Test und Verlässlichkeit Foliensatz 1: Kenngrößen und Maßnahmen zur Sicherung der Verlässlichkeit

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_F1)

May 2, 2017

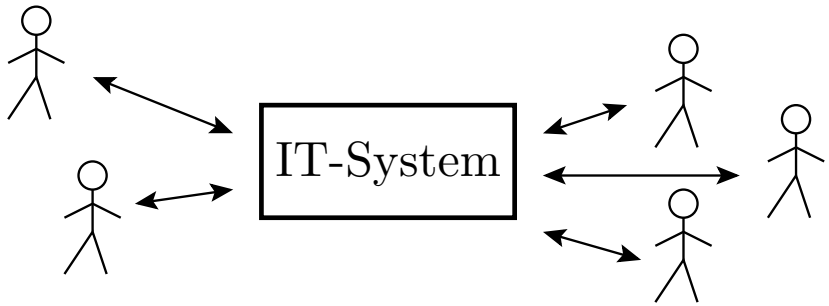
Inhalt Foliensatz TV_F1

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, ...).

Verlässlichkeit von IT-Systemen wird nach[1] beschrieben durch:

- Threats (Gefährdungen): Fehler, Fehlfunktionen (FF), Störungen, Ausfälle, ...
- Attributes (Teilaspekte / Kenngrößen): Verfügbarkeit, Zuverlässigkeit, Betriebs-, Daten-, Zugangssicherheit, Wartbarkeit, ...
- Means (Maßnahmen zur Sicherung der Verlässlichkeit): Fehlervermeidung, Workarounds, Test, Fehlerbeseitigung, Überwachungsfunktionen, Fehlertoleranz, Wartung, ...

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

Threats (Gefährdungen):

- Fehlfunktionen (FF) verursachen Schaden.
- Ursache von FF: Fehler und Störungen im System.
- Fehler entstehen im Entstehungsprozess des Systems.

Attributes (Teilaspekte / Kenngrößen):

- Verfügbarkeit: Wie sicher ist es, dass ein IT-Service bei Bedarf verfügbar ist?
- Zuverlässigkeit: Welcher Anteil der Service-Leistungen (SL) ist brauchbar/unbrauchbar?
- Sicherheit: Wie oft verursachen die FFs Schaden?

Means (Maßnahmen zur Sicherung der Verlässlichkeit):

- Fehlervermeidung: Minderung der Häufigkeit der Fehlerentstehung. Verbesserung der Technologie des Entstehungsprozesses.
- Workarounds: Erlernen von Benutzungsabläufen, bei der das System funktioniert.
- Fehlerbeseitigung: Iteration aus Test, Fehlerlokalisierung, ...

Der Preis für Verlässlichkeit

- Auf Fehlervermeidung, prüfgerechten Entwurf, Test und Fehlerbeseitigung entfallen typisch $> 80\%$ der Produktkosten.
- In sicherheitskritischen Anwendungen z.B. in Fahrzeugsteuergeräten dienen die meisten Funktionen zur Überwachung und Reaktion auf Fehlfunktionen.

Mitwirkung aus allen Unternehmensbereichen:

- Management: Organisatorischer Rahmen für fehlerarme Entstehungsprozesse, ausreichendes Testen, ...
- Fertigung: Fehlervermeidung in den Fertigungsabläufen, Test, ...
- Entwurf: Prüfgerechter Entwurf, einprogrammieren von Überwachungsfunktionen, Entwurf von Testbeispielen, ...
- Qualitätskontrolle: Prozesskontrolle, Produktkontrolle, ...
- Vertrieb: Rückmeldung über Verbesserungsmöglichkeiten und Fehler, ...

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

Threats (Gefährdungen):

- Modelle und Verfahren für die Abschätzung der Anzahl und Auftrittshäufigkeiten von Fehler und Fehlfunktionen.
- Klassifizierung nach Schaden, Möglichkeit der Erkennung, Vermeidung, ...

Attributes (Teilaspekte / Kenngrößen):

- Definition von Kenngrößen.
- Typische Werte, Schätzverfahren, ...

Means (Maßnahmen zur Sicherung der Verlässlichkeit):

- Möglichkeiten für die Überwachung auf und den Umgang mit Fehlfunktionen.
- Fehlerbeseitigung: Testauswahl, Testdurchführung, Prüftechnologien, ...
- Möglichkeiten der Fehlervermeidung.

Themenspezifische Einführung in die Stochastik: Wahrscheinlichkeit, Fehlerbäume, Markov-Ketten, Verteilungen insbesondere für Zählwerte. Schätzen von wahrscheinlichen Bereichen, Erwartungswerten und Eintrittswahrscheinlichkeiten.

Schwerpunkt liegt auf den Kontrollen zur Erkennung der Probleme, hier wiederum auf dynamischen Tests (Ausprobieren der Funktion mit Beispieleingaben) und dabei wiederum auf dem Zufallstest.

Foliensätze

- F1: Modelle, Wahrscheinlichkeit, Kenngrößen und Maßnahmen zur Sicherung der Verlässlichkeit.
- F2: Zufallstest, Verteilungen, Schätzen von Kenngrößen.
- F3: Überwachung: Fehlererkennende und -korrigierende Codes, Format- und Wertekontrollen, Diversität, Probe.
- F4: Statische Tests: direkte Kontrollen auf Fehlerabwesenheit.
- F5: Dynamische Tests: Ausprobieren der Funktion mit einer Stichprobe von Eingaben.
- F6: Problembeseitigungsprozesse: Fehlervermeidung, Fehlerbeseitigung, Wartung und Tolerierung von Fehlfunktionen.

Modelle

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 1

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

In dieser Vorlesung sind wesentlich:

- zähl- oder abschätzbare Anzahl von Problemen und korrekten Leistungen, messbare Bezugszeiten,
- Problemeinteilung (Erkenn-, Vermeidbarkeit, Schaden, ...)

Unwesentlich sind meist Funktion und Realisierung der Systeme.

Service-Modell

Das Service-Modell

Modell zur Diskretisierung (zählbar Gestaltung) von angeforderten, erbrachten, korrekten, fehlerhaften, ... Leistungen:

Definition 2

Eine Service ist ein Vorgang, der mit einer Service-Anforderung gestartet wird und aus Eingaben Ergebnisse erzeugt.

- Die Ein- und Ausgaben sind (Informations-) Container mit Format und Bedatung.
- Im Sinne der Vorlesung wesentliche Aspekte eines IT-Systems: zählbare Anforderungen, erbrachte, zulässige, korrekte Leistungen, Antwortzeit, Möglichkeiten der Kontrolle, Fehlervermeidung, -beseitigung, ...
- Vernachlässigbar: Funktion, Realisierung.

Anwendungsbereiche des Service-Modells

Das Service-Modell eignet sich für alle informations- und objekt-verarbeitenden Systeme mit gerichtetem Verarbeitungsfluss:

- Digitalschaltungen: Gatter, Rechnerbausteine, Rechner, ...
- Programme: Einzelanweisung, Module, Server-Dienste, ...
- Systeme aus Hard- und Software: programmierte Rechner, ...
- CPS[3]: Smartphones, Motorsteuergeräte, ...
- Entstehungsprozesse: Entwurf, Fertigung, Reparatur, ...

[3] CPS (Cyber-Physical Systems) sind informationsverarbeitende Systeme mit Fähigkeiten zur Interaktion in der physikalischen Welt (Radhakisan Baheti and Helen Gill: Cyber - physical Systems. http://ieeecss.org/sites/ieeecss.org/files/documents/IoCT-Part3-02 CyberphysicalSystems.pdf)

Programmmodul als Service

C-Funktion:

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

- Ein- und Ausgabe sind Daten. Format siehe Funktionsdekl.
- Service-Anforderung durch Funktionsaufruf.
- Sollfunktion: Rückgabe »23*(a+b)« nach kurzer Zeit.

Beispielprogramm fehlerhaft. Bei welchen Eingaben gibt es eine Fehlfunktion? Was für bzw. wie viele Fehler hat das Programm?

Zählbarkeit der FF und Fehler am Beispiel

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

Service-Anforderungen (SA), -Leistungen (SL), FF, ... zählbar. √

Beschreibung und Zählbarkeit der Fehler:

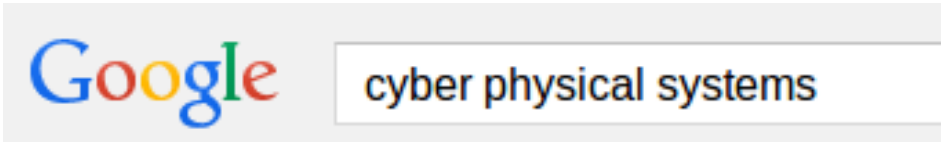
- falsches Ergebnis bei 23*(a+b) größer max. und kleiner min. mit »int16_t« darstellbarer Wert.
- falscher Ergebnistyp,
- fehlende WB-Kontrolle der Eingabe, ...

Ein Denkfehler, mehrere falsche Zeichen, eine oder mehrere fehlende / falsche / überflüssige Anweisungen, ...?

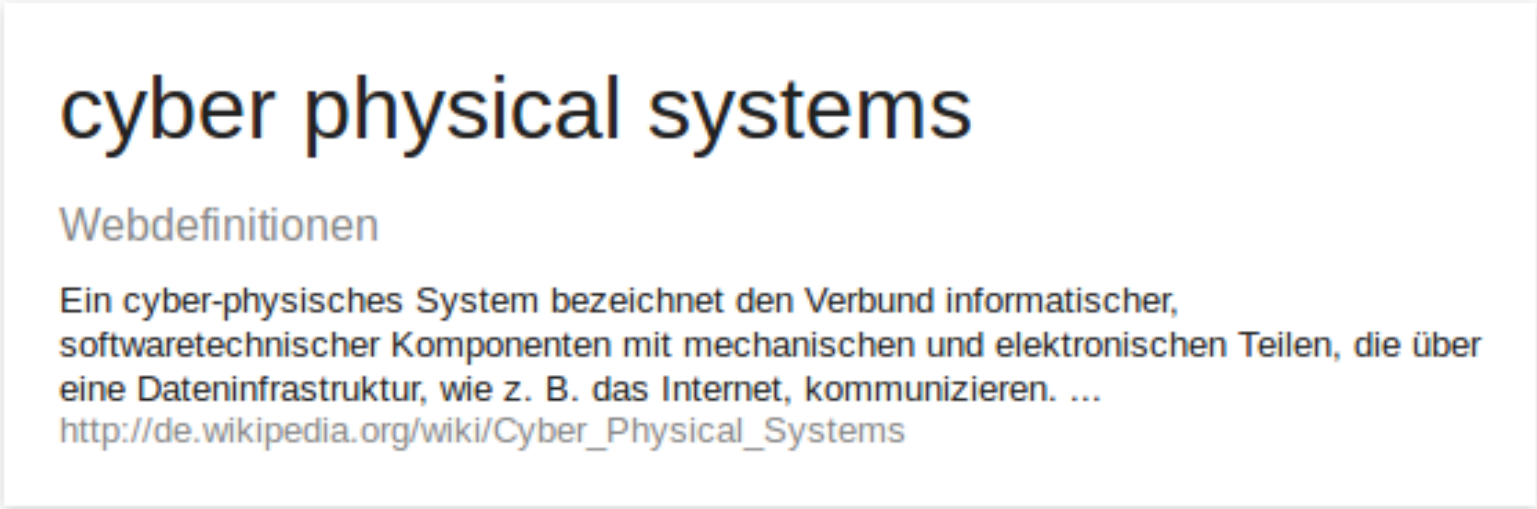
Fehlerart und -anzahl nicht eindeutig. An der Begriffsdefinition für »Fehler« muss noch »gefeilt« werden.

Server-Dienst als Service

- Beispiel einer Service-Anforderung:

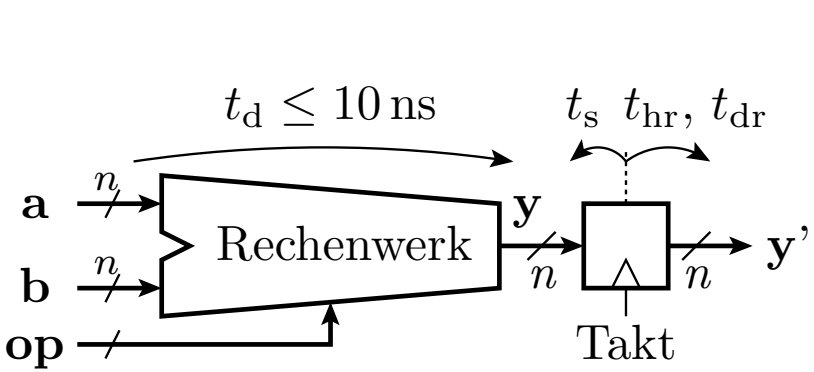


- Ausschnitt aus dem gelieferten Ergebnis

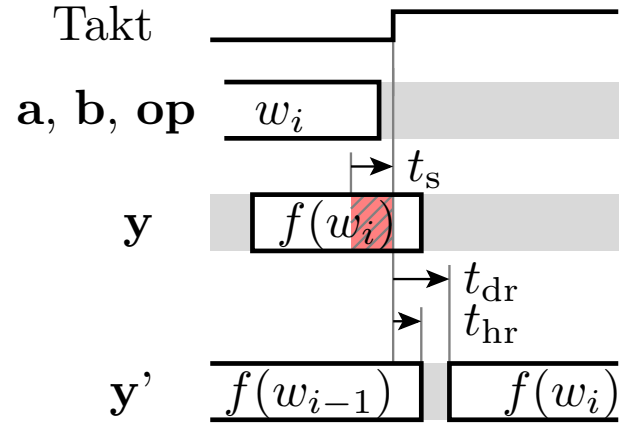


Service-Anforderungen (SA), -Leistungen (SL), FF, ... zählbar. √

Digitalschaltung als Service



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



t_s	Vorhaltezeit
t_{dr}	Registerverzögerung
t_{hr}	Registerhaltezeit
	Abtastfenster

- Ein- und Ausgabe sind Signale.
- Service-Anforderung durch Eingabeänderung.
- Formate: Stabile Daten ...

Service-Anforderungen (SA), -Leistungen (SL), FF, ... zählbar. √

CP-Systeme als Service-Anbieter

Motorsteuergerät:

- Eine SL (Service-Leistung) je Schrittzeit.
- Eingabe: Sensordaten vom Motor, Benutzereingaben, Nachrichten anderer Steuergeräte, ...
- Ausgaben: Stellwerte für Aktoren (Schalter, Ventile, ...), Benutzerausgaben, Nachrichten an andere Steuergeräte.

Service-Anforderungen (SA), -Leistungen (SL), FF, ... zählbar. √

Ein Service kann auch komplette physikalische Vorgänge »kapseln«.
Beispiel »Waschvorgang einer Waschmaschine«:

- Service-Anforderung: Start des Waschvorgangs.
- Eingabe: Programmauswahl, Wäsche bzw. deren Beschreibung durch Daten.
- Ergebnis: saubere Wäsche (bzw. Bewertungsdaten der Sauberkeit) nach Abarbeitungsdauer.

Entstehungsprozesse

Vorgänge, in denen Systeme und ihre Fehler entstehen:

- Entwurfsprozesse: überwiegend Informationsverarbeitung,
- Fertigungsprozesse: zusätzlich mit physikalischen Vorgängen,
- Reparatur, Nachbesserung: auch dabei entstehen Fehler.

Modellierung als Service:

- Anforderung: Entwicklungs-, Produktions-, Reparaturauftrag.
- Eingaben: Ressourcen, Material, Daten.
- Ergebnis: Entwurfsbeschreibungen, Prototypen, Produkte.

Fehlfunktionen von einem Entstehungs-Service sind auf der nächsten Modellebene Fehler im entstandenen Service.

Determinismus, Gedächtnis, Hierarchie

Determinismus

Definitionen 3

Ein Service arbeitet deterministisch, wenn er immer gleich ausgeführt wird und für gleiche Eingaben (und gespeicherte Zustände) gleiche Ergebnisse liefert.

Determinismus ist u.a. für folgende Maßnahmen (means) zur Sicherung der Verlässlichkeit Voraussetzung:

- Ergebniskontrolle durch Soll-/Ist-Vergleich,
- Fehlerausschluss durch Test,
- Reparaturkontrolle durch Testwiederholung,
- Fehlerlokalisierung durch Rückverfolgung, ...

Für Informationsverarbeitung ist Determinismus (fast immer) eine selbstverständliche Anforderung, um die gelisteten »Means« zu nutzen. Für physikalische Prozesse wird Determinismus angestrebt.

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 jede Realisierungsart (SW, HW, CPS, ...):

	ohne Gedächtnis	mit Gedächtnis
Programm-bausteine	Unterprogramme ohne private Daten	OOP-Methoden zur Objektbearbeitung.
Programm	Compiler	Textverarbeitung
Server-Dienst	Ohne Nutzung fremder Daten.	Datenbankanfrage
digitale Schaltung	Rechenwerk	Prozessor
CP-System	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):

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

Prüfgerechter Entwurf

- Maßnahmen zur Vermeidung von Testproblemen, wie Strukturrierung des Systems in getrennt testbare Module[4]
- Steuer- und Beobachtbarkeit interner Zustände, um Module mit Gedächtnis wie Module ohne Gedächtnis testen zu können,
- ...

[4] In der Informatik gilt auch »divide et impera«, aber mehr im Sinne von teile das System und beherrsche den Test, die Fehlersuche, ...

Hierarchie

IT-Systeme werden nach dem Baukastenprinzip entworfen:

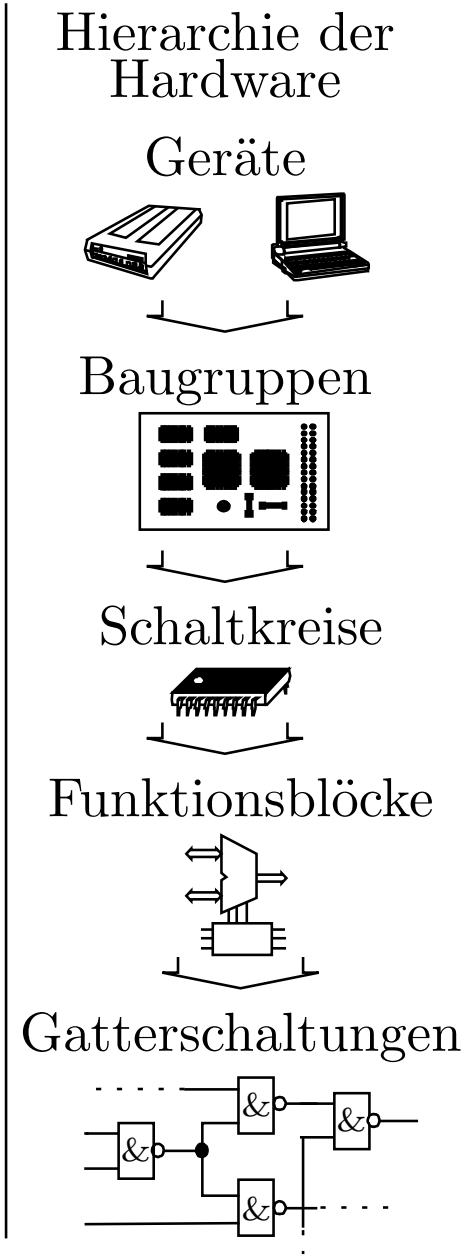
- Top-Down: Beschreibung der Zielfunktion durch miteinander kommunizierende Teilsysteme,
- Bottom-Up: Zusammensetzen aus vorentworfenen Bausteinen.

