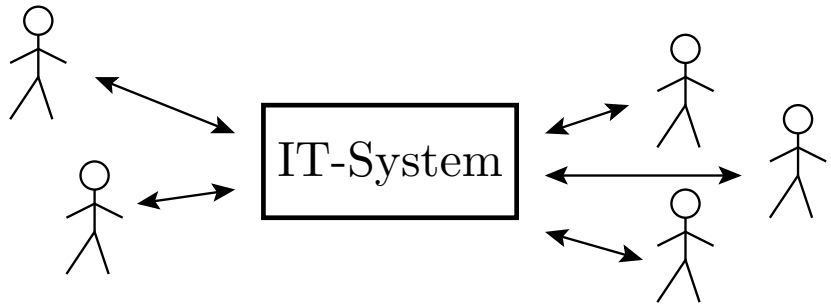
Test und Verlässlichkeit (F1) Kapitel 1: Modellbildung, Wahrscheinlichkeit, Experimente

Prof. G. Kemnitz

Institut für Informatik, Technische Universität Clausthal

11. Juni 2015

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.

Fakt 1

Vertrauen setzt Verlässlichkeit voraus.

Fehlfunktionen in IT-Systemen müssen nicht, aber können erheblichen Schaden verursachen:

- 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 [3].

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

In dem Begriff der Verlässlichkeit treffen Wunschvorstellungen und Wirklichkeit zusammen. Das macht eine objektive Bewertung schwierig[1]. Sprichworte mit tiefem Wahrheitsgehalt:

- Allen Leuten recht getan, ist eine Kunst, die keine kann.
- Verlorenen Vertrauen ist schwer wieder herzustellen.
- Whatever can go wrong will go wrong. (Murphys Law[2])
- It ist not a Bug, it is a feature. (Wegreden von Fehlern, statt Beseitigung.)

Der Schlüssel zu objektiv verlässlichen Systemen sind Kontrollen und das Abstellen der dabei erkannten Mängel auf drei Ebenen:

- während Entwurf und Fertigung (Fehlervermeidung),
- vor dem Einsatz und zur Wartung (Fehlerbeseitigung) und
- im laufenden Betrieb (Fehlertoleranz, Schadensvermeidung).

[1] Wie bei der Verlässlichkeit zwischenmenschlichen Beziehungen, in der Politik, Wirtschaft ... ist es auch für IT-Systeme kaum möglich, allgemein akzeptierte mess- oder abschätzbare Kriterien zu definieren.

[2] Viele Menschen denken pessimistisch, d.h. die negativen Erfahrungen bleiben viel stärker im Gedächtnis haften als die positiven.

Verlässlichkeit ist quantifizierbar durch

- Zählen/Schätzen der Anzahl unerwünschter Ereignisse (entstandender Fehler, Fehlfunktionen, Schadensfälle, ...) pro Zeit oder
- des Kehrwerts (mittlere Zeit pro unerwünschtes Ereignis).

Die verlässlichkeitssichernde Maßnahmen (Fehlervermeidung, -beseitigung, -toleranz, ...) sind quantifizierbar durch

- den Anteil der vermiedenen unerwünschten Ereignisse oder
- die Verlängerung mittleren Zeit pro unerwünschtes Ereignis.

Vielleicht wird einmal in einer KFZ-Beschreibung stehen: Fahren ohne ESP[3] hat für normal geübte Fahrer eine Verlässlichkeit von x Stunden pro Unfall und das Zuschalten von ESP erhöht die Verlässlichkeit um den Faktor y auf $x \cdot y$ Stunden.

[3] ESP (Electronic Stability Control) ist ein elektronisch gesteuertes Fahrassistenzsystem für Kraftfahrzeuge, das durch gezieltes Abbremsen einzelner Räder Unfällen durch Ausbrechen des Wagens entgegenwirkt.

Inhalt und Lernziel der Vorlesung

- Bewertung der Verlässlichkeit
- Kontrollen, Fehlertoleranz und Schadensvermeidung
- Test und Fehlerbeseitigung
- Fehlervermeidung.

Inhalt Foliensatz F1

Modellbildung

Der Begriff »Modell« in der Informatik

Selbst die einfachsten Sachverhalte in der Informatik wie die Abarbeitung eines Befehls werden sehr schnell kompliziert, wenn alle Details berücksichtigt werden.

Definition 2

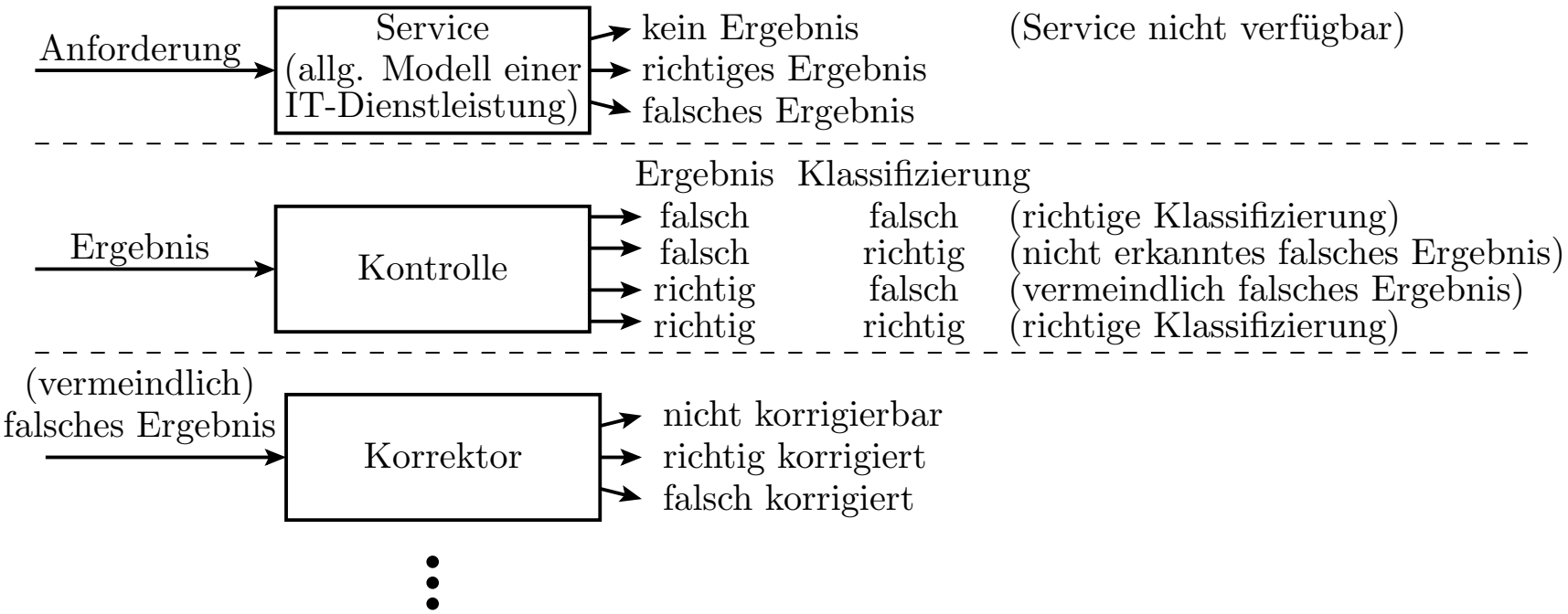
Ein Modell ist ein Mittel, um einen Zusammenhang zu veranschaulichen. Es stellt die wesentlichen Sachverhalte dar und verbirgt unwesentliche Details.

In dieser Vorlesung sind die Modelle Zufallsexperimente für

- das Funktionieren und Versagen von IT-Systemen,
- für Kontrollen, Tests, Reviews, Fehler, Ausfälle, ... ,
- Fehlervermeidung, Fehlerbeseitigung und Schadensbegrenzung.

für Systeme aus Hardware und/oder Software [+ Mechanik].

Modelle zur Beschreibung der Verlässlichkeit



- Unwesentlich sind tatsächliche Funktionen und Ergebnisse.
- Wesentlich ist die Unterscheidung zwischen gewünschten und unerwünschten Ergebnissen, ...
- Zählen bzw. Zufallsexperimente für gewünschte und unerwünschte Ergebnisse, ...

Zufallsexperiment

Zufallsexperiment

Definition 3

Ein Zufallsexperiment ist ein Experiment mit mehreren möglichen Ergebnissen und zufälligem Ausgang.

Zufallsexperimente zu Test und Verlässlichkeit:

- Anforderung einer Service-Leistung. WB[4]: richtig, falsch, ...
- Ergebniskontrolle: WB: richtig, falsch, ...
- Korrektur falscher Ergebnisse: WB: erfolgreich, ...
- Zählen der Fehler in einem System. WB: 0, 1, 2, ...
- Aufdecken eines Fehlers mit einem Test. WB: ja, nein
- Messen der Zeit bis zum Ausfall: WB: $t_A \geq 0\,s$
- ...

[4] Wertebereich der experimentellen Ergebnisse.

Bernoulli-Versuche

Das einfachste Zufallsexperiment ist der Bernoulli-Versuch. Er hat zwei mögliche Ergebnisse 0/1 (nein/ja, falsch/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:

- Kontrolle, ob ein Service verfügbar ist?
- Kontrolle, ob ein Service korrekt ausgeführt wird?
- Test, ob ein System fehlerhaft ist?
- Test, ob ein Fehler nachweisbar ist?

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

Service-Modell

Das Service-Modell

Definition 4

Eine Service sei ein Vorgang, der mit der Entgegennahme der Service-Anfrage beginnt, aus den Daten der Service-Anfrage Ausgaben berechnet und diese weitergibt.

Die Ein- und Ausgabe sind ganz allgemein bedatete Objekte mit einem auf die Art des Services abgestimmten Format. Das Format hängt von der Art des Systems ab und legt die Struktur und Bedeutung der Daten festlegt. Die Berechnung hat eine Soll-Funktion und optional weitere Vorgaben z.B. eine max. Ausführungszeit.

- Das Service-Modell ist für die meisten IT-Strukturen von den Grundbausteinen bis zum Gesamtsystem geeignet (Software, Hardware, Cyper-physikalische Systeme[5]) .
- Es beschreibt die wesentlichen Aspekte für den Test und die Verlässlichkeit:
  - Gibt es ein Ergebnis?
  - Wenn ja, ist es richtig?
  - ...

[5] Verbund informatischer Komponenten aus Soft- und Hardware mit mechanischen und elektronischen Teilen. Kopplung cyper- (informationstechner) mit physikalischen Komponenten.

Programme und Serverdienste als Service

Unterprogrammaufruf:

```
int16_t UP(int16_t16 a, int16_t b){
    return 23*(a+b);
};
```

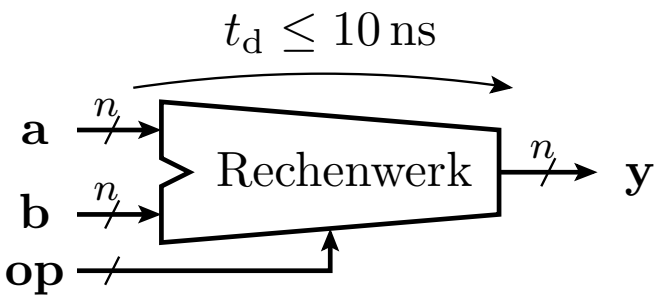
- Eingabe: Variable a und b vom Typ int16_t[6] bedatet mit den Aufrufwerten.
- Ausgabe: Rückgabewert vom Typ int16_t.
- Soll-Funktion[7]: Rückgabe ← 23*(a+b)

Server-Anfrage, z.B. an eine Suchmaschine:

- Eingabe: Internet-Datenpaket
- Ausgabe: Internet-Datenpaket
- Soll-Funktion: Erstellung einer Liste von Suchergebnissen.

[6] int16_t – 16-Bit-Typ Zweierkomplement in AVR-Studio.
[7] Die Soll-Funktion weicht im Beispiel von der Ist-Funktion ab.

Hardware- und Cyper-physikalische Systeme



a, **b**	Operanden
op	Operationscode
y	Ergebnis
n	Bitbreite
t_d	Verzögerungszeit

Rechenwerk als Beispiel für eine digitale Verarbeitungsfunktion:

- Eingabe: Operanden und Op.-Code.
- Ausgabe: Ergebnis.
- Funktion: arithmetische oder logische Operation

Motorsteuergerät als Beispiel für ein CP-System:

- Eingabe: Messwerte am Motor, Soll-Position, Ist-Position, ...
- Ausgabe: Stellwert, Anzeigewerte, ...
- Soll-Funktion: Reglung der Zündzeitpunkte, ...

Service-Leistungen ohne und mit Gedächtnis

Eine Service-Leistung ist, um testbar zu sein, i.allg. deterministisch. 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 Funktion:

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

und einer Ausgabefunktion

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

Die Unterteilung »ohne/mit Gedächtnis« gilt für jeden Service-Typ (Programme, Hardware, CP-Systeme, ...):

	ohne Gedächtnis	mit Gedächtnis
Programm-bausteine	Unterprogramme ohne private Daten	OOP-Methoden zur Objektbearbeitung.
Programm	Compiler	Textverarbeitung
Serverdienst	Ohne Nutzung fremder Daten.	Datenbankanfrage
digitale Schaltung	Rechenwerk	Prozessor
CP-System	Maschine, die aus Vorgaben Werkstücke herstellt	Steuergeräte, die sich Daten merken

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

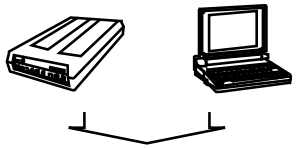
Service-Hierarchie

IT-Systeme sind hierarchisch aufgebaut:

- Client-Server-Systeme bestehen aus Rechnern und Netzwerkkomponenten.
- Rechner, Netzwerkkomponenten, ... bestehen aus Hard- und Software.
- Software besteht aus Programmbausteinen, diese sind aus Programmieranweisungen zusammengesetzt, die ihrerseits mit Maschienenbefehlen nachgebildet werden.
- Maschinenbefehle sind Service-Leistungen der Hardware. Die Hardware bestehen aus Funktionsbausteinen, diese meist aus Gattern und diese wiederum aus Transistoren.

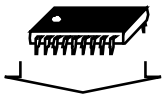
Hierarchie der Hardware

Geräte

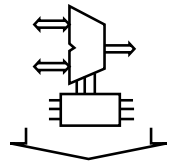


Baugruppen

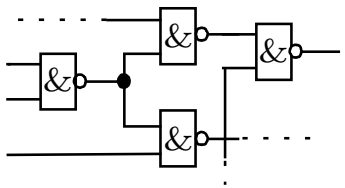
Schaltkreise



Funktionsblöcke



Gatterschaltungen



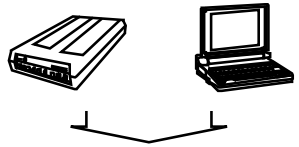
Im Service-Modell

- stellen die Transistoren elementare Schaltfunktionen bereit (ein/aus) mit denen Gatterfunktionen und Speicherelemente gebildet werden.
- Mit Gattern und Speicherelementen werden komplexere Funktionseinheiten wie Rechenwerke, Register bis hin zu kompletten Rechnern nachbildet.
- Die Software nutzen Hardware-Funktionen, ...

Ein IT-System funktioniert korrekt, wenn alle Service-Leistung hierarchisch absteigend korrekt arbeiten und der Informationsfluss dazwischen korrekt abläuft.

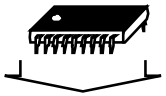
Hierarchie der Hardware

Geräte

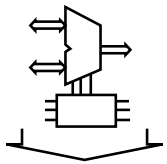


Baugruppen

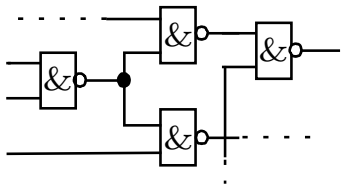
Schaltkreise



Funktionsblöcke



Gatterschaltungen



Fehlfunktionen und Fehler

Fehlfunktionen, Fehler, Störungen und Ausfälle

Fehlfunktionen sind erkennbare Abweichungen vom Sollverhalten.

Die Ursachen (root cause) für Fehlfunktionen können sein:

- Fehler:
  - wirken ständig,
  - sind durch Reperatur oder Ersatz beseitigbar,
  - entstehen im Entwurfs- oder Fertigungsprozess,
  - sind durch Beseitigung ihrer Entstehungsursache vermeidbar.
- Störungen:
  - spontane, nicht reproduzierbare Wirkung,
  - schwer zu vermeiden oder abzustellen.
- Ausfälle:
  - Während des Betriebs entstehende Fehler.

Aufgelistetet sind die wesentlichen Aspekte (siehe Modelldefinition).

