Test und Verlässlichkeit Grosse Übung

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_GU1)

29. Oktober 2024

Inhalt Große Übung

Modellbildung Teil 1

Verlässlichkeit

Aufgabe 1.1: Verlässlichkeit, Service-Modell

a) *Auf welchen drei Ebenen erfolgt die Sicherung der Verlässlichkeit?*

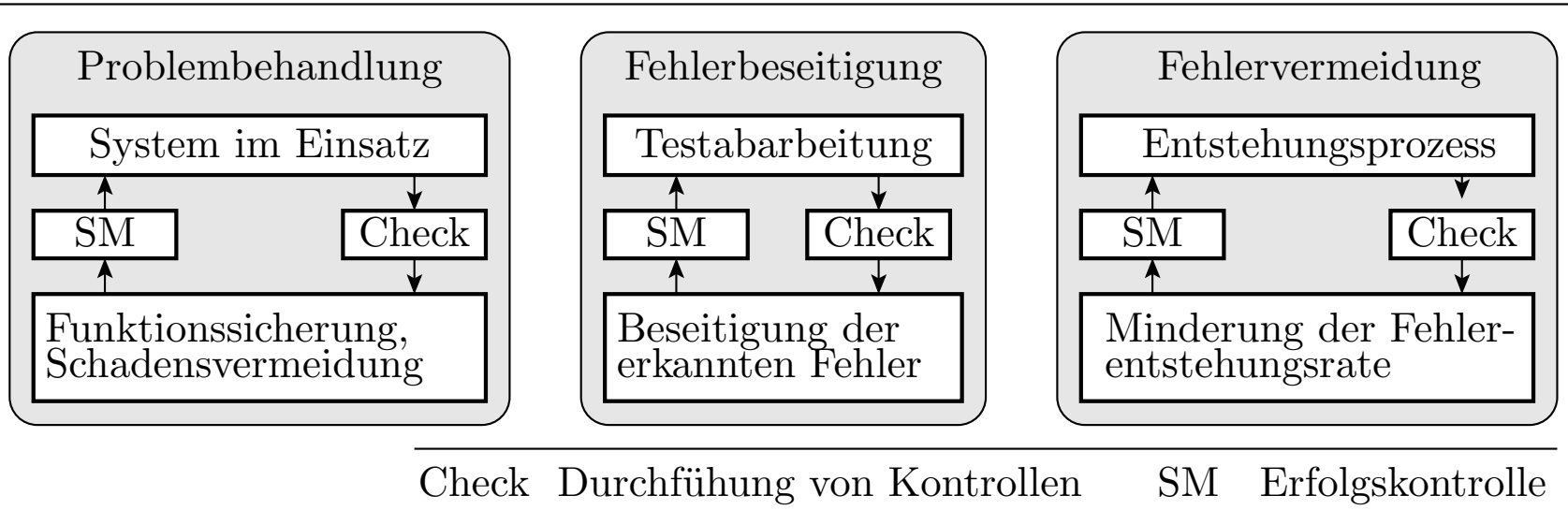
b) *Was ist eine Fehlerkultur? Was für eine Fehlerkultur unterstellt die Vorlesung und warum?*

c) *Ein Modell in der Informatik hebt die wesentlichen Aspekte hervor und vernachlässigt unwesentliche Details. Was sind wesentliche Aspekte und was sind vernachlässigte unwesentliche Details das Service-Modells?*

d) *Auf was für Systemtypen ist das Service-Modell anwendbar?*

e) *Was hat es mit der Kennzeichung »ACR« auf sich?*

a) *Auf welchen drei Ebenen erfolgt die Sicherung der Verlässlichkeit?*



- Überwachung und »Entschärfen« erkannter Probleme (Fehlfunktionen, Abstürze) während der Nutzung.
- Fehlerbeseitigung vor der Nutzung und in Nutzungspausen. Fehler definieren wir in Abgrenzung von Störungen als die beseitigbaren Ursachen von Fehlfunktionen und Abstürzen.
- Fehlervermeidung durch verbesserte Entstehungsprozesse. Iteration aus Überwachung von Zuständen, Zwischen- und Endergebnissen und Beseitigung erkannter Probleme.

b) *Was ist eine Fehlerkultur? Was für eine Fehlerkultur unterstellt die Vorlesung und warum?*

Fehlerkultur ist die Art und Weise, wie eine Kultur mit Fehlern und deren Folgen umgeht.

Idealisierte Fehlerkultur in der Vorlesung: Für alle erkannten Probleme laufen solange Beseitigungsversuche, bis sie nicht mehr erkennbar sind.

Wir betrachten oft nur den Endzustand nach Beseitigung aller erkennbaren Probleme, teilweise auch den Weg dahin und ignorieren

- Probleme, die bei vernünftigem Umgang nicht da sind,
- Kosten für die Beseitigung, Wirtschaftlichkeit,
- kulturelle Barrieren und Gepflogenheiten, ...

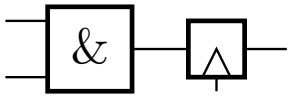
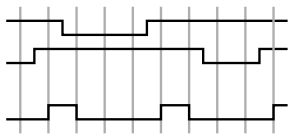
Erheblich einfacherere Modellierung als mit »Kulturfaktoren«.

c) *Ein Modell in der Informatik hebt die wesentlichen Aspekte hervor und vernachlässigt unwesentliche Details. Was sind wesentliche Aspekte und was sind vernachlässigte unwesentliche Details das Service-Modells?*

Wesentlich: Abzählbare Anzahl der Service-Anforderungen (SR), erbrachten Leistungen (DS), nicht erbrachten Leistungen (NS), korrekten Leistungen (CS) und Fehlfunktionen (MF).
Vernachlässigte Details: Funktion, Realisierung.

Das erlaubt, die positiven und negativen Ergebnisse zu zählen und Raten für deren Häufigkeit zu definieren und damit die einzelnen Teilaspekte der Verlässlichkeit (Verfügbarkeit, Zuverlässigkeit, ...) und die Wirksamkeit verlässlichkeitssichernder Massnahmen (Tests, Problembeseitigung, ...) quantitativ zu beschreiben.

d) *Auf was für Systemtypen ist das Service-Modell anwendbar?*

getaktete Digitalschaltung		E: A: 

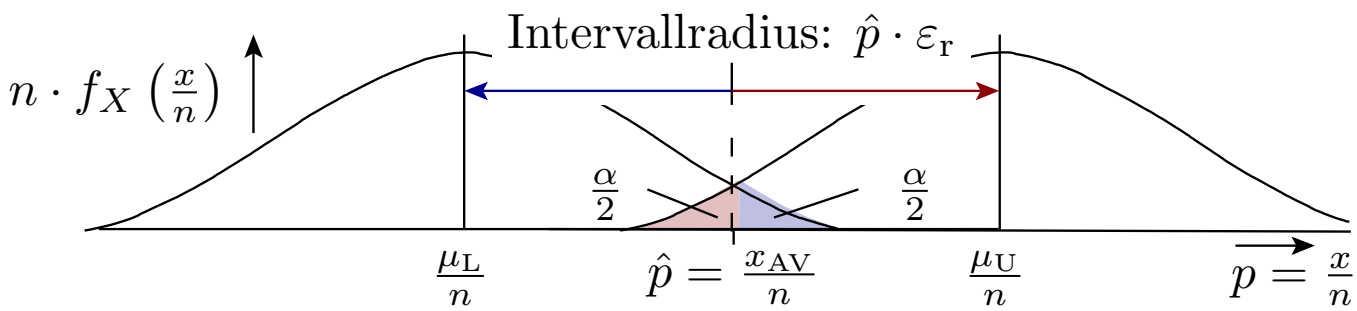
Programm mit EVA-Struktur	`uint8_t up(uint8_t a){`
	`  return 23 * a;`
	`}`
		E: 10 101 ...
		A: 320 19 ...

Server	E: z.B. eine Datenbankanfrage A: Ergebnisdatensatz	
Fertigungsprozess	E: Fertigungsauftrag, Material, ... A: gefertigtes Produkt	
Entwurfsprozess	E: Entwurfsauftrag A: Entwurf	

Anwendbar auf alle Systeme, die auf Anforderung aus Eingaben Ausgaben erzeugen: Hardware, Software, Mechatronische Systeme, Entwurfsprozesse, Fertigungsprozesse incl. der für die Hardware, ...

E, A Eingabe, Ausgabe.

e) *Was hat es mit der Kennzeichung »ACR« auf sich?*



ACR: Brauchbare Schätzwerte nur bei geeigneten Zählwertgröße (Useful estimates only with appropriate counting ranges).

Unsere Kenngrößen für Verfügbarkeit, Zuverlässigkeit, Testgüte, Problembeseitigungserfolg, ... ergeben sich alle aus Zählwerten für zufällige Ereignisse (Ergebnis erbracht, richtig, falsch, ...).

Die beste Vorhersage der künftigen Häufigkeit zufälliger Ereignisse ist der Erwartungswert. Eine brauchbare Abschätzung von Erwartungswerten verlangt ausreichend große Zählwerte. Wie groß, behandelt erst Foliensatz 4.

Aufgabe 1.2: Verfügbarkeit, Problembehandlungsdauer

Eine Steuerung mit einer mittleren Zeit *zwischen* den Fehlfunktionen von zwei Jahren soll eine Verfügbarkeit von $1 - 10^{-6}$ haben. In 99% der Fälle startet das System ohne Reparatur und Korrektur automatisch neu und ist nach $t_{\mathrm{TS1}} = 30\,\mathrm{s}$ wieder betriebsbereit und in 1% der Fälle muss zusätzlich die Steuerung getauscht werden. Andere Aspekte der Nichtverfügbarkeit bleiben unbeachtet.

$\bar{t}_{\mathrm{NoP}} = 2\,\mathrm{Jahre}$, $A \geq 1 - 10^{-6}$, für 99% der MF automatische Fehlfunktionsbehandlung mit $t_{\mathrm{TS1}} = 30\,\mathrm{s}$, 1% der MF durch Ausfall, Reparaturdauer t_{TS2}.

a) *Wie viel Zeit steht im Mittel für Problembehandlung zu Verfügung?*

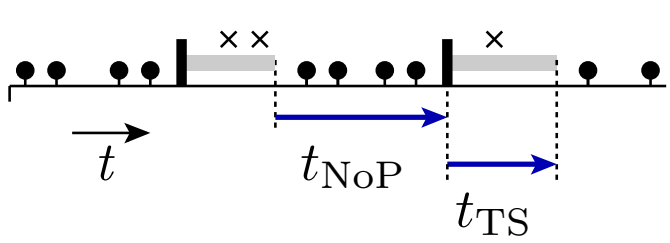
b) *Wie groß darf die mittlere Zeit $\bar{t}_{\mathrm{TS2}}$ für den Tausch der Steuerung betragen?*

c) *Wiederholen Sie die Abschätzung für eine geforderte Verfügbarkeit von nur $A = 1 - 10^{-5}$?*

$\bar{t}_{\mathrm{NoP}} = 2\,\mathrm{Jahre}$, $A \geq 1 - 10^{-6}$, für 99% der MF automatische Fehlfunktionsbehandlung mit $t_{\mathrm{TS1}} = 30\,\mathrm{s}$, 1% der MF durch Ausfall, Reparaturdauer t_{TS2}.

a) *Wie viel Zeit steht im Mittel für Problembehandlung zu Verfügung?*

(1.2) $$A = \frac{\bar{t}_{\mathrm{NoP}}}{\bar{t}_{\mathrm{NoP}} + \bar{t}_{\mathrm{TS}}}$$



- nutzbare Service-Leistung
- × Service-Verweigerung
- erkanntes Problem
- Problembehandlung

$$\bar{t}_{\mathrm{TS}} = \frac{\bar{t}_{\mathrm{NoP}}}{A} - \bar{t}_{\mathrm{NoP}} = \bar{t}_{\mathrm{NoP}} \cdot \left(\frac{1-A}{A}\right)$$
$$= 2\,\mathrm{Jahre} \cdot 10^{-6} = 31{,}54\,\mathrm{s}$$

$\bar{t}_{\mathrm{NoP}}$	Mittlere problemfreie Zeit.
t_{TS}, $\bar{t}_{\mathrm{TS}}$	Zeit und mittlere Zeit für die Problembehebung (troubleshooting).
A	Verfügbarkeit (Availability).

