Test und Verlässlichkeit
Grosse Übung zu Foliensatz 1

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_GU1)

16. Mai 2022

Inhalt: Große Übungen zu Foliensatz 1

Verlässlichkeit

Aufgabe 1.1: Aspekte und Ebenen der Verlässlichkeit

1. Welche drei Arten von Aspekten der Verlässlickeit unterscheidet Lapri?
2. Auf welchen drei Ebenen erfolgt die Sicherung der Verlässlichkeit?

1. Welche drei Arten von Aspekten der Verlässlickeit unterscheidet Lapri?
2. Auf welchen drei Ebenen erfolgt die Sicherung der Verlässlichkeit?

1. Aspekten der Verlässlickeit:
   1. Gefährdungen (Threats),
   2. Gegenmaßnahmen zur Gefährdungsminderung (Means) und
   3. Kenngrößen (Attributes) zur Quantizierung der Gefährdungen und Gegenmaßnahmen.
2. Ebenen zur Sicherung der Verlässlichkeit:
   1. Fehlervermeidung,
   2. Fehlerbeseitigung,
   3. Überwachung und Umgang mit FF einschließlich Fehlertoleranz.

Verfügbarkeit

Aufgabe 1.2: Zulässige mittlere Reparaturzeit

Für eine Steuerung mit einer $MTTF \geq 2\,\mathrm{Jahre}$ ist eine Verfügbarkeit von

$$V \geq 1 - 10^{-6}$$

gefordert. In 99% der Fälle startet das System ohne Reparatur automatisch neu und ist nach 30 s wieder betriebsbereit und in 1% der Fälle muss zusätzlich die Steuerung getauscht werden.

a) Wie groß ist die zulässige mittlere Reparaturzeit $MTTR$?

b) Wie lange darf der Tausch der Steuerung im Mittel dauern?

Für eine Steuerung mit einer $MTTF \geq 2\,\text{Jahre}$ ist eine Verfügbarkeit von

$$V \geq 1 - 10^{-6}$$

gefordert. In 99% der Fälle startet das System ohne Reparatur automatisch neu und ist nach 30 s wieder betriebsbereit und in 1% der Fälle muss zusätzlich die Steuerung getauscht werden.

a) Wie groß ist die zulässige mittlere Reparaturzeit $MTTR$?

$$V = \frac{MTTF}{MTTF + MTTR}$$

$$MTTR = MTTF \cdot \left(\frac{1}{V} - 1\right)$$

$$MTTR \geq 2\,\text{Jahre} \cdot \left(\frac{1}{1 - 10^{-6}} - 1\right) = 2\,\text{Jahre} \cdot \left(\frac{1 + 10^{-6}}{(1 - 10^{-6}) \cdot (1 + 10^{-6})} - 1\right)$$

$$= 2\,\text{Jahre} \cdot \left(\frac{1 + 10^{-6}}{1 - 10^{-12}} - 1\right) \approx \frac{2\,\text{Jahre}}{10^6} = 61{,}5\,\text{s}$$

Für eine Steuerung mit einer $MTTF \geq 2\,\mathrm{Jahre}$ ist eine Verfügbarkeit von

$$V \geq 1 - 10^{-6}$$

gefordert. In 99% der Fälle startet das System ohne Reparatur automatisch neu und ist nach 30 s wieder betriebsbereit und in 1% der Fälle muss zusätzlich die Steuerung getauscht werden.

b) Wie lange darf der Tausch der Steuerung im Mittel dauern?

MTTR abzüglich der 30 s für den Neustart sind im Mittel 31,6 s je Versagen für weitere Reparaturmaßnahmen übrig, d.h. für 1% der Versagen 3160 s = 52,7 min.

Der Tausch der Steuerung ist so zu organaisieren, dass er im Mittel weniger als eine Stunde dauert.

Zuverlässigkeit

Aufgabe 1.3: Zuverlässigkeit Gesamtsystem

Ein IT-System bestehe aus folgenden Komponenten:

Teilsystem	Rechner	Fest-platte	Stromver-sorgung	sonstiges
Teilzuverlässigkeit	Z_{R}	Z_{FP}	Z_{SV}	Z_{*}
Wert in SL/FF	1000	500	700	2000

Die Anzahl der gleichzeitigen FF mehrerer Teilsysteme und die Anzahl der FF eines Teilsystems ohne Gesamt-FF seien vernachlässigbar.

a) Welche Zuverlässigkeit hat das Gesamtsystem?

b) Welche FF-Rate hat das Gesamtsystem?

Ein IT-System bestehe aus folgenden Komponenten:

Teilsystem	Rechner	Fest-platte	Stromver-sorgung	sonstiges
Teilzuverlässigkeit	Z_{R}	Z_{FP}	Z_{SV}	Z_{*}
Wert in SL/FF	1000	500	700	2000

Die Anzahl der gleichzeitigen FF mehrerer Teilsysteme und die Anzahl der FF eines Teilsystems ohne Gesamt-FF seien vernachlässigbar.

a) Welche Zuverlässigkeit hat das Gesamtsystem?

b) Welche FF-Rate hat das Gesamtsystem?

a)

$$Z_{\mathrm{ges}} = \frac{1}{\frac{1}{1000} + \frac{1}{500} + \frac{1}{700} + \frac{1}{2000}} = 203\,\frac{\mathrm{SL}}{\mathrm{FF}}$$

b)

$$\zeta = \frac{1}{Z_{\mathrm{ges}}} = 4{,}93 \cdot 10^{-3}\,\frac{\mathrm{FF}}{\mathrm{SL}}$$

Sicherheit

Aufgabe 1.4: Zuverlässigkeit und Betriebssicherheit

Bei einem IT-System mit einer mittleren Zeit bis zur nächsten Fehlfunktionen von 10^3 Stunden gefährdet im Mittel jede hundertste Fehlfunktion die Betriebssicherheit $\left(\eta_{\mathrm{G}} = 10^{-2}\right)$. Mittlere Service-Dauer $MTS = 1\,\mathrm{h/SL}$.

a) Welche Fehlfunktionsrate und welche Zuverlässigkeit hat der Service?

b) Welche Betriebssicherheit hat der Service?