Fehler in Systemen ohne Gedächtnis

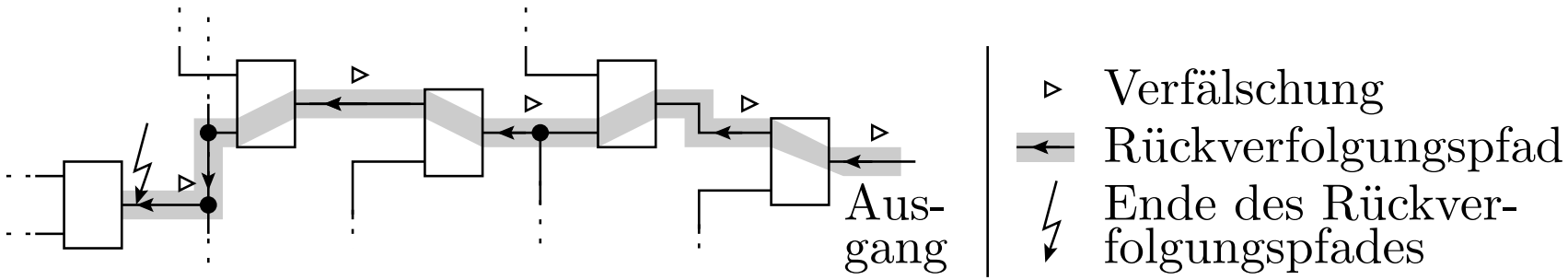
Fehler + beeinträchtigte Servic-Anforderung ⇒ Fehlfunktion

Fehlernachweis:

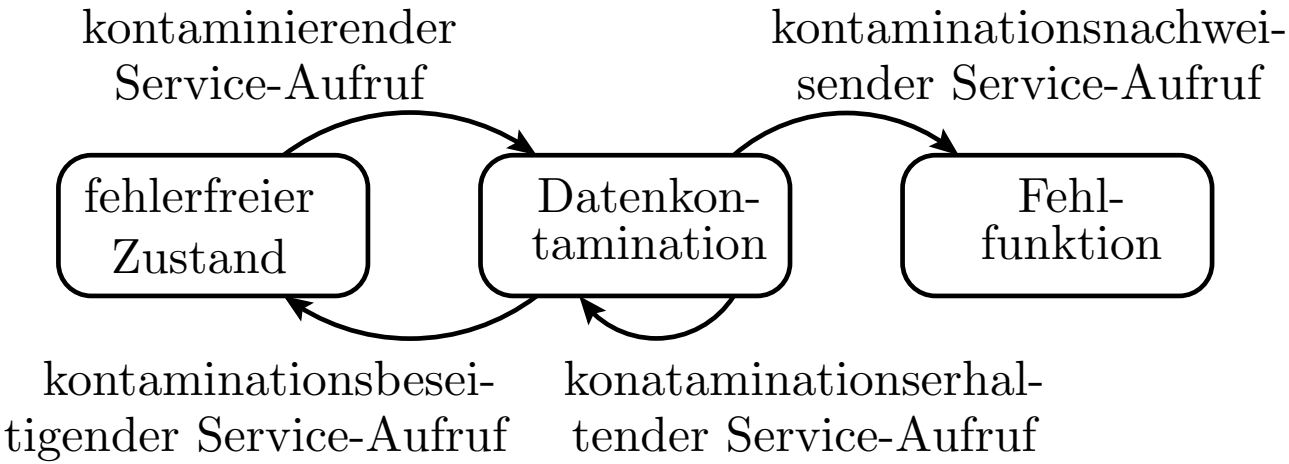
- Service mit fehlernachweisender Bedatung anfordern.
- Kontrolle der Ausgabe.

Fehlerlokalisierung und Reparatur:

- Suche der untersten Teilservice-Leistung oder Kommunikation, die mit korrekten Daten falsch ausgeführt wird.
- Ersatz, Reparatur, ... der lokalisierten Teilservice-Leistung.
- Erfolgskontrolle durch Wiederholung der Anforderung.



Fehler in Systemen mit Gedächtnis



Fehlernachweis:

- Verlangt eine Folge kontaminationserzeugender, -erhaltender und -nachweisender Service-Anforderungen + Kontrollen.

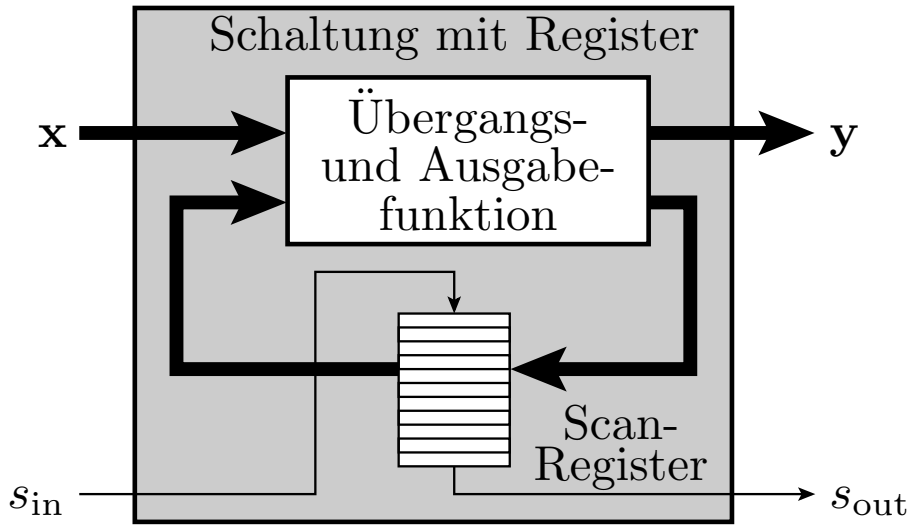
Fehlerlokalisierung:

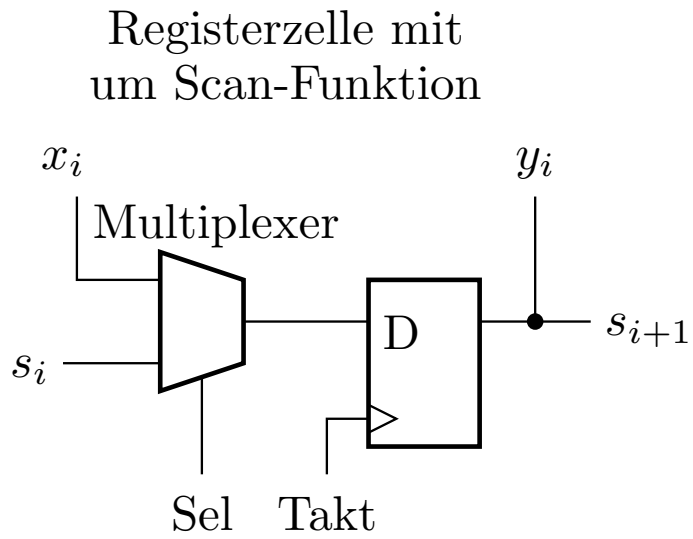
- Rückwärts über mehrere Service-Anforderungen. System mehrfach neu starten, um die kontaminierende Anforderung zu finden, ... Lokalisierung der kontaminierenden Anforderungen anhand mitgeschriebener interner Daten.

Isolierter Test der Übergangs- und Ausgabefunktion

Fehlernachweis und -lokalisierung ist in Systemen mit Gedächtnis viel schwieriger als in Systemen ohne. Isolierter Test der Übergangs- und Ausgabefunktion:

- Debugger: Programm anhalten und Variablen kontrollieren.
- Trace: Mitschreiben der internen Daten.
- Hardware: Lesen (und Überschreiben) der gespeicherten Daten nach jedem Testschritt z.B. mit Scan-Registern.





Potentielle und Modellfehler

Potentielle Fehler

In den nachfolgenden statistischen Modellen hat jedes System eine abzählbare Menge potentieller Fehler, die mit gewisser Wahrscheinlichkeit vorhanden sein könnten.

Eine zweckmäßige, aber nicht perfekte Definition:

Definition 5

Potentielle Fehler seien hierachisch absteigend alle Teil-Service-Leistungen und Kommunikationswege, die falsch ausgeführt werden können, ohne dass in ihnen eine genauere Lokalisierung möglich ist.

Beispiele potentieller Fehler:

- Transistorfehler, Gatterfehler, Prozessorfehler, ...
- Anweisungsfehler, vertauschte Variablen, fehlerhaftes Unterprogramm, fehlerhafter Service, ...

Die Fehlerhierarchie folgt der Service-Hierarchie.
Digitale Schaltung:

- Transistorfehler: Transistor schaltet nicht ein oder aus.
- Gatterfehler: falsche logische Ausgabe, ...
- Rechner: falsche/keine Operationsausführung

Software:

- falsche Ausführung von Maschinenbefehlen,
- falsche Ausführung von Befehlsfolgen, Unterprogrammen,
- fehlerhafte Programmbausteine, ...

Die Anzahl der potentiellen Fehler ist etwa proportional zur Systemgröße, aber

- jeder potentielle Fehler kann unterschiedlichste Fehlerwirkungen haben.
- Sein Verhalten lässt sich nicht simulieren und
- nur ungefähr mit einer Nachweiswahrscheinlichkeit beschreiben.

Zu erwartende Fehler

Nicht alle potentiellen Fehler und ihre möglichen Funktionsverfälschungen sind gleichwahrscheinlich. Die zu erwartenden Fehler hängen vom Entstehungsprozess ab:

- Fertigungsfehler (z.B. bestückte Baugruppen): Kurzschlüsse, Unterbrechungen, Fehlbestückungen, Lötfehler, ...
- Entwurfsfehler: vergessene oder falsch interpretierte Anforderungen, falscher Algorithmus, fehlerhafte Programmzeilen, durch Compilieren entstande Fehler, ...

- Entwurf birgt mehr Fehlermöglichkeiten als Fertigung.
- Mehrfach genutzte Komponenten gleiche Entwurfsfehler. ...
- Unbeständige Fehlerwirkung durch Fremdeinflüssen (Temperatur, Versorgungsspannung, ..), unzugängliche gespeicherte Zustände, ...

Modellfehler

Für die Bewertung von Testsätzen und die geziele Suche von Testbeispielen wird eine Menge von in das System einfügbarer oder simulierbarer Beispielfehler benötigt.

Definition 6

Ein Modellfehler ist eine Beispielfehler mit exakt vorgegebenem Fehlverhalten.

Beispiele für Modellfehler:

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

Ein Algorithmus für die Berechnung von Modellfehlermengen wird als Fehlermodell bezeichnet.

Ausfall

Die Hardware und Mechanik eines IT-Systems unterliegt einem Verschleiß, der zur Zerstörung von Teilsystemen führen kann.

Definition 7

Ein Ausfall ist ein Fehler, der während des Einsatzes entsteht.

Die meisten Fehler in IT-Systemen sind solche, die von den Tests vor dem Einsatz nicht erkannt wurden. Da die Iteration aus Test und Fehlerbeseitigung vor dem Einsatz vorrangig die gut nachweisbaren Fehler beseitigt, versagen Systeme im Einsatz nur selten aufgrund nicht erkannter Entwurfs- und Fertigungsfehler.

Ausfälle können auch gut oder schlecht nachweisbar sein und so die Verlässlichkeit kaum bis komplett beeinträchtigen. In der Umgangssprache werden nur die Ausfälle als solche gezählt, die die Verlässlichkeit spürbar beeinträchtigen.

Aufgaben

Aufgabe 1.1: Wertebereichsproblem

Eine Service-Leistung sei definiert durch:

- Eingabeformat: a, b: 16-Bit Zweierkomplement
- Ausgabeformat: Rückgabewert 16-Bit Zweierkomplement
- Soll-Funktion: Rückgabe des Wertes des Ausdrucks a-b+25
- Implementierung als C-Funktion:

```
int16_t fkt(int16_t a, int16_t b){
    return a-b+25;
}
```

1. Wie groß sind die kleinsten und größten darstellbaren Ein- und Ausgabewerte?
2. Für welche Bedatungen von a und b unterscheidet sich der Ausgabe-Ist- vom Ausgabe-Soll-Wert?
3. Wie sind Ist- und die Soll-Funktion zu verändern, so dass bei einem Bereichsüber- bzw. -unterlauf des Ergebnisses der größte bzw. kleinste darstellbare Wert zurückgegeben wird?

Aufgabe 1.2: C-typischer Multiplikationsfehler

Eine Service-Leistung sei definiert durch:

- Eingabeformat: zwei Variablen a und b, 8-Bit vorzeichenfrei
- Ausgabeformat: Rückgabewert 16-Bit vorzeichenfrei
- Sollfunktion: Rückgabe des Produkts a*b
- Implementierung als C-Funktion:

```
uint16_t umult16(uint8_t a, uint8_t b){
 return a*b;
}
```

1. Kleinster und größter darstellbarer Ein- und Ausgabewerte?
2. Für welche Bedatungen von a und b unterscheidet sich der Ist- vom Soll-Wert der Ausgabe[8]?
3. Wie ist die Ist-Funktion zu verändern, dass für alle Eingabewerte das korrekte Ergebnis berechnet wird?

[8] In C hat ein Produkt den Typ des Operanden mit dem größten Wertebereichs. Typenumwandlung der Zuweisung erst nach Produktbildung.

Aufgabe 1.3: Typ. Fehler einer Gleitkommadivision

Eine Service-Leistung sei definiert durch:

- Ein- und Ausgabegabeformat: 32-Bit Gleitkommaformat IEEE 754 »single«
- Soll-Funktion: Rückgabe von y=sin(x)/x mit maximaler Soll-/Ist-Abweichung:

$$\frac{|y_{\text{Soll}} - y_{\text{Ist}}|}{y_{\text{Ist}}} < 0.01\%$$

- Implementierung als C-Funktion:

```c
#include <math.h>
float sinc(float x){
  return sin(x)/x;
}
```

1. Beschreiben Sie den Aufbau das Gleitkommaformats IEEE 754 »single«[9].
2. Wie wird der Eingabewert -5.0 dargestellt?
3. Für welchen Eingabebereich weicht das Ist-Ergebnis vom Soll-Ergebnis ab.
4. Verbessern Sie die Implementierung, so dass sie auch für den im Aufgabenteil zuvor bestimmten Wertebereich der Eingabe korrekte Ergebnisse liefert.

[9] Die benötigten Informationen finden unter dem Suchbegriff »IEEE Gleitkommaformat« im Internet.

Aufgabe 1.4: Initialisierungsfehler

Das nachfolgende Unterprogramm soll für das mit einem Zeiger auf den Anfang und der Länge übergebene Feld den kleinsten Wert zurückgeben und hat ein unbeständiges Fehlverhalten.

```
int16_t Feld[]= {231, -13, ...}; // Beispiel für ein Feld
...
int16_t kleinsterWert(int16_t *Feld, uint16_t len){
  int16_t tmp, *ptr;
  for (ptr=Feld; ptr <Feld+len; ptr++){
    if (*ptr<tmp) tmp = *ptr;
  }
 }
```

1. Mit welchen Eingaben und Zusatzbedingungen ist der Fehler nachweisbar?
2. Ändern Sie das Programm so, dass es korrekt funktioniert.

Aufgabe 1.5: Fehler in kombinatorischer Schaltung

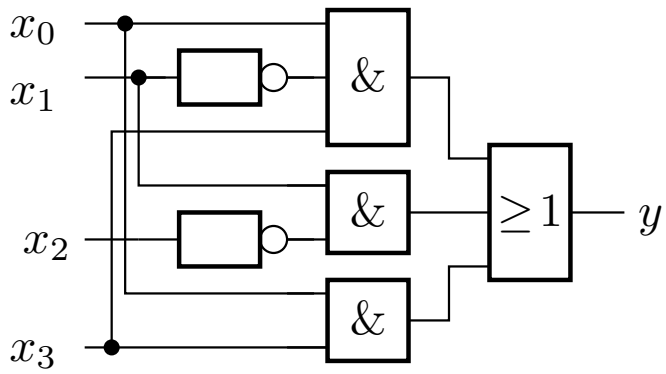
Eine kombinatorische Schaltung mit der Soll-Funktion entsprechend der nachfolgenden Wertetabelle ist durch die Schaltung daneben realisiert.

Soll-Funktion

x_3	x_2	x_1	x_0	y
0	0	0	0	1
0	0	0	1	0
0	0	1	0	1
0	0	1	1	0
0	1	0	0	0
0	1	0	1	1
0	1	1	0	0
0	1	1	1	0

x_3	x_2	x_1	x_0	y
1	0	0	0	1
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	0
1	1	1	1	0

Realisierung

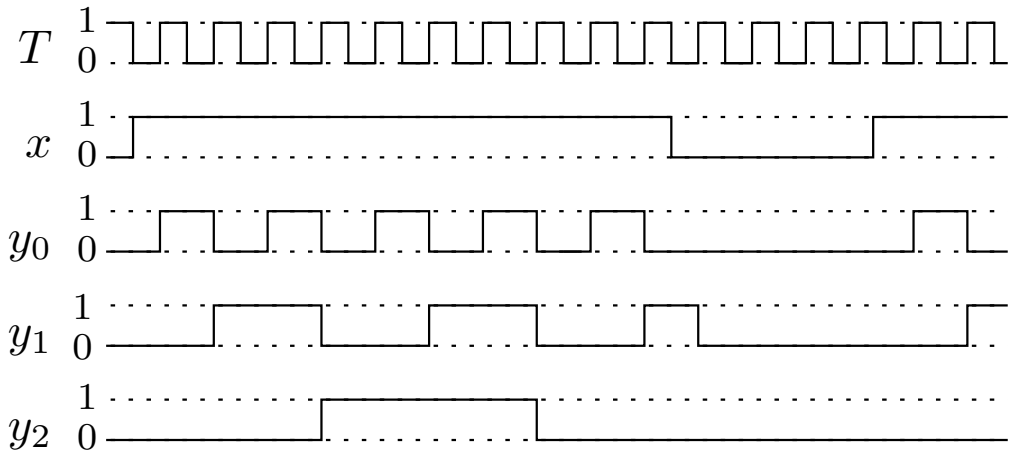


1. Stellen Sie die Wertetabelle der Realisierung auf. Für welche Eingaben weicht die Ausgabe vom Soll-Wert ab.
2. Verbessern Sie die Realisierung so, dass Sie für alle Eingaben richtige Ergebnisse liefert.

