Test und Verlässlichkeit 1: Threads & Means

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_F1.pdf)
7. November 2023

Organisation

Web-Seite Vorlesung: http://techwww.in.tu-clausthal.de/TestVerl

- Foliensätze, Handouts, Hausübungen, Videoaufzeichnungen
- Abgabe der Hausübungen per Mail an ha-tv@in.tu-clausthal.de als pdf. Abgabetermine siehe Web-Seite.
- Hausübungen werden bewertet und zurückgegeben. Zusätzliche Veröffentlichung der Punkteanzahl auf der Webseite.
- Prüfungszulassung 50% der erzielbaren Hausübungspunkte. Für größere Punkteanzahl bis zu 2 Bonuspunkten für die Prüfung.
- Fragen und Kommentare an: gkemnitz@in.tu-clausthal.de

Prüfung

- Prüfung ab 10 Teilnehmer schriftlich.
- Erlaubte Hilfsmittel Prüfungsklausur: Eigene Ausarbeitung incl. Handouts mit eigenen Kommentaren und die eigenen Hausübungen, Taschenrechner.
- Erlaubte Hilfsmittel mündlichen Prüfung: Ein A4-Blatt (einseitig) mit eigenen Ausarbeitungen.

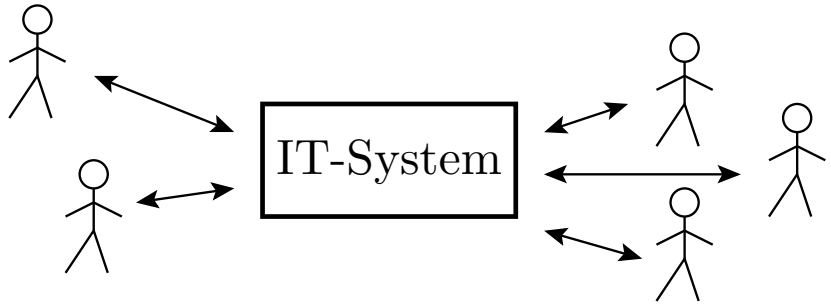
Alle weiteren Infos siehe Web-Seite.

Inhalt Foliensatz 1

Vorlesung	1	2	3	4
ca. ab Folie	2	52	133	201

Einführung

Vertrauen und Verlässlichkeit



IT-Systeme automatisierten intellektuelle Aufgaben:

- betriebliche Abläufe,
- Steuerung von Prozessen und Maschinen,
- Entwurfsaufgaben, ...

Einsatzvoraussetzung ist Vertrauen, dass

- das System, wenn es gebraucht wird, funktioniert,
- seine Service-Leistungen korrekt und pünktlich ausführt,
- keine unkalkulierbaren Schäden und Kosten verursacht.

Das Vertrauen in ein IT-System setzt Verlässlichkeit voraus.

Verlässlichkeit

Umgangssprachlich beschreibt Verlässlichkeit (von Personen, Rechnern, ...), dass man ihnen trauen kann. Dabei treffen unterschiedliche Aspekte zusammen (Wünsche, Erwartungen, ...).

Subjektive Einflussfaktoren auf die Wahrnehmung der Verlässlichkeit:

- Lebenserfahrungen insbesondere aus der Kindheit,
- Katastrophen oder langsam Veränderungen,
- Persönlichkeitstyp (Optimist, Pessimist, konservativ, Spieler), ...

Objektivierung durch Zählen positiver und negativer Erfahrungen und deskriptive Attribute:

- wofür verlässlich:
  - Dozent verlässlich, dass pünktlich,
  - Student verlässlich, dass HA abgegeben werden, ...
- warum verlässlich:
  - Arzt verlässlich, weil abgeschlossenes Medizinstudium,
  - Auto verlässlich, weil technische Zulassung und gültiger TÜV.

Wichtig sind bestandene Tests und Kontrollen für die zugesicherten Leistungen und Fähigkeiten, aber auch die Fehlerkultur ...

Fehlerkultur

Art und Weise, wie Gesellschaften, Kulturen und soziale Systeme mit Fehlern und deren Folgen umgehen.

Negative Sichtweise: Fehler verstecken, wegreden, ...

Positive Sichtweisen: Aus Fehlern lernen, Fehler beseitigen. ...

- Pädagogik: positives Klima für Lernen aus Fehlern.
- Qualitätsmanagement: Minimierung der Fehlerkosten.
- Innovationsmanagement: Streben nach Neuerungen. Fehler als Chance / produktives Potential.

Die Vorlesung unterstellt eine idealisierte Fehlerkultur:

- Alle erkannten Probleme werden beseitigt.
- Beseitigungserfolg wird durch Testwiederholung kontrollieren.

Für menschliche Interaktionen mit Freunden, Vorgesetzten und Partnern und auch für Kostenoptimierungen für Entwurf, Fertigung, ... sind meist weniger radikale (tolerantere) Fehlerkulturen zielführender.

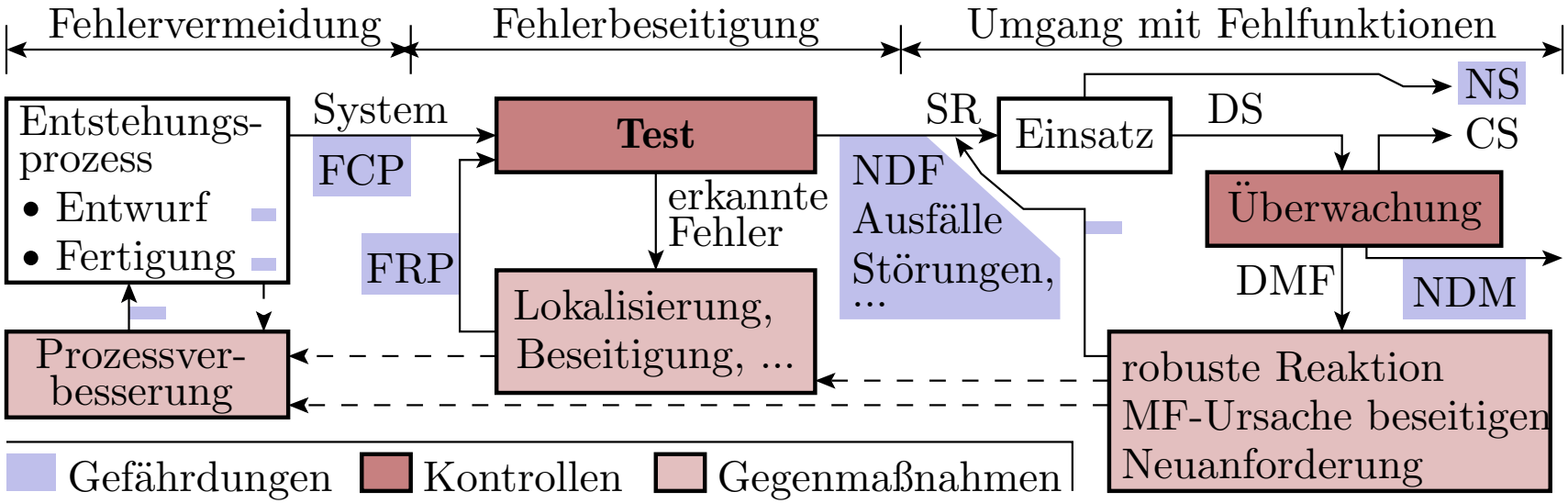
Gefährdungen & Gefährdungsabwendung

Verlässlichkeit wird durch Gefährdungen und Gefährdungsabwendung auf drei Ebenen beschrieben:

- Fehlfunktionen (malfunction, MF) und nicht erbringbare Service-Leistungen (no service, NS) im Betrieb, insbesondere
  - nicht erkannte Fehlfunktionen (not detected malfunction, NDM) und
  - davon wiederum insbesondere sicherheitsgefährdende Fehlfunktionen (hazzarous malfunction HM).
- Ursachen für die Entstehung von Fehlfunktionen:
  - Fehler,
  - Störungen und
  - Ausfälle
- Entstehungsursachen für Fehler, Störungs- und Ausfallanfälligkeit.
  - Schwachstellen,
  - Fehler (faults),
  - Störungen (distortions) und
  - Ausfälle (failurs)

  in den Entstehungs- und Reparaturprozessen.

1. Einführung



Gegenmaßnahmen zur Gefährdungsabwendung (Means) sind Iterationen aus Kontrollen, Problembeseitigungsversuchen und Wiederholung der Kontrollen:

1. Fehlervermeidung durch Verbesserung der Entstehungsprozesse.
2. Test und Fehlerbeseitigung.
3. Überwachung und geeignete Reaktion auf erkannte MF.

FCP	Fehler, die während Entstehungsprozess entstanden sind.
RPF	Fehler, die bei der Fehlerbeseitigung entstanden sind.
NDF	Nicht erkannte Fehler.
SR	Service-Anforderung.
DS	Erbrachte Service-Leistung.

Was kostet Verlässlichkeit?

Der Preis für Verlässlichkeit sind die Gesamtkosten aller Maßnahmen für die Gefährdungsabwendung auf allen drei Ebenen:

- Kontrollen und geeignete Reaktion auf erkannte MF: Kann mehr als 50% der Gesamtfunktionalität erfordern, plus Kosten für Reparatur, Schadensbegrenzung, ...
- Test, Fehlersuche und Fehlerbeseitigung: Für HW und SW typisch mehr als 50% des Gesamtentwurfsaufwands.
- Fehlervermeidung durch Verbesserung der Entstehungsprozesse: Kosten für die Qualitätssicherung und die Weiterentwicklung und Verbesserung der Entstehungsprozesse.

Verlässlichkeit ist selbst für IT-Systemen ohne erhöhte Anforderungen an die Verlässlichkeit eine teuere Produkteigenschaft. Bei erhöhten Anforderungen betragen die anteiligen Produktkosten für die Sicherung der Verlässlichkeit weit über 50%.

Der Preis fehlender Verlässlichkeit

Wenn Verlässlichkeit teuer, warum kein Verzicht? – Schadenskosten:

- Datenverlust, Hintertüren für den Datenmissbrauch[1],
- Unfälle, Selbstzerstörung, Produktionsausfälle, ...

Am 3. Juni 1980 meldete ein Rechner des nordamerikanischen Luftverteidigungszentrums den Anflug sowjetischer Nuklearraketen. Sofort wurden Vergeltungsmaßnahmen vorbereitet. Eine Überprüfung der Daten von Radarstationen und Satelliten konnte den Angriff nicht bestätigen[2] *...*

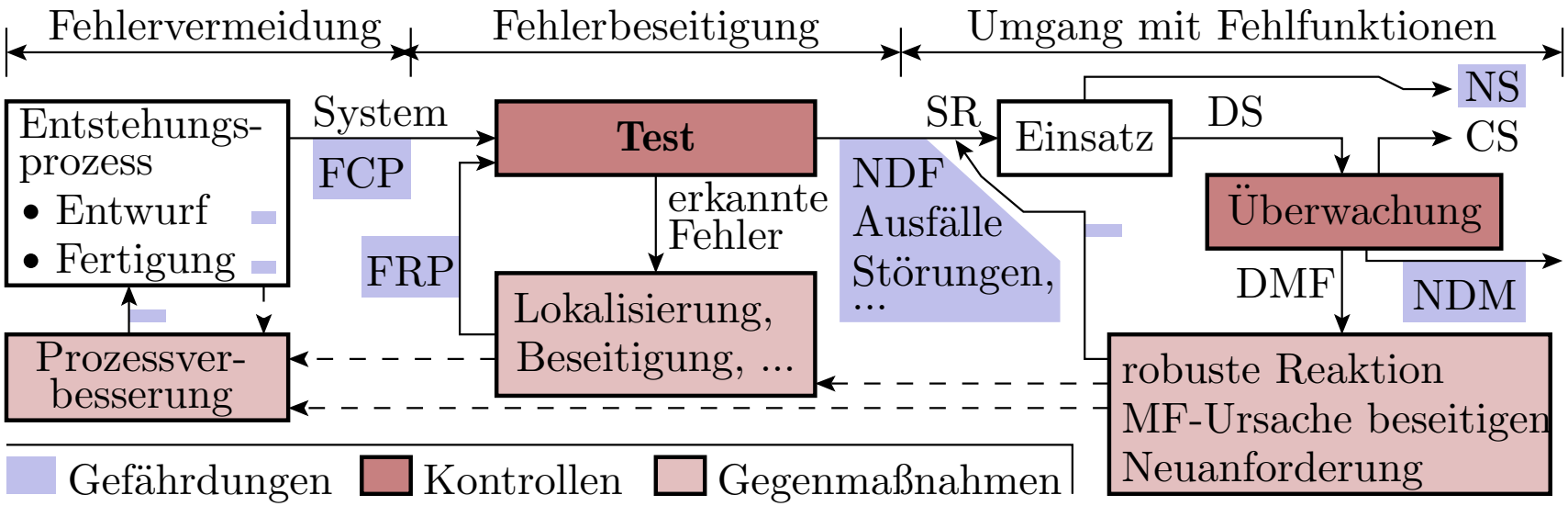
Ursache des beinahe atomaren Schlagabtauschs: defekter Schaltkreis.

Unzuverlässige IT-Systeme können nicht eingesetzt werden.

[1] https://www.faz.net/aktuell/wirtschaft/diginomics/43-milliarden-euro-schaden-durch-hackerangriffe-15786660.html

[2] Hartmann, J., Analyse und Verbesserung der probabilistischen Testbar- keit kombinatorischer Schaltungen, Diss. Universität des Saarlandes, 1992

Warum heißt Vorlesung »Test & Verlässlichkeit«



Verlässlichkeit wird durch Iterationen aus Kontrollen, Beseitigung erkannter Gefährdungen und Erfolgskontrollen gesichert. Mit der unterstellten Fehlerkultur *»Beseitigung alle erkannten Gefährdungen (MF, Fehler, ...)«* hängt die Verlässlichkeit der Systeme im Einsatz hauptsächlich von der Güte der Tests und Kontrollen auf den drei Ebenen ab.

MF Fehlfunktion.
DS Erbrachte Service-Leistung.

Lernziel und Inhalt

Modellierung der Gefährdungen und der Maßnahmen zu Gefährdungsabwendung mit Schwerpunkt auf Tests und Kontrollen und wie sich deren Güte auf die Verlässlichkeit eingesetzter IT-Systeme auswirkt.

Entstehung und Abwendung von Gefährdungen sowie Einfluss nicht abgewendeter Gefährdungen auf die Verlässlichkeit sind stochastischer Natur. Hierzu themenspezifische Einführung in die Stochastik.

Foliensätze:

1. Threads & Means: Verlässlichkeit, Umgang mit Fehlfunktionen, Fehlerbeseitigung, Fehlervermeidung.
2. Wahrscheinlichkeiten: Fehlerbäume, Markov-Ketten, ...
3. Verteilungen insbesondere für Zählwerte, Bereichsschätzungen, ...
4. Test, Überwachung, Fehlertoleranz
5. HW: Fehlermodellierung, Testsuche, Selbsttest.
6. SW: Einfluss der Programmiersprache, Vorgehen beim Entwurf & Verlässlichkeit, Testauswahl.

Verlässlichkeit

Beschreibung der Verlässlichkeit

Die Verlässlichkeit von IT-Systemen wird durch die Entstehung und Abwendung von Gefährdungen und deren Wahrscheinlichkeiten auf drei Ebenen beschrieben:

	entstehende Gefährdungen	Gefährdungsabwendung
Fehlervermeidung	Fehler	Minderung Entstehungsrate
Test und Fehlerbeseitigung	Fehler durch Reparatur	Beseitigung vorhandener Fehler
Betrieb + Kontrolle + MF-Behandlung	MF und Schaden durch MF	Schadensvermeidung und Beseitigung von MF

Quantitative Abschätzungen von Verlässlichkeitsaspekten benötigen:

- Zählwerte für entstandene, vermiedene, ..., nicht erkannte MF,
- dasselbe für Fehler und deren Entstehungsursachen.

Deshalb müssen wir IT-Systeme so modellieren, dass erbrachte Leistungen, Fehlfunktionen, Fehler, ... zählbar sind.

Das Service-Modell

Das Service-Model

Ein »Service« oder »Service-Leister« ist ein System, das auf

- SR: Service-Anforderungen (service request)

aus Eingaben Ausgaben erzeugt. Klassifizierung Service-Leistungen:

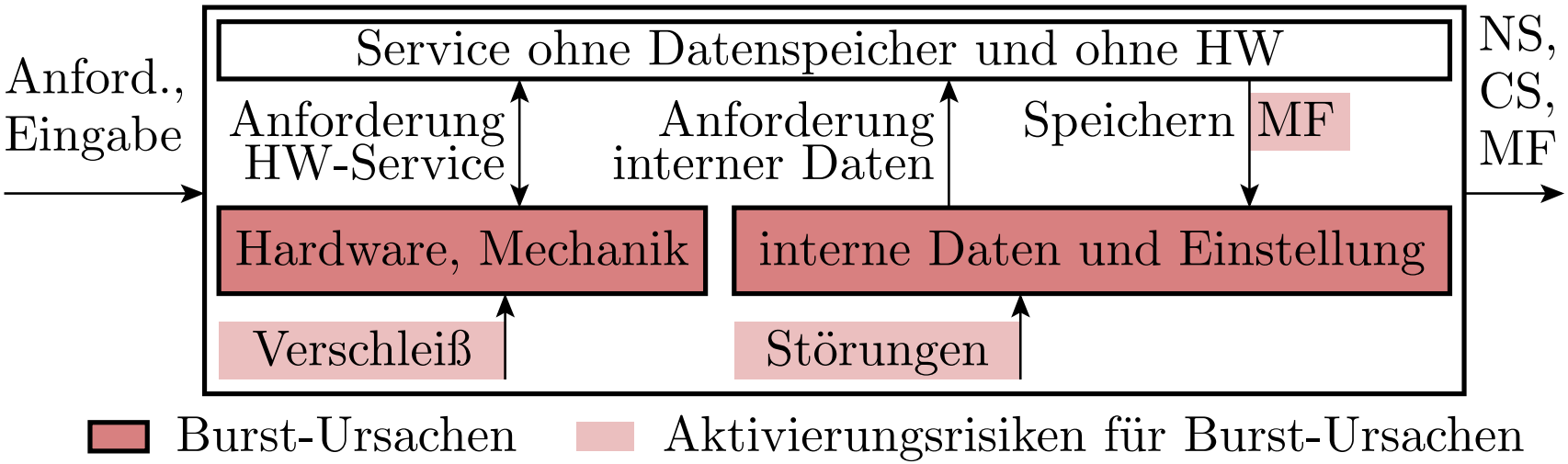
- NS: nicht erbracht (no service)
- DS: erbracht (delivered service)
  - CS: korrektes Service-Ergebnis (correct service)
  - MF: Fehlfunktion (malfunction).

Schätzbare Kennwerte zu Beschreibung der Verlässlichkeit:

- Verfügbarkeit: Wahrscheinlichkeit, dass das System in der Lage ist, aus Anforderungen aus Eingaben Ergebnisse zu produzieren,
- Zuverlässigkeit*: zu erwartende Anzahl DS je MF und
- Sicherheit*: zu erwartende Anzahl DS je HM.

HM Sicherheitsgefährdende Fehlfunktion.
* Zweckmäßige, in der Fachwelt jedoch noch unübliche Definitionen.

Fehlfunktions-Burst



HW-Ausfälle und / oder Verfälschung gespeicherter Daten beeinträchtigen nicht nur eine, sondern alle folgenden Service-Leistungen:

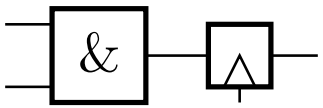
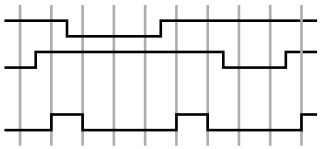
- keine weitere Service-Ausführung,
- erkennbar erhöhte MF-Rate oder
- nicht erkennbar erhöhte MF-Rate

bis defekte HW repariert und Datenverfälschungen behoben sind.

Erkannte MF-Bursts zählen nur als eine MF und DS und das System gilt als nicht verfügbar, solange die Ursache nicht beseitigt ist.

Anwendungsbereiche des Service-Modells

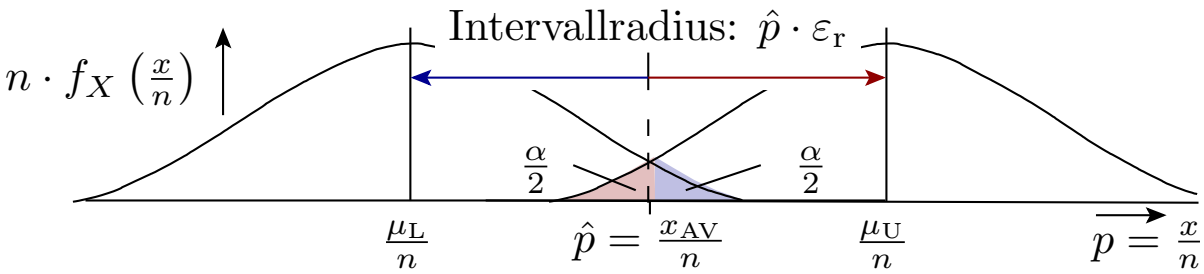
Das Service-Modell ist auf unterschiedliche Abstaktionsebenen für IT-Systeme, menschliche Dienstleistungen, technische Steuerungen, Fertigungs- und, Entwurfsprozesse, ... anwendbar.

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	

E, A Eingabe, Ausgabe.

Geeignete Zählwertgrößen

Geeignete Zählwertgrößen (ACR)

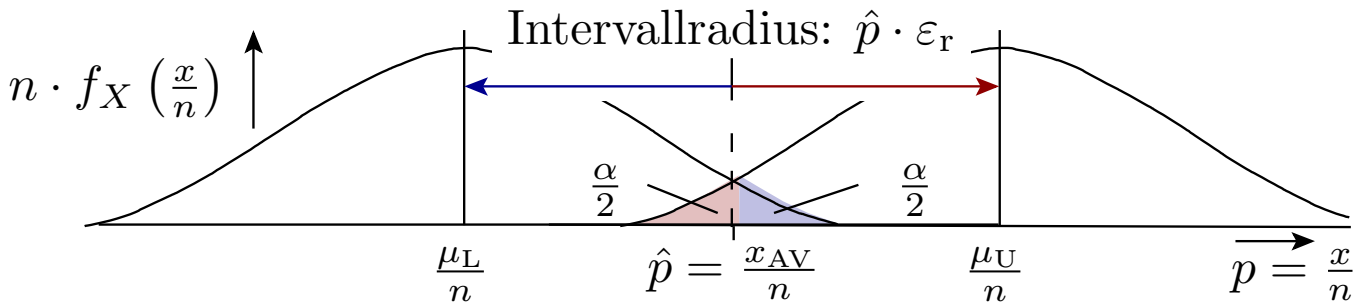


Viele der nachfolgend eingeführten Kenngrößen werden als Zählwerte und deren Verhältnisse definiert:

- Fehlfunktionen (aufgetretene, vermiedene, ...),
- Fehler (vorhandenen, modellierte, nachweisbare, vermiedene, ...),
- Zuverlässigkeit als Verhältnis der Anzahl erbrachten Service-Leistungen zur Anzahl der Fehlfunktion, ...

Experimentell bestimmte Ist-Zählwerte erlauben nur mit Irrtumswahrscheinlichkeiten behaftete Bereichsaussagen über Erwartungswerte und Eintrittswahrscheinlichkeiten bei Versuchswiederholung.

$f_X(x)$	Dichtefunktion der Zufallsvariablen X mit den möglichen Zählwerten x.
x_AV	Experimentell bestimmter Ist-Zählwert, Schätzwert für den Erwartungswert.
n	Anzahl der Zählversuche, maximaler Zählwert.
ε_p	Intervallradius der geschätzten Eintrittswahrscheinlichkeit für Zählereignisse.



Vertrauenswürdige Schätzungen erfordern geeignete Zählwertgrößen (ACR). Einige Beispielzahlen vorab mit $\alpha = 4{,}5\%$ (siehe Folie 3.89):

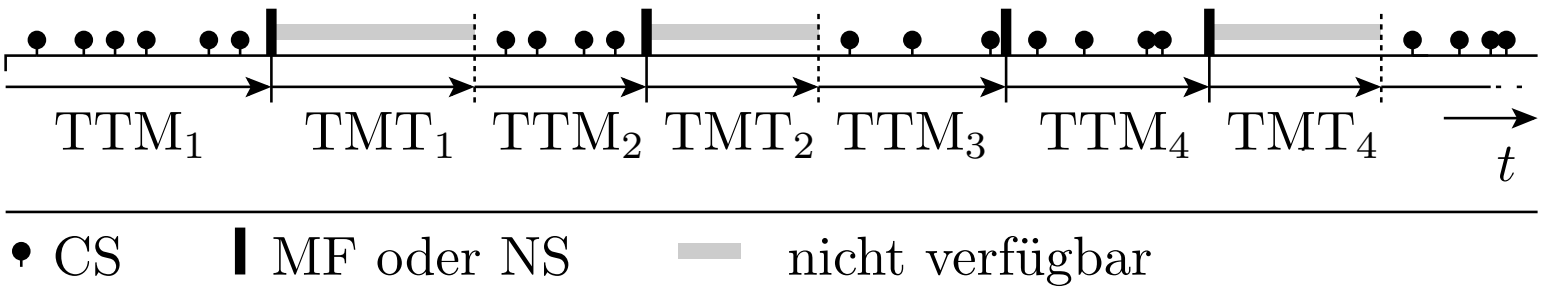
ε_r	$p = 10\%$		$p = 50\%$		$\varepsilon_{\tilde{\mathrm{r}}}$	$p = 90\%$	
	$x_{\mathrm{AV.min}}$	n_min	$x_{\mathrm{AV.min}}$	n_min		$x_{\mathrm{AV.\,max}}$	n_min
20%	90	900	50	100	20%	810	900
2%	9.000	90.000	5.000	50.000	2%	81.000	90.000

Kennzeichnung zählwertbasierter Abschätzungen mit $\ldots|_\mathrm{ACR}$.

x_AV	Experimentell bestimmter Ist-Zählwert, Schätzwert für den Erwartungswert.
n	Anzahl der Zählversuche, maximaler Zählwert.
$\hat{p}$	Schätzwert der Eintrittswahrscheinlichkeit.
$\mu_\mathrm{L}, \mu_\mathrm{U}$	Untere und obere Schranke des wahrscheinlichen Bereichs des Erwartungswerts.
α	Irrtumswahrscheinlichkeit Werte außerhalb des geschätzten Bereichs.
$\varepsilon_\mathrm{r}, \varepsilon_{\tilde{\mathrm{r}}}$	Intervallradius realtiv zum erwarteten Eintritts- bzw. Nichteintritts-Zählwert.

Verfügbarkeit

Fehlfunktionen und Verfügbarkeit



- Mittlere Zeit zwischen MF (**m**ean **t**ime **b**etween **m**alfunctions):

$$MTBM = \left(\frac{1}{\#MF} \cdot \sum_{i=1}^{\#MF} TTM_i \right)_{\text{ACR}}$$

- Mittlere Zeit der MF-Behandlung bis zur Wiederherstellung der Betriebsbereitschaft:

$$MTMT = \left(\frac{1}{\#MF} \cdot \sum_{i=1}^{\#MF} TMT_i \right)_{\text{ACR}}$$

$\#MF$	Anzahl der Fehlfunktionen (Number of malfunctions).
TTM_i	Zeit bis zur Fehlfunktion i.
TMT_i	Dauer der Fehlfunktionsbehandlung für Fehlfunktion i.

Verfügbarkeit und PFD

Die Wahrscheinlichkeit der Verfügbarkeit, kurz Verfügbarkeit (**a**vailability) ist der Zeitanteil, in dem das System nutzbar, d.h. nicht mit einer MF-Behandlung beschäftigt ist. Zur MF-Behandlung gehören:

- Schadensvermeidung (Datenrettung, sicherer Zustand, ...),
- Protokollierung (Kontrolle Verlässlichkeit, Fehlersuche, ...),
- Ursachenbeseitigung (Reparatur, Neuinitialisierung, ...),
- optional Korrektur der MF (Neuberechnung):

$$A = \frac{MTBM}{MTBM + MTMT} \tag{1}$$

$$A = 1 - PFD \tag{2}$$

MF	Fehlfunktion.
A	Verfügbarkeit (Availability).
$MTBM$	Mittlere Nutzungsdauer zwischen Fehlfunktion (Mean service life between malfunctions).
$MTMT$	Mittlere Dauer der Fehlfunktionsbehandlung.
PFD	Wahrscheinlichkeit der Nichtverfügbarkeit bei Anforderung.

Teilverfügbarkeiten

- Lieferverfügbarkeit, Rate der erbringbaren Service-Leistungen:

$$A_{\mathrm{DS}} = \eta_{\mathrm{DS}} \tag{3}$$

  Die Rate der erbringbaren Service-Leistungen nimmt typ. in einem Lernprozess des Nutzers mit der Nutzungsdauer zu (siehe Folie 1.74 *Fehlerumgehung*).
- MT-Verfügbarkeit: Zeitanteil, den nicht ausgefallene Systeme nicht mit interner MT (malfunction treatment) beschäftigt sind. Für beispielhafte MT mit Basisbehandlungdauer MTB und Wiederholdauer je Beseitigungsversuch gleich der mittleren Service-Dauer:

$$A_{\mathrm{MT}} = \frac{MTBT}{MTBT + (MTB + \mu_{\mathrm{CM}} \cdot MTS)} \tag{4}$$

A_{DS}	Lieferverfügbarkeit.
η_{DS}	Anteil der erbringbaren Service-Leistungen.
A_{MT}	MT-Verfügbarkeit, Zeitanteil, den das System nicht mit MT beschäftigt ist.
$MTBT$	Mittlere Zeit zwischen MF-Behandlungen ohne Reparatur.
MTB	Mittlere Zeit für die grundlegende Fehlfunktionsbehandlung.
μ_{CM}	Mittlere Anzahl der Neuberechnungen (Korrekturversuche) je MF.
MTS	Mittlere Service-Dauer (Mean time to service).

- Ausfall-Verfügbarkeit: Zeitanteil, den das System nicht durch Hardware-Ausfälle (failure) nicht nutzbar ist:

$$A_{\mathrm{F}} = \frac{MTBF}{MTBF + MTTR} \tag{5}$$

- PWA-Verfügbarkeit: Zeitanteil, den Nutzer nicht mit der Umgehung von Benutzbarkeitsproblemen (Bedienprobleme, Inkompatipilitäten, ...) beschäftigt sind.

  Sowohl private als auch berufliche IT-Nutzer verbringen seit Jahrzehnten typ. 20% ihrer Zeit am Computer mit Problemumgehung (problem workarounds). Das entspricht $A_{\mathrm{PWA}} \approx 80\%$ [Herz20].

A_{F}	F-Verfügbarkeit, Zeitanteil, den das System ausfallbedingt unbenutzbar ist.
$MTBF$	Mittlere Zeit zwischen Fehlfunktionen (Mean time between failures).
$MTTR$	Mittlere Reparaturzeit (Mean time to repair).
A_{PWA}	PWA-Verfügbarkeit, Zeitanteil, in den Nutzer nicht mit Problemumgehungen beschäftigt.
[Herz20]	Morten Hertzum: Usability Testing. Springer International Publishing (Verlag) 978-3-031-01099-6 (ISBN) , 2020.

Meist werden die vier Teilverfügbarkeiten getrennt betrachtet. Sie können aber auch zu einer Gesamtverfügbarkeit zusammengefasst werden.

Bei geringen PFD -Werten oder gegenseitigem Ausschuss addieren sich die PFD-Werte der Teilverfügbarkeiten (siehe Abschn. 2.1.2 *Verkettete Ereignisse*):

$$1 - A = \sum_{i=1}^{\#A_i} (1 - A_i)$$

$$A = \left(\sum_{i=1}^{\#A_i} A_i \right) - \#A_i + 1 = A_{\mathrm{DS}} + A_{\mathrm{MT}} + A_{\mathrm{F}} + A_{\mathrm{PWA}} - 3 \qquad (6)$$

A	Gesamtverfügbarkeit (Overall availability).
A_{DS}	Lieferverfügbarkeit.
A_{MT}	MT-Verfügbarkeit, Zeitanteil, den das System nicht mit MT beschäftigt ist.
A_{F}	F-Verfügbarkeit, Zeitanteil, den das System ausfallbedingt unbenutzbar ist.
A_{PWA}	PWA-Verfügbarkeit, Zeitanteil, in den Nutzer nicht mit Problemumgehungen beschäftigt.

Hochverfügbare Systeme

»Hochverfügbarkeit« betrachtet meist nur Ausfälle und hängt erheblich von der mittleren Reparaturdauer ab:

$$A_{\mathrm{F}} = \frac{MTBF}{MTBF+MTTR} \tag{1.5}$$

Verfügbarkeit A_{F}	PFD_{F}	zul. mittlere Reparaturzeit $MTTR$	
		pro Monat	pro Jahr
99%	1%	7,2 h	87,6 h
99,9%	0,1%	43 min	8,8 h
99,99%	0,01%	4,3 min	53 min

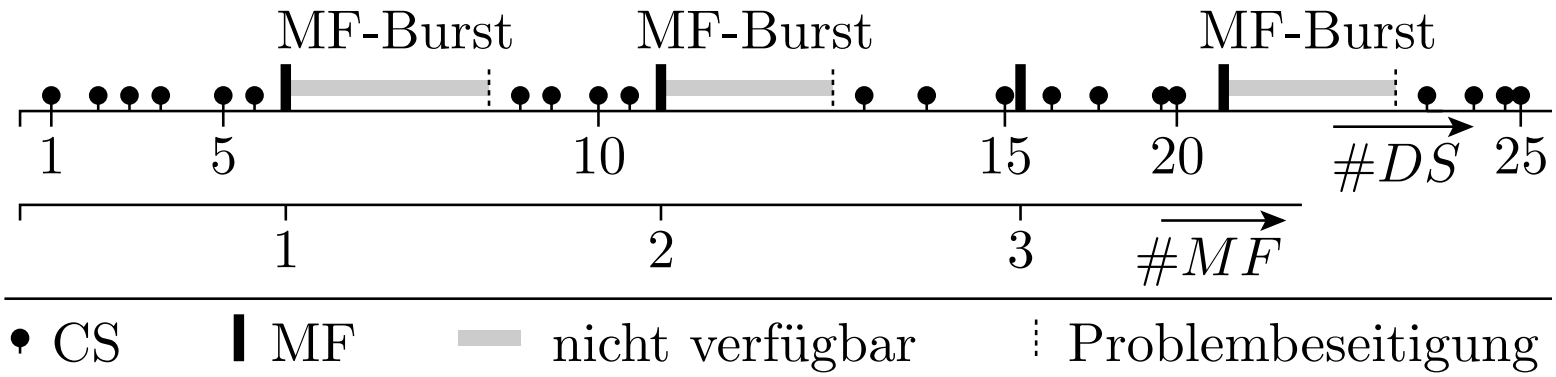
$A_{\mathrm{F}} \approx 99\%$ ist normal. Hohe Verfügbarkeiten ab 99,9% verlangen spezielle Maßnahmen (siehe Abschn. 4.3 *Fehlertoleranz*):

- unterbrechungsfreie Stromversorgung,
- RAID (**R**edundant **A**rray of **I**ndependent **D**isks),
- gespiegelte Server, vorbeugende Wartung, ...

$MTTR$ Mittlere Reparaturzeit (Mean time to repair).
$MTBF$ Mittlere Zeit zwischen Fehlfunktionen (Mean time between failures).

Zuverlässigkeit

Fehlfunktionsrate und Zuverlässigkeit



Die Fehlfunktionsrate sei der Anteil der Fehlfunktionen an den erbrachten Service-Leistungen:

$$\zeta = \frac{\#MF}{\#DS}\Big|_{\mathrm{ACR}} \tag{7}$$

und das Verhältnis aus mittlerer Service-Dauer und mittlerer Zeit bis zu nächsten MF:

$$\zeta = \frac{MTS}{MTTM} \tag{8}$$

Service-Anforderungen innerhalb einer MF-Burst und Reparaturzeiten zählen nicht mit*.

CS, MF Korrekte Service-Leistung, Fehlfunktion.

* auch zur Minderung der Abhängigkeiten zwischen den Zählwerten (siehe 3.2.7).

Zuverlässigkeit

Zuverlässigkeit sei die Anzahl der erbrachten Service-Leistungen je Fehlfunktion bzw. der Kehrwert der MF-Rate:

$$R = \left.\frac{\#DS}{\#MF}\right|_{\mathrm{ACR}} \tag{9}$$

$$= \frac{MTBM}{MTS} \tag{10}$$

$$= 1/\zeta \tag{11}$$

R	Zuverlässigkeit (Reliability).
$\#DS$	Anzahl der erbrachten Service-Leistungen (Number of delivered services).
$\#MF$	Anzahl der Fehlfunktionen (Number of malfunctions).
$MTBM$	Mittlere Nutzungsdauer zwischen Fehlfunktion (Mean service life between malfunctions).
MTS	Mittlere Service-Dauer (Mean time to service).
ζ	Fehlfunktionsrate.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

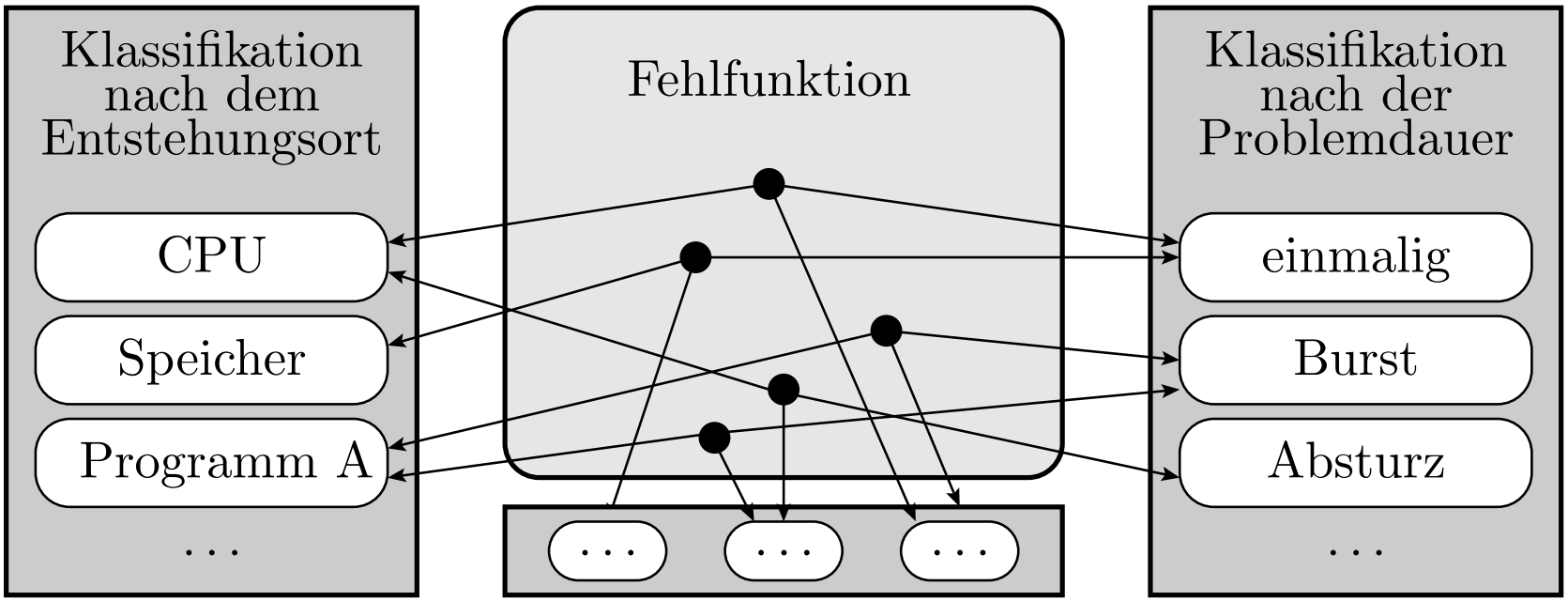
Beispiel 1.1: Zuverlässigkeit und MF-Rate

Innerhalb von 300 h Programmnutzung sind 30 Fehlfunktionen aufgetreten, $MTS = 0{,}1\,\mathrm{h}$*. Wie groß sind Zuverlässigkeit und MF-Rate?*

$$MTBM = \frac{300\,\mathrm{h}}{30\,[\mathrm{MF}]} = 10\,\mathrm{h}$$
$$R = \frac{10\,\mathrm{h}}{0{,}1\,\mathrm{h}} = 100\,\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$
$$\zeta = R^{-1} = 10^{-2}\,\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$$

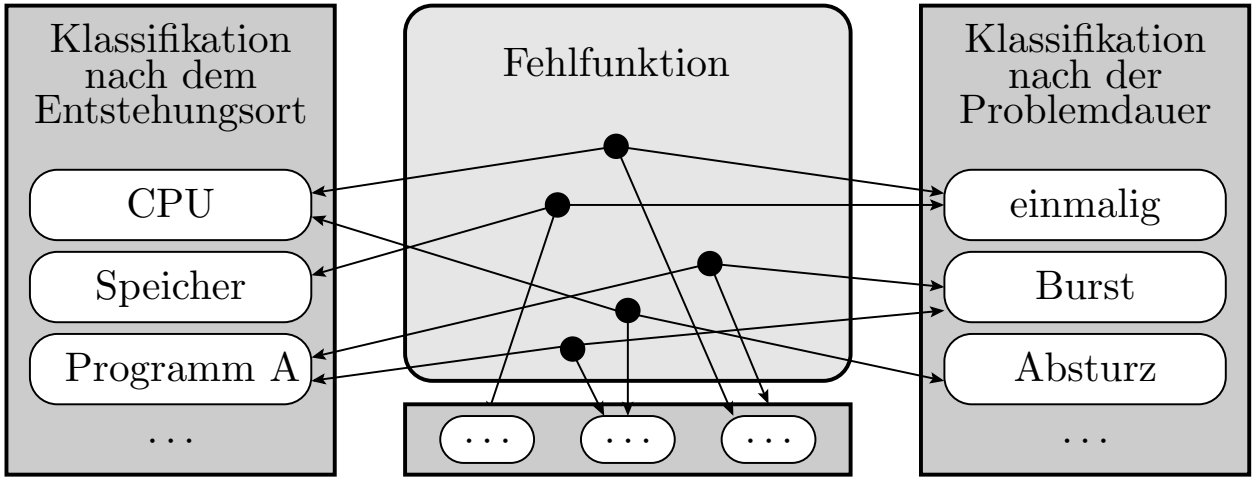
$MTBM$	Mittlere Nutzungsdauer zwischen Fehlfunktion (Mean service life between malfunctions).
MTS	Mittlere Service-Dauer (Mean time to service).
ζ	Fehlfunktionsrate.
R	Zuverlässigkeit (Reliability).
$\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$	Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.
$\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$	Zählwertverhältnis in Fehlfunktionen je erbrachte Service-Leistung.

