Test und Verlässlichkeit Foliensatz 1: Modelle, Begriffe, Wahrscheinlichkeiten, Kenngrößen

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_F1)

May 31, 2018

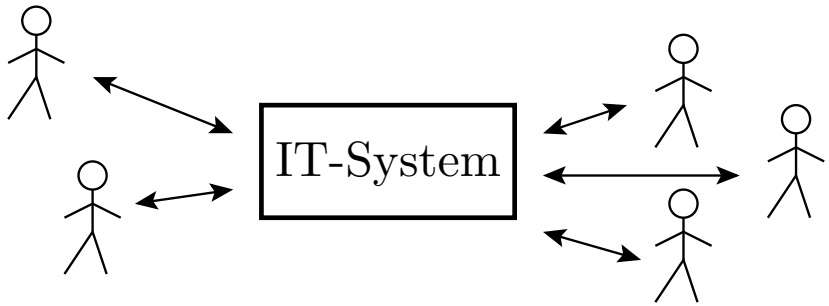
Inhalt Foliensatz TV_F1

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 eine IT-System setzt Verlässlichkeit des Systems voraus.

Verlässlichkeit

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

Die Verlässlichkeit von IT-Systemen wird durch eine Vielzahl von Aspekten beschrieben. Lapri[1] unterscheidet:

- Gefährdungen (Threats): Fehler, Fehlfunktionen (FF), Störungen, Ausfälle, ...
- Maßnahmen zur Gefährdungsminderung (Means):
  - Überwachung & Fehlerbehandlung incl. Fehlertoleranz,
  - Test & Fehlerbeseitigungsprozesse,
  - Fehlervermeidung, Fehlerumgehung, Wartung, ...
- Kenngrößen (Attributes): Verfügbarkeit, Zuverlässigkeit, Betriebs-, Daten-, Zugangssicherheit, Wartbarkeit, ...

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

Verlässlichkeit mehr als 50% der Produktkosten

- Mehrheit der Entwurfskosten für IT-Systeme: prüfgerechten Entwurf, Test, Fehlerbeseitigung, ...
- Mehrheit der Funktionen in sicherheitskritischen Anwendungen: Überwachung, zur Reaktion auf Fehlfunktionen, zum Aufspühren von Fehlern, ...

Bereiche, die an der Sicherung der Verlässlichkeit mitwirken:

- Management: Organisationsrahmen für fehlerarme Entstehungsprozesse, Unternehmenskultur ...
- Fertigung: Fehlervermeidung, Überwachung, ...
- Entwurf: Prüfgerechter Entwurf, Einprogrammieren von Überwachungsfunktionen, Entwurf von Testbeispielen, ...
- Qualitätskontrolle: Prozesskontrolle, Produktkontrolle, ...
- Vertrieb: Rückmeldung über beobachtete Fehlfunktionen, Schwachstellen, ...

Der Preis fehlender Verlässlichkeit

- Datenverlust,
- Hintertüren für den Datenmissbrauch,
- 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, so dass der Start amerikanischer Raketen mit Nuklearsprengköpfen in letzter Minute gestoppt wurde[2].

Urheber der nahen Katastrophe war ein defekter Schaltkreis in einem Rechner.

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

Lernziele der Vorlesung »Test und Verlässlichkeit«

- Modellierung der »Threads« (Fehlern, Fehlfunktionen, Ausfällen, ...) in IT-Systemen.
- Maßnahmen zur Gefährdungsminderung (»Means«):
  - Überwachung & Fehlerbehandlung incl. Fehlertoleranz,
  - Test & Fehlerbeseitigungsprozesse,
  - Fehlervermeidung, Fehlerumgehung, Wartung, ...
- Kenngrößen (»Attributes«) für die »Threads & Means« .

Tests sind die »Means« zur Erkennung der »Threads«. Da nur auf erkennbare »Threads« schadensmindernde Reaktionen möglich sind, begrenzt die »Testdurchlässigkeit« die erzielbare Verlässlichkeit.

Themenspezifische Einführung in die Stochastik: Fehlerbäume, Markov-Ketten, ... Verteilungen für die Anzahl der Fehler, Fehlfunktionen, ... Vorhersagbarkeit. Garantierbare Schranken, ...

Foliensätze

- F1: Modelle, Begriffe, Wahrscheinlichkeit und Kenngrößen.
- F2: Problembeseitigung: Fehlerbeseitigung, Reifeprozesse, Umgang mit Ausfällen und Fehlfunktionen, Fehlervermeidung.
- F3: Ergebnisüberwachung: Fehlererkennende und -korrigierende Codes, Formatkontrollen, Wertekontrollen.
- F4: Statische Tests: Direkte Kontrolle von Merkmalen.
- F5: Dynamische Tests: Ausprobieren der Funktion.
- F6: Verteilungen und zusicherbare Kenngrößen.

Modelle und Begriffe

Der Begriff »Modell« in der Informatik

Alle Sachverhalte in der Informatik, selbst die Abarbeitung eines Befehls, werden schnell zu kompliziert, wenn alle Details berücksichtigt werden.

Definition Modell

Mittel, um einen Zusammenhang zu veranschaulichen. Es stellt die wesentlichen Sachverhalte dar und verbirgt unwesentliche Details.

In TV werden potentielle Gefährdungen als abzählbare Mengen modelliert. Für deren Elemente werden Wahrscheinlichkeiten für das vorhanden sein, wirksam werden, ... abgeschätzt. Die Modell für gefährdungsmindernde Maßnahmen sind Filter, die einen Teil der Gefährdungen erkennen, beseitigen, ...

Unwesentlich: Funktion und Realisierung der Systeme.

Service-Modell

Das Service-Modell

Modellierung der Verarbeitung als eine Folge von diskreten Schritten, in denen aus Eingaben Ausgaben produziert werden. Jede Ausgabe für korrekte Eingaben ist eine potenielle Fehlfunktion (FF) der Service-Leistung (SL).

- Anzahl der potentiellen FF gleich Anzahl der SL und damit abzählbar.
- Wahrscheinl. FF abschätzbar durch Zählen der SL und FF.

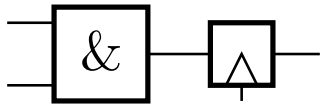
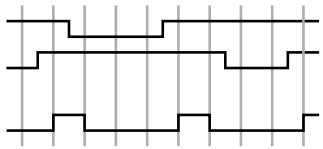
Definition Service

Vorgang, der in zeitdiskreten Schritten aus Eingaben Ausgaben erzeugt, die richtig oder FFs sein können.

Mögliche Systeme für die Erbringung von SL:

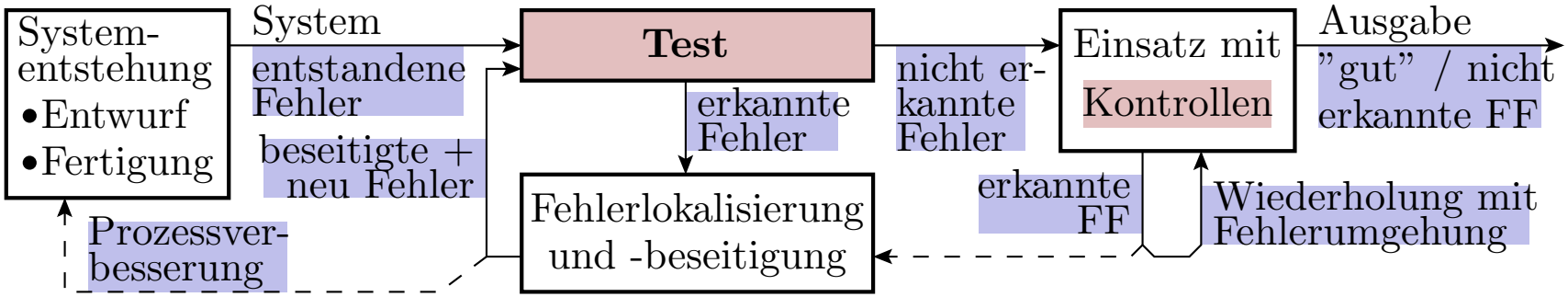
- Digitale Schaltungen, Rechner, Programme,
- Server, Steuergeräte, Maschinen, ...

Beispiele für Service-Leister

getaktete Digitalschaltung		E: A: 
Programm mit EVA-Struktur	`uint8_t up(uint8_t a){ return 23 * a; }`	E: 10 101 ... A: 33 124 ...
Server	E: z.B. eine Datenbankanfrage A: Ergebnisdatensatz	
Fertigungsprozess	E: Fertigungsauftrag, Material, ... A: gefertigtes Produkt	
Entwurfsprozess	E: Entwurfsauftrag A: Entwurf	

IT-Systeme etc. sind nicht von Natur aus Service-Leister, sondern sie werden als SL konzipiert, um die Inbetriebnahme, den Test, ... zu beherrschen. Voraussetzung für Verlässlichkeit im Einsatz.

»Means« als Service



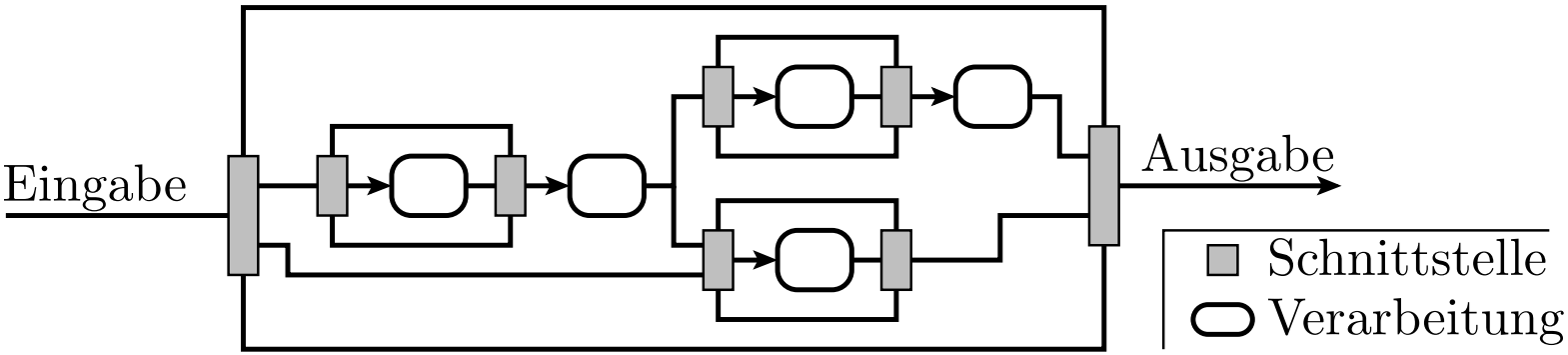
Verlässlichkeit wird auf drei Ebenen gesichert:

- Fehlervermeidung (Prozessverbesserung),
- Test + Fehlebeseitigung und
- Kontrollen + Fehlerbehandlung.

Die »Means« auf jeder Ebene umfassen Kontrollen und Maßnahmen zur Reaktion auf erkannte »Theads« zur Gefährdungsminderung.

»Means« sind auch Service-Leister. Ein Kontrolle z.B. bildet zu überwachende Daten auf eine Gut/Schlecht-Ausgabe ab.

Hierarchie und Sequenz von Service-Leistungen (SL)



Komplexe SL bestehen aus Teil-SL. Wichtige Relationen:

- Hierarchie: Gesamt-SL nutzt Teil-SLs, z.B. Programme Unterprogramme, Gatter Transistoren, ...
  - Gesamt-SL enthält damit auch die Fehler aller Teil-SL.
  - Lokalisierung und Reparatur durch systematisches Tauschen, ...
- Sequenz: Gesamt-SL ist eine Folge von Teil-SL.
  - Fortpflanzung von FF,
  - Lokalisierung durch Rückverfolgung, ...

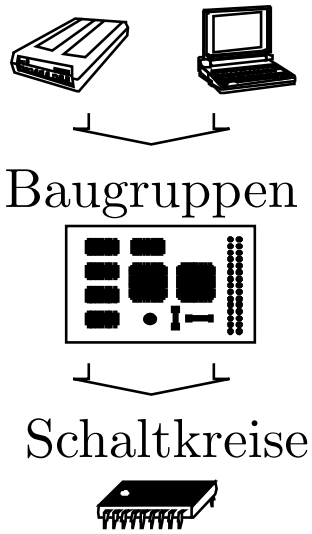
Reparatur durch Tausch

Reparaturgerechte Systeme haben eine hierarchische Struktur aus tauschbaren Komponenten, z.B.

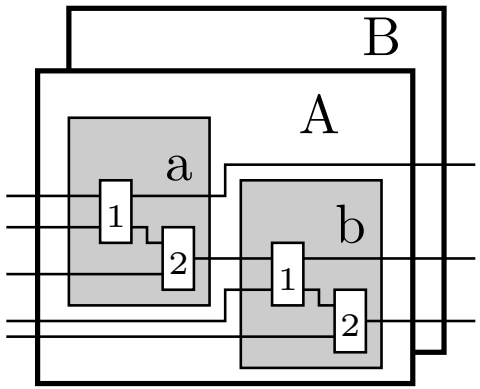
1. Ebene: Austauschbare Geräte.
2. Ebene: Austauschbare Baugruppen.
3. Ebene: Austauschbare Schaltkreise.

Fehlerlokalisierung durch systematisches Tauschen:

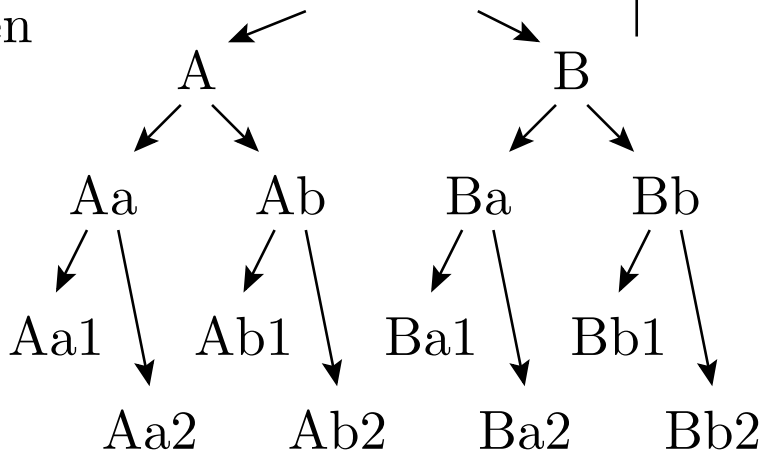
Hierarchie der Hardware



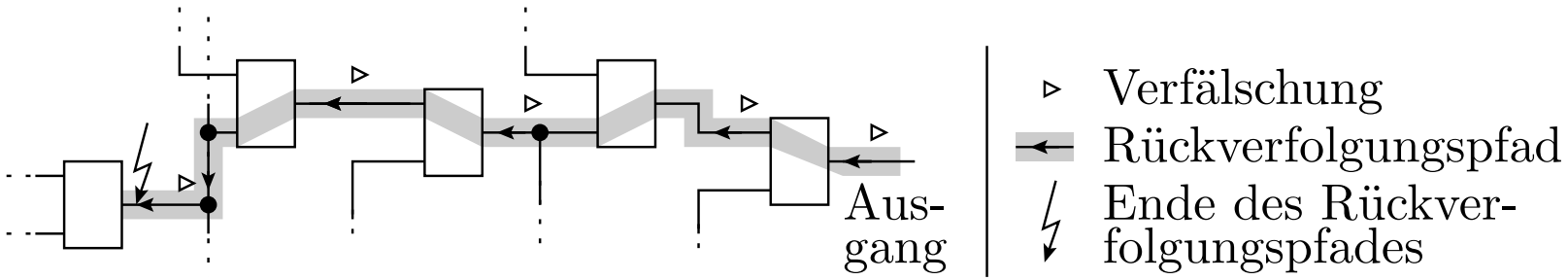
hierarchisches System mit tauschbaren Komponenten



Tauschbaum



Fehlerlokalisierung durch Rückverfolgung



- Ausgehend von einer erkannten falschen Ausgabe Rückwärtsuche nach dem Entstehungsort.
- Suche endet am Teil-Service, der aus richtigen Eingaben falsche Ergebnisse erzeugt.
- Tausch oder weiter hierarchisch absteigende Suche.
- Verfälschungsursache kann außer dem erzeugenden Service auch ein anderer, z.B. mit fehlgeleitetem Schreibzugriff, sein.

Determinismus

Definition Determinismus

Ein Service arbeitet deterministisch, wenn gleiche Eingaben immer auf gleiche Ergebnisse abgebildet werden.

Determinismus ist Voraussetzung für:

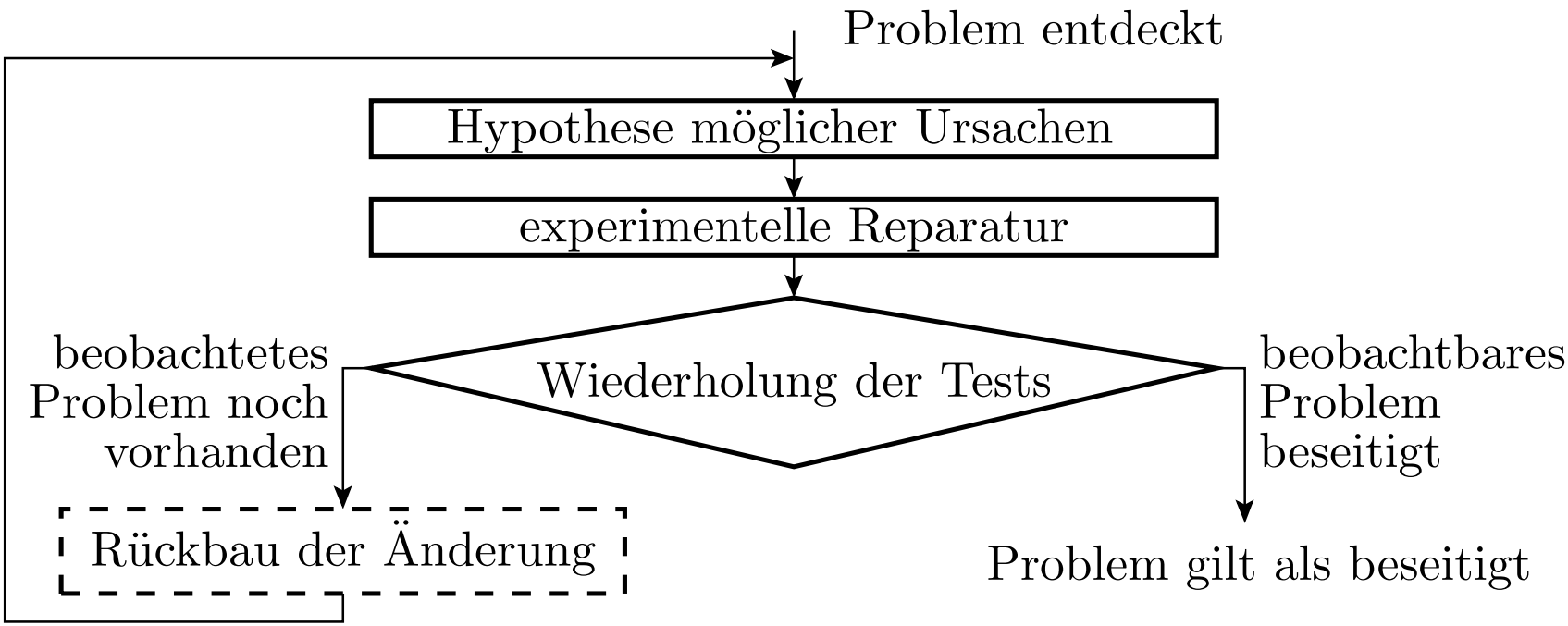
- Lokalisierung durch Testwiederholung und Rückverfolgung.
- Test mit Ergebniskontrolle durch Soll-/Ist-Vergleich.
- Ausschluss von Fehlfunktionen durch Tests.
- Kontrolle der Fehlerbeseitigung durch Testwiederholung.

Nicht-Deterministmus nicht immer vermeidbar. Erforderlich für:

- Zufällige Ergebnisauswahl aus großen Lösungsmengen.
- Korrektur von FF durch Wiederholung auf einem zufallsgesteuerten alternativen Rechenweg.
- Verschlüsselung in der Kryptographie, ...

Probleme von Nicht-Determinismus

Für nicht deterministische SL funktioniert die übliche Fehlerbeseitigung durch experimentelle Reparatur nicht:



Deshalb vorzugsweise Zusammensetzung nicht det. SL aus separat testbaren deterministischen Teil-SL.

Prüfgerechter Entwurf für nicht det. SL

Prüfgerechter Entwurf am Beispiel einer heuristischen Suche:

- Programmieren des Suchalgorithmus mit Steuereingaben zur Variation des Lösungswegs (det. SL).
- Pseudo-Zufallsgeneratoren[3] zum »auswürfeln« der Steuerparameter (det. SL).
- Begrenzung des Nicht-Determinismus auf die Auswahl eines zufälligen Startwerts zur Initialisierung des Pseudo-Zufallsgenerators (Systemzeit, echte Zufallszahl, ...).

Signalverarbeitung:

- nicht deterministisch: analoge Vorverarbeitung und Wandlung.
- deterministisch: digitale und programmgesteuerte Verarbeitung.

Auch bei Entstehungsprozessen (Entwurfs-SL und Fertigungs-SL) wird Determinismus angestrebt (siehe später TV_F2, Abschn. 5.1).

[3] Ein Pseudo-Zufallsgenerator ist ein deterministischer Automat, der eine sehr lange Zustandsfolge in pseudo-zufälliger Reihenfolge durchläuft.

Gedächtnis

Ein deterministischer Service ohne Gedächtnis realisiert im math. Sinne eine Funktion:

$$y = f(x)$$

die jedem zulässigen Eingabewert x genau einen Ausgabewert y zuordnet.

Ein deterministischer Service mit Gedächtnis ist im math. Sinne ein Automat mit einem Zustand s, einer Übergangsfunktion

$$s = f_{\mathrm{s}}(s, x)$$

und einer Ausgabefunktion:

$$y = f_{\mathrm{y}}(s, x)$$

(x – Eingabe; y – Ausgabe).

Service-Leistungen ohne und mit Gedächtnis gibt es für jeden Systemtyp (SW, HW, mit/ohne physikalischer Interaktion, ...):

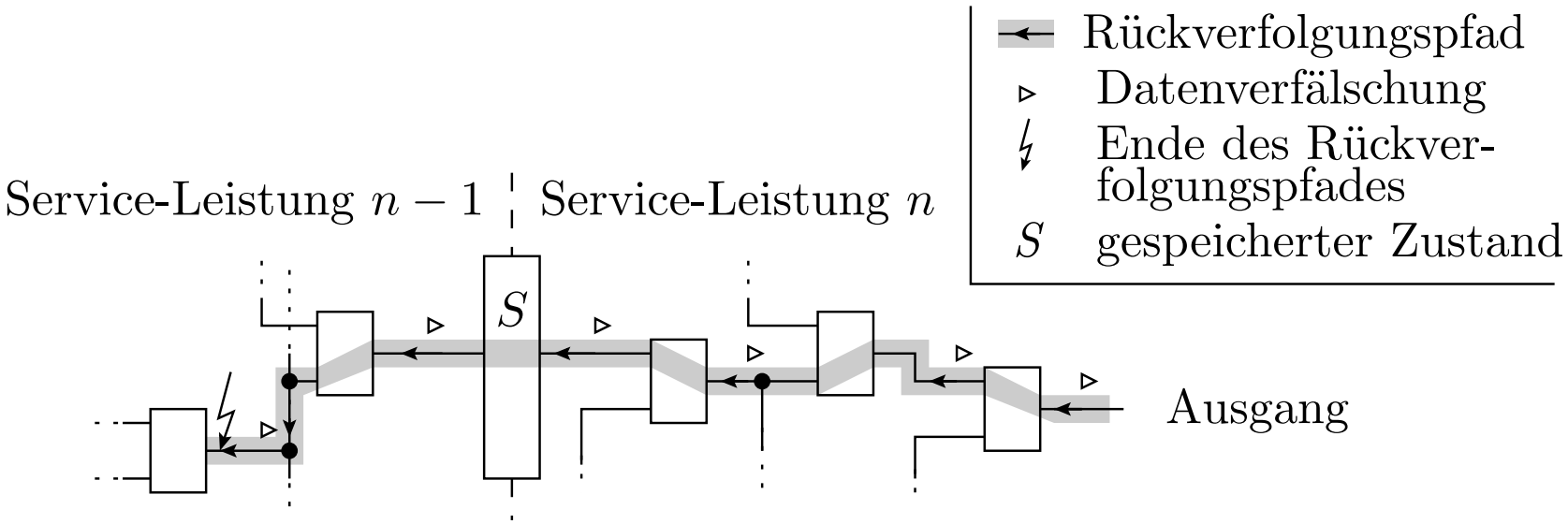
	ohne Gedächtnis	mit Gedächtnis
Programmbausteine	Unterprogramme ohne private Daten	OOP-Methoden zur Objektbearbeitung.
Programme	Compiler	Textverarbeitung
Server-Dienste	Ohne Nutzung fremder Daten.	Datenbankanfrage
digitale Schaltungen	Rechenwerk	Prozessor
Systeme mit physikalischer Interaktion	Maschine, die aus Vorgaben Werkstücke herstellt	Steuergerät, das sich Daten merkt

Eine Gesamstsystem ohne Gedächtnis kann auch Teilsysteme mit Gedächnis nutzen (z.B. ein Server-Dienst den Server).

