

5. Sicherheit

10 Punkte, 10 Minuten

Ein Industrie-Roboter setzt Teile zusammen und bewegt sich dabei sehr schnell. Ein Arbeiter, der etwa jede Stunde prüfen muss, ob die richtigen Teile zur Verfügung stehen, könnte erfasst und so verletzt werden, dass er medizinische Behandlung benötigt um wieder geheilt zu werden.

Für die Risikobewertung soll die Norm DIN EN 62 061 benutzt werden. Sowohl die Eintrittswahrscheinlichkeit als auch die Möglichkeit zur Vermeidung werden als „möglich“ eingestuft.

Der Roboter arbeitet in einem abgeäugten Bereich, der nur über eine Türe betretbar ist. Wenn diese nicht geschlossen ist wird der Roboter gestoppt bzw. blockiert. Ob sie geschlossen ist soll ein induktiver Geber melden. Von diesem ist bekannt, dass er max. 2 mal in 10^6 Std. fälschlicherweise „geschlossen“ meldet und 3 mal in 10^6 Stunden fälschlicherweise „offen“. Beide Fehler können nicht erkannt werden.

a) Welcher Safety Integrity Level ist zu fordern? $S=2, F=5, W=3, P=3, \rightarrow K=11, \rightarrow SIL1$ (3) 3

b) Welche Fehler-Wahrscheinlichkeit (PFD oder PFH?) ist für den induktiven Geber zu fordern, wenn man die „Standard-Verteilung“ über die gesamte Sicherheitseinrichtung anwendet? $\rightarrow PFH_{Geber} \leq 0,25 * 10^{-5}$ (2) 2

c) Ist der induktive Geber geeignet? (nur PFD / PFH betrachten, nicht FMEDA) $\rightarrow ja$ (2) 5

Begründung: $PFH \sim \lambda_{DU} = 2 * 10^{-6},$ (2) $< 0,25 * 10^{-5}$ (1)

5. Sicherheit (vgl. Aufg. 1 u. 2, aber unabhängig lösbar)

10 Punkte, 10 Minuten

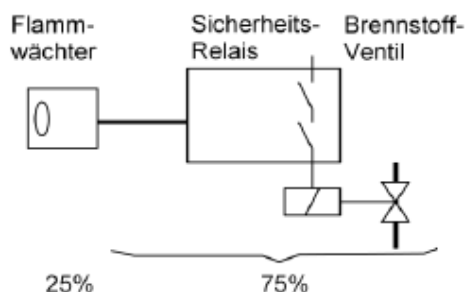
Die Brenner eines Industriekessels werden durch eine nicht sicherheitsgerichtete SPS gesteuert. Die Flammenüberwachung muss jedoch Sicherheits- Anforderungen für niedrige Ausfallrate entsprechen. Dazu ist hier der Sicherheitsgraph nach DIN 61508 anzuwenden.

Wenn die Flamme eines Brenners erlischt und weiterhin Brennstoff in den Feuerraum gelangt, kann durch die Flamme eines anderen Brenners eine Explosion ausgelöst werden, bei der mehrere Personen zu Tode kommen könnten. Allerdings halten sich nur selten Personen beim Kessel auf, und die Wahrscheinlichkeit einer Explosion ist gering.

Das Schließen des Brennstoff-Ventils erfolgt durch ein Sicherheitsrelais, das die Zündzeit überbrückt. Es erfüllt die Aufgaben der Verarbeitung, der Signalausgabe und mit einem speziellen Magnetventil die des Aktors, das entspricht 75% der Ausfall-Verteilung gemäß Norm. Für diese Aufgaben ist es bis SIL3 zugelassen.