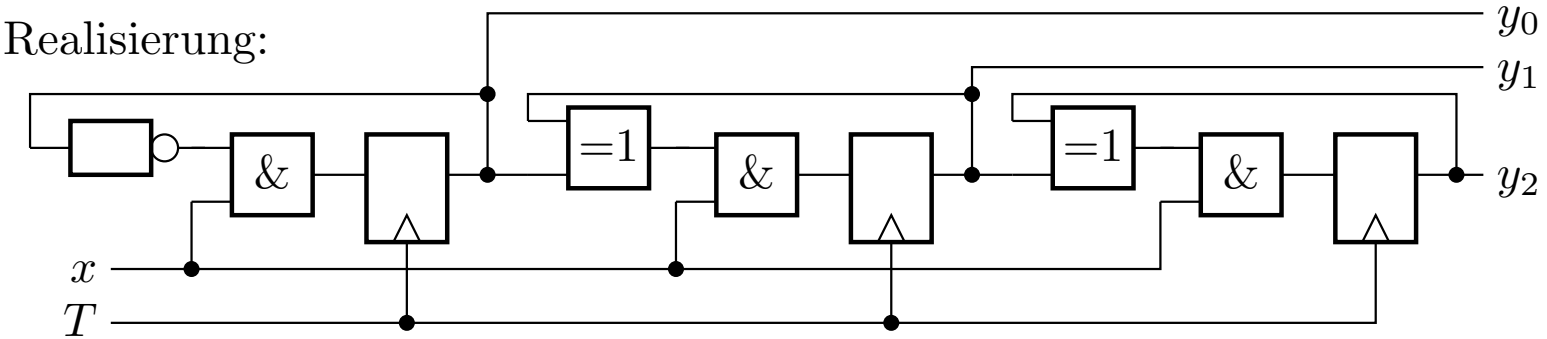
Aufgabe 1.6: Seqentielle Schaltung mit Fehler

Eine Schaltung soll bei $x = 0$ in den Zustand $\mathbf{y} = y_2 y_1 y_0 = 000$ übergehen und sonst bei jeder aktiven Taktflank seinen Wert um eins erhöhen (Binärzähler).

Testbeispiel mit Soll-Werten für die Ausgabe



Realisierung:



Gezeigt sind ein Testbeispiel mit Soll-Signalverläufen und eine fehlerhafte Realisierung.

1. Bestimmen Sie die tatsächlichen Ausgabesignalverläufe y_i für das Testbeispiel.
2. Korrigieren Sie die Schaltungsrealisierung so, dass sie das Testbeispiel richtig abarbeitet.

Aufgabe 1.7: Wurzelberechnung

Eine Service-Leistung sei definiert durch:

- Eingabeformat: uint16_t (16 Bit, vorzeichenfrei)
- Ausgabegabeformat: uint8_t (8 Bit, vorzeichenfrei)
- Soll-Funktion: Rückgabe der ganzzahligen Anteils der Wurzel
- Implementierung als C-Funktion:

```
uint8_t wurzel(uint16_t x){
 uint8_t w=0;
 uint16_t sum=0;
 while (sum<x){sum += (w<<1)+1;
 w++;}
 return w;
} <ausprobieren>
```

1. Mit welchen Eingaben ist der Fehler nachweisbar?
2. Ändern Sie das Programm so, dass es korrekt funktioniert.

Wahrscheinlichkeit

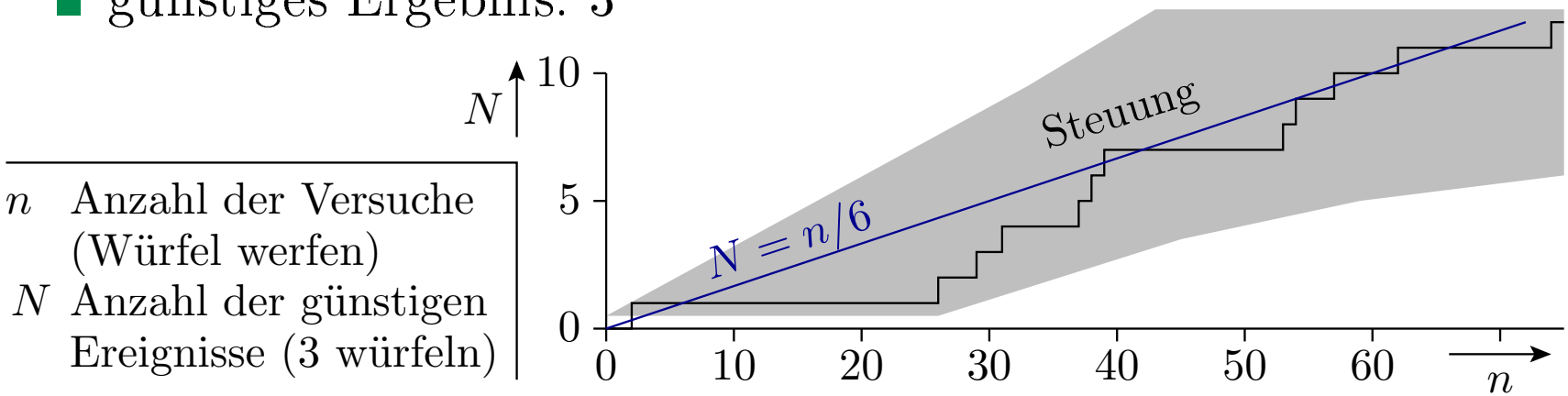
Die Wahrscheinlichkeit von Zufallsexperimenten

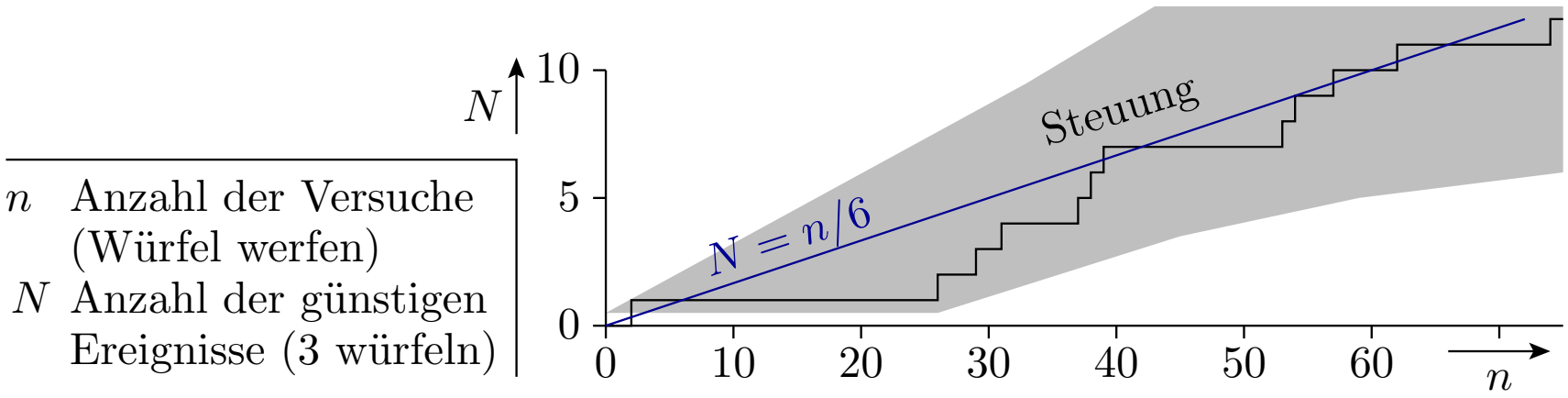
Definition 8

Wahrscheinlichkeit ist das 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





Beim Würfeln wird davon ausgegangen, das alle 6 Möglichkeiten gleichwahrscheinlich sind. Mit Versuchsanzahl $n \to \infty$ strebt das Verhältnis aus günstigen Ergebnisse 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 keineswegs, dass bei jedem sechsten Versuch eine 3 gewürfelt wird. Es ist durchaus zu beobachten, dass hintereinander mehrere Dreien und auch mal lange Zeit keine Dreien gewürfelt werden.

Aufteilen und verketteten von Experimenten

Zufallsexperimente lassen sich u.U. in mehrere Experimente 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 eine unauffällige und beliebte Technik, Statistiken zu fälschen[10].

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

Verkettete Ereignisse

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 alle eintreten:

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

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

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

Beispiel: Nachweis unabhängiger Fehler

In einem System mit drei Fehlern seien diese unabhängig voneinander mit den Nachweiswahrscheinlichkeiten $p_1 = 10\%$, $p_2 = 5\%$ 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?

Lösung: Definition von Ereignissen F_i für Fehler i nachweisbar und Beschreibung von E_i durch logische Verknüpfungen:

- 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:

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

- 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 Fehlern 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, nächste Folie):

$$\begin{aligned} E_4 &= \left(F_1 \wedge F_2 \wedge \bar{F}_3\right) \vee \left(\bar{F}_1 \wedge F_2 \wedge F_3\right) \vee \left(F_1 \wedge \bar{F}_2 \wedge F_3\right) \\ P(E_4) &= p_1 \cdot p_2 \cdot (1 - p_3) + (1 - p_1) \cdot p_2 \cdot p_3 + p_1 \cdot (1 - p_2) \cdot p_3 \\ &= 90\% \cdot 5\% \cdot 20\% + 10\% \cdot 95\% \cdot 20\% + 10\% \cdot 5\% \cdot 80\% = 6{,}8\% \end{aligned}$$

Abhängige Ereignisse

Die Wahrscheinlichkeiten der UND- oder ODER-Verknüpfung von abhängigen Ereignissen $A \wedge B$ und $A \vee B$ lassen sich nur aus den Wahrscheinlichkeiten $P(A)$ und $P(B)$ der Einzelereignisse bestimmen, wenn sich die Ereignisse ausschließen:

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

Die Wahrscheinlichkeit, dass eines von beiden eintritt ist dann die Summe der Einzelwahrscheinlichkeiten:

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

Ist diese Voraussetzung nicht erfüllt, ist das Experiment so umformulieren, dass sich danach alle zu verkettenden Ereignisse gegenseitig ausschließen oder voneinander unabhängig sind.

Beispiel »abhängiger Fehlernachweis«

Wie groß sind die Wahrscheinlichkeiten, dass von zwei Fehlern in einem 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[11]:

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

[11] 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:

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

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

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

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

$$90\% + 2\% + 8\% = 100\%\surd$$

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" bedatet wird, wenn

1. unabhängig voneinander für jedes Bit mit einer Wahrscheinlichkeit[12] 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 höchtwertigen vier Bits immer derselben Zufallswert ausgewählt wird.

[12] Die Wahscheinlichkeit g wird auch als Wichtung der Bitstelle bezeichnet. Wichtung wird beim Test 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 Teilaufgaben gilt:

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

Für die letzte Teilaufgabe folgt aus $G_7 = G_6 = G_5 = G_4$:

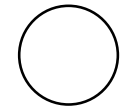
$$\begin{aligned} \mathbf{x} = \text{"11111110"} &= G_4 \wedge G_3 \wedge G_2 \wedge G_1 \wedge \bar{G}_0 \\ P(\mathbf{x} = \text{"11111110"}) &= g^4 \cdot (1-g) \end{aligned}$$

g	50%	60%
G_4 bis G_7 unabhängig	$2^{-8} \approx 0{,}004$	$0{,}6^7 \cdot 0{,}4 = 0{,}01$
$G_7 = G_6 = G_5 = G_4$	$2^{-5} \approx 0{,}03$	$0{,}6^4 \cdot 0{,}4 = 0{,}05$

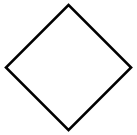
Fehlerbaumanalyse

Fehlerbaumanalyse (FTA – fault tree analysis)

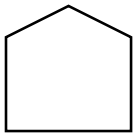
Die FTA dient zur Beschreibung von Fehlersituationen und zur Abschätzung deren Wahrscheinlichkeiten. Sie unterscheidet:



Basisereignisse, die nicht weiter untersucht werden, weil sie gut bekannt sind, oder Wahrscheinlichkeiten dafür existieren.



Nicht untersuchte Ereignisse.

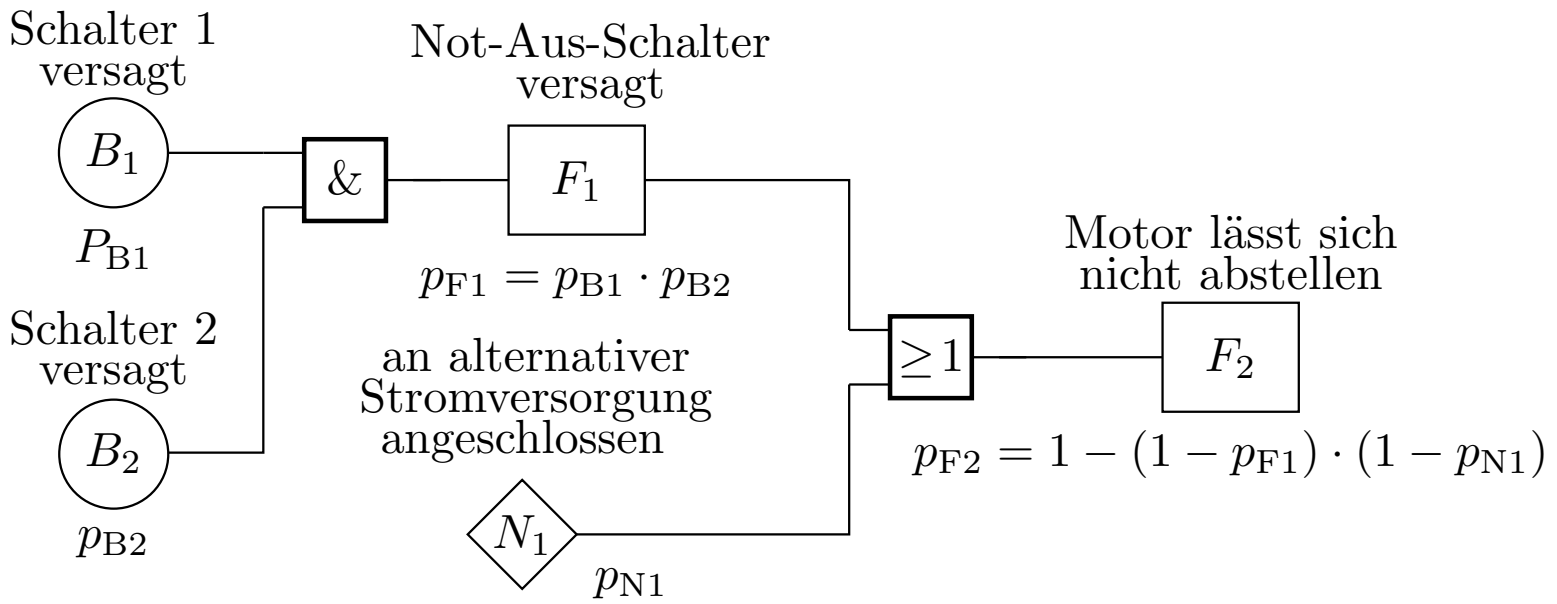


Ereignisse, die im gewöhnlichen Betrieb auftreten, aber in Kombination mit anderen Ereignissen Fehlerquelle sein können.

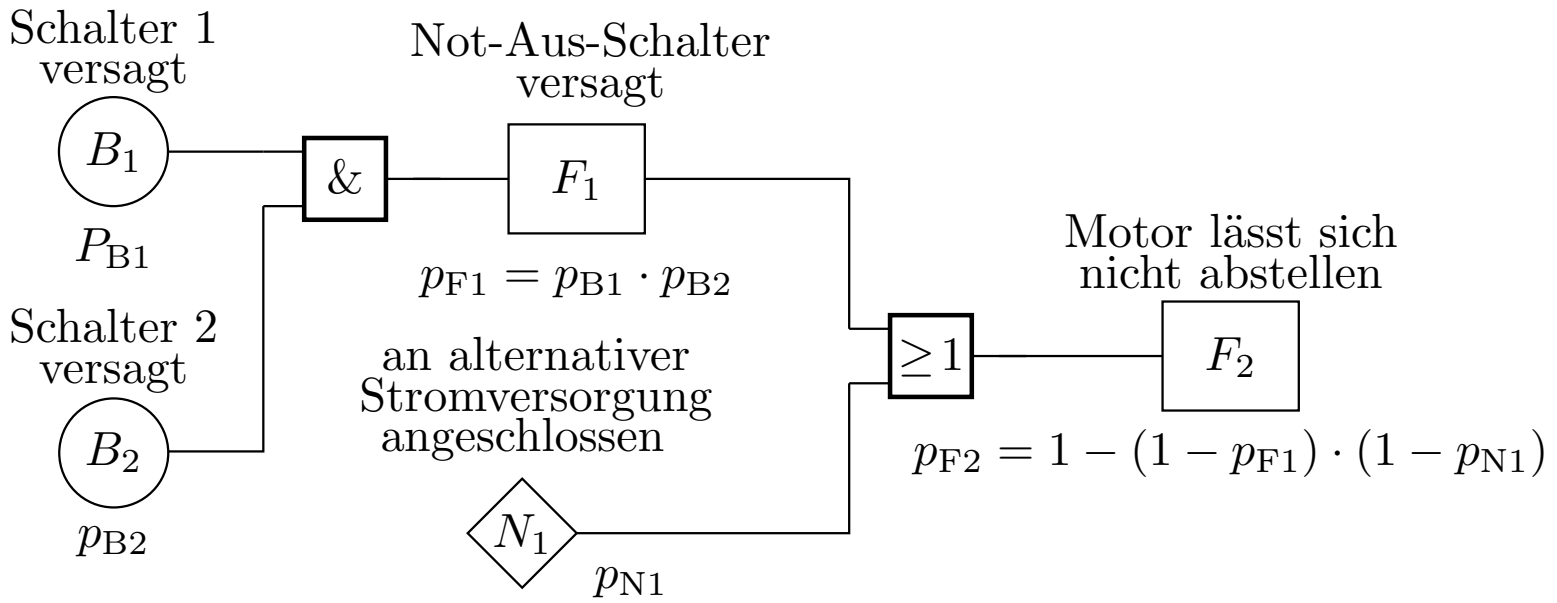
Fehlerereignisse, die sich nicht weiter aufteilen lassen.

Die Ereignisse können direkt oder als Komplementereignis UND und ODER verknüpft sein.

