Test und Verlässlichkeit 2: Modellbildung Teil 2

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_F2.pdf)
10. November 2024

Inhalt Foliensatz TV_F2.pdf

2.1 Fehlerbeseitigung
2.1.1 Beseitigungsiteration
2.1.2 Fehlerdiagnose & -isolation
—— Vorlesung 5 (2.17) ——
2.1.3 Test
2.1.4 Vielfalt der Tests
2.1.5 Haftfehler
2.1.6 Defektanteil und Ausbeute
—— Vorlesung 6 (2.58) ——
2.2 Zuverlässigkeit und Test
2.2.1 Einfache Abschätzung
2.2.2 Verbessertes Modell
2.2.3 Vortests
2.2.4 Effektive Testanzahl
2.2.7 Reifen von Produkten
—— Vorlesung 7 (2.117) ——
2.3 Fehlervermeidung
2.3.1 Fehlerentstehung
2.3.2 Reifen von Prozessen
2.3.3 Vorgehensmodelle
2.3.4 Qualität und Kreativität

Fehlerbeseitigung

Wiederholung: Ursachen für Fehlfunktionen

- Fehler,
- Störungen (z.B. ein zufällig invertiertes Bit),
- Ausfälle.

Für Fehler lassen sich in der Regel Tests konstruieren, die sie reproduzierbar nachweisen, so dass der Beseitigungserfolg durch Testwiederholung kontrollierbar ist. Dafür sind die verursachten Fehlfunktionen meist nicht durch Wiederholung korrigierbar.

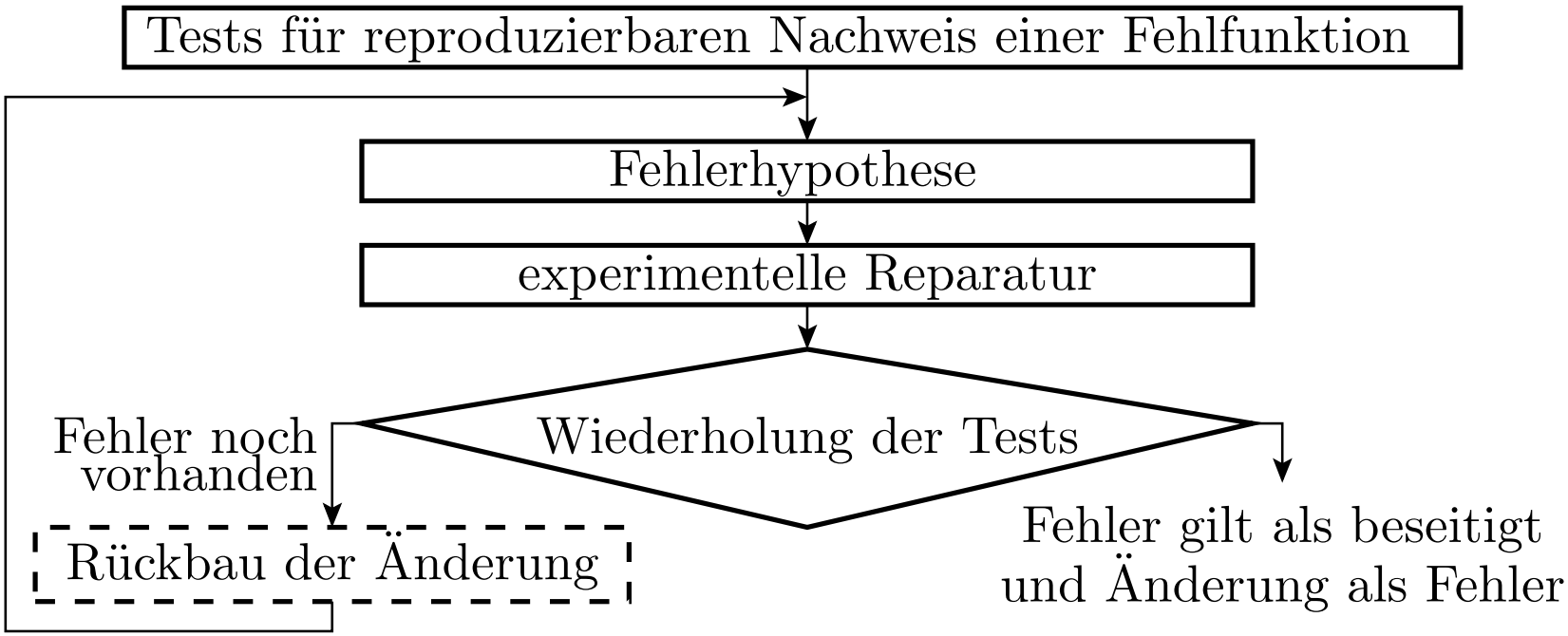
Störungen verursachen in der Regel diversitäre Fehlerfunktionen, die sich durch Wiederholung korrigieren lassen. Dafür Lokalisierung und Beseitigung der Ursache schwierig, da Wirkung nicht reproduzierbar.

Ausfälle sind Fehler, die während des Betriebs entstehen. Gefährdungsabwendung durch Fehlfunktionsbehandlung, Wartungstest, Redundanzen, ... (siehe später Abschn. 6.5).

Fehler sind die abstellbaren Probleme.

Beseitigungsiteration

Experimentelle Reparatur

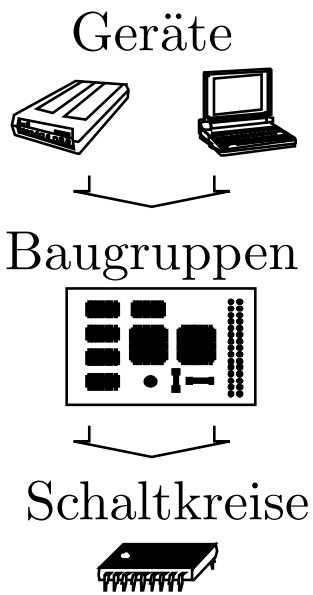


- Iteration aus Beseitigungsversuchen für hypothetische Fehler und Erfolgskontrolle durch Testwiederholung.
- Setzt deterministische Fehlerwirkung voraus und beseitigt alle vom Test nachweisbaren Fehler.
- Zur Vermeidung neu entstehender Fehler bei der Reparatur, Rückbau nach erfolglosen Reparaturversuchen.

Reparatur bei wenig tauschbaren Komponenten

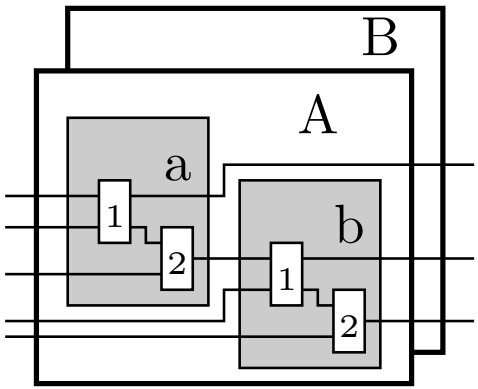
Ein reparaturgerechtes System hat eine hierarchische Struktur aus tauschbaren Komponenten, z.B.