Mehrere Gründe:

- Voraussetzung für Fehlerbeseitigung durch Komponentenaustausch,
- ermöglicht Zwischenkontrollen an den Schnittstellen im Betrieb,
- vereinfacht Testauswahl, -durchführung, Fehlerlokalisierung.
- Voraussetzung für eine hohe Fehlerüberdeckung,
- ermöglicht zeitgleiche Entwicklung an mehren Systemteilen,
- Nachnutzung von Teilentwürfen in anderen Systemen, ...

Strukturelle Hierarchie von Rechnersystemen

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

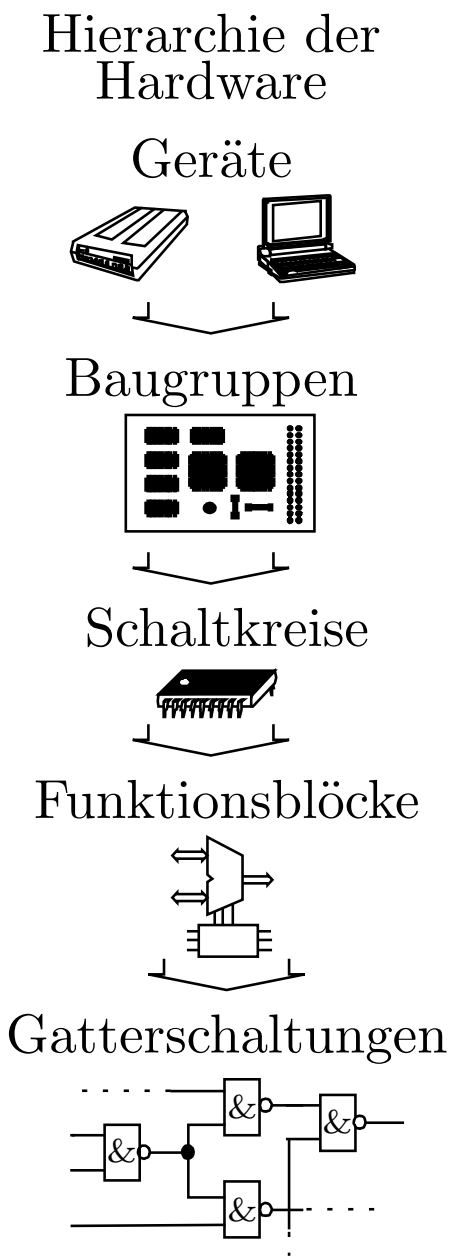


Service-Hierarchie

Im Service-Modell

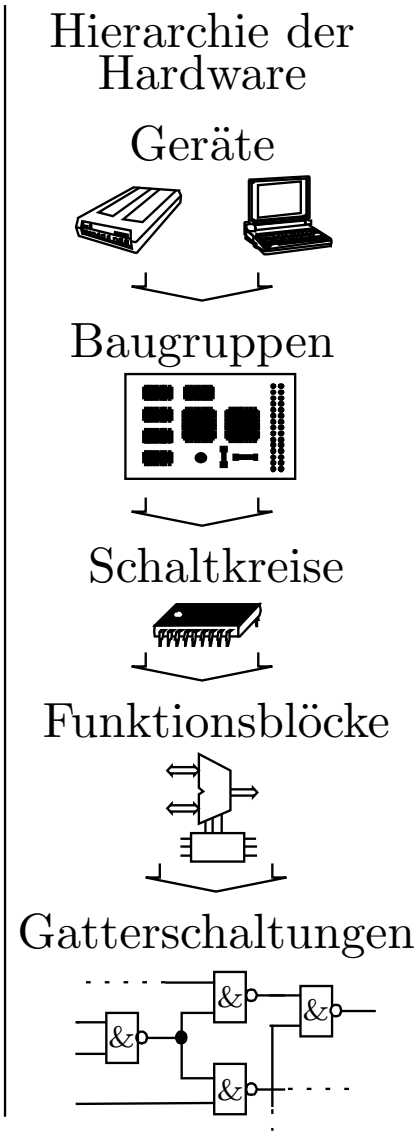
- stellen die Transistoren elementare Schaltfunktionen bereit (ein/aus) mit denen Gatterfunktionen und Speicherelemente gebildet werden.
- Mit Gattern und Speicherelementen werden komplexere Funktionseinheiten wie Rechenwerke, Register bis hin zu kompletten Rechnern nachgebildet.
- Die Software nutzt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

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



Fehler-Hierarchie

Jeder übergeordnete Service »erbt« die Fehler, Fehlfunktionen, Kontrollen, aller von ihm genutzten Teil-Service-Leistungen.



Fehlfunktionen und Fehler

Fehlfunktionen

Definition 4

Eine Fehlfunktion (FF) ist eine fehlerhaft ausgeführte Service-Leistung. Fehlerhaft bedeutet, dass das Ergebnis vom spezifizierten Sollverhalten abweicht.

Wesentliche Aspekte dieser Definition:

- Nur eine Service-Anforderung (SA) mit Ergebnis kann eine Fehlfunktion sein[5].
- Was eindeutig als FF zählt, was möglicherweise als FF zählt, hängt von den Kontrollmöglichkeiten ab und davon, wie genau das Sollverhalten spezifiziert ist.

[5] In späteren Modellen sind Service-Leistungen (SL) potentielle Fehlfunktionen, die mit Auftrittswahrscheinlichkeiten vorhanden sind, mit Erkennungswahrscheinlichkeiten erkannt werden, ...

Zählbarkeit der Fehlfunktionen

Prinzipiel zählbar, aber auch die Kontrollen zur Klassifizierung erbrachter Service-Leistungen und das Zählen der FF selbst sind Service-Leistungen mit Fehlern und potentiellen Fehlerfunktionen:

- Maskierung (Nichterkennen von FF),
- Phantomfehler (Erkennen nicht vorhandener FFs),

und es gibt Interpretationsspielraum, was eine FF ist:

- Uneindeutiges Sollverhalten.
- Wegdiskutieren von FF's:

It is not a bug, it is a feature.

Klassifizierungsfehler und Unsicherheiten lassen sich mit Wahrscheinlichkeiten beschreiben.

Die Ursachen von Fehlfunktionen

- Fehler:
  - ständig vorhanden,
  - sind durch Reparatur oder Ersatz beseitigbar,
  - entstehen in Entwurfs-, Fertigungs-, Reparaturprozessen,
  - sind durch Beseitigung ihrer Entstehungsursache vermeidbar.
- Störungen:
  - spontane, nicht reproduzierbare Wirkung,
  - vermeidbar durch Verringerung der Störanfälligkeit.
- Ausfälle:
  - während des Betriebs entstehende Fehler.
  - Schadensvermeidung: Wartungsintervalle, Einschalttests, ...

Störungen und Ausfälle sind an physikalische Prozesse gebunden. In software-lastigen Systemen dominieren Fehler als Ursache für FF.

Fehler

Definition 5

Fehler sind beseitigbare Ursachen für die Entstehung von Fehlfunktionen.

Im weiteren wird unterschieden zwischen

- tatsächlichen Fehlern,
- potentiellen Fehlern und
- Modellfehlern.

Tatsächliche Fehler sind vor ihrer Entdeckung und Beseitigung unbekannt und danach nicht mehr vorhanden. Ihre Möglichkeiten sind nicht abzählbar und ihr Verhalten ist nicht vorhersagbar. Beschrieben werden sie in der Regel durch die Art ihrer Beseitigung, z.B. falscher (korrigierter) Datentyp, kaputter (getauschter) Schaltkreis, ...

Tatsächliche Fehler

Fehlerbeschreibung bei der Erfassung und Beseitigung:

- Nach einmaliger Beobachtung einer Fehlfunktion: Art der Fehlfunktion (Absturz, falsches Ergebnis, ...) und Bedienungsablauf, bei dem sie aufgetreten ist.
- Nach wiederholter Beobachtung: Bedienungsabläufe, unter denen die FF zu erwarten ist und Workaround für ihre Vermeidung.
- Erfassung als zu beseitigender Fehler: Fehlerbezeichner und Zusammenfassung aller Beobachtungen zu FF, hinter denen derselbe Fehler vermutet wird.
- Nachweisbarer Fehler: Reproduzierbarer Test.
- Beseitigter Fehler: Durchgeführte Änderungen am System.

Tatsächliche Fehler sind erst dann genau bekannt, wenn sie nicht mehr vorhanden sind. Gezählt werden Beseitigungserfolge.

Was für einen Fehler enthält das Programm?

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

Sollfunktion: »Rückgabe 23*(a+b)«. Das Ergebnis nur richtig für:

$$-2^{-15} \leq 23 \cdot (a+b) \leq 2^{15} - 1$$

Mögliche Beschreibungen des Fehlers:

WB-Eingabekontrolle fehlt	Ausgabe-WB falsch

int16_t UP(int16_t a, in16_tt b){
int32_t y=23*(a+b);
assert (y>=2**-15 && y<=2**15-1)
return (int16_t) y;
};
	int32_t UP(int16_t a,
	int16_t b){
	int32_t y=23*(a+b);
	return y;
	};

Fehlernachweis, -lokalisierung und -beseitigung

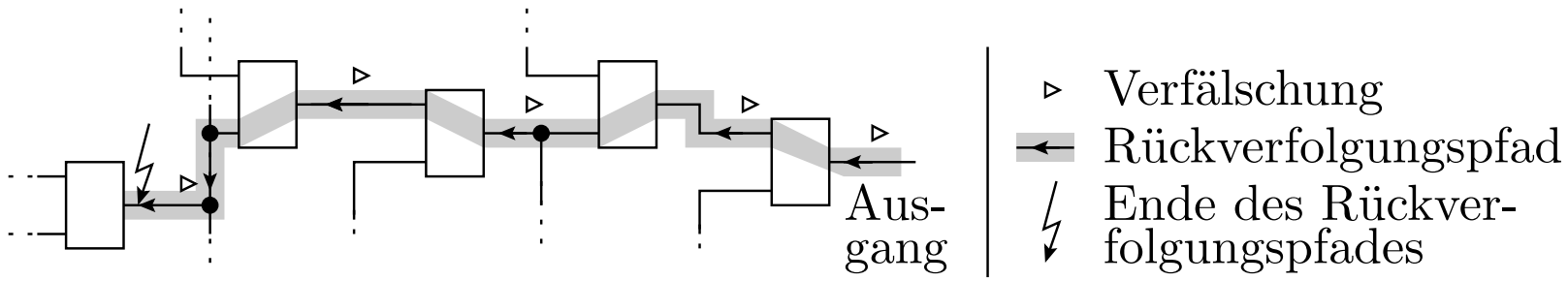
Fehler + beeinträchtigte Service-Anforderung ⇒ Fehlfunktion

Fehlernachweis:

- Service-Anforderung mit fehlernachweisenden Eingaben.
- Kontrolle der Ausgabe.

Fehlerbeseitigung durch experimentelle Reparatur:

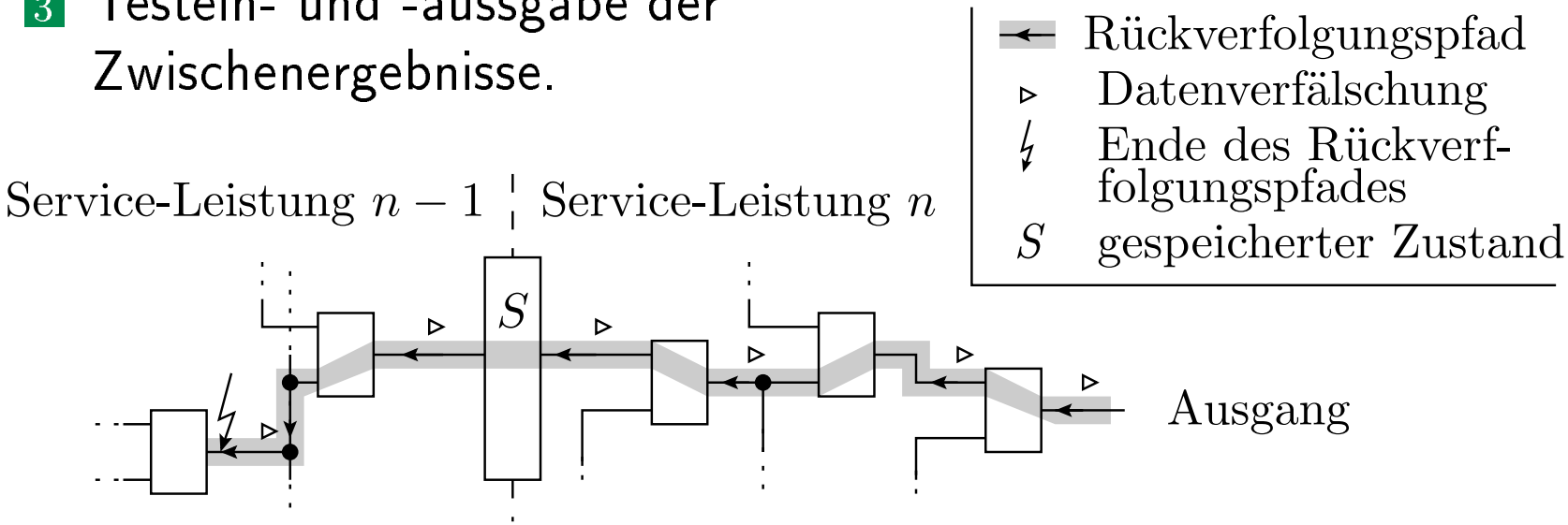
- Suche der untersten Teil-Service-Leistung oder Kommunikation, die mit korrekten Daten falsch ausgeführt wird.
- Ersatz, Reparatur, ... der lokalisierten Teil-Service-Leistung.
- Erfolgskontrolle durch wiederholte Service-Anforderung.



Lokalisierung mit Gedächtnis

Rückverfolgung über mehrere Service-Anforderungen:

1. Wiederholung aller Service-Anfragen ab Initialisierung bis zu den potentiellen Verursachern.
2. Trace-Aufzeichung der Zwischenergebnisse.
3. Testein- und -aussgabe der Zwischenergebnisse.



Lokalisierbarkeit setzt Prüfgerechtheit voraus: Determinismus (Punkt 1), testspezifische Zusatzfunktionen (Punkte 2 und 3), ...

Unbeständiges Fehlverhalten

Fehler in deterministischen Systemen haben meist ein beständiges Fehlverhalten zur Folge, d.h.

- Ein Service ohne Gedächtnis versagt mit denselben Eingaben immer in derselben Weise.
- Ein Service mit Gedächtnis versagt bei gleicher Initialisierung, derselben Eingabefolge immer in derselben Weise.

Es gibt jedoch auch Ursachen für unbeständige Fehlverhalten:

- unbeabsichtigte Abhängigkeiten von anderen Daten, Speicherbelegungen, Verarbeitung physikalischer Größen, ...
- Störungen, ...

Vor dem Einsatz von »Means«, die Determinismus voraussetzen:

- Fehlerausschluss durch Test, experimentelle Reparatur,
- Lokalisierung durch Rückverfolgung, ...

Kontrolle auf / Schaffung von Beständigkeit.

Kontrolle auf / Schaffung von Beständigkeit

Kontrolle auf Beständigkeit erfolgt durch mehrfache Wiederholung der Tests und Vergleich der Ergebnisse. Bei Unbeständigkeit:

- Verbesserung der Tests, feinere Modularisierung, ...
- Beseitigung von Störeinflüssen, ...
- Erraten und versuchsweise Beseitigung der Ursachen.

Erst bei beständigem Fehlverhalten gezielte Fehlersuche.

Mittel zur Schaffung von Beständigkeit:

- Fehlerisolation: Verhinderung der Ausbeitung von Datenfälschungen über Teilsystemgrenzen durch Kontrollen und Blockierung, Speicherschutz unter Betriebssystemen, ...
- Minderung physikalischer Einflüsse (Rauschen, Strahlung, ...) auf die Datendarstellung, Abtastung, Digitalisierung, Mittelwertbildung, ...
- Vermeidung / Erkennung von Ausfällen: Intervallwartung, ...

Potentielle und Modellfehler

Potentielle und Modellfehler

Die Abschätzung der Anzahl der entstandenen, vermiedenen, beseitigten, ... Fehler in einem System und der Anzahl der durch sie verursachten, vermiedenen, ... Fehlfunktionen, die Testauswahl, ... verlangen

- abzählbare Mengen potentieller Fehler,
- abschätzbare Auftrittswahrscheinlichkeiten,
- simulierbares Verhalten und
- abschätzbare Häufigkeit verursachter Fehlfunktionen (FF).

Da ein Modell das nicht leistet, zwei Modelle:

- potentielle Fehler: Abschätzung der Fehleranzahl,
- Modellfehler: simulierbares Fehlverhalten, Abschätzung der Häufigkeiten verursachter FF.

Bindeglied FHSF-Funktion (**F**ehlerauftritts**h**äufigkeit in Abhängigkeit von der mittleren Anzahl von **S**L je **F**F).

Potentielle Fehler

Potenzielle Fehler seien zähl- und lokalisierbar[6]. Eine abzählbare Menge möglicher Fehler lässt sich ableiten aus:

1. den Schritten das Entstehungsprozesses:
2. der System-Hierarchie und
3. den Reparaturmöglichkeiten.

In jedem Entstehungsschritt kann ein Fehler entstehen. Jedes Element und jede Verbindung in der Hierarchie kann fehlerhaft sein. Jedes austauschbare Element kann fehlerhaft sein. Lokalisierbar sind davon die Reparaturmöglichkeiten:

Definition 6

Potentielle Fehler seien alle Teil-Service-Leistungen und Kommunikationswege, die falsch ausgeführt werden können, ohne dass innerhalb von ihnen eine genauere Lokalisierung erfolgt.

[6] Damit ihnen Auftrittshäufigkeiten zugeordnet werden können.

Abschätzung der Fehleranzahl

Aus den Entstehungsschritten und den Elementen in der Hierarchie lassen sich Metriken für die Systemgröße (und Kompliziertheit) abschätzen:

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

Diese Metriken charakterisieren nicht nur Systemgröße, Entwurfs- und Fertigungsaufwand, sondern auch die Anzahl der entstehenden Fehler. Verlässlichkeitsbezogene Gütemaße von Entstehungsprozessen:

- Fehler pro Arbeitstag,
- Fehler pro 1.000 NLOC (typ. 30 bis 100),
- Fehler pro Schaltkreis, Baugruppe, ... umrechenbar in Fehler pro Transistoranzahl, Bauteil, ...

Modellfehler

Potenzielle Fehler der Form »Schaltkreis defekt«, »Anweisung falsch« haben viele mögliche Fehlverhalten. Für die Bewertung und Suche von Testsätzen, die Abschätzung der Häufigkeit der FF je Fehler, ... kann von den möglichen Fehlverhalten nur eine Stichprobe berücksichtigt werden.

Definition 7

Ein Modellfehler ist ein Fehler 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

Definitions 8

Ein Fehlermodell ist ein 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 Werteberechnungen 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).

