Test und Verlässlichkeit 1: Modellbildung Teil 1

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_F1.pdf)

10. November 2024

Inhalt Foliensatz TV_F1.pdf

Vorlesung 1 (1.3)

1.1 Verlässlichkeit

1.1.1 Service-Modell

1.1.2 Verfügbarkeit

Vorlesung 2 (1.37)

1.1.3 Zuverlässigkeit

1.1.4 Sicherheit

Vorlesung 3 (1.72)

1.2 Problembehandlung

1.2.1 Überwachung

1.2.2 Formatkontrollen

1.2.3 Wertekontrollen

1.2.4 Neuanforderung

Vorlesung 4 (1.105)

1.2.5 Mehrheitsentscheid

1.2.6 Reaktion ab Erkennung

1.2.7 Spezielle Lösungen

Lernziel der Vorlesung

Verlässlichkeit bedeutet, IT-Systemen trauen zu können, dass sie

- auf Anforderungen Ergebnisse liefern,
- die Ergebnisse richtig sind und, wenn sie falsch sind,
- keine katastrophalen Schäden entstehen.

Verlässlichkeit wird auf drei Ebenen gesichert:

- Überwachung und geeignete Reaktionen auf erkannte Probleme,
- Test und Fehlerbeseitigung und
- Fehlervermeidung.

Lernziel ist ein Überblick über die Teilaspekte der Verlässlichkeit, die Maßnahmen zu ihrer Sicherung und darauf aufbauend quantitativen Abschätzungen und konkrete Maßnahmen.

Studierende lernen den Einfluss ihrer Arbeit und den anderer Mitwirkender an der Entstehung und dem Betrieb von IT-Systemen auf deren Verlässlichkeit einzuschätzen, konkrete verlässlichkeitssichernde Maßnahmen zu planen und durchzuführen. Am wichtigsten sind die durchgeführten Tests und Kontrollen.

Organisation

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

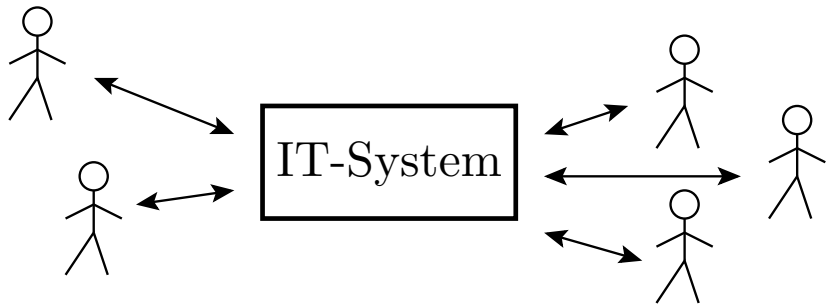
- Foliensätze, Handouts, Hausübungen, Videoaufzeichnungen
- Abgabe der Hausübungen per Mail an ha-tv@in.tu-clausthal.de als PDF. Abgabetermine siehe Web-Seite.
- Hausübungen werden bewertet und zurückgegeben. Zusätzlich Veröffentlichung der Punkteanzahl auf der Webseite.
- Prüfungszulassung 50% der erzielbaren Punkte für alle Hausübungen insgesamt. 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.

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 langsame 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 kontrolliert.

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

Gefährdungen & Gefährdungsabwendung

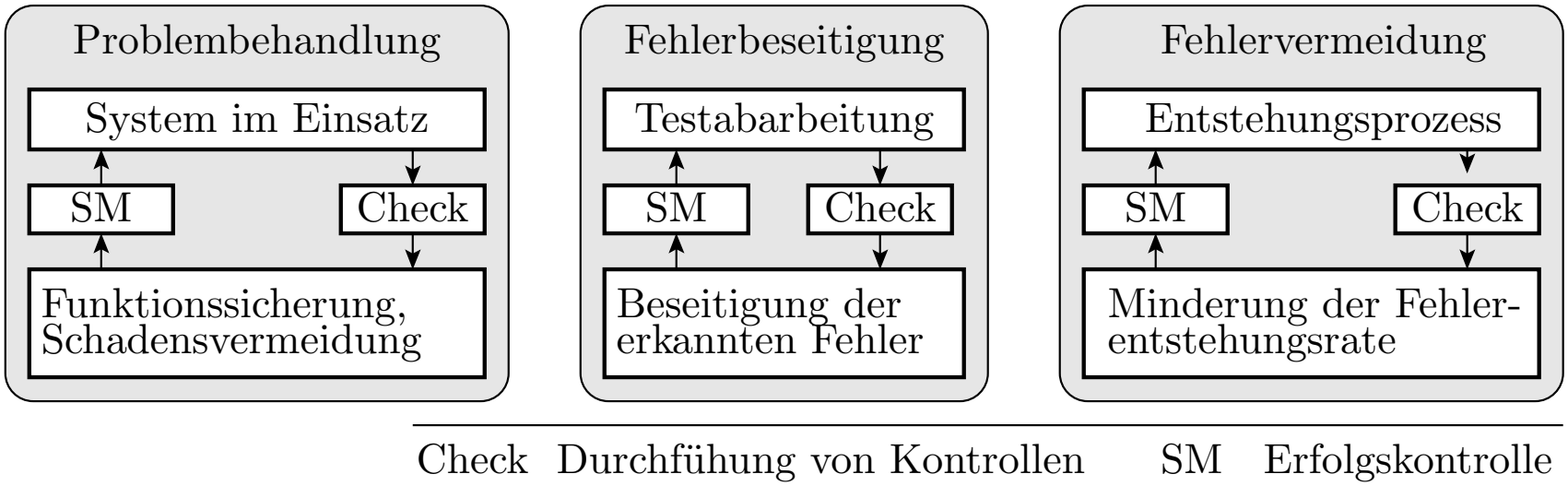
Verlässlichkeit wird durch Abwesenheit / Abwendung / Ausschluss von Gefährdungen beschrieben[Lapri81], und zwar auf drei Ebenen:

- Probleme während des Einsatzes:
  - Service-Verweigerung (no service, NS).
  - Fehlfunktionen (malfunction, MF),
- Ursachen der Probleme:
  - Fehler (beseitigbare Ursachen für NS und MF),
  - Störungen (Ursachen zufällig auftretender Probleme),
  - Ausfälle (währen des Einsatzes entstehende Fehler).
- Entstehungsursachen der Problemursachen:
  - Schwachstellen, Fehler,
  - Störungen und Ausfälle

  in den Entstehungs- und Reparaturprozessen.

[Lapri81] J.C. Laprie. "Dependable Computing and Fault Tolerance: Concepts and Terminology,"15th IEEE Int. Symp. on Fault-Tolerant Computing, 1985.

Gefährdungsabwendung



Gefährdungsabwendung erfolgt durch Iterationen aus Kontrollen, Problembeseitigung und Erfolgskontrolle auf drei Ebenen:

- Problembehandlung während der Nutzung,
- Fehlerbeseitigung vor der Nutzung und in Nutzungspausen.
- Fehlervermeidung durch verbesserte Entstehungsprozesse.

Was kostet Verlässlichkeit?

Kosten für die Gefährdungsabwendung:

- 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-Systeme ohne erhöhte Anforderungen an die Verlässlichkeit eine teure Produkteigenschaft. Bei erhöhten Anforderungen betragen die anteiligen Produktkosten für die Sicherung der Verlässlichkeit weit über 50%.

HW, SW Hardware, Software.

Der Preis fehlender Verlässlichkeit

Wenn Verlässlichkeit teuer, warum kein Verzicht? – Schadenskosten:

- Keine / eingeschränkte Benutzbarkeit,
- 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] ...*

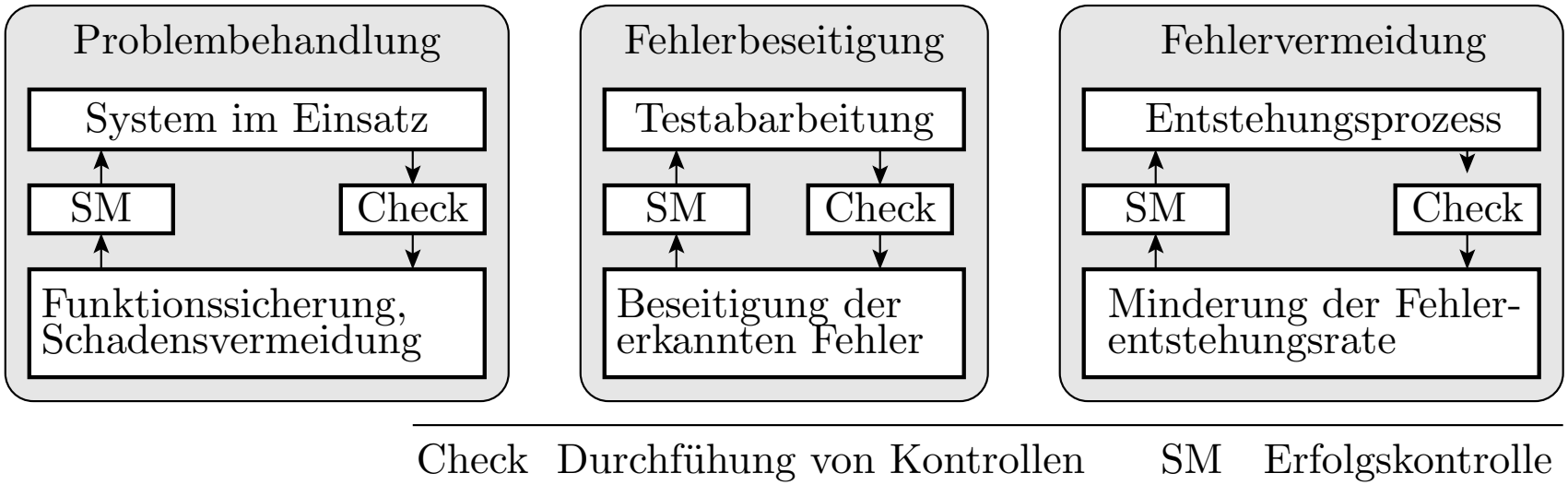
Ursache des beinahe atomaren Schlagabtauschs: defekter Schaltkreis.

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 den Tests in den Problembeseitigungsiterationen

- währen des Einsatzes,
- vor dem Einsatz und
- während der Entstehung ab.

Lernziel und Inhalt

Lernziel

Einschätzung der unterschiedlichen Einflüsse auf die Verlässlichkeit von IT-Systemen. Am wichtigsten sind durchgeführte Tests und Kontrollen.

Die Gefährdungen und Gegenmaßnahmen sind stochastischer Natur. Hierzu themenspezifische Einführungen in die Stochastik.

Foliensätze:

1. Modellbildung 1: Service-Modell, Verlässlichkeit, Umgang mit Fehlfunktionen, Problemvermeidung.
2. Modellbildung 2: Fehlerbeseitigung, Fehlervermeidung, ...
3. Wahrscheinlichkeiten: Fehlerbäume, Markov-Ketten, ...
4. Verteilungen insbesondere für Zählwerte, Bereichsschätzungen, ...
5. Überwachung: Informationsredundanz, Fehler erkennende Codes, Prüfkennzeichen, Protokolle, Invarianten, Syntax
6. HW: Fehlermodellierung, Testsuche, Selbsttest, Ausfälle.
7. SW: Programmiersprache, Vorgehen, Testauswahl.

Verlässlichkeit

Verlässlichkeit

IT-Nutzung setzt Vertrauen voraus. Verlässlichkeit beschreibt, in welchem Maße gerechtfertigt. Objektive Beschreibung durch Zählwerte für positive und negative Erfahrungen. Unterscheidung nach Aspekten:

Erbringung

- positive Erfahrungen: Erbringung auf Anforderung
- negative Erfahrungen: keine Erbringung auf Anforderung

Richtigkeit:

- positive Erfahrungen: erbrachte Ergebnisse richtige
- negative Erfahrungen: falsche Ergebnisse

Quantitative Abschätzungen:

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

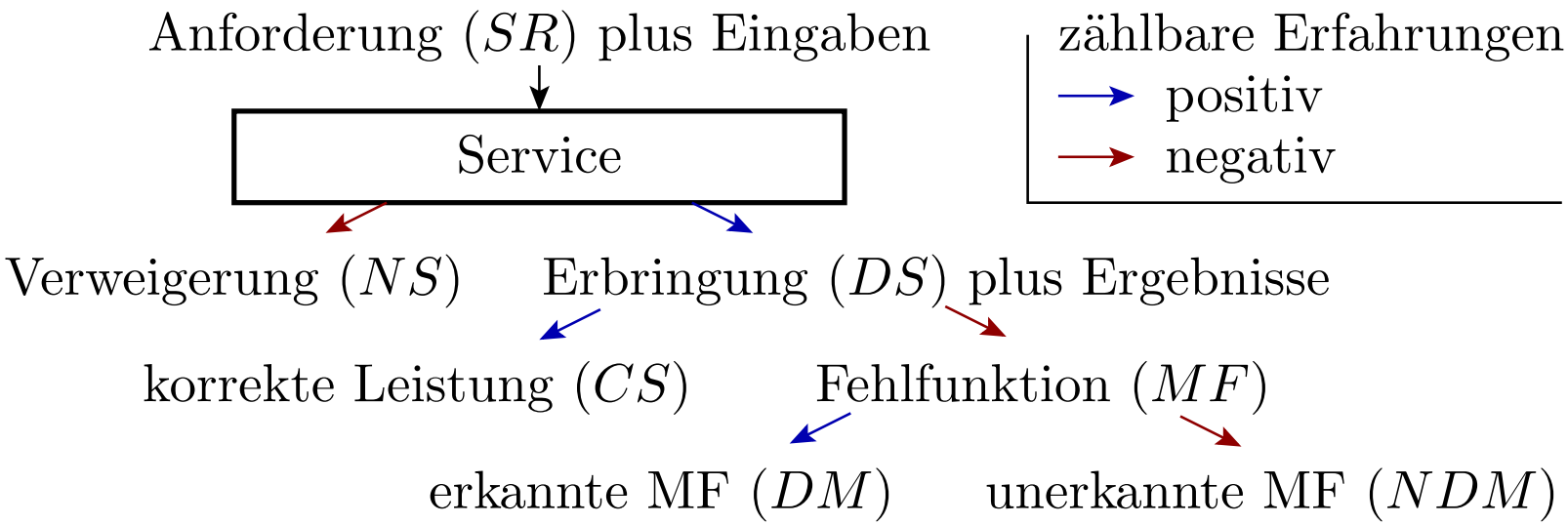
IT-Systeme so modellieren, dass erbrachte und nicht erbrachte Leistungen, richtige und falsche Ergebnisse und anderen betrachtete potentielle und vermiedenen Probleme zählbar sind.

MF Fehlfunktion (Malfunction).

Service-Modell

Service

System, das auf Anforderung aus Eingaben Ausgaben erzeugt.



Das Ergebnis auf eine Anforderung kann sein:

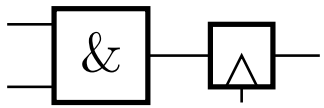
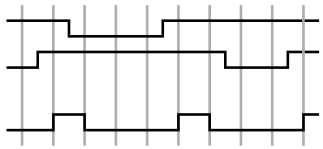
- Erbringung (DS, delivered service),
- Verweigerung (NS, no service).

Erbrachte Leistungen können sein

- richtig (CS, correct service) oder
- falsch (MF, malfunction).

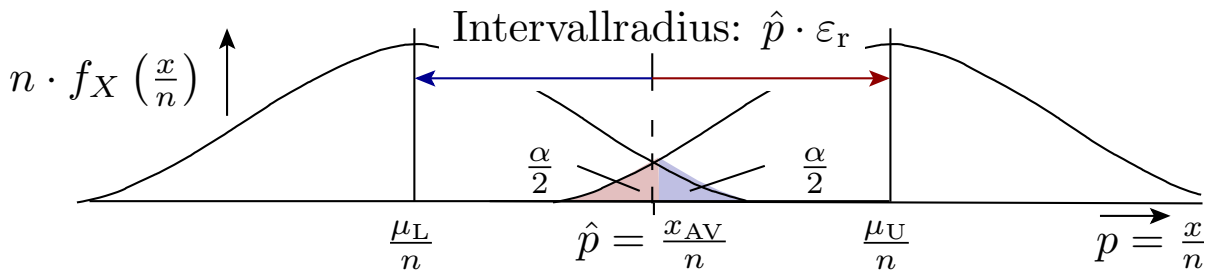
Anwendungsbereiche des Service-Modells

Das Service-Modell ist auf unterschiedliche Abstraktionsebenen 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: 230 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 (ACR)



Experimentell bestimmte Zählwerte sind Schätzer für Eintrittswahrscheinlichkeiten, die nur Bereichsaussagen erlauben. Vorhersagegenauigkeit (relativer Intervallradius ε_r) abhängig von:

- der Anzahl der Zählversuche n,
- der Verteilung (im Bild Dichtefunktion f_X) der Zählwerte X,
- der Größe des experimentellen Zählergebnisses x_AV bzw. der zu schätzenden Eintrittswahrscheinlichkeit $\hat{p} = \frac{x_\mathrm{AV}}{n}$,
- der zulässigen Irrtumswahrscheinlichkeit α, ...

Erforderliche Größenordnung von x_AV und n siehe später Foliensatz 4 (siehe Abschn. 4.2.7 *Schätzen von Zählwerten*). Bis dahin Kennzeichnung zählwertbasierter Abschätzungen mit $\ldots|_\mathrm{ACR}$.

ACR Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

Verfügbarkeit

Verfügbarkeit als Kenngröße

Die Kenngröße Verfügbarkeit (availability) sei die Erbringungsrate für angeforderte Service-Leistungen:

$$A = \left.\frac{\#DS}{\#SR}\right|_{\mathrm{ACR}} \tag{1.1}$$

- Auch über mittlere Zeit zwischen Problemen und mittlere Problembehandlungsdauern abschätzbar. Problembehandlung, was steckt drin und wie viel Zeit kostet sie?
- Es gibt unterschiedliche Gründe für Nichtverfügbarkeit, auf die unterschiedlich zu reagieren ist. Getrennte Zählung ...

Rate	Relative Auftrittshäufigkeit eines betrachteten Ereignisses.
A	Verfügbarkeit (Availability).
$\#SR$	Anzahl der Service-Anforderungen (Number of service requests).
$\#DS$	Anzahl der erbrachten Service-Leistungen.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

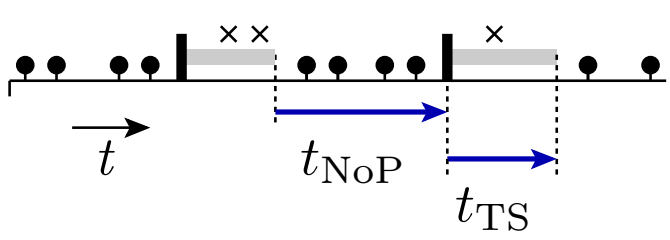
Problembehandlung – Aufgaben und Aufwand

Wenn kein verwertbare Service-Leistung erbracht wird:

- Schadensminderung (Datenrettung, sicherer Zustand, ...),
- Wiederherstellung der Betriebsbereitschaft (Reparatur, Neuinitialisierung, ...),
- Protokollierung und Speicherung von Daten zur Ursachenlokalisierung,
- Abbruch ohne Leistung oder Neuanforderung.

Vor allem Reparaturen nach Hardware-Ausfällen, aber auch Datenrettung, Herstellung sicherer Zustände, ... Neuanforderung dauern.

Verfügbarkeit und Problembehandlungsdauer



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

Ein System arbeitet immer für einen Zeit t_{NoP} ohne erkennbare Probleme (d.h. ohne Service-Verweigerung, Absturz, erkennbare Fehlfunktion, ...) gefolgt von einer Problembehandlung (Reparatur, Neuinitialisierung, ...) der Dauer t_{TS}. Verfügbarkeit als mittlere anteilige Zeit:

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

Erhebliche Abhängigkeit von der mittleren Problembehebungsdauer.

t_{NoP}	Zeit ab letzter Problembehebung bis zum nächsten beobachteten Probleme.
$\bar{t}_{\mathrm{NoP}}$	Mittlere problemfreie Zeit.
$t_{\mathrm{TS}}, \bar{t}_{\mathrm{TS}}$	Zeit und mittlere Zeit für die Problembehebung (troubleshooting).
A	Verfügbarkeit (Availability).

Differenziertere Modellierung

Nicht-Verfügbarkeit kann unterschiedliche Ursachen haben:

1. Hardware-Ausfall (FL, failure)
2. Annahmeverweigerung (DA, denial of acceptance),
3. Absturz (CR, crash),
4. erkannte Fehlfunktion (DM, detected malfunction).

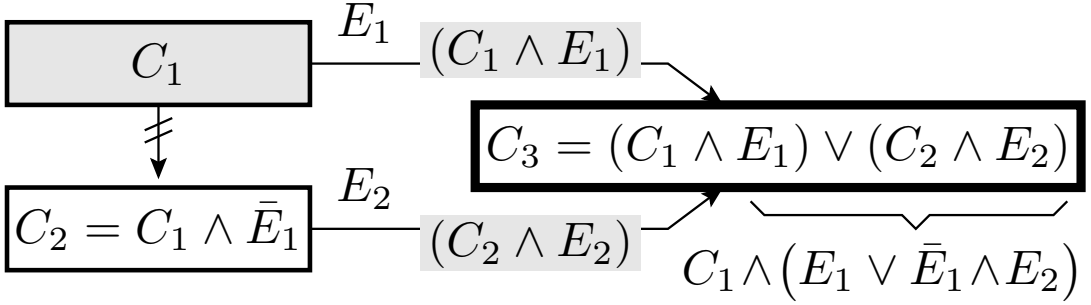
mit eigenen Zählwerten, eigenen Maßnahmen zum Umgang damit und eigenen Eintritts- und Tolerierungsraten.

	Ausfall	DA	Absturz	DM
Zählwert neg. Ereignisse	$\#FL$	$\#DA$	$\#CR$	$\#DM$
Zählwert pos. Ereignisse	$\#HA$	$\#RA$	$\#DR$	$\#DS$
Eintrittsrate	ζ_{FL}	ζ_{DA}	ζ_{CR}	ζ_{DM}
Tolerierungsrate	ν_{FL}	ν_{DA}	ν_{CR}	ν_{DM}

Für solche komplexen Zählwertbeziehung soll zuerst eine graphische Darstellung eingeführt werden.

CVA- (Zählwertzuordnungs-) Graphen

Zähl- und Zuordnungsereignisse



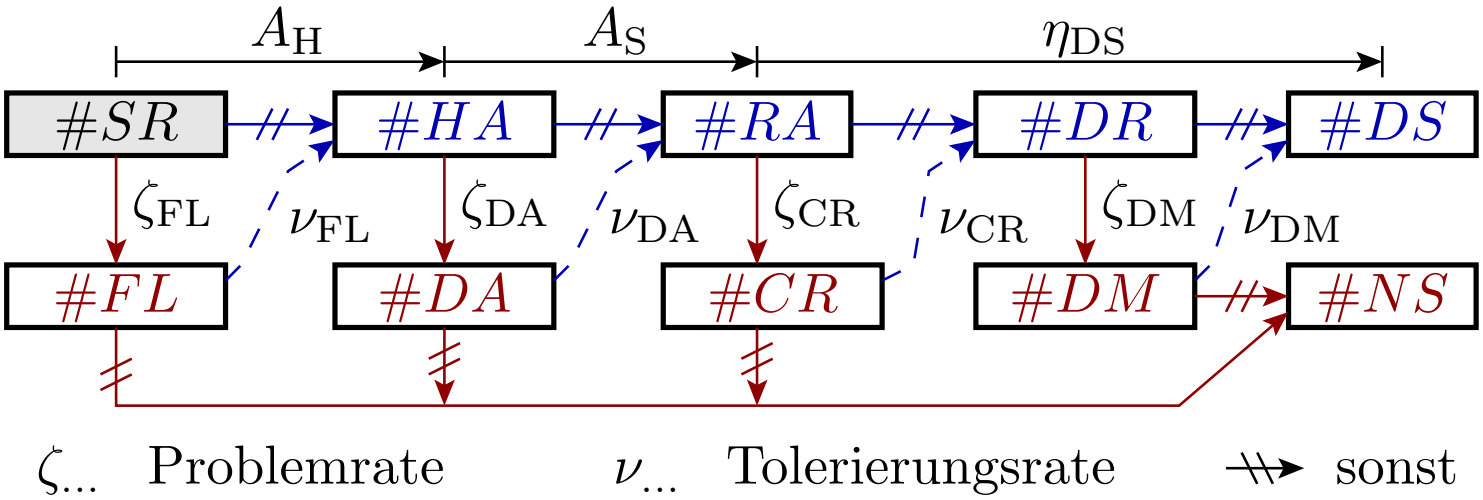
C_i	Zählereignis i
$\#C_i$	Zählwert i
E_j	Zuordnungsereignis j
η_{Ej}	Zuordnungrate j
$\dashrightarrow$	sonst

Zählwertzuordnungsgraph (CVA-Graph, count value anssignment graph)

- alle ($\xrightarrow{E_i}$)-Zuordnungen: unabhängige Ereignisse $\Rightarrow$ Produkt: $\#_i = \#C_i \cdot \eta_i$
- alle ( )-Rekonvergenz: gegenseitig Ausschluss $\Rightarrow$ Summe: $\#C_j = \sum \#_i$

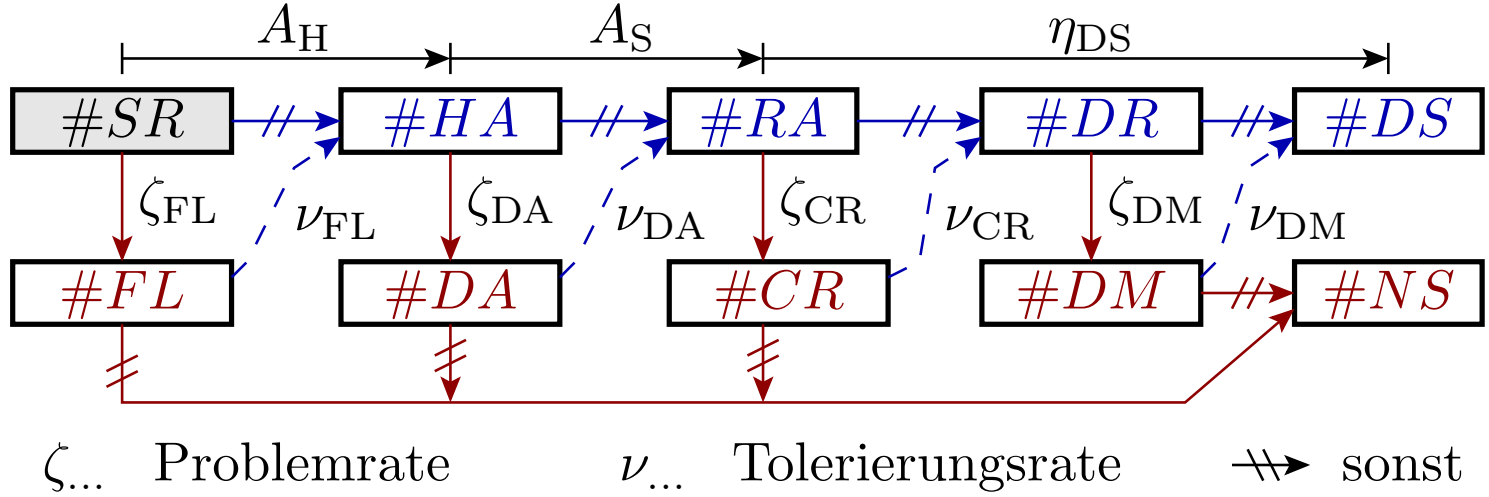
Vorgriff auf verketteten Zufallsereignisse (siehe Abschn. 3.1.2 *Verkettete Ereignisse*).

Aufspaltung in drei Teilverfügbarkeiten



	Ausfall	DA	Absturz	DM
Zählwert neg. Ereignisse	$\#FL$	$\#DA$	$\#CR$	$\#DM$
Zählwert pos. Ereignisse	$\#HA$	$\#RA$	$\#DR$	$\#DS$
Eintrittsrate	ζ_{FL}	ζ_{DA}	ζ_{CR}	ζ_{DM}
Tolerierungsrate	ν_{FL}	ν_{DA}	ν_{CR}	ν_{DM}

- $\#HA$ zählt Anforderungen, für die Hardware verfügbar ist,
- $\#RA$ zählt Anforderungen, für die auch der Service verfügbar ist,
- $\#DR$ zählt die erbrachten akzeptierten Service-Leistungen, ...



Hardware-Verfügbarkeit:

$$A_H = \left.\frac{\#HA}{\#SR}\right|_{ACR}$$

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

Service-Verfügbarkeit:

$$A_S = \left.\frac{\#RA}{\#HA}\right|_{ACR}$$

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

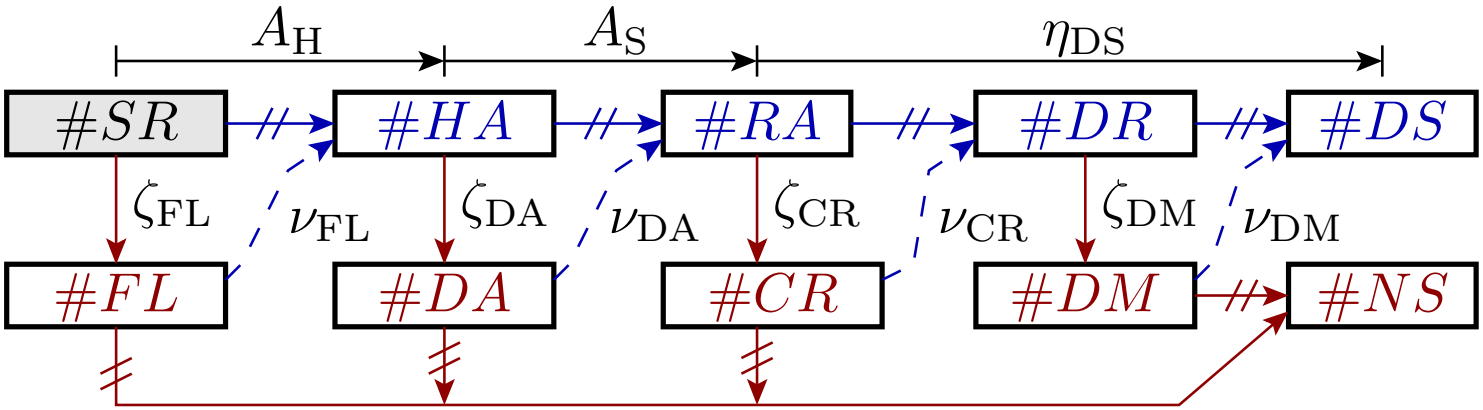
Erbringungsrate:

$$\eta_{DS} = \left.\frac{\#DS}{\#RA}\right|_{ACR} = \ldots$$

Gesamtverfügbarkeit:

$$A = \left.\frac{\#DS}{\#SR}\right|_{ACR}$$

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

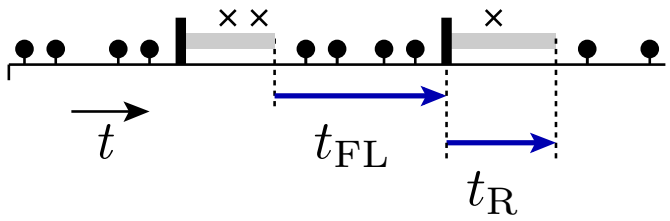


Für unabhängige Ereignisse FL, TFL, DA, TDA,... werden entlang aller Pfade vom Zählwert #CR zu anderen Zählwerten nur

- unabhängige Ereignisse UND- und
- sich ausschließende Ereignisse ODER-verknüpft.

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

Hardware-Verfügbarkeit



(1.3) $$A_{\mathrm{H}} = (1 - \zeta_{\mathrm{FL}}) + \zeta_{\mathrm{FL}} \cdot \nu_{\mathrm{FL}}$$

Abschätzung in der Regel über die anteilige Zeit der Verfügbarkeit (Gl. 1.2):

$$A_{\mathrm{H}} = \frac{\bar{t}_{\mathrm{FL}}}{\bar{t}_{\mathrm{FL}} + \bar{t}_{\mathrm{R}}} \tag{1.6}$$

Gegenwahrscheinlichkeit «Probability of Failure on Demand«:

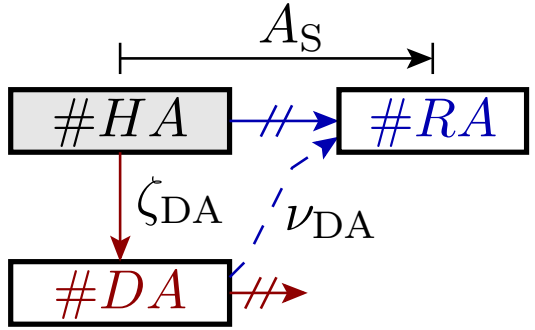
$$PFD = 1 - A_{\mathrm{H}} = \frac{\bar{t}_{\mathrm{R}}}{\bar{t}_{\mathrm{FL}} + \bar{t}_{\mathrm{R}}} \tag{1.7}$$

Fortsetzung (siehe Abschn. 6.5 *Ausfälle*).

A_{H}	Hardware-Verfügbarkeit.
ζ_{FL}, ν_{FL}	HW-Nichtverfügbarkeitsrate, Tolerierungsrate für nicht verfügbare HW.
$\bar{t}_{\mathrm{FL}}$, $\bar{t}_{\mathrm{R}}$	Mittlere Zeit bis zum nächsten Ausfall, mittlere Reparaturdauer.
PFD	Wahrscheinlichkeit der Nicht-Verfügbarkeit durch Hardware-Ausfälle.

Service-Verfügbarkeit

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



Verweigerung der Service-Annahme bei verfügbarer Hardware, z.B. wegen:

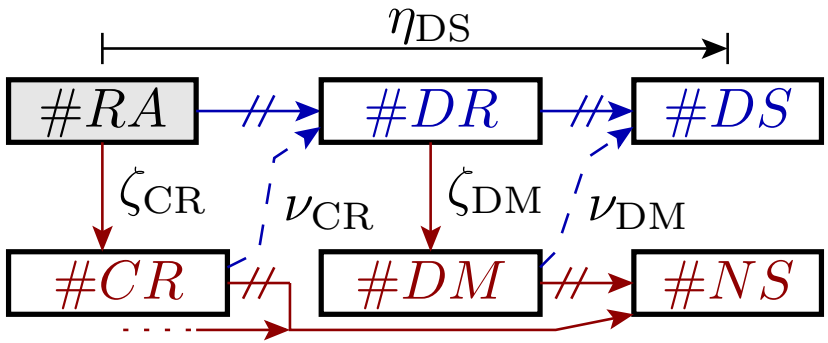
- Problembehandlung nach Absturz oder erkannter Fehlfunktion,
- zu lange Abarbeitungszeit,
- Überlastung durch zu viele Service-Anforderungen, ...

Durch ausreichende Leistungsreserve vermeidbar. Tolerierbar durch Zulassen verspäteter Abarbeitung, Aufgabenumverteilung, ...

Stark mit funktionalen Aspekten verzahnt. Die Vorlesung wird im Weiteren in der Regel $\zeta_{DA} = 0$ oder $A_S = 1$ unterstellen.

A_S	Service-Verfügbarkeit.
$\#HA$	Anzahl der Service-Anforderungen, für die die Hardware verfügbar ist.
$\#RA$	Anzahl der akzeptierte Service-Anfragen.
$\#DA$	Anzahl der Annahmeverweigerungen.
ζ_{DA}, ν_{DA}	Service-Verweigerungsrate, Tolerierungsrate für Service-Verweigerungen.

Erbringungsrate für akzeptierte Anforderungen



Die Erbringungsrate

$$\eta_{\mathrm{DS}} = \left.\frac{\#DS}{\#RA}\right|_{\mathrm{ACR}}$$

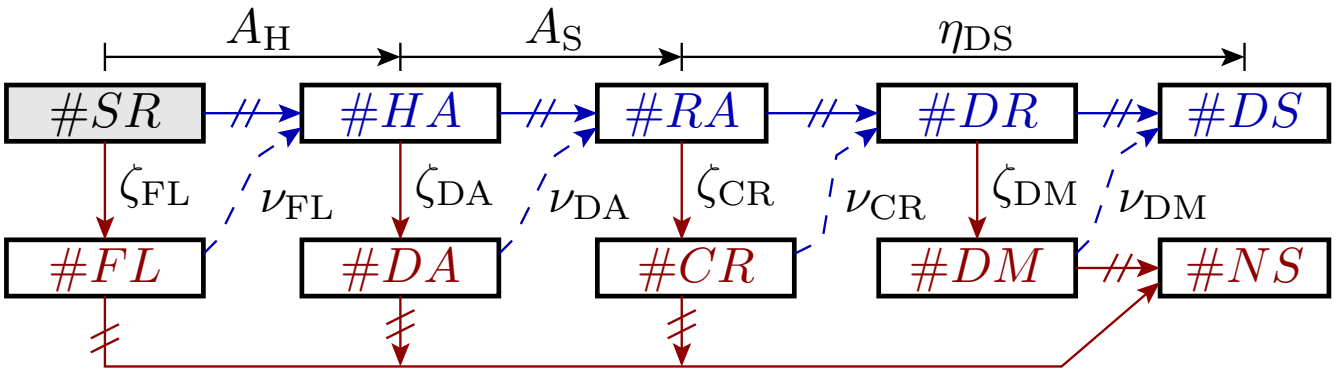
hängt ab von

- der Absturzrate ζ_{CR}, der Rate der erkannten Fehlfunktionen ζ_{DM} ,
- den zugehörigen Tolerierungsrate ν_{CR} und ν_{DM} und
- dem Umgang mit erkannten Fehlfunktionen.

Fortsetzung (siehe Abschn. 1.2 *Problembehandlung*).

RA, DR	Service-Anforderung akzeptiert, erbrachtes Ergebnis.
DS, NS	Erbrachte Service-Leistung, keine Service-Leistung.
CR, DM	Nichtverfügbarkeit wegen Absturz bzw. erkannter Fehlfunktion.

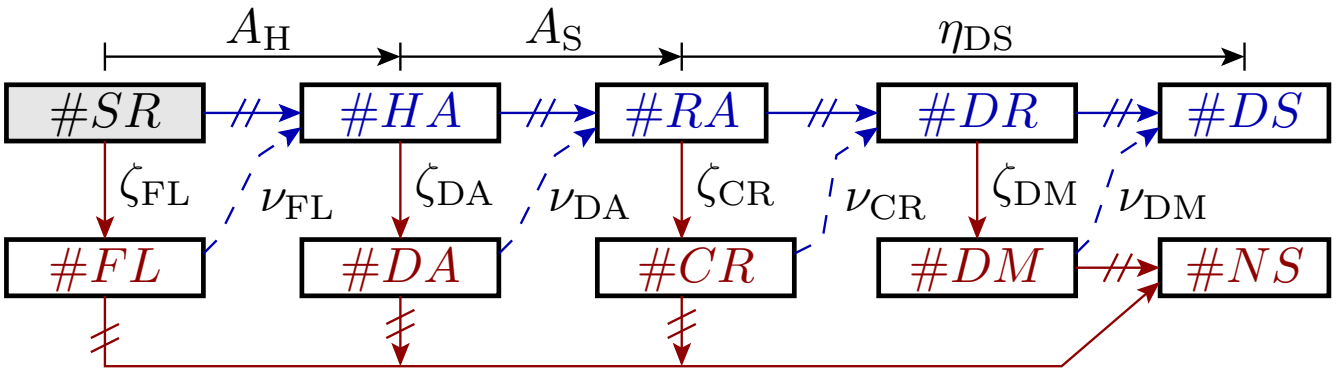
Beispiel 1.1: CVA-Graph und Verfügbarkeit



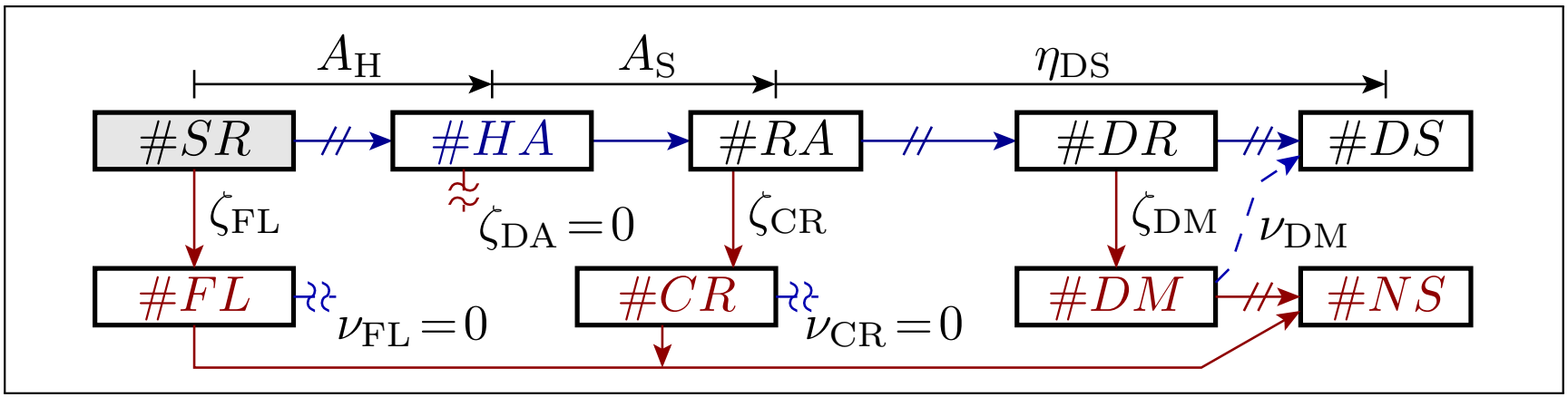
a) *Passen Sie den CVA-Graph so an, dass Ausfälle nie toleriert, Service-Anforderungen bei verfügbarer Hardware immer akzeptiert und bei Absturz nie Leistung erbracht werden.*

b) *Wie groß sind Hardware-Verfügbarkeit, Service-Verfügbarkeit, Erbringungsrate und Gesamtverfügbarkeit mit dem CVA-Graph aus Aufgabe a?*

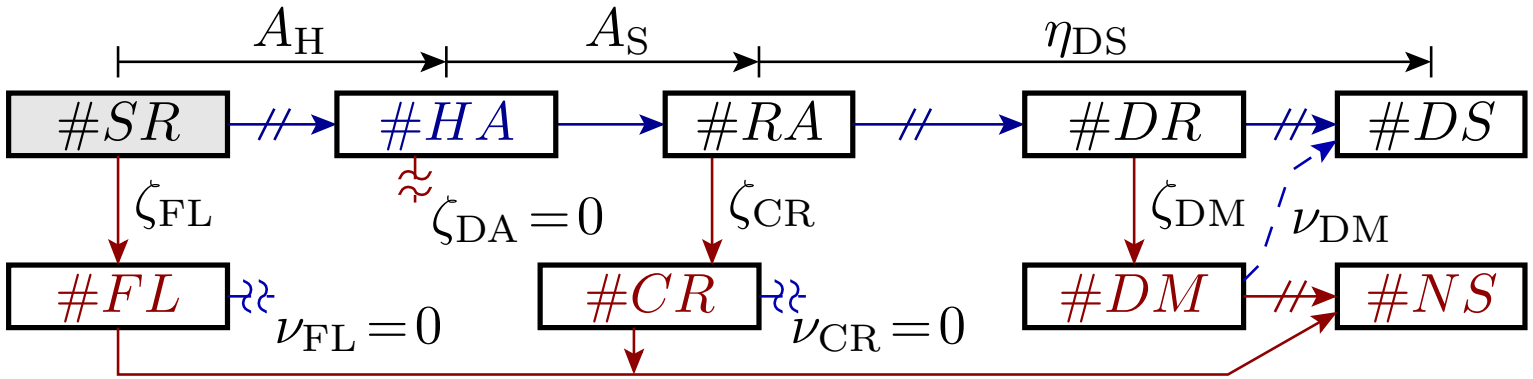
SR, HA	Service-Anforderung, Hardware verfügbar.
RA, DR	Service-Anforderung akzeptiert, erbrachtes Ergebnis.
DS, NS	Erbrachte Service-Leistung, keine Service-Leistung.
FL, DA	Nichtverfügbarkeit wegen Hardware-Ausfall bzw. Annahmeverweigerung.
CR, DM	Nichtverfügbarkeit wegen Absturz bzw. erkannter Fehlfunktion.



a) *Passen Sie den CVA-Graph so an, dass Ausfälle nie toleriert, Service-Anforderungen bei verfügbarer Hardware immer akzeptiert und bei Absturz nie Leistung erbracht werden.*



ζ_{FL}, ν_{FL} HW-Nichtverfügbarkeitsrate, Tolerierungsrate für nicht verfügbare HW.
ζ_{DA}, ν_{DA} Service-Verweigerungsrate, Tolerierungsrate für Service-Verweigerungen.
ζ_{CR}, ν_{CR} Absturzrate, Rate der Tolerierung von Abstürzen.



b) *Wie groß sind Hardware-Verfügbarkeit, Service-Verfügbarkeit, Erbringungsrate und Gesamtverfügbarkeit mit dem CVA-Graph aus Aufgabe a?*

$$A_\mathrm{H} = (1-\zeta_\mathrm{FL})\,;\ A_\mathrm{S} = 1$$
$$\eta_\mathrm{DS} = (1-\zeta_\mathrm{CR})\cdot(1-\zeta_\mathrm{DM}+\zeta_\mathrm{DM}\cdot\nu_\mathrm{DM})$$
$$A = (1-\zeta_\mathrm{FL})\cdot(1-\zeta_\mathrm{CR})\cdot(1-\zeta_\mathrm{DM}\cdot(1-\nu_\mathrm{DM}))$$

$\zeta_\mathrm{DM}, \nu_\mathrm{DM}$	Rate der erkannten Fehlfunktionen, Tolerierungsrate für erkannte Fehlfunktionen.
$A_\mathrm{H}, A_\mathrm{S}$	Hardware-Verfügbarkeit, Service-Verfügbarkeit.
η_DS, A	Rate der erbrachen Service-Leistungen, Gesamtverfügbarkeit.

Zuverlässigkeit

Wiederholung

IT-Nutzung setzt Vertrauen voraus. Verlässlichkeit beschreibt, in welchem Maße gerechtfertigt. Objektive Beschreibung durch Zählwerte für positive und negative Erfahrungen. Unterscheidung nach Aspekten:

Erbringung

- positive Erfahrungen: Erbringung auf Anforderung
- negative Erfahrungen: Service-Verweigerung
- Kenngrößen: Verfügbarkeit, aufspaltbar in das Produkt von Teilverfügbarkeiten.

Richtigkeit:

- positive Erfahrungen: erbrachte Ergebnisse richtige
- negative Erfahrungen: erbrachte Ergebnisse falsch
- Kenngrößen: ‹hier geht es weiter›

Kenngrößen für die Richtigkeit

Zuverlässigkeit*: Anzahl der erbrachten Service-Leistungen (DS) je nicht erkannte Fehlfunktion (NDM):

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

Fehlfunktionsrate: Kehrwert der Zuverlässigkeit.

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

Rate der korrekten Service-Leistungen (hier nicht weiter verwendet):

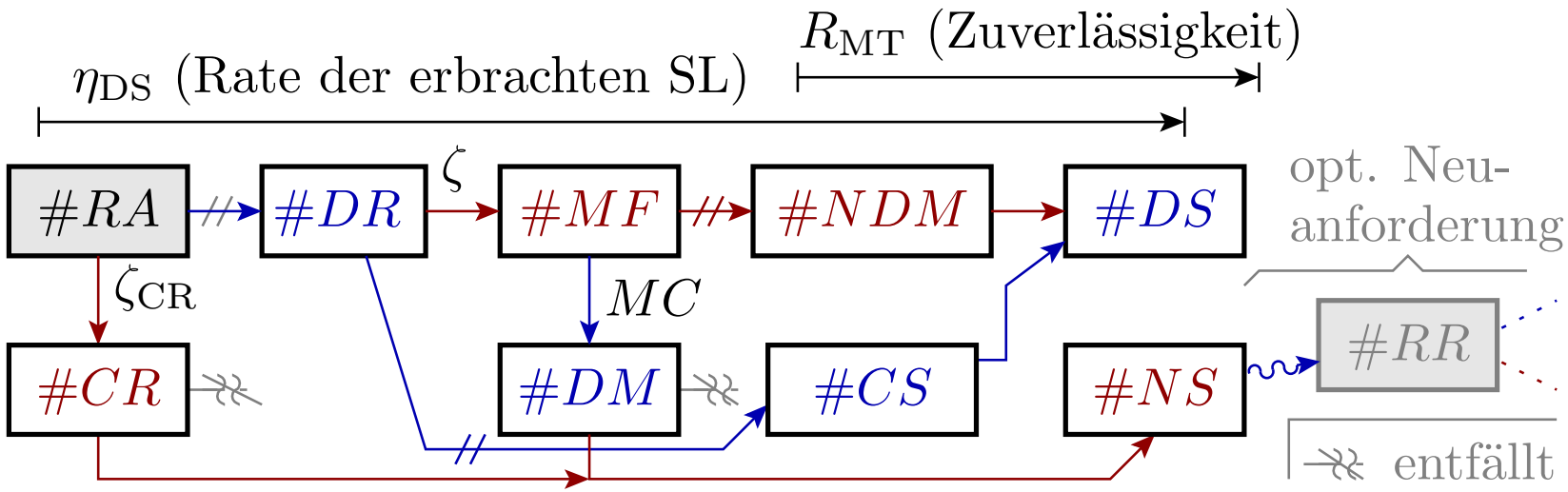
$$\eta_{\mathrm{CS}[\mathrm{MT}]} = 1 - \zeta_{[\mathrm{MT}]}$$

Wir bevorzugen die Zuverlässigkeit R als Maß der Richtigkeit:

> *Zuverlässigkeitsverbesserung um Faktor x bedeutet x-mal so viele richtige Ergebnisse je nicht erkannte Fehlfunktion.*

$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
$\#DS$	Anzahl der erbrachten Service-Leistungen.
$\#NDM$	Anzahl der nicht erkannten Fehlfunktionen (Number of not detected malfunctions).
$\zeta_{[\mathrm{MT}]}$	Fehlfunktionsrate mit bzw. ohne Fehlfunktionsbehandlung.
*	Zweckmäßige, in der Fachwelt jedoch noch unübliche Definitionen.

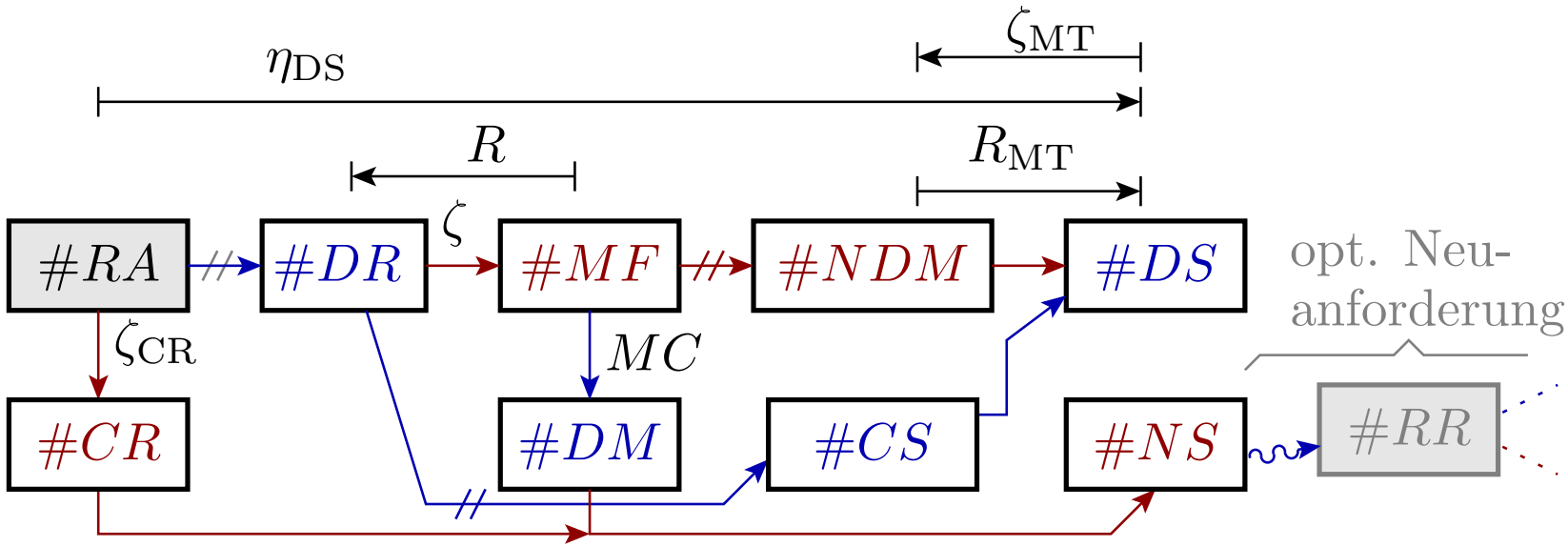
Nachbesserung CVA-Graph



Ergänzung eines Zählwerts für nicht erkannte Fehlfunktionen:

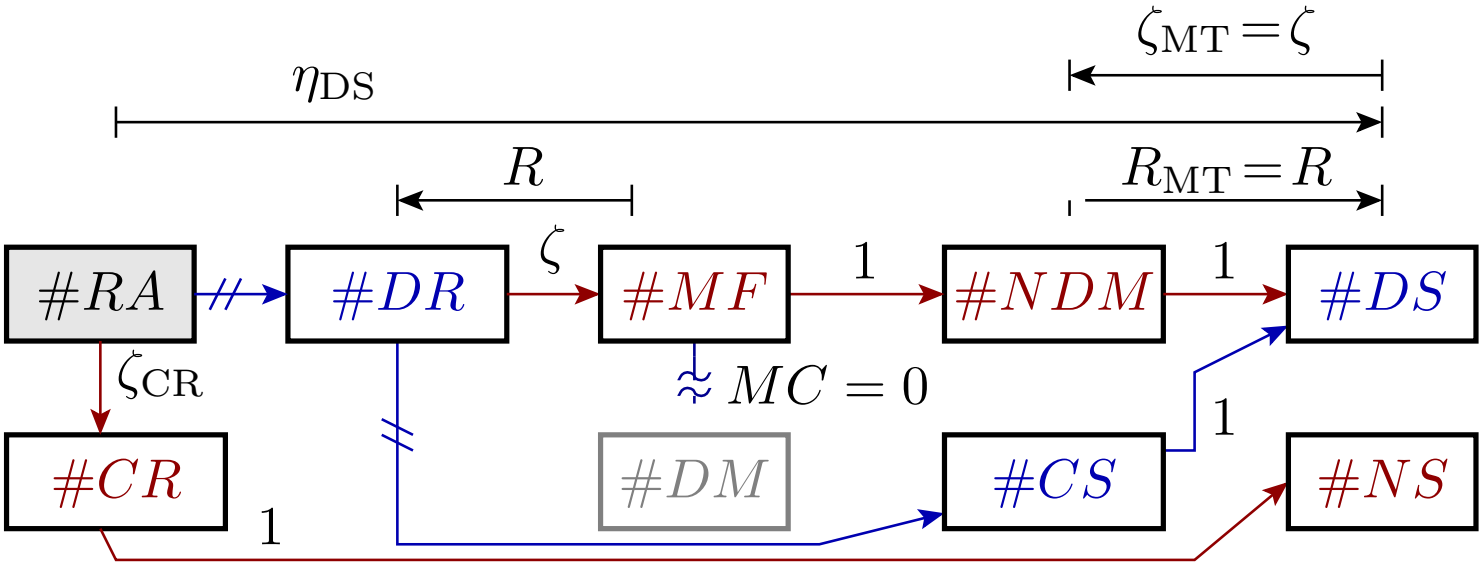
- Fehlfunktionen (MF) werden mit Häufigkeit MC erkannt (DM) und sonst nicht erkannt (NDM).
- Für Abstürze (CR) und erkannte Fehlfunktionen (DM) keine Leistungserbringung (NS).

Das ist der CVA-Graph ohne Leistungserbringung bei erkannten Problemen. Erweiterung um Tolerierungsfähigkeiten später.



η_{DS}	Rate der erbrachen Service-Leistungen.
$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
$\zeta_{[\mathrm{MT}]}$	Fehlfunktionsrate mit bzw. ohne Fehlfunktionsbehandlung.
$\#\langle evt \rangle$	Anzahl der Zählereignisse, $evt \in \{RA, DR, \ldots\}$.
RA, DR	Service-Anforderung akzeptiert, erbrachtes Ergebnis.
MF, NDM	Fehlfunktion, nicht erkennbare Fehlfunktion.
DS, NS	Erbrachte Service-Leistung, keine Service-Leistung.
CR, DM	Nichtverfügbarkeit wegen Absturz bzw. erkannter Fehlfunktion.
ζ_{CR}, MC	Absturzrate, Fehlfunktionsabdeckung.

Ohne Überwachung und Problembehandlung



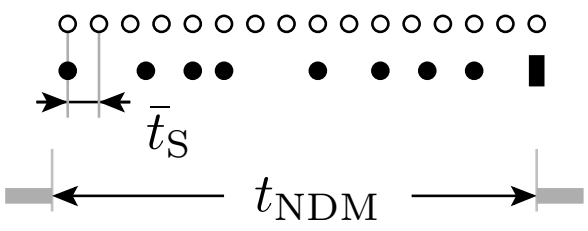
Ohne Problembehandlung sind alle gelieferten Ergebnisse erbrachten Service-Leistungen und keine der Fehlfunktionen wird erkannt:

$$\#DS = \#DR$$
$$\#NDM = \#MF$$

Fehlfunktionsrate gleich Rate der entstehenden MF ohne Abstürze:

$$\zeta_{\mathrm{MT}} = \left.\frac{\#NDM}{\#DS}\right|_{\mathrm{ACR}} = \left.\frac{\#MF}{\#DR}\right|_{\mathrm{ACR}} = \zeta$$
$$R_{\mathrm{MT}} = \left.\frac{\#DS}{\#NDM}\right|_{\mathrm{ACR}} = \left.\frac{\#DR}{\#MF}\right|_{\mathrm{ACR}} = R$$

Abschätzung aus zeitlichen Mittelwerten



nutzbare Zeit zwischen zwei Fehlfunktionen

$$\#DS_{NDM} \approx \eta_{SU} \cdot \#SS_{NDM}$$
$$\bar{t}_{NDM} \approx \#SS_{NDM} \cdot \bar{t}_S$$

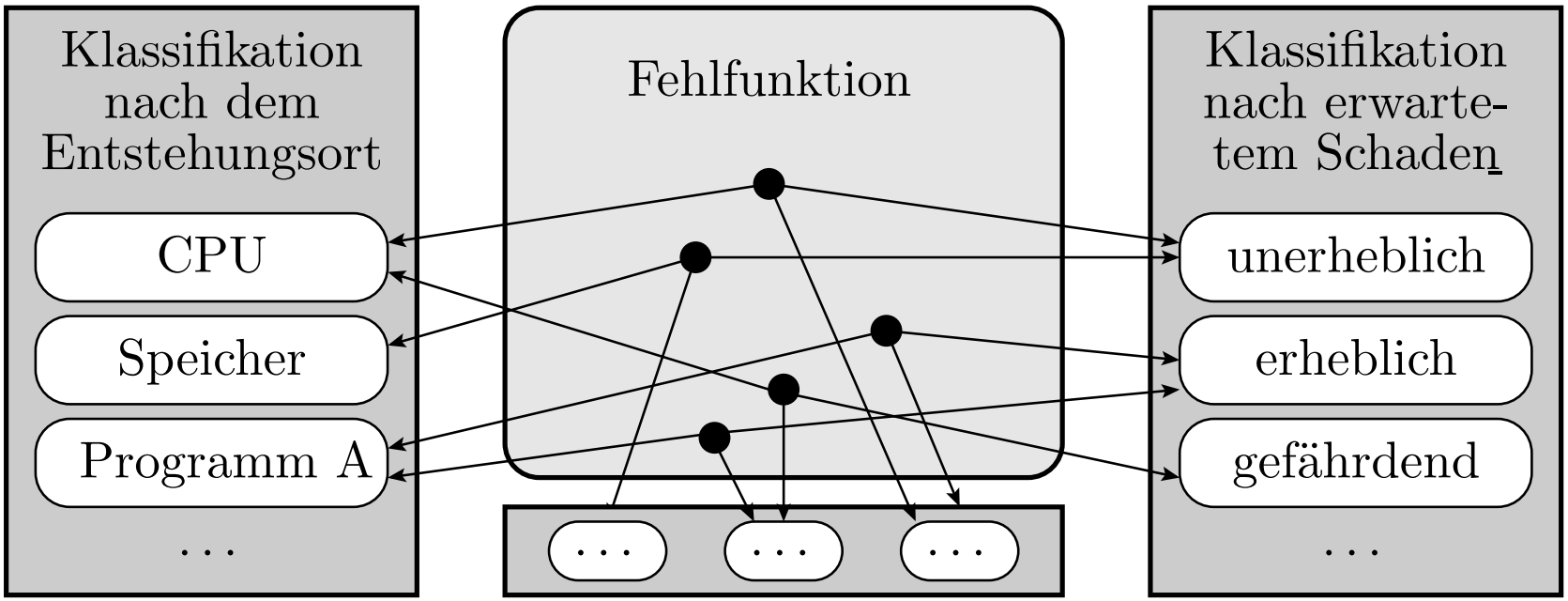
- Service nicht verfügbar
- ∘ Service-Zeitslots (SS)
- • erbrachte Service-Leistungen (DS)

Die zu erwartende Anzahl der erbrachten Leitungen je Fehlfunktionen ist etwa Systemauslastung (η_{SU}) mal mittlere Zeit bis zur nächsten Fehlfunktion abzüglich Problembehebungsdauer $\bar{t}_{MF}$ durch mittlere Service-Dauer ($\bar{t}_S$):

$$R_{[MT]} = \frac{\eta_{SU} \cdot \bar{t}_{NDN}}{\bar{t}_S} \tag{1.10}$$

$\#SS_{NDM}$	Anzahl der Service-Zeitslots je nicht erkannte Fehlfunktion.
$\#DS_{NDM}$	Anzahl der erbrachte Leistungen je nicht erkannte Fehlfunktion.
η_{SU}	Systemauslastungsrate.
$\bar{t}_{NDM}, \bar{t}_S$	Mittlere Service-Zeit je nicht erkannte Fehlfunktion, mittlere Service-Dauer.
$R_{[MT]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.

Teilzuverlässigkeiten



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

- nach Ort, Ursache, Schaden, ... :
- nur Fehlfunktionen eines bestimmten Teilsystems,
- fehler-, störungs- und ausfallbezogene Teilzuverlässigkeit,
- nur MF, die die Betriebs-, Daten- oder Zugangssicherheit mindern.

Bei *eindeutiger Zuordnung* jeder Fehlfunktion *genau zu einer Klasse*:

- Summe aller Fehlfunktionen gleich Summe der Fehlfunktionen aller Klassen:

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

  Das gilt auch für erkannte und nicht erkannte Fehlfunktionen:

$$\#\left[N\right]DM = \sum_{i=1}^{\#MFC} \#\left[N\right]DM_i$$

- Die gesamte Fehlfunktionsrate ist mit und ohne Fehlfunktionsbehandlung die Summe aller Teilfehlfunktionsraten:

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

$\#MFC$	Anzahl der MF-Klassen (Number of malfunction classes).
MF, MF_i	Fehlfunktion, Fehlfunktion der Klasse i.
DM, DM_i	Erkannten Fehlfunktion, erkannte Fehlfunktion der Klasse i.
$\zeta_{[\mathrm{MT}]}$	Fehlfunktionsrate mit bzw. ohne Fehlfunktionsbehandlung.
$\zeta_{[\mathrm{MT}].i}$	Fehlfunktionsrate Fehlfunktionsklasse i mit bzw. ohne Fehlfunktionsbehandlung.

Kehrwert der Gesamtzuverlässigkeit gleich Summe der Kehrwerte der Teilzuverlässigkeiten:

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

$\#MFC$	Anzahl der MF-Klassen (Number of malfunction classes).
$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
$R_{[\mathrm{MT}].i}$	Teilzuverlässigkeit Fehlfunktionsklasse i mit bzw. ohne Fehlfunktionsbehandlung.

Beispiel 1.2: Teilzuverlässigkeiten

In einem System mit Fehlfunktionsbehandlung werden die Fehlfunktionen vom Speicher, vom Prozessor, von der Software oder vom Rest verursacht. Mittleren Zeiten zwischen Fehlfunktionen der Teilsysteme:

Teilsystem i	Speicher	Prozessor	Software	alle anderen
$\bar{t}_{\mathrm{NDM}.i}$	1.000 h	6.000 h	2000 h	4.000 h

Mittlere Service-Dauer $\bar{t}_{\mathrm{S}} = 1\,\mathrm{min}$. Systemauslastung $\eta_{\mathrm{SU}} = 50\%$.

a) *Wie groß sind die vier aus den Zeitangaben abschätzbaren Teilzuverlässigkeiten $R_{\mathrm{MT}.i}$ und Teilfehlfunktionsraten $\zeta_{\mathrm{MT}.i}$?*

b) *Wie groß sind Fehlfunktionsrate ζ_{MT} und Zuverlässigkeit R_{MT} des Gesamtsystems?*

$\bar{t}_{\mathrm{NDM}}, \bar{t}_{\mathrm{S}}$	Mittlere Service-Zeit je nicht erkannte Fehlfunktion, mittlere Service-Dauer.
η_{SU}	Systemauslastungsrate.
$\zeta_{\mathrm{MT}.i}$	Fehlfunktionsrate Fehlfunktionsklasse i mit Fehlfunktionsbehandlung.
$R_{\mathrm{MT}}, \zeta_{\mathrm{MT}}$	Zuverlässigkeit und Fehlfunktionsrate mit Fehlfunktionsbehandlung.

Teilsystem i	Speicher	Prozessor	Software	alle anderen
$\bar{t}_{\mathrm{NDM}.i}$	1.000 h	6.000 h	2000 h	4.000 h

Mittlere Service-Dauer $\bar{t}_{\mathrm{S}} = 1\,\mathrm{min}$. Systemauslastung $\eta_{\mathrm{SU}} = 50\%$.

a) *Wie groß sind die vier aus den Zeitangaben abschätzbaren Teilzuverlässigkeiten $R_{\mathrm{MT}.i}$ und Teilfehlfunktionsraten $\zeta_{\mathrm{MT}.i}$?*

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

Teilsystem i	Speicher	Prozessor	Software	Rest
$\eta_{\mathrm{SU}} \cdot \bar{t}_{\mathrm{NDM}}$ in min	$3 \cdot 10^4$	$18 \cdot 10^4$	$6 \cdot 10^4$	$12 \cdot 10^4$
$R_{\mathrm{MT}.i}$ in $\left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]$	$3 \cdot 10^4$	$18 \cdot 10^4$	$6 \cdot 10^4$	$12 \cdot 10^4$
$\zeta_{\mathrm{MT}.i} = \frac{1}{R_{\mathrm{MT}.i}}$ 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
$\bar{t}_{\mathrm{NDM}.i}$	1.000 h	6.000 h	2000 h	4.000 h

Mittlere Service-Dauer $\bar{t}_{\mathrm{S}} = 1\,\mathrm{min}$. Systemauslastung $\eta_{\mathrm{SU}} = 50\%$.

b) *Wie groß sind Fehlfunktionsrate ζ_{MT} und Zuverlässigkeit R_{MT} des Gesamtsystems?*

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

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

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

$$\begin{aligned}
\zeta_{\mathrm{MT}} &= \left(3{,}33 \cdot 10^{-5} + 5{,}56 \cdot 10^{-6} + 1{,}67 \cdot 1 + 8{,}33 \cdot 10^{-6}\right) \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right] \\
&= 6{,}39 \cdot 10^{-5} \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right] \\
\frac{1}{R_{\mathrm{MT}}} &= \left(\frac{1}{3{\cdot}10^4} + \frac{1}{18{\cdot}10^4} + \frac{1}{6{\cdot}10^4} + \frac{1}{12{\cdot}10^4}\right) \left[\frac{\mathrm{MF}}{\mathrm{DS}}\right] = \zeta_{\mathrm{MT}} \\
R_{\mathrm{MT}} &= \frac{1}{\zeta_{\mathrm{MT}}} = 1{,}57 \cdot 10^4 \left[\frac{\mathrm{DS}}{\mathrm{MF}}\right]
\end{aligned}$$

Sicherheit

Schaden durch Fehlfunktionen

Auch für Sicherheiten sind gegenwärtig noch subjektive Einschätzung ohne Zählen positiver und negativer Erfahrungen üblich. Sicherheitsstufen (SIL – **S**afety **I**ntegrity **L**evel) für Industriegeräte nach IEC 61508:

- 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 werden Sicherheiten als Teilzuverlässigkeiten für sicherheitsgefährdende Probleme (SP) modellieren.

Sicherheitgefährdende Probleme

Sicherheiten beziehen sich auf angenommene Gefährdungen:

Sicherheit	Sicher wovor?
Betriebssicherheit (safty)	Personen- und Umweltschäden
Zugangssicherheit (data protection)	Datendiebstahl
Datensicherheit (data security)	Datenverlust
...	...

Die Rate der die Sicherheit gefährdenden Probleme:

$$\zeta_{\mathrm{S}} = \frac{\#SP}{\#SR}\Big|_{\mathrm{ACR}} \tag{1.13}$$

Bei Zuordnung von jedem Problem zu genau einer Problemklasse ist die Gesamtrate die Summe der Teilproblemraten aller Problemklassen:

$$\zeta_{\mathrm{S}} = \sum_{i=1}^{\#SPC} \zeta_{\mathrm{S}.i} \tag{1.14}$$

DS, SP	Service-Anforderung, sicherheitsgefährdende Probleme.
$\#SPC$	Anzahl der Sicherheitsproblemklassen (Number of safety and security problem classes).
$\zeta_{\mathrm{S}}, \zeta_{\mathrm{S}.i}$	Rate der sicherheitsgefährdenden Probleme insgesamt, für jede Problemklasse einzeln.

Sicherheit und Teilsicherheiten

Sicherheit ist der Kehrwert der Rate der sicherheitsgefährdenden Probleme:

$$S = \frac{\#SR}{\#SP}\Big|_{\mathrm{ACR}}$$
$$S = \frac{1}{\zeta_{\mathrm{S}}} \tag{1.15}$$

Bei Zuordnung von jedem Problem zu genau einer Problemklasse ist der Kehrwert der Gesamtsicherheit die Summe der Kehrwerte alle Teilsicherheiten:

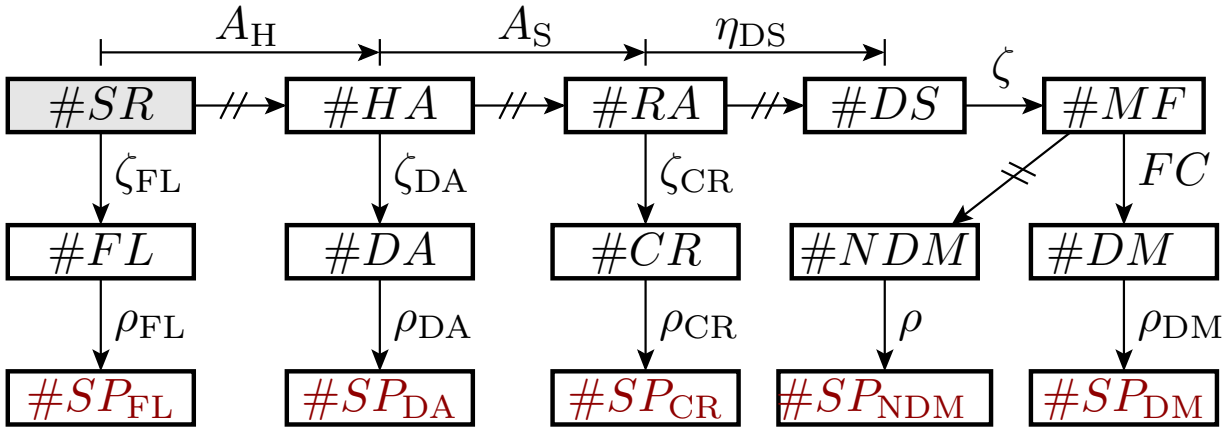
$$\frac{1}{S} = \sum_{i=1}^{\#SPC} \frac{1}{S_i} \tag{1.16}$$

Bisherige Problemaufteilung:

- Hardware-Ausfall, Service-Verweigerung,
- Absturz, erkannte/nicht erkannte Fehlfunktion.

S, S_i	Gesamtsicherheit, Teilsicherheiten i.
$\#SPC$	Anzahl der Sicherheitsproblemklassen (Number of safety and security problem classes).
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

CVA-Graph Sicherheitsgefährdungen



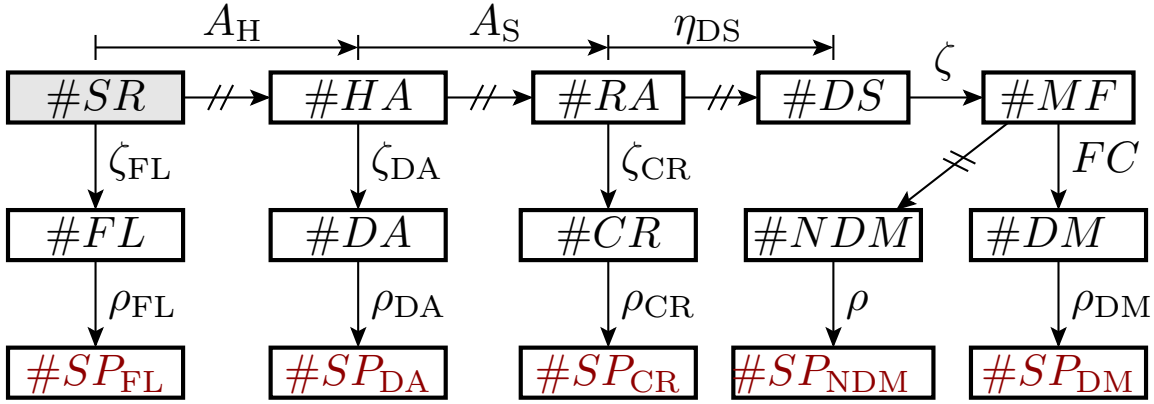
$\zeta_{...}$	Problemraten
$\rho_{...}$	sicherheitskritische Anteile
$\#SP_{...}$	Zählwerte für sicherheitskritische Probleme

Raten der Sicherheitsgefährdungen

- durch Hardware-Ausfälle (FL failture):

$$\zeta_{S.FL} = \zeta_{FL} \cdot \rho_{FL} \tag{1.17}$$

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



- durch Annahmeverweigerung (DA deny of acceptance):

$$\zeta_{S.DA} = A_H \cdot \zeta_{DA} \cdot \rho_{DA} \tag{1.18}$$

- durch Abstürze (CR crash):

$$\zeta_{S.CR} = A_H \cdot A_S \cdot \zeta_{CR} \cdot \rho_{CR} \tag{1.19}$$

- durch erkannte Fehlfunktionen (MF malfunction):

$$\zeta_{S.DM} = A \cdot \zeta \cdot FC \cdot \rho_{DM} \tag{1.20}$$

- durch nicht erkannte Fehlfunktionen):

$$\zeta_{S.NDM} = A \cdot \zeta \cdot (1 - FC) \cdot \rho \tag{1.21}$$

Gesamtrate der sicherheitsgefährdenden Probleme:

$$\zeta_S = \zeta_{S.FL} + \zeta_{S.DA} + \zeta_{S.CR} + \zeta_{S.DM} + \zeta_{S.NDM} \tag{1.22}$$

Sicherheiten und Zuverlässigkeiten

IT-Systeme haben Verfügbarkeiten von typ $A > 99{,}9\%$, so dass die Teilverfügbarkeiten A_{H}, A_{S}und η_{DS} in Gl. 1.22 praktisch als eins betrachtet werden können:

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

Auf erkannte Probleme (Hardware-Ausfall, Service-Verweigerung, Absturz oder erkannte Fehlfunktion) reagieren System oder Nutzer mit einer Problembehandlung. Wenn dabei für alle erkannten Probleme ein sicherer Zustand hergestellt wird, verbleibt als sicherheitsgefährdend nur die nurch nicht erkannte Fehlfunktionen:

$$\zeta_{\mathrm{S}} = \zeta \cdot (1 - FC) \cdot \rho = \frac{\rho}{R_{\mathrm{MT}}}$$

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

ζ_i, σ_i	Problemrate, sicherheitsgefährdender Anteil jeweils für Problemklasse i.
FL, DA	Ausfall, Annahmeverweigerung.
CR, DM	Absturz, erkannte Fehlfunktion.
S	Sicherheit (Safety or security).
ρ	Anteil sicherheitskritischer Fehlfunktionen an den nicht erkannten Fehlfunktionen.
ζ, MC	Fehlfunktionsrate, Fehlfunktionsabdeckung.

Sicherheitsverbesserung durch Zusatzeinheit

Die Verringerung der sicherheitskritischen Anteil der einzelnen Problemraten verlangen Zusatzeinheiten:

- Reserve-Hardware, Notstromversorgung,
- Notprogramme, Schutzvorrichtungen, Sicherheitseinrichtungen, ...

die selbst zu den Problemraten beitragen.

Wenn für alle erkannten Probleme ein sicherer Zustand hergestellt wird, sind nur NDM potentielle Sicherheitsgefährdungen:

- Minderung des Anteils der sicherheitsgefährdenen MF durch die Sicherheitseinheit um Faktor ν und
- Erhöhung der MF-Rate um die der Sicherheitseinheit ζ_{SU}:

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

S_{SU}, ζ_{SU}	Sicherheit mit Sicherheitseinheit, Fehlfunktionsrate der Sicherheitseinheit.
ρ, ν	Anteil sicherheitsritischer Fehlfunktionen, Anteilverringerung durch Sicherheitseinheit.

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_{SU} *verringert den Anteil der gefährdenden MF auf ein Zehntel. Systemauslastung 100%.*

$\bar{t}_{\mathrm{NDM}} = 1000\,\mathrm{h}$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 1$, $\rho = 1\%$ $\left[\frac{\mathrm{SP}}{\mathrm{NDM}}\right]$, $\nu = 0{,}1$

a) *Zuverlässigkeit und Sicherheit ohne das zusätzliche Steuergerät?*

b) *Mindestzuverlässigkeit Steuergerät* R_{SU}*, damit sich die Sicherheit verfünffacht (*$S_{\mathrm{SU}} \geq 5 \cdot S$*)?*

$\bar{t}_{\mathrm{NDM}}$, $\bar{t}_{\mathrm{S}}$	Mittlere Service-Zeit je nicht erkannte Fehlfunktion, mittlere Service-Dauer.
η_{SU}	Systemauslastungsrate.
ρ, ν	Anteil sicherheitsritischer Fehlfunktionen, Anteilverringerung durch Sicherheitseinheit.
S, S_{SU}	Sicherheit ohne Zusatzsteuergerät, Sicherheit mit Zusatzsteuergerät.

$\bar{t}_{\mathrm{NDM}} = 1000\,\mathrm{h}$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 1$, $\rho = 1\%$ $\left[\frac{\mathrm{SP}}{\mathrm{NDM}}\right]$, $\nu = 0{,}1$

a) *Zuverlässigkeit und Sicherheit ohne das zusätzliche Steuergerät?*

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

Die Aufgabe betrachtet als Problem nur die Rate der nicht erkannten, von der Fehlfunktionsbehandlung als korrekt weitergereichten Fehlfunktionen

$$\zeta = \frac{1}{R_{\mathrm{MT}}} = \frac{\bar{t}_{\mathrm{S}}}{\eta_{\mathrm{SU}} \cdot \bar{t}_{\mathrm{NDM}}} = 10^{-3} \left[\frac{\mathrm{NDM}}{\mathrm{DS}}\right]$$

die mit einer Rate $\sigma = 1\%$ die Sicherheit gefährden. Zuverlässigkeit und Sicherheit:

$$R = \frac{1}{\zeta} = 10^{3} \left[\frac{\mathrm{DS}}{\mathrm{NDM}}\right]$$

$$S = \frac{1}{\zeta \cdot \rho} = 10^{5} \left[\frac{\mathrm{DS}}{\mathrm{SP}}\right]$$

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

ζ_{NDM} Rate der nicht erkannten Fehlfunktionen.

$\bar{t}_{\mathrm{NDM}} = 1000\,\mathrm{h}$, $\bar{t}_{\mathrm{S}} = 1\,\mathrm{h}$, $\eta_{\mathrm{SU}} = 1$, $\rho = 1\%$ $\left[\frac{\mathrm{SP}}{\mathrm{NDM}}\right]$, $\nu = 0{,}1$

b) *Mindestzuverlässigkeit Steuergerät R_{SU}, damit sich die Sicherheit verfünffacht ($S_{\mathrm{SU}} \geq 5 \cdot S$)?*

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

Maximale Zuverlässigkeitsverringerung durch das Steuergerät:

$$\underbrace{(\zeta + \zeta_{\mathrm{SU}}) \cdot \rho \cdot \nu}_{1/S_{\mathrm{SU}}} \leq \frac{1}{5} \cdot \underbrace{\zeta \cdot \rho}_{1/S}$$

$$(\zeta + \zeta_{\mathrm{SU}}) \cdot \cancel{\rho} \cdot \frac{1}{10} \leq \frac{1}{5} \cdot \zeta \cdot \cancel{\rho}$$

$$\cancel{\zeta} + \zeta_{\mathrm{SU}} \leq \cancel{2} \cdot \zeta$$

$$R_{\mathrm{SU}} \geq R_{\mathrm{MT}} = 10^3 \left[\frac{\mathrm{DS}}{\mathrm{NDM}}\right]$$

Zusatzsteuergerät mindestens so zuverlässig wie Fahrzeug.

Anmerkungen zur Aufgabe

Es gibt aktuelle Ethik-Diskussionen, ob autonome Fahrzeuge in kritischen Fahrsituationen Kinder, Rentner, ... überfahren sollten.

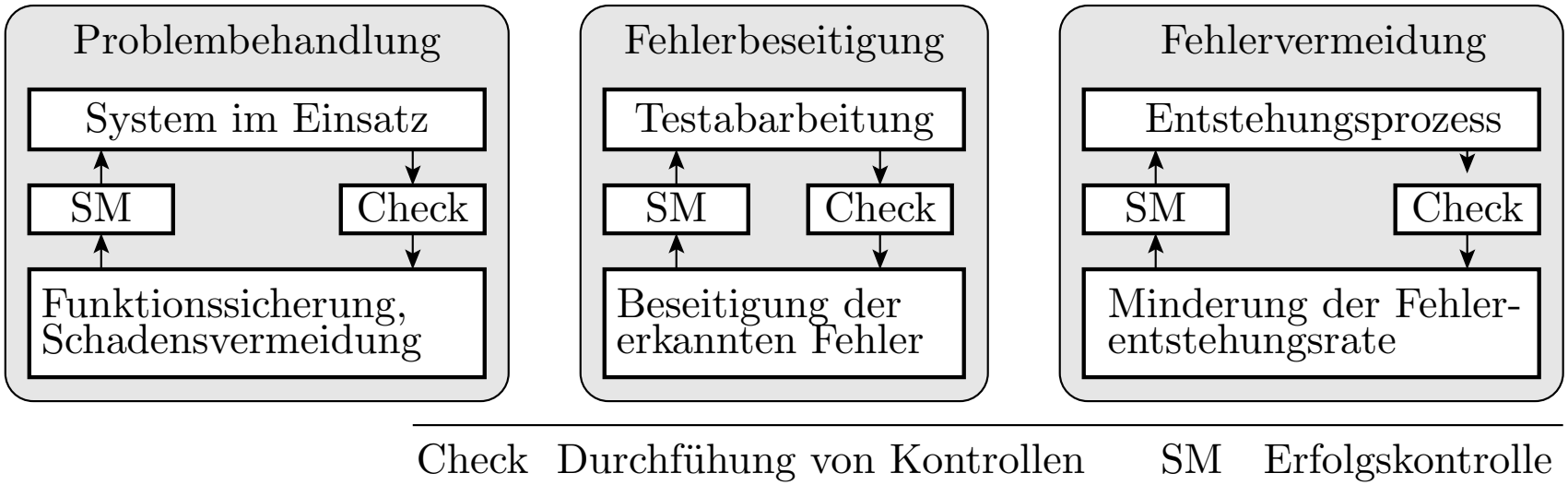
- Smarte Reaktionen verlangen komplizierte Zusatzsysteme, die tendentiell unzuverlässig sind.
- Unzuverlässige Sicherheitseinrichtungen sind keine gute Idee.
- Für nicht erkennbare Fehlfunktionen ist überhaupt kein Notfallverhalten einprogrammierbar.

Hohe Sicherheit:

- hohe Zuverlässigkeit,
- Vermeidung von Sicherheitsrisiken durch erkannte Probleme.
- Haftflichversicherung für Restrisiko durch Systembetreiber.

Zusammenfassung

Sicherung der Verlässlichkeit

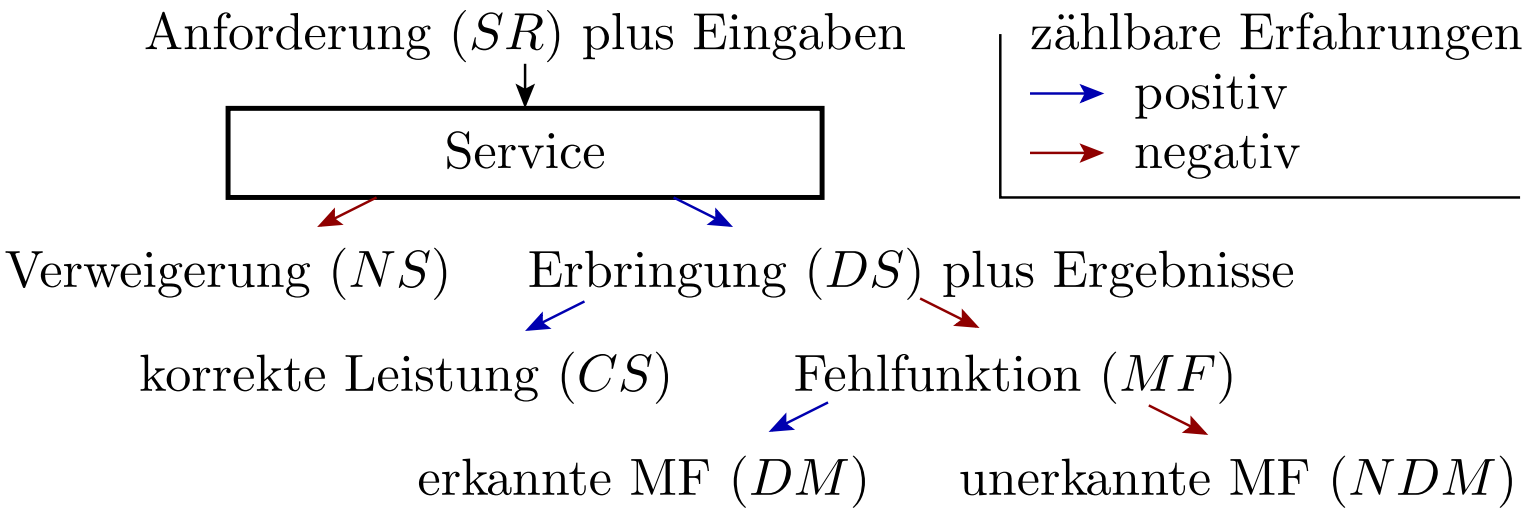


Verlässlichkeit beschreibt, wie weit das Vertrauen in ein IT-System gerechtfertigt ist. Sicherung durch Iterationen aus Kontrolle, Korrektur und Erfolgskontrolle auf drei Ebenen:

- Problembehandlung im Einsatz,
- Fehlerbeseitigung vor der Nutzung und in Nutzungspausen,
- Fehlervermeidung durch verbesserte Entstehungsprozesse.

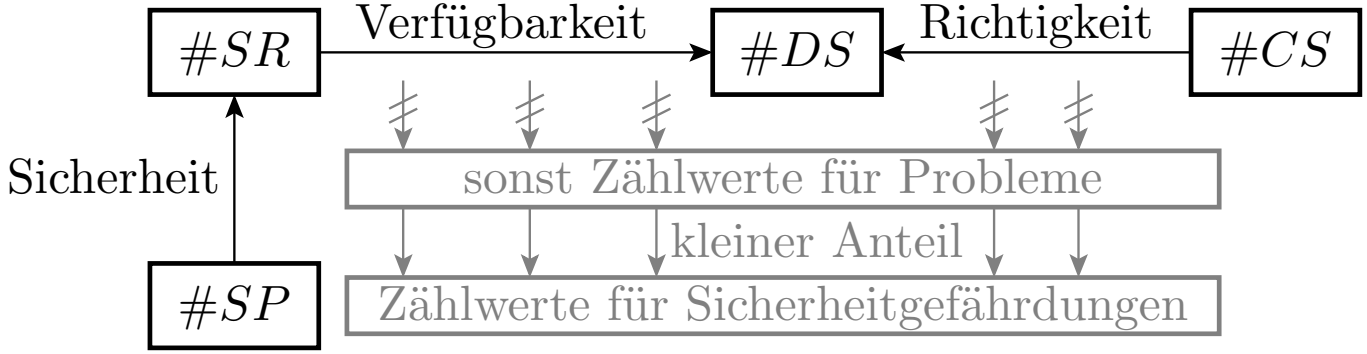
Mit der Fehlerkultur »Beseitigung aller erkannten Probleme und Problemursachen« bestimmen vor allem die Kontrollen die Verlässlichkeit.

Kenngrößen, Service-Modell, ACR



- **Kenngrößensystem** Beschreibung der Verlässlichkeit und ihrer Teilaspekte durch Zählwerte für positive und negative Erfahrungen.
- **Service-Modell**: Diskretisierung der Leistungserbringung. Auf Anforderung wird keine (NS) oder ein Leistung erbracht (DS). Die Leistung kann richtig (CS) oder falsch (MF) sein. ...
- **ACR**: Brauchbare Schätzungen verlangen ausreichend große Zählwerte (siehe Abschn. 4.2.7 *Schätzen von Zählwerten*).

Kenngrößen der Verlässlichkeit



Erbringung:

- Verfügbarkeit: (1.1) $A = \frac{\#DS}{\#SR}\Big|_{\mathrm{ACR}}$

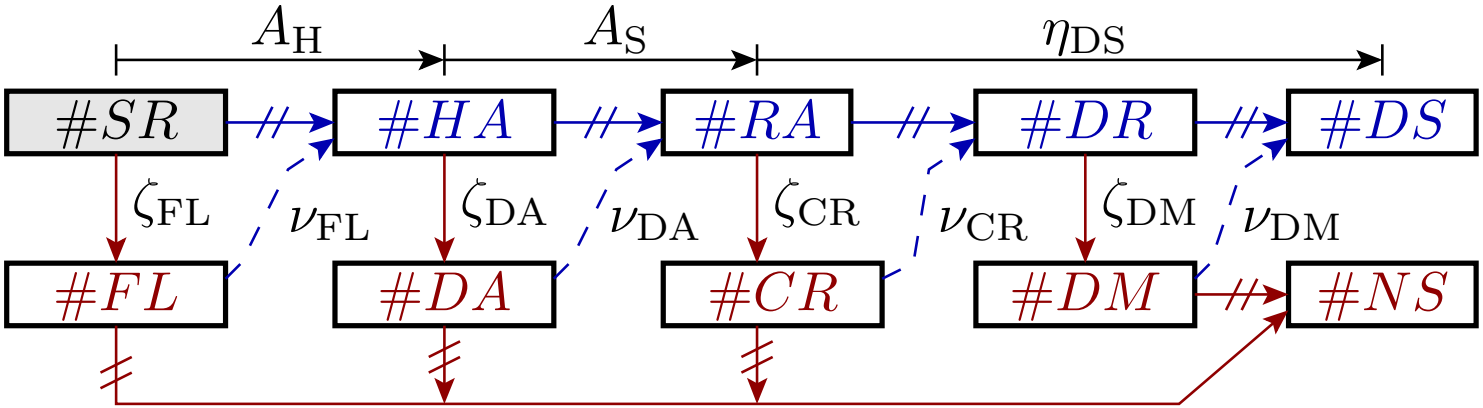
Richtigkeit:

- Zuverlässigkeit: (1.8) $R_{[\mathrm{MT}]} = \frac{\#DS}{\#NDM}\Big|_{\mathrm{ACR}}$
- MF-Rate: (1.9) $\zeta_{[\mathrm{MT}]} = \frac{1}{R_{[\mathrm{MT}]}} = \frac{\#NDM}{\#DS}\Big|_{\mathrm{ACR}}$

Sicherheit:

- Rate Sich.-Prob.: (1.13) $\zeta_{\mathrm{S}} = \frac{\#SP}{\#SR}\Big|_{\mathrm{ACR}}$
- Sicherheit: (1.15) $S = \frac{1}{\zeta_{\mathrm{S}}}$

Gesamt- und Teilverfügbarkeiten



Aufteilung nach Ursache der Nichtverfügbarkeit (und Reaktion darauf):

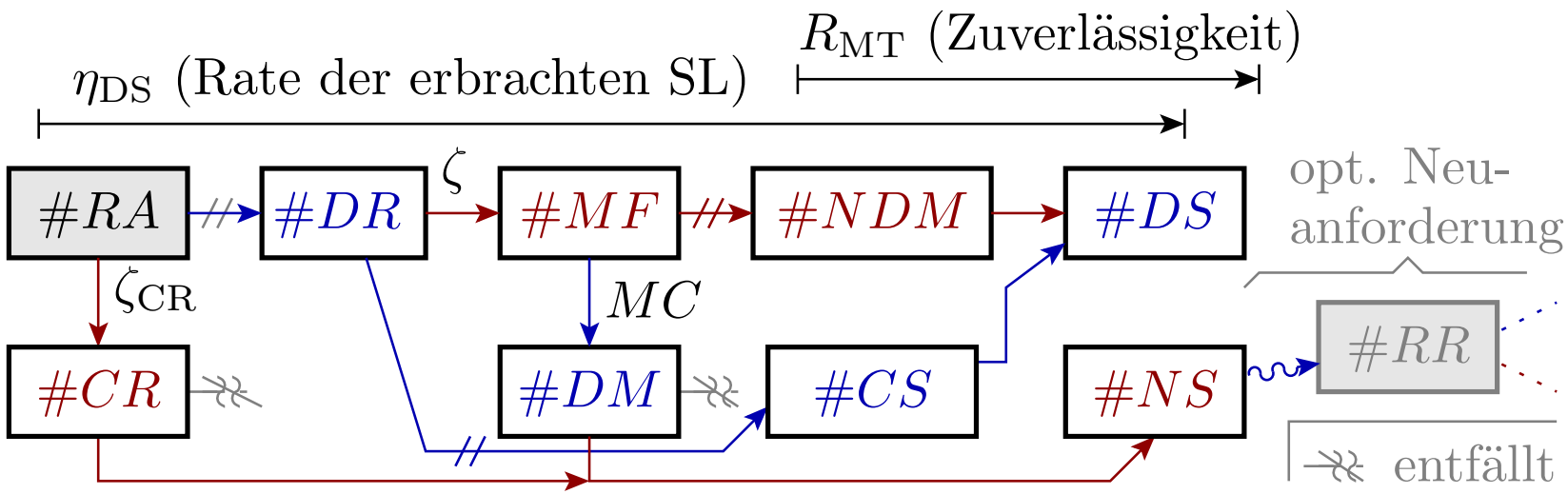
- FL: Hardware ausgefallen (hardware failure),
- DA: Annahmeverweigerung (denial of acceptance),
- CR: Absturz bei der Service-Ausführung (crash),
- DM: erkannte Fehlfunktion (detected malfunction).

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

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

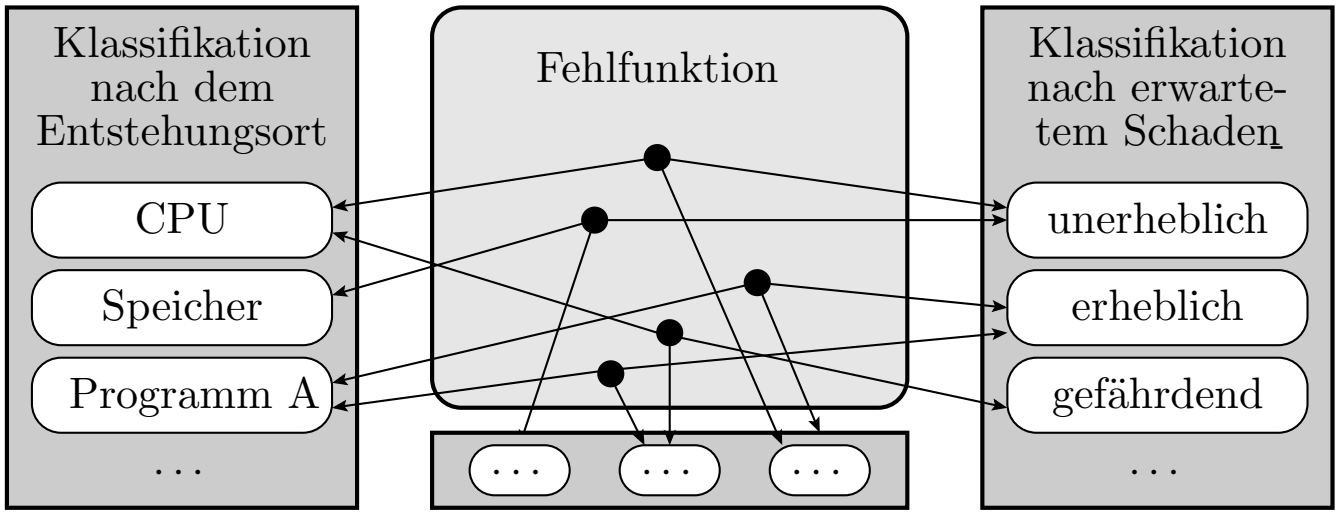
Gesamtverfügbarkeit: (1.5) $$A = A_H \cdot A_S \cdot \eta_{DS}$$

Erbringungsrate und Zuverlässigkeit



Die Erbringungsrate in erbrachte Leistungen je akzeptierte Anforderungen und die Zuverlässigkeit in erbrachte Leistungen je Fehlfunktionen hängen erheblich von der Fehlefunktionsbehandlung ab. Im einfachten Fall erfolgt nach einem Absturz oder einer erkannten Fehlfunktion ein Berechnungsabbruch ohne Leistungsauslieferung. Alternativ wird die Berechnung wiederholt. Fehlfunktionsbehandlung erst im Folgeabschnitt.

Teilzuverlässigkeiten



Wenn man alle Fehlfunktionen so Klassen zuordnet, dass jede genau einmal enthalten ist:

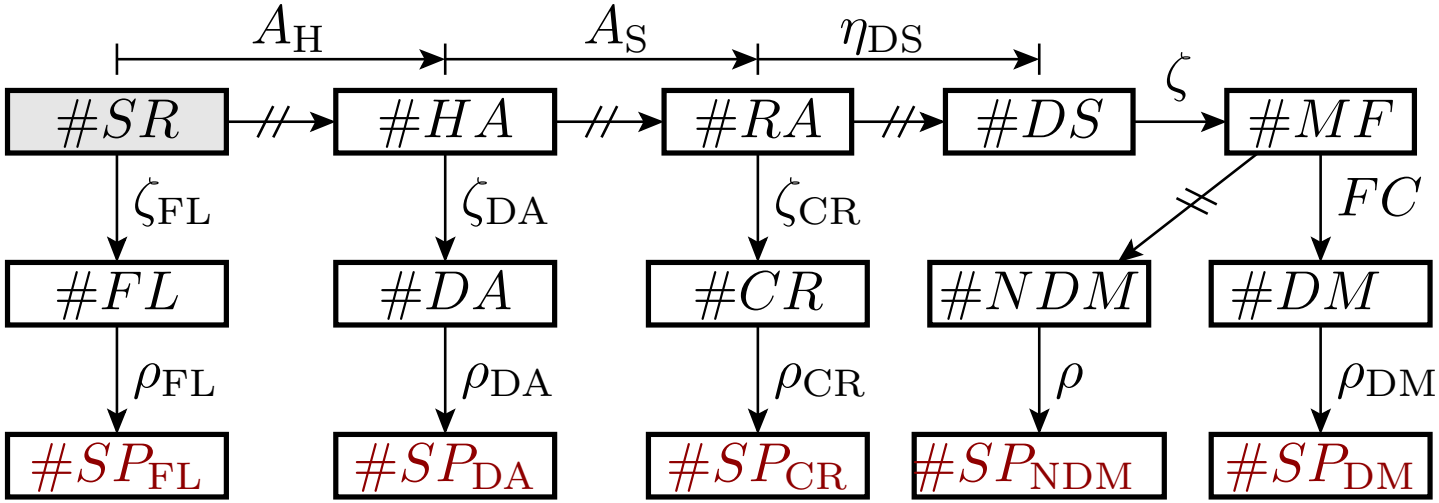
- Gesamtfehlfunktionsrate gleich Summe der Teilfehlfunktionsraten:

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

- Kehrwert Gesamtzuverlässigkeit gleich Kehrwertsumme der Teilzuverlässigkeiten:

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

Sicherheit mehr im Detail



Sicherheit bezieht sich

- auf angenommenen Gefährungen (Betriebssicherheit, Zugangssicherheit, Datensicherheit) und
- betrachtete Probleme:
  - erkannte Ausfälle, Leistungsverweigerungen, Abstürze, Fehlerfunktionen,
  - nicht erkannte Fehlfunktionen.

Bei einer im Normalfall hohen Verfügbarkeit $A \to 1$:

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

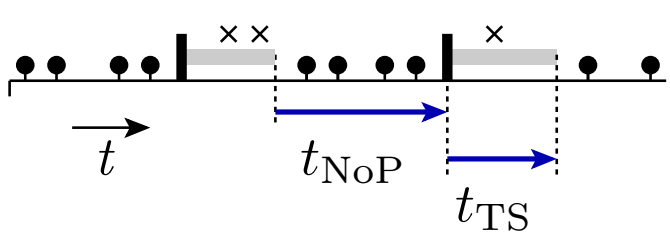
Idealerweise reagiert ein System auf erkannte Probleme (Ausfälle, Abstürze , erkannte Fehlfunktionen, ...) so, dass Gefährdungen ausgeschlossen sind. Nur auf nicht erkannte Fehlfunktionen ist keine schadesausschließende Reaktion möglich. Wenn für erkannte Probleme Sicherheitsgefährdungen ausgeschlossen sind, verhält sich die Sicherheit proportional zur Zuverlässigkeit:

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

Sicherheitseinrichtungen zur Minderung des Anteils der sicherheitsgefährdenden Probleme sind selbst Problemquellen, die die Zuverlässigkeit beeinträchtigen. Die Fehlfunktionsrate nimmt insgesammt zu und der sicherheitskritische Anteil davon ab:

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

Abschätzung aus Zeiten



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

Zeiten lassen oft einfacher abschätzen als Zählwerte.

Verfügbarkeit in Abhängigkeit von der mittleren problemfreien Zeit und der mittleren Zeit für die Problembehebung:

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

Hardware-Verfügbarkeit in Abhängigkeit von der mittleren Zeit bis zum nächsten Ausfall und der mittleren Reparaturdauer:

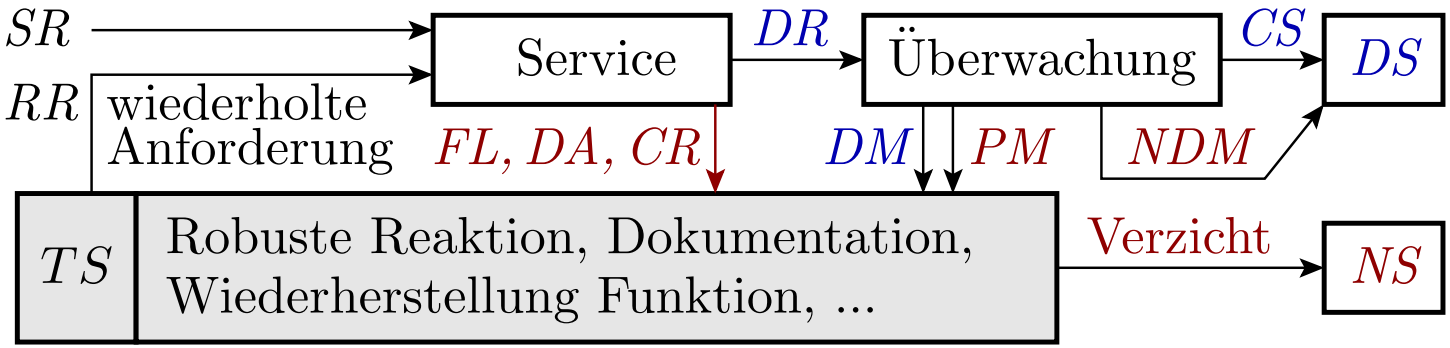
(1.6) $$A_{\mathrm{H}} = \frac{\bar{t}_{\mathrm{FL}}}{\bar{t}_{\mathrm{FL}} + \bar{t}_{\mathrm{R}}}$$

Zuverlässigkeit in Abhängigkeit von der mittleren Zeit zwischen Fehlfunktionen, der mittleren Service-Dauer etc.:

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

Problembehandlung

Problembehandlung im laufenden Betrieb



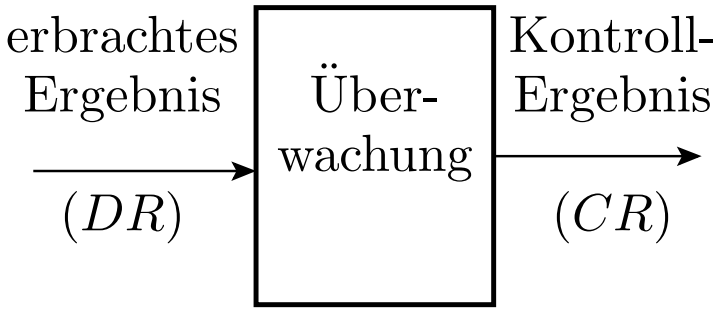
Iteration aus Überwachung, Problembeseitigung und Erfolgskontrolle.

- Abstürze (CR) und erkannte Fehlfunktionen (DM) werden aussortiert (NS) oder über eine wiederholte Anforderung (RR) beseitigt.
- Nicht erbrachte Leistungen (NS) mindern die Erbringungsrate η_{DS}.
- Nicht erkannte Fehlfunktionen (NDM) beeinträchtigen Zuverlässigkeit (R) und Sicherheiten (S).

SR, RR	Service-Anforderung, Wiederholanforderung.
DR, CS	Erbrachtes Ergebnis, korrekte Service-Leistung.
NDM, PM	Nicht erkannte Fehlfunktion, Phantomfehlfunktion.
DS, NS	Erbrachter Service, keine Service-Leistung.
FL, DA	Nichtverfügbarkeit wegen Hardware-Ausfall bzw. Annahmeverweigerung.
CR, TS	Absturz, Problembehandlung (Troubleshooting).

Überwachung

Kenngrößen der Überwachung



DR	CR	Kontroll-MF
CS	CSC	—
CS	PM	Phantom-MF
MF	DM	—
MF	NDM	Maskierung

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

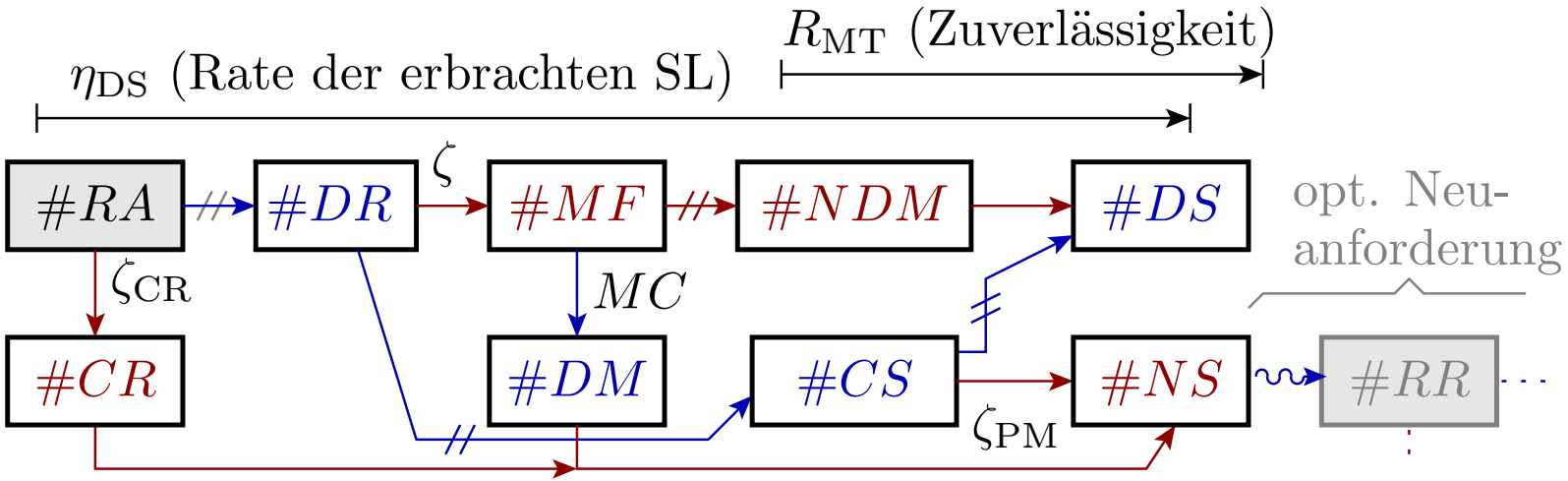
$$MC = \left.\frac{\#DM}{\#MF}\right|_{\mathrm{ACR}} \tag{1.26}$$

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

$$\zeta_{\mathrm{PM}} = \left.\frac{\#PM}{\#CS}\right|_{\mathrm{ACR}} \tag{1.27}$$

DS, CR	Erbrachte Service-Leistung, Kontrollergebnis.
CS, MF	Korrekte Service-Leistung, Fehlfunktion.
DM, CSC	Erkannte Fehlfunktion, korrekte als korrekt erkannte Service-Leistung.
NDM, PM	Nicht erkannte Fehlfunktion, Phantom-Fehlfunktion.
MC, ζ_{PM}	Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.

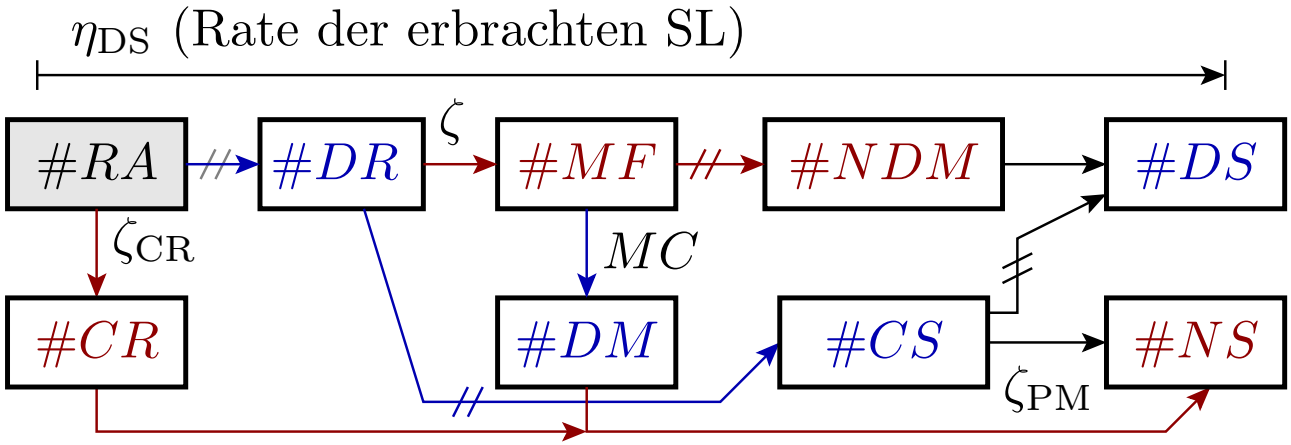
Anpassung Zählwertzuordnungsgraph



- Fehlfunktionen (MF) werden mit Häufigkeit MC erkannt (DM) und sonst nicht erkannt (NDM).
- Korrekte Service-Leistungen (CS) werden mit Häufigkeit ζ_{PM} wie Fehlfunktionen behandelt.
- Ohne Tolerierung werden Abstürze (CR), erkannte Fehlfunktionen (DM) und Phantom-MF nicht erbrachte Leistung (NS).
- Opt. Tolerierungsversuche durch erneute Anforderung (RR).

$\zeta_{\mathrm{CR}}, \zeta$	Absturzrate, Fehlfunktionsrate.
MC, ζ_{PM}	Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.

Erbringungsrate ohne Neuanforderung



$$\eta_{\mathrm{DS}} = \left.\frac{\#DS}{\#RA}\right|_{\mathrm{ACR}} = (1-\zeta_{\mathrm{CR}}) \cdot (\zeta \cdot (1-MC) + (1-\zeta) \cdot (1-\zeta_{\mathrm{PM}}))$$

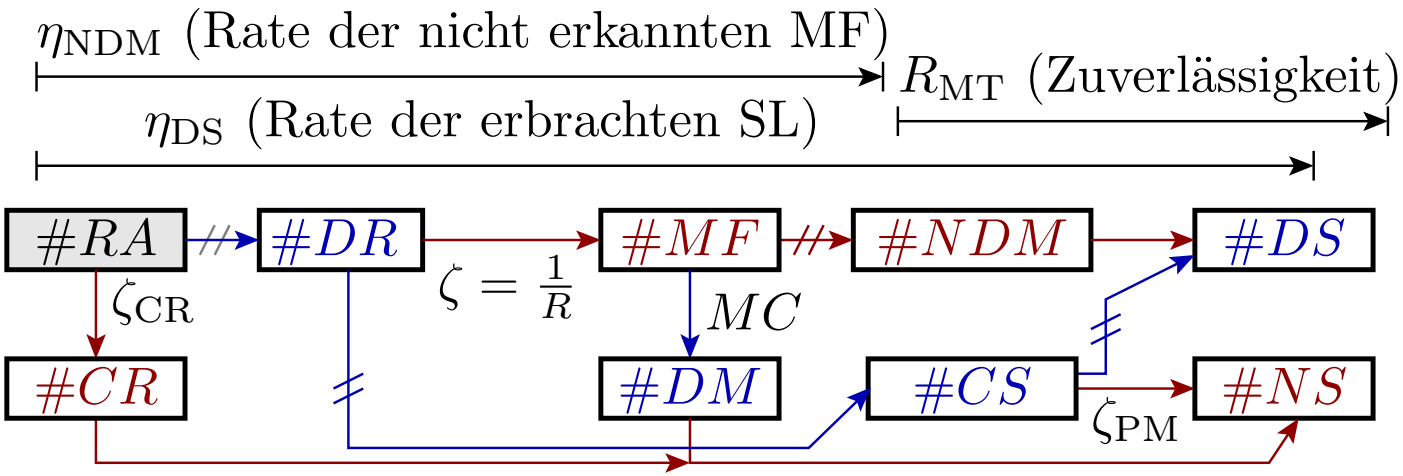
$$\eta_{\mathrm{DS}} = (1-\zeta_{\mathrm{CR}}) \cdot (1-\zeta_{\mathrm{SMF}}) \quad \text{mit } \zeta_{\mathrm{SMF}} = \zeta_{\mathrm{PM}} + \zeta \cdot MC - \zeta \cdot \zeta_{\mathrm{PM}} \tag{1.28}$$

Für Erbringungsrate nahe eins $\eta_{\mathrm{DS}} \to 1$:

$$\eta_{\mathrm{DS}} = 1 - \zeta_{\mathrm{CR}} - \zeta_{\mathrm{PM}} - \zeta \cdot MC \tag{1.29}$$

η_{DS}	Rate der erbrachen Service-Leistungen.
MC, ζ_{PM}	Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.
ζ_{CR}, ζ	Absturzrate, Fehlfunktionsrate.
ζ_{SMF}	Rate der signalisierten Fehlfunktionen.

Zuverlässigkeit ohne Neuanforderung



$$\eta_{\mathrm{NDM}} = \frac{\#NDM}{\#RA}\Big|_{\mathrm{ACR}} = (1-\zeta_{\mathrm{CR}}) \cdot \zeta \cdot (1-MC) \tag{1.30}$$

$$R_{\mathrm{MT}} = \frac{\#DS}{\#NDM}\Big|_{\mathrm{ACR}} = \frac{\eta_{\mathrm{DS}}}{\eta_{\mathrm{NDM}}} = \frac{\cancel{(1-\zeta_{\mathrm{CR}})} \cdot (1-\zeta_{\mathrm{SMF}})}{\cancel{(1-\zeta_{\mathrm{CR}})} \cdot \zeta \cdot (1-MC)}$$

$$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R \tag{1.31}$$

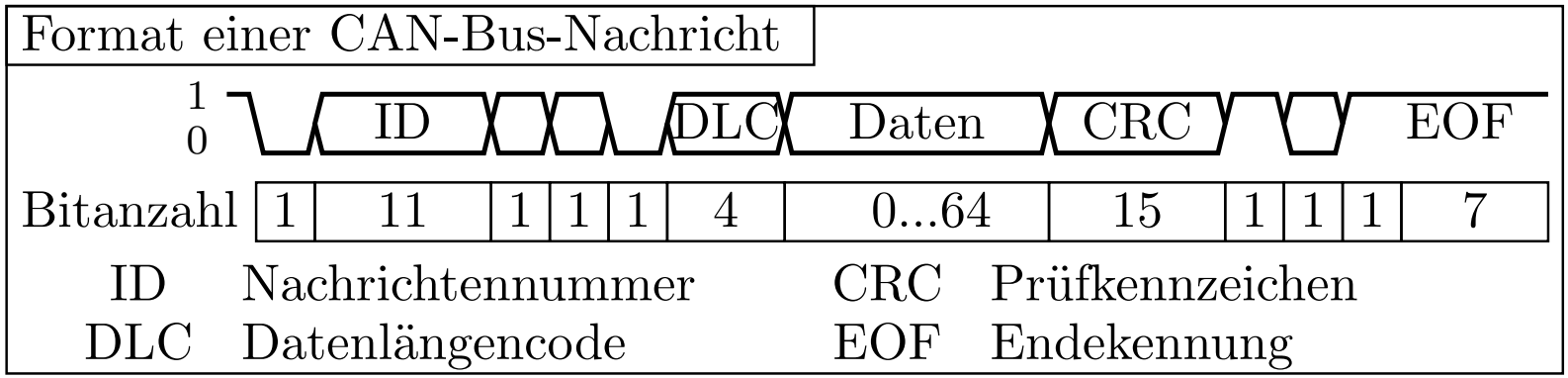
Für geringe Rate signalisierter Fehlfunktionen $\zeta_{\mathrm{SMF}} \to 0$:

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

η_{NDM} Rate der nicht erkannten Fehlfunktionen.
$R_{[\mathrm{MT}]}$ Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.

Formatkontrollen

Format- und Wertekontrollen



Eine Service-Leistungen umfasst Daten eingebettet in ein Format:

- Format: werteunabhängige Merkmale: Zeitschranken, WB, ...
- Daten: Werte, die mit dem Datenobjekt dargestellt werden.

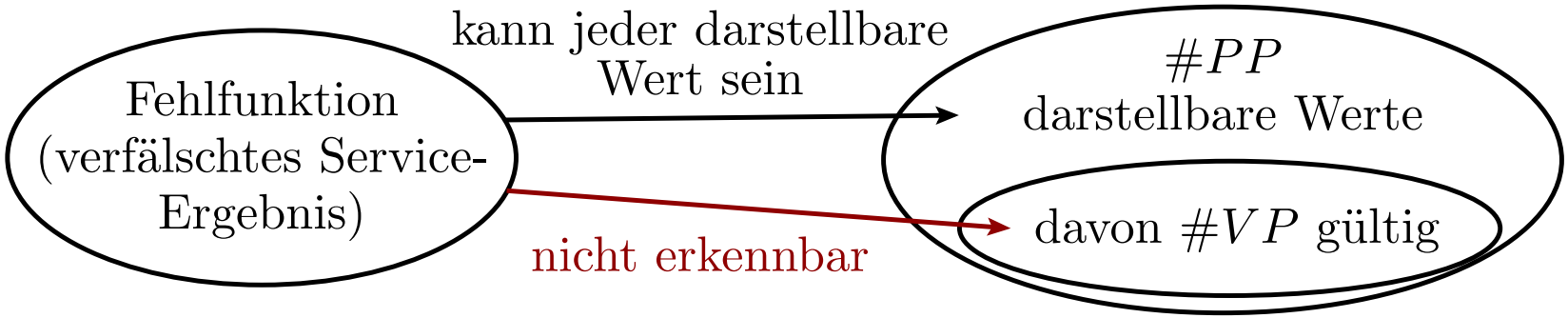
Einteilung Überwachungsverfahren für digitale Service-Leistungen:

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 zu realisieren und erzielen oft höhere MC und kleinere Phantom-MF-Raten als Wertekontrollen.

Informationsredundanz

Formatkontrollen (Fehler erkennende Codes, Prüfkennzeichen, Wertebereichskontrollen, ...) nutzen oft die Informationsredundanz.



Die Fehlfunktionsabdeckung ist tendenziell um so höher, je geringer der Anteil der zulässigen Bitmuster ist. Wenn alle Verfälschungsmöglichkeiten gleichhäufig auftreten, alle unzulässige Muster als unzulässig und alle zulässigen Werte als zulässig erkannt werden:

$$MC = 1 - \frac{\#VP}{\#PP} \tag{1.33}$$

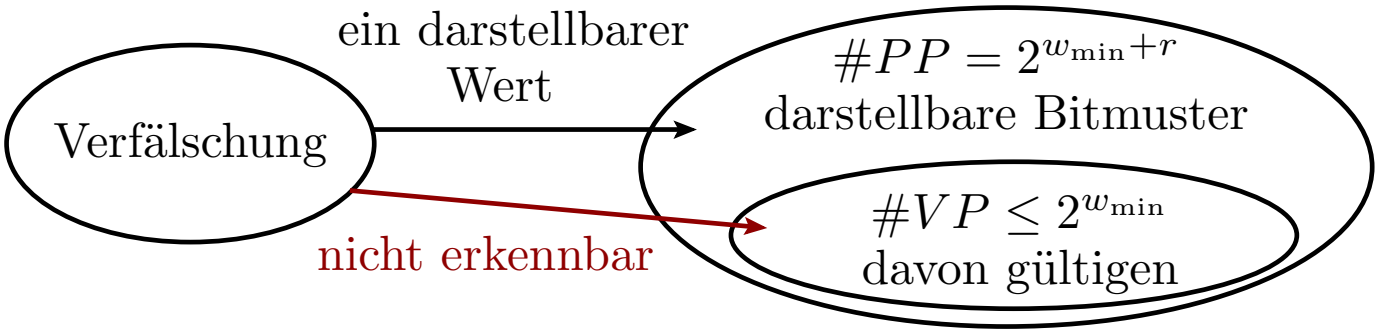
$$\zeta_{\mathrm{PM}} = 0 \tag{1.34}$$

$\#VP$	Anzahl der gültigen Bitmuster (Number of valid bit patterns).
$\#PP$	Anzahl der darstellbaren Bitmuster (Number of presentable bit patterns).
ζ_{PM}	Phantom-Fehlfunktionsrate.

Redundante Bits

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

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



$$MC = 1 - \frac{\#VP}{\#PP} \geq 1 - \frac{2^{w_{\min}}}{2^{w_{\min}+r}}$$

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

r	10	20	30
MC (mindestens)	99,9%	$1 - 10^{-6}$	$1 - 10^{-9}$

$\#VP, \#PP$ Anzahl der gültigen Bitmuster, Anzahl der darstellbaren Bitmuster.
MC, r Fehlfunktionsabdeckung, Anzahl der redundanten Bits.
$w_{\min}$ Erforderliche Bitanzahl zu Unterscheidung aller zuslässigen Werte.

Zuverlässigkeitsverbesserung

Zuverlässigkeitsverbesserung bei idealer Formatkontrolle ohne Neuanforderung

(1.31) $$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R$$

mit r redundanten Bits

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

und geringer Rate signalisierter Fehlfunktionen $\zeta_{\mathrm{SMF}} \to 0$:

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

Voraussetzung, keine bevorzugte Abbildung verfälscher Ergebnisse auf zulässige Werte.

$R_{[\mathrm{MT}]}$ Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
MC, r Fehlfunktionsabdeckung, Anzahl der redundanten Bits.

Ideale und reale Formatkontrollen

Das Idealverhalten *»gleichmäßige Abbildung der Verfälschungen auf mögliche Werte und Nachweis aller unzulässigen Werte«* gibt es nur näherungsweise bei der Übertragung und Speicherung mit fehlererkennenden Codes und Prüfkennzeichen (siehe Abschn. 5.2.2 *Informationsredundanz*).

Formatkontrollen ohne gleichmäßige Abbildung von Verfälschungen auf zulässige und unzulässige Werte, z.B. Kontrollen von

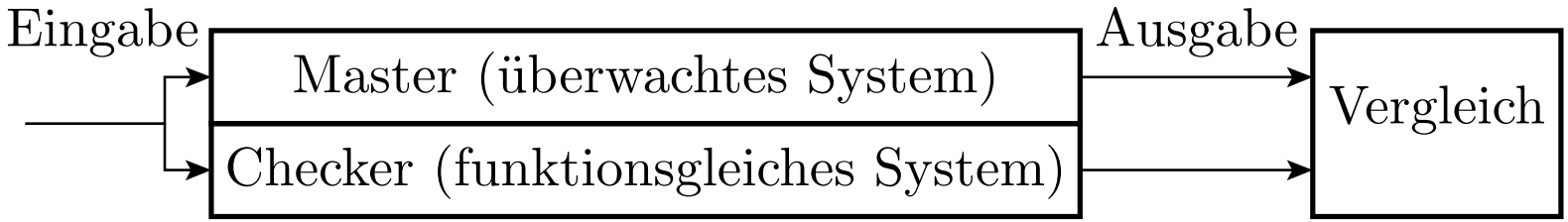
- Wertebereichen, Datentypen,
- Syntax, ...

haben in der Regel wesentlich geringere Fehlfunktionsabdeckung, aber dennoch ein sehr gutes Aufwand-Nutzen-Verhältnis.

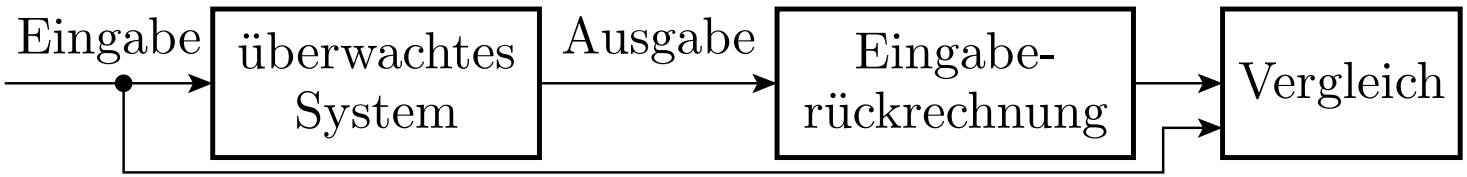
Wertekontrollen

Kontrollverfahren für Werte

- Master-Checker-Prinzip (Verdopplung und Vergleich). Nutzbar für alle deterministischen Berechnungen.

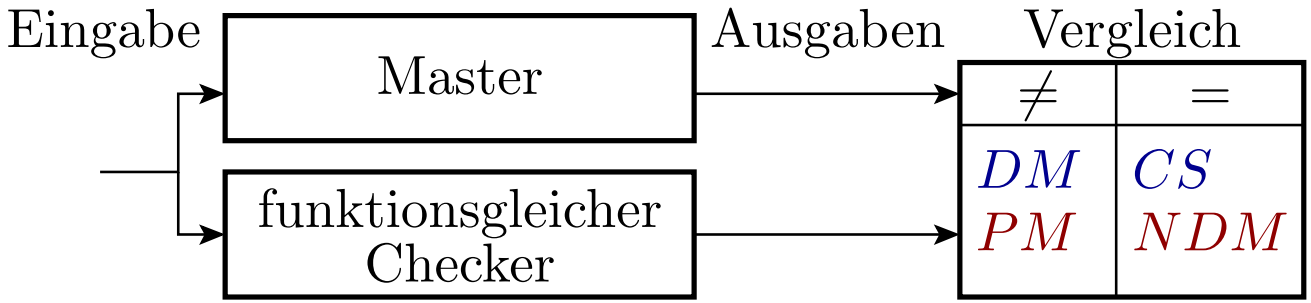


- Loop-Test (Eingaberückberechnung und Vergleich), z.B. Überwachung Versenden durch Empfang und Vergleich der empfangenen mit den Sendedaten. Nur für umkehrbar eindeutige Funktionen.



- Aufgabenspezifische Korrektheitskontrolle, z.B. für Suche Weg von A nach B durch einen Graphen ist die Kontrolle, dass der gefundene Weg von A nach B führt. Für die wenigsten Aufgaben nutzbar.

Eigenschaften von Master-Checker-Systemen



Die Fehlerüberdeckung ist die Diversitätsrate (Rate der Verschiedenartigkeit, siehe nächste Folie):

$$MC = \frac{\#DM}{\#MF}\Big|_{\mathrm{ACR}} = \eta_{\mathrm{Div}} \tag{1.37}$$

und die Phantom-Fehlfunktionsrate ist die Rate der diversitären Checker-Fehlfunktionen (Checker-MF ohne gleichzeitige Master-MF):

$$\zeta_{\mathrm{PM}} = \eta_{\mathrm{Div}} \cdot \zeta_{\mathrm{Chk}} \tag{1.38}$$

DM, PM	Erkannte Fehlfunktion, Phantomfehlfunktion.
CS, NDM	Korrekte Service-Leistung, nicht erkannte Fehlfunktion.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
ζ_{Chk}	Fehlfunktionsrate des Checkers.

Diversität im IT-Bereich

Diversität beschreibt bei IT-Systemen die Verschiedenartigkeit der Wirkung von Problemen bei mehrfacher Bearbeitung derselben Aufgabe. Praktisch gilt immer:

- Probleme (Fehlfunktionen, Abstürze) sind sehr selten und
- es gibt sehr viele Verfälschungsmöglichkeiten durch MF.

Gleichzeitige Probleme und übereinstimmende Fehlfunktionen durch Zufall praktisch ausgeschlossen, d.h. nur mit gemeinsamer Ursache:

- falsche Eingaben, gleiche Fehler,
- Ausfall gemeinsam genutzter Hardware, ...
- übereinstimmende Fehlerentstehungsursachen, ...

Diversitätsrate η_{Div}: Anteil der Probleme mit unterschiedlicher oder unterschiedlich wirkender Ursache, Praktisch gleich der

- Fehlfunktionsabdeckung Mehrfachberechnung und Vergleich,
- Korrekturerfolgsrate Neuberechnung nach erkannten Fehlfunktionen und Abstürzen.

Natürliche Diversität

Mehrfachberechnung und Vergleich mit derselbe Hard- und Software erkennt im Wesentlich nur Fehlfunktionen durch Störungen plus Abbruch ohne Ergebnis oder Neuberechnung

- erhöht die störungsbezogene Teilzuverlässigkeiten R_{D},
- aber kaum die fehlerbezogene Teilzuverlässigkeit R_{F}.

R_{F}	Fehlerbezogene Teilzuverlässigkeit (Fault-related partial reliability).
R_{D}	Störungsbezogene Teilzuverlässigkeit (Disturbance-related partial reliability).

Erweiterte Diversität

Konstruktive und organisatorische Maßnahmen zur Erhöhung der Diversität durch Vermeidung gemeinsamer MF-Ursachen:

Erweiterte Diversität	konstr. und org. Maßnahmen	Minderung der Teilzuverlässigkeit in Bezug auf
HW-Diversität	Ausführung auf verschiedener HW	Fertigungsfehler, Ausfälle
HW-Entwurfsdiversität	unabhängig entworfene HW	zusätzlich HW-Entwurfsfehler
Syntaktische Diversität	unterschiedlich übersetzte SW	SW-Übersetzungsfehler
Software-Diversität	unabhängig entworfene SW	zusätzlich SW-Entwurfsfehler
diversitäre Nutzung (Fehlerumgehung)	Wiederholung mit geänderter SR*	zusätzlich, Eingabefehler

* Bei abweichenden Sollwerte ungeeignet für Mehrfachberechnung und Vergleich.

Diversitäre Zweitrechnung und Fehlerumgehung

Komplexe IT-Systeme bieten oft viele Lösungswege für eine Aufgabe, die nicht alle funktionieren. Für zwei Aspekte von großer Bedeutung

Diversitäre Zweitrechungen über alternative Lösungswege mindern das Risiko, dass gemeinsame Ursachen identische und damit nicht erkennbare Verfälschungen verursachen. Allerdings liefern abweichende Lösungswege oft abweichende richtige Ergebnisse, die bei Verdopplung und Vergleich zu Phantom-Fehlfunktionen werden.

Fehlerumgehung / Nutzerlernprozesse: 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.

Diversität von Software-Versionen

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

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

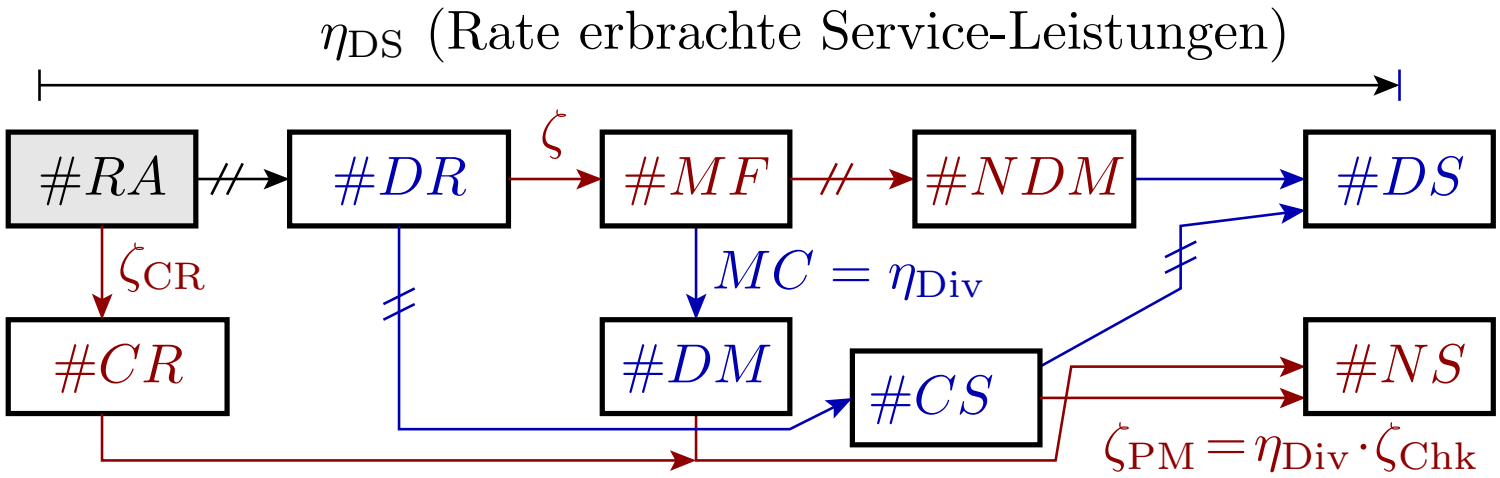
Die ursprüngliche euphorische Meinung, dass so Diversität gegenüber allen Fehlern, außer denen in der Spezifikation erzielbar ist, nicht bestätigt. Die direkte oder indirekte Kommunikation der Entwicklungsteams über die Interpretation der Spezifikation, während des Test etc. trägt Gemeinsamkeiten in die Entwürfe. Neigung von Menschen, gewisse Fehler zu wiederholen*, ... $\eta_{\mathrm{Div}} \leq 90\%$, nach Gl. 1.37:

$$MC = \eta_{\mathrm{Div}} \leq 90\%$$

Eine Kontrolle mit $r = 10$ Bit Informationsredundanz erreicht nach Gl. 1.35 $MC \geq 99{,}9\%$ fast ohne Zusatzaufwand und ohne PM.

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

Erbringungsrate von Master-Checker-Systemen



Erbringungsrate ohne Neuanforderung allgemein:

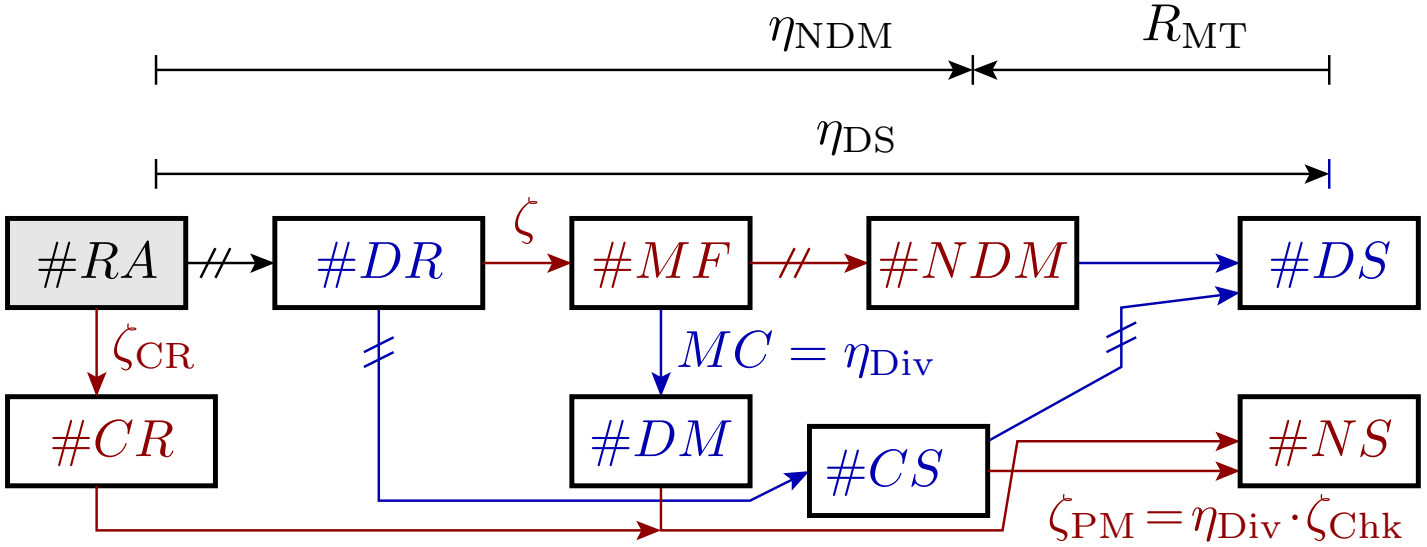
(1.28) $\eta_{\mathrm{DS}} = (1 - \zeta_{\mathrm{CR}}) \cdot (1 - \zeta_{\mathrm{SMF}})$ mit $\zeta_{\mathrm{SMF}} = \zeta_{\mathrm{PM}} + \zeta \cdot MC - \zeta \cdot \zeta_{\mathrm{PM}}$

mit $MC = \eta_{\mathrm{Div}}$, $\zeta_{\mathrm{PM}} = \eta_{\mathrm{Div}} \cdot \zeta_{\mathrm{Chk}}$ und $\zeta_{\mathrm{SMF}} \ll 1$:

$$\eta_{\mathrm{DS}} = (1 - \zeta_{\mathrm{CR}}) \cdot (1 - \zeta_{\mathrm{SMF}}) \text{ mit } \zeta_{\mathrm{SMF}} = \eta_{\mathrm{Div}} \cdot (\zeta + \zeta_{\mathrm{Chk}}) \qquad (1.39)$$

ζ, ζ_{Chk}	Fehlfunktionsrate Master und damit des Gesamtsystems, Fehlfuntionsrate Checker.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
ζ_{CR}	Absturzrate.
MC, ζ_{PM}	Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.
ζ_{SMF}	Rate der signalisierten Fehlfunktionen.

Zuverlässigkeit von Master-Checker-Systemen



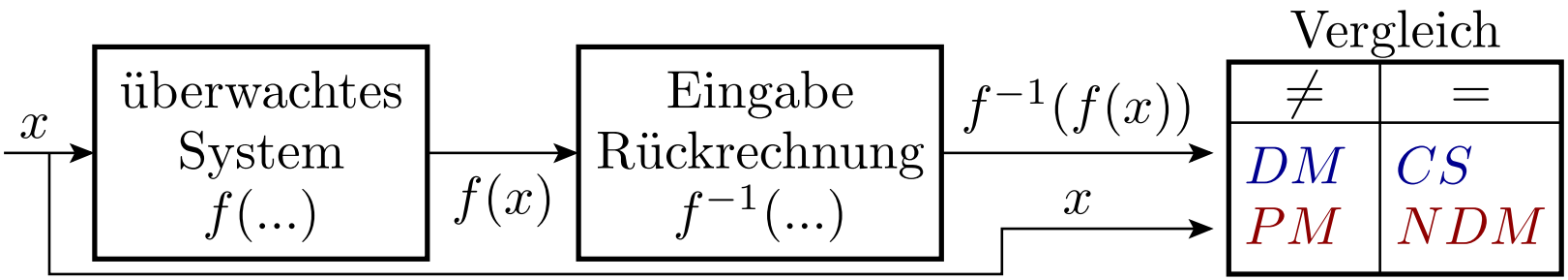
(1.31)
$$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R$$

mit $MC = \eta_{\mathrm{Div}}$ und $\zeta_{\mathrm{SMF}} = \eta_{\mathrm{Div}} \cdot (\zeta + \zeta_{\mathrm{Chk}})$:

$$R_{\mathrm{MT}} = \frac{(1-\eta_{\mathrm{Div}} \cdot (\zeta+\zeta_{\mathrm{Chk}}))}{(1-\eta_{\mathrm{Div}})} \cdot R \qquad (1.40)$$

$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
MC	Fehlfunktionsabdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.

Eigenschaften Loop-Test

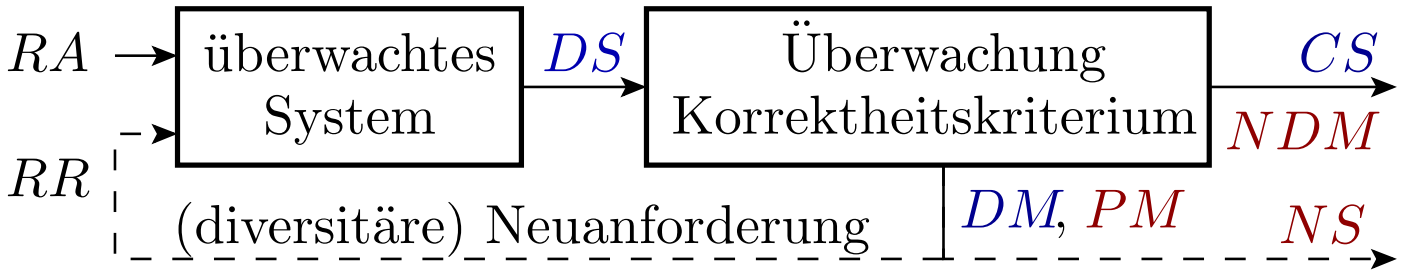


Da $f(\ldots)$ und $f^{-1}(\ldots)$ sich in Algorithmus und Fehlerwirkung unterscheiden, ist auch ohne zusätzliche konstruktive und organisatorische Maßnahmen ein höheres Maß an Verschiedenartigkeit der Wirkung von Fehlern und damit eine höhere MC zu erwarten.

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 Wurzelberechnung.

$f(\ldots)$	Funktion des zu überwachenden Systems.
$f^{-1}(\ldots)$	Inverse Funktion.
DM, PM	Erkannte Fehlfunktion, Phantomfehlfunktion.
CS, NDM	korrekte Service-Leistung, nicht erkannte Fehlfunktion.

Aufgabenspezifische Korrektheitskontrolle

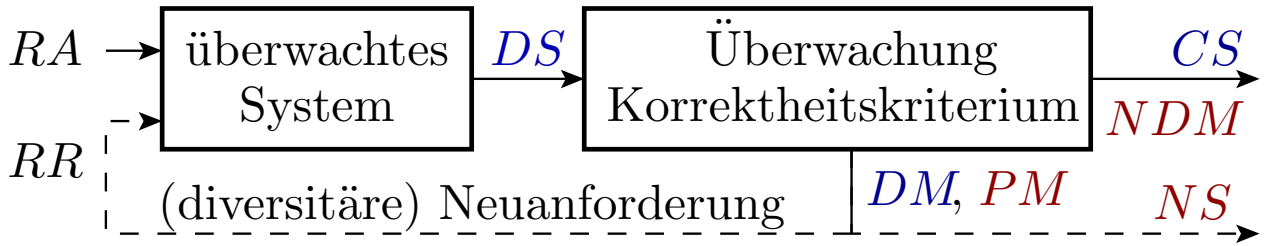


Wenn es eine aufgabenspezifische Kontrollmöglichkeit gibt, Korrektheit nachzuweisen:

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

Fehlfunktionsabdeckung MC gleich der Zuverlässigkeit der Kontrolle, oft sehr hoch, aber bei einer Lösungssuche mit vielen Fehlversuchen ...

RA, DS	Akzeptierte Anforderung, erbrachte Service-Leistung.
CS, NDM	korrekte Service-Leistung, nicht erkannte Fehlfunktion.
DM, PM	Erkannte Fehlfunktion, Phantomfehlfunktion.
NS, RR	Abbruch ohne Service-Leistung, Neuanforderung.



Achtung: Suchalgorithmen der Form:

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

benötigen im Mittel $\mu_{\mathrm{Trl}} \gg 1$ Versuche bis zum Erfolg. Zu erwartende Anzahl ist Kehrwert der Rate der als korrekt erkannten Ergebnisse:

$$\mu_{\mathrm{Trl}} = \frac{1}{1-\zeta_{\mathrm{SMF}}}$$

Eingesetzt in

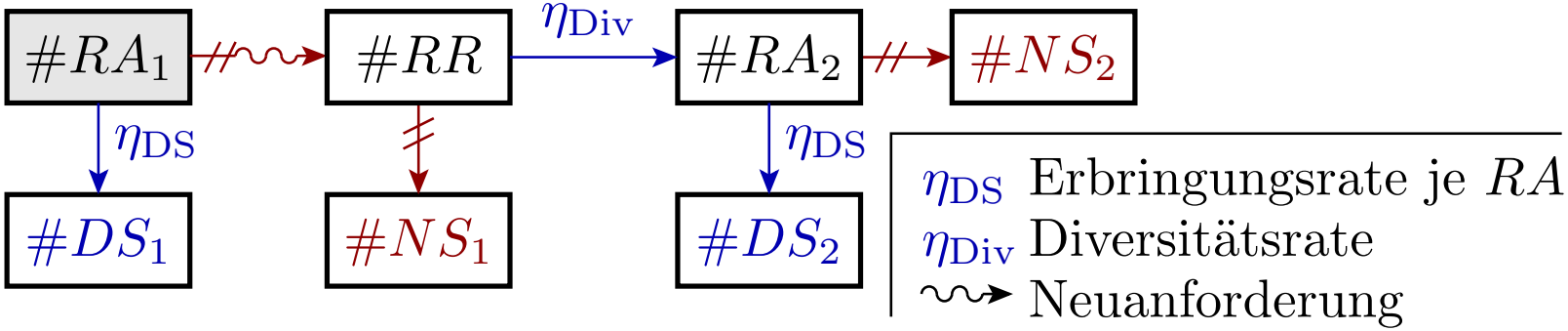
(1.31)
$$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R$$

nimmt die Zuverlässigkeit umgekehrt proportional mit μ_{Trl} ab (Gl. 1.43).

$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
ζ_{SMF}	Rate der signalisierten Fehlfunktionen.
ζ, MC	Fehlfunktionsrate, Fehlfunktionsabdeckung.
μ_{Trl}	Zu erwartende Anzahl der Versuche.

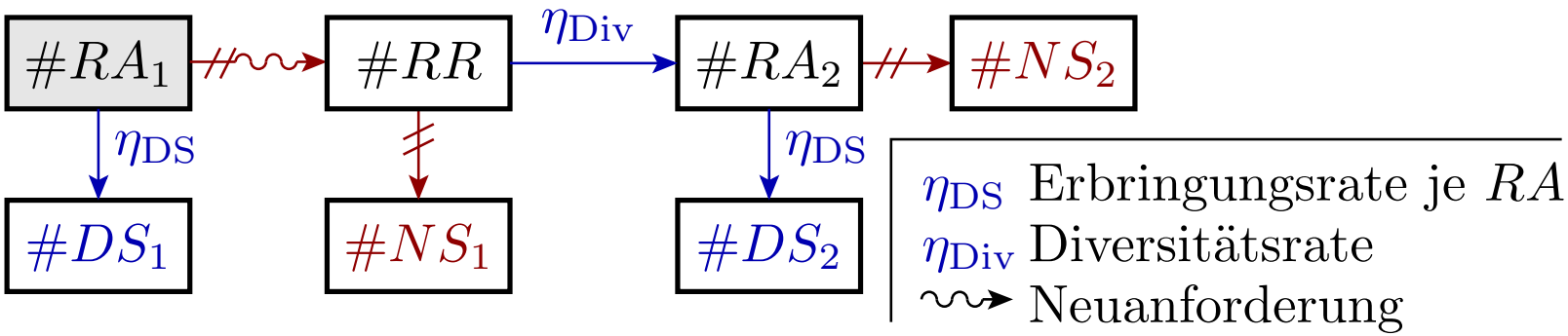
Neuanforderung

Erbringungsrate bei max. einer Neuanforderung



- Nach akzeptierter Erstanforderung (RA_1) Erbringung mit η_{DS} (DS_1), sonst Neuanforderung bis Anforderung akzeptiert (RR).
- Akzeptierte Neuanforderung mit Diversitätsrate η_{Div} abweichende Reaktion (RA_2), sonst Abbruch ohne Leistung (NS_1).
- Abweichende Reaktion mit η_{DS} erbrachtes Ergebnis (DS_2), sonst Abbruch ohne Leistung (NS_2).

RA_1, DS_1	Akzeptierte Erstanforderung, erbrachte Service-Leistung nach Erstanforderung.
RR, NS_1	Neuanforderung, Abbruch ohne Service-Leistung nach Erstanforderung.
RA_2, DS_2	Akzeptierte Neuanforderung, erbrachte Service-Leistung nach Neuanforderung.
NS_2	Abbruch ohne Service-Leistung nach Neuanforderung.



Eine Neuanforderung erhöht die Erbringungsrate auf:

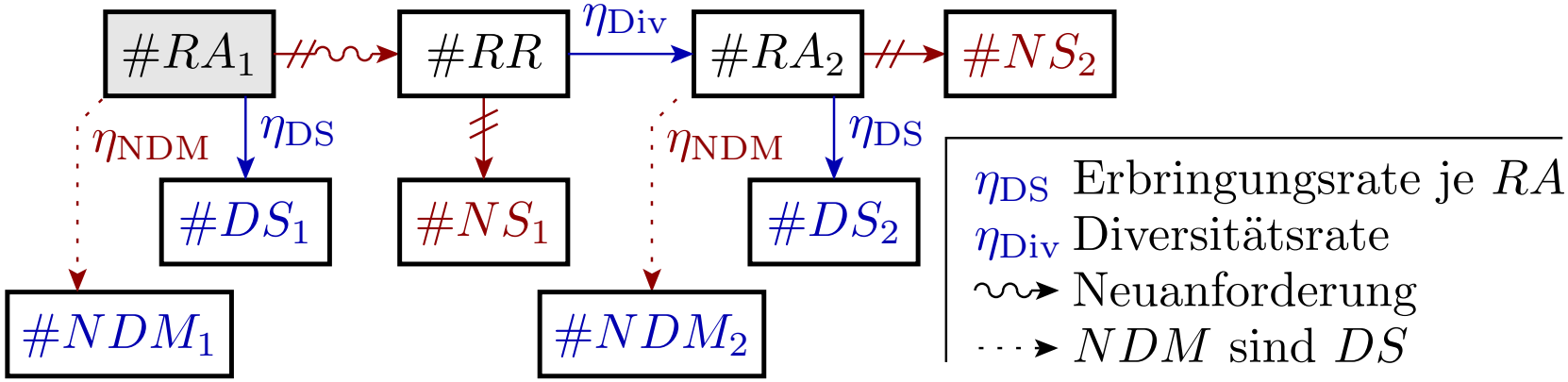
$$\eta_{\mathrm{DS.SR}} = \left.\frac{\#DS_1 + \#DS_2}{\#RA_1}\right|_{\mathrm{ACR}}$$

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

Für hohe Erbringungsraten $\eta_{\mathrm{DS}} \to 1$ praktisch keine Gewinn gegenüber »Abbruch nach Fehlfunktion«.

$\eta_{\mathrm{DS}}, \eta_{\mathrm{Div}}$ Erbringungsrate je Anforderung, Diversitätsrate.
$\eta_{\mathrm{DS.SR}}$ Erbringungsrate bei max. einer Wiederholung nach Nichterbringung.

Zuverlässigkeit bei max. einer Neuanforderung



Der Anteil der der nicht erkannten Fehlfunktionen erhöht sich um denselben Faktor wie die Erbringungsrate:

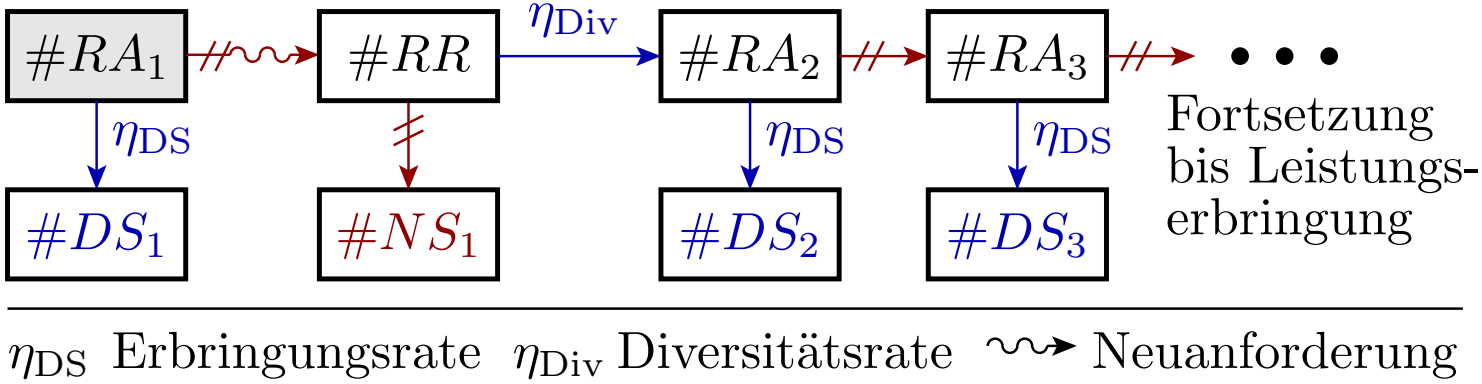
$$\eta_{\text{NDM.SR}} = \left.\frac{\#NDM+\#NDM_2}{\#RA_1}\right|_{\text{ACR}} = \eta_{\text{NDM}} + (1-\eta_{\text{DS}}) \cdot \eta_{\text{Div}} \cdot \eta_{\text{NDM}}$$

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

$$R_{\text{MT.SR}} = \left.\frac{\#DS_1+\#DS_2}{\#NDM_1+\#NDM_2}\right|_{\text{ACR}} = \frac{\eta_{\text{DS.SR}}}{\eta_{\text{NDM.SR}}} = \frac{\eta_{\text{DS}} \cdot \cancel{(1+(1-\eta_{\text{DS}}) \cdot \eta_{\text{Div}})}}{\eta_{\text{NDM}} \cdot \cancel{(1+(1-\eta_{\text{DS}}) \cdot \eta_{\text{Div}})}}$$

Max. eine Neuanforderung hat keinen Einfluss auf die Berechnung der Zuverlässigkeit.

Wiederholung bis Erbringung



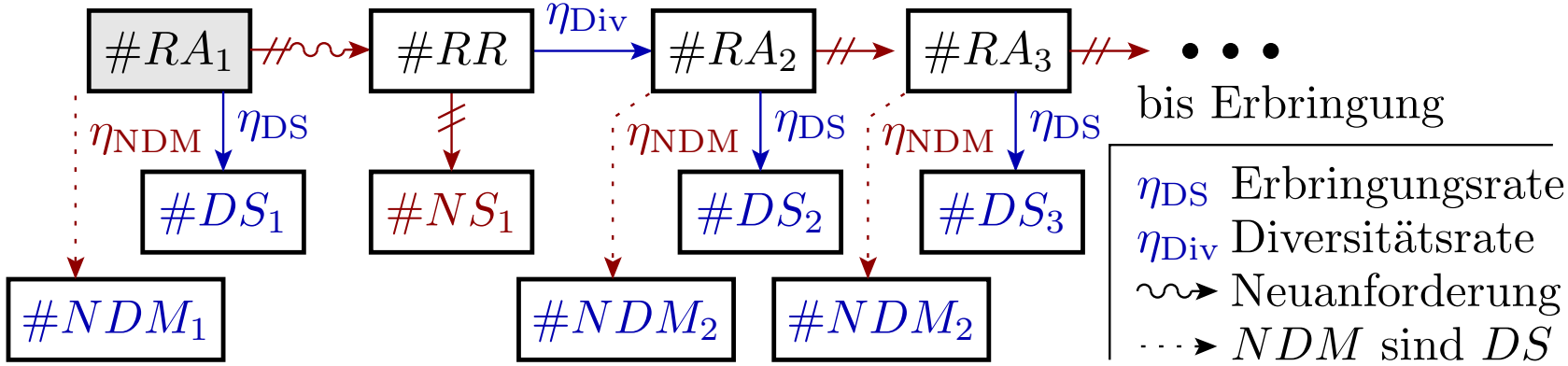
Annahme, dass bei Diversität dasselbe Problem praktisch nie ein zweites mal auftritt. Abbruch nur, wenn bei der ersten Neuanforderung genau dasselbe Problem auftritt (NS_1) oder Ergebnislieferung (DS_i). Erbringungsrate:

$$\eta_{\text{DS.MR}} = \left.\frac{\sum_{i=1}^{\infty} \#DS_i}{\#RA_1}\right|_{\text{ACR}} = 1 - \left.\frac{NS_1}{\#RA_1}\right|_{\text{ACR}}$$

$$\eta_{\text{DS.MR}} = 1 - (1 - \eta_{\text{DS}}) \cdot (1 - \eta_{\text{Div}}) \tag{1.42}$$

RA_i, DS_i	Akzeptierte Neuanforderung i, erbrachte Service-Leistung nach Neuanforderung i.
RR, NS_1	Neuanforderung, Abbruch ohne Service-Leistung nach Erstanforderung.
$\eta_{\text{DS.MR}}$	Erbringungsrate bei Wiederholung nach diverstären Problemen bis Erbringung.
η_{DS}, η_{Div}	Erbringungsrate je Anforderung, Diversitätsrate.

Zuverlässigkeit bei Wiederholung bis Erbringung



Auch bei Mehrfachwiederholung erhöht sich Anteil nicht erkennbarer Fehlfunktionen um denselben Faktor wie die Erbringungsrate:

$$R_{\mathrm{MT.MR}} = \left.\frac{\sum_{i=1}^{\infty} \#DS_i}{\sum_{i=1}^{\infty} \#NDM_i}\right|_{\mathrm{ACR}} = \frac{\eta_{\mathrm{NDM}}}{\eta_{\mathrm{DS}}}$$

Auch mehrfache Neuanforderung hat keinen Einfluss auf die Zuverlässigkeit.

NDM_i	Nicht erkannte Fehlfunktion nach Service-Anforderung i.
$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
RA_i, DS_i	Akzeptierte Neuanforderung i, erbrachte Service-Leistung nach Neuanforderung i.

Geringe Erbringungsrate je Versuch

Mehrfachwiederholung nur zweckmäßig für geringe Erbringungsrate je Versuch. Das impliziert eine große sichtbare Problemrate $\zeta_{\mathrm{SMF}} \gg 0$ in

(1.31) $$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R$$

Unter Vernachlässigung der »nutzlosen« Neuberechungsversuche«, um Common-Cause-Probleme zu erkennen, ist die sichtbare Problemrate die Gegenwahrscheinlichkeit des Kehrwerts der zu erwartenden Versuchsanzahl bis zur Erbringung:

$$\zeta_{\mathrm{SMF}} = 1 - \frac{1}{\mu_{\mathrm{Trl}}}$$

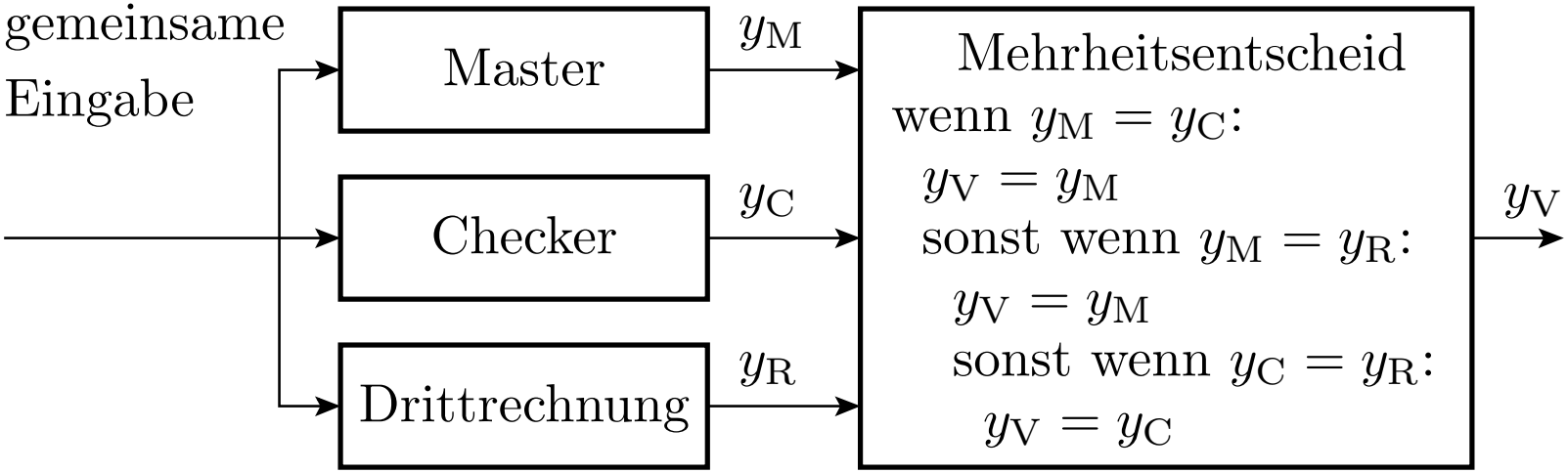
Abnahme der Zuverlässigkeit umgekehrt proportional mit μ_{Trl}:

$$R_{\mathrm{MT.MR}} = \frac{R}{\mu_{\mathrm{Trl}} \cdot (1-MC)} \tag{1.43}$$

R_{MT}	Zuverlässigkeit mit Wiederholung bei erkannten Problemen bis Beseitigung.
ζ_{SMF}	Rate der signalisierten Fehlfunktionen.
μ_{Trl}	Zu erwartende Anzahl der Versuche.

Mehrheitsentscheid

Dreifachberechnung und Mehrheitsentscheid



Bei Erbringung von mindestens zwei gleichen Ergebnissen, Ausgabe des übereinstimmenden Ergebnisses, sonst kein Ergebnis.

Die Drittrechnung wird nur bei abweichendem Master- und Checker-Ergebnis benötigt und muss auch erst dann erfolgen.

Drei Rechner mit Mehrheitsentscheid hatte John von Neumann vergeschlagen, allerdings zur Verbesserung der Hardware-Verfügbarkeit (siehe Folie Mehrheitseinscheid mit Notbetrieb, Abschn. 6.5.5).

Annahmen zur Vereinfachung:

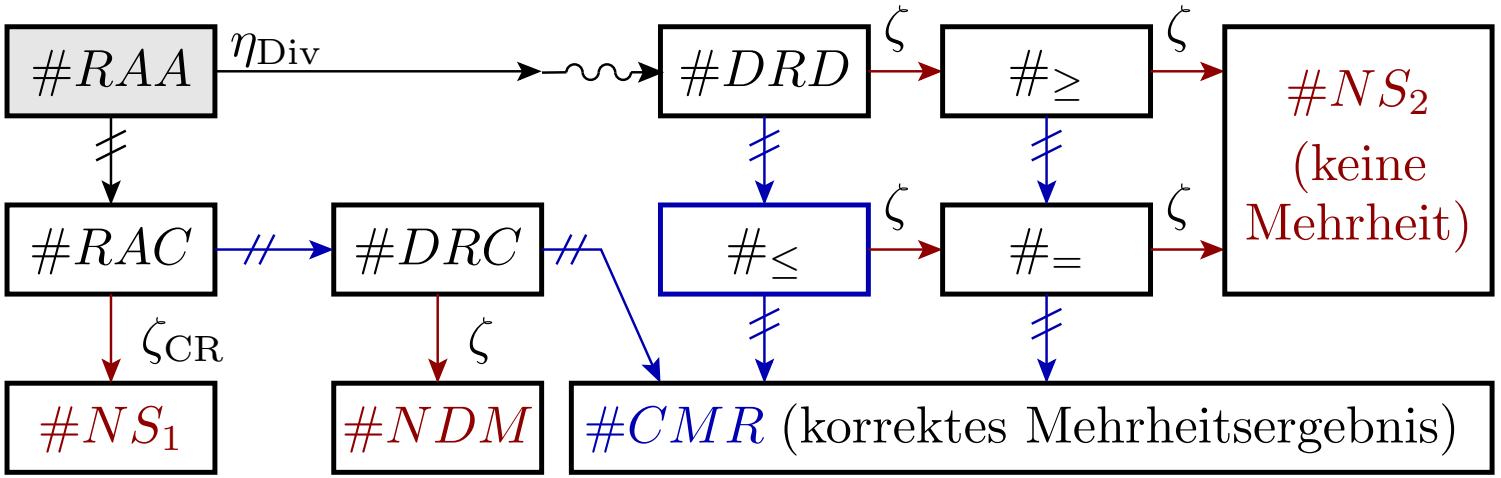
- Auftretende Probleme (Abstürze, Fehlfunktionen) haben mit Häufigkeit η_{Div} unabhängige Ursachen bzw. unterschiedliche Wirkung.
- Mit Häufigkeit $1 - \eta_{\mathrm{Div}}$ ist die Wirkung gleich, d.h. Abstürze sind nicht korrigierbar und MF nicht erkennbar.
- Abstürze ohne gemeinsame Ursache werden durch Neuberechnung bis zur Ergebniserbringung toleriert.
- Zufällige Übereinstimmung vin Ergebnissen so unwahrscheinlich, dass vernachlässigbar.

η_{Div} Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.

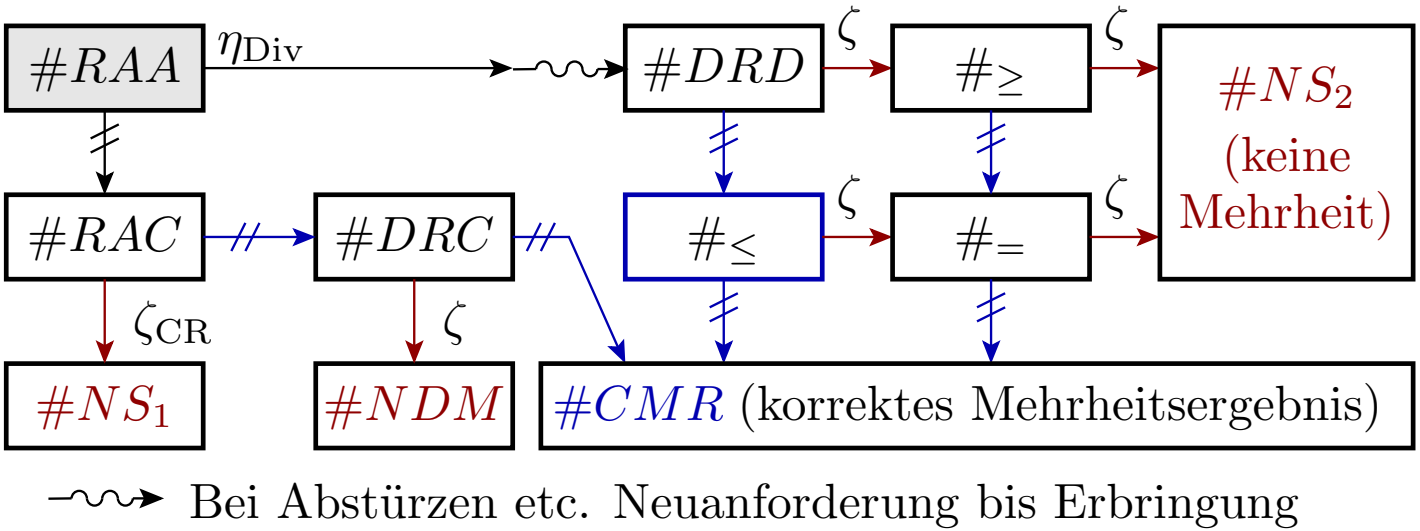
R DRD

Alle drei Ergebnis erbracht, mögliche Fehlfunktionen haben diversitäre Ursachen.

CVA-Graph

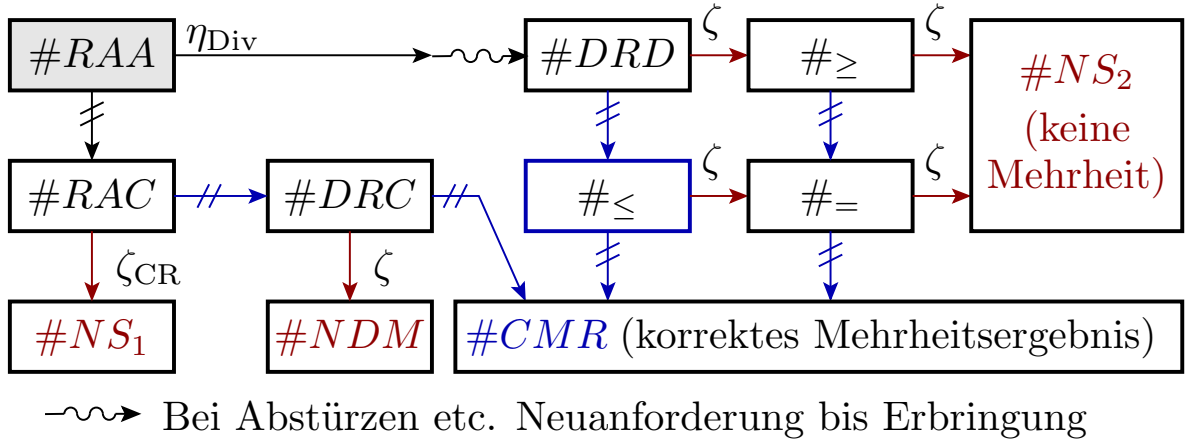


RAA	Alle drei Service-Anforderungen akzeptiert.
RAC	Alle drei Anforderungen akzeptiert, mögliche Probleme haben gemeinsame Ursache.
DRC	Alle drei Ergebnis erbracht, mögliche Fehlfunktionen haben gemeinsame Ursache.
DRD	Alle drei Ergebnis erbracht, mögliche Fehlfunktionen haben diversitäre Ursachen.
$\#_{\geq}$, $\#_{\leq}$, $\#_{=}$	Mindestens, maximal bzw. genau eine Fehlfunktion bei zwei Berechnungen.
NDM, NS	Nicht erkannte Fehlfunktion, keine Service-Leistung.
ζ_{CR}	Absturzrate.
ζ	Übereinstimmende Fehlfunktionsrate der Master-, Slave- und der dritte Berechnung.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.



- Ausgehend von »alle drei Anforderungen akzeptiert« (RAA) haben diese mit Rate η_{Div} nur diversitäre Probleme (RAD), sonst nur Common-Cause-Probleme (RAC).
- Probleme mit gemeinsamer Ursache haben dieselbe Wirkung auf alle drei Berechnungen, bei Absturz kein Ergebnis (NS_1), übereinstimmene Fehlfunktionen werden nicht erkannt (NDM).
- Für diversitäre Probleme »Wiederholung bis Erbringung« (DAD). Ab zwei korrekten Ergebnissen »korrektes Mehrheitsergebnis« (CMR), ab zwei Fehlfunktionen »kein Mehrheitsergebnis« (NS_2).

Erbringungsrate



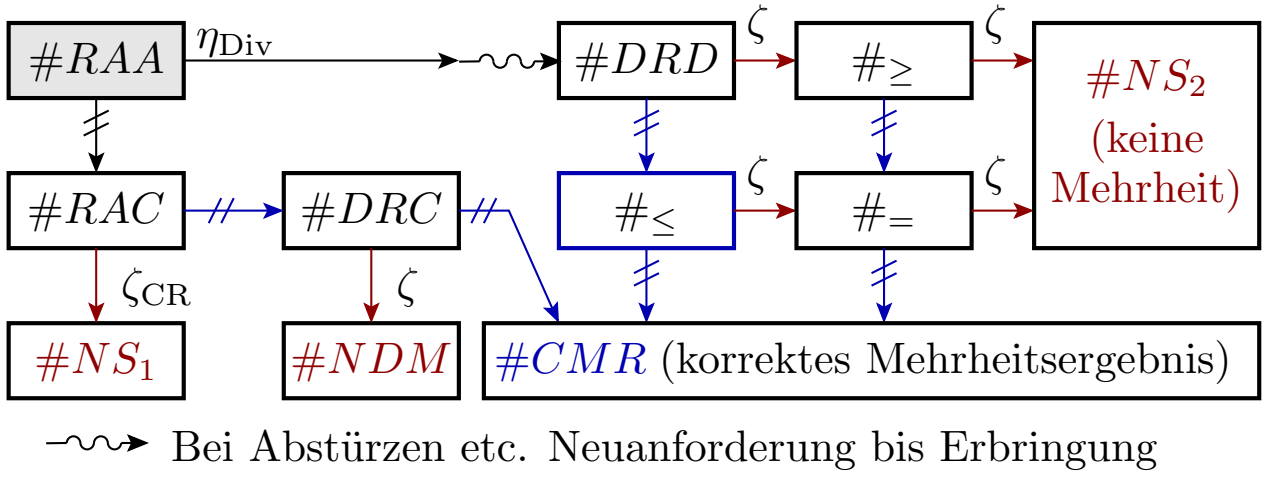
Übereinstimmende diversitäre Ergebnisse sind bei den in der Regel viele Bits umfassenden Ergebnissen praktisch unmöglich.
Nichterbrinung ab zwei diversitären Fehlfunktionen oder Absturz durch gemeinsame Ursache:

$$\eta_{\mathrm{DS}} = 1 - \eta_{\mathrm{Div}} \cdot \left(\zeta^2 + 2 \cdot (1-\zeta) \cdot \zeta^2\right) + (1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{CR}}$$

$$\eta_{\mathrm{DS}} = 1 - \eta_{\mathrm{Div}} \cdot \left(3 \cdot \zeta^2 - 2 \cdot \zeta^3\right) + (1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{CR}} \qquad (1.44)$$

η_{DS}	Rate der erbrachen Service-Leistungen.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
ζ_{CR}	Absturzrate.

Zuverlässigkeit



Nicht erkannt werden praktisch nur MF durch gemeinsame Ursachen:

$$\eta_{\text{NDM}} = (1 - \eta_{\text{Div}}) \cdot (1 - \zeta_{\text{CR}}) \cdot \zeta$$

Zuverlässigkeit:

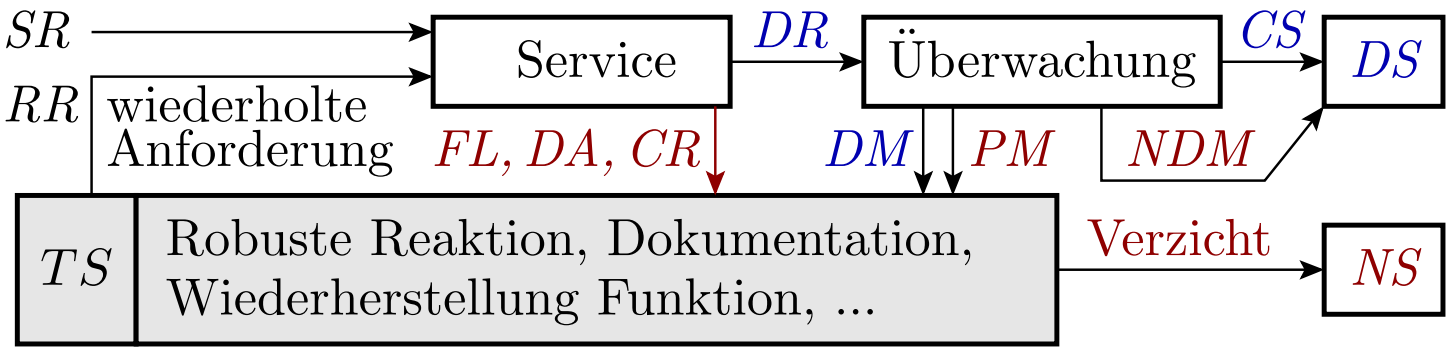
$$R_{\text{MV}} = \frac{\eta_{\text{DS}}}{\eta_{\text{NDM}}} = \frac{1-\eta_{\text{Div}} \cdot \left(3 \cdot \zeta^2 - 2 \cdot \zeta^3\right) + (1-\eta_{\text{Div}}) \cdot \zeta_{\text{CR}}}{(1-\eta_{\text{Div}}) \cdot (1-\zeta_{\text{CR}}) \cdot \zeta} \tag{1.45}$$

Bei hoher Erbringungs- und geringer Absturzrate: ($\eta_{\text{DS}} \to 1$, $\zeta_{\text{CR}} \to 0$)
Zuverlässigkeit wie Master-Checker ohne Wiederholung (Gl. 1.31):

$$R_{\text{MV}} = \frac{R}{(1-\eta_{\text{Div}})} \tag{1.46}$$

Reaktion ab Erkennung

Reaktion auf erkannte Probleme



Erkennbare Probleme während der Nutzung:

- Nichterbringung (NS): Hardware ausgefallen (FL), Service-Verweigerung (DA), Absturz (CR).
- Erkannte Fehlfunktion (DM).
- Phantomfehlfunktion (PM).

Reaktion ab Erkennung ...

SR, RR	Service-Anforderung, Wiederholanforderung.
DR, CS	Erbrachtes Ergebnis, korrekte Service-Leistung.
NDM, PM	Nicht erkannte Fehlfunktion, Phantomfehlfunktion.
DS, NS	Erbrachter Service, keine Service-Leistung.
FL, DA	Nichtverfügbarkeit wegen Hardware-Ausfall bzw. Annahmeverweigerung.
CR, TS	Absturz, Problembehandlung (Troubleshooting).

Robuste Reaktion zur Schadensvermeidung:
- Abbruch nach Zeitüberschreitung (Absturzprävention).
- Herstellen eines sicheren Zustands, ...

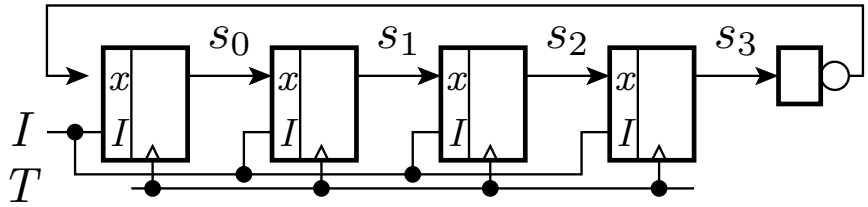
Dokumentation des erkannten Problems:
- Fehlermeldung für den manuellen Umgang,
- Sichern von Daten für die spätere Fehlersuche: Core-Dump, Cap-Datei (Windows), ... (siehe Abschn. 2.2.7 *Reifen von Produkten*)

Wiederherstellung Funktionsfähigkeit:
- Bei vermutetem Hardware-Ausfall Reparatur / Rekonfiguration,
- Auch ohne erkennbare Verfälschung interner Zustände in der Regel prophylaktische Neuinitialisierung.

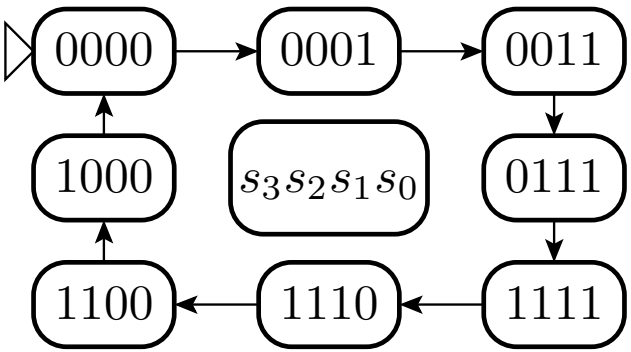
Abbruch mit Leistungsverzicht (NS) oder Neuanforderung (RR):
- Bei hinreichend seltenen Fehlfunktionen genügt Leistungsverzicht.
- Sonst für $\zeta \to 0$ genügt ein Wiederholversuch.
- Sonst* Wiederholung mit anderem System oder geänderter Anforderung (siehe Folie Erweiterte Diversität, Abschn. 1.2.3)

Erheblicher Anteil an der Funktionalität einer Software. Unterstützung durch Programmiersprache (siehe Abschn. 7.1.4).

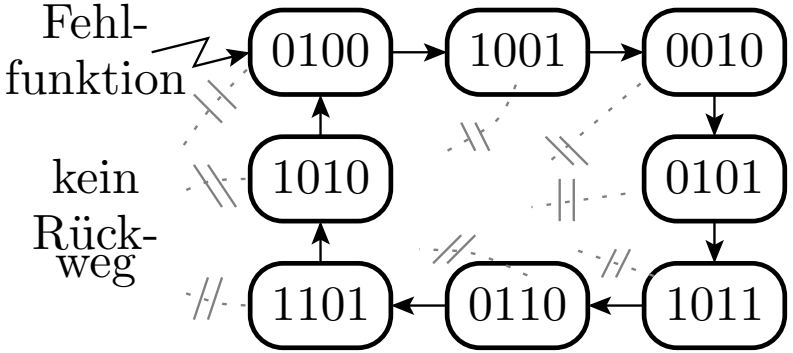
Absturz (Crash)



Soll-Funktion

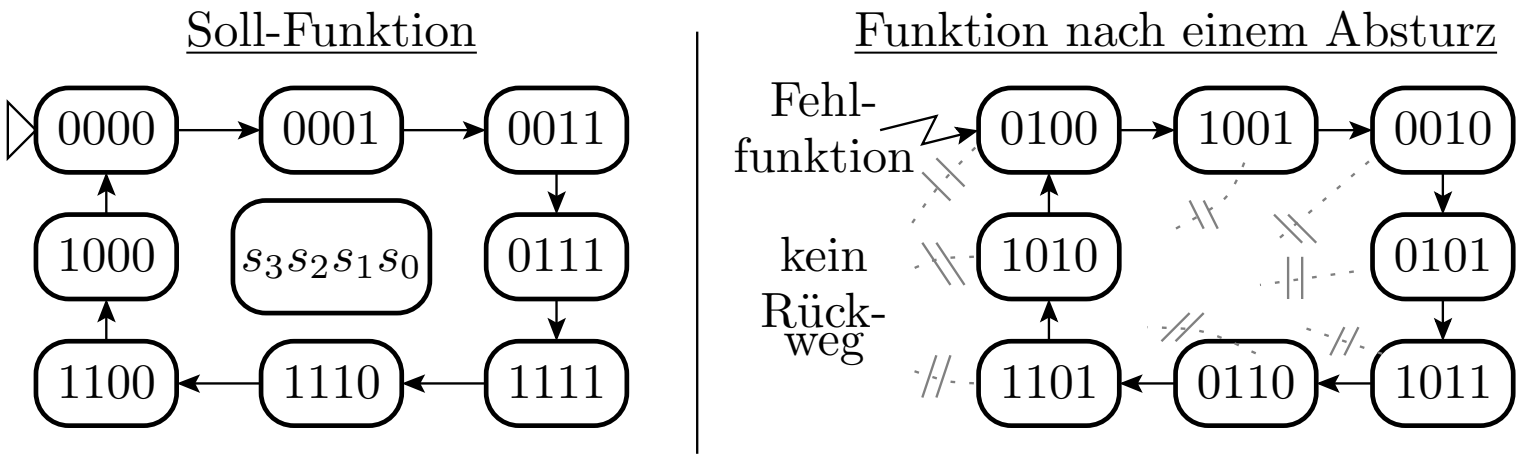


Funktion nach einem Absturz



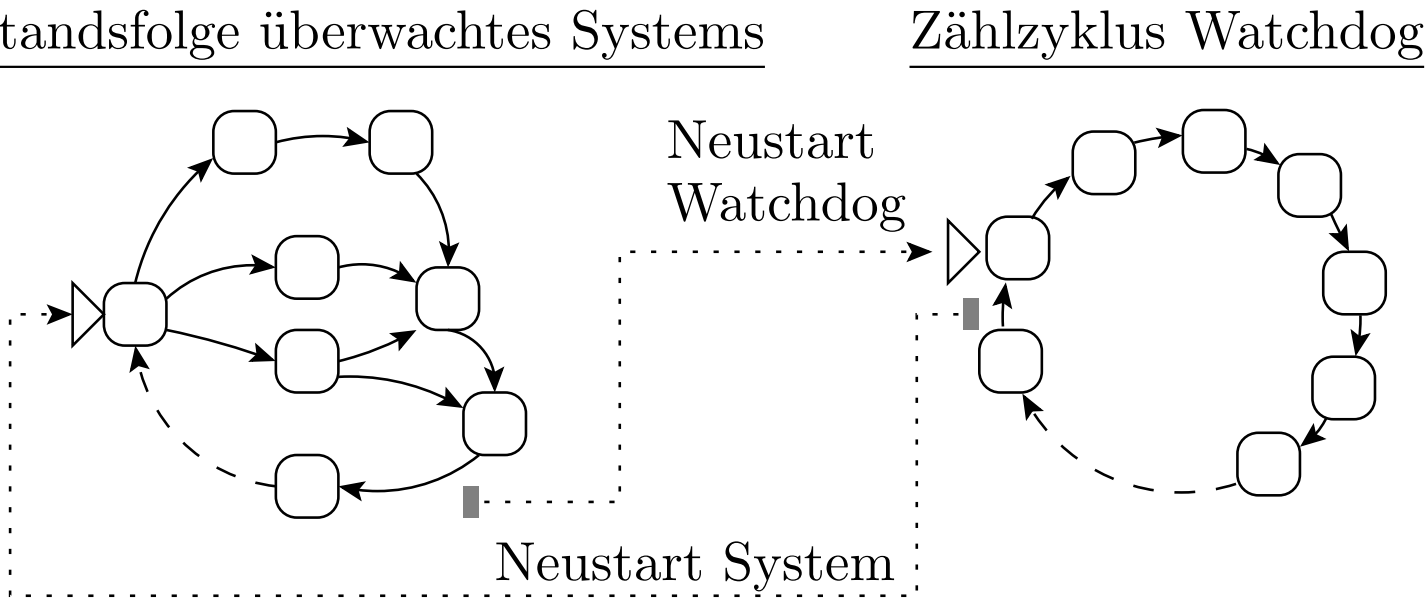
- Automaten und Programme nutzen nur einen kleinen Teil der $2^{\#SB}$ möglichen Zustände ($\#SB$ – Anzahl Zustandsbits).
- Der 4-Bit-Johnson-Zähler durchläuft zyklisch 8 der 16 Zustände.
- Die restlichen (redundanten) 8 Zustände bilden einen Zyklus, der nicht mehr verlassen wird.
- Der Übergang in unzulässige Zustände, die ohne Neuinitialisierung nicht verlassen werden, ist ein Absturz.

I, T, s_i Initialisierungssignal, Taktsignal, Zustandsbit i.



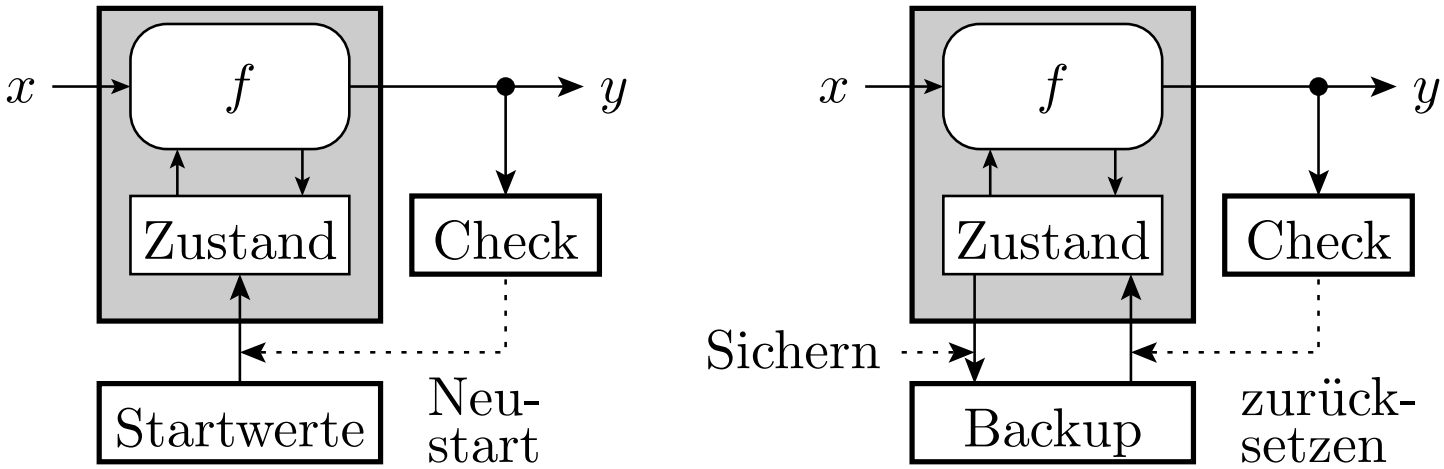
- Komplexer Hardware und Software hat Millionen von Zustandsbits und unüberschaubar viele Absturzmöglichkeiten.
- Ein Absturz (CR) ist daran zu erkennen, dass das System ab der letzten akzeptierte Service-Anforderung (SA) kein Ergebnis (DR) liefert und keine Anforderungen mehr akzeptiert.
- Der Umgang mit Abstürzen verlangt Zeitüberwachung.

Zeitüberwachung und Watchdog



Das überwachte System setzt in periodisch zu erreichenden Sollzuständen einen Zeitzähler zurück, der bei Überlauf das System neu startet und dabei auch wieder einen zulässigen Zustand herstellt (Zeitüberwachung auf Lebenszeichen).

Statische und dynamische Neuinitialisierung



Bei einer Fehlfunktion 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 während 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.

Spezielle Lösungen

Ergänzende Techniken zur Problembehandlung*

Problemvermeidung:

- Für vermiedene Probleme entfallen Überwachung, Reaktion, ...
- Variablen initialisieren, keine unsicheren Beschreibungsmittel,
- Anwendungs- und Arbeitsschutzrichtlinien, Sicherheitsvorkehrungen,
- Ruhestromprinzip, Trennung vom Internet, ...

Beseitigung und Vermeidung der Problemursachen

- Fehlerbeseitigung (siehe Abschn. 2.1).
- Fehlervermeidung (siehe Abschn. 2.3).
- Robustheit gegen Störungen, ...

Toleranz gegenüber Problemen in der Regel durch Redundanzen:

- Backup, fehlerkorrigierende Codes (Informationsredundanz).
- Hardware-Redundanz (Ausfalltoleranz) (siehe Abschn. 6.5.4).
- ...

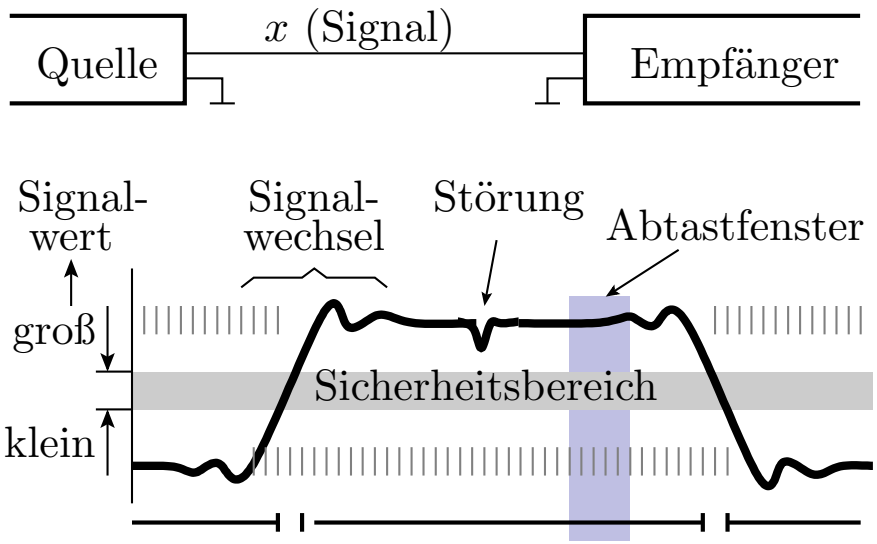
* Standarvorgehen für den Umgang mit potentiellen Problemen während des Betriebs ist Überwachung und Fehlfunktionsbehandlung.

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, ...

Robustheit gegen Störungen



Signalwert	
erweitert	binär
$x = 1$	$x = 1$
$x = \mathrm{X}$	nicht darstellbar
$x = 0$	$x = 0$

Gültigkeitsfenster

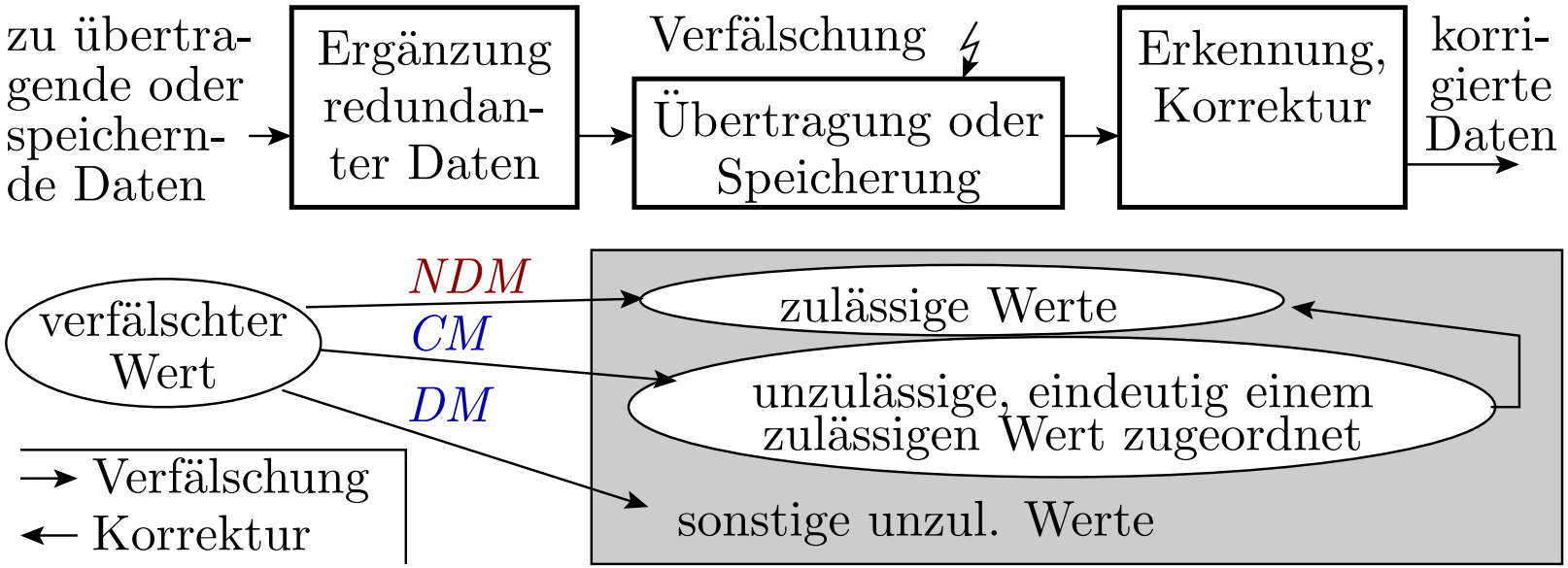
Informationsweitergabe durch Bits:

- Werteunterteilung in groß, klein und ungültig,
- Abtastung im Gültigkeitsfenster.

Robustheit gegen Störungen wird durch große Sicherheitsbereich im Verhältnis zur Größe zu erwartender Störsignale erzielt.

0, 1, X Logische Signalwerte für klein, groß und ungültig.

Fehlerkorrigierende Codes (Datenverlust)



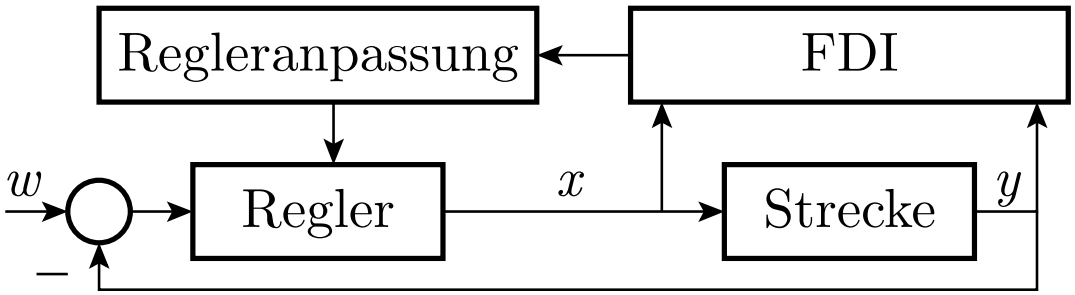
Korrektur verfälschter Daten nach Übertragung und Speicherung:

- Ergänzung zusätzlicher (redundanter) Bits vor der Übertragung oder Speicherung, mehr als für fehlererkennende Codes.
- Ersatz verfälschter korrigierbarer Werte durch korrekte Wert.

Praktische Umsetzung siehe später Abschn. 5.3.1.

CM, DM Korrigierbare Fehlfunktion, erkennbare Fehlfunktion.
NDM Nicht erkannte Fehlfunktion.

Fehlertolerantes Regelungssystem*



In einem Reglersystem wird vom Sollwert w der zu regelnde Ist-Wert y abgezogen. Aus der Differenz bildet der Regler den Stellwert x für die Regelstrecke (z.B. eine Heizung, wenn y eine Temperatur ist).

Hinzufügen einer Überwachungs- und Fehlerbehandlungsschicht (FDI) mit den Aufgaben:

- Überwachung von Regler und Regelstrecke auf unzulässige Werte und Zustände und
- Anpassung der Regelung an den aktuellen Fehlerzustand so, dass die Mindestfunktionalität gewährleistet bleibt.

* Beispiel für Problemtolerierung mit Zusatzeinheiten.
FDI Fehlerdetektion, -isolation und -identifikation.

Standby-Hardware

Hardware-Verfügbarkeit und mittlere Reparaturdauer:

(1.6) $$A_{\mathrm{H}} = \frac{\bar{t}_{\mathrm{FL}}}{\bar{t}_{\mathrm{FL}} + \bar{t}_{\mathrm{R}}}$$

A_{H}	PFD	zulässige mittlere Reparaturzeit $\bar{t}_{\mathrm{R}}$	
		pro Monat	pro Jahr
99%	1%	7,2 h	87,6 h
99,99%	0,01%	4,3 min	53 min

$A_{\mathrm{H}} \approx 99\%$ ist normal. Hohe Verfügbarkeiten ab 99,9% verlangen Zusatzmaßnahmen:

- Standby-Hardware: Komplettsystem, Sensoren, Aktoren, ... für eine schnelle Aufgabenübernahme (siehe Abschn. 6.5 *Ausfälle*).
- unterbrechungsfreie Stromversorgung, gespiegelte Server,
- RAID (**R**edundant **A**rray of **I**ndependent **D**isks, Abschn. 5.3.2),

$\bar{t}_{\mathrm{FL}}, \bar{t}_{\mathrm{R}}$	Mittlere Zeit bis zum nächsten Ausfall, mittlere Reparaturdauer.
A_{H}	Hardware-Verfügbarkeit.
PFD	Wahrscheinlichkeit der Nicht-Verfügbarkeit durch Hardware-Ausfälle.

Zusammenfassung

Problembehandlung im laufenden Betrieb

Iteration aus Überwachung und Reaktion auf erkannte Probleme während der Systemnutzung.

- Zeitüberwachung auf Abstürze,
- Format- [und Werte-] Kontrollen für erbrachte Ergebnisse,
- Bei erkannten Problemen
  - Herstellen eines sicheren (gefährdungsfreien) Zustands,
  - Problemdokumentation,
  - Neuinitialisierung (dynamisch, statisch),
  - bei vermutetem Hardware-Ausfall, Reparatur,
  - Leistungsverweigerung (NS) oder Wiederholversuch (RR).

Problembehandlung im laufenden Betrieb verbessert die Zuverlässigkeit und mindert über die Erbringungsrate die Verfügbarkeit.

Kenngrößen der Überwachung

Fehlfunktionsabdeckung:

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

Phantomfehlfunktionsrate:

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

Zuverlässigkeitsverbesserung (ohne und mit Wiederholung):

(1.31) $$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R$$

Bei geringer Rate signalisierter Fehlfunktionen:

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

Bei vielen zu erwartenden Berechnungsversuchen je Leistung:

(1.43) $$R_{\mathrm{MT.MR}} = \frac{R}{\mu_{\mathrm{Trl}} \cdot (1-MC)}$$

Mehrheitsentscheid (3 Versionen):

(1.46) $$R_{\mathrm{MV}} = \frac{R}{(1-\eta_{\mathrm{Div}})}$$

Erbringungsrate

Minderung der Erbringungsrate bei nur einem Erbringungsversuch:

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

Bei geringe, aber dennoch unakzeptabler Problemrate genügt eine Wiederholung:

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

Bei hoher diversitärer Problemrate hilft Wiederholung bis Erbringung:

(1.42) $$\eta_{\mathrm{DS.MR}} = 1 - (1 - \eta_{\mathrm{DS}}) \cdot (1 - \eta_{\mathrm{Div}})$$

Mehrheitsentscheid (3 Versionen):

(1.44) $$\eta_{\mathrm{DS}} = 1 - \eta_{\mathrm{Div}} \cdot \left(3 \cdot \zeta^2 - 2 \cdot \zeta^3\right) + (1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{CR}}$$

Diversität

- Natürliche Diversität insbesondere für für MF durch Störungen.
- Erweiterte Diversität: verschiedene Hardware, verschiedene Übersetzung, Mehrversions-Software-Entwürfe, ...
- Erzielbare Diversitätsraten mit zwei diversitären Entwürfen ausgehend von einer gemeinsamen Spezifikation $\eta_{\mathrm{Div}} \leq 90\%$.

Wiederholung beseitigt nur diversitäre Probleme.

Geringe Problemraten (Fehlfunktionen, Abstürze, Phantomfehlfunktionen) lassen sich deutlich einfacher erzielen als große Diversitätsraten.

Formatkontrolle

Ausnutzung der Informationsredundanz. Im Idealfall, gleichmäßige Abbildung von Fehlfunktionen auf zulässige und unzulässige Werte und Nachweis aller unzulässigen Formate:

- Fehlfunktionsabdeckung:

  (1.33) $$MC = 1 - \frac{\#VP}{\#PP}$$

- Mit r redundanten Bits:

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

- Phantomfehlfunktionsrate:

  (1.34) $$\zeta_{\mathrm{PM}} = 0$$

- Zuverlässigkeitsverbesserung:

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

Wertekontrolle

Master-Checker-Prinzip als universell einsetzbares Verfahren:

- Fehlfunktionsabdeckung:

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

- Phantomfehlfunktionsrate:

  (1.38) $$\zeta_{\mathrm{PM}} = \eta_{\mathrm{Div}} \cdot \zeta_{\mathrm{Chk}}$$

Loop-Test:

- Nur für umkehrbarer Funktionen geeignet.
- Höhere zu erwartende Fehlfunktionsabdeckung als bei Master-Slave-Systemen.

Aufgabenspezifische Korrektheitskontrollen:

- Für Aufgaben, die durch Kontrollkriterien definiert sind.
- Gute Kontrollgüte, aber bei Lösungssuche durch Probieren wie bei »Wiederholung bis Erfolg« umgekehrt proportionale Abnahme der Zuverlässigkeit mit der zu erwartenden Anzahl der Versuche μ_{Trl}.

Spezielle Lösungen

Außer »Überwachung und robuste Reaktion« gibt es etablierte Alternativen und Ergänzungen:

- Problemvermeidung und Ursachenbeseitigung.
- Ruhestromprinzip zur Vermeidung sicherkritischer Situation.
- Störungsunempfindliche Hardware.
- Fehlerkorrigierende Codes speziell für die Datenübertragung und Speicherung.
- Einprogrammierter Notbetrieb wie bei fehlertoleranten Regelern.
- Standby-Reserve für hohe Verfügbarkeit durch kurze Reparaturzeiten.