

Lösungen: Übungsaufgaben zur Fehlerbaumanalyse

Lösung 5.1

$$\begin{aligned}
 y &= (x_1 \wedge x_2) \vee (x_3 \wedge \overline{x_4}) \\
 \rightarrow R_s &= 1 - (1 - R_1 R_2) \cdot (1 - R_3 \underbrace{(1 - R_4)}_{F_4})
 \end{aligned}$$

Negieren und Anwenden von de Morgan:

$$\begin{aligned}
 \overline{y} &= \overline{(x_1 \wedge x_2) \vee (x_3 \wedge \overline{x_4})} \\
 \overline{y} &= \overline{(x_1 \wedge x_2)} \wedge \overline{(x_3 \wedge \overline{x_4})} \\
 \overline{y} &= (\overline{x_1} \vee \overline{x_2}) \wedge (\overline{x_3} \vee x_4)
 \end{aligned}$$

Fehlerbaum:

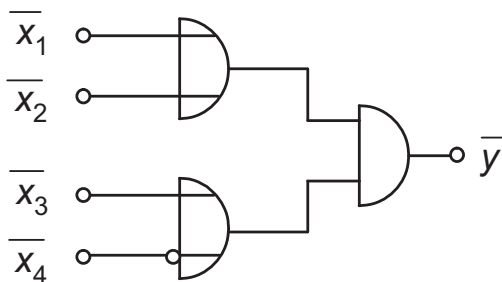
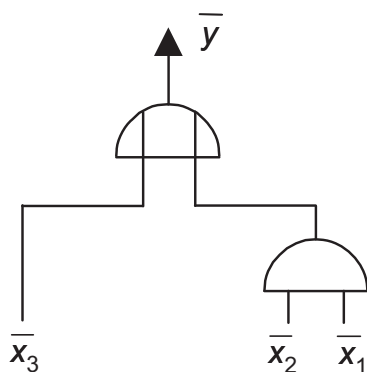


Abb. Lösung 5.1

Lösung 5.2

a) Fehlerbaum



Funktionsbaum

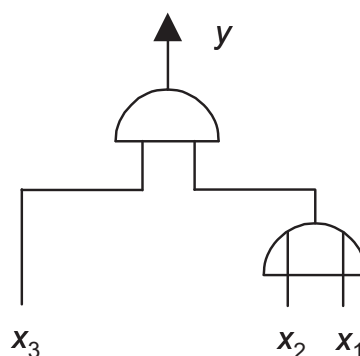


Abb. Lösung 5.2a

$$\begin{aligned}
 \overline{y} &= \overline{x_3} \vee (\overline{x_1} \wedge \overline{x_2}) \\
 F_s &= 1 - (1 - F_3) \cdot (1 - F_1 \cdot F_2) \\
 F_s &= 1 - R_3 \cdot (1 - (1 - R_1) \cdot (1 - R_2))
 \end{aligned}$$

b)

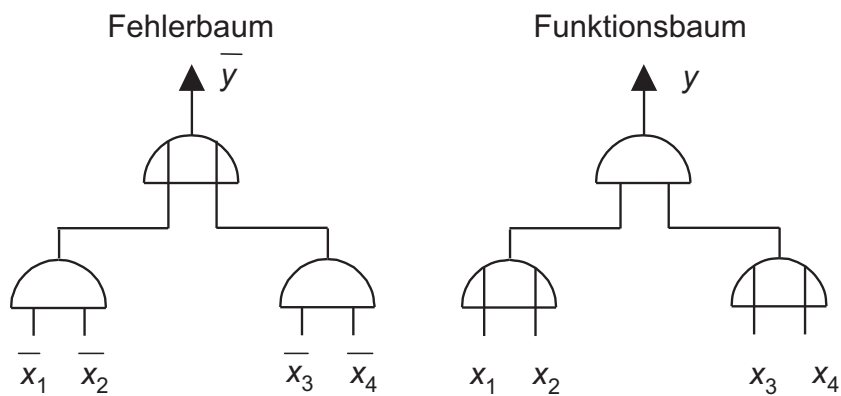


Abb. Lösung 5.2b

$$\bar{y} = (\bar{x}_1 \wedge \bar{x}_2) \vee (\bar{x}_3 \wedge \bar{x}_4)$$

$$F_S = 1 - (1 - F_1 \cdot F_2) \cdot (1 - F_3 \cdot F_4)$$

$$F_S = 1 - (1 - (1 - R_1) \cdot (1 - R_2)) \cdot (1 - (1 - R_3) \cdot (1 - R_4))$$

c)