Teilzuverlässigkeiten



Die Fehlfunktionen (MF) eines Systems können in unterschiedlicher Weise klassifiziert werden, z.B.

- nach Ort, Ursache, Schaden, ... :
- nur Fehlfunktionen eines bestimmten Teilsystems,
- nur durch HW, nur durch SW verursachte Fehlfunktionen,
- nur MF, die die Betriebs-, Daten- oder Zugangssicherheit mindern.



Bei einer eindeutigen Zuordnung jeder Fehlfunktion zu genau einer Klasse i ist die Gesamtanzahl der Fehlfunktionen $\#MF$ die Summe der Anzahl der Fehlfunktionen $\#MF_i$ aller Klassen i:

$$\#MF = \sum_{i=1}^{\#MFC} \#MF_i$$

Die Fehlfunktionsrate als relative Häufigkeit der MF je DS

$$\zeta = \frac{\#MF}{\#DS}\Big|_{\mathrm{ACR}} \tag{1.7}$$

$\#MF$ Anzahl der Fehlfunktionen (Number of malfunctions).
$\#MFC$ Anzahl der MF-Klassen (Number of malfunction classes).
$\#MF_i$ Anzahl der MF der MF-Klasse i.

... ist die Summe der Fehlfunktionsraten aller Fehlfunktionsklassen

$$\zeta = \sum_{i=1}^{\#MFC} \zeta_i \tag{12}$$

und der Kehrwert der Gesamtzuverlässigkeit ist gleich der Summe der Kehrwerte der Teilzuverlässigkeiten aller Fehlfunktionsklassen:

$$\frac{1}{R} = \sum_{i=1}^{\#MFC} \frac{1}{R_i} \tag{13}$$

ζ	Gesamte Fehlfunktionsrate (Total malfunction rate).
R	Gesamtzuverlässigkeit (Total reliability).
$\#MFC$	Anzahl der MF-Klassen (Number of malfunction classes).
ζ_i	MF-Rate der MF-Klasse i (MF rate of MF class i).
R_i	Teilzuverlässigkeit (partitial reliability) von MF-Klasse i.

Beispiel 1.2: Teil- und Gesamtzuverlässigkeit

MFs seien entweder vom Speicher, vom Prozessor, von der Software oder vom Rest verursacht. Die Teilsysteme haben folgende $MTBM$s:

Teilsystem i	Speicher	Prozessor	Software	alle anderen
$MTBM_i$	500 h	3.000 h	1000 h	2.000 h

Mittlere Service-Dauer $MTS = 1\,\mathrm{min}$.

a) *Wie groß sind die vier aus den $MTBM_i$-Werten ableitbaren MF-Raten ζ_i und die Teilzuverlässigkeiten R_i?*

b) *Wie groß ist sind die MF-Rate ζ und die Zuverlässigkeit R des Gesamtsystems?*

$MTBM$	Mittlere Nutzungsdauer zwischen Fehlfunktion (Mean service life between malfunctions).
$MTBM_i$	Mittlere Nutzungsdauer zwischen Fehlfunktionen der Klasse i.
MTS	Mittlere Service-Dauer (Mean time to service).
ζ_i	MF-Rate der MF-Klasse i (MF rate of MF class i).
R_i	Teilzuverlässigkeit (partitial reliability) von MF-Klasse i.

Teilsystem i	Speicher	Prozessor	Software	alle anderen
$MTBM_i$	500 h	3.000 h	1000 h	2.000 h

Mittlere Service-Dauer $MTS = 1\,\mathrm{min}$.

a) *Wie groß sind die vier aus den $MTBM_i$-Werten ableitbaren MF-Raten ζ_i und die Teilzuverlässigkeiten R_i?*

Teilsystem i	Speicher	Prozessor	Software	Rest
$MTBM_i$ in min	$3 \cdot 10^4$	$18 \cdot 10^4$	$6 \cdot 10^4$	$12 \cdot 10^4$
$R_i = \frac{MTBM_i}{MTS}$ in $\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$	$3 \cdot 10^4$	$18 \cdot 10^4$	$6 \cdot 10^4$	$12 \cdot 10^4$
$\zeta_i = \frac{1}{R_i}$ in $\left[\frac{\mathrm{MF}}{\mathrm{DS}}\right]$	$3{,}33 \cdot 10^{-5}$	$5{,}56 \cdot 10^{-6}$	$1{,}67 \cdot 10^{-5}$	$8{,}33 \cdot 10^{-6}$

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

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

Teilsystem i	Speicher	Prozessor	Software	alle anderen
$MTBM_i$	500 h	3.000 h	1000 h	2.000 h

Mittlere Service-Dauer $MTS = 1\,\text{min}$.

b) *Wie groß ist sind die MF-Rate ζ und die Zuverlässigkeit R des Gesamtsystems?*

$$\begin{aligned}
\zeta &= \left(3{,}33 \cdot 10^{-5} + 5{,}56 \cdot 10^{-6} + 1{,}67 \cdot 1 + 8{,}33 \cdot 10^{-6}\right) \left[\frac{\text{MF}}{\text{DS}}\right] \\
&= 6{,}39 \cdot 10^{-5} \left[\frac{\text{MF}}{\text{DS}}\right] \\
R &= \frac{1}{\zeta} = 1{,}57 \cdot 10^{4} \left[\frac{\text{DS}}{\text{MF}}\right]
\end{aligned}$$

ζ Gesamte Fehlfunktionsrate (Total malfunction rate).
R Gesamtzuverlässigkeit (Total reliability).

Sicherheit

Schaden durch Fehlfunktionen

Der potentielle Schaden durch Fehlfunktionen reicht von unerheblich bis sehr groß. Für Industriegeräte werden nach IEC 61508 folgende Sicherheitsstufen (SIL – **S**afety **I**ntegrity **L**evel) unterschieden:

- SIL1: Kleine Schäden an Anlagen und Eigentum.
- SIL2: Große Schäden an Anlagen, Personenverletzung.
- SIL3: Verletzung von Personen, einige Tote.
- SIL4: Katastrophen, viele Tote, gravierende Umweltschäden.

Die Sicherheitsstufe legt weitere Grenzwerte für Kenngrößen fest:

- PFH (**p**robability of **f**ailure per **h**our),
- PFD (**p**robability of **f**ailure on **d**emand), ...

SIL	1	2	3	4
$PFH_{\max}$	10^{-5}	10^{-6}	10^{-7}	10^{-8}
$PFD_{\max}$	10^{-1}	10^{-2}	10^{-3}	10^{-4}

Wir definieren Sicherheiten als eine Teilzuverlässigkeiten.

Sicherheitgefärdende Fehlfunktionen

Sicherheiten bezieht sich auf angenommene Gefährdungen:

Sicherheit	Sicher vor welchen Gefährdungen?
Betriebssicherheit (safty)	Personen- und Umweltschäden
Datensicherheit (security)	Datendiebstahl
Sicherheit Datenerhalt	Datenverlust
...	...

Die Rate der die betrachtete Sicherheit gefährdenden MF

$$\zeta_{\mathrm{S}} = \frac{\#HM}{\#DS}\Big|_{\mathrm{ACR}} \tag{14}$$

ist um einen Faktor η_{SE} kleiner als die Rate aller MF:

$$\zeta_{\mathrm{S}} = \zeta \cdot \eta_{\mathrm{SE}} \tag{15}$$

$$= \frac{MTS}{MTTH} \tag{16}$$

ζ_{S}	Rate der sicherheitsgefährdenden Fehlfunktionen.
$\#HM$	Anzahl der sicherheitsgefährdenden Fehlfunktionen (Number of hazzardous malfunctions).
$\#DS$	Anzahl der erbrachten Service-Leistungen (Number of delivered services).
$MTTH$	Mittlere Zeit bis zur nächsten Gefährdung (Mean time to hazzard).

Sicherheit als Teilzuverlässigkeit

Eine Sicherheit vor einer bestimmten Klasse von MFs ist der Kehrwert der MF-Rate durch die MFs dieser Klasse

$$S = \left.\frac{\#DS}{\#HM}\right|_{\mathrm{ACR}} \tag{17}$$

$$S = 1/\zeta_{\mathrm{s}} \tag{18}$$

und damit die Zuverlässigkeit geteilt durch den Anteil der gefährdenden MFs:

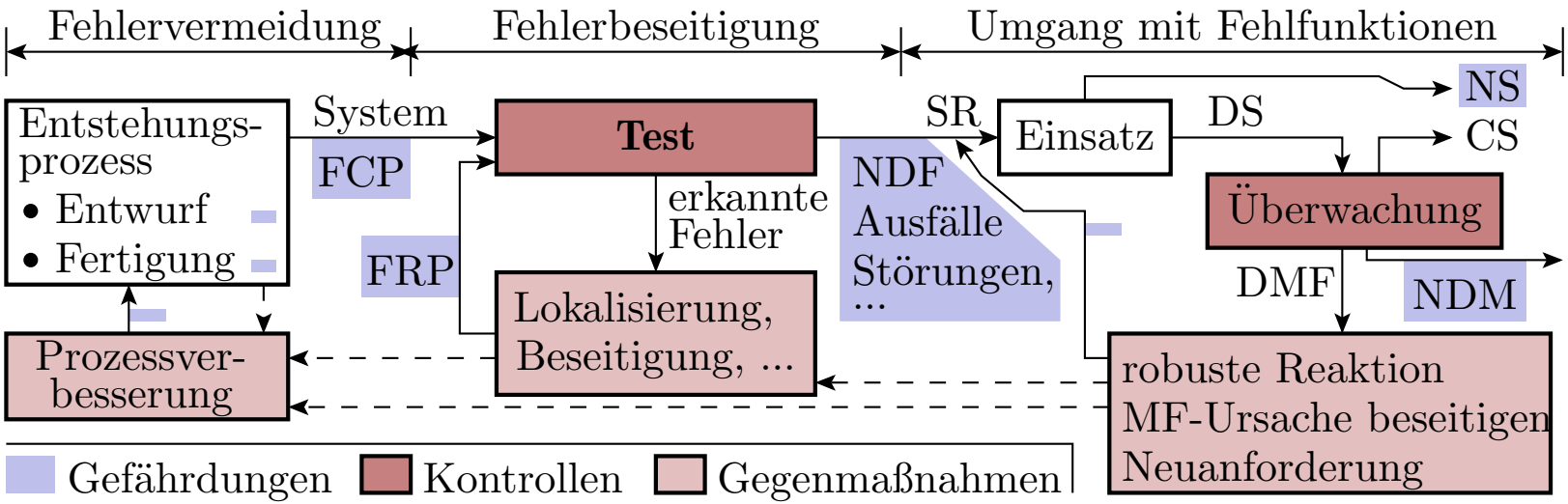
$$S = \frac{R}{\eta_{\mathrm{SE}}} \tag{19}$$

Hohe Sicherheit verlangt hohe Zuverlässigkeit und/oder einen kleineren Anteil sicherheitsgefährdender Fehlerfunktionen η_{SE}.

S	Sicherheit (Safety or security).
$\#HM$	Anzahl der sicherheitsgefährdenden Fehlfunktionen (Number of hazzardous malfunctions).
$\#DS$	Anzahl der erbrachten Service-Leistungen (Number of delivered services).
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.
ζ_{S}	Rate der sicherheitsgefährdenden Fehlfunktionen.
R	Zuverlässigkeit (Reliability).
η_{SE}	Anteil der sicherheitsgefährdenden Fehlfunktionen.

Zusammenfassung

Sicherung der Verlässlichkeit



Verlässlichkeit wird auf drei Ebenen gesichert:

- Schadensvermeidung durch Überwachung und geeigneten Umgang mit den erkannten Fehlfunktionen, die durch Fehler, Störungen und Ausfälle verursacht sein können.
- Beseitigung erkannter Fehler.
- Beseitigung bzw. Minderung von Fehlerentstehungsursachen.

Service-Modell

IT-Systeme und die Entstehungsprozesse der HW und SW werden als Service-Leister betrachtet, die auf Anforderung aus Eingaben Ausgaben erzeugen:

- Service-Leistungen und Fehlerfunktionen werden dadurch zählbar und Zeiten der Verfügbarkeit, für Reparatur ... , messbar.
- Fehlfunktions-Bursts haben meist eine gemeinsame Ursache und werden als eine MF gezählt.

Die Abschätzung von Verlässlichkeitskenngrößen aus Zählwerten (Anzahl der Service-Leistungen, Fehlfunktionen, ...) verlangt in Abhängigkeit von der Schätzgenauigkeit ausreichend große bzw. ausreichend von ihrem Maximum abweichende Zählwerte.

Verfügbarkeit

Relative Häufigkeit, dass das System bei Service-Anforderung verfügbart ist, beschreibar als

- mittlere anteilmäßige Zeit der Verfügbarkeit:

$$A = \frac{MTBM}{MTBM+MTMT} \tag{1.1}$$

- Gegenwahrscheinlichkeit der Nichtverfügbarkeit:

$$A = 1 - PFD \tag{1.2}$$

Teilverfügbarkeiten:

- Lieferverfügbarkeit (Service erbringbar):

$$A_{\mathrm{DS}} = \eta_{\mathrm{DS}} \tag{1.3}$$

- MT-Verfügbarkeit (System nicht mit interner MF-Behandlung beschäftigt):

$$A_{\mathrm{MT}} = \frac{MTBT}{MTBT+(MTB+\mu_{\mathrm{CM}}\cdot MTS)} \tag{1.4}$$

- Ausfall-Verfügbarkeit (keine ausgefallene Hardware):

$$A_{\mathrm{F}} = \frac{MTBF}{MTBF+MTTR} \tag{1.5}$$

- PWA-Verfügbarkeit (Nutzer nicht mit Problemumgehung beschäftigt):

$$A_{\mathrm{PWA}} \approx 80\%$$

Meist werden die aspektbezogenen Teilverfügbarkeiten getrennt betrachtet, aber auch zu einer Gesamtverfügbarkeit zusammenfassbar:

$$A = A_{\mathrm{NS}} + A_{\mathrm{MT}} + A_{\mathrm{F}} + A_{\mathrm{PWA}} - 3 \tag{1.6}$$

Hochverfügbarkeit (ausfallbezogen) verlangt Zusatzmaßnahmen wie USV, Raid, ...

Fehlfunktionsrate und Zuverlässigkeit

Fehlfunktionsrate

- relative Häufigkeit von Fehlfunktionen je Service-Leistung:

$$\zeta = \frac{\#MF}{\#DS}\Big|_{\mathrm{ACR}} \tag{1.7}$$

- Verhältnis der mittleren Service-Dauer MTS zur $MTBM$:

$$\zeta = \frac{MTS}{MTBM} \tag{1.8}$$

- Summe der MF-Raten aller MF-Klassen:

$$\zeta = \sum_{i=1}^{\#MFC} \zeta_i \tag{1.12}$$

Zuverlässigkeit

- zu erwartende Anzahl der Service-Leistungen je Fehlfunktion:

$$R = \frac{\#DS}{\#MF}\Big|_{\mathrm{ACR}} \tag{1.9}$$

- Kehrwert der MF-Rate:

$$R = 1/\zeta \tag{1.11}$$

- Kehrwert der Kehrwertsumme von Teilzuverlässigkeiten:

$$\frac{1}{R} = \sum_{i=1}^{\#MFC} \frac{1}{R_i} \tag{1.13}$$

Gefährdende Fehlfunktionen und Sicherheit

Rate der sicherheitsgefährdenden Fehlfunktionen

- relative Häufigkeit sicherheitsgefährdendender MF je DS:

$$\zeta_{\mathrm{S}} = \frac{\#HM}{\#DS}\Big|_{\mathrm{ACR}} \tag{1.14}$$

- Anteilige MF-Rate:

$$\zeta_{\mathrm{S}} = \zeta \cdot \eta_{\mathrm{SE}} \tag{1.15}$$

- Verhältnis der mittleren Service-Dauer MTS zur $MTTH$:

$$\zeta_{\mathrm{S}} = \frac{MTS}{MTTH} \tag{1.16}$$

Sicherheit

- zu erwartende Anzahl der DS je gefährdende MF:

$$S = \frac{\#DS}{\#HM}\Big|_{\mathrm{ACR}} \tag{1.17}$$

- Kehrwert der Rate der sicherheitsgefährdenden MF:

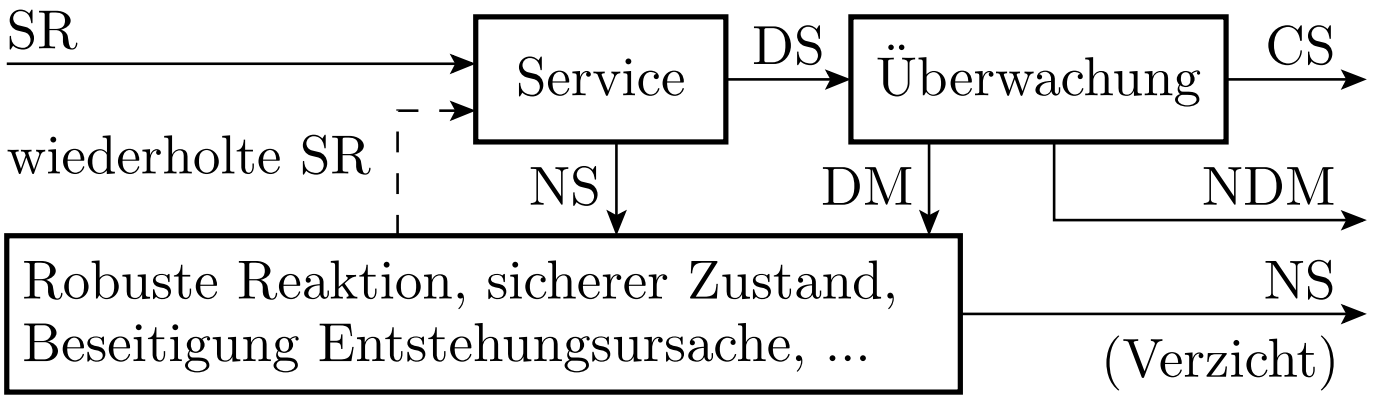
$$S = \frac{1}{\zeta_{\mathrm{S}}} \tag{1.18}$$

- Zuverlässigkeit durch Anteil der sicherheitsgefährdenden MF:

$$S = \frac{R}{\eta_{\mathrm{SE}}} \tag{1.19}$$

Umgang mit MF

Umgang mit MF im laufenden Betrieb

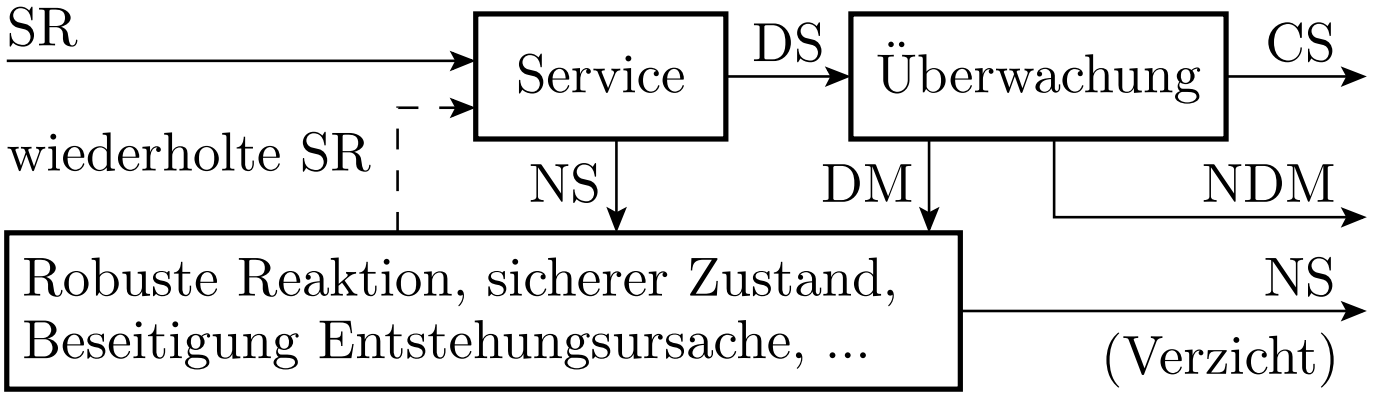


Überwachung der Service-Leistungen

- erkennt nur einen Teil der Fehfunktionen und
- klassifiziert möglicherweise korrekte Service-Leistungen als MF.

SR	Service-Anforderung.
DS	Erbrachte Service-Leistung.
NS	Keine Service-Leistung.
DM	Erkannte Fehlfunktion.
NDM	Nicht erkannte Fehlfunktion.
CS	Korrekte Service-Leistung.

3. Umgang mit MF



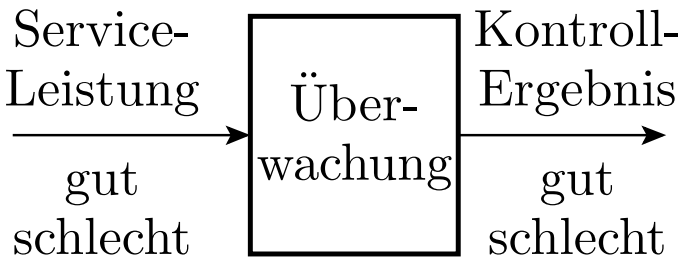
Reaktion auf erkannte MF:

- Robuste Reaktion auf erkannte Fehlfunktionen: Kontrolliertes Verhalten, um Schäden und Gefahren zu vermeiden (DS nicht nutzen, wenn erforderlich Herstellen eines sicheren Zustands, ...).
- Protokollierung des beobachteten Fehlverhaltens für den Hersteller zur Fehlerbeseitigung.
- Wiederherstellung Funktionsfähigkeit: Reparatur / Rekonfiguration, Neuinitialisierung.
- Korrektur von MF durch wiederholte Service-Anforderung.
- Wenn nicht korrigierbar, Verzicht auf die Service-Leistung (NS).

SR Service-Anforderung.
DS Erbrachte Service-Leistung.

Kenngr. Überwachung

Kenngrößen der Überwachung



Service-Ergebnis	Kontroll-ergebnis	Fehlfunktion der Kontrolle
schlecht	schlecht	—
gut	gut	—
schlecht	gut	Maskierung
gut	schlecht	Phantom-MF

1. MF-Überdeckung (MF coverage), Anteil nachweisbare MF:

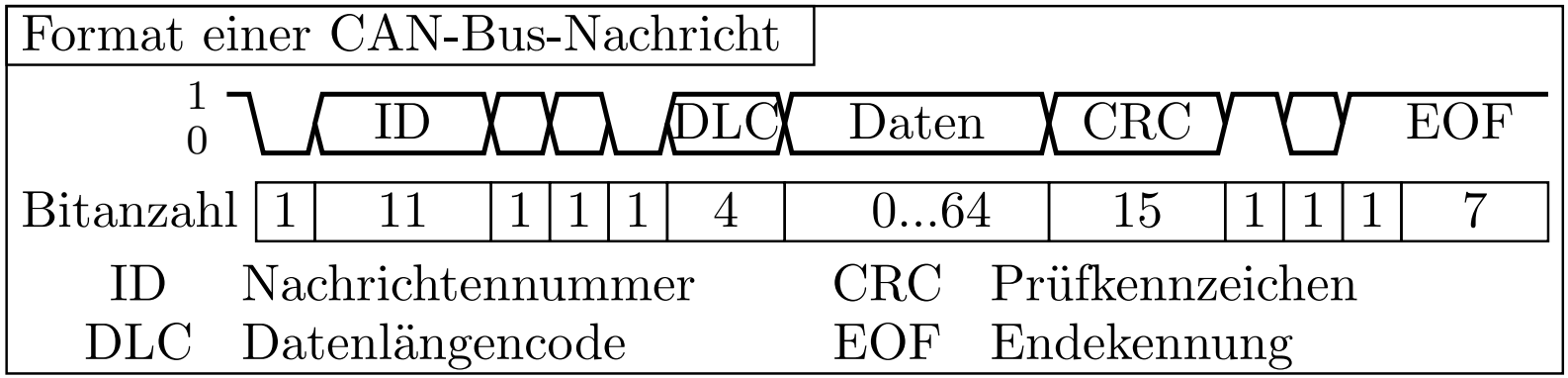
$$MC = \left.\frac{\#DM}{\#MF}\right|_{\text{ACR}} \tag{20}$$

2. Phantom-MF-Rate, Anteil der korrekten DS, die als MF klassifiziert werden:

$$\zeta_{\text{Phan}} = \left.\frac{\#PM}{\#DS}\right|_{\text{ACR}} \tag{21}$$

$\#DM$	Anzahl der erkannten Fehlfunktionen (Number of detected MFs).
$\#MF$	Anzahl der Fehlfunktionen (Number of malfunctions).
$\#PM$	Anzahl der Phantom-MF, d.h. der korrekten DS, die als MF klassifiziert werden.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

Format- und Wertekontrollen



Eine Service-Leistungen umfassst Daten eingebettet in einem Format:

- Format: werteunabhängige Merkmale: Zeitschranken, WB, ...
- Daten: Werte der Datenobjekte.

Einteilung Überwachungsverfahren für digitale Service-Leistungen:

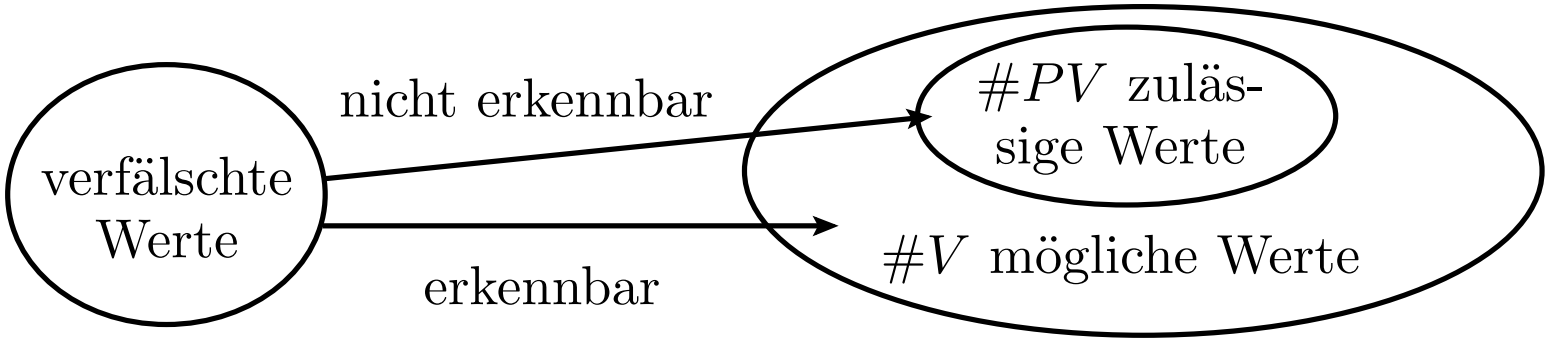
1. Formatkontrollen: nur Kontrolle werteunabhängiger Merkmale. DS mit Formatfehlern sind immer falsch und DS mit korrektem Format können falsche Daten haben, d.h. nur Kontrolle auf Zulässigkeit.
2. Wertekontrollen: (Zusätzliche) Kontrolle von Datenwerten.

Formatkontrollen sind einfacher durchzuführen und erzielen bei digitalen DS oft höhere MC und kleinere Phantom-MF-Raten.

Formatkontrollen

Informationsredundanz

Formatkontrollen (Fehlererkennende Codes, Prüfkennzeichen, Wertebereichskontrollen, ...) nutzen Informationsredundanz.



Die Fehlfunktionsüberdeckung ist tendentiell um so höher, je geringer der Anteil der zulässigen Werte ist. Wenn alle Verfälschungsmöglichkeiten gleichhäufig auftreten, alle unzulässige Werte als unzulässig und alle unzulässigen Werte als unzulässig erkannt werden:

$$MC = 1 - \frac{\#PV}{\#V} \tag{22}$$

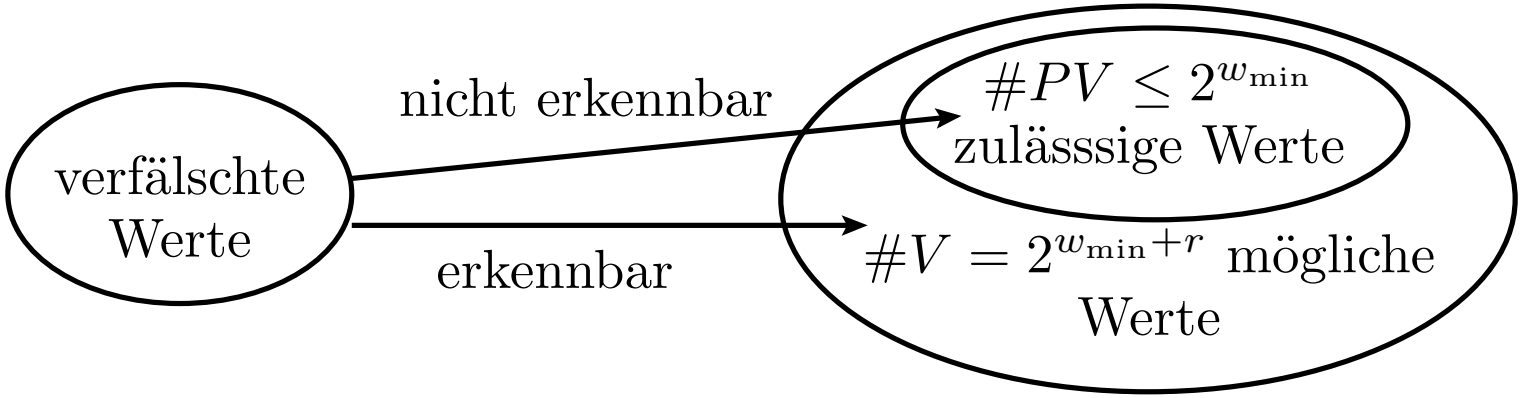
$$\zeta_{\mathrm{Phan}} = 0 \tag{23}$$

$\#PV$	Anzahl der zulässigen Werte (Number of permitted values).
$\#V$	Anzahl der möglichen Werte (Number of possible values).
ζ_{Phan}	Phantom-Fehlfunktionsrate.

Redundante Bits

Angenommen, es genügen $w_{\min}$ Bits für die Unterscheidung aller zulässigen Werte. Bei Darstellung mit r zusätzlichen (redundanten) Bits:

$$w = r + w_{\min}$$



$$MC = 1 - \frac{\#PV}{\#V} \geq 1 - \frac{2^{w_{\min}}}{2^{w_{\min}+r}} = 1 - 2^{-r} \tag{24}$$

MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
$\#PV$	Anzahl der zulässigen Werte (Number of permitted values).
$\#V$	Anzahl der möglichen Werte (Number of possible values).
$w_{\min}$	Minimale Datenbitanzahl.
r	Anzahl der redundanten Bits.

Formatüberwachung mit r redundanten Bits

Bei gleichmäßiger Abbildung der Verfälschungen auf mögliche Werte und Nachweis aller unzulässigen Werte:

$$MC \geq 1 - 2^{-r} \tag{1.24}$$

r	10	20	30
MC	$\approx 99{,}9\%$	$\approx 1 - 10^{-6}$	$\approx 1 - 10^{-9}$

Bei angenommen $w_{\min} = 10^3$ kein nennenswerter Zusatzaufwand.

Idealverhalten: fehlererkennende Codes und Prüfkennzeichen.

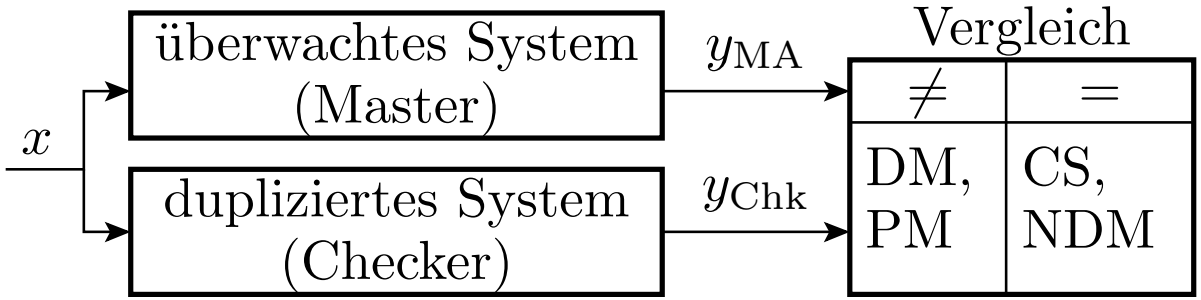
Formatkontrollen ohne gleichmäßige Abbildung von Verfälschungen auf zulässige und unzulässige Werte mit dennoch gutem Aufwand-Nutzen-Verhältnis: Kontrollen von Wertebereichen, Datentypen, Syntax, ... (siehe Abschn. 4.2.2 *Informationsredundanz*).

MC Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
r Anzahl der redundanten Bits.

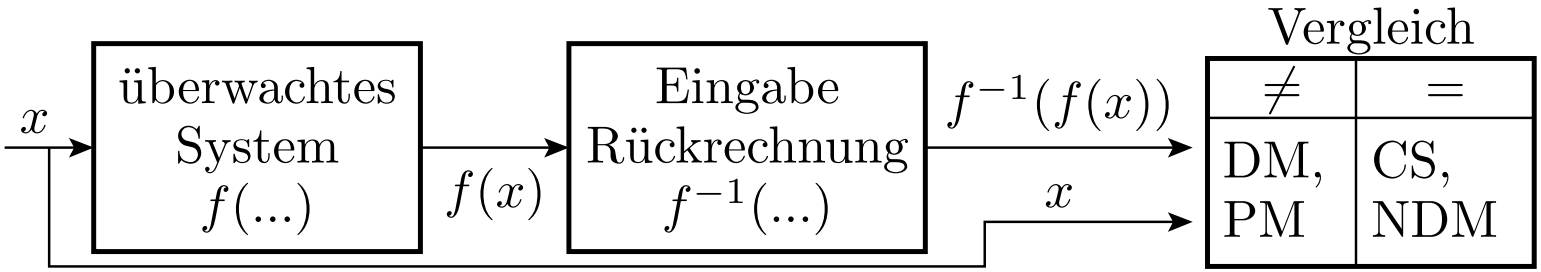
Wertekontrollen

Kontrollverfahren für Werte

- Master-Checker-Prinzip (Verdopplung und Vergleich):

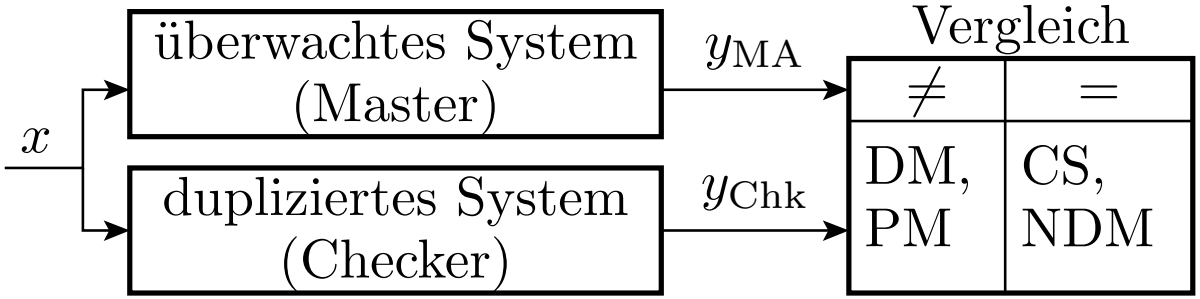


- Loop-Test (Eingaberückberechnung und Vergleich), z.B. Überwachung Versenden durch Empfang und Vergleich der empfangenen mit den Sendedaten:



- Korrektheitstest für spezielle Aufgaben, z.B. für Suche Weg von A nach B durch einen Graphen ist der Korrektheitstest, dass der gefundener Weg von A nach B führt.

Eigenschaften von Master-Checker-Systemen



Bei einem DS mit vielen Bits und geringer MF-Rate sind praktisch alle Master- und Checker-MF ohne gemeinsame Ursache nachweisbar:

$$MC = \eta_{\mathrm{Div}} \tag{25}$$

Checker-MFs mit abweichender Ursache werden Phantom-MFs:

$$\zeta_{\mathrm{Phan}} = \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}}) \tag{26}$$

CS	Korrekte Service-Leistung.
DM	Erkannte Fehlfunktion.
NDM	Nicht erkannte Fehlfunktion.
PM	Phantomfehlfunktion.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
ζ_{MS}	Übereinstimmende Fehlfunktionsrate von Master und Checker.

Diversität

In der Technik versteht man unter Diversität verschiedenartige Realisierungen gleicher Aufgaben zur Vermeidung gleicher MF bei Mehrfachberechnung oder Wiederholung. Wenn

- MF sehr selten auftreten und es
- ganz viele Möglichkeiten für unterschiedliche MF gibt,

ist es praktisch ausgeschlossen, dass beide Berechnungen gleichzeitig übereinstimmend verfälscht werden. Wenn jedoch beide Systeme denselben Fehler haben, stimmen die Verfälschungen durch MF, die der Fehler verursacht, fast immer überein. Bei Verschiedenartigkeit der Berechnungen ist nur ein Teil der MF durch Fehler gleich:

$$\eta_{\mathrm{Div}} = 1 - \eta_{\mathrm{CF}} \cdot \eta_{\mathrm{F}} \tag{27}$$

η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
η_{F}	Anteil der Fehlfunktionen durch Fehler.
η_{CF}	Anteil der MF durch identische Fehler, die ein Ergebnisvergleich nicht erkennt.

