

Test und Verlässlichkeit Grosse Übung

Prof. G. Kemnitz

28. Oktober 2024

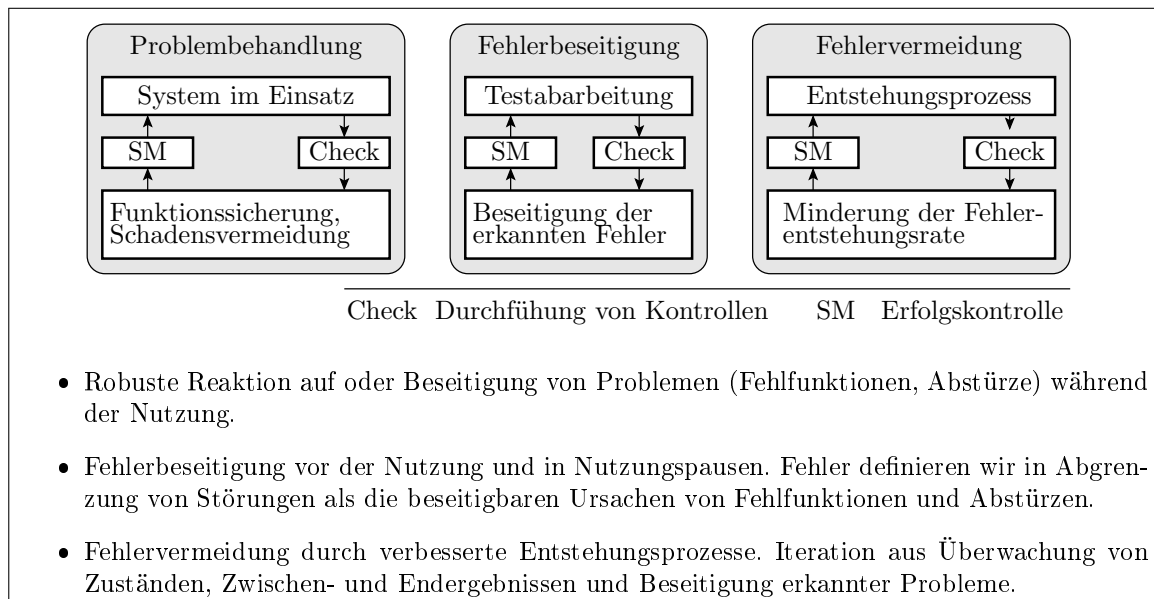
1. Foliensatz	Übung 1 (1.1)	2.1	Fehlerbeseitigung
1.1	Verlässlichkeit	2.2	Zuverlässigkeit und Test
1.2	Problembehandlung	2.3	Fehlervermeidung
2. Foliensatz	Übung 2 (2.6)		

1 Modellbildung

1.1 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?

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 die Systeme 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.

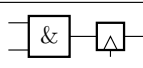
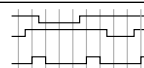
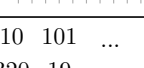
c) *Ein Modell in der Informatik hebt die wesentlichen Aspekte hervor und vernachlässigt unwesentliche Details. Was sind wesentliche Aspekte und was sind vernachlässigte unwesentliche Details das Service-Modells?*

Anforderung (SR) + Eingabe → Service → Ausgabe: NS, DS: CS oder MF

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

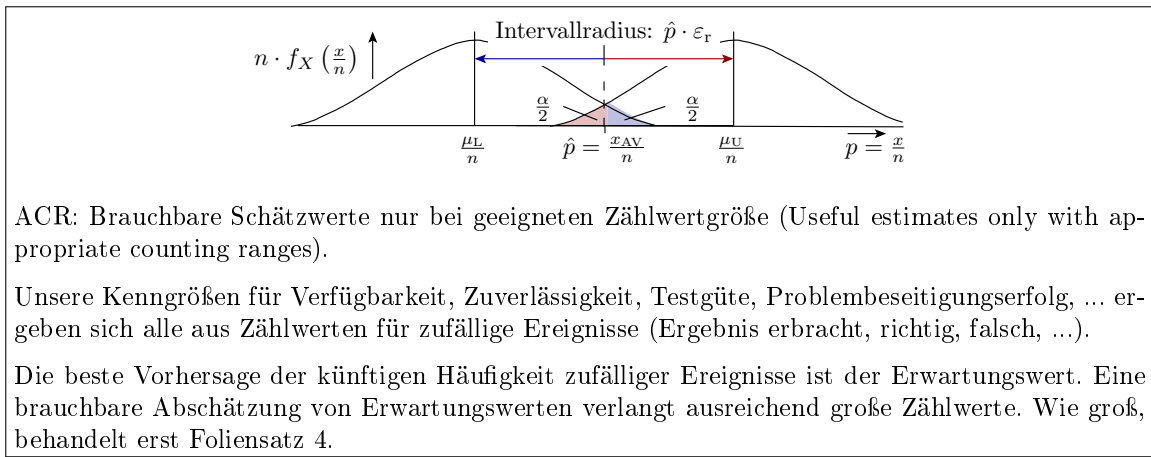
Das erlaubt, die positiven und negativen Ergebnisse zu zählen und Raten für deren Häufigkeit zu definieren und damit die einzelnen Teilaspekte der Verlässlichkeit (Verfügbarkeit, Zuverlässigkeit, ...) und die Wirksamkeit verlässlichkeitssichernder Massnahmen (Tests, Problembeseitigung, ...) quantitativ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