Bei einem IT-System mit einer mittleren Zeit bis zur nächsten Fehlfunktionen von 10^3 Stunden gefährdet im Mittel jede hundertste Fehlfunktion die Betriebssicherheit $\left(\eta_\mathrm{G} = 10^{-2}\right)$. Mittlere Service-Dauer $MTS = 1\,\mathrm{h/SL}$.

a) Welche Fehlfunktionsrate und welche Zuverlässigkeit hat der Service?

b) Welche Betriebssicherheit hat der Service?

a) FF-Rate / Zuverlässigkeit:

$$\zeta = \frac{MTTF}{MTS} = 10^{-3}\,\mathrm{FF/SL}$$
$$Z = 1/\zeta = 10^3\,\mathrm{SL/FF}$$

b) Betriebssicherheit:

$$Z_\mathrm{S} = Z/\eta_\mathrm{G} = 10^5\,\mathrm{SL/GFF}$$

Fehlerbehandlung

Kenngrößen

Aufgabe 1.5: Scheinbare und tatsächliche Zuverlässigkeit

Bei der Kontrolle von 10^5 SL sind 10^3 FF aufgetreten, von denen 600 FF erkannt wurden. Darüber hinaus wurden 10 SL als FF ausgewiesen, die in Wirklichkeit korrekt ausgeführt wurden. Welche Schätzwerte ergeben sich daraus für

a) die beobachtete Zuverlässigkeit?

b) die tatsächliche Zuverlässigkeit?

c) die Fehlfunktionsüberdeckung der Kontrolle?

d) die Phantom-FF-Rate?

Bei der Kontrolle von 10^5 SL sind 10^3 FF aufgetreten, von denen 600 FF erkannt wurden. Darüber hinaus wurden 10 SL als FF ausgewiesen, die in Wirklichkeit korrekt ausgeführt wurden. Welche Schätzwerte ergeben sich daraus für

a) die beobachtete Zuverlässigkeit?

b) die tatsächliche Zuverlässigkeit?

a) Beobachtete Zuverlässigkeit:

$$Z_{\text{Beob}} = \frac{\#SL}{\#EFF + \#PFF} \approx \frac{10^5\,\text{SL}}{610\,\text{FF}} = 164\,\frac{\text{SL}}{\text{FF}}$$

($\#EFF$ – Anzahl der erkannten FF, $\#PFF$ – Anzahl der Phantom-FF).

b) Tatsächliche Zuverlässigkeit:

$$Z = \frac{\#SL}{\#FF} = \frac{10^5\,\text{SL}}{10^3\,\text{FF}} = 100\,\frac{\text{SL}}{\text{FF}}$$

Bei der Kontrolle von 10^5 SL sind 10^3 FF aufgetreten, von denen 600 FF erkannt wurden. Darüber hinaus wurden 10 SL als FF ausgewiesen, die in Wirklichkeit korrekt ausgeführt wurden. Welche Schätzwerte ergeben sich daraus für

c) die Fehlfunktionsüberdeckung der Kontrolle?

d) die Phantom-FF-Rate?

c) Erkennungs- und Maskierungswahrscheinlichkeit der Kontrolle:

$$FFC = \frac{\#EFF}{\#FF} = \frac{600\,\mathrm{FF}}{1000\,\mathrm{FF}} = 60\%$$

d) Phantom-FF-Rate:

$$\zeta_{\mathrm{Phan}} = \frac{\#PFF}{\#SL} = \frac{10\,\mathrm{PFF}}{10^5\,\mathrm{SL}} = 10^{-4\,\mathrm{PFF}/\mathrm{SL}}$$

Aufgabe 1.6: Fehlertoleranz und Phantomfehler

Ein IT-System hat ohne Fehlertoleranz eine FF-Raten von $\zeta = 10^{-4}$ FF je SL. Die eingebaute Funktionen zur Überwachung und Ergebniskorrektor korrigieren $FT = 80\%$ der FF.

a) Wie hoch ist die Fehlfunktionsüberdeckung der Überwachungseinheiten mindestens?

b) Welche FF-Rate ζ_{FT} und Zuverlässigkeit Z_{FT} hat der fehlertolerante Rechner?

c) Für die Überwachung sei zusätzlich eine Phantomfehlerrate von $\zeta_{\mathrm{Phan}} = 10^{-4\,\mathrm{PFF}/\mathrm{SL}}$ unterstellt und die Korrekturfunktionen soll 10% der Phantom-FF in tatsächliche FF umwandeln. Auf welchen Wert verringert sich die Zuverlässigkeit?

Ein IT-System hat ohne Fehlertoleranz eine FF-Raten von $\zeta = 10^{-4}$ FF je SL. Die eingebaute Funktionen zur Überwachung und Ergebniskorrektor korrigieren $FT = 80\%$ der FF.

a) Wie hoch ist die Fehlfunktionsüberdeckung der Überwachungseinheiten mindestens?

Die FF-Überdeckung muss mindestens so hoch sein, wie der Anteil der beiseitigten FF:

$$FFC \geq FT = 80\%$$

Ein IT-System hat ohne Fehlertoleranz eine FF-Raten von $\zeta = 10^{-4}$ FF je SL. Die eingebaute Funktionen zur Überwachung und Ergebniskorrektor korrigieren $FT = 80\%$ der FF.

b) Welche FF-Rate ζ_{FT} und Zuverlässigkeit Z_{FT} hat der fehlertolerante Rechner?

$$\zeta_{\mathrm{FT}} = (1 - FT) \cdot \zeta = 2 \cdot 10^{-5} \frac{\mathrm{FF}}{\mathrm{SL}}$$

$$Z_{\mathrm{FT}} = \frac{1}{\zeta_{\mathrm{FT}}} = 5 \cdot 10^{4} \frac{\mathrm{SL}}{\mathrm{FF}}$$

Ein IT-System hat ohne Fehlertoleranz eine FF-Raten von $\zeta = 10^{-4}$ FF je SL. Die eingebaute Funktionen zur Überwachung und Ergebniskorrektor korrigieren $FT = 80\%$ der FF.

c) Für die Überwachung sei zusätzlich eine Phantomfehlerrate von $\zeta_{\mathrm{Phan}} = 10^{-4\,\mathrm{PFF}/\mathrm{SL}}$ unterstellt und die Korrekturfunktionen soll 10% der Phantom-FF in tatsächliche FF umwandeln. Auf welchen Wert verringert sich die Zuverlässigkeit?