$\bar{t}_{\mathrm{NoP}} = 2\,\mathrm{Jahre}$, $A \geq 1 - 10^{-6}$, für 99% der MF automatische Fehlfunktionsbehandlung mit $t_{\mathrm{TS1}} = 30\,\mathrm{s}$, 1% der MF durch Ausfall, Reparaturdauer t_{TS2}.

b) *Wie groß darf die mittlere Zeit $\bar{t}_{\mathrm{TS2}}$ für den Tausch der Steuerung betragen?*

$$\begin{aligned}\bar{t}_{\mathrm{TS}} &= 99\% \cdot t_{\mathrm{TS1}} + 1\% \cdot \bar{t}_{\mathrm{TS2}} \\ \bar{t}_{\mathrm{TS2}} &= \frac{\bar{t}_{\mathrm{TS}} - 99\% \cdot t_{\mathrm{TS1}}}{1\%} \\ &= 100 \cdot (31{,}54\,\mathrm{s} - 99\% \cdot 30\,\mathrm{s}) = 164\,\mathrm{s}\end{aligned}$$

Der Tausch einer Steuerung innerhalb von im Mittel 2,5 min verlangt eine Ersatzsteuerung vor Ort, die automatisch und ohne manuelle Unterstützung die Aufgaben der ausgefallenen Steuerung übernimmt.

$\bar{t}_{\mathrm{NoP}} = 2\,\mathrm{Jahre}$, $A \geq 1 - 10^{-6}$, für 99% der MF automatische Fehlfunktionsbehandlung mit $t_{\mathrm{TS1}} = 30\,\mathrm{s}$, 1% der MF durch Ausfall, Reparaturdauer t_{TS2}.

c) *Wiederholen Sie die Abschätzung für eine geforderte Verfügbarkeit von nur $A = 1 - 10^{-5}$?*

(1.2) $$A = \frac{\bar{t}_{\mathrm{NoP}}}{\bar{t}_{\mathrm{NoP}} + \bar{t}_{\mathrm{TS}}}$$

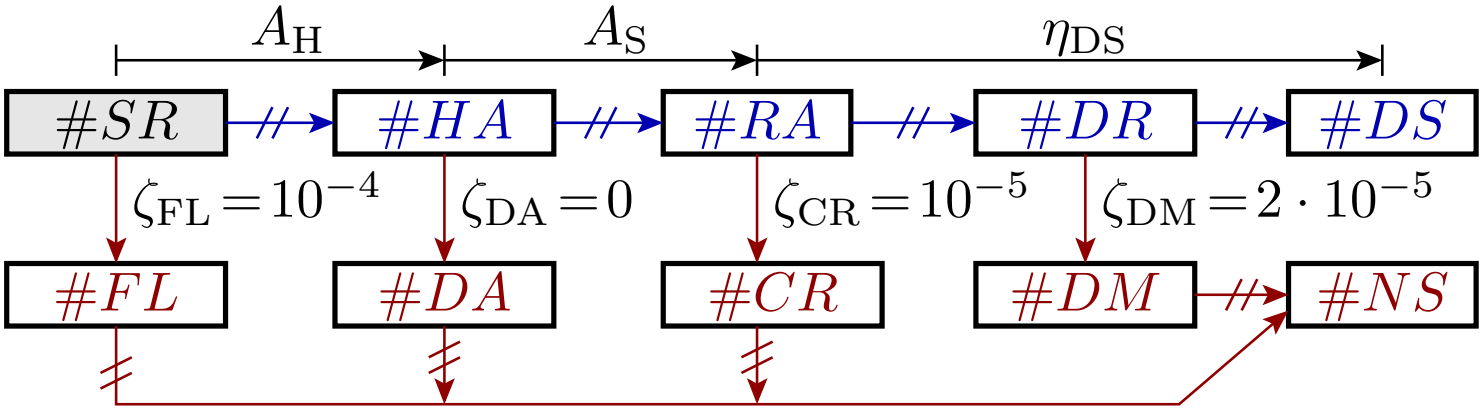
$$\bar{t}_{\mathrm{TS}} = \bar{t}_{\mathrm{NoP}} \cdot \left(\tfrac{1-A}{A}\right) = 315{,}4\,\mathrm{s}$$

Zehnfacher Wert gegenüber Aufgabenteil a.

$$\begin{aligned}\bar{t}_{\mathrm{TS2}} &= \frac{\bar{t}_{\mathrm{TS}} - 99\% \cdot t_{\mathrm{TS1}}}{1\%} \\ &= 100 \cdot (315{,}4\,\mathrm{s} - 99\% \cdot 30\,\mathrm{s}) \approx 8\,\mathrm{Stunden}\end{aligned}$$

Ein Tausch in 8 Stunden verlangt, dass 7 Tage pro Woche für 24 Stunden Reparaturpersonal bereit steht und die Ersatzsteuerung schnell beschaffbar ist.

Aufgabe 1.3: Verfügbarkeit, CVA-Graph

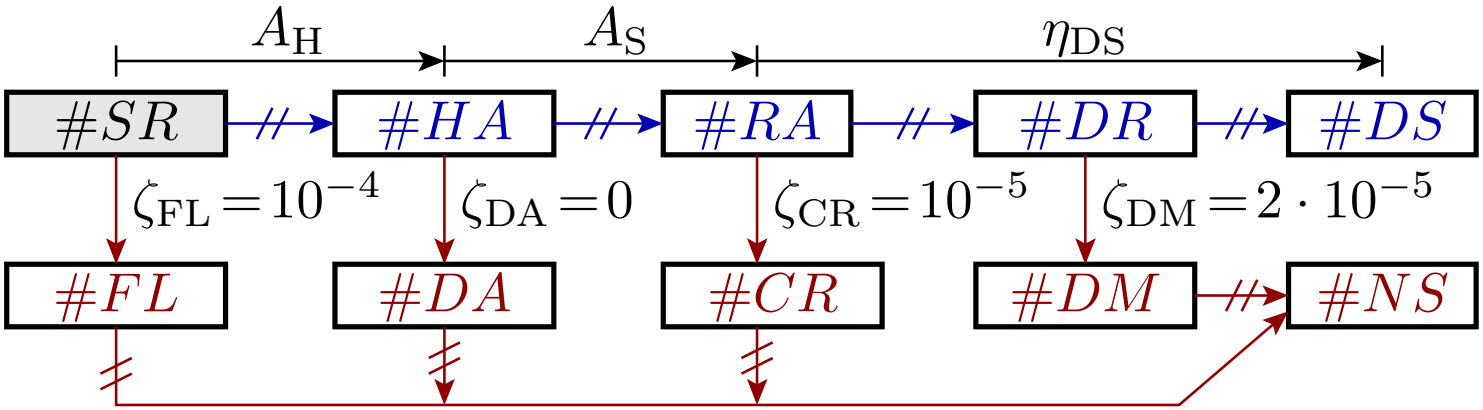


a) *Wie heißen die Zählwerte und Problemraten?*

b) *Wie groß sind die einzelnen Teilverfügbarkeiten?*

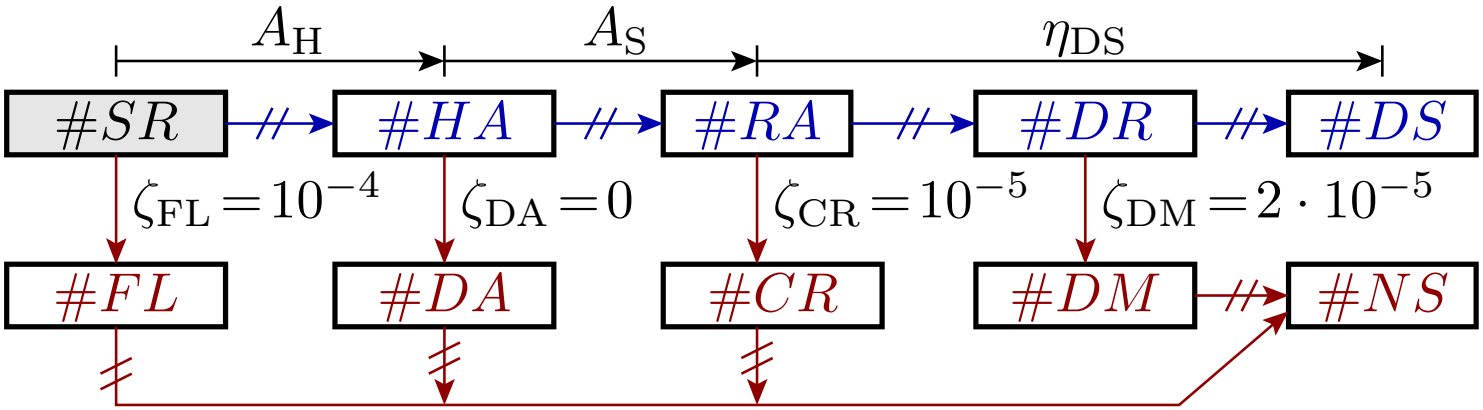
c) *Wie groß ist die Verfügbarkeit insgesamt?*

A_{H}	Hardware-Verfügbarkeit.
A_{S}	Service-Verfügbarkeit.
η_{DS}	Rate der erbrachen Service-Leistungen.



a) *Wie heißen die Zählwerte und Problemraten?*

$\#\langle evt \rangle$	Anzahl der Zählereignisse, $evt \in \{SR, HA, \ldots\ldots\}$.
SR, HA	Service-Anforderung, Hardware verfügbar.
RA, DR	Service-Anforderung akzeptiert, erbrachtes Ergebnis.
DS, NS	Erbrachte Service-Leistung, keine Service-Leistung.
FL, DA	Nichtverfügbarkeit wegen Hardware-Ausfall bzw. Annahmeverweigerung.
CR, DM	Nichtverfügbarkeit wegen Absturz bzw. erkannter Fehlfunktion.
ζ_{FL}, ζ_{DA}	HW-Nichtverfügbarkeitsrate, Service-Verweigerungsrate.
ζ_{CR}, ζ_{DM}	Absturzrate, Rate der erkannten Fehlfunktionen.



b) *Wie groß sind die einzelnen Teilverfügbarkeiten?*

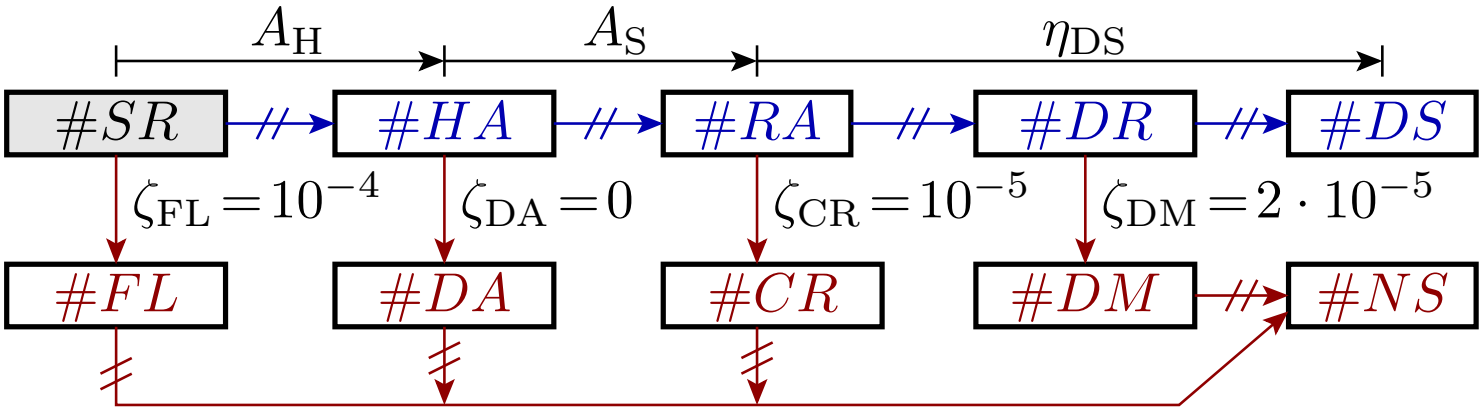
(1.3) $$A_H = (1 - \zeta_{FL}) + \zeta_{FL} \cdot \nu_{FL}$$