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

getaktete Digitalschaltung		E:  A: 
Programm mit EVA-Struktur	<pre>uint8_t up(uint8_t a){ return 23 * a; }</pre>	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) *Was hat es mit der Kennzeichnung »ACR« auf sich?*



E, A Eingabe, Ausgabe.

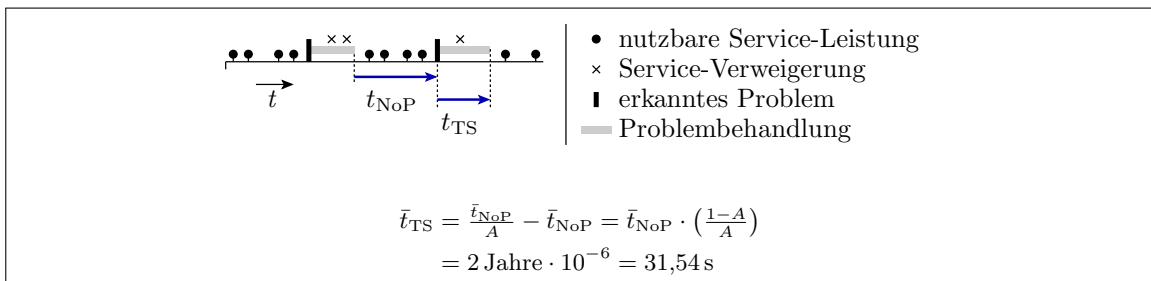
Aufgabe 1.2: Verfügbarkeit, Problembehandlungsdauer

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 $t_{TS1} = 30$ s wieder betriebsbereit und in 1% der Fälle muss zusätzlich die Steuerung getauscht werden. Andere Aspekte der Nichtverfügbarkeit bleiben unbeachtet.

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

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

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



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

$$\bar{t}_{TS} = 99\% \cdot t_{TS1} + 1\% \cdot \bar{t}_{TS2}$$

$$\bar{t}_{TS2} = \frac{\bar{t}_{TS} - 99\% \cdot t_{TS1}}{1\%}$$

$$= 100 \cdot (31,54 \text{ s} - 99\% \cdot 30 \text{ s}) = 164 \text{ s}$$

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.

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

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

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

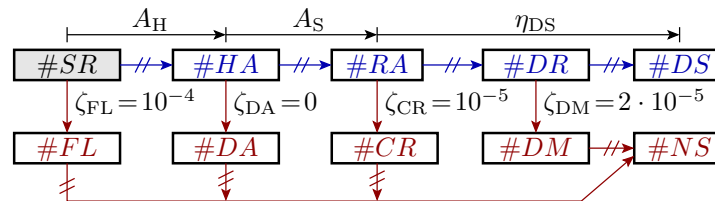
Zehnfacher Wert gegenüber Aufgabenteil a.

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

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

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

Aufgabe 1.3: Verfügbarkeit, CVA-Graph



a) Wie heißen die Zählwerte und Problemraten?

# <i>(evt)</i>	Anzahl der Zählereignisse, $evt \in \{SR, HA, \dots\}$.
<i>SR, HA</i>	Service-Anforderung, Hardware verfügbar.
<i>RA, DR</i>	Service-Anforderung akzeptiert, erbrachtes Ergebnis.
<i>DS, NS</i>	Erbrachte Service-Leistung, keine Service-Leistung.
<i>FL, DA</i>	Nichtverfügbarkeit wegen Hardware-Ausfall bzw. Annahmeverweigerung.
<i>CR, DM</i>	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?