Der Preis für ein Gedächtnis

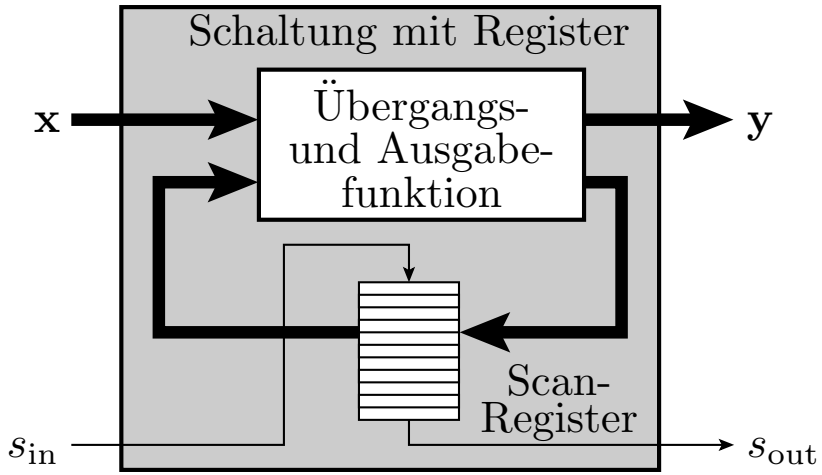
Zustandskontaminierung (versteckte Datenverfälschungen):

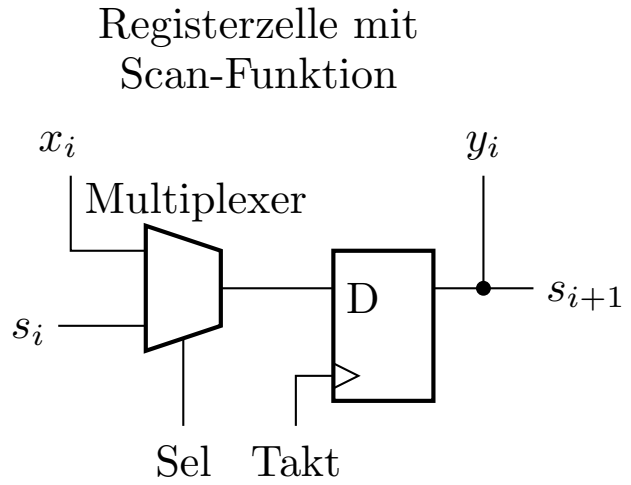
- Systemabstürze durch Übergang in unzulässige Zustände, die das fehlerhafte System nicht selbstständig wieder verlässt. ...
- Neuinitialisierung nach Fehlfunktionen.
- Fehleranregung über mehrere Service-Anforderungen.
- Rückverfolgung über mehrere SL.



Prüfgerechte SL mit Gedächtnis

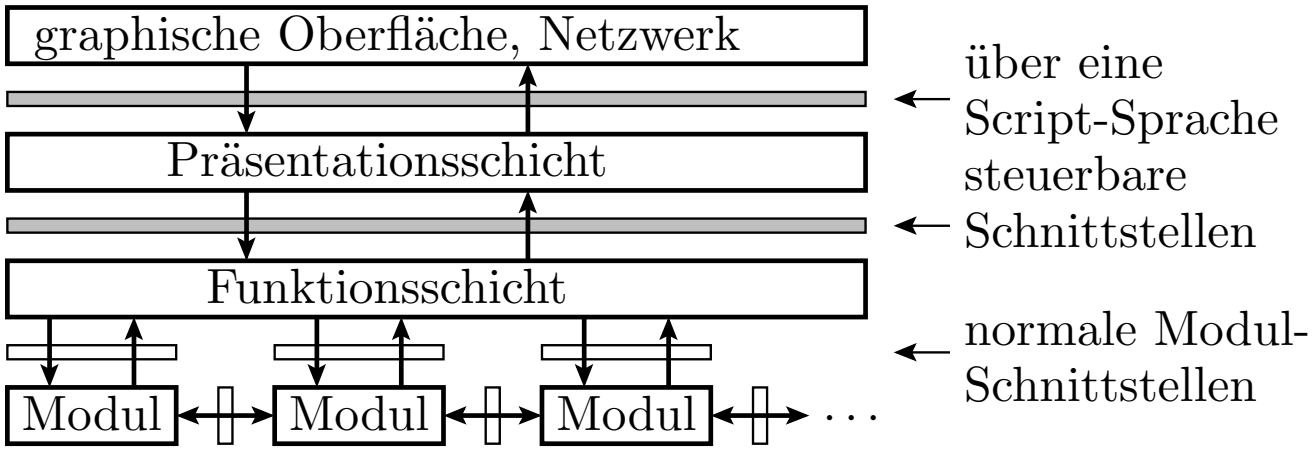
- Initialisierbarkeit aller internen Zustandsgrößen (Mindestanforderung).
- Seperate Testbarkeit der Übergangsfunktion f_s und der Ausgabefunktion f_y durch Lese- und Schreibzugriff auf den Zustand s (Maximallösung).





Reaktive Systeme

die auf unterschiedliche nebenläufig in zufälliger zeitlicher Abfolge eingehende Ereignisse reagieren, z.B. GUI-Programme[4], sind keine SL gemäß Definition, aber ...



Prüfgerechter Entwurf: Schichtenarchitektur[5].

[4] GUI – Graphical User Interface

[5] Schichten sind Sammlungen von Funktionen. Es gilt, dass Funktionen höherer Schichten nur solche niederer Schichten nutzen dürfen und nicht umgekehrt.

Schichtenarchitektur

Konzeptionelle Zuordnung von Aspekten eines Software-Systems zu einer Schicht:

- graphische Oberfläche,
- Funktionsschicht,
- Datenbankschicht, ...

Prüfgerechter Entwurf:

- Zusammensetzen der Schichten aus überwiegend separat testbaren deterministischen SL.
- Funktionen zur Aufzeichnung[6] und Steuerung des Datentransfers zwischen den Schichten, in großen Systemen über Script-Sprachen (Phyton, TCL, ...).

[6] Protokollierung in eine Log-Datei.

Fehler und Fehlfunktionen

Fehlfunktion (FF)

Definition Fehlfunktion (FF)

Fehlerhaft ausgeführte Service-Leistung.

Fehlerhaft bedeutet, dass das Ergebnis vom spezifizierten Sollverhalten abweicht. Bei uneindeutiger Spezifikation liegt »fehlerhaft« im Emessen des Betrachters:

»It is not a bug, it is a feature.

- Bei ungetesteten Systemen ist oft fast jede SL eine FF. Nach Test und Fehlerbeseitigung ist der Anteil der FF an den SL gering, z.B. $< 10^{-6}$.
- Die Abschätzung des Anteils der nicht erkennbaren FF ist problematisch.

Fehler

Definition Fehler

Beseitigbare Ursachen für die Entstehung von Fehlfunktionen.

Fehler sind

- ständig vorhanden,
- entstehen in Entwurfs-, Fertigungs-, Reparaturprozessen.
- Beseitigung: Reparatur / Ersatz fehlerhafter Komponenten.
- Vermeidung: Beseitigung der Entstehungsursache.

In Abgrenzung zu Fehlern haben Störungen:

- zufällige, nicht reproduzierbare Wirkungen,
- vermeidbar durch Verringerung der Störanfälligkeit.

Eine dritte Kategorie von »Threads« sind Ausfälle:

- Während des Betriebs entstehende Fehler.
- Schadensvermeidung: Wartungsintervalle, Einschalttests, ...

Potentielle Fehler und Fehleranzahl

Suche einer geeigneten Definition für potentielle Fehler:

- In Analogie zur Begriffsdefinition von FF sind die potentiellen Fehler Entstehungs-SL[7].
- Besser zählbar und auf ihre Wirkung hin untersuchbar sind die Reparaturmöglichkeiten (potentiell fehlerhafte Komponenten, Verbindungen, ...).

Potentielle Fehler können im weiteren Entstehungs-SL **oder** Reperaturmöglichkeiten sein.

Schätzen der Fehleranzahl:

- über Metriken für die Systemgröße und Kompliziertheit.
- aus der Hierarchie und dem Fehleranteil der Komponenten.

[7] Einen Entstehungs-SL kann entweder korrekt ausgeführt werden oder eine FF sein. Entstehungs-FFs sind Fehler im entstehenden Produkt.

Metriken zur Abschätzung der Fehleranzahl

- Arbeitsaufwand in Manntagen, -wochen oder -monaten,
- Programmgröße in NLOC (Netto Lines of Code),
- Schaltkreisgröße in Transistoren oder Gatteräquivalenten.

Beispielabschätzungen:

1. 30 Fehler / 1000 NLOC, Programm mit 2000 NLOC.
   Zu erwartende Anzahl der entstehenden Programmierfehler: 60
2. 1 Fehler je 10^6 Transistoren. Schaltkreis mit 10^5 Transistoren.
   Zu erwartende Anzahl der entstehenden Fehler je Schaltkreis: 0,1.

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

Das Pareto-Prinzip

Das Pareto-Prinzip besagt dass oft[8]:

»ein kleiner Anteil K der Ursachen für einen großen Anteil G der Wirkungen verantwortlich ist.«

- $K \ll 50\%$ Entstehungsursachen verursachen $G \gg 50\%$ Fehler,
- $K \ll 50\%$ der Fehler verursacht $G \gg 50\%$ der FF,
- $K \ll 50\%$ FF verursacht $G \gg 50\%$ des Schadens.

[8] Vilfredo Pareto untersuchte die Verteilung des Bodenbesitzes in Italien. Er fand heraus, dass ca. 20% der Bevölkerung ca. 80% des Bodens besitzen und leitete daraus das Pareto-Prinzip ab. Im Jahr 1989 wurde festgestellt, dass 20% der Bevölkerung 82,7% des Weltvermögens besitzen. Tendez zu 1% der Weltbevölkerung besitzen 99% der Weltvermögens, ... Hyperlink: Andreas Haufler. Das Pareto Prinzip. (abgerufen 20.02.2018)

Das Pareto-Prinzip rekursiv

Das Pareto-Prinzip gilt in der Regel auch rekursiv nach Beseitigung des kleinen Teils der dominanten Ursachen.

> *Nach Beseitigung der* $K \ll 50\%$ *der Fehler, die* $G \gg 50\%$ *der FF verursacht haben sind es weiterhin* $K \ll 50\%$ *der Fehler, die* $G \gg 50\%$ *der FF verursacht, etc.*

Dieses Prinzip dient im Weiteren als Schätzgrundlage für den Zusammenhang zwischen der Anzahl der nicht beseitigten Fehler und der Häufigkeit der FF durch diese.

Modellfehler

Modellfehler

Potenzielle Fehler (sowohl »Entsteungs-SL« als auch »Reparaturmöglichkeiten«) haben viele mögliche Fehlverhalten. Für die Bewertung und Suche von Testsätzen müssen die unterstellten Fehler ein eindeutiges (simulierbares) Fehlverhalten haben:

Definition Modellfehler

Fehlerannahme mit simulierbarem Verhalten.

Beispiele für Modellfehler:

- Setze Signal auf ständig null / ständig eins.
- Setze Sprungbedingung auf ständig wahr / ständig falsch.
- Verfälsche Zwischenergebnisse +1 / -1.

Fehlermodell

Definition Fehlermodell

Algorithmus für die Berechnung einer Menge von Modellfehlern.

Beispiele:

- Für jeden Anschluss für jedes Gatter einer Schaltung, setze den Anschluss einmal auf ständig 0 und einmal auf ständig 1.
- Für alle Werteberechungen und Auswertungen in einem Programm, unterstelle für jede berechnete und jede ausgewertete Variable, dass sie einmal um eins erhöht und einmal um eins verringert sei. ...

Nach Zusammenstellung einer Anfangsfehlermenge werden identisch nachweisbare Fehler zu einem Modellfehler zusammengefasst, redundante (nicht nachweisbare) Fehler gestrichen, ...

Haftfehlermodell

Das Haftfehlermodell

Für jeden logischen Wert (binäres Signal, Entscheidung, ...)
Annahme von zwei Modellfehlern:

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

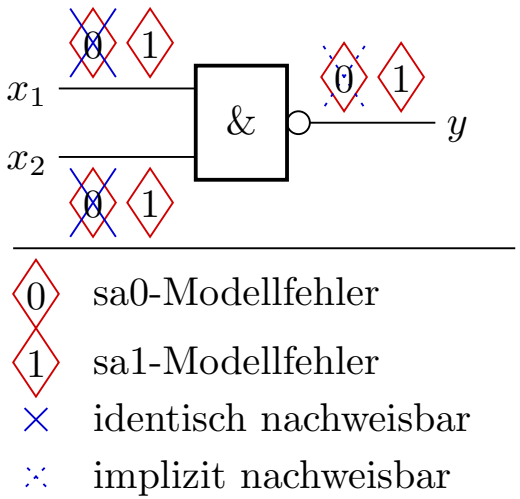
In der Praxis am meisten verbreitetes Fehlermodell (siehe später TV-F4):

- Erprobt seit 4 bis 5 Jahrzehnten für die Fehlersimulation und Testsatzberechung große digitale Schaltungen.
- Neuere systematische Techniken für die Testauswahl und Bewertung für Software auf das Haftfehlermodell zurückführbar, so dass die lange bewährten Techniken übernehmbar sind.

Haftfehler für Logikgatter

Für jeden Gatteranschluss wird unterstellt:

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



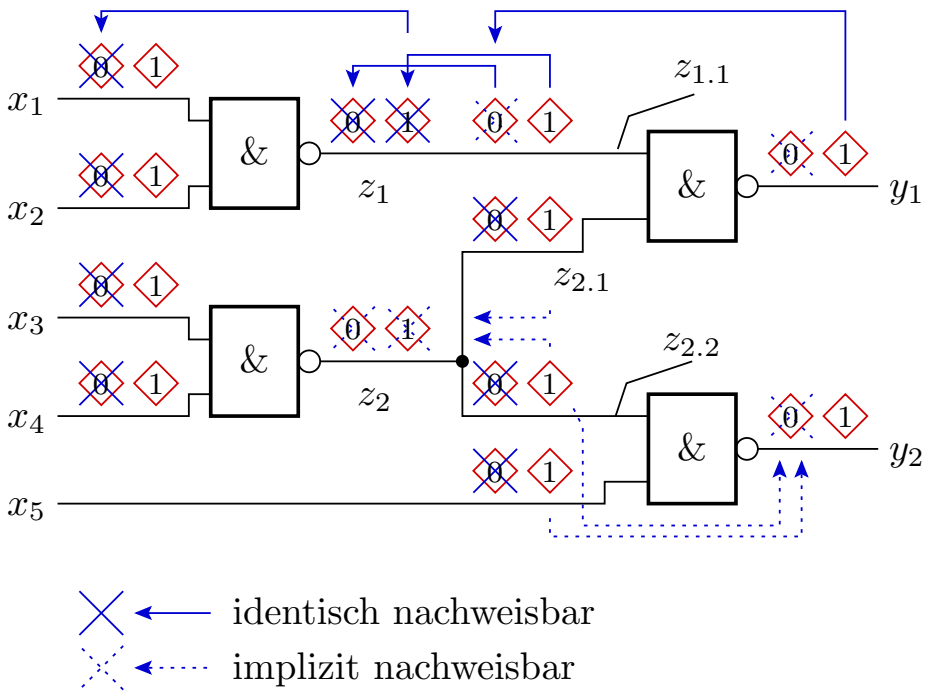
x_2	x_1	$\overline{x_2 \wedge x_1}$	sa0(x_1)	sa1(x_1)	sa0(x_2)	sa1(x_2)	sa0(y)	sa1(y)
0	0	1	1	1	1	1	0	1
0	1	1	1	1	1	0	0	1
1	0	1	1	0	1	1	0	1
1	1	0	1	0	1	0	0	1
				Nachweisidentität (gleiche Nachweismenge)				

Nachweisimplikation

zugehörige Eingabe ist Element der Nachweismenge

Zusammenfassung identisch nachweisbarer Fehler. Optionale Streichung redundanter und implizit nachweisbarer Modellfehler. Modellierte Fehler sind ähnlich wie Transistorfehler in Gattern nachweisbar.

Streichen identischer und implizit nachweisbarer Fehler



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

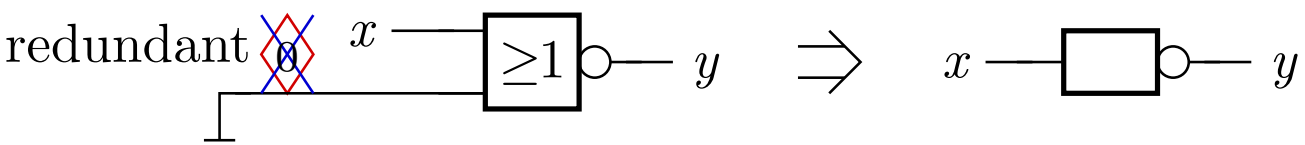
	Mengen von identisch nachweisbaren Fehlern	Nachweis impliziert durch
1	sa0(x_1), sa0(x_2), sa1(z_1), sa1($z_{1.1}$)	
2	sa1(x_1)	
3	sa1(x_2)	
4	sa0(x_3), sa0(x_4), sa1(z_2)	9, 12
5	sa1(x_3)	
6	sa1(x_4)	
7	sa0(z_2)	5, 6, 8, 11
8	sa0(z_1), sa0($z_{1.1}$), sa0($z_{2.1}$), sa1(y_1)	2, 3
9	sa1($z_{2.1}$)	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

Redundante Fehler

Definition redundanter (Modell-) Fehler

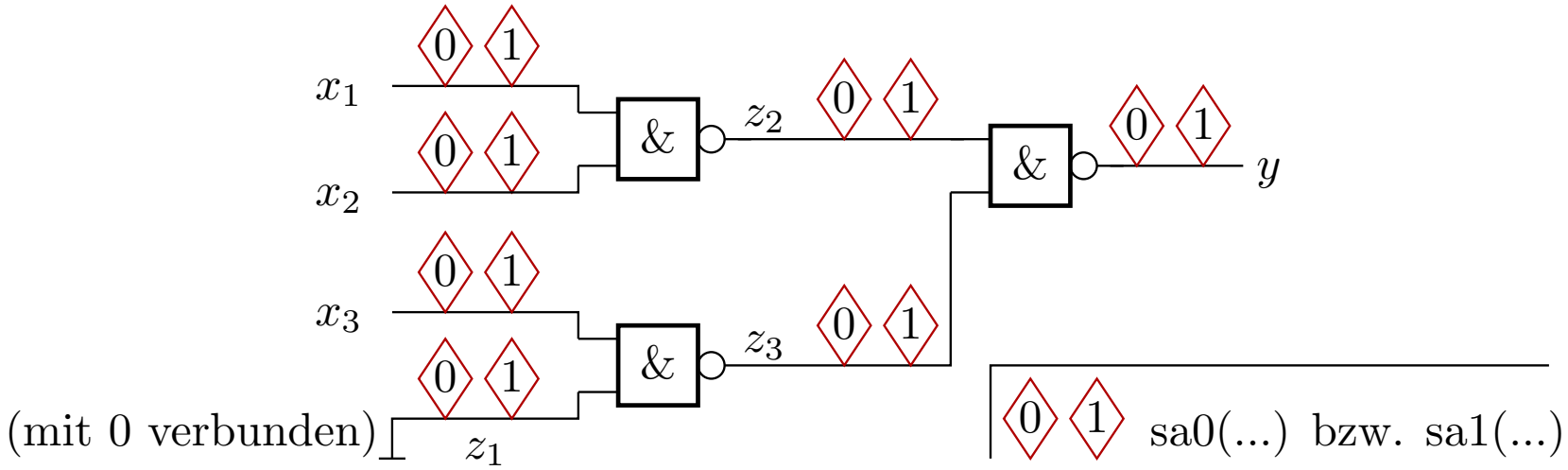
Fehler in einem Teilsystem, der die Funktion des Gesamtsystems nicht beeinträchtigt.

- Der Gatteranschluss kann mit »0« (sa0-Fehler nicht nachweisbar) bzw. »1« (sa1-Fehler nicht nachweisbar) verbunden sein, ohne dass sich die Funktion ändert.
- Umformungen zur Beseitigung redundanter Modellfehler dienen auch zur Systemoptimierung.



Beispielaufgabe

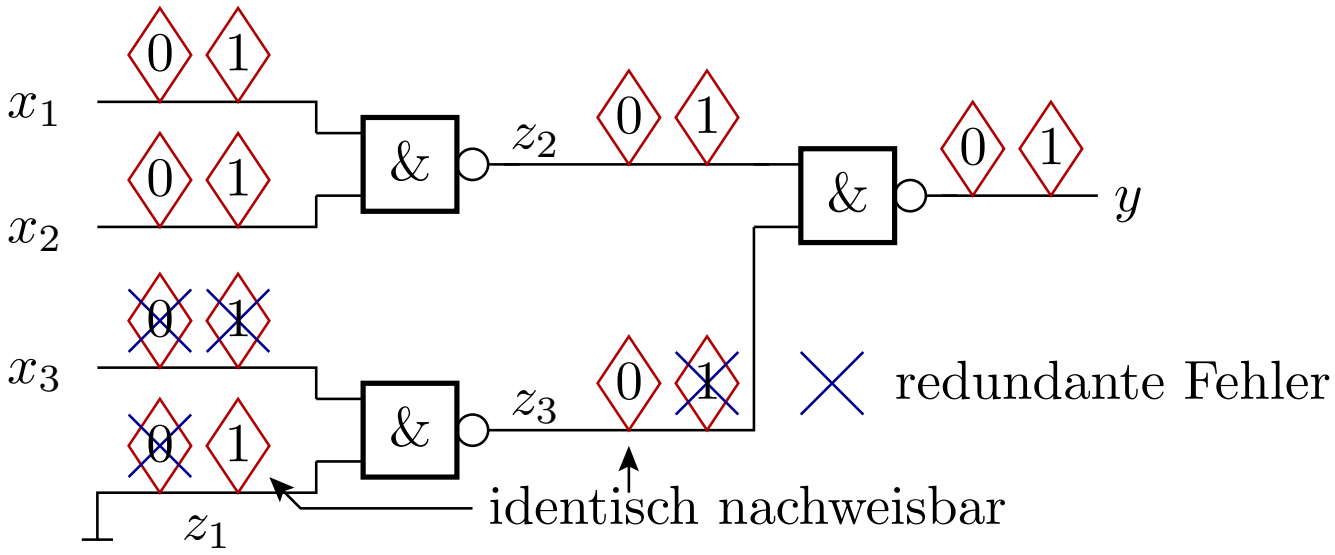
Gegeben ist die nachfolgende Schaltung mit 12 eingezeichneten Haftfehlern.