(1.4) $$A_S = (1 - \zeta_{DA}) + \zeta_{DA} \cdot \nu_{DA}$$

$$A_H = (1 - \zeta_{FL}) + \zeta_{FL} \cdot 0 = 1 - 10^{-4} \left[\frac{HA}{SR}\right]$$

$$A_S = (1 - \zeta_{DA}) + \zeta_{DA} \cdot 0 = 1 \left[\frac{RA}{HA}\right]$$

$$\eta_{DS} = \left.\frac{\#DS}{\#RA}\right|_{ACR} = (1 - \zeta_{CR}) \cdot (1 - \zeta_{DM}) = 1 - 3 \cdot 10^{-5} \left[\frac{DS}{RA}\right]$$



c) *Wie groß ist die Verfügbarkeit insgesamt?*

(1.5) $$A = A_H \cdot A_S \cdot \eta_{DS}$$

$$\begin{aligned} A &= \left(1 - 10^{-4}\right) \left[\frac{\text{HA}}{\text{SR}}\right] \cdot 1 \left[\frac{\text{RA}}{\text{HA}}\right] \cdot \left(1 - 3 \cdot 10^{-5}\right) \left[\frac{\text{DS}}{\text{RA}}\right] \\ &= 1 - \left(10^{-4} - 3 \cdot 10^{-5}\right) \left[\frac{\text{DS}}{\text{SR}}\right] \end{aligned}$$

A_H	Hardware-Verfügbarkeit.
A_S	Service-Verfügbarkeit.
η_{DS}	Rate der erbrachen Service-Leistungen.

Aufgabe 1.4: Transistorausfall

Durch den Ausfall eines Transistors in einem Schaltkreis steigt die Fehlfunktionsrate eines Rechners von $\zeta_1 = 10^{-5}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$ auf $\zeta_2 = 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$.

a) *Wie hoch ist die Zuverlässigkeit des Rechners vor und nach dem Ausfall des Transistors?*

b) *Welche MF-Rate verursacht der ausgefallene Transistor?*

ζ Fehlfunktionsrate.

$\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$ Zählwertverhältnis in Fehlfunktionen je erbrachte Service-Leistung.

Durch den Ausfall eines Transistors in einem Schaltkreis steigt die Fehlfunktionsrate eines Rechners von $\zeta_1 = 10^{-5}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$ auf $\zeta_2 = 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$.

a) *Wie hoch ist die Zuverlässigkeit des Rechners vor und nach dem Ausfall des Transistors?*

(1.9) $$\zeta_{[\mathrm{MT}]} = \frac{1}{R_{[\mathrm{MT}]}} = \frac{\#NDM}{\#DS}\Big|_{\mathrm{ACR}}$$

Vor dem Ausfall:

$$R_1 = \frac{1}{10^{-5}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]} = 10^5\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

Nach dem Ausfall:

$$R_2 = \frac{1}{10^{-4}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]} = 10^4\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

R	Zuverlässigkeit (Reliability).
$\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$	Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.

Durch den Ausfall eines Transistors in einem Schaltkreis steigt die Fehlfunktionsrate eines Rechners von $\zeta_1 = 10^{-5}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$ auf $\zeta_2 = 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$.

b) *Welche MF-Rate verursacht der ausgefallene Transistor?*

(1.11) $$\zeta_{[\mathrm{MT}]} = \sum_{i=1}^{\#MFC} \zeta_{[\mathrm{MT}].i}$$

MF-Rate des ausgefallenen Transistors:

$$\begin{aligned} \zeta_2 &= \zeta_1 + \zeta_{\mathrm{Tr}} \\ \zeta_{\mathrm{Tr}} &= \zeta_2 - \zeta_1 \\ &= 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right] - 10^{-5}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right] = 9 \cdot 10^{-5}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right] \end{aligned}$$

ζ	Gesamte Fehlfunktionsrate (Total malfunction rate).
$\#MFC$	Anzahl MF-Klassen, hier MF durch ausgefallenen Transistor und sonstige MF.
ζ_i	MF-Rate der MF-Klasse i (MF rate of MF class i).
ζ_{Tr}	Fehlfunktionsrate verursacht durch den ausgefallenen Transistor.

Aufgabe 1.5: Zuverlässigkeit Gesamtsystem

Ein IT-System bestehe aus folgenden Komponenten:

Teilsystem	Rechner	Fest-platte	Stromver-sorgung	sonstiges
Teilzuverlässigkeit	R_{R}	R_{Disc}	R_{Power}	R_{others}
Wert in DS/MF	1000	500	700	2000

Die Anzahl zeitgleicher MF durch mehrere Teilsysteme und die Anzahl der MF eines Teilsystems ohne Gesamt-MF seien vernachlässigbar.

a) *Welche Zuverlässigkeit hat das Gesamtsystem?*

b) *Welche MF-Rate hat das Gesamtsystem?*

$[\frac{\mathrm{DS}}{\mathrm{MF}}]$ Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.

Ein IT-System bestehe aus folgenden Komponenten:

Teilsystem	Rechner	Fest-platte	Stromver-sorgung	sonstiges
Teilzuverlässigkeit	R_{R}	R_{Disc}	R_{Power}	R_{others}
Wert in DS/MF	1000	500	700	2000

a) *Welche Zuverlässigkeit hat das Gesamtsystem?*

(1.12)
$$\frac{1}{R_{[\mathrm{MT}]}} = \sum_{i=1}^{\#MFC} \frac{1}{R_{[\mathrm{MT}].i}}$$

$$R = \frac{1}{\frac{1}{1000} + \frac{1}{500} + \frac{1}{700} + \frac{1}{2000}} = 203\,\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

R	Gesamtzuverlässigkeit (Total reliability).
$\#MFC$	Anzahl der MF-Klassen (Number of malfunction classes).
R_i	Teilzuverlässigkeit (partitial reliability) von MF-Klasse i.

Ein IT-System bestehe aus folgenden Komponenten:

Teilsystem	Rechner	Fest-platte	Stromver-sorgung	sonstiges
Teilzuverlässigkeit	R_{R}	R_{Disc}	R_{Power}	R_{others}
Wert in DS/MF	1000	500	700	2000

b) *Welche MF-Rate hat das Gesamtsystem?*

(1.9)
$$\zeta_{[\mathrm{MT}]} = \frac{1}{R_{[\mathrm{MT}]}} = \frac{\#NDM}{\#DS}\Big|_{\mathrm{ACR}}$$

$$\zeta = \frac{1}{203\,\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]} = 4{,}93 \cdot 10^{-3}\,\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$$

ζ Gesamte Fehlfunktionsrate (Total malfunction rate).

$\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$ Zählwertverhältnis in Fehlfunktionen je erbrachte Service-Leistung.

Aufgabe 1.6: Zuverlässigkeit und Betriebssicherheit

Bei einem IT-System mit einer mittleren Zeit bis zur nächsten nicht erkannten Fehlfunktionen von 10^3 Stunden gefährdet im Mittel jede hundertste Fehlfunktion die Betriebssicherheit. Mittlere Service-Dauer $1\,\mathrm{h}$, Systemauslastung 100%. Sicherheitgefährdungen durch erkennbare Probleme (Ausfälle, Annahmeverweigerung, Absturz und erkannte MF vernachlässigbar.

$\bar{t}_{\mathrm{NDM}} = 10^3\,\mathrm{h}$, $\rho = 10^{-2}\ \left[\frac{\mathrm{SP}}{\mathrm{NDM}}\right]$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 1$, $\zeta_{\mathrm{S.OP}} = \zeta_{\mathrm{S.FL}} = 0$

a) *Zuverlässigkeit und Sicherheit?*

b) *Um welchen Faktor ν muss eine Sicherheitseinheit mit $R_{\mathrm{SU}} = 5.000\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$ den Anteil der sicherheitskritischen Fehlfunktionen mindestens reduzieren, zur Erhöhung der Sicherheit auf $S_{\mathrm{SU}} = 10^6\ \left[\frac{\mathrm{DS}}{\mathrm{SP}}\right]$?*

$\bar{t}_{\mathrm{NDM}}, \bar{t}_{\mathrm{S}}$ Mittlere Service-Zeit je nicht erkannte Fehlfunktion, mittlere Service-Dauer.
η_{SU} Systemauslastungsrate.

$\bar{t}_{\mathrm{NDM}} = 10^3\,\mathrm{h}$, $\rho = 10^{-2}\ [\frac{\mathrm{SP}}{\mathrm{NDM}}]$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 1$, $\zeta_{\mathrm{S.OP}} = \zeta_{\mathrm{S.FL}} = 0$

a) *Zuverlässigkeit und Sicherheit?*

(1.10) $$R_{[\mathrm{MT}]} = \frac{\eta_{\mathrm{SU}} \cdot \bar{t}_{\mathrm{NDN}}}{\bar{t}_{\mathrm{S}}}$$

(1.24) $$S = \frac{R_{\mathrm{MT}}}{\rho}$$

$$R = \frac{10^3\,\mathrm{h}}{1\,\mathrm{h}} = 10^3\ [\frac{\mathrm{DS}}{\mathrm{MF}}]$$
$$S = \frac{R}{\rho} = 10^5\ [\frac{\mathrm{DS}}{\mathrm{SP}}]$$

$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
ζ	Fehlfunktionsrate.
R	Zuverlässigkeit (Reliability).
$[\frac{\mathrm{DS}}{\mathrm{MF}}]$	Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.
$[\frac{\mathrm{MF}}{\mathrm{DS}}]$	Zählwertverhältnis in Fehlfunktionen je erbrachte Service-Leistung.

$\bar{t}_{\mathrm{NDM}} = 10^3\,\mathrm{h}$, $\rho = 10^{-2}\ [\frac{\mathrm{SP}}{\mathrm{NDM}}]$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 1$, $\zeta_{\mathrm{S.OP}} = \zeta_{\mathrm{S.FL}} = 0$

b) *Um welchen Faktor ν muss eine Sicherheitseinheit mit $R_{\mathrm{SU}} = 5.000\,[\frac{\mathrm{DS}}{\mathrm{MF}}]$ den Anteil der sicherheitskritischen Fehlfunktionen mindestens reduzieren, zur Erhöhung der Sicherheit auf $S_{\mathrm{SU}} = 10^6\ [\frac{\mathrm{DS}}{\mathrm{SP}}]$?*

(1.25) $$S_{\mathrm{SU}} = \frac{1}{(\zeta+\zeta_{\mathrm{SU}})\cdot\rho\cdot\nu}$$

$$\nu \leq \frac{1}{S_{\mathrm{SU}}\cdot\left(\frac{1}{R}+\frac{1}{R_{\mathrm{SU}}}\right)\cdot\rho} = \frac{1}{10^6\cdot\left(\frac{1}{10^3}+\frac{1}{5\cdot10^3}\right)\cdot1\%} = \frac{1}{12}$$

Die Sicherheitseinheit muss bewirken, dass im Mittel von zuvor 12 nur noch ein Problem sicherheitskritisch bleibt.

$[\frac{\mathrm{DS}}{\mathrm{SP}}]$ Verhältnis in erbrachten Service-Leistungen je sicherheitsgefährdende Fehlfunktion.

MF-Beseitigung

Aufgabe 1.7: Kenngrößen Überwachung

Von 10^5 erbrachten Service-Leitungen sind 10^3 Fehlfunktionen aufgetreten, von denen die Kontrolle 600 erkannt hat. Von den korrekte Service-Leistungen hat die Kontrolle 10 als Fehlfunktionen ausgewiesen.