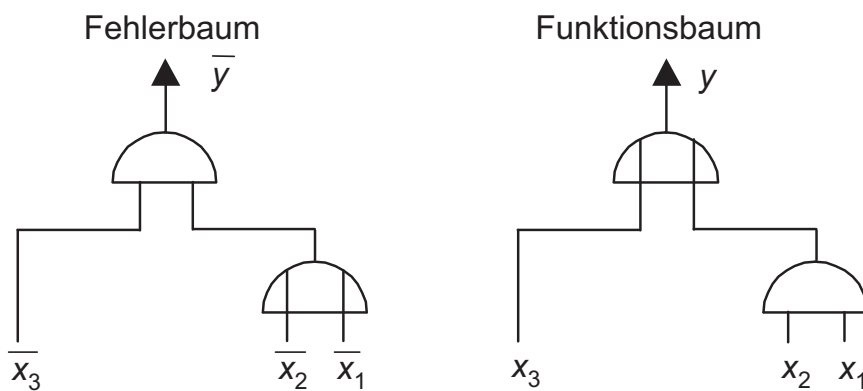


Abb. Lösung 5.2c

$$\bar{y} = \bar{x}_3 \wedge (\bar{x}_1 \vee \bar{x}_2)$$

$$F_S = F_3 \cdot (1 - (1 - F_1) \cdot (1 - F_2))$$

$$F_S = (1 - R_3) \cdot (1 - R_1 \cdot R_2)$$

d)

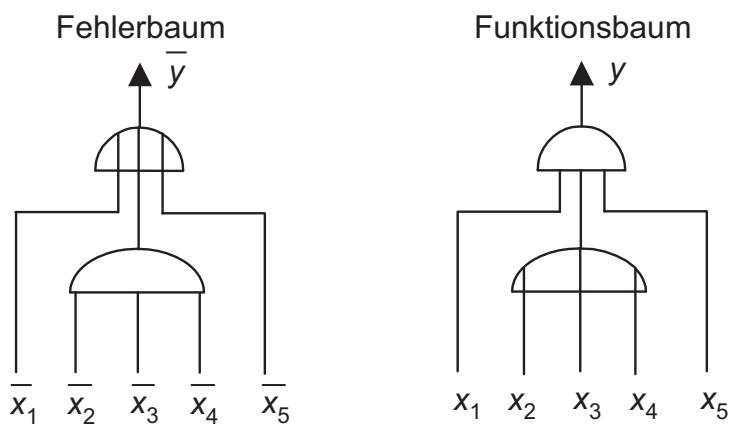


Abb. Lösung 5.2d

$$\bar{y} = \bar{x}_1 \vee (\bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4) \vee \bar{x}_5$$

$$F_S = 1 - (1 - F_1) \cdot (1 - F_2 \cdot F_3 \cdot F_4) \cdot (1 - F_5)$$

$$F_S = 1 - R_1 \cdot (1 - (1 - R_2) \cdot (1 - R_3) \cdot (1 - R_4)) \cdot R_5$$

e)

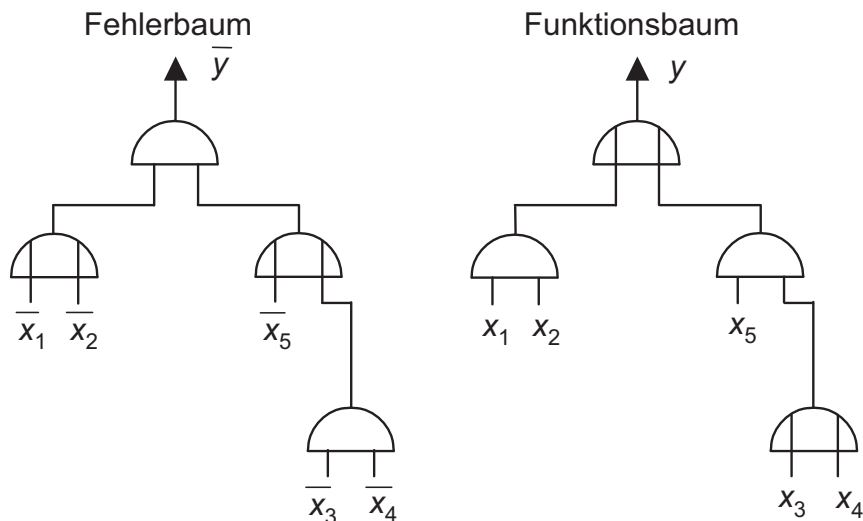


Abb. Lösung 5.2e

$$\bar{y} = (\bar{x}_1 \vee \bar{x}_2) \wedge (\bar{x}_5 \vee (\bar{x}_3 \wedge \bar{x}_4))$$

$$F_S = F_a \cdot F_b \text{ und } F_a = 1 - (1 - F_1) \cdot (1 - F_2)$$

$$F_b = 1 - (1 - F_5) \cdot (1 - F_3 \cdot F_4)$$

$$F_S = (1 - (1 - F_1) \cdot (1 - F_2)) \cdot (1 - (1 - F_5) \cdot (1 - F_3 \cdot F_4))$$

$$F_S = (1 - R_1 \cdot R_2) \cdot (1 - R_5 \cdot (1 - (1 - R_3) \cdot (1 - R_4)))$$