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

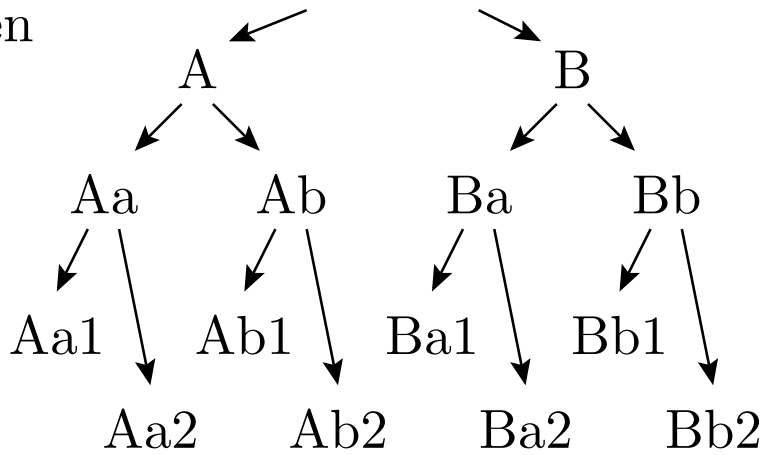


Fehlerlokalisierung durch systematisches Tauschen:

hierarchisches System mit tauschbaren Komponenten



Tauschbaum



Übliches Vorgehen eines Reperateurs

- Grobabschätzung, welches Rechnerteil defekt sein könnte aus den Fehlersymptomen*.
- Kontrolle der Steckverbinder auf Kontaktprobleme durch Abziehen, Reinigen, Zusammenstecken, Testwiederholung.
- Ersatz möglicherweise defekter Teile durch Ersatzteile, Testwiederholung, ...

Voraussetzungen:

- Wiederholbare Tests, die den Fehler nachweisen.
- Ausreichend Ersatzteile. Allgemeine Mechnikerkenntnisse*.

Fragen:

- Günstig ist der Tausch der Hälfte, von der fehlerhaften Hälfte auch die Hälfte, ... Warum?
- Kann man so auch Fehler in SW suchen, wenn ja, was für Fehler?

* Verständnis der kompletten Funktion des zu reparierenden Systems ist nicht zwingend.

Fehlerdiagnose & -isolation

Fehlerdiagnose

Abschätzung von Ort-, Ursache und Beseitigungsmöglichkeiten von Fehlern aus Testergebnissen zur Minderung:

- der Anzahl der Reparaturversuche,
- des Bedarf an Ersatzteilen,
- der Anzahl der bei Reparaturversuchen entstehenden Fehler
- inc. der, die nicht durch Rückbau beseitigt werden.

Allgemeine Diagnosetechniken:

- erfolgsorientiertes Tauschen und
- Rückverfolgung von Verfälschungen entgegen dem Daten- oder Berechnungfluss.

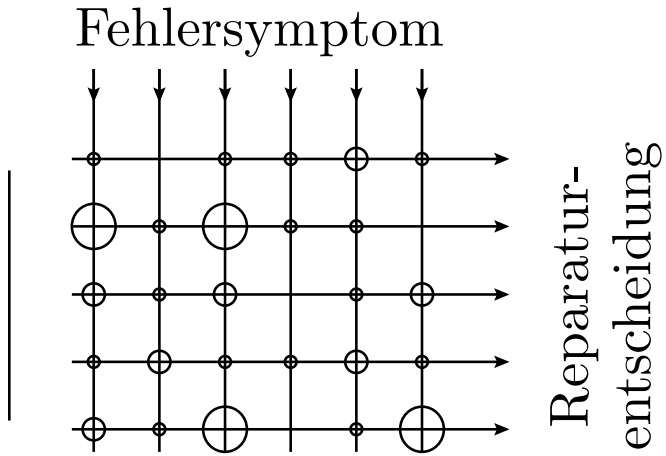
Voraussetzung ist ein prüf- und reparaturgerechter Entwurf.

Erfolgsorientiertes Tauschen

Produkte haben Schwachstellen. Die meisten Probleme geht auf einen kleinen Anteil der möglichen Ursachen zurück, Pareto-Prinzip*:

- Zählen der Erfolge unterschiedlicher Reparaturalternativen.
- Bei Reparatur, Beginn mit der erfolgsversprechendsten Möglichkeit.

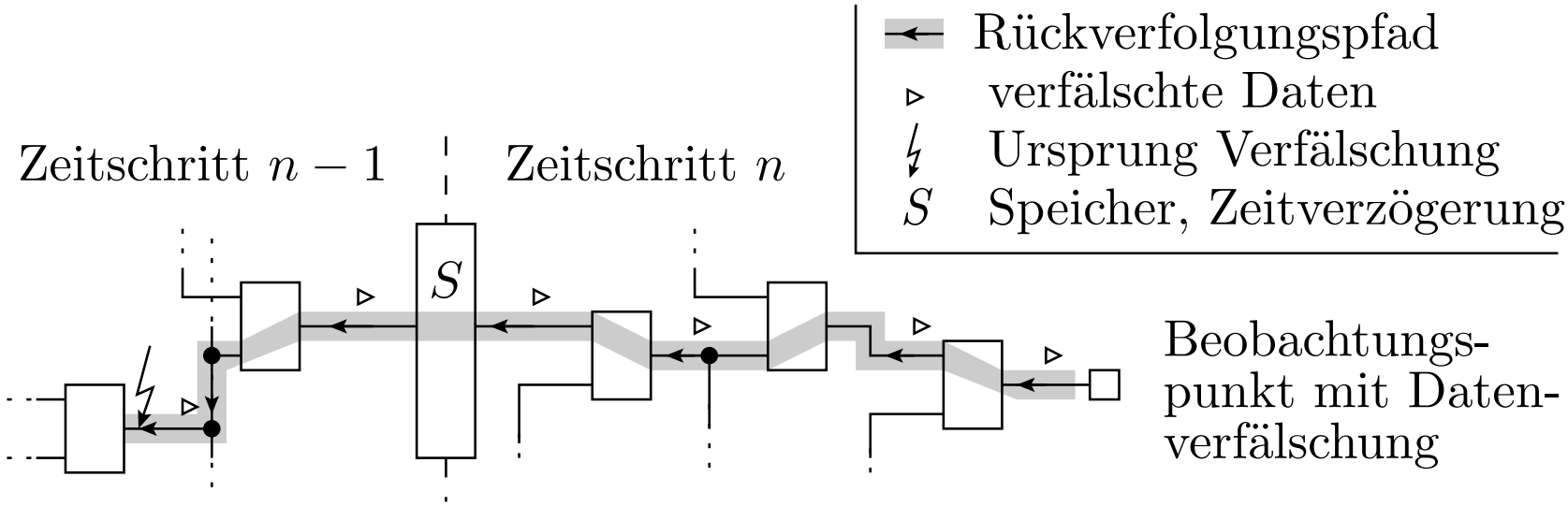
◎ Häufigkeit, mit der die Reparaturentscheidung für das Symstem bisher erfolgreich war



Nach erfolglosen Reparaturversuchen Rückbau der Änderung zur Minderung der Fehlerentstehungsrate bei der Reparatur.

* Der italienische Ökonom Vilfredo Pareto untersuchte 1906 die Verteilung des Grundbesitzes in Italien und fand heraus, dass ca. 20% der Bevölkerung ca. 80% des Bodens besitzen. Das ist in den Sprachgebrauch als Pareto-20%-80%-Regel eingegangen.