$$\zeta_{\mathrm{FT}} = \underbrace{(1-FT)\cdot\zeta}_{\mathrm{NKFF}} + \underbrace{\zeta_{\mathrm{Phan}}\cdot 10\%\frac{\mathrm{FF}}{\mathrm{PFF}}\cdot}_{\mathrm{ZFF}} = 3\cdot 10^{-5}\frac{\mathrm{FF}}{\mathrm{SL}}$$

$$Z_{\mathrm{FT}} = \frac{1}{\zeta_{\mathrm{FT}}} = 3{,}33\cdot 10^{4}\frac{\mathrm{SL}}{\mathrm{FF}}$$

(NKFF – nicht korrigierte FF; ZFF – durch Korrektur von Phantom-FF entstandene FF)

Aufgabe 1.7: Sicherheitserhöhung durch Fehlertoleranz

Bei einem IT-System mit einer $MTTF = 10^3\,\mathrm{h}/\mathrm{FF}$, Service-Dauer $MTS = 1\,\mathrm{h}/\mathrm{SL}$, gefährde abschätzungsweise jede hundertste FF die Betriebssicherheit. Um die Betriebssicherheit auf $10^6\,\mathrm{SL}/\mathrm{GFF}$ zu erhöhen, soll das System um eine Funktionsüberwachung erweitert werden, die es bei Erkennen einer Fehlfunktion in einen sicheren Zustand überführt.

a) Wie hoch muss die Fehlfunktionsüberdeckung mindestens sein, wenn beim Überführen in den sicheren Zustand keine Fehlfunktionen auftreten?

b) Wie hoch muss die Fehlfunktionsüberdeckung sein, wenn zu erwarten ist, dass jeder 20te Versuch, einen sicheren Zustand herzustellen, scheitert?

c) In welchem mittleren zeitlichen Abstand wird überschlagsweise ein sicherer Zustand hergestellt, ohne dass die Betriebssicherheit gefährdet ist?

Bei einem IT-System mit einer $MTTF = 10^3\,\mathrm{h}/\mathrm{FF}$, Service-Dauer $MTS = 1\,\mathrm{h}/\mathrm{SL}$, gefährde abschätzungsweise jede hundertste FF die Betriebssicherheit. Um die Betriebssicherheit auf $10^6\,\mathrm{SL}/\mathrm{GFF}$ zu erhöhen, soll das System um eine Funktionsüberwachung erweitert werden, die es bei Erkennen einer Fehlfunktion in einen sicheren Zustand überführt.

a) Wie hoch muss die Fehlfunktionsüberdeckung mindestens sein, wenn beim Überführen in den sicheren Zustand keine Fehlfunktionen auftreten?

Schätzwert der Sicherheit ohne Fehlerbehandlung:

$$S = \frac{10^3\,\mathrm{SL}}{1\%\,\mathrm{GFF}} = 10^5\,\mathrm{SL}/\mathrm{GFF}$$

Für eine Erhöhung auf $10^6\,\mathrm{SL}/\mathrm{GFF}$ genügt es, 90% der (sicherheitskritischen) Fehlfunktionen zu erkennen:

$$FCC = 90\%$$

Bei einem IT-System mit einer $MTTF = 10^3\,{}^{\mathrm{h}}/_{\mathrm{FF}}$, Service-Dauer $MTS = 1\,{}^{\mathrm{h}}/_{\mathrm{SL}}$, gefährde abschätzungsweise jede hundertste FF die Betriebssicherheit. Um die Betriebssicherheit auf $10^6\,{}^{\mathrm{SL}}/_{\mathrm{GFF}}$ zu erhöhen, soll das System um eine Funktionsüberwachung erweitert werden, die es bei Erkennen einer Fehlfunktion in einen sicheren Zustand überführt.

b) Wie hoch muss die Fehlfunktionsüberdeckung sein, wenn zu erwarten ist, dass jeder 20te Versuch, einen sicheren Zustand herzustellen, scheitert?

Wenn jeder 20-te Versuch scheidert, dann müssen 19 von 20 (sicherheitskritische) Fehlfunktionen erkannt werden, damit in 9 von 10 Fällen ein sicherer Zustand erreicht wird:

$$FCC = 95\%$$

Bei einem IT-System mit einer $MTTF = 10^3\,\mathrm{h}/\mathrm{FF}$, Service-Dauer $MTS = 1\,\mathrm{h}/\mathrm{SL}$, gefährde abschätzungsweise jede hundertste FF die Betriebssicherheit. Um die Betriebssicherheit auf $10^6\,\mathrm{SL}/\mathrm{GFF}$ zu erhöhen, soll das System um eine Funktionsüberwachung erweitert werden, die es bei Erkennen einer Fehlfunktion in einen sicheren Zustand überführt.

c) In welchem mittleren zeitlichen Abstand wird überschlagsweise ein sicherer Zustand hergestellt, ohne dass die Betriebssicherheit gefährdet ist?

Ein sicherer Zustand wird etwa aller 1000 h hergestellt, in 99% der Fälle für eine ungefährliche FF. Mittlerer zeitlicher Abstand:

$$\frac{1000\,\mathrm{h}}{99\%} = 1010\,\mathrm{h}$$

Überwachungsverfahren

Aufgabe 1.8: FF-Überdeckung Informationsredundanz

Eine 10 MByte große Datei wird um r redundante Bits so erweitert, dass bei einer Verfälschung alle darstellbaren Werte aus Datenbits und redundanten Bits etwa mit der gleichen Häufigkeit auftreten. Die Überwachungsfunktion soll alle unzulässigen Gesamtwerte erkennen.

a) Welche FF-Überdeckung wird mit $r = 10$ redundanten Bits erzielt?

b) Wie viele redundante Bits genügen für eine FF-Überdeckung von $FFC \geq 99{,}99\%$?

Eine 10 MByte große Datei wird um r redundante Bits so erweitert, dass bei einer Verfälschung alle darstellbaren Werte aus Datenbits und redundanten Bits etwa mit der gleichen Häufigkeit auftreten. Die Überwachungsfunktion soll alle unzulässigen Gesamtwerte erkennen.

a) Welche FF-Überdeckung wird mit $r = 10$ redundanten Bits erzielt?