Lösung 5.3

a) Fehlerbaum aus Prinzipskizze und Beschreibung:

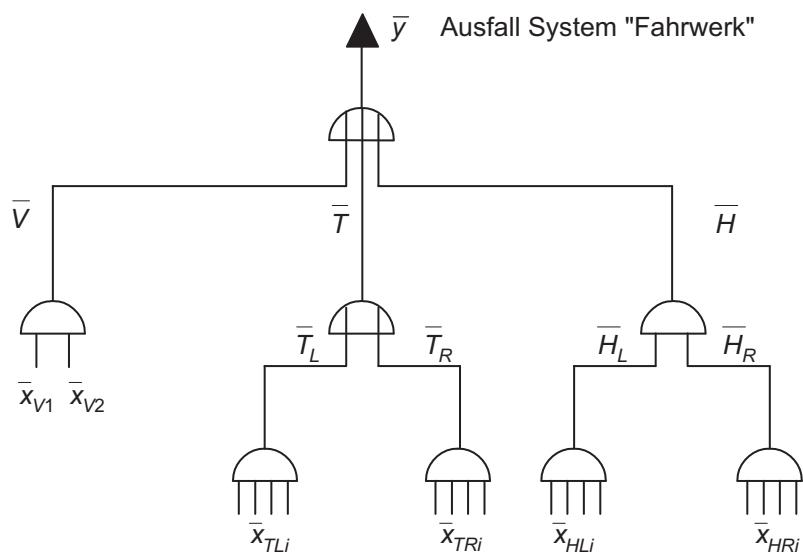


Abb. Lösung 5.3a

b) Geben Sie die Boolesche Systemfunktion für den Ausfall des Systems Fahrwerk an.

$$\text{aus a) } \bar{y} = \bar{V} \vee \bar{T} \vee \bar{H}$$

$$\text{mit } \bar{V} = \bar{x}_{V1} \wedge \bar{x}_{V2}$$

$$\text{und } \bar{T} = \bar{T}_L \vee \bar{T}_R$$

$$\text{mit } \bar{T}_L = \bigwedge_{i=1}^4 \bar{x}_{TLi}, \bar{T}_R = \bigwedge_{i=1}^4 \bar{x}_{TRi} \text{ und } \bar{H} = \bar{H}_L \wedge \bar{H}_R$$

$$\text{mit } \bar{H}_L = \bigwedge_{i=1}^4 \bar{x}_{HLi} \text{ und } \bar{H}_R = \bigwedge_{i=1}^4 \bar{x}_{H Ri}.$$

Einsetzen ergibt:

$$\bar{y} = (\bar{x}_{V1} \wedge \bar{x}_{V2}) \vee \left(\left(\bigwedge_{i=1}^4 \bar{x}_{TLi} \right) \vee \left(\bigwedge_{i=1}^4 \bar{x}_{TRi} \right) \right) \vee \left(\left(\bigwedge_{i=1}^4 \bar{x}_{HLi} \right) \wedge \left(\bigwedge_{i=1}^4 \bar{x}_{H Ri} \right) \right).$$

c) Ermitteln sie die Systemgleichung für die Ausfallwahrscheinlichkeit F_S .

Aus Zusatzaufschrieb:

$$F_S = 1 - (1 - F_V) \cdot (1 - F_T) \cdot (1 - F_H)$$

$$\text{mit } F_V = F_{V1} \cdot F_{V2}, F_T = 1 - \left(1 - \prod_{i=1}^4 F_{TLi} \right) \cdot \left(1 - \prod_{i=1}^4 F_{TRi} \right) \text{ und}$$

$$F_H = \prod_{i=1}^4 F_{HLi} \cdot \prod_{i=1}^4 F_{H Ri}.$$

d) Geben sie die Boolesche Systemfunktion für die Zuverlässigkeit des Fahrwerks an.