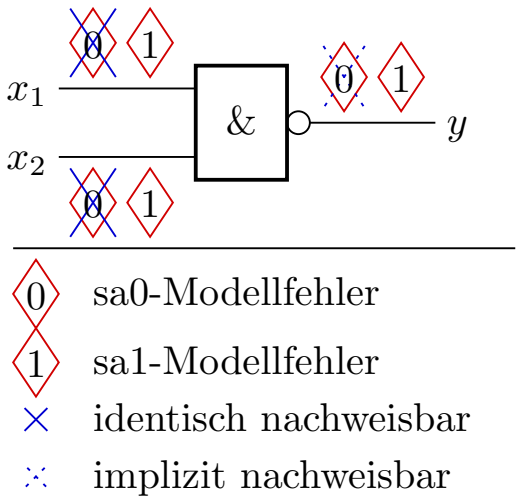
In der Praxis am meisten verbreitetes Fehlermodell.

- Erprobt für die Fehlersimulation und Testsatzberechnung für digitale Schaltungen mit tausenden Gattern.
- Bei Entwürfen/Software wird zur Minderung der Fehlervielfalt in der Regel eine binarisierte Ebene über die Beschreibung gelegt. Eigentliche Testbewertung/-auswahl rückführbar auf die für Haftfehler.

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

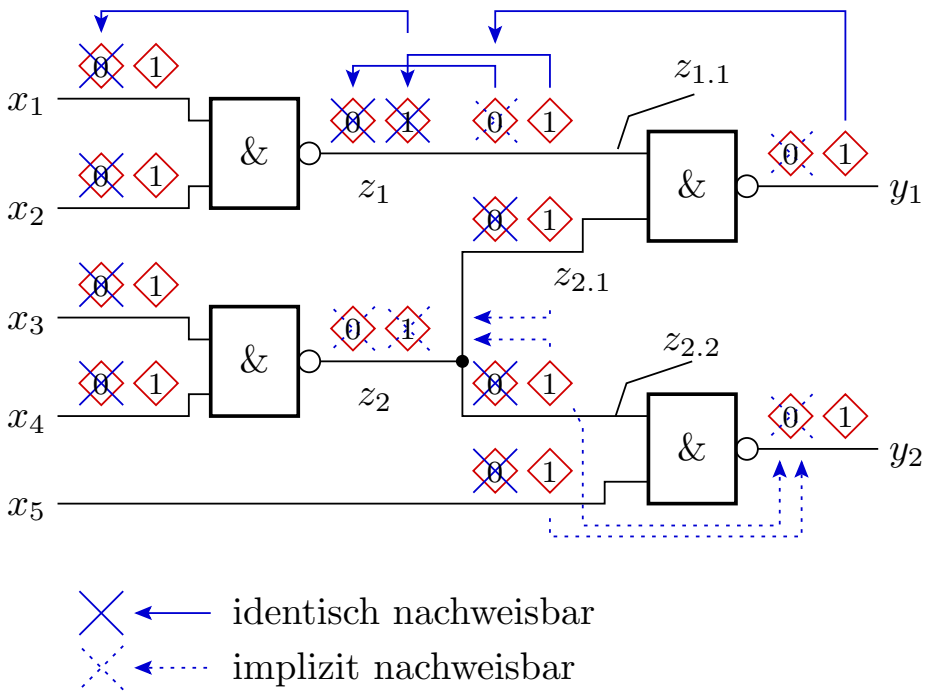
Nachweisidentität (gleiche Nachweismenge)

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

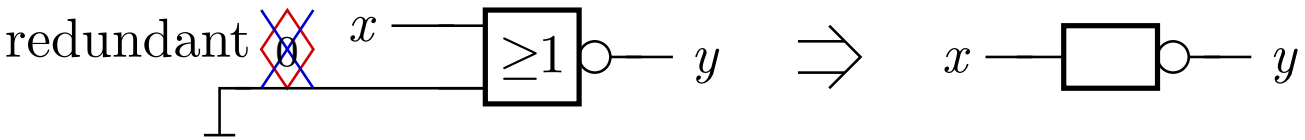
	Mengen von identisch nachweisbaren Fehlern	Nachweis impliziert durch
1	sa0(x_1), sa0(x_2), sa1(z_1), sa1($z_{1.1}$)	
2	sa1(x_1)	
3	sa1(x_2)	
4	sa0(x_3), sa0(x_4), sa1(z_2)	9, 12
5	sa1(x_3)	
6	sa1(x_4)	
7	sa0(z_2)	5, 6, 8, 11
8	sa0(z_1), sa0($z_{1.1}$), sa0($z_{2.1}$), sa1(y_1)	2, 3
9	sa1($z_{2.1}$)	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

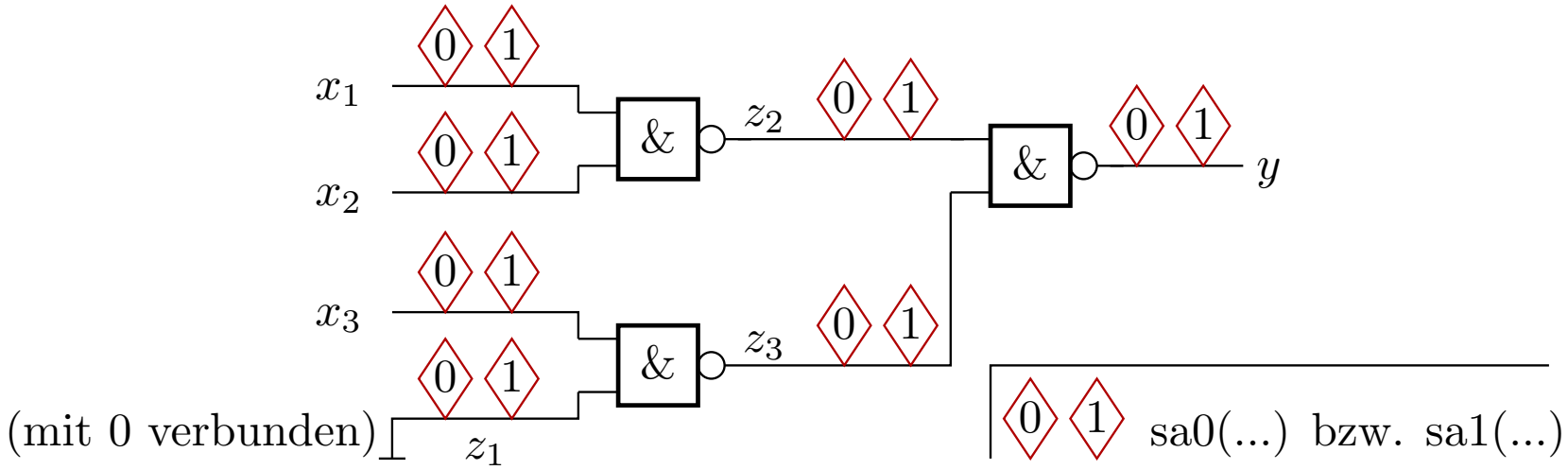
Ein redundanter (Modell-) Fehler ist ein Fehler in einemTeilsystem, der die Funktion des Gesamtsystems nicht beeinträchtigt.

- 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

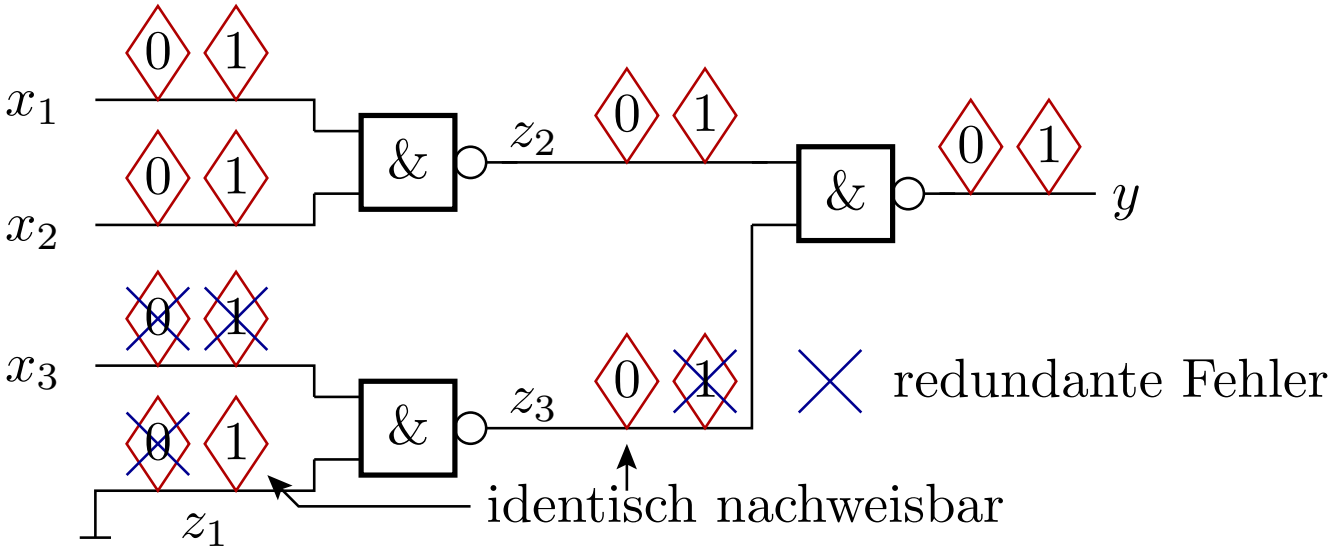
Gegeben ist die nachfolgende Schaltung mit 12 eingezeichneten Haftfehlern.



Welche der Haftfehler sind

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

Lösung Aufgabenteil 1

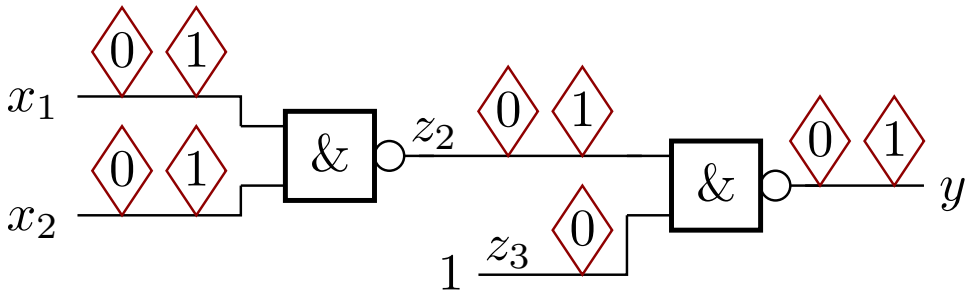


$z_1 = 0$ impliziert, dass

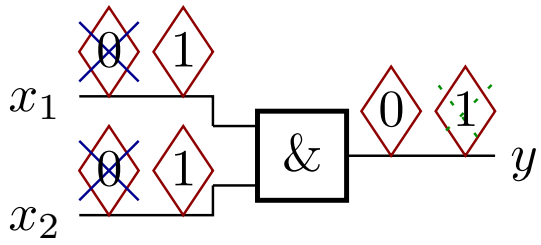
- sa0(z_1) nicht anregbar ist,
- $z_3 = 1$, so dass sa1(z_3) nicht anregbar ist und
- dass x_3 nicht beobachtbar ist, so dass sa0(x_3) und sa1(x_3) auch redundant sind.

Lösung Aufgabenteil 2 und 3

Schaltung ohne redundante Fehler



Konstantenelimination



— identischer Nachweis

— impliziter Nachweis

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 sa1(x_1), sa1(x_2) und sa0(y).

FHSF-Funktion

Entstehungs- und FF-Häufigkeit

Potentielle Fehler (kleinste lokalisierbare fehlerhafte Einheiten):

- abschätzbare Anzahl,
- abschätzbare Entstehungshäufigkeit.

Modellfehler (simulierbares Fehlverhalten):

- Abschätzmöglichkeit der FF-Häufigkeit, ...

FHSF-Funktion:

- Bindeglieder zwischen Entstehungs- und FF-Häufigkeit,
- Abschätzgrundlage der Häufigkeit der durch entstandene, beseitigte, ... Fehler verursache, vermiedene, ... FF.

Definitions 10

Die FHSF-Funktion $H(x)$ beschreibt die Auftrittshäufigkeit von Fehlern in Abhängigkeit von der mittleren Anzahl von Service-Leistungen zwischen zwei Fehlfunktionen x, die der Fehler verursacht.

Pareto-Prinzip

Für Fehler und Fehlfunktionen gilt meist das Pareto-Prinzip[7]:

»20% der Ursachen erzielen 80% der Wirkungen.«

20% und 80% sind Stellvertreterwerte für »kleiner Anteil der Ursachen« und »großer Anteil der Wirkungen«.

- Die meisten Fehler gehen auf wenige Ursachen zurück.
- Ein kleiner Anteil der Fehler verursacht den überwiegenden Anteil der Fehlfunktionen.

Fehlervermeidung während der Entstehung, Fehlerbeseitigung nach der Entstehung, Schadensbegrenzung und Ergebniskorrektur konzentriert sich vorrangig auf den kleinen Teil der Ursachen , die den großen Teil der Probleme verursachen.

[7] 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.

Pareto-Prinzip rekursiv und FHSF-Funktion

Das Pareto-Prinzip für Fehler und Fehlfunktionen gilt rekursiv. Wenn die »20% Fehler, die die 80% der FF verursachen« gefunden und beseitigt sind, sind meist wieder ca. 20% der verbleibenden Fehler Verursacher von 80% der FF, etc.

Dominante Fehler, die die Mehrheit der FF verursachen, sind die, für die die mittlere Anzahl der SL je FF $x \leq d$ ist. Zu erwartende Anzahl:

$$E\left(\varphi\left(d\right)\right) = \int_0^d H\left(x\right) \cdot dx$$

(φ – Fehleranzahl). Zu erwartende Anzahl aller Fehler:

$$E\left(\varphi\right) = \int_0^\infty H\left(x\right) \cdot dx$$

Die Rechengröße d ist so zu wählen, dass der Anteil der dominanten Fehler 20% oder ein andere »kleiner« Anteil ist:

$$\varphi\left(d\right)/\varphi \approx 20\%$$

Wenn bereits so viele Fehler beseitigt sind, dass die meisten Service-Leistungen richtig ausgeführt werden, ist die Wahrscheinlichkeit einer FF durch einen dominanten Fehler die Summe der p_{FFF}'s der Fehler mit im Mittel bis zu $x \leq d$ SL je FF und damit das Integral:

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

Die Wahrscheinlichkeit einer FF durch einen beliebigen Fehler:

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

Laut Pareto-Prinzip ist die bedingte Wahrscheinlichkeit, dass eine durch Fehler verursachte FF, durch einen dominanten Fehler verursacht ist, etwa 80% oder ein anderer »großer« Anteil:

$$\frac{p_{\mathrm{FFF}}(d)}{p_{\mathrm{FFF}}} \approx 80\%$$

Potenz-FHSF-Funktion

Nachstellung des Pareto-Prinzips mit einer FHSF-Funktionen:

$$\frac{\int_0^d H(x) \cdot dx}{\int_0^\infty H(x) \cdot dx} = 20\% \quad \text{und} \quad \frac{\int_0^d \frac{H(x)}{x} \cdot dx}{\int_0^\infty \frac{H(x)}{x} \cdot dx} = 80\%$$

Eine FHSF-Funktion, die das Pareto-Prinzip auch rekursiv erfüllt:

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

Mit dieser FHSF-Potenzfunktion beträgt die zu erwartende Anzahl

- der Fehler mit im Mittel mindestens einer FF je d SL:

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

- aller Fehler:

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

Für die Wahrscheinlichkeit der durch Fehler verursachten FF gilt:

- dominante Fehler mit $x \leq d$ SL je FF:

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

- alle Fehler:

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

Mit dem Postulat »20% der Fehler verursachen 80% der FF«

$$\frac{\int_0^d H(x) \cdot dx}{\int_0^\infty H(x) \cdot dx} = 20\% = 1 - \left(\frac{d}{x_0}\right)^{-k} \quad \text{und} \quad \frac{\int_0^d \frac{H(x)}{x} \cdot dx}{\int_0^\infty \frac{H(x)}{x} \cdot dx} = 80\% = 1 - \left(\frac{d}{x_0}\right)^{-(k+1)}$$

ergibt sich für das Verhältnis $\frac{d}{x_0}$:

$$\left(\frac{d}{x_0}\right)^{-k} = 80\% \quad \text{und} \quad \left(\frac{d}{x_0}\right)^{-(k+1)} = 20\%$$

$$\left(\frac{d}{x_0}\right)^{-k} = 80\% \quad \text{und} \quad \left(\frac{d}{x_0}\right)^{-(k+1)} = 20\%$$

Division beider Gleichungen:

$$\frac{\left(\frac{d}{x_0}\right)^{-k}}{\left(\frac{d}{x_0}\right)^{-(k+1)}} = \frac{d}{x_0} = \frac{80\%}{20\%} = 4$$

Für die FHSF-Potenzfunktion

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

sind die 20% der dominanten Fehler, die 80% der FF verursachen, die, die im Mittel mindestens eine FF je $4 \cdot x_0$ SL verursachen.

Die »80% für großer Anteil« und die »20% für kleiner Anteil« können durch andere große und kleine Prozentanteile ersetzt werden.

Wahrscheinlichkeit

Bewertung der Verlässlichkeit

Viele der bisher behandelten Aspekte:

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

lassen sich nur mit Wahrscheinlichkeiten beschreiben.

Die Basis für die Definition von Wahrscheinlichkeiten sind Zufallsexperimente.

Dieser Abschnitt behandelt

- Grundlagen der Wahrscheinlichkeitsrechnung,
- Wahrscheinlichkeitsabschätzungen,
- Fehlerbäume und Markov-Ketten.

Zufallsexperiment

Definition 11

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

Zufallsexperimente zu Test und Verlässlichkeit {Wertebereich[8]}:

- Anforderung einer Service-Leistung {richtig, falsch, ...}.
- Ergebniskontrolle {richtig, falsch, ...}.
- Korrektur falscher Ergebnisse {erfolgreich, ...}.
- Zählen der Fehler in einem System {0, 1, 2, ... }.
- Aufdecken eines Fehlers mit einem Test {ja, nein}.
- Messen der Zeit bis zum Ausfall {Zeit größer null}.
- ...

[8] Wertebereich der möglichen Ergebnisse des Experiments

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:

- Anforderung einer Service-Leistung {richtig, falsch}.
- Aufdecken eines Fehlers mit einem Test {ja, nein}.
- ...