Es gibt mindestens 2^{10} mal so viel mögliche wie zulässige Werte, so dass im Mittel von 2^{10} Verfälschungen nur eine auf einen zulässigen Wert abgebildet und nicht erkannt wird. Anteil der erkennbaren Verfälschungen:

$$FFC \geq 1 - 2^{-10} = 99{,}9\%$$

Eine 10 MByte große Datei wird um r redundante Bits so erweitert, dass bei einer Verfälschung alle darstellbaren Werte aus Datenbits und redundanten Bits etwa mit der gleichen Häufigkeit auftreten. Die Überwachungsfunktion soll alle unzulässigen Gesamtwerte erkennen.

b) Wie viele redundante Bits genügen für eine FF-Überdeckung von $FFC \geq 99{,}99\%$?

$$FFC = 1 - 2^{-r}$$

$$r \geq -\frac{\ln(1 - FC)}{\ln(2)} = 13{,}29$$

Es genügen $r = 14$ redundante Bit.

Fehlerbeseitigung

Ursachen von FF

Aufgabe 1.9: Warum zwischen Fehlern und Störungen zu unterscheiden ist?

a) Warum ist es viel einfacher, Fehlfunktionen durch Störungen zu korrigieren als Fehlfunktionen, die durch Fehler verursacht werden?
b) Warum ist es bei der Beseitigung der Ursachen genau umgekehrt, dass sich Fehler gut beseitigen lassen, aber die Beseitigung von Störquellen erheblich schwieriger ist?

a) Warum ist es viel einfacher, Fehlfunktionen durch Störungen zu korrigieren als Fehlfunktionen, die durch Fehler verursacht werden?
b) Warum ist es bei der Beseitigung der Ursachen genau umgekehrt, dass sich Fehler gut beseitigen lassen, aber die Beseitigung von Störquellen erheblich schwieriger ist?

a) Störungen wirken diversitär. Eine erkannte FF durch eine Störung lässt sich in der Regel durch Wiederholung der Service-Leistung mit gleichen Eingaben korrigieren. Bei Fehlern als Ursache verlangt ein erfolgreiche Korrektur andere Formen der Diversität, geänderte Eingaben oder eine diversitäre Verarbeitung.

b) Nach Beseitigungsversuchen für Fehler kann der Erfolg durch eine einzelne Testwiederholung kontrolliert werden, während nach Beseitungsversuchen für Ursachen von Störung die Verringerung die FF-Raten überprüft werden muss. Dazu muss solange getestet werden, bis eine signifikante Abnahme der Anzahl der FF im Testzeitintervall nachweisbar ist, also mit Millionen, Milliarden oder mehr SL.

Test

Aufgabe 1.10: Nicht beseitigte Programmierfehler

Wie groß ist die zu erwartende Fehleranzahl in einem Programm mit 10^5 NLOC (Netto Lines of Code) bei einer Fehlerentstehungsrate von 40 Fehlern je 1000 NLOC, wenn der Test 80% der Fehler erkennt und und in der Reparaturiteration im Mittel bei der Beseitigung von 20 Fehlern ein neuer entsteht?

Wie groß ist die zu erwartende Fehleranzahl in einem Programm mit 10^5 NLOC (Netto Lines of Code) bei einer Fehlerentstehungsrate von 40 Fehlern je 1000 NLOC, wenn der Test 80% der Fehler erkennt und und in der Reparaturiteration im Mittel bei der Beseitigung von 20 Fehlern ein neuer entsteht?

Anzahl der entstehenden Fehler:

$$\#F = 10^5\,\mathrm{NLOC} \cdot 40\,\frac{\mathrm{F}}{\mathrm{NLOC}} = 4000\,\mathrm{F}$$

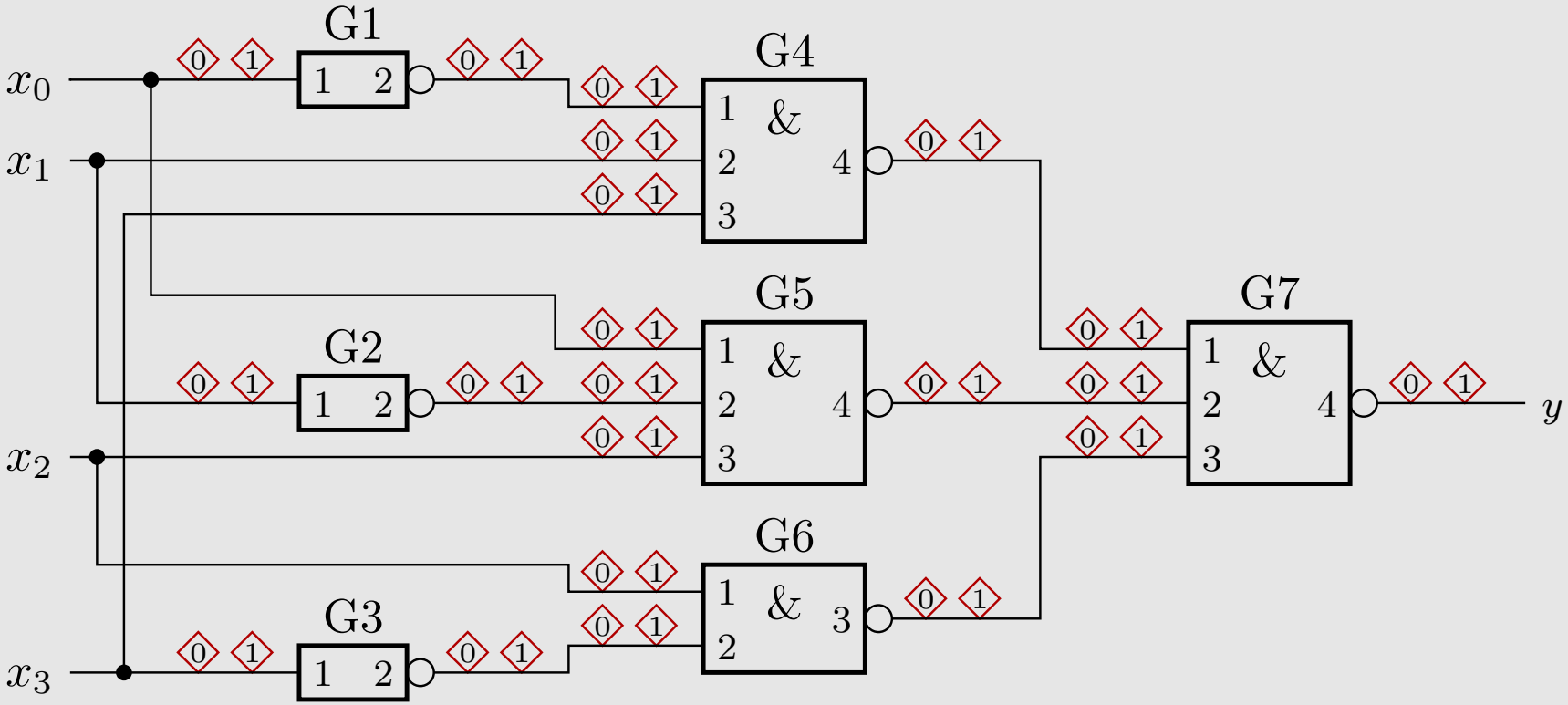
Bei der Reparatur entstehen weitere $80\% \cdot 5\% \cdot 4000\,\mathrm{F}$. Von der Gesamtfehleranzahl werden $1 - FC = 20\%$ nicht aussortiert:

$$\#F_{\mathrm{NB}} = \#F \cdot (1 + 80\% \cdot 5\%) \cdot 20\% = 832$$

Wie zuverlässig ein Programm mit fast tausend Fehlern ist, hängt von der mittleren FF-Rate der Fehler ab.

Haftfehler

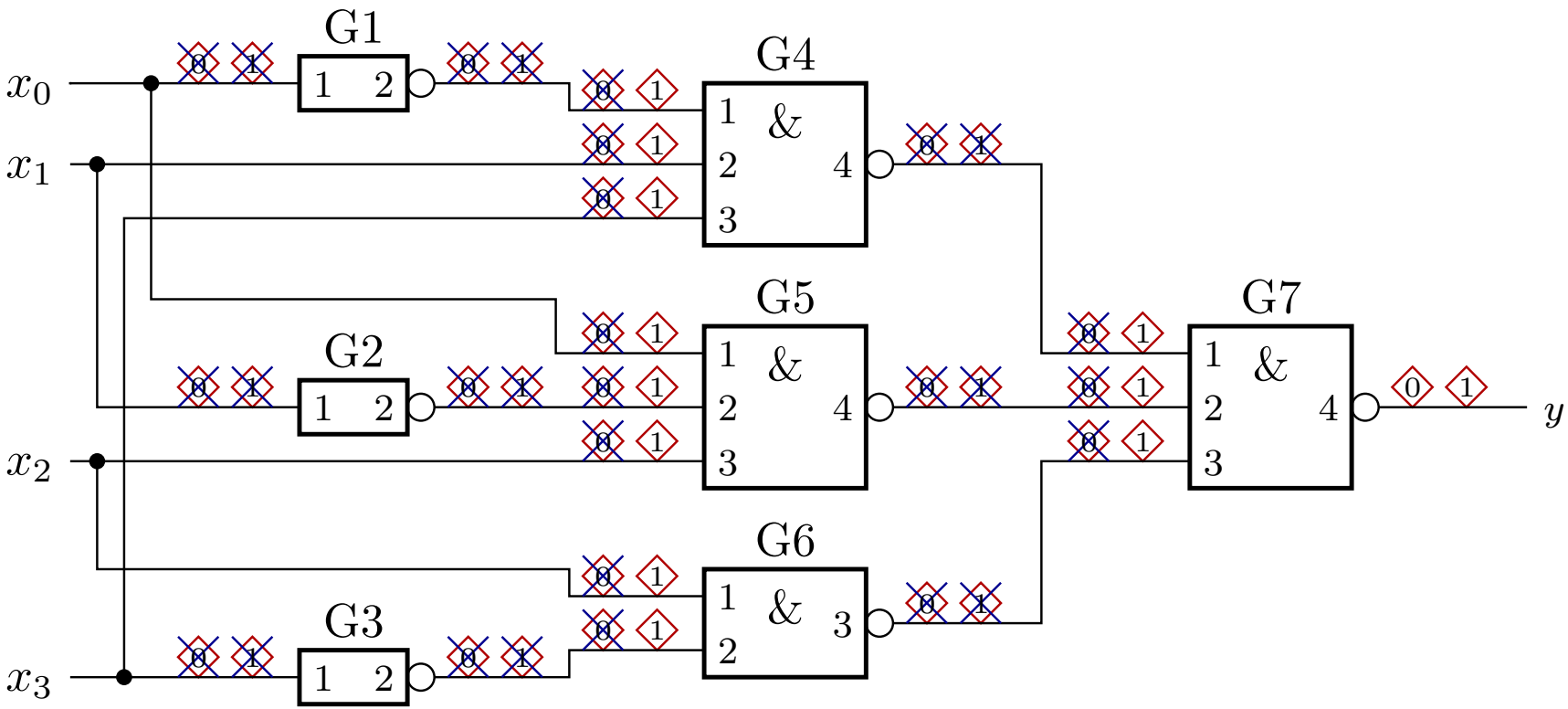
Aufgabe 1.11: Vereinfachung einer Haftfehlermenge



a) Fassen Sie alle identisch nachweisbaren Haftfehler zu einem Modellfehler zusammen.

b) Bestimmen Sie anschließend alle implizit nachweisbaren Haftfehler.