Für die Erfassung der Flamme soll ein Flammwächter eingesetzt werden, der gemäß Tests einmal in 10^5 Stunden durch Verschmutzung unnötigerweise Flammen-Ausfall meldet, und max. 5 mal in 10^6 Stunden fälschlicherweise keinen Flammenausfall meldet. Durch regelmäßigen Test kann eine „Unklarzeit“ t_{CE} von 44 Std. angenommen werden.

a) Welcher Sicherheits-Integrity-Level ist für den Flammwächter notwendig, und welche Ausfallwahrscheinlichkeit (PFD oder PFH und Wert) ist zulässig?



Nach Sicherheitsgraph: C3 – F1 – W2: e, $\rightarrow SIL3$ (2)

„Niedrige“ Anforderungsrate: PFD (1)

PFD_{gesamt} bei SIL3: 10^{-3} (1)

$PFD_{Flammw.} = 25\% = 0,25 * 10^{-3}$ (2)

b) Ist der beschriebene Flammwächter geeignet? (nur nach PFD / PFH bewerten)

$\lambda_D = 5 * 10^{-6}$ $PFD = \lambda_D * t_{CE} = 5 * 10^{-6} * 44 = 0,22 * 10^{-3}$ (2)

ist kleiner als zulässig, Flammwächter ist geeignet (2)

2012 / 1

5. Sicherheit

10 Punkte, Vorgabe 10 Minuten

An einer automatischen Fräsmaschine muss ein Arbeiter während einer ganzen Schicht die Werkstücke ein- und ausspannen. Während die Maschine fräst wäre es möglich, dass er in den Arbeitsbereich hineingreift und dabei einen Finger verliert. Eine Vermeidung wäre ihm natürlich möglich.

Der Arbeitsbereich der Maschine ist durch eine Abdeckung gesichert, die geschlossen sein muss, damit der Motor Spannung erhält. Ob die Abdeckung geschlossen ist prüft ein Initiator (Dreileiterschaltung), ein angeschlossenes Auswertegerät liefert bei geschlossener Abdeckung 24 V / max. 1 A an ein Relais, das dann die Spannungszufuhr zum Motor durchschaltet. Für den Initiator mit Auswertegerät ist das folgende Auftreten von Fehlern bekannt:

- keine Spannung am Ausgang, obwohl die Abdeckung geschlossen ist: 7 mal in 10^7 Stunden,
 - Spannung am Ausgang, obwohl die Abdeckung nicht geschlossen ist: 4 mal in 10^7 Stunden.
- Beide Fehler können nicht überwacht (entdeckt) werden.

a) Bestimmen Sie den zu fordernden SIL anhand der Tabellen in DIN 62061

$S=3; F=5; W=3; P=3$; somit $K=11$; bei $S=3$ ergibt sich SIL2 (2)

2

b) Welche Ausfallwahrscheinlichkeit ist für Sensor + Auswertegerät zulässig? Verwenden Sie die Fehlerrisiko- Aufteilung nach Norm

Hohe Anforderungsrate, daher PFH (1)

Bei SIL2: $PFH = 10^{-6}$ (1)

Sensor + Eingabe + Verarbeitung: 50% (alternativ: 60%) (2)

Das bedeutet $PFH = 0,5 \cdot 10^{-6} / 0,6 \cdot 10^{-6}$ (1)

5

c) Genügt der Initiator mit seinem Auswertegerät den Sicherheitsanforderungen?

(nur die Ausfallwahrscheinlichkeit betrachten, nicht FMEDA usw.)

$\lambda_{DU} = 4 \cdot 10^{-7}$, mit $PFH \cong \lambda_{DU}$ $PFH = 0,4 \cdot 10^{-6}$ (1) d.h. ausreichend (1)

(1)

3

2012 / 2

4. Betriebsmittelanforderungen: Sicherheit

8 Punkte, Vorg. 10 Minuten

An einer automatischen Fräsmaschine muss ein Arbeiter während einer ganzen Schicht die Werkstücke ein- und ausspannen. Während die Maschine fräst könnte er in den Arbeitsbereich hineingreifen und einen Finger verlieren. Die Maschine ist durch eine Abdeckung gesichert, die während des Fräsens geschlossen sein muss. Dies wird mit einem mechanischen Schalter überprüft, der ein Relais schaltet, das die Motorspannung durchschaltet.

a) Welchen Sicherheitslevel (SIL) muss diese Einrichtung nach DIN 62061 erreichen?