Beispiel: Motor lässt sich nicht abstellen



- Zusammenstellen und Klassifizierung der zu berücksichtigenden Ereignisse.
- Verknüpfung mit UND-, ODER-, NICHT
- Abschätzung der Wahrscheinlichkeit der verketteten Ereignisse nach den Gl. 1 bis 5:



Angenommen, die Schalter versagen mit einer Wahrscheinlichkeit von 10^{-3} und die Wahrscheinlichkeit, dass eine alternative Stromversorgung existiert, ist nicht größer als 10^{-8}, ergibt sich für den betrachteten Fehlerfall eine Wahrscheinlichkeit:

$$p_{F2} < 10^{-3} \cdot 10^{-3} + 10^{-8} - 10^{-3} \cdot 10^{-3} \cdot 10^{-8} \approx 10^{-6}$$

Am Überschlags kann jetzt diskutiert werden, ob das Risiko von 10^{-6}, dass der Motor nicht abschaltet, akzeptiert wird oder weitere Maßnahmen ergriffen werden, z.B. dritter Schalter.

Beispiel Überlebenswahrscheinl. mit Redundanz

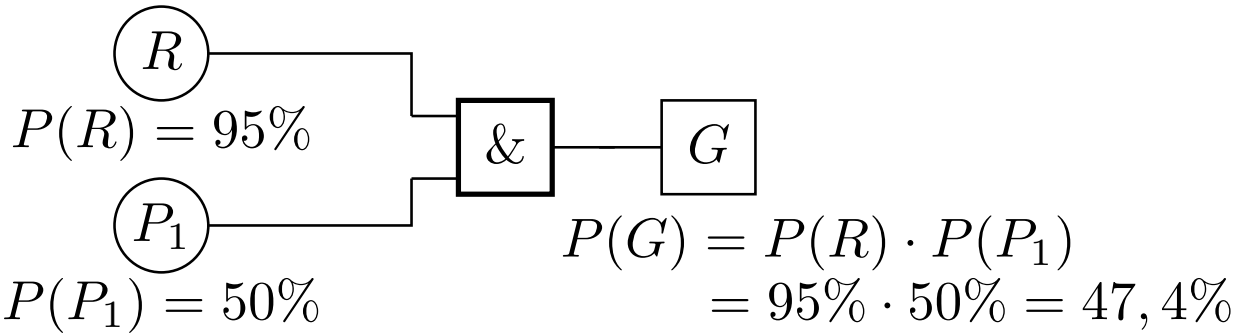
Mit dem Modell »Fehlerbaum« lässt sich auch das Überleben eines Systems mit mehreren Komponenten beschreiben.

Beispiel: Rechner mit redundantem Plattensystem. Der Rechner soll ohne die Berücksichtigung der Plattenausfälle über den betrachteten Zeitraum eine Überlebenswahrscheinlichkeit $p_{\mathrm{R}} = 95\%$ und die Platten von $p_{\mathrm{P}} = 50\%$ haben.

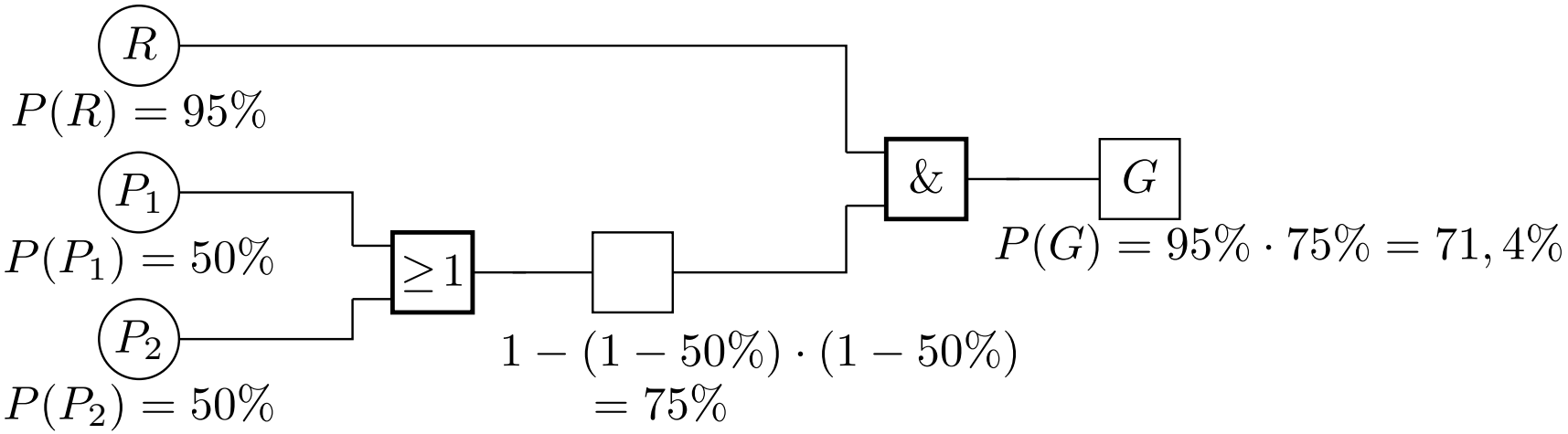
- Wie groß ist die Überlebenswahrschenlichkeit $p_{1\mathrm{P}}$ des Rechners mit nur einer Platte?
- Wie groß ist die Überlebenswahrschenlichkeit $p_{2\mathrm{P}}$ mit zwei Platten, wenn der Rechner auch nur mit einer Platte benutzbar bleibt?

Lösung: Die Ereignisse, Gesamtsystem, Rechner ohne Platte und die beiden Platten überleben, sollen mit den zweiwertigen Zufallsvariablen G, R, P_1 und P_2 bezeichnet werden.

Mit einer Platte überlebt das Gesamtsystem, wenn Platte und Rechner überleben. Überlebenswahrsch. 47,4%:

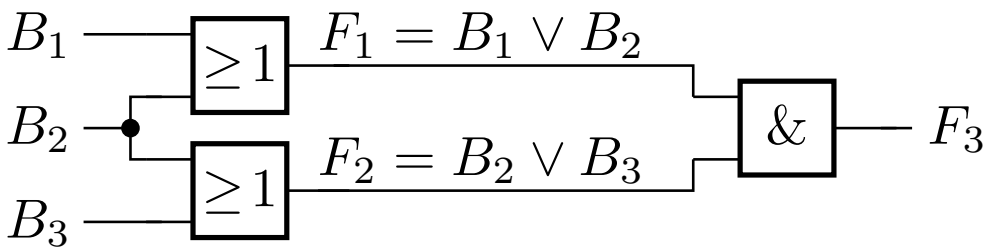


Mit zwei Platten überlebt der Rechner, solange Rechner und mindestens eine Platte überleben. Überlebenswahrsch. 71,4%:



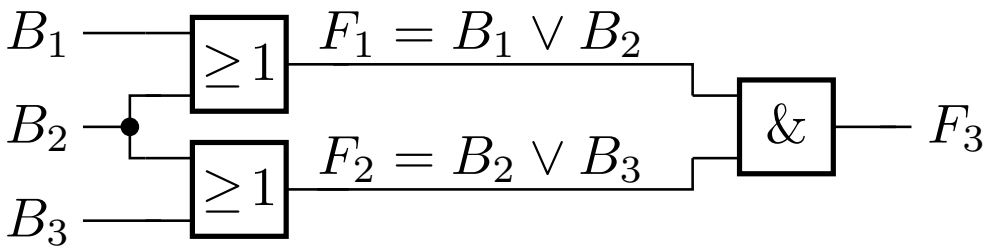
Fehlerbäume mit rekonvergenten Auffächerungen

- Rekonvergente Auffächerungen sind Schlaufen in gerichteten Graphen.
- An den Verzweigungen am Schlaufenbeginn werden abhängige Ereignisse gebildet und am Schlaufenende miteinander verknüpft.



- Im Beispiel sind die beiden ODER-verknüpften Ereignisse beide von B_2 abhängig, schließen sich aber auch nicht aus, so das für die UND-Verknüpfung weder Gl. 2 noch 4 gilt.

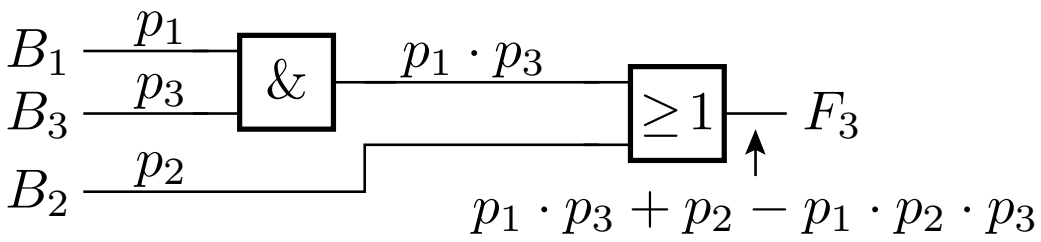
Beseitigung der Rekonvergenz durch Umformung



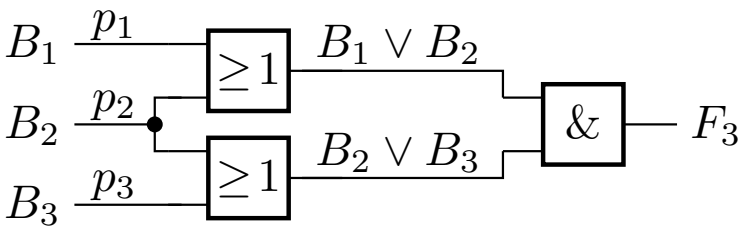
- Extraktion und Umformung/Vereinfachung des nachgebildeten logischen Ausdrucks:

$$(B_1 \vee B_2) \wedge (B_2 \vee B_3) = B_2 \vee (B_1 \wedge B_3)$$

- Funktionsgleicher rekonvergenzfreier Fehlerbaum:



Umformung über Wertetabelle



1 Ereignis eingetreten
0 Ereignis nicht eingetreten

B_1	B_2	B_3	F_3	Wahrscheinlichkeit
0	0	0	0	
0	0	1	0	
0	1	0	1	$(1-p_3)\cdot p_2\cdot(1-p_1)$
0	1	1	1	$+\quad(1-p_3)\cdot p_2\cdot p_1$
1	0	0	0	
1	0	1	1	$+\,(1-p_3)\cdot p_2\cdot(1-p_1)$
1	1	0	1	$+\quad p_3\cdot p_2\cdot(1-p_1)$
1	1	1	1	$+\quad p_3\cdot p_2\cdot p_1$

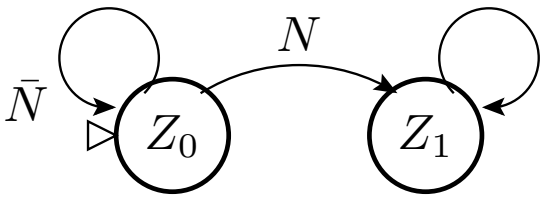
Jede logische Funktion ist durch eine Wertetabelle beschreibbar. Die Auswahlwahrscheinlichkeiten der Zeilen sind Wahrscheinlichkeitprodukte. Die gleichzeitige Auswahl mehrerer Zeilen ist ausgeschlossen, so dass die Gesamtwahrscheinlichkeit die Summe der Wahrscheinlichkeitsprodukte der »günstigen Eingabezeilen« ist.

Markov-Ketten

Markow-Ketten[13]

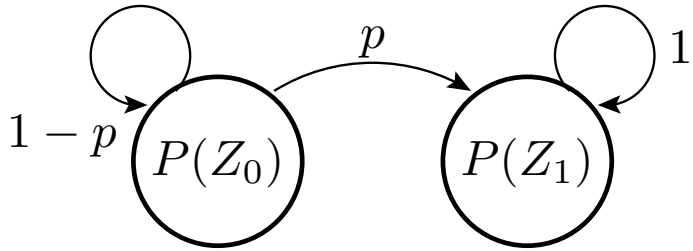
Modellierung eines stochastischen Prozesses durch einen Zustandsautomaten, dessen Kanten mit Übergangswahrscheinlichkeiten beschriftet sind. Ein einfaches Beispiel ist die Beschreibung des Nachweises eines Fehlers mit n Service-Aufrufen. Das System habe die Zustände Z_0 (Fehler nicht nachgewiesen) und F_1 (Fehler nachgewiesen).

Automat zur Beschreibung des Fehlernachweise



Z_i	Zustände
N	Nachweisereignis
$\triangleright$	Anfangszustand

Markov-Kette zum Automaten



$P(Z_i)$	Zustandswahrscheinlichkeiten
p	Nachweiswahrscheinlichkeit
	Anfangswert: $P(Z_0) = 1$

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

Eine Markov-Kette ist ein lineares System, das sich auch als Matrixgleichung beschreiben lässt. Rekursive Form:

$$\begin{pmatrix} P(Z_0) \\ P(Z_1) \end{pmatrix}_{i+1} = \begin{pmatrix} 1-p & 0 \\ p & 1 \end{pmatrix} \cdot \begin{pmatrix} P(Z_0) \\ P(Z_1) \end{pmatrix}_i$$

Die Summe der Zustandswahrscheinlichkeiten und die Summe der Übergangswahrscheinlichkeiten aus einem Zustand (in einer Spalte) muss immer eins sein. Die Zustandswahrscheinlichkeiten nach n Service-Aufrufen betragen im Beispiel:

$$\begin{pmatrix} P(Z_0) \\ P(Z_1) \end{pmatrix}_n = \begin{pmatrix} 1-p & 0 \\ p & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Die Wahrscheinlichkeit, dass ein Fehler mit n Service-Aufrufen nachgewiesen wird, ist die, dass er nicht mit keinem nachgewiesen wird:

$$p(n) = 1 - (1-p)^n$$

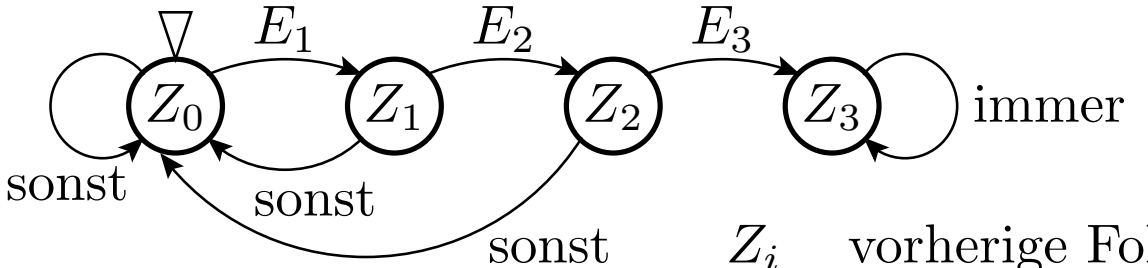
Unsere spezielle Markov-Kette geht in n-Schritten mit dieser Wahrscheinlichkeit von Zustand Z_0 (Fehler nicht nachgewiesen) nach Z_1 (Fehler nachgewiesen) und verbleibt dort:

$$\begin{pmatrix} Z_0 \\ Z_1 \end{pmatrix}_n = \begin{pmatrix} (1-p)^n & 0 \\ 1-(1-p)^n & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Auftrittswahrscheinlichkeit fehlernachweisender Testeingabefolgen

Ein Zufallsgenerator erzeugt die Testeingabewerte X_i jeweils mit einer Wahrscheinlichkeit p_i. Wie groß ist die Wahrscheinlichkeit, dass in einer Folge der Länge n in drei aufeinanderfolgenden Schritten die Teilfolge $X_1X_2X_3$ enthalten ist?

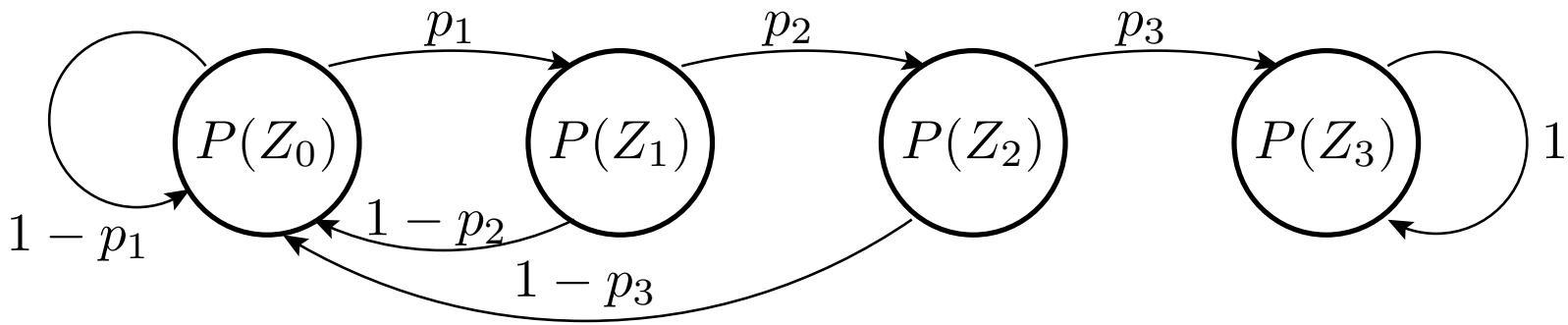
- Entwurf eines Akzeptorautomaten, der in einem Anfangszustand startet und bei Erkennen der Folge $X_1X_2X_3$ in einen Endzustand übergeht.