Linke und rechte Seite der Systemfunktion aus b) negieren

$$y = \overline{\bar{V} \vee \bar{T} \vee \bar{H}}$$

$$\text{De Morgan anwenden: } y = V \wedge T \wedge H \quad \text{mit } V = x_{V1} \vee x_{V2}$$

$$\text{und } T = T_L \wedge T_R, T_L = \bigvee_{i=1}^4 x_{TLi} \text{ und } T_R = \bigvee_{i=1}^4 x_{TRi}$$

$$\text{und } H = H_L \vee H_R, H_L = \bigvee_{i=1}^4 x_{HLi} \text{ und } H_R = \bigvee_{i=1}^4 x_{H Ri}$$

$$\Rightarrow y = (x_{V1} \vee x_{V2}) \wedge \left(\left(\bigvee_{i=1}^4 x_{TLi} \right) \wedge \left(\bigvee_{i=1}^4 x_{TRi} \right) \right) \wedge \left(\left(\bigvee_{i=1}^4 x_{HLi} \right) \vee \left(\bigvee_{i=1}^4 x_{H Ri} \right) \right).$$

e) Ermitteln sie die Systemgleichung für die Zuverlässigkeit R_S .

$$R_S = R_V \cdot R_T \cdot R_H \quad (\text{aus Folie, oder } R = 1 - F)$$

$$\text{mit } R_V = 1 - (1 - R_{V1}) \cdot (1 - R_{V2}),$$

$$R_T = \left(1 - \prod_{i=1}^4 (1 - R_{TLi}) \right) \cdot \left(1 - \prod_{i=1}^4 (1 - R_{TRi}) \right) \text{ und}$$

$$R_H = 1 - \left(1 - \left(1 - \prod_{i=1}^4 (1 - R_{HLi}) \right) \cdot \left(1 - \left(1 - \prod_{i=1}^4 (1 - R_{H Ri}) \right) \right) \right).$$

- f) Stellen sie das dazugehörige Blockschaltbild dar
(aus Boolescher Systemfunktion für Funktionsfähigkeit des Fahrwerks).

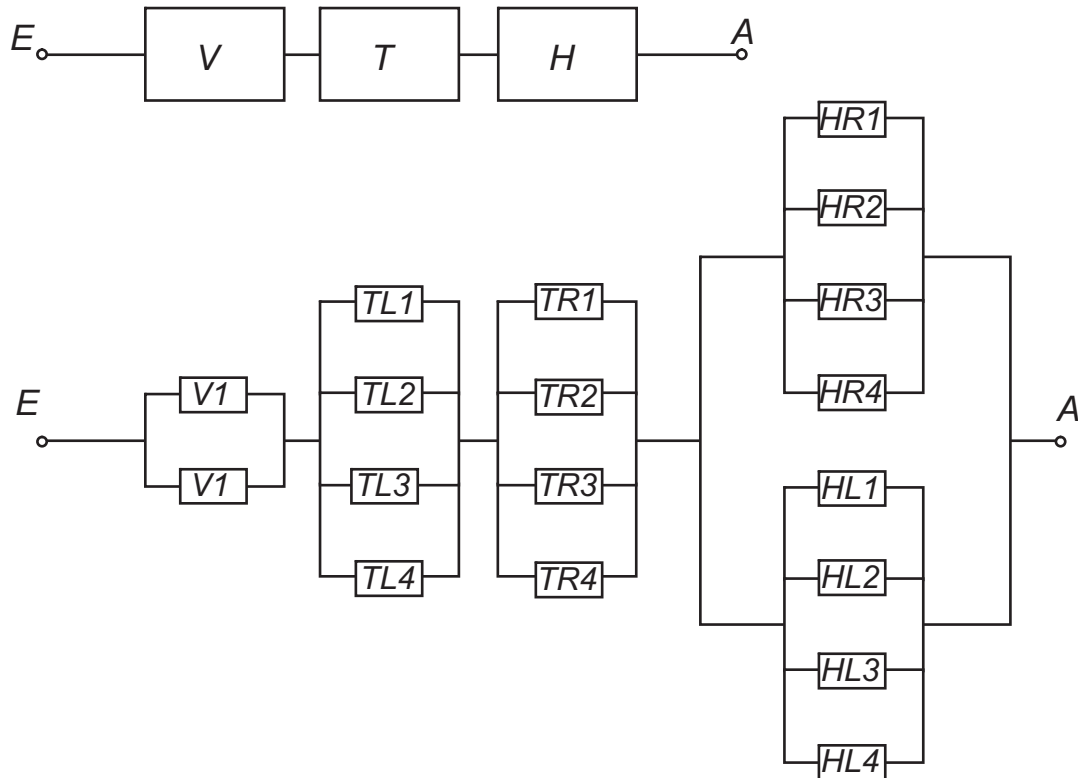
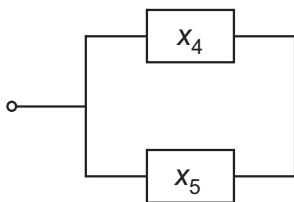