Vermeidung gleicher MF durch Fehler

Die Diversität und damit die MC von Master-Checker-Systemen lässt sich durch konstruktive und organisatorische Maßnahmen gegenüber der für zwei identische Berechnungen mit denselben Fehlern erhöhen:

Erweiterte Diversität	konstr. und org. Maßnahmen	zusätzlich Vermeidung nicht diversitärer
HW-Diversität	Ausführung auf verschiedener HW	Fertigungsfehler, Ausfälle
HW-Entwurfsdiversität	unabhängig entworfene HW	HW-Entwurfsfehler
Syntaktische Diversität	unterschiedlich übersetzte SW	SW-Übersetzungsfehler
Software-Diversität	unabhängig entworfene SW	SW-Entwurfsfehler
diversitäre Nutzung (Fehlerumgehung)	Wiederholung mit geänderter SR*	Fehler im System, Eingabefehler

* bei abweichenden Sollwerten ungeeignet für Mehrfachberechung und Vergleich.

Diversität von Software-Versionen

Software-Fehler als Hauptquelle für MFs verlangen Verschiedenartigkeit der Arbeistprozesse, in denen sie entstehen:

- Komplette Entwicklung mindestens zweimal
- durch getrennte Teams, keine Kommunikation,
- aus einer nicht diversitären Spezifikation, ...

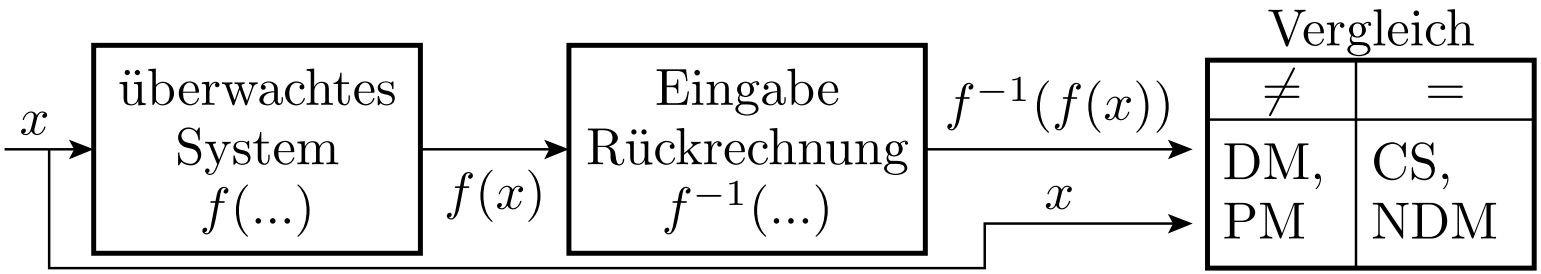
Die ursprüngliche euphorische Meinung, dass so Diversität gegenüber allen Fehlern, außer denen in der Spezifikation erzielbar ist, nicht bestätigt. Die direkte oder indirekte Kommunikation der Entwicklungsteams über die Interpretation der Spezifikation, während des Test etc. trägt Gemeinsamkeiten in die Entwürfe. Neigung von Menschen, gewisse Fehler zu wiederholen*, ... $\eta_{\mathrm{CF}} \geq 10\%$. MF-Überdeckung Verdopplung und Vergl. nach Gl. 1.25 und 1.27:

$$MC \leq 1 - 10\% \cdot \eta_{\mathrm{CF}}$$

Eine Kontrolle mit $r = 10$ Bit Informationsredundanz erreicht nach Gl. 1.24 $MC \geq 99{,}9\%$ fast ohne Zusatzaufwand und ohne PM.

* U. Voges, Software-Diversität und ihre Modellierung - Software-Fehlertoleranz und ihre Bewertung durch Fehler- und Kostenmodelle, Springer (1989).

Eigenschaften Loop-Test

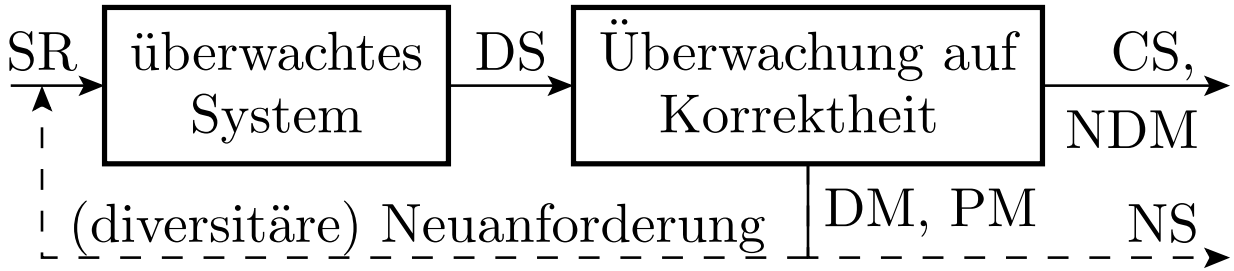


Da $f(\ldots)$ und $f^{-1}(\ldots)$ sich in Algorithmus und Fehlerwirkung unterscheiden, ist auch für MF durch Fehler ohne zusätzliche konstruktive und organisatorische Maßnahmen eine akzeptable Fehlfunktionsüberdeckung zu erwarten.

Nur einsetzbar, wenn, $f(\ldots)$ eine umkehrbar eindeutige Abbildung ist. Besonders geeignet, wenn $f^{-1}(\ldots)$ viel einfacher als $f(\ldots)$ realisiert ist, z.B. Quadratbildung zur Kontrolle der Wurzelberechung.

$f^{-1}(\ldots)$	Inverse Funktion.
CS, MF	Korrekte Service-Leistung, Fehlfunktion.
DM, PM	Erkannte Fehlfunktion, Phantomfehlfunktion.
NDM	Nicht erkannte Fehlfunktion.

Korrektheitstest

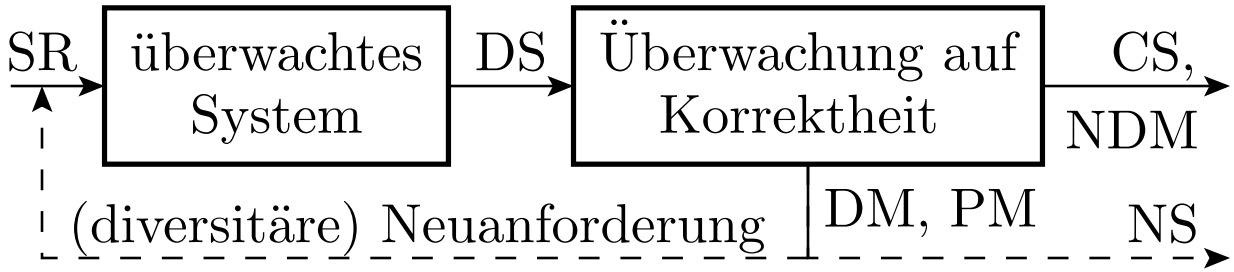


Wenn Zielfunktion durch eine Korrektheitskriterium spezifiziert ist:

- Sortieren einer Liste $\Rightarrow$ Liste sortiert und enthält alle Elemente,
- Suche Weg durch einen Graphen $\Rightarrow$ zulässiger Weg,
- Suche Test für Fehlernachweis $\Rightarrow$ Fehlersimulation, ...

Nur sehr eingeschränkt anwendbar. Fehlfunktionsüberdeckung MC gleich der Zuverlässigkeit der Kontrolle, oft sehr hoch, aber bei einer Lösungssuche mit vielen Fehlversuchen ...

SR	Service-Anforderung.
DS	Erbrachte Service-Leistung.
DM	Erkannte Fehlfunktion.
CS	Korrekte Service-Leistung.
NDM	Nicht erkannte Fehlfunktion.



Typische Form von Suchalgorithmen:

```
Probiere, bis Kontrolle bestanden
    Errate das Ergebnis
```

Entspricht der MF-Behandlung »Wiederholung nach Fehlfunktion bis MF beseitigt oder nicht mehr erkennbar«. Bei einer hohen MF-Rate vor der Kontrolle $\zeta \to 1$ strebt die Anzahl der Wiederholungen bis zur Lösungsfindung $\mu_{\mathrm{MC}} \to \infty$ und die Zuverlässigkeit $R_{\mathrm{MT}} \to 1$, siehe später GI.

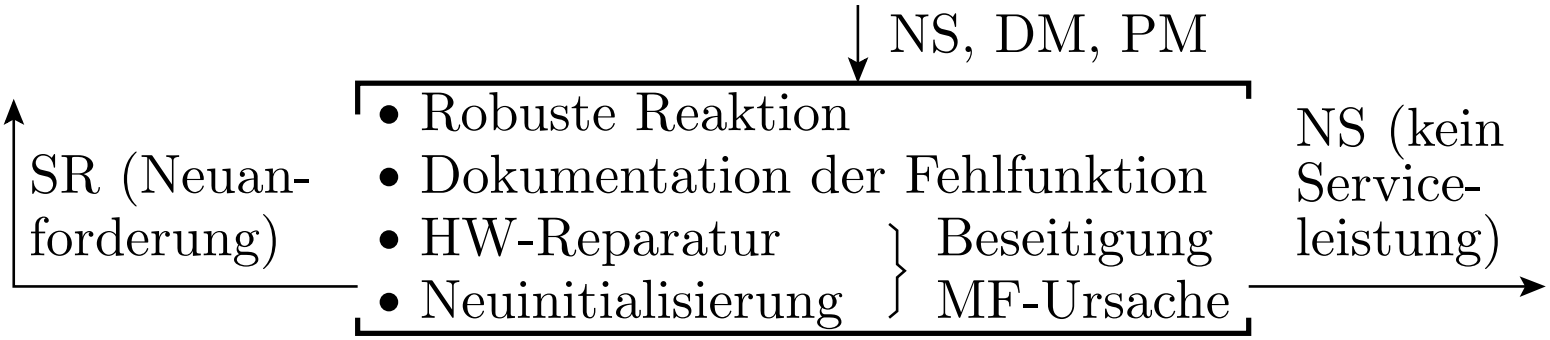
$$\mu_{\mathrm{CM}} = \frac{1}{1-\zeta \cdot MC} - 1 \tag{1.46}$$

$$R_{\mathrm{MT}} = \frac{(1-\zeta \cdot MC)}{\zeta \cdot (1-MC)} \tag{1.48}$$

μ_{CM}	Mittlere Anzahl der Neuberechnungen (Korrekturversuche) je MF.
ζ	Fehlfunktionsrate ohne Fehlfunktionsbehandlung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
R_{MT}	Zuverlässigkeit Zufallssuche plus Korrektheitskontrolle.

Umgang mit erkannten MF

Reaktion auf erkannte Fehlfunktionen



Robuste Fehlfunktionsbehandlung (Schaden vermeiden):

- erkannte MF nicht nutzen, wichtige Daten sichern,
- sicheren Zustand herstellen, z.B. Notausschaltung.

Dokumentation der Fehlfunktion für die Fehlersuche:

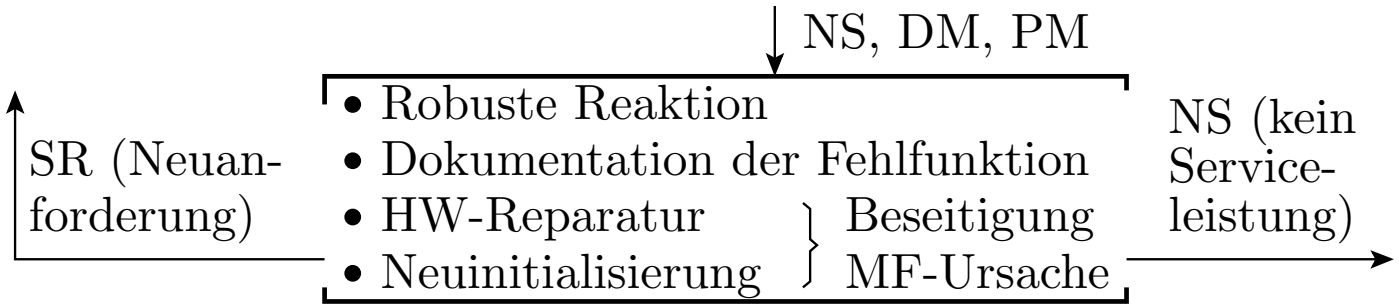
- Fehlermeldung, Core-Dump, Cap-Datei (Windows) erzeugen, ... (siehe Abschn. 1.4.6 *Reifeprozess*).

Beseitigung der MF-Entstehungsursache nach Ausfall:

- Reparatur ausgefallener HW oder
- Rekonfiguration mit/ohne verringerter Leistung, ...
- Wiederherstellung eines /des letzten zulässigen Systemzustands.

DM, PM Erkannte Fehlfunktion, Phantomfehlfunktion.

Fehlfunktion ohne Ausfall als Ursache



- Auch ohne erkennbare Verfälschung in der Regel prophylaktische Neuinitialisierung aller internen Zustände.
- Service-Abbruch nach Fehlfunktion (STMF),
- Identische Wiederholung, max. einmal* (R1MF) oder solange sich die Verfälschung ändert (RFCM).
- Wiederholung mit anderem (diversitären) System (Folie 1.63),
- Fehlerumgehung mit geänderter Service-Anforderung (Folie 1.74).

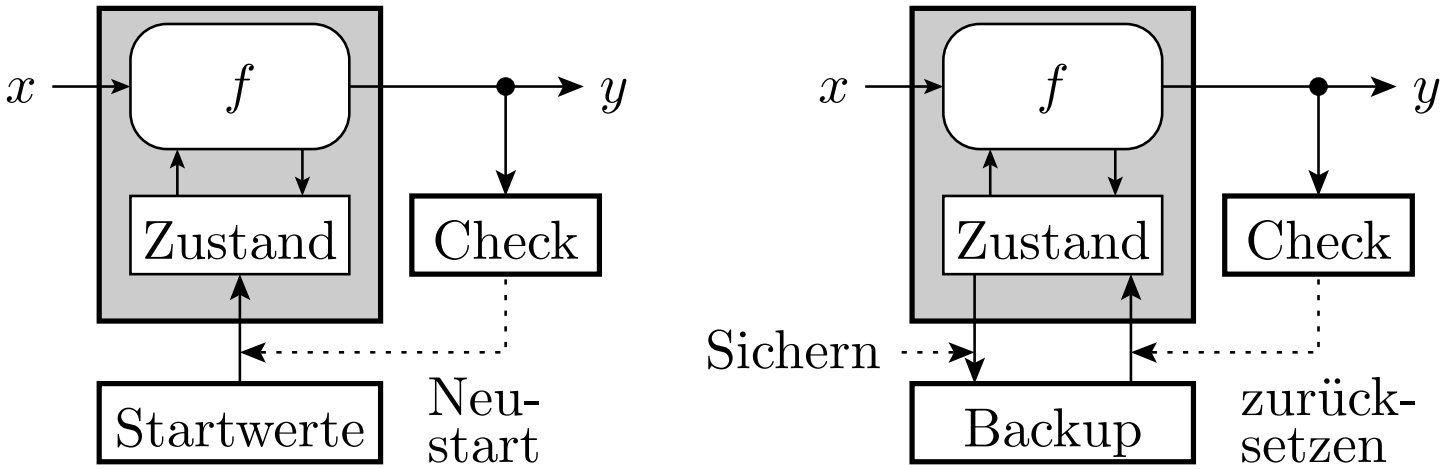
* Bei übereinstimmender Entstehungsursache (gleicher Fehler) entsteht bei Wiederholung wieder dieselbe Fehlfunktion.

STMF Service-Abbruch bei Fehlfunktion (keine Korrektur).

R1MF Ein Korrekturversuch nach Fehlfunktion durch identische Wiederholung.

RFCM Identische Wiederholung nach Fehlfunktion, solange sich die Verfälschung ändert.

Wiederherstellung zulässiger Systemzustand



Bei einer MF werden oft interne Daten verfälscht. Zur Rückkehr in einen funktionsfähigen Zustand sind die internen Daten erneut mit zulässigen Werten zu initialisieren:

- Statische Neuinitialisierung (Reset): fester Anfangszustand,
- Dynamische Neuinitialisierung: Regelmäßiges Backup wärend des Betriebs. Laden des letzten Backups nach erkannter MF.

Oft werden nur Daten gesichert, die sich nicht problemlos neu berechnen lassen, bei Editoren, Logistiksysteme, Datenbanken, ... die Eingaben seit dem letzten kompletten Backup.

Vermeidung problematischer MF

Ausschluss von HM, für die eine robuste Reaktion schwierig ist, durch

- Systemgestaltung, Anwendungsrichtlinien,
- Arbeitsschutzverordnungen, Zertifizierungsprozesse, ...

Gestaltungsprinzipien für sicherheitskritische Systeme:

- Ruhestromprinzip: Konstruktionsprinzip, bei dem das System bei Versagen automatisch in einen sicheren Zustand übergeht.
  - Eisenbahnsignaltechnik: bei fehlendem Ruhestrom Störungsmeldung.
  - Brandmeldeanlage: bei Drahtbruch Alarm.
  - Fahrzeugbremse: Bremsen, wenn Bremsschlauch platzt, ...
- MF-Isolation: Ausschluss der MF-Ausbreitung zwischen funktional unabhängigen Komponenten, z.B. getrennten Prozessen, die vom selben Rechner ausgeführt werden.
- Brandmauern: Ausschluss der MF-Ausbreitung über besonders zu schützende Teilsystemschnittstellen, auch gegen Cyber-Angriffe.

MF Fehlfunktion.
HM Sicherheitsgefährdende Fehlfunktion.

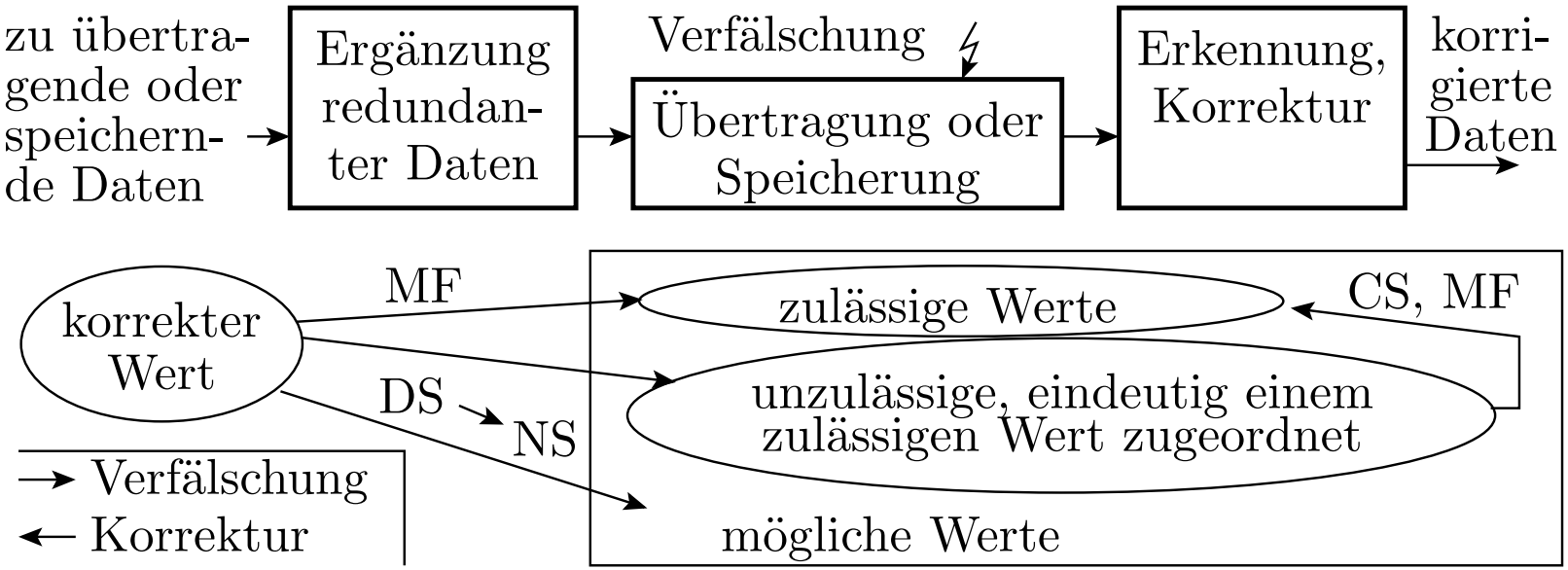
Fehlerumgehung

Bei übereinstimmenden Fehlern als Entstehungsursache und identischer Service-Anforderung entsteht bei gleicher Wiederholung wieder dieselbe Fehlerfunktion.

Fehlerumgehung: Änderung der Service-Anforderung (andere Daten, geänderter Reihenfolge, anderer Service-Anbieter, ...).

Fehlerumgehung als Reifeprozess: Bei der Einarbeitung eines Nutzers in ein neues System sind typisch viele MF beobachtbar, nicht nur durch Bedienungsfehler, sondern auch durch Fehler im System. Mit zunehmender Nutzung lernt der Nutzer problematische Eingaben zu vermeiden und seine Service-Anforderungen an die Möglichkeiten des Systems anzupassen. Zunahme der beobachtbaren Systemzuverlässigkeit.

Fehlerkorrigierende Codes (ECC)



Alternative Korrekturmöglichkeit für verfälschte Daten nach der Übertragung und Speicherung (siehe Abschn. 4.3.1 *Fehlerkorrigierende Codes*):

- Ergänzung zusätzlicher (redundanter) Bits vor der Übertragung oder Speicherung, mehr als für fehlererkennende Codes.
- Bei erkennbarer Verfälschung, Bestimmung der verfälschten Bits mit Hilfe der redundanten Bits. Rückgewinnung der korrekten Werte.

ECC Fehlerkorrigierenden Codes.

Zu den nachfolgenden Abschätzungen

Lernziel ist, dass Sie

- die Möglichkeit quantitativer Abschätzungen akzeptieren,
- Beispielrechnungen durchführen und
- den ungefähren Einfluss der MF-Behandlung auf die einzelnen Verlässlichkeitskenngrößen eines Systems einschätzen lernen.

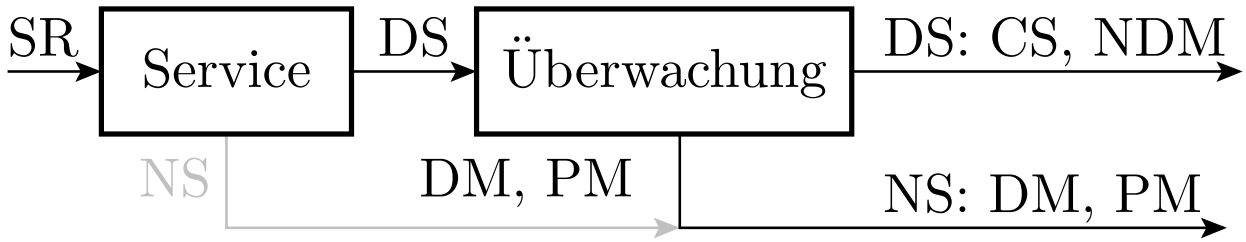
Die Herleitung der Formeln nutzt von Foliensatz 2 vorab zwei Regeln:

- Bei sich ausschließenden Ereignissen ist die Wahrscheinlichkeit, dass mindestens eines der Ereignisse entritt, die Summe der Eintrittswahrscheinlichkeiten der Einzelereignisse.
- Bei mehreren unabhängigen Eintrittsbedingungen ist die Gesamteintrittswahrscheinlichkeitt das Produkt der Eintrittswahrscheinlichkeiten aller Bedingungen.

Die Mathematik dahinter und die für die Herleitungen benutzten Techniken folgen auf Foliensatz 2.

Verlässlichkeit STMF

Service-Abbruch bei Fehlfunktion (STMF)



MT-Verfügbarkeit (Wahrsch. keine MT bei Anforderung):

$$A_{\mathrm{MT}} = \frac{MTBT}{MTBT+(MTB+\mu_{\mathrm{CM}}\cdot MTS)} \tag{1.4}$$

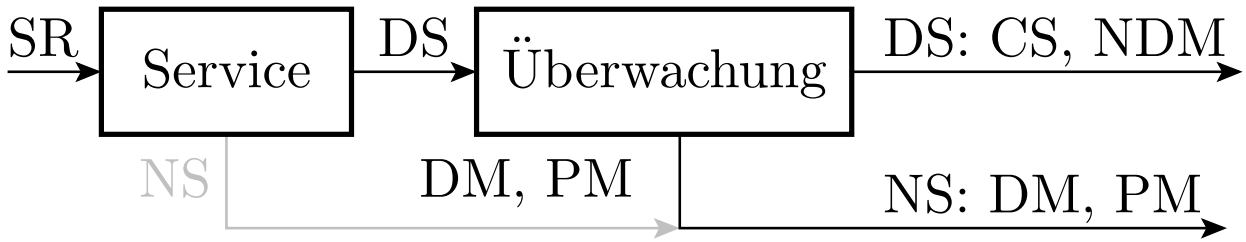
Ohne Korrekturversuche $\mu_{\mathrm{CP}} = 0$:

$$A_{\mathrm{MT}} = \frac{MTBT}{MTBT+MTB} \tag{28}$$

Abschn. 1.3.5: Verlässlichkeit bei STMF.

STMF	Service-Abbruch bei Fehlfunktion (keine Korrektur).
MT	Fehlfunktionsbehandlung.
A_{MT}	MT-Verfügbarkeit, Zeitanteil, den das System nicht mit MT beschäftigt ist.
$MTBT$	Mittlere Zeit zwischen MF-Behandlungen ohne Reparatur.
MTB	Mittlere Zeit für die grundlegende Fehlfunktionsbehandlung.
μ_{CM}	Mittlere Anzahl der Neuberechnungen (Korrekturversuche) je MF.
MTS	Mittlere Service-Dauer (Mean time to service).

Rate der erbringbaren Service-Leistungen STMF



Bei Abbruch nach jeder beobachtbaren MF ohne Ausfall ist die Lieferverfügbarkeit, gleichzeitig Rate der erbringbaren Service-Leistungen (Gl. 1.3), eins abzüglich der Rate der erkennbaren und der Phantom-MFs:

$$A_{\mathrm{DS}} = \eta_{\mathrm{DS}} = 1 - (\zeta \cdot MC + \zeta_{\mathrm{Phan}}) \tag{29}$$

SR, DS	Service-Anforderung, erbrachte Service-Leistung.
DM, PM	Erkannte Fehlfunktion, Phantomfehlfunktion.
CS, MF	Korrekte Service-Leistung, Fehlfunktion.
NDM, NS	Nicht erkannte Fehlfunktion, keine Service-Leistung.
η_{DS}	Anteil der erbringbaren Service-Leistungen.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
ζ	Fehlfunktionsrate.
ζ_{Phan}	Phantom-Fehlfunktionsrate.

MF-Raten und Zuverlässigkeit

Rate der erbrachten nicht erkannten MF:

$$\zeta_{\mathrm{MT}} = \frac{(1-MC)\cdot\zeta}{\eta_{\mathrm{DS}}} = \frac{(1-MC)\cdot\zeta}{1-(\zeta\cdot MC+\zeta_{\mathrm{Phan}})} \tag{30}$$

Zuverlässigkeit als Kehrwert der MF-Rate:

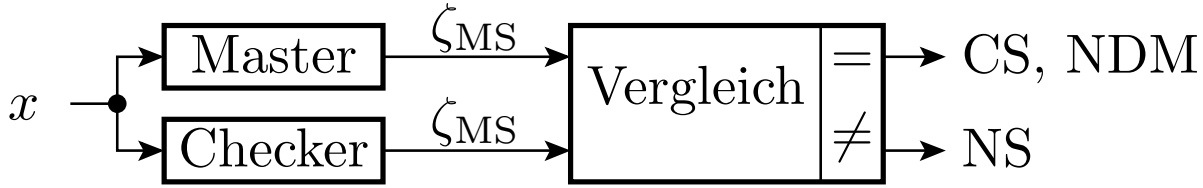
$$R_{\mathrm{MT}} = \frac{\eta_{\mathrm{DS}}}{(1-MC)\cdot\zeta} = \frac{1-(\zeta\cdot MC+\zeta_{\mathrm{Phan}})}{(1-MC)\cdot\zeta} \tag{31}$$

In der Praxis gilt fast immer η_{DS} sehr nahe an eins:

$$R_{\mathrm{MT}} = \frac{1}{(1-MC)\cdot\zeta} = \frac{R}{1-MC} \tag{32}$$

ζ_{MT}	Fehlfunktionsrate nach Fehlfunktionsbehandlung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
ζ	Fehlfunktionsrate ohne Fehlfunktionsbehandlung.
η_{DS}	Anteil der erbringbaren Service-Leistungen.
ζ_{Phan}	Phantom-Fehlfunktionsrate.
R_{MT}	Zuverlässigkeit mit Fehlfunktionsbehandlung (Reliability with malfunction treatment).
R	Zuverlässigkeit (reliability) ohne Fehlfunktionsbehandlung.

Master-Checker-Überwachung STMF (MCST)



Für Master-Checker-Paare wurde auf Folie 1.62 abgeschätzt:

$$MC = \eta_{\mathrm{Div}} \tag{1.25}$$

$$\zeta_{\mathrm{Phan}} = \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}}) \tag{1.26}$$

Rate der erbrachten MF nach Gl. 1.29:

$$\begin{aligned} \eta_{\mathrm{DS}} &= 1 - (\zeta \cdot MC + \zeta_{\mathrm{Phan}}) \\ &= 1 - (\zeta_{\mathrm{MS}} \cdot \eta_{\mathrm{Div}} + \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}})) = 1 - \zeta_{\mathrm{MS}} \end{aligned} \tag{33}$$

MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
ζ_{Phan}	Phantom-Fehlfunktionsrate.
ζ_{MS}	Übereinstimmende Fehlfunktionsrate von Master und Checker.
η_{DS}	Anteil der erbringbaren Service-Leistungen.

MT-Verfügbarkeit MCST

Eine MF-Behandlung erfolgt bei jeder abweichenden MF. Die mittlere Zeit zwischen beobachtbaren MS ist etwa die Hälfte der mittleren Zeit zwischen diversitären MF des Masters (bzw. der als gleich angenommenen Checker-MTBM):

$$MTBT = \frac{MTBM}{2 \cdot \eta_{\mathrm{Div}}}$$

Eingesetzt in (Gl. 1.28) für die MT-Verfügbarkeit:

$$A_{\mathrm{MT}} = \frac{MTBT}{MTBT + MTB} = \frac{MTBM}{MTBM + 2 \cdot \eta_{\mathrm{Div}} \cdot MTB} \tag{34}$$

MCST	Master-Checker-System mit Service-Abbruch bei abweichenden Ergebnissen.
$MTBT$	Mittlere Zeit zwischen MF-Behandlungen ohne Reparatur.
$MTBM$	Mittlere Zeit zwischen MF jeweils von Master und Checker.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
MTB	Mittlere Zeit für die grundlegende Fehlfunktionsbehandlung.

Fehlfunktionsrate und Zuverlässigkeit MCST

Fehlfunktionsrate nach (Gl. 1.30):

$$\zeta_{\mathrm{MT}} = \frac{(1 - MC) \cdot \zeta}{\eta_{\mathrm{DS}}} = \frac{(1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{MS}}}{1 - \zeta_{\mathrm{MS}}} \tag{35}$$

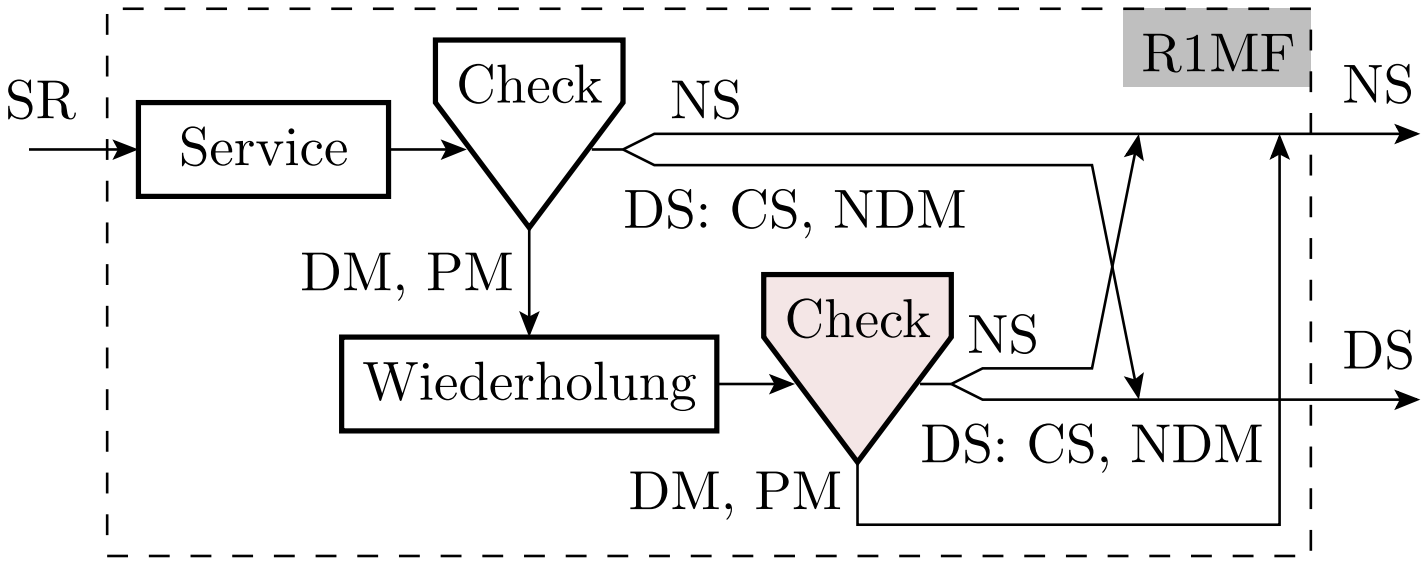
Zuverlässigkeit als Kehrwert der Fehlfunktionsrate:

$$R_{\mathrm{MT}} = \frac{1 - \zeta_{\mathrm{MS}}}{(1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{MS}}} = \frac{R_{\mathrm{MS}} - 1}{(1 - \eta_{\mathrm{Div}})} \tag{36}$$

MCST	Master-Checker-System mit Service-Abbruch bei abweichenden Ergebnissen.
ζ_{MT}	Fehlfunktionsrate nach Fehlfunktionsbehandlung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
ζ_{MS}	Übereinstimmende Fehlfunktionsrate von Master und Checker.
η_{DS}	Anteil der erbringbaren Service-Leistungen.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
ζ_{MS}	Übereinstimmende Fehlfunktionsrate von Master und Checker.
R_{MT}	Zuverlässigkeit mit Fehlfunktionsbehandlung (Reliability with malfunction treatment).
R_{MS}	Zuverlässigkeit von Master und Checker jeweils als Einzelsysteme.

Verlässl. nach Wiederholung

Ein Korrekturversuch nach MF (R1MF)



Häufigkeit einer beobachtbaren (nicht korrigierten) MF (erkannte oder Phantom-MF) bei Wiederholung nach einer beobachtbaren MF:

- bei unabhängiger Ursache (Anteil η_{Div}) gleich der Rate beobachtbarer MF, für geringe Raten praktisch null
- gleicher Ursache (Anteil $1 - \eta_{\mathrm{Div}}$) praktisch eins.

Die Rate der erbrachten SL:

$$\eta_{\mathrm{DS}} = 1 - (\zeta \cdot MC + \zeta_{\mathrm{Phan}}) \cdot (1 - \eta_{\mathrm{Div}}) \tag{37}$$

MT-Verfügbarkeit R1MF

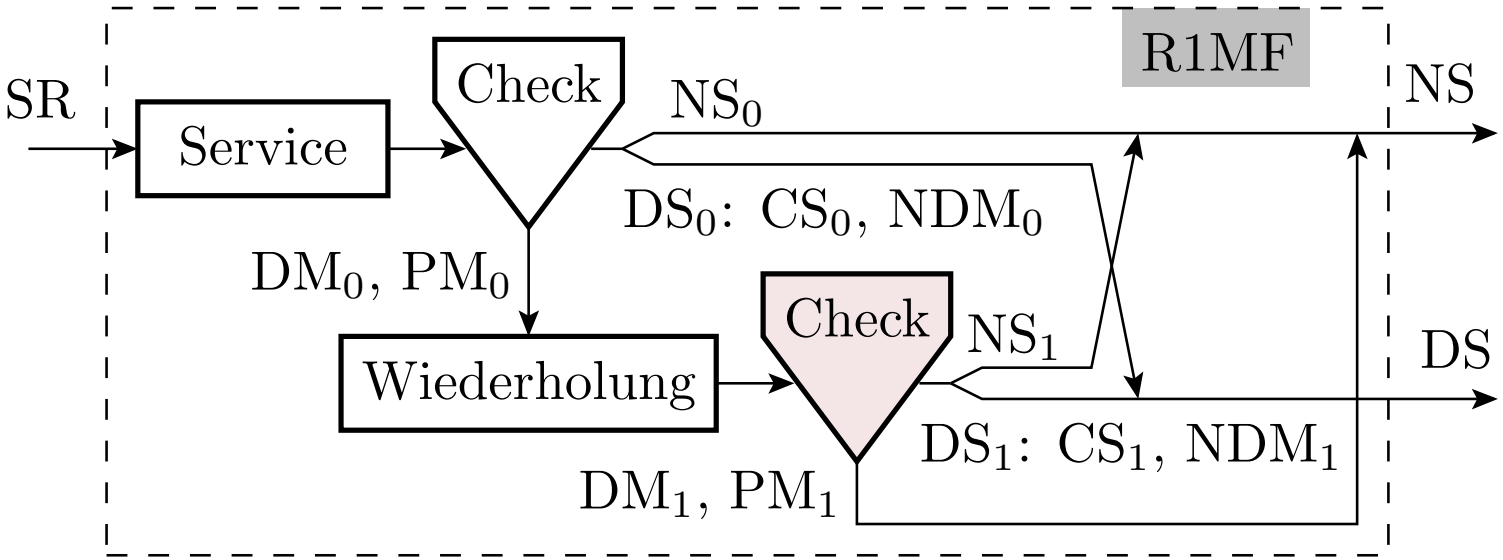
$$\eta_{\mathrm{DS}} = 1 - (\zeta \cdot MC + \zeta_{\mathrm{Phan}}) \cdot (1 - \eta_{\mathrm{Div}}) \tag{1.37}$$

MT-Verfügbarkeit nach (Gl. 1.4) bei genau einer Wiederholung für alle erkannten MF ($\mu_{\mathrm{CM}} = 1$):

$$A_{\mathrm{MT}} = \frac{MTBT}{MTBT + (MTB + MTS)} \tag{38}$$

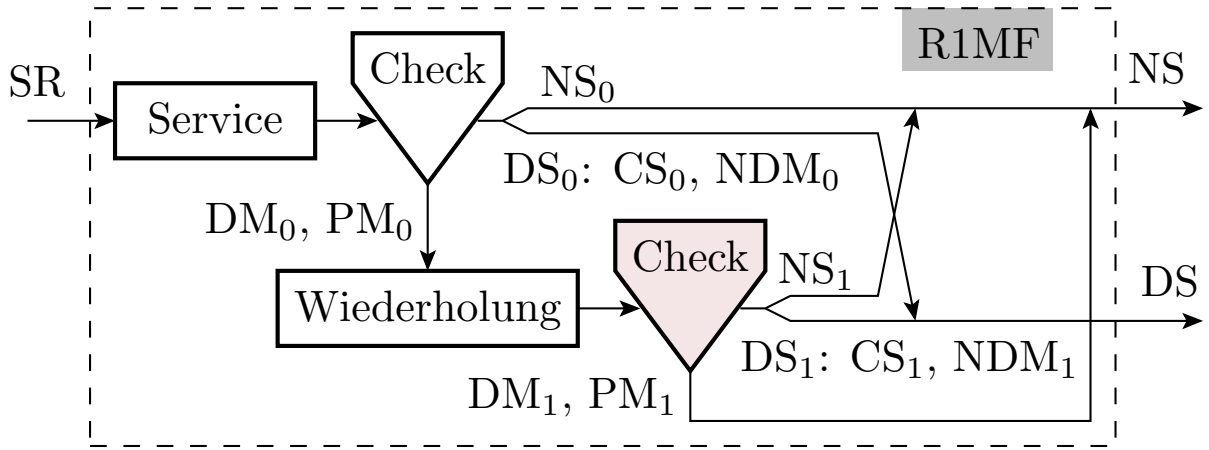
R1MF	Ein Korrekturversuch nach Fehlfunktion durch identische Wiederholung.
η_{DS}	Anteil der erbringbaren Service-Leistungen.
ζ	Fehlfunktionsrate ohne Fehlfunktionsbehandlung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
ζ_{Phan}	Phantom-Fehlfunktionsrate.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
μ_{CM}	Mittlere Anzahl der Neuberechnungen (Korrekturversuche) je MF.
A_{MT}	MT-Verfügbarkeit, Zeitanteil, den das System nicht mit MT beschäftigt ist.
$MTBT$	Mittlere Zeit zwischen MF-Behandlungen ohne Reparatur.
MTB	Mittlere Zeit für die grundlegende Fehlfunktionsbehandlung.
MTS	Mittlere Service-Dauer (Mean time to service).