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

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

$$\begin{aligned} A_H &= (1 - \zeta_{FL}) + \zeta_{FL} \cdot 0 = 1 - 10^{-4} \left[\frac{HA}{SR} \right] \\ A_S &= (1 - \zeta_{DA}) + \zeta_{DA} \cdot 0 = 1 \left[\frac{RA}{HA} \right] \\ \eta_{DS} &= \frac{\#DS}{\#RA} \Big|_{ACR} = (1 - \zeta_{CR}) \cdot (1 - \zeta_{DM}) = 1 - 3 \cdot 10^{-5} \left[\frac{DS}{RA} \right] \end{aligned}$$

c) Wie groß ist die Verfügbarkeit insgesamt?

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

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

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

Aufgabe 1.4: Transistorausfall

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

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

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

Vor dem Ausfall:

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

Nach dem Ausfall:

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

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

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

MF-Rate des ausgefallenen Transistors:

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

ζ	Fehlfunktionsrate.
$\left[\frac{MF}{DS} \right]$	Zählwertverhältnis in Fehlfunktionen je erbrachte Service-Leistung.
R	Zuverlässigkeit (Reliability).
$\left[\frac{DS}{MF} \right]$	Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.
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	Festplatte	Stromversorgung	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?*

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

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

b) Welche MF-Rate hat das Gesamtsystem?

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

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

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

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

ζ	Gesamte Fehlfunktionsrate (Total malfunction rate).
$\left[\frac{MF}{DS} \right]$	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 h, Systemauslastung 100%. Sicherheitgefährdungen durch erkennbare Probleme (Ausfälle, Annahmeverweigerung, Absturz und erkannte MF vernachlässigbar.

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

a) Zuverlässigkeit und Sicherheit?

$$(1.10) \quad R_{[MT]} = \frac{\eta_{SU} \cdot \bar{t}_{NDM}}{\bar{t}_S}$$

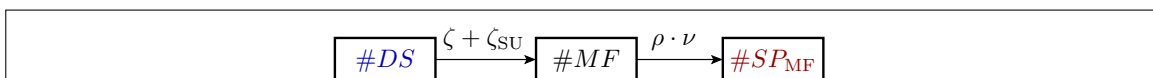
$$(1.23) \quad S = \frac{R_{MT}}{\rho}$$

$$R = \frac{10^3 \text{ h}}{1 \text{ h}} = 10^3 \left[\frac{DS}{MF} \right]$$

$$S = \frac{R}{\rho} = 10^5 \left[\frac{DS}{SP} \right]$$

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

$$(1.24) \quad S_{SU} = \frac{1}{(\zeta + \zeta_{SU}) \cdot \rho \cdot \nu}$$



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

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

$\bar{t}_{\text{NDM}}, \bar{t}_S$	Mittlere Service-Zeit je nicht erkannte Fehlfunktion, mittlere Service-Dauer.
η_{SU}	Systemauslastungsrate.
$R_{[\text{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
ζ	Fehlfunktionsrate.
R	Zuverlässigkeit (Reliability).
$\left[\frac{\text{DS}}{\text{MF}}\right]$	Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.
$\left[\frac{\text{MF}}{\text{DS}}\right]$	Zählwertverhältnis in Fehlfunktionen je erbrachte Service-Leistung.
$\left[\frac{\text{DS}}{\text{SP}}\right]$	Verhältnis in erbrachten Service-Leistungen je sicherheitsgefährdende Fehlfunktion.

1.2 MF-Beseitigung

Aufgabe 1.7: Kenngrößen Überwachung

Von 10^5 erbrachten Service-Leistungen sind 10^3 Fehlfunktionen aufgetreten, von denen die Kontrolle 600 erkannt hat. Von den korrekten 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?*

$$(1.8) \quad R_{[\text{MT}]} = \left. \frac{\#DS}{\#NDM} \right|_{\text{ACR}}$$

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:

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

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

$$(1.25) \quad MC = \left. \frac{\#DM}{\#MF} \right|_{\text{ACR}}$$

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

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

$$(1.26) \quad \zeta_{\text{PM}} = \left. \frac{\#PM}{\#CS} \right|_{\text{ACR}}$$

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

$\#DS$	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.
$\left[\frac{\text{DS}}{\text{MF}}\right]$	Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.
R	Zuverlässigkeit (Reliability).
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.
MC, ζ_{PM}	Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.