Abb. Lösung 5.3f

Lösung 5.4

x_2 ständig funktionsfähig

$R_I(t)$



x_2 ständig ausgefallen

$R_{II}(t)$

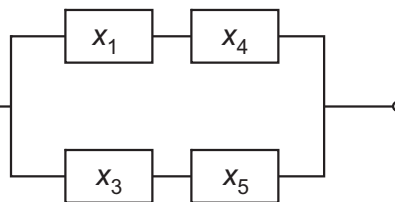


Abb. Lösung 5.4

$$R = R_2 \cdot R_I + (1 - R_2) \cdot R_{II}$$

mit $R_I = 1 - (1 - R_4) \cdot (1 - R_5)$

$$R_{II} = 1 - (1 - R_1 \cdot R_4) \cdot (1 - R_3 \cdot R_5)$$

$$R = R_2(1 - (1 - R_4) \cdot (1 - R_5)) + (1 - R_2) \cdot (1 - (1 - R_1 \cdot R_4) \cdot (1 - R_3 \cdot R_5)).$$

Lösung 5.5

a) Ermitteln Sie die Systemfunktion für den Ausfall des Steuergeräts.

$$\begin{aligned}\overline{y} &= \overline{x_1} \vee \overline{x_2} \vee \overline{x_{34}} \vee \overline{x_5} \vee \overline{x_{69}} \vee \overline{x_{10}} \\ \overline{x_{34}} &= \overline{x_3} \wedge \overline{x_4} \\ \overline{x_{69}} &= \overline{x_{68}} \wedge \overline{x_9} \\ \overline{x_{68}} &= \overline{x_6} \vee \overline{x_7} \vee \overline{x_8} \\ y &= \overline{x_1} \vee \overline{x_2} \vee (\overline{x_3} \wedge \overline{x_4}) \vee \overline{x_5} \vee ((\overline{x_6} \vee \overline{x_7} \vee \overline{x_8}) \wedge \overline{x_9}) \vee \overline{x_{10}}\end{aligned}$$

b) Berechnen Sie die Ausfallwahrscheinlichkeit des Systems.

$$\begin{aligned}F_S &= 1 - (1 - F_1) \cdot (1 - F_2) \cdot (1 - F_{34}) \cdot (1 - F_5) \cdot (1 - F_{69}) \cdot (1 - F_{10}) \\ F_{34} &= F_3 \cdot F_4 \\ F_{69} &= F_{68} \cdot F_9 \\ F_{68} &= 1 - (1 - F_6) \cdot (1 - F_7) \cdot (1 - F_8) \\ F_S &= 1 - (1 - F_1) \cdot (1 - F_2) \cdot (1 - F_3 F_4) \cdot (1 - F_5) \\ &\quad \cdot (1 - [1 - (1 - F_6) \cdot (1 - F_7) \cdot (1 - F_8)] \cdot F_9) \cdot (1 - F_{10})\end{aligned}$$

c) Geben Sie die Systemfunktion für die Funktionsfähigkeit des Steuergeräts an.

Negieren und Anwenden von De Morgan

$$\begin{aligned}\overline{\overline{y}} &= \overline{\overline{x_1} \vee \overline{x_2} \vee \overline{x_{34}} \vee \overline{x_5} \vee \overline{x_{69}} \vee \overline{x_{10}}} \\ y &= \overline{x_1} \wedge \overline{x_2} \wedge \overline{x_{34}} \wedge \overline{x_5} \wedge \overline{x_{69}} \wedge \overline{x_{10}} \\ x_{34} &= x_3 \vee x_4 \\ x_{69} &= x_{68} \vee x_9 \\ x_{68} &= x_6 \wedge x_7 \wedge x_8 \\ y &= \overline{x_1} \wedge \overline{x_2} \wedge (x_3 \vee x_4) \wedge \overline{x_5} \wedge ((x_6 \wedge x_7 \wedge x_8) \vee x_9) \wedge \overline{x_{10}}\end{aligned}$$

d) Stellen Sie das Blockschaltbild dar.