Rückverfolgung von Datenverfälschungen



Ausgehend von einer erkannten falschen Ausgabe Rückverfolgung entgegen Berechnungs- bzw. Signalfluss bis zu der Komponente, die richtige Eingaben auf verfälschte Ausgaben abbildet, gegebenenfalls über Zeitschritte und/oder hierarchisch absteigend.

Quelle der Verfälschung kann außer der gefundenen Komponente bei HW z.B. auch ein Kurzschluss oder bei SW ein fehlgeleiteter Schreibzugriff sein.

Reparatur- und prüfgerechter Entwurf

Sammlungen von

- Regeln »of good practise«, zur Ermöglichung / Vereinfachung von Test, Fehlerlokalisierung und Reparatur und
- Antipattern (typ. Vorgehensfehler, die Probleme verursachen).

Einige Regeln »of good practise«:

- Modulares System aus tauschbaren / seperat testbaren Funktionsblöcken.
- Deterministisches Verhalten mit gerichtetem Berechnungsfluss.
- MF-Isolation zur Verhinderung der Ausbreitung von Fehlfunktionen über Modulgrenzen.

Hässlichstes Antipattern:

- »Big ball of mud«: großes, unstrukturiertes, mangelhaft dokumentiertes System, das niemand mehr richtig versteht.

Fehlerisolation

Verhinderung des Übergreifens von Fehlfunktionen auf andere Teilsysteme:

- Physikalische und räumliche Trennung von Teilsystemen zur Minderung des Risikos übereinstimmender MF-Ursachen (gemeinsame Fehler, zeitgleicher Ausfälle, ...).
- Beschränkung von MF-Ausbreitung auf den Informations- und Verarbeitungsfluss.
- Keine Zugriffmöglichkeit auf Daten und Resourcen anderer Funktionseinheiten außer über definierte Schnittstellen.
- Verhinderung, dass fehlerhaft arbeitende Teilsysteme korrekt arbeitende Teilsysteme beeinträchtigen können.

Wichtiges Gestaltungsprinzip für

- Betriebssysteme,
- eingebettete Systeme,
- verteilte Systeme,
- sicherheitskritische Systeme, ...

Blindfehlersuche

Die Alternative zum systematischen Tauschen mit oder ohne Fehlerdiagnose ist ein »Blindfehlersuche«, d.h. ein intuitives Probieren.

Aufwändig, oft nicht erfolgreich, frustrierend aber:

- bei fehlenden Tauschmöglichkeiten,
- keiner Möglichkeit zur Rückverfolgung,
- fehlender Quallifikation oder fehlenden Dokumentationen

die einzige Möglichkeit der Fehlerbeseitigung.

Die Vorlesung unterstellt einen reparatur- und prüfgerechten Entwurf, der es ermöglicht, alle erkennbaren Fehler zu beseitigen.

Test

Testen

Verfahren zum Aufspühren von Fehlern. Grundeinteilung:

- Statische Tests: direkte Kontrolle von Merkmalen.
- Dynamische Tests: Ausprobieren der Funktion mit einer Stichprobe von Beispieleingaben.

Mit statischen Tests kontrollierbare Merkmale:

- Dokumentationen: Verständlichkeit, Vollständigkeit, ...
- Software: Syntax, statische Code-Analyse (Entwurfsregeln, Typenverträglichkeit, API-Benutzerregeln, ...).
- Leiterplatten: Widerstand entlang und zwischen Leitungen zum Ausschluss von Kurzschlüssen und Unterbrechungen.

Dynamische Tests erst am funktionierenden (Teil-) System möglich, statische Tests bereits nach einzelnen Entwurfs- und Fertigungsschritten.

IT-Systeme werden vor dem Einsatz in der Regel einer Vielzahl statischer und dynamischer Tests unterzogen.

Kenngrößen von Tests

Kein Test ist vollkommen. Jeder Test

- erkennt nur einen Teil der möglichen Fehler und
- ist selbst ein System mit begrenzter Zuverlässigkeit.

Kenngrößen zur Beschreibung der Güte von Tests:

- Fehlerabdeckung:

$$FC = \left.\frac{\#DF}{\#F}\right|_{\mathrm{ACR}} \tag{2.1}$$

- Phantomfehlerate, Anteil der korrekten Testerausgaben, die der Test als falsch klassifiziert:

$$\zeta_{\mathrm{PF}} = \left.\frac{\#PM}{N}\right|_{\mathrm{ACR}} \tag{2.2}$$

FC	Fehlerabdeckung (fault coverage), Anteil der nachweisbaren Fehler.
$\#F$, $\#DF$	Fehleranzahl, Anzahl der davon nachweisbaren Fehler.
ζ_{PF}	Phantomfehlerrate des Tests.
N, $\#PM$	Testanzahl, Anzahl der Phantomfehler.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

Umgang mit Phantomfehlern

Phantomfehler, z.B. durch falsche Sollwerte bei der Kontrolle von Testausgaben,

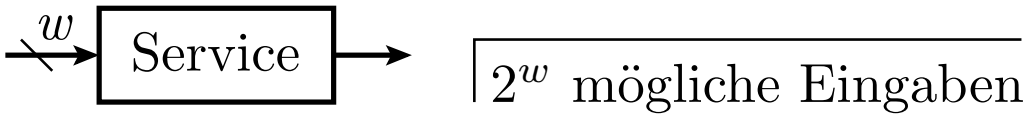
- starten überflüssige Beseitigungsiterationen,
- in denen neue nicht nachweisbare Fehler entstehen können.

Unsere idealisierte Fehlerkultur unterstellt, dass

- neu entwickelte Tests auf Phantomfehler gestetet und
- bei signalisierten Fehlern Phantomfehler ausgeschlossen werden.

Bei vernünftigem Umgang mit Phantomfehlern ist deren Einfluss auf die Verlässlichkeit vernachlässigbar.

Dynamische Tests



Dynamische Tests kontrollieren die Funktion nur für eine winzige Stichprobe der möglichen Eingaben.

	w	2^w	t_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*

t_T – Testzeit, wenn jeder Einzeltest $1\mu\mathrm{s}$ dauert.

- Die meisten Systeme verarbeiten $w \gg 100$ Eingabebits.
- Hinzu kommen oft tausende oder mehr gespeicherte Bits.

Vollständige Kontrolle mit allen Eingaben und Zuständen unmöglich!

w Anzahl der Eingabebits.

* Geschätzte Zeit seit dem Urknall nur $4 \cdot 10^9$ Jahre.

Testauswahl und Fehlerabdeckung

Die Fehlerabdeckung hängt von der Anzahl und der Auswahl der Testbeispiele ab.

Strategien der Testauswahl:

- fehlerorientiert,
- zufällig hinsichtlich der zu erwartenden Fehler oder
- Mischformen.

