses Ventil öffnet wenn an seiner Spule Spannung anliegt. Die Temperaturregelung erfolgt über ein zweites Ventil in Reihe.

a) Skizzieren Sie die Schaltung von Kontakt und Spule. Bei Drahtbruch oder Spannungsausfall / Erdschluss soll das Ventil schließen.

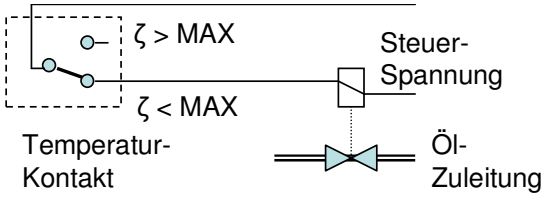
b) Das Fehlerrisiko des Temperaturkontaktes liege bei 60%, das des Ventils bei 40%, keine Redundanz. Für SFF liegen gut gesicherte Werte von 95% bzw. 97% vor.
Welche Ausfallwahrscheinlichkeit (Wert gemäß PFD oder PFH?) ist für die beiden Teile nachzuweisen?

Lösung:

12.4 Sicherheitsabschaltung

Von einer sicherheitsrelevanten Temperaturbegrenzung in einer Heizungsanlage, die nur ganz selten einzugreifen hat (voraussichtlich alle 2 Jahre), wird SIL 2 verlangt. Sie besteht aus einer Temperaturmessung mit einem Wechslerkontakt, der bei „Temp. zu hoch“ umschaltet, sowie einem Magnetventil zur Unterbrechung der Ölzufuhr an den Brenner. Dieses Ventil öffnet wenn an seiner Spule Spannung anliegt. Die Temperaturregelung erfolgt über ein anderes Ventil in Reihe.

a) ***Skizzieren Sie die Schaltung*** von Kontakt und Spule. Bei Drahtbruch oder Spannungsausfall / Erdschluss soll das Ventil schließen.



b) Das Fehlerrisiko des Temperaturkontaktes liege bei 60%, das des Ventils bei 40%, keine Redundanz. Für SFF liegen gut gesicherte Werte von 95% bzw. 97% vor, die Anlage wird jedes Jahr gewartet.
Welche Ausfallwahrscheinlichkeit (Wert gemäß PFD oder PFH?) ist für die beiden Teile nachzuweisen?

Bei 1 Anforderung in ca. 2 Jahren gilt „PFD“,
SIL2 bedeutet dann ein PFD_{gesamt} von 10^{-2} für die gesamte Anordnung.

Es gilt: $PFD_{gesamt} = PFD_{Kontakt} + PFD_{Ventil}$

also: $PFD_{Kontakt} = 0{,}6 * PFD_{gesamt} = 0{,}6*10^{-2}$
$PFD_{Ventil} = 0{,}4 * PFD_{gesamt} = 0{,}4*10^{-2}$