Aus Systemfunktion für Funktionsfähigkeit → Blockschaltbild

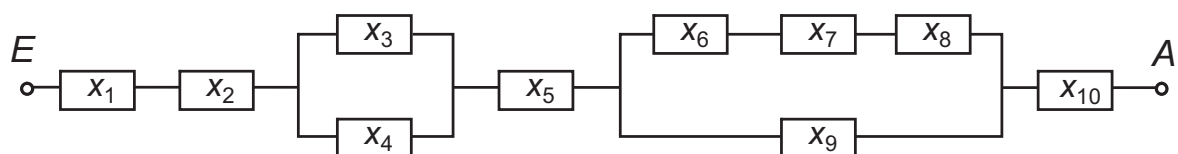


Abb. Lösung 5.5d

Lösung 5.6

a) Multilinearform

x_1	x_2	x_3	x_4	System
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	1
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

$$0,1 \cdot 0,9 \cdot 0,1 \cdot 0,1 = 0,0009$$

$$0,1 \cdot 0,9 \cdot 0,1 \cdot 0,9 = 0,0081$$

$$0,1 \cdot 0,9 \cdot 0,9 \cdot 0,1 = 0,0081$$

$$0,1 \cdot 0,9 \cdot 0,9 \cdot 0,9 = 0,0729$$

$$0,9 \cdot 0,1 \cdot 0,1 \cdot 0,9 = 0,0081$$

$$0,9 \cdot 0,1 \cdot 0,9 \cdot 0,1 = 0,0081$$

$$0,9 \cdot 0,1 \cdot 0,9 \cdot 0,9 = 0,0729$$

$$0,9 \cdot 0,9 \cdot 0,1 \cdot 0,1 = 0,0081$$

$$0,9 \cdot 0,9 \cdot 0,1 \cdot 0,9 = 0,0729$$

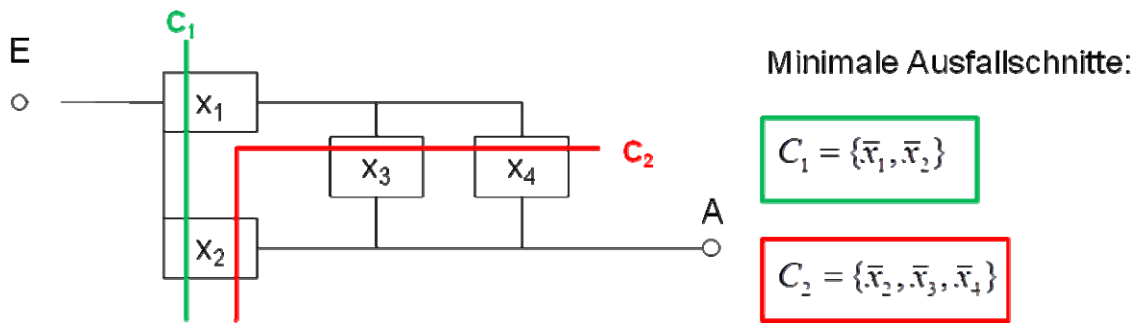
$$0,9 \cdot 0,9 \cdot 0,9 \cdot 0,1 = 0,0729$$

$$0,9 \cdot 0,9 \cdot 0,9 \cdot 0,9 = 0,6561$$

Systemüberlebenswahrscheinlichkeit MLNF:

$$R_{\text{Sys,MLNF}} = 0,1^3 \cdot 0,9 + 5 \cdot 0,1^2 \cdot 0,9^2 + 4 \cdot 0,1 \cdot 0,9^3 + 0,9^4 = 0,9891$$

b) Cut-Sets-Methode



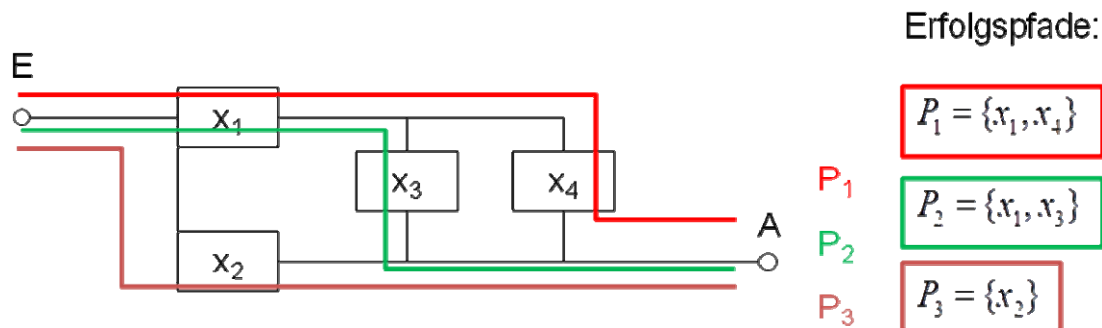
Verknüpfte Ausfallschnitte:

$$\bar{y} = (\bar{x}_1 \wedge \bar{x}_2) \vee (\bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4)$$

Systemzuverlässigkeit Cut-Sets:

$$R_{\text{Sys},C} = [1 - (1 - R_1)(1 - R_2)][1 - (1 - R_2)(1 - R_3)(1 - R_4)]$$

Path-Sets-Methode:



Verknüpfte Erfolgspfade:

$$y = (x_1 \wedge x_4) \vee (x_1 \wedge x_3) \vee (x_2)$$

Systemzuverlässigkeit Path-Sets:

$$R_{\text{Sys},P} = 1 - (1 - R_1 R_4)(1 - R_1 R_3)(1 - R_2)$$

c)

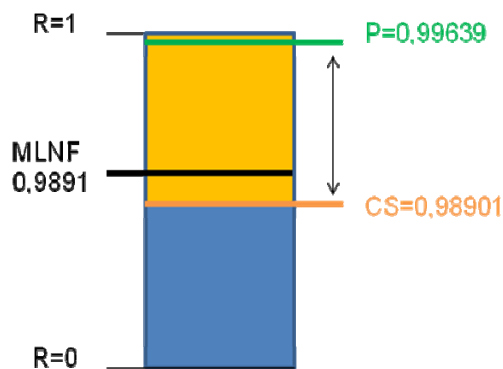
$$R_{Sys,C} = [1 - (1 - R_1)(1 - R_2)][1 - (1 - R_2)(1 - R_3)(1 - R_4)] =$$

$$= [1 - (1 - 0,9)(1 - 0,9)][1 - (1 - 0,9)(1 - 0,9)(1 - 0,9)] = 0,98901$$

$$R_{Sys,P} = 1 - (1 - R_1 R_4)(1 - R_1 R_3)(1 - R_2) =$$

$$= 1 - (1 - 0,9 \cdot 0,9)(1 - 0,9 \cdot 0,9)(1 - 0,9) = 0,99639$$

→ Das wahre Ergebnis, also das der MLNF liegt zwischen den Ergebnissen der Cut-Sets (Untergrenze) und der Path-Sets Methode (Obergrenze)



$$R_{Sys,C} \leq R_{Sys,MLNF} \leq R_{Sys,P}$$

Lösung 5.7

Eine Kollision des Zuges mit Fahrzeugen ist möglich, wenn sich der Zug auf dem Bahnübergang befindet und die Schranken nicht geschlossen sind. Die FTA versucht nun die Ursachen dafür auf die einzelnen Komponenten zu verteilen.

Eine Kollision kann entstehen, wenn der Zug nicht bremst, obwohl der Bahnübergang nicht signalisiert hat, dass er gesichert ist (keine Freigabe), oder wenn der Bahnübergang sich als gesichert betrachtet (sendet Freigabe), obwohl die Schranken noch offen sind. Das ist die oberste Zerlegung im Fehlerbaum. Die Ursache dafür, dass der Zug nicht bremst, ist ein Defekt der Bremsen (primär oder sekundär) oder die Bremsen haben kein Brems-Signal bekommen. Dann liegt ein Fehler in der Zugsteuerung vor. Die weitere Analyse der Zugsteuerung kann aus dem Fehlerbaum entnommen werden und wird hier nicht weiter beschrieben.