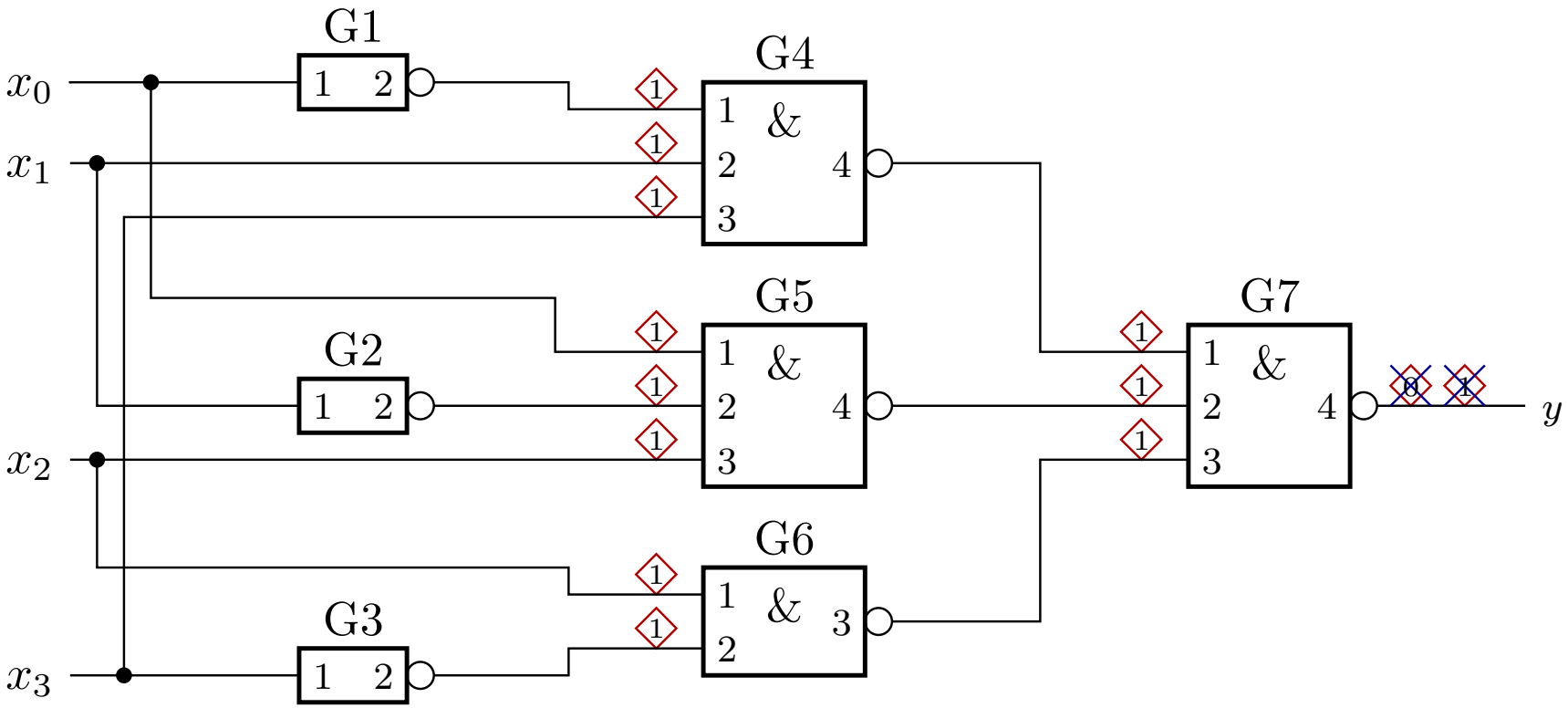
a) Fassen Sie alle identisch nachweisbaren Haftfehler zu einem Modellfehler zusammen.



Identisch nachweisbare Haftfehler:

- sa0(G1-1), sa1(G1-2), sa_1(G4-1)
- sa1(G1-1), sa0(G1-2), sa0(G4-1), sa1(G4-4), sa_1(G7-1), ...

b) Bestimmen Sie anschließend alle implizit nachweisbaren Haftfehler.



Implizit nachweisbare Haftfehler:

- sa0(G7-4): sa1(G7-1), sa1(G7-2), sa1(G7-3)
- sa1(G7-4): sa1(G4-1), sa1(G4-2), sa1(G4-3), sa1(G5-1), ...

Test und Zuverlässigkeit

Aufgabe 1.12: Fehleranzahl, FF-Rate und Zuverlässigkeit

In einer Iteration aus Test und Fehlerbeseitigung, bei der alle erkannten Fehler sofort beseitigt wurden, war bei Erhöhung der Testsatzlänge von $n_0 = 10^5$ auf $n_1 = 10^6$ eine Verringerung der FF-Rate von $\zeta_0 = 10^{-3}$ auf $\zeta_1 = 4 \cdot 10^{-5}$ FF/SL zu beobachten.

a) Auf welchen Exponenten k für die Dichte der FF-Rate lässt sich unter den Modellannahmen in der Vorlesung daraus schließen?

b) Wie viele Fehler werden in der Iteration aus Test und Beseitigung der erkennbaren Fehler bei Erhöhung der Testsatzlänge von n_0 auf n_1 abschätzungsweise beseitigt?

c) Welche Zuverlässigkeit hat das System mit einer Testsatzlänge n_1 und welche Testsatzlänge n_2 ist nach den Modellannahmen erforderlich, um eine Zuverlässigkeit von 10^8 SL/FF zu erzielen?

FF durch Störungen sind zu vernachlässigen.

In einer Iteration aus Test und Fehlerbeseitigung, bei der alle erkannten Fehler sofort beseitigt wurden, war bei Erhöhung der Testsatzlänge von $n_0 = 10^5$ auf $n_1 = 10^6$ eine Verringerung der FF-Rate von $\zeta_0 = 10^{-3}$ auf $\zeta_1 = 4 \cdot 10^{-5}$ FF/SL zu beobachten.

a) Auf welchen Exponenten k für die Dichte der FF-Rate lässt sich unter den Modellannahmen in der Vorlesung daraus schließen?

a) Die FF-Rate nimmt mit Exponent $-(k+1)$ ab

$$\frac{\zeta_1}{\zeta_0} \approx \frac{\zeta(n_1)}{\zeta(n_0)} = \left(\frac{n_1}{n_0}\right)^{-(k+1)}$$

$$k \approx -\left(\frac{\ln(\zeta_1/\zeta_0)}{\ln(n_1/n_0)} + 1\right) = -\left(\frac{\ln\left(\frac{4\cdot 10^{-5}}{10^{-3}}\right)}{\ln\left(\frac{10^6}{10^5}\right)} + 1\right) = 0{,}4$$

In einer Iteration aus Test und Fehlerbeseitigung, bei der alle erkannten Fehler sofort beseitigt wurden, war bei Erhöhung der Testsatzlänge von $n_0 = 10^5$ auf $n_1 = 10^6$ eine Verringerung der FF-Rate von $\zeta_0 = 10^{-3}$ auf $\zeta_1 = 4 \cdot 10^{-5}$ FF/SL zu beobachten.

b) Wie viele Fehler werden in der Iteration aus Test und Beseitigung der erkennbaren Fehler bei Erhöhung der Testsatzlänge von n_0 auf n_1 abschätzungsweise beseitigt?