Welche der Haftfehler sind

1. redundant, d.h. mit keiner Eingabebelegung nachweisbar,
2. nach einer Konstanteneliminierung identisch nachweisbar,
3. implizit durch die Tests anderer Haftfehler nachweisbar?

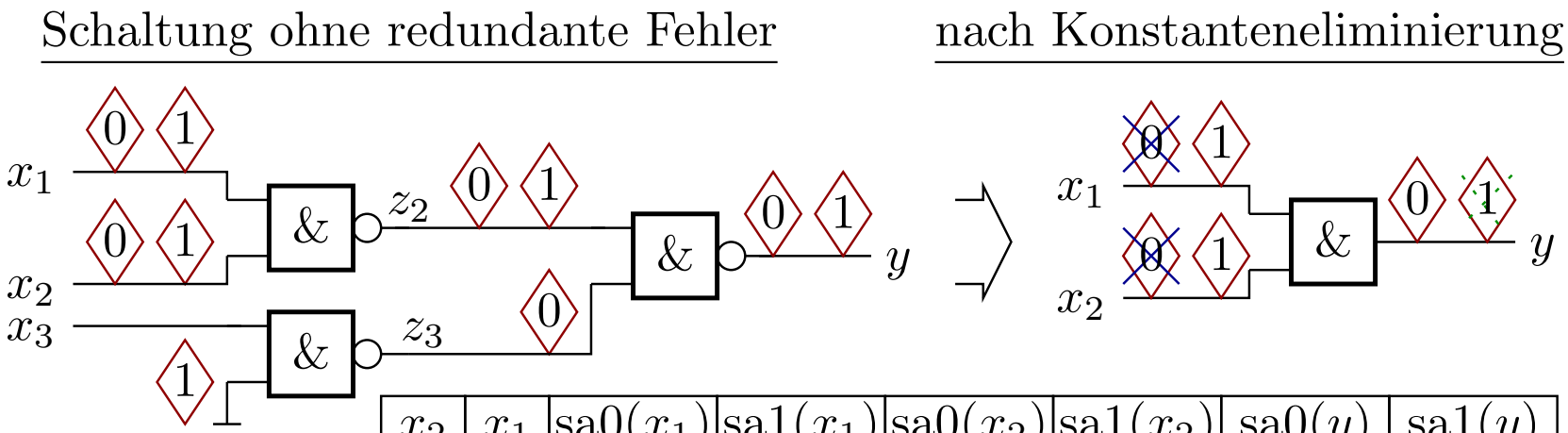
Lösung Aufgabenteil 1



$z_1 = 0$ impliziert, dass

- sa0(z_1) nicht anregbar ist,
- $z_3 = 1$, so dass sa1(z_3) nicht anregbar ist und
- dass x_3 nicht beobachtbar ist, so dass sa0(x_3) und sa1(x_3) auch redundant sind.

Lösung Aufgabenteil 2 und 3



x_2	x_1	sa0(x_1)	sa1(x_1)	sa0(x_2)	sa1(x_2)	sa0(y)	sa1(y)
0	0	–	–	–	–	–	+
0	1	–	–	–	+	–	+
1	0	–	+	–	–	–	+
1	1	+	–	+	–	+	–

Die Fehlermenge ohne redundante, identisch und implizit nachweisbare Haftfehler umfasst $\mathrm{sa1}(x_1)$, $\mathrm{sa1}(x_2)$ und $\mathrm{sa0}(y)$.

Wahrscheinlichkeit

Zufallsexperiment

Zufallsexperiment

Die Zusammenhänge zwischen »Threads« und ihren Wirkungen:

- Ist ein potentieller Fehler vorhanden?
- Verursacht ein vorhandener Fehler eine FF?
- ...

werden durch Wahrscheinlichkeiten beschreiben. Die Basis für die Definition von Wahrscheinlichkeiten sind Zufallsexperimente.

Definition Zufallsexperiment

Experiment mit mehreren möglichen Ergebnissen und zufälligem Ausgang.

Im weiteren betrachtete Zufallsexperimente:

- Anforderung einer Service-Leistung {ok, FF},
- Zählen der Fehler {0, 1, 2, ... }, ...

{...} – Wertebereich möglicher Ergebnisse.

Bernoulli-Versuch

Das einfachste Zufallsexperiment ist der Bernoulli-Versuch. Er hat zwei mögliche Ergebnisse $\{0, 1\}$, die bedeuten können $\{\text{nein}, \text{ja}\}$, $\{\text{falsch}, \text{wahr}\}$, ..., und die Verteilung

$$\begin{aligned} P\{X = 0\} &= 1 - p \\ P\{X = 1\} &= p \end{aligned}$$

(p – Wahrscheinlichkeit, dass das Ergebnis 1, ja oder wahr ist).
Bernoulli-Versuche für Aspekte der Verlässlichkeit:

- Anzahl der FF je SL$\{0, 1\}$.
- Anzahl nachweisbare Fehler je potentieller Fehler $\{0, 1\}$.
- ...

In der Vorlesung werden fast alle statistisch untersuchten Zusammenhänge auf Bernoulli-Versuche zurückgeführt, z.B. die Fehleranzahl als Summe potentieller Fehler, ob vorhanden ...

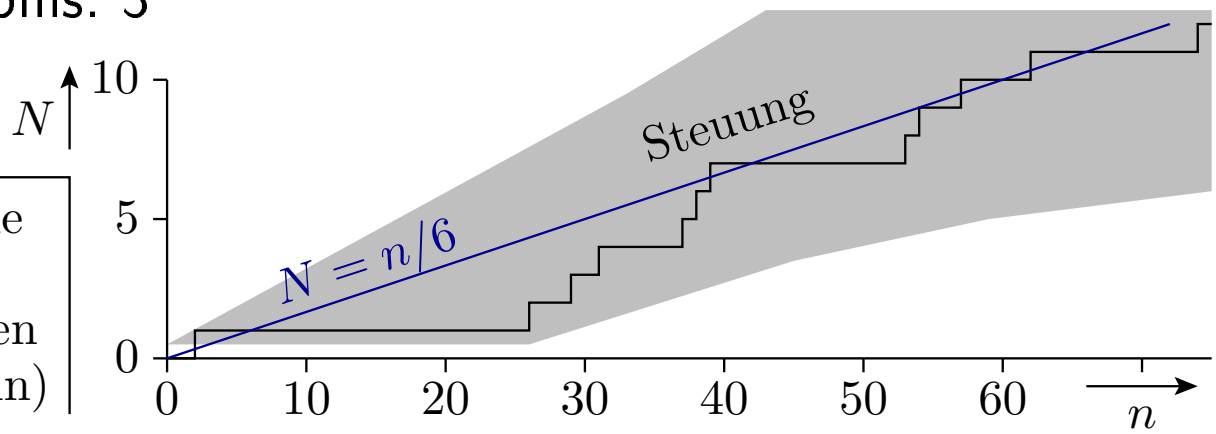
Die Wahrscheinlichkeit von Zufallsexperimenten

Definition Wahrscheinlichkeit

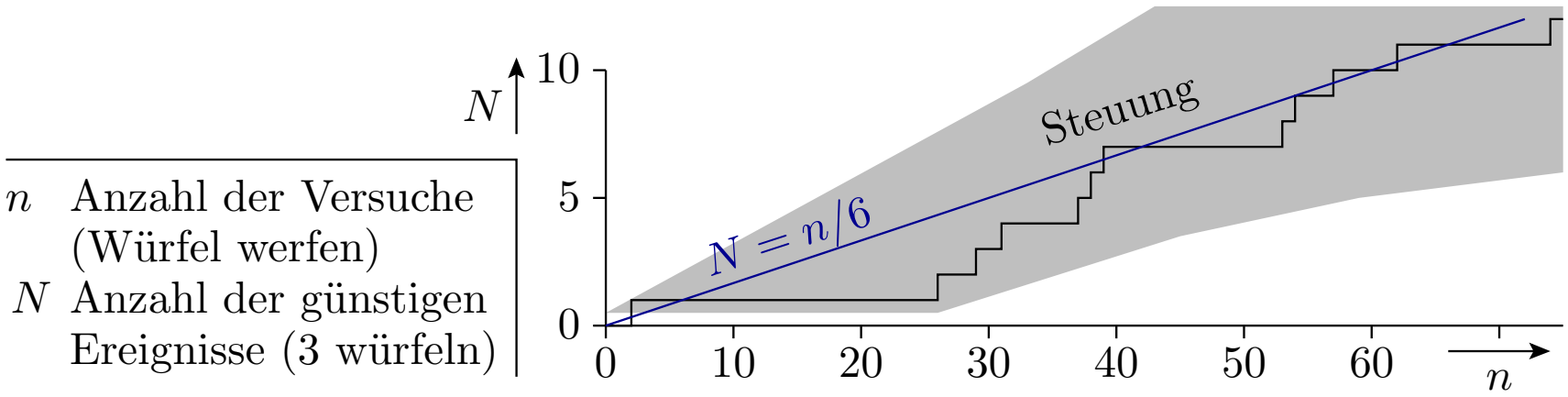
Verhältnis, gegen das bei einem Zufallsexperiment die Anzahl der »günstigen« zur Anzahl aller möglichen Ereignisse mit zunehmender Versuchsanzahl strebt.

Wahrscheinlichkeit, dass eine 3 gewürfelt wird.

- Zufallsexperiment: Würfeln
- Mögliche Ergebnisse: 1, 2, ..., 6
- günstiges Ergebnis: 3



n Anzahl der Versuche (Würfel werfen)
N Anzahl der günstigen Ereignisse (3 würfeln)



Beim Würfeln wird davon ausgegangen, das alle 6 Möglichkeiten gleichwahrscheinlich sind. Mit Versuchsanzahl $n \to \infty$ strebt das Verhältnis aus günstigen Ergebnissen N zur Versuchsanzahl gegen das Verhältnis aus möglichen günstigen und möglichen Ereignissen:

$$p = \lim_{n\to\infty} \left(\frac{N}{n} \right) = \frac{1}{6}$$

Das bedeutet aber nicht, dass bei jedem sechsten Versuch eine 3 gewürfelt wird. Es ist durchaus zu beobachten, dass hintereinander mehrere Dreien und lange Zeit keine Dreien gewürfelt werden.

Erwartungswert

Erwartungswert

Definition Erwartungswert

Im Mittel zu erwartendes Ergebnis eines Zufallsexperiments. Mit ihren Auftrittswahrscheinlichkeiten gewichteter Mittelwert aller Realisierungen, ...

- Mittlere gewürfelte Augenzahl:

$$E(X) = \sum_{i=1}^{6} \frac{i}{6} = 3{,}5$$

- Für einen Bermoulli-Versuch mit der Verteilung:

$$P(X) = \begin{cases} 1-p & \text{für } X = 0 \\ p & \text{für } X = 1 \end{cases}$$

ist der Erwartungswert die Eintrittswahrscheinlichkeit p:

$$E(X) = 0 \cdot (1-p) + 1 \cdot p = p$$

Lineare Transformation, Summe von Zufallsgrößen

Lineare Transformationen sind die Multiplikation und Addition einer Zufallsgröße mit reellen Zahlen. Der Erwartungswert vergrößert und verschiebt sich um dieselben Werte:

$$E\left(a \cdot X + b\right) = a \cdot E\left(X\right) + b$$

Für die Summe von Zufallsgrößen ist der Erwartungswert gleich der Summe der Erwartungswerte:

$$E\left(X + Y\right) = E\left(X\right) + E\left(Y\right)$$

Erwartungswert der Summe von n Bernoulli-Versuchen:

$$E\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} p_i$$

bei gleicher Eintrittswahrscheinlichkeit $p = p_i$:

$$E\left(n \cdot X_i\right) = n \cdot p$$

Schätzen von Erwartungswerten und Wahrsch.

Als Schätzfunktion für den Erwartungswert aus empirischen Daten x_i (Zählwerten) dient im Weiteren das arithmetische Mittel:

$$E(X) \approx \bar{x} = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i$$

Für n Bernoulli-Versuche und x eingetretene Ereignisse:

$$E(X) = p \approx \frac{x}{n}$$

Zu erwartende Abweichungen zwischen Schätzwert und Wahrscheinlichkeitsparameter, wahrscheinliche Bereiche, ... (siehe später TV_F5).

Verkettete Ereignisse

Aufteilen und verketten von Experimenten

Zufallsexperimente lassen sich u.U. in mehrere Teilexperimente aufteilen oder mehrere unabhängige Experimente zu einem zusammenfassen. Im nachfolgenden wird bei jedem Experiment zweimal gewürfelt (Ereignisse A und B, Wertebereich jeweils $\{1, 2, \ldots, 6\}$. Daraus werden mit Vergleichsoperatoren die zweiwertigen Ereignisse C und D gebildet und diese einmal UND- und einmal ODER verknüpft und gezählt.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	... 20 ...	40
A	6	1	5	4	1	1	2	2	4	6	4	3	1	6	5
B	6	5	6	2	1	3	3	6	4	5	1	3	1	4	3
$C = (A > 3)$	1	0	1	1	0	0	0	0	1	1	1	0	0	1	1
$D = (B < 3)$	0	0	0	1	1	0	0	0	0	0	1	0	1	0	0
$E = (C \wedge D)$	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
$F = (C \vee D)$	1	0	1	1	1	0	0	0	1	1	1	0	1	1	1
$\sum C$	1	1	2	3	3	3	3	3	4	5	6	6	6	11	21
$\sum D$	0	0	0	1	2	2	2	2	2	2	3	3	4	6	9
$\sum E$	0	0	0	1	1	1	1	1	1	1	2	2	2	5	6
$\sum F$	1	1	2	3	4	4	4	4	5	6	7	7	8	13	24

Nach 40 Versuchen betragen die Schätzwerte der Wahrscheinlichkeiten als Verhältnis der günstigen Ergebnisse, dass die Bedingungen C bis F erfüllt sind, zur Versuchsanzahl:

Ereignis	Schätzwert	Wahrscheinlichkeit
$C = (A > 3)$	$21/40 = 53\%$	$3/6 = 50\%$
$D = (B < 3)$	$9/40 = 23\%$	$2/6 = 33\%$
$E = (C \wedge D)$	$6/40 = 15\%$	$6/36 = 17\%$
$F = (C \vee D)$	$24/40 = 60\%$	$24/36 = 67\%$

Die Wahrscheinlichkeit als Grenzwerte für $n \to \infty$ ergibt sich für jeden Versuch aus dem Verhältnis der günstigen zur Anzahl der möglichen Ergebnisse. Die Würfelexperimente haben 6 mögliche Ergebnisse. Davon sind für die Ereignisse C und D 3 bzw. 2 günstig. Die verketten Ereignisse E und F haben $6^2 = 36$ mögliche Ergebnisse, von denen 6 bzw. 24 günstig sind.

Die Schätzung einer Wahrscheinlichkeit mit weniger als 100 günstigen Ereignissen ist recht ungenau.

Bedingte Wahrscheinlichkeiten

Bei einer bedingten Wahrscheinlichkeit werden nur die Versuche und Ereignisse gezählt, die die Bedingung erfüllen. Beispiel sei die ODER-Verknüpfung sich ausschließender Ereignisse:

$$E = C \vee D \text{ unter der Bedingung } C \wedge D = 0.$$

																				$\sum$	$\sum$
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	20	16
C	1	0	1	1	0	0	0	0	1	1	1	0	0	1	1	0	1	0	1	1	11	7
D	0	0	0	1	1	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	6	2
$C \vee D$	1	0	1	1	1	0	0	0	1	1	1	0	1	1	1	0	1	0	1	1	13	9

nicht mitgezählte Ereignisse bzw. Summe ohne diese Ereignisse

Sowohl die Anzahl der gezählten Versuche als auch die günstigen Ergebnisse verringern sich um die vier nicht mitzuzählenden Ergebnisse mit $C \wedge D = 1$. Das undokumentierte Aussortieren ungewollter Ergebnisse ist ein unauffälliger und beliebter Trick, Statistiken zu fälschen[9].

[9] Traue nie einer Statistik, die du nicht selbst gefälscht hast

Wahrscheinlichkeit verketteter Ereignisse

- Wahrscheinlichkeit, dass ein Ereignis A nicht eintritt:

$$P\left(\bar{A}\right) = 1 - P\left(A\right) \tag{1}$$

- Wahrscheinlichkeit, dass von zwei unabhängigen Ereignissen A und B beide eintreten:

$$P\left(A \wedge B\right) = P\left(A\right) \cdot P\left(B\right) \tag{2}$$

- Wahrscheinlichkeit, dass von zwei unabhängigen Ereignissen mindestens eines eintritt:

$$\begin{aligned} P\left(A \vee B\right) = P\left(\overline{\bar{A} \wedge \bar{B}}\right) &= 1 - \left(1 - P\left(A\right)\right) \cdot \left(1 - P\left(B\right)\right) \\ &= P\left(A\right) + P\left(B\right) - P\left(A\right) \cdot P\left(B\right) \end{aligned} \tag{3}$$

Beispielaufgabe

In einem System mit drei Fehlern seien diese unabhängig voneinander mit den Wahrscheinlichkeiten $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$ nachweisbar. Wie groß sind die Wahrscheinlichkeiten der verketten Ereignisse, dass

E_1 : alle Fehler,
E_2 : kein Fehler,
E_3 : mindestens ein Fehler und
E_4 : genau zwei Fehler nachgewiesen werden?

Hilfestellung:

- Definition von Ereignissen F_i für Fehler i nachweisbar.
- Beschreibung der Ereignisse E_i durch logische Verknüpfungen von Ereignissen F_i bzw. anderer Ereignisse E_i, ...

Lösung

- Alle Fehler nachweisbar:

$$\begin{aligned} E_1 &= F_1 \wedge F_2 \wedge F_3 \\ P(E_1) &= P(F_1) \cdot P(F_2) \cdot P(F_3) \\ &= p_1 \cdot p_2 \cdot p_3 = 10\% \cdot 5\% \cdot 20\% = 0{,}1\% \end{aligned}$$

- Kein Fehler nachweisbar:

$$\begin{aligned} E_2 &= \overline{F_1 \vee F_2 \vee F_3} = \bar{F}_1 \wedge \bar{F}_2 \wedge \bar{F}_3 \\ P(E_2) &= (1 - P(F_1)) \cdot (1 - P(F_2)) \cdot (1 - P(F_3)) \\ &= (1 - p_1) \cdot (1 - p_2) \cdot (1 - p_3) = 90\% \cdot 95\% \cdot 80\% = 68{,}4\% \end{aligned}$$

- Mindestens ein (nicht kein) Fehler nachweisbar:

$$\begin{aligned} E_3 &= \bar{E}_2 \\ P(E_3) &= 1 - P(E_2) = 1 - 68{,}4\% = 31{,}6\% \end{aligned}$$

- Genau 2 Fehler werden nachgewiesen, wenn
  - die ersten beiden und der dritte nicht,
  - die zweiten beiden und der erste nicht oder
  - der erste und der dritte, aber nicht der zweite

  nachgewiesen werden (ausschließendes ODER):

$$
\begin{aligned}
E_4 &= \left(F_1 \wedge F_2 \wedge \bar{F}_3\right) \vee \left(\bar{F}_1 \wedge F_2 \wedge F_3\right) \vee \left(F_1 \wedge \bar{F}_2 \wedge F_3\right) \\
P\left(E_4\right) &= p_1 \cdot p_2 \cdot (1 - p_3) + (1 - p_1) \cdot p_2 \cdot p_3 + p_1 \cdot (1 - p_2) \cdot p_3 \\
&= 10\% \cdot 5\% \cdot 80\% + 90\% \cdot 5\% \cdot 20\% + 10\% \cdot 95\% \cdot 20\% = 3{,}2\%
\end{aligned}
$$

Abhängige Ereignisse

Definition Abhängigkeit von Ereignissen

Ein Ereignis B ist von einem Ereignis A abhängig, wenn das Eintreten von A die Eintrittswahrscheinlichkeit von B beeinflusst.

Für sich ausschließende Ereignisse ist die Wahrscheinlichkeit für das gleichzeitige Eintreten

$$P(A \wedge B) = 0 \tag{4}$$

und für das Eintreten des einen oder des anderen Ereignisses:

$$P(A \vee B)|_{P(A \wedge B)=0} = P(A) + P(B) \tag{5}$$

Für abhängige, aber sich nicht ausschließende Ereignisse ist das Experiment so umformulieren, dass die UND oder ODER zu verknüpfenden Teilereignisse danach entweder unabhängig sind oder sich gegenseitig ausschließen.

Beispielaufgabe »abhängiger Fehlernachweis«

Wie groß sind die Wahrscheinlichkeiten, dass von zwei Fehlern im System 0, 1 oder 2 Fehler nachweisbar sind, wenn die Nachweiswahrscheinlichkeit für Fehler 1 unabhängig vom Nachweis von Fehler 2 $p_1 = 10\%$ beträgt und für Fehler 2 bei Nachweis von Fehler 1 $p_2 = 20\%$ und sonst 0 beträgt. (Der Nachweis des zweiten Fehler hängt vom Nachweis des ersten ab.)

Lösung: Definition von Ereignissen F_i für Fehler i nachweisbar und E_i für i Fehler nachweisbar.

- Kein Fehler ist nachweisbar, wenn der erste Fehler nicht nachweisbar ist[10]:

$$\begin{aligned} E_0 &= \bar{F}_1 \\ P(E_0) &= 1 - P(F_1) = 1 - p_1 = 1 - 10\% = 90\% \end{aligned}$$

[10] Der Fall, Nachweis des zweiten ohne den ersten Fehler ist ausgeschlossen.

- Ein Fehler ist nachweisbar, wenn der erste Fehler nachweisbar ist und der zweite nicht:

$$\begin{aligned} E_1 &= F_1 \wedge \bar{F}_2 \\ P(E_1) &= p_1 \cdot (1 - p_2) = 10\% \cdot 80\% = 8\% \end{aligned}$$

- Zwei Fehler sind nachweisbar, wenn beide Fehler nachweisbar sind:

$$\begin{aligned} E_2 &= F_1 \wedge F_2 \\ P(E_2) &= p_1 \cdot p_2 = 10\% \cdot 20\% = 2\% \end{aligned}$$

- Probe: Summe der Wahrscheinlichkeiten aller möglichen Ergebnisse muss immer 100% sein:

$$P(E_0) + P(E_1) + P(E_2) = 90\% + 2\% + 8\% = 100\%\surd$$

Beispiel »Bedatungswahrscheinlichkeit«

Wie groß ist die Wahrscheinlichkeit, dass ein 8-Bit-Vektor für eine Service-Anfrage an eine Schaltung mit dem Wert $\mathbf{x} =$ "11111110" angefordert wird, wenn

1. unabhängig voneinander für jedes Bit mit einer Wahrscheinlichkeit[11] von $g = 50\%$ zufällig eine Eins und sonst eine Null gewählt wird.
2. Dasselbe wie im Aufgabenteil zuvor, nur mit $g = 60\%$.
3. Dasselbe wie in den Aufgabenteilen zuvor, nur dass für die höchstwertigen vier Bits immer derselben Zufallswert ausgewählt wird.

[11] Die Wahrscheinlichkeit g wird auch als Wichtung der Bitstelle bezeichnet. Bitweise Wichtung wird beim Test digitaler Schaltungen eingesetzt, um die Nachweiswahrscheinlichkeiten sehr schlecht nachweisbarer Fehler zu erhöhen.

Lösung

Definieren von Ereignissen G_i, dass für Bit i eine Eins ausgewählt wird.