MF-Rate und Zuverlässigkeit R1MF



$$\begin{aligned}
\mathrm{NDM}_0: &\quad \zeta \cdot (1 - MC) \\
\mathrm{DM}_0: &\quad \zeta \cdot MC \\
\mathrm{PM}_0: &\quad \zeta_{\mathrm{Phan}} \\
\mathrm{NDM}_1: &\quad (\zeta \cdot MC + \zeta_{\mathrm{Phan}}) \cdot \zeta \cdot \eta_{\mathrm{Div}} \cdot (1 - MC)
\end{aligned}$$

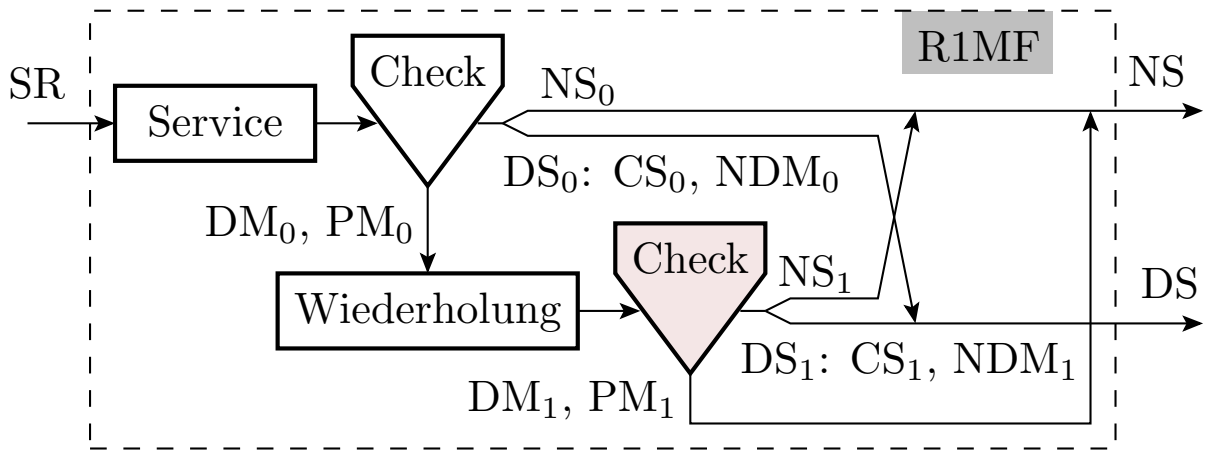
Für typ. MF-Raten nahe Null sind nicht erkennbare MF nach der ersten Wiederholung vernachlässigbar.



$$\zeta_{\mathrm{MT}} = \frac{(1-MC)\cdot\zeta}{\eta_{\mathrm{DS}}} = \frac{(1-MC)\cdot\zeta}{1-(\zeta\cdot MC+\zeta_{\mathrm{Phan}})\cdot(1-\eta_{\mathrm{Div}})} \tag{39}$$

$$R_{\mathrm{MT}} = \frac{\eta_{\mathrm{DS}}}{(1-MC)\cdot\zeta} = \frac{(1-(\zeta\cdot MC+\zeta_{\mathrm{Phan}})\cdot(1-\eta_{\mathrm{Div}}))}{(1-MC)\cdot\zeta} \tag{40}$$

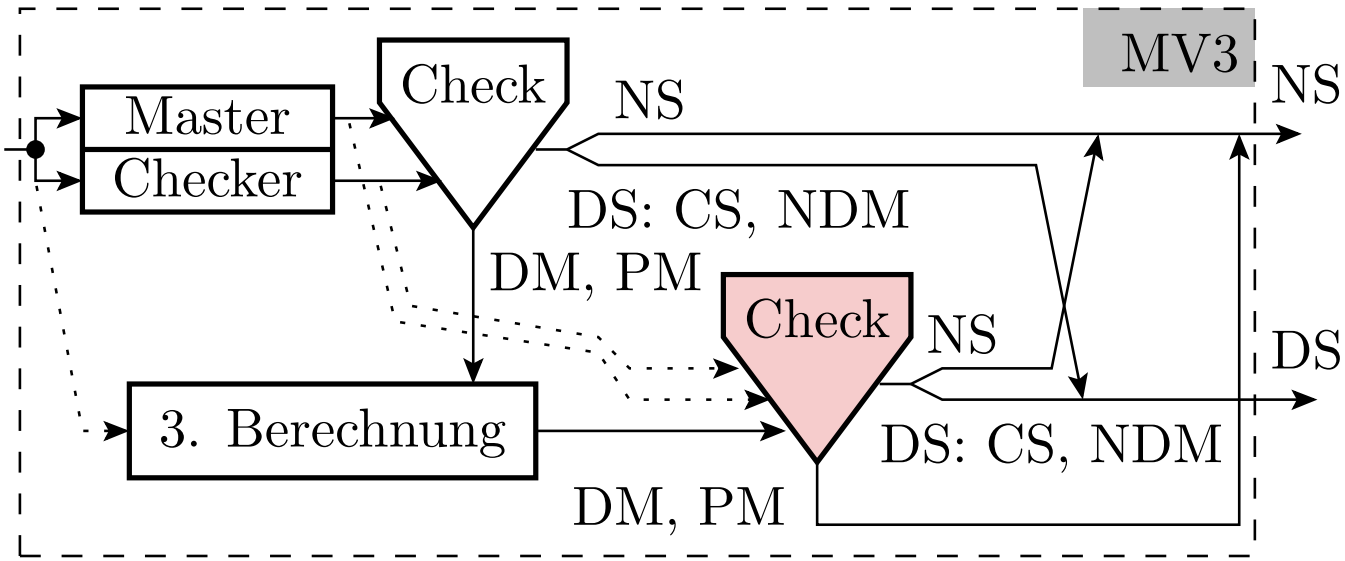
NDM	Nicht erkannte Fehlfunktion.
DM	Erkannte Fehlfunktion.
PM	Phantomfehlfunktion.
ζ	Fehlfunktionsrate ohne Fehlfunktionsbehandlung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
ζ_{Phan}	Phantom-Fehlfunktionsrate.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
ζ_{MT}	Fehlfunktionsrate nach Fehlfunktionsbehandlung.
η_{DS}	Anteil der erbringbaren Service-Leistungen.
R_{MT}	Zuverlässigkeit mit Fehlfunktionsbehandlung (Reliability with malfunction treatment).



Im Vergleich zu »Abbruch ohne Wiederholung« (Gl. 1.28) und (Gl. 1.31) liegt die Verfügbarkeit näher bei 1 und die Zuverlässigkeit näher bei

$$R_{\mathrm{MT}} = \frac{R}{1-MC} \tag{1.32}$$

3-Versionen-Mehrheitsentscheid (MV3)



- Ergebnisüberwachung mit einem Master-Checker-Paar.
- Bei einem Vergleichsfehler, Mehrheitsentscheid unter Einbeziehung einer dritten Berechnung.
- Wenn keine Mehrheit, keine Ergebnisausgabe (NS).

MV3	3-Versions-Mehrheitsentscheid.
DM, PM	Erkannte Fehlfunktion, Phantomfehlfunktion.
NDM	Nicht erkannte Fehlfunktion.
NS	Keine Service-Leistung.

Rate der erbrachten Service-Leistungen MV3

Für Master-Checker-Paare wurde auf Folie 1.62 abgeschätzt:

$$MC = \eta_{\mathrm{Div}} \tag{1.25}$$

$$\zeta_{\mathrm{Phan}} = \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}}) \tag{1.26}$$

Rate der erbrachten MF bei einer Wiederholung nach Gl. 1.37:

$$\begin{aligned} \eta_{\mathrm{DS}} &= 1 - (\zeta \cdot MC + \zeta_{\mathrm{Phan}}) \cdot (1 - \eta_{\mathrm{Div}}) \\ &= 1 - (\zeta_{\mathrm{MS}} \cdot \eta_{\mathrm{Div}} + \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}})) \cdot (1 - \eta_{\mathrm{Div}}) \\ &= 1 - \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}}) \end{aligned} \tag{41}$$

η_{DS}	Anteil der erbringbaren Service-Leistungen.
ζ	Fehlfunktionsrate ohne Fehlfunktionsbehandlung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
ζ_{Phan}	Phantom-Fehlfunktionsrate.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
ζ_{MS}	Übereinstimmende Fehlfunktionsrate von Master und Checker.

MT-Verfügbarkeit MV3

Eine MF-Behandlung erfolgt bei jeder abweichenden MF. Die mittlere Zeit zwischen beobachtbaren MS ist die Hälfte der mittleren Zeit zwischen diversitären MF des Masters (bzw. Checkers):

$$MTBT = \frac{MTBM}{2 \cdot \eta_{\mathrm{Div}}}$$

Eingesetzt in Gl. 1.38 für die Verfügbarkeit:

$$\begin{aligned} A_{\mathrm{MT}} &= \frac{MTBT}{MTBT + (MTB + MTS)} \\ &= \frac{MTBM}{MTBM + 2 \cdot \eta_{\mathrm{Div}} \cdot (MTB + MTS)} \end{aligned} \tag{42}$$

A	Verfügbarkeit (Availability).
$MTBT$	Mittlere Zeit zwischen MF-Behandlungen ohne Reparatur.
$MTBM$	Mittlere Zeit zwischen MF jeweils von Master und Checker.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
MTB	Mittlere Zeit für die grundlegende Fehlfunktionsbehandlung.
MTS	Mittlere Service-Dauer (Mean time to service).

Fehlfunktionsrate und Zuverlässigkeit MV3

Fehlfunktionsrate nach (Gl. 1.39):

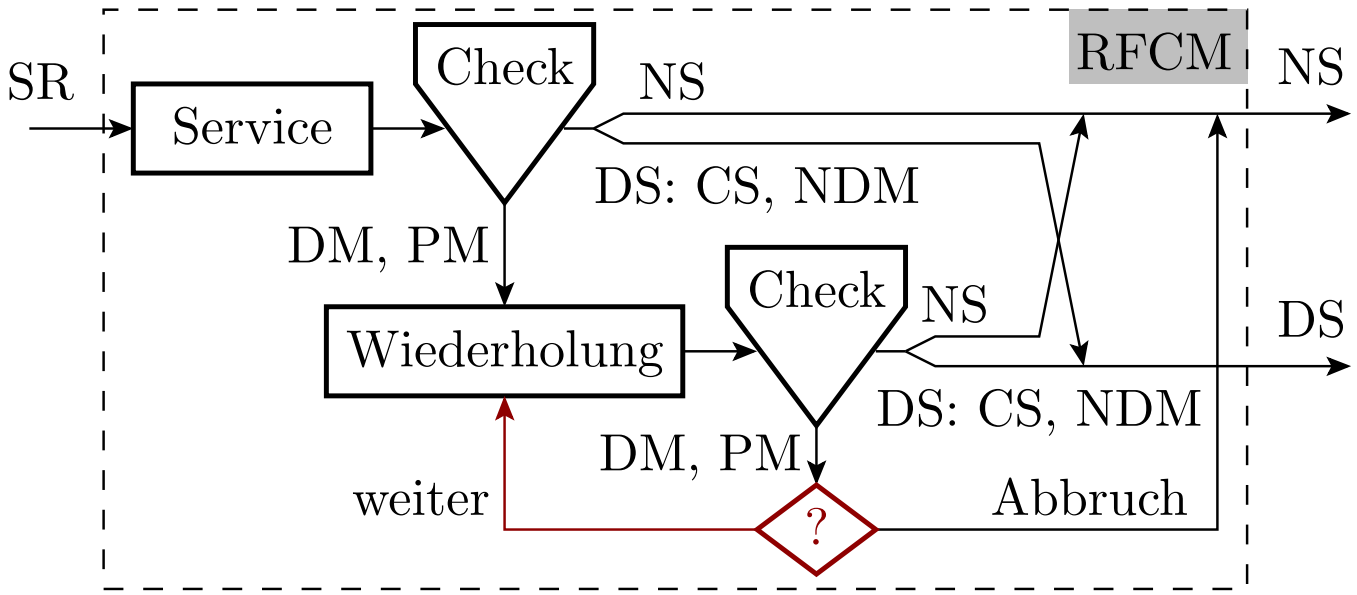
$$\zeta_{\mathrm{MT}} = \frac{(1 - MC) \cdot \zeta}{\eta_{\mathrm{DS}}} = \frac{(1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{MS}}}{1 - \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}})} \tag{43}$$

Zuverlässigkeit als Kehrwert der Fehlfunktionsrate:

$$R_{\mathrm{MT}} = \frac{1 - \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}})}{(1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{MS}}} = \frac{R_{\mathrm{MS}}}{(1 - \eta_{\mathrm{Div}})} - 1 \tag{44}$$

ζ_{MT}	Fehlfunktionsrate nach Fehlfunktionsbehandlung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
ζ	Fehlfunktionsrate ohne Fehlfunktionsbehandlung.
η_{DS}	Anteil der erbringbaren Service-Leistungen.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
ζ_{MS}	Übereinstimmende Fehlfunktionsrate von Master und Checker.
R_{MT}	Zuverlässigkeit mit Fehlfunktionsbehandlung (Reliability with malfunction treatment).
R_{MS}	Zuverlässigkeit von Master und Checker jeweils als Einzelsysteme.

Wiederholung bis Abbruchkriterium (RFCM)



Zweckmäßige Abbruchkriterien:

- keine erkennbare Fehlfunktion mehr,
- bei Wiederholung identische Fehlfunktion oder
- max. Wiederholzahl erreicht.

Anwendung:

- stark gestörte Datenübertragung mit Prüfkennzeichen.
- Erraten von Lösungen und Kontrolle mit Korrektheitskriterium.

Rate der erbrachten Service-Leistungen RFCM

Bei Wiederholung, bis alle diversitären Fehlfunktionen beseitigt und $\zeta_{\mathrm{Phan}} = 0$, werden alle Service-Leistungen bis auf die mit nicht diversitären erkennbaren MF erbracht:

$$\eta_{\mathrm{DS}} = 1 - \zeta \cdot MC \cdot (1 - \eta_{\mathrm{Div}})$$

RFCM	Identische Wiederholung nach Fehlfunktion, solange sich die Verfälschung ändert.
ζ_{Phan}	Phantom-Fehlfunktionsrate.
η_{DS}	Anteil der erbringbaren Service-Leistungen.
ζ	Fehlfunktionsrate ohne Fehlfunktionsbehandlung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.

Mittler Anzahl der Wiederholungen RFCM

Wiederholungshäufigkeit diversitärer MF für $\zeta_{\mathrm{Phan}} = 0$:

	Häufigkeit
Service-Ausführung	$h_0 = 1$
1. Wiederholung	$h_1 = h_0 \cdot \zeta \cdot MC$
2. Wiederholung	$h_2 = h_1 \cdot \zeta \cdot \eta_{\mathrm{Div}} \cdot MC$
n-te Wiederholung	$h_n = h_{n-1} \cdot \zeta \cdot \eta_{\mathrm{Div}} \cdot MC$

Mittlere Anzahl bis keine MF mehr zu erkennen ist:

$$\mu_{\mathrm{CM}} = \sum_{i=1}^{\infty} (\zeta \cdot \eta_{\mathrm{Div}} \cdot MC)^i + \underbrace{\zeta \cdot (1 - \eta_{\mathrm{Div}}) \cdot MC}_{\text{ein Wiederholung für erkennbare CC-MF}^{(*)}}$$

$$=^{(**)} \frac{1}{1 - \zeta \cdot \eta_{\mathrm{Div}} \cdot MC} - 1 \tag{45}$$

RFCM	Identische Wiederholung nach Fehlfunktion, solange sich die Verfälschung ändert.
h_i	Relative Häufigkeit einer i-ten Wiederholung.
μ_{CM}	Mittlere Anzahl der Neuberechnungen (Korrekturversuche) je MF.
*	In den weiteren Überschlägen vernachlässigt.
**	Summe einer geometrischen Reihe: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

Fehlfunktionsrate RFCM

Nicht erkennbare Fehlfunktionen entstehen:

- bei einem Versuch, eine nicht diversitären MF und
- bei im Mittel $(\mu_{\mathrm{CM}} + 1)$ Versuchen eine diversitäre MF

»unbemerkt durch den Test zu schleusen«:

$$\zeta_{\mathrm{MT}} = \frac{1}{\eta_{\mathrm{DS}}} \left(\underbrace{\zeta \cdot (1 - \eta_{\mathrm{Div}}) \cdot (1 - MC)}_{\text{Häuf. nicht erk. identische MF}} + \underbrace{(\mu_{\mathrm{CM}} + 1) \cdot \zeta \cdot \eta_{\mathrm{Div}} \cdot (1 - MC)}_{\text{Häuf. nicht erk. diversitärer MF}} \right)$$

Wiederholung bis Abbruchkriterium lohnt nur, wenn MF-Rate, Diversität und die Fehlfunktionsüberdeckung groß sind.

ζ_{MT}	Fehlfunktionsrate nach Fehlfunktionsbehandlung.
η_{DS}	Anteil der erbringbaren Service-Leistungen.
ζ	Fehlfunktionsrate ohne Fehlfunktionsbehandlung.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
μ_{CM}	Mittlere Anzahl der Neuberechnungen (Korrekturversuche) je MF.

Unabhängige Verfälschungen RFCM

Für komplett unabhängige Verfälschungen ($\eta_{\mathrm{Div}} = 1$) ohne Phantom-MF, hohe MF-Rate und Fehlfunktionsüberdeckung, typisch für

- stark gestörte Datenübertragung mit Prüfkennzeichen.
- Erraten von Lösungen und Kontrolle mit Korrektheitskriterium:

$$\mu_{\mathrm{CM}} = \frac{1}{1 - \zeta \cdot MC} - 1 \tag{46}$$

$$\zeta_{\mathrm{MT}} = (\mu_{\mathrm{CM}} + 1) \cdot \zeta \cdot (1 - MC) = \frac{\zeta \cdot (1 - MC)}{1 - \zeta \cdot MC} \tag{47}$$

$$R_{\mathrm{MT}} = \frac{(1 - \zeta \cdot MC)}{\zeta \cdot (1 - MC)} = \frac{R \cdot (1 - {}^{MC}/_{R})}{1 - MC} \tag{48}$$

Für Rate der erkennbaren MF $\zeta \cdot MC \to 1$ streben $\mu_{\mathrm{CM}} \to \infty$, $\zeta_{\mathrm{MT}} \to \infty$ und $R_{\mathrm{MT}} \to 1$.

η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechung.
μ_{CM}	Mittlere Anzahl der Neuberechnungen (Korrekturversuche) je MF.
ζ	Fehlfunktionsrate ohne Fehlfunktionsbehandlung.
MC	Fehlfunktionsüberdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
ζ_{MT}	Fehlfunktionsrate nach Fehlfunktionsbehandlung.
R_{MT}	Zuverlässigkeit mit Fehlfunktionsbehandlung (Reliability with malfunction treatment).

Sicherheitverbesserung

Umgang mit nicht erbringbaren SL

Abbruch nach erkannten MF setzt voraus, dass von nicht erbrachten SL kein erhebliches Schadensrisiko ausgeht:

- Betriebssicherheit: Schaden für System, Personen, Umwelt,
- Zugangssicherheit: unberechtigter Zugang,
- Datensicherheit: Verlust schwer wiederbeschaffbarer Daten, ...

Das kann Zusatzmaßnahmen erfordern:

- Systeme ohne einen in kurzer Zeit erreichbaren sicheren Zustand, z. B.: Flugzeugsteuerungen, Atomkraftwerke, Chemiereaktoren benötigen Redundanzen für die Übernahme sicherheitskritischer Service-Leistungen (siehe Folie 4.179 *Nutzung von Redundanzen in der Praxis*).
- Beim Verlassen der zulässigen Bereiche von Sensor- und Stellwerten, Anpassung der Regelung so an den aktuellen Fehlerzustand, dass eine Mindestfunktionalität gewährleistet bleibt (siehe Folie 4.190 *Fehlertolerantes Regelungssystem*).
- ...

Sicherheitsverbesserung

Wenn von nicht erbrachten MF keine Gefahr ausgeht, erhöht Fehlfunktionsbehandlung ohne zusätzliche Sicherheitsfunktionen die Sicherheit proportional mit der Zuverlässigkeit (Gl. 1.19):

$$S_{\mathrm{MT}} = \frac{R_{\mathrm{MT}}}{\eta_{\mathrm{SE}}} \tag{49}$$

Eine Verringerung des Anteils der sicherheitskritischen MF von η_{SE} auf einen geringeren Wert $\eta_{\mathrm{SESF}} < \eta_{\mathrm{SE}}$ verlangt in der Regel zusätzliche Sicherheitsfunktionen, die die MF-Rate erhöhen und die Zuverlässigkeit auf einen Anteil $\eta_{\mathrm{RSF}} < 1$ verringern. Sicherheit insgesamt:

$$S_{\mathrm{MTSF}} = \frac{R_{\mathrm{MT}} \cdot \eta_{\mathrm{RSF}}}{\eta_{\mathrm{SESF}}} \tag{50}$$

$$\eta_{\mathrm{RSF}} = \frac{\frac{1}{R_{\mathrm{MT}}}}{\frac{1}{R_{\mathrm{MT}}} + \frac{1}{R_{\mathrm{SF}}}} = \frac{R_{\mathrm{SF}}}{R_{\mathrm{MT}} + R_{\mathrm{SF}}} \tag{51}$$

S_{MT}	Sicherheit mit Fehlfunktionsbehandlung.
η_{RSF}	Zuverlässigkeitsverringerung durch MF der zusätzliche Sicherheitsfunktionen.
S_{MTSF}	Sicherheit mit Fehlfunktionsbehandlung und zusätzlichen Sicherheitsfunktionen.
η_{SE}	Anteil der sicherheitsgefährdenden Fehlfunktionen.
η_{SESF}	Verringerter Anteil sicherheitsgefährdender MF mit Sicherheitsfunktionen.

Beispiel 1.3: Sicherheit durch Zusatzsteuergerät

Eine Fahrzeug habe eine mittlere Zeit zwischen MF von $1000\,\mathrm{h}$. *Der Anteil der betriebssicherheitsgefährdenden MF sei* 1% *und die mittlere Service-Dauer (mittlere Fahrtdauer) betrage* $1\,\mathrm{h}$. *Ein zusätzliches elektronisches Steuergerät mit Zuverlässigkeit* R_{SF} *verringert den Anteil der gefährdenden MF auf* $10^{-3}\ \left[\frac{\mathrm{HM}}{\mathrm{MF}}\right]$.

$$MTBM = 1000\,\mathrm{h},\ \eta_{\mathrm{SE}} = 1\%,\ MTS = 1\,\mathrm{h},\ \eta_{\mathrm{SESF}} = 10^{-3}\ \left[\frac{\mathrm{HM}}{\mathrm{MF}}\right]$$

a) *Wie groß sind die Zuverlässigkeit und die Sicherheit des Systems ohne das zusätzliche Steuergerät?*

b) *Wie hoch muss die Zuverlässigkeit des Steuergeräts* R_{SF} *mindestens sein, damit das zusätzliche Steuergerät die Sicherheit des Gesamtsystems mindestens verfünffacht (*$S_{\mathrm{MTSF}} \geq 5 \cdot S_{\mathrm{MT}}$*)?*

$MTBM$	Mittlere Nutzungsdauer zwischen Fehlfunktion (Mean service life between malfunctions).
MTS	Mittlere Service-Dauer (Mean time to service).
η_{SE}	Anteil der sicherheitsgefährdenden Fehlfunktionen.
η_{SESF}	Verringerter Anteil sicherheitsgefährdender MF mit Sicherheitsfunktionen.

$MTBM = 1000\,\mathrm{h}$, $\eta_{\mathrm{SE}} = 1\%$, $MTS = 1\,\mathrm{h}$, $\eta_{\mathrm{SESF}} = 10^{-3}\ \left[\frac{\mathrm{HM}}{\mathrm{MF}}\right]$

a) *Wie groß sind die Zuverlässigkeit und die Sicherheit des Systems ohne das zusätzliche Steuergerät?*

$$R = \frac{MTBM}{MTS} \tag{1.10}$$

$$S_{\mathrm{MT}} = \frac{R_{\mathrm{MT}}}{\eta_{\mathrm{SE}}} \tag{1.49}$$

Zuverlässigkeit mit Fehlfunktionsbehandlung genau wie ohne, wenn die $MTBF$ die mit MF-Behandlung ist:

$$R_{\mathrm{MT}} = \frac{MTBM}{MTS} = \frac{10^3\,\mathrm{h}}{1\mathrm{h}} = 10^3\ \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$$

Betriebssicherheit ohne zusätzliches Steuergerät:

$$S_{\mathrm{MT}} = 10^3\ \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right] / 1\%\ \left[\frac{\mathrm{HM}}{\mathrm{MF}}\right] = 10^5\ \left[\frac{\mathrm{DS}}{\mathrm{HM}}\right]$$

R	Zuverlässigkeit (reliability) ohne Fehlfunktionsbehandlung.
R_{MT}	Zuverlässigkeit mit Fehlfunktionsbehandlung (Reliability with malfunction treatment).
S_{MT}	Sicherheit mit Fehlfunktionsbehandlung.
$\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$	Zählwertverhältnis in erbrachten Service-Leistungen je Fehlfunktion.
$\left[\frac{\mathrm{DS}}{\mathrm{HM}}\right]$	Verhältnis in erbrachten Service-Leistungen je sicherheitsgefährdende Fehlfunktion.

$MTBM = 1000\,\mathrm{h}$, $\eta_{\mathrm{SE}} = 1\%$, $MTS = 1\,\mathrm{h}$, $\eta_{\mathrm{SESF}} = 10^{-3}\ \left[\frac{\mathrm{HM}}{\mathrm{MF}}\right]$

b) *Wie hoch muss die Zuverlässigkeit des Steuergeräts R_{SF} mindestens sein, damit das zusätzliche Steuergerät die Sicherheit des Gesamtsystems mindestens verfünffacht ($S_{\mathrm{MTSF}} \geq 5 \cdot S_{\mathrm{MT}}$)?*

$$S_{\mathrm{MT}} = \frac{R_{\mathrm{MT}}}{\eta_{\mathrm{SE}}} \tag{1.49}$$

$$S_{\mathrm{MTSF}} = \frac{R_{\mathrm{MT}} \cdot \eta_{\mathrm{RSF}}}{\eta_{\mathrm{SESF}}} \tag{1.50}$$

$$\eta_{\mathrm{RSF}} = \frac{R_{\mathrm{SF}}}{R_{\mathrm{MT}} + R_{\mathrm{SF}}} \tag{1.51}$$

Maximale Zuverlässigkeitsverringerung durch das Steuergerät:

$$5 \leq \frac{S_{\mathrm{MTSF}}}{S_{\mathrm{MT}}} = \frac{\frac{R_{\mathrm{MT}} \cdot \eta_{\mathrm{RSF}}}{\eta_{\mathrm{SESF}}}}{\frac{R_{\mathrm{MT}}}{\eta_{\mathrm{SE}}}} = \frac{\eta_{\mathrm{RSF}} \cdot \eta_{\mathrm{SE}}}{\eta_{\mathrm{SESF}}}$$

$$\eta_{\mathrm{RSF}} \geq \frac{5 \cdot \eta_{\mathrm{SESF}} \cdot}{\eta_{\mathrm{SE}} \cdot} = \frac{5 \cdot 10^{-3}}{10^{-2}} = 0{,}5$$

Das zusätzliche Steuergerät darf die Zuverlässigkeit des Gesamtsystems nicht weniger als halbieren.

$MTBM = 1000\,\mathrm{h}$, $\eta_{\mathrm{SE}} = 1\%$, $MTS = 1\,\mathrm{h}$, $\eta_{\mathrm{SESF}} = 10^{-3}$ $\left[\frac{\mathrm{HM}}{\mathrm{MF}}\right]$

b) *Wie hoch muss die Zuverlässigkeit des Steuergeräts R_{SF} mindestens sein, damit das zusätzliche Steuergerät die Sicherheit des Gesamtsystems mindestens verfünffacht ($S_{\mathrm{MTSF}} \geq 5 \cdot S_{\mathrm{MT}}$)?*

... $\eta_{\mathrm{RSF}} \geq 0{,}5$.

$$\frac{R_{\mathrm{SF}}}{R_{\mathrm{MT}} + R_{\mathrm{SF}}} \geq 0{,}5; \quad R_{\mathrm{SF}} \geqq R_{\mathrm{MT}}$$

Das zusätzliche Steuergerät zur Sicherheitserhöhung muss mindestens so zuverlässig wie das Fahrzeug mit der sonstigen MF-Behandlung sein.

Alternativ zu aktuellen Ethik-Diskussionen, ob autonome Fahrzeuge Kinder, Rentner, ... überfahren sollen, Einfordern der vielfachen Sicherheit gegenüber fahrergesteuerten Fahrzeugen + Haftpflicht für Fahrzeuge.

S_{MTSF}	Sicherheit mit Fehlfunktionsbehandlung und zusätzlichen Sicherheitsfunktionen.
η_{RSF}	Zuverlässigkeitsverringerung durch MF der zusätzliche Sicherheitsfunktionen.
R_{SF}	Zuverlässigkeit der zusätzlichen Sicherheitsfunktionen.

Zusammenfassung

Kenngrößen der Überwachung

- Fehlfunktionsüberdeckung und Phantom-MF-Rate allgemein:

$$MC = \frac{\#DM}{\#MF}\Big|_{\mathrm{ACR}} \tag{1.20}$$

$$\zeta_{\mathrm{Phan}} = \frac{\#PM}{\#DS}\Big|_{\mathrm{ACR}} \tag{1.21}$$

- Unterteilung der Kontrollverfahren in Format- und Wertekontrollen.

Formatkontrollen:

- Gleichmäßiger Abbildung von MF auf zulässige und unzulässige Werte und r redundante Bits (fehlererkennende Codes und Prüfkennzeichen):

$$MC \geq 1 - 2^{-r} \tag{1.24}$$

- keine Phantomfehlfunktionen.
- Bildung fehlererkennender Codes und Prüfkennzeichen sowie weitere Formatkontrollen (z.B. Syntax, Wertebereich, ...) werden später in Absch. 4.3 behandelt.

Verfahren zur Wertekontrolle:,

- Master-Checker als universelles Verfahren:

$$MC = \eta_{\mathrm{Div}} \tag{1.25}$$

$$\zeta_{\mathrm{Phan}} = \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}}) \tag{1.26}$$

$$\eta_{\mathrm{Div}} = 1 - \eta_{\mathrm{F}} \cdot \eta_{\mathrm{CF}} \tag{1.27}$$

  Nachweis aller MF durch Störungen und mit diversitären Entwürfen bis zu 90% der MF durch Fehler.
- Loop-Test: höhere zu erwartende MC und weniger PM als Master-Checker, aber nur für umkehrbar eindeutige Funktionen einsetzbar.
- Korrektheitstests: auch oft gute MC, aber auch für die meisten Anwendungen nicht einsetzbar.

Meist werden im laufenden Betrieb nur Formateigenschaften überwacht.

Reaktion auf erkannte MF

- Robuste Reaktion, um Schaden durch MF zu vermeiden.
- Protokollierung der MF zur Unterstützung der Fehlerbeseitigung.
- Wiederherstellung Funktionsfähigkeit:
  - nach Ausfall: Reparatur oder Rekonfiguration,
  - praktisch immer Neuinitialisierung (statisch, dynamisch).
- Umgang mit erkannten Fehlfunktionen
  - Service-Abbruch nach Fehlfunktion (STMF)
  - max. eine identische Wiederholung (R1MF)
  - Identische Wiederholung solange sich Verfälschung erkennbar und sich ändert (RFCM)
  - diversitäre Wiederholung mit einem diversitären Reservesystem oder Fehlerumgehung mit diversitären Service-Anforderungen.
  - Fehlererkennende Codes (EEC) als Speziallösung für die Datenübertragung und -speicherung.

Vermeidung schwer handhabarer und gefährlicher MF z.B. durch:

- Ruhestromprinzip, Fehlerisolation,
- Brandmauern, ...

Verlässlichkeit bei Abbruch nach MF (STMF)

Allgemein:

$$A_{\mathrm{MT}} = \frac{MTBT}{MTBT+MTB} \tag{1.28}$$

$$\eta_{\mathrm{DS}} = 1 - (\zeta \cdot MC + \zeta_{\mathrm{Phan}}) \tag{1.29}$$

$$\zeta_{\mathrm{MT}} = \frac{(1-MC)\cdot\zeta}{1-(\zeta\cdot MC+\zeta_{\mathrm{Phan}})} \tag{1.30}$$

$$R_{\mathrm{MT}} = \frac{1-(\zeta\cdot MC+\zeta_{\mathrm{Phan}})}{(1-MC)\cdot\zeta} \tag{1.31}$$

Für $\zeta \ll 1$ und $\zeta_{\mathrm{Phan}} \ll 1$:

$$R_{\mathrm{MT}} = \frac{R}{1-MC} \tag{1.32}$$

Master-Check-System (Verdopplung und Vergleich):

$$\eta_{\mathrm{DS}} = 1 - \zeta \tag{1.33}$$

$$A_{\mathrm{MT}} = \frac{MTBM}{MTBM+2\cdot\eta_{\mathrm{Div}}\cdot MTB} \tag{1.34}$$

$$\zeta_{\mathrm{MT}} = \frac{(1-\eta_{\mathrm{Div}})\cdot\zeta}{1-\zeta} \tag{1.35}$$

$$R_{\mathrm{MT}} = \frac{R_{\mathrm{MS}}-1}{(1-\eta_{\mathrm{Div}})} \tag{1.36}$$

Verlässlichkeit bei Wiederholung nach MF

Verfügbarkeit und Zuverlässigkeit nach max. einer Wiederholung (R1MF):

$$\eta_{\mathrm{DS}} = 1 - (\zeta \cdot MC + \zeta_{\mathrm{Phan}}) \cdot (1 - \eta_{\mathrm{Div}}) \tag{1.37}$$

$$A_{\mathrm{MT}} = \frac{MTBT}{MTBT+(MTB+MTS)} \tag{1.38}$$

$$\zeta_{\mathrm{MT}} = \frac{(1-MC)\cdot\zeta}{1-(\zeta\cdot MC+\zeta_{\mathrm{Phan}})\cdot(1-\eta_{\mathrm{Div}})} \tag{1.39}$$

$$R_{\mathrm{MT}} = \frac{(1-(\zeta\cdot MC+\zeta_{\mathrm{Phan}})\cdot(1-\eta_{\mathrm{Div}}))}{(1-MC)\cdot\zeta} \tag{1.40}$$

3-Versionen-Mehrheitsentscheid (Master-Checker-System mit einer Wiederholung nach MF):

$$\eta_{\mathrm{DS}} = 1 - \zeta_{\mathrm{MS}} \cdot (1 - \eta_{\mathrm{Div}}) \tag{1.41}$$

$$A_{\mathrm{MT}} = \frac{MTBM}{MTBM+2\cdot\eta_{\mathrm{Div}}\cdot(MTB+MTS)} \tag{1.42}$$

$$\zeta_{\mathrm{MT}} = \frac{(1-\eta_{\mathrm{Div}})\cdot\zeta_{\mathrm{MS}}}{1-\zeta_{\mathrm{MS}}\cdot(1-\eta_{\mathrm{Div}})} \tag{1.43}$$

$$R_{\mathrm{MT}} = \frac{R_{\mathrm{MS}}}{(1-\eta_{\mathrm{Div}})} - 1 \tag{1.44}$$

Mehrfachwiederholung nach MF

Wiederholung, solange eine Fehlfunktion erkennbar ist und sich das falsche Ergebnis ändert, keine Phantom-MF $(\zeta_{\mathrm{Phan}} = 0)$ beträgt die mittlere Anzahl der Wiederholungen:

$$\mu_{\mathrm{CM}} = \frac{1}{1-\zeta\cdot\eta_{\mathrm{Div}}\cdot MC} - 1 \tag{1.45}$$

Für den praktisch interessanten Sonderfall, hohe Rate unabhängiger Fehlfunktionen $(\eta_{\mathrm{Div}} = 1)$:

$$\mu_{\mathrm{CM}} = \frac{1}{1-\zeta\cdot MC} - 1 \tag{1.46}$$

$$\zeta_{\mathrm{MT}} = \frac{\zeta\cdot(1-MC)}{1-\zeta\cdot MC} \tag{1.47}$$

$$R_{\mathrm{MT}} = \frac{R\cdot\left(1-\frac{MC}{R}\right)}{1-MC} \tag{1.48}$$

Sicherheit von Systemen mit MF-Behandlung

Umgang mit nicht erbringbaren SL:

- System so gestalten, dass nicht erbrachte Service-Leistungen die Sicherheit nicht gefährden oder
- Redundanzen, die bei Nichterbringung die sicherheitskritischen Service-Leistungen übernehmen.