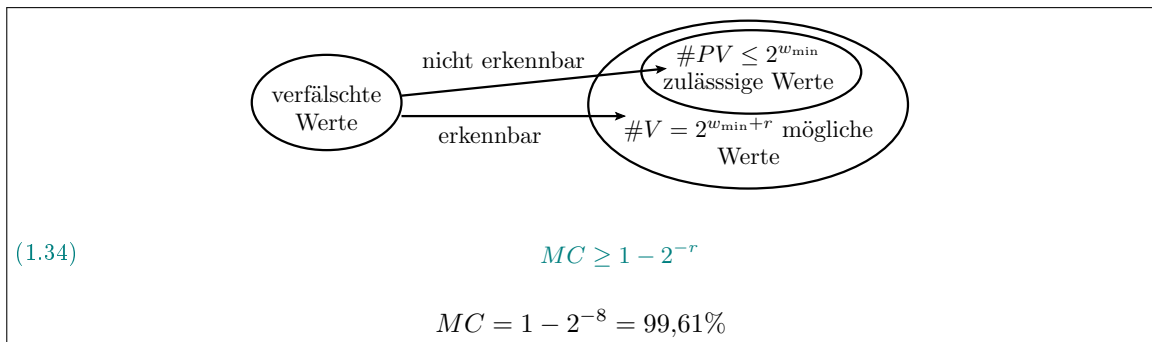
- [MF] Zählwert in Fehlfunktionen.
- $\left[\frac{PM}{DS}\right]$ Zählwertverhältnis in Phantom-Fehlfunktionen je erbrachte Service-Leistung.

Aufgabe 1.8: Übertragung mit Wiederholung nach MF

Datenübertragung mit Fehlfunktionsrate $10^{-6} \left[\frac{MF}{DS}\right]$ 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-Ursache zu 100% Störungen. Ausfälle sollen nicht betrachtet werden.

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

a) *Fehlfunktionsüberdeckung?*



b) *Zuverlässigkeit ohne und mit Fehlfunktionsbehandlung?*

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

$$(1.35) \quad R_{MT} = 2^r \cdot R$$

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

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

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

$$(1.27) \quad \eta_{DS} = (1 - \zeta_{CR}) \cdot (1 - \zeta_{SMF}) \quad \text{mit } \zeta_{SMF} = \zeta_{PM} + \zeta \cdot MC - \zeta \cdot \zeta_{PM}$$

$$(1.40) \quad \eta_{DS.SR} = \eta_{DS} \cdot (1 + (1 - \eta_{DS}) \cdot \eta_{Div})$$

Erbringungsrate ohne Wiederholanforderung:

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

Erbringungsrate bei max. einer Wiederholanforderung:

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

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

$$(1.35) \quad R_{MT} = 2^r \cdot R$$

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

Mindestens $r = 14$ redundante Bits.

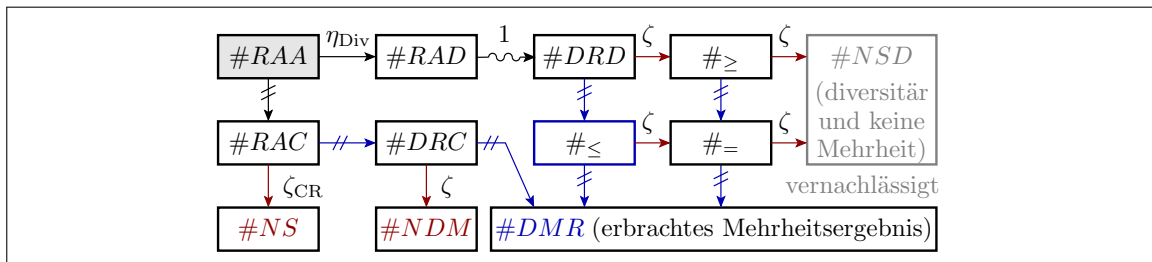
ζ_{CR}, ζ	Absturzrate, Fehlfunktionsrate.
r	Anzahl der redundanten Bits.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
ζ_{PM}	Phantom-Fehlfunktionsrate.
$\#VP, \#PP$	Anzahl der gültigen Bitmuster, Anzahl der darstellbaren Bitmuster.
MC, r	Fehlfunktionsabdeckung, Anzahl der redundanten Bits.
w_{min}	Erforderliche Bitanzahl zu Unterscheidung aller zulässigen Werte.
$R_{[MT]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
$\left[\frac{DS}{MF}\right]$	Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.
η_{DS}	Rate der erbrachten Service-Leistungen.
$\eta_{DS.SR}$	Erbringungsrate bei max. einer Wiederholung nach Nichterbringung.