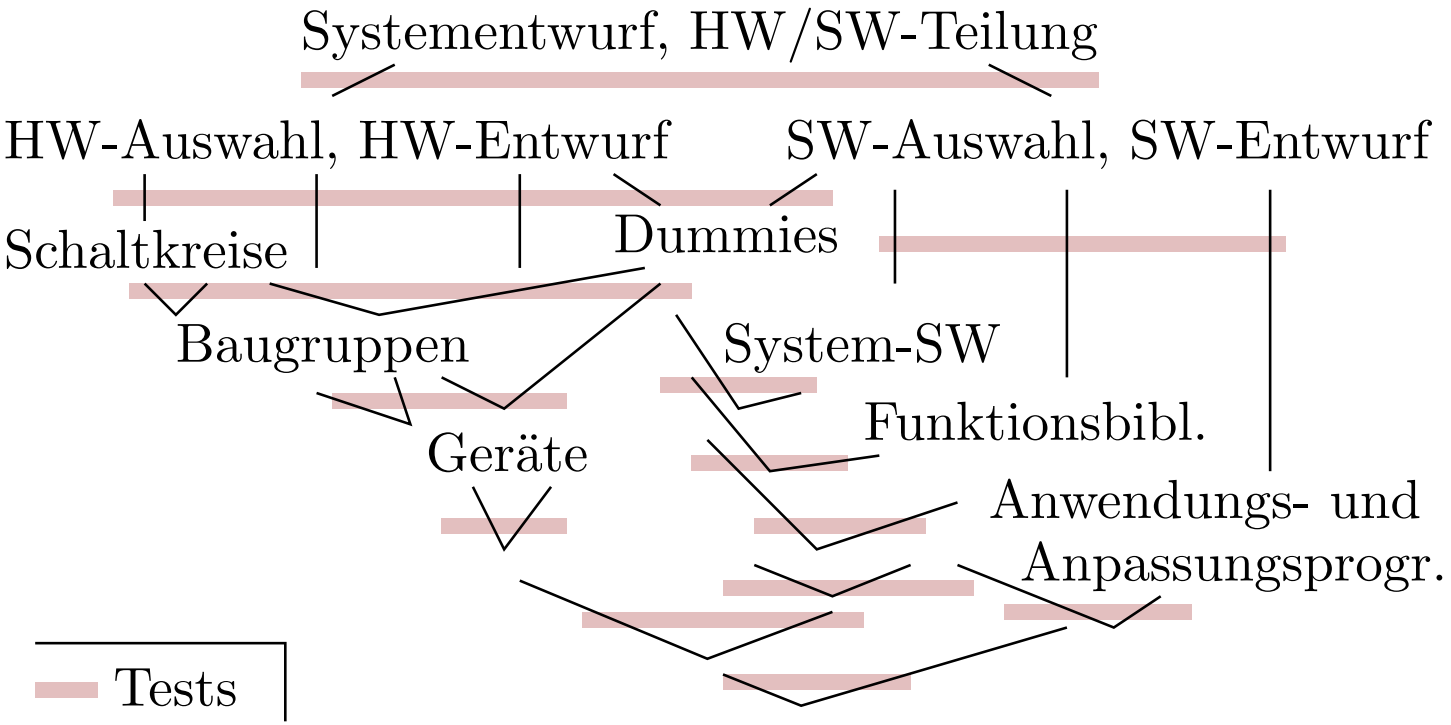
Zum Zeitpunkt der Testauswahl sind die zu findenden und nach dem Test die nicht gefundenen Fehler nicht bekannt.

- Die fehlerorientierte Auswahl und Bewertung von Tests erfolgt auf Basis von Fehlerannahmen (Modellfehlern oder Mutationen).
- Der Nachweis der tatsächlichen Fehler ist immer Zufall.

Eine nachträgliche Kontrolle der Fehlerüberdeckung kann auch nur die im späteren Einsatz gefundenen und beseitigten Fehler, aber nicht die, die dauerhaft unerkannte geblieben sind, zählen.

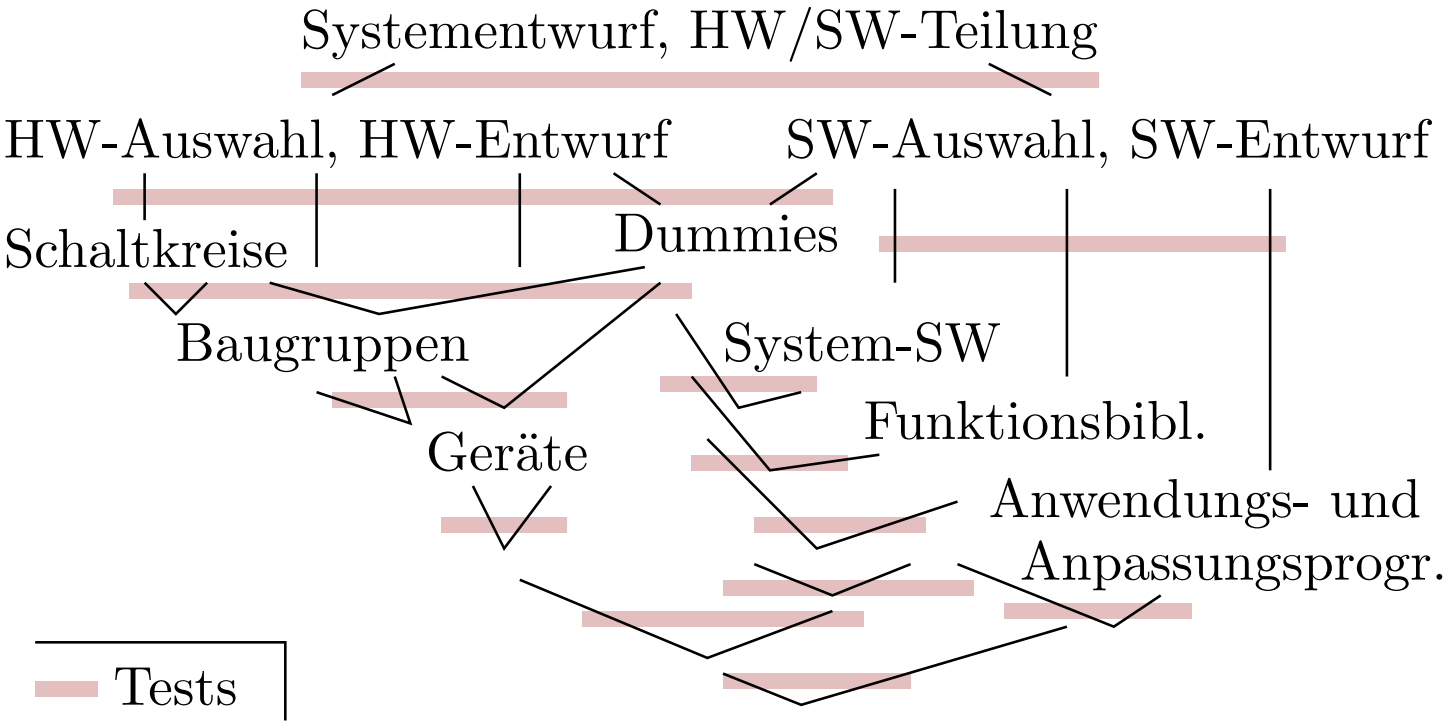
Vielfalt der Test

Entwurf und Test



Es gibt nicht den Test, sondern, ...

