Test und Verlässlichkeit 1: Modellbildung Teil 1

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_F1.pdf)
16. September 2024

Inhalt Foliensatz TV_F1.pdf

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 Fehlfunktionen,
- 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

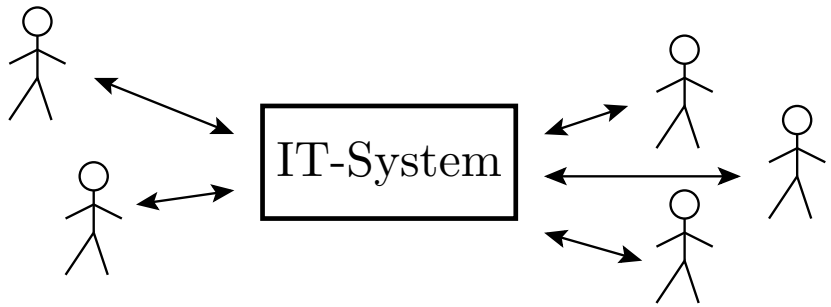
Prüfung

- 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.

Einführung

Vertrauen und Verlässlichkeit



IT-Systeme automatisierten intellektuelle Aufgaben:

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

Einsatzvoraussetzung ist Vertrauen, dass

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

Das Vertrauen in ein IT-System setzt Verlässlichkeit voraus.

Verlässlichkeit

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

Subjektive Einflussfaktoren auf die Wahrnehmung der Verlässlichkeit:

- Lebenserfahrungen insbesondere aus der Kindheit,
- Katastrophen oder 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

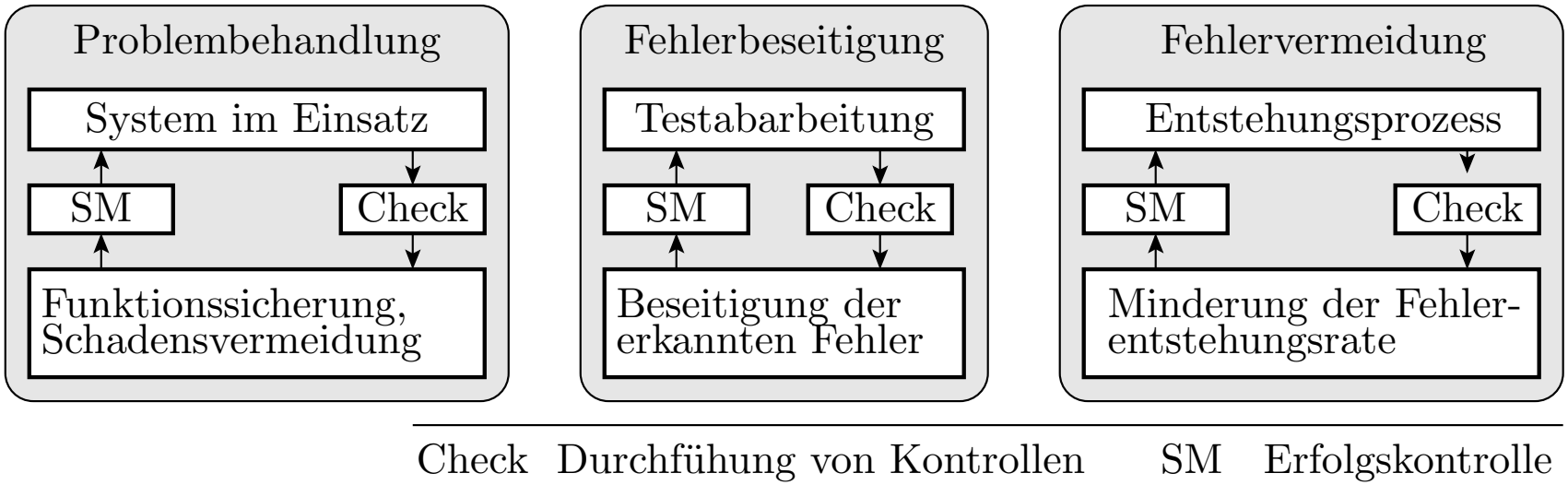
Verlässlichkeit wird durch Gefährdungen und Gefährdungsabwendungen beschrieben[Lapri81], und zwar auf drei Ebenen:

- Probleme während des Einsatzes:
  - Service-Verweigerung (no service, NS).
  - Fehlfunktionen (malfunction, MF),
- Ursachen der Probleme:
  - Fehler (Problemursachen),
  - Störungen (zufällig auftretende 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 auf allen drei Ebenen:

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

Verlässlichkeit ist selbst für IT-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

Folie 1.13: Der Preis fehlender Verlässlichkeit.

Wenn Verlässlichkeit teuer, warum kein Verzicht? – Schadenskosten:

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

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

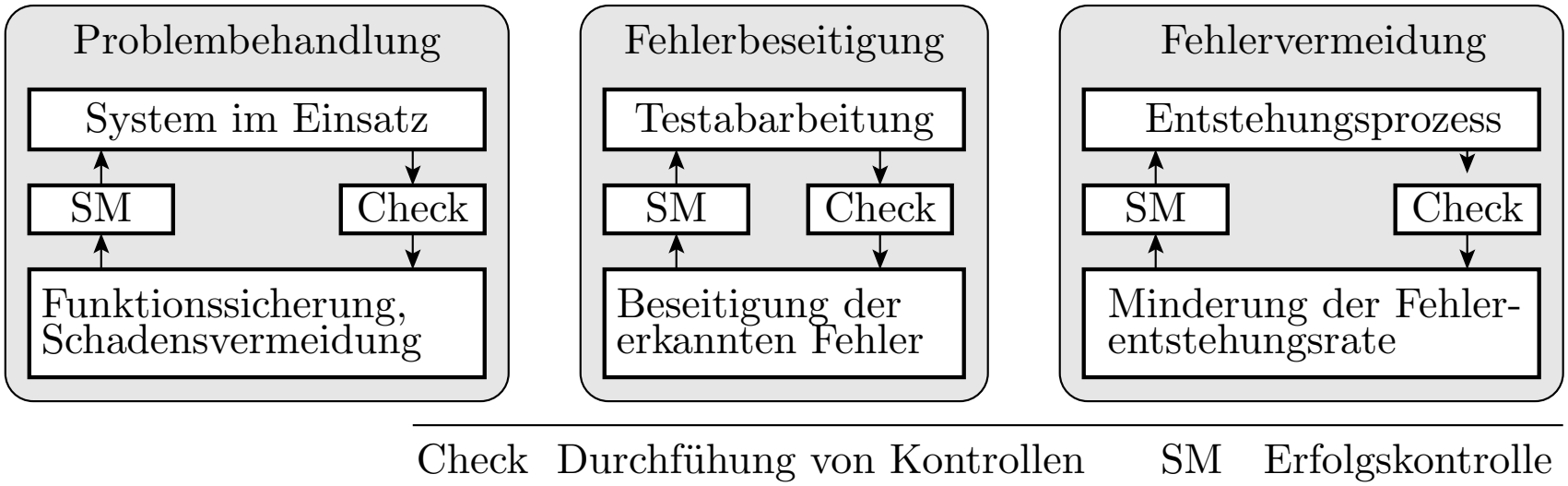
Ursache des beinahe atomaren Schlagabtauschs: defekter Schaltkreis.

Unzuverlässige IT-Systeme können nicht eingesetzt werden.

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

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

Warum heißt Vorlesung »Test & Verlässlichkeit«



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

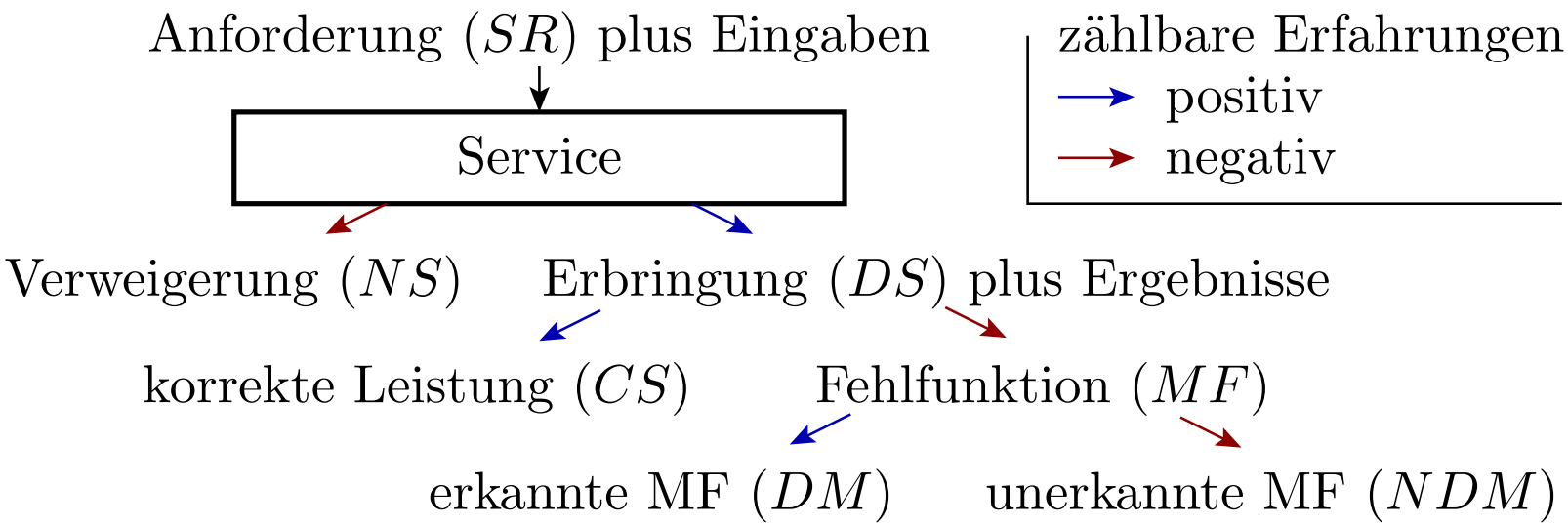
- Zählwerte für entstandene, vermiedene, ..., nicht erkannte MF,
- dasselbe für Fehler und deren Entstehungsursachen.

IT-Systeme sind entsprechend so zu modellieren, dass erbrachte und nicht erbrachte Leistungen, richtige und falsche Ergebnisse und auch alle anderen betrachteten potentiellen, entstandenen und vermiedenen Probleme zählbar sind.

Service-Modell

Service

System, das auf Anforderung aus Eingaben Ausgaben erzeugt.



Das Ergebnis auf eine Anforderung kann sein:

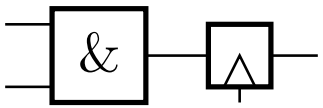
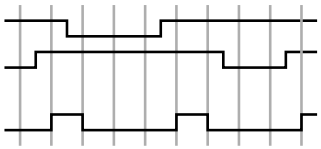
- Erbringung (DS, delivered service),
- Verweigerung (NS, no service).

Erbrachte Leistungen können sein

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

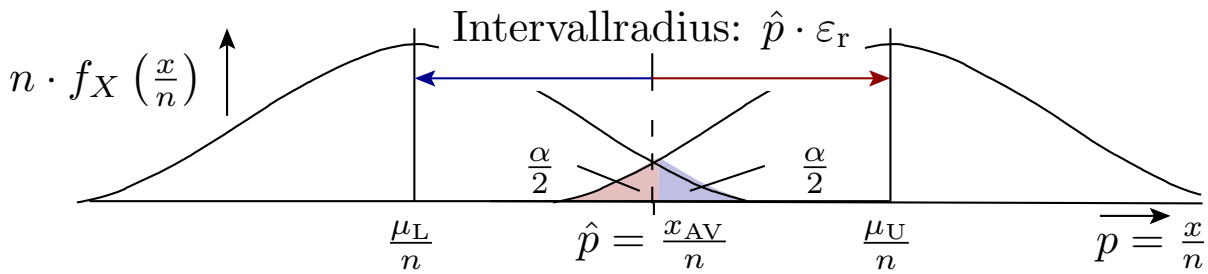
Anwendungsbereiche des Service-Modells

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:

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

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.

Abschn. 1.2.2: Verfügbarkeit.

Problembehandlung

Wenn kein verwertbare Service-Leistung erbracht wird, folgt eine Problembehandlung (PT, problem treatment):

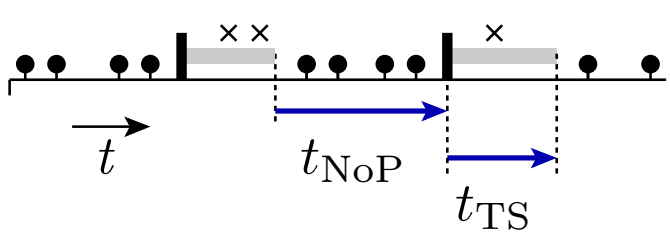
- Schadensminderung (Datenrettung, sicherer Zustand, ...),
- Ursachenbeseitigung (Reparatur, Neuinitialisierung, ...) und
- optional Tolerierungsversuche.

Toleranz (von lateinisch tolerare »erleiden, erdulden«), hier Erbringung verwertbarer Ergebnisse trotz erkannter Probleme.

Grundreaktion auf erkannte Probleme ist Leistungsverweigerung (NS, no service). Tolerierungmaßnahmen für Verfügbarkeitsproblemen:

- Hardware-Rekonfiguration,
- nochmalige Service-Anforderung,
- Änderung der Service-Anfrage, ...

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).

Teilverfügbarkeiten

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).

Die unterschiedlichen Nichtverfügbarkeitsursachen haben

- eigene Zählwerte für positive und negative Erfahrungen,
- eigene Eintritts- und Tolerierungsraten,

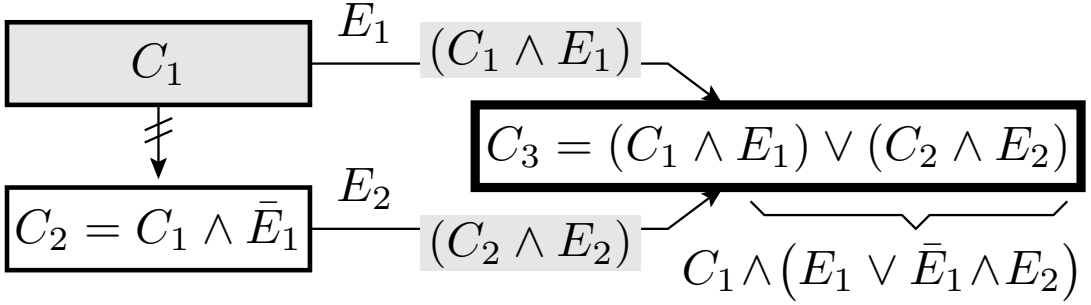
	Ausfall	DA	Absturz	DM
Zählwert neg. Ereignisse	$\#FL$	$\#DA$	$\#CR$	$\#DM$
Zählwert pos. Ereignisse	$\#HA$	$\#RA$	$\#DR$	$\#DS$
Eintrittsrate	ζ_{FL}	ζ_{DA}	ζ_{CR}	ζ_{DM}
Tolerierungsrate	ν_{FL}	ν_{DA}	ν_{CR}	ν_{DM}

- eigene Maßnahme zur Vermeidung und Tolerierung und

werden in unterschiedlichen Teilverfügbarkeiten erfasst.

CVA- (Zählwertzuordnungs-) Graphen

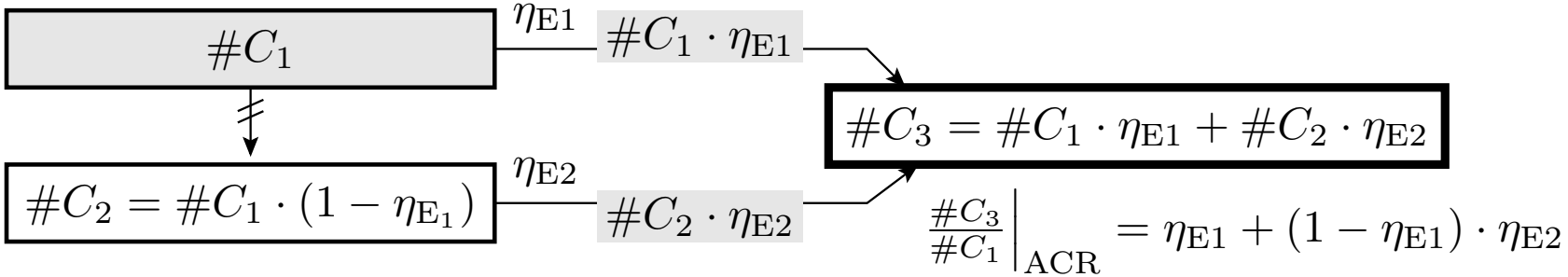
Zähl- und Zuordnungsereignisse



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

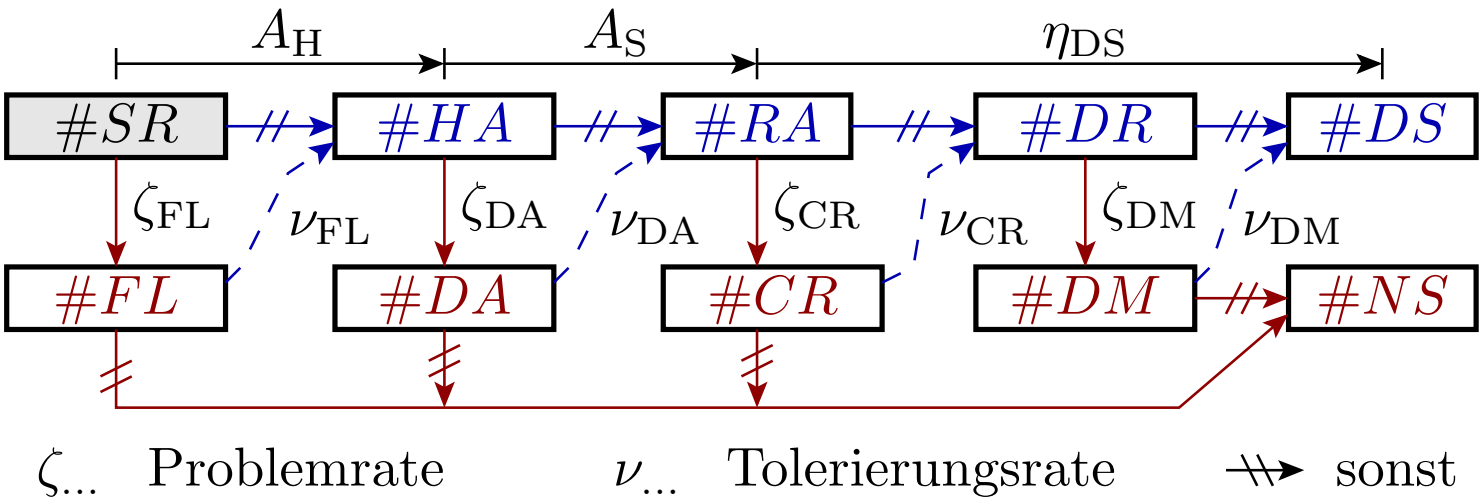
Zählwertzuordnungsgraph (CVA-Graph, count value anssignment graph)

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



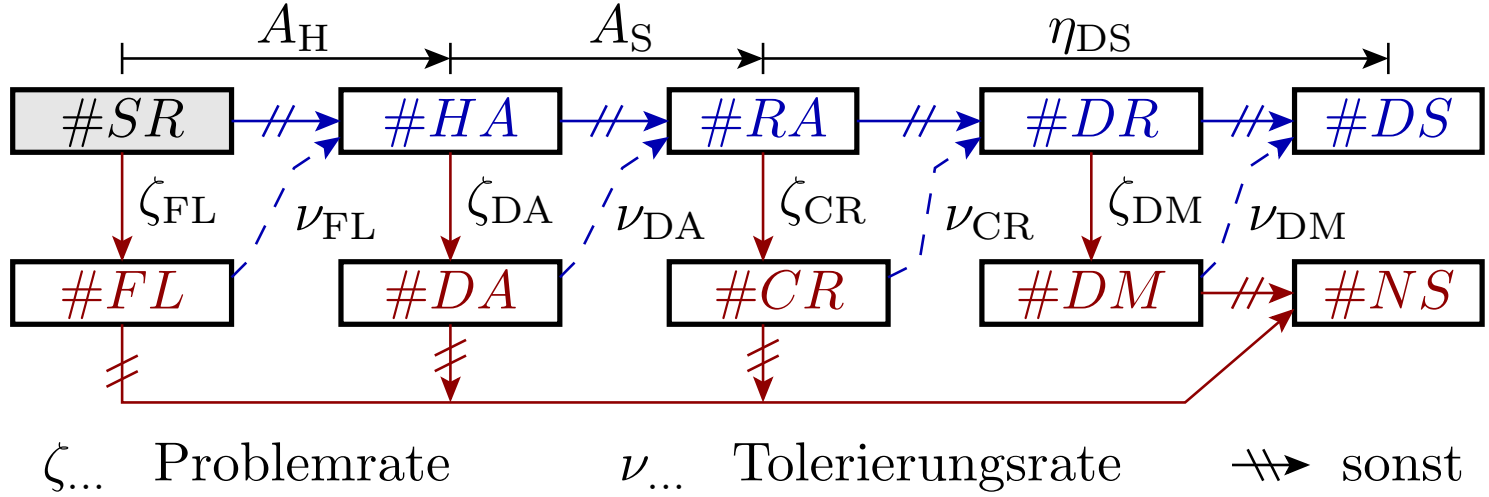
Vorgriff auf verketteten Zufallsereignisse (siehe Abschn. 3.1.2 *Verkettete Ereignisse*).

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:

$$A_H = \left.\frac{\#HA}{\#SR}\right|_{ACR} = (1 - \zeta_{FL}) + \zeta_{FL} \cdot \nu_{FL} \quad (1.3)$$

Service-Verfügbarkeit:

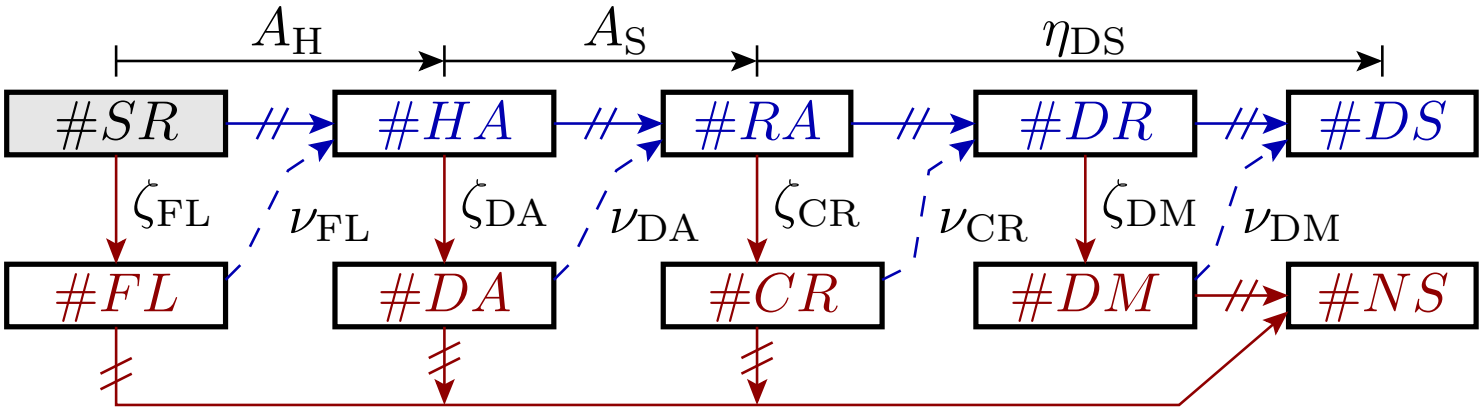
$$A_S = \left.\frac{\#RA}{\#HA}\right|_{ACR} = (1 - \zeta_{DA}) + \zeta_{DA} \cdot \nu_{DA} \quad (1.4)$$

Erbringungsrate:

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

Gesamtverfügbarkeit:

$$A = \left.\frac{\#DS}{\#SR}\right|_{ACR} = A_H \cdot A_S \cdot \eta_{DS} \quad (1.5)$$

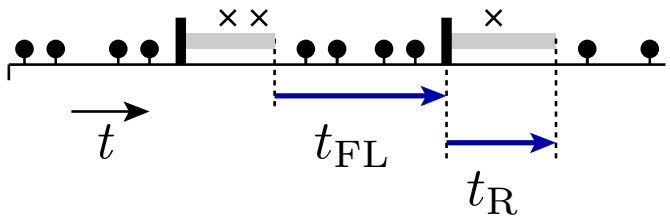


Für unabhängige Ereignisse FL, TFL, DA, TDA,... werden entlang aller Pfade vom Zählwert #CR zu anderen Zählwerten nur

- 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 Sevice-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



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

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

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

Gegenwahrscheinlichkeit «Probability of Failure on Demand«:

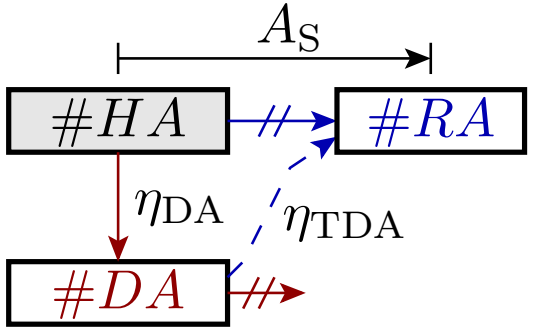
$$PFD = 1 - A_\mathrm{H} = \frac{\bar{t}_\mathrm{R}}{\bar{t}_\mathrm{FL} + \bar{t}_\mathrm{R}} \qquad (1.7)$$

Fortsetzung (siehe Abschn. 6.5 *Ausfälle*).

A_H	Hardware-Verfügbarkeit.
$\#\langle evt \rangle$	Anzahl der Zählereignisse, $evt \in \{SR, HA, \ldots\ldots\}$.
SR, HA	Service-Anforderung, Hardware verfügbar.
FL	Nichtverfügbarkeit wegen Hardware-Ausfall.
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

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



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

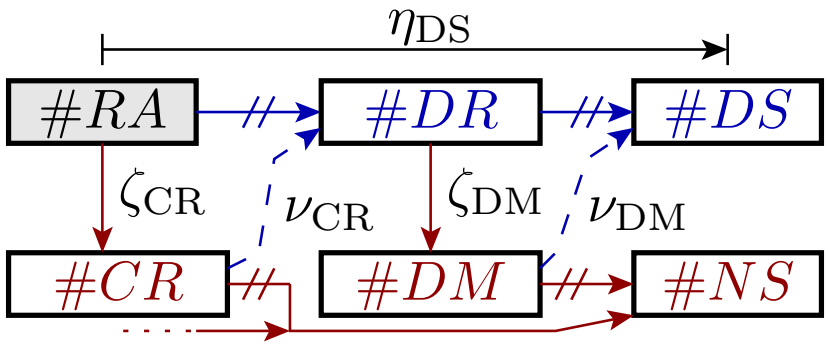
- Problembehandlung nach Absturz oder erkannter Fehlfunktion,
- zu lange Abarbeitungszeit,
- Überlastung durch zu viele Service-Anforderungen, ...

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

Stark mit funktionalen Aspekten verzahnt. Die Vorlesung wird im Weiteren nur hypothetischen Beispielzahlen annehmen, in der Regel $\eta_{DA} = 0$ oder $A_S = 1$.

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

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

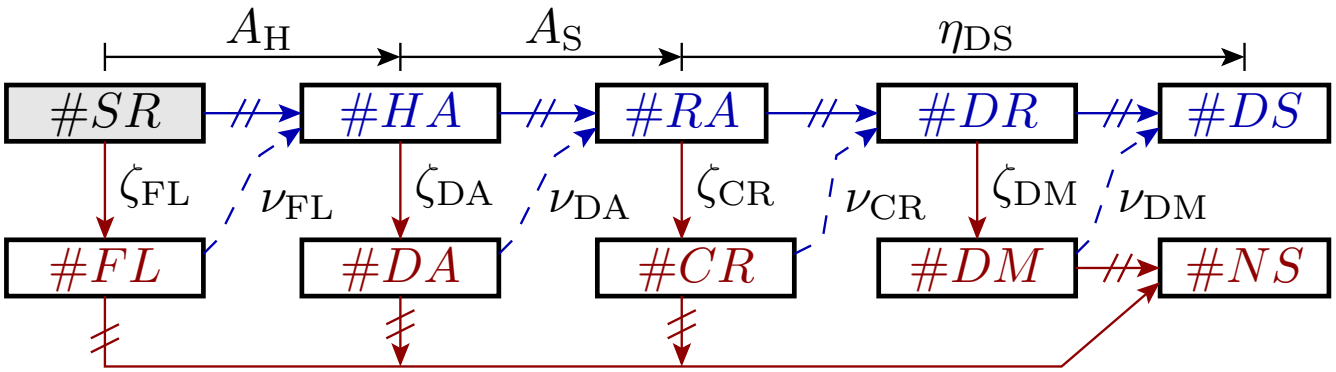
hängt ab von

- 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. 1.3 *Problembehandlung*).

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

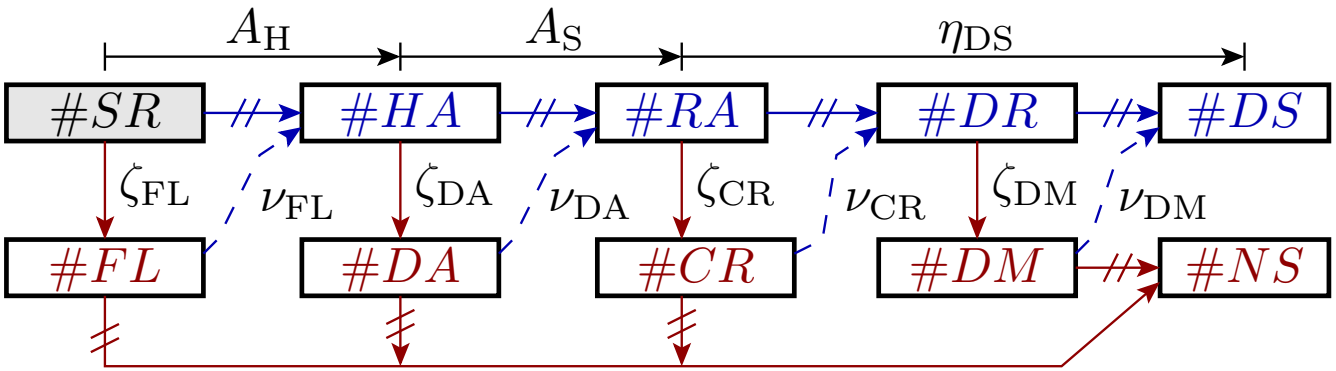
Beispiel 1.1: CVA-Graph und Verfügbarkeit



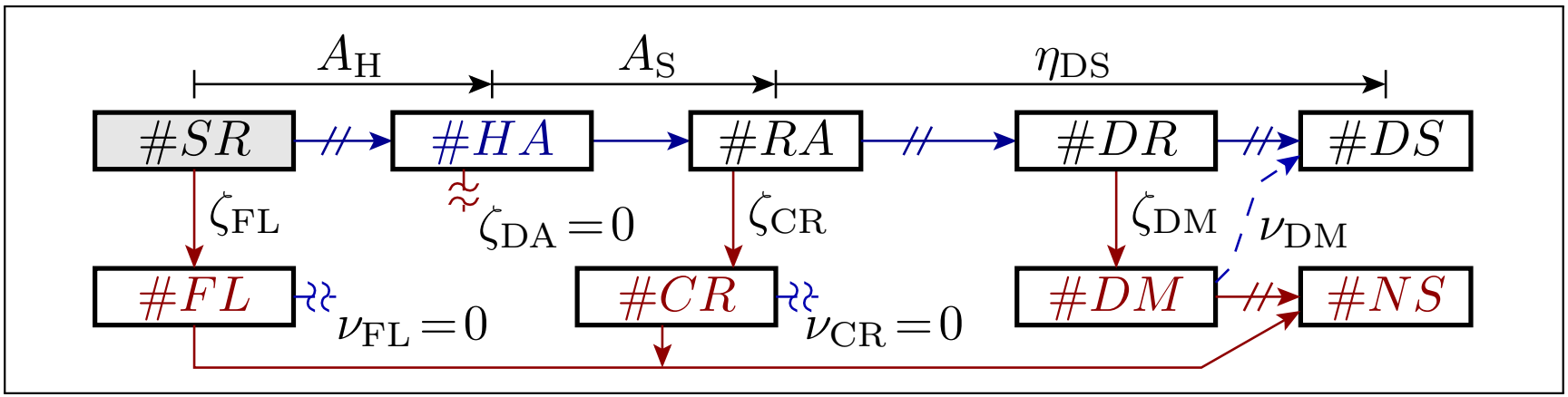
a) *Passen Sie den CVA-Graph so an, dass Ausfälle nie toleriert, Service-Anforderungen bei verfügbarer Hardware immer akzeptiert und bei Absturz nie Leistung erbracht werden.*

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

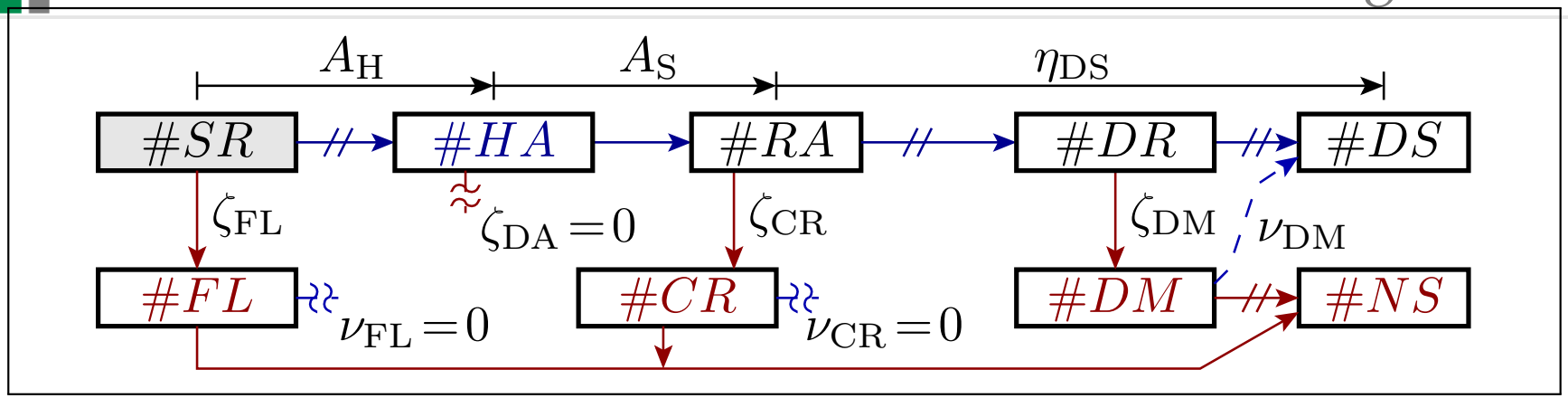
SR, HA	Service-Anforderung, Hardware verfügbar.
RA, DR	Service-Anforderung akzeptiert, erbrachtes Ergebnis.
DS, NS	Erbrachte Sevice-Leistung, keine Service-Leistung.
FL, DA	Nichtverfügbarkeit wegen Hardware-Ausfall bzw. Annahmeverweigerung.
CR, DM	Nichtverfügbarkeit wegen Absturz bzw. erkannter Fehlfunktion.



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):

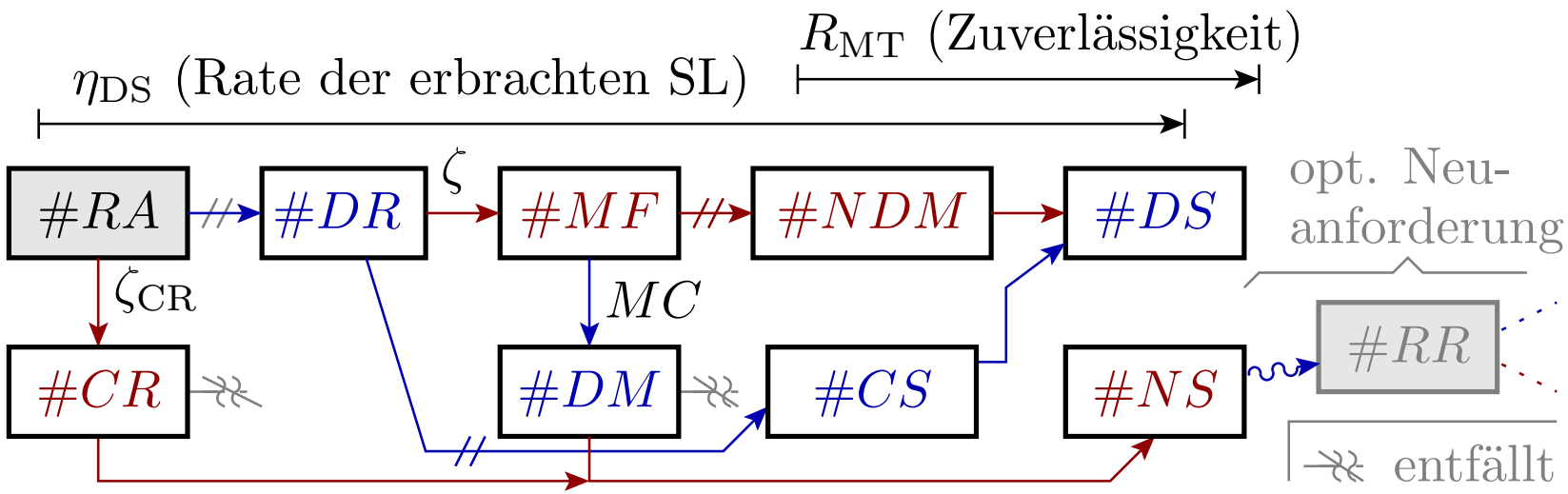
$$\eta_{\mathrm{CS}[\mathrm{MT}]} = 1 - \zeta_{[\mathrm{MT}]}$$

Wir bevorzugen die Zuverlässigkeit R als Maß der Richtigkeit:

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

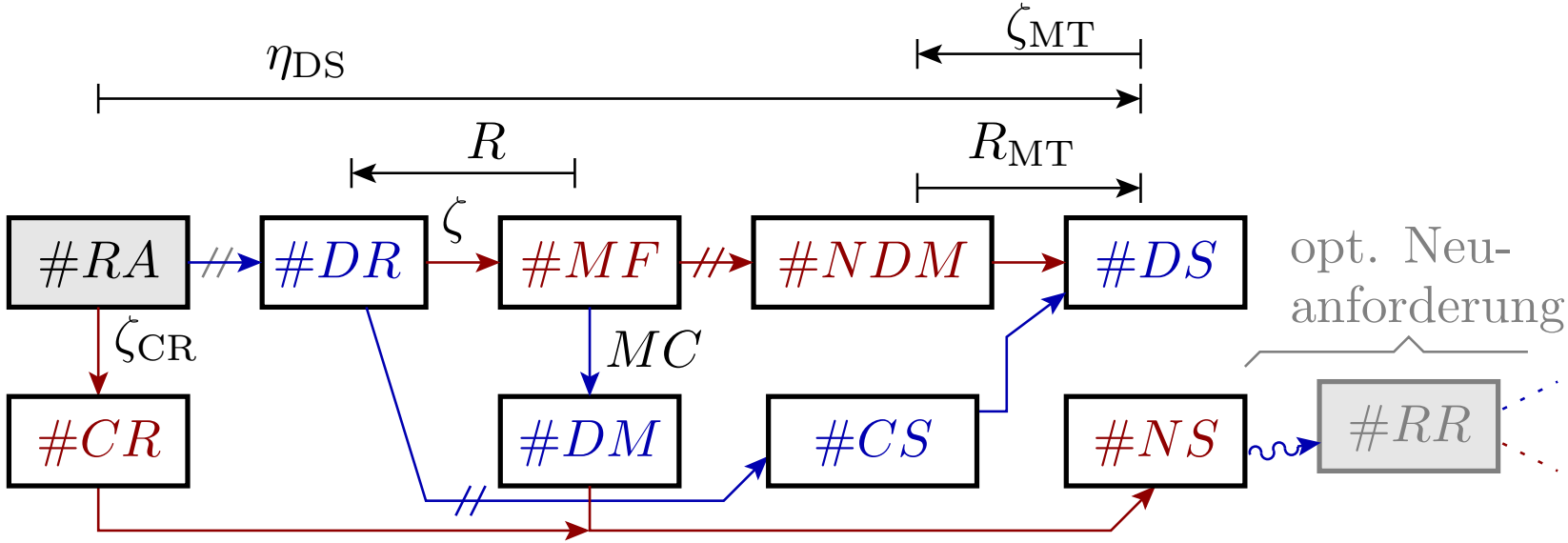
$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
$\#DS$	Anzahl der erbrachten Service-Leistungen.
$\#NDM$	Anzahl der nicht erkannten Fehlfunktionen (Number of not detected malfunctions).
$\zeta_{[\mathrm{MT}]}$	Fehlfunktionsrate mit bzw. ohne Fehlfunktionsbehandlung.
*	Zweckmäßige,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

Nachbesserung CVA-Graph



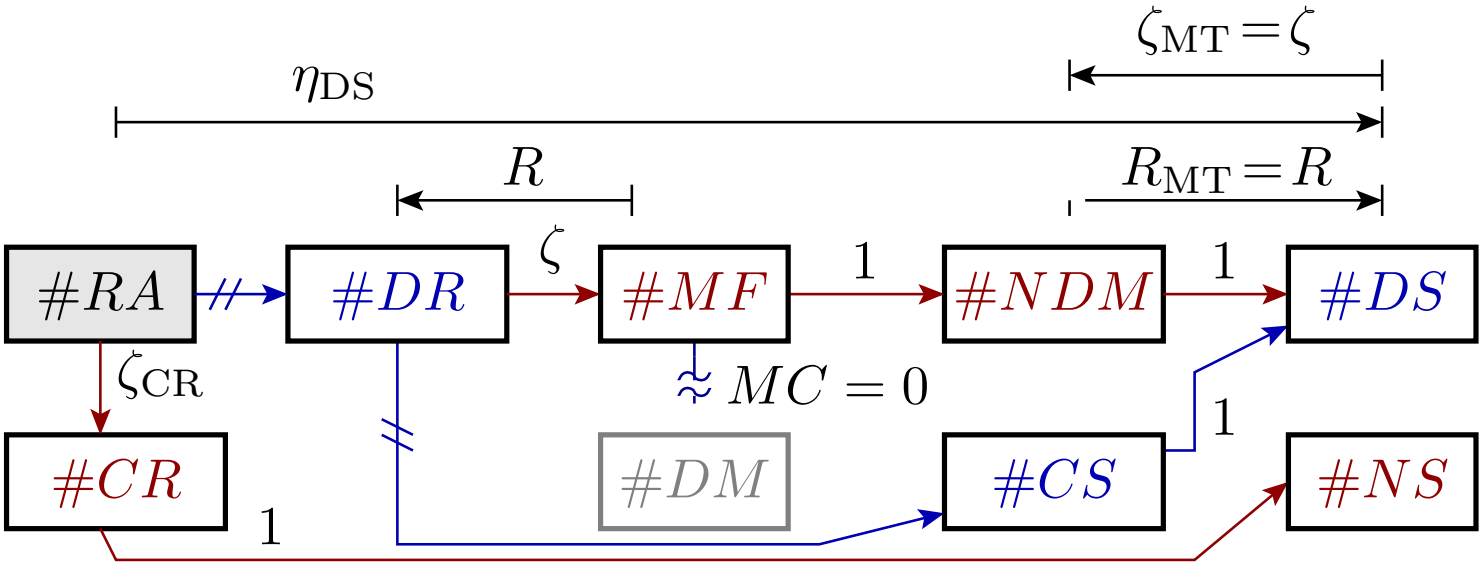
Ergänzung eines Zählwerts für nicht erkannte Fehlfunktionen:

- Fehlfunktionen (MF) werden mit Häufigkeit MC erkannt (DM) und sonst nicht erkannt (NDM).
- Für Abstürze (CR) und erkannte Fehlfunktionen (DM) keine Leistungserbringung (NS).
- Wenn keine Leistungserbringung im Erstversuch optionale Tolerierungsversuche durch Neuanforderung (RR, ersetzt Tolerierungskanten von CR und DM).



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, $evt \in \{SR, HA, \ldots\ldots\}$.
RA, DR	Service-Anforderung akzeptiert, erbrachtes Ergebnis.
MF, NDM	Fehlfunktion, nicht erkennbare Fehlfunktion.
DS, NS	Erbrachte Sevice-Leistung, keine Service-Leistung.
CR, DM	Nichtverfügbarkeit wegen Absturz bzw. erkannter Fehlfunktion.
ζ_{CR}, MC	Absturzrate, Fehlfunktionsabdeckung.

Ohne Überwachung und Problembehandlung



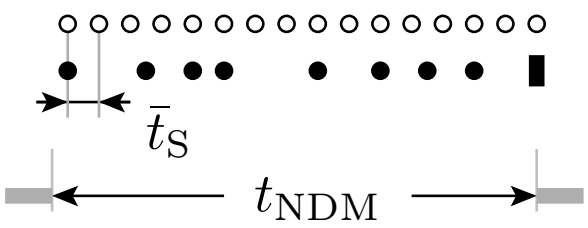
Ohne Problembehandlung sind alle gelieferten Ergebnisse erbrachten Service-Leistungen und keine der Fehlfunktionen wird erkannt:

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

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

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

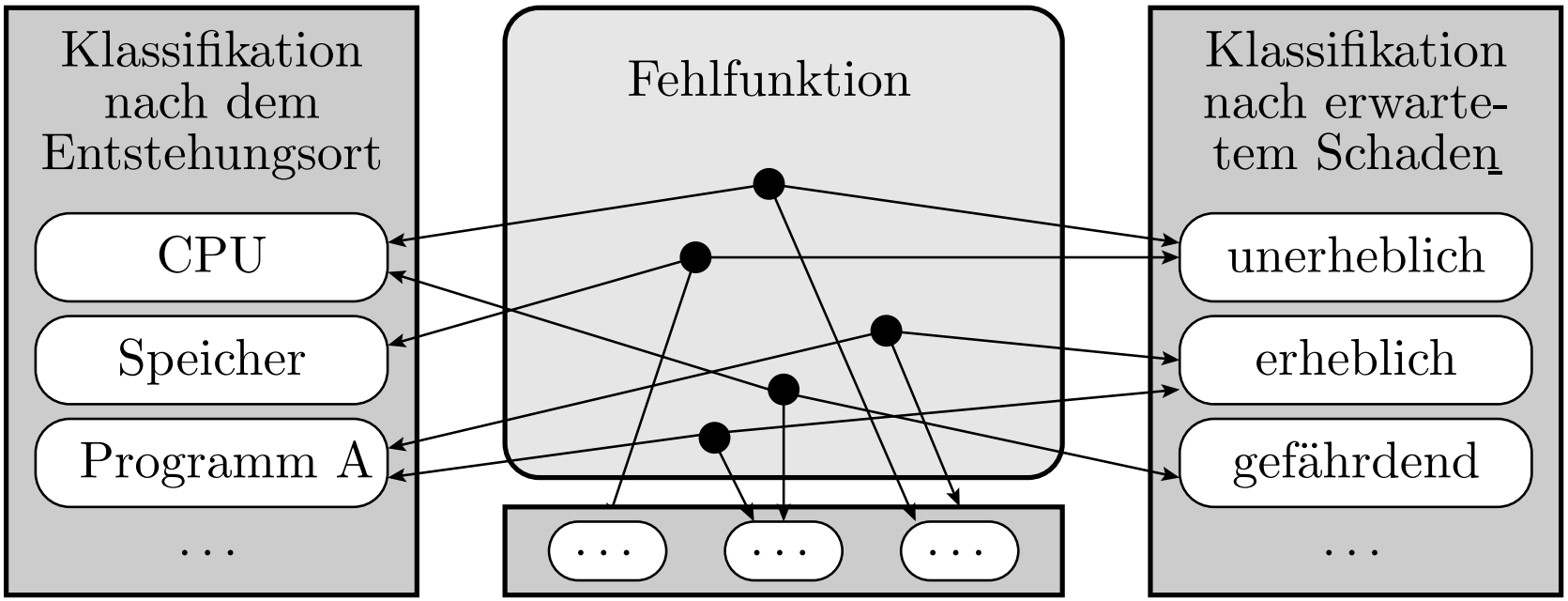
- Service nicht verfügbar
- ∘ Service-Zeitslots (SS)
- • erbrachte Service-Leistungen (DS)

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 und Teilfehlfunktionsraten?*

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.
$R_{\mathrm{MT}.i}$	Zuverlässigkeit mit Fehlfunktionsbehandlung der Fehlfunktionsklasse i.
$R_{\mathrm{MT}}, \zeta_{\mathrm{MT}}$	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 und Teilfehlfunktionsraten?*

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

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?*

$$\zeta_{[\mathrm{MT}]} = \frac{1}{R_{[\mathrm{MT}]}} \tag{1.9}$$

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

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

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

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
...	...

Rate der die Sicherheit gefährdenden Probleme:

$$\zeta_{\mathrm{S}} = \left.\frac{\#SP}{\#DS}\right|_{\mathrm{ACR}} \tag{1.13}$$

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	Erbrachte Service-Leistungen, 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, Gefährdungsabwendung

Kehrwert der Rate der sicherheitsgefährdenden Fehlfunktionen:

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

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

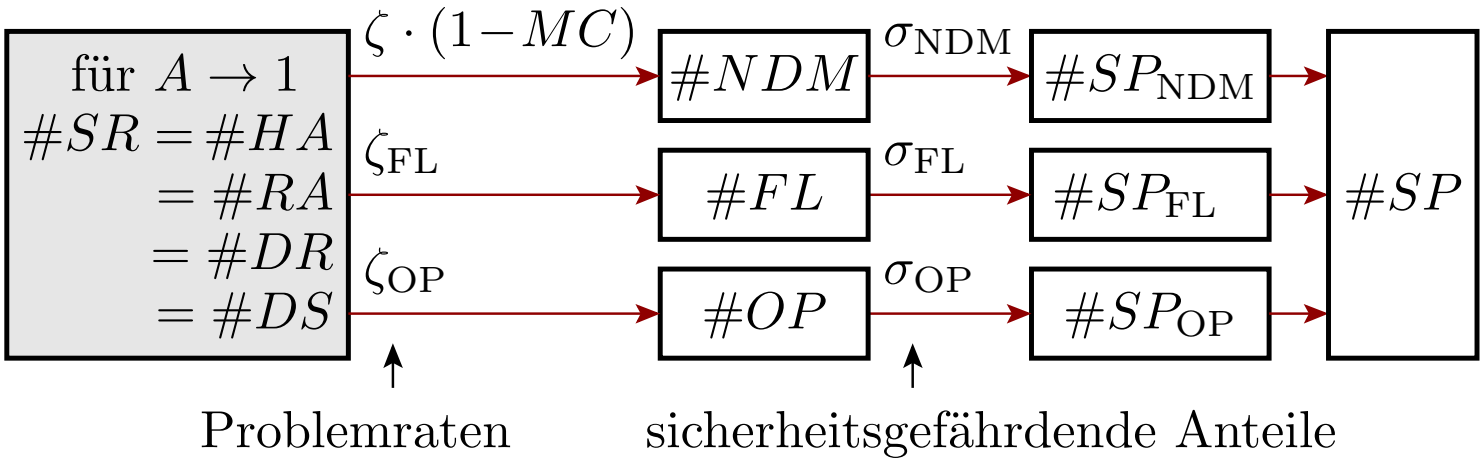
$$\frac{1}{S} = \sum_{i=1}^{\#SPC} \frac{1}{S_i} \tag{1.16}$$

Aufteilung in Problemklassen nach Gefährdungsabwendung:

- nicht erkennbare Fehlfunktionen $\Rightarrow$ Zusatzkontrollen,
- ausgefallene Hardware $\Rightarrow$ Reserve-Hardware,
- sonstige erkannte Probleme ohne Leistungserbringung $\Rightarrow$ Reservefunktionen.

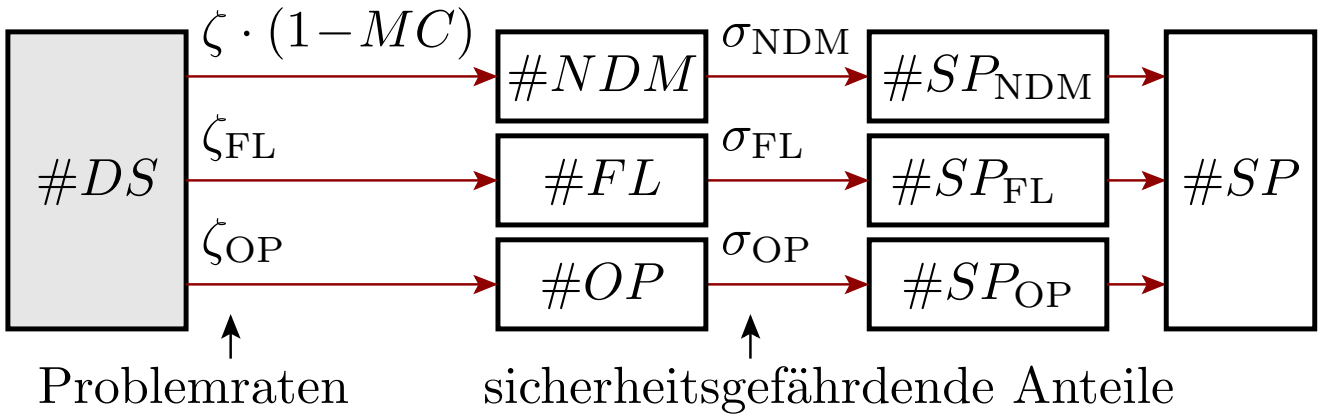
S, S_i	Gesamtsicherheit, Teilsicherheiten i.
$\#SPC$	Anzahl der Sicherheitsproblemklassen (Number of safety and security problem classes).
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

Sicherheiten als Teilzuverlässigkeiten



- Bei typ. Verfügbarkeit nahe eins sind die Zählwerte für Service-Anforderungen (SR), Hardware bei Anforderung verfügbar (HA), Anforderung akzeptiert (RA), Ergebnis erbracht (DR) und Service erbracht (DS) praktisch gleich.
- Probleme jeder betrachteten Klasse haben eine Auftrittsrate ζ_i je DS und sind mit einer Rate σ_i sicherheitsgefährdend.

ζ_i, σ_i	Problemrate, sicherheitsgefährdender Anteil jeweils für Problemklasse i.
$\#SP_i$	Zählwert für sicherheitsgefährdende Probleme der Klasse i.
i	Problemklasse $i \in \{\mathrm{NDM}, \mathrm{FL}, \mathrm{OP}\}$. NDM: nicht erkannte Fehlfunktion, FL: Hardware-Ausfall, OP: sonstiges erkanntes Problem ohne Leistungserbringung.



Raten der sicherheitsgefährdenden Fehlfunktionen durch

- nicht erkannter Fehlfunktionen:

$$\zeta_{\mathrm{S.NDM}} = \frac{1}{S_{\mathrm{NDM}}} = \frac{\#SP_{\mathrm{NDM}}}{\#DS}\Big|_{\mathrm{ACR}} = \zeta \cdot (1 - MC) \cdot \sigma_{\mathrm{NDM}} \qquad (1.17)$$

- Hardwareausfälle:

$$\zeta_{\mathrm{S.FL}} = \frac{1}{S_{\mathrm{FL}}} = \frac{\#SP_{\mathrm{FL}}}{\#DS}\Big|_{\mathrm{ACR}} = \zeta_{\mathrm{FL}} \cdot \sigma_{\mathrm{FL}} \qquad (1.18)$$

- sonstige erkannte Probleme ohne Leistungserbringung:

$$\zeta_{\mathrm{S.OP}} = \frac{1}{S_{\mathrm{OP}}} = \frac{\#SP_{\mathrm{OP}}}{\#DS}\Big|_{\mathrm{ACR}} = \zeta_{\mathrm{OP}} \cdot \sigma_{\mathrm{OP}} \qquad (1.19)$$

- Sicherheit nach Gl. 1.14 und 1.15 insgesamt:

$$S = \frac{\#DS}{\#SP}\Big|_{\mathrm{ACR}} = \frac{1}{\zeta_{\mathrm{S.NDM}} + \zeta_{\mathrm{S.FL}} + \zeta_{\mathrm{S.OP}}}$$

Stellschrauben für hohe Sicherheit

Nicht erkannte MF in Anwendungen mit hohen Gefährdungsrisiken:

- geringe Fehlfunktionsrate ζ, hohe Fehlfunktionsabdeckung MC,
- Überwachung auf sicherheitskritische Zustände, Notfallpläne, ...

Systeme, die nicht problemlos in einen sicheren Zustand gebracht werden können (Fahrzeuge, Reaktoren, ...):

- hohe Hardware-Verfügbarkeit, Wartung,
- Redundanz (siehe Abschn. 6.5 *Ausfälle*).

Systeme mit hohem potentiellen Schaden bei Nichterbringung (Logistik, Kommunikation, Finanzwesen, ...):

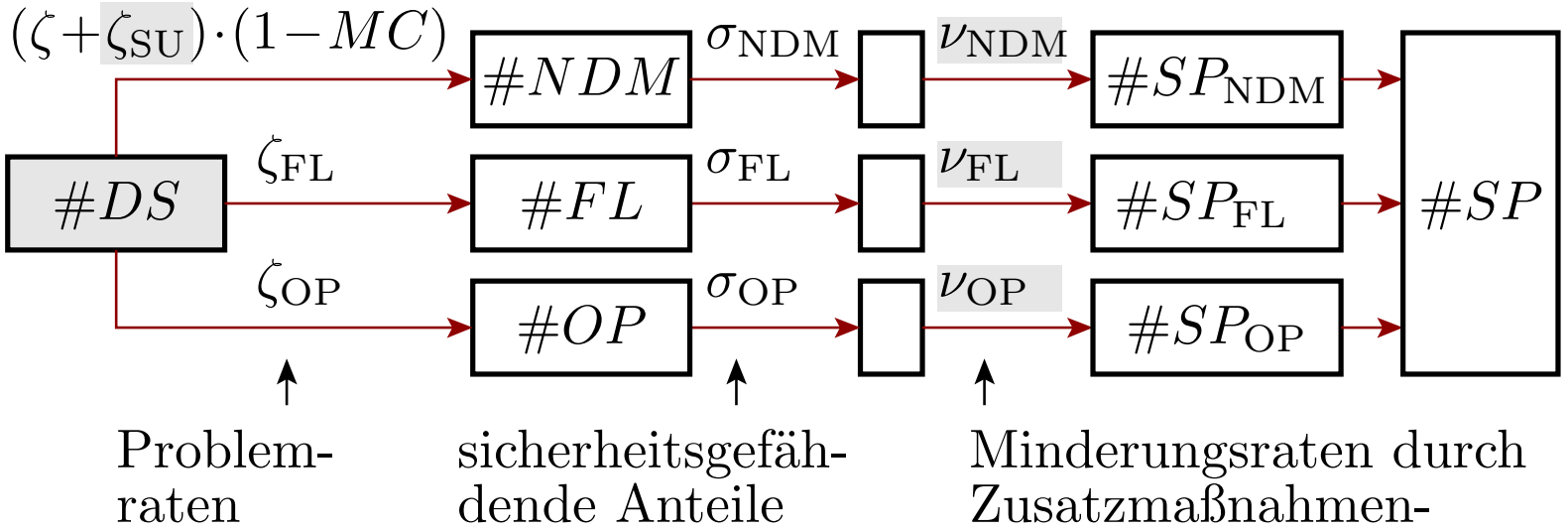
- Hohe Verfügbarkeit, geringe Fehlfunktions- und Absturzrate,
- Problemtolerierung durch Wiederholung, Reservefunktionen für wichtige Leistungen, ...

Systeme mit hohem potentiellen Schaden bei Datenverlust:

- redundante Speicherung, fehlerkorrigierende Codes,
- RAIDs, Backups, ...

...

Sicherheitsverbesserung durch Zusatzeinheiten



- Minderung der Schadenshäufigkeit in sicherheitskritischen Situationen, im Bild modelliert durch Minderungsraten $\nu_{\ldots}$.
- Zusätzliche Sicherheitsrisiken, im Bild modelliert als zusätzliche Fehlfunktionsrate ζ_{SU} für die Zusatzeinheiten.

Sicherheitsverbesserung für den Beispiel-CVA-Graph:

$$S = \frac{1}{(\zeta+\zeta_{\mathrm{SU}})\cdot(1-FC)\cdot\sigma_{\mathrm{NDM}}\cdot\nu_{\mathrm{NDM}}+\zeta_{\mathrm{FL}}\cdot\sigma_{\mathrm{FL}}\cdot\nu_{\mathrm{FL}}+\zeta_{\mathrm{OP}}\cdot\sigma_{\mathrm{OP}}\cdot\nu_{\mathrm{OP}}}$$

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%.*

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

a) *CVA-Graph und die Sicherheit ohne das zusätzliche Steuergerät?*

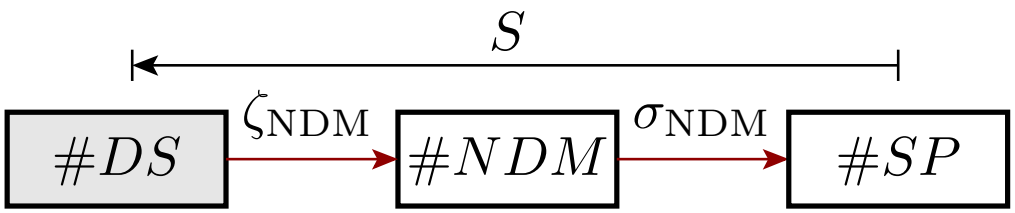
b) *CVA-Graph mit Zusatzsteuergerät. Mindestzuverlässigkeit Steuergerät* R_{SU}*, damit sich die Sicherheit verfünffacht* ($S_{\mathrm{SU}} \geq 5 \cdot S$)*?*

$\bar{t}_{\mathrm{NDM}}, \bar{t}_{\mathrm{S}}$	Mittlere Service-Zeit je nicht erkannte Fehlfunktion, mittlere Service-Dauer.
η_{SU}	Systemauslastungsrate.
σ_{NDM}	Sicherheitsgefährdender Anteil der nicht erkannten Fehlfunktionen.
ν_{MDM}	Minderung der Sicherheitsgefärdung durch das Zusatzsteuergerät.
S, S_{SU}	Sicherheit ohne Zusatzsteuergerät, Sicherheit mit Zusatzsteuergerät.

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

a) *CVA-Graph und die Sicherheit ohne das zusätzliche Steuergerät?*

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



Die Aufgabe betrachtet als Problem nur die Rate der nicht erkannter Fehlfunktionen

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

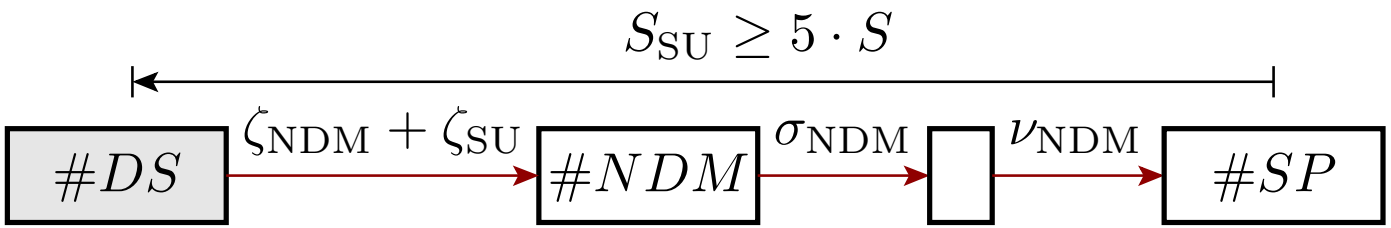
die mit einer Rate $\sigma_{\mathrm{NDM}} = 1\%$ die Sicherheit gefährden. Sicherheit:

$$S = \frac{1}{\zeta_{\mathrm{NDM}} \cdot \sigma_{\mathrm{NDM}}} = 10^{5}\ \left[\frac{\mathrm{DS}}{\mathrm{SP}}\right]$$

DS, SP Erbrachte Service-Leistungen, sicherheitsgefährdende Probleme.
ζ_{NDM} Rate der nicht erkannten Fehlfunktionen.

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

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



Maximale Zuverlässigkeitsverringerung durch das Steuergerät:

$$\underbrace{(\zeta_{\mathrm{NDM}} + \zeta_{\mathrm{SU}}) \cdot \sigma_{\mathrm{NDM}} \cdot \nu_{\mathrm{NDM}}}_{1/S_{\mathrm{SU}}} \leq \frac{1}{5} \cdot \underbrace{\zeta_{\mathrm{NDM}} \cdot \sigma_{\mathrm{NDM}}}_{1/S}$$

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

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

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

Das zusätzliche Steuergerät muss mindestens so zuverlässig wie das Fahrzeug sein.

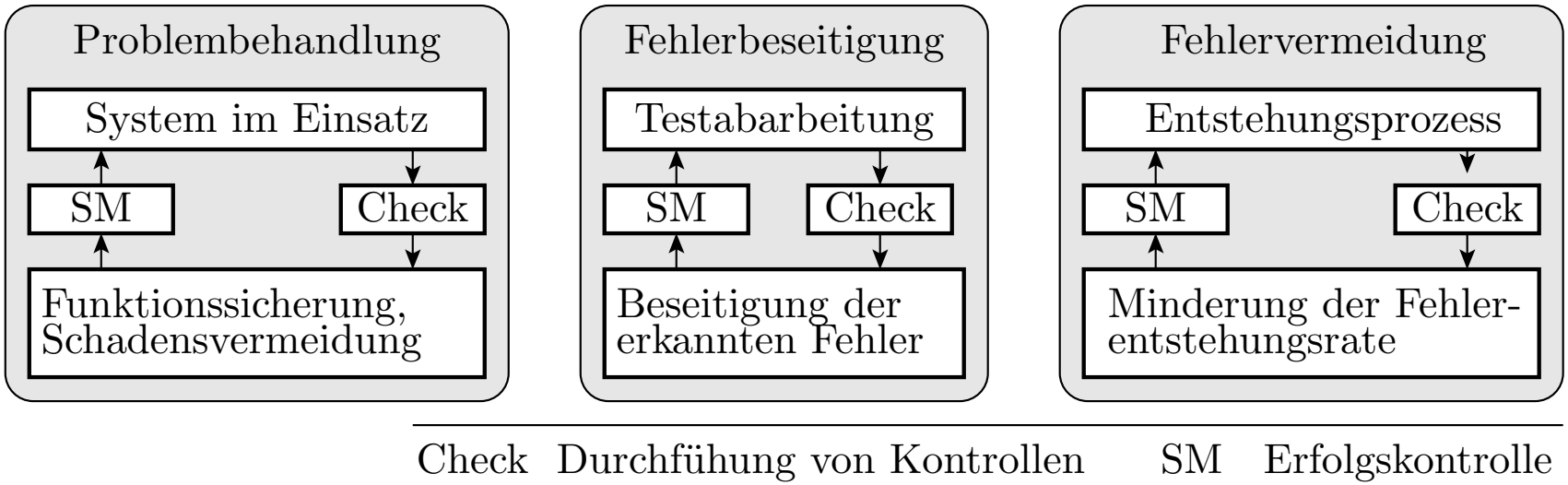
Anmerkungen zur Aufgabe

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

- Das sind komplexe Zielfunktionen und für den Umgang mit sicherheitsgefährdenden Fehlfunktionen ungeeignet.
- Bei erkannten Fehlfunktionen ist mit hoher Zuverlässigkeit ein sicherer Zustand zu erreichen.
- Hohe Zuverlässigkeit verlangt Fehlerarmut, geringe Störanfälligkeit, ..., idealerweise ein kleines, einfaches, gut testbares, isolierte Teilsystem für die Fehlfunktionsbehandlung ohne unnötige komplexe Berechnungen und Entscheidungen.
- Für nicht erkennbare Fehlfunktionen ist überhaupt kein Notfallverhalten vorgebbar.
- Autonome Fahrzeuge können jedoch wesentlich zuverlässiger und sicherer als manuell gesteuerte Fahrzeug gestaltet werden.
- Das Restrisiko muss eine Art Haftpflichtversicherung abdecken. Das erfordert neue rechtlichen Rahmenbedingungen.

Zusammenfassung

Sicherung der Verlässlichkeit

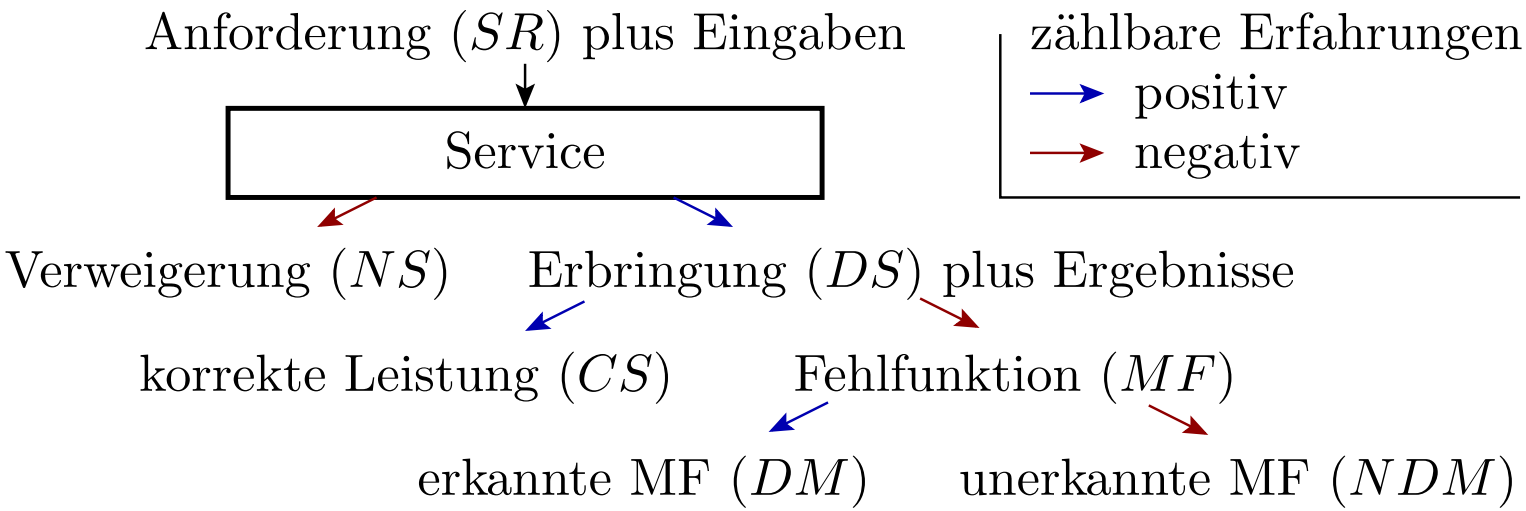


Verlässlichkeit beschreibt, wie weit das Vertrauen in ein IT-System gerechtfertigt ist. Sicherung durch Iterationen aus Kontrolle, Korrektur und Erfolgskontrolle auf drei Ebenen:

- 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** zur Beschreibung aller Teilaspekte der und Einflüsse auf die Verlässlichkeit durch Zählwerte für positive und negative Erfahrungen.
- **Service-Modell**: Diskretisierung der Leistungserbringung. Auf Anforderung wird kein (NS) oder ein Leistung erbracht (DS). 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

Maß für die Erbringung:

- Verfügbarkeit:

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

Maße für die Richtigkeit

- Zuverlässigkeit

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

- Fehlfunktionsrate

$$\zeta_{[\mathrm{MT}]} = \frac{1}{R_{[\mathrm{MT}]}} \tag{1.9}$$

Maße für die Sicherheit vor Schaden:

- Rate Sich.-Prob.

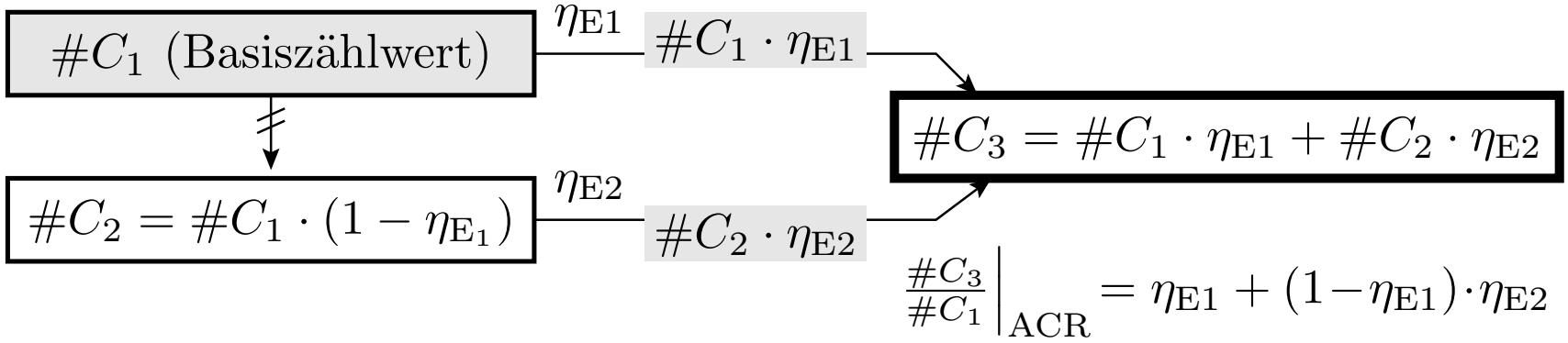
$$\zeta_{\mathrm{S}} = \frac{\#SP}{\#DS}\Big|_{\mathrm{ACR}} \tag{1.13}$$

- Sicherheit

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

SR, DS	Service-Anforderung, erbrachter Service.
NDM,SP	Nicht erkannte Fehlfunktion, sicherheitsgefährdende Probleme.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

CVA- (Zählwertzuordnungs-) Graph

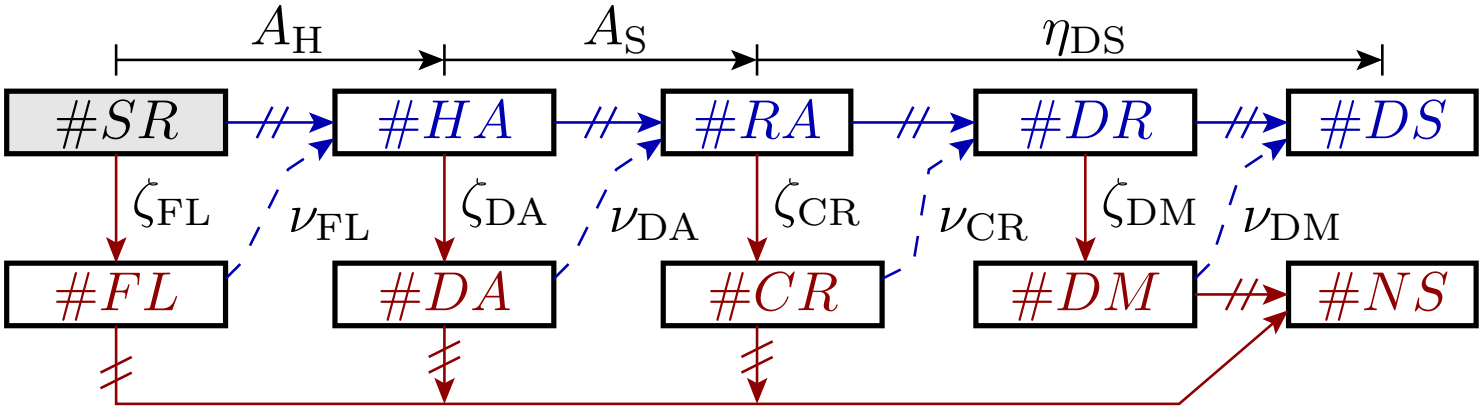


Gerichteter Graph zur Abschätzung von Zählwertverhältnissen.

Ein Basiszählwert (z.B. für Service-Anforderung) wird über rel. Häufigkeitskanten auf abgeleitete Zählwerte (z.B. erbrachte Leistungen) so abbildet, dass sich die Kantenhäufigkeiten

- nacheinander durchlaufener Kanten multiplizieren (UND unabhängiger Zufallsereignisse) und
- bei rekonvergenter Zusammenfassung addieren (ODER sich ausschließender Zufallsereignisse).

CVA-Graph 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:

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

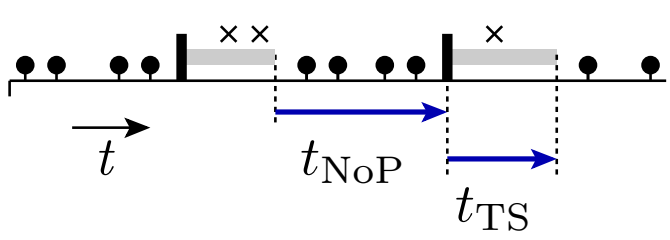
Service-Verfügbarkeit:

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

Gesamtverfügbarkeit:

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

Verfügbarkeit und Fehlfunktionsbehandlung



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

Nach Schadensereignissen (Hardware ausgefallen, ...) folgt eine Fehlfunktionsbehandlung (Schadensbegrenzung, Ursachenermittlung, Reparatur, Neuinitialisierung, ...).

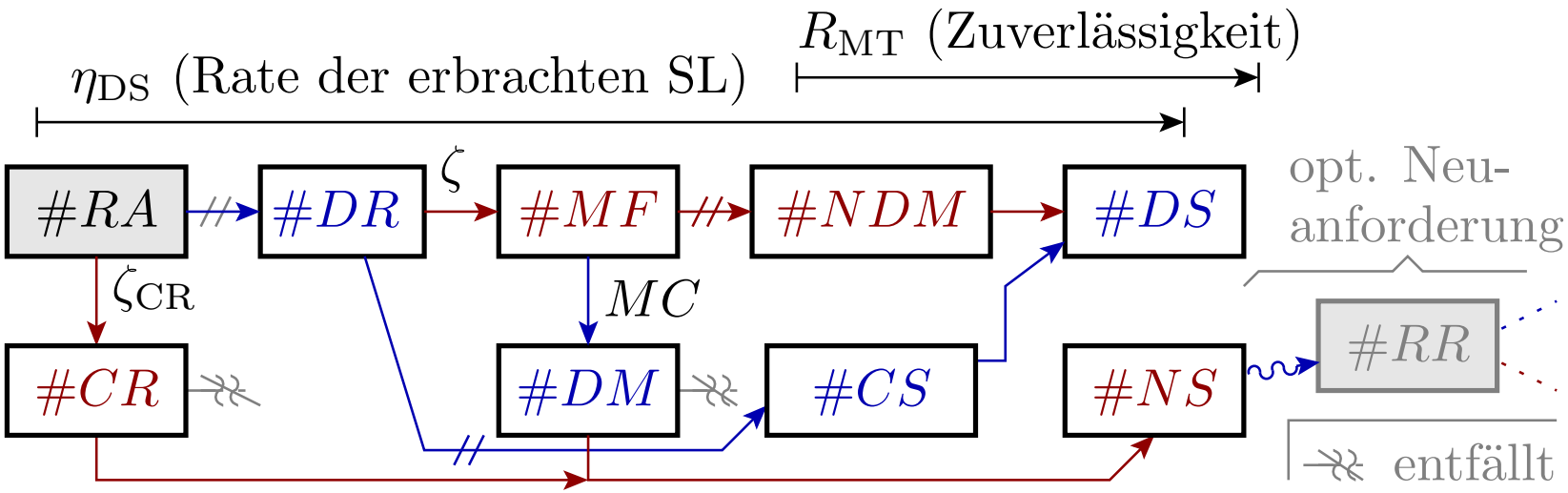
Verfügbarkeit in Abhängigkeit von der mittleren problemfreien Zeit und der mittleren Zeit für die Problembehebung:

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

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

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

Zuverlässigkeit



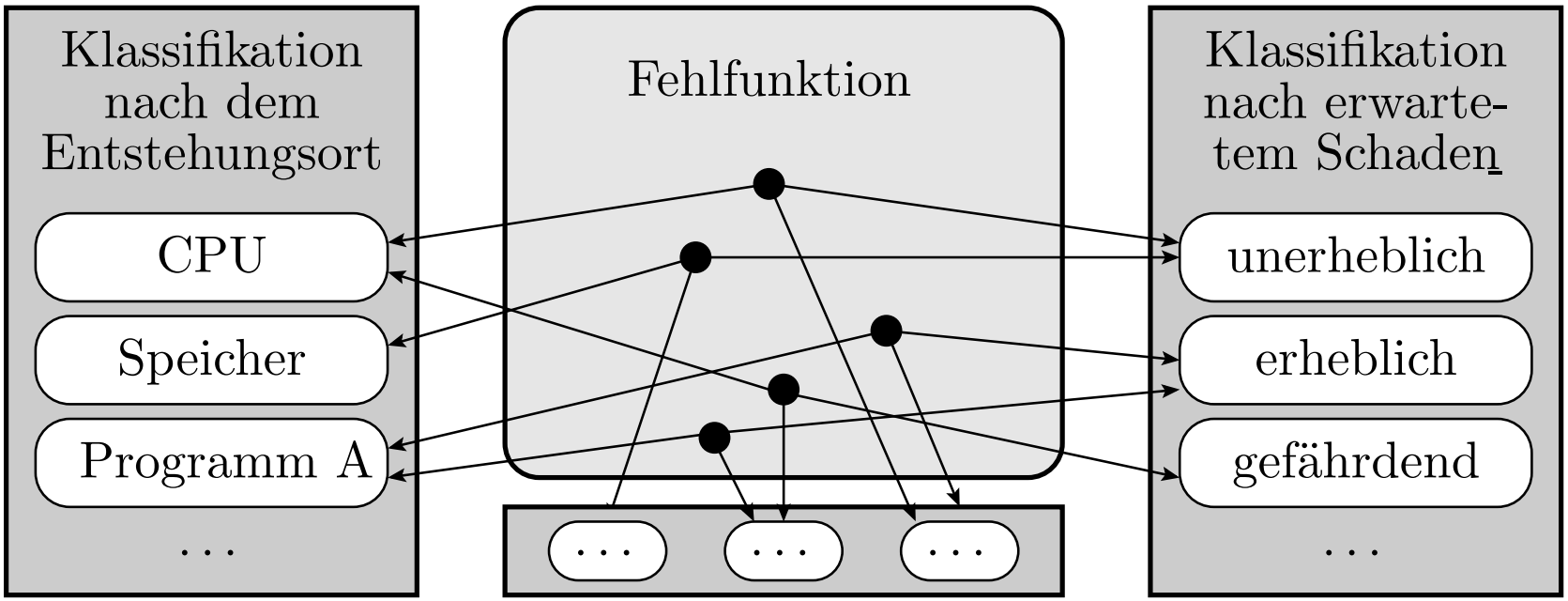
$$R_{[\mathrm{MT}]} = \frac{\#DS}{\#NDM}\Big|_{\mathrm{ACR}} \tag{1.8}$$

$$\zeta_{[\mathrm{MT}]} = \frac{1}{R_{[\mathrm{MT}]}} \tag{1.9}$$

- Abschätzung aus der mittlerer Zeit zwischen Fehlfunktionen:

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

Teilzuverlässigkeiten

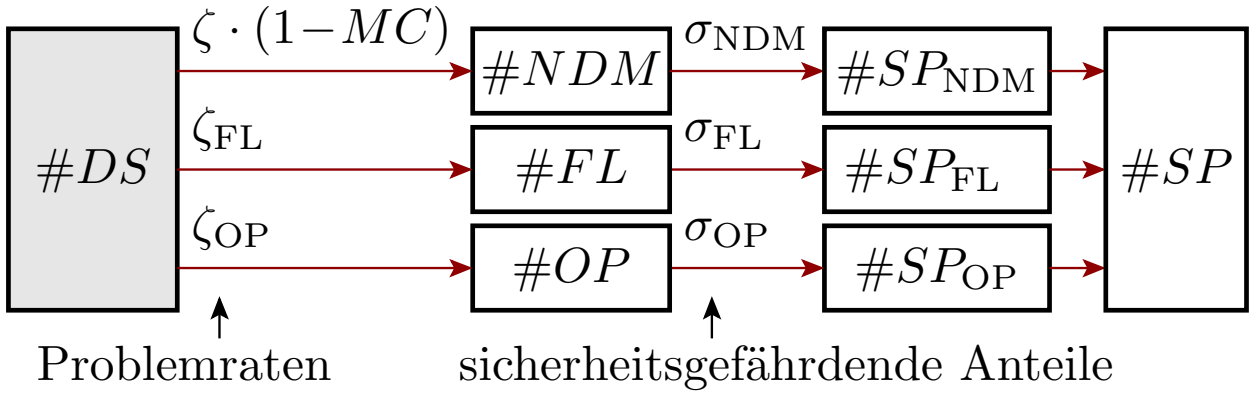


Bei eindeutiger Zuordnung jeder Fehlfunktion genau zu einer Klasse:

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

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

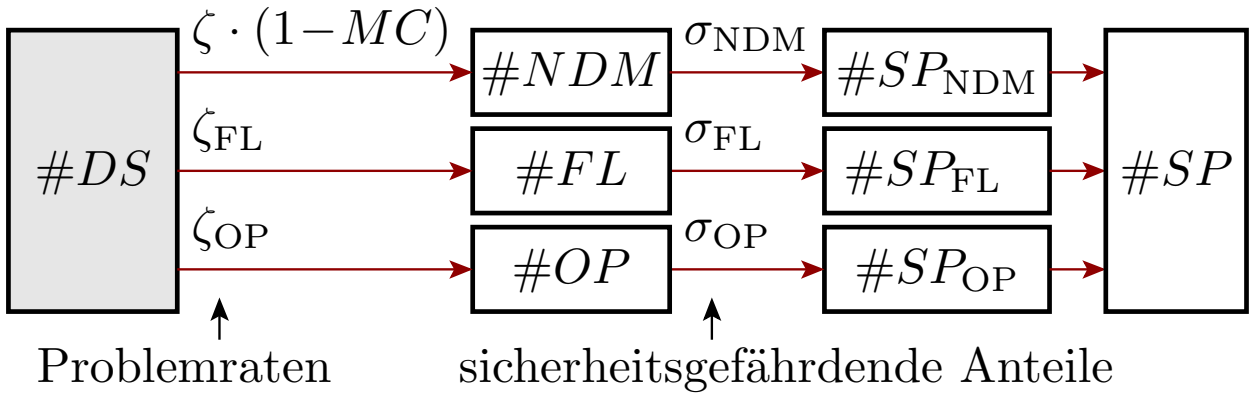
Sicherheit als System von Teilzuverlässigkeiten



Bei hoher Verfügbarkeit lassen sich alle Problemraten auf den Zählwert der erbrachten Leistungen beziehen. Bei Zuordnung aller Probleme genau zu einer Teilsicherheit addieren sich die Problemraten und die Kehrwerte der Teilsicherheiten:

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

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



Teilsicherheiten nach Gefährdungsabwendung:

- nicht erkennbare Fehlfunktionen ⇒ Zusatzkontrollen:

$$\zeta_{\mathrm{S.NDM}} = \frac{1}{S_{\mathrm{NDM}}} = \zeta \cdot (1 - MC) \cdot \sigma_{\mathrm{NDM}} \tag{1.17}$$

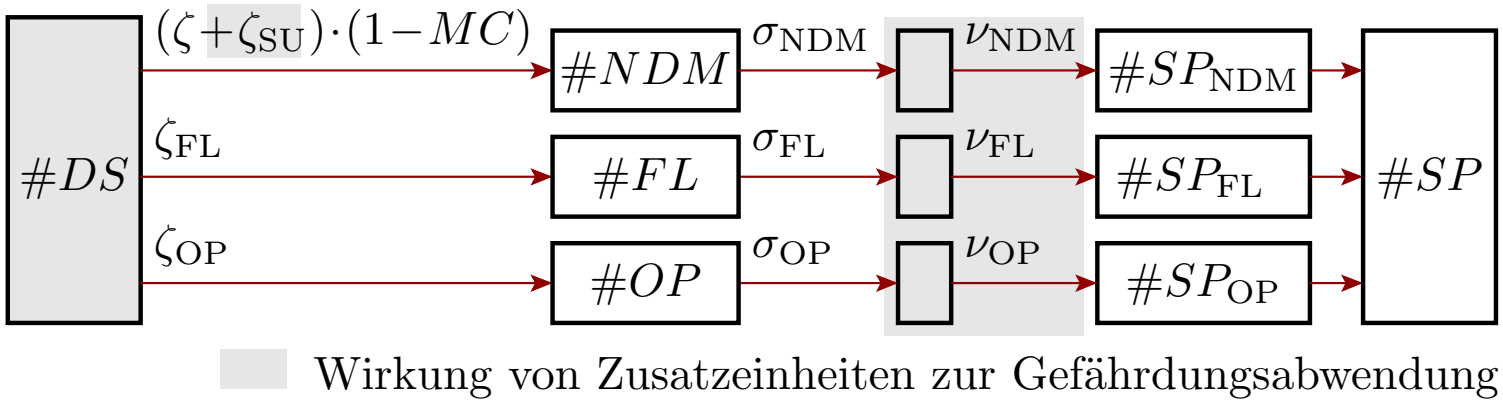
- ausgefallene Hardware ⇒ Ausfalltoleranz:

$$\zeta_{\mathrm{S.FL}} = \frac{1}{S_{\mathrm{FL}}} = \zeta_{\mathrm{FL}} \cdot \sigma_{\mathrm{FL}} \tag{1.18}$$

- sonstige erkannte Probleme ⇒ Reservefunktionen:

$$\zeta_{\mathrm{S.OP}} = \frac{1}{S_{\mathrm{OP}}} = \zeta_{\mathrm{OP}} \cdot \sigma_{\mathrm{OP}} \tag{1.19}$$

Sicherheitsverbesserung durch Zusatzeinheiten

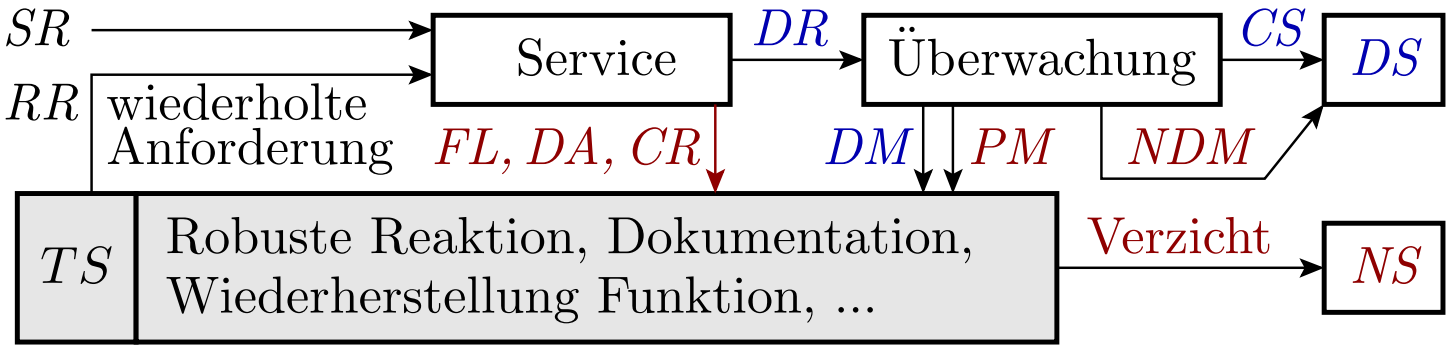


Sicherheitsverbesserung für den Beispiel-CVA-Graph:

$$S = \frac{1}{(\zeta+\zeta_{\mathrm{SU}})\cdot(1-FC)\cdot\sigma_{\mathrm{NDM}}\cdot\nu_{\mathrm{NDM}}+\zeta_{\mathrm{FL}}\cdot\sigma_{\mathrm{FL}}\cdot\nu_{\mathrm{FL}}+\zeta_{\mathrm{OP}}\cdot\sigma_{\mathrm{OP}}\cdot\nu_{\mathrm{OP}}}$$

Problembehandlung

Problembehandlung im laufenden Betrieb



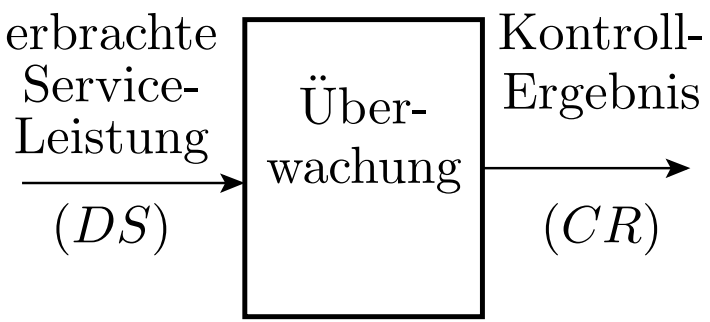
Iteration aus Überwachung, Problembeseitigung und Erfolgskontrolle.

- 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



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

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

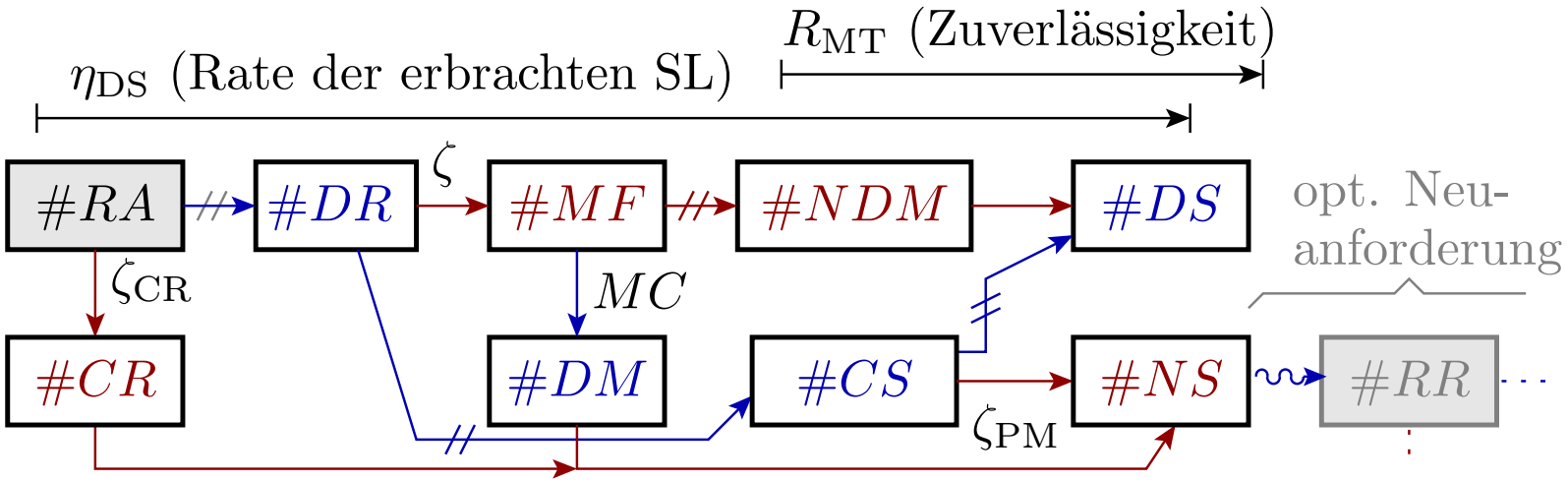
$$MC = \left.\frac{\#DM}{\#MF}\right|_{\text{ACR}} \tag{1.20}$$

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

$$\zeta_{\text{PM}} = \left.\frac{\#PM}{\#CS}\right|_{\text{ACR}} \tag{1.21}$$

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.

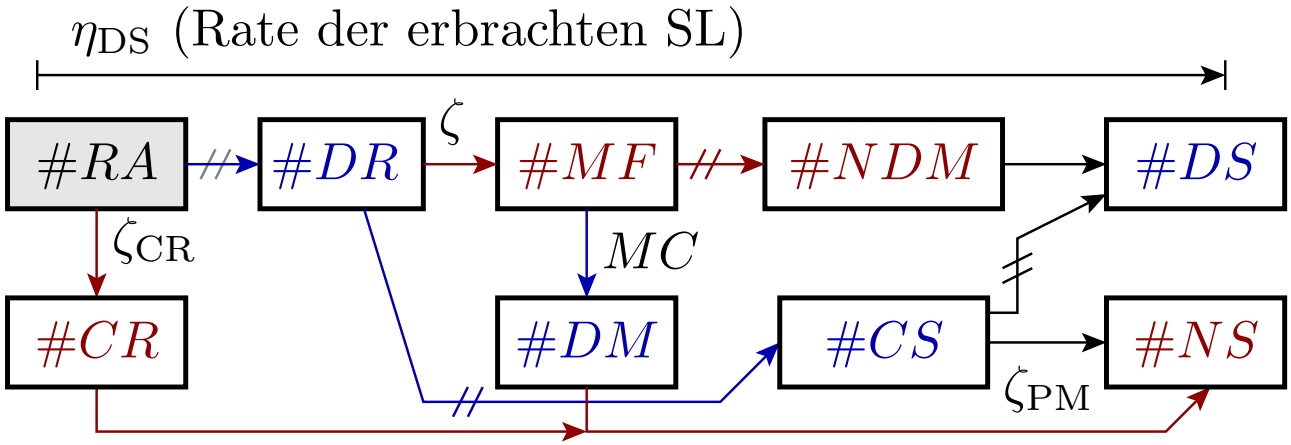
Anpassung Zählwertzuordnungsgraph



- 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



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

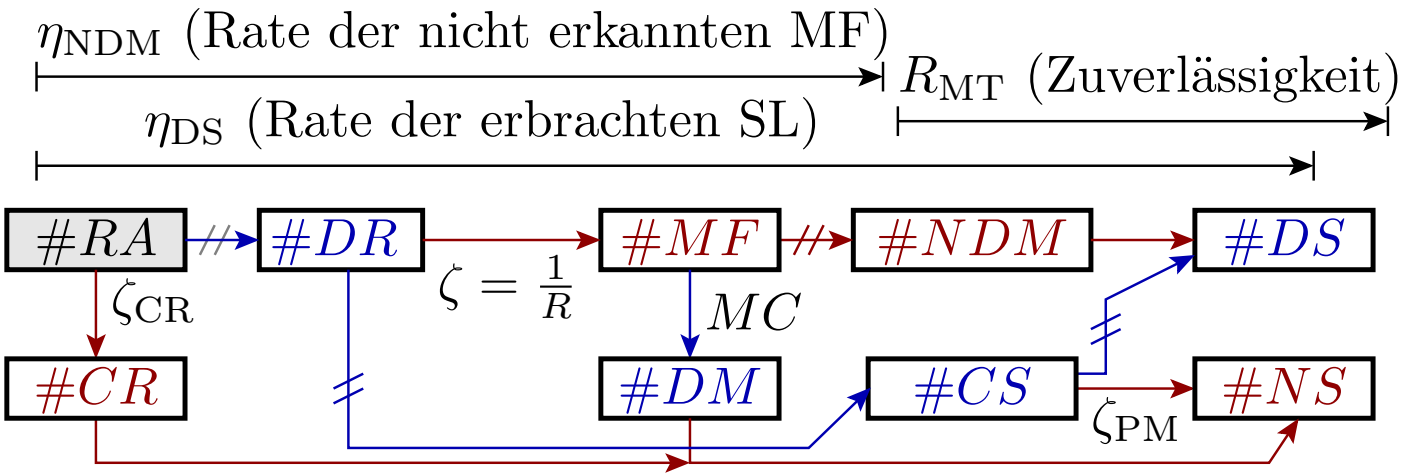
$$= (1-\zeta_{\mathrm{CR}})\cdot(1-\zeta_{\mathrm{SMF}}) \quad \text{mit } \zeta_{\mathrm{SMF}} = \zeta_{\mathrm{PM}} + \zeta\cdot MC - \zeta\cdot\zeta_{\mathrm{PM}} \qquad (1.22)$$

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

$$\eta_{\mathrm{DS}} = 1 - \zeta_{\mathrm{CR}} - \zeta_{\mathrm{PM}} - \zeta\cdot MC \qquad (1.23)$$

MC, ζ_{PM} Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.
MC, ζ_{PM} Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.
ζ_{SMF} Rate der signalisierten Fehlfunktionen.

Zuverlässigkeit ohne Neuanforderung



$$\eta_{\mathrm{NDM}} = \left.\frac{\#NDM}{\#RA}\right|_{\mathrm{ACR}} = (1-\zeta_{\mathrm{CR}})\cdot\zeta\cdot(1-MC) \tag{1.24}$$

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

$$= \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)}\cdot R \;\text{ mit }\zeta_{\mathrm{SMF}} = \zeta_{\mathrm{PM}} + \zeta\cdot MC - \zeta\cdot\zeta_{\mathrm{PM}} \tag{1.25}$$

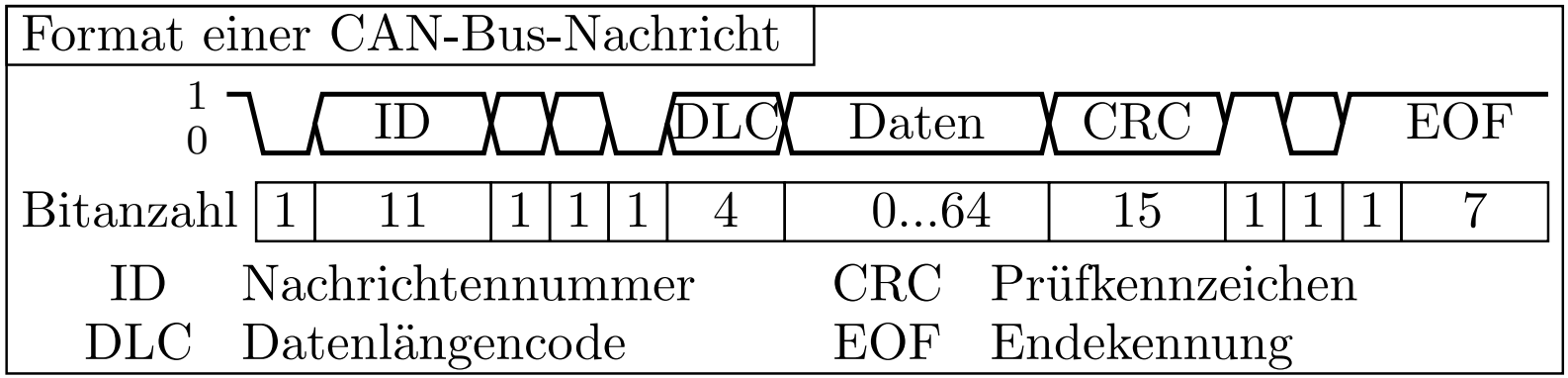
Für geringe Rate signalisierter Fehlfunktionen $\zeta_{\mathrm{SMF}} \to 0$:

$$R_{\mathrm{MT}} = \frac{R}{(1-MC)} \tag{1.26}$$

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.

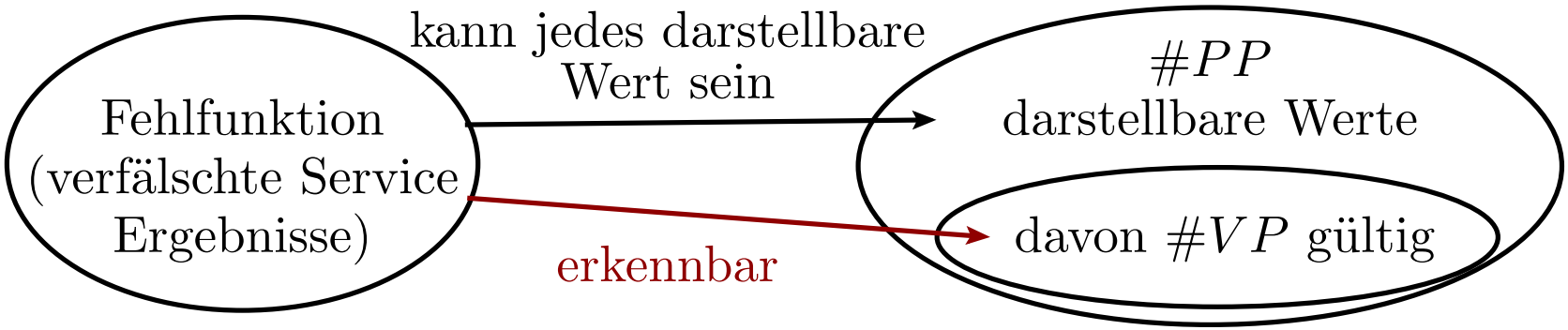
Einteilung Überwachungsverfahren für digitale Service-Leistungen:

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:

$$MC = 1 - \frac{\#VP}{\#PP} \tag{1.27}$$

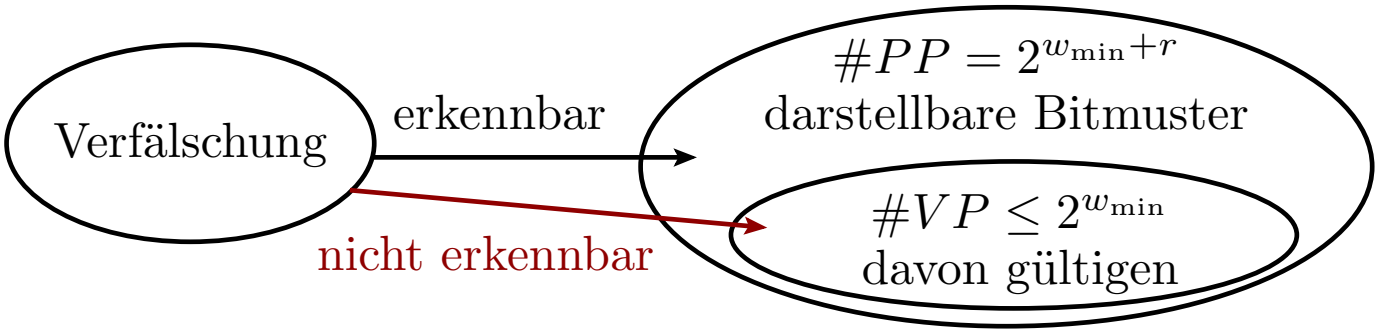
$$\zeta_{\mathrm{PM}} = 0 \tag{1.28}$$

$\#VP$	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:

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



$$MC = 1 - \frac{\#VP}{\#PP} \geq 1 - \frac{2^{w_{\min}}}{2^{w_{\min}+r}} = 1 - 2^{-r} \tag{1.29}$$

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

MC	Fehlfunktionsabdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
$\#VP$	Anzahl der gültigen Bitmuster (Number of valid bit patterns).
$\#PP$	Anzahl der darstellbaren Bitmuster (Number of presentable bit patterns).
r	Anzahl der redundanten Bits.

Ideale und reale Formatkontrollen

Zuverlässigkeit bei idealer Formatkontrolle mit r redundanten Bits, geringer Rate signalisierter Fehlfunktionen, ohne Neuanforderung (Gl. 1.26):

$$R_{\mathrm{MT}} = \frac{R}{(1-MC)} = \frac{R}{1-(1-2^{-r})} = 2^r \cdot R \qquad (1.30)$$

Das Idealverhalten *»gleichmäßiger Abbildung der Verfälschungen auf mögliche Werte und Nachweis aller unzulässigen Werte«* hat man in der Praxis hauptsächlich bei der Übertragung und Speicherung mit fehlererkennenden Codes oder 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, ...

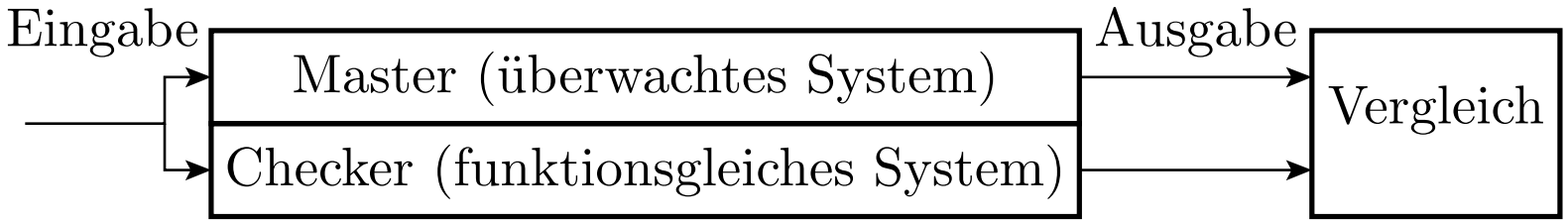
haben in der Regel wesentlich geringere Fehlfunktionsabdeckung, aber dennoch ein sehr gutes Aufwand-Nutzen-Verhältnis.

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

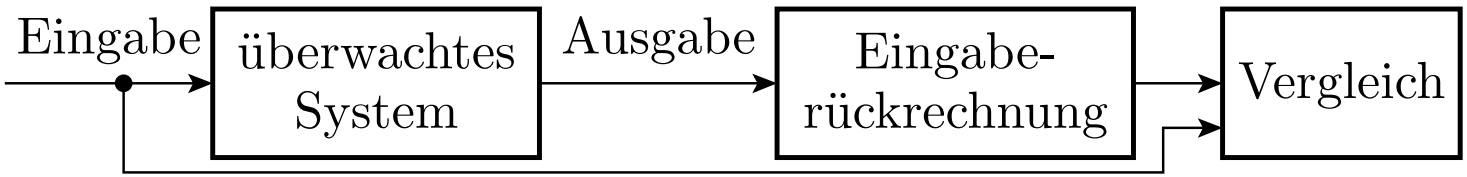
Wertekontrollen

Kontrollverfahren für Werte

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

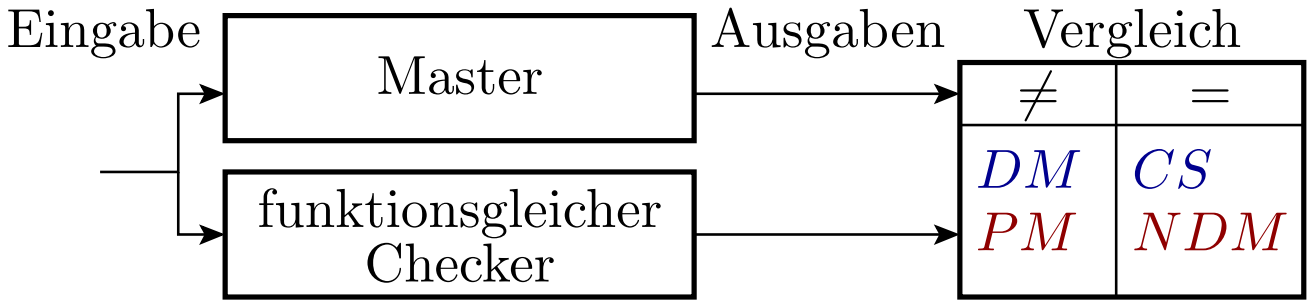


- Loop-Test (Eingaberückberechnung und Vergleich), z.B. Überwachung Versenden durch Empfang und Vergleich der empfangenen mit den Sendedaten. Nur für umkehrbar eindeutige Funktionen.



- 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):

$$MC = \frac{\#DM}{\#MF}\Big|_{\mathrm{ACR}} = \eta_{\mathrm{Div}} \tag{1.31}$$

und die Phantom-Fehlfunktionsrate ist die Rate der nicht diversitären Checker-Fehlfunktionen (Checker-MF bei bei nicht gleichzeitiger Master-MF):

$$\zeta_{\mathrm{PM}} = \eta_{\mathrm{Div}} \cdot \zeta_{\mathrm{Chk}} \tag{1.32}$$

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.

Folie 1.82: Eigenschaften von Master-Checker-Systemen.

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.

Folie 1.83: Diversität.

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.

Folie 1.85: Erweiterte Diversität.

Fehlerumgehung

Lösung derselben Aufgabe mit geänderter Service-Anforderung, geänderten Daten, ...

Komplexe IT-Systeme bieten oft viele Lösungswege für eine Aufgabe, die nicht alle funktionieren. 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.

In der Regel nicht für Mehrfachberechnung und Vergleich geeignet, weil

- oft abweichende korrekte Ergebnisse (Vergleichsfehler) und
- damit Phantom-Fehlfunktionen.

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, ...

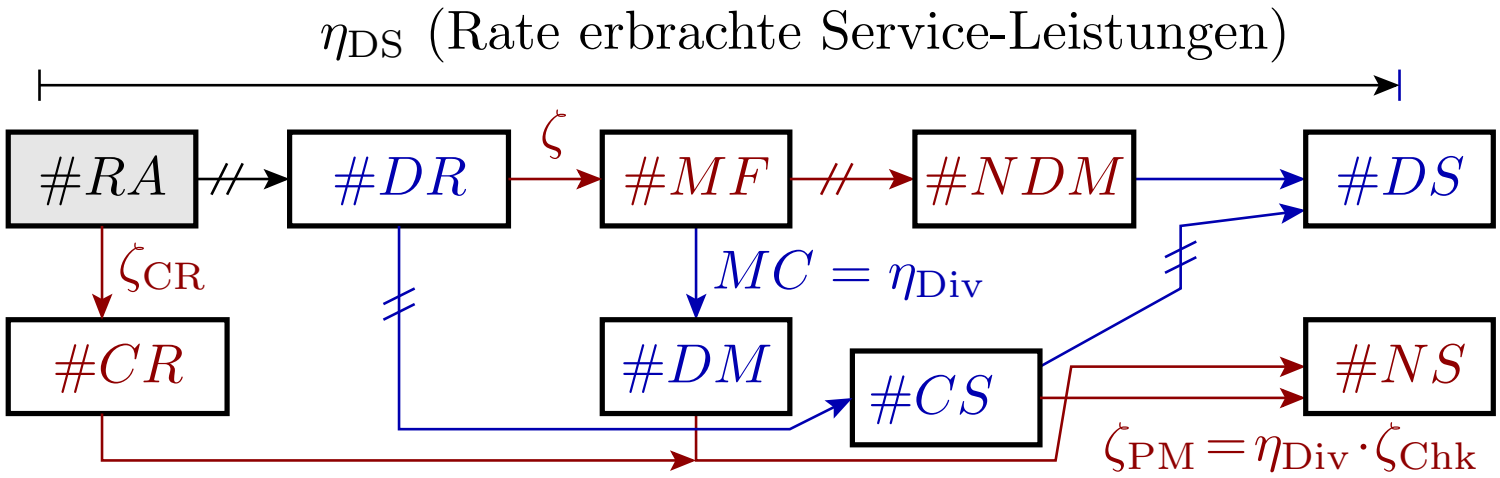
Die ursprüngliche euphorische Meinung, dass so Diversität gegenüber allen Fehlern, außer denen in der Spezifikation erzielbar ist, nicht bestätigt. Die direkte oder indirekte Kommunikation der Entwicklungsteams über die Interpretation der Spezifikation, während des Test etc. trägt Gemeinsamkeiten in die Entwürfe. Neigung von Menschen, gewisse Fehler zu wiederholen*, ... $\eta_{\mathrm{Div}} \leq 90\%$, nach Gl. 1.31:

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

Eine Kontrolle mit $r = 10$ Bit Informationsredundanz erreicht nach Gl. 1.29 $MC \geq 99{,}9\%$ 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:

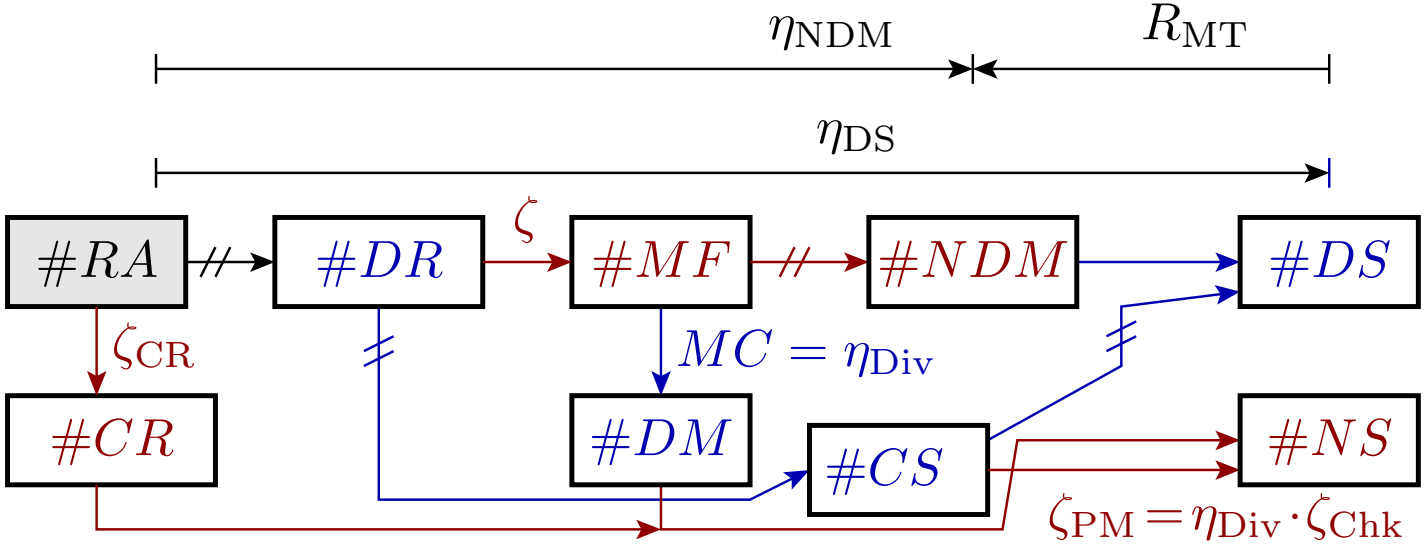
$$\eta_{\mathrm{DS}} = (1 - \zeta_{\mathrm{CR}}) \cdot (1 - \zeta_{\mathrm{PM}} - \zeta \cdot MC + \zeta \cdot \zeta_{\mathrm{PM}}) \tag{1.22}$$

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

$$\eta_{\mathrm{DS}} = (1 - \zeta_{\mathrm{CR}}) \cdot (1 - \eta_{\mathrm{Div}} \cdot (\zeta + \zeta_{\mathrm{Chk}} - \zeta \cdot \zeta_{\mathrm{Chk}})) \tag{1.33}$$

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

Zuverlässigkeit von Master-Checker-Systemen



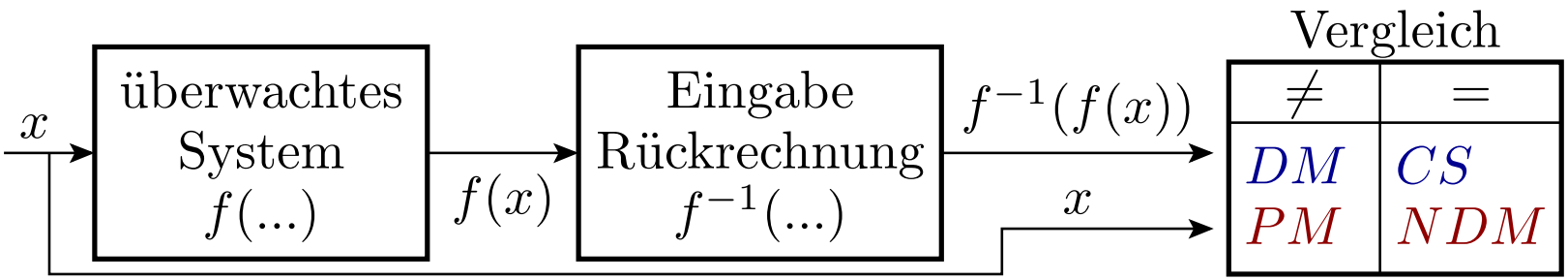
$$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R \text{ mit } \zeta_{\mathrm{SMF}} = \zeta_{\mathrm{PM}} + \zeta \cdot MC - \zeta \cdot \zeta_{\mathrm{PM}} \quad (1.25)$$

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

$$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-\eta_{\mathrm{Div}})} \cdot R \text{ mit } \zeta_{\mathrm{SMF}} = \eta_{\mathrm{Div}} \cdot (\zeta + \zeta_{\mathrm{Chk}} - \zeta \cdot \zeta_{\mathrm{Chk}}) \quad (1.34)$$

$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
ζ_{SMF}	Rate der signalisierten Fehlfunktionen.
$\zeta_{\mathrm{CR}}, \zeta$	Absturzrate, Fehlfunktionsrate.
MC, ζ_{PM}	Fehlfunktionsabdeckung, Phantomfehlfunktionsrate.

Eigenschaften Loop-Test

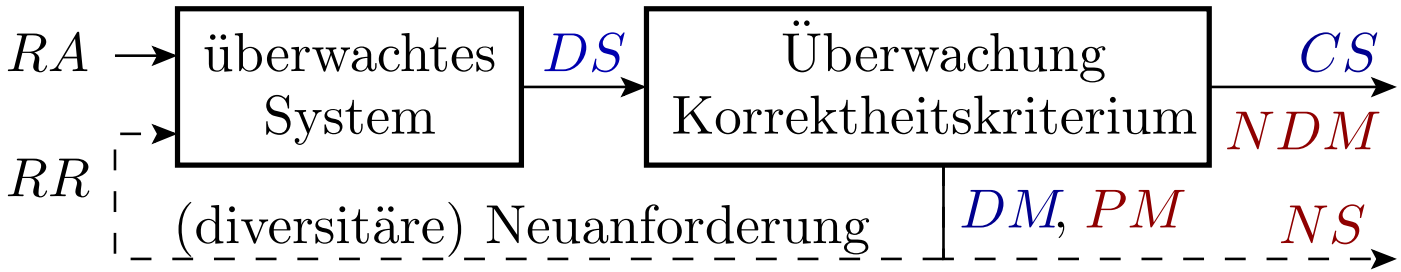


Da $f(\ldots)$ und $f^{-1}(\ldots)$ sich in Algorithmus und Fehlerwirkung unterscheiden, ist auch ohne zusätzliche konstruktive und organisatorische Maßnahmen eines höheres Maß an Verschiedenartigkeit der Wirkung von Fehlern und damit eine höhere MC zu erwarten.

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

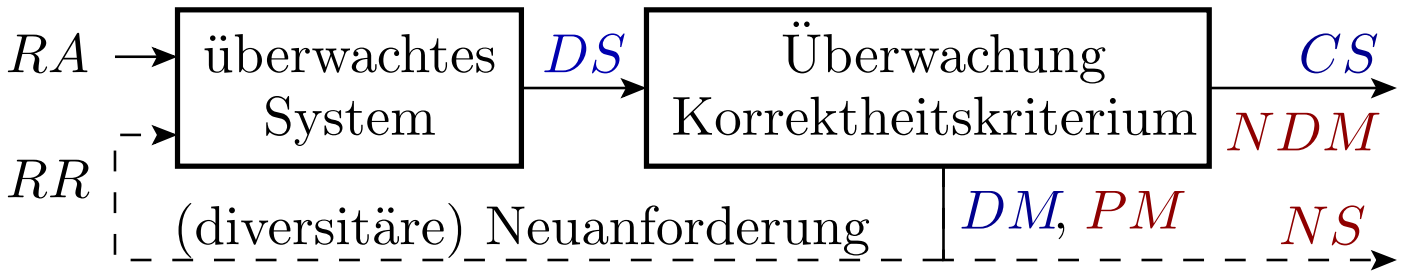


Wenn es eine aufgabenspezifische Kontrollmöglichkeit gibt, Korrektheit nachzuweisen:

- 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.



Der typische Suchalgorithmus:

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

entspricht einer MF-Behandlung *»Wiederholung nach Fehlfunktion bis MF nicht mehr nachweisbar«* mit einer hohen Rate signalisierter Fehlfunktionen bzw. Wiederholversuchen $\zeta_{\mathrm{SMF}} \to 1$.
Zuverlässigkeitsverbesserung

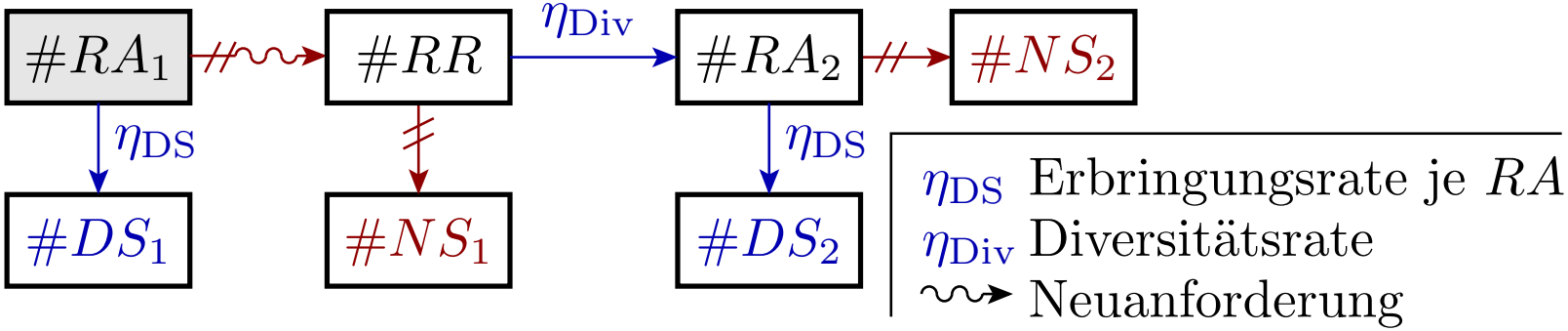
$$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R \tag{1.25}$$

viel kleiner als der Kehrwert des Anteils der nicht nachweisbaren MF der Kontrolle.

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

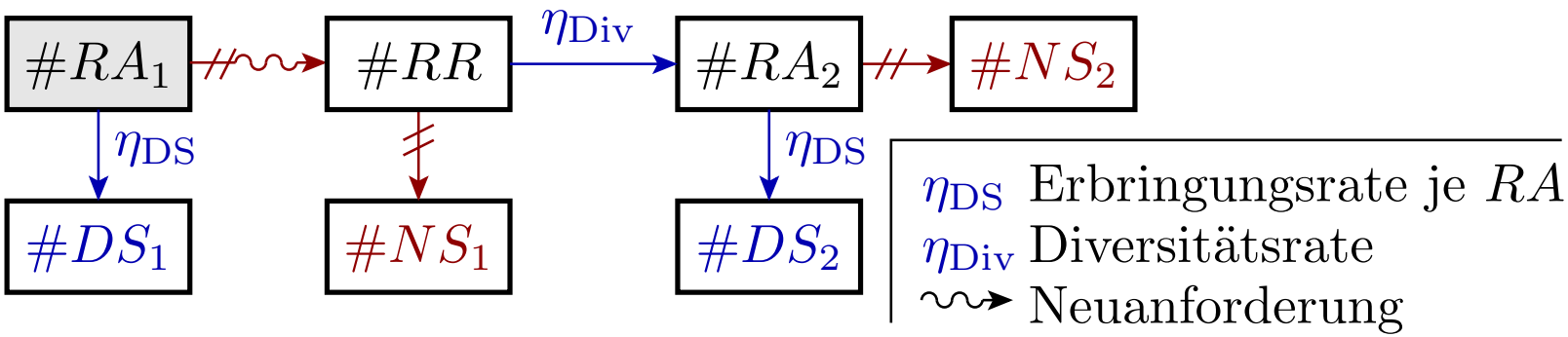
Neuanforderung

Erbringungsrate bei max. einer Neuanforderung



- Nach akzeptierter Erstanforderung (RA_1) Erbringung mit η_{DS} (DS_1), sonst Neuanforderung bis Anforderung akzeptiert (RR).
- Nach RR mit Rate $1 - \eta_{\text{Div}}$ identisches Problem und Abbruch ohne erbrachtes Ergebnis (NS_1), sonst diversitäre Neuanforderungsergebnis (RA_2).
- RA_2 mit Rate η_{DS} erbrachtes Ergebnis (DS_2), sonst Abbruch ohne Ergebnis (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.



Erbringungsrate für max. eine Neuanforderung insgesamt:

$$\eta_{\mathrm{DS.SR}} = \left.\frac{\#DS_1+\#DS_2}{\#RA_1}\right|_{\mathrm{ACR}} = \eta_{\mathrm{DS}} + (1-\eta_{\mathrm{DS}}) \cdot \eta_{\mathrm{Div}} \cdot \eta_{\mathrm{DS}} \tag{1.35}$$

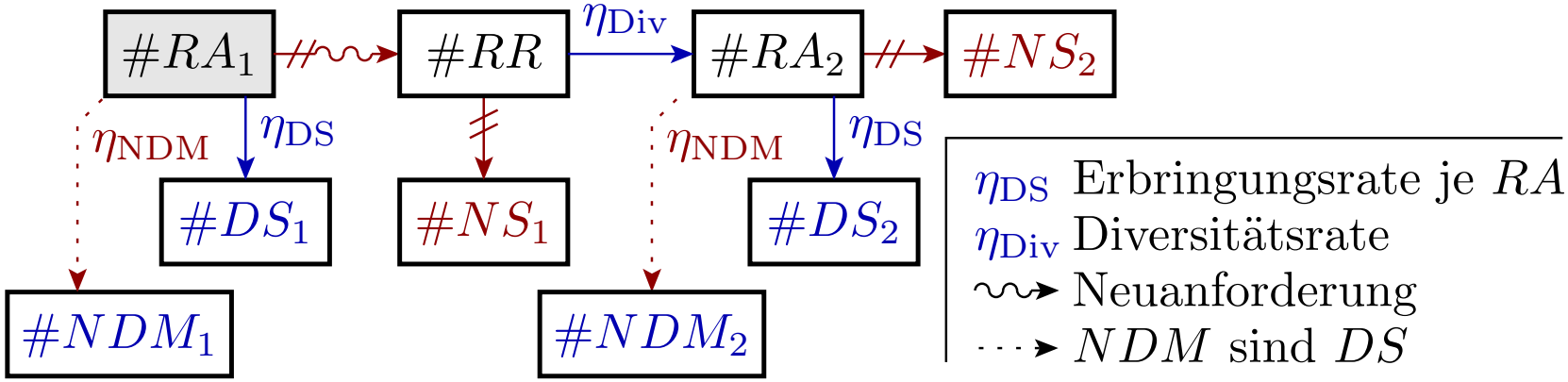
Für hohe Erbringungsraten $\eta_{\mathrm{DS}} \to 1$:

$$\eta_{\mathrm{DS.SR}} = 1 - (1-\eta_{\mathrm{DS}}) \cdot (1-\eta_{\mathrm{Div}}) \tag{1.36}$$

verringert bereits eine Wiederholung den Anteil der nicht erbrachten Leistungen auf den nicht diversitären Anteil. Nicht diversitäre Probleme (Abstürze, nachweisbare Fehlfunktionen und Phantomfehlfunktionen) auch durch weitere Wiederholversuche nicht erbringbar.

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

Zuverlässigkeit bei max. einer Neuanforderung



Bei akzeptierter Erstanforderung (RA_1) und akzeptierter diversitäre Neuanforderungen (RA_2) ist im Anteil der erbrachten Leistungen η_{DS} ein Anteil von nicht erkannte Fehlfunktionen enthalten:

$$\eta_{\mathrm{NDM}} = (1 - \zeta_{\mathrm{CR}}) \cdot \zeta \cdot (1 - MC) \tag{1.24}$$

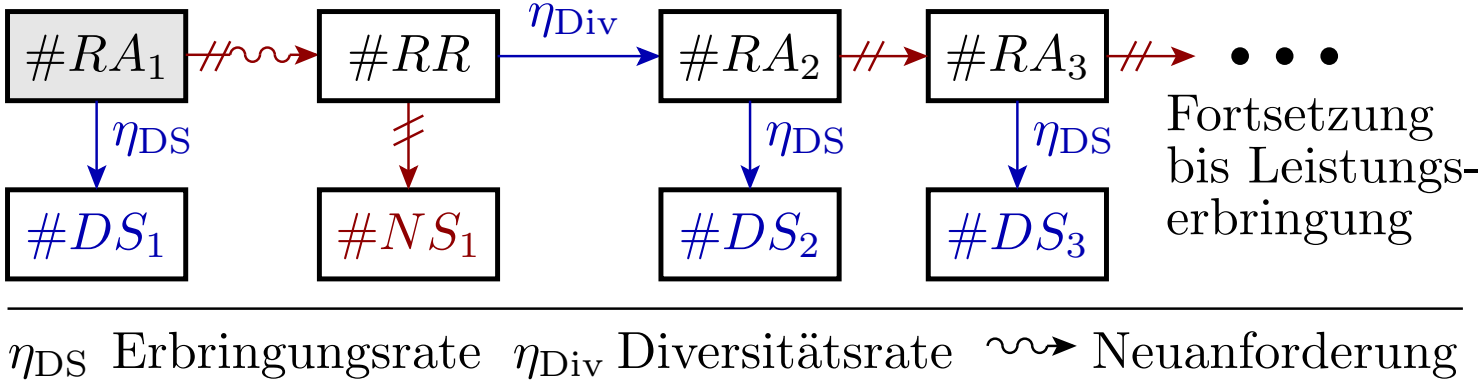
Dieselbe Zuverlässigkeit wie ohne Neuanforderung (Gl. 1.25):

$$R_{\mathrm{MT}} = \left.\frac{\#DS_1 + \#DS_2}{\#NDM_1 + \#NDM_2}\right|_{\mathrm{ACR}} = \frac{\eta_{\mathrm{NDM}}}{\eta_{\mathrm{DS}}}$$

$$= \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R \;\text{ mit } \zeta_{\mathrm{SMF}} = \zeta_{\mathrm{PM}} + \zeta \cdot MC + \zeta \cdot \zeta_{\mathrm{PM}}$$

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

Wiederholung bis Erbringung



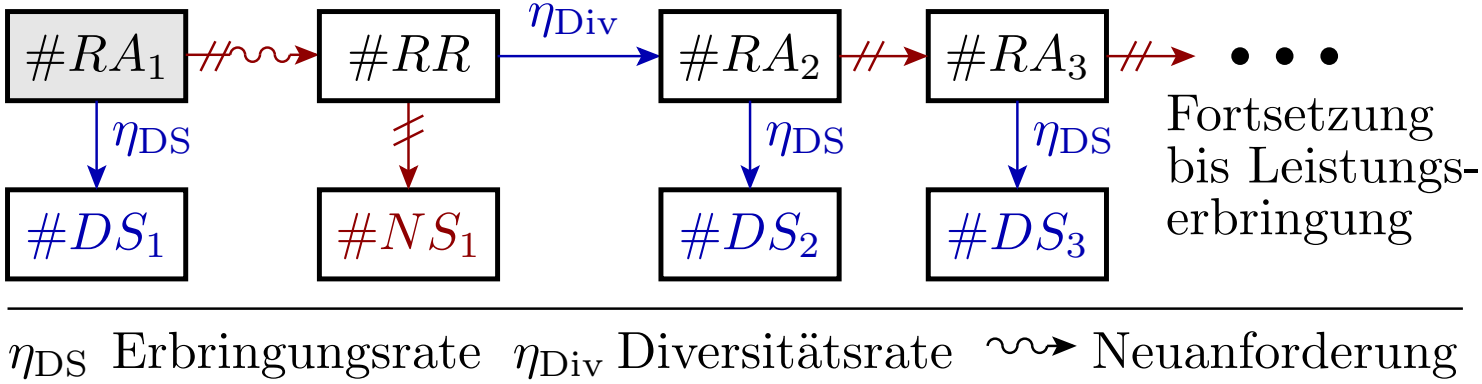
Anteil der mit jeder Wiederholung zusätzlich erbrachten Leistungen nimmt nach einer geometrischen Reihe ab

$$\left.\frac{\#DS_i}{\#RA_1}\right|_{\mathrm{ACR}} = \eta_{\mathrm{Div}} \cdot \eta_{\mathrm{DS}}^{i} \quad \text{für } i \geq 2$$

und strebt gegen null. Iterationsabbruch, erst wenn alle diversitären Probleme (Abstürze, erkannte MF und Phantom-MF) toleriert sind.

RA_1, DS_1	Akzeptierte Erstanforderung, erbrachte Service-Leistung nach Erstanforderung.
RR, NS_1	Neuanforderung, Abbruch ohne Service-Leistung nach Erstanforderung.
RA_i, DS_i	Akzeptierte Neuanforderung i, erbrachte Service-Leistung nach Neuanforderung i.
η_{DS}, η_{Div}	Erbringungsrate je Anforderung, Diversitätsrate.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

Erbringungsrate bei Wiederholung bis Erfolg

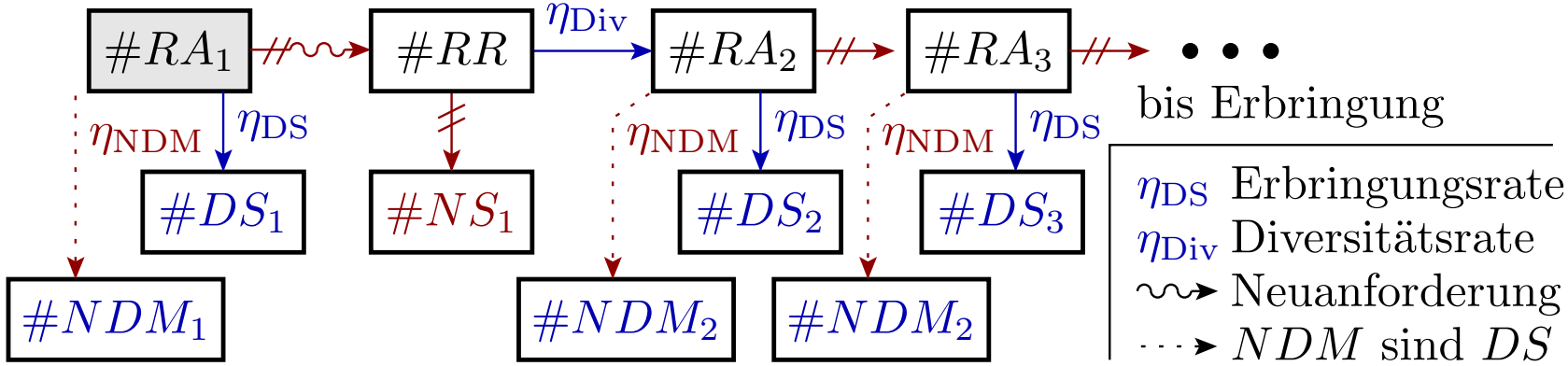


$$\eta_{\mathrm{DS.MR}} = \left.\frac{\sum_{i=1}^{\infty} \#DS_i}{\#RA_1}\right|_{\mathrm{ACR}} = 1 - \left.\frac{NS_1}{\#RA_1}\right|_{\mathrm{ACR}}$$
$$= 1 - (1 - \eta_{\mathrm{DS}}) \cdot (1 - \eta_{\mathrm{Div}}) \qquad (1.37)$$

Wie bei hoher Erbringungsrate und max. einer Wiederholung werden alle Leistungen mit diversitären Problemen (Abstürze, erkannte Fehlfunktionen) erbracht. Nicht diversitäre Probleme generell nicht durch identische Wiederholung behebbar.

$\eta_{\mathrm{DS.MR}}$	Erbringungsrate bei Wiederholung nach diverstären Problemen bis Erbringung.
RA_1, DS_i	Akzeptierte Erstanforderung, erbrachte Service-Leistung nach Anforderung i.
η_{DS}, η_{Div}	Erbringungsrate je Anforderung, Diversitätsrate.

Zuverlässigkeit bei Wiederholung bis Erbringung



Auch bei Mehrfachwiederholung enthalten alle erbrachten Leistungen (DS_i) denselben Anteil nicht erkennbare Fehlfunktionen.
Zuverlässigkeit gleichfalls wie ohne Neuanforderung (Gl. 1.25):

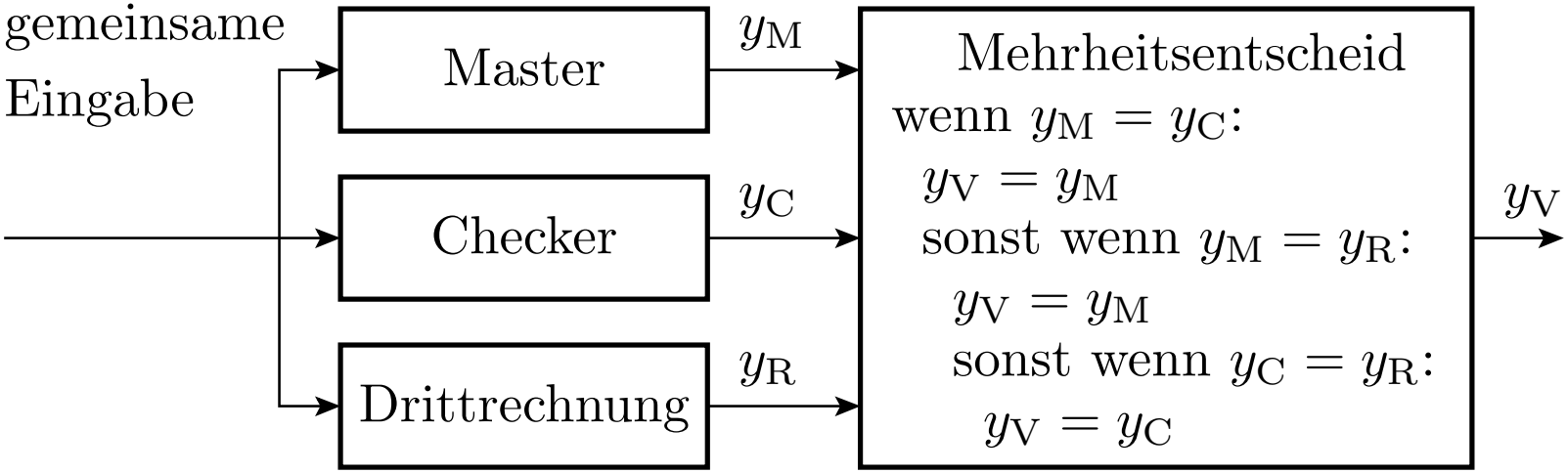
$$R_{\mathrm{MT}} = \left.\frac{\sum_{i=1}^{\infty} \#DS_i}{\sum_{i=1}^{\infty} \#NDM_i}\right|_{\mathrm{ACR}} = \frac{\eta_{\mathrm{NDM}}}{\eta_{\mathrm{DS}}}$$

$$= \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R \quad \text{mit } \zeta_{\mathrm{SMF}} = \zeta_{\mathrm{PM}} + \zeta \cdot MC - \zeta \cdot \zeta_{\mathrm{PM}}$$

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.
ζ_{SMF}	Rate der signalisierten Fehlfunktionen.

Mehrheitsentscheid

Dreifachberechnung und Mehrheitsentscheid



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

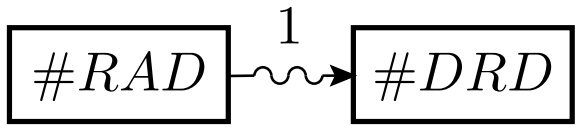
Bei Erbringung von mindestens zwei gleichen Ergebnissen, Ausgabe des übereinstimmenden Ergebnisses, sonst kein Ergebnis.

CVA-Graph mit Wiederhol. bei Nichterbringung wegen Abhängigkeiten zwischen MF-Nachweis und Diversität der Neuberechnung ungeeignet.

y_M, y_C Master-Ergebnis, Checker-Ergebnis.
y_R, y_V Ergebnis der Drittrechnung, Mehrheitsergebnis.

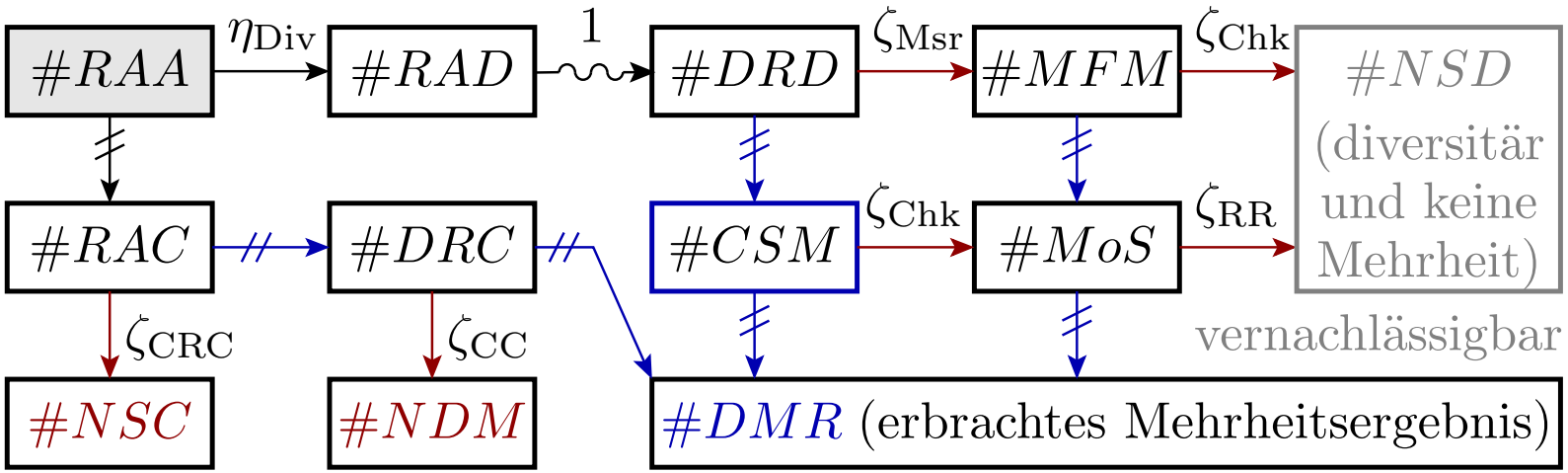
Annahmen zur Vereinfachung:

- 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.

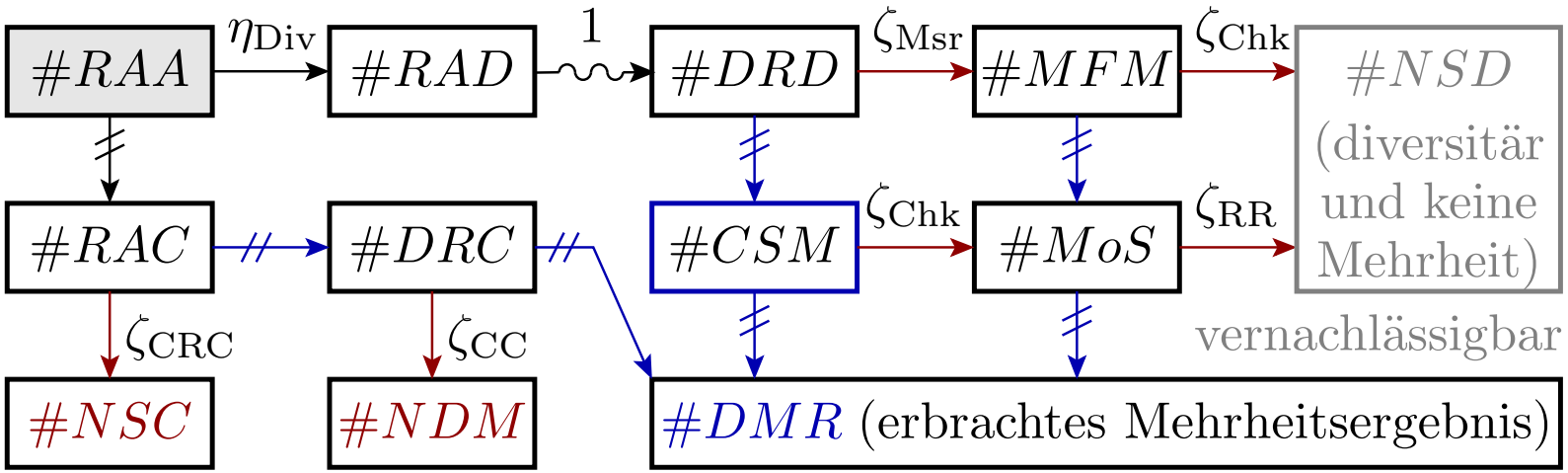


η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
$\#RAD$	Alle drei Anforderungen akzeptiert, mögliche Probleme haben diversitäre Ursachen.
$\#DRD$	Alle drei Ergebnis erbracht, mögliche Fehlfunktionen haben diversitäre Ursachen.

CVA-Graph



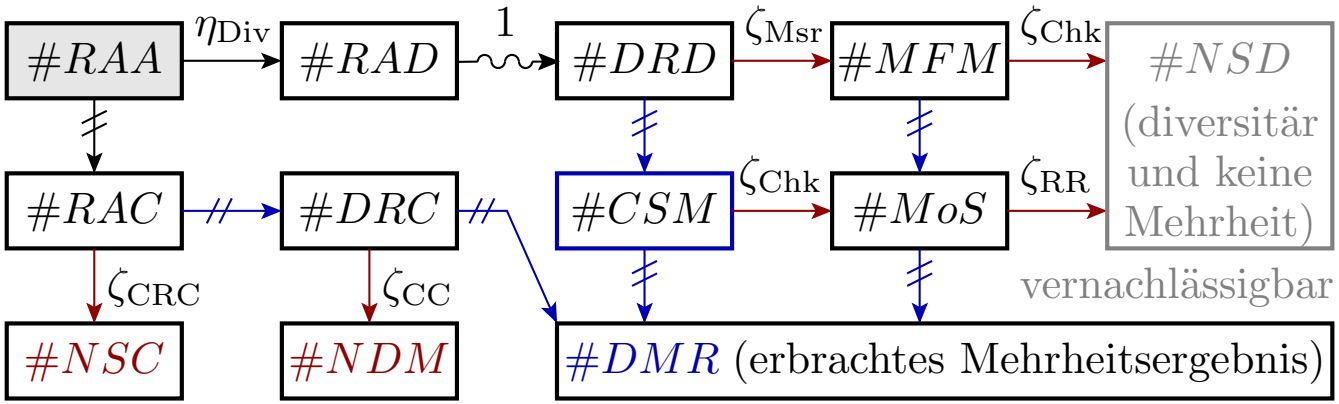
$\#RAA$	Alle drei Service-Anforderungen akzeptiert.
$\#RAC$	Alle drei Anforderungen akzeptiert, mögliche Probleme haben gemeinsame Ursache.
$\#RAD$	Alle drei Anforderungen akzeptiert, mögliche Probleme haben diversitäre Ursachen.
$\#DRC$	Alle drei Ergebnis erbracht, mögliche Fehlfunktionen haben gemeinsame Ursachen.
$\#DRD$	Alle drei Ergebnis erbracht, mögliche Fehlfunktionen haben diversitäre Ursachen.
$\#CSM$	Korrektes Service-Ergebnis Master.
$\#MFM$	Fehlfunktion Master.
$\#MoS$	Korrekte Service-Leistung von Master- oder Slave, aber nicht von beiden.
η_{Div}	Diversitätsrate, Anteil der nicht übereinstimmenden MF bei Mehrfachberechnung.
ζ_{CRC}	Rate gleichzeitiger Abstürze durch dieselbe Ursache.
ζ_{CC}	Rate identischer Fehlfunktionen durch dieselbe Ursache.



- 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, Zählwertaufteilung wie Einzelsystem.
- Für akzeptiere Anforderung und nur diversitäre Probleme (RAD) ab zwei korrekten Ergebnissen »erbrachtes Mehrheitsergebnis (DMR)« und ab zwei Fehlfunktionen kein Ergebnis (NSD).

ζ_{M} Rate diversiärer Master-Fehlfunktionenen.
ζ_{C} Rate diversiärer Checker-Fehlfunktionenen.
ζ_{R} Rate diversiärer Neuanforderungs-Fehlfunktionenen.

Erbringungsrate



Nicht erbracht werden

- gleichzeitige Abstürze durch gemeinsame Ursachen (NSC):

$$\eta_{\mathrm{DS.CC}} = 1 - (1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{CRC}}$$

- oder ≥ 2 zufällig gleichzeitig verfälsche Ergebnisse (NSD):

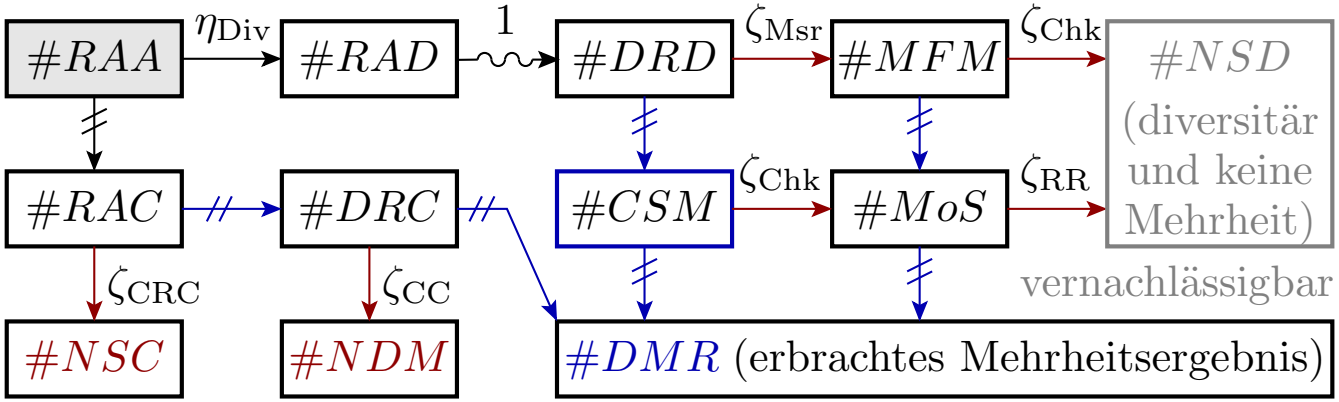
$$\eta_{\mathrm{DS.Div}} = \eta_{\mathrm{Div}} \cdot (\zeta_{\mathrm{M}} \cdot \zeta_{\mathrm{C}} + ((1 - \zeta_{\mathrm{M}}) \cdot \zeta_{\mathrm{C}} + \zeta_{\mathrm{M}} \cdot (1 - \zeta_{\mathrm{C}})) \cdot \zeta_{\mathrm{R}})$$

Erbringungsrate für kleine Problemraten ($\zeta_{\mathrm{M}} \to 0$, $\zeta_{\mathrm{C}} \to 0$ und $\zeta_{\mathrm{R}} \to 0$):

$$\eta_{\mathrm{DS.MV}} = 1 - (1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{CRC}} \tag{1.38}$$

ζ_{CRC} Rate gleichzeitiger Abstürze durch dieselbe Ursache.

Zuverlässigkeit



Nicht erkannt werden praktisch nur MF durch gemeinsame Ursachen:

$$\eta_{\mathrm{NDM}} = (1-\eta_{\mathrm{Div}}) \cdot (1-\zeta_{\mathrm{CRC}}) \cdot \zeta_{\mathrm{CC}}$$

Zuverlässigkeit:

$$R_{\mathrm{MV}} = \frac{\eta_{\mathrm{DS}}}{\eta_{\mathrm{NDM}}} = \frac{1-(1-\eta_{\mathrm{Div}})\cdot\zeta_{\mathrm{CRC}}}{(1-\eta_{\mathrm{Div}})\cdot(1-\zeta_{\mathrm{CRC}})\cdot\zeta_{\mathrm{CC}}} \tag{1.39}$$

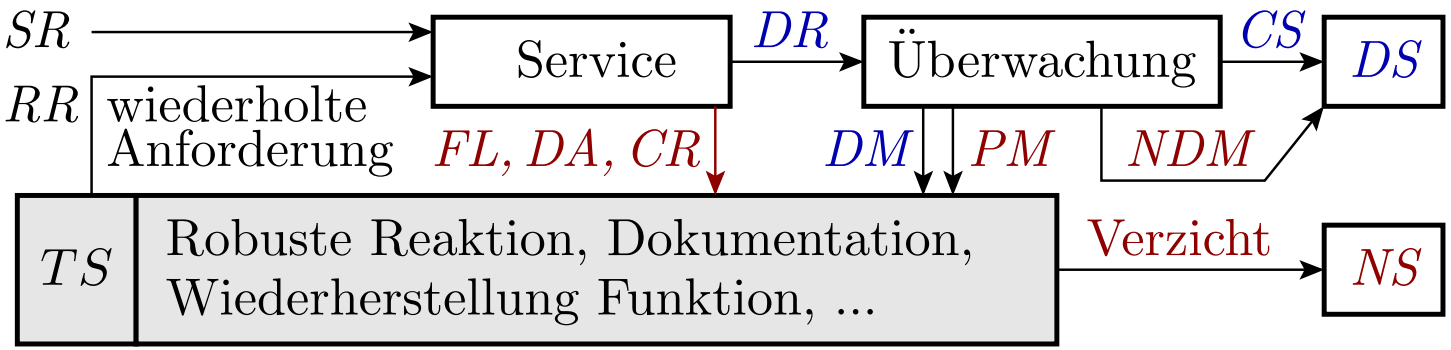
Vernachlässigung Common-Cause-Abstürze ($\zeta_{\mathrm{CRC}} \to 0$) und $\zeta_{\mathrm{M}} = \zeta_{\mathrm{CC}}$
Zuverlässigkeit wie Master-Checker ohne Wiederholung (Gl. 1.25):

$$R_{\mathrm{MV}}|_{\zeta_{\mathrm{CRC}}\to 0} = \frac{R}{(1-\eta_{\mathrm{Div}})} \tag{1.40}$$

R_{MV}, R Zuverässigkeit mit Mehrheitsentscheid, Zuverlässigkeit des Master ohne MT.

Reaktion ab Erkennung

Reaktion auf erkannte Probleme



Erkennbare Probleme während der Nutzung:

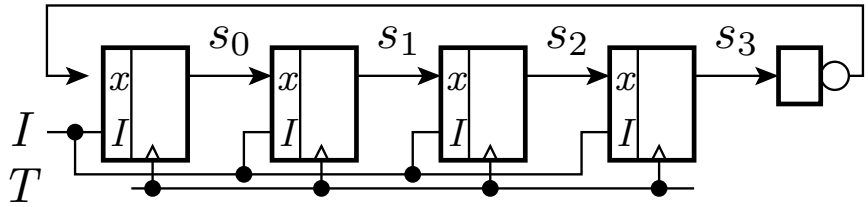
- Nichterbringung (NS): Hardware ausgefallen (FL), Service-Verweigerung (DA), Absturz (CR).
- Erkannte Fehlfunktion (DM).
- Phantomfehlfunktion (PM).

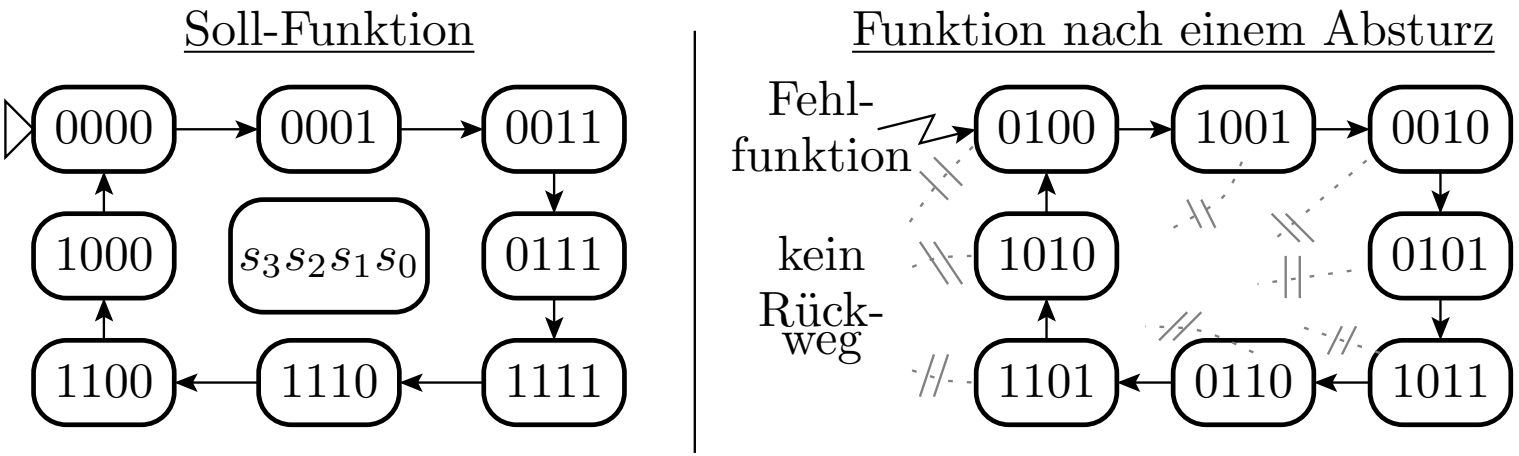
Mögliche Reaktionen darauf während des Betriebs:

- Abbruch mit Leistungsverzicht (NS),
- Wiederholung der Service-Anforderung (RR), ...

SR, RR	Service-Anforderung, Wiederholanforderung.
DR, CS	Erbrachtes Ergebnis, korrekte Service-Leistung.
NDM, PM	Nicht erkannte Fehlfunktion, Phantomfehlfunktion.

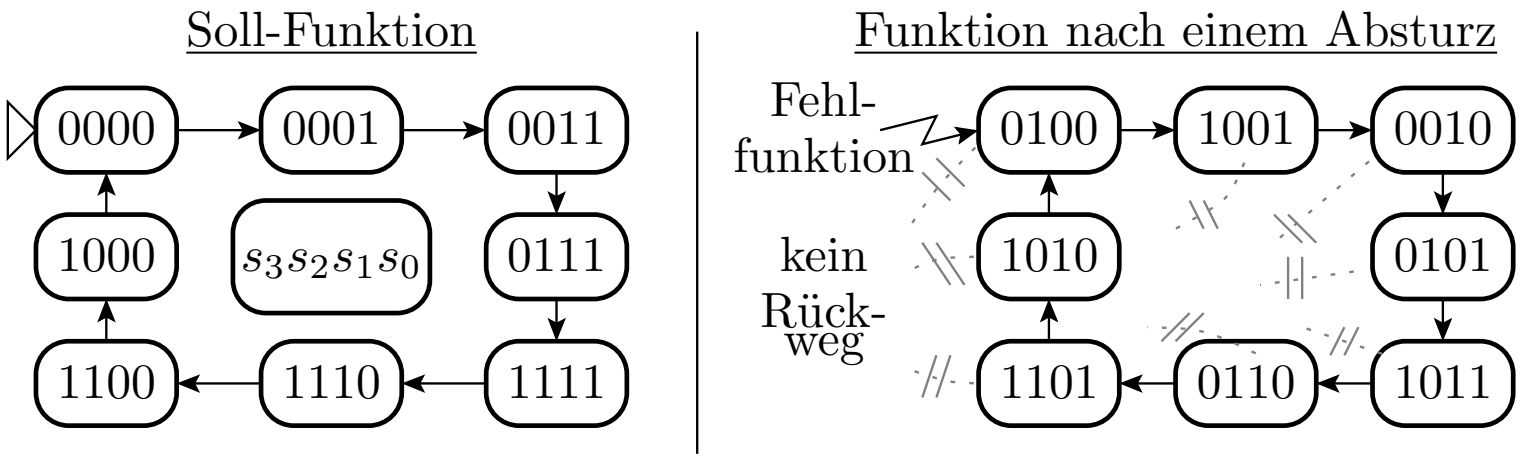
Absturz (Crash)





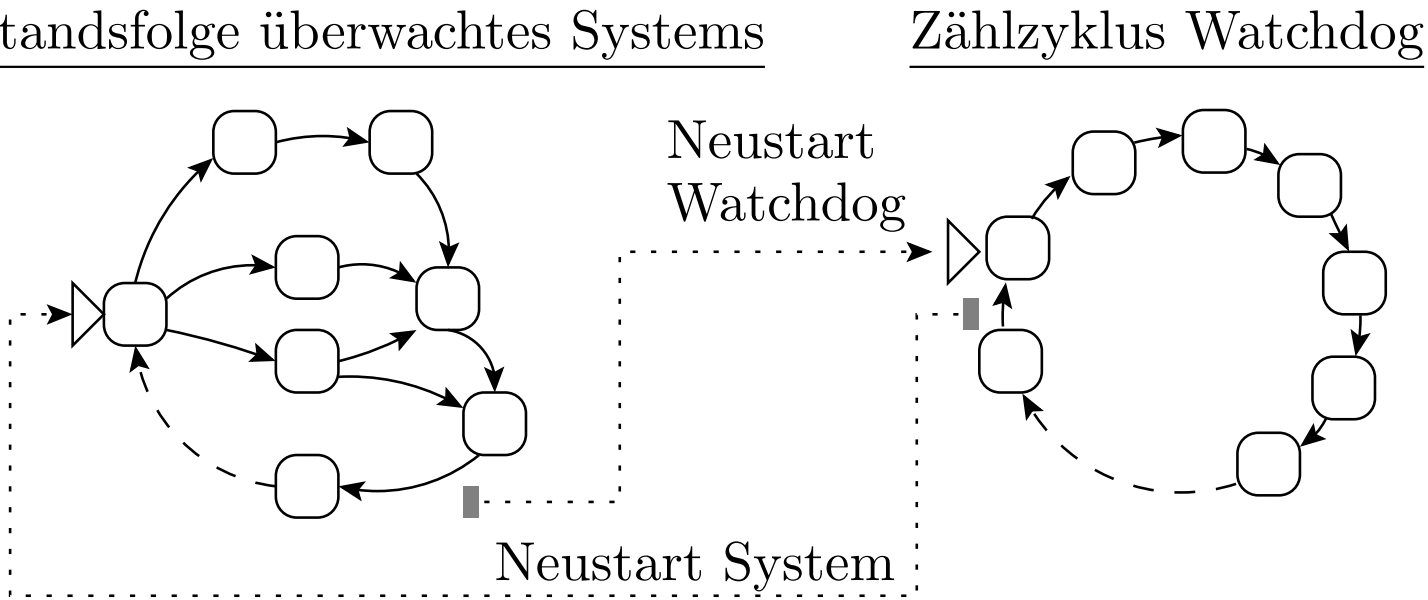
- Automaten und Programme nutzen nur einen kleinen Teil der $2^{\#SB}$ möglichen Zustände ($\#SB$ – Anzahl Zustandsbits).
- Der 4-Bit-Johnson-Zähler durchläuft zyklisch 8 der 16 Zustände.
- Die restlichen (redundanten) 8 Zustände bilden einen Zyklus, der nicht mehr verlassen wird.
- Der Übergang in unzulässige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

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



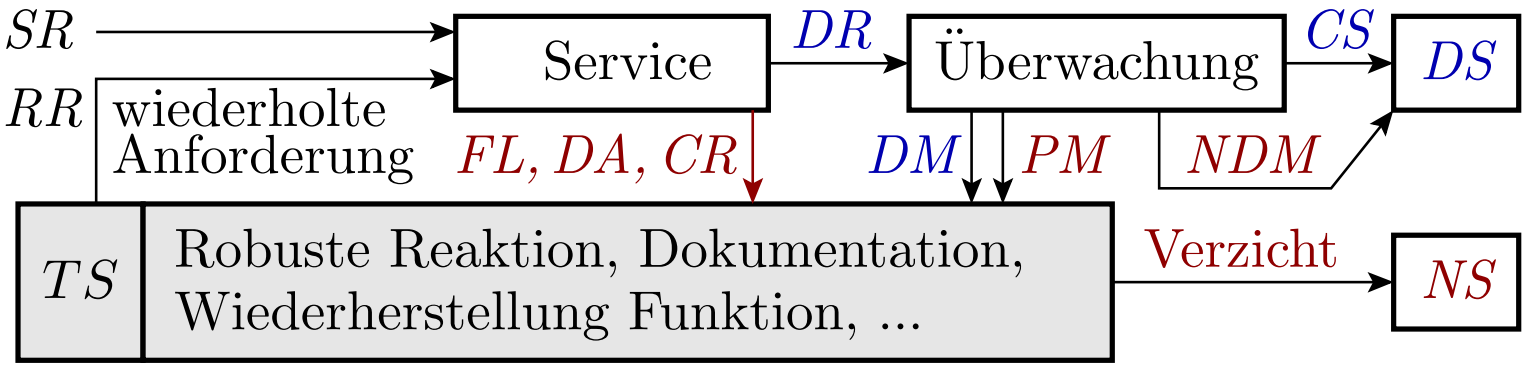
- Komplexer Hardware und Software hat Millionen von Zustandsbits und unüberschaubar viele Absturzmöglichkeiten.
- Ein Absturz (CR) ist daran zu erkennen, dass das System ab der letzten akzeptierte Service-Anforderung (SA) kein Ergebnis (DR) liefert und keine Anforderungen mehr akzeptiert.
- Der Umgang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

Fehlfunktionsbehandlung mehr im Detail



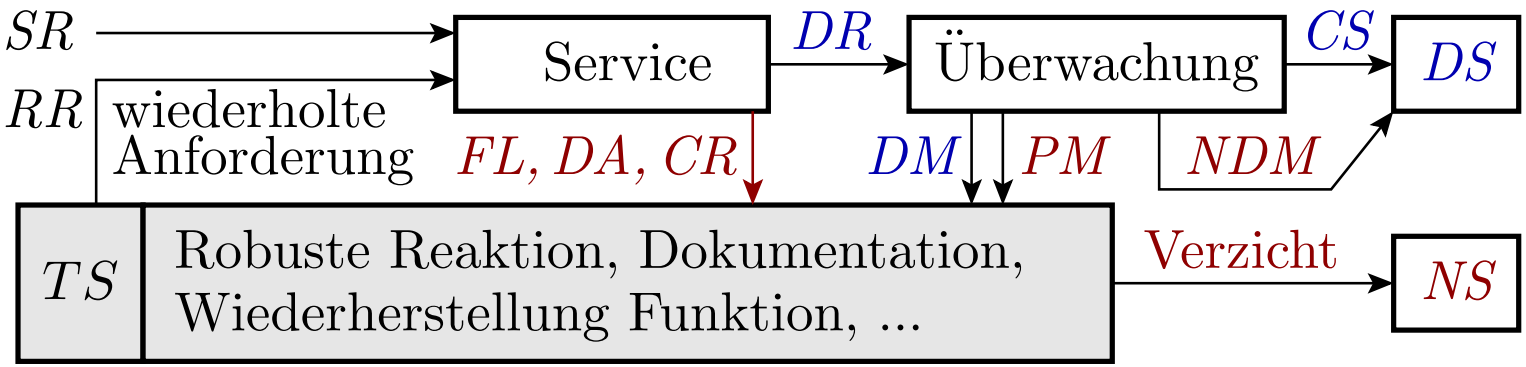
Robuste Reaktion zur Schadensvermeidung:

- Abbruch nach Zeitüberschreitung (Absturzprävention).
- Herstellen eines sicheren Zustands, ...

Dokumentation der Fehlfunktion:

- Fehlermeldung für den manuellen Umgang,
- Sichern von Daten für die spätere Fehlersuche: Core-Dump, Cap-Datei (Windows), ... (siehe Abschn. 2.2.5 *Reifeprozess*)

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.



Wiederherstellung Funktionsfähigkeit:

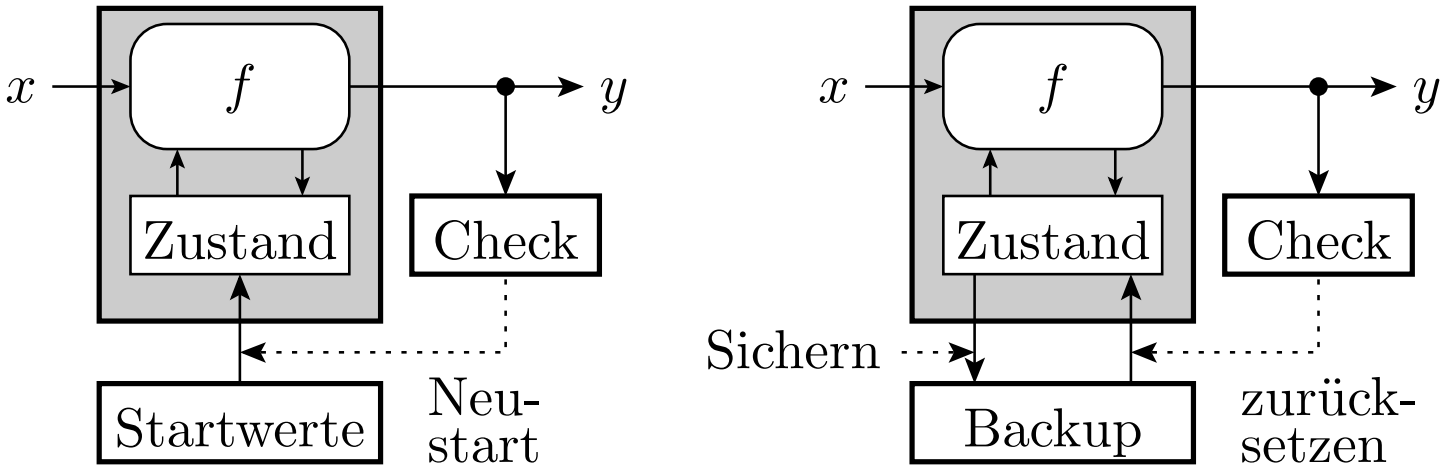
- Bei vermutetem Hardware-Ausfall Reparatur / Rekonfiguration,
- Auch ohne erkennbare Verfälschung interner Zustände in der Regel prophylaktische Neuinitialisierung.

Optionaler Tolerierungsversuch z.B. Wiederholanforderung (RR):

- Bei auch so ausreichender Verfügbarkeit nicht erforderlich.
- Sonst für $\zeta \ll 1$ genügt ein Wiederholversuch.
- Sonst* Wiederholung mit anderem System oder geänderter Service-Anforderung (siehe Folie 1.85 *Erweiterte Diversität*).

FL, DA Nichtverfügbarkeit wegen Hardware-Ausfall bzw. Annahmeverweigerung.
CR, TS Absturz, Problembehandlung (Troubleshooting).
* Bei übereinstimmender Entstehungsursache (gleicher Fehler) entsteht bei Wiederholung wieder dieselbe Fehlfunktion.

Statische und dynamische Neuinitialisierung



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

- Statische Neuinitialisierung (Reset): fester Anfangszustand,
- Dynamische Neuinitialisierung: Regelmäßiges Backup 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.

Korrektur durch Neuanforderung

Diversität erforderlich!

Bei übereinstimmender MF-Ursache liefert Wiederholung immer wieder dieselbe Fehlerfunktion.

Ausschluss von Fehlern, Hardware-Ausfällen, ... als gemeinsame Ursachen verlangt erweiterte Diversität (siehe Folie 1.85):

- für Fertigungsfehler unterschiedliche Hardware,
- für Hardware-Entwurfsfehlern unabhängig entworfene Hardware,
- für einige SW-Fehlern unterschiedlich übersetzte Software,
- für viele HW- und SW-Fehlern unabhängig entworfene SW oder
- Fehlerumgehung mit geänderter Service-Anforderung (siehe Folie 1.86).

Problemvermeidung

Problemvermeidung

Probleme, die sich vermeiden lassen, müssen nicht erkannt und behoben werden.

Arten der Problemvermeidung

- Robuste Systemgestaltung und Nutzung:
  - Robuste Reaktion auf erkannte Probleme (siehe Abschn. zuvor),
  - Anwendungs- und Arbeitsschutzrichtlinien, Sicherheitsvorkehrungen,
  - Systemgestaltung, z.B. Ruhestromprinzip, Trennung vom Internet, ...
  - ...
- Vermeidung und Beseitigung der Problemursachen
  - Fehlerbeseitigung (siehe Abschn. 2.1).
  - Fehlervermeidung (siehe Abschn. 2.3).
  - Vorgehensmodelle, Zertifizierungsprozesse, ...
- Toleranz in der Regel durch Redundanzen:
  - Backup, fehlerkorrigierende Codes (Informationsredundanz).
  - Hardware-Redundanz (Ausfalltoleranz) (siehe Abschn. 6.5.4).
  - ...

Robustheit

Außer robuste Reaktion auf erkannte Probleme gibt es weitere allgemeine Gestaltungsprinzipien:

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

Folie 1.126: Vermeidung problematischer MF.

Ursachenbeseitigung

Bei robustem Umgang mit allen erkannten Problemen, Zuverlässigkeitsbeeinträchtigung nur noch durch die nicht erkannten Fehlfunktionen.

Ursache dieser sind überwiegend Fehler, die vor dem Einsatz nicht erkannt und beseitigt wurden, aber auch Störungen und Ausfälle. Beziehung zwischen Test und Zuverlässigkeit (siehe Abschn. 2.2).

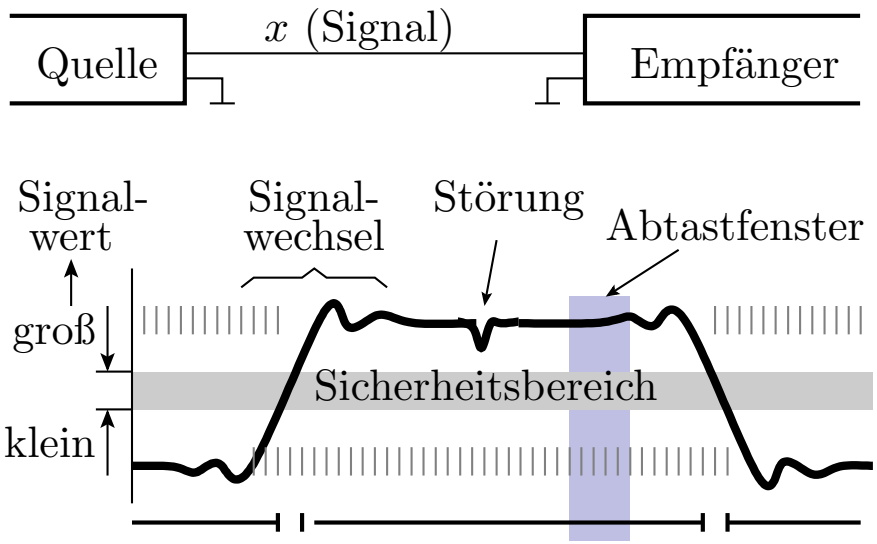
Die Anzahl der zu beseitigenden Fehler, von denen ein Teil nicht erkannt wird, hängt ab von der Systemgröße und dem Entstehungsprozesses. Fehlervermeidung ist Prozessverbesserung (siehe Abschn. 2.3).

Wesentliche Bestandteile der Prozessverbesserung sind Vorgehensmodelle (siehe Abschn. 2.3.3). Zertifizierungen und andere Techniken der Qualitätssicherung gehören dazu.

Andere Problemursachen anderer Umgang:

- Störungen: Digitalisierung zur Vermeidung, Wiederholung zur Korrektur erkannter Fehlfunktionen.
- Ausfälle: Wartung zur Vermeidung, Redundanz zur Tolerierung.

Robustheit durch digitale Verarbeitung



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.

Schafft Robustheit gegen Fertigungsstreuungen, Störungen, ...

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

Toleranz und Redundanz

Anwendungsspezifische und aufwändige Techniken zur Problemvermeidung.

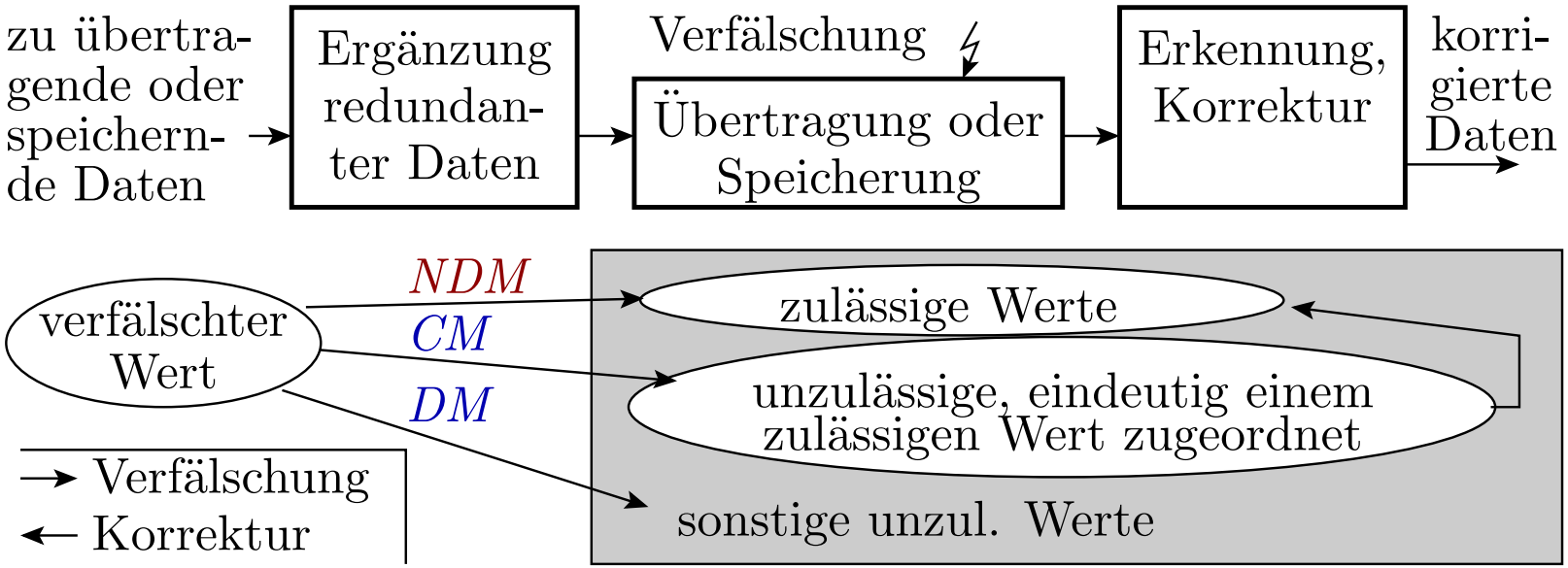
Toleranz (von lateinisch tolerare »erleiden, erdulden«): in der Technik aufrechterhalten der Funktion beim Auftreten von Problemen. Erfordert in der Regel Redundanzen.

Redundanz (von lateinisch redundare, überlaufen, sich reichlich ergießen), in der Technik sind Redundanzen zusätzliche Ressourcen, die im fehler- und störungsfreien Betrieb nicht benötigt werden:

- Hardware-Redundanz: Motoren, Baugruppen, komplette Geräte, Steuerleitungen, Stromversorgung, ...
- Funktionale Redundanz: Leistungsreserve, Zusatzfunktionen, ...
- Datenredundanz: fehlererkennende- und korrigierende Codes, Backup, ...

.

Fehlerkorrigierende Codes (gegen Datenverlust)



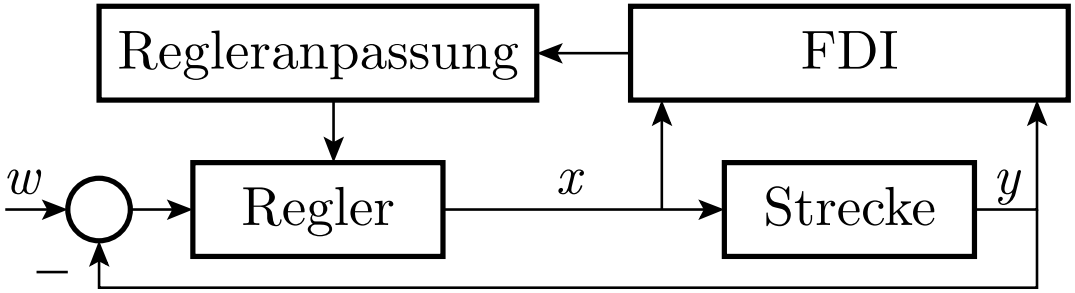
Korrektur verfälschter Daten nach Übertragung und Speicherung:

- 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 zur Zusatzeinheiten.
FDI Fehlerdetektion, -isolation und -identifikation.

Standby-Reserve

Hardware-Verfügbarkeit und mittlere Reparaturdauer:

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

A_{H}	zulässige mittlere Reparaturzeit $MTTR$	
	pro Monat	pro Jahr
99%	7,2 h	87,6 h
99,99%	4,3 min	53 min

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

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

$MTTR$	Mittlere Reparaturzeit (Mean time to repair).
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,
  - Leistungsverzicht (NS) oder Wiederholversuch (RR).

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

Kenngrößen der Überwachung

Fehlfunktionsabdeckung:

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

Phantomfehlfunktionsrate:

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

Zuverlässigkeitsverbesserung:

$$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-MC)} \cdot R \text{ mit } \zeta_{\mathrm{SMF}} = \zeta_{\mathrm{PM}} + \zeta \cdot MC - \zeta \cdot \zeta_{\mathrm{PM}} \tag{1.25}$$

Für eine geringe Rate signalisierter Fehlfunktionen:

$$R_{\mathrm{MT}} = \frac{R}{(1-MC)} \tag{1.26}$$

Erbringungsrate

Ohne Wiederholung:

$$\eta_{\mathrm{DS}} = (1 - \zeta_{\mathrm{CR}}) \cdot (1 - \zeta_{\mathrm{PM}} - \zeta \cdot MC + \zeta \cdot \zeta_{\mathrm{PM}}) \tag{1.22}$$

- Für geringe Problemraten:

$$\eta_{\mathrm{DS}} = 1 - \zeta_{\mathrm{CR}} - \zeta_{\mathrm{PM}} - \zeta \cdot MC \tag{1.23}$$

Bei maximal einer Wiederholung:

$$\eta_{\mathrm{DS.SR}} = \eta_{\mathrm{DS}} + (1 - \eta_{\mathrm{DS}}) \cdot \eta_{\mathrm{Div}} \cdot \eta_{\mathrm{DS}} \tag{1.35}$$

- Für geringe Problemraten:

$$\eta_{\mathrm{DS.SR}} = 1 - (1 - \eta_{\mathrm{DS}}) \cdot (1 - \eta_{\mathrm{Div}}) \tag{1.36}$$

Bei diversitären Problemen Wiederholung bis zur Beseitigung:

$$\eta_{\mathrm{DS.MR}} = 1 - (1 - \eta_{\mathrm{DS}}) \cdot (1 - \eta_{\mathrm{Div}}) \tag{1.37}$$

Diversität

- Natürliche Diversität nur 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.

Zielführender als erweiterte Diversität und Wiederholung für hohe Erbringungsraten sind geringe Problemraten insbesondere durch Fehlerbeseitigung vor der Nutzung und durch Fehlervermeidung.

Formatkontrolle

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

- Fehlfunktionsabdeckung:

$$MC = 1 - \frac{\#VP}{\#PP} \tag{1.27}$$

- Phantomfehlfunktionsrate:

$$\zeta_{\mathrm{PM}} = 0 \tag{1.28}$$

- Fehlfunktionsabdeckung mit r redundanten Bits:

$$MC \geq 1 - 2^{-r} \tag{1.29}$$

- Zuverlässigkeitsverbesserung:

$$R_{\mathrm{MT}} = 2^r \cdot R \tag{1.30}$$

Wertekontrolle

Master-Checker-Prinzip als universell einsetzbares Verfahren:

- Fehlfunktionsabdeckung:

$$MC = \eta_{\mathrm{Div}} \tag{1.31}$$

- Phantomfehlfunktionsrate:

$$\zeta_{\mathrm{PM}} = \eta_{\mathrm{Div}} \cdot \zeta_{\mathrm{Chk}} \tag{1.32}$$

Loop-Test:

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

Aufgabenspezifische Korrektheitskontrollen:

- Für Aufgaben, die durch kontrollierbare Korrektheit definiert sind.
- Gute Kontrollgüte, aber bei Lösungssuche durch Probieren signifikante Abnahme der Zuverlässigkeit bei einer hohen Rate signalisierter Fehlfunktionen bzw. Wiederholversuchen $\zeta_{\mathrm{SMF}} \to 1$.

Zuverlässigkeit und Erbringungsrate

Master-Checker ohne Wiederholung nach erkannten Problemen:

- Zuverlässigkeitsverbesserung

$$R_{\mathrm{MT}} = \frac{(1-\zeta_{\mathrm{SMF}})}{(1-\eta_{\mathrm{Div}})} \cdot R \text{ mit } \zeta_{\mathrm{SMF}} = \eta_{\mathrm{Div}} \cdot (\zeta + \zeta_{\mathrm{Chk}} - \zeta \cdot \zeta_{\mathrm{Chk}}) \quad (1.34)$$

- Erbringungsrate ohne Wiederholung:

$$\eta_{\mathrm{DS}} = (1 - \zeta_{\mathrm{CR}}) \cdot (1 - \eta_{\mathrm{Div}} \cdot (\zeta + \zeta_{\mathrm{Chk}} - \zeta \cdot \zeta_{\mathrm{Chk}})) \quad (1.33)$$

Dreifachberechnung mit Mehrheitsentscheid bzw. Master-Checker mit Neuberechnung nach erkannten Problemen:

- Erbringungsrate:

$$\eta_{\mathrm{DS.MV}} = 1 - (1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{CRC}} \quad (1.38)$$

- Zuverlässigkeitsverbesserung

$$R_{\mathrm{MV}} = \frac{1-(1-\eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{CRC}}}{(1-\eta_{\mathrm{Div}}) \cdot (1-\zeta_{\mathrm{CRC}}) \cdot \zeta_{\mathrm{CC}}} \quad (1.39)$$

$$R_{\mathrm{MV}}|_{\zeta_{\mathrm{CRC}} \to 0} = \frac{R}{(1-\eta_{\mathrm{Div}})} \quad (1.40)$$

Problemvermeidung

Überwachung und robuste Reaktion hilft bei vielen Problemen. Es gibt Alternativen und Ergänzungen:

- Fehlerbeseitigung und Vermeidung (siehe nächster Abschnitt).
- Robustheit auch für nicht nur erkannte Probleme, z.B. Ruhestromprinzip, Fehlfunktionsisolation, Brandmauern, Verzicht auf Anbindung an das Internet.
- Robustheit auch gegenüber Störungen, insbesondere durch digitale Verarbeitung.
- Toleranz und Redundanz: Aufrechterhalten der Funktion bei Problemen, in der Regel durch Redundanzen:
  - Fehlerkorrigierende Codes (Informationsredundanz).
  - Zusatzfunktionen wie bei fehlertoleranten Regelungssystemen.
  - Standby-Reserve für hohe Verfügbarkeit durch kurze Reparaturzeiten.