Aufgabe 1.9: Mehheitsentscheid

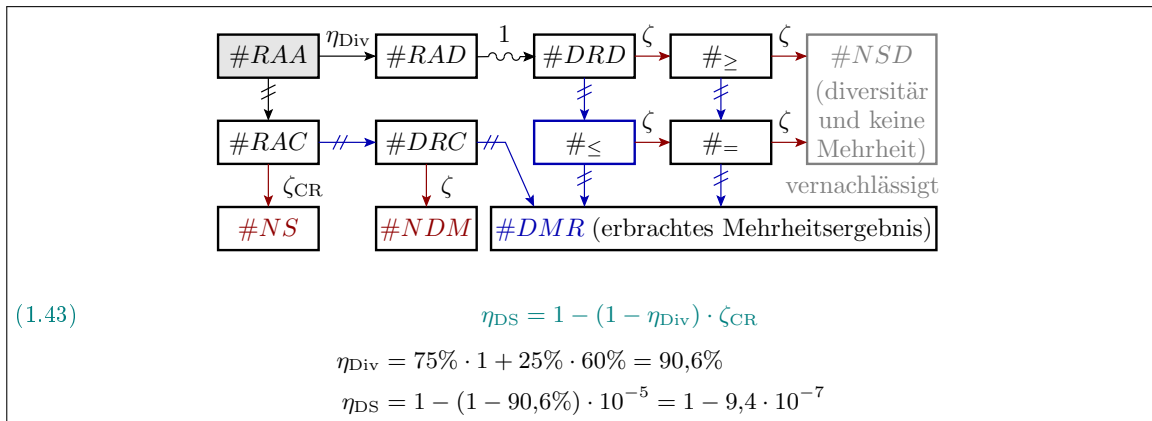
Alle drei Einzelsysteme haben die übereinstimmende Absturzrate $\zeta_{CR} = 10^{-5}$ und MF-Raten $\zeta = 10^{-4}$. 75% der Fehlfunktionen entstehen durch Störungen und sind diversitär. Die restlich 25% der Fehlfunktionen werden durch Fehler verursacht und sind nur zu 60% diversitär. Nicht erbrachte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

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

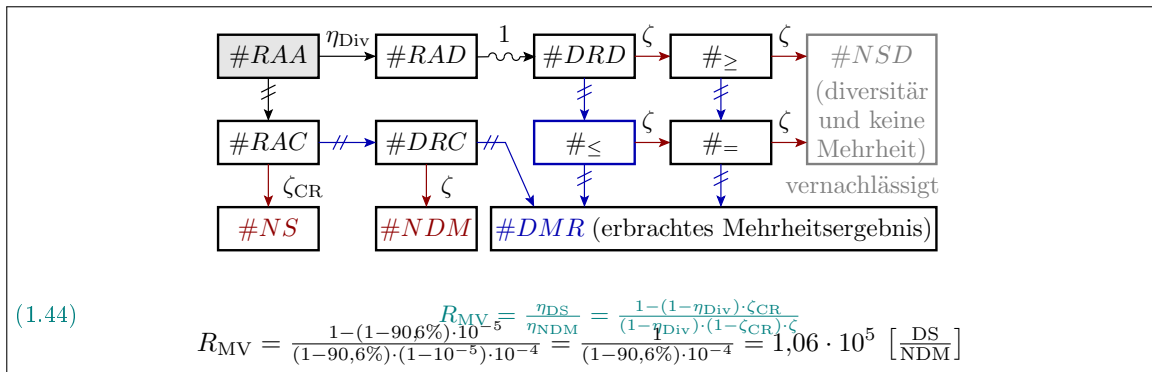
a) Wiederholung des CVA-Graphen aus der Vorlesung?