- Für die beiden ersten Aufgabenteile gilt:

$$\begin{aligned} \mathbf{x} = \text{"}11111110\text{"} &= G_7 \wedge G_6 \wedge G_5 \wedge G_4 \wedge G_3 \wedge G_2 \wedge G_1 \wedge \bar{G}_0 \\ P\left(\mathbf{x} = \text{"}11111110\text{"}\right) &= g^7 \cdot (1-g) \end{aligned}$$

- Für den letzten Aufgabenteil folgt aus $G_7 = G_6 = G_5 = G_4$:

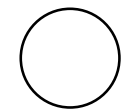
$$\begin{aligned} \mathbf{x} = \text{"}11111110\text{"} &= G_4 \wedge G_3 \wedge G_2 \wedge G_1 \wedge \bar{G}_0 \\ P\left(\mathbf{x} = \text{"}11111110\text{"}\right) &= g^4 \cdot (1-g) \end{aligned}$$

g	50%	60%
G_4 bis G_7 unabhängig	$2^{-8} \approx 0{,}4\%$	$0{,}6^7 \cdot 0{,}4 = 1\%$
$G_7 = G_6 = G_5 = G_4$	$2^{-5} \approx 3\%$	$0{,}6^4 \cdot 0{,}4 = 5\%$

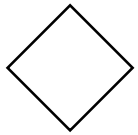
Fehlerbaumanalyse

Fehlerbaumanalyse (FTA – fault tree analysis)

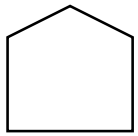
Verfahren zur Abschätzung der Eintrittswahrscheinlichkeit von Ereignissen in Abhängigkeit vom Eintreten anderer Ereignisse (Gefahrensituationen, Ausfälle, Service-Versagen, ...). Einteilung der Ereignisse:



Ereignis mit bekannter oder auf anderem Wege abgeschätzter Eintrittswahrscheinlichkeit.



Ereignis, dessen Eintrittswahrscheinlichkeit nicht untersucht wurde.

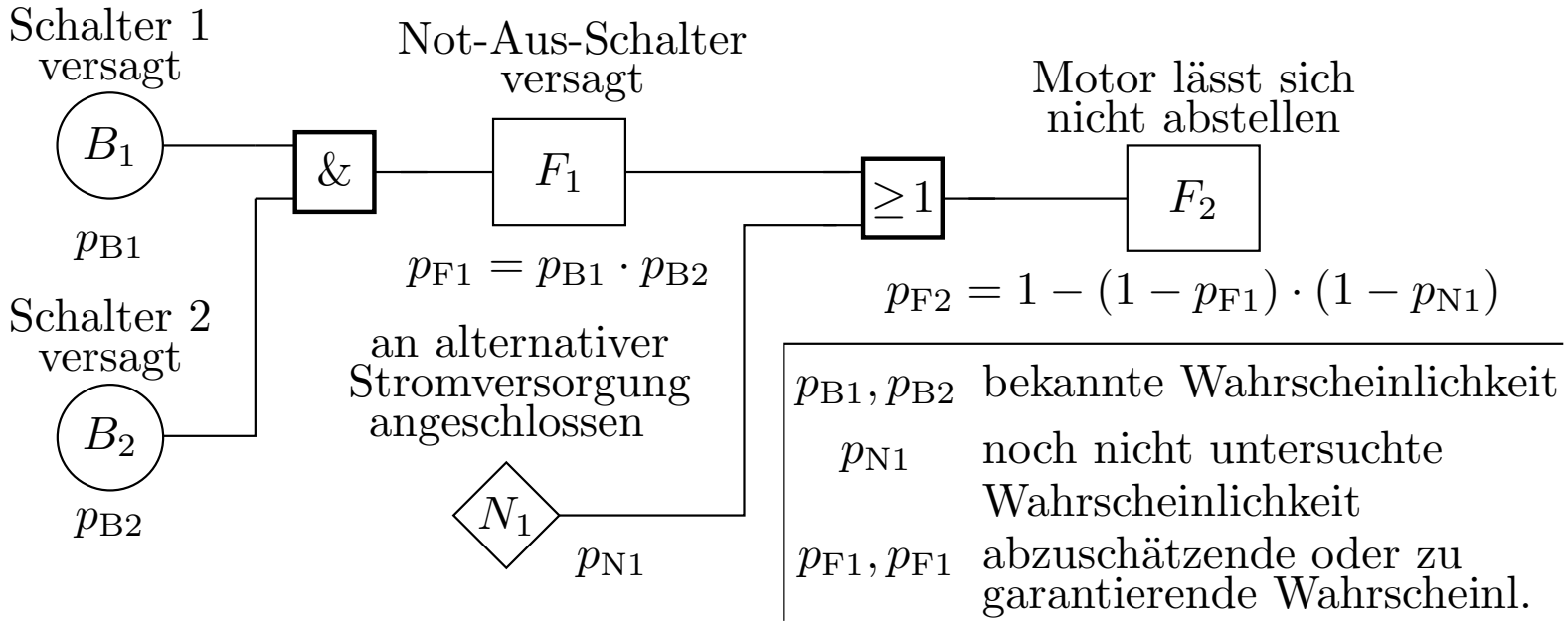


Ereignis im gewöhnlichen Betrieb, das in Kombination mit anderen Probleme verursachen kann.

Ereignis, dessen Eintrittswahrscheinlichkeit aus denen von ○, ◇ oder ⬠-Ereignissen folgt.

Verknüpfung mit UND, ODER, NICHT.

Beispiel: Motor lässt sich nicht abstellen



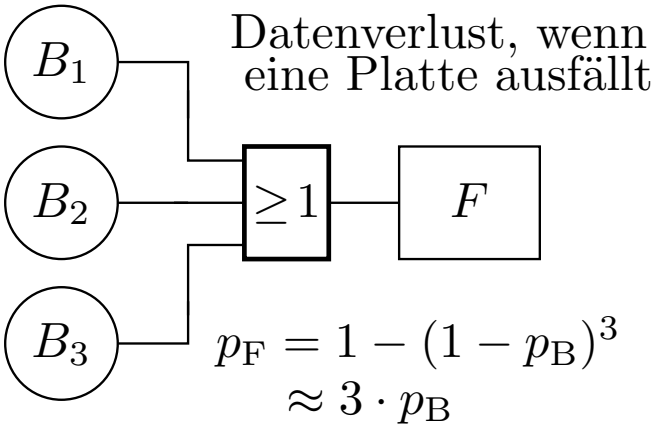
Formulierbare Aufgabe: Wenn $p_{B1} = p_{B2} = 10^{-3}$ ist und $p_{F2} \leq 10^{-6}$ sein darf

- ist dieses Ziel erreichbar?
- Wie groß darf p_{N1} dann maximal sein?

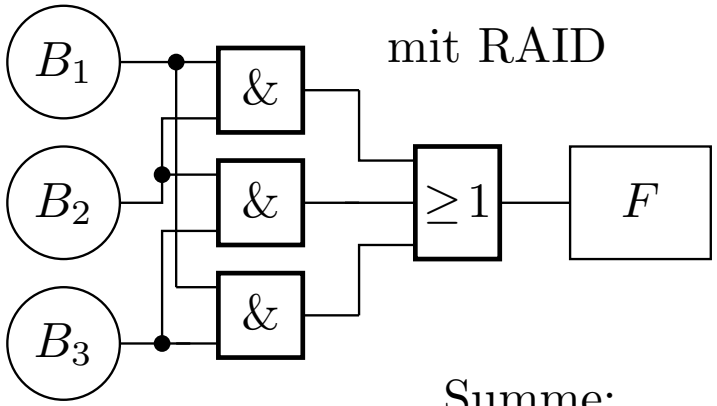
(Ziel hier nur mit $p_{N1} = 0$ erreichbar. Realistisch/andere Lösung?)

Datenverlust mit RAID

Bei einem RAID 3 und RAID 5 tritt nur ein Datenverlust ein, wenn zwei Platten gleichzeitig versagen. Fehlerbaum für $n = 3$ Platten:



$$p_F = 1 - (1 - p_B)^3 \approx 3 \cdot p_B$$



B_3	B_2	B_1	F	
0	0	0	0	
0	0	1	0	
0	1	0	0	
0	1	1	1	$p_B^2 \cdot (1 - p_B)$
1	0	0	0	
1	0	1	1	$p_B^2 \cdot (1 - p_B)$
1	1	0	1	$p_B^2 \cdot (1 - p_B)$
1	1	1	1	p_B^3

Summe:

$$p_F = 3 \cdot p_B^2 - 2 \cdot p_B^3$$

p_B	Wahrscheinlichkeit Plattenversagen
p_F	Wahrscheinlichkeit Datenverlust

Rekonvergente Auffächerungen

Wenn sich der Bedingungsfluss verzweigt und wieder zusammentrifft, werden zum Teil abhängige Ereignisse verknüpft. Im Beispiel:

$$F = B_1 B_2 \vee B_2 B_3 \vee B_1 B_3$$

haben die ODER-verknüpften UND-Terme jeweils eine gemeinsame Variable. Für Wahrscheinlichkeitsabschätzung ungeeignet.

Umstellung in Verknüpfung sich ausschließender Ereignisse:

- disjunktive Normalform:

$$\begin{aligned} F &= B_1 B_2 \bar{B}_3 \vee \bar{B}_1 B_2 B_3 \vee B_1 \bar{B}_2 B_3 \vee B_1 B_2 B_3 \\ p_\mathrm{F} &= p_\mathrm{B}^2 \cdot (1-p_\mathrm{B}) + p_\mathrm{B}^2 \cdot (1-p_\mathrm{B}) + p_\mathrm{B}^2 \cdot (1-p_\mathrm{B}) + p_\mathrm{B}^3 = 3 \cdot p_\mathrm{B}^2 - 2 \cdot p_\mathrm{B}^3 \end{aligned}$$

- Alternative Umstellung:

$$\begin{aligned} F &= B_1 B_2 \vee \bar{B}_1 B_2 B_3 \vee B_1 \bar{B}_2 B_3 \\ p_\mathrm{F} &= p_\mathrm{B}^2 + p_\mathrm{B}^2 \cdot (1-p_\mathrm{B}) + p_\mathrm{B}^2 \cdot (1-p_\mathrm{B}) = 3 \cdot p_\mathrm{B}^2 - 2 \cdot p_\mathrm{B}^3 \end{aligned}$$

Verallgemeinerung auf n Platten

Die Wahrscheinlichkeit, dass mindestens eine von n Platten versagt, ist etwa:

$$p_{\mathrm{F}} \approx n \cdot p_{\mathrm{B}}$$

(p_{B} – Wahrscheinlichkeit, dass eine Platte versagt). Die Wahrscheinlichkeit, dass mindestens zwei Platten versagen, ist eins abzüglich der Wahrscheinlichkeiten, dass null oder eine Platte versagen:

$$p_{\mathrm{F}} \approx 1 - (1 - p_{\mathrm{B}})^n - n \cdot p_{\mathrm{B}} \cdot (1 - p_{\mathrm{B}})^{n-1}$$

Die Anzahl der versagenden Platten ist bei dieser Aufgabenstellung binomialverteilt (siehe Foliensatz 2, Abschnitt »Verteilungen, Binomialverteilung«).

Zur Geschichte der Fehlerbaumanalyse

- Einführung 1960: Abschlusssicherheitsbewertung von Interkontinentalraketen vom Typ LGM-30 Minuteman.
- Folgejahre: Auch für Sicherheitsbewertung kommerzieller Flugzeuge.
- Ab 70er bis 80er Jahre: Sicherheitsbewertung Atomkraftwerke.
- Später auch Automobilindustrie und deren Zulieferer.

Beim Einsatz zur Sicherheitsbewertung:

- sind die sicherheitsrelevanten Ereignisse,
- die Basisereignisse und
- deren Wahrscheinlichkeiten

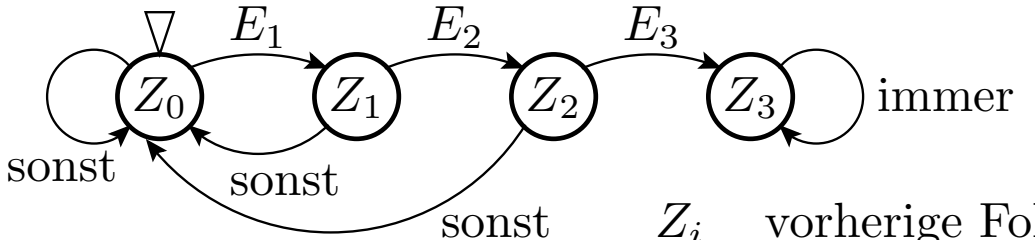
zuvor auf andere Weise abzuschätzen: Vorexperimente, Expertenbefragungen, Ursache-Wirkungs- (Ishikawa-) Diagramme, ...

Markov-Ketten

Markov-Ketten[12]

Modellierung eines stochastischen Prozesses durch einen Zustandsautomaten mit Übergangswahrscheinlichkeiten an den Kanten, z.B. zur Bestimmung von Fehlernachweis- und Fehlerbeseitigungswahrscheinlichkeiten.

Fehlernachweis mit einer Eingabefolge $E_1E_2E_3$:

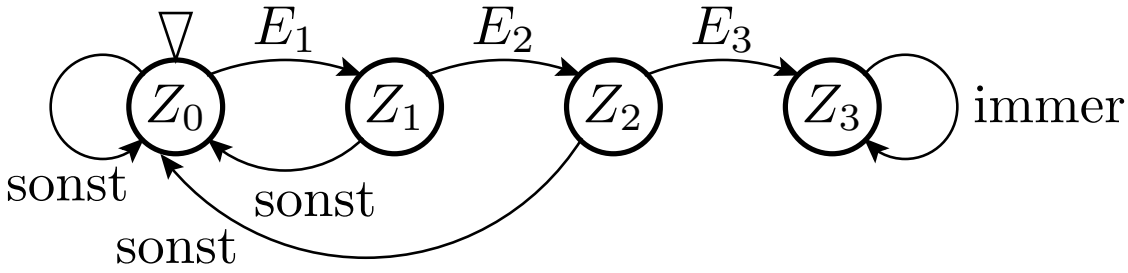


Z_i vorherige Folge bestand aus den ersten i richtigen Werten

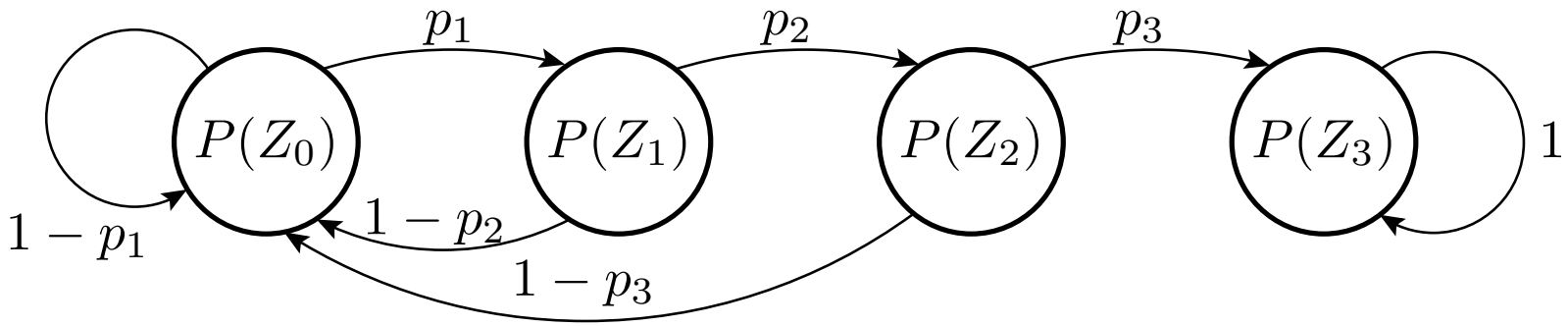
E_i Wert ist X_i

Start im Zustand Z_0 »keine richtige Eingabe« und Verbleib nach drei richtigen Eingaben im Zustand Z_3 »Fehler nachgewiesen«.

[12] Nach Andrej Andreevič Markov, russischer Mathematiker, 1856-1922.

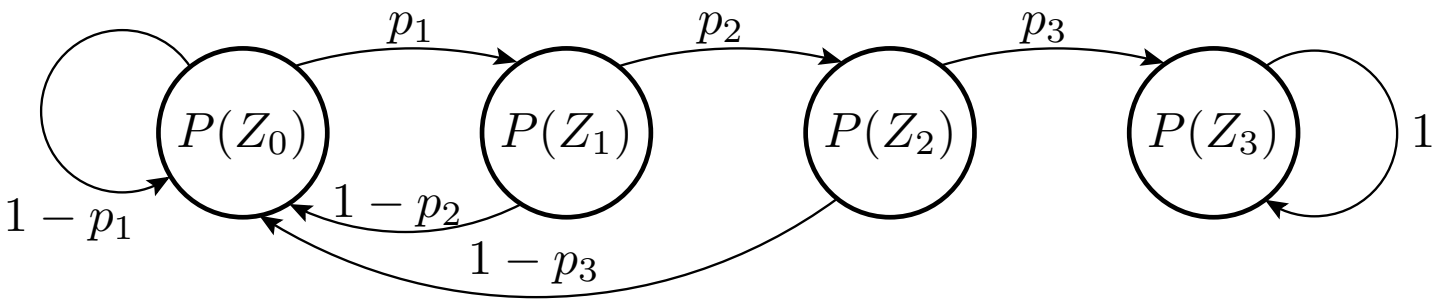


Zur Umwandlung in eine Markov-Kette werden die Übergangsbedingungen durch die Übergangswahrscheinlichkeiten p_{E1} bis p_{E3} und die Zustände durch Zustandswahrscheinlichkeiten $P\left(Z_i\right)$ ersetzt.



Der Anfangszustand hat zu Beginn die Zustandswahrscheinlichkeit $P\left(Z_0\right)=1$ und die anderen $P\left(Z_{i\neq 0}\right)=0$.

Simulation von Markov-Ketten



Eine Markov-Kette beschreibt ein lineares Gleichungssytem zur Berechnung der Zustandswahrscheinlichkeiten für den Folgeschritt:

$$\begin{pmatrix} P(Z_0) \\ P(Z_1) \\ P(Z_2) \\ P(Z_3) \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_2 & 1-p_3 & 0 \\ p_1 & 0 & 0 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} P(Z_0) \\ P(Z_1) \\ P(Z_2) \\ P(Z_3) \end{pmatrix}_{n-1}$$

mit $\begin{pmatrix} P(Z_0) & P(Z_1) & P(Z_2) & P(Z_3) \end{pmatrix}^T = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$.

$$\begin{pmatrix} P(Z_0) \\ P(Z_1) \\ P(Z_2) \\ P(Z_3) \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_2 & 1-p_3 & 0 \\ p_1 & 0 & 0 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} P(Z_0) \\ P(Z_1) \\ P(Z_2) \\ P(Z_3) \end{pmatrix}_{n-1}$$

Zur Kontrolle:

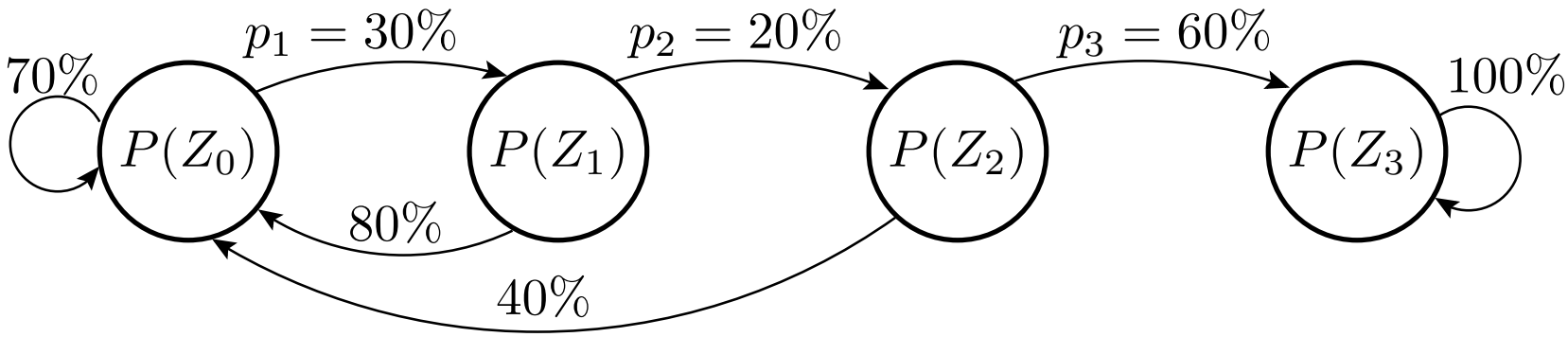
- Die Summe der Wahrscheinlichkeiten in jeder Spalte muss eins sein.
- Die Summe der Zustandswahrscheinlichkeiten $P(Z_i)$ muss in jedem Schritt eins sein.

$$\begin{pmatrix} P(Z_0) \\ P(Z_1) \\ P(Z_2) \\ P(Z_3) \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_2 & 1-p_3 & 0 \\ p_1 & 0 & 0 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} P(Z_0) \\ P(Z_1) \\ P(Z_2) \\ P(Z_3) \end{pmatrix}_{n-1}$$

Simulation mit Octave bzw. Matlab:

```
p1=...;  p2=...;  p3=...;
M=[1-p1  1-p2  1-p3  0;
     p1     0     0    0;
      0     p2    0    0;
      0     0     p3   1];
Z=[1;  0;  0;  0];
for idx=1:100
 Z = M * Z;
 printf('%3i %6.2f%% %6.2f%% %6.2f%% %6.2f%%\n',  ...
          idx,  100*Z);
end;
```

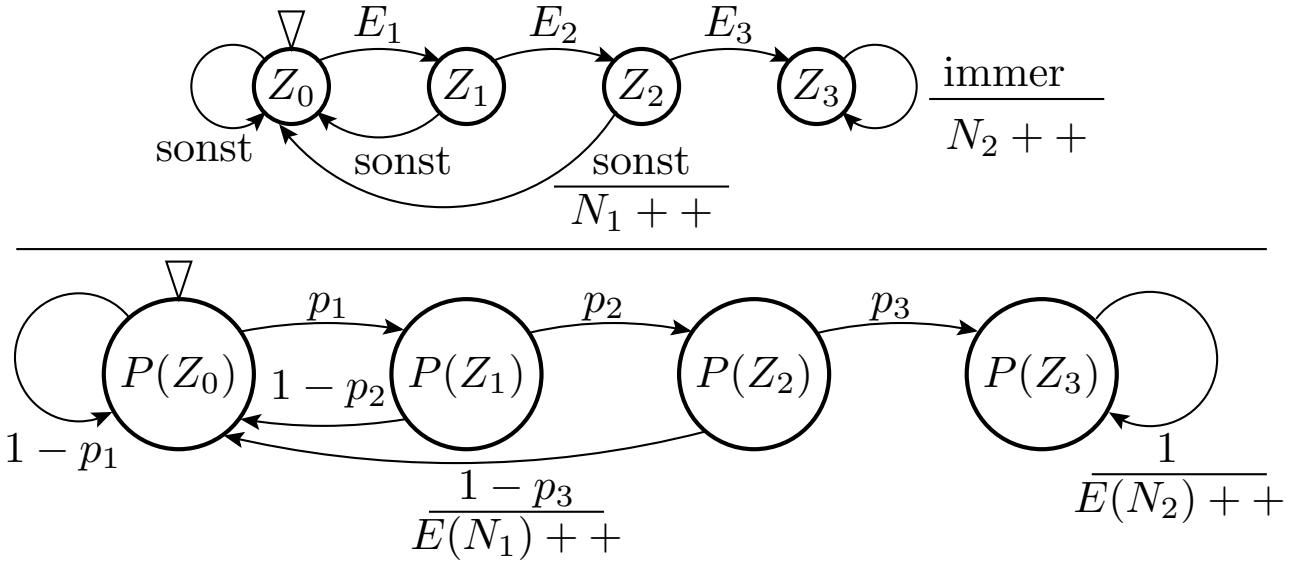
Simulation mit den Beispielwerten $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



Schritt	$P(Z_0)$	$P(Z_1)$	$P(Z_2)$	$P(Z_3)$	Summe
0	100,00	0,00	0,00	0,00	100,00
1	70,00	30,00	0,00	0,00	100,00
2	73,00	21,00	6,00	0,00	100,00
3	70,30	21,90	4,20	3,60	100,00
4	68,41	21,09	4,38	6,12	100,00
...	...	...	...	...	...
10	59,43	18,34	3,77	18,46	100,00
...	...	...	...	...	...
50	19,27	5,95	1,22	73,56	100,00
...	...	...	...	...	...
100	4,73	1,46	0,30	93,53	100,00

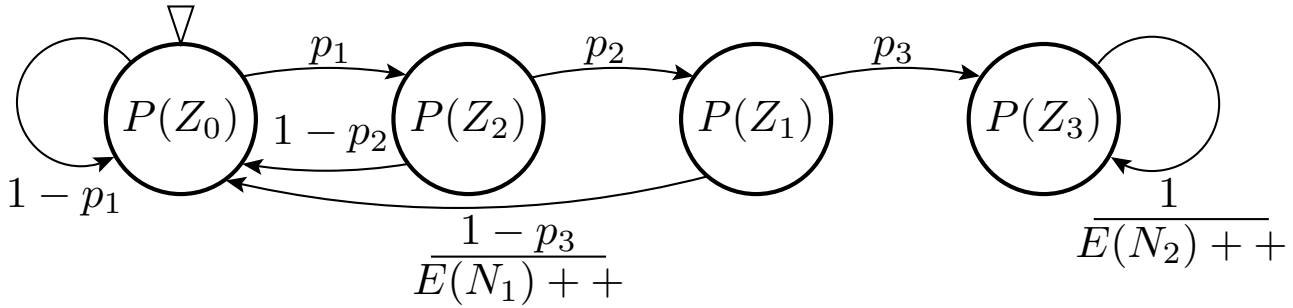
Kantenkosten

Mit Zählern an den Kanten lässt sich zusätzlich die zu erwartende Anzahl der Kantenübergänge bestimmen:



Der Zähler N_1 zählt, wie oft nach zwei richtigen Eingaben eine falsche folgt, der Zähler N_2 die Anzahl der Eingaben im Zustand Z_3 (Fehler nachgewiesen). Die zu erwartende Anzahl der Schritte bis zum Nachweis ist $n - N_2$ (n – Anzahl simulierter Schritte).