Sicherheitsverbesserung

- ohne zusätzliche Sicherheitsfunktionen:

$$S_{\mathrm{MT}} = \frac{R_{\mathrm{MT}}}{\eta_{\mathrm{SE}}} \tag{1.49}$$

- mit zusätzlichen Sicherheitsfunktionen:

$$S_{\mathrm{MTSF}} = \frac{R_{\mathrm{MT}} \cdot \eta_{\mathrm{RSF}}}{\eta_{\mathrm{SESF}}} \tag{1.50}$$

$$\eta_{\mathrm{RSF}} = \frac{R_{\mathrm{SF}}}{R_{\mathrm{MT}} + R_{\mathrm{SF}}} \tag{1.51}$$

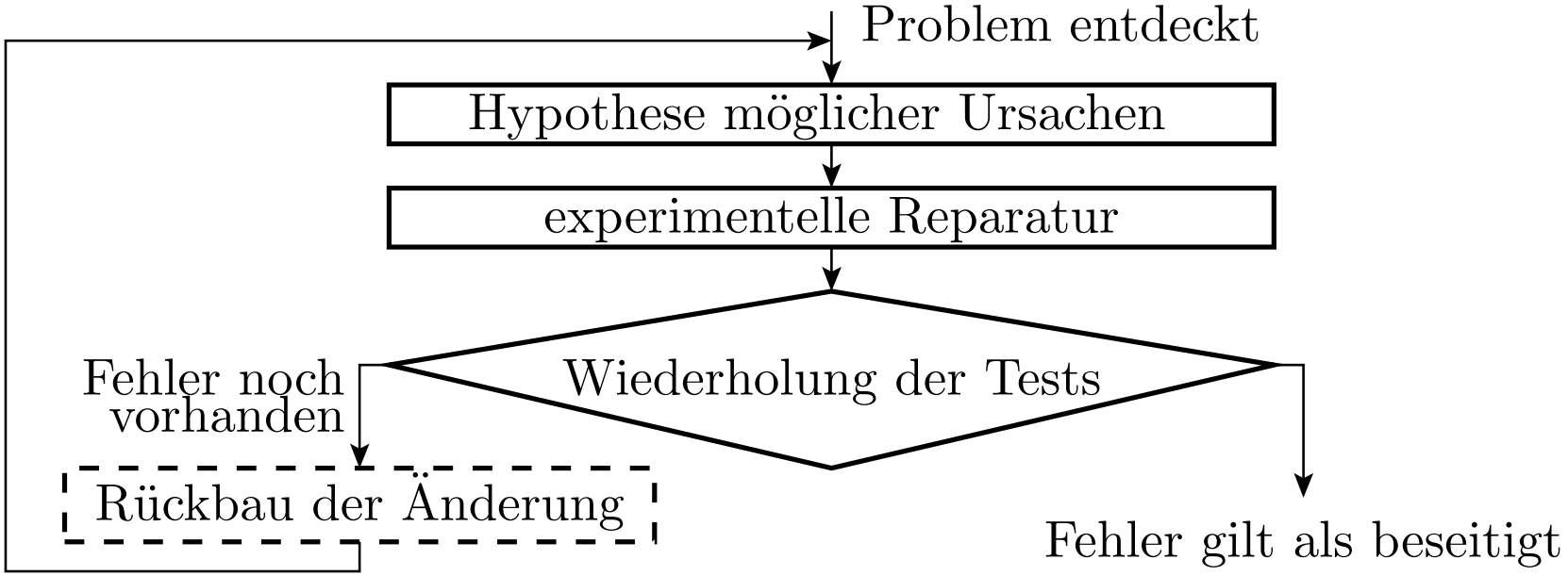
Fehlerbeseitigung

Wiederholung: Ursachen für Fehlfunktionen

- Störungen:
  - Zufällige, nicht reproduzierbare Ursache-Wirkungs-Beziehungen,
  - Gefährdungsabwendung: Überwachung und Fehlfunktionsbehandlung, in der Regel Korrektur durch identische Wiederholung.
- Fehler:
  - Entstehen mit dem System oder bei der Fehlerbeseitigung,
  - Gefährdungsabwendung: *Fehlerbeseitigung*, Fehlervermeidung.
- Ausfälle:
  - während des Betriebs entstehende Fehler,
  - Gefährdungsabwendung durch Fehlfunktionsbehandlung, Wartungstest und Redundanzen (siehe später Abschn. 4.3).

Beseitigungsiteration

Experimentelle Reparatur

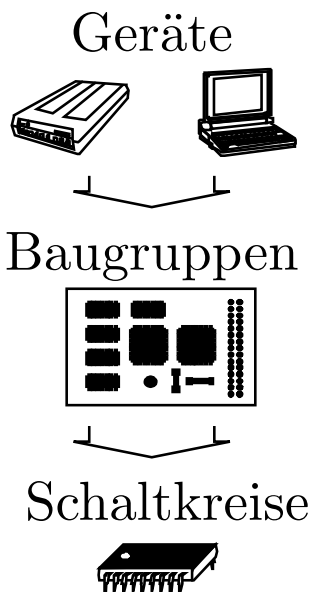


- Iteration aus Beseitigungsversuchen für hypothetische Fehler und Erfolgskontrolle durch Testwiederholung.
- Beseitigt alle vom Test nachweisbaren Fehler.
- Zur Minderung der Rate der neu entstehenden Fehler je beseitigter Fehler Rückbau nach erfolglosen Reparaturversuchen.

Reparatur bei wenig tauschbaren Komponenten

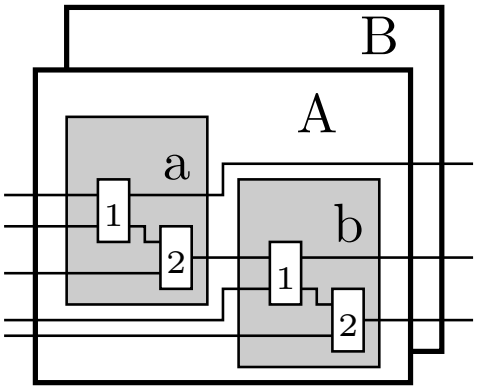
Ein reparaturgerechtes System hat eine hierarchische Struktur aus tauschbaren Komponenten, z.B.

1. Ebene: Austauschbare Geräte.
2. Ebene: Austauschbare Baugruppen.
3. Ebene: Austauschbare Schaltkreise.

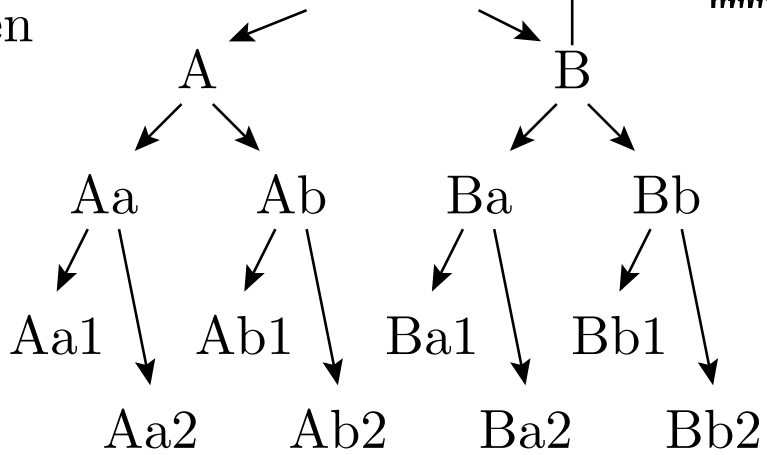


Fehlerlokalisierung durch systematisches Tauschen:

hierarchisches System mit tauschbaren Komponenten



Tauschbaum



Übliches Vorgehen eines Reperateurs

- Grobabschätzung, welches Rechnerteil defekt sein könnte aus den Fehlersymptomen.
- Kontrolle der Steckverbinder auf Kontaktprobleme durch Abziehen, Reinigen, Zusammenstecken, Testwiederholung.
- Ersatz möglicherweise defekter Teile durch Ersatzteile, Testwiederholung, ...

Voraussetzungen:

- Wiederholbare Tests, die den Fehler nachweisen.
- Ausreichend Ersatzteile. Allgemeine Mechnikerkenntnisse*.

Ist der Rücktausch nach erfolglosem Ersatzteileinbau notwendig? Wenn ja, warum?

Günstig ist der Tausch der Hälfte, von der fehlerhaften Hälfte auch die Hälfte, ... Warum?

* Verständnis der kompletten Funktion des zu reparierenden Systems ist nicht zwingend.

Fehlerdiagnose & -isolation

Fehlerdiagnose

Abschätzung von Ort-, Ursache und Beseitigungsmöglichkeiten von Fehlern aus Testergebnissen zur Minderung:

- der Anzahl der Reparaturversuche,
- des Bedarf an Ersatzteilen,
- der Anzahl der bei Reparaturversuchen entstehenden Fehler
- inc. der, die nicht durch Rückbau beseitigt werden.

Allgemeine Diagnosetechniken:

- erfolgsorientiertes Tauschen und
- Rückverfolgung von Verfälschungen entgegen dem Daten- oder Berechnungfluss.

Die Alternative zur Fehlerdiagnose ist eine Blindfehlersuche, d.h. zufälliges Erraten der MF-Ursachen und ihrer Beseitigungsmöglichkeiten:

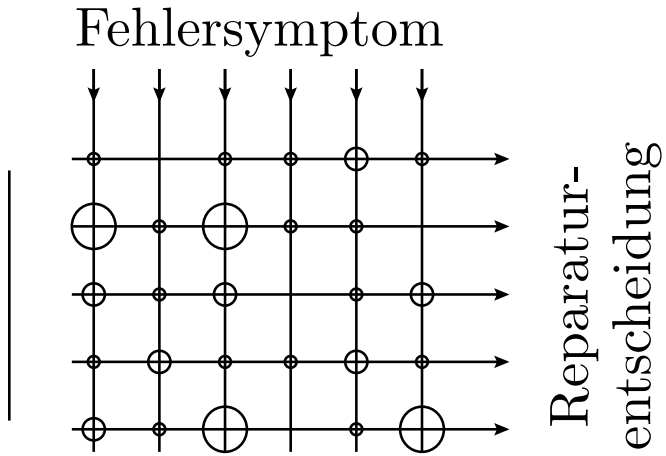
- bei Systemen ohne Möglichkeit für systematisches Tauschen, z.B. SW und HW-Entwürfe Erfolgschancen gering, aber
- bei fehlenden Dokus oder Systemverständnis einzige Möglichkeit.

Erfolgsorientiertes Tauschen

Produkte haben Schwachstellen. Die meisten Probleme geht auf einen kleinen Anteil der möglichen Ursachen zurück, Pareto-Prinzip*:

- Zählen der Erfolge unterschiedlicher Reparaturalternativen.
- Bei Reparatur, Beginn mit der erfolgsversprechendsten Möglichkeit.

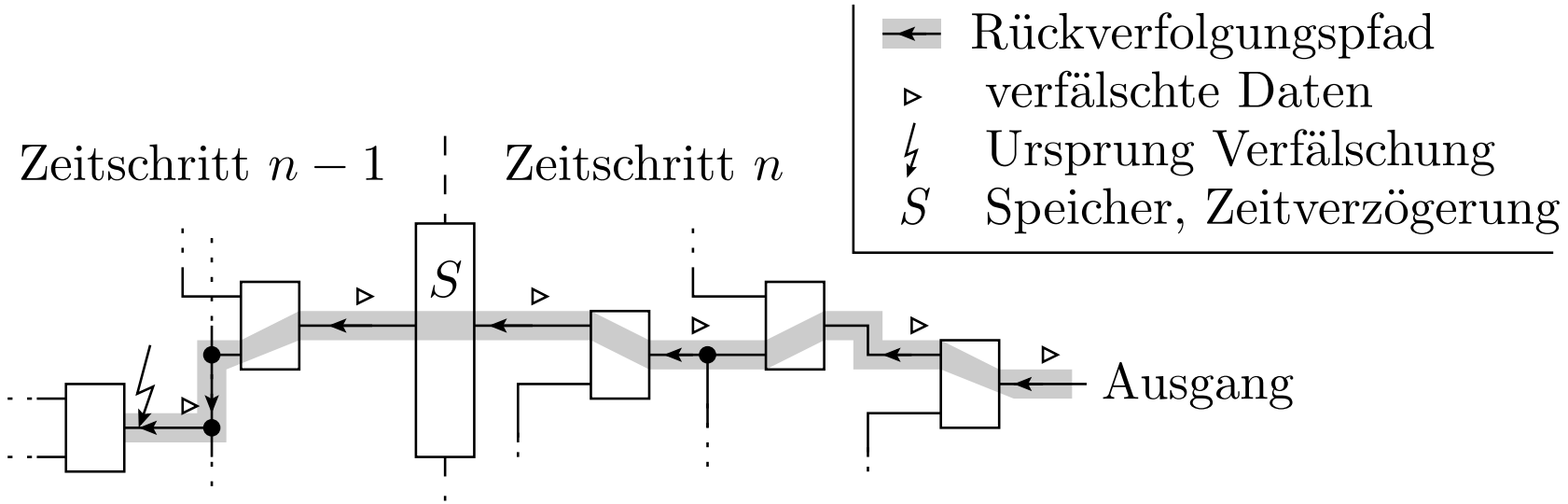
◎ Häufigkeit, mit der die Reparaturentscheidung für das Symstem bisher erfolgreich war



Nach erfolglosen Reparaturversuchen Rückbau der Änderung zur Minderung der Fehlerentstehungsrate bei der Reparatur.

* Der italienische Ökonom Vilfredo Pareto untersuchte 1906 die Verteilung des Grundbesitzes in Italien und fand heraus, dass ca. 20% der Bevölkerung ca. 80% des Bodens besitzen. Das ist in den Sprachgebrauch als Pareto-20%-80%-Regel eingegangen.

Rückverfolgung von Datenverfälschungen



Ausgehend von einer erkannten falschen Ausgabe Rückverfolgung entgegen Berechnungs- bzw. Signalfluss bis zu der Komponente, die richtige Eingaben auf verfälschte Ausgaben abbildet, gegebenenfalls über Zeitschritte und/oder hierarchisch absteigend.

Quelle der Verfälschung kann außer der gefundenen Komponente bei HW z.B. auch ein Kurzschluss oder bei SW ein fehlgeleiteter Schreibzugriff sein.

Reparatur- und prüfgerechter Entwurf

Sammlungen von

- Regeln »of good practise«, zur Ermöglichung / Vereinfachung von Test, Fehlerlokalisierung und Reparatur und
- Antipattern (typ. Vorgehensfehler, die Probleme verursachen).

Einige Regeln »of good practise«:

- Modulares System aus tauschbaren / seperat testbaren Funktionsblöcken.
- Deterministisches Verhalten mit gerichtetem Berechnungsfluss.
- MF-Isolation zur Verhinderung der Ausbreitung von Fehlfunktionen über Modulgrenzen.

Hässlichstes Antipattern:

- »Big ball of mud«: großes, unstrukturiertes, mangelhaft dokumentiertes System, das niemand mehr richtig versteht.

Die Vorlesung unterstellt einen reparatur- und prüfgerechten Entwurf.

Fehlerisolation

Verhinderung des Übergreifens von Fehlfunktionen auf andere Teilsysteme:

- Physikalische und räumliche Trennung von Teilsytemen zur Minderung des Risikos übereinstimmender MF-Ursachen (gemeinsame Fehler, zeitgleicher Ausfälle, ...).
- Beschränkung von MF-Ausbreitung auf den Informations- und Verarbeitungsfluss.
- Keine Zugriffmöglichkeit auf Daten und Resourcen anderer Funktionseinheiten außer über definierte Schnittstellen.
- Verhinderung, dass fehlerhaft arbeitende Teilsysteme korrekt arbeitende Teilsysteme beeinträchtigen können.

Test

Testen

Verfahren zum Aufspühren von Fehlern. Grundeinteilung:

- Statische Tests: direkte Kontrolle von Merkmalen.
- Dynamische Tests: Ausprobieren der Systemfunktion mit einer Stichprobe von Beispieleingaben.

Mit statischen Tests kontrollierbare Merkmale:

- Dokumentationen: Verständlichkeit, Vollständigkeit, ...
- Software: Syntax, Entwurfsregeln, Typenverträglichkeit und API-Benutzerregeln,
- Leiterplatten: keine Kurzschlüsse und Unterbrechungen, ...

Dynamische Tests sind erst am fertigen Produkt möglich, statische Tests bereits nach einzelnen Entwurfs- und Fertigungsschritten.

Vor dem Einsatz werden IT-Systeme in der Regel den verschiedensten statischen und dynamischen Tests unterzogen.

Kenngrößen von Tests

Wie bei jeder Kontrolle mit den möglichen Ergebnissen gut oder schlecht sind zwei Arten von Fehlklassifikationen möglich:

- Nichterkennbare Fehler. Modelliert durch die Kenngröße Fehlerüberdeckung:

$$FC = \left.\frac{\#F_{\mathrm{D}}}{\#F}\right|_{\mathrm{ACR}} \tag{52}$$

- Phantomfehler. Tests, die korrekte Testergebnisse als falsch klassifizieren. Modelliert durch die Phantom-MF-Rate des Tests:

$$\zeta_{\mathrm{PhanT}} = \left.\frac{\#PM}{N}\right|_{\mathrm{ACR}} \tag{53}$$

$\#F_{\mathrm{D}}$	Anzahl der erkennbaren Fehler (Number of detectable faults).
$\#F$	Anzahl der Fehler (Number of faults).
ζ_{PhanT}	Phantom-MF-Rate des Tests (Phantom MF rate during test).
$\#PM$	Anzahl der Phantom-MF, d.h. der korrekten DS, die als MF klassifiziert werden.
N	Anzahl der Tests.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

Auch Tests müssen getestet werden

Eine Phantomfehler (z.B. eine MF beim der Testauswertung)

- startet eine überflüssige Beseitigungsiteration
- in der ein neuer nicht nachweisbarer Fehler entstehen kann.

Kontrolle Testergebnisse meist durch Vergleich mit Sollwerten:

- Maskierungen von Fehlern durch Vergleichs-MF und
- Phantomfehler durch falsche Sollwerte, ...

Für neu entwickelte Tests ist zu kontrollieren, dass

- richtige Testergebnisse als richtig und
- falsche Testergebnisse als falsch klassifiziert werden.

Wenn ein Test einen Fehler erkennt, sollte zuerst ausgeschlossen werden, dass es kein Phantomfehler ist.

Bei vernünftigem Umgang mit Phantomfehlern ist deren Einfluss auf die Gesamtanzahl der entstehenden Fehler unerheblich. Wir werden Phantomfehler in später entwickelten Modellen vernachlässigen.

Testauswahl für dynamische Tests

Dynamische Tests kontrollieren die Funktion nur für eine winzige Stichprobe der möglichen Eingaben. Die FC hängt vom Umfang und der Auswahl der Testbeipiele ab.

Strategien der Testauswahl:

- fehlerorientiert.
- zufällig hinsichtlich der zu erwartenden Fehler oder
- Mischform.

Zum Zeitpunkt der Testauswahl sind die zu findenden und nach dem Test die nicht gefundenen Fehler nicht bekannt.

Ohne Kenntnis der zu findenden Fehler:

- erfolgt die fehlerorientierte Auswahl und Bewertung auf Basis von Fehlerannahmen (Modellfehlern oder Mutationen) und
- ist der Nachweis der tatsächlichen Fehler Zufall.

Haftfehler

Modellfehler und Fehlermodell

Ein *Fehlermodell* ist ein Algorithmus zur Berechnung einer Menge von möglichen Verfälschungen aus einer Entwurfsbeschreibung.

Ein *Modellfehler* ist eine einzelne dieser Verfälschungen.

Fehlersimulation zur Bestimmung der *Modellfehlerüberdeckung*:

- Wiederhole für jeden Test:
  - Bestimmung der Sollausgaben.
  - Wiederhole für alle Fehler der Modellfehlermenge:
    - Bestimme, ob der Fehler die Ausgabe verfälscht.
    - Wenn ja, kennzeichnen oder Nachweis zählen.

Fehlerorientierte Testsuche:

- Wiederhole für alle Fehler der Modellfehlermenge:
  - Suche Eingaben, für die der Fehler Ausgaben verfälscht.

Beide Arten der modellfehlerorientierte Testauswahl:

- Sehr hoher Rechenaufwand.
- Für digitale ICs seit Jahrzehnten etabliert (siehe Abschn. 5.2), für SW Anfänge erkennbar (siehe Abschn. 6.3).

Das Haftfehlermodell

Seit Jahrzehnten das verbreitetste Fehlermodell für digitale Schaltkreise. In der Vorlesung das Standardfehlermodell für Beispiele.

Das Haftfehlermodell generiert für eine Schaltung aus Logikgattern für alle Anschlüsse aller Gatter zwei Modellfehler:

- Wert ständig null (sa0, stuck-at-0) und
- Wert ständig eins (sa1, stuck-at-1).

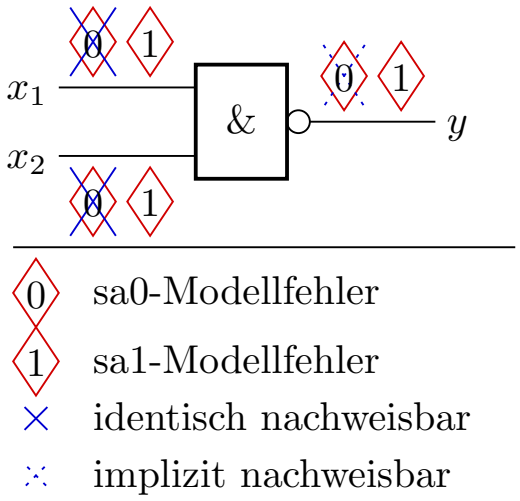
Die initiale Fehlermenge wird von identisch oder implizit nachweisbaren und redundanten (nicht nachweisbaren) Modellfehlern bereinigt.

Bei den sich aktuell entwickelnden Testauswahltechniken für Software lassen sich Parallen zum Haftfehlermodell aufzeigen (siehe Abschn. 6.3 *Testauswahl*).

Haftfehler für ein Logikgatter

Für jeden Gatteranschluss wird unterstellt:

- ein sa0 (stuck-at-0) Fehler
- ein sa1 (stuck-at-1) Fehler



x_2	x_1	$\overline{x_2 \wedge x_1}$	sa0(x_1)	sa1(x_1)	sa0(x_2)	sa1(x_2)	sa0(y)	sa1(y)
0	0	1	1	1	1	1	0	1
0	1	1	1	1	1	0	0	1
1	0	1	1	0	1	1	0	1
1	1	0	1	0	1	0	0	1

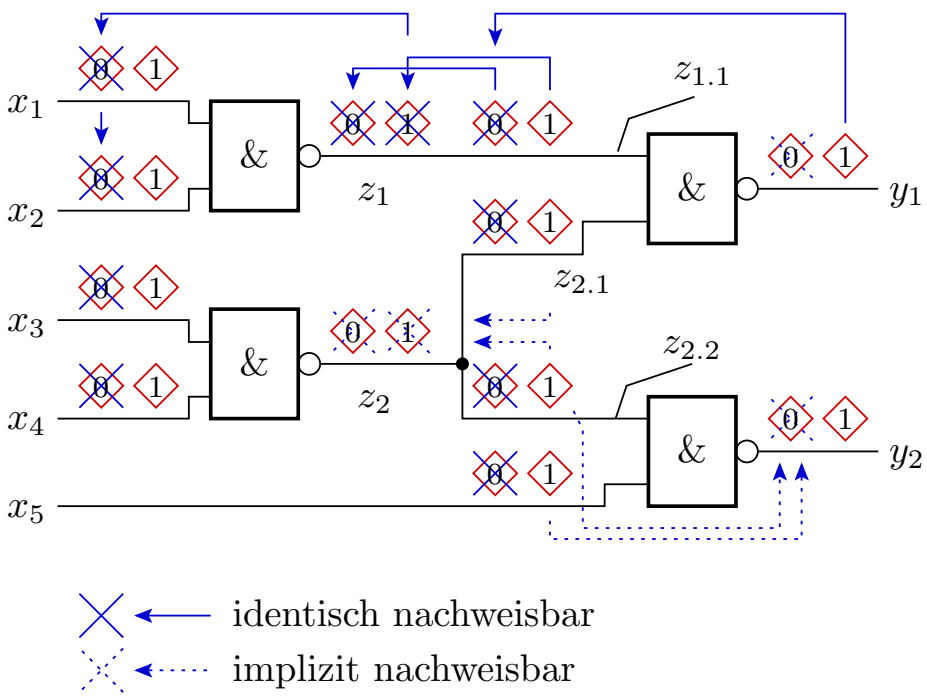
Nachweisidentität (gleiche Nachweismenge)

Nachweisimplikation

zugehörige Eingabe ist Element der Nachweismenge

- Zusammenfassung identisch nachweisbarer Fehler. Optionale Streichung redundanter und implizit nachweisbarer Modellfehler.
- Die generierte Fehlermenge enthält für alle potentiellen Fehler der echten Schaltung ähnlich nachweisbare Modellfehler(siehe Abschn. 5.1.4 *Nachweisbeziehungen*).

Identische und implizit nachweisbarer Fehler im Schaltungsverbund



Größe der Anfangsfehlermenge:	24
Anzahl der nicht identisch nachweisbaren Fehler:	14
ohne implizit nachgewiesene Fehler:	10

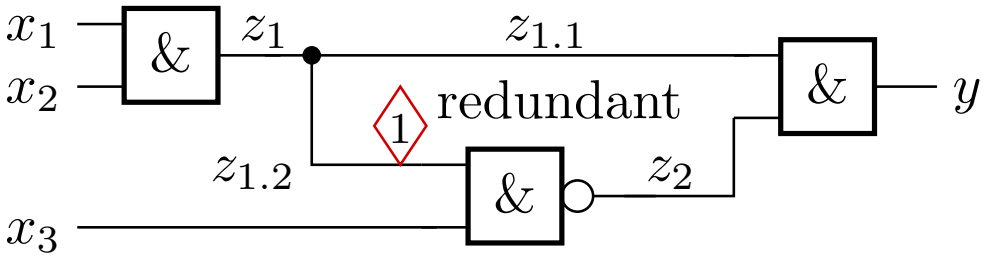
	Mengen von identisch nachweisbaren Fehlern	Nachweis impliziert durch
1	sa0(x_1), sa0(x_2), sa1(z_1), sa1($z_{1.1}$)	
2	sa1(x_1)	
3	sa1(x_2)	
4	sa0(x_3), sa0(x_4), sa1(z_2)	9, 12
5	sa1(x_3)	
6	sa1(x_4)	
7	sa0(z_2)	5, 6, 8, 11
8	sa0(z_1), sa0($z_{1.1}$), sa0($z_{2.1}$), sa1(y_1)	2, 3
9	sa1($z_{2.1}$)	
10	sa0(y_1)	1, 9
11	sa0($z_{2.2}$), sa0(x_5), sa1(y_2)	
12	sa1($z_{2.2}$)	
13	sa1(x_5)	
14	sa0(y_2)	12, 13

Redundante Fehler

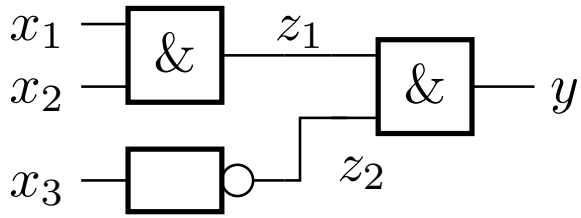
Definition redundanter (Modell-) Fehler

Verfälschung der Systembeschreibung, die die Funktion nicht beeinträchtigt und damit auch nicht mit dynamischen Tests nachweisbar ist.

redundanter Haftfehler



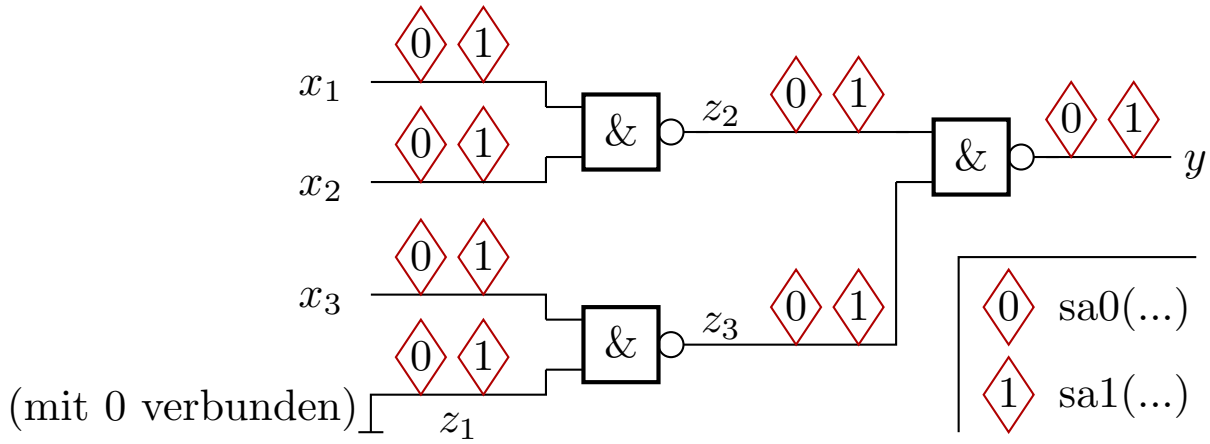
vereinfachte Schaltung



- Die Fehleranregung verlangt $z_1 = 0$ und die Beobachtbarkeit von z_2 an y verlangt $z_2 = 1$. Keine Eingabe $x_3x_2x_1$ kann den Fehler nachweisen.
- Die Beseitigung redundanter Fehler dient auch zur Vereinfachung der Systembeschreibung.

Beispiel 1.4: Haftfehlermenge

Schaltung mit 12 eingezeichneten Haftfehlern:



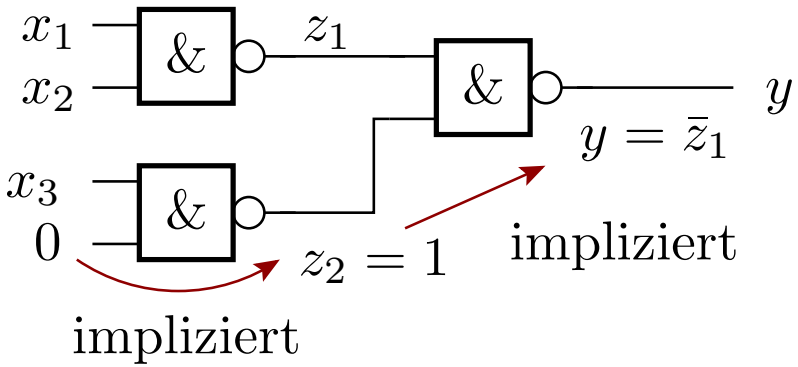
a) *Bestimmen Sie die initiale Haftfehlermenge nach Beseitigung der Redundanz.*

b) *Streichen der identisch und implizit nachweisbare Haftfehler in der verbleibenden Modellfehlermenge.*

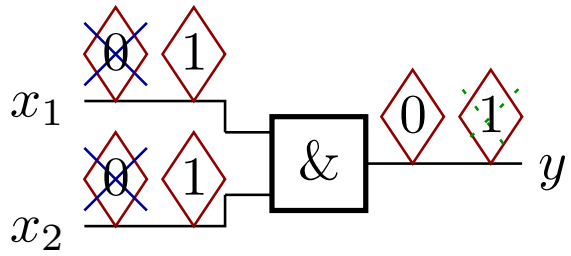
a) *Bestimmen Sie die initiale Haftfehlermenge nach Beseitigung der Redundanz.*

Die Funktion hängt nicht von x_3 ab und ist: $y = x_1 \wedge x_2$

Vereinfachungsmöglichkeiten



Redizierung der Fehlermenge für die vereinfachte Schaltung



b) *Streichen der identisch und implizit nachweisbare Haftfehler in der verbleibenden Modellfehlermenge.*

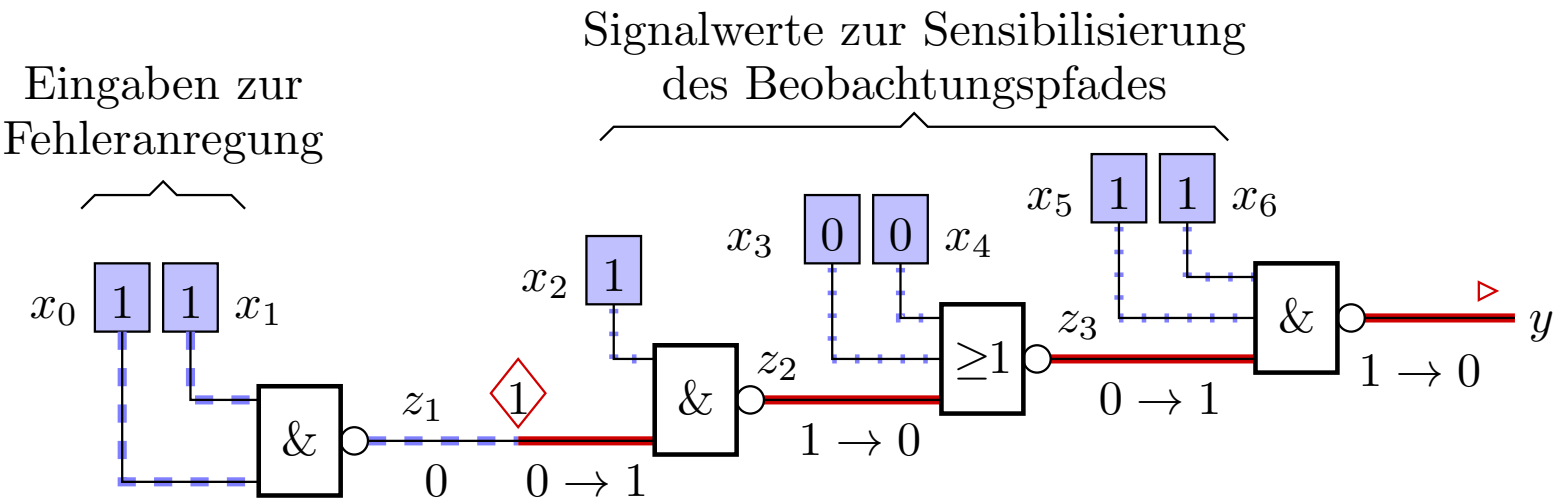
An dem verbleibenden AND-Gatter sind sa0(x_i) identisch mit sa0(y) nachweisbar und der Nachweis von sa1(x_1) und sa1(x_2) impliziert den von sa1(y).

Testsuche und Nachweiswahrscheinlichkeit

Suche durch Pfadsensibilisierung(siehe Abschn. 5.2.2 *D-Algorithmus*):

- Suche von Eingaben zur Einstellung »0« am Fehlerort und
- Sensibilisierung eine Beobachtungspfades zu einem Ausgang.

Fehlernachweismengen

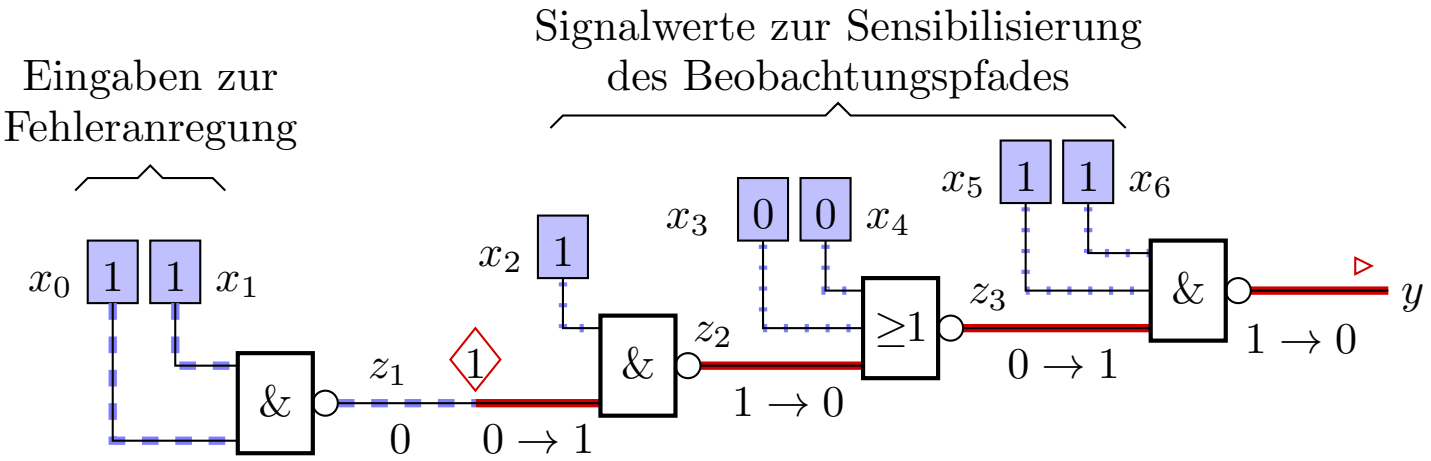


- Signalwerte für den Fehlernachweis
- Fehler (ständig 1, stuck-at 1)
- Fehlfunktion (Ausgabeinvertierung)
- Eingaben zur Fehleranregung
- Einstellung der Beobachtbarkeit
- Beobachtungspfad

Nachweismenge (Eingabemengen für den Fehlernachweis):

Eingabemenge Fehleranregung: $M_1 = \{\text{-----11}\}$
Eingabemenge Beobachtbarkeit: $M_2 = \{\text{11001--}\}$
Fehlernachweismenge: $M_1 \cap M_2 = \{1100111\}$

Nachweiswahrscheinlichkeit



- Signalwerte für den Fehlernachweis
- Fehler (ständig 1, stuck-at 1)
- Fehlfunktion (Ausgabeinvertierung)
- Eingaben zur Fehleranregung
- Einstellung der Beobachtbarkeit
- Beobachtungspfad

Zufallstest und Annahme von 128 gleichhäufigen Eingabewerte:

- Anregung mit $2^5 = 32$ von 128 Eingaben: $p_{\mathrm{FS}} = 2^{-2}$
- beobachtbar mit $2^2 = 4$ von 128 Eingaben: $p_{\mathrm{FO}} = 2^{-5}$
- nachweisbar mit einer von 128 Eingaben: $p_{\mathrm{FD}} = p_{\mathrm{FS}} \cdot p_{\mathrm{FO}} = 2^{-7}$

p_{FS} Fehleranregungswahrscheinlichkeit (Probability of fault stimulation).
p_{FO} Fehlerbeobachtbarkeitswahrscheinlichkeit (Probability of fault observation).
p_{FD} Fehlererkennungswahrscheinlichkeit (zu erwartende Fehlerüberdeckung).

Zuverlässigkeit danach

Zuverl. nach Beseitigung aller erkannten Fehler

Beispiel 1.5: Anzahl der nicht beseitigten Fehler

Programmgröße 10.000 NLOC. 30 ... 100 Fehler je 1000 NLOC. Fehlerüberdeckung der Tests $FC = 70\%$. Zu erwartende Fehleranzahl nach Beseitigung aller erkennbaren Fehler?

$$10.000\,\mathrm{NLOC} \cdot \frac{30\ [\mathrm{F}]\ \ldots\ 100\,[\mathrm{F}]}{1000\,\mathrm{NLOC}} \cdot (1 - 70\%) = 100\,[\mathrm{F}]\ \ldots\ 300\ [\mathrm{F}]$$

Wie zuverlässig ist ein System mit 100 bis 300 Fehlern?

Vorgriff: Bei einem Zufallstest und Beseitigung aller erkannten Fehler verhält sich die fehlerbezogene Teilzuverlässigkeit R_F proportional zur Anzahl der dynamischen Tests N und umgekehrt proportional zur zu erwartenden Anzahl der nicht beseitigten Fehler μ_F:

$$R_\mathrm{F}(N) \sim \frac{N}{\mu_\mathrm{F}(N)}$$

[F] Zählwert in Fehlern.

Fehlfunktionsrate durch Fehler

Jeder nicht beseitigte Fehler i verursacht mit der MF-Rate ζ_i (in MF je DS) Fehlfunktionen. Die Summe der MF-Raten aller Fehler

$$\zeta_\Sigma = \sum_{i=1}^{\#F} \zeta_i$$

ist eine Obergrenze $\zeta_\mathrm{F} \leq \zeta_\Sigma$ und, wenn fast alle MF nur einen Fehler als Ursache haben, praktisch gleich der MF-Rate durch alle Fehler:

$$\zeta_\mathrm{F} = \sum_{i=1}^{\#F} \zeta_i \quad \text{für} \quad \zeta_\Sigma \ll 1$$

$\#F$	Anzahl der vorhandenen Fehler (Number of existing).
ζ_i	MF-Rate verursacht durch Fehler i.
ζ_F	Fehlfunktionsrate durch Fehler.

$\mu_\mathrm{F}\,(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
$R_\mathrm{F}\,(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehlern.
N	Anzahl der Tests, für die alle erkannten Fehler beseitigt sind.

Einfache Abschätzung

Unter den Annahmen:

- Beseitigung aller nachweisbaren Fehler,
- mittlere MF-Rate je nicht beseitigten Fehler $\bar{\zeta} \leq 1/N$
- je Fehlerfunktion hat nur einen Fehler als Ursache

beträgt die MF-Rate für alle nicht beseitigten Fehler zusammen:

$$\zeta_{\mathrm{F}}(N) = \mu_{\mathrm{F}}(N) \cdot \bar{\zeta}(N) \tag{54}$$

$$\zeta_{\mathrm{F}}(N) \leq \frac{\mu_{\mathrm{F}}(N)}{N}$$

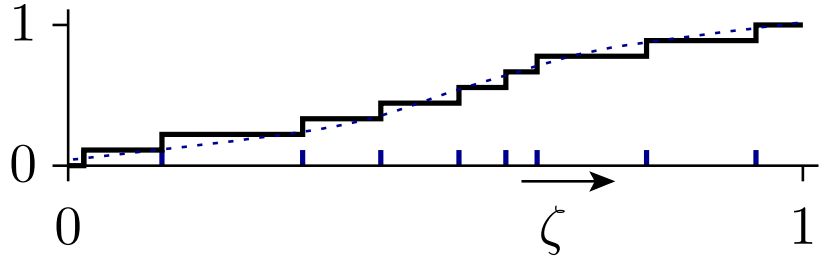
Die fehlerbezogene Teilzuverlässigkeit beträgt mindestens:

$$R_{\mathrm{F}} \geq \frac{N}{\mu_{\mathrm{F}}(N)}$$

$\zeta_{\mathrm{F}}(N)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.
$\mu_{\mathrm{F}}(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
$\bar{\zeta}(N)$	Mittlere Fehlfunktionsrate je Fehler als Funktion der Testanzahl N.
N	Anzahl der Tests, für die alle erkannten Fehler beseitigt sind.
$R_{\mathrm{F}}(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehlern.