Z_i vorherige Folge bestand aus den ersten i richtigen Werten

E_i Wert ist X_i

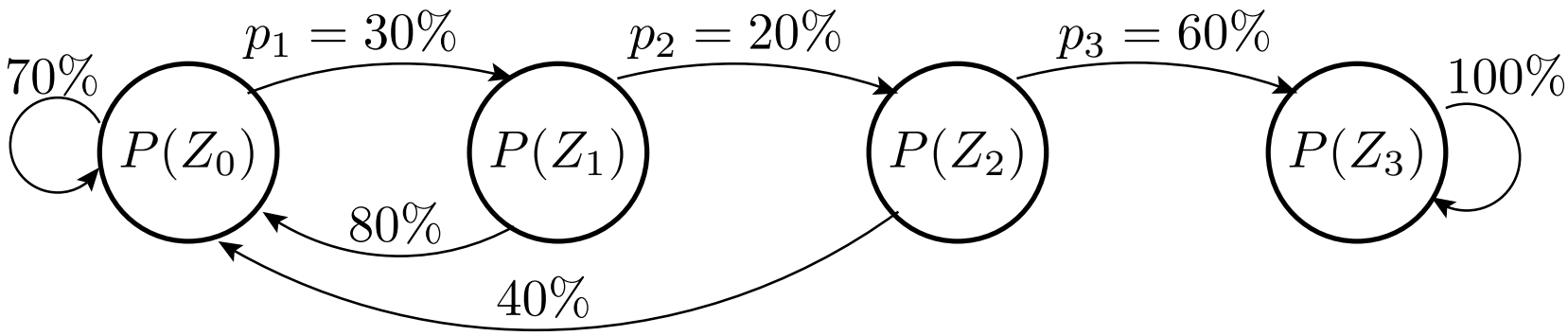
- Ersatz der Übergangsbedingungen durch die Übergangswahrscheinlichkeiten $p_i = P(E_i)$ und der Zustände durch Zustandswahrscheinlichkeiten $P(Z_i)$.



- Simulation mit den Startwert Z_0 ($P(Z_0) = 1$ und $P(Z_{i\neq 0}) = 0$) für n Schritte:

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

Mit Beispielwerten für p_1 bis p_3:



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

Verfügbarkeit Redundanter Master-Checker System

Ein Rechnersystem für höchste Sicherheitsanforderungen soll aus vier Rechnern bestehen, einem Master, der rechnet, einem Checker, der die Ergebnisse kontrolliert, und zwei Reserverechnern, die bei Ausfall die Service-Anforderungen des Masters oder des Checkers übernehmen. Das System startet mit Rechner 1 als Master und Rechner 2 als Checker und gilt solange als funktionsfähig, wie noch ein Master und ein Checker funktionieren. Die Ausfallwahrscheinlichkeit p der Rechner je Service-Abforderung sei 10%.

1. Beschreiben Sie dem Sachverhalts durch eine Markov-Kette in Matrixform.
2. Erweiterung der Fehlerreaktion um einen Reparaturprozess, in dem jeder defekte Rechner während, Master und Checker eine Service-Anfage abarbeitet, mit einer Wahrscheinlichkeit von 20% repariert wird.

Die relevanten Systemzustände sind 0, 1, 2 und mehr als 2 Rechner ausgefallen (Z_0 bis Z_3). Ohne Reparatur erhöht sich die Anzahl der ausgefallenen Rechner

- um zwei, wenn Master und Checker gleichzeitig ausfallen $p_2 = p^2 = 1\%$,
- um eins, wenn entweder der Master oder der Checker ausfällt, $p_1 = 18\%$ oder
- um keinen, wenn weder Master noch Checker ausfällt, $p_0 = (1-p)^2 = 81\%$:

$$\begin{pmatrix} P(Z_0) \\ P(Z_1) \\ P(Z_2) \\ P(Z_3) \end{pmatrix}_n = \begin{pmatrix} 81\% & 0\% & 0 & 0 \\ 18\% & 81\% & 0 & 0 \\ 1\% & 18\% & 81\% & 0 \\ 0 & 1\% & 19\% & 100\% \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Mit Reparatur können bis zu zwei fehlerhafte Rechner hinzukommen und max. alle zuvor fehlerhaften Rechner repariert werden. Das wird recht kompliziert ...(Fortsetzung als Aufgabe 3.16).

Problembeseitigung

Kontrolle und Problembeseitigung

Der Schlüssel zu objektiv verlässlichen Systemen sind Kontrollen und eine Nachbesserungsiteration zur Beseitigung der dabei erkannten Probleme auf drei Ebenen:

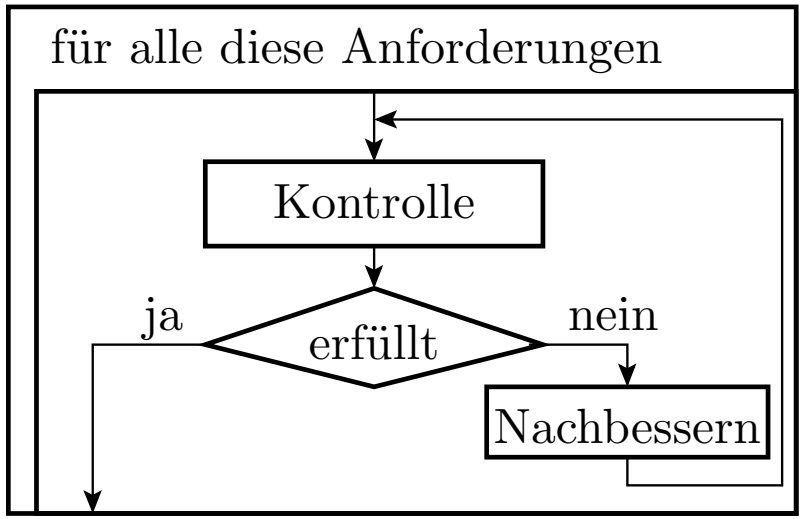
- während Entwurf und Fertigung (Fehlervermeidung),
- vor dem Einsatz und zur Wartung (Fehlerbeseitigung) und
- im laufenden Betrieb (Fehlertoleranz, Schadensvermeidung).

Zusammenstellung überprüfbarer Anforderungen:

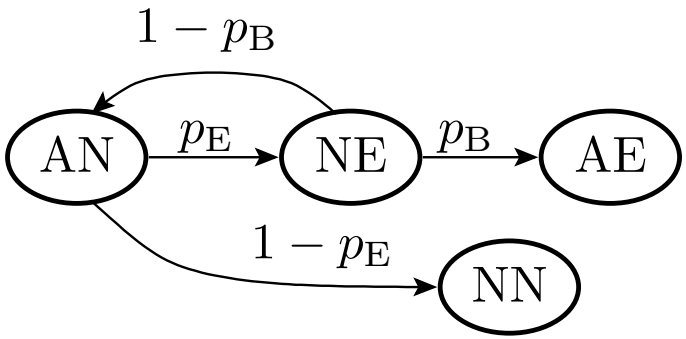
- für Entwurf und Fertigung
- für den Test
- während des Betriebs

Nachbesserung:

- Veränderung am System
- Änderung der Anforderung
- Änderung der Nutzung



Problembeseitigung als Markov-Kette



AN Anforderung nicht erfüllt.
NE Nicht erfüllte Anforderung erkannt.
NN Nicht erfüllte Anforderung nicht erkannt, Problem bleibt bestehen.
AE Anforderung erfüllt. Problem beseitigt.
p_E Erkennungswahrscheinlichkeit
p_B Beseitigungswahrscheinlichkeit

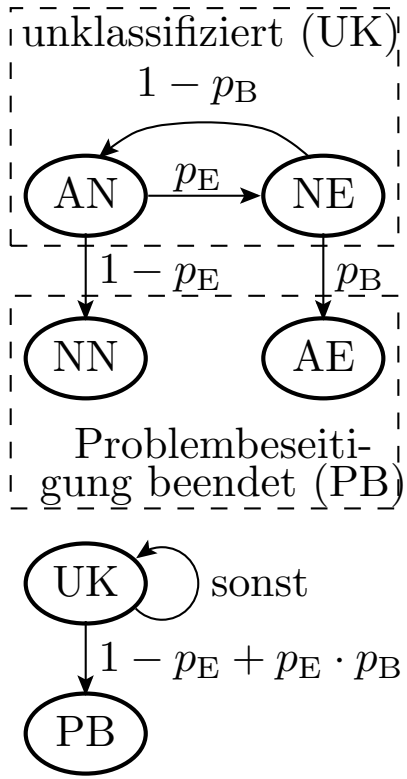
Zustand der Markov-Kette nach n Kontroll- und Beseitigungsschritten:

$$\begin{pmatrix} p_{AN} \\ p_{NE} \\ p_{NN} \\ p_{AE} \end{pmatrix} = \begin{pmatrix} 0 & 1-p_B & 0 & 0 \\ p_E & 0 & 0 & 0 \\ 1-p_E & 0 & 1 & 0 \\ 0 & p_B & 0 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Beispielsimulationen

Simulation der Wahrscheinlichkeiten p_{AE} (Problem erfolgreich beseitigt), p_{NN} (Problem nicht (mehr) erkennbar), $p_{\mathrm{AN}} + p_{\mathrm{NE}}$ (unklassifiziert) und $\frac{p_{\mathrm{AE}}}{p_{\mathrm{NN}}+p_{\mathrm{AE}}}$ (wenn klassifiziert, dann beseitigt) nach jedem Doppelschritt mit $p_{\mathrm{E}} = 99\%$ und $p_{\mathrm{B}} = 20\%$:

n	$p_{\mathrm{AN}}+p_{\mathrm{NE}}$	p_{NN}	p_{AE}	$\frac{p_{\mathrm{AE}}}{p_{\mathrm{NN}}+p_{\mathrm{AE}}}$
2	79.2	1.0	19.8	95.2
4	62.7	1.8	35.5	95.2
6	49.7	2.4	47.9	95.2
8	39.3	2.9	57.7	95.2
10	31.2	3.3	65.5	95.2
12	24.7	3.6	71.7	95.2
14	19.5	3.9	76.6	95.2
16	15.5	4.1	80.5	95.2
18	12.3	4.2	83.5	95.2



Beseitigungsaufwand und -wahrscheinlichkeit

Die Wahrscheinlichkeit, das ein erkanntes Problem nach einem Beseitigungsversuch beseitigt oder nicht mehr zu erkennen ist, beträgt:

$$p_{\mathrm{PB}}(1) = 1 - p_{\mathrm{E}} + p_{\mathrm{E}} \cdot p_{\mathrm{B}}$$

Nach m Beseitigungsversuchen beträgt sie:

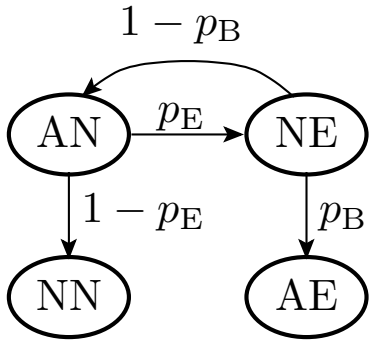
$$p_{\mathrm{PB}}(m) = 1 - (p_{\mathrm{E}} \cdot (1 - p_{\mathrm{B}}))^m$$

Die mittlere Anzahl der Beseitigungsversuche ist der Kehrwert der Beseitigungswahrscheinlichkeit je Versuch:

$$\bar{m} = \frac{1}{1 - p_{\mathrm{E}} + p_{\mathrm{E}} \cdot p_{\mathrm{B}}}$$

Bei einer Erkennungswahrscheinlichkeit nahe 100% ist die Beseitigungswahrscheinlichkeit abschätzungsweise $p_{\mathrm{B}} \approx 1/\bar{m}$, bei bei 1,25 ca. 80%. und bei 5 Versuchen ca. 20%.

Erfolgswahrscheinlichkeit



Die Wahrscheinlichkeit, dass das betrachtete Problem nach einer Beseitigungsiteration nicht mehr existiert, beträgt unabhängig von der Anzahl der Beseitigungsversuche:

$$p_{AE} \backslash p_{PB} = \frac{p_E \cdot p_B}{(1 - p_E) + p_E \cdot p_B}$$

Für die Verlässlichkeit ist eine hohe Erkennungs- und eine moderate Beseitigungswahrscheinlichkeit wichtig. Viele Beseitigungsiterationen ($p_B \ll 1$) erhöhen allerdings das Risiko, dass dabei neue Fehler entstehen.

p_B \ p_E	80%	90%	95%	99%
20%	44,4%	64,3%	79,2%	95,2%
50%	66,7%	81,8%	90,5%	98,0%
80%	76,2%	87,8%	93,8%	98,8%

Aufgaben

Aufgabe 1.8: Wahrscheinlichkeiten von Würfelexperimenten

X und Y seien die zufälligen Augenzahlen bei der Durchführung des Versuchs »Würfeln mit zwei Würfeln«. Berechnen Sie die Wahrscheinlichkeiten folgender Ereignisse:

1. $X + Y > 8$
2. $X > Y$
3. $(X = 5) \wedge (Y < 5)$
4. $X \cdot Y$ ist durch drei teilbar.

Geben Sie jeweils die Anzahl der möglichen Ereignisse an und zählen Sie die günstigen Ereignisse auf.

Aufgabe 1.9: Verkettete Würfelereignisse

- Welche möglichen Ergebnisse hat das Zufallsexperiment »auswürfeln einer Zahl, bei einer Sechs darf ein zweites Mal gewürfelt werden«?
- Mit welcher Wahrscheinlichkeit tritt jedes der möglichen Ergebnisse ein?

Aufgabe 1.10: Fehlfunktionen und Fehlernachweis

Ein System habe vier unabhängig voneinander nachweisbare Fehler mit den Nachweiswahrscheinlichkeiten je Service-Aufruf von $p_1 = 10\%$, $p_2 = 20\%$, $p_3 = 5\%$ und $p_4 = 1\%$.

1. Mit welcher Wahrscheinlichkeit versagt eine einzelne Service-Anforderung?
2. Wie hoch ist die Wahrscheinlichkeit, dass zehn aufeinanderfolgende Service-Anforderungen korrekt ausgeführt werden?
3. Wie groß ist die Wahrscheinlichkeit für jeden der vier Fehler, dass er bei einem der zehn aufeinanderfolgenden Service-Aufrufe nachgewiesen wird (mindestens ein Versagen verursacht)?

Aufgabe 1.11: Erstellen eines Fehlerbaums

Herr M. möchte um Mitternacht in seinem Büro einen Bericht lesen. Er muss dazu in sein Büro, braucht Licht und eine Brille. Ereignisse (B_i Basisereignisse ; N_i nicht untersuchte Ereignisse; F_i Fehlerereignisse):

- B_1 Tür klemmt, $p_{\mathrm{B1}} = 0,1\%$
- B_2 Deckenlampe defekt, $p_{\mathrm{B1}} = 0,2\%$
- B_3 Tischlampe defekt, $p_{\mathrm{B1}} = 0,2\%$
- B_4 Lesebrille defekt, $p_{\mathrm{B1}} = 0,3\%$
- B_5 Ersatzbrille defekt, $p_{\mathrm{B1}} = 0,5\%$
- N_1 Schlüssel vergessen, p_{N1} unbekannt
- N_2 Lesebrille vergessen, p_{N2} unbekannt
- N_3 Ersatzbrille im Schreibtisch eingeschlossen, p_{N3} unbekannt
- F_1 Büro verschlossen

- F_2 Büro unbeleuchtet
- F_3 Keine Brille
- F_4 Bericht ungelesen

1. Stellen Sie den Fehlerbaum auf.
2. Schätzen Sie die Wahrscheinlichkeiten der Fehlerereignisse F_1 bis F_4 unter der Annahme, dass die Wahrscheinlichkeiten der unberücksichtigten Ereignisse nicht größere als 1% sind.

Aufgabe 1.12: Fehlerbaumanalyse 2

1. Entwickeln Sie den Fehlerbaum für folgenden Zusammenhang:
   - Ereignis F_1 tritt ein, wenn entweder B_1 und nicht B_2 oder nicht B_1 und B_2 eintritt.
   - Das Ereignis F_2 tritt nur ein, wenn F_1 und B_3 eintreten.

2. Berechnen Sie die Wahrscheinlichkeit für F_1 und F_2 für den Fall, dass die Wahrscheinlichkeiten der Basisereignisse $p_{\mathrm{B1}} = 2\%$, $p_{\mathrm{B2}} = 10\%$ und $p_{\mathrm{B3}} = 5\%$ betragen.

Aufgabe 1.13: Übertragungsfehler

Bei der Übertragung von vier möglichen Zeichen A, B, C und D betrage die Wahrscheinlichkeit, das ein Zeichen in eines der drei anderen verfälscht wird, je $p_F = 5\%$. Die Wahrscheinlichkeit, dass es unverfälscht übertragen wird, ist $p_\mathrm{U} = 1 - 3 \cdot p_\mathrm{F} = 85\%$:

1. Stellen Sie den Zusammenhang als Markov-Kette dar.
2. Bestimmen Sie die Wahrscheinlichkeit, dass ein »A« nach der 5. Übertragung immer noch ein »A« ist.

Aufgabe 1.14: Risikoanalyse

Eine schwerwiege Fehlfunktion bei einer Maschine kann nur auftreten, wenn sie vom Normalzustand Z_0 nacheinander in höhere Riskozustände Z_1 bis Z_4 übergeht. Das Bedienpersonal erkennt erhöhte Risikozustände mit einer Wahrscheinlichkeit $p_1 = 80\%$ und initialisiert das System dann neu (Rückkehr in den Grundzustand Z_0). Die Wahrscheinlichkeit für den Übergang von einem in den nächsten Risikozustand betrage in jedem Zeitschritt, wenn nicht neuinitialisiert wird, $p_2 = 10\%$. In Risikozustand Z_4 tritt ohne rechtzeitige Neuinitialisierung mit $p_3 = 5\%$ die schwerwiegende Fehlersituation ein.

1. Beschreiben Sie den Sachverhalt mit einer Markov-Kette und einer Matrixgleichung zur Simulation mit Matlab.
2. Bestimmen Sie für 100 Schritte die Zustandswahrscheinlichkeiten $P(Z_0)$ bis $P(Z_4)$ und die Wahrscheinlichkeit, dass die schwerwiegende Fehlersituation eintritt.