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

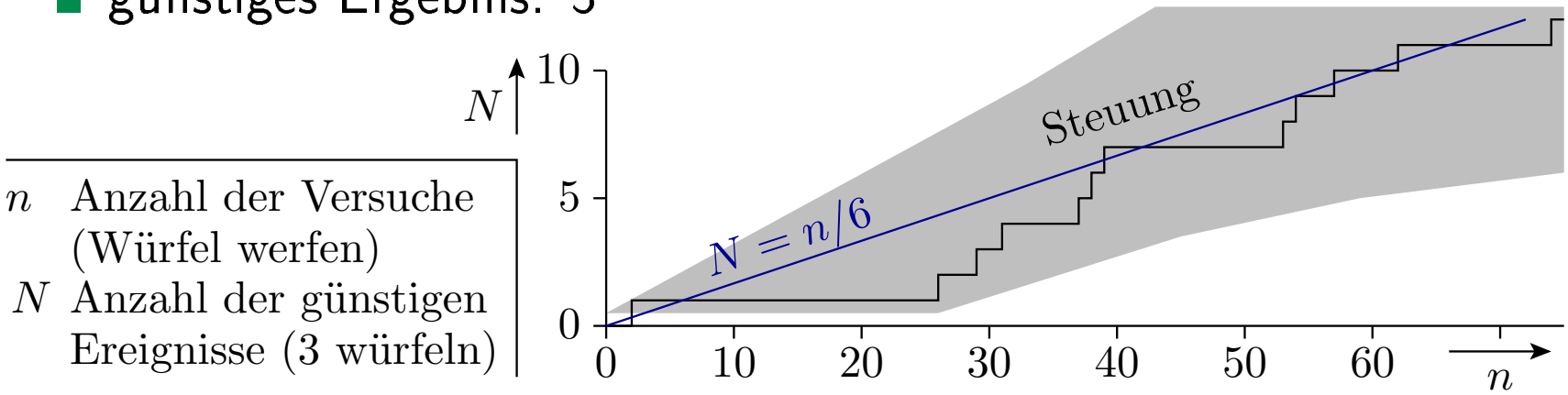
Die Wahrscheinlichkeit von Zufallsexperimenten

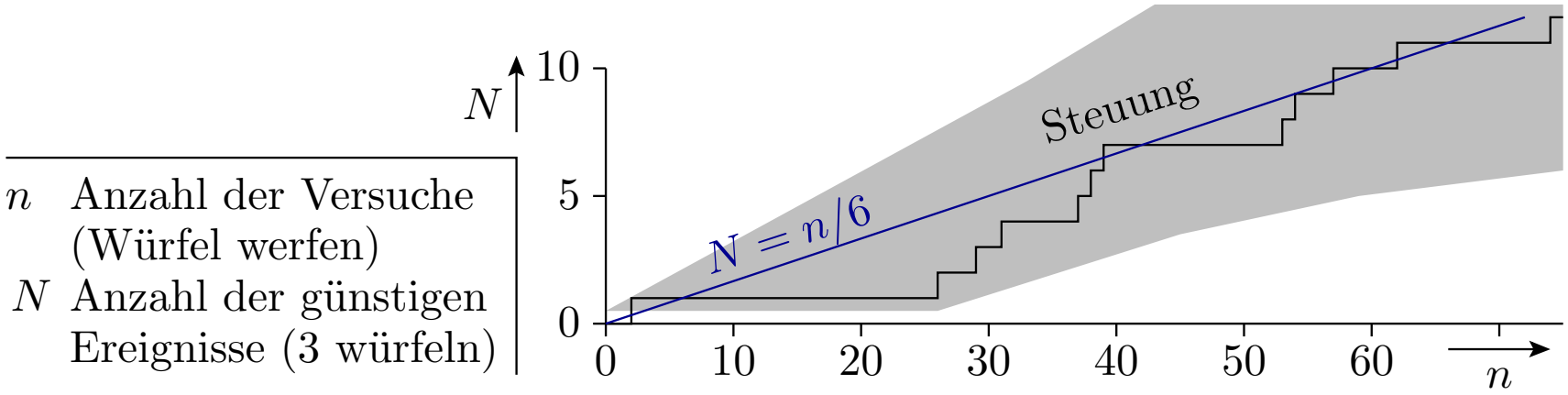
Definition 12

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 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 keineswegs, dass bei jedem sechsten Versuch eine 3 gewürfelt wird. Es ist durchaus zu beobachten, dass hintereinander mehrere Male die Drei und auch mal lange Zeit keine Drei gewürfelt wird.

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.

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 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 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?

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:

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

- 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 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, nächste Folie):

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

Abhängige Ereignisse

Fakt 13

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 $G_7 = G_6 = G_5 = G_4$:

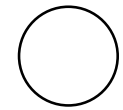
$$\begin{aligned} \mathbf{x} = \text{"}11111110\text{"} &= G_4 \wedge G_3 \wedge G_2 \wedge G_1 \wedge \bar{G}_0 \\ P\left(\mathbf{x} = \text{"}11111110\text{"}\right) &= g^4 \cdot (1-g) \end{aligned}$$

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

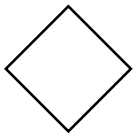
Fehlerbaumanalyse

Fehlerbaumanalyse (FTA – fault tree analysis)

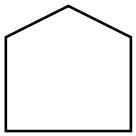
Verfahren zur Abschätzung der Eintrittswahrscheinlichkeit von Problemen in Abhängigkeit vom Eintreten anderer Ereignisse (Gefahrensituationen, Ausfälle, Service-Versagen, ...). Arten von Ereignissen bzw. Problemen:



Problem mit bekannter oder auf anderem Wege abgeschätzter Eintrittswahrscheinlichkeit.



Problem, dessen Eintrittswahrscheinlichkeit nicht untersucht wurde.

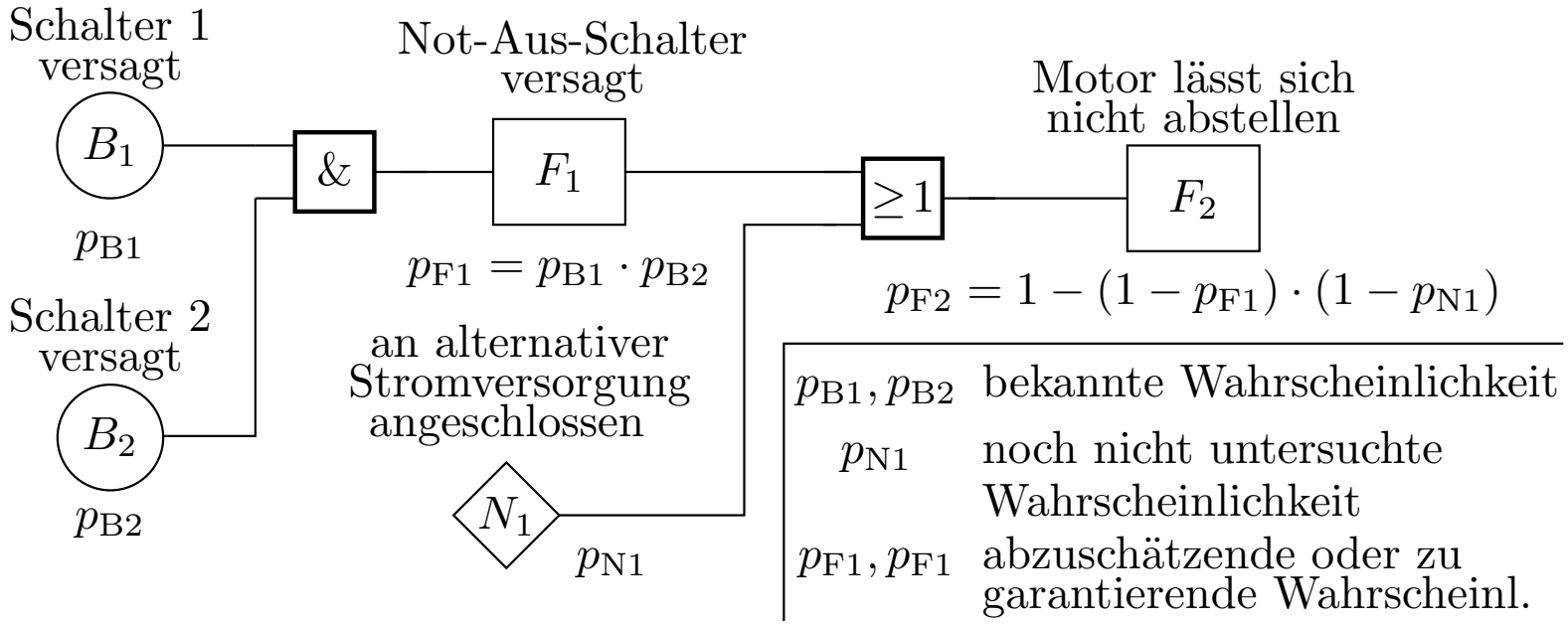


Ereignis im gewöhnlichen Betrieb, das in Kombination mit anderen Probleme verursachen kann.

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

Verknüpfung mit UND, ODER, NICHT.

Beispiel: Motor lässt sich nicht abstellen



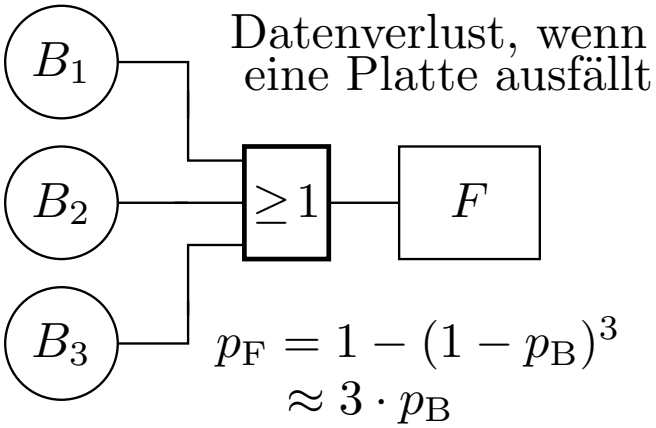
Formulierbare Aufgabe: Wenn $p_{B1} = p_{B2} = 10^{-3}$ ist und $p_{F2} \leq 10^{-6}$ sein darf

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

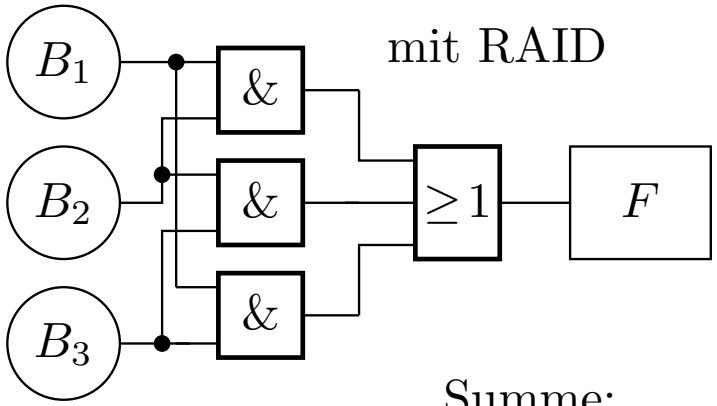
(Ziel hier nur mit $p_{N1} = 0$ erreichbar. Realistisch/andere Lösung?)

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 Interkontinantalraketen 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

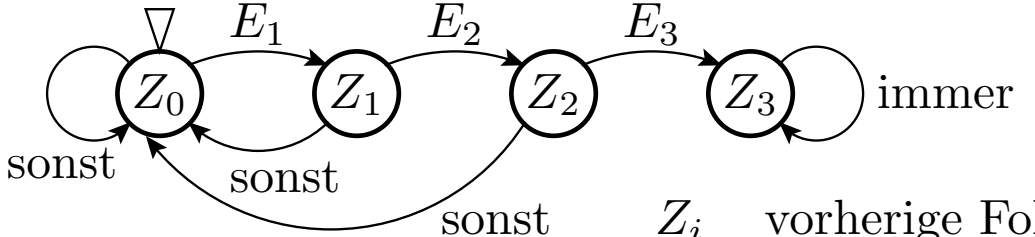
zuvor auf andere Weise abzuschätzen: Vorexperimente, Expertenbefragungen, Ursache-Wirkungs- (Ishikawa-) Diagramm, ...

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 $E_1E_2E_3$:

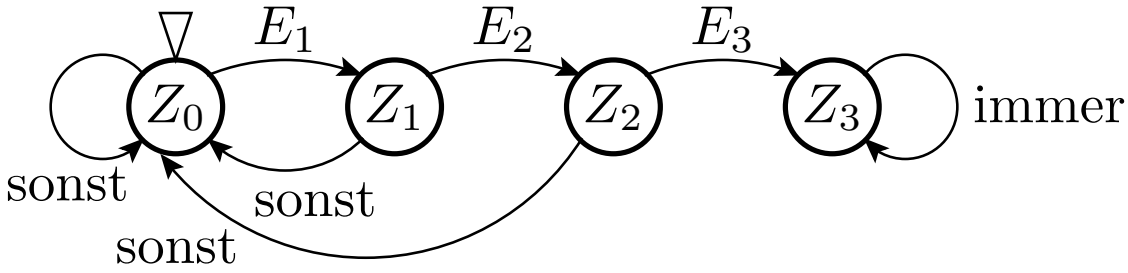


Z_i vorherige Folge bestand aus den ersten i richtigen Werten

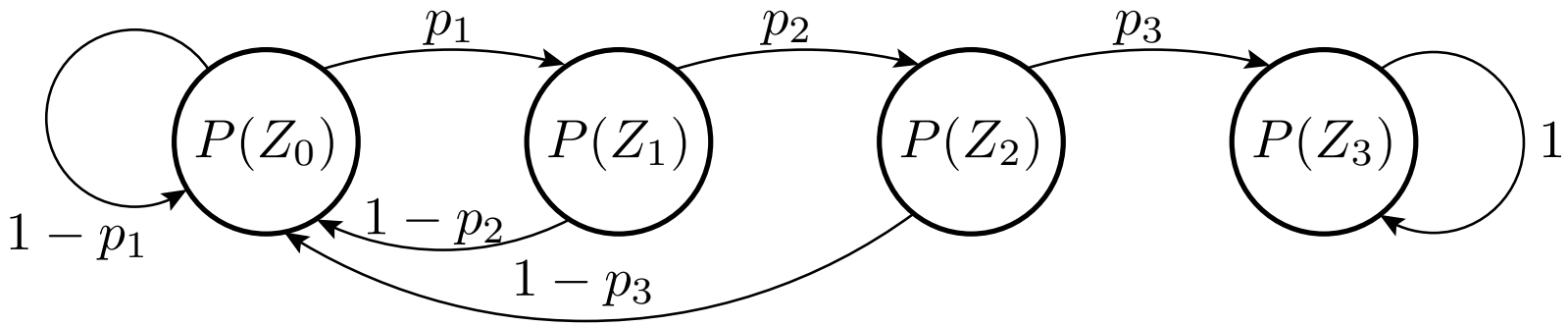
E_i Wert ist X_i

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.

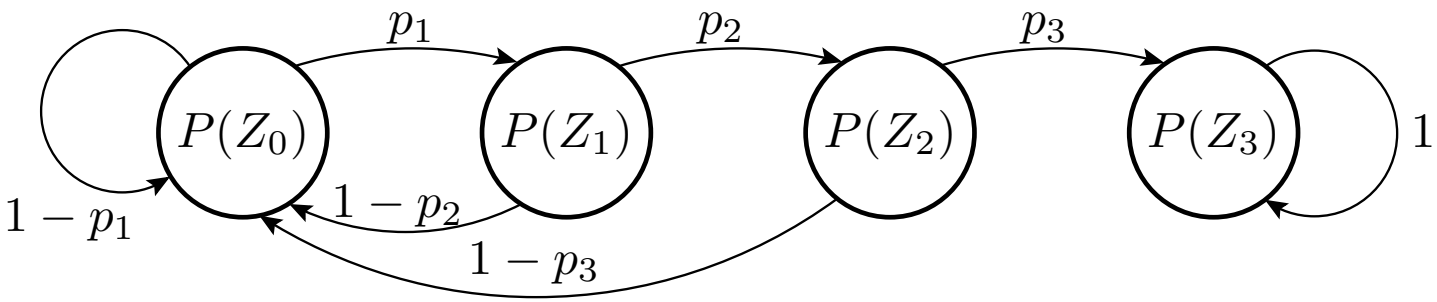


Zur Umwandlung in eine Markov-Kette werden die Übergangsbedingungen durch die Übergangswahrscheinlichkeiten p_{E1} bis p_{E3} und die Zustände durch Zustandswahrscheinlichkeiten $P\left(Z_i\right)$ ersetzt.



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:

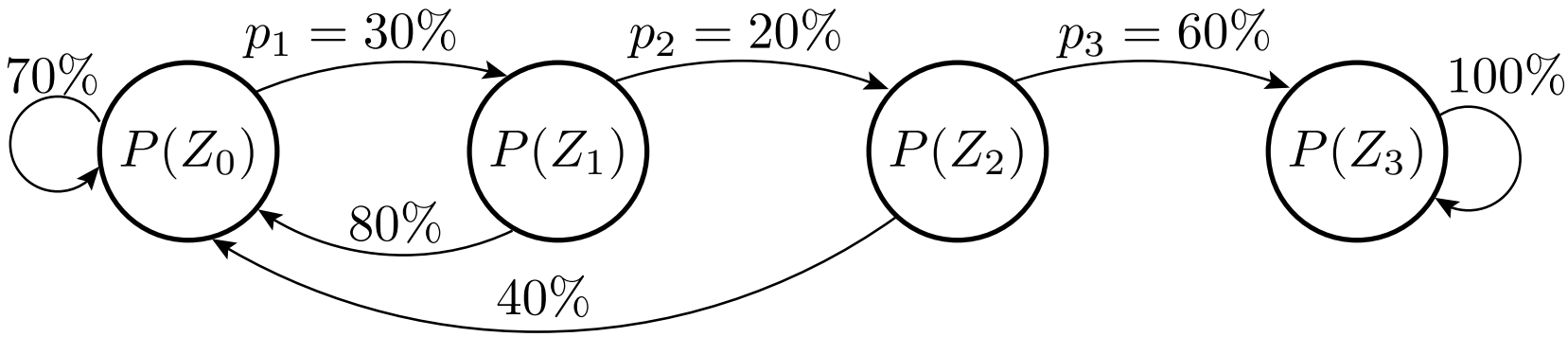
- Die Summe der Wahrscheinlichkeiten in jeder Spalte muss eins sein.
- Die Summe der Zustandswahrscheinlichkeiten $P(Z_i)$ muss in jedem Schritt eins sein.