Eine genauere Abschätzung

$$F_Z(\zeta) = \mathbf{P}[Z \leq \zeta]$$



Treppenfunktion für eine endliche Fehleranzahl

Annäherung durch eine stetige Funktion

Die Verteilung $F_Z(\zeta)$ der MF-Rate beschreibt für jeden Wert $\zeta \in (0, 1)$ die Wahrscheinlichkeit, dass sie nicht größer als ζ ist. Bei Annäherung von $F(\zeta)$ durch eine stetige Verteilungsfunktion beträgt die Dichte der MF-Rate (siehe später Foliensatz 3):

$$h(\zeta) = f_Z(\zeta) = \frac{\mathrm{d}F_Z(\zeta)}{\mathrm{d}\zeta} \text{ mit } \int_0^1 h(\zeta) \cdot d\zeta = 1$$

$F_Z(\zeta)$ Verteilungsfunktion der Fehlfunktionsrate, Z – Zufallsvariable, ζ – Wert.
$h(\zeta)$ Dichtefunktion der Fehlfunktionsrate.

Testaufwand, Fehlerüberdeckung und MF-Rate

Der zu erwartende Anteil der mit N Tests nicht beseitigten Fehler ist die mit $h(\zeta)$ gewichtete Nichtbeseitigungswahrscheinlichkeit $p_{\mathrm{F}}(\zeta, N)$, die im allgemeinen von ζ und N abhängt:

$$1 - \mu_{\mathrm{FC}}(N) = \frac{\mu_{\mathrm{F}}(N)}{\mu_{\mathrm{F}}} = \int_0^1 p_{\mathrm{F}}(\zeta, N) \cdot h(\zeta) \cdot \mathrm{d}\zeta \tag{55}$$

Dichte der MF-Rate nach Beseitigung aller erkannten Fehler:

$$h(\zeta, N) = \frac{p_{\mathrm{F}}(\zeta,N) \cdot h(\zeta)}{1-\mu_{\mathrm{FC}}(N)}$$

MF-Rate durch nicht beseitigter Fehler:

$$\bar{\zeta}(N) = \frac{\int_0^1 p_{\mathrm{F}}(N) \cdot \zeta \cdot h(\zeta) \cdot \mathrm{d}\zeta}{1-\mu_{\mathrm{FC}}}$$

$$\zeta_{\mathrm{F}}(N) = \underbrace{\mu_{\mathrm{F}}(N) \cdot \bar{\zeta}(N)}_{\text{Gl. (Gl. 1.54)}} = \mu_{\mathrm{F}} \cdot \int_0^1 p_{\mathrm{F}}(\zeta, N) \cdot \zeta \cdot h(\zeta) \cdot \mathrm{d}\zeta \tag{56}$$

$\mu_{\mathrm{FC}}(N)$ Zu erwartende Fehlerüberdeckung in Abhängigkeit von der Testanzahl.
$p_{\mathrm{F}}(\zeta, N)$ Wahrscheinlichkeit, dass Fehler mit MF-Rate ζ nach N Tests noch vorhanden sind.
$\mu_{\mathrm{F}}(N)$ Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.

Typische Fehlerüberdeckung von Zufallstests

Bei einem Zufallstest erfordert eine Verringerung des Anteils der nicht nachweisbaren Fehler $1 - FC\,(N)$ um eine Dekade eine Erhöhung der Testanzahl N um mehr als eine Dekade. Das ist die Eigenschaft einer Potenzfunktion:

$$1 - \mu_{\mathrm{FC}}\,(N) = \frac{\mu_{\mathrm{F}}(N)}{\mu_{\mathrm{F}}(N_0)} = \left(\frac{N}{N_0}\right)^{-K} \quad \text{mit } N \geq N_0 \text{ und } 0 < K < 1 \qquad (57)$$

K	1	0,5	0,33	0,25
$\frac{N}{N_0}$ für $1 - \mu_{\mathrm{FC}}\,(N) = 0{,}1$	10	100	10^3	10^4

Zugehöringe Abnahme der zu erwartenden Fehleranzahl:

$$\mu_{\mathrm{F}}\,(N_2) = \mu_{\mathrm{F}}\,(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \qquad (58)$$

N_0	Testanzahl, für die vorher alle Fehler beseitigt wurden, also für $FC = 0$.
N	Anzahl der Tests, für die erkannten Fehler beseitigt werden, incl. N_0.
K	Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.
$N_1\,, N_2$	Testanzahl mit bekannter oder gesuchter zu erwartender Fehleranzahl.

Zugehörige Dichte der MF-Rate

Mit der Vereinfachung, dass ein Zufallstest der Länge N alle Fehler mit einer MF-Rate $\zeta \geq \frac{1}{N}$ nachweist:

$$p_{\mathrm{F}}(\zeta, N) = \begin{cases} 1 & \zeta \geq \frac{1}{N} \\ 0 & \text{sonst} \end{cases}$$

$$1 - \mu_{\mathrm{FC}}(N) = \frac{\mu_{\mathrm{F}}(N)}{\mu_{\mathrm{F}}} = \int_0^1 p_{\mathrm{F}}(\zeta, N) \cdot h(\zeta) \cdot \mathrm{d}\zeta \tag{1.55}$$

$$1 - \mu_{\mathrm{FC}}(N) = \left(\frac{N}{N_0}\right)^{-K} \tag{1.57}$$

beträgt die Dichte der MF-Rate ohne Beseitigung der Fehler, die mit den $N - N_0$ zusätzlichen Tests nachweisbar sind:

$$\left(\frac{N}{N_0}\right)^{-k} = \int_0^{\frac{1}{N}} h(\zeta, N_0) \cdot \mathrm{d}\zeta \quad \text{für } N \geq N_0$$

$$h(\zeta, N_0) = \begin{cases} K \cdot N_0^K \cdot \zeta^{K-1} & 0 \leq \zeta < \frac{1}{N_0} \\ 0 & \text{sonst} \end{cases}$$

N_0 Testanzahl, für die vorher alle Fehler beseitigt wurden, also für $FC = 0$.

Nach der Fehlerbeseitigung

Wenn alle mit N incl. N_0 Tests erkennbaren Fehler beseitigt sind:

$$h(\zeta, N) = \begin{cases} k \cdot N^K \cdot \zeta^{K-1} & 0 \leq \zeta < \frac{1}{N} \\ 0 & \text{sonst} \end{cases} \tag{59}$$

Mittlere MF-Rate je nicht beseitigter Fehler und zu erwartende MF-Rate durch alle nicht beseitigten Fehler:

$$\bar{\zeta}(N) = \int_0^{\frac{1}{N}} h(\zeta, N) \cdot \zeta \cdot \mathrm{d}\zeta = \frac{K}{\cancel{(K+1)} \cdot N}$$

$$\zeta_\mathrm{F}(N) = \underbrace{\mu_\mathrm{F}(N) \cdot \bar{\zeta}(N)}_{\text{(Gl. 1.54)}} = \frac{\mu_\mathrm{F}(N) \cdot K}{\cancel{(K+1)} \cdot N}$$

$h(\zeta, N)$	Dichte der Fehlfunktionsrate nach Beseitigung der mit N Tests nachweisbaren Fehler.
K	Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.
$\bar{\zeta}$	Mittlere Fehlfunktionsrate je Fehler.
$\mu_\mathrm{F}(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
$\cancel{(K+1)}$	Term, der entfällt, wenn die Nachweiswahrsch von Zufallstests exakt modelliert wird.

MF-Rate nach Beseitigung der erkannten Fehler

$$\zeta_{\mathrm{F}}(N) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{\cancel{(K+1)} \cdot N} \tag{60}$$

Mit dem Potenzgesetz für die Abnahme der Fehleranzahl:

$$\mu_{\mathrm{F}}(N_2) = \mu_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \tag{1.58}$$

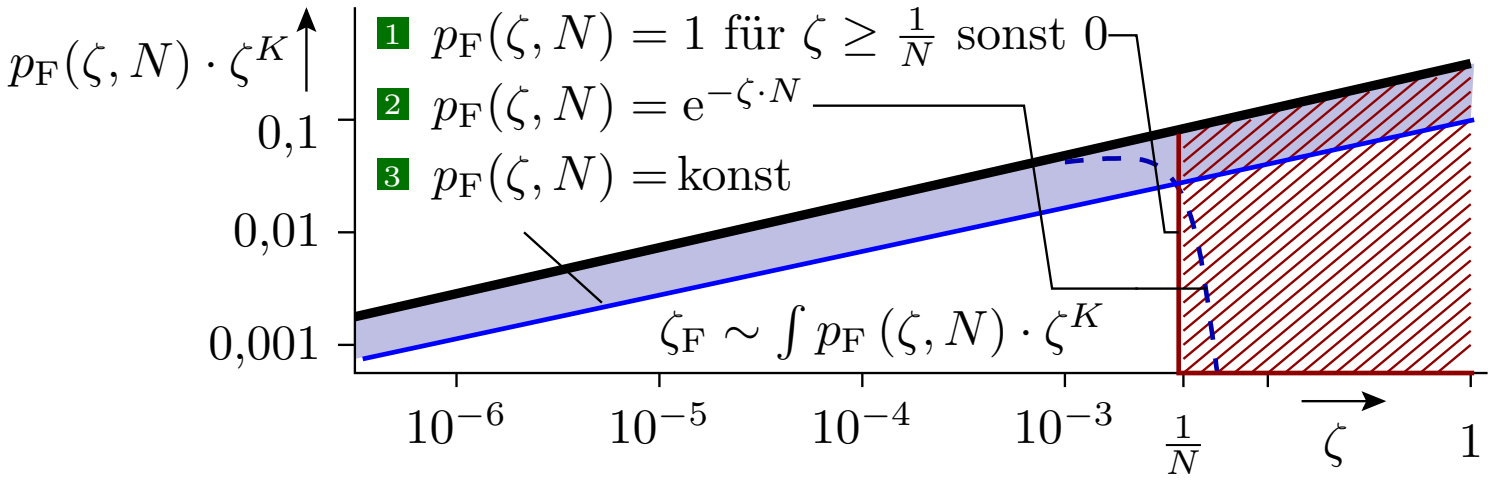
$$\frac{\zeta_{\mathrm{F}}(N_2) \cdot \cancel{(K+1)} \cdot N_2}{K} = \frac{\zeta_{\mathrm{F}}(N_1) \cdot \cancel{(K+1)} \cdot N_1}{K} \cdot \left(\frac{N_2}{N_1}\right)^{-K}$$

$$\zeta_{\mathrm{F}}(N_2) = \zeta_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-(K+1)} \tag{61}$$

Anmerkung: Die Gleichheit gilt nur, wenn fast alle MF nur einen Fehler als Ursache haben (siehe Folie 1.140), d.h. für $\zeta_{\mathrm{F}}(N) \ll 1$ und auch $\zeta_{\mathrm{F}}(N_0) \ll 1$, also für $N_0 \gg 1$.

$\zeta_{\mathrm{F}}(N)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.
N_1, N_2	Testanzahl mit bekannter / gesuchter Fehlfunktionsrate oder Fehleranzahl.
$\cancel{(K+1)}$	Term, der entfällt, wenn die Nachweiswahrsch von Zufallstests exakt modelliert wird.

Beseitigungswahrscheinlichkeit für reale Tests

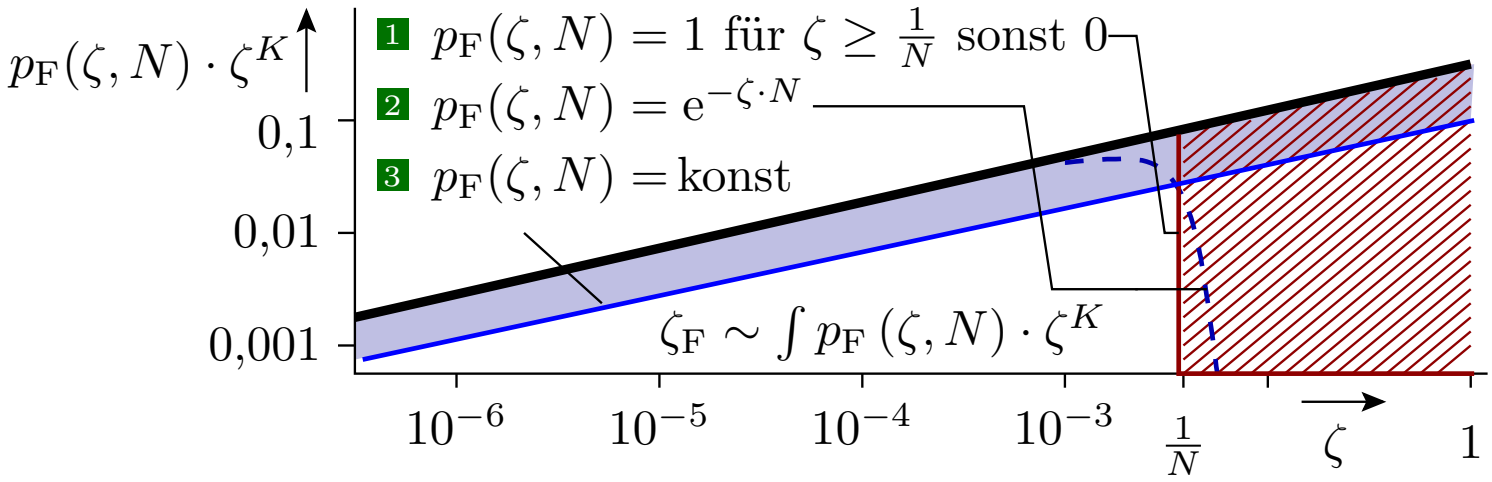


$$\zeta_F(N) = \mu_F \cdot \int_0^1 p_F(\zeta, N) \cdot \zeta \cdot h(\zeta) \cdot d\zeta \quad (1.56)$$

Mit $h(\zeta, N) \sim \zeta^{K-1}$ für $N \gg N_0$ (siehe Folie 1.145) verhält sich die Fehlfunktionsrate proportional zur Fläche unter der Kurve:

$$\zeta_F(N) \sim p_F(\zeta, N) \cdot \zeta^K$$

1. Nachweis genau mit $\frac{1}{\zeta}$ Tests: ...
2. Nachweis mit im Mittel $\frac{1}{\zeta}$ Tests: ...
3. Nachweiswahrscheinlichkeit $p_F(\zeta, N) = \mu_{FC} \neq f(\zeta)$: ...



1. Nachweis genau mit $\frac{1}{\zeta}$ Tests (unsere Vereinfachung):

$$\zeta_F(N) = \frac{\mu_F(N) \cdot K}{(K+1) \cdot N} \tag{1.60a}$$

2. Nachweis mit im Mittel $\frac{1}{\zeta}$ Tests (siehe später Absch. 2.2.1)*:

$$\zeta_F(N) = \frac{\mu_F(N) \cdot K}{N} \tag{1.60}$$

3. Nachweiswahrscheinlichkeit $p_F(\zeta, N) = \mu_{FC} \neq f(\zeta)$:

$$\zeta_F(N) \neq f(N) \sim 1 - \mu_{FC}$$

* Die Herleitung folgt später (siehe Abschn. 3.5.1 *Gammaverteilung*). Wir lassen den Term $K + 1$ im Nenner trotzdem auch im Folgenden schon weg.

Aufteilung in Vortest und Zufallstest

Vor einem gründlichen Zufallstest erfolgen Vortests:

- statische Tests: Reviews, Syntax, ...
- Grobtests, ob überhaupt etwas funktioniert und
- gezielt gesuchte Tests für Grenz- und Sonderfälle.

Bei statischen und fehlerorientiert gesuchten Tests hängt $p_{\mathrm{F}}(\zeta, N)$ weniger von ζ als beim Zufallstest ab. Pauschalannahme, dass die Vortests einen Anteil von FC_{PT} Fehler erkennen, die alle beseitigt werden und $N_0 \geq 1$ dynamische Tests enthalten:

$$\mu_{\mathrm{F}}(N_0) = \mu_{\mathrm{FCR}} \cdot (1 - FC_{\mathrm{PT}}) \tag{62}$$

$$\zeta_{\mathrm{F}}(N_0) = \frac{K \cdot \mu_{\mathrm{F}}(N_0)}{N_0} \tag{63}$$

$p_{\mathrm{F}}(\zeta, N)$	Fehlerbeseitigungswahrsch. in Abhängigkeit von der Fehler-MF-Rate ζ und N.
$\mu_{\mathrm{F}}(N_0)$	Zu erwartende Anzahl Fehler, die nach N_0 Vortests nicht erkannt und beseitigt sind.
N_0	Anzahl der dynamischen Tests aller Vortests zusammen.
μ_{FCR}	Zu erwartende Fehleranzahl aus den Entstehungs- und Reparaturprozessen insgesamt.
FC_{PT}	Fehlerüberdeckung der Vortests (Fault coverage of the pre tests).
$\zeta_{\mathrm{F}}(N_0)$	Fehlfunktionsrate nach Beseitigung der von Vortests erkannten Fehler.

Anschließender Zufallstests

In den Testsatzlängen N, N_1, N_2 ist die Anzahl der dynamischen Vortests N_0 immer mit enthalten:

$$\mu_{\mathrm{F}}\left(N_2\right) = \mu_{\mathrm{F}}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \tag{1.58}$$

$$\zeta_{\mathrm{F}}\left(N\right) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{N} \tag{1.60}$$

$$\zeta_{\mathrm{F}}\left(N_2\right) = \zeta_{\mathrm{F}}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{-(K+1)} \tag{1.61}$$

Formfaktor:

$$K = \log\left(\frac{\zeta_{\mathrm{F}}(N_1)}{\zeta_{\mathrm{F}}(N_2)}\right) / \log\left(\frac{N_2}{N_1}\right) - 1 \tag{64}$$

$\mu_{\mathrm{FC}}\left(N\right)$	Zu erwartende Fehlerüberdeckung in Abhängigkeit von der Testanzahl.
N_1, N_2	Testanzahl mit bekannter / gesuchter Fehlfunktionsrate oder Fehleranzahl.
K	Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.
$\zeta_{\mathrm{F}}\left(N\right)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.

Fehlerbezogene Teilzuverlässigkeit

Fehlerbezogene Teilzuverlässigkeit als Kehrwert der MF-Rate durch Fehler nach Gl. 1.60 bzw. 1.61:

$$R_{\mathrm{F}}(N) = \frac{N}{K \cdot \mu_{\mathrm{F}}(N)} \tag{65}$$

$$R_{\mathrm{F}}(N_2) = R_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{K+1} \tag{66}$$

$R_{\mathrm{F}}(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehlern.
$\mu_{\mathrm{F}}(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
K	Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.
N_1, N_2	Testanzahl mit bekannter oder gesuchter Zuverlässigkeit.

Beispiel 1.6: Zuverlässigkeit dreifacher Testaufwand

a) *Um welchen Faktor verringern sich MF-Rate $\zeta_{\mathrm{F}}(N)$ und Fehleranzahl $\mu_{\mathrm{F}}(N)$, wenn die Anzahl der dynamischen Tests verdreifacht wird? Formfaktoren der Verteilung der MF-Rate $K \in \{0{,}3,\ 0{,}5\}$.*

b) *Welcher Erhöhung von R_{F} ist zu erwarten, wenn das Personal der Testabteilung verdreifacht wird?*

a) *Um welchen Faktor verringern sich MF-Rate $\zeta_{\mathrm{F}}(N)$ und Fehleranzahl $\mu_{\mathrm{F}}(N)$, wenn die Anzahl der dynamischen Tests verdreifacht wird? Formfaktoren der Verteilung der MF-Rate $K \in \{0{,}3,\ 0{,}5\}$.*

Geschätzte Reduzierung der MF-Rate und der Fehlerzahl sowie die Erhöhung der Zuverlässigkeit als Kehrwert der MF-Rate:

$$\frac{\zeta_{\mathrm{F}}(3 \cdot N)}{\zeta_{\mathrm{F}}(N)} = 3^{-(K+1)}; \quad \frac{\mu_{\mathrm{F}}(3 \cdot N)}{\mu_{\mathrm{F}}(N)} = 3^{-K}; \quad \frac{R_{\mathrm{F}}(3 \cdot N)}{R_{\mathrm{F}}(N)} = 3^{K+1}$$

	$\frac{\mu_{\mathrm{F}}(3 \cdot N)}{\mu_{\mathrm{F}}(N)}$	$\frac{\zeta_{\mathrm{F}}(3 \cdot N)}{\zeta_{\mathrm{F}}(N)}$	$\frac{R_{\mathrm{F}}(3 \cdot N)}{R_{\mathrm{F}}(N)}$
$K = 0{,}3$	0,72	0,24	4,17
$K = 0{,}5$	0,56	0,19	5,19

b) *Welcher Erhöhung von R_{F} ist zu erwarten, wenn das Personal der Testabteilung verdreifacht wird?*

Ein 3-facher Personaleinsatz für Tests und Fehlersuche erhöht die fehlerbezogenen Teilzuverlässigkeit auf etwa das 4- bis 5-fache.

Zuverl. und Sicherheit nach Fehlerbeseitigung

Zur abgeschätzen MF-Rate durch Fehler kommt die MF-Rate durch Störungen hinzu. Zuverlässigkeit ohne Fehlfunktionsbehandlung:

$$R = \frac{1}{\zeta_{\mathrm{F}} + \zeta_{\mathrm{D}}} \tag{67}$$

Nach Gl.1.32 erhöht die MF-Behandlung die Zuverlässigkeit typ. um den Kehrwert des Anteils der nicht nachweisbaren Fehlfunktionen:

$$R_{\mathrm{MT}} = \frac{1}{(\zeta_{\mathrm{F}} + \zeta_{\mathrm{D}}) \cdot (1 - MC)} \tag{68}$$

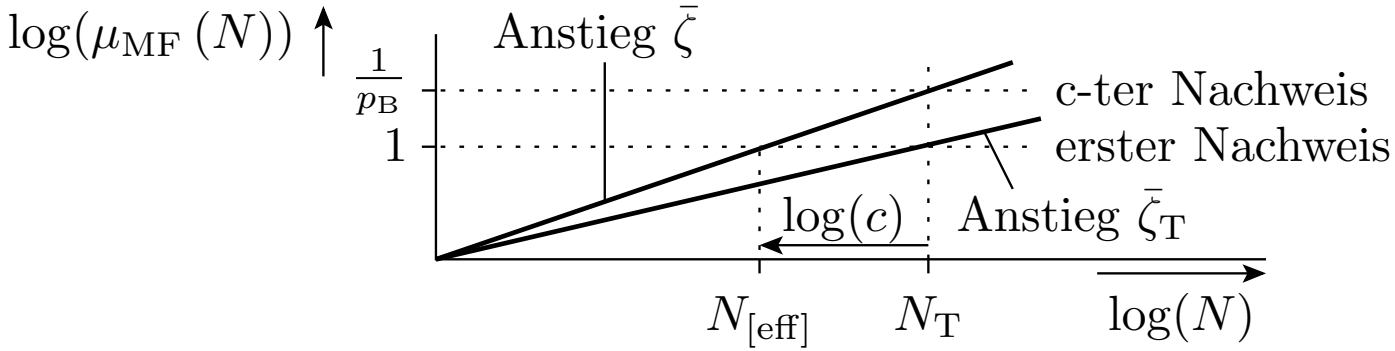
Ohne zusätzliche Sicherheitsfunktionen ist die Sicherheit nach (Gl. 1.49) zusätzlich um den Kehrwert des Anteil der sicherheitsgefährdenden MF η_{SE} größer:

$$S_{\mathrm{MT}} = \frac{1}{(\zeta_{\mathrm{F}} + \zeta_{\mathrm{D}}) \cdot (1 - MC) \cdot \eta_{\mathrm{SE}}} \tag{69}$$

ζ_{F}	Fehlfunktionsrate durch Fehler.
ζ_{D}	Fehlfunktionsrate durch Störungen (Malfunction rate due to disturbance).
R_{MT}	Zuverlässigkeit mit Fehlfunktionsbehandlung (Reliability with malfunction treatment).
η_{SE}	Anteil der sicherheitsgefährdenden Fehlfunktionen.

Effektive Testanzahl

Effektive Testanzahl $n_{[\mathrm{eff}]}$ ist die äquivalente Anzahl der Tests, für die alle erkennbaren Fehler beseitigt werden.



Unterschiede zwischen der mittleren MF-Rate je Fehler während des Tests, für die die verursachenden Fehler beseitigt werden, und der im Einsatz können durch eine Testlängenskalierung ausgeglichen werden:

$$N_{[\mathrm{eff}]} = c \cdot N_{\mathrm{T}} \quad \text{mit } c = \frac{\bar{\zeta}}{\bar{\zeta}_{\mathrm{T}}} \tag{70}$$

$\mu_{\mathrm{MF}}(N)$	Zu erwartende Anzahl der Fehlfunktionen für N Service-Leistungen oder Tests.
c	Testlängenvergrößerung (Test number enlargement).
N_{T}	Anzahl der Tests (Number of tests).
$\bar{\zeta}$	mittlere Fehlfunktionsrate je Fehler im Einsatz.
$\bar{\zeta}_{\mathrm{T}}$	Mittlere Fehlfunktionsrate je Fehler während des Tests.

- Wenn Fehler während des Test die halbe MF-Rate haben wie im Betrieb, dann erreicht man im Betrieb mit der halben Anzahl von Tests die gleiche Fehlerüberdeckung:

$$c = \frac{\bar{\zeta}}{\bar{\zeta}_\mathrm{T}} = 2; \quad N_{[\mathrm{eff}]} = 2 \cdot N_\mathrm{T}$$

- In Reifeprozessen werden beim Auftreten einer Fehlfunktion zugrundeliegende Fehler nur mit einer Wahrscheinlichkeit $p_\mathrm{FE} \ll 1$ beseitigt:

$$N_{[\mathrm{eff}]} = p_\mathrm{FE} \cdot \#DS \tag{71}$$

- Abweichende mittlere MF-Rate der Modellfehler $\bar{\zeta}_\mathrm{MF}$ von der der tatsächlichen Fehler $\bar{\zeta}_\mathrm{F}$:

$$N_{[\mathrm{eff}]} = c_\mathrm{MF} \cdot N_\mathrm{T} \quad \text{mit } c_\mathrm{MF} = \frac{\bar{\zeta}}{\bar{\zeta}_\mathrm{M}} \tag{72}$$

Die Testanzahl N ist im weiteren die effektive Testanzahl.

$N_{[\mathrm{eff}]}$	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
p_FE	Fehlerbeseitigungswahrsch., dass Fehler, wenn sie eine MF verursachen beseitigt werden.
$\#DS$	Anzahl aller genutzten Service-Leistungen von allen Anwendern zusammen.
c_MF	Fehlermodellspezifische Skalierung der effektiven Testanzahl.
$\bar{\zeta}_\mathrm{M}$	Mittlere Fehlfunktionsrate je Modelfehler während des Tests.

Reifeprozesse

Das Problem immer größerer IT-Systeme

Die zu erwartende Fehleranzahl wächst proportional mit der Systemgröße bzw. dem Entstehungsaufwand, siehe später Gl.

$$\mu_{\mathrm{CF}} = \xi \cdot C \tag{1.91}$$

und die fehlerbezogene Teilzuverlässigkeit sinkt umgekehrt proportional mit der zu erwartenden Fehleranzahl aus den Entstehungsprozessen (vergl. Gl. 1.62, 1.65):

$$R_{\mathrm{F}}(N) \sim \frac{N^{K+1}}{\mu_{\mathrm{CF}}}$$

μ_{CF}	Zu erwartende Anzahl der Fehler aus den Entstehungsprozessen.
ξ	Fehlerentstehungsrate.
C	Metrik für den Entstehungsaufwand oder die Größe des Produkts.
$R_{\mathrm{F}}(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehlern.
N	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
K	Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.

$$R_{\mathrm{F}}(N) \sim \frac{N^{K+1}}{\xi \cdot C}$$

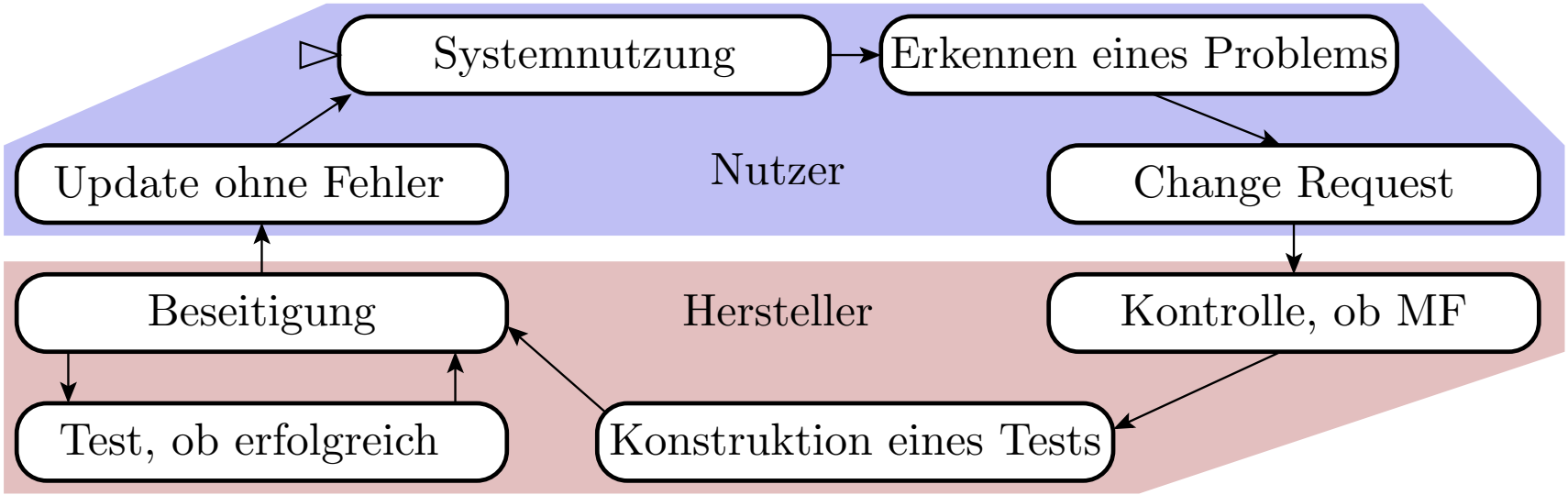
Die Kompensation des Zuverlässigkeitsverlust durch die wachsende Systemgröße verlangt eine Vergrößerung der Testanzahl:

$$N_2 = N_1 \cdot \left(\frac{C_2}{C_1}\right)^{\frac{1}{K+1}} \tag{73}$$

$R_{\mathrm{F}}(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehlern.
N	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
K	Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.
ξ	Fehlerentstehungsrate.
C	Metrik für den Entstehungsaufwand oder die Größe des Produkts.

Reifeprozess

Die Alternative zu immer längeren Testzeiten vor dem Einsatz ist die Installation eines Reifeprozesses mit den Nutzern als Tester.



- Erfassen der MF in der Einsatzphase.
- Sammeln der Daten, um die MF nachzustellen.
- Übermittlung an den Hersteller.
- Suche von Tests für reproduzierbaren Fehlernachweis.
- Beseitigung durch experimentelle Reparatur.
- Herausgabe und Installieren von Updates.

Fehlerbeseitigungswahrscheinlichkeit

Die Fehlerbeseitigungswahrscheinlichkeit p_{FE} ist die bedingte Wahrscheinlichkeit, dass, wenn eine Fehlfunktion auftritt,

1. Nutzer oder System diese erkennen,
2. an den Hersteller einen MF-Report bzw. Änderungswunsch (Change Request) senden,
3. die vermeindliche MF vom Hersteller als solche bestätigt und für die Beseitigung priorisiert wird,
4. der Hersteller Tests für den Nachweis der MF findet,
5. den verursachenden Fehler findet und beseitigt und
6. der Anwender das Update, in dem der Fehler beseitigt ist, übernimmt.

Zu 3: MF-Reports werden in Schubladen vermuteter gleicher Ursache gesammelt. Der Hersteller bevorzugt für die Beseitigung Schubladen, die Fehler mit häufigen schwerwiegenden MF vermuten lassen.

$$p_{\mathrm{FE}} \ll 1$$

p_{FE} Fehlerbeseitigungswahrsch., dass Fehler, wenn sie eine MF verursachen beseitigt werden.

Effektive Testanzahl

Reifende Systeme werden von sehr vielen Nutzern über lange Zeit mit sehr vielen Service-Anforderungen getestet. Geschätze effektive Testanzahl:

$$N = p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot t_{\mathrm{M}} + N_{\mathrm{T}} \tag{74}$$

Genau genommen nimmt die effektive Testanzahl nicht kontinuierich mit der Reifedauer, sondern zeitdiskret mit den Versionsfreigaben ab. Zunahme der effektiven Testanzahl mit der Versions-Anzahl bei gleich langen Release-Intervallen:

$$N = \underbrace{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot t_{\mathrm{VR}}}_{N_{\mathrm{MV}}} \cdot u + N_{\mathrm{T}} \tag{75}$$

N	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
p_{FE}	Fehlerbeseitigungswahrsch., dass Fehler, wenn sie eine MF verursachen beseitigt werden.
μ_{NU}	Zu erwartende Nutzeranzahl (Expected **n**umber of **u**ser).
η_{SU}	Mittlere Anzahl der **S**ervice-Leistungen pro Nutzer (**u**ser) und Nutzungszeit.
t_{M}	Reifedauer (Maturing time).
N_{T}	Effektive Testanzahl Version 0, d.h. der Fehlerbeseitigungsiteration vor dem Einsatz.
t_{VR}	Versionsintervall, Zeit zwischen der Freigabe aufeinanderfolgender Version.
N_{MV}	Erhöhung der effektive Testanzahl mit jeder Version.
u	Versionnummer des reifenden Objekts, Zählweis 0, 1, 2, ...

Abnahme der Fehleranzahl mit der Reifedauer

In diesem Abschnitt wird im weiteren nur der Fall betrachtet:

- keine Entstehung neuer Fehler bzw.
- Beseitigung neu entstandener Fehler vor Versionsfreigabe.

Mit Gl. 1.74 bzw. 1.75 in

$$\mu_{\mathrm{F}}\left(N_2\right) = \mu_{\mathrm{F}}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \tag{1.58}$$

verringert sich die zu erwartende Fehleranzahl etwa mit der K-ten Potenz mit der Reifedauer bzw. Versionsanzahl:

$$\mu_{\mathrm{F}}\left(t_{\mathrm{M}}\right) = \mu_{\mathrm{F}}\left(t_{\mathrm{M0}}\right) \cdot \left(\frac{t_{\mathrm{M}}+t_{\mathrm{V0}}}{t_{\mathrm{M0}}+t_{\mathrm{V0}}}\right)^{-K} \quad \text{mit} \quad t_{\mathrm{V0}} = \frac{N_{\mathrm{T}}}{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}}} \tag{76}$$

$$\mu_{\mathrm{F}}\left(u_i\right) = \mu_{\mathrm{F}}\left(u_j\right) \cdot \left(\frac{u_i+u_{\mathrm{V0}}}{u_j+u_{\mathrm{V0}}}\right)^{-K} \quad \text{mit} \quad u_{\mathrm{V0}} = \frac{N_{\mathrm{T}}}{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot t_{\mathrm{VR}}} \tag{77}$$

$\mu_{\mathrm{F}}\left(t_{\mathrm{M}}\right)$	Zu erwartende Anzahl der nicht beseitigten Fehler in Abhängigkeit von der Reifedauer.
t_{M0}	Bezugsreifedauer.
t_{V0}	Reifedauer vor Freigabe von Version null.
K	Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.
$\mu_{\mathrm{F}}\left(u\right)$	zu erwartende Anzahl der nicht beseitigten Fehler in Abhängigkeit von der Versionszahl.
u_{V0}	Verhältnis equivalente Reifedauer vor Version null zum Versionsintervall.

Fehlerbezogene Teilzuverlässigkeit

Mit Gl. 1.74 bzw. 1.75 in

$$R_{\mathrm{F}}\left(N_2\right) = R_{\mathrm{F}}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{K+1} \tag{1.66}$$

wächst die fehlerbezogene Teilzuverlässigkeit etwa mit der $k+1$-ten Potenz der Reifedauer bzw. Versionsnummer:

$$R_{\mathrm{F}}\left(t_{\mathrm{M}}\right) = R_{\mathrm{F}}\left(t_{\mathrm{M0}}\right) \cdot \left(\frac{t_{\mathrm{M}}+t_{\mathrm{V0}}}{t_{\mathrm{M0}}+t_{\mathrm{V0}}}\right)^{K+1} \tag{78}$$

$$R_{\mathrm{F}}\left(u_i\right) = R_{\mathrm{F}}\left(u_j\right) \cdot \left(\frac{u_i+u_{\mathrm{V0}}}{u_j+u_{\mathrm{V0}}}\right)^{K+1} \tag{79}$$

mit t_{V0} und u_{V0} aus den Gl. 1.76 und 1.77.

$R_{\mathrm{F}}\left(t_{\mathrm{M}}\right)$	Fehlerbezogene Teilzuverlässigkeit in Abhängigkeit von der Reifedauer.
t_{M0}	Bezugsreifedauer.
t_{V0}	Reifedauer vor Freigabe von Version null.
K	Formfaktor der Verteilung der Fehlfunktionsrate $(0 < K < 1)$.
$R_{\mathrm{F}}\left(u\right)$	Fehlerbezogene Teilzuverlässigkeit in Abhängigkeit von der Versionszahl.
u	Versionnummer des reifenden Objekts, Zählweis 0, 1, 2, ...
u_{V0}	Verhältnis equivalente Reifedauer vor Version null zum Versionsintervall.

Zunahme der Zuverlässigkeit und Sicherheit

Bei vernachlässigbarer MF-Rate durch Störungen $\zeta_{\mathrm{D}} \ll \zeta_{\mathrm{F}}$ ist nach

$$R = \frac{1}{\zeta_{\mathrm{F}} + \zeta_{\mathrm{D}}} \tag{1.67}$$

die Gesamtzuverlässigkeit:

$$R = R_{\mathrm{F}}$$

Zuverlässigkeit und Sicherheit mit Fehlfunktionsbehandlung:

$$R_{\mathrm{MT}} = \frac{R}{1 - MC} \tag{1.32}$$

$$S_{\mathrm{MT}} = \frac{R_{\mathrm{MT}}}{\eta_{\mathrm{SE}}} \tag{1.49}$$

$$S_{\mathrm{MTSF}} = \frac{R_{\mathrm{MT}} \cdot R_{\mathrm{SF}}}{(R_{\mathrm{MT}} + R_{\mathrm{SF}}) \cdot \eta_{\mathrm{SESF}}} \tag{1.51a}$$

S_{MT}	Sicherheit mit Fehlfunktionsbehandlung.
R_{MT}	Zuverlässigkeit mit Fehlfunktionsbehandlung (Reliability with malfunction treatment).
η_{SE}	Anteil der sicherheitsgefährdenden Fehlfunktionen.
S_{MTSF}	Sicherheit mit Fehlfunktionsbehandlung und zusätzlichen Sicherheitsfunktionen.
η_{RSF}	Zuverlässigkeitsverringerung durch MF der zusätzliche Sicherheitsfunktionen.
η_{SESF}	Verringerter Anteil sicherheitsgefährdender MF mit Sicherheitsfunktionen.
R_{SF}	Zuverlässigkeit der zusätzlichen Sicherheitsfunktionen.