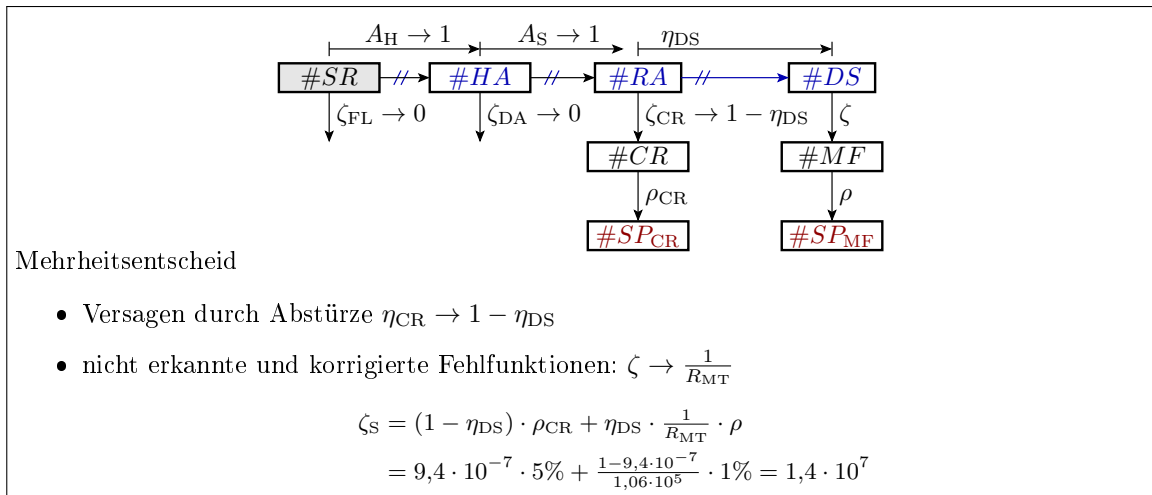
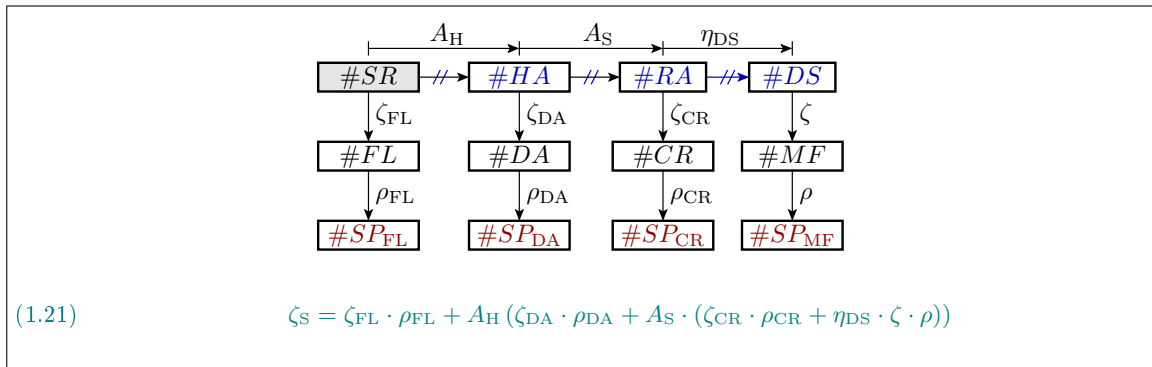
b) Erbringungsrate?



c) Zuverlässigkeit?



d) Sicherheit?



- η_{DS} Rate der erbrachten Service-Leistungen.
- η_{Div} Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
- ζ_{CR}, ζ Absturzrate, Fehlfunktionsrate.
- ρ Anteil sicherheitskritischer Fehlfunktionen an den nicht erkannten Fehlfunktionen.
- ρ, ν Anteil sicherheitskritischer Probleme an den nicht diversitären Abstürzen.
- 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.
- $\#_{=}$
- η_{DS} Rate der erbrachten Service-Leistungen.
- R_{MV} Zuverlässigkeit Gesamtsystem mit Mehrheitsentscheid.
- SR, FL Service-Anforderung, Hardware ausgefallen.
- HA, DA Hardware verfügbar, Annahme verweigert.

RA, CR Anforderung akzeptiert, Absturz.
DS, MF Erbrachte Leistung, Fehlfunktion.

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 $10^6 \left[\frac{DS}{SP} \right]$ zu erhöhen, soll das System um eine MF-Behandlung erweitert werden, die es bei Erkennen einer Fehlfunktion in einen sicheren Zustand überführt.

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

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

$$(1.10) \quad R_{[MT]} = \frac{\eta_{SU} \cdot \bar{t}_{NDM}}{\bar{t}_S}$$

Sicherheitskritische Probleme nur durch nicht erkannte Fehlfunktionen:

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

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

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

- 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.

- 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:

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

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

$$2778 \text{ h}/99\% = 2800 \text{ h}$$

\bar{t}_{NDM}, \bar{t}_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.
 $\left[\frac{DS}{SP} \right]$ Verhältnis in erbrachten Service-Leistungen je sicherheitsgefährdende Fehlfunktion.
 R Zuverlässigkeit (Reliability).
 MC Fehlfunktionsabdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
 XXXX