b) FF-Raten als Funktion der Fehleranzahl:

$$\zeta(n) \approx \frac{k \cdot \#F(n)}{(k+1) \cdot n}$$

$$\#F(n_0) \approx \frac{(k+1) \cdot n_0}{k} \cdot \zeta(n_0) = \frac{(0{,}4+1) \cdot 10^5}{0{,}4} \cdot 10^{-3} = 351$$

$$\#F(n_1) \approx \frac{(k+1) \cdot n_1}{k} \cdot \zeta(n_1) = \frac{(0{,}4+1) \cdot 10^6}{0{,}4} \cdot 4 \cdot 10^{-5} = 140$$

Zu erwartende Anzahl der beseitigten Fehler: $351 - 140 = 211$

In einer Iteration aus Test und Fehlerbeseitigung, bei der alle erkannten Fehler sofort beseitigt wurden, war bei Erhöhung der Testsatzlänge von $n_0 = 10^5$ auf $n_1 = 10^6$ eine Verringerung der FF-Rate von $\zeta_0 = 10^{-3}$ auf $\zeta_1 = 4 \cdot 10^{-5}$ FF/SL zu beobachten.

c) Welche Zuverlässigkeit hat das System mit einer Testsatzlänge n_1 und welche Testsatzlänge n_2 ist nach den Modellannahmen erforderlich, um eine Zuverlässigkeit von 10^8 SL/FF zu erzielen?

c) Die Zuverlässigkeit ist der Kehrwert der FF-Rate und nimmt weiter mit $k+1$ zu:

$$Z(n_1) = \frac{1}{\zeta_1} = \frac{1}{4 \cdot 10^{-5}} \frac{\text{SL}}{\text{FF}} = 25000 \frac{\text{SL}}{\text{FF}}$$

$$Z(n_2) \approx Z(n_1) \cdot \left(\frac{n_2}{n_1}\right)^{k+1}$$

$$n_2 \approx n_1 \cdot \left(\frac{Z(n_2)}{Z(n_1)}\right)^{\frac{1}{k+1}} = 10^6 \cdot \left(\frac{10^8}{2{,}5 \cdot 10^4}\right)^{\frac{1}{0{,}4+1}} = 3{,}77 \cdot 10^8$$

Reifeprozesse

Aufgabe 1.13: Zuverlässigkeitswachstum

Ein bei vielen Nutzern eingesetztes Software-System hat nach einer Reifedauer von $t_0 = 100$ Tagen eine fehlerbezogene Teilzuverlässigkeit von $Z(t_0) = 10^5 \frac{\mathrm{SL}}{\mathrm{FF}}$. Der Exponent für die Abnahme der Anzahl der nicht nachweisbaren Fehler mit der Testsatzlänge sei $k = 0{,}4$. Nach wie vielen weiteren Tagen

a) verdoppelt und

b) verzehnfacht

sich die Zuverlässigkeit? Annahmen für die Abschätzung:

- Die Testanzahl n_T vor dem Einsatz sei vernachlässigbar $n_\mathrm{T} \ll c \cdot n_\mathrm{R}$,
- die Fehlerbeseitigungswahrsch. c soll sich nicht ändern,
- die Anzahl der SL bei den Anwendern sei proportional zur Anzahl der Nutzungstage $n_\mathrm{R} \sim t$ und
- FF durch Störungen seien vernachlässigbar.

Ein bei vielen Nutzern eingesetztes Software-System hat nach einer Reifedauer von $t_0 = 100$ Tagen eine fehlerbezogene Teilzuverlässigkeit von $Z(t_0) = 10^5 \frac{\mathrm{SL}}{\mathrm{FF}}$. Der Exponent für die Abnahme der Anzahl der nicht nachweisbaren Fehler mit der Testsatzlänge sei $k = 0{,}4$. Nach wie vielen weiteren Tagen

a) verdoppelt und

b) verzehnfacht

Unter Annahme derselben mittleren Service-Dauer MTS, Beseitigungswahrscheinlichkeit, ... ist das Verhältnis aus der Anzahl der SL etwa gleich dem Verhältnis der Nutzungsdauern:

$$\frac{Z(n)}{Z(n_0)} \approx \left(\frac{n}{n_0}\right)^{k+1} \approx \left(\frac{t}{t_0}\right)^{k+1}$$

$$t \approx t_0 \cdot \left(\frac{Z(t)}{Z(t_0)}\right)^{\frac{1}{k+1}} = 100\,\mathrm{Tage} \cdot \left(\frac{Z(t)}{Z(t_0)}\right)^{\frac{1}{1{,}4}}$$

Ein bei vielen Nutzern eingesetztes Software-System hat nach einer Reifedauer von $t_0 = 100$ Tagen eine fehlerbezogene Teilzuverlässigkeit von $Z(t_0) = 10^5 \frac{\mathrm{SL}}{\mathrm{FF}}$. Der Exponent für die Abnahme der Anzahl der nicht nachweisbaren Fehler mit der Testsatzlänge sei $k = 0{,}4$. Nach wie vielen weiteren Tagen

a) verdoppelt und

b) verzehnfacht

$$\frac{Z(n)}{Z(n_0)} \approx \left(\frac{n}{n_0}\right)^{k+1} \approx \left(\frac{t}{t_0}\right)^{k+1}$$

$$t \approx t_0 \cdot \left(\frac{Z(t)}{Z(t_0)}\right)^{\frac{1}{k+1}} = 100\,\mathrm{Tage} \cdot \left(\frac{Z(t)}{Z(t_0)}\right)^{\frac{1}{1{,}4}}$$

Zusätzlich erforderliche Reifedauer:

$\frac{Z(t)}{Z(t_0)}$	2	10
$t - t_0$	64 Tage	418 Tage

Aufgabe 1.14: Erforderliche Reifedauer

Der Exponent für die Abnahme der Anzahl der nicht nachweisbaren Fehler mit der Testsatzlänge liege im Bereich von $k = 0{,}3 \ldots 0{,}5$. Um welchen Faktor muss die Reifedauer t gegenüber t_0 erhöht werden,

a) damit 90% der noch nicht beseitigten Fehler erkannt und beseitigt werden?
b) um die fehlerbezogene Teilzuverlässigkeit Z auf das zehnfache zu erhöhen?