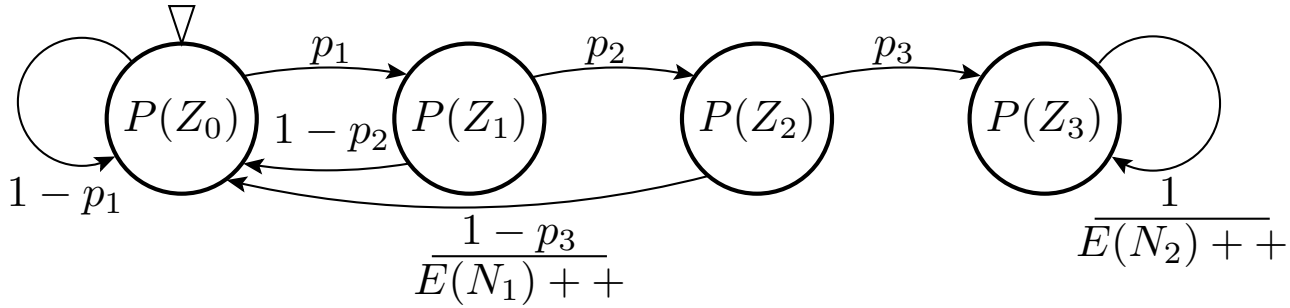
Die korrespondierenden Zähler in der Markov-Kette berechnen die Erwartungswerte der Zählgrößen.



Erweiterung des Simulationsprogramms:

```
...
N1=0; N2=0;
for idx=1:100
 Z = M * Z;
 N1 = N1+Z(3)*(1-p3);
 N2 = N2+Z(4);
 printf('%3i %6.2f%% %6.2f%% %6.2f%% %6.2f%%', ...
        idx, 100*Z);
 printf(' %6.2f %6.2f\n', N1, N2);
end;
```

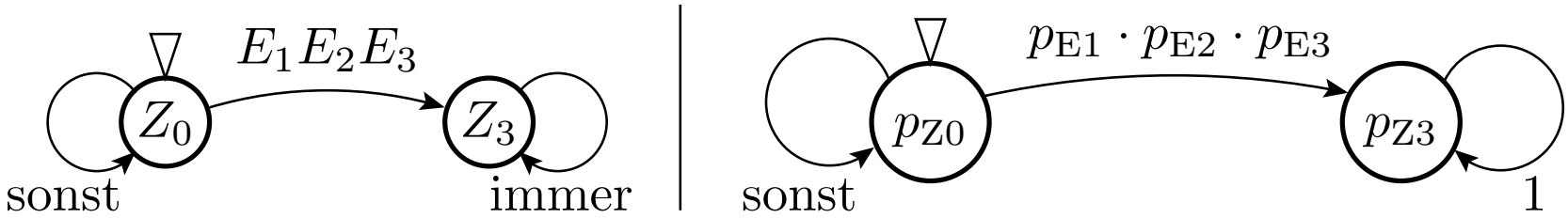
Simulation mit den Beispielwerten $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



n	$P(Z_0)$	$P(Z_1)$	$P(Z_2)$	$P(Z_3)$	$E(N_1)$	$E(N_2)$
1	70,00%	30,00%	0,00%	0,00%	0,00	0,00
2	73,00%	21,00%	6,00%	0,00%	0,02	0,00
3	70,30%	21,90%	4,20%	3,60%	0,04	0,04
4	68,41%	21,09%	4,38%	6,12%	0,06	0,10
...	...	...	...	...	...	...
10	57,78%	17,83%	3,67%	20,73%	0,15	0,99
...	...	...	...	...	...	...
50	18,74%	5,78%	1,19%	74,29%	0,50	22,23
...	...	...	...	...	...	...
100	4,59%	1,42%	0,29%	93,71%	0,63	65,43

- Die zu erwartende Anzahl der Schritte bis zum Nachweis $n - N_2$ (n – Anzahl der simulierten Schritte) ist etwa 35.

»Drei richtige Eingaben« als Einzelereignis



Gleichungssystem der modifizierten Markov-Kette:

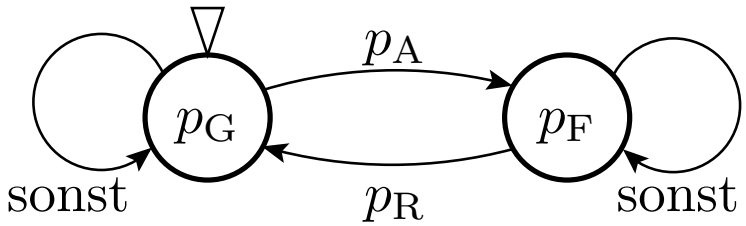
$$\begin{pmatrix} p_{Z0} \\ p_{Z3} \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_{E1} \cdot p_{E2} \cdot p_{E3} & 0 \\ p_{E1} \cdot p_{E2} \cdot p_{E3} & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{Z0} \\ p_{Z3} \end{pmatrix}_n \text{ mit } \begin{pmatrix} p_{Z0} \\ p_{Z3} \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{aligned} p_{Z0}(n) &= (1 - p_{E1} \cdot p_{E2} \cdot p_{E3}) \cdot p_{Z0}(n-1) = (1 - p_{E1} \cdot p_{E2} \cdot p_{E3})^n \\ p_{Z3}(n) &= 1 - p_{Z0}(n) = 1 - (1 - p_{E1} \cdot p_{E2} \cdot p_{E3})^n \end{aligned}$$

Wie stark werden $p_{Z0}(n)$ und $p_{Z3}(n)$ von den Ergebnissen der Simulation mit allen vier Zuständen auf den Folien zuvor abweichen?

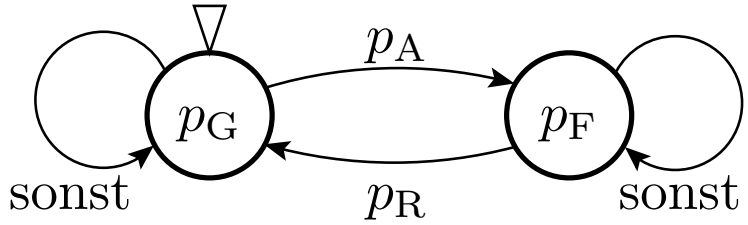
Reparaturprozess als Markov-Kette

Ein System sei zu Beginn funktionsfähig (Zustand G), fällt in jedem Zeitschritt, wenn es ganz ist, mit einer Wahrscheinlichkeit p_A aus (Übergang in Zustand F) und wird, wenn es kaputt ist, mit einer Wahrscheinlichkeit p_R repariert (Übergang in Zustand G):

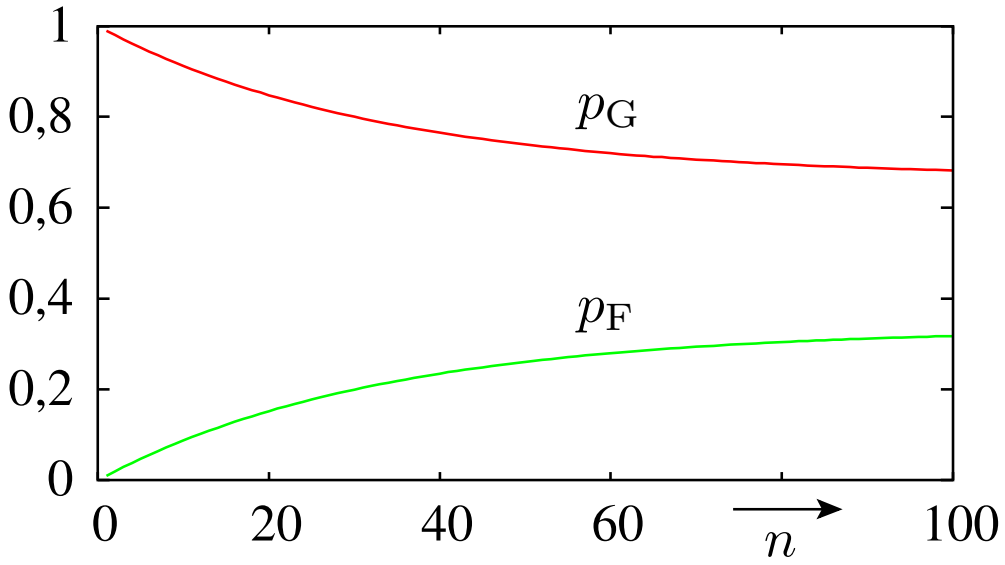


Beschreibung als simulierbares Gleichungssystem:

$$\begin{pmatrix} p_\mathrm{G} \\ p_\mathrm{F} \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_\mathrm{A} & p_\mathrm{R} \\ p_\mathrm{A} & 1-p_\mathrm{R} \end{pmatrix} \cdot \begin{pmatrix} p_\mathrm{G} \\ p_\mathrm{F} \end{pmatrix}_n \text{ mit } \begin{pmatrix} p_\mathrm{G} \\ p_\mathrm{F} \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$



Simulation mit $p_A = 1\%$ und $p_R = 2\%$:

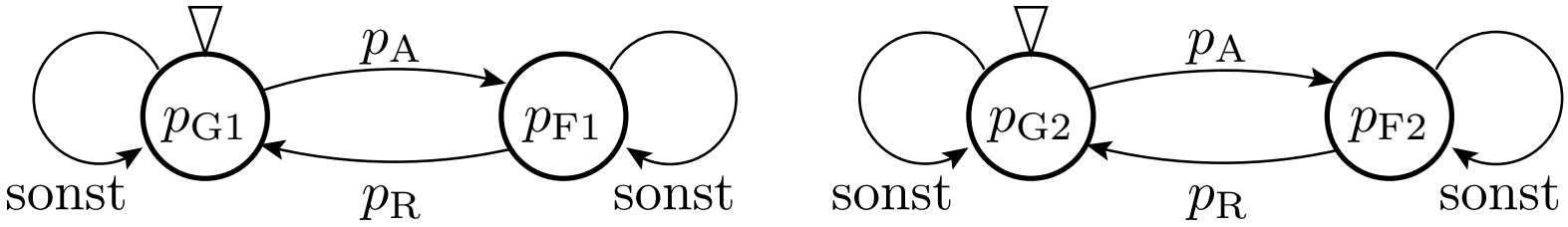


Für große n strebt der Reparaturprozess gegen den stationären Zustand:

$$p_G = \frac{p_R}{p_R + p_A};\ p_F = \frac{p_A}{p_R + p_A}$$

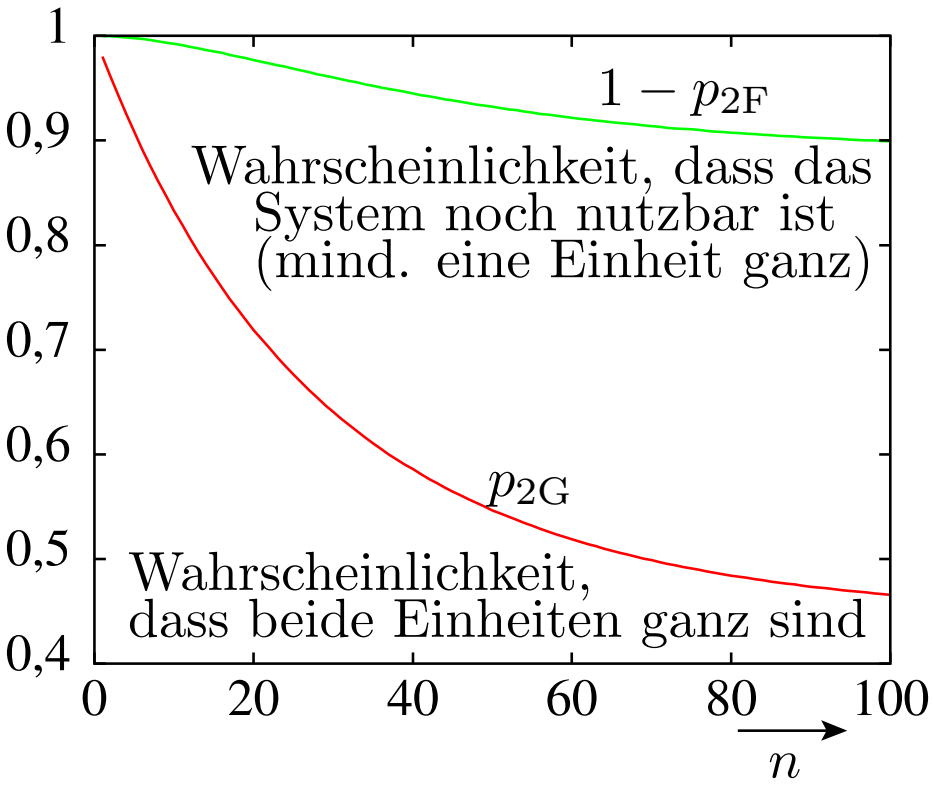
Reparatur mit Redundanz

System aus zwei gleichartigen Teilsystemen, das solange funktioniert, wie ein Teilsystem funktioniert:




```
pA=0.01; pR=0.02;
M=[1-pA  pR; pA  1-pR];
Z=[1; 0];
for n=1:100
  Z = M * Z;
  p2G(n)=Z(1)**2; % beide Einheiten ganz
  p2F(n)=Z(2)**2; % beide Einheiten defekt
end;
plot(1:100, p2G, 1:100, 1-p2F)
```

Simulation mit $p_A = 1\%$ und $p_R = 2\%$:



n Anzahl der Simulationsschritte

Fehlernachweis

Fehlernachweiswahrscheinlichkeit

Ein Fehler wird nachgewiesen, wenn er eine FF verursacht. Die Nachweiswahrscheinlichkeit für einen Fehler i ist der Kehrwert der mittleren Anzahl von SL je FF, die der Fehler verursacht:

$$p_i = \frac{1}{x_i}$$

Die Wahrscheinlichkeit für den Nachweis mit n SL:

$$p_i\left(n\right) = 1 - \left(1 - p_i\right)^n$$

Voraussetzung: Der Fehler wird von jeder SL unabhängig von den anderen SL mit p_i nachgewiesen. Gilt genau genommen nur für SL ohne Gedächtnis. Mit Gedächtnis Modellierung durch Markov-Ketten. Aber für sehr lange Testsätze, seltene FF, Neuinitialisierung nach erkannten FF, ... auch für Systeme mit Gedächtnis brauchbar (siehe große Übung, Aufgabe »Speicherfehler«).

Übergang zur e-Funktion

$$p_i\left(n\right) = 1 - e^{n \cdot \ln(1-p_i)}$$

mit der Taylor-Reihe

$$\ln\left(1-p_i\right) = -\sum_{k=1}^{\infty} \frac{p_i^k}{k} = -\left(p_i + \frac{p_i^2}{2} + \ldots\right)$$

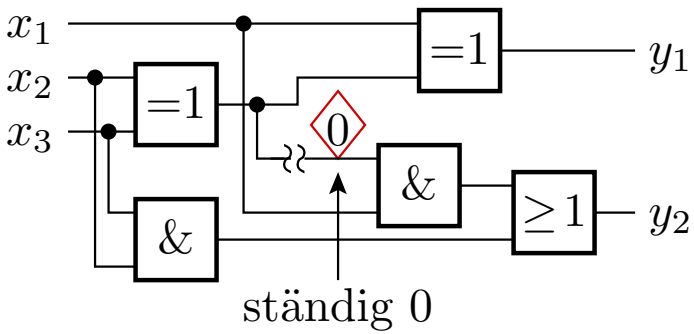
Für den für die Testauswahl interessierender Bereich[13] $p_i < 0{,}1$:

$$\boxed{p_i\left(n\right) = 1\text{-}e^{-n \cdot p_i}} \tag{6}$$

[13] Gut nachweisbare Fehler mit $p_i \gg \frac{1}{n}$ werden sicher erkannt.

Nachweiswahrscheinlichkeit eines Haftfehlers

Die Beispielschaltung enthält einen sa0-Fehler (Gattereingang ständig 0). Nachweis mit zwei der acht Eingabemöglichkeiten. Nachweiswahrscheinlichkeit gleich Summe der Auftrittshäufigkeiten beider Eingaben:



Eingaben die den Fehler nachweisen

Eingabe x_3	x_2	x_1	Ausgabe y_2	y_1	Auftrittshäufigkeit		
0	0	0	0	0	0,125	0,1	0,1
0	0	1	0	1	0,125	0,05	0,1
0	1	0	0	1	0,125	0,15	0,2
0	1	1	1	0	0,125	0,2	0,05
1	0	0	0	1	0,125	0,05	0,2
1	0	1	1	0	0,125	0,2	0,05
1	1	0	1	0	0,125	0,05	0,2
1	1	1	1	1	0,125	0,2	0,1
Nachweiswahrscheinlichkeit:					0,25	0,4	0,1

Nachweiswahrscheinlichkeiten hängen offenbar nicht nur vom Fehler, sondern auch von den Auftrittshäufigkeiten der Eingaben ab.

Beispielaufgabe

Für einen Speicher mit 2^{32} Speicherplätzen sei angenommen, dass kein Fehler seltener als im Mittel aller 50 Zugriffe auf einen der 2^{32} Speicherplätze eine FF verursacht.

1. Ab welcher Testsatzlänge n in Speicherzugriffen erkennt ein Zufallstest jeden Fehler mindestens mit einer Wahrscheinlichkeit von 99%?
2. Wie viele Stunden dauert der Test mindestens bei 10^8 Speicherzugriffen pro Sekunde?

Lösung

1. Mindestnachweiswahrscheinlichkeit je Speicherzugriff:

$$p_{\min} = \left(50 \cdot 2^{32}\right)^{-1}$$

Mindestnachweiswahrscheinlichkeit bei n Speicherzugriffen:

$$p_{\min}(n) = 1 - e^{-n \cdot p_{\min}}$$

Gesuchte Testsatzlänge:

$$n = -\frac{1}{p_{\min}} \cdot \ln\left(1 - p_{\min}(n)\right) = -50 \cdot 2^{32} \cdot \ln(1\%) \approx 10^{12}$$

2. Mindesttestdauer: $t = n \cdot 10^{-8}\,\mathrm{s} = 2{,}75\,\mathrm{h}$

Kenngrößen der Verlässl.

Anzahl Fehler und FF

Abschätzung der Anzahl der Fehler und FF

Empirische Abschätzung über Metriken[14] (vergl. Foliensatz TV_F1, Abschn. 2.2 »Fehler und FF«)

- Arbeitsaufwand in Manntagen, -wochen oder -monaten,
- Programmgröße in NLOC (Netto Lines of Code),
- Schaltkreisgröße in Transistoren oder Gatteräquivalenten, ...

und aus Erfahrungswerten abgeleiteten Güteparametern

- 10 bis 100 Fehler auf 1000 NLOC,
- 200 Defekte auf 10^6 eingesetzte Schaltkreise,
- 1 bis 10 FF pro Tag Systemnutzung, ...

Abschätzung über die Menge der potentiellen Fehler und FF (Threads) und ihren Auftrittswahrscheinlichkeiten[15].

[14] Die Abschätzung über Metriken ist einfacher und gebräuchlicher.

[15] Abschätzungen über Threads und deren Eintrittswahrscheinlichkeiten stellt die Wirkung der »Means« besser dar.

Erwartungswert von Zählgrößen

Annahme von N potentiell zu zählenden Ereignissen, die mit einer Wahrscheinlichkeit p_i eintreten. Der anteilige Zählwert von jedem potentiellen Ereignis ist eine Zufassgröße X_i mit dem Wertebereich $\{0, 1\}$ (Bernoulli-Verteilung):

$$X_i = \begin{cases} 0 & \text{Fehler nicht vorhanden: } P(X_i = 0) = 1 - p_i \\ 1 & \text{Fehler vorhanden: } P(X_i = 1) = p_i \end{cases}$$

Der Zählwert ist die Summe dieser Zufallsgrößen:

$$X = \sum_{i=1}^{N} X_i$$

Erwartungswert:

$$E(X) = \sum_{i=1}^{N} E(X_i) = \sum_{i=1}^{N} p_i$$

(vergl. TV_F1, Abschn. 3.2).

Entstandene, erkannt und beseitigte Fehler

System mit N_{PF} potentiellen Fehlern. Erwartungswert für die:

- Anzahl der entstehenden Fehler:

$$E\left(\varphi_{\mathrm{Ents}}\right) = \sum_{i=1}^{N_{\mathrm{PF}}} p_{\mathrm{Ents}.i}$$

- Anzahl der vom Test erkennbaren Fehler:

$$E\left(\varphi_{\mathrm{Erk}}\right) = \sum_{i=1}^{N_{\mathrm{PF}}} p_{\mathrm{Ents}.i} \cdot p_{\mathrm{Erk}.i}$$

- Anzahl der beseitigten Fehler:

$$E\left(\varphi_{\mathrm{Bes}}\right) = \sum_{i=1}^{N_{\mathrm{PF}}} p_{\mathrm{Ents}.i} \cdot p_{\mathrm{Erk}.i} \cdot p_{\mathrm{Bes}.i}$$

($p_{\mathrm{Ents}.i}$ – Entstehungsw.; $p_{\mathrm{Erk}.i}$ – Erkennungsw. entstandener; $p_{\mathrm{Bes}.i}$ – Beseitungsw. entstandener erkannter potentieller Fehler i).

Getestete Systeme im Einsatz

Zu erwartende Fehleranzahl in getesteten Systemen im Einsatz:

$$E(\varphi) = \sum_{i=1}^{N_{\mathrm{PF}}} p_{\mathrm{Ents}.i} \cdot (1 - p_{\mathrm{Erk}.i} \cdot p_{\mathrm{Bes}.i}) \tag{7}$$

- $p_{\mathrm{Ents}.i}$ – Entstehungswahrscheinlichkeit potentieller Fehler i;
- $p_{\mathrm{Erk}.i}$ – Erkennungswahrscheinlichkeit entstandener potentieller Fehler i ;
- $p_{\mathrm{Bes}.i}$ – Beseitungswahrscheinlichkeit erkannter, entstandener potentieller Fehler i.

Entstandene Fehler, die nicht erkannt oder erkannte Fehler, die nicht beseitigt werden, verursachen während des Einsatzes Fehlfunktionen.