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

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;
```

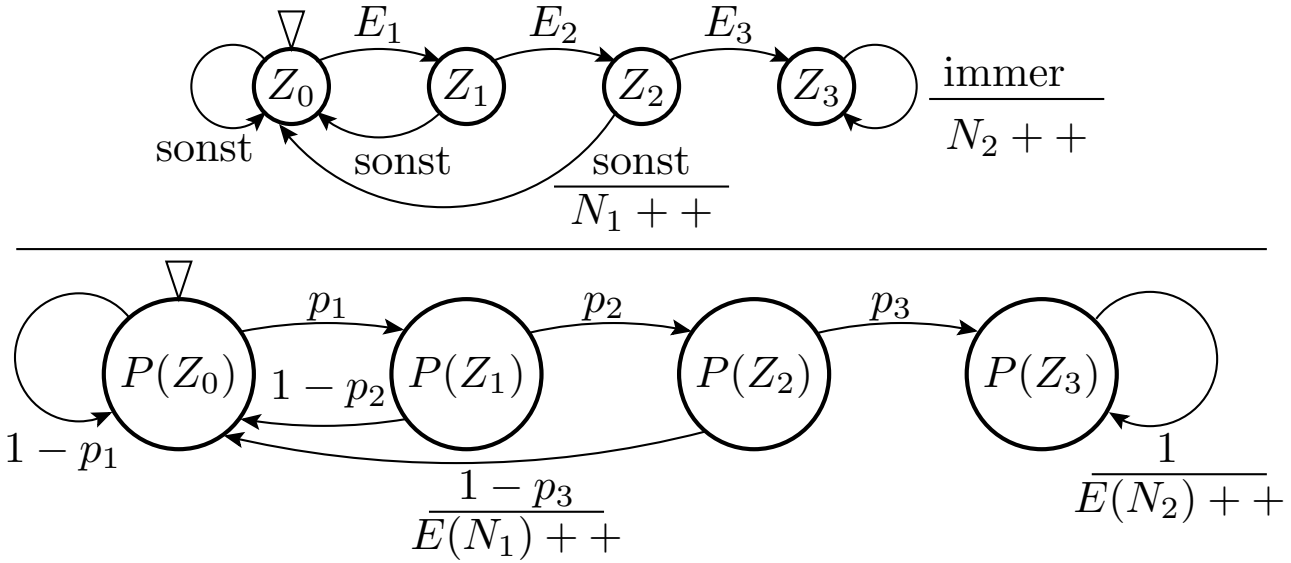
Simulation mit den Beispielwerten $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



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

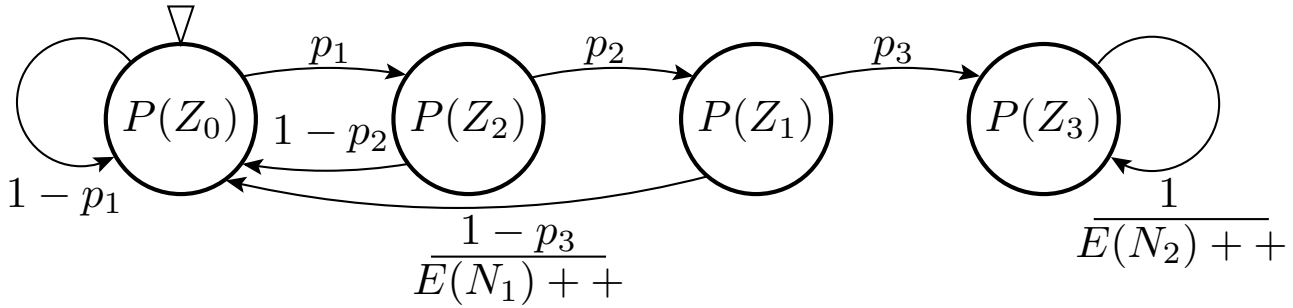
Kantenkosten

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).

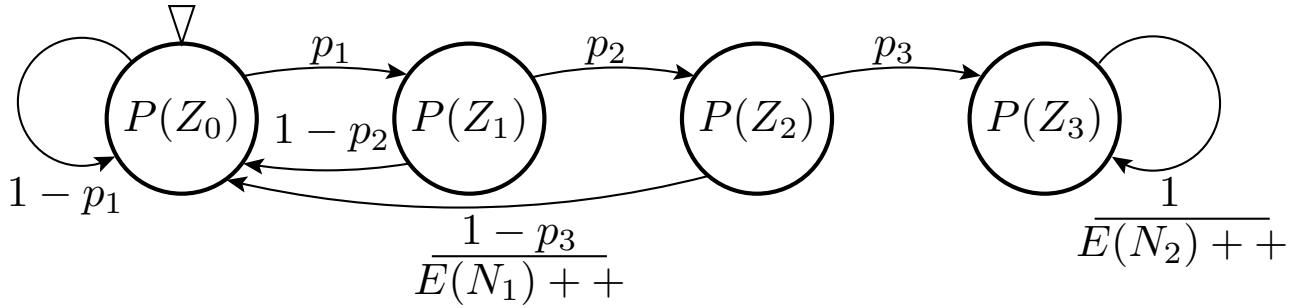
Die korrespondierenden Zähler in der Markov-Kette berechnen die Erwartungswerte der Zählgrößen.



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;
```

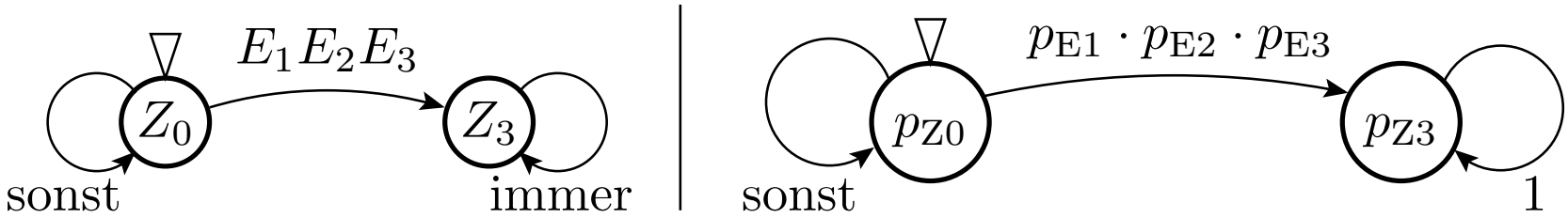
Simulation mit den Beispielwerten $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



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:

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

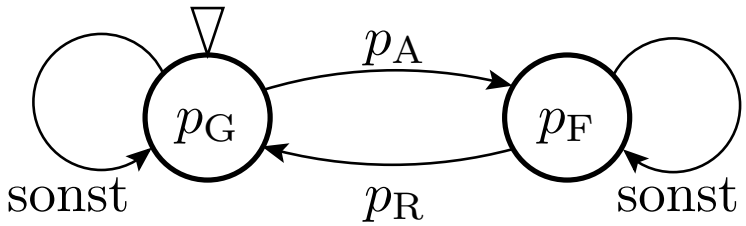
Daraus ablesbar:Die mittlere Anzahl $E(N_1)$, dass nach zwei richtigen Eingaben eine falsche folgt, strebt gegen einen Wert < 1.

- Die mittlere Nachweisdauer $n - E(N_2)$ strebt gegen $\approx 100 - 65 = 35$

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

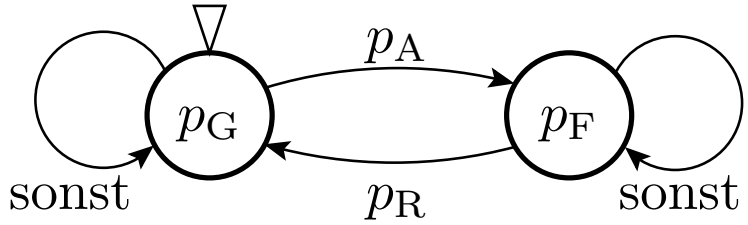
Reparaturprozess als Markov-Kette

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):

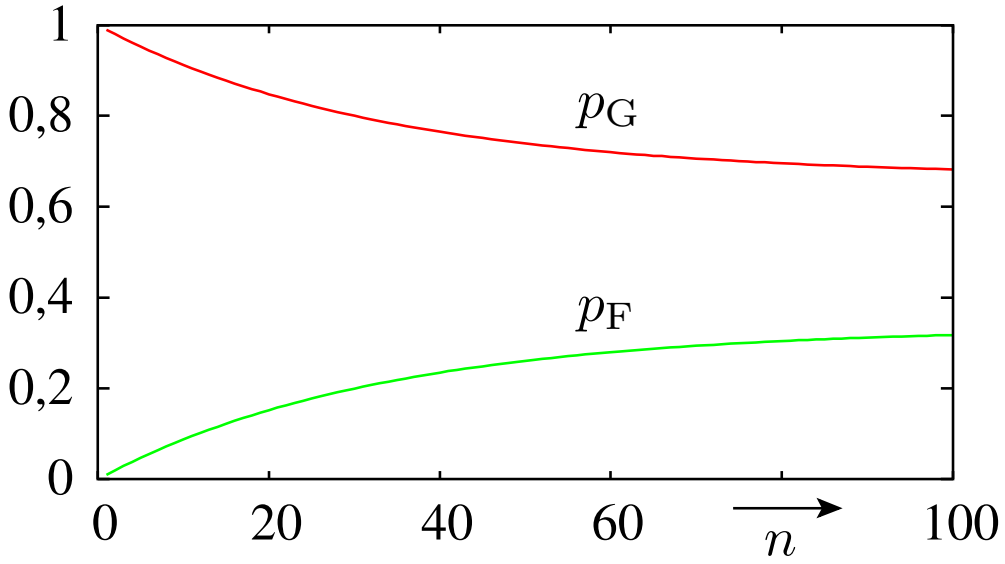


Beschreibung als simulierbares Gleichungssystem:

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



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

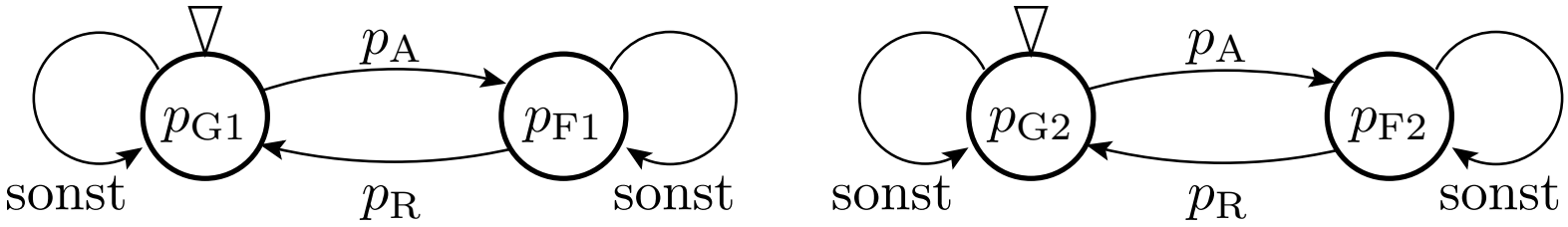


Für große n strebt der Reparaturprozess gegen den stationären Zustand:

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

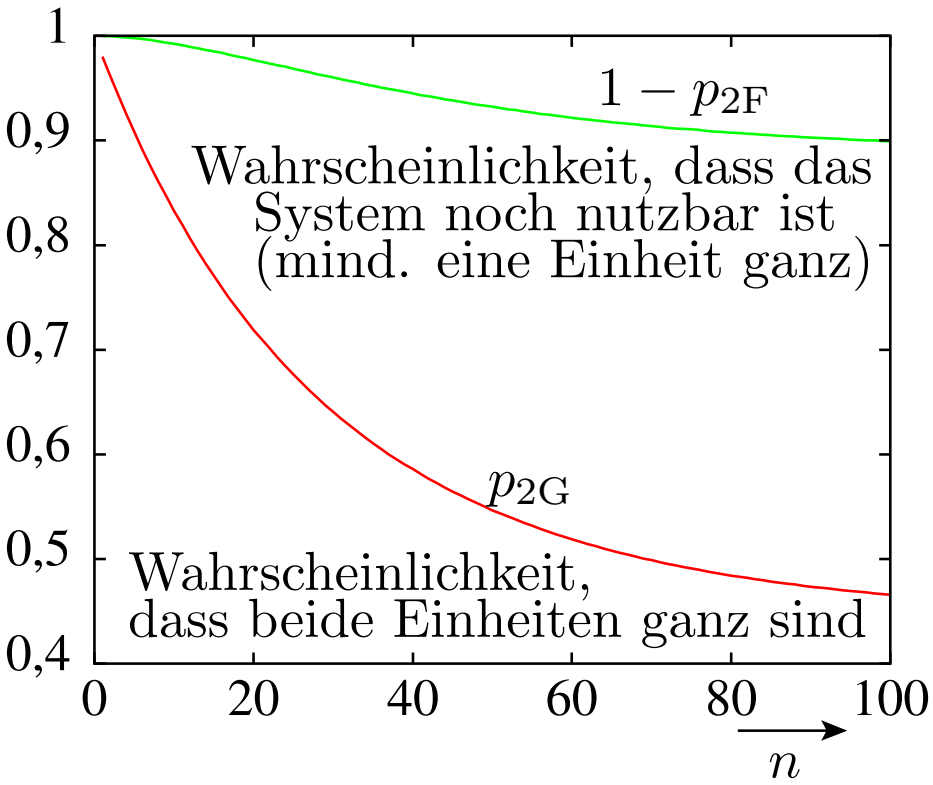
Reparatur mit Redundanz

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 idx=1:100
  Z = M * Z;
  p2G(idx)=Z(1)**2; % beide Einheiten ganz
  p2F(idx)=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

Kenngrößen der Verlässl.

Kenngrößen der Verlässlichkeit

Kenngrößen der Verlässlichkeit werden aus Zählwerten und gemessenen Zeiten abgeschätzt. Es wird unterschieden zwischen

- Eintrittswahrscheinlichkeiten,
- mittleren Zeiten zwischen / bis zum eintreten, ...

Für Eintrittswahrscheinlichkeiten nahe 100% ist aus »emotionaler Sicht« der Kehrwert der Gegenwahrscheinlichkeit ausdrucksstärker. Aus einer Wahrscheinlichkeit für die Zuverlässigkeit

$$p_{\mathrm{Z}} \approx \frac{999}{1000}\left[\frac{\mathrm{KS}}{\mathrm{SL}}\right] \approx 1$$

wird die Kenngröße »Zuverlässigkeit«

$$Z = \frac{1}{1-p_{\mathrm{Z}}} \approx \frac{1}{1-p_{\mathrm{Z}} \approx \frac{999\,\mathrm{KS}}{1000\,\mathrm{SL}}} = 1000\,\frac{\mathrm{SL}}{\mathrm{FF}} \gg 1$$

(SL – Service-Leistungen; KSL – korrekte Service-Leistungen; FF – Fehlerfunktionen).

Service als Zufallsexperiment

Ein Service arbeitet Anfragen ab. Jede Anfrage ist ein Zufallsexperiment. Nach dem Service-Modell sind mögliche Ergebnisse

- NSL Keine Service-Leistung (Service nicht verfügbar),
- KSL Service korrekt ausgeführt,
- FF Fehlfunktion.

und optional eine Ausführungs- bzw. Nichtverfügbarkeitszeit.

Beispielprotokoll für eine Folge von 7 Service-Anforderungen:

	1	2	3	4	5	6	7	...
Ergebnis	KSL	KSL	FF	NSL	KSL	KSL	FF	...
Zeit	10 ms	25 ms	11 ms	30 ms	15 ms	18 ms	41 ms	...

Verfügbarkeit

Verfügbarkeit

Die Wahrscheinlichkeit der Verfügbarkeit ist der Anteil der Zeit, die ein Service verfügbar ist:

$$p_{\mathrm{V}} = \frac{MTBF_{\mathrm{V}}}{MTBF_{\mathrm{V}} + MTTR}$$

($MTBF_{\mathrm{V}}$ Mean Time between Failures[13], mittlere Zeit zwischen zwei Nichtverfügbarkeiten abzüglich der Wiederherstellung der Betriebsbereitschaft; $MTTR$ – Mean Time to Repair, mittlere Zeit für die Wiederherstellung der Betriebsbereitschaft (Reparatur- + Wiederanlaufzeit). Verfügbarkeit als positiv motivierte Zahl:

$$V = \frac{1}{1 - p_{\mathrm{V}}} \quad \text{Masseinheit}: \ [V] = \frac{\mathrm{SA}}{\mathrm{NSL}}$$

(SA – Service-Anfragen; NSL – davon nicht erbracht).

[13] »Failures« sind hier Ereignisse, nach denen das System nicht verfügbar ist, z.B. durch Ausfälle oder Abstürze. Nach ihnen folgt eine Reparaturzeit und/oder Wiederanlaufzeit (Neustart, Datenwiederherstellung, ...).

Abschätzung der Verfügbarkeit am Beispiel

	1	2	3	4	5	6	7	...
Ergebnis	SL	SL	SL	NSL	SL	SL	NSL	...
Zeit	10 ms	25 ms	11 ms	30 ms	15 ms	19 ms	20 ms	...

$$MTBF_{\mathrm{V}} \approx \frac{10\,\mathrm{ms} + 25\,\mathrm{ms} + 11\,\mathrm{ms} + 15\,\mathrm{ms} + 19\,\mathrm{ms}}{2} = \frac{80\,\mathrm{ms}}{2}$$

$$MTTR \approx \frac{30\,\mathrm{ms} + 20\,\mathrm{ms}}{2} = \frac{50\,\mathrm{ms}}{2}$$

Wahrscheinlichkeit der Verfügbarkeit:

$$p_{\mathrm{V}} = \frac{MTBF_{\mathrm{V}}}{MTBF_{\mathrm{V}} + MTTR} \approx \frac{40\,\mathrm{ms}}{65\,\mathrm{ms}} = 61{,}5\%$$

Verfügbarkeit in Service-Anfragen je nicht erfüllte SL:

$$V = \frac{1}{1 - p_{\mathrm{V}}} \approx \frac{1}{1 - 61{,}5\%} = 2{,}6\,\frac{\mathrm{SA}}{\mathrm{NSL}}$$

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 $MTBF_\mathrm{V}$ dafür mindestens sein?

Lösung

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

Zuverlässigkeit

Zuverlässigkeit

Die Wahrscheinlichkeit, dass ein System zuverlässig ist, ist die bedingte Wahrscheinlichkeit, dass die Ergebnisse eines geleisteten Service korrekt sind, 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-Leitungen; KSL – korrekte SL; FF – Fehlfunktion).
Alternative Abschätzung aus der zuverlässigkeitsbezogenen $MTBF_{\mathrm{Z}}$:

$$p_{\mathrm{Z}} \approx 1 - \frac{MTS}{MTBF_{\mathrm{Z}}} \tag{6}$$

($MTBF_{\mathrm{Z}}$ – mittlere betriebsbereite Zeit zwischen zwei FF; MTS – mittlere Service-Dauer).

Zuverlässigkeit als positiv motivierte Zahl:

$$Z = \frac{1}{1 - p_{\mathrm{Z}}} \quad \text{Masseinheit}: \; [Z] = \frac{\mathrm{SL}}{\mathrm{FF}} \tag{7}$$

(SL – Service-Leitungen; FF – Fehlfunktionen).

Abschätzung der Zuverlässigkeit am Beispiel

	1	2	3	4	5	6	7	...
Ergebnis	KSL	KSL	FF	NSL	KSL	KSL	FF	...
Zeit	10 ms	25 ms	11 ms	30 ms	15 ms	18 ms	41 ms	...