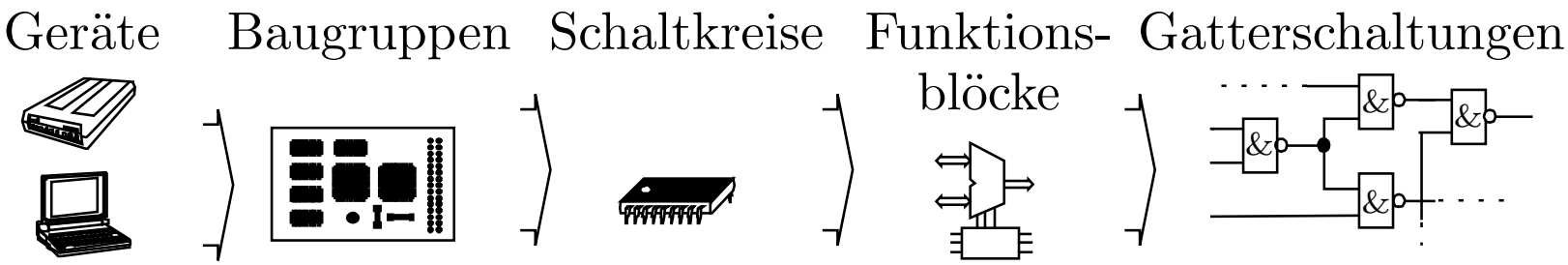
Der Entwurf eines IT-Systems ist ein komplexer Prozess, in dem ein modulares System aus HW- und SW-Bausteinen entsteht. Zwischen den Entwurfsschritten erfolgen vielfältige statische und dynamische Tests der entstandenen Beschreibungen.



Ein Entwurfsablauf ist idealerweise testgetrieben und strebt in jeder Entwurfsphase eine kontrollierbare Zwischenbeschreibung an. Die Entwurfsergebnisse der ersten Phasen (Sammlungen von Anforderungen, Lösungsideen, Entscheidungen) werden auf Machbarkeit, Verständlichkeit, Konsistenz, ... getestet, in der Regel statisch durch Inspektion.

Dynamische Tests sind erst möglich, wenn die Entwurfsbeschreibungen ein ausführ- oder simulierbares Ein-Ausgabeverhalten beschreibt.

Hierarchie und Test



- Rechner-Systeme bestehen aus Rechnern, EA-Geräten, Druckern, Netzwerkkomponenten, diese aus ...
- Die Hardware stellt der SW Grundfunktionen (Maschinenbefehler, EA-Einheiten, ...).
- Software gliedert sich in Teilsysteme, Module, Bibliotheken, ...

Die durchgeführten Tests folgen der Hierarchie.

- Bauteil-, Schaltkreis-, Baugruppen- und Gerätetest.
- Modul-, Teilsystem-, Systemtest.

Da separate Tests mit weniger Aufwand höhere Fehlerüberdeckungen versprechen (siehe später Abschn. 2.2.4), verwenden übergeordnete Systeme in der Regel nur gründlich getestete Bausteine und die übergeordneten Tests zielen nur noch auf Fehler im Zusammenwirken.

Wartungstests

Ein Hardware-Ausfall in der Nutzungsphase verursacht einen neuen Fehler, der wie auch die bei der Fertigung und Reparatur entstehenden Fehler unterschiedliche Wirkung haben kann:

- komplette Funktionsuntüchtigkeit,
- ein anderes unübersehbares Fehlverhalten, z.B. gehäufte Abstürze, oder
- nur ein wenig offenkundiges Absinken der Zuverlässigkeit.

Zur zeitnahen Beseitigung der Zuverlässigkeitsminderungen durch Ausfälle wird Hardware regelmäßigen Wartungstests unterzogen, z.B. in Form von Einschalttests (siehe später Abschn. 6.5.3).

Zusammenfassung Test und Testvielfalt

IT-Systeme werden einer Vielzahl von

- statischen Tests (direkte Merkmalskontrolle) und
- dynamischen Tests (Ausprobieren mit Beispieleingaben)

unterzogen:

- dem Entwurfsfluss folgend nach jeder Entwurfsphase,
- dem Fertigungsfluss folgend bausteinweise und danach das Zusammenwirken der Bausteine im übergeordneten System,
- zur Fehlerbeseitigung vor dem Einsatz und später in der Einsatzphase als Wartungstest.

Kenngrößen zur Beschreibung der Güte von Tests:

- Fehlerabdeckung und
- Phantomfehlerrate.

Die Testauswahl und Bewertung erfolgen mit Hilfe von Modellfehlern:

- zielgerichtet (Testsuche für jeden Modellfehler) oder
- zufällig (nur modellfehlerorientierte Bewertung).

Haftfehler

Modellfehler und Fehlermodell

Die mit einem Test zu suchenden Fehler sind zum Zeitpunkt der Testauswahl unbekannt. Ein *Fehlermodell* ist ein Algorithmus zur Berechnung einer Menge von möglichen Verfälschungen aus einer Entwurfsbeschreibung. Ein *Modellfehler* ist eine einzelne dieser Verfälschungen.

Fehlersimulation zur Bestimmung der *Modellfehlerabdeckung*:

- Wiederhole für jeden Test:
  - Bestimmung der Sollausgaben.
  - Wiederhole für alle Fehler der Modellfehlermenge:
    - Bestimme, ob der Fehler die Ausgabe erkennbar verfälscht.
    - Wenn ja, als nachweisbar kennzeichnen oder Nachweisanzahl erhöhen.

Fehlerorientierte Testsuche:

- Wiederhole für alle Fehler der Modellfehlermenge:
  - Suche Eingaben, für die der Fehler Ausgaben verfälscht.

Fehlersimulation und fehlerorientierte Testsuche erfordern einen sehr hohen Rechenaufwand.

Für digitale ICs seit Jahrzehnten etabliert (siehe später Abschn. 6.2).

Für Software sind Ansätze und Parallelentwicklungen erkennbar, aber noch nicht der konsequente Ansatz, die Güte von Testsätzen durch die Fehlerüberdeckung für ein vorgegebenes Fehlermodell zu beschreiben (siehe später Abschn. 7.3).

Nach der allgemeinen Regel, dass zielgerichtete Verbesserung der Software-Tests hinreichend genaue Überprüfbarkeit der erzielten tatsächlichen Fehlerüberdeckung voraussetzt, ist hier noch Weiterentwicklung zu erwarten.

Das Haftfehlermodell

Seit Jahrzehnten das verbreitetste Fehlermodell für digitale Schaltkreise. In der Vorlesung das Beispielfehlermodell.

Das Haftfehlermodell generiert für eine Schaltung aus Logikgattern für alle Anschlüsse aller Gatter zwei Modellfehler:

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

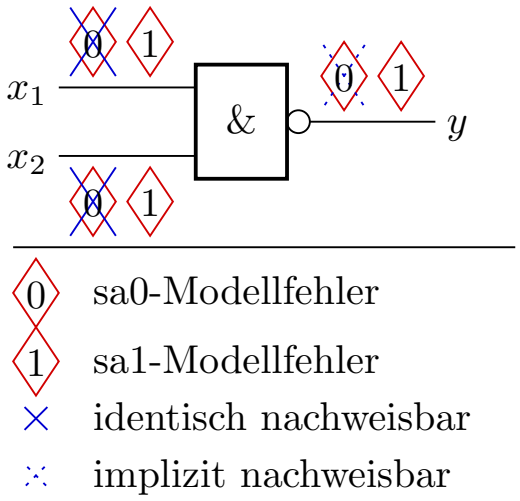
Die initiale Fehlermenge wird von identisch oder implizit nachweisbaren und redundanten (nicht nachweisbaren) Modellfehlern bereinigt.

Die Nachweisbeziehungen zwischen Haftfehlern und den tatsächlichen zu erwartendene Fehlern wird erst später in Abschn. 6.1.3 untersucht.