$\#DS = 10^5, \#MF = 10^3, \#DM = 600, \#PM = 10$

a) *Wie groß sind die beobachtete und die tatsächliche Zuverlässigkeit?*

b) *Wie groß ist die Fehlfunktionsüberdeckung der Überwachung?*

c) *Wie groß ist die Phantom-MF-Rate der Überwachung?*

$\#DS$	Anzahl der erbrachten Service-Leistungen.
$\#MF$	Anzahl der Fehlfunktionen (Number of malfunctions).
$\#DM$	Anzahl der erkannten Fehlfunktionen (Number of detected MFs).
$\#PM$	Anzahl der Phantom-MF, d.h. der korrekten DS, die als MF klassifiziert werden.
$[\frac{\mathrm{DS}}{\mathrm{MF}}]$	Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.

$\#DS = 10^5, \#MF = 10^3, \#DM = 600, \#PM = 10$

a) *Wie groß sind die beobachtete und die tatsächliche Zuverlässigkeit?*

(1.8) $$R_{[\mathrm{MT}]} = \frac{\#DS}{\#NDM}\Big|_{\mathrm{ACR}}$$

Beobachtet werden als Fehlfunktionen die erkannten plus die Phantom-Fehlfunktionen:

$$R = \frac{\#DS}{\#DM+\#PM} = \frac{10^5}{610} = 164$$

Als tatsächliche Fehlfunktionen zählen zusätzlich die nicht erkannten, aber nicht die Phantomfehlfunktionen:

$$R = \frac{\#DS}{\#MF} = \frac{10^5}{10^3}\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right] = 100\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

R	Zuverlässigkeit (Reliability).
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

$\#DS = 10^5, \#MF = 10^3, \#DM = 600, \#PM = 10$

b) *Wie groß ist die Fehlfunktionsüberdeckung der Überwachung?*

(1.26) $$MC = \frac{\#DM}{\#MF}\Big|_{\mathrm{ACR}}$$

$$MC = \frac{600\,[\mathrm{DM}]}{1000\,[\mathrm{MF}]} = 60\%$$

c) *Wie groß ist die Phantom-MF-Rate der Überwachung?*

(1.27) $$\zeta_{\mathrm{PM}} = \frac{\#PM}{\#CS}\Big|_{\mathrm{ACR}}$$

$$\zeta_{\mathrm{PM}} = \zeta_{\mathrm{PM}} = \frac{\#PM}{\#DS - \#MF}\Big|_{\mathrm{ACR}} = \frac{10\,[\mathrm{PM}]}{\left(10^5 - 10^3\right)[\mathrm{CS}]} = 1{,}01 \cdot 10^{-4}\left[\frac{\mathrm{PM}}{\mathrm{DS}}\right]$$

MC, ζ_{PM}	Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.
$[\mathrm{MF}]$	Zählwert in Fehlfunktionen.
$\left[\frac{\mathrm{PM}}{\mathrm{DS}}\right]$	Zählwertverhältnis in Phantom-Fehlfunktionen je erbrachte Service-Leistung.

Aufgabe 1.8: Übertragung mit Wiederholung nach MF

Datenübertragung mit Fehlfunktionsrate $10^{-6}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$ und 8 redundanten Bits je Datensatz. Verfälschung werden gleichhäufig auf alle darstellbaren Werte verteilt und Erkennung aller unzulässigen Werte. Max. eine Wiederholung nach erkannten Problemen. MF-Usache zu 100% Störungen. Ausfälle sollen nicht betrachtet werden.

$\zeta = 10^{-6}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$, $r = 8$, $\eta_{\mathrm{Div}} = 1$, $\zeta_{\mathrm{PM}} = \zeta_{\mathrm{CR}} = 0$.

a) *Fehlfunktionsüberdeckung?*

b) *Zuverlässigkeit ohne und mit Fehlfunktionsbehandlung?*

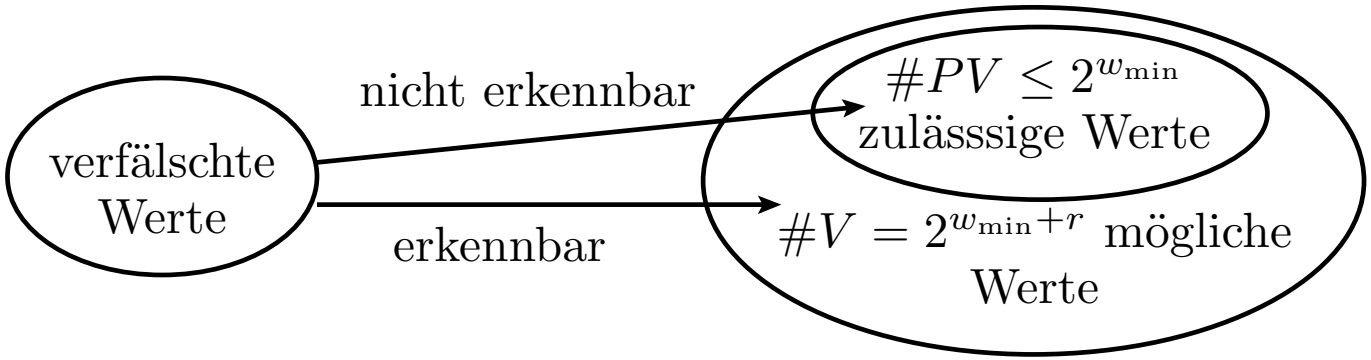
c) *Erbringungsrate ohne und mit max. einer Wiederholanforderung bei Empfang einer erkannten verfälschten Nachricht?*

d) *Erforderliche Anzahl der redundanten Datenbits zur Erhöhung der Zuverlässigkeit auf 10^{10} übertragene Datensätze je nicht erkannte Datenverfälschung?*

$\zeta_{\mathrm{CR}}, \zeta$	Absturzrate, Fehlfunktionsrate.
r	Anzahl der redundanten Bits.

$\zeta = 10^{-6}\ [\frac{\mathrm{MF}}{\mathrm{DS}}], r = 8, \eta_{\mathrm{Div}} = 1, \zeta_{\mathrm{PM}} = \zeta_{\mathrm{CR}} = 0.$

a) *Fehlfunktionsüberdeckung?*



(1.35) $MC \geq 1 - 2^{-r}$

$MC = 1 - 2^{-8} = 99{,}61\%$

η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
ζ_{PM}	Phantom-Fehlfunktionsrate.
$\#VP, \#PP$	Anzahl der gültigen Bitmuster, Anzahl der darstellbaren Bitmuster.
MC, r	Fehlfunktionsabdeckung, Anzahl der redundanten Bits.
$w_{\min}$	Erforderliche Bitanzahl zu Unterscheidung aller zuslässigen Werte.

$\zeta = 10^{-6}\ [\frac{\mathrm{MF}}{\mathrm{DS}}], r = 8, \eta_{\mathrm{Div}} = 1, \zeta_{\mathrm{PM}} = \zeta_{\mathrm{CR}} = 0.$

b) *Zuverlässigkeit ohne und mit Fehlfunktionsbehandlung?*

(1.9) $$\zeta_{[\mathrm{MT}]} = \frac{1}{R_{[\mathrm{MT}]}} = \frac{\#NDM}{\#DS}\Big|_{\mathrm{ACR}}$$

(1.36) $$R_{\mathrm{MT}} = 2^r \cdot R$$

$$R = \frac{1}{\zeta} = \frac{1}{10^{-6}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]} = 10^6\ \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

$$R_{\mathrm{MT}} = 2^8 \cdot 10^6\ \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right] = 2{,}56 \cdot 10^8\ \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

$R_{[\mathrm{MT}]}$ Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.

$[\frac{\mathrm{DS}}{\mathrm{MF}}]$ Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.

$\zeta = 10^{-6}\ [\frac{\text{MF}}{\text{DS}}], r = 8, \eta_{\text{Div}} = 1, \zeta_{\text{PM}} = \zeta_{\text{CR}} = 0.$

c) *Erbringungsrate ohne und mit max. einer Wiederholanforderung bei Empfang einer erkannten verfälschten Nachricht?*

(1.28) $\eta_{\text{DS}} = (1 - \zeta_{\text{CR}}) \cdot (1 - \zeta_{\text{SMF}})$ mit $\zeta_{\text{SMF}} = \zeta_{\text{PM}} + \zeta \cdot MC - \zeta \cdot \zeta_{\text{PM}}$

(1.41) $\eta_{\text{DS.SR}} = \eta_{\text{DS}} \cdot (1 + (1 - \eta_{\text{DS}}) \cdot \eta_{\text{Div}})$

Erbringungsrate ohne Wiederholanforderung:

$$\eta_{\text{DS}} = 1 - \zeta \cdot MC = 1 - 10^6\ [\tfrac{\text{DS}}{\text{MF}}] \cdot (1 - 2^{-8}) = 1 - 10^6\ [\tfrac{\text{DS}}{\text{MF}}]$$

Erbringungsrate bei max. einer Wiederholanforderung:

$$\eta_{\text{DS.SR}} = (1 - 10^6) \cdot (1 + 10^6) = 1 - 10^{12}$$

η_{DS} Rate der erbrachen Service-Leistungen.
$\eta_{\text{DS.SR}}$ Erbringungsrate bei max. einer Wiederholung nach Nichterbringung.

$\zeta = 10^{-6}\ [\frac{\mathrm{MF}}{\mathrm{DS}}]$, $r = 8$, $\eta_{\mathrm{Div}} = 1$, $\zeta_{\mathrm{PM}} = \zeta_{\mathrm{CR}} = 0$.

d) *Erforderliche Anzahl der redundanten Datenbits zur Erhöhung der Zuverlässigkeit auf 10^{10} übertragene Datensätze je nicht erkannte Datenverfälschung?*

(1.36) $$R_{\mathrm{MT}} = 2^r \cdot R$$

$$r = -\log_2\left(\frac{R_{\mathrm{MT}}}{R}\right) = -\log_2\left(\frac{10^{10}}{10^6}\right) \geq 13{,}3$$

Mindestens $r = 14$ redundante Bits.

Aufgabe 1.9: Mehrheitsentscheid

Alle drei Einzelsysteme haben die übereinstimmende Absturzrate $\zeta_{\mathrm{CR}} = 10^{-5}$ und MF-Raten $\zeta = 10^{-4}$. 75% der Fehlfunktionen entstehen durch Störungen und sind diversitär. Die restlich 25% der Fehlfunktionen werden durch Fehler verursacht und sind nur zu 60% diversitär. Nicht erbrachte Leistungen sind mit 5% und nicht erkannten Fehlfunktionen mit 1% sicherheitsgefährdent.