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

$$MTS \approx \frac{10\,\text{ms} + 25\,\text{ms} + 11\,\text{ms} + 15\,\text{ms} + 18\,\text{ms} + 41\,\text{ms}}{6} = 20\,\text{ms}$$

Wahrscheinlichkeit der Zuverlässigkeit:

$$p_Z \approx \frac{N_{\text{KSL}}}{N_{\text{SL}}} = \frac{4}{6};\ \text{bzw. } p_Z \approx 1 - \frac{MTS}{MTBF} = 1 - \frac{20\,\text{ms}}{60\,\text{ms}} = 66{,}7\%$$

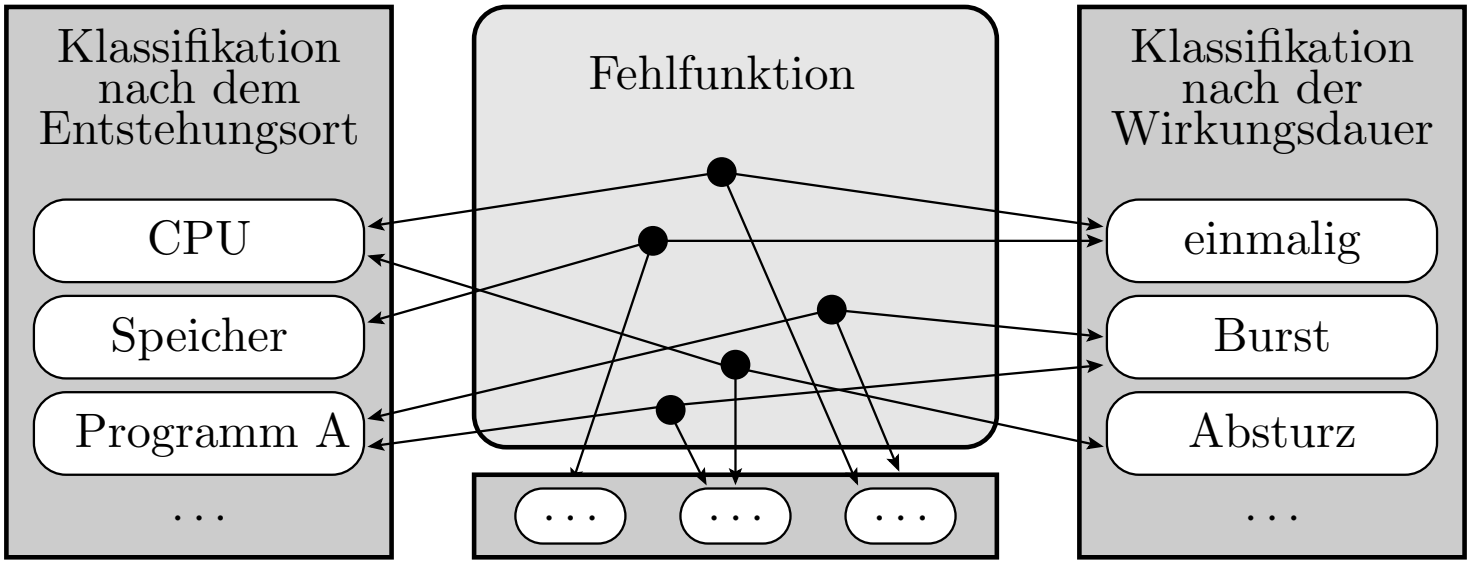
Zuverlässigkeit in Service-Leistungen je Fehlfunktion:

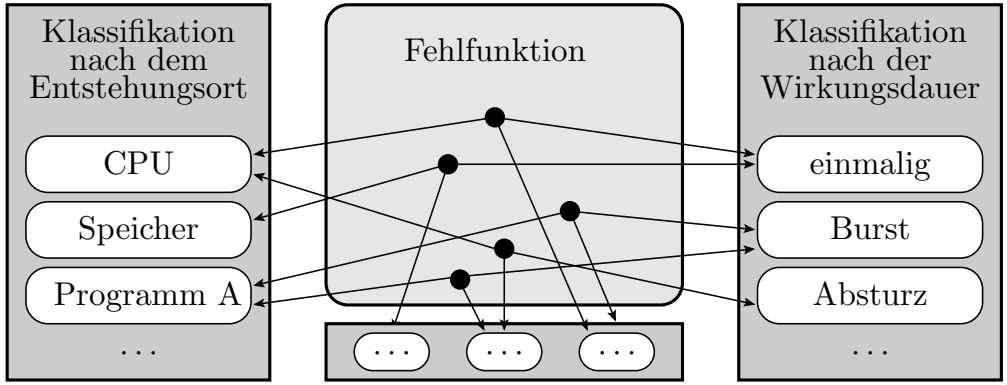
$$Z = \frac{1}{1 - p_V} \approx \frac{1}{1 - \frac{2}{3}} = 3\,\frac{\text{SL}}{\text{FF}}$$

Teilzuverlässigkeiten

Die Fehlfunktionen (FF) eines Systems lassen sich nach Ort, Ursache und 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 zuverlässigkeitsbezogene $MTBF_{\mathrm{Z}.i}$-Werte vor:

Teilsystem	Speicher	Prozessor	Software	Rest
$MTBF_{\mathrm{Z}.i}$	500 h	3.000 h	1000 h	2.000 h

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

1. Wie groß sind die vier aus den $MTBF_{\mathrm{Z}.i}$-Werten abschätzbaren Teilzuverlässigkeiten?
2. Wie groß ist die Zuverlässigkeit des Gesamtsystems?
3. Wie groß ist die Wahrscheinlichkeit einer Fehlfunktion des Gesamtsystems?

Lösungen

1. Teilzuverlässigkeiten ($MTS = 1\,\text{min}$):

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

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

2. Zuverlässigkeit des Gesamtsystems:

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

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

3. Wahrscheinlichkeit einer FF je SL des Gesamtsystems:

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

Sicherheit

Sicherheit

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 gefährlich):

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

Wahrscheinlichkeit, dass eine Service-Leistung sicher ist, abschätzbar aus dem Anteil der gefährlichen 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 – gefährliche FF).
Alternativ abschätzbar:

$$p_{\mathrm{S}} = 1 - \frac{MTS}{MTBF_{\mathrm{S}}} = 1 - p_{\mathrm{G}} \cdot \frac{MTS}{MTBF_{\mathrm{Z}}}$$

($MTBF_{\mathrm{S}} = \frac{MTBF_{\mathrm{Z}}}{p_{\mathrm{g}}}$ – sicherheitsbezogene $MTBF$, mittlere Zeit zwischen zwei gefählichen FF; MTS – mittlere Service-Dauer).

Sicherheit als positiv motivierte Zahl in Service-Leistungen je gefährliche Fehlfunktion:

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

(p_{S} – Wahrscheinlichkeit, dass eine SL sicher ist; Z – Zuverlässigkeit; p_{G} – Gefährdungswahrscheinlichkeit).

Sicherheit lässt sich auf zwei Wegen erhöhen:

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

Beispielaufgaben

Eine Fahrzeug habe eine zuverlässigkeitsbezogene $MTBF_{\mathrm{Z}} = 1000\,\mathrm{h}$ je Fehlfunktion. Die Wahrscheinlichkeit, dass eine FF die Betriebssicherheit gefährdet, sei $p_{\mathrm{G}} = 1\%$ und die mittlere Service-Dauer (mittlere Fahrtdauer) betrage $MTS = 1\,\mathrm{h}$.

1. Wie hoch sind die Zuverlässigkeit, die auf die Betriebssicherheit bezogene $MTBF_{\mathrm{S}}$ (mittlere Zeit zwischen zwei für die Betriebssicherheit gefährliche 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 Gl. 6 und Gl. 7:

$$Z = \frac{MTBF_{\mathrm{Z}}}{MTS} = \frac{10^3\mathrm{h}}{1\mathrm{h}} \cdot \frac{\mathrm{SL}}{\mathrm{FF}} = 10^3 \frac{\mathrm{SL}}{\mathrm{FF}}$$

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

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

Betriebssicherheit:

$$S = \frac{MTBF_{\mathrm{S}}}{MTS} \approx \frac{10^5\mathrm{h}}{1\mathrm{h}} = 10^5 \frac{\mathrm{SL}}{\mathrm{GFF}}$$

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:

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

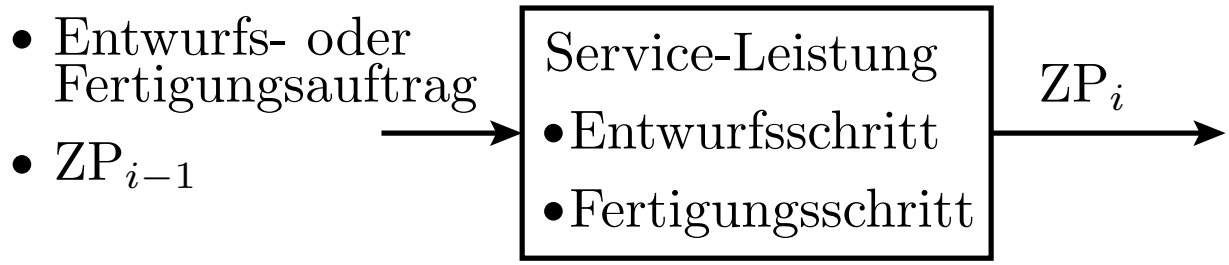
$$\begin{aligned} 5 \cdot S = 5 \cdot \frac{Z}{p_{\mathrm{G}}} \quad &\leq \quad S_{\mathrm{mSG}} = \frac{Z_{\mathrm{mSG}}}{p_{\mathrm{G.mSG}}} = \frac{10}{p_{\mathrm{G}}} \cdot \frac{1}{\frac{1}{Z} + \frac{1}{Z_{\mathrm{SG}}}} \\ \frac{Z}{2} \quad &\leq \quad \frac{1}{\frac{1}{Z} + \frac{1}{Z_{\mathrm{SG}}}};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

Das Steuergerät muss mindestens so zuverlässig wie das Fahrzeug sein.

Fehlerentstehung

Entstehungsprozesse als Service-Leistungen

Ein Entstehungsprozess besteht aus vielen Schritten:



Jeder Schritt

- startet mit einen Entwurfs- oder Fertigungsauftrag,
- hat als Eingabe Daten und Produkte ZP_{i-1} (Teilentwürfe, Komponenten, Material) mit potentiellen Fehlern,
- liefert als Ergebnis ein End- oder Zwischenprodukt für den Folgeschritt oder Endprodukt ZP_i, das die Fehler der Zwischenprodukte und die neu entstandenen Fehler enthält.

Erkannte fehlerhafte Produkte werden aussortiert oder repariert.

Verlässlichkeit von Entstehungsprozessen

Die Verlässlichkeit von einem »Entstehungs-Service« lässt sich genau wie für jeden anderen Service charakterisieren durch:

- seine Verfügbarkeit (Service-Anfragen je nicht erbrachte Service-Leistung),
- seine Zuverlässigkeit (Service-Leistungen je Fehlfunktion) und
- unterschiedliche Sicherheiten (SL je gefährliche FF).

Fehlfunktionen in einem Entstehungsprozess sind Produktfehler.

Produktfehlerbezogene Kenngrößen sind:

- Fehleranteil DL (Defect Level), Anteil der fehlerhaften Objekte,
- Ausbeute $Y = 1 - DL$ (Yield), Anteil der fehlerfreien Objekte,
- Fehleranzahl.

Fehleranzahl[14]

Anzahl der potentiellen Fehler, die entstanden, vorhanden, beseitigt, ... sind, bzw. Anzahl der kleinsten fehlerhaften lokalisierbaren Elemente.
Die Fehleranzahl wird aus Metriken für die Größe / Kompliziertheit von Entstehungsprozess und Produkt, z.B.

- für Programme die Anzahl der Programmzeilen ohne Leer- und Kommentarzeilen (NLOC, netto lines of code),
- für Schaltkreise die Transistoranzahl und die Anzahl der Signale,
- für Baugruppen die Anzahl der Bauteile und Verbindungen

und Gütekennwerten für den Prozess (z.B. NLOC je Fehler, Transistoren je Fehler, ...) abgeschätzt.

[14] Fehleranzahl erhält zur Abgrenzung von allen anderen Zählwerten, die mit $N_{\ldots}$ bezeichnet werden, als eigenes Symbol das φ, weil es in der Vorlesung im Weiteren sehr oft um die Anzahl der Fehler (entstanden, vorhanden, beseitigt, ...) gehen wird.

Fehleranteil, Ausbeute

Der Fehleranteil und die Ausbeute beziehen sich auf gefertigte Objekte mit nur einem potentiellen Fehler. Die Ausbeute ist hier die Wahrscheinlichkeit, dass der Entstehungsprozess zuverlässig ist, abschätzbar aus dem Anteil der fehlerfrei gefertigten Objekte:

$$Y = p_Z = 1 - \frac{1}{Z} \approx \frac{N_{KSL}}{N_{SL}}$$

Der Fehleranteil ist der Kehrwert der Prozesszuverlässigkeit, abschätzbar aus dem Anteil der fehlerhaft gefertigten Objekte:

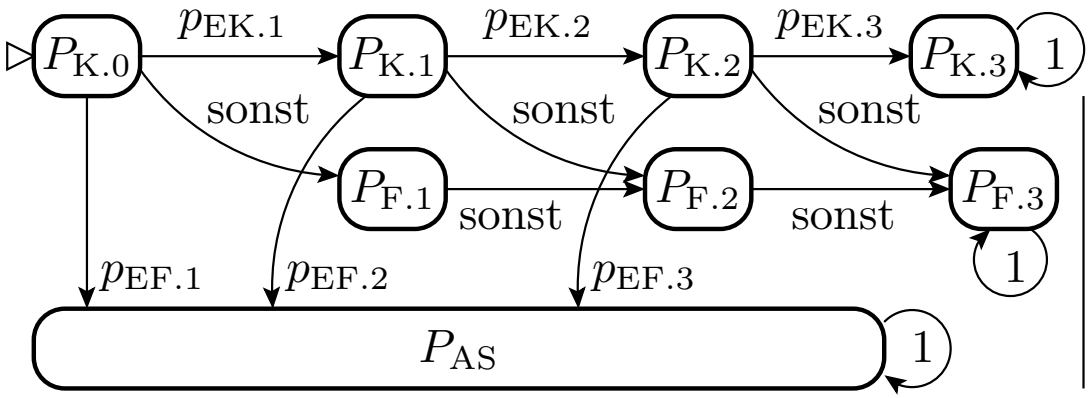
$$DL = 1 - Y = \frac{1}{Z} \approx \frac{N_{SL}}{N_{FF}}$$

(SL – (Entstehungs-) Service-Leistung; KSL – korrekte SL; FF – Fehlfunktion, Entstehung eines Objekts mit Fehler).

Die Ausbeute wird in % angegeben, der Fehleranteil in dpm (defects per million) oder dpu (defects per unit).

Entstehungsprozess als Markov-Kette

Für die Abschätzung der Zuverlässigkeit, des Fehleranteils, ... aus dem Prozessablauf eignen sich Markov-Ketten:



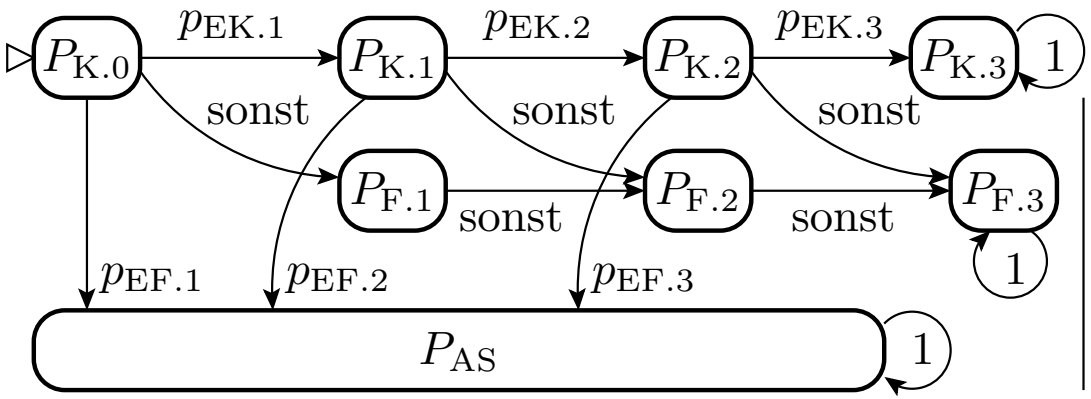
Zustände:

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

Der Beispielprozess hat $i = 1$ bis 3 Schritte, in denen

- mit einer Wahrscheinlichkeit $p_{EK.i}$ kein Fehler und
- mit $p_{EF.i}$ ein erkennbarer Fehler ensteht.

Zwischenprodukte mit erkennbarem Fehler werden aussortiert.



Zustände:

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

- Prozesszuverlässigkeit und Fehleranteil:

$$Z = \frac{P_{K.3} + P_{F.3}}{P_{F.3}}; \quad DL = \frac{1}{Z}$$

- Ausbeute, Wahrscheinlichkeit, dass der Prozess zuverlässig ist:

$$Y = p_Z = 1 - DL = 1 - \frac{1}{Z} = \frac{P_{K.3}}{P_{K.3} + P_{F.3}}$$

($P_{K.3}$ – Wahrsch. für das Entstehen eines fehlerfreien Produkts; $P_{F.3}$ – ~ eines fehlerhaften Produkts; P_{AS} – Wahrsch., dass kein Produkt entsteht).

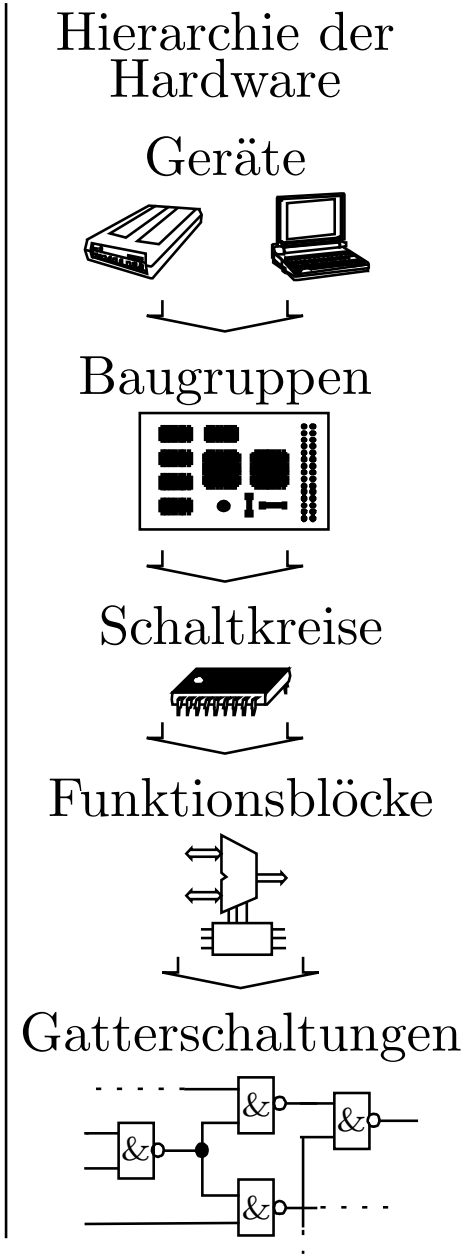
Entstehungsprozesse können Reparturiterationen enthalten.