Aufgabe 1.15: Ausfall, Reparatur und Verfügbarkeit

Für eine stark ausfallgefährdete Rechnerbaugruppe, die eine hohe Verfügbarkeit haben muss, hat der Hersteller drei Ersatzkomponenten dazugestellt, von denen jede bei Ausfall der aktuell genutzten Komponente die Aufgabe übernehmen kann. Bei jeder Service-Anfrage betrage die Ausfallwahrscheinlichkeit der genutzten Komponente $p_A = 10\%$ und die der Ersatzkomponenten null. Die defekten Ersatzpomponenten werden während der Dauer jeder Service-Anfrage mit einer Wahrscheinlichkeit von $p_R = 8\%$ repariert. Wenn mehrere kaputt sind, wird jede mit einer Wahrscheinlichkeit p_R repariert.

1. Beschreiben Sie den Sachverhalt mit einer Markov-Kette mit der Anzahl der defekten Komponenten als Zustandsnummer.
2. Stellen Sie die Übergangsmatrix auf.
3. Bestimmen Sie durch Simulation die Wahrscheinlichkeit, dass der Service der Rechnerbaugruppe verfügbar ist.

Aufgabe 1.16: Master-Checker-System mit Reparatur

Stellen Sie für das Beispiel auf Folie 75 die Übergangsmatrix für den Fall auf, dass nicht nur Master und Checker mit einer Wahrscheinlichkeit von 10% ausfallen, sondern dass auch jeder defekte Rechner mit 20% Wahrscheinlichkeit repariert wird.

1. Erweiterung um einen Zustand Z_4 (4 Rechner ausgefallen).
2. Bestimmen Sie für die Zustände Z_0 bis Z_4, wie viele Rechner in Summe ausfallen und repariert werden können, und die zugehörigen Übergangswahrscheinlichkeiten dafür.
3. Schreiben Sie ein Matlab-Programm zur Simulation dieser Markov-Kette.
4. Bestimmen Sie die Zustandswahrscheinlichkeiten nach 100, 200 und 1000 Service-Anforderungen. Gegen welche Wahrscheinlichkeit strebt die Wahrscheinlichkeit, dass der Service verfügbar, d.h. die Markov-Kette in einem der

Aufgabe 1.17: Fehlerbeseitigungsiteration

Es seien 1000 Anforderungen zu überprüfen. Bei 20% treten Probleme auf. Die Problembeseitigung erfordert im Mittel 3 Versuche. Wie groß muss die Erkennungswahrscheinlichkeit der Kontrolle mindestens sein, damit nach der Problembeseitigungsiteration im Mittel nicht mehr als zehn Anforderung problembehaftet sind?

Hinweis: Die gegebene mittlere Anzahl der Reparaturversuche und der indirekt gegebene Anteil der zu beseitigenden Probleme sind beides Funktionen der Beseitigungs- und Erkennungswahrscheinlichkeit. Die Erkennungswahrscheinlichkeit muss überschlagsweise fast eins sein, so dass sie in einer der beiden Gleichungen praktisch keinen Einfluss hat, so dass sich Beseitigungs- und Erkennungswahrscheinlichkeit nacheinander über jeweils eine Gleichung bestimmen lassen.

Aufgabe 1.18: Fehlerbeseitigungsiteration

Bei einer praktischen Fehlerbeseitigung, z.B. bei der Beseitigung von Programmfehlern, ist es nicht untypisch, dass neu Probleme in Form von anderen danach nicht mehr erfüllten Anforderungen entstehen. Es sei angenommen, dass jeder Beseitigungsversuch für jede der bis dahin erfüllten Anforderung mit einer Wahrscheinlichkeit von 10% ein neues Problem verursacht.

1. Wie viele Probleme entstehen unter Beibehaltung aller anderen Werte aus der Aufgabenstellung zuvor zusätzlich durch die Problembeseitigungsversuche?
2. Auf welchen Erwartungswert erhöht sich die Anzahl der Probleme, die nach der Beseitigungsiteration noch vorhanden sind, ohne von den Kontrollen erkannt zu werden?

Zählexperimente

Aspekte und Zählgrößen der Verlässlichkeit

- Verlässlichkeit beschreibt die Abwesenheit von Problemen (Fehler, Fehlfunktionen, Ausfälle, Datenverlust, ...).
- Quantitative Bewertung durch Zählen potentieller, anwesender, vermiedener, beseitigter, ... Probleme

Nach den jeweils betrachteten Problemen wird zwischen zahlreichen Teilaspekten der Verlässlichkeit unterschieden:

Verlässlichkeitsaspekt	relevante Zählgrößen
Verfügbarkeit	nicht ausgeführte / ausgeführte SL
Zuverlässigkeit	korrekt / fehlerhafte ausgeführte SL
Betriebssicherheit	SL mit / ohne sicherheitskritischer FF
Entstehungsprozesse	potentielle und entstandene Fehler
...	...

(SL – Service-Leistung; FF – Fehlfunktion).

Verfügbarkeit

Service als Zufallsexperiment

Die Verfügbarkeit ist die Wahrscheinlichkeit, dass ein Service ein Ergebnis liefert.

Service als Zufallsexperiment:

Anfragenr.	1	2	3	4	5	6	7	8	9	10 ...
Ergebnis	K	K	K	N	K	K	F	K	F	K ...

Fehlerbehandlung nach jedem Versagen

K Ergebnis korrekt
N kein Ergebnis
F Ergebnis fehlerhaft
n Anzahl der Service-Anfragen

Schätzer für die Verfügbarkeit:

$$V \approx 1 - \frac{\text{Anz}\,(\text{N})}{n} \tag{6}$$

Nach einem Versagen ist meist eine Fehlerbehandlung erforderlich (Reparatur, Neuinitialisierung, Wiederholung, ...), während der gleichfalls keine Service-Leistungen erbracht werden.

Schätzung über MTBF und MTTR

Verfügbarkeitsprobleme sind in der Regel seltene Ereignisse mit langer Dauer zur Wiederherstellung der Betriebsbereitschaft.
Alternative Abschätzung über:

MTBF mittlere Dauer zwischen dem Eintritt zweier Probleme (mean time between failure).

MTTR mittlere Dauer für die Problembseitigung (mean time to repair).

$$V \approx \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \tag{7}$$

Die Verfügbarkeit hängt erheblich von der Dauer für die Neuinitialisierung nach Abstürzen und der Reperaturzeit nach Ausfällen ab.auch vom Umgang mit Ausfällen und Abstürzen ab.

Aussagekräftige Schätzungen nach Gl. 7 verlangen eine lange Beobachtungsdauer.

Zuverlässigkeit

Zuverlässigkeit

Anfragenr.	1	2	3	4	5	6	7	8	9	10	...
Ergebnis	K	K	K	N	K	K	F	K	F	K	...

K Ergebnis korrekt
N kein Ergebnis
F Ergebnis fehlerhaft
n Anzahl der Service-Anfragen

Fehlerbehandlung nach jedem Versagen

Für die Zuverlässigkeit werden nur die erbrachten Service-Leistungen (bei denen das Systen verfügbar ist) gezählt. Schätzer:

- mittlere Anzahl korrekt abgearbeiteter Service-Leitungen zwischen zwei Fehlfunktionen:

$$Z_{\mathrm{n}} \approx \frac{\mathrm{Anz\,(K)} + \mathrm{Anz\,(F)}}{\mathrm{Anz\,(F)}}$$

- mittlere Zeit zwischen zwei Fehlfunktionen:

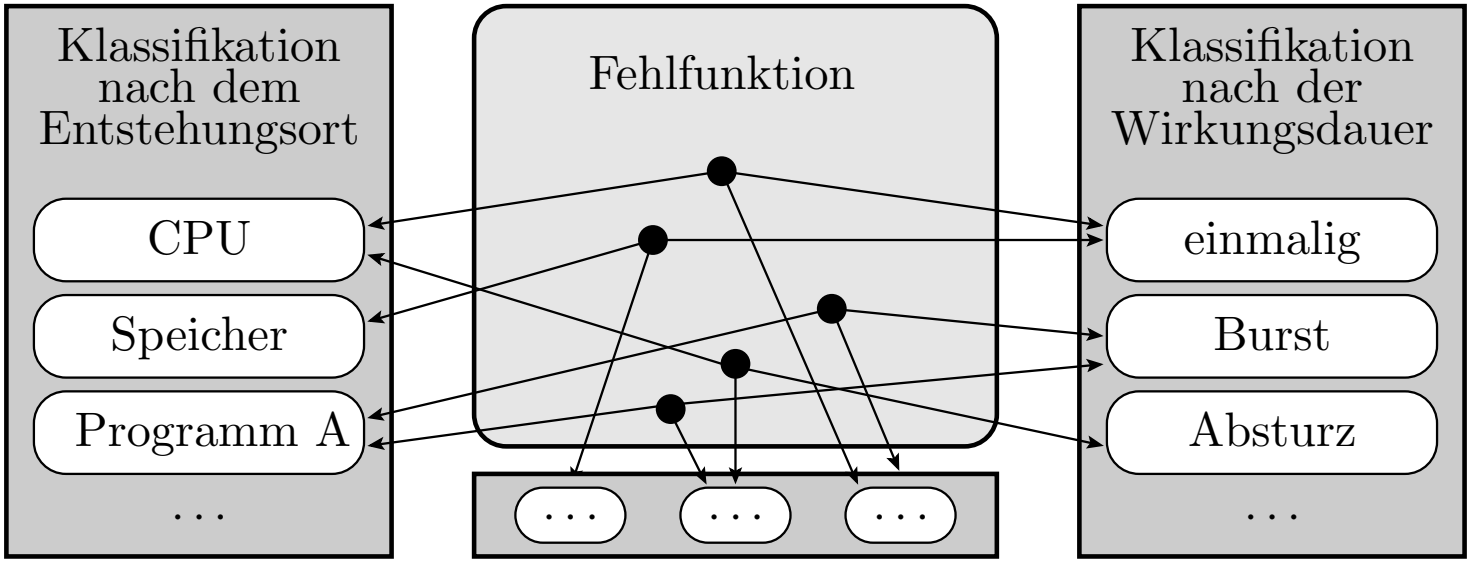
$$Z_{\mathrm{t}} \approx \frac{t_{\mathrm{B}}}{\mathrm{Anz\,(F)}}$$

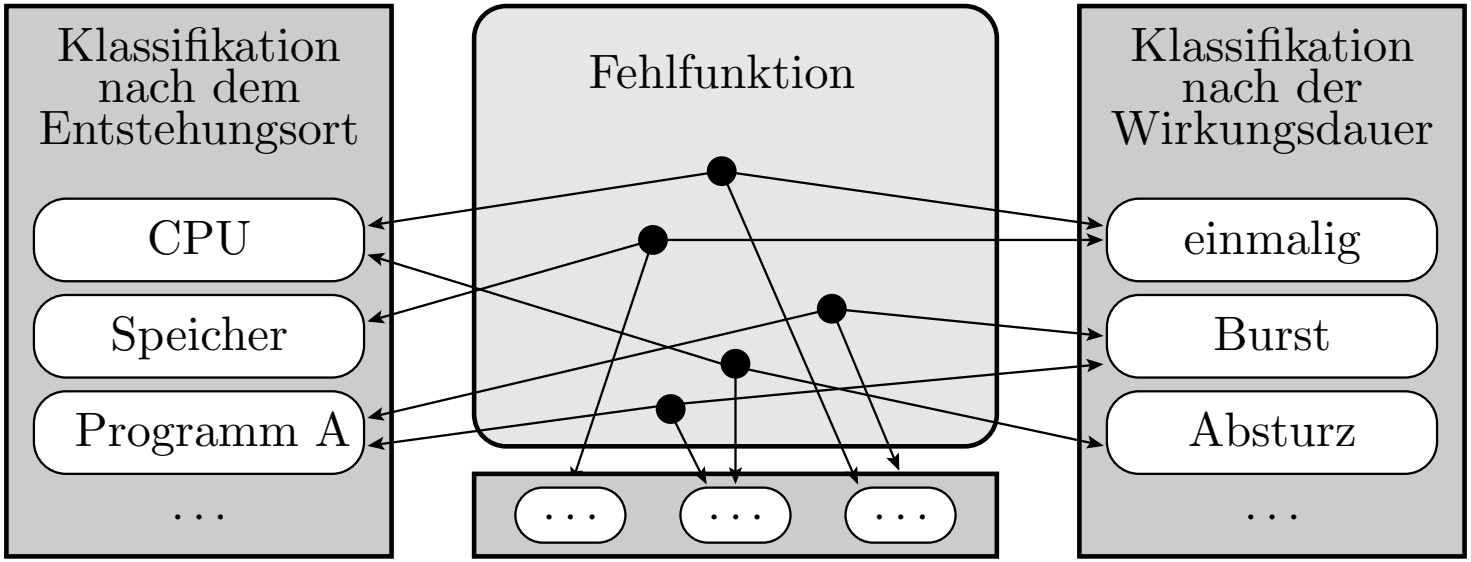
(t_{B} – Beobachtungsdauer; $\mathrm{Anz\,(F)} \gg 10$, siehe später Foliensatz F9)

Teilzuverlässigkeiten und Gesamtzuverässigkeit

Wenn nur ein Teil der Fehlfunktionen (FF) Probleme sind:

- nur FFs eines bestimmten Teilsystems,
- nur Eingabefehler, nur Störungen, ...,
- nur durch HW, nur durch SW verursachte FFs,
- nur FF, die Betriebssicherheit / die Datensicherheit / die Zugangssicherheit gefährden:





Bei einer eindeutigen Zuordnung aller Fehlfunktionen zu einer der »PKlass« Problemklassen ist die Summe aller Fehlfunktionen FF gleich der Summe der Fehlfunktionen $\mathrm{FF_{PK.i}}$ aller Klassen i:

$$\mathrm{Anz}\,(\mathrm{FF}) = \sum_{i=1}^{\mathrm{Anz(PKlass)}} \mathrm{Anz}\,(\mathrm{FF_{PK.}}i) \tag{8}$$

Bei der mittleren Anzahl korrekter Service-Leistungen bzw. Zeit zwischen zwei FFs addieren sich die Kehrwerte:

$$\frac{1}{Z_{\mathrm{N}}} = \sum_{i=1}^{\mathrm{Anz(PKlass)}} \frac{1}{Z_{\mathrm{PKN}.i}}; \quad \frac{1}{Z_{\mathrm{T}}} = \sum_{i=1}^{\mathrm{Anz(PKlass)}} \frac{1}{Z_{\mathrm{PKT}.i}}$$

Beispiel: jede Fehlfunktionen in einem System sei entweder dem Speicher, dem Prozessor oder der Software zugeordnet.
Geschätzte Zuverlässigkeitswerte der drei Teilsysteme:

- Prozesser: $Z_{\mathrm{CPU}} = 10000\,\mathrm{h}$
- Speicher: $Z_{\mathrm{Mem}} = 3000\,\mathrm{h}$
- Software: $Z_{\mathrm{SW}} = 100\,\mathrm{h}$.

Gesamtzuverlässigkeit:

$$Z_{\mathrm{T}} = \frac{1}{\frac{1}{10000\,\mathrm{h}} + \frac{1}{3000\,\mathrm{h}} + \frac{1}{100\,\mathrm{h}}} \approx 96\,\mathrm{h}$$

Das Gesamtsystem ist immer unzuverlässiger als das unzuverlässigste Teilsystem.

Sicherheit

Sicherheit

Definition 9

Eine Sicherheit ist eine Teilzuverlässigkeit in Bezug auf Fehlfunktionen mit erheblichem Schaden.

Schadenskategorien für Fehlfunktionen:

- unerheblicher Schaden,
- erheblich Nutzungsbeeinträchtigung,
- für die Betriebssicherheit kritisch[14],
- für die Datenssicherheit kritisch, ...

[14] Fehlfunktionen mit Personen- oder großem materiellen Schaden.

Betreibssicherheit, Datensicherheit

Definition 10

Die Betriebssicherheit (Safty) wird durch die mittlere Zeit oder die mittlere Anzahl der Service-Anforderungen zwischen betriebssicherheitskritischen Problemen charakterisiert.

Definition 11

Die Datensicherheit (security) wird durch die mittlere Zeit oder die mittlere Anzahl der Service-Anforderungen zwischen zwei signifikannten Datenproblemen charakterisiert. Als signifikannte Datenprobleme können wahlweise Datenverlust, Datendiebstahl oder beides[a] zählen.

[a] Klarer wäre die Definition von zwei Datensicherheiten.

Zuverlässigkeit und Sicherheit

Unter der Annahme, dass die sicherheitskritischen Fehlfunktionen etwa immer denselben Anteil an allen Fehlfunktionen haben, erhöht eine Maßnahme zur Verbesserung der Zuverlässigkeit die Sicherheiten etwa um denselben Faktor.

Die drei Ebenen zur Schaffung von Zuverlässigkeit

- Fehlervermeidung
- Fehlerbeseitigung und
- die Fehlerbehandlung im laufenden Betrieb

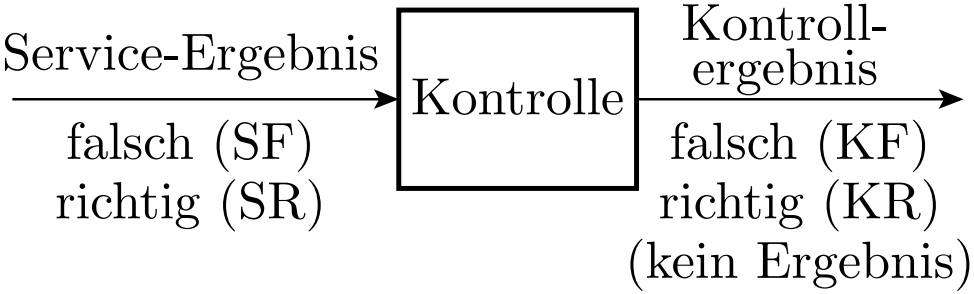
schaffen in gleichem Maße Sicherheit.