$S=3; F=5; W=3; P=3$; somit $K=11$; bei $S=3$ ergibt sich SIL2 (2)

2

b) Aus Erfahrung mit solchen Schaltern ist bekannt: In 10^7 Std. kann ein Schalter 2 mal so hängen bleiben, dass er „Abdeckung zu“ meldet, obwohl diese offen ist, und in der gleichen Zeit 4 mal „Abdeckung offen“ melden, obwohl diese zu ist.

Wenn der Schalter 1/3 der insgesamt (mit Relais und Motorspannungsabschaltung) erlaubten

Ausfallwahrscheinlichkeit ausnutzen darf: **erfüllt er dann die Forderung nach a)? Begründung?**

SIL2 $\rightarrow PFH \leq 10^{-6}$ für Sensor $0,33 \cdot 10^{-6}$ erlaubt. $PFH \sim \lambda_{DU}$ $PFH_{\text{Sensor}} = 2 \cdot 10^{-7} = 0,2 \cdot 10^{-6}$, also: OK (1) (1) (1) (2)

6

5. Sicherheit

14 Punkte, Vorgabe 15 Minuten

An einer automatischen Fräsmaschine muss ein Arbeiter während einer ganzen Schicht die Werkstücke ein- und ausspannen. Während die Maschine fräst wäre es möglich dass er in den Arbeitsbereich hineingreift und dabei einen Finger verliert. Eine Vermeidung wäre ihm natürlich möglich.

Der Arbeitsbereich der Maschine ist durch eine Abdeckung gesichert, die geschlossen sein muss, damit der Motor Spannung erhält. Ob die Abdeckung geschlossen ist prüft ein Initiator (Dreileiterschaltung), ein angeschlossenes Auswertegerät liefert bei geschlossener Abdeckung 24 V / max. 1 A an ein Relais, das dann die Spannungszufuhr zum Motor durchschaltet. Für den Initiator mit Auswertegerät ist das folgende Auftreten von Fehlern bekannt:

- keine Spannung am Ausgang, obwohl die Abdeckung geschlossen ist: 7 mal in 10^7 Stunden,
- Spannung am Ausgang, obwohl die Abdeckung nicht geschlossen ist: 4 mal in 10^7 Stunden.

Beide Fehler können nicht überwacht (entdeckt) werden.

2

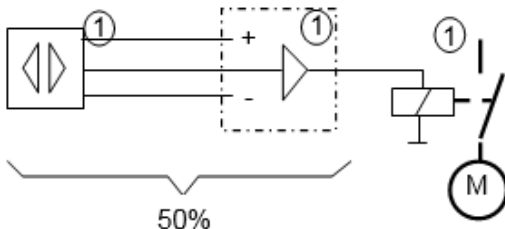
a) Bestimmen Sie den zu fordernden SIL anhand der DIN 62061

$S=3; F=5; W=3; P=3$; somit $K=11$; bei $S=3$ ergibt sich SIL2

②

b) Skizzieren Sie sich die Anordnung. Welche Ausfallwahrscheinlichkeit ist für Sensor + Auswertegerät zulässig? (Verwenden Sie die Fehlerrisiko- Aufteilung nach Norm)

8



Hohe Anforderungsrate, daher PFH ①

Bei SIL2: $PFH = 10^{-6}$ ①

Sensor + Eingabe + Verarbeitung: 50% (alternativ: 60%) ②

Das bedeutet $PFH = 0,5 \cdot 10^{-6} / 0,65 \cdot 10^{-6}$ ①

c) Genügen der Initiator mit seinem Auswertegerät den Sicherheitsanforderungen?