Fehlfunktionen im Einsatz durch Fehler

Jeder Fehler in einem eingesetzten System verursacht bei jeder SL mit einer sehr kleinen $p_{\mathrm{FF}.i}$ eine FF. Zu erwartende Anzahl der Fehler, die je SL einen FF verursachen:

$$E(\varphi) = \sum_{i=1}^{N_{\mathrm{PF}}} p_{\mathrm{Ents}.i} \cdot (1 - p_{\mathrm{Erk}.i} \cdot p_{\mathrm{Bes}.i}) \cdot p_{\mathrm{FF}.i}$$

Im Einsatz sind sehr wenige SL FFs ($p_{\mathrm{FFF}} \ll 1$). Wirksamkeit von mehr als einem Fehler je FF unwahrscheinlich:

$$p_{\mathrm{FFF}} = P(\varphi_{\mathrm{FF}} > 0) \stackrel{!}{=} E(\varphi_{\mathrm{FF}})$$

$$p_{\mathrm{FFF}} = \sum_{i=1}^{N_{\mathrm{PF}}} p_{\mathrm{Ents}.i} \cdot (1 - p_{\mathrm{Erk}.i} \cdot p_{\mathrm{Bes}.i}) \cdot p_{\mathrm{FF}.i} \qquad (8)$$

QQ[16]-Funktion für Fehler und FF

Einführung einer QQ-Funktion $h(x)$ für die Auftrittswahrscheinlichkeit potentieller Fehler in Abhängigkeit von der mittleren Anzahl von Service-Leistungen je FF $x = p_{\mathrm{FFF}}^{-1}$. Mit $h(x)$ ist die zu erwartende Anzahl der Fehler das Integral über $h(x)$ für alle x:

$$E(\varphi) = \int_0^\infty h(x) \cdot dx$$

Wahrscheinlichkeit einer FF durch einen Fehler:

$$p_{\mathrm{FFF}} = \int_0^\infty \frac{h(x)}{x} \cdot dx$$

[16] QQ – Quantil-Quantil-Funktion. Auftrittshäufigkeiten und Mittelwerte sind in der Mathematik keine Zahlenwerte sondern Bereiche, die als Quantille bezeichnet werden. $h(x)$ und x sind Quantille, deren Größe gegen 0 strebt.

Pareto-QQ-Funktion

Nach TV_F1, Abschn. 2.2 verursacht oft ein kleiner Anteil von $K \ll 50\%$ der Fehler einen großen Anteil von $G \gg 50\%$ der FF. Die dominanten Fehler sind die mit $x \leq d$ (die im Mittel mindesten alle d SL eine FF verursachen). Es muss gelten:

$$K = \frac{\int_0^d h(x) \cdot dx}{\int_0^\infty h(x) \cdot dx}; \qquad G = \frac{\int_0^d \frac{h(x)}{x} \cdot dx}{\int_0^\infty \frac{h(x)}{x} \cdot dx}$$

Eine QQ-Funktion, die das Pareto-Prinzip auch rekursiv erfüllt[17]:

$$h(x) = \begin{cases} 0 & \text{für } x < x_0 \\ c \cdot x^{-(k+1)} & \text{für } x \geq x_0 \end{cases} \quad \text{mit } k > 0$$

(x_0 – Mindestabstand zwischen zwei FF; c – Skalierungsfaktor; k – Exponent[18]).

[17] Mit $E(\varphi_{\mathrm{FF}})$ multiplizierte Dichtefunktion der Pareto-Verteilung.
[18] $k < 0$ Voraussetzung für die Lösbarkeit $\int_0^\infty H(x) \cdot dx$.

$$\int_0^\infty h(x)\cdot dx = \int_{x_0}^\infty c\cdot x^{-(k+1)} = c\cdot\frac{x_0^{-k}}{k}$$

$$\int_0^d h(x)\cdot dx = \int_{x_0}^d c\cdot x^{-(k+1)} = c\cdot\frac{x_0^{-k}-d^{-k}}{k}$$

$$\int_0^\infty \frac{h(x)}{x}\cdot dx = \int_{x_0}^\infty \frac{c\cdot x^{-(k+1)}}{x}\cdot dx = c\cdot\frac{x_0^{-(k+1)}}{k+1}$$

$$\int_0^d \frac{h(x)}{x}\cdot dx = \int_{x_0}^d c\cdot x^{-(k+1)}\cdot dx = c\cdot\frac{x_0^{-(k+1)}-d^{-(k+1)}}{k+1}$$

$$K = \frac{\int_0^d h(x)\cdot dx}{\int_0^\infty h(x)\cdot dx} = 1-\left(\frac{d}{x_0}\right)^{-k}$$

$$G = \frac{\int_0^d \frac{h(x)}{x}\cdot dx}{\int_0^\infty \frac{h(x)}{x}\cdot dx} = 1-\left(\frac{d}{x_0}\right)^{-(k+1)}$$

$$\frac{1-K}{1-G} = \frac{d}{x_0};\quad d = x_0\cdot\frac{1-K}{1-G}$$

Die dominanten $K \ll 50\%$ Fehler, die $G \gg 50\%$ der FF verursachen, sind die, die im Mittel alle x mit

$$x_0 \leq x \leq d = x_0 \cdot \frac{1-K}{1-G}$$

SL eine FF verursachen (x_0 – mittlere Mindestanzahl der SL je FF).

Angenommen, $K = 20\%$ der Fehler verursachen $G = 80\%$ der FF. Bis zu welchen mittleren Anzahl d von SL je FF zählen die Fehler als dominant?

$$\begin{aligned} d &= x_0 \cdot \frac{1-K}{1-G} \\ &= x_0 \cdot \frac{1-20\%}{1-80\%} \\ &= 4 \cdot x_0 \end{aligned}$$

Die K=20% der Fehler mit $x_0 \leq x \leq 4 \cdot x_0$ SL je FF verursachen 80% der FF und die G=20% der Fehler mit $x > 4 \cdot x_0$ SL je FF verursachen 20% der FF.

Auswahlstrategien für die zu beseitigenden Fehler

Zu beseitigende Threads (Fehler, Fehlfunktionen, ...) werden durch Kontrollen/Tests gefunden/ausgewählt. Der Idealfall, Beseitigung in der Reihenfolge des zu erwartenden Schadens ist oft nicht praktikabel. Alternative Auswahltechniken:

- Schadensunabhängige Auswahl:
  - Statische Tests (Reviews, Syntaxtest, Code-Analyse, ...).
  - Gezielte Testauswahl.
- Zufallstest (Beseitigungswahrscheinlichkeit proportional zur Wahrscheinlichkeit einer FF durch den Fehler):
  - Test mit zufälligen Eingaben vor dem Einsatz.
  - Beseitigung von Fehlern, die durch FF im Einsatz erkannt werden.

Schadensunabhängige Auswahl

- Beseitigungswahrscheinlichkeit für alle potentiellen Fehler: p_{Bes}
- QQ-Funktion nach Beseitigung aller erkannten Fehler:

$$h\left(x, p_{\mathrm{Bes}}\right) = \left(1 - p_{\mathrm{Bes}}\right) \cdot h\left(x\right)$$

- Fehleranzahl nach Beseitigung:

$$E\left(\varphi\left(p_{\mathrm{Bes}}\right)\right) = \int_0^\infty \left(1 - p_{\mathrm{Bes}}\right) \cdot h\left(x\right) \cdot dx = \left(1 - p_{\mathrm{Bes}}\right) \cdot E\left(\varphi\right)$$

- Wahrscheinlichkeit ein FF je SL durch einen Fehler nach Beseitigung aller erkannten Fehler:

$$p_{\mathrm{FFF}}\left(p_{\mathrm{Bes}}\right) = \int_0^\infty \frac{\left(1 - p_{\mathrm{Bes}}\right) \cdot h\left(x\right)}{x} \cdot dx = \left(1 - p_{\mathrm{Bes}}\right) \cdot p_{\mathrm{FFF}} \quad (9)$$

Zu erwartende Fehleranzahl und Wahrsch. einer FF verringern sich im selben Maße um die Nichtbeseitigungswahrscheinlichkeit $\left(1 - p_{\mathrm{Bes}}\right)$.

Beseitigung zufällig erkannter Fehler

Die Wahrscheinlichkeit, dass ein Fehler, der im Mittel aller x SL eine FF verursacht, bei einer zufällig ausgewählten SL erkannt wird:

$$p_{\mathrm{Erk}} = \frac{1}{x}$$

Unter der Annahme, dass erkannte Fehler mit einer Wahrscheinlichkeit p_{Bes} beseitigt werden, beträgt die Wahrscheinlichkeit der Nichtbeseitigung je SL

$$p_{\mathrm{NBes}}(1) = 1 - \frac{p_{\mathrm{Bes}}}{x}$$

Bei n SL veringert sich die Wahrscheinlichkeit, dass ein vorhandener Fehler, nicht beseitigt, d.h. noch vorhanden ist, auf:

$$p_{\mathrm{NBes}}(n) = \left(1 - \frac{p_{\mathrm{Bes}}}{x}\right)^n \text{ für } \frac{p_{\mathrm{Bes}}}{x} \ll 0{,}1 \quad p_{\mathrm{NBes}} = e^{-\frac{p_{\mathrm{Bes}} \cdot n}{x}}$$

Mit einer schadensunabhängigen Beseitigungswahrscheinlichkeit p_{Bes} je FF reduziert sich die Auftrittshäufigkeit von Fehlern, die im Mittel aller x SL eine FF verursachen, auf:

$$h\left(x,n\right)=h\left(x\right)\cdot e^{-\frac{p_{\mathrm{Bes}}\cdot n}{x}}$$

Aus der aus dem Pareto-Prinzip abgeleitete QQ-Funktion wird:

$$h\left(x,n,p_{\mathrm{Bes}}\right)=\begin{cases}0 & \text{für } x<x_0\\ c\cdot x^{-(k+1)}\cdot e^{-\frac{p_{\mathrm{Bes}}\cdot n}{x}} & \text{für } x\geq x_0\end{cases}\quad \text{mit } k>0$$

Für Testlängen $n\gg x_0$ kann die Fallunterscheidung entfallen:

$$h\left(x,n,p_{\mathrm{Bes}}\right)=c\cdot x^{-(k+1)}\cdot e^{-\frac{p_{\mathrm{Bes}}\cdot n}{x}}$$

Anzahl der Fehler nach Beseitigung ...

Die Beseitigung der mit n zufälligen SL erkannten Fehler reduziert die zu erwartende Fehleranzahl auf:

$$E\left(\varphi\left(n\right)\right) = \int_0^\infty c \cdot x^{-(k+1)} \cdot e^{-\frac{p_{\text{Bes}} \cdot n}{x}} \cdot dx$$

Mit der Substitution $z = \frac{p_{\text{Bes}} \cdot n}{x}$; $dx = -\frac{p_{\text{Bes}} \cdot n}{z^2} \cdot dz$

$$\begin{aligned} E\left(\varphi\left(n\right)\right) &= \int_\infty^0 c \cdot \frac{\left(p_{\text{Bes}} \cdot n\right)^{-(k+1)}}{z^{-(k+1)}} \cdot e^{-z} \cdot \left(-\frac{p_{\text{Bes}} \cdot n}{z^2} \cdot dz\right) \\ &= \frac{c}{\left(p_{\text{Bes}} \cdot n\right)^k} \cdot \int_0^\infty z^{k-1} \cdot e^{-z} \cdot dz \end{aligned}$$

Das bestimmte Integral

$$\int_0^\infty z^{k-1} \cdot e^{-z} \cdot dz = \Gamma\left(k\right)$$

ist die Gamma-Funktion.

Die Gamma-Funktion ist eine Erweiterung der Fakultät auf reelle Zahlen. Für den Exponenten $0 < k \leq 1$ beträgt sie überschlagsweise $1/k$ und für $k > 1$ gilt $\Gamma(k+1) = k \cdot \Gamma(k)$.

k	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
$\Gamma(k)$	9,51	4,59	2,99	2,22	1,77	1,49	1,30	1,16	1,07

Insgesamt ergibt sich:

$$E(\varphi(n)) = \frac{c \cdot \Gamma(k)}{(p_{\text{Bes}} \cdot n)^k} \tag{10}$$

bzw.

$$E(\varphi(n)) = E(\varphi(n_0)) \cdot \left(\frac{n}{n_0}\right)^{-k} \tag{11}$$

(n_0 – Bezugstestaufwand, für den ein Schätzwert für die zu erwartende Fehleranzahl vorliegt). Der Exponent k, mit dem die zu erwartende Fehleranzahl mit der Testsatzlänge n abnimmt, ist in der Regel kleiner eins. Bei $k = 0{,}5$ verlangt eine Halbierung der Fehleranzahl einer Vervierfachung des Testaufwands.

FF durch nicht beseitigte Fehler

$$p_{\mathrm{FFF}}(n) = \int_0^\infty \frac{h(x,n,p_{\mathrm{Bes}})}{x} \cdot dx \text{ mit } h(x,n,p_{\mathrm{Bes}}) = c \cdot x^{-(k+1)} \cdot e^{-\frac{p_{\mathrm{Bes}} \cdot n}{x}}$$

$$= \int_0^\infty c \cdot x^{-(k+2)} \cdot e^{-\frac{p_{\mathrm{Bes}} \cdot n}{x}} \cdot dx$$

Mit der Substitution $z = \frac{p_{\mathrm{Bes}} \cdot n}{x}$; $dx = -\frac{p_{\mathrm{Bes}} \cdot n}{z^2} \cdot dz$:

$$p_{\mathrm{FFF}}(n) = \int_\infty^0 c \cdot \frac{(p_{\mathrm{Bes}} \cdot n)^{-(k+2)}}{z^{-(k+2)}} \cdot e^{-z} \cdot \left(-\frac{p_{\mathrm{Bes}} \cdot n}{z^2} \cdot dz\right)$$

$$= \frac{c}{(p_{\mathrm{Bes}} \cdot n)^{k+1}} \cdot \underbrace{\int_0^\infty z^k \cdot e^{-z} \cdot dz}_{\Gamma(k+1) = k \cdot \Gamma(k)}$$

$$= \frac{c \cdot \Gamma(k+1)}{(p_{\mathrm{Bes}} \cdot n)^{k+1}} \tag{12}$$

($\Gamma(\ldots)$ – Gamma-Funktion).

Mit $\Gamma(k+1) = k \cdot \Gamma(k)$ und $E(\varphi(n)) = \frac{p_{\mathrm{Bes}} \cdot c \cdot \Gamma(k)}{(p_{\mathrm{Bes}} \cdot n)^k}$:

$$p_{\mathrm{FFF}}(n) = \frac{k \cdot E(\varphi(n))}{p_{\mathrm{Bes}} \cdot n} \tag{13}$$

Wenn für einen Bezugstestaufwand n_0 ein Schätzwert für $E(\varphi(n_0))$ oder $p_{\mathrm{FFF}}(n_0)$ vorliegt:

$$p_{\mathrm{FFF}}(n) = p_{\mathrm{FFF}}(n_0) \cdot \left(\frac{n}{n_0}\right)^{-(k+1)} \tag{14}$$

$$p_{\mathrm{FFF}}(n) = \frac{k \cdot E(\varphi(n_0))}{p_{\mathrm{Bes}} \cdot n_0} \cdot \left(\frac{n}{n_0}\right)^{-(k+1)} \tag{15}$$

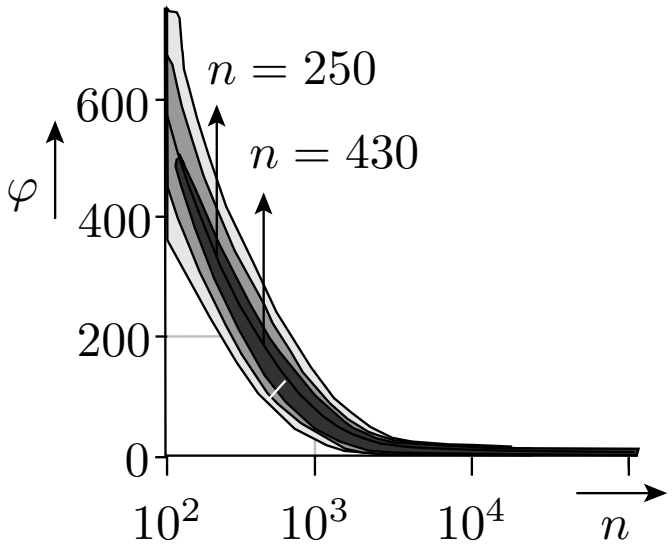
Abnahme der zu erwartenden Fehleranzahl mit n^{-k} und der Wahrscheinlichkeit einer FF mit $n^{-(k+1)}$ (n – Testaufwand; $0 < k < 1$ – Exponent der QQ-Funktion).

Bei $k = 0{,}5$ halbiert eine Erhöhung der Testdauer auf $n = 4 \cdot n_0$ die zu erwartende Fehleranzahl und verringert die Wahrscheinlichkeit einer durch Fehler verursachten FF auf ein Achtel.

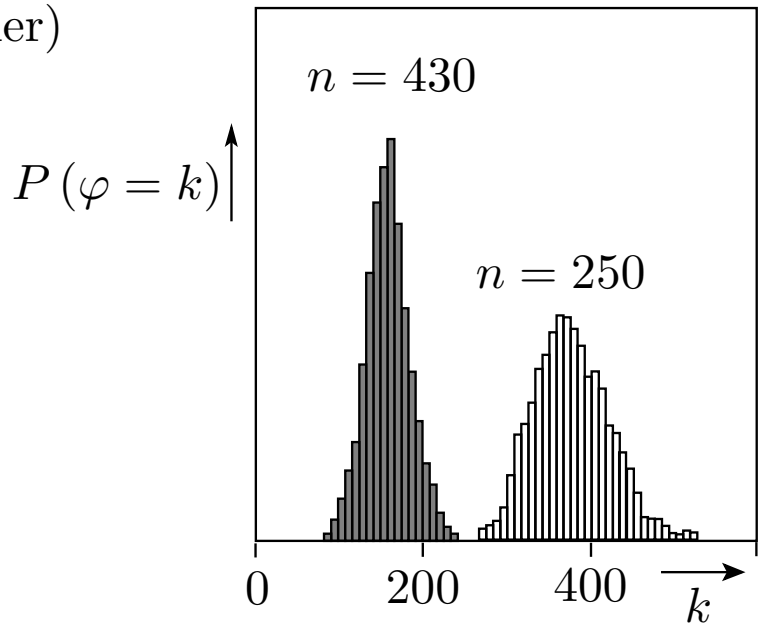
Experiment zur Haftfehlerüberdeckung

Kombinatorische Beispielschaltung (Benchmark c3540). 3606 simulierte, unterschiedlich nachweisbare Haftfehler. Bestimmung der Verteilung mit 1000 verschiedenen Zufallstestsätzen.

Verteilung der Anzahl der nicht erkannten Modellfehler als Funktion von n (Benchmark c3540, 3606 Haftfehler)



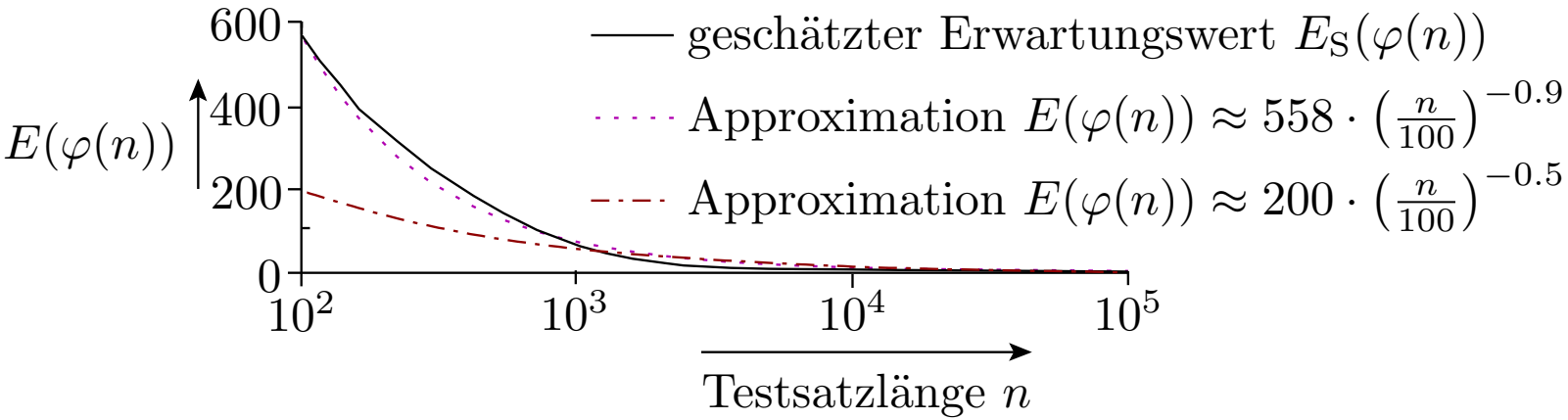
Verteilung für zwei Testsatzlängen



Annäherung von $E(\varphi(n))$ durch Gl. 11

Annäherung der zu erwartenden Anzahl der nachweisbaren Fehler:

$$E(\varphi(n)) = E(\varphi(n_0)) \cdot \left(\frac{n}{n_0}\right)^{-k}$$



Die Approximation mit $k = 0{,}9$ nähert den Bereich $n < 1000$ und die mit $k = 0{,}5$ den Bereich $n > 1000$ Testschritte besser an.

Beispielaufgabe

Nach einem Zufallstest mit $n_0 = 10^5$ Testbeispielen und Fehlerbeseitigung nach jeder FF mit derselben Erfolgswahrscheinlichkeit $p_{\mathrm{Bes}} = 80\%$ betrug die Wahrscheinlichkeit einer FF durch Fehler:

$$p_{\mathrm{FFF}}\left(n_0\right) \approx 10^{-4}$$

Schätzen Sie für die Exponenten der QQ-Funktion $k \in \{0{,}3, 0{,}4, 0{,}5, 0{,}6, 0{,}7\}$:

1. die zu erwartende Anzahl der nicht beseitigten Fehler für $n_0 = 10^5$ Testbeispiele,
2. die zu erwartende Anzahl der nicht beseitigten Fehler für $n = 10 \cdot n_0 = 10^6$ Testbeispiele,
3. die Wahrscheinlichkeit einer FF je SL für $n = 10 \cdot n_0 = 10^6$ Testbeispiele.

Lösung Aufgabenteil 1 und 2

Zufallstest Länge $n_0 = 10^5$. Beseitigungswahrsch. $p_{\text{Bes}} = 80\%$.
Wahrscheinlichkeit einer FF durch Fehler $p_{\text{FFF}}(n_0) \approx 10^{-4}$.

1. Umstellung von Gl. 12 nach der Anzahl der nicht beseitigten Fehler:

$$p_{\text{FFF}}(n_0) = \frac{k \cdot E(\varphi(n_0))}{p_{\text{Bes}} \cdot n_0}$$

$$E(\varphi(n_0)) = \frac{p_{\text{Bes}} \cdot n_0 \cdot p_{\text{FFF}}(n_0)}{k} = \frac{8}{k}$$

k	$E(\varphi(10^5))$
0,3	26,7
0,4	20
0,5	16
0,6	13,3
0,7	11,2

2. Nicht beseitigte Fehler mit der 10-fachen Testsatzlänge:

$$E(\varphi(n)) = E(\varphi(n_0)) \cdot \left(\frac{n}{n_0}\right)^{-k}$$

$$= \frac{8}{k} \cdot 10^{-k}$$

k	$E(\varphi(10^6))$
0,3	13,4
0,4	7,96
0,5	5,06
0,6	3,45
0,7	2,28

Lösung Aufgabenteil 3

3 Häufigkeit der Fehlfunktionen mit der 10-facher Testsatzlänge:

$$p_{\mathrm{FFF}}(n) = p_{\mathrm{FFF}}(n_0) \cdot \left(\frac{n}{n_0}\right)^{-(k+1)} = \frac{10^{-4}}{10^{1+k}}$$

Zusammenfassung der Ergebnisse:

	k=0,3	k=0,4	k=0,5	k=0,6	k=0,7
$p_{\mathrm{FFF}}(10^5)$	10^{-4}	10^{-4}	10^{-4}	10^{-4}	10^{-4}
$E(\varphi(10^5))$	26,7	20	16	13,3	11,2
$p_{\mathrm{FFF}}(10^6)$	$5{,}01 \cdot 10^{-6}$	$3{,}98 \cdot 10^{-6}$	$3{,}16 \cdot 10^{-6}$	$2{,}51 \cdot 10^{-6}$	$2{,}00 \cdot 10^{-6}$
$E(\varphi(10^6))$	13,4	7,96	5,06	3,45	2,28

Die Häufigkeit der Fehlfunktionen verringert sich im Gegensatz zur Anzahl der nicht erkannten und beseitigten Fehler auf weniger als ein Zehntel und hängt deutlich weniger von k ab.