Kontrolle der Kontrolle

Kontrolle

Eine Kontrolle ist ein Service

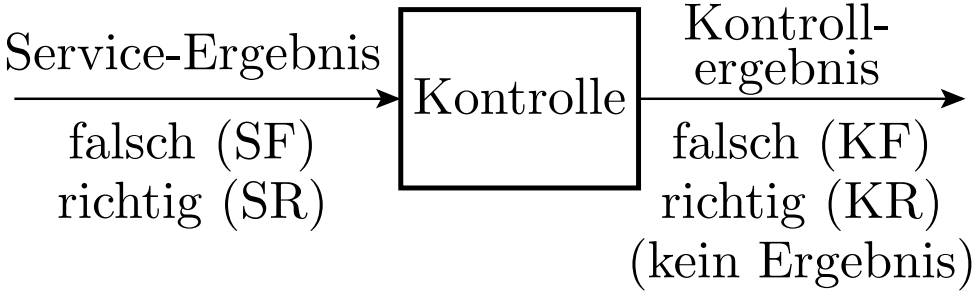
- der Probleme erkennen soll und
- eine begrenzte Zuverlässigkeit hat.



Ergebnis	Kontroll-ergebnis	Kontroll-aussage
falsch	falsch	FF
falsch	richtig	FR
richtig	falsch	RF
richtig	richtig	RR

Kontrollfehler:

- Fehlermaskierung (FR): Ohne Erkennung keine Schadensbegrenzung oder Korrektur.
- Phantomfehler (RF): Unnütze Schadensbegrenzungs- oder Korrektormaßnahmen. Können Fehlfunktionen verursachen.



Ergebnis	Kontroll-ergebnis	Kontroll-aussage
falsch	falsch	FF
falsch	richtig	FR
richtig	falsch	RF
richtig	richtig	RR

Experimentell schätzbare Größen:

- Erkennungswahrscheinlichkeit:

$$p_{\mathrm{E}} \approx \frac{\mathrm{Anz}\,(\mathrm{FF})}{\mathrm{Anz}\,(\mathrm{SF})}$$

- Maskierungswahrscheinlichkeit:

$$p_{\mathrm{M}} = 1 - p_{\mathrm{E}} \approx \frac{\mathrm{Anz}\,(\mathrm{FR})}{\mathrm{Anz}\,(\mathrm{SF})}$$

- Phantomfehlerwahrscheinlichkeit:

$$p_{\mathrm{Ph}} \approx \frac{\mathrm{Anz}\,(\mathrm{RF})}{\mathrm{Anz}\,(\mathrm{SR})}$$

Brauchbare Schätzungen verlangen viele ($\gg 10$) gezählte Ereignisse für FF, FR, RF, ... (siehe später Foliensatz F2).

Phantomfehler

Wenn nur sehr selten wirkliche Fehler oder Gefahrensituationen auftreten, sind die meisten diagnostizierten Fehler Phantomfehler.

Jeder im Institut für Mathematik bisher ausgelöste Feuerarlarm war ein Fehlalarm.

Es gab und gibt in der Informatik Tendenzen, wirkliche Fehler zu Phantomfehlern zu erklären: »It is not a bug, it is a feature.«

Kontrollen für Tests

Test

Ein Test ist eine Kontrolle auf Abwesenheit von Fehlern:

- statischer Test: direkte Kontrolle der Eigenschaften

wiederhole für eine Menge direkt überprüfbarer Merkmale
Kontrolle, dass sie erfüllt sind

- dynamischer Test: indirekte Kontrolle über Service-Aufrufe

Wiederhole für eine Menge von Testbeispielen
Service anfordern
Ergebnisse kontrollieren

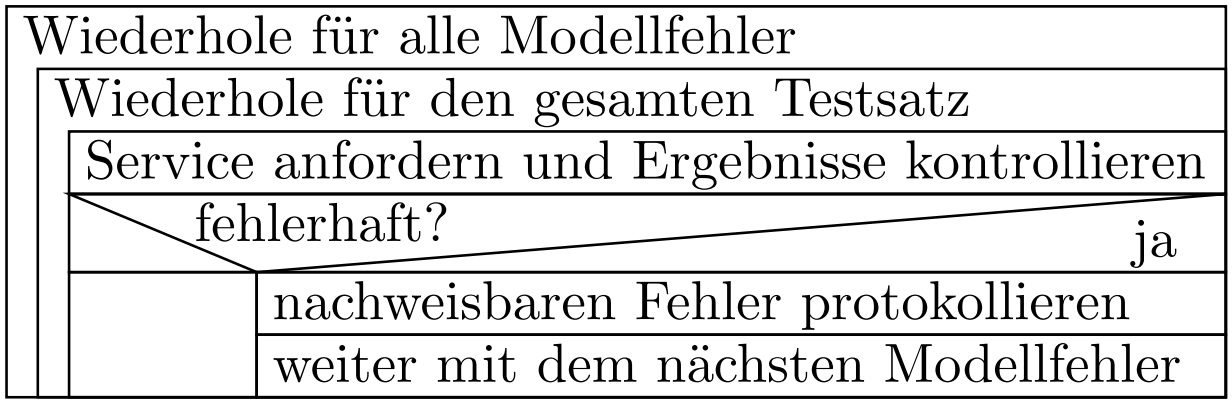
Das Mindestergebnis ist eine gut/schlecht-Aussage. Bei der Testaussage »schlecht« (nicht zu korrekten Leistungen fähig) kann ein Test weitere Zusatzinformationen liefern, z.B. eine Zuordnung zu potentiellen Fehlern.

Fehlerüberdeckung

Anteil der nachweisbaren Fehler

$$FC = \frac{\varphi_{\text{Erk}}}{\varphi}$$

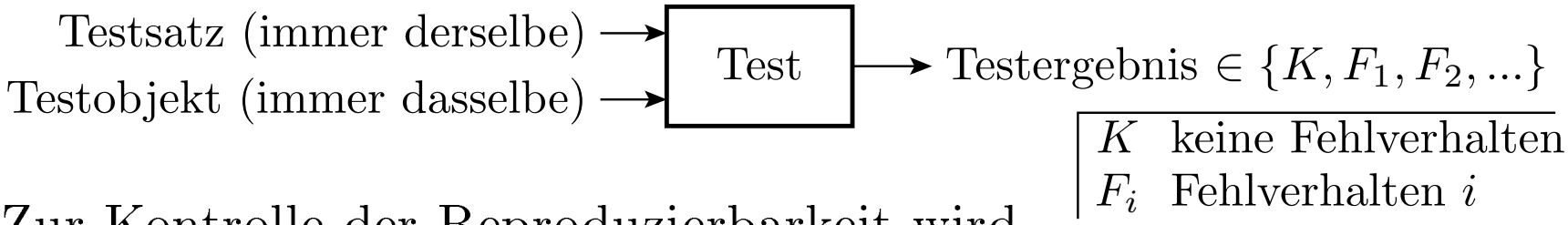
(φ_{Erk} – Anzahl der nachweisbaren, φ – Anzahl der vorhandenen Fehler). Abschätzung mit Modellfehlermengen[15]. Zählexperiment:



- Die Modellfehler im System werden simuliert oder emuliert.

[15] Von den tatsächlichen Fehler sind nur die nachweisbaren bekannt.

Reproduzierbarkeit

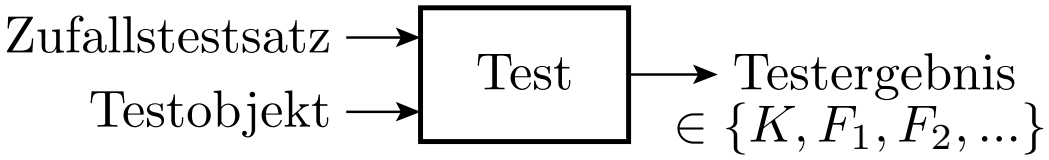


Zur Kontrolle der Reproduzierbarkeit wird derselbe Test mit demselben Testobjekt mehrfach wiederholt und als Ereignisse korrekte und falsche Service-Ergebnisse gezählt.
Mögliche Diagnosen:

- einmaliges Fehlverhalten ⇒ Störung,
- seltenes Fehlverhalten ⇒ Schwachstelle im System, die Störungen begünstigt.
- häufiges, aber unterschiedliches Fehlverhalten ⇒ unbeständiger Fehler.
- immer dasselbe Fehlverhalten ⇒ beständiger Fehler.

Zählergebnisse zur Reproduzierbarkeit helfen bei der Fehlerlokalisierung, bei der Abschätzung von Diversitäten, ...

Fehlernachweiswahrscheinlichkeiten



K	keine Fehlverhalten
F_i	Fehlverhalten i

Bei einer zufälligen Bedatung der Testeingaben oder beim Test im laufenden Betrieb ist der Nachweis eines Fehlers Zufall.
Experimente:

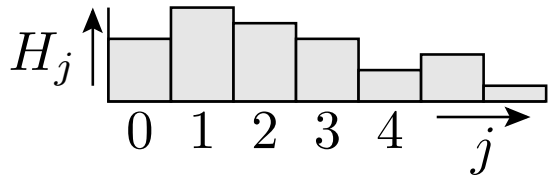
- Zählen der Fehlerfunktion für jeden (Modell-) Fehler i .
- »Abhaken der nachweisbaren Fehler«.

Schätzer für Fehlernachweiswahrscheinlichkeiten:

$$p_i \approx \frac{\mathrm{Anz}\left(\mathrm{FF}_{\mathrm{F}.i}\right)}{n};\ p_i \approx \frac{1}{n_{\mathrm{F}.i}}$$

($\mathrm{Anz}(\mathrm{FF}_{\mathrm{F}.i})$ – Anzahl der FF verursacht von Fehler i; n – Anzahl aller Test; $n_{\mathrm{F}.i}$ – Anzahl der Tests bis zum ersten Nachweis von Fehler i.

Fehlernachweishäufigkeit



Die Fehlernachweishäufigkeit beschreibt die Auftrittshäufigkeit von Fehlern in Abhängigkeit von deren Nachweiswahrscheinlichkeit. Typische Beobachtung, für mit einer Potenzfunktion abgestufte Wahrscheinlichkeitsintervalle

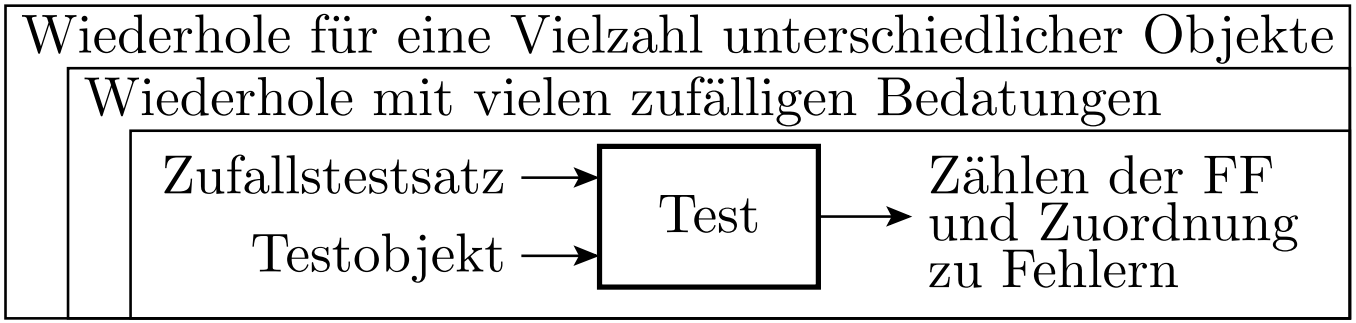
$$I_j = \left[v^{-j}, v^{-(j+1)}\right)$$

($j \in \{0, 1, 2, \ldots\}$ – Intervallnummer; v – Parameter für die Intervallgröße, z.B. 2 für $\left[1, \frac{1}{2}\right)$, $\left[\frac{1}{2}, \frac{1}{4}\right)$, ...) nimmt die Häufigkeit

$$H_j = \frac{\text{Anz}\left(F_i|_{p_i \in I_j}\right)}{\text{Anz}\left(F_i\right)}$$

der den Intervallen zuzurechnenden Fehler mit der Intervallnummer, d.h. abnehmender Nachweiswahrscheinlichkeit ab[16].

[16] vergl. Pareto-Verteilung, bei der die überwiegende Mehrheit der Probleme durch einen kleinen Anteil von Fehlern verursacht wird.



Das Experiment zur Abschätzung der Fehlernachweishäufigkeit besteht aus den Experimenten zum Schätzen der Nachweiswahrscheinlichkeit vorhandener Fehler für eine Vielzahl unterschiedlicher Objekte einer betrachteten Klasse von Systemen. Jedes Einzelexperiment schätzt die Nachweiswahrscheinlichkeiten der Fehler im getesteten Objekt und liefert eine Menge von Wahrscheinlichkeitswerten. Jeder Wahrscheinlichkeitswert wird seinem Wahrscheinlichkeitsbereich j zugeordnet, in dem für diesen der Häufigkeitswert um eins erhöht wird. Abschließende Division aller Häufigkeitswerte durch die Anzahl der untersuchten Objekte.

Die Fehlernachweishäufigkeit dient später zur Abschätzung der Anzahl der nicht gefundenen Fehler in Systemen und der Häufigkeit, mit der diese Fehler im Einsatz Service-Leistung versagen lassen.

Das skizzierte Experiment ist extrem aufwändig und vermutlich noch nie mit einer aussagekräftigen Versuchsanzahl durchgeführt wurden. Im nächsten Foliensatz werden Abschätzungen von Nachweiswahrscheinlichkeiten aus der Systemstruktur diskutiert, die zeigen, dass

- die meisten Fehler gut nachweisbar sind,
- es aber in der Regel auch Systembestandteile mit schlecht nachweisbaren Fehlern gibt und
- Fehler, die fast nie oder erst nach einer sehr langen Betriebsdauer erstmalig eine Fehlsfunktion verursachen, nicht ausschließbar sind.

Fehleranteil und Entst.-Proz.

Fehleranteil

Der Fehleranteil DL (Defekt Level) ist der Anteil der defekten Systeme in einer Menge gleichartiger Systeme und ein Schätzer für die Wahrscheinlichkeit, dass ein System defekt ist:

$$DL = \frac{\text{Anz(DS)}}{\text{Anz(Sys)}}$$

(Anz(DS) – Anzahl der defekten Systeme; Anz(Sys) – Anzahl aller Systeme). Richtwerte für ungtestete Systeme:

Typ	DL
NLOC	0,01...0,03 dpu
Schaltkreise	200 dpm
diskrete Bauteile	10 dpm
Lötstellen	1 dpm

(dpu – Defects per Unit; dpm – Defects per Million; NLOC – Netto Lines of Code, Codezeilen ohne Kommentar- und Leerzeilen).

Bestimmung des Fehleranteils durch Zählen

Für einen geringen Fehleranteil enthalten die meisten defekten System nur einen Fehler. Die Fehlerüberdeckung ist etwa:

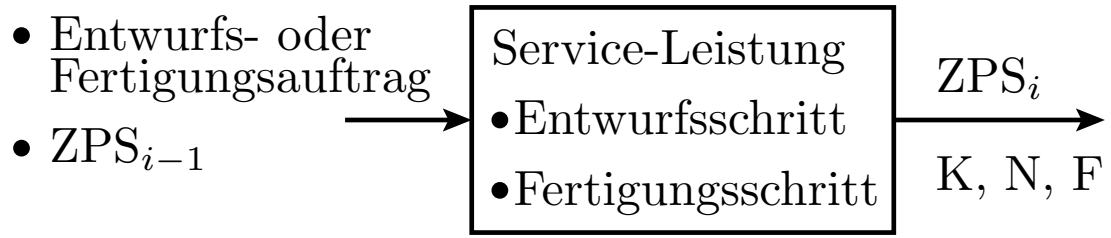
$$FC = \frac{\varphi_{\text{Erk}}}{\varphi} \approx \underbrace{\frac{\text{Anz(DS)}}{\text{Anz(DS)} + \text{Anz(DS}^*\text{)}}}_{\text{ca. Anzahl vorhandene Fehler}}$$

(Anz(DS) – Anzahl der erkannten defekten Systeme (etwa gleich der Anzahl der nachweisbaren Fehler), Anz(DS*) – Anzahl der nicht erkennbaren defekten Systemen). Fehleranteil unter Berücksichtigung der nicht erkannten defekten Systeme:

$$DL = \frac{\text{Anz(DS)} + \text{Anz(DS}^*\text{)}}{\text{Anz(Sys)}} = \frac{\text{Anz(DS)}}{FC \cdot \text{Anz(Sys)}} > \underbrace{\frac{\text{Anz(DS)}}{FC \cdot \text{Anz(Sys)}}}_{\text{scheinbarer Fehleranteil}}$$

Um den Kehrwert der Fehlerüberdeckung größer als der scheinbare Fehleranteil.