Haftfehler für ein 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

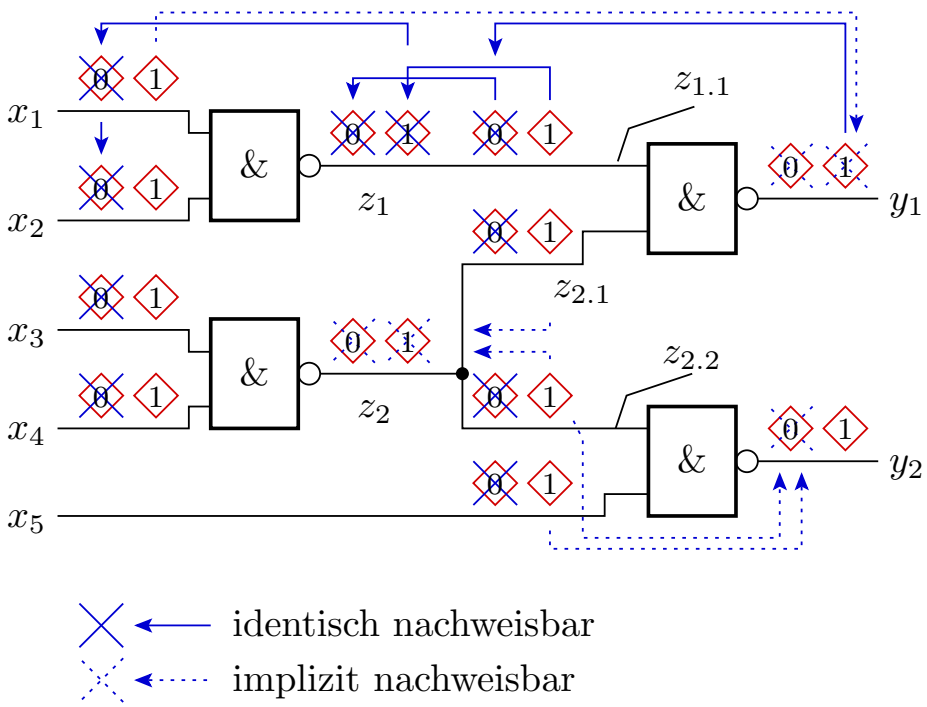
Nachweisidentität (gleiche Nachweismenge)

Nachweisimplikation

zugehörige Eingabe ist Element der Nachweismenge

- Zusammenfassung identisch nachweisbarer Fehler. Optionale Streichung redundanter und implizit nachweisbarer Modellfehler.
- Die generierte Fehlermenge enthält für alle potentiellen Fehler der echten Schaltung ähnlich nachweisbare Modellfehler (siehe Abschn. 6.1.3 *Nachweisbeziehungen*).

Identische und implizit nachweisbarer Fehler im Schaltungsverbund



Größe der Anfangsfehlermenge:	24
Anzahl der nicht identisch nachweisbaren Fehler:	14
ohne implizit nachgewiesene Fehler:	9

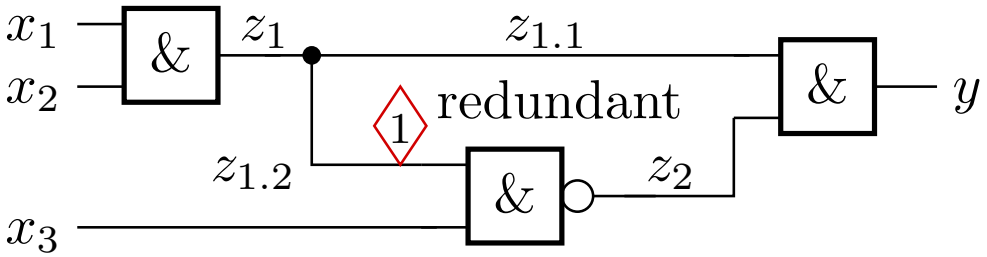
	Mengen von identisch nachweisbaren Fehlern	Nachweis impliziert durch
1	sa0(x_1), sa0(x_2), sa1(z_1), sa1($z_{1.1}$)	
2	sa1(x_1)	
3	sa1(x_2)	
4	sa0(x_3), sa0(x_4), sa1(z_2)	9, 12
5	sa1(x_3)	
6	sa1(x_4)	
7	sa0(z_2)	5, 6, 8, 11
8	sa0(z_1), sa0($z_{1.1}$), sa0($z_{2.1}$), sa1(y_1)	2, 3
9	sa1($z_{2.1}$)	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

Redundante Fehler

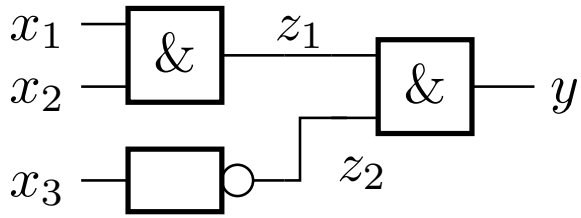
Definition redundanter (Modell-) Fehler

Verfälschung der Systembeschreibung, die die Funktion nicht beeinträchtigt und damit auch nicht mit dynamischen Tests nachweisbar ist.

redundanter Haftfehler



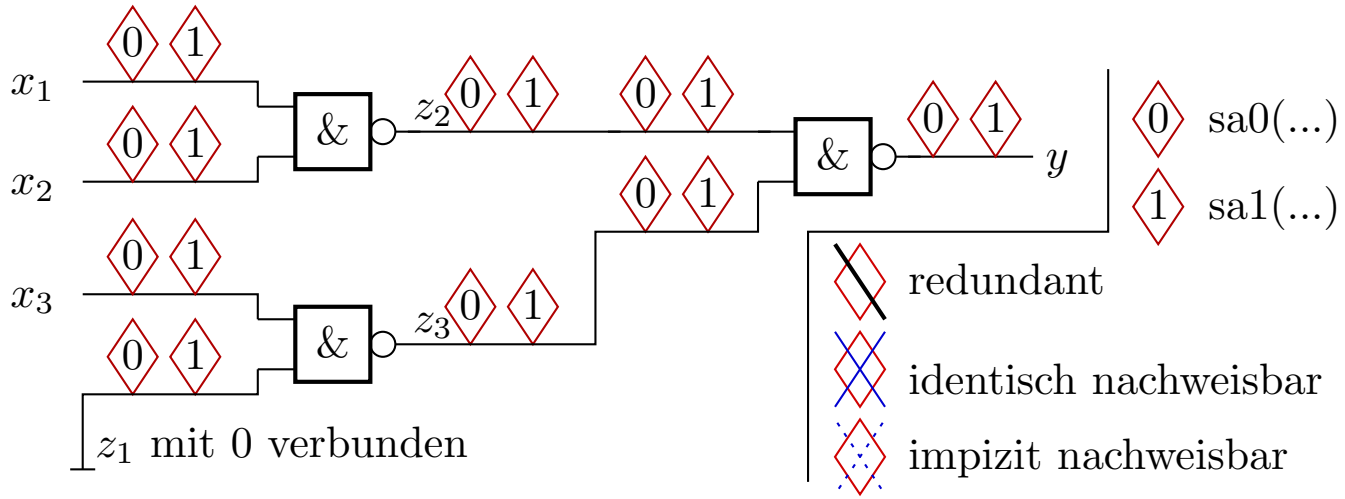
vereinfachte Schaltung



- Die Fehleranregung verlangt $z_1 = 0$ und die Beobachtbarkeit von z_2 an y verlangt $z_2 = 1$. Keine Eingabe $x_3x_2x_1$ kann den Fehler nachweisen.
- Die Beseitigung redundanter Fehler dient auch zur Vereinfachung der Systembeschreibung.