Zuverlässigkeit

Zuverlässigkeit

Zuverlässigkeit wird durch die Wahrscheinlichkeit, dass SL korrekt sind, charakterisiert, abschätzbar aus dem Anteil der korrekten Service-Leistungen:

$$p_{\mathrm{Z}} \approx \frac{N_{\mathrm{KSL}}}{N_{\mathrm{SL}}} = 1 - \frac{N_{\mathrm{FF}}}{N_{\mathrm{SL}}}$$

(SL – Service-Leitung; KSL – korrekte SL; FF – Fehlfunktion).

Definition der Zuverlässigkeit als Kenngröße

Kehrwert der Wahrscheinlichkeit der »Unzuverlässigkeit«:

$$Z = \frac{1}{1 - p_{\mathrm{Z}}} \tag{16}$$

Maßeinheit der Zuverlässigkeit SL/FF (Service-Leistungen je Fehlfunktion). Ein System mit $p_{\mathrm{Z}} = 99\%$ korrekten SL hat z.B. die Zuverlässigkeit $Z = 100\,\frac{\mathrm{SL}}{\mathrm{FF}}$.

Empirische Abschätzung aus Zeiten und Zählwerten

Gut mess-, zähl- und schätzbare Größen für die empierische Abschätzung der Zuverlässigkeit sind:

- Nutzungsdauer t_{N},
- mittlere Service-Dauer $\bar{t}_{\mathrm{SL}}$,
- Anzahl der FF während der Nutzungsdauer N_{FF},
- daraus abschätzbar die mittlere Zeit zwischen zwei FF[19]

$$MTBF = \frac{\bar{t}_{\mathrm{SL}}}{(1 - p_{\mathrm{Z}})} \approx \frac{t_{\mathrm{N}}}{N_{\mathrm{FF}}}$$

Wahrscheinlichkeit der Zuverlässigkeit:

$$p_{\mathrm{Z}} = 1 - \frac{\bar{t}_{\mathrm{SL}}}{MTBF} \tag{17}$$

Zuverlässigkeit:

$$Z = \frac{MTBF}{\bar{t}_{\mathrm{SL}}} \tag{18}$$

[19] $MTBF$– Mean Time between Failures.

Beispielabschätzung

	1	2	3	4	5	6	...
Ergebnis	KSL	KSL	FF	KSL	KSL	FF	...
Zeit	10 ms	25 ms	11 ms	15 ms	18 ms	41 ms	...

$$MTBF \approx \frac{10\,\text{ms} + 25\,\text{ms} + 11\,\text{ms} + 15\,\text{ms} + 18\,\text{ms} + 41\,\text{ms}}{2} = 60\,\text{ms}$$

$$\bar{t}_{\text{SL}} \approx \frac{10\,\text{ms} + 25\,\text{ms} + 11\,\text{ms} + 15\,\text{ms} + 18\,\text{ms} + 41\,\text{ms}}{6} = 20\,\text{ms}$$

Wahrscheinlichkeit der Zuverlässigkeit:

$$p_{\text{Z}} \approx \frac{N_{\text{KSL}}}{N_{\text{SL}}} = \frac{4}{6};\ \text{bzw. } p_{\text{Z}} \approx 1 - \frac{\bar{t}_{\text{SL}}}{MTBF} = 1 - \frac{20\,\text{ms}}{60\,\text{ms}} = 66{,}7\%$$

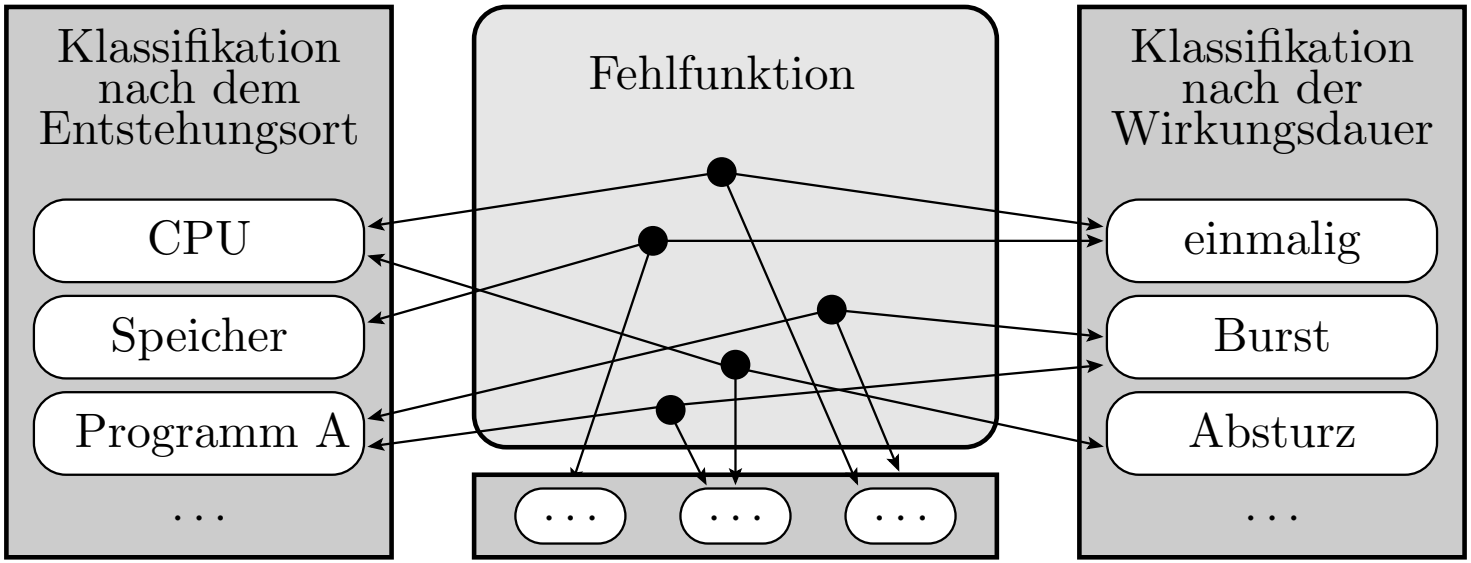
Zuverlässigkeit :

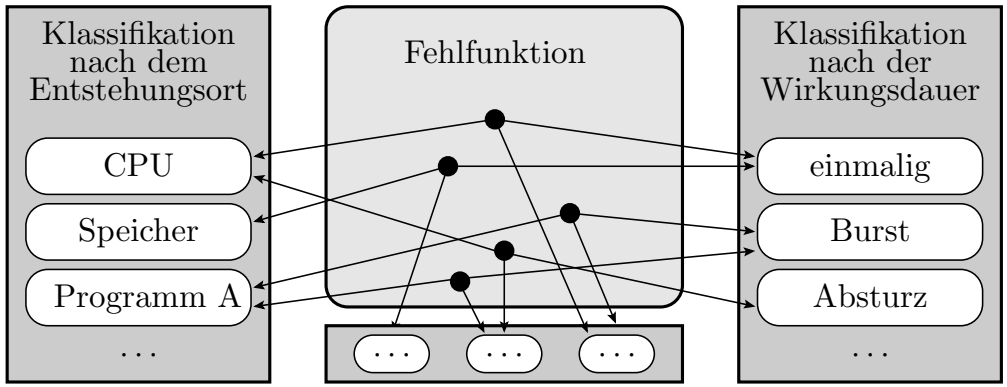
$$Z = \frac{MTBF}{\bar{t}_{\text{SL}}} \approx \frac{60\,\text{ms}}{20\,\text{ms}} = 3\,\frac{\text{SL}}{\text{FF}}$$

Teilzuverlässigkeiten

Die Fehlfunktionen (FF) eines Systems lassen sich nach Ort, Ursache, Schaden, ... unterschiedlichen Klassen zuordnen:

- nur FFs eines bestimmten Teilsystems,
- nur durch HW, nur durch SW verursachte FFs,
- nur FF, die für die Betriebs- / Daten- / Zugangssicherheit relevant sind, ...:





Bei einer eindeutigen Zuordnung jeder Fehlfunktion zu genau einer Klasse i ist die Gesamtanzahl der Fehlfunktionen N_{FF} die Summe der Fehlfunktionen aller Klassen i:

$$N_{\mathrm{FF}} = \sum_{i=1}^{N_{\mathrm{FFKl}}} N_{\mathrm{FF}.i}$$

(N_{FFKl} – Anzahl der Fehlfunktionsklassen). Der Kehrwert der Gesamtzuverlässigkeit ist die Summe der Kehrwerte der Teilzuverlässigkeiten:

$$\frac{1}{Z} \approx \frac{N_{\mathrm{FF}}}{N_{\mathrm{SL}}} = \sum_{i=1}^{N_{\mathrm{FFKl}}} \frac{N_{\mathrm{FF}.i}}{N_{\mathrm{SL}}}; \quad \frac{1}{Z} = \sum_{i=1}^{N_{\mathrm{FFKl}}} \frac{1}{Z_i}$$

Beispielaufgabe

Die Fehlfunktionen seien entweder vom Speicher, vom Prozessor, von der Software oder vom Rest verursacht. Es liegen folgende $MTBF$-Werte für Teilsysteme vor:

Teilsystem i	Speicher	Prozessor	Software	Rest
$MTBF_i$	500 h	3.000 h	1000 h	2.000 h

Mittlere Service-Dauer $\bar{t}_{\mathrm{SL}} = 1\,\mathrm{min}$.

1. Wie groß sind die vier aus den $MTBF$-Werten abschätzbaren Teilzuverlässigkeiten Z_i?
2. Wie groß ist die Zuverlässigkeit Z des Gesamtsystems?
3. Wie groß ist die Wahrscheinlichkeit p_{FF} einer Fehlfunktion des Gesamtsystems?

Lösungen

1. Teilzuverlässigkeiten ($\bar{t}_{\mathrm{SL}} = 1\,\mathrm{min}$):

Teilsystem	Speicher	Prozessor	Software	Rest
$MTBF_i$	500 h	3.000 h	1000 h	2.000 h
Z_i	$3 \cdot 10^4 \frac{\mathrm{SL}}{\mathrm{FF}}$	$1{,}8 \cdot 10^5 \frac{\mathrm{SL}}{\mathrm{FF}}$	$6 \cdot 10^4 \frac{\mathrm{SL}}{\mathrm{FF}}$	$1{,}2 \cdot 10^5 \frac{\mathrm{SL}}{\mathrm{FF}}$

($\frac{\mathrm{SL}}{\mathrm{FF}}$ – Service-Leistungen je Fehlfunktion).

2. Zuverlässigkeit des Gesamtsystems:

$$\frac{1}{Z} \approx \frac{1}{3 \cdot 10^4 \frac{\mathrm{SL}}{\mathrm{FF}}} + \frac{1}{1{,}8 \cdot 10^5 \frac{\mathrm{SL}}{\mathrm{FF}}} + \frac{1}{6 \cdot 10^4 \frac{\mathrm{SL}}{\mathrm{FF}}} + \frac{1}{1{,}2 \cdot 10^5 \frac{\mathrm{SL}}{\mathrm{FF}}}$$

$$Z \approx 1{,}5 \cdot 10^4 \frac{\mathrm{SL}}{\mathrm{FF}}$$

3. Wahrscheinlichkeit einer FF je SL des Gesamtsystems:

$$p_{\mathrm{FF}} = 1 - p_{\mathrm{Z}} = \frac{1}{Z} \approx 6{,}7 \cdot 10^{-5}$$

Fehler- und störungsbezogene Teilzuverlässigkeit

Für die fehlerbezogene Teilzuverlässigkeit werden nur die FF, die durch Fehler verursacht werden, gezählt. Kehrwert der Wahrscheinlichkeit von durch Fehler verursachten FF:

$$Z_{\mathrm{F}} = \frac{1}{p_{\mathrm{FFF}}} \tag{19}$$

Alle anderen FF haben Störungen[20] zur Ursachen. Störungsbezogene Teilzuverlässigkeit

$$Z_{\mathrm{S}} = \frac{1}{p_{\mathrm{FS}}}$$

(p_{FS} – Wahrscheinlichkeit einer FF durch eine Störung).

[20] Störungen nach TV_F1, Abschn. 2.2: Zufällige, nicht reproduzierbare Wirkungen, vermeidbar durch Verringerung der Störanfälligkeit.

Zuverlässigkeitswachstum durch Fehlerbeseitigung

- Schadensunabhängige Fehlerbeseitigung mit p_{Bes} nach Gl. 9:

$$p_{\mathrm{FFF}}\left(p_{\mathrm{Bes}}\right) = \left(1 - p_{\mathrm{Bes}}\right) \cdot p_{\mathrm{FFF}} \quad \Rightarrow \quad Z_{\mathrm{F}}\left(p_{\mathrm{Bes}}\right) = \frac{Z_{\mathrm{F}}}{\left(1 - p_{\mathrm{Bes}}\right)}$$

- Beseitigungswahrsch. proportional zur Wahrscheinlichkeit einer FF durch den Fehler. Aus Gl. 14 folgt:

$$p_{\mathrm{FFF}}\left(n\right) = p_{\mathrm{FFF}}\left(n_0\right) \cdot \left(\frac{n}{n_0}\right)^{-(k+1)} \quad \Rightarrow \quad Z_{\mathrm{F}}\left(n\right) = Z_{\mathrm{F}}\left(n_0\right) \cdot \left(\frac{n}{n_0}\right)^{k+1}$$

Die störungsbezogene Teilzuverlässigkeit Z_{S} wird durch Fehlerbeseitigung nicht verbessert. Zuverlässigkeitsverbesserung insgesammt:

$$\frac{1}{Z\left(*\right)} = \frac{1}{Z_{\mathrm{S}}} + \frac{1}{Z_{\mathrm{F}}\left(*\right)}$$

($*$ – Testaufwand charakterisiert durch p_{Bes} bzw. n).

Sicherheit

Sicherheiten

Sicherheiten sind Teilzuverlässigkeiten, bei denen nur die FF einer bestimmten Gefährdung zählen:

Art der Sicherheit	zu zählende Gefährdungen
Betriebssicherheit (safty)	Personen- und Umweltschäden
Datensicherheit (security)	Datendiebstahl
Sicherheit Datenerhalt	Datenverlust
...	...

Kenngrößen für Sicherheiten

Gefährdungswahrscheinlichkeit (Wahrsch., dass FF gefährdend):

$$p_{\mathrm{G}} \approx \frac{N_{\mathrm{GFF}}}{N_{\mathrm{FF}}}$$

Wahrscheinlichkeit, dass eine Service-Leistung sicher ist, abschätzbar aus dem Anteil der gefährdenden FF:

$$p_{\mathrm{S}} \approx 1 - \frac{N_{\mathrm{GFF}}}{N_{\mathrm{SL}}} = 1 - p_{\mathrm{G}} \cdot \frac{N_{\mathrm{FF}}}{N_{\mathrm{SL}}}$$

(SL – Service-Leistung; FF – Fehlfunktion; GFF – gefährdende FF).
Alternativ abschätzbar:

$$p_{\mathrm{S}} = 1 - \frac{\bar{t}_{\mathrm{S}}}{MTBF_{\mathrm{S}}} = 1 - \frac{p_{\mathrm{G}} \cdot \bar{t}_{\mathrm{S}}}{MTBF}$$

($MTBF_{\mathrm{S}} = \frac{MTBF}{p_{\mathrm{G}}}$ – sicherheitsbezogene $MTBF$, mittlere Zeit zwischen zwei gefährdenden FF; $\bar{t}_{\mathrm{S}}$ – mittlere Service-Dauer).

Definition der Kenngröße für Sicherheiten

Kehrwert der Wahrscheinlichkeit der »Unsicherheit«:

$$S = \frac{1}{1 - p_{\mathrm{S}}} = \frac{Z}{p_{\mathrm{G}}} \tag{20}$$

(p_{S} – Wahrscheinlichkeit, dass eine SL sicher ist; Z – Zuverlässigkeit; p_{G} – Gefährdungswahrscheinlichkeit). Maßeinheit von Sicherheiten SL/GFF (Service-Leistungen je gefährdende Fehlfunktion).

Sicherheiten lassen sich erhöhen durch

- Erhöhung der Zuverlässigkeit Z und
- Verringerung der Gefährdungswahrscheinlichkeit p_{G}.

Beispielaufgaben

Eine Fahrzeug habe eine $MTBF = 1000\,\mathrm{h}$ zwischen zwei Fehlfunktionen. Die Wahrscheinlichkeit, dass eine FF die Betriebssicherheit gefährdet, sei $p_\mathrm{G} = 1\%$ und die mittlere Service-Dauer (mittlere Fahrtdauer) betrage $\bar{t}_\mathrm{S} = 1\,\mathrm{h}$.

1. Wie hoch sind die Zuverlässigkeit, die auf die Betriebssicherheit bezogene $MTBF_\mathrm{S}$ (mittlere Zeit zwischen zwei die Betriebssicherheit gefährdende FFs), die Betriebssicherheit S und die Wahrscheinlichkeit p_S, dass von einer Service-Leistung keine Gefahr für die Betriebssicherheit ausgeht?
2. Ein zusätzliches elektronisches Steuergerät senkt die Gefährdungswahrscheinlichkeit auf ein Zehntel ab. Wie groß muss die Zuverlässigkeit des Steuergeräts Z_SG mindestens sein, damit das Steuergerät die Sicherheit mindestens verfünffacht?

Lösung Aufgabenteil 1

Zuverlässigkeit nach Gl. 18:

$$Z = \frac{MTBF}{\bar{t}_\mathrm{S}} = \frac{10^3\mathrm{h}}{1\mathrm{h}} \cdot \frac{\mathrm{SL}}{\mathrm{FF}} = 10^3 \, \frac{\mathrm{SL}}{\mathrm{FF}}$$

$MTBF_\mathrm{S}$ zwischen zwei für die Betriebssicherheit gefährliche FFs:

$$MTBF_\mathrm{S} = \frac{MTBF}{p_\mathrm{G}} = \frac{1000\,\mathrm{h}}{1\%} = 10^5\mathrm{h}$$

Betriebssicherheit nach Gl. 20:

$$S = \frac{MTBF_\mathrm{S}}{\bar{t}_\mathrm{S}} \approx \frac{10^5\mathrm{h}}{1\mathrm{h}} = 10^5 \, \frac{\mathrm{SL}}{\mathrm{GFF}}$$

Wahrscheinlichkeit, dass von einer Service-Leistung keine Gefahr für die Betriebssicherheit ausgeht:

$$p_\mathrm{S} = 1 - \frac{1}{S} \approx 1 - 10^{-5}$$

Lösung Aufgabenteil 2

Ein zusätzliches elektronisches Steuergerät senkt die Gefährdungswahrscheinlichkeit auf ein Zehntel ab:

$$p_{\mathrm{G.mSG}} = 0{,}1 \cdot p_{\mathrm{G}}$$

Wie groß muss die Zuverlässigkeit des Steuergeräts Z_{SG} mindestens sein, damit das Steuergerät die Sicherheit mindestens verfünffacht:

$$S_{\mathrm{mSG}} \geq 5 \cdot S$$

$$\begin{aligned} 5 \cdot S = 5 \cdot \frac{Z}{p_{\mathrm{G}}} \quad &\leq \quad S_{\mathrm{mSG}} = \frac{Z_{\mathrm{mSG}}}{p_{\mathrm{G.mSG}}} = \frac{10}{p_{\mathrm{G}}} \cdot \frac{1}{\frac{1}{Z} + \frac{1}{Z_{\mathrm{SG}}}} \\ \frac{Z}{2} \quad &\leq \quad \frac{1}{\frac{1}{Z} + \frac{1}{Z_{\mathrm{SG}}}}; \quad Z_{\mathrm{SG}} \geq Z = 10^3 \, \frac{\mathrm{SL}}{\mathrm{FF}} \end{aligned}$$

Das Steuergerät muss mindestens so zuverlässig wie das Fahrzeug sein.

Schadenskosten

Schaden durch FF

Für die Schadenskosten durch FF gilt auch in der Regel das Pareto-Prinzip:

> *Ein kleiner Teil der FF verursacht den überwiegenden Teil der Schadenskosten.*

Für die Häufigkeit der Schadensfälle $h(x)$ in Abhängigkeit von der Schadensgröße x gilt dieselbe Empirie wie zwischen der Fehlerhäufigkeit und der mittleren Anzahl von SL je FF (Fehlerbezogene Teilzuverlässigkeit):

$$h(x) = \begin{cases} 0 & \text{für } x < x_0 \\ c \cdot x^{-(k+1)} & \text{für } x \geq 0 \end{cases} \quad \text{mit } k > 0 \tag{21}$$

Für eine Schadenshöhe $d > x_0$ beträgt die zu erwartende Anzahl der Schadensfälle mit einem Schaden $s \geq d$

$$H(s \geq d) = \int_d^\infty c \cdot x^{-(k+1)} \cdot dx = \frac{c \cdot d^{-k}}{k}$$

Beispiel Haftpflichschäden

Für Haftpflichtschäden über 100000 SF (SF – Schweizer Franken) einer Schweizer Autoversicherung liegen die folgenden Daten vor[21]:

```
103765, 109168, 112341, 113800, 114791, 115731, 118264,
123464, 127611, 133504, 142821, 152270, 163491, 164968,
168915, 169346, 172668, 191954, 193102, 208522, 209070,
219111, 243910, 280302, 313898, 330461, 418074, 516218,
595310, 742198, 791874, 822787, 1074499.
```

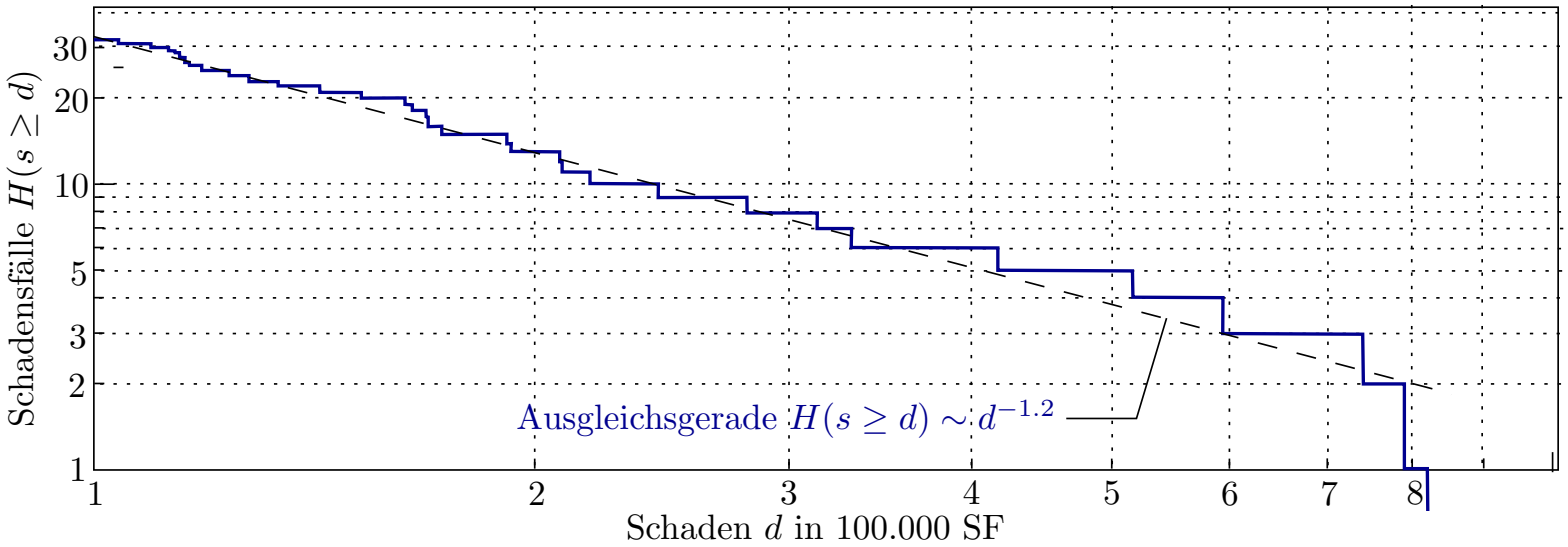
Gesucht ist eine Näherungsfunktion für die Schadenshäufigkeit von Schäden größer d SF (Schweizer Franken):

$$H\left(s \geq d\right) = \int_{d}^{\infty} c \cdot x^{-(k+1)} \cdot dx = \frac{c \cdot d^{-k}}{k}$$

[21] Aus Klüppelberg, C. and Villasenor, J. A. (1993) Estimation of distribution tails – A semiparametric approach, Bl. Dtsch. Ges. Versicherungsmath. 21, No.2, 213-235.