Entstehungschritte als Service



ZP	Zwischenprodukt	N	kein Ergebnis (oder erkennbar defekt)
K	korrekt	F	nicht erkennbar defekt

Jeder Fertigungs- oder Entwurfsschritt kann das Zwischenprodukt

- korrekt belassen,
- einen erkennbaren Defekt oder
- einen nicht erkannbaren Defekt

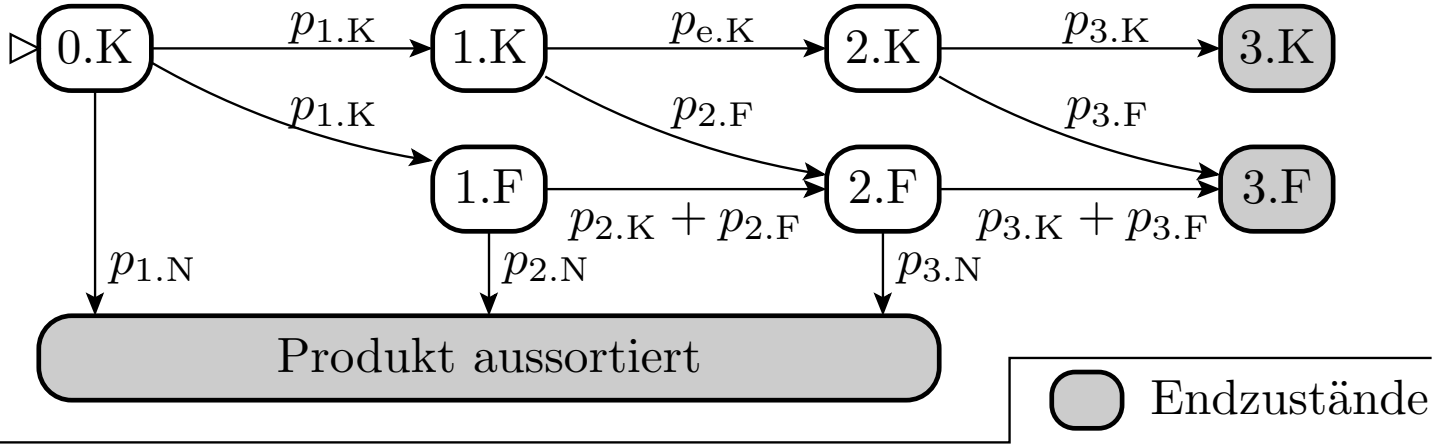
einbauen. Als defekt erkannte Objekte werden aussortiert oder repariert. Reparaturen sind als Rückgriffe (Wiederholungen von Enstehungsschritten) modellierbar.

Entstehungsprozess als Markov-Kette

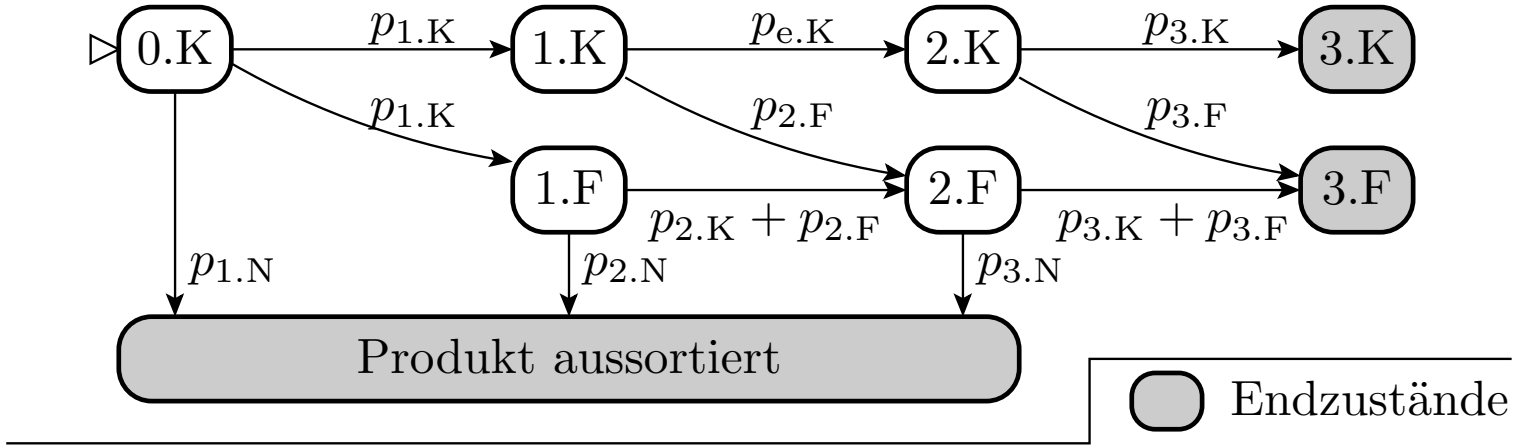
Beschreibung der Wahrscheinlichkeit in einem 2D-Zustandraum:

- Dimension 1: abgeschlossener Entstehungsschritt
- Dimension 2: K (korrekt), F (nicht erkennbarer Defekt), N (erkennbarer Defekt).

Bspiel: 3 Entstehungsschritte, Aussortieren erkennbarer Defekte



$p_{i.K}$ Wahrscheinlichkeit, dass in Schritt i kein Fehler entsteht
$p_{i.F}$ Wahrsch., dass in Schritt i ein nicht erkannter Fehler entsteht
$p_{i.N}$ Wahrscheinlich., dass in Schritt i ein erkannter Fehler entsteht



$p_{i.K}$ Wahrscheinlichkeit, dass in Schritt i kein Fehler entsteht
$p_{i.F}$ Wahrsch., dass in Schritt i ein nicht erkannter Fehler entsteht
$p_{i.N}$ Wahrscheinlich., dass in Schritt i ein erkannter Fehler entsteht

Bestimmung der Wahrscheinlichkeiten, dass ein korrektes, defektes oder kein Produkt entsteht durch Simulation:

- Startwert P(0K)=100% und für die anderen Zustände null.
- (mindestens) 3 Simulationschritte.

Für sehr klein $p_{i.N}$ ist die Wahrsscheinlichkeit, dass ein korrektes Produkt entsteht gleich dem Fehleranteil:

$$DL_3 \approx P\,(3.\mathrm{K}) = \prod_{i=1}^{3} p_{i.\mathrm{K}}$$

System aus Teilsystemen

Das bisherige Modell gilt für den sequentiellen Durchlauf von Entstehungsschritten eines Einzelobjekts ohne Hirarchie.

Beim Zusammenfügen einen Systems aus Teilsystemen erbt das Gesamtsystem die Fehler aller Teilsysteme. Fehleranteil eines zusammengesetztes Systems:

$$DL_{\text{Zus}} > p_{\text{K}} \cdot \left(1 - \prod_{i=1}^{\text{Anz(Komp)}} (1 - DL_{\text{Komp}.i}) \right)$$

(p_{K} – Wahrscheinlichkeit fehlerfreier Zusammenbau; $DL_{\text{Komp}.i}$ – Fehleranteil Komponente i; Anz(Komp) – Anzahl der Komponenten.

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

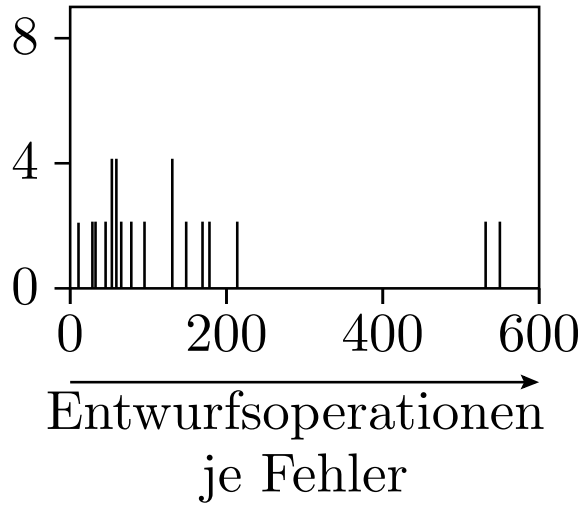
Welcher Fehleranteil ist für die Baugruppe zu erwarten, wenn die bei der Baugruppenfertigung zusätzlich entstehenden Fehler zahlenmäßig vernachlässigbar sind oder alle beseitigt werden:

$$\begin{aligned} DL_{\mathrm{Sys}} &= 1 - \left(1 - 10^{-5}\right) \cdot \left(1 - 2 \cdot 10^{-4}\right)^{20} \cdot \left(1 - 10^{-5}\right)^{35} \cdot \left(1 - 10^{-6}\right)^{560} \\ &\approx 10^{-5} + 20 \cdot 2 \cdot 10^{-4} + 35 \cdot 10^{-5} + 560 \cdot 10^{-6} \\ &\approx 5000\,\mathrm{dpm} = 0{,}005\,\mathrm{dpu} \end{aligned}$$

Experiment aus [1]

Eine Gruppe von 72 Studenten hatte die Aufgabe, aus der Beschreibung eines PLAs[17] eine Gatterschaltung zu entwickeln und diese über die grafische Benutzeroberfläche eines CAD-Systems in den Rechner einzugeben. Für jeden Entwurf wurden u.a. die elementaren Entwurfsoperationen[18] und die Entwurfsfehler gezählt.

Die Fehlerentstehungswahrscheinlichkeit je Entwurfsoperation ist der Kehrwert der in der Abb. dargestellten »Entwurfsoperationen je Fehler und lag im Experiment bei 0,005 bis 0,1 Entwurfsfehler pro Entwurfsschritt.



[17] PLA: programmable logic array

[18] Als elementare Entwurfsoperationen galten das Anordnen eines Gatters auf dem Bildschirm und das Zeichnen einer Verbindung.

Reifeprozesse

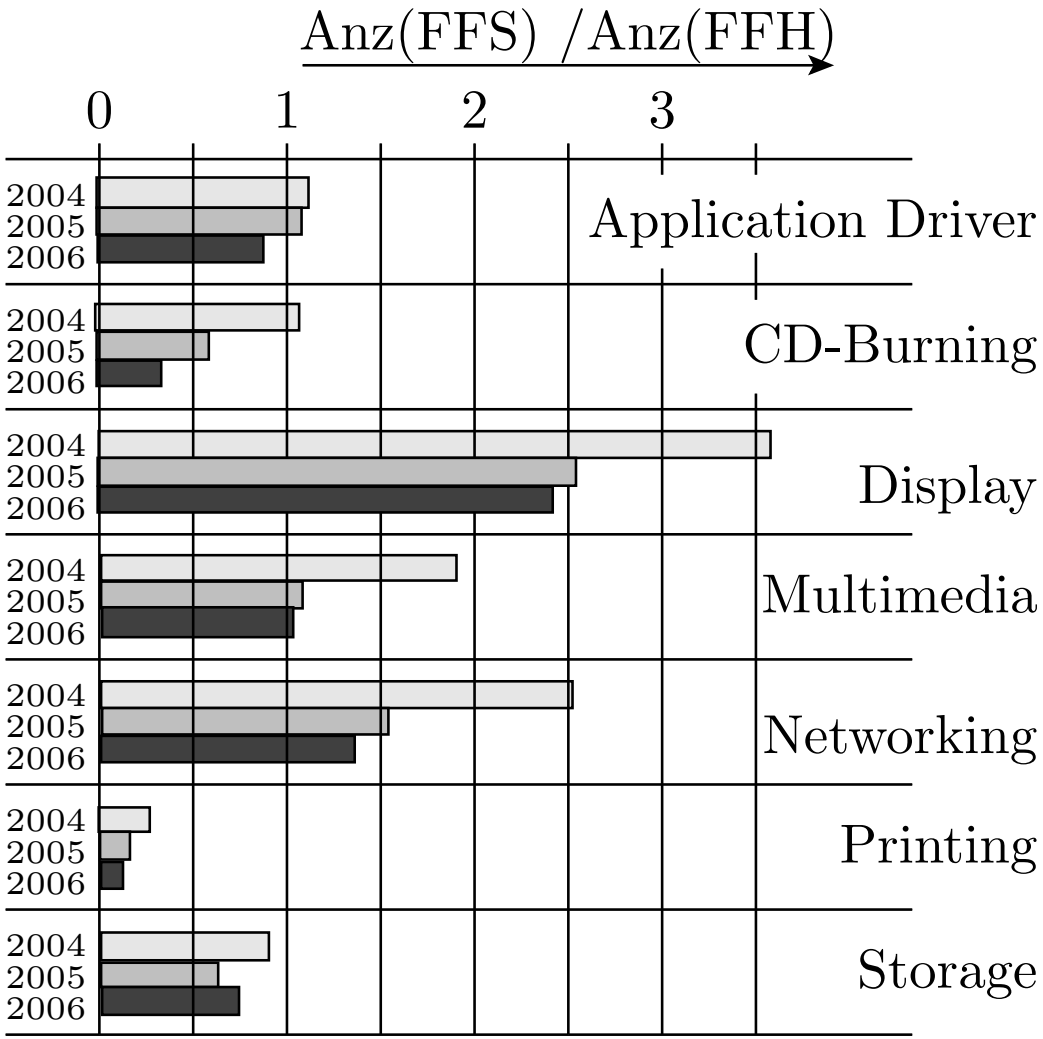
Reifeprozesse

Große Systeme enthalten auch im Einsatz noch ein große Anzahl von Fehlern. Bei Software und rekonfigurierbarer Hardware reift in der Einsatzphase:

- Für jede Service-Anforderung
  - Ergebniskontrolle
  - Bei beobachtbarer Fehlfunktion
    - »Change Request« durch den Anwender
    - Fehlersuche und Beseitigung durch den Hersteller
    - Herausgabe fehlerärmerer Versionen

Reifeprozesse sind an der Abnahme der Häufigkeit von Fehlfunktionen beobachtbar.

Abnahme der durch Software-Fehler verursachten Treiberabstürze (FFS) im Verhältnis zu denen durch Hardware verursachten (FFH) für Windows [2, Fig.15].



Aufgaben

Aufgabe 1.19: Service-Versagen und Kontrolle 1

In einem System, in dem auf die Ereignisse »keine Service-Leistung« oder »kein Kontrollergebnis« solange mit einer wiederholten Service- oder Kontrollanforderung reagiert wird, seien die Wahrscheinlichkeiten für Kontrollergebnis »richtig«: $p_{\mathrm{KR}} = 95\%$ und die beiden korrekten Klassifikationen $p_{\mathrm{FF}} = 90\%$ und $p_{\mathrm{RR}} = 97\%$ bekannt. Wie groß sind die Wahrscheinlichkeiten

1. p_{SF} dass ein Service-Ergebnis korrekt ist,
2. p_{RF} dass richtige Service-Ergebnis als falsch klassifiziert und
3. p_{FR} dass falsche Service-Ergebnis als richtig klassifiziert werden?

Aufgabe 1.20: Service-Versagen und Kontrolle 2

Ein Service und seine Kontrolle seien mit 100%-iger Wahrscheinlichkeit verfügbar. Wie groß ist die Wahrscheinlichkeit, dass der Service fehlerhaft ausgeführt wird, wenn 99% der Kontrollen keinen Fehler erkennen und die Kontrollerkennungswahrscheinlichkeit 80% beträgt und keine Phantomfehler auftreten?

Aufgabe 1.21: Schätzen des Fehleranteils

In einem Experiment zur Abschätzung des Fehleranteils wurden 31 Objekte als fehlerhaft und 712.981 Objekte als fehlerfrei klassifiziert. Für den Testsatz sei anzunehmen, dass er mindesten 80% der Fehler nachweisen kann. Schätzen Sie ab, in welchem Bereich der Fehleranteil liegt.

Aufgabe 1.22: Fehleranteil eines Rechners

Ein Rechner besteht aus Leiterplatten, Schaltkreisen, diskreten Bauteilen (Widerstände, Kondensatoren, ...) und Lötstellen. Die nachfolgende Tabelle zeigt für einen Beispielrechner für alle eingesetzten Bauteiltypen deren Anzahl und deren zu erwartenden Fehleranteil DL_{BT}.

Typ	Anzahl	$E\left(DL_{\mathrm{BT}}\right)$
Leiterplatten	10	10 dpm
Schaltkreise	100	200 dpm
diskrete Bauteile	200	10 dpm
Lötstellen	10000	1 dpm

Was für einen Fehleranteil hat ein solcher Rechner, wenn alle anderen Arten von Fehlern anzahlmäßig vernachlässigt werden können?

Aufgabe 1.23: Fehlerentstehung 1

- Wie viele Fehler sind in einem großen Software-System mit 10^5 Programmzeilen zu erwarten, wenn beim Entwurf 3% der Programmzeilen falsch sind und der Test 60% der Fehler erkennt?

Aufgabe 1.24: Fehlerentstehung 2

- Durch eine Störung in einem Fertigungsprozess verdoppelt sich die Anzahl der fehlerhaft gefertigten Bauteile. Wie wirkt sich das auf die Häufigkeit der Fehlfunktionen eines Systems aus, bei dem dieser Bauteiltyp bisher 10% der Fehlfunktionen verursacht hat?

Aufgabe 1.25: Chipgröße, Fehleranteil und Herstellungskosten

Der Fehleranteil der Transistoren eines Fertigungsprozesses für integrierte Schaltkreise sei bekannt und betrage:

$$DL_{\mathrm{Tr}} \approx 10^{-6}$$

Andere Fehlerarten seien zu vernachlässigen. Wie hoch ist der Fehleranteil für Chips mit

1. 10^5
2. 10^6 und
3. 10^7 Transistoren.

Schätzen Sie die Herstellungskosten der Halbleiter-Chips ab unter der Annahme, dass ein Chip mit 10^6 Transistoren 1\$ beträgt, die Kosten sich proportional zur Chipfläche verhalten und die Kosten für die auszusortierenden defekten Schaltkreise zu denen der fehlerfrei gefertigten hinzugefügt werden müssen.

Literatur

4. Literatur

[1] J. E. Aas and I. Sundsbo.
Harnessing the human factor for design quality.
IEEE Circuits and Devices Magazine, 11(3):24–28, 1995.

[2] K. Glerum.
Debugging in the (Very) Large: Ten Years of Implementation and Experince.
In SOSP, pages 11–14, 2009.

[3] J. Hartmann.
Analyse und Verbesserung der probabilistischen Testbarkeit kombinatorischer Schaltungen.
PhD thesis, Diss. Unversität des Saarlandes, 1992.