$\zeta_{\mathrm{CR}} = 10^{-5}\ \left[\frac{\mathrm{CR}}{\mathrm{RA}}\right], \zeta = 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right], \eta_{\mathrm{Div}} = 75\% \cdot 1 + 25\% \cdot 60\%,$
$\rho_{\mathrm{CR}} = 5\%, \rho = 1\%$

a) *Wiederholung des CVA-Graphen aus der Vorlesung?*

b) *Erbringungsrate?*

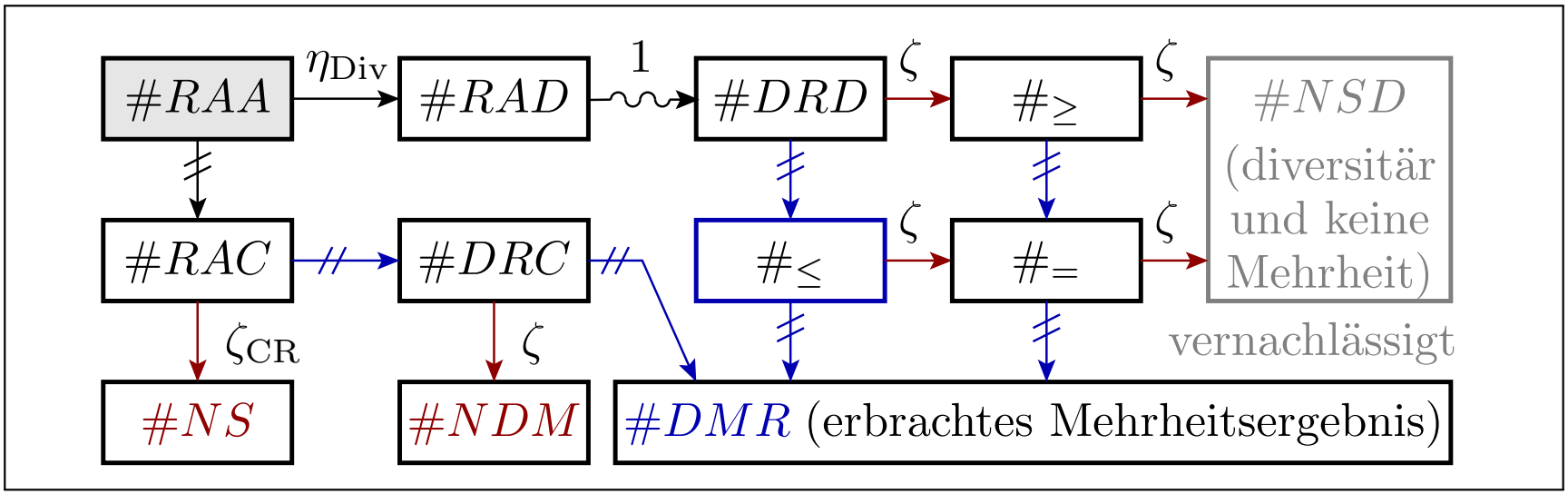
c) *Zuverlässigkeit?*

d) *Sicherheit?*

η_{DS} Rate der erbrachen Service-Leistungen.
η_{Div} Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
$\zeta_{\mathrm{CR}}, \zeta$ Absturzrate, Fehlfunktionsrate.
ρ Anteil sicherheitskritischer Fehlfunktionen an den nicht erkannten Fehlfunktionen.

$\zeta_{\mathrm{CR}} = 10^{-5}\ \left[\frac{\mathrm{CR}}{\mathrm{RA}}\right], \zeta = 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right], \eta_{\mathrm{Div}} = 75\% \cdot 1 + 25\% \cdot 60\%,$
$\rho_{\mathrm{CR}} = 5\%, \rho = 1\%$

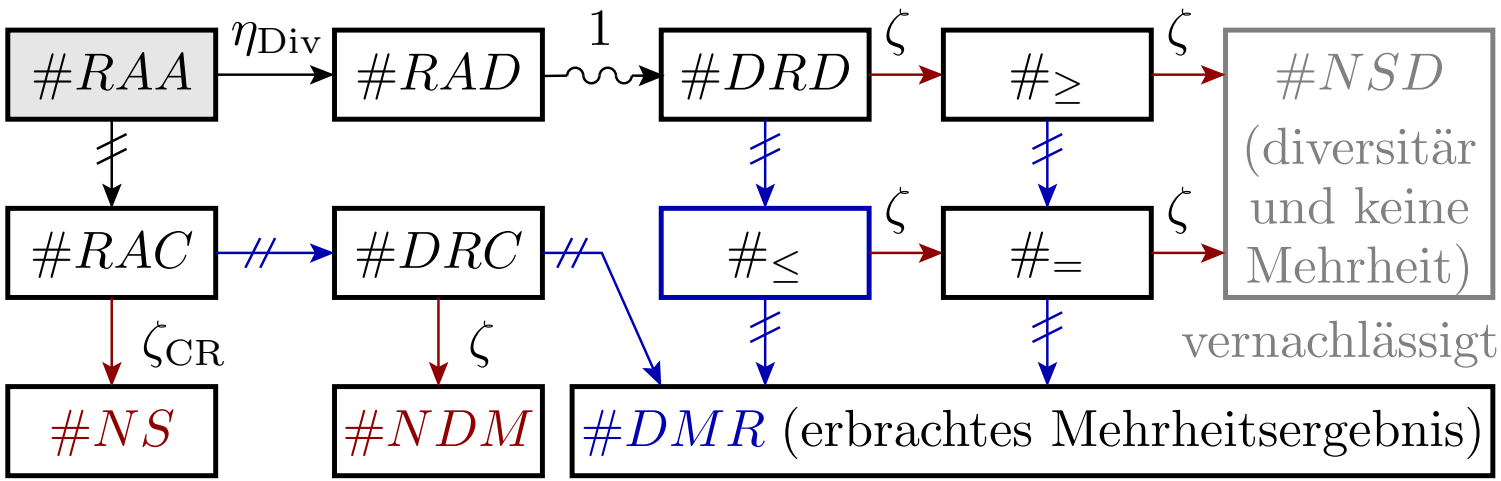
a) *Wiederholung des CVA-Graphen aus der Vorlesung?*



RAA	Alle drei Service-Anforderungen akzeptiert.
RAC	Alle drei Anforderungen akzeptiert, mögliche Probleme haben gemeinsame Ursache.
RAD	Alle drei Anforderungen akzeptiert, mögliche Probleme haben diversitäre Ursachen.
DRC	Alle drei Ergebnis erbracht, mögliche Fehlfunktionen haben gemeinsame Ursachen.
DRD	Alle drei Ergebnis erbracht, mögliche Fehlfunktionen haben diversitäre Ursachen.
NDM, NS	Nicht erkannte Fehlfunktion, keine Service-Leistung.
$\#_{\geq}, \#_{\leq}, \#_{=}$	Mindestens, maximal bzw. genau eine Fehlfunktion bei zwei Berechnungen.

$\zeta_{\mathrm{CR}} = 10^{-5}\ \left[\frac{\mathrm{CR}}{\mathrm{RA}}\right], \zeta = 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right], \eta_{\mathrm{Div}} = 75\% \cdot 1 + 25\% \cdot 60\%,$
$\rho_{\mathrm{CR}} = 5\%, \rho = 1\%$

b) *Erbringungsrate?*



(1.44) $\eta_{\mathrm{DS}} = 1 - (1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{CR}}$

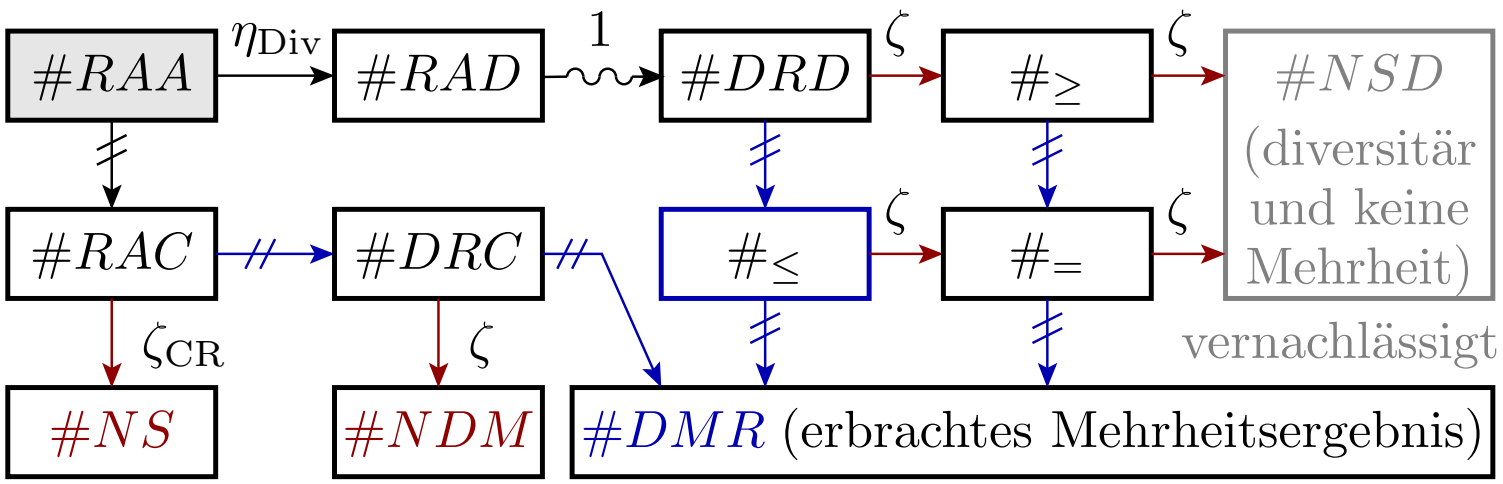
$\eta_{\mathrm{Div}} = 75\% \cdot 1 + 25\% \cdot 60\% = 90{,}6\%$

$\eta_{\mathrm{DS}} = 1 - (1 - 90{,}6\%) \cdot 10^{-5} = 1 - 9{,}4 \cdot 10^{-7}$

η_{DS} Rate der erbrachen Service-Leistungen.

$\zeta_{\mathrm{CR}} = 10^{-5}\ \left[\frac{\mathrm{CR}}{\mathrm{RA}}\right], \zeta = 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right], \eta_{\mathrm{Div}} = 75\% \cdot 1 + 25\% \cdot 60\%,$
$\rho_{\mathrm{CR}} = 5\%, \rho = 1\%$

c) *Zuverlässigkeit?*



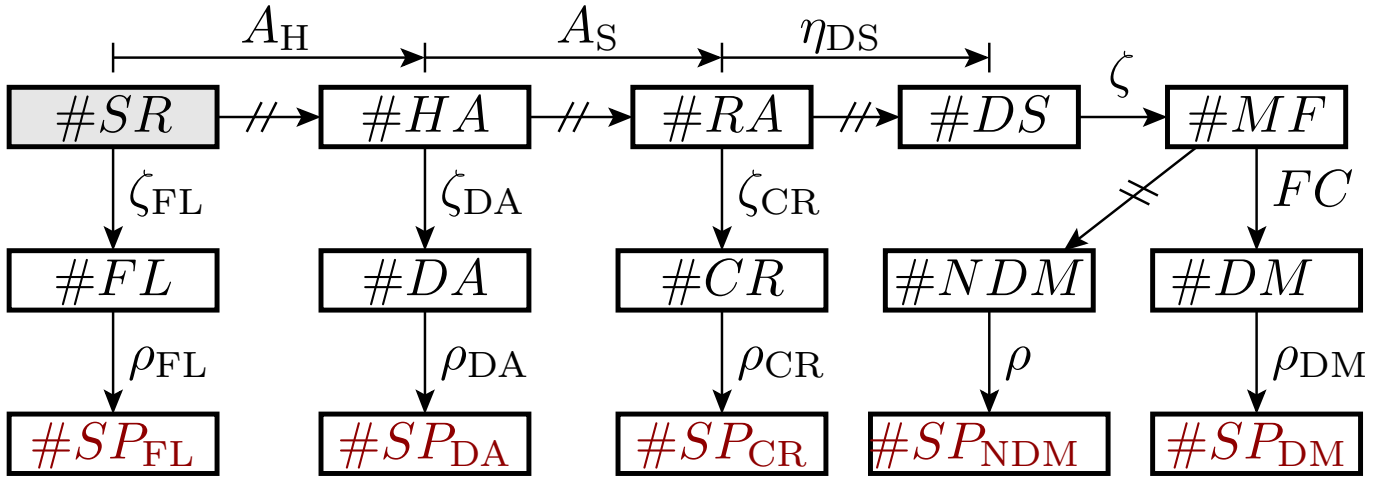
(1.45) $$R_{\mathrm{MV}} = \frac{\eta_{\mathrm{DS}}}{\eta_{\mathrm{NDM}}} = \frac{1-(1-\eta_{\mathrm{Div}})\cdot\zeta_{\mathrm{CR}}}{(1-\eta_{\mathrm{Div}})\cdot(1-\zeta_{\mathrm{CR}})\cdot\zeta}$$

$$R_{\mathrm{MV}} = \frac{1-(1-90{,}6\%)\cdot 10^{-5}}{(1-90{,}6\%)\cdot(1-10^{-5})\cdot 10^{-4}} = \frac{1}{(1-90{,}6\%)\cdot 10^{-4}} = 1{,}06 \cdot 10^{5}\ \left[\frac{\mathrm{DS}}{\mathrm{NDM}}\right]$$

R_{MV} Zuverlässigkeit Gesamtsystem mit Mehrheitsentscheid.