Die Testdauer vor dem Einsatz sei wieder gegenüber der effektiven Reifedauer vernachlässigbar, die Fehlerbeseitigungswahrscheinlichkeit c, dass ein Fehler, wenn er bei einem Anwender eine FF verursacht, beseitigt wird, soll sich nicht ändern und FF durch Störungen seien vernachlässigbar.

Der Exponent für die Abnahme der Anzahl der nicht nachweisbaren Fehler mit der Testsatzlänge liege im Bereich von $k = 0{,}3 \ldots 0{,}5$. Um welchen Faktor muss die Reifedauer t gegenüber t_0 erhöht werden,

a) damit 90% der noch nicht beseitigten Fehler erkannt und beseitigt werden?

$$\frac{\#F(t)}{\#F(t_0)} = 0{,}1 \approx \left(\frac{t}{t_0}\right)^{-k}$$

$$\frac{t}{t_0} \approx 0{,}1^{-1/k}$$

k	0,3	0,4	0,5
$\frac{t}{t_0}$	2154	316	100

Zur Verringerung der Anzahl der nicht beseitigten Fehler auf ein Zehntel muss die Reifedauer in Abhängigkeit von k auf das hundet bis mehr als 2.000-fache erhöht werden.

Der Exponent für die Abnahme der Anzahl der nicht nachweisbaren Fehler mit der Testsatzlänge liege im Bereich von $k = 0{,}3 \ldots 0{,}5$. Um welchen Faktor muss die Reifedauer t gegenüber t_0 erhöht werden,

b) um die fehlerbezogene Teilzuverlässigkeit Z auf das zehnfache zu erhöhen?

$$\frac{Z(t)}{Z(t_0)} = 10 = \left(\frac{t}{t_0}\right)^{k+1}$$

$$\frac{t}{t_0} = 10^{1/(k+1)}$$

k	0,3	0,4	0,5
$\frac{t}{t_0}$	5,88	5,18	4,64

Zur Erhöhung der fehlerbezogenen Teilzuverlässigkeit auf das zehnfache muss die Reifedauer in Abhängigkeit von k auf etwa das 5 bis 6-fache erhöht werden. Viel geringere Abhängigkeit von k als in der Teilaufgabe zuvor.

Fehlervermeidung

Fehleranteil und Ausbeute

Aufgabe 1.15: Fehleranteil eines Rechners

Ein Steuerrechner besteht aus Leiterplatten, Schaltkreisen, diskreten Bauteilen (Widerständen, Kondensatoren, . . .) und Lötstellen.

Bauteil	Anzahl	Fehleranteil	Summation für den gesamten Rechner	
Leiterplatten	2	600 dpm		dpm
Schaltkreise	30	200 dpm	+	dpm
diskrete Bauteile	180	10 dpm	+	dpm
Lötstellen	5000	1 dpm	+	dpm
			=	dpm

a) Wie groß ist der zu erwartende Fehleranteil des Rechners, wenn anderen Arten von Fehlern anzahlmäßig vernachlässigbar sind?

b) Auf welchen Wert verringert sich der Fehleranteil, wenn für alle Arten von Bauteilen die Anzahl halbiert wird?

Ein Steuerrechner besteht aus Leiterplatten, Schaltkreisen, diskreten Bauteilen (Widerständen, Kondensatoren, . . .) und Lötstellen.

a) Wie groß ist der zu erwartende Fehleranteil des Rechners, wenn anderen Arten von Fehlern anzahlmäßig vernachlässigbar sind?

Bauteil	Anzahl	Fehleranteil	Produkt
Leiterplatten	2	600 dpm	1200 dpm
Schaltkreise	30	200 dpm	+ 6000 dpm
diskrete Bauteile	180	10 dpm	+ 1800 dpm
Lötstellen	5000	1 dpm	+ 5000 dpm
			= 14000 dpm

Von 1000 Rechner enthalten im Mittel 14 beim Verkauf einen Bauteilfehler.

Ein Steuerrechner besteht aus Leiterplatten, Schaltkreisen, diskreten Bauteilen (Widerständen, Kondensatoren, . . .) und Lötstellen.

b) Auf welchen Wert verringert sich der Fehleranteil, wenn für alle Arten von Bauteilen die Anzahl halbiert wird?

Bei der halben Bauteilzahl und ansonsten gleichen Werten enthalten im Mittel nur 7 von 1000 Rechnern einen Bauteilfehler.

Determinismus und Zufall

Aufgabe 1.16:

a) Warum sollten Entstehungsprozesse möglichst deterministisch arbeiten?

b) Wie wird der Reparaturerfolg bei nicht deterministischen Prozessen kontrolliert?

c) Warum hat der Fehleranteil von Produkten typischerweise einen sägezahnförmigen Verlauf über die Jahre, die das Produkt gefertigt wird?

a) Warum sollten Entstehungsprozesse möglichst deterministisch arbeiten?

Determinismus ist Voraussetzung für die Erfolgskontrolle einer Fehlerbeseitigung durch Testwiederholung. Eine Erfolgskontrolle mit klarer ja/nein-Aussage ist die Voraussetzung für den Rückbau nach erfolglosen Fehlerbeseitigungsversuchen und die Fortsetzung der Prozessverbesserung mit den nächsten Fehlersymtomen.

b) Wie wird der Reparaturerfolg bei nicht deterministischen Prozessen kontrolliert?

Bei nicht deterministischen Prozessen wird der Erfolg von Verbesserungen anhand von Erwartungswerten, Varianzen, Verteilungen, ... messbarerer Produkteigenschaften kontrolliert. Verlangt statt einer Prozesswiederholung eine statistisch signifikante Anzahl von sehr vielen Wiederholungen.

c) Warum hat der Fehleranteil von Produkten typischerweise einen sägezahnförmigen Verlauf über die Jahre, die das Produkt gefertigt wird?

Bei der Einführung neuer Maschinen, Verfahren, ... kommen Fehler in den Prozess und verringern die Prozesszuverlässigkeit. Mit der Prozessnutzung werden diese Fehler und Schwachstellen beseitigt, so dass die Prozesszuverlässigkeit zunimmt, bis die nächste grosse Neuerung eingeführt wird. Neuerungen haben oft geringere störungsbedingte Teilzuverlässigkeit, so dass die Prozesszuverlässigkeit über mehrere »Sägezähne« zunimmt.