Hierarchie als Fehlerbaum

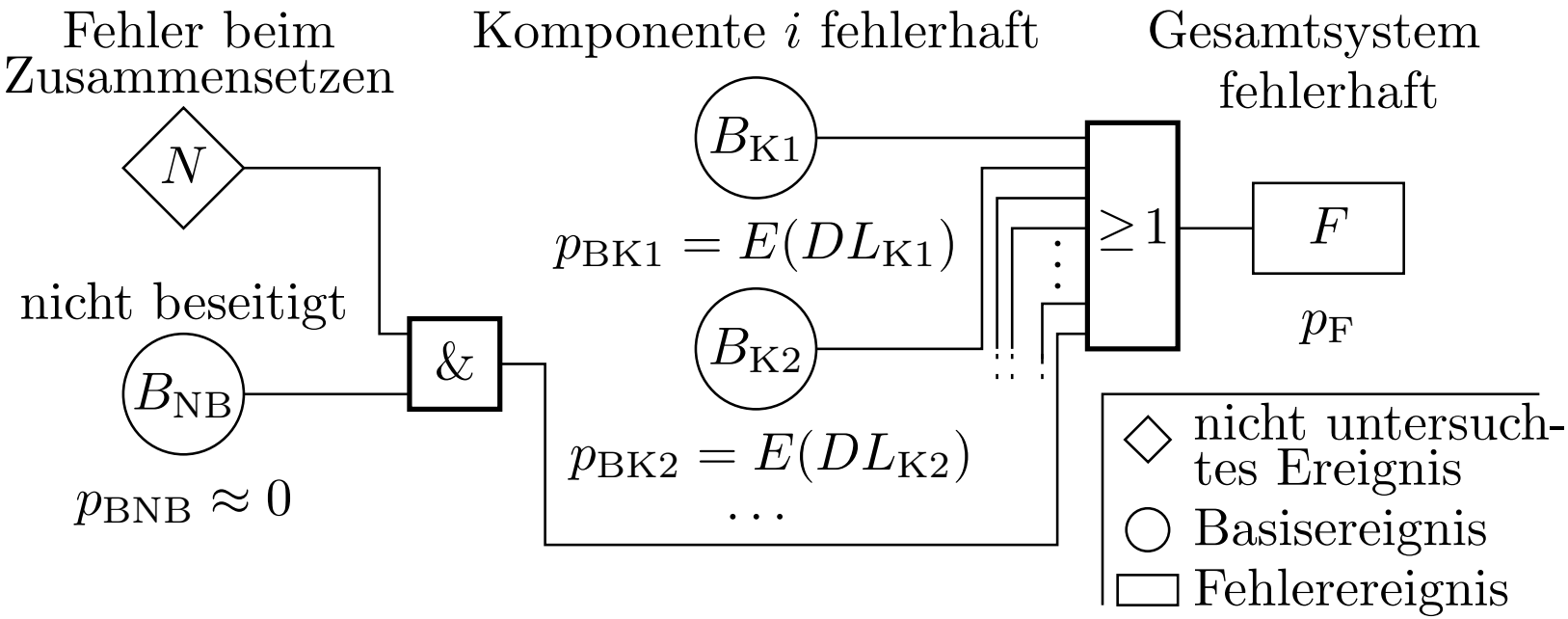
Fehlerbäume eignen sich zur Abschätzung von Fehlerentstehungswahrscheinlichkeiten aus der Hierarchie:

Ein übergeordneter Service wird korrekt ausgeführt, wenn

- *alle genutzten Teil-Service-Leistungen korrekt ausgeführt werden*
- *UND die Zwischenprodukte und Informationen korrekt weitergegeben werden,*
- *NOT <Bedingungen, die Korrektheit ausschließen>, ...*
  ODER <Alternativen für korrekte Ausführung>, ...



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).

Sicherung der Verlässl.

Sicherung der Verlässlässlichkeit

Die Sicherung der Verlässlichkeit erfolgt durch Kontrollen und Abstellung erkannter Probleme auf drei Ebenen:

- Fehlervermeidung: Kontrolle der Entstehungsprozesse und Produkte. Abstellung der Ursachen für die Fehlerentstehung.
- Fehlerbeseitigung: Kontrolle der Produkte und Beseitigung erkannter Fehler.
- Umgang mit Fehlfunktionen im Betrieb: Überwachung der Anwortzeit, Ein- und Ausgabeformat und -werte. Bei ausbleibender SL oder Fehlfunktion Schadensbegrenzung, Neustart, Wiederholung, ..., Korrektur.

Die Kontrollen und Reaktionen auf Probleme sind Service-Leistungen deren Verlässlichkeit sich wie bei allen anderen Service-Leistungen durch die Attribute Verfügbarkeit, Zuverlässigkeit und unterschiedliche Sicherheiten beschreiben lässt.

Überwachung

Überwachung

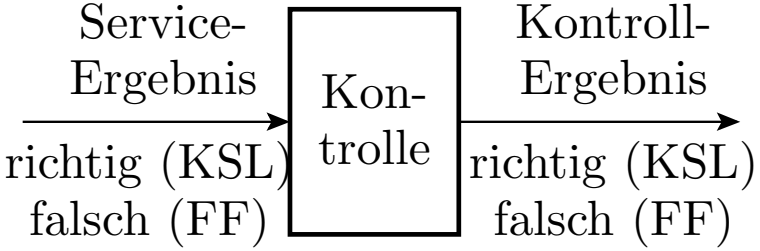
Überwachung kontrolliert die Ergebnisse von Service-Leistungen im laufenden Betrieb. Mögliche Service-Ergebnisse:

- NSL Keine Service-Leistung (Service nicht verfügbar),
- KSL korrekte Service-Leistung,
- FF Fehlfunktion.

Kontrolle auf »kein Ergebnis« erfolgt mit einer Zeitüberwachung. Die Ergebniskontrolle (Kontrolle auf »Service korrekt ausgeführt«) erfolgt mit:

- Formatkontrollen (Kontrolle auf Zulässigkeit) und
- Wertekontrollen (Kontrolle auf Richtigkeit).

Kenngrößen von Format- und Wertekontrollen



Service-Ergebnis	Kontroll-Ergebnis	Kontroll-Fehlfunktion
FF	FF	—
KSL	KSL	—
FF	KSL	Maskierung
KSL	FF	Phantom-FF

Erkennungswahrscheinlichkeit:

$$p_{\mathrm{E}} \approx \frac{N_{\mathrm{EFF}}}{N_{\mathrm{FF}}}$$

Maskierungswahrscheinlichkeit:

$$p_{\mathrm{M}} = 1 - p_{\mathrm{E}} \approx \frac{N_{\mathrm{MFF}}}{N_{\mathrm{FF}}}$$

Wahrscheinlichkeit für Phantomfehlfunktionen:

$$p_{\mathrm{Phan}} \approx \frac{N_{\mathrm{Phan}}}{N_{\mathrm{SL}}}$$

(FF – Fehlfunktionen; EFF – erkennbare FF; MFF – maskierte FF; Phan – Phantom-FF; SL – Service-Leistung).

Kontrollbedingte Schätzfehler für Zuverlässigkeiten

Die Zuverlässigkeitsabschätzung

$$Z \approx \frac{N_{\mathrm{SL}}}{N_{\mathrm{FF}}}$$

benötigt Zählwert für FF. Diese sind durch Kontroll-FF verfälscht. Im Mittel werden $p_{\mathrm{Phan}} \cdot N_{\mathrm{SL}}$ Phantomfehlfunktionen zu viel und $p_{\mathrm{M}} \cdot N_{\mathrm{FF}}$ nicht erkannte FF zu wenig gezählt:

$$N^*_{\mathrm{FF}} \approx N_{\mathrm{FF}} - p_{\mathrm{M}} \cdot N_{\mathrm{FF}} + p_{\mathrm{Phan}} \cdot N_{\mathrm{SL}}$$

Zuverlässigkeitsabschätzung mit Kompensation der Kontroll-FF:

$$\begin{aligned} N_{\mathrm{FF}} &\approx \frac{N^*_{\mathrm{FF}} - p_{\mathrm{Phan}} \cdot N_{\mathrm{SL}}}{1 - p_{\mathrm{M}}} = \frac{N^*_{\mathrm{FF}} - p_{\mathrm{Phan}} \cdot N_{\mathrm{SL}}}{p_{\mathrm{E}}} \\ Z &\approx \frac{p_{\mathrm{E}} \cdot N_{\mathrm{SL}}}{N^*_{\mathrm{FF}} - p_{\mathrm{Phan}} \cdot N_{\mathrm{SL}}} \end{aligned}$$

(SL – Service-Leistungen; N^*_{FF} – Anzahl der von der Kontrolle erkannten Fehlfunktionen). Abschätzungen von p_{Z}, $MTBF_{\mathrm{Z}}$, S, ... verlangen eine vergleichbare Kompensation für Kontroll-FF.

Beispielaufgabe

Mit einer Überwachung mit Erkennungswahrscheinlichkeit $p_{\mathrm{E}} = 80\%$ und einer Wahrscheinlichkeit, das eine SL eine Phantom-FF ist, von $p_{\mathrm{Phan}} = 6 \cdot 10^{-4}$ wurde eine zuverlässigkeitsbezogene $MTBF_{\mathrm{Z}}^{*} = 1000\,\mathrm{h}$ zwischen zwei bemerkten FF beobachtet. Mittlere Service-Dauer $MTS = 1\,\mathrm{h}$.

1. Wie groß ist die Anzahl der beobachteten FF in Abhängigkeit von der Anzahl der SL?
2. Wie groß ist die Anzahl der tatsächlichen FF in Abhängigkeit von der Anzahl der SL?
3. Wie groß sind die beobachtete und die tatsächliche Zuverlässigkeit?

Lösung

1. Zu erwartende Anzahl N^*_{FF} der zu beobachtenden FF in Abhängigkeit von der Anzahl der SL:

$$\frac{N^*_{\mathrm{FF}}}{N_{\mathrm{SL}}} \approx \frac{MTS}{MTBF^*_{\mathrm{Z}}}, \quad N^*_{\mathrm{FF}} \approx 10^{-3} \cdot N_{\mathrm{SL}}$$

2. Zu erwartende Anzahl N_{FF} der tatsächlichen FF in Abhängigkeit von der Anzahl der SL:

$$N_{\mathrm{FF}} \approx \frac{N^*_{\mathrm{FF}} - p_{\mathrm{Phan}} \cdot N_{\mathrm{SL}}}{p_{\mathrm{E}}} = \frac{\left(10^{-3} - 6 \cdot 10^{-4}\right) \cdot N_{\mathrm{SL}}}{80\%} \approx 5{\cdot}10^{-4} {\cdot} N_{\mathrm{SL}}$$

3. Scheinbare und tatsächliche Zuverlässigkeit:

$$\begin{array}{lcll} \frac{N_{\mathrm{SL}}}{N^*_{\mathrm{FF}}} & \approx & Z^* = 10^3 \, \frac{\mathrm{SL}}{\mathrm{FF}} & \text{(scheinbare Zuverlässigkeit)} \\ \frac{N_{\mathrm{SL}}}{N_{\mathrm{FF}}} & \approx & Z = 2 \cdot 10^3 \, \frac{\mathrm{SL}}{\mathrm{FF}} & \text{(tatsächliche Zuverlässigkeit)} \end{array}$$

Die tatsächliche Zuverlässigkeit ist im Beispiel doppelt so groß wie die scheinbare.

Test

Tests sind in dieser Vorlesung Kontrollen auf An-, bzw. Abwesenheit von Fehlern

- während oder nach Entstehungs-Service-Leistungen zur Prozesskontrolle und Fehlervermeidung,
- nach der Entstehung zur Fehlerbeseitigung,
- in Wartungsintervallen, um Fehler durch Ausfälle zu erkennen und zu beseitigen,
- nach beobachteten Fehlfunktionen zur Lokalisierung und Beseitigung der zugrunde liegenden Fehler.

Vollständiger Test unmöglich

Für den Nachweis, dass ein Service für alle Eingabedaten korrekte Ergebnisse liefert, müsste er mindestens mit allen Eingaben ausprobiert werden. Bereits ab wenigen Eingabebits unmöglich:

	m	2^m	t^*
Gatter, 4 Eingänge	4	16	16 µs
ALU, 68 Eingänge	68	$3 \cdot 10^{20}$	10^7 Jahre
vier Eingabevariablen vom Typ int32_t	128	$3 \cdot 10^{38}$	10^{25} Jahre

(m – Anzahl der Eingabebits; 2^m – Anzahl der Eingabemöglichkeiten; t^* – Testdauer bei einer Service-Ausführungszeit von 1µs.)

- Die meisten Systeme verarbeiten mehr als 128 Eingabebits.
- Hinzu kommen oft tausende oder mehr gespeicherte Bits.
- Die geschätzte Zeit seit dem Urknall ist nur $14 \cdot 10^9$ Jahre.

Kenngrößen und Testarten

- Fehlerüberdeckung, Anteil der nachweisbaren Fehler:

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

  (φ – Anzahl der vorhandenen; φ_{Erk} – ... der erkannten Fehler).
- Erkennungswahrscheinlichkeit, abschätzungsweise FC:

$$p_{\mathrm{E}} \approx FC$$

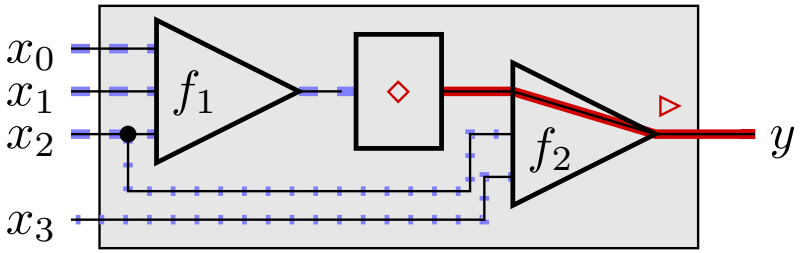
Testarten:

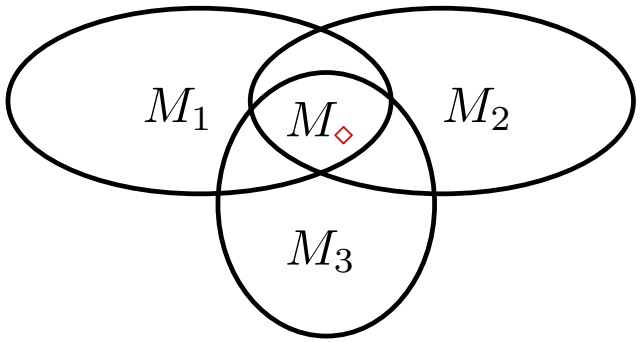
- statische Tests: direkte Kontrollen auf Fehler (Syntaxfehler, Suche nach Kurzschlüssen, ...),
- dynamische fehlerorientierte Tests: Test mit Beispieleingaben, die gezielt für Modellfehlern ausgewählt werden,
- Zufallstest: dynamische Test mit zufälligen Eingaben.

Fehlernachweis mit dynamischen Tests

Der Nachweis eines lokalen Fehlers in einem System verlangt Testeingaben, die

- den Fehler anregen (lokale Datenverfälschung bewirkt) und
- einen Beobachtungspfad erzeugen, entlang dem sich die Verfälschung zu einem beobachtbaren Ausgang fortplanzt.





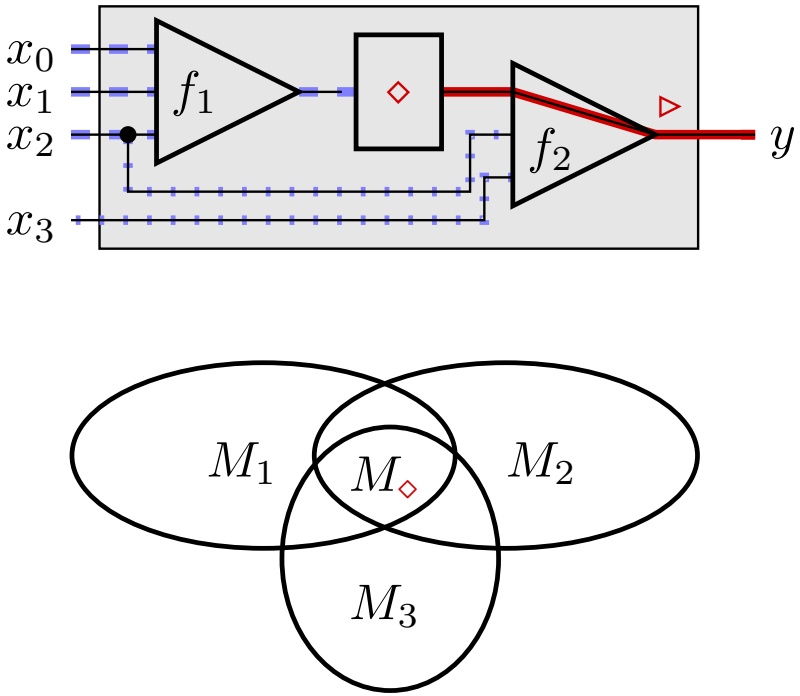
◇ Fehler
▷ Fehlfunktion (Datenverfälschung)
Eingaben zur Fehleranregung
Einstellen der Beobachtbarkeit
Beobachtungspfad

M_1 Eingabemenge, mit der der Fehler angeregt wird

M_2 Eingabemenge, bei der der Fehlerort beobachtbar ist

M_3 Eingabemenge für den lokalen Fehlernachweis

$M_\diamond$ Nachweismenge des Fehlers



◇ Fehler

▷ Fehlfunktion (Datenverfälschung)

Eingaben zur Fehleranregung

Einstellen der Beobachtbarkeit

Beobachtungspfad

M_1 Eingabemenge, mit der der Fehler angeregt wird

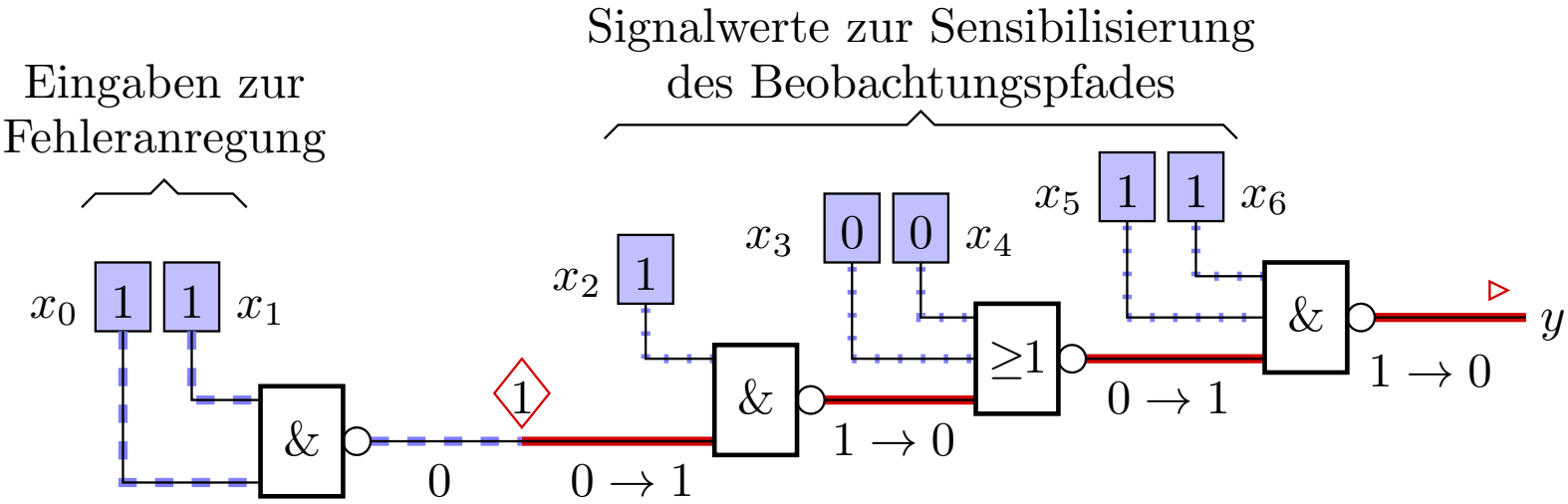
M_2 Eingabemenge, bei der der Fehlerort beobachtbar ist

M_3 Eingabemenge für den lokalen Fehlernachweis

$M_\diamond$ Nachweismenge des Fehlers

Die Nachweismenge eines (Modell-) Fehlers ist die Schnittmenge der Eingabemengen, die die einzelnen Nachweisbedingungen erfüllen.