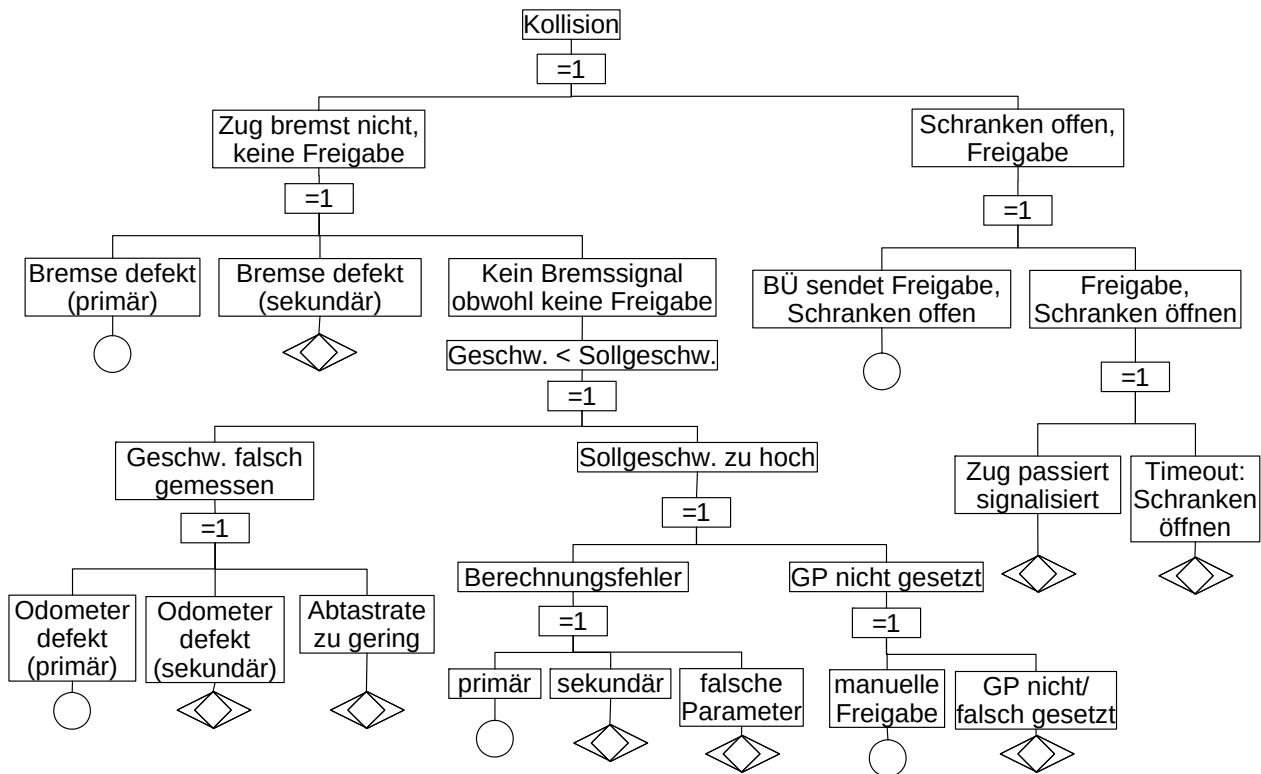


Abb. Fehlerbaum funkbasierter Bahnübergang

Auf Seite des Bahnübergangs ist der Grund für eine Freigabe bei offenem Bahnübergang entweder das Senden der Freigabe, obwohl die Schranken nicht geschlossen sind (dies ist ein Basisfehler, den die Bahnübergangsteuerung nicht zulassen darf), oder der Bahnübergang hat eine Freigabe gesendet, öffnet aber die Schranken, obwohl der Zug noch nicht passiert hat. Die Gründe dafür sind entweder, dass die Schranken wieder geöffnet werden, da die maximale Schrankenschließzeit erreicht wurde, oder, dass fälschlicherweise das Passieren des Zugs signalisiert wird. Gründe dafür werden nicht weiter untersucht.

Bei der Auswertung des Fehlerbaums sieht man, dass die Modellierung keine Redundanzen enthält, da keine Und-Gatter vorkommen. Deshalb sind die minimalen Schnittmengen einelementig. Des Weiteren erkennt man, dass die manuelle Freigabe, bei der das Zugpersonal den Bahnübergang sichert, ein Risiko darstellt, das nicht durch technische Maßnahmen verringert werden kann. Deshalb müssen strenge Vorschriften für diesen Vorgang definiert werden. Weiterhin kann ein defekter Ausschaltkontakt den Bahnübergang zum Öffnen veranlassen, obwohl der Zug noch nicht passiert hat.

Die FTA zeigt außerdem eine Sicherheitslücke in der Anforderungsbeschreibung der Steuerung auf. Die Beschreibung der Bahnübergangsteuerung fordert, dass nach einer maximalen Schließzeit der Bahnübergang öffnet und als ungesichert zu betrachten ist. Dies gilt auch dann, wenn der Zug den Bahnübergang noch nicht passiert hat. In der ersten Variante der Beschreibung der funkbasierten Bahnübergangsteuerung gab es keinen Hinweis darauf, wie in diesem Fall weiter zu verfahren ist.

Das Szenario für eine mögliche Kollision sieht nun folgendermaßen aus. Der Zug nähert sich einem Bahnübergang und stößt den Schließvorgang an. Die Bahnübergangsteuerung sichert den Bahnübergang, der Zug fordert die Freigabe an und erhält sie. Wegen einer Störung benötigt der Zug aber länger als die maximale Schrankenschließzeit, um den Bahnübergang zu passieren. Ist die maximale Schrankenschließzeit abgelaufen, gilt der Bahnübergang als ungesichert und die Schranken öffnen wieder. Nun kann der Zug,

der ja eine Freigabe für den Bahnübergang besitzt, in den geöffneten Bahnübergang einfahren. Das Fehlerszenario ist im Fehlerbaum der Abbildung ganz rechts zu sehen (Timeout: Schranken öffnen).

In der aktuellen Version der Fallstudienbeschreibung ist diese Sicherheitslücke nicht mehr enthalten. Einmal erkannt, ist die Lösung sehr einfach: die Freigabe für den Zug verfällt nach der maximalen Schrankenschließzeit und der Zug muss erneut eine Freigabe anfordern.