Systeme mit hoher Zuverlässigkeit

Hohe Zuverlässigkeit verlangt:

- hohe Zuverlässigkeit $R\left(n_{\mathrm{M0}}\right)$ bei Produktfreigabe,
- hohe MC der Fehlerfunktionsbehandlung und eine
- eine hohe effektive Testanzahl

$$N = p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot t_{\mathrm{M}} + N_{\mathrm{T}} \tag{1.74}$$

  - hohe Wahrscheinlichkeit p_{FE}, dass, wenn eine MF beobachtet wird, der verursachenden Fehler beseitigt wird,
  - eine große zu erwartende Anzahl von Nutzern μ_{NU},
  - viele genutzte Service-Leistungen je Nutzer und Zeit η_{ST} und
  - eine lange Reifezeit t_{M}.

Systeme, die viele Jahre gereift sind, haben hohe, auf anderem Wege unerreichbare Zuverlässigkeiten. Schwer ersetzbar durch neue Systeme (siehe Jahr2000-Problem).

Neue / alternative Systeme sind in den ersten Nutzungsjahren vielfach viel unzuverlässer als die Systeme, die sie ersetzen. Wenn das die Akzeptanz beeinträchtigt, reifen sie auch nicht.

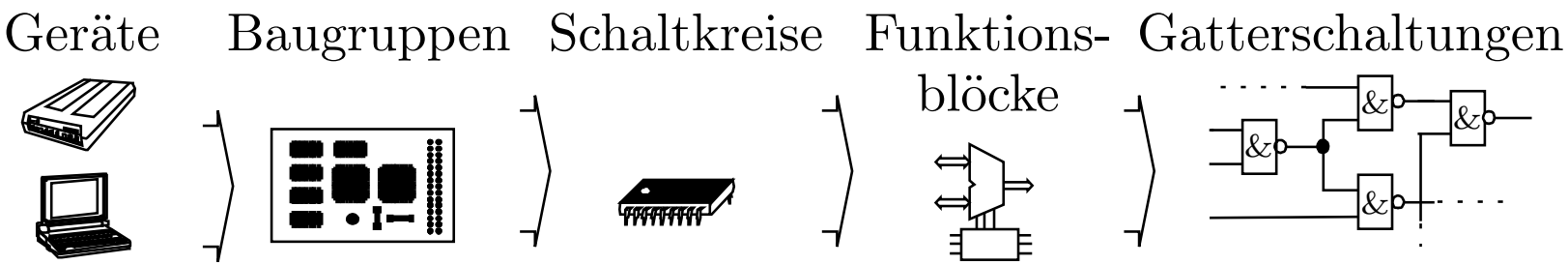
MF-Vermeidung – Lernprozesse der Nutzer

Bei der Einarbeitung in ein neues IT-System ist es typisch, dass zu Beginn häufig und mit zunehmender Nutzung immer seltener Fehlfunktionen auftreten, weil der Nutzer lernt, die Fehler und Schwachstellen im System zu umgehen (siehe Folie 1.74 *Fehlerumgehung*). Auch hier ist ein Zuverlässigkeitswachtum mit der Nutzungdauer zu beobachten.

Wenn Wissen über Fehlerumgehungsmöglichkeiten weitergegeben wird, z.B. über Foren, FAQ-Seiten, lernt die gesamte Nutzergemeinschaft. Summierung der Nutzungsdauern t_{M} vieler Nutzer.

Modularer Test

IT-Systeme sind modular



- Rechner-Systeme bestehen aus Rechnern, EA-Geräten, Druckern, Netzwerkkomponenten, ...
- Rechner und Zubehör, ...bestehen aus Hard- und Software.
- Software besteht aus Programmbausteinen, diese sind aus Anweisungen zusammengesetzt, die ihrerseits mit Maschinenbefehlen nachgebildet werden.
- Maschinenbefehle sind Service-Leistungen der Hardware. Die Hardware besteht aus Funktionsbausteinen, diese meist aus Gattern und diese wiederum aus Transistoren.
- Übergeordnete Systeme erben die Funktionen und Fehler ihrer Teilsysteme.

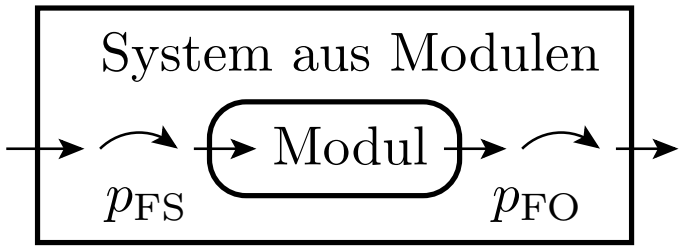
Modularität ist wichtig für ...

- Entwurfsprozess: Aufspaltung in Teilaufgaben, Nachnutzung von Teilentwürfen, ...
- Test: Gründlicher Test der Komponenten vor Einfügung in das übergeordnete System.
- Reparatur: Austauschbare Komponenten.
- Erhöhung der effektive Testsatzlänge für komponenteninterne Fehler.

Effektive Testanzahl, Testorganisation

MF-Rate Systems für modulinterne Fehler:

$$\bar{\zeta}_{\mathrm{Sys}} = p_{\mathrm{FS}} \cdot p_{\mathrm{FO}} \cdot \bar{\zeta}_{\mathrm{Mod}}$$



Erhöhung der effektiven Testanzahl:

$$N_{[\mathrm{eff}]} = c \cdot N_{\mathrm{T}} \quad \text{mit } c = \frac{\bar{\zeta}_{\mathrm{Mod}}}{\bar{\zeta}_{\mathrm{Sys}}} = \frac{1}{p_{\mathrm{FE}} \cdot p_{\mathrm{FO}}} \gg 1 \tag{80}$$

In einer vernünftige Prüftechnologie werden Module vor Einbau in ein System gründlich getestet. Die Tests des übergeordneten Systems überprüfen hauptsächlich die Verbindungen zwischen den Modulen.

$\bar{\zeta}_{\mathrm{Sys}}$	Mittlere MF-Rate modulinterner Fehler im Gesamtsystem.
p_{FS}	Fehleranregungswahrscheinlichkeit (Probability of fault stimulation).
p_{FO}	Fehlerbeobachtbarkeitswahrscheinlichkeit (Probability of fault observation).
$\bar{\zeta}_{\mathrm{Mod}}$	Mittlere MF-Rate je Fehler beim isolierter Modultest.
c	Testlängenvergrößerung (Test number enlargement).
N	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
N_{T}	Hier Anzahl der Modultests.

Ausbeute, Defektanteil

Defektanteil

Bei nicht reparierbaren Systemen und tauschbaren Komponenten interessiert nicht die Fehleranzahl, sondern der Anteil der defekten Produkte mit mindestens einem Fehler. Defektanteil:

$$DL = \left.\frac{\#DP}{\#P}\right|_{\mathrm{ACR}} \tag{81}$$

Maßeinheiten dpu (defects per unit), dpm (defects per million):

$$1\,\mathrm{dpu} = 10^6\,\mathrm{dpm}$$

Für zu erwartende Fehleranzahl $\mu_\mathrm{F} \ll 1$ (fast nie mehr als ein Fehler je Produkt):

$$DL = \mu_\mathrm{F}$$

DL	Defektanteil (Defect level).
$\#P$	Anzahl der Produkte (Number of products).
$\#DP$	Anzahl der davon defekten Produkte.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.
μ_F	Zu erwartende Fehleranzahl.

Defektüberdeckung und Ausbeute

Die Defektüberdeckung ist der Anteil der erkannten defekten Produkte:

$$DC = \left.\frac{\#IDP}{\#DP}\right|_{\mathrm{ACR}} \tag{82}$$

Die Ausbeute ist der Anteil der als gut befundenen Produkte

$$Y = 1 - \left.\frac{\#IDP}{\#P}\right|_{\mathrm{ACR}} \tag{83}$$

und hängt vom Defektanteil nach der Fertigung und der Defektüberdeckung des Tests ab, mit dem die fehlerhaften Teile aussortiert werden:

$$Y = 1 - DL_{\mathrm{M}} \cdot DC \tag{84}$$

DC	Defektüberdeckung (defect coverage), Anteil der erkennbar defekten Produkte.
$\#IDP$	Anzahl der identifizierten defekten Produkte.
$\#DP$	Anzahl der davon defekten Produkte.
Y	Ausbeute (Yield).
$\#P$	Anzahl der Produkte (Number of products).
DL_{M}	Defektanteil nach der Fertigung vor Ersatz erkannter defekter Bauteile.

$$Y = 1 - DL_{\mathrm{M}} \cdot DC \tag{1.84}$$

Ohne Test ist $DC = 0$ und die Ausbeute $Y = 1$.

Beispiel 1.7: Ausbeute und Defektanteil

Ausbeute $Y = 95\%$, abgeschätzt mit einem Test, der $DC = 50\%$ der fehlerhaften Objekte erkennt. Gesucht Defektanteil.

Umstellung von Gl. 1.84 nach dem Defektanteil:

$$DL = \frac{1 - Y}{DC} = \frac{0{,}95\%}{50\%} = 10\%$$

Y	Ausbeute (Yield).
DL	Defektanteil (Defect level).
DC	Defektüberdeckung (defect coverage), Anteil der erkennbar defekten Produkte.

Defektanteil nach Ersatz

Beim Aussortieren der erkannten fehlerhaften Objekte verringern sich die Anzahl der fehlerhaften Objekte in Zähler und Nenner jeweils um die Anzahl der erkannten fehlerhaften Objekte $\#P \cdot DL_{\mathrm{M}} \cdot DC$:

$$DL = \frac{\#P \cdot DL_{\mathrm{M}} - \#P \cdot DL_{\mathrm{M}} \cdot DC}{\#P - \#P \cdot DL_{\mathrm{M}} \cdot DC} = \frac{DL_{\mathrm{M}} \cdot (1 - DC)}{1 - DL_{\mathrm{M}} \cdot DC} \tag{85}$$

Anzahl der zu fertigenen Produkte für $\#P$ als gut befundene Produkte:

$$\#P_{\mathrm{M}} = \frac{\#P}{1 - DL_{\mathrm{M}} \cdot DC}$$

Ersatz des Defektanteils nach der Fertigung durch die Ausbeute:

$$Y = 1 - DL_{\mathrm{M}} \cdot DC \tag{1.84}$$

$$DL = \frac{(1-Y) \cdot (1-DC)}{DC \cdot Y} \tag{86}$$

DL	Defektanteil nach Ersatz der Produkte mit erkannten Fehlern.
$\#P$	Anzahl der Produkte (Number of products).
DL_{M}	Defektanteil nach der Fertigung vor Ersatz erkannter defekter Bauteile.
DC	Defektüberdeckung (defect coverage), Anteil der erkennbar defekten Produkte.
Y	Ausbeute (Yield).

Beispiel 1.8: Defektanteil getesteter Schaltkreise

Schaltkreisausbeute $Y = 80\%$*, Defektanteil nach Test und Aussortieren der erkannten defekten ICs sei* $DL = 1000\,\mathrm{dpm}$*. Gesucht* DC*.*

$$DL = \frac{(1-Y)\cdot(1-DC)}{DC\cdot Y} = 1000\,\mathrm{dpm}$$
$$DC = \frac{1-Y}{DL\cdot Y+1-Y} = \frac{1-80\%}{10^{-3}\cdot 80\%+1-80\%} = 99{,}6\%$$

Für getestete ICs findet man in der Literatur $DL = 200\,\mathrm{dpm}$ bis $1000\,\mathrm{dpm}$, für die Haftfehlerüberdeckungen der Testsätze nur $FC_{\mathrm{SA}} = 95\%$ bis 99%. Der Anteil der nicht nachweisbaren Haftfehler ist offenbar eine Zehnerpotenz größer ist als der Anteil der nicht erkennbaren defekten ICs (siehe Abschn. 5.1.4 *Nachweisbeziehungen*):

- Ist DC viel höher als die Haftfehlerüberdeckung oder
- sind die Angaben für DL der getestenen ICs viel zu optimistisch?

DC	Defect coverage, percentage of detectable defective devices.
DL	Defect level after replacing products with detected faults.
Y	Yield.

Systeme aus getesteten Teilsystemen

System aus getesteten als gut befundenen Bauteilen. Jedes Bauteil hat einem kleinen Defektanteil $DL_i \ll 1$. Der Baugruppentest kontrolliert hauptsächlich auf Verbindungsfehler, aber fast nicht mehr auf Bauteilfehler. Warum?
Zu erwartende Fehleranzahl des Gesamtsystem:

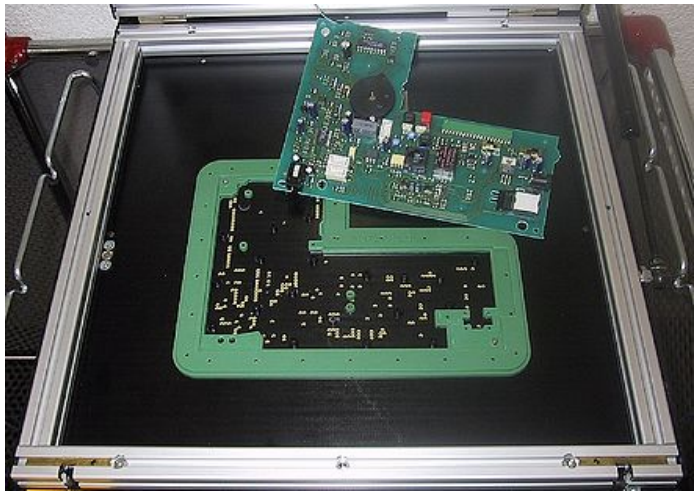
$$\mu_{\mathrm{FSys}} = \mu_{\mathrm{FCon}} \cdot (1 - FC_{\mathrm{Con}}) + \sum_{i=1}^{\#Prt} DL_i \tag{87}$$

Für $\mu_{\mathrm{FSys}} \ll 1$:

$$DL_{\mathrm{Sys}} = \mu_{\mathrm{FSys}} \tag{88}$$

μ_{FSys}	zu erwartende Fehleranzahl des Gesamtsystem.
μ_{FCon}	Zu erwartende Anzahl der Verbindungsfehler (connection faults).
FC_{Con}	Fehlerübedeckung für Verbindungsfehler (Fault coverange for connection faults).
$\#Prt$	Anzahl der Bauteile (Number of parts).
DL_i	Defektanteil von Bauteil i (Defect level of component i).
DL_{Sys}	Defektanteil des Systems (Defect level of the system).

Leiterplatten



Bestückte Leiterplatten bestehen aus geprüften Bauteilen und werden für den Test in der Regel auf einem Nadelbett gespannt. Zielfehler: Leitungsunterbrechungen, Kurzschlüsse und Bestückungsfehler.

(Kurzschüsse und Unterbrechungen) und Bestückungsfehler praktisch $FC_{\mathrm{Con}} = 1$ und kein Nachweis für defekte Bauteile:

$$\mu_{\mathrm{FSys}} = \sum_{i=1}^{\#Prt} DL_i \tag{89}$$

Für $\mu_{\mathrm{FSys}} \ll 1$ hat das Gesamtsystem den Defektanteil:

$$DL_{\mathrm{Sys}} = \mu_{\mathrm{FSys}} \tag{1.88}$$

μ_{FSys}	zu erwartende Fehleranzahl des Gesamtsystem.
$\#Prt$	Anzahl der Bauteile (Number of parts).
DL_i	Defektanteil von Bauteil i (Defect level of component i).

Beispiel 1.9: Defektanteil einer Baugruppe

Anzahl und Defektanteil für alle Bauteiltypen:

Typ	Anzahl	DL_i
Leiterplatte	1	20 dpm
Schaltkreise	20	200 dpm
diskrete Bauteile	35	10 dpm
Lötstellen	560	1 dpm

$$DL_{\mathrm{Sys}} = \mu_{\mathrm{FSys}} = 10\,\mathrm{dpm} + 20 \cdot 200\,\mathrm{dpm} + 35 \cdot 10\,\mathrm{dpm} + 560 \cdot 1\,\mathrm{dpm}$$
$$= 5000\,\mathrm{dpm} = 0{,}005\,\mathrm{dpu}$$

Etwa jedes 200ste Gerät enthält ein nicht erkanntes defektes Bauteil. Rechner-Hardware kann defekte Schaltkreise enthalten, aber nur solche, die ganz selten MF verursachen.

DL_{Sys}	Defektanteil des Systems (Defect level of the system).
DL_i	Defektanteil von Bauteil i (Defect level of component i).
dpm	Anzahl der defekten Objekte pro Million (defecs per million).

Zusammenfassung

4.1 Beseitigungsiteration, 4.2 Fehlerdiagnose

Fehlerbeseitigung: Iteration aus Beseitigungsversuchen für hypothetische Fehler und Erfolgskontrolle durch Testwiederholung:

- Beseitigung aller erkennbaren Fehler.
- Rückbau nach erfolglosen Reparaturversuchen.
- In modularen Systemen durch systematisches Tauschen.

Fehlerdiagnose: Abschätzung von Ort-, Ursache und Beseitigungsmöglichkeiten von Fehlern aus Testergebnissen:

- Pareto-Prinzip: Für die Mehrheit der Fehler ist in der Regel nur ein kleiner Teil möglicher Ursachen verantwortlich.
- Rückverfolgung entgegen den Berechnungs. bzw. Signalfluss.

Reparaturgerechter Entwurf:

- Tauschbare Module, deterministische Verhalten,
- gerichteter Berechnungfluss, Fehlerisolation, ...

Bei einer vernünftigen Reparaturtechnologie ist der Anteil der beseitigten Fehler fast so groß wie die Fehlerüberdeckung der Tests.

4.3 Test

Einteilung der Testarten:

- Statische Tests: direkte Kontrolle von Merkmalen.
- Dynamische Tests: Ausprobieren der Systemfunktion.

Kenngrößen:

- Fehlerüberdeckung, Anteil der nachweisbaren Fehler:

$$FC = \frac{\#F_{\mathrm{D}}}{\#F}\Big|_{\mathrm{ACR}} \tag{1.52}$$

- Phantom-MF-Rate während des Tests, Anteil der Testausgaben, die als fehlerhaft erkannt werden, aber in Wirklichkeit korrekt sind:

$$\zeta_{\mathrm{PhanT}} = \frac{\#PM}{N}\Big|_{\mathrm{ACR}} \tag{1.53}$$

Vor der Fehlerbeseitigung »Test der Tests« auf Phantomfehler!

Auswahlstrategien für dynamische Tests:

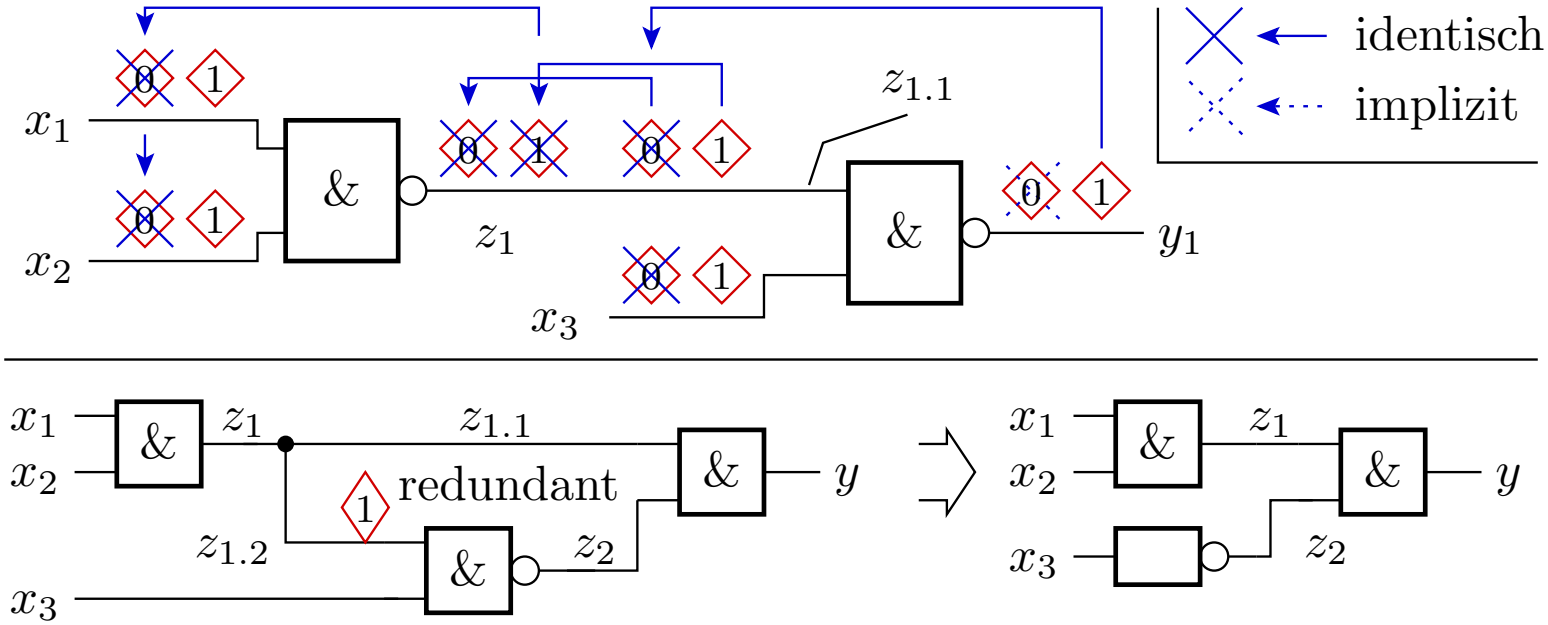
- Fehlerorientiert: Zusammenstellung von Modellfehlern oder Mutationen. Suche von Eingaben, bei denen diese MF verursachen.
- Zufällig: Auswahl ohne Rücksicht auf Fehlerannahmen.
- Mischformen.

Auch bei fehlerorientierte Auswahl ist der Nachweis der tatsächlichen Fehler Zufall.

Fehlermodell: Algorithmus zur Berechnung einer Menge möglicher Verfälschungen aus einer Entwurfsbeschreibung.

Modellfehler: einzelne unterstellten Verfälschungen.

4.4 Haftfehler



Beispiel für ein Fehlermodell:

- Initialfehlermenge: je Gatteranschluss sa0 und sa1.
- Zusammenfassen identisch nachweisbarer Fehler, streichen redundanter und implizit nachweisbarer Fehler.
- Die resultierende Fehlermenge dient zur Fehlersimulation und Testberechung.

4.5 Zuverlässigkeit nach Fehlerbeseitigung

Wenn alle mit n dynamischen Tests erkannten Fehler beseitigt werden, dann ist die MF-Rate je nicht beseitigter Fehler im Mittel $\leq 1/N$.
MF-Rate durch Fehler nicht größer als:

$$\zeta_{\mathrm{F}} \leq \frac{\mu_{\mathrm{F}}}{N}$$

Typische Abnahme der zu erwartenden Anzahl der nicht beseitigten Fehler mit der Testanzahl:

$$\mu_{\mathrm{F}}(N_2) = \mu_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \tag{1.58}$$

Daraus lässt sich auf die Verteilung und Dichte der MF-Rate und daraus wiederum auf die Abnahme MF-Rate mit N schließen:

$$\zeta_{\mathrm{F}}(N_2) = \zeta_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-(K+1)} \tag{1.61}$$

$$\zeta_{\mathrm{F}}(N) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{N} \tag{1.60}$$

$$K = \log\left(\frac{\zeta_{\mathrm{F}}(N_1)}{\zeta_{\mathrm{F}}(N_2)}\right) / \log\left(\frac{N_2}{N_1}\right) - 1 \tag{1.64}$$

Vortests

Mit Vortests vor den langen Zufallstests für die Zuverlässigkeit

- statisch Tests (z.B. Syntax)
- dynamische Grobtests, ob überhaupt etwas funktioniert,
- fehlerorientierte Tests z.B. für Grenzwerte, ...

werden alle Fehler, die die Funktionalität komplett oder fast vollständig beeinträchtigen gefunden und beseitigt.

Fehleranzahl und MF-Rate zu Beginn des Zuverlässigkeitstest:

$$\mu_{\mathrm{F}}\left(N_0\right) = \mu_{\mathrm{FCR}} \cdot \left(1 - FC_{\mathrm{PT}}\right) \tag{1.62}$$

$$\zeta_{\mathrm{F}}\left(N_0\right) = \frac{K \cdot \mu_{\mathrm{F}}(N_0)}{N_0} \tag{1.63}$$

Effektive Testanzahl, Zuverlässigkeit, Sicherheit

Die effektive Testanzahl ist die äquivalente Service-Anzahl, für die alle verursachenden Fehler beseitigt werden:

$$N_{[\mathrm{eff}]} = c \cdot N_{\mathrm{T}} \quad \text{mit } c = \frac{\bar{\zeta}}{\bar{\zeta}_{\mathrm{T}}} \tag{1.70}$$

- Testlängenskalierung bei Reifeprozessen:

$$N = p_{\mathrm{FE}} \cdot \#DS \tag{1.71}$$

- Testlängenskalierung für Modellfehler

$$N_{[\mathrm{eff}]} = c_{\mathrm{MF}} \cdot N_{\mathrm{T}} \quad \text{mit } c_{\mathrm{MF}} = \frac{\bar{\zeta}}{\bar{\zeta}_{\mathrm{M}}} \tag{1.72}$$

Die fehlerbezogene Teilzuverlässigkeit ohne MF-Behandlung nimmt überproportional mit der Testanzahl zu:

$$R_{\mathrm{F}}(N) = \frac{N}{K \cdot \mu_{\mathrm{F}}(N)} \tag{1.65}$$

$$R_{\mathrm{F}}(N_2) = R_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{K+1} \tag{1.66}$$

Die Zuverlässigkeit mit MF-Behandlung und die Sicherheit nehmen proportional zur Zuverlässsigkeit ohne MF-Behandlung zu.

1.4.6 Reifeprozess

Die Zuverlässigkeit im Einsatz sinkt umgekehrt proportional mit der Systemgröße bzw. dem Entstehungsaufwand:

- Erforderliche Vergrößerung der Testanzahl zu Kompensation des Zuverlässigkeitsverlusts:

$$N_2 = N_1 \cdot \left(\frac{C_2}{C_1}\right)^{\frac{1}{K+1}} \tag{1.73}$$

Fortsetzung der Fehlerbeseitigung im Einsatz mit Nutzern als Tester:

- effektive Testanzahl:

$$N = p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot t_{\mathrm{M}} + N_{\mathrm{T}} \tag{1.74}$$

- effektive Testanzahl je Update-Intervall:

$$N = \underbrace{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot t_{\mathrm{VR}}}_{N_{\mathrm{MV}}} \cdot u + N_{\mathrm{T}} \tag{1.75}$$

- Abnahme der Fehleranzahl mit der Reifedauer:

$$\mu_{\mathrm{F}}\left(t_{\mathrm{M}}\right) = \mu_{\mathrm{F}}\left(t_{\mathrm{M0}}\right) \cdot \left(\frac{t_{\mathrm{M}} + t_{\mathrm{V0}}}{t_{\mathrm{M0}} + t_{\mathrm{V0}}}\right)^{-K} \tag{1.76}$$

$$t_{\mathrm{V0}} = \frac{N_{\mathrm{T}}}{p_{\mathrm{FEM}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}}} \tag{1.76a}$$

- Abnahme der Fehleranzahl mit der Versionsanzahl:

$$\mu_{\mathrm{F}}\left(u_i\right) = \mu_{\mathrm{F}}\left(u_j\right) \cdot \left(\frac{u_i + u_{\mathrm{V0}}}{u_j + u_{\mathrm{V0}}}\right)^{-K} \tag{1.77}$$

- Zunahme der fehlerbezogene Teilzuverlässigkeit:

$$R_{\mathrm{F}}\left(t_{\mathrm{M}}\right) = R_{\mathrm{F}}\left(t_{\mathrm{M0}}\right) \cdot \left(\frac{t_{\mathrm{M}} + t_{\mathrm{V0}}}{t_{\mathrm{M0}} + t_{\mathrm{V0}}}\right)^{K+1} \tag{1.78}$$

$$R_{\mathrm{F}}\left(u_i\right) = R_{\mathrm{F}}\left(u_j\right) \cdot \left(\frac{u_i + u_{\mathrm{V0}}}{u_j + u_{\mathrm{V0}}}\right)^{K+1} \tag{1.79}$$

Zuverlässigkeit mit MF-Behandlung und Sicherheit im Einsatz, wenn die MF-Rate durch Störungen vernachlässigbar ist oder alle MF-durch Störungen erkannt und beseitigt werden $(R = R_{\mathrm{F}})$:

$$R_{\mathrm{MT}} = \frac{R}{1 - MC} \tag{1.32}$$

$$S_{\mathrm{MT}} = \frac{R_{\mathrm{MT}}}{\eta_{\mathrm{SE}}} \tag{1.49}$$

- Lange Reifeprozesse über Jahre und Jahrzehnte erzielen auf andere Weise unerreichbare Zuverlässigkeiten.
- Alte, lange gereifte Software ist schwer zu ersetzen, weil gleichwertiger Ersatz auch lange bei vielen Nutzern reifen muss.

1.4.7 Modularer Test

Modularität ist wichtig für:

- Entwurfsprozess: Aufspaltung in Teilaufgaben, Nachnutzung von Teilentwürfen, ...
- Test: Gründlicher Test der Komponenten vor Einfügung in das übergeordnete System.
- Reparatur: Austauschbare Komponenten.
- Erhöhung der effektive Testsatzlänge für komponenteninterne Fehler:

$$N_{[\mathrm{eff}]} = c \cdot N_{\mathrm{T}} \quad \text{mit } c = \frac{\bar{\zeta}_{\mathrm{Mod}}}{\bar{\zeta}_{\mathrm{Sys}}} = \frac{1}{p_{\mathrm{FE}} \cdot p_{\mathrm{FO}}} \gg 1 \tag{1.80}$$

1.4.8 Defektanteil, Ausbeute

Bei nicht reparierbaren Systemen und tauschbaren Komponenten interessiert statt der zu erwartenden Fehleranzahl, der Fehleanteil:

$$DL = \left.\frac{\#DP}{\#P}\right|_{\mathrm{ACR}} \tag{1.81}$$

Defektüberdeckung als Anteil der erkennbaren defekten Produkte:

$$DC = \left.\frac{\#IDP}{\#DP}\right|_{\mathrm{ACR}} \tag{1.82}$$

Ausbeute: Anteil der als gut erkannten Produkte.

$$Y = 1 - \left.\frac{\#IDP}{\#P}\right|_{\mathrm{ACR}} \tag{1.83}$$

$$Y = 1 - DL_{\mathrm{M}} \cdot DC \tag{1.84}$$

Defektanteil nach Ersatz der erkannten defekten Teile:

$$DL = \frac{DL_{\mathrm{M}} \cdot (1 - DC)}{1 - DL_{\mathrm{M}} \cdot DC} \tag{1.85}$$

$$DL = \frac{(1 - Y) \cdot (1 - DC)}{DC \cdot Y} \tag{1.86}$$

Modulare Systeme aus getesteten Bauteilen

Fehleranzahl:

$$\mu_{\mathrm{FSys}} = \mu_{\mathrm{FCon}} \cdot (1 - FC_{\mathrm{Con}}) + \sum_{i=1}^{\#Prt} DL_i \tag{1.87}$$

Für $\mu_{\mathrm{FSys}} \ll 1$:

$$DL_{\mathrm{Sys}} = \mu_{\mathrm{FSys}} \tag{1.88}$$

Für getestete Leiterplatten gilt in der Regel $FC_{\mathrm{Con}} = 1$. Die Fehleranzahl ist die Summe der Defektanteile aller Bauteile:

$$\mu_{\mathrm{FSys}} = \sum_{i=1}^{\#Prt} DL_i \tag{1.89}$$

Für $\mu_{\mathrm{FSys}} \ll 1$ gilt auch hier Gl.1.88.

Fehlervermeidung

Geplante Themen

Fehlervermeidung	Fehlerbeseitigung	FF-Behandlung
Beseitigung von Fehler-entstehungsursachen	Test und Beseitigung erkannter Fehler	Überwachung, robuste R. Fehlertoleranz Störungen

5.1 Fehlerentstehung
Modellierung von Entstehungsprozessen als Service-Leister und Fehler als dessen MF.

5.2 Determinismus und Zufall
Fehlervermeidung ist ein Reifeprozess für Entstehungsprozesse. Insbesondere manuellen Arbeitsschritten fehlt jedoch der Determinismus. Wie reifen nicht deterministische Entstehungsprozesse?

5.3 Projekte, Vorgehensmodelle
Reifeprozesse benötigen eine große Wiederholanzahl gleicher Abläufe, um aus erkannten Fehlern lernen zu können. Projekte sind einmalige Entstehungsabläufe. Vorgehensmodelle vereinheitlichen das Vorgehen, um dennoch aus Fehlern lernen zu können.

Fehlerentstehung

Fehler als MF der Entstehungsprozesse

Ein Entstehungsprozess ist ein Service

- mit Entwurfsvorgaben bzw. Material (-Eigenschaften) als Eingabe
- und Entwurfsergebnissen bzw. Produkten (oder ihren Eigenschaften) als Ausgabe.

Verlässlichkeit beschreibbar mit denselben Kenngrößen:

- Verfügbarkeit, MF-Rate (hier die Fehlerentstehungsrate),
- Zuverlässigkeit, Sicherheit, ...

Sicherung der Verlässl. erfordert vergleichbare Maßnahmen.

Fehlervermeidung ist ein Reifeprozess für einen Entstehungsprozess:

- Überwachung der entstehenden Entwürfe oder Produkte.
- Beseitigung erkannter Fehlerentstehungsursachen.

CS, MF Korrekte Service-Leistung, Fehlfunktion.

Fehlerentstehungsraten und -metriken

Die Fehlerentstehungsrate ist die Anzahl der entstehenden Fehler bezogen auf eine Metrik C für den Entstehungsaufwand:

$$\xi = \left.\frac{\#F_{\mathrm{C}}}{C}\right|_{\mathrm{ACR}} \tag{90}$$

Bei konstanter Fehlerentstehungsrate nimmt die zu erwartende Fehleranzahl proportional zum Entstehungsaufwand zu:

$$\mu_{\mathrm{CF}} = \xi \cdot C \tag{91}$$

Die Metrik für den Entstehungsaufwand kann sich auch auf die Systemgröße beziehen:

- Dokumentationen: Fehler pro Seite,
- Programmcode: Fehler je 1000 NLOC (Netto Lines of Code),
- Schaltkreise: Fehler je 10^6 Transistoren, ...

ξ	Fehlerentstehungsrate.
$\#F_{\mathrm{C}}$	Anzahl der Fehler aus den Entstehungsprozessen.
C	Metrik für den Entstehungsaufwand oder die Größe des Produkts.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.
μ_{CF}	Zu erwartende Anzahl der Fehler aus den Entstehungsprozessen.

Beispiel 1.10: Programmfehler

$\xi = 30$ Fehler / 1000 NLOC, Programm mit $C = 2000$ NLOC.

Wie groß ist die zu erwartende Anzahl der Programmierfehler vor Test und Fehlerbeseitigung?

$$\mu_{\mathrm{CF}} = \xi \cdot C = \frac{30\,\mathrm{Fehler} \cdot 2000\,\mathrm{NLOC}}{1000\,\mathrm{NLOC}} = 60\,\mathrm{Fehler}$$

Beispiel 1.11: Schaltkreisfehler

$\xi = 1$ Fehler je 10^6 Transistoren. Schaltkreis mit $C = 10^5$ Transistoren.

Wie groß ist die zu erwartende Anzahl der Fehler je Schaltkreis vor dem Aussortieren der erkennbar defekten Schaltkreise?

$$\mu_{\mathrm{CF}} = \xi \cdot C = \frac{1\,\mathrm{Fehler} \cdot 10^5\,\mathrm{Transistoren}}{10^6\,\mathrm{Transistoren}} = 0{,}1\mathrm{Fehler}$$

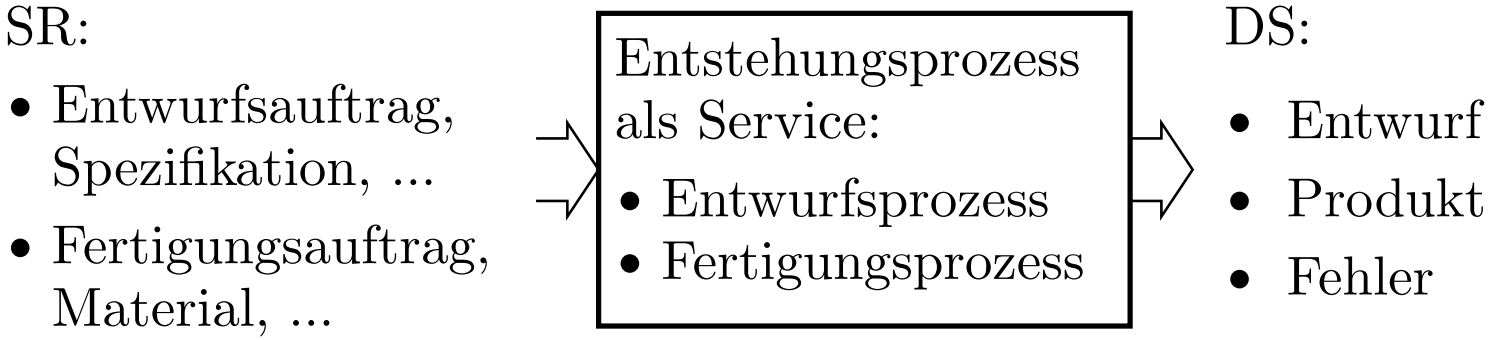
ξ	Fehlerentstehungsrate.
C	Metrik für den Entstehungsaufwand oder die Größe des Produkts.
μ_{CF}	Zu erwartende Anzahl der Fehler aus den Entstehungsprozessen.

Es gibt auch empirische Modelle, die eine Zunahme der Fehlerentstehungsrate mit der Systemgröße postulieren. Für Software-Module wird z.B. unterstellt, dass die Fehleranzahl je NLOC ab etwa 3 Quellcode-Seiten je Funktionsbaustein überproportional zunimmt, weil die Entwerfer die Übersicht verlieren.

Ein vernünftig gestalteter Entstehungsprozess vermeidet alle bekannten negative Einflüsse auf die Fehlerentstehungsrate.