(nur die Ausfallwahrscheinlichkeit betrachten, nicht FMEDA usw.)

4

$\lambda_{DU} = 4 \cdot 10^{-7}$, mit $PFH \cong \lambda_{DU}$ $PFH = 0,4 \cdot 10^{-6}$ ① d.h. ausreichend ②

①

4. Betriebsmittelanforderungen: Sicherheit, Verfügbarkeit, Beschaltung 15 Punkte, Vorg. 15 Minuten

An einer automatischen Fräsmaschine muss ein Arbeiter während einer ganzen Schicht die Werkstücke ein- und ausspannen. Während die Maschine fräst könnte er in den Arbeitsbereich hineingreifen und dabei einen Finger verlieren. Eine Vermeidung wäre möglich. Der Arbeitsbereich der Maschine ist durch eine Abdeckung gesichert, die geschlossen sein muss. Dies wird bisher mit einem mechanischen Schalter überprüft, der ein Relais schaltet, das die Motorspannung durchschaltet.

a) **Welchen Sicherheitslevel (SIL) muss diese Einrichtung nach DIN 62061 erreichen?**

2

$S=3; F=5; W=3; P=3$; somit $K=11$; bei $S=3$ ergibt sich **SIL2** (2)

b) **Wie hoch ist die Verfügbarkeit der Maschine**, wenn der Schalter durchschnittlich 4 x im Jahr so ausfällt, dass er auch bei geschlossener Abdeckung die Spannung nicht durchschaltet? Die Maschine wird pro Tag 7 Std. benötigt, rechnen Sie mit 20 Tagen pro Monat. Die Ausfallkosten betragen ca. 600 € / Std., die Reparatur kostet 150 € / Std. und dauert 2 Std.

Ausfall alle 3 Monate, $3 \cdot 20 \text{ Tg.} \cdot 7 \text{ Std.} = 420 \text{ Betriebsstunden} = \text{MTBF}$, $\text{MTTR} = 2 \text{ Std.}$

$$V = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = \frac{420}{420 + 2} = 0,995 \quad (2)$$

2

c) **Durch welche Maßnahmen könnte die Verfügbarkeit verbessert werden?**

- vorbeugende Wartung: Schalter außerhalb der Betriebszeit rechtzeitig wechseln (2)
- besseren Schalter einsetzen (1)

3

d) **Nach welcher Zeit würde sich ein induktiver Initiator amortisieren**, der in 2 Jahren (Betriebszeit) nur einmal ausfällt? Der Austausch würde ca. 9000 € kosten.

2

$$\text{Ausfälle(gespart)} = \frac{\text{Austauschkosten}}{\text{Ausfallkosten(alt)}} = \frac{9000}{2 \cdot (600 + 150)} = 6, \text{ d.h. nach } 6 \cdot \text{MTBF}_{\text{alt}} = 1,5 \text{ Jahren} \\ (= 18 \text{ Mon.}) \quad (2) \\ \text{oder } 6 \cdot 420 = 2520 \text{ Betr. Std.}$$

e) **Mit welchem Bauelement (Typ, Werte) könnte das Schütz beschaltet werden**, das den Motor schaltet und die neue Messung stört? Spule: 230 V AC / 10 mA, Gleichspannungswiderstand 6 kΩ, max. 1 Schalt. / s

6

$$L = \frac{\sqrt{Z^2 - R^2}}{\omega} = \frac{\sqrt{529 \cdot 10^6 - 36 \cdot 10^6}}{314} = 70,7 \text{ H} \quad P = \frac{0,5LI^2}{T} = \frac{0,5 \cdot 70,7 \cdot 0,1 \cdot 10^{-3}}{1} = 3,5 \text{ mW}$$

$$U_{\text{Spitze}} = 230 \cdot 1,41 = 324 \text{ V}$$

d.h.: Bauelement: Varistor, ca. 5 mW / 350 V

(2) (2) (2)