Nachweisbedingungen in einer Gatterschaltung



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

Eingabemenge Fehleranregung: $M_1 = \{-----11\}$

Eingabemenge Beobachtbarkeit: $M_2 = \{11001--\}$

Fehlernachweismenge: $M_1 \cap M_2 = \{1100111\}$

Verallgemeinerung

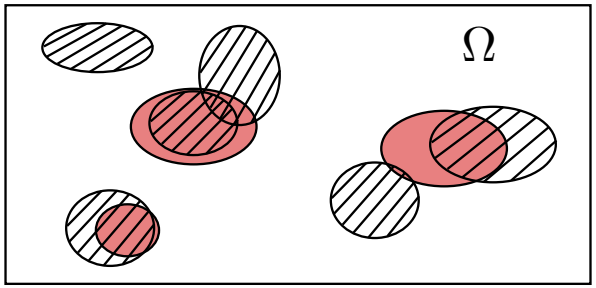
- Der Fehlernachweis kann auch von gespeicherten Zuständen abhängen. Anregung/Beobachtung über eine Eingabefolge.
- Der Fehlernachweis kann weiterhin von eingabeunabhängigen Bedingungen abhängen, z.B. Bereich der Versorgungsspannung, ...

Aufspaltung des Fehlernachweises in mehrere Einzelbedingungen:

$$\mathrm{x} \in (M_1 \cap M_2 \cap \ldots \neq \varnothing) \wedge B_1 \wedge B_2 \wedge \ldots$$

(M_i – Eingabemenge einer notwendigen Anregungs- oder Beobachtungsbedingung; B_i – eingabeunabhängige Nachweisbedingung; $\varnothing$ – leere Menge).

Geziele und zufällige Testauswahl



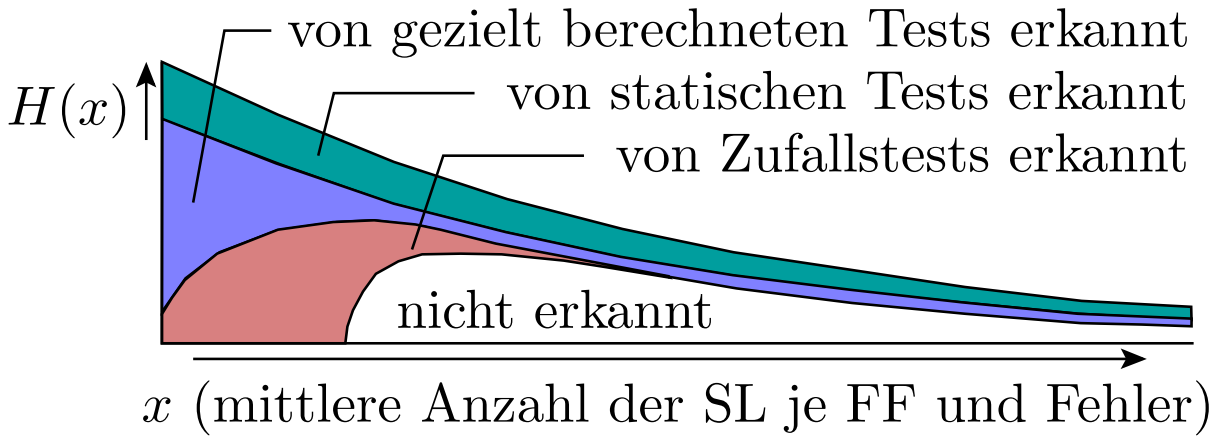
Ω Menge der Eingabewerte / Teilfolgen die einen Fehler nachweisen können

Nachweismenge eines Modellfehlers

Nachweismenge eines tatsächlichen Fehlers

- Ein Fehlermodell erzeugt viele Modellfehler.
- Alle potentiellen Fehler und alle Modellfehler haben Nachweismengen, die sich mehr oder weniger überschneiden.
- Gezielte Testauswahl sucht für jeden Modellfehler nach Tests und hofft, mit den Tests auch die tatsächlichen Fehler zu finden.
- Ein Zufallstest wählt die Tests, ohne die Nachweismengen der Modellfehler zu bevorzugen, sondern zählt nur die »Treffer« zur Abschätzung der Fehlerüberdeckung.

Testart und FHSF-Funktion



Jede Testart hat ihren speziellen Einfluss auf die FHSF-Funktion nach Beseitigung der erkennbaren Fehler:

- Statische Tests: Fehlernachweis weitgehend unabhängig davon, wie oft diese FF im Einsatz verursachen.
- Zufallstests: Es werden grob überschlagen alle Fehler mit $x \leq n$ beseitigt (n – Anzahl der Tests, Herleitung später).
- Gezielte Testauswahl: Fehler werden unabhängig bis bevorzugt mit zunehmender Häufigkeit von FF's im Einsatz erkannt.

Fehleranzahl und Zuverlässigkeit nach Beseitigung

Anzahl der nicht erkannten / beseitigten Fehler :

$$\varphi_{\mathrm{NErk}} = (1 - FC) \cdot \varphi$$

Für die fehlerbezogene Zuverlässigkeit als Kehrwert der Wahrscheinlichkeit einer FF je SL durch einen Fehler gilt, wenn

- Fehlernachweis unabhängigkeit von der Häufigkeit der FF im Einsatz (statische Tests):

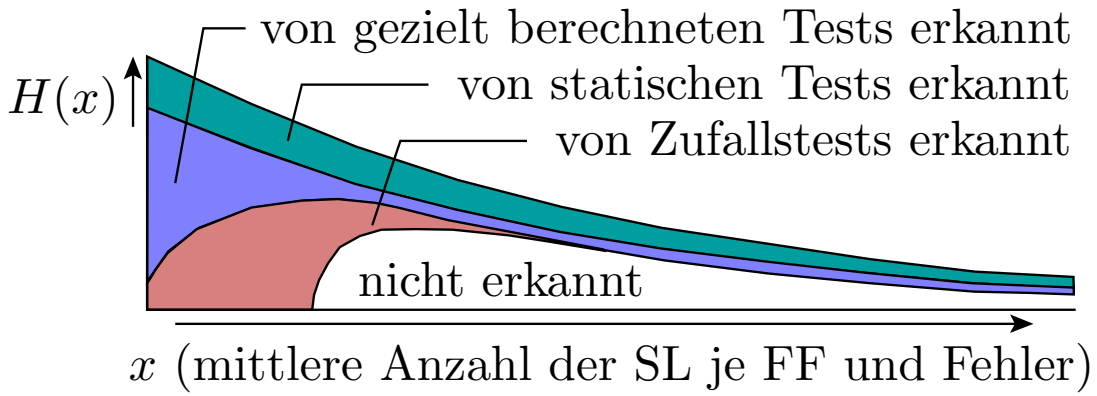
$$Z_{\mathrm{F}} \sim \frac{1}{\varphi_{\mathrm{NErk}}} \sim \frac{1}{1 - FC}$$

- Zufallstest:

$$Z_{\mathrm{F}} \sim \frac{n}{\varphi_{\mathrm{NErk}}} \sim \frac{n}{1 - FC}$$

Die Herleitung folgt auf Foliensatz 2.

Prüf- und Reparaturtechnologie



Die typische Prüf- und Reparaturtechnologie umfasst hierarchisch aufsteigend für alle getrennt testbaren Komponenten:

- statische Tests + Fehlerbeseitigung.
- fehlerorientiert ausgewählte Tests + Fehlerbeseitigung,
- Zufallstests + Fehlerbeseitigung.

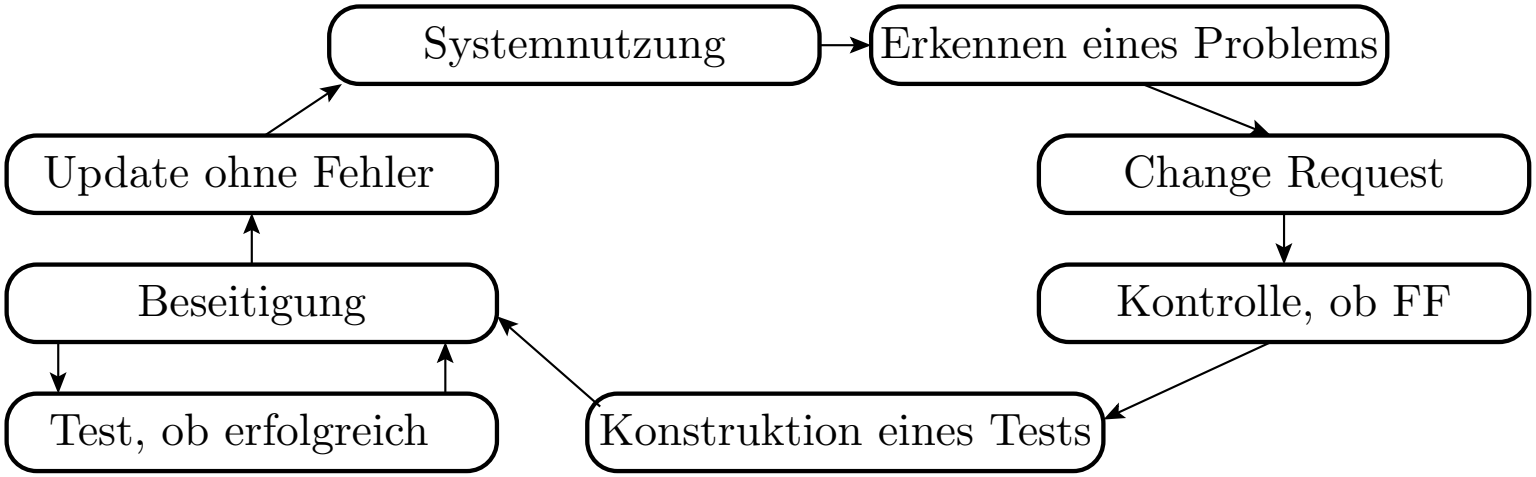
Nach den Herstellertests folgt oft ein Reifeprozess, in dem die Systeme mit Anwendungsdaten betrieben, FF erfasst und zu grunde liegende Fehler beseitigt werden (sehr langer Zufallstest).

Reifeprozesse

Reifeprozesse

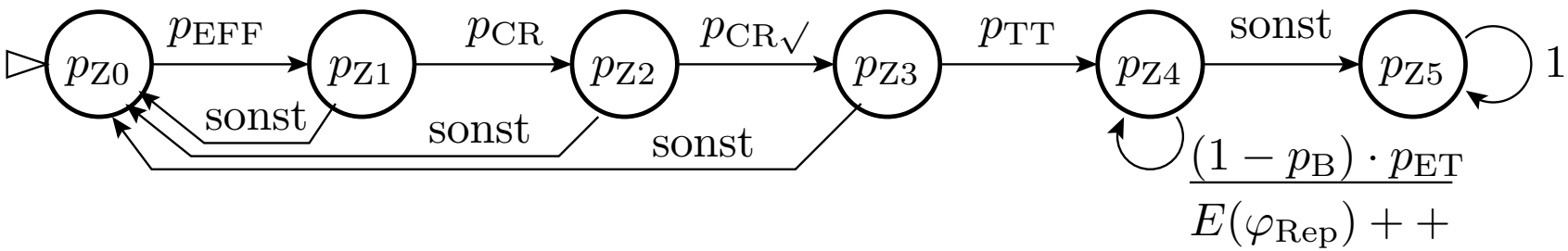
Ein Reifeprozess ist die Fortsetzung der Iteration aus Test und Fehlerbeseitigung für Entwurfsfehler großer Systeme im Einsatz.

- Die Anzahl der Entwurfsfehler in einem System nimmt mit der Systemgröße zu.
- Tests wirken wie Filter, die einen Anteil, aber nicht alle Fehler erkennen, so dass mehr gefundene auch mehr nicht gefundene Fehler erwarten lassen.
- Die Zunahme der Fehleranzahl lässt sich nicht ausreichend durch mehr / bessere Herstellertests kompensieren.
- Einbeziehung der Nutzer als Tester.



- Bei einer vermuteten Fehlfunktionen stellt der Anwender einen Änderungsanforderung (Change Request).
- Der Hersteller prüft diese, selektiert daraus FFs und versucht, für jede FF reproduzierbare Testbeispiele zu finden.
- Die Testbeispiele dienen zur Fehlerlokalisierung und zur Erfolgskontrolle nach jedem Beseitigungsversuch.
- Fehlerbeseitigung beim Nutzer erfolgt über Einspielen von Updates, in seltenen Ausnahmen über eine Rückrufaktion für Hardware oder komplette Geräte.

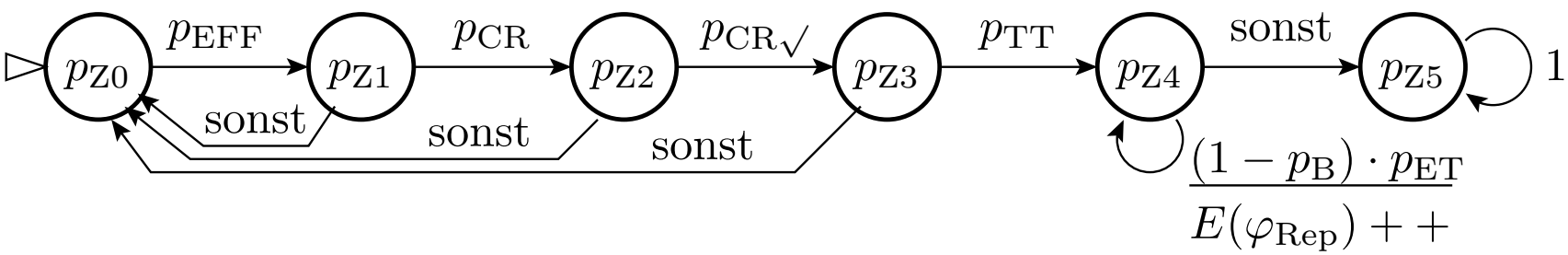
Reifeprozess für einen Fehler als Markov-Kette



p_{EFF}	Fehlererkennungswahrscheinlichkeit	Z_0	System mit Fehler i
p_{CR}	Wahrsch. Change Request gestellt	Z_1	Change Request gestellt
$p_{CR\surd}$	Wahrsch., dass als FF eingestuft	Z_2	Fehlfunktion bestätigt
p_{TT}	Wahrsch. Test konstruierbar	Z_3	Test gefunden
p_{ET}	Erkennungswahrscheinlichkeit des Tests	Z_4	Beseitigungsversuch
p_B	Beseitigungswahrscheinlichkeit	Z_5	Fehler i beseitigt
φ_{Rep}	Anzahl der bei einem Reperaturversuch entstehenden neuen Fehler		

Die Wahrscheinlichkeit, dass ein Fehler beseitigt wird, ist das Produkt der Wahrscheinlichkeiten, dass

- der Fehler bei irgend einem Anwender eine FF verursacht,
- ein Änderungsantrag (Change Request) gestellt, ...



- ...
- der Hersteller die FF bestätigt,
- einen Test für ihren Nachweis findet,
- die Beseitigungsiteraton erfolgreich ist.

- Bei den Fehlerbeseitigungsversuchen und anderen Verbesserungsversuchen entstehen neue Fehler.
- Wenn mehr Fehler beseitigt werden als neue entstehen, reift das System.
- Reifen ist erkennbar an einer mit der Nutzungsdauer abnehmenden Häufigkeit der beobachtbaren Fehlfunktionen (Bedienprobleme, Abstürze, falsche Ergebnisse, ...).

Anmerkungen

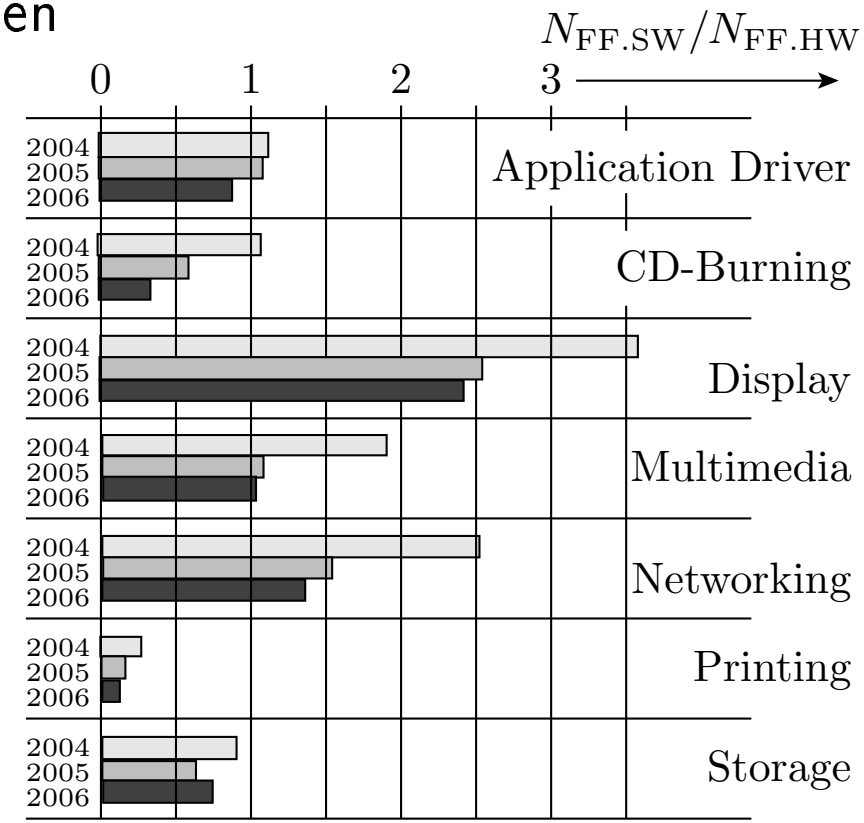
- Bei einem Reifeprozess nimmt die Zuverlässigkeit mit der akkumulierten Nutzungsdauer zu.
- Wichtig für die Geschwindigkeit eines Reifeprozesses sind der Informationsfluss über bemerkte FFs von den Anwendern zum Hersteller und ausreichend Bearbeitungskapazität des Herstellers für die Fehlerbeseitigung.
- Systeme, die lange gereift sind, haben hohe, auf anderem Wege schwer zu erreichende Zuverlässigkeiten. Schwer ersetzbar durch neue Systeme. (siehe Y2K[15] -Problem).
- Neue (innovative) Systeme sind in den ersten Nutzungsjahren vielfach unzuverlässer als die zuvor genutzten Systeme. Wenn das die Akzeptanz beeinträchtigt, reifen sie auch nicht ...

[15] Year 2000.

Zuverlässigkeitswachstum von Windows-Betriebssystemen[16]:

- Windows 98: $MTBF \approx 1$ Woche
- NT 4.0: $MTBF \approx 5{,}5$ Wochen
- Windows 2000 Professional: $MTBF \approx 4$ Monate.

Durch Treiber verursachten Abstürze unter Windows im Verhältnis zur Anzahl der durch Hardware-Fehler verursachen Abstürze[17].



[16] NSTL Test Report, Microsoft Windows 2000 Professional – Comparison of the Reliability of Desktop Operating Systems. Die Quelle sagt nicht, für welche Arten von FF die angegebenen MTBFs gelten.

[17] Glerum, K., Debugging in the (Very) Large: Ten Years of Implementation and Experience (2009), S. 11-14, Fig. 15