Determinismus und Zufall

Fehlerentstehung

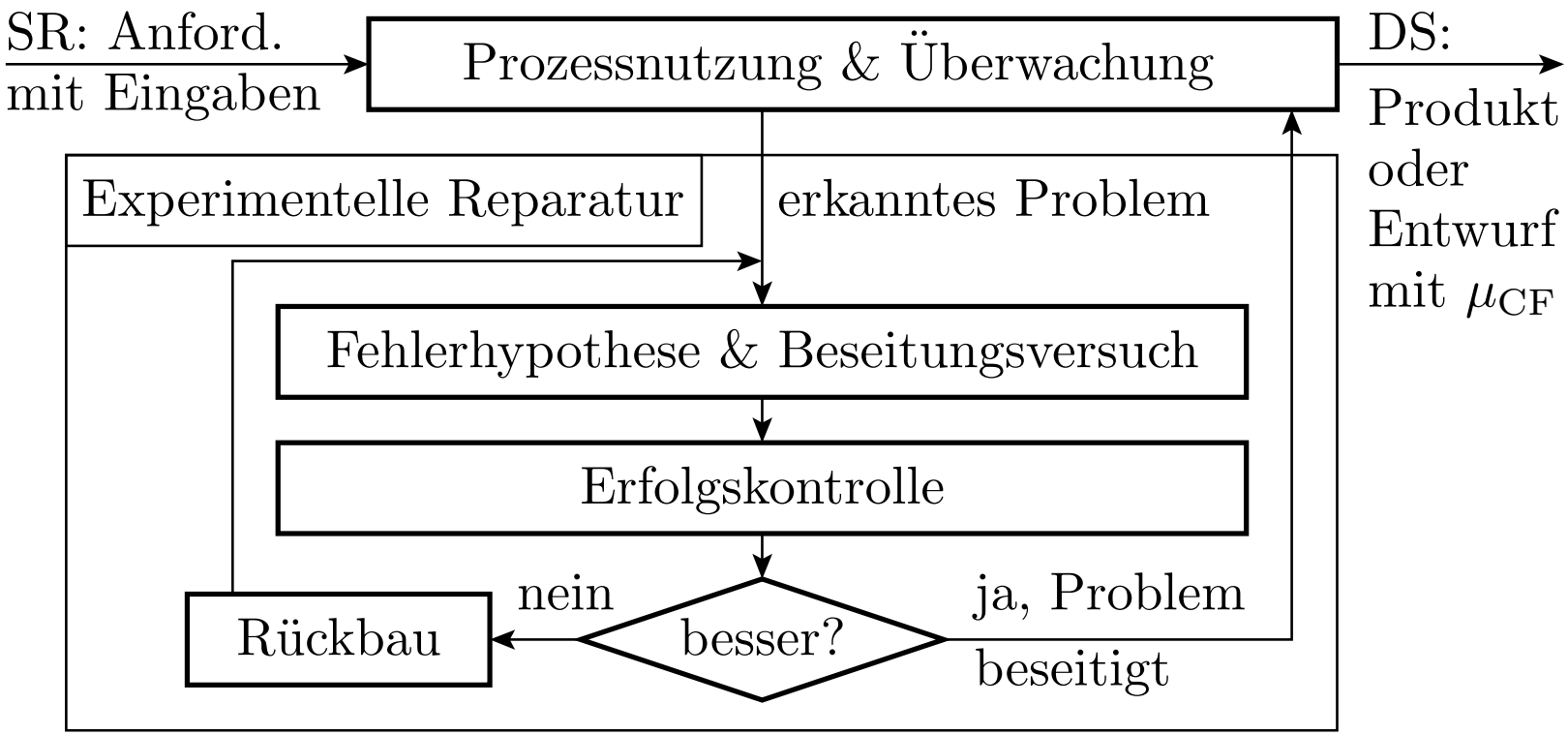


Ursachen für die Fehlerentstehung:

- Fehler: deterministische Ursache-Wirkungsbeziehung
  - beseitigbare Ursachen,
  - Erfolgskontrolle durch Testwiederholung, ...
- Störungen: zufällige Ursache-Wirkungsbeziehung
  - MF durch Wiederholung beseitigbar,
  - Erfolgskontrolle Ursachenbeseitigung schwierig, ...
- Ausfälle: bei Service-Nutzung entstehende Fehler, ...

Fehlervermeidung erfolgt durch Beseitigung von Fehlern in Entstehungsprozessen und durch Minderung der Störanfälligkeit.

Fehlervermeidung als Reifeprozess



Fehlervermeidung ist ein Reifeprozess für einen Entstehungsprozess mit experimenteller Reparatur zur Problembeseitigung. Iteration aus:

- Problemerkennung, Lokalisierung, Beseitigungsversuchen,
- Erfolgkontrolle durch Wiederholung der Entstehungsabläufe und
- Rückbau nach erfolglosen Beseitigungsversuchen.

Experimentelle Reparatur und Determinismus

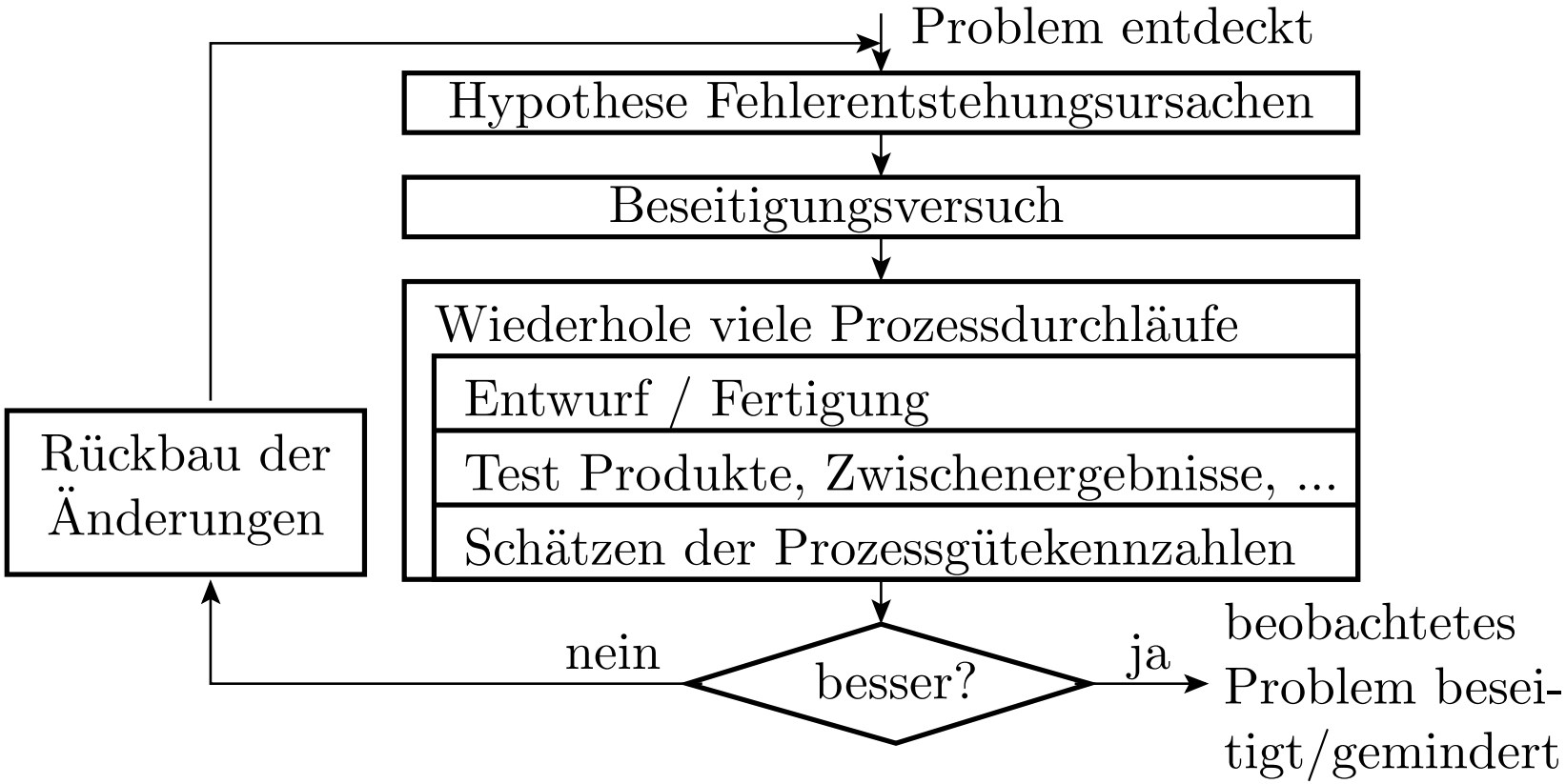
Determinismus bedeutet, dass das fehlerfreie System für denselben Entwurfs- oder Fertigungsauftrag (nach derselben Spezifikation, mit demselben Material, ...) immer dieselben Ausgaben (dasselbe Entwurfsergebnis, ein identisches Produkt, ...) liefert.

Für Fehler in deterministischen Prozessen lassen sich in der Regel Prozessabläufe mit Soll/Ist-Kontrollen an Zwischenergebnissen und Endprodukte finden, die eindeutige ja/nein-Aussage über das Vorhandensein/Beseitigung von Fehlern liefern.

Für nicht deterministische Prozesse, Fehler mit nicht deterministischer Wirkung und Prozessstörungen verlangt die Kontrolle der erfolgreichen Problembeseitigung in der Regel

- eine statistisch signifikannte Stichprobe von Prozessdurchläufen zur Bestimmung von Prozessgütekennzahlen (typ. 1000) und
- Entscheidungen mit Irrtumswahrscheinlichkeiten, typ. wenige %).

... nicht deterministische Prozesse, Fehlerwirkungen, Störungen:



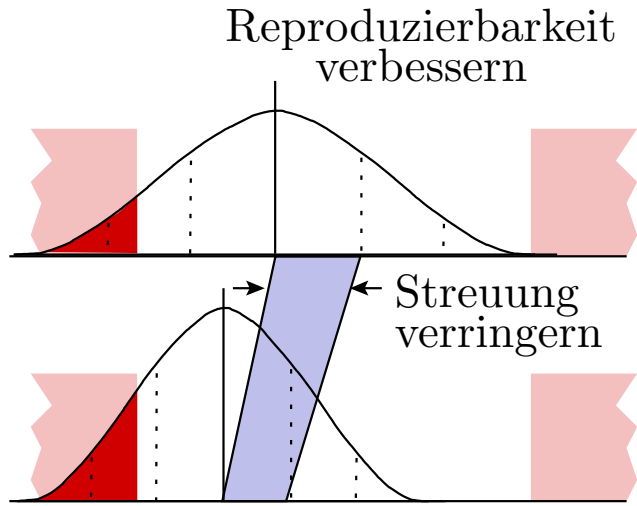
Nicht deterministische Prozesse benötigen für dieselben Absenkung der MF-Rate um Zehnerpotenzen mehr Prozessdurchläufe und haben ein deutlich höheres Risiko, dass bei Beseitigungsversuchen neue Fehler entstehen, die nicht durch Rückbau beseitigt werden.

Prozesszentrierung und -verbesserung

Es gibt einfach und schwer zu beseitigende Fehlerentstehungsursachen, Beispiel Prozesszentrierung / Verbesserung.

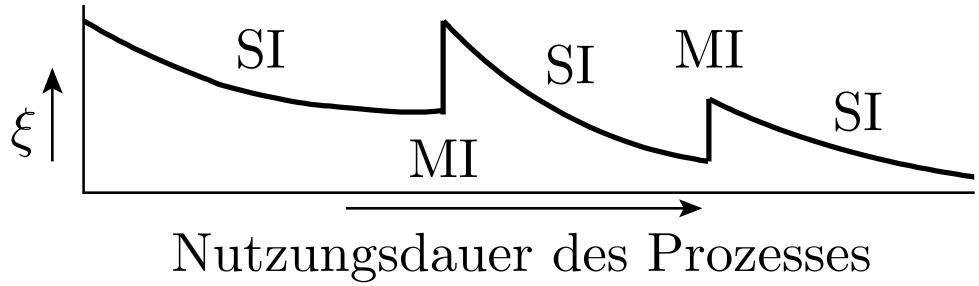
Bei der mechanischen Fertigung haben die Zielparameter, z.B. bei einer Bohrung Durchmesser und Tiefe, eine Verteilung und einen Toleranzbereich. Entstehungshäufigkeit eines Parameterfehlers ist etwa die Wahrscheinlichkeit, Parameter außerhalb Toleranzbereich:

- Prozesszentrierung: Verschiebung der Verteilung mit Hilfe von Einstelloptionen in die Mitte des Toleranzbereichs.
- Prozessverbesserung: Verringerung der Streuung durch technologische Neuerungen neue Maschinen, Verfahren, ...



Bei einer technologischen Neuerung geht die Zentrierung verloren. Sprunghafte Zunahme der Fehlerenstehungsrate.

Sägezahnverlauf der Fehlerentstehungsrate



Technologische Verbesserungen (neue Maschienen, Programmierwerkzeuge, Technologien, ...) werden in großen Zeitschritten (Jahre) eingeführt und haben das Potential, die Fehlerentstehungsrate zu verringern.

- Bei jeder technologischen Umstellung geht die Zentrierung verloren und die Fehlerentstehungsrate steigt sprunghaft.
- Die potentiell geringere Fehlerentstehungsrate wird erst durch erneute Zentrierung nach einer gewissen Nutzungsdauer erreicht.
- Mit der Prozesszentrierung nimmt die Fehlerentsehungsrate ab.

ξ	Fehlerentstehungsrate.
MI	Große Innovationen (Major innovations).
SI	Kleine Verbesserungen (Small improvements).

Auch bei anderen Fertigungsprozessen und Entwurfsprozessen

- gibt es in größeren Zeitschritten technologische Neuerungen, die die erreichbare Fehlerenstehungsrate durch geringere Störanfälligkeit, höhere Reproduzierbarkeit, ... absenken. Bei Neuerungen entstehen jedoch neue Prozessfehler, die die beobachtbare Fehleranzahl bzw. den Defektanteil der Produkte sprunghaft erhöhen.
- Dazwischen eine kontinuierliche Suche und Beseitigung der hinzugekommenen Fehlerentstehungsursachen, beginnend mit denen, die die meisten Fehler verursachen. Wirkung auf den Prozess ähnlich wie Zentrierung.

Schlussfolgerung

Am qualitativ hochwertigsten sind tendentiell Produkte kurz vor technologischen Neuerungen. Minima der Fehlerentstehungsrate.

Die Schattenseite von Innovationen

Technologische Reifeprozesse sind heute bei jeder Art von Produkten und Service-Leistungen zu beobachten:

- Verbesserte Wiederholgenauigkeit der Abläufe,
- verbesserte / vorhersagbare Material- und Produkteigenschaften,
- weniger entstehende Fehler, Ausbeute ↑, Kosten ↓, ...

Schattenseite:

- Neuerungen führen fasts zwangsläufig zu »neuen Kinderkrankheiten«, die erst nach einer gewissen Reifezeit beseitigt sind.
- Mehr entstehende Fehler bedeutet nicht nur schlechtere Ausbeute und mehr Kosten, sondern auch mehr Fehler in den eingesetzten Systemen, mehr Frühausfälle, ...

Bei Programmen (z.B. Linux) unterscheidet die Versionsverwaltung typ. zwischen:

- »Innovative« Beta-Versionen mit vielen Kinderkrankheiten, ...
- und einsatztauglichen (zuverlässige) Stable-Versionen.

Projekte, Vorgehensmodelle

Der Technologiegedanke

Technologie: Lehre von reproduzierbaren Abläufen zur Erzeugung von Produkten.

Technologiegedanke

Ein technologischer Prozess ist so zu gestalten, dass, wenn er unter gleichen Bedingungen wiederholt wird, gleiche Produkte mit (nahezu) gleichen Eigenschaften entstehen*.

Die technologische Entwicklung hin

- zur automatisierten menschenfreien Fertigung und
- zu rechnergestützten / automatisierten Entwurfsprozessen

hilft nicht nur bei der Kostensenkungung, sondern ist auch eine wesentliche Säule der Fehlervermeidung.

* Der Begriff *Technologie* wurde erstmalig von dem Göttinger Professor Johann Beckmann (1739-1811) in seinem Lehrbuch "Grundsätze der teutschen Landwirthschaft" verwendet. Heute interdisziplinäres Gebiet.

Übertragung des Technologiegedanken auf Projekte

Technologien reifen dadurch, dass derselbe Ablauf sehr oft wiederholt wird, um möglichst viele Fehler zu erkennen und den Beseitigungserfolg zu kontrollieren.

Wie verhält es sich mit Projekten:

- Manuelle kreative Teile der Entwurfsprozesse[3] und
- Fertigung von Prototypen, Demonstratoren, ... ?

Ein Projekt ist ein zielgerichtetes, einmaliges Vorhaben, das aus einem Satz von abgestimmten, gelenkten Tätigkeiten besteht. ...

Projekten fehlt aus Sicht der Fehlervermeidung die Reproduzierbarkeit und die häufige Wiederholung.

Schließt das Projekte von der Fehlervermeidung durch Lernen aus Fehlern aus?

[3] Hier inbesondere der Software- und Hardware-Entwurf.

Vorgehensmodelle

Vereinheitlichung des Vorgehens für große Klassen von Projekten

- zur Aufwandsminimierung, besseren Vorhersagbarkeit und
- zur Fehlervermeidung durch »Lernen aus Fehlern«.

Typische Vorgehensmodelle für den Entwurf und die Fertigung von IT-Komponenten umfassen:

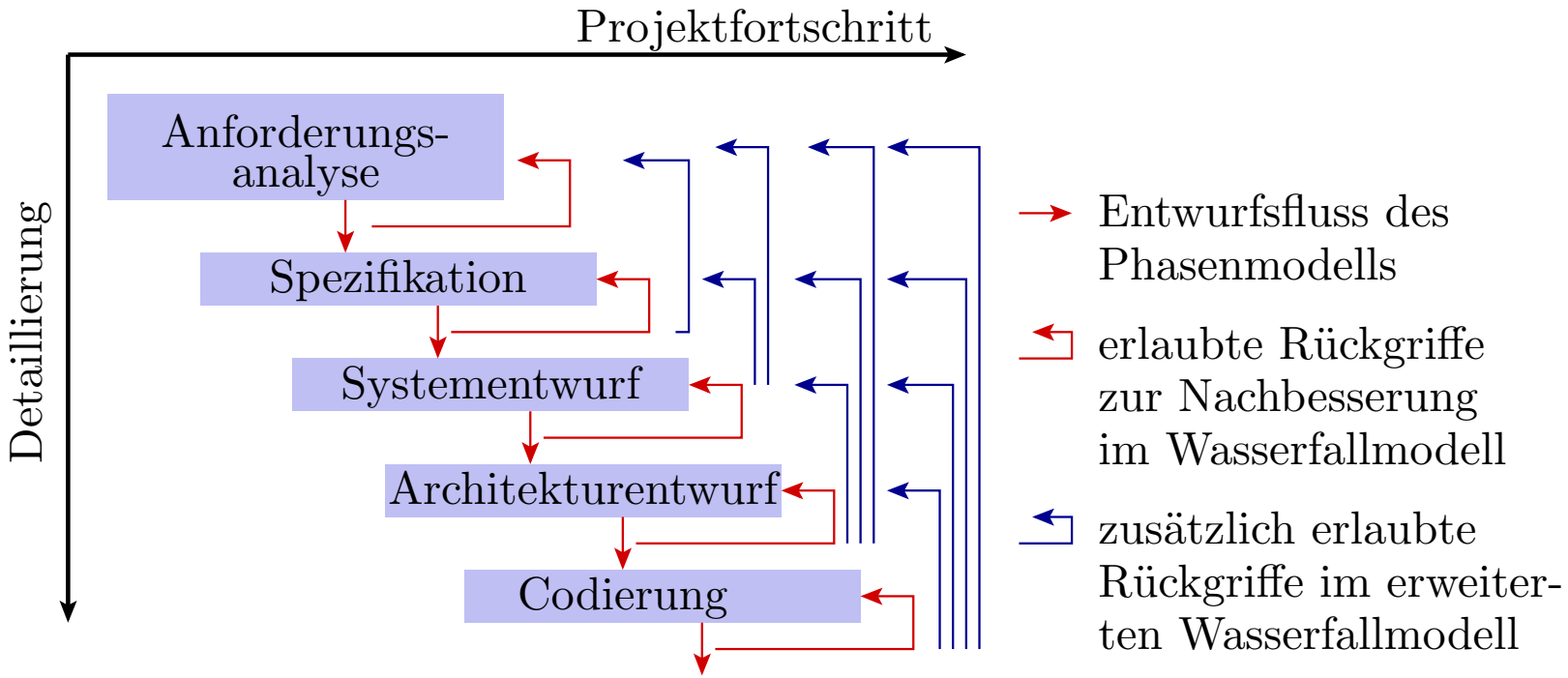
- Aufteilung in Schritte und Phasen,
- Referenzabläufe,
- Definition von Zwischen- und Endkontrollen, ...

Die klassischen Vorgehensmodelle für den Software-Entwurf sind Stufenmodelle. Sie unterteilen Entstehungsprozesse in Phasen:

- Anforderungsanalyse,
- Spezifikation der Ziele,
- Architekturentwurf, Codierung, Test, ...

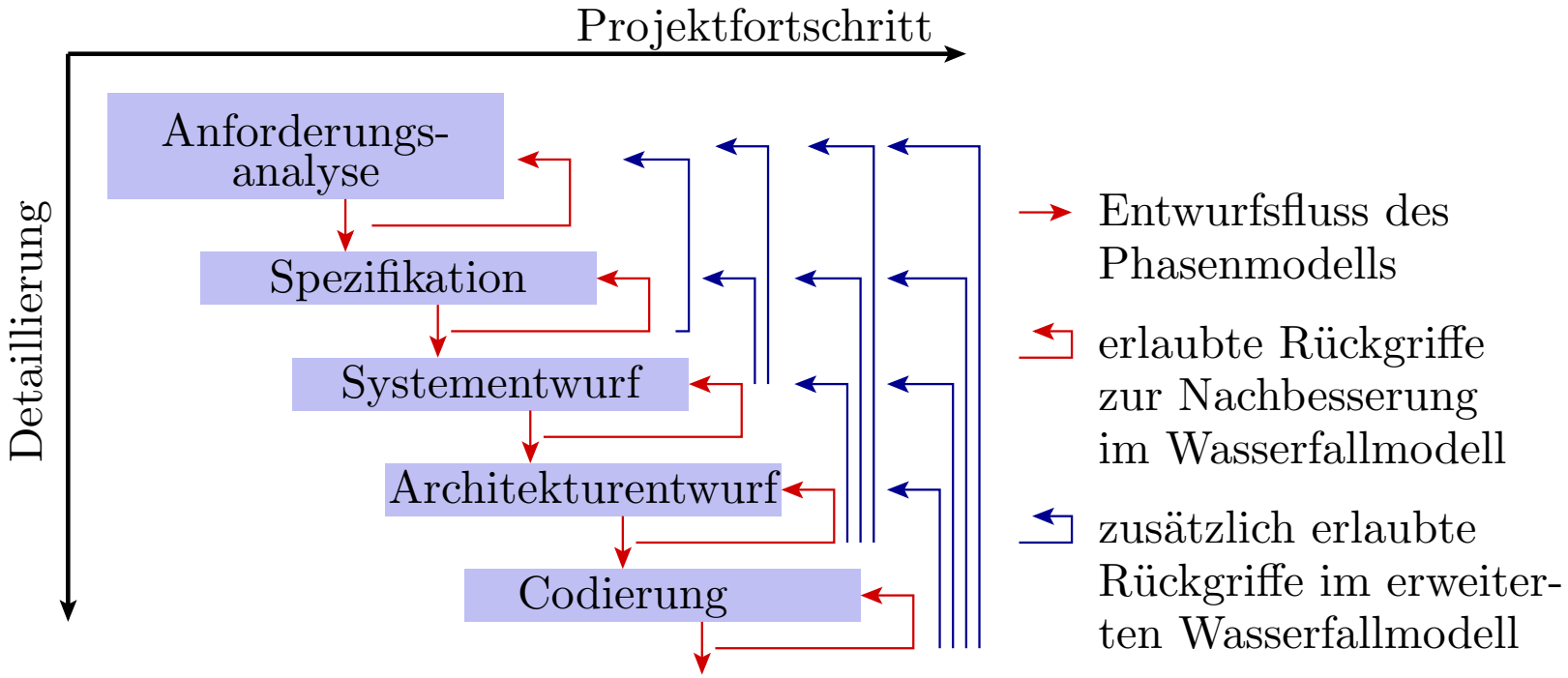
Fehlervermeidung bei Projektarbeit ist die kontinuierliche empirische Verbesserung (d.h. der Reifeprozess) der Vorgehensmodelle.

Stufenmodelle



Stufenmodelle variieren in

- der praktischen Arbeitsgestaltung,
- den Abgrenzungen der Entwurfsphasen,
- Dokumentation und Kontrolle bei Phasenübergängen,
- dem Vorgehen bei Rückgriffen (rückwirkende Änderungen an den Ergebnissen bereits abgeschlossener Phasen). ...



Gestaltbare Einflussfaktoren auf Qualität und Kosten:

- Arbeitsorganisation der Phasen,
- geforderte Tests, Dokumentation, ... bei Phasenübergängen,
- Regeln für Rückgriffe zur Nachbesserung, ...

Rückgriffe verlängern die Anzahl der Entstehungsschritte für einen Entwurf, und darüber die Anzahl der Fehler. Ein Workaround um einen Fehler kann jedoch auch den Arbeitsaufwand erheblich erhöhen und darüber die Fehleranzahl. Schwieriger Kompromiss.

Bewertung von Vorgehensmodellen

Jede Art der Fehlervermeidung benötigt eine Erfolgskontrolle:

Daraus resultierende Frage

An welchen mess- oder abschätzbaren Parametern ist eine Verbesserung eines Vorgehensmodells erkennbar?

Diese Parameter müssen zwischen unterschiedlichen realen Projekten und Vorgehensmodellen vergleichbar sein:

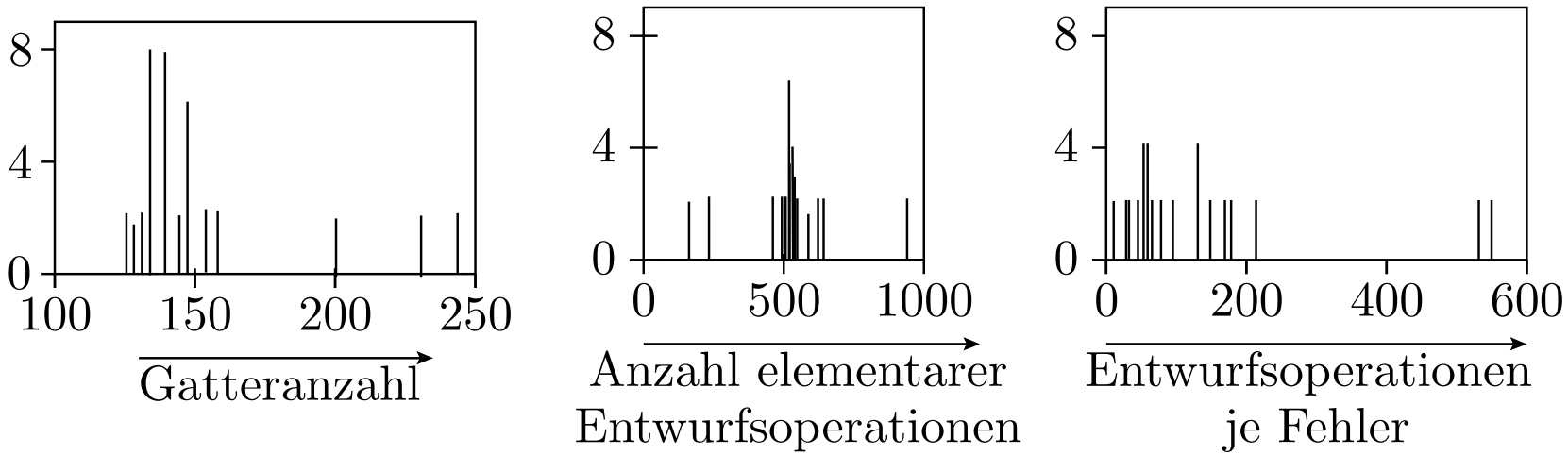
- Dauer, Kosten bezogen auf die Projektgröße
- Arbeitsschritte je entstehender Fehler, Umfrageergebnisse, ...

Erwartungswerte, Streuungen, Skalierbarkeit auf Projektgröße, Schwierigkeit, ...

Signifikante Aussagen über Vorgehensmodelle verlangen die Beobachtung tausender Projekte mit vergleichbarem Vorgehen.

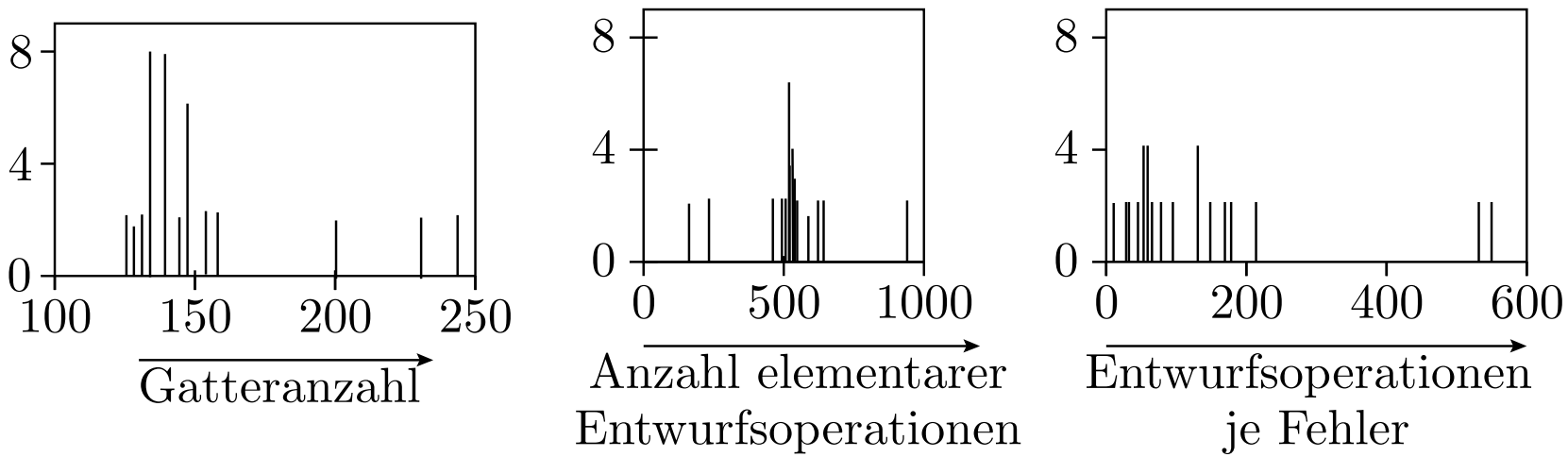
Ein Experiment [4]

Eine Gruppe von 72 Studenten sollte aus einer PLA- (**P**rogrammable **L**ogic **A**rray) Beschreibung eine Gatterschaltungen entwickeln und diese über eine GUI in ein CAD-System eingeben. Für jeden Entwurf wurden die elementaren Entwurfsoperationen, die Gatteranzahl und die Entwurfsfehler gezählt. Als elementare Entwurfsoperationen galten das Anordnen eines Gatters auf dem Bildschirm, das Zeichnen einer Verbindung, ...



[4] Aas, J. E., Sundsbo, I.: Harnessing the Human Factor for Design Quality, IEEE Circuits and Devices Magazine, 3/1995, S. 24-28

Welche Rückschlüsse erlaubt das Experiment?



Angenommen, der Versuch wird genauso an anderen Hochschulen wiederholt:

- auch hier dieselben Kenngrößen je Student bestimmt und
- Verteilung, Erwartungswert und Varianz verglichen.
- Unterschiede statistisch signifikant?

Aus den Vergleichergebnissen ließe sich bei signifikannten Unterschieden schlussfolgern, an welcher Hochschule Studierende für diese Aufgabe besser ausgebildet werden.

Qualität und Kreativität

Qualität und Kreativität

Qualität verlangt Fehlervermeidung. Fehlervermeidung verlangt:

- eine hohe Wiederholrate gleicher oder ähnlicher Tätigkeiten,
- einzuhaltende Arbeitsabläufe mit reproduzierbaren Ergebnissen,
- Protokollierung aller Unregelmäßigkeiten und Probleme, ...

Kreativität verlangt »Einzigartigkeit«:

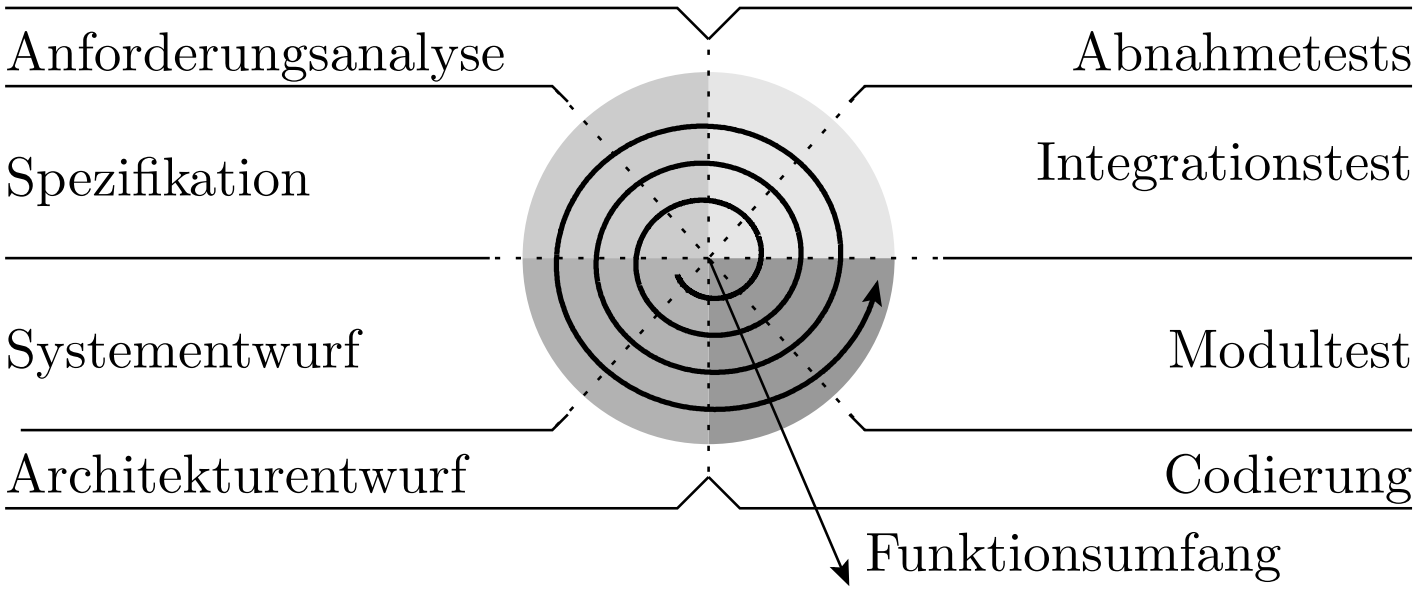
- Einbringen neuer Konzepte,
- Ausprobieren neuer Lösungswege,
- flexible Anpassung an sich ändernde Anforderungen.

Schlussfolgerung

Qualität und Kreativität haben entgegengesetzte Anforderungen an die Gestaltung von Arbeitsabläufen. IT-Entwurf verlangt Qualität und Kreativität. Wie lässt sich beides in einem Vorgehensmodell unterbringen?

Spiralmodell als Beispiel evolutionärer Modelle

Evolutionäre Vorgehensmodelle versuchen einen Rahmen für Projekte zu bieten, bei denen sich Kundenwünsche, Ziele, Vorgehen, ... mit dem Projekt weiterentwickeln. Weniger starre Abläufe. Mehr kreativer Gestaltungsspielraum. Beispiel Spiralmodell:



- Aufteilung einer Entwicklung auf ein mehrmaliges Durchlaufen eines Stufenmodells.

Aufteilung auf mehrmalige Durchläufe eines Stufenmodells.

- Durchlauf 1: Spezifikation von Grundanforderungen, Entwurf, Codierung, Test, ..., Abnahme und Einsatz.
- Durchlauf 2 bis n: Ideensammlung und Auswahl gewünschter Zusatzanforderungen und Änderungen. Entwurf bis Einsatz.

Ziel:

- Minimierung der Anzahl der Entstehungsschritte und der Anzahl der entstehenden Fehler je Stufenmodelldurchlauf.
- Kreativer Freiraum in Form einer Ideensammlung für den nächsten Stufenmodelldurchlauf.

Idealerweise dürften nach jedem Stufenmodelldurchlauf an bereits implementierten Features keine Änderungen vorgenommen werden, außer Fehlerbeseitigung.

Grundidee gut, der tatsächlich erzielbare Nutzen steckt in den Umsetzungsdetails.

Querverbindungen zum akademischen Alltag

Auch für die Gestaltung von Lernprozesses werden Vorgehensmodelle genutzt. Der Bolonia-Prozess (Bachelor-Master) strebt danach, Referenzabläufe zu etablieren.

Dahinter verbirgt sich die Hoffnung, dass sich mit dem Technologiegedanken im Bildungssystem ähnlich spektakuläre Fortschritte wie in Naturwissenschaft und Technik erzielen lassen:

- Vereinheitlichung der Abläufe.
- Verbesserung der Vorhersagbarkeit und Vergleichbarkeit der Bildungsergebnisse und Kosten.
- Übernahme der »Vorgehen« aus Bildungseinrichtungen mit besseren Ergebnissen von Bildungseinrichtungen mit schlechteren Ergebnissen.

Wie ist das an unserer Uni:

- Reift die Organisation der Lehr- und Forschungsabläufe?
- Welche Arten von Kreativität werden eingeschränkt und welche nicht? ...

Ein Abstecher zu Lernrozessen

In der Schule und beim Erlernen praktischer Tätigkeiten werden zum erheblichen Teil Vorgehensmodelle vermittelt und trainiert:

- Rechnen, Schreiben, Handwerkern, Programmieren, ...
- Bewertung in Service-Leistungen pro MF und Zeit.

Lernphasen:

1. Wissenvermittlung: anlesen, erklärt bekommen, ...
2. Training, bis Ergebnisse vorhersagbar.
3. Professionalisierung: Prozessüberwachung; Beseitigung von Schwachstellen und Problemen in den Abläufen.

An Universitäten:

- Phase 1: Vorlesung, Seminare, Selbststudium, ...
- Phase 2: Übung, Klausurvorbereitung*, Praktika.
- Phase 3: Aus Zeitgründen erst in der Berufspraxis für den eigenen eingeschränkten Tätigkeitsbereich.

* Auch Bewertung in Arbeitsmenge pro Klausurdauer und Fehler pro Arbeitsmenge.

Querverbindung Drittmittelprojekte

- Die Professionalisierungsphase durchlaufen erst die Absolventen in der Praxis.
- Akademiker und Studenten sind nicht für »fehlerarme Arbeitsabläufe« trainiert.
- In industriellen Software-Projekten entstehen durch Akademiker tendenziell mehr Fehler je Aufgabengröße.
- Die Kosten für die Fehlerbeseitigung trägt der Industriepartner.
- Deshalb rechnet es sich normalerweise für die Industrie nicht, Hochschulen und Studenten in ihr Tagesgeschäft einzubinden.
- Industrielle Studenten-Projekte dienen der Ausbildung.
- Drittmittelforschung ist wertvoll für den Knowhow-Transfer, Literaturstudien, Demostratoren, ... aber im IT-Bereich ungeeignet für die Einbindung in die Produktentwicklung.

Fehlervermeidung eröffnet interessante Blickwinkel auf Technologien, Institutionen, Behörden, ... und deren Weiterentwicklung.

Zusammenfassung

Abschn: 5.1: Fehlerentstehung

Modellierung von Entstehungsprozessen als Service und Fehler als dessen MF. Zu erwartende Fehleranzahl und Fehlerentstehungsrate:

$$\mu_{\mathrm{CF}} = \xi \cdot C \tag{1.91}$$

$$\xi = \left.\frac{\#F_{\mathrm{C}}}{C}\right|_{\mathrm{ACR}} \tag{1.90}$$

Abschn. 5.2: Determinismus und Zufall

Fehlt der Determinismus erfordert die Erfolgskontrolle statistische Untersuchungen an tausenden von entstandenen Produkten. Das verlangsamt die Reifeprozesse. Aus dem üblichen Ablauf

- Prozessverbesserung alle paar Jahre und
- kontinuierliche Suche nach Möglichkeiten zur Minderung von Fehlerentstehungsursachen

folge ein sägezahnfömiger Verlauf der Fehlerentstehungsrate mit Maxima kurz vor größerer Prozessumstellungen.

Abschn. 5.3: Projekte, Vorgehensmodelle

Reifeprozess benötigen eine große Wiederholanzahl gleicher Abläufe. Um auch bei Projekten aus erkannten Fehlern lernen zu können, erfolgt Projektarbeit nach Vorgehensmodellen. Klassiker sind die Stufenmodelle, die Entwürfe in Phasen teilen und Kontrollen und Aktivitäten beim Stufenübergang definieren. Problematisch ist die Überprüfung, ob eine Änderung einer Verbesserung bewirkt.

Abschn. 5.4: Qualität und Kreativität

Vorgehensmodelle findet man überall dort, wo ein beständiges Lernen aus Fehlern angestrebt wird, also auch in Verwaltungen, Schulen, ... In den evolutionären Vorgehensmodellen wird Kreativität so untergebracht, dass neue Ideen für die Spezifikation von Folgeprojekte gesammelt werden, die dann wieder idealweise nach einem rückgriff-freien Stufenmodell ablaufen.

Fehlervermeidung eröffnet interessante Blickwinkel, wie und wohin die Entwicklung von Technologien, Arbeitsabläufen in Institutionen und Behörden und auch die Ausbildung an Schulen verläuft.