Beispiel 2.1: Haftfehlermenge

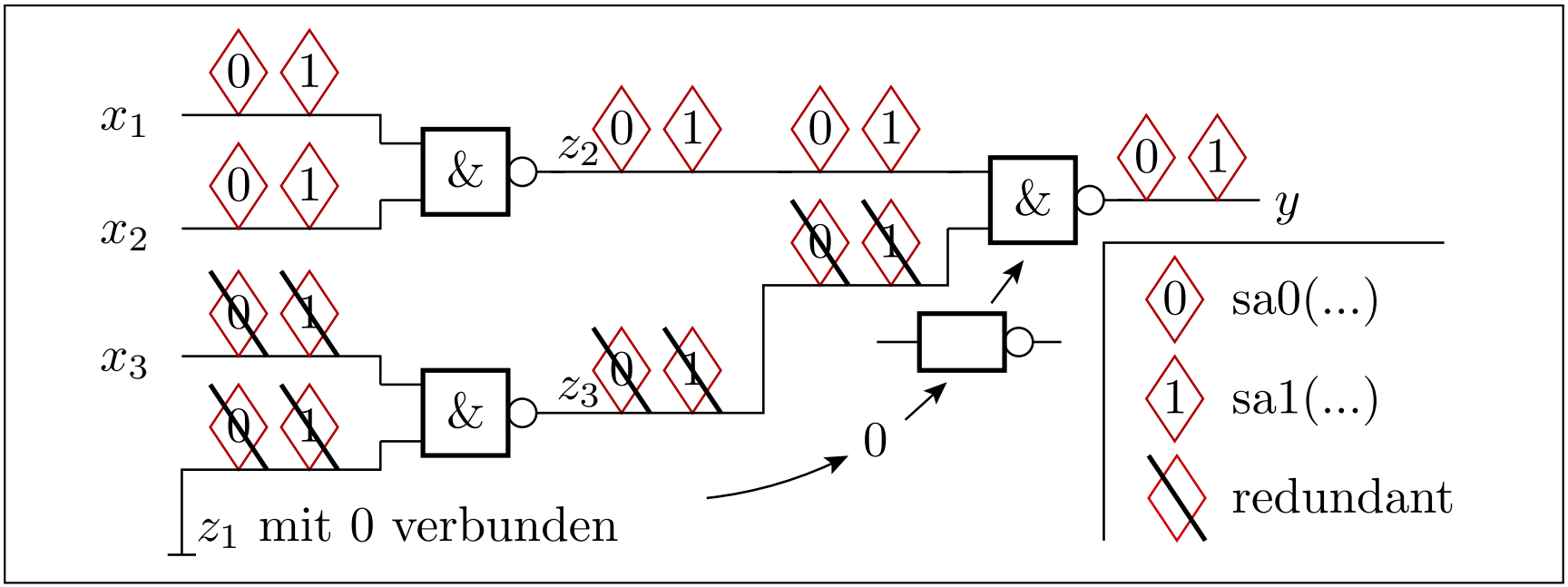
Schaltung mit 14 eingezeichneten Haftfehlern:



a) *Welche der Haftfehler sind redundant (nicht anregbar und/oder nicht beobachtbar).*

b) *Zeichen der vereinfachten Schaltung ohne redundante Haftfehler mit der Initalfehlermenge. Streichen der identisch nachweisbaren Fehler bis auf einen und Kennzeichnen des implizit nachweisbaren Haftfehlers.*

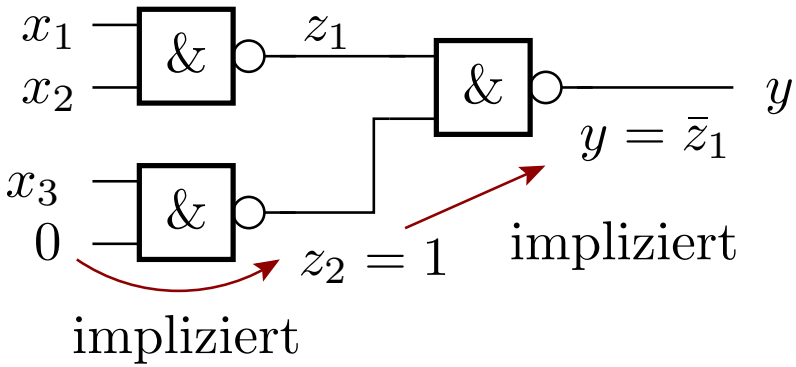
a) *Welche der Haftfehler sind redundant (nicht anregbar und/oder nicht beobachtbar).*



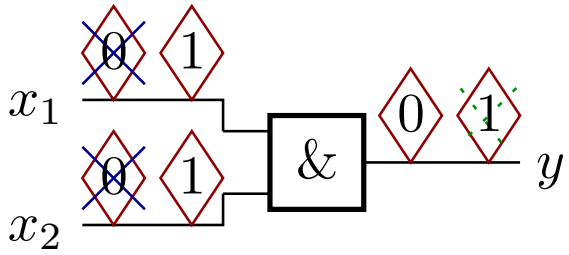
b) *Zeichen der vereinfachten Schaltung ohne redundante Haftfehler mit der Initalfehlermenge. Streichen der identisch nachweisbaren Fehler bis auf einen und Kennzeichnen des implizit nachweisbaren Haftfehlers.*

Die Funktion hängt nicht von x_3 ab und ist: $y = x_1 \wedge x_2$

Vereinfachungsmöglichkeiten

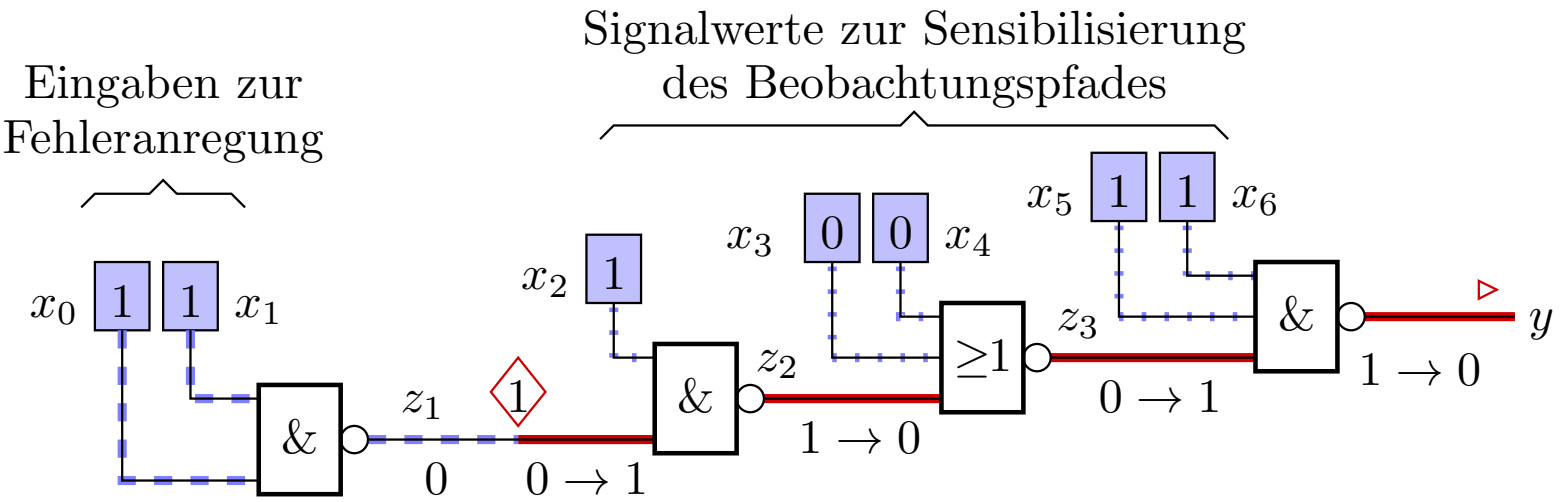


Redizierung der Fehlermenge für die vereinfachte Schaltung



An dem verbleibenden AND-Gatter sind sa0(x_i) identisch mit sa0(y) nachweisbar und der Nachweis von sa1(x_1) und sa1(x_2) impliziert den von sa1(y).

Testsuche

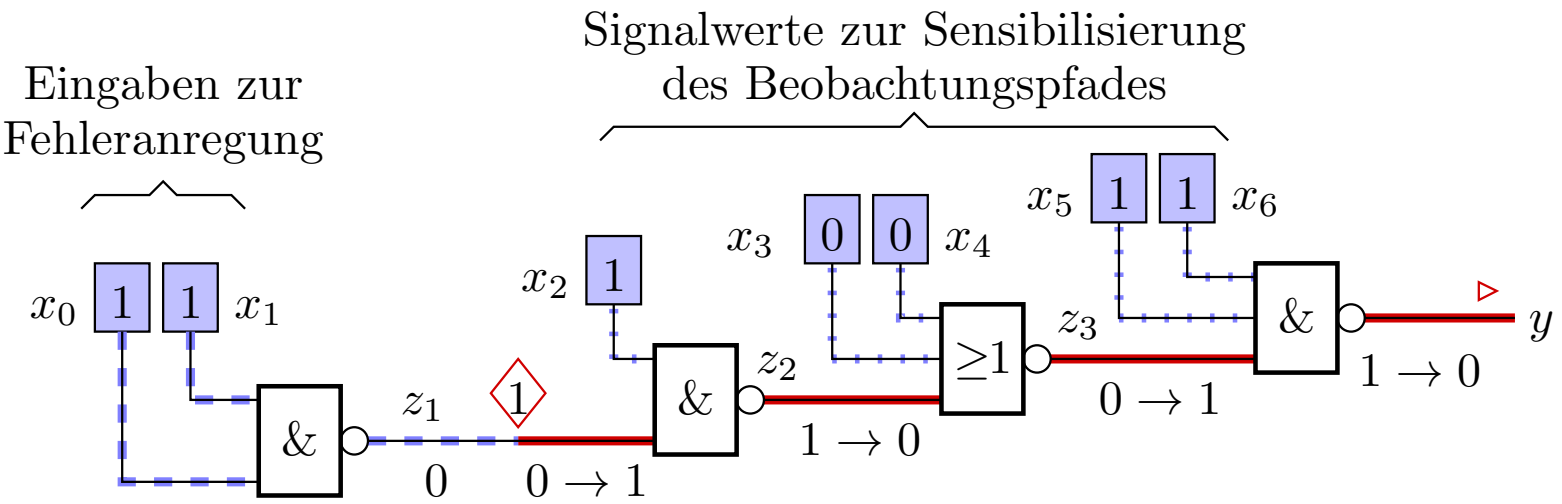


- Signalwerte für den Fehlernachweis
- Fehler (ständig 1, stuck-at 1)
- Fehlfunktion (Ausgabeinvertierung)
- Eingaben zur Fehleranregung
- Einstellung der Beobachtbarkeit
- Beobachtungspfad

Suche durch Pfadsensibilisierung(siehe Abschn. 6.2.2 *D-Algorithmus*):

- Suche von Eingaben zur Einstellung »0« am Fehlerort und
- Sensibilisierung eine Beobachtungspfades zu einem Ausgang.

Fehlernachweismengen



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

Beschreibung des Fehlernachweises über Mengenbeziehungen:

Fehleranregung:	$M_1 = \{\text{-----11}\}$	2^5 Möglichkeiten*
Beobachtbarkeit:	$M_2 = \{\text{11001--}\}$	2^2 Möglichkeiten*
Fehlernachweis:	$M_1 \cap M_2 = \{1100111\}$	2^0 Möglichkeiten*

* Geeignete Werte von insgesamt 2^7 möglichen Eingabewerten.

Von Mengen zu Wahrscheinlichkeiten

Eingabemengen:

Fehleranregung:	$M_1 = \{\text{-----11}\}$	2^5 Möglichkeiten*
Beobachtbarkeit:	$M_2 = \{\text{11001--}\}$	2^2 Möglichkeiten*
Fehlernachweis:	$M_1 \cap M_2 = \{1100111\}$	2^0 Möglichkeiten*

Mit zufälligen Eingaben sind Fehleranregung, Beobachtbarkeit und Nachweis zufällige Ereignisse. Wenn alle 2^7 möglichen Eingaben gleichhäufig auftreten, betragen die Eintrittswahrscheinlichkeiten im Beispiel:

Anregungswahrscheinlichkeit;	$p_{\mathrm{FS}} = 2^{-2}$
Beobachtbarkeit:	$p_{\mathrm{FO}} = 2^{-5}$
Nachweiswahrscheinlichkeit:	$p_{\mathrm{FD}} = p_{\mathrm{FS}} \cdot p_{\mathrm{FO}} = 2^{-7}$

Für Abschätzungen der Fehlerabdeckung für unbekannte tatsächliche Fehler werden diese Mengen- und Wahrscheinlichkeitsbeziehungen später die Grundlage bilden.

Zusammenfassung

Das Haftfehlermodell generiert für Schaltungen aus Logikgattern

- für alle Gatteranschlüsse die beiden Modellfehler sa0 und sa1,
- bereinigt die initiale Fehlermenge von identisch und implizit nachweisbaren und um redundanten Fehlerannahmen.

Die so berechneten Modellfehlermengen dienen

- zur Suche von Tests,
- zur Abschätzung der Fehlerabdeckung sowie
- zur Abschätzung von Mengen und Wahrscheinlichkeitsbeziehungen für Anregung Nachweis und Beobachtbarkeit.

Die Forschung zu Fehlermodellen ist nicht abgeschlossen. Die Etablierung des Haftfehlermodell deutet darauf hin, dass folgende Modellfehlereigenschaften wichtig sind:

- einfach überprüfbarer Fehlernachweis,
- nur linear mit der Systemgröße wachsende Fehleranzahl,
- ähnlich anreg- und beobachtbare Modellfehler für die tatsächlich zu erwartenden Fehler (siehe hierzu auch später Abschn. 6.1.3).

Ausbeute, Defektanteil

Ausbeute und Defektanteil

Bei nicht reparierbaren Systemen und Komponenten interessiert nicht die Fehleranzahl, sondern der Anteil der verwendbaren bzw. der defekten Produkte.

Die Ausbeute ist der Anteil der als gut befundenen Produkte:

$$Y = 1 - \left.\frac{\#DD}{\#P}\right|_{\mathrm{ACR}} \tag{2.3}$$

Der Defektanteil ist der Anteil der tatsächlich defekten Produkte:

$$DL = \left.\frac{\#D}{\#P}\