$\zeta_{\mathrm{CR}} = 10^{-5}\ \left[\frac{\mathrm{CR}}{\mathrm{RA}}\right], \zeta = 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right], \eta_{\mathrm{Div}} = 75\% \cdot 1 + 25\% \cdot 60\%,$
$\rho_{\mathrm{CR}} = 5\%, \rho = 1\%$

d) *Sicherheit?*



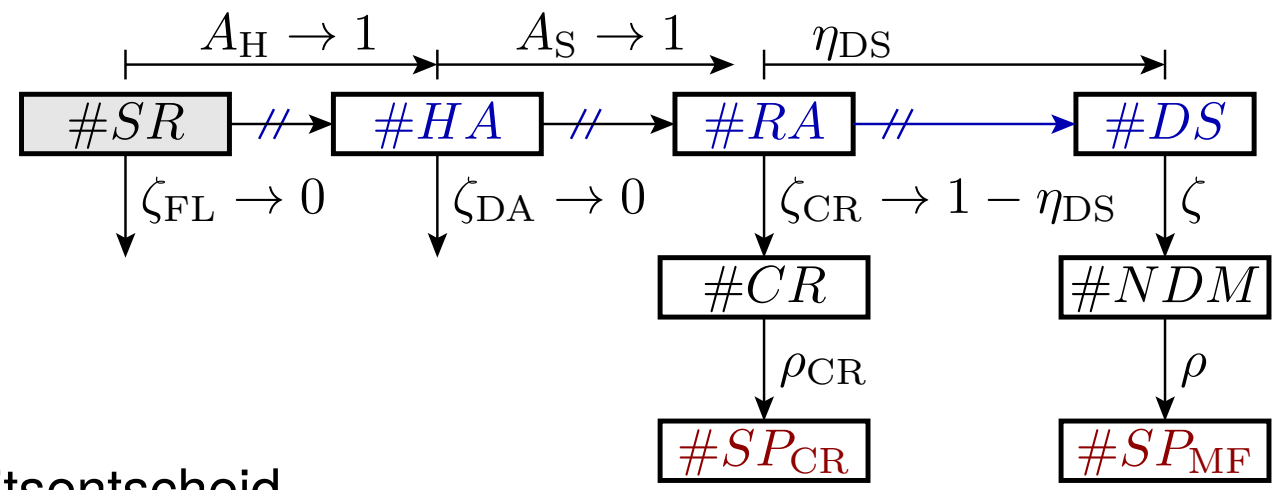
Für A_{H}, A_{S}und η_{DS} nahe eins:

(1.23) $\zeta_{\mathrm{S}} = \zeta_{\mathrm{FL}} \cdot \rho_{\mathrm{FL}} + \zeta_{\mathrm{DA}} \cdot \rho_{\mathrm{DA}} + \zeta_{\mathrm{CR}} \cdot \rho_{\mathrm{CR}} + \zeta \cdot (FC \cdot \rho_{\mathrm{DM}} + (1 - FC) \cdot \rho)$

SR, FL	Service-Anforderung, Hardware ausgefallen.
HA, DA	Harware verfügbar, Annahme verweigert.
RA, CR	Anforderung akzeptiert, Absturz.
DS, MF	Erbrachte Leistung, Fehlfunktion.

$\zeta_{\mathrm{CR}} = 10^{-5}\ \left[\frac{\mathrm{CR}}{\mathrm{RA}}\right], \zeta = 10^{-4}\ \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right], \eta_{\mathrm{Div}} = 75\% \cdot 1 + 25\% \cdot 60\%,$
$\rho_{\mathrm{CR}} = 5\%, \rho = 1\%$

d) *Sicherheit?*



Mehrheitsentscheid

- Versagen durch Abstürze $\eta_{\mathrm{CR}} \to 1 - \eta_{\mathrm{DS}}$
- nicht erkannte und korrigierte Fehlfunktionen: $\zeta \to \frac{1}{R_{\mathrm{MT}}}$

$$\zeta_{\mathrm{S}} = (1 - \eta_{\mathrm{DS}}) \cdot \rho_{\mathrm{CR}} + \eta_{\mathrm{DS}} \cdot \frac{1}{R_{\mathrm{MT}}} \cdot \rho$$
$$= 9{,}4 \cdot 10^{-7} \cdot 5\% + \frac{1-9{,}4 \cdot 10^{-7}}{1{,}06 \cdot 10^{5}} \cdot 1\% = 1{,}4 \cdot 10^{7}$$

Aufgabe 1.10: Sicherheitserhöhung durch MF-Behandlung

Bei einem IT-System mit einer mittleren Nutzungsdauer zwischen zwei MF von 2500 Stunden, einer mittleren Service-Dauer von einer Stunde, Systemauslastung 40% gefährde abschätzungsweise jede hundertste MF die Betriebssicherheit. Um die Betriebssicherheit auf $10^6\ \left[\frac{\mathrm{DS}}{\mathrm{SP}}\right]$ zu erhöhen, soll das System um eine MF-Behandlung erweitert werden, die es bei Erkennen einer Fehlfunktion in einen sicheren Zustand überführt.

$\bar{t}_{\mathrm{NDM}} = 2.500\,\mathrm{h}$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 40\%$, $\rho = 1\%$, $S = 10^6\ \left[\frac{\mathrm{DS}}{\mathrm{SP}}\right]$

a) *Erforderliche Fehlfunktionsüberdeckung, wenn beim Überführen in den sicheren Zustand keine Fehlfunktionen auftreten?*

b) *Erforderliche Fehlfunktionsüberdeckung, wenn im Mittel jeder 20te Versuch, einen sicheren Zustand herzustellen, scheitert?*

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

$\bar{t}_{\mathrm{NDM}}, \bar{t}_{\mathrm{S}}$	Mittlere Service-Zeit je nicht erkannte Fehlfunktion, mittlere Service-Dauer.
η_{SU}, S	Systemauslastungsrate, Sicherheit.
ρ	Anteil sicherheitskritischer Fehlfunktionen an den nicht erkannten Fehlfunktionen.
$\left[\frac{\mathrm{DS}}{\mathrm{SP}}\right]$	Verhältnis in erbrachten Service-Leistungen je sicherheitsgefährdende Fehlfunktion.

$\bar{t}_{\mathrm{NDM}} = 2.500\,\mathrm{h}$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 40\%$, $\rho = 1\%$, $S = 10^6$ $\left[\frac{\mathrm{DS}}{\mathrm{SP}}\right]$

a) *Erforderliche Fehlfunktionsüberdeckung, wenn beim Überführen in den sicheren Zustand keine Fehlfunktionen auftreten?*

(1.10) $$R_{[\mathrm{MT}]} = \frac{\eta_{\mathrm{SU}} \cdot \bar{t}_{\mathrm{NDN}}}{\bar{t}_{\mathrm{S}}}$$

Sicherheitskritische Probleme nur durch nicht erkannte Fehlfunktionen:

$$S = \frac{1}{\rho \cdot \zeta \cdot (1 - MC)} = \frac{R}{\rho \cdot (1 - MC)}$$

$$R = \frac{40\% \cdot 2.500\,\mathrm{h}}{1\,\mathrm{h}} = 1000$$

$$MC = 1 - \frac{R}{\rho \cdot S} = 1 - \frac{1000}{1\% \cdot 10^6} = 90\%$$

R	Zuverlässigkeit (Reliability).
MC	Fehlfunktionsabdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.

$\bar{t}_{\mathrm{NDM}} = 2.500\,\mathrm{h}$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 40\%$, $\rho = 1\%$, $S = 10^6$ $\left[\frac{\mathrm{DS}}{\mathrm{SP}}\right]$

b) *Erforderliche Fehlfunktionsüberdeckung, wenn im Mittel jeder 20te Versuch, einen sicheren Zustand herzustellen, scheitert?*

Potentielle sicherheitskritische Probleme zusätzlich für jede zwanzigste, d.h. 5% der erkannten Fehlfunktionen:

$$S = \frac{1}{\rho\cdot(\zeta\cdot(1-MC)+5\%\cdot\zeta\cdot MC)} = \frac{R}{\rho\cdot((1-MC)+5\%\cdot MC)}$$

$$MC = \frac{1-\frac{R}{\rho\cdot S}}{95\%} = \frac{90\%}{95\%} = 94{,}7\%$$

Überschlag zur Kontrolle: Statt 1 von 10 darf etwa nur 1 von 20 Fehlfunktionen unerkannt bleiben.

$\bar{t}_{\mathrm{NDM}} = 2.500\,\mathrm{h}$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 40\%$, $\rho = 1\%$, $S = 10^6\ \left[\frac{\mathrm{DS}}{\mathrm{SP}}\right]$

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

Ein sicherer Zustand wird für 95% der erkannten Fehlfunktionen, d.h. für

$$MC \cdot 95\% = 90\%$$

aller Fehlfunktionen hergestellt. Mittlerer Zeitabstand:

$$\bar{t}_{\mathrm{NDM}}/90\% = 2778\,\mathrm{h}$$

In 99% der Fälle ist die Fehlfunktion nicht sicherheitskritisch. Mittlere Zeit zwischen dem Herstellen eines sicheren Zustands ohne Gefährdung der Betriebssicherheit:

$$2778\,\mathrm{h}/99\% = 2800\,\mathrm{h}$$

Modellbildung Teil 2

Fehlerbeseitigung

Aufgabe 2.1: Fehler und Störungen

a) *Warum ist es viel einfacher, Fehlfunktionen durch Störungen zu korrigieren als solche, 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?*

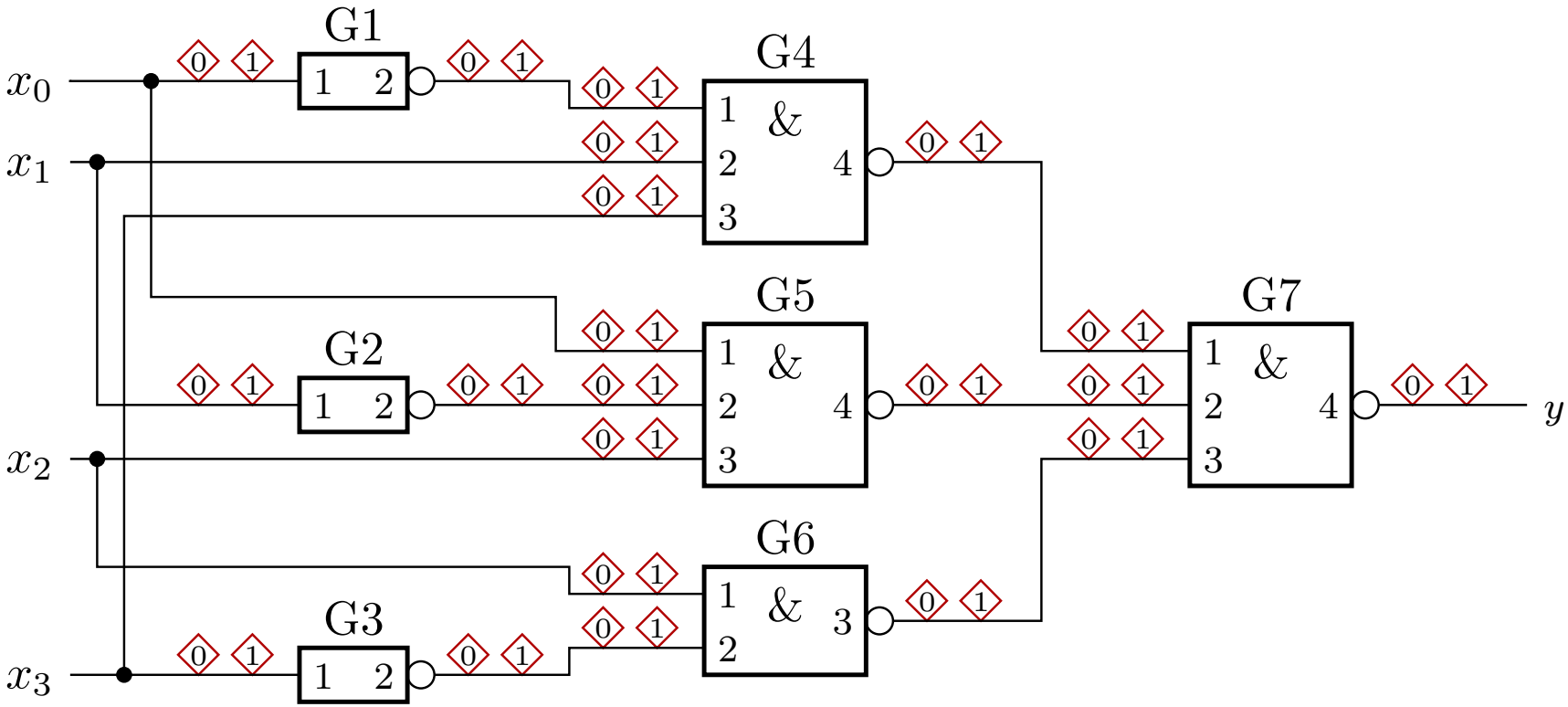
a) *Warum ist es viel einfacher, Fehlfunktionen durch Störungen zu korrigieren als solche, die durch Fehler verursacht werden?*

Störungen wirken diversitär. Eine erkannte Fehlfunktion 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) *Warum ist es bei der Beseitigung der Ursachen genau umgekehrt, dass sich Fehler gut beseitigen lassen, aber die Beseitigung von Störquellen erheblich schwieriger ist?*

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

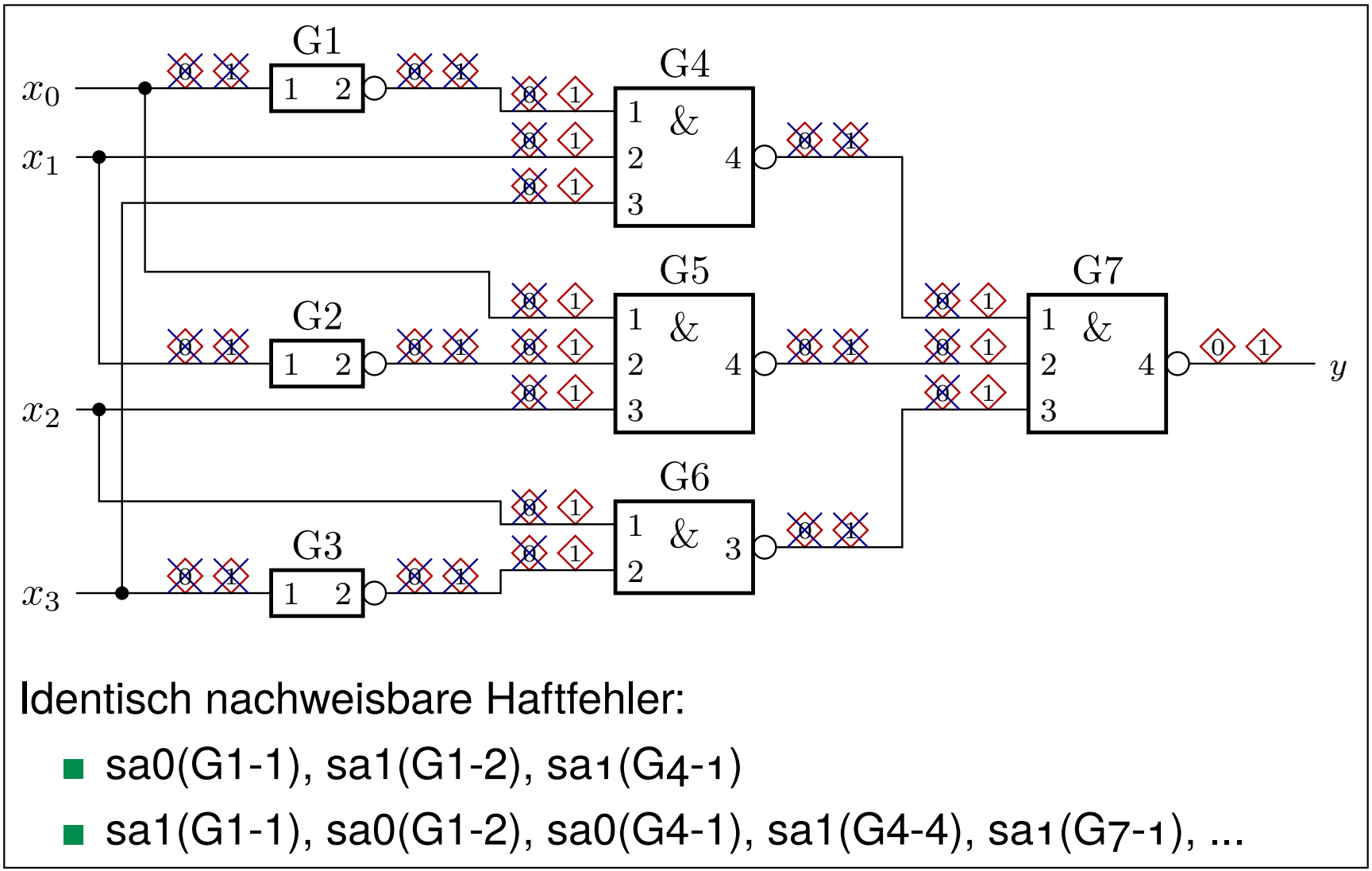
Aufgabe 2.2: Vereinfachung einer Haftfehlermenge



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

b) *Bestimmen Sie davon alle implizit nachweisbaren Haftfehler.*

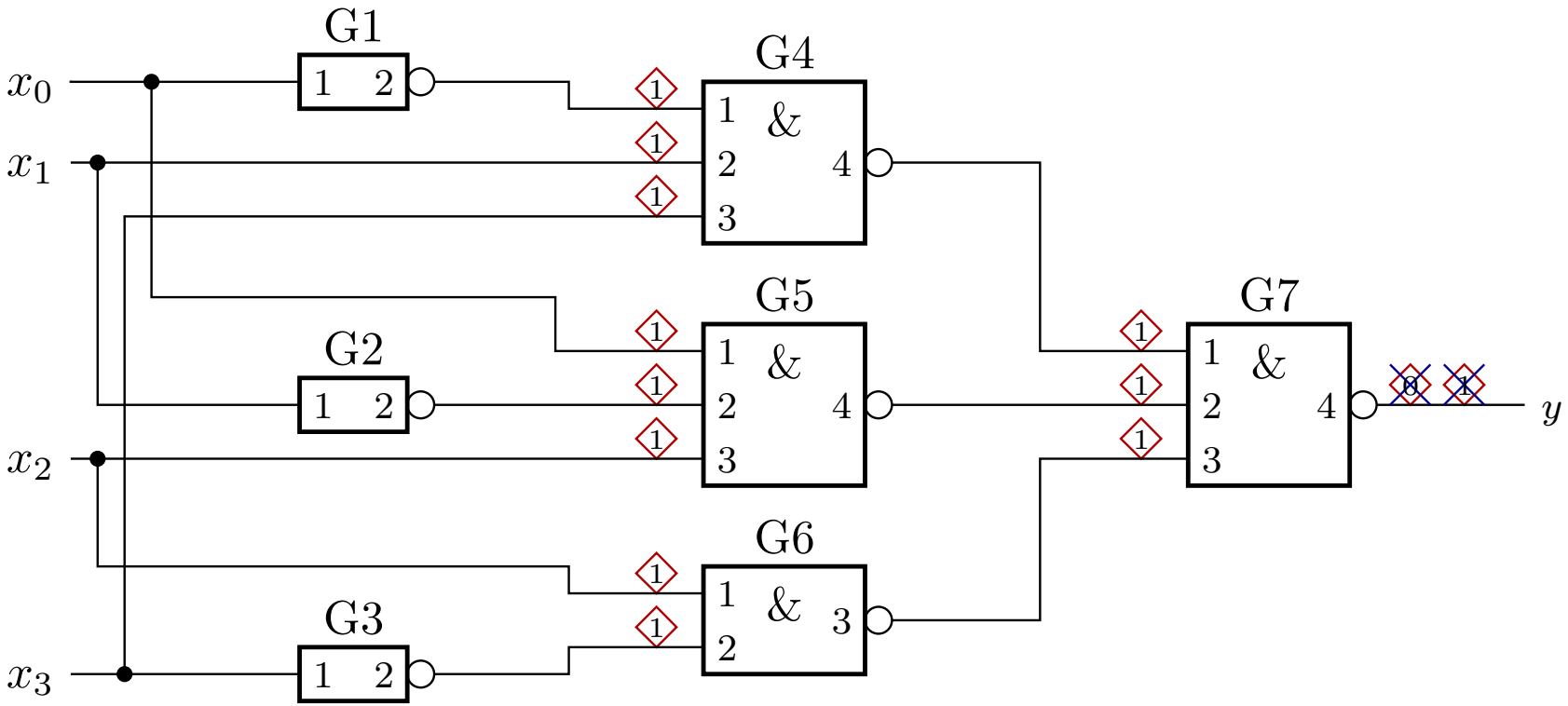
a) *Fassen Sie alle identisch nachweisbaren Haftfehler zu einem Modellfehler zusammen.*



Identisch nachweisbare Haftfehler:

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

b) *Bestimmen Sie davon 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), ...

Zuverlässigkeit und Test

Aufgabe 2.3: Fehleranzahl, MF-Rate und Zuverlässigkeit

In einer Iteration aus Test und Fehlerbeseitigung, bei der alle erkannten Fehler beseitigt wurden, war bei Erhöhung der Anzahl der dynamischen Tests von 10^5 auf 10^6 eine Verringerung der MF-Rate von 10^{-3} auf $4{\cdot}10^{-5}$ MF je DS zu beobachten. MF durch Störungen sind zu vernachlässigen.

$N_1 = 10^5$, $N_2 = 10^6$, $\zeta(N_1) = 10^{-3}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$, $\zeta(N_2) = 4 \cdot 10^{-5}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$, $\zeta_{\mathrm{D}} = 0$

a) *Auf welchen Exponenten K für die Dichte der MF-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_1 auf N_2 abschätzungsweise beseitigt?*

c) *Welche Zuverlässigkeit ist nach N_2 Tests zu erwarten und welche Testsatzlänge N_3 ist nach den Modellannahmen erforderlich, um die zu erwartende Zuverlässigkeit auf $10^8\ \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$ zu erhöhen?*

N_1, N_2 Testanzahl mit bekannter / gesuchter Fehleranzahl oder Zuverlässigkeit.

$N_1 = 10^5$, $N_2 = 10^6$, $\zeta\left(N_1\right) = 10^{-3}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$, $\zeta\left(N_2\right) = 4 \cdot 10^{-5}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$, $\zeta_\mathrm{D} = 0$

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

(2.22)
$$K = \log\left(\frac{\zeta_\mathrm{F}(N_1)}{\zeta_\mathrm{F}(N_2)}\right) / \log\left(\frac{N_2}{N_1}\right) - 1$$

Wegen $\zeta_\mathrm{D} = 0$ ist $\zeta_\mathrm{F} = \zeta$:

$$K = \left(\ln\left(\frac{10^{-3}}{4 \cdot 10^{-5}}\right) / \ln\left(\frac{10^{-5}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]}{10^{-6}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]}\right)\right) - 1 = 0{,}4$$

$\zeta_\mathrm{F}\left(N\right)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.
$\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$	Zählwertverhältnis in Fehlfunktionen je erbrachte Service-Leistung.
ζ_D	Fehlfunktionsrate durch Störungen (Malfunction rate due to disturbance).
K	Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.

$N_1 = 10^5$, $N_2 = 10^6$, $\zeta\left(N_1\right) = 10^{-3}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$, $\zeta\left(N_2\right) = 4 \cdot 10^{-5}\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$,
$\zeta_{\mathrm{D}} = 0$

b) *Wie viele Fehler werden in der Iteration aus Test und Beseitigung der erkennbaren Fehler bei Erhöhung der Testsatzlänge von N_1 auf N_2 abschätzungsweise beseitigt?*

(2.21) $$\zeta_{\mathrm{F}}\left(N\right) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{N}$$

$$\mu_{\mathrm{F}}\left(N_1\right) = \frac{N_1}{K} \cdot \zeta\left(N_1\right) = \frac{10^5}{0{,}4} \cdot 10^{-3} = 251\ [\mathrm{F}]$$

$$\mu_{\mathrm{F}}\left(N_2\right) = \frac{N_2}{K} \cdot \zeta\left(N_2\right) = \frac{10^6}{0{,}4} \cdot 4 \cdot 10^{-5} = 100\ [\mathrm{F}]$$

Zu erwartende Anzahl der zu beseitigenden Fehler:

$$\mu_{\mathrm{F}}\left(N_1\right) - \mu_{\mathrm{F}}\left(N_2\right) = 151\ [\mathrm{F}]$$

$\mu_{\mathrm{F}}\left(N\right)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
$[\mathrm{F}]$	Zählwert in Fehlern.

$N_1 = 10^5$, $N_2 = 10^6$, $\zeta(N_1) = 10^{-3}\ [\frac{\text{MF}}{\text{DS}}]$, $\zeta(N_2) = 4 \cdot 10^{-5}\ [\frac{\text{MF}}{\text{DS}}]$, $\zeta_\text{D} = 0$

c) *Welche Zuverlässigkeit ist nach N_2 Tests zu erwarten und welche Testsatzlänge N_3 ist nach den Modellannahmen erforderlich, um die zu erwartende Zuverlässigkeit auf $10^8\ [\frac{\text{DS}}{\text{MF}}]$ zu erhöhen?*

(2.26)
$$R_\text{F}(N_2) = R_\text{F}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{K+1}$$

Wegen $\zeta_\text{D} = 0$ ist $\zeta_\text{F} = \zeta$ und $R_\text{F} = R$:

$$R(N_2) = \frac{1}{\zeta(N_2)} = \frac{1}{4 \cdot 10^{-5}\ [\frac{\text{DS}}{\text{MF}}]} = 25000\ [\frac{\text{DS}}{\text{MF}}]$$

$$N_3 = N_2 \cdot \left(\frac{R(N_3)}{R(N_2)}\right)^{\frac{1}{K+1}} = 10^6 \cdot \left(\frac{10^8\ [\frac{\text{DS}}{\text{MF}}]}{2{,}5 \cdot 10^4\ [\frac{\text{DS}}{\text{MF}}]}\right)^{\frac{1}{0{,}4+1}} = 3{,}77 \cdot 10^8$$

$R_\text{F}(N)$ $[\frac{\text{DS}}{\text{MF}}]$ Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehler. Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.

Aufgabe 2.4: Vortest und Zufallstest

Von 1000 entstandenen Fehlern erkennt der vorgelagerte statische Test 80%, von den verbleibenden 20% erkennen 20 gezielt gesuchte dynamische Tests 60% und von den dann noch verbleibenden $20\% \cdot 40\%$ erkennen weitere 80 zufällige Tests 50%. Beseitigung aller erkannten Fehler.

$\mu_{\mathrm{FCR}} = 10^3$, $FC_{\mathrm{PT}} = 1 - 0{,}2 \cdot 0{,}4$, $N_0 = 20$, $N_1 = N_0 + 80$, $\frac{\mu_{\mathrm{F}}(N_1)}{\mu_{\mathrm{F}}(N_0)} = \frac{1}{2}$.

a) *Mit welchem Exponenten K nimmt der zu erwartende Anteil der nicht erkannten Fehler bei Erhöhung der Testsatzlänge von $N_0 = 20$ auf $N_1 = 100$ ab?*

b) *Zu erwartende Fehleranzahl und fehlerbezogene Teilzuverlässigkeit nach Beseitigung aller erkannten Fehler?*

c) *Wie groß sind Fehleranzahl und fehlerbezogene Teilzuverlässigkeit nach Erhöhung der Anzahl der Tests von $N_1 = 100$ auf $N_2 = 1000$?*

μ_{FCR}	Zu erwartende Fehleranzahl aus den Entstehungs- und Reparaturprozessen insgesamt.
FC_{PT}	Fehlerabdeckung aller Vortests zusammen.
N_0	Anzahl der dynamischen Tests aller Vortests zusammen.
N_1, N_2	Testanzahl mit bekannter Fehlfunktionsrate bzw. zu erwartender Fehleranzahl.
$\mu_{\mathrm{F}}(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.

$\mu_{\mathrm{FCR}} = 10^3$, $FC_{\mathrm{PT}} = 1 - 0{,}2 \cdot 0{,}4$, $N_0 = 20$, $N_1 = N_0 + 80$, $\frac{\mu_{\mathrm{F}}(N_1)}{\mu_{\mathrm{F}}(N_0)} = \frac{1}{2}$.

d) *Wie viele zusätzliche Zufallstests erfordert eine Verringerung der zu erwartenden Anzahl nicht erkennbarer Fehler auf 4?*

e) *Wie viele zusätzliche Zufallstests erfordert eine Erhöhung der fehlerbezogenen Teilzuverlässigkeit auf $R_{\mathrm{F}}(N) = 1000\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$?*

$R_{\mathrm{F}}(N)$ Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehler.
$\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$ Zählwertverhältnis in Fehlfunktionen je erbrachte Service-Leistung.

$\mu_{\mathrm{FCR}} = 10^3$, $FC_{\mathrm{PT}} = 1 - 0{,}2 \cdot 0{,}4$, $N_0 = 20$, $N_1 = N_0 + 80$, $\frac{\mu_{\mathrm{F}}(N_1)}{\mu_{\mathrm{F}}(N_0)} = \frac{1}{2}$.

a) *Mit welchem Exponenten K nimmt der zu erwartende Anteil der nicht erkannten Fehler bei Erhöhung der Testsatzlänge von $N_0 = 20$ auf $N_1 = 100$ ab?*

(2.17)
$$K = -\log\left(\frac{\mu_{\mathrm{F}}(N_2)}{\mu_{\mathrm{F}}(N_1)}\right) / \log\left(\frac{N_2}{N_1}\right)$$

Bei der Vergrößerung der Anzahl der Zufallstests von $N_0 = 20$ auf $N_1 = 100$ halbiert sich die Anzahl der nicht nachweisbaren Fehler:

$$\frac{\mu_{\mathrm{F}}(N_1)}{\mu_{\mathrm{F}}(N_0)} = \frac{1}{2} = \left(\frac{N_1}{N_0}\right)^{-K} = 5^{-K}$$

$$K = -\frac{\ln(0{,}5)}{\ln(5)} = 0{,}431$$

K Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.

$\mu_{\mathrm{FCR}} = 10^3$, $FC_{\mathrm{PT}} = 1 - 0{,}2 \cdot 0{,}4$, $N_0 = 20$, $N_1 = N_0 + 80$, $\frac{\mu_{\mathrm{F}}(N_1)}{\mu_{\mathrm{F}}(N_0)} = \frac{1}{2}$.

b) *Zu erwartende Fehleranzahl und fehlerbezogene Teilzuverlässigkeit nach Beseitigung aller erkannten Fehler?*

(2.23) $$\mu_{\mathrm{F}}(N_0) = \mu_{\mathrm{FCR}} \cdot (1 - FC_{\mathrm{PT}})$$

(2.25) $$R_{\mathrm{F}}(N) = \frac{N}{K \cdot \mu_{\mathrm{F}}(N)}$$

Von den entstandenen Fehlern erkennen die statischen Vortests 80%, davon die dynamischen Vortests 60% und davon die Zufallstests 50%:

$$\mu_{\mathrm{F}}(N_1) = \mu_{\mathrm{FCR}} \cdot (1 - FC_{\mathrm{PT}}) \cdot 0{,}5 = 1000\ [\mathrm{F}] \cdot 0{,}2 \cdot 0{,}4 \cdot 0{,}5 = 40\ [\mathrm{F}]$$

Fehlerbezogene Teilzuverlässigkeit:

$$R_{\mathrm{F}}(N_1) = \frac{100}{0{,}431 \cdot 40} = 5{,}8\ \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

$\mu_{\mathrm{FCR}} = 10^3$, $FC_{\mathrm{PT}} = 1 - 0{,}2 \cdot 0{,}4$, $N_0 = 20$, $N_1 = N_0 + 80$, $\frac{\mu_{\mathrm{F}}(N_1)}{\mu_{\mathrm{F}}(N_0)} = \frac{1}{2}$.

c) *Wie groß sind Fehleranzahl und fehlerbezogene Teilzuverlässigkeit nach Erhöhung der Anzahl der Tests von $N_1 = 100$ auf $N_2 = 1000$?*

(2.16) $$\mu_{\mathrm{F}}(N_2) = \mu_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit } 0 < K < 1$$

(2.26) $$R_{\mathrm{F}}(N_2) = R_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{K+1}$$

Zu erwartende Fehleranzahl:

$$\mu_{\mathrm{F}}(N_2) = 40\ [\mathrm{F}] \cdot \left(\frac{1000}{100}\right)^{-0{,}431} = 14{,}8\ [\mathrm{F}]$$

Fehlerbezogene Teilzuverlässigkeit:

$$R_{\mathrm{F}}(N_2) = 5{,}8\ \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right] \cdot \left(\frac{1000}{100}\right)^{1+0{,}431} = 157\ \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

$\mu_{\mathrm{FCR}} = 10^3$, $FC_{\mathrm{PT}} = 1 - 0{,}2 \cdot 0{,}4$, $N_0 = 20$, $N_1 = N_0 + 80$, $\frac{\mu_{\mathrm{F}}(N_1)}{\mu_{\mathrm{F}}(N_0)} = \frac{1}{2}$.

d) *Wie viele zusätzliche Zufallstests erfordert eine Verringerung der zu erwartenden Anzahl nicht erkennbarer Fehler auf* 4*?*

(2.16) $$\mu_{\mathrm{F}}(N_2) = \mu_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit } 0 < K < 1$$

Umstellung nach der gesuchten Testanzahl N_3:

$$N_3 = N_1 \cdot \left(\frac{\mu_{\mathrm{F}}(N_3)}{\mu_{\mathrm{F}}(N_1)}\right)^{-\frac{1}{K}}$$

$$= 100 \cdot \left(\frac{4}{40}\right)^{-\frac{1}{0{,}431}} = 20.900$$

Eine Verringerung der zu erwartenden Anzahl der nicht beseitigten Fehler von 40 auf 4 erfordert zusätzlich 20.800 zufällig ausgewählte Tests, d.h. die 209-fache Testsatzlänge.

$\mu_{\mathrm{FCR}} = 10^3$, $FC_{\mathrm{PT}} = 1 - 0{,}2 \cdot 0{,}4$, $N_0 = 20$, $N_1 = N_0 + 80$, $\frac{\mu_{\mathrm{F}}(N_1)}{\mu_{\mathrm{F}}(N_0)} = \frac{1}{2}$.

e) *Wie viele zusätzliche Zufallstests erfordert eine Erhöhung der fehlerbezogenen Teilzuverlässigkeit auf* $R_{\mathrm{F}}(N) = 1000\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$*?*

(2.26)
$$R_{\mathrm{F}}(N_2) = R_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{K+1}$$

Umstellung nach der gesuchten Testanzahl N_4:

$$N_4 = N_1 \cdot \left(\frac{R_{\mathrm{F}}(N_4)}{R_{\mathrm{F}}(N_1)}\right)^{\frac{1}{1+K}}$$

$$= 100 \cdot \left(\frac{1000\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]}{5{,}8\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]}\right)^{\frac{1}{1{,}431}} = 3.656$$

Eine Erhöhung der Zuverlässigkeit von 5,8 auf 1000 (etwa das 170-fache) verlangt nur zusätzlich 3.556 zufällig ausgewählte Tests, d.h. die 25-fache Testsatzlänge.