Schäden größer 100.000 in Schweizer Franken:

103765, 109168, 112341, 113800, 114791, 115731, 118264,
123464, 127611, 133504, 142821, 152270, 163491, 164968,
168915, 169346, 172668, 191954, 193102, 208522, 209070,
219111, 243910, 280302, 313898, 330461, 418074, 516218,
595310, 742198, 791874, 822787, 1074499.



In log. QQ-Darstellung ist zu erkennen, dass die Häufigkeit des Schades größer d mit dem Exponenten $k \approx 1{,}2$ abnimmt.

Kosten für pareto-verteile Schadensfälle

Bei einer Häufigkeit der Schadensfälle

$$h(x) = \begin{cases} 0 & \text{für } x < x_0 \\ c \cdot x^{-(k+1)} & \text{für } x \geq 0 \end{cases}$$

(x – Schadeskosten, k – Exponent der QQ-Funktion) betragen die zu erwartenden Schadenskosten für alle Schäden zusammen:

$$\begin{aligned} E(K_S) &= \int_{x_0}^{\infty} x \cdot h(x) \cdot dx \\ &= \frac{c}{k-1} \cdot \left(x_0^{-(k-1)} \right) \end{aligned}$$

Für $k > 1$ ergibt sich die endliche Schadensgröße:

$$E(K_S) = \frac{c}{k-1} \cdot \left(x_0^{-(k-1)} \right)$$

Haftungsbegrenzung

Für kleinere Exponenten $0 < k \leq 1$ ist eine Haftungsbegrenzung auf einem Maximalbetrag $x_{\max}$ je Schadensfall erforderlich:

$$\begin{aligned} E(K_S) &= \int_{x_0}^{x_{\max}} x \cdot h(x) \cdot dx + x_{\max} \cdot \int_{x_{\max}}^{\infty} x \cdot h(x) \cdot dx \\ &= \frac{c}{1-k} \cdot \left(x_{\max}^{1-k} - x_0^{1-k} \right) + \frac{c \cdot x_{\max} \cdot x_{\max}^{-k}}{k} \end{aligned}$$

Wer trägt die Schadenskosten?

Bei großen Schadenskosten wird rückwirkend nach der Ursache gesucht. Potentielle Ursachen:

- Entwurfs- und Fertigungsfehler,
- Ausfall (nachträglich entstehende Fehler),
- Störungen (keine genau zuordenbare Ursache).

Der Hersteller haftet bei Verletzung seiner »Sorgfaltspflicht« und muss im Schadensfall nachweisen, dass er nach Stand der Technik alles für die Schadensabwendung getan zu hat.

Theoretisch müssten Hersteller von sicherheitskritischen IT-Systemen nach aktueller Rechtslage in ihre Preise die zu erwartenden Schadenskosten einrechnen.

Da die zu erwartenden Schadenskosten auch erheblich von der Art der Nutzung abhängen, wäre eine »Haftpflichtversicherung« angemessener.

Folgen der aktuellen Gesetzenslage

Wie lässt sich die Erfüllung der »Sorgfaltspflicht« bei einem vom Test übersehenen Fehler nachweisen?

Dazu dienen Standards, die in »abhakbarer« Weise beschreiben, was für Tests und andere verlässlichkeitssichernde Maßnahmen als ausreichend gelten und wie deren Erbringung zu dokumentieren ist.

Für einen Testfall nach [ANSI/IEEE-Standard 829] sind zusätzlich zu den Eingaben und Sollausgaben zu dokumentieren:

- Testfall-Identifikation: eindeutiger Bezeichner.
- Testgegenstand: Referenz auf die Beschreibung, aus der Anforderungen überprüft werden.
- Zweck: Anforderung, deren Erfüllung der Test bestätigt.
- Testfallstatus: spezifiziert, durchgeführt, ...

Weitere relevante Standards:

- ISO 9126/DIN 66272: Qualitätsmerkmale für Software.
- ANSI/IEEE Std 829-1998: Standard für Software Test Dokumentationen.
- ANSI/IEEE Std 1008-1993: Standard für Software Unit Test.
- ANSI/IEEE Std 1012-1998: Standard für Software Verfication and Validation Plans.
- ...

Erheblicher Aufwand zur Vermeidung von Produkthaftung, der bei anderer Gesetzeslage nutzbringender zur Verbesserung der Verlässlichkeit und Sicherheit eingesetzt werden könnte.

Verfügbarkeit

Verfügbarkeit

Definition der Verfügbarkeit von IT-Systemen

Anteil der Zeit, während der (Wahrscheinlichkeit, dass) das System einsatzbereit ist:

$$V = p_{\mathrm{V}} = \frac{t_{\mathrm{ges}} - t_{\mathrm{a}}}{t_{\mathrm{ges}}}$$

(t_{ges} – Gesamtzeit; t_{a} – Ausfallzeiten).

Ausfallzeiten sind Zeiten für Wartung, Reparatur und Wiederanlauf nach Fehlfunktionen. Alternative Abschätzung über die mittlere Zeit der Verfügbarkeit $\bar{t}_{\mathrm{V}}$ und die mittlere Zeit für die Problembehebung $MTTR$ (Mean Time to Repair):

$$V = \frac{\bar{t}_{\mathrm{V}}}{\bar{t}_{\mathrm{V}} + MTTR}$$

Beispielaufgabe

Ein System soll mit einer Wahrscheinlichkeit $p_\mathrm{V} \geq 99{,}9\%$ verfügbar sein. Die mittlere Reparaturzeit beträgt $MTTR = 1\,\mathrm{h}$. Wie groß muss die mittlere Zeit der Verfügbarkeit $\bar{t}_\mathrm{V}$ dafür mindestens sein?

Lösung:
Die Wahrscheinlichkeit, dass ein System zu einem beliebigen Zeitpunkt verfügbar ist, ist die oben definierte Verfügbarkeit:

$$\begin{aligned} 99{,}9\% \leq p_\mathrm{V} = V &= \frac{\bar{t}_\mathrm{V}}{\bar{t}_\mathrm{V} + 1\,\mathrm{h}} \\ \bar{t}_\mathrm{V} &\geq 1\,\mathrm{h} \cdot \frac{99{,}9\%}{1 - 99{,}9\%} \approx 10^3\,\mathrm{h} \end{aligned}$$

Hoch verfügbare Systeme

Verfügbarkeit	t_a pro Monat	t_a pro Jahr
99%	7,2 h	87,6 h
99,9%	43 min	8,8 h
99,99%	4,3 min	53 min

99% ist normal. Hohe Verfügbarkeit ab 99,9% verlangt spezielle Maßnahmen:

- unterbrechungsfreie Stromversorgung,
- Raid-Speicher,
- Fehlertoleranz,
- gespiegelte Server,
- bereitstehende Ersatzkomponenten für Ausfälle,
- vorbeugende Wartung, Austausch von Verschleißteilen wie Festplatten nach vorgegebenen Nutzungsdauern,
- ...

Fehlerbäume und Verfügbarkeitspläne

- Ein System aus N_{TS} Teilsystemen, die alle für die Gesamtfunktion benötigt werden, ist verfügbar, wenn alle Teilsysteme verfügbar sind. Bei unabhängigen Verfügbarkeiten:

$$V_{\mathrm{ges}} = \prod_{i=1}^{N_{\mathrm{TS}}} V_i$$

  Im Fehlerbaum UND, im Verfügbarkeitsplan Reihenschaltung.
- Ein System aus N_{TS} Teilsystemen, die alle dieselbe Funktion übernehmen können, ist verfügbar, wenn mindestens ein Teilsysteme verfügbar ist. Bei unabhängigen Verfügbarkeiten:

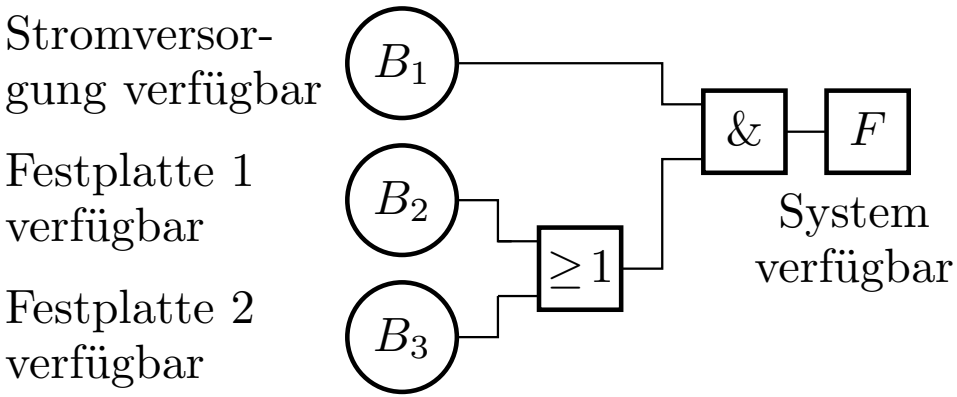
$$V_{\mathrm{ges}} = 1 - \prod_{i=1}^{N_{\mathrm{TS}}} (1 - V_i)$$

  Im Fehlerbaum ODER, im Verfügbarkeitsplan Parallelschaltung.

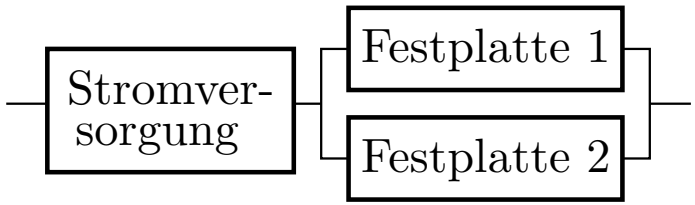
Beispiel

Ein System sei verfügbar, wenn die Stromversorgung und eine von zwei gespiegelten Festplatten verfügbar ist:

Fehlerbaum $p_{\mathrm{B}.i} = V_i$ und $p_{\mathrm{F}} = V$



Verfügbarkeitsplan



$$V = V_1 \cdot (1 - (1 - V_2) \cdot (1 - V_3))$$

Fehleranteil

Fehleranteil DL (Defect Level)

Definition Fehleranteil

Anteil der fehlerhaften Objekte in einer Menge gleichartiger Objekte.

Der zu erwartende Fehleranteil ist die Wahrscheinlichkeit, dass ein Objekt mindestens einen Fehler enthält

$$E(DL) = P(\varphi \geq 1)$$

und ist die »messbare« Fehleranzahl für nicht reparierbare Systeme:

- Viele zu erwartende Fehler $E(\varphi) \gg 1$: $E(DL) = 1$
- Wenig zu erwartende Fehler $E(\varphi) \ll 1$: $E(DL) = E(\varphi)$.

Für getestete elektronische Komponenten:

Typ	Leiterplatte	Schaltkreise	diskrete Bauteile	Lötstellen
DL	10 dpm	200 dpm	10 dpm	1 dpm

(dpm – Defects per Million).

Fehleranteil und Ausbeute

Für ungetestete nicht reparierbare Objekte ist der zu erwartende Fehleranteil die Wahrscheinlichkeit der Fehlerentstehung im Entwurfs- und Fertigungsprozess und damit der Kehrwert der Prozesszuverlässigkeit:

$$E(DL) = \frac{1}{Z_{\mathrm{P}}}$$

Die Kenngröße für den Anteil der fehlerfrei gefertigten Objekte:

Definition Ausbeute

Anteil der als gut befundenen gefertigten Objekte in einer Menge gleichartiger Objekte.

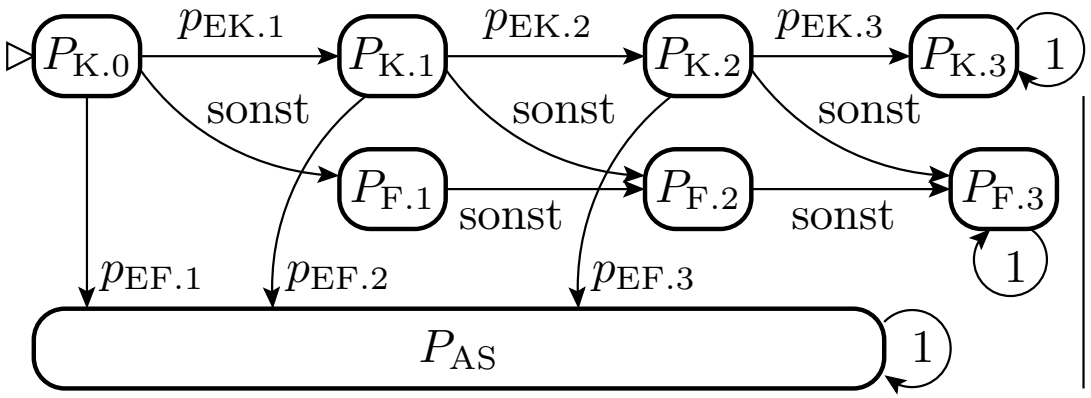
Zu erwartene Ausbeute in Abhängigkeit vom Fehleranteil:

$$E(Y) = 1 - p_{\mathrm{E}} \cdot E(DL)$$

(p_{E} – Erkennungswahrscheinlichkeit für defekte Objekte).

Fehleranteil und Entstehungsprozess

Markov-Kette für die Entstehung einen Produkts in 3 Schritten mit einer Kontrolle nach jedem Schritt:

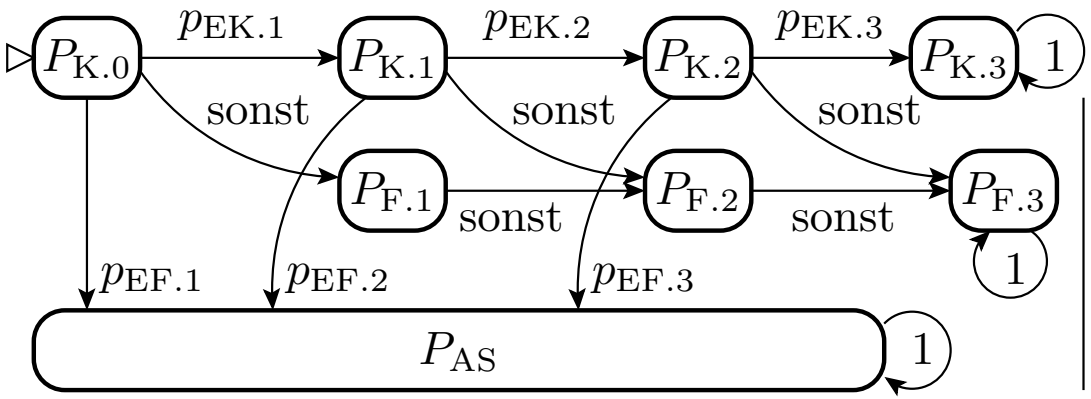


Zustände:

K.i	i Schritte abgearbeitet, kein Fehler entstanden
F.i	i Schritte abgearbeitet, mindestens ein Fehler, kein Fehler erkannt
AS	Produkt aussortiert

In jedem Schritt + Kontrolle entsteht mit einer

- Wahrscheinlichkeit $p_{EK.i}$ kein Fehler,
- mit $p_{EF.i}$ ein erkennbarer Fehler und
- sonst mit $1 - p_{EK.i}$- $p_{EF.i}$ ein nicht erkennbarer Fehler.



Zustände:

K.i	i Schritte abgearbeitet, kein Fehler entstanden
F.i	i Schritte abgearbeitet, mindestens ein Fehler, kein Fehler erkannt
AS	Produkt aussortiert

- Zu erwartender Fehleranteil:

$$E(DL) = \frac{p_{F.3}}{p_{K.3} + p_{F.3}}$$

- Prozesszuverlässigkeit:

$$Z_P = \frac{p_{K.3} + p_{F.3}}{p_{F.3}}$$

- Zu erwartende Ausbeute:

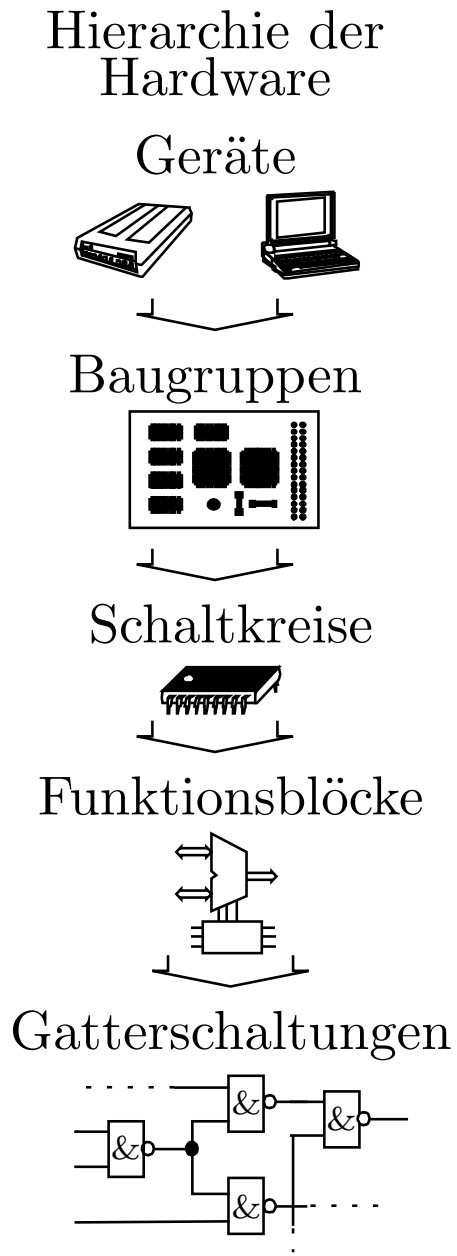
$$E(Y) = 1 - \frac{p_E \cdot p_{F.3}}{p_{K.3} + p_{F.3}}$$

(p_E – Erkennungswahrscheinlichkeit für defekte Objekte).

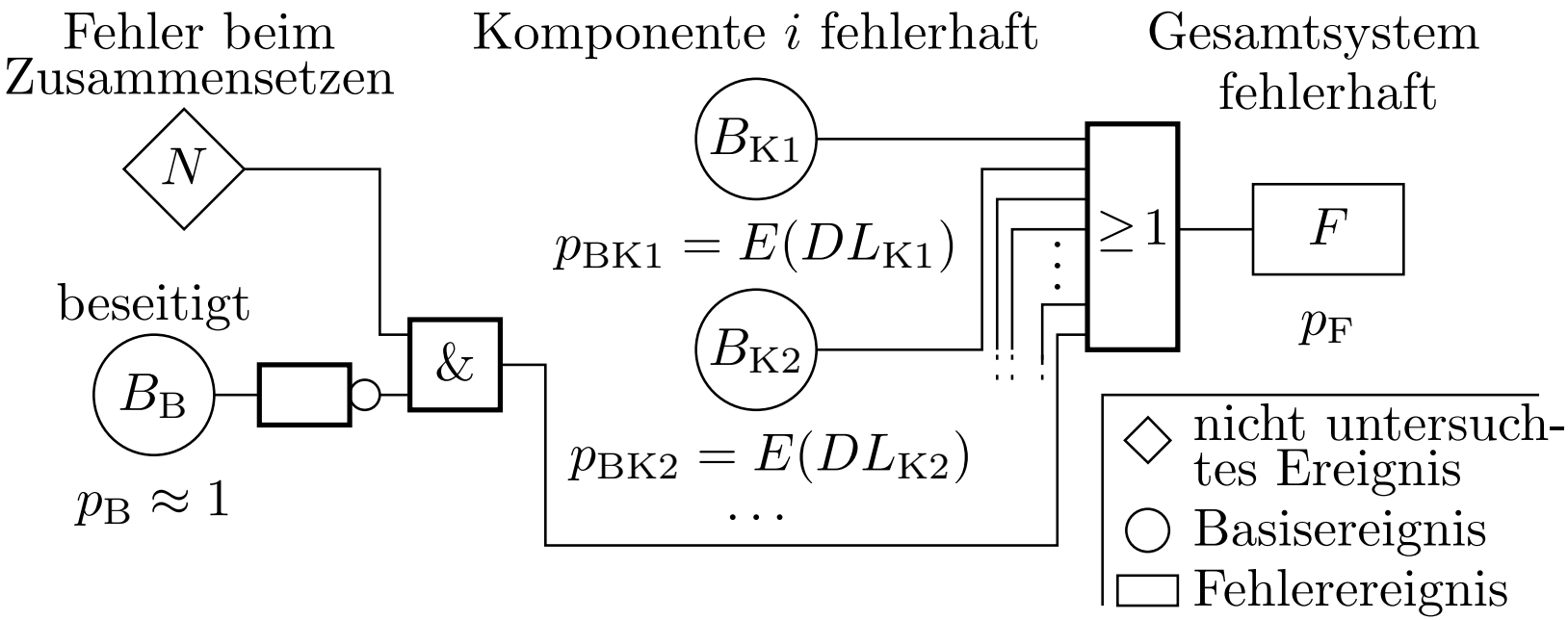
Zusammengesetzte System

In einem hierarchisch zusammengesetzten System werden die Komponenten vor dem Einbau in das übergeordnete System gründlich getestet.

- Die Tests im Verbund zielen hauptsächlich auf Verbindungsfehler.
- In einem Fehlerbaum für das getestete Gesamtsystem sind Komponentenfehler Basisereignisse mit dem zu erwartenden Fehleranteil als Wahrscheinlichkeit.
- Die Wahrscheinlichkeit von Verbindungsfehlern verringert sich um eine Beseitigungswahrscheinlichkeit ...



Fehleranteil beim Zusammensetzen eines Systems aus N_K Komponenten als Fehlerbaum:



Fehleranteil des zusammengesetzten Systems für $p_\mathrm{BNB} = 0$:

$$DL_\mathrm{ges} = \begin{cases} 1 - \prod_{i=1}^{N_\mathrm{K}} (1 - DL_{\mathrm{K}.i}) & \text{allgemein} \\ \sum_{i=1}^{N_\mathrm{K}} DL_{\mathrm{K}.i} & \text{für } DL_\mathrm{ges} \ll 1 \end{cases}$$

($DL_{\mathrm{K}.i}$ – Fehleranteil Komponente i).

Fehleranteil einer Baugruppe

Eine Baugruppe soll aus nachfolgenden Komponenten mit gegebenen Fehleranteilen bestehen:

Typ	Anzahl	DL_{BT}
Leiterplatte	1	10 dpm
Schaltkreise	20	200 dpm
diskrete Bauteile	35	10 dpm
Lötstellen	560	1 dpm

Welcher Fehleranteil ist für die Baugruppe zu erwarten, wenn die bei der Baugruppenfertigung zusätzlich entstehenden Fehler alle beseitigt werden:

$$\begin{aligned} DL_{\mathrm{Sys}} &\approx 1-\left(1-10^{-5}\right)\cdot\left(1-2\cdot10^{-4}\right)^{20}\cdot\left(1-10^{-5}\right)^{35}\cdot\left(1-10^{-6}\right)^{560} \\ &\approx 10^{-5}+20\cdot2\cdot10^{-4}+35\cdot10^{-5}+560\cdot10^{-6}=5000\,\mathrm{dpm} \end{aligned}$$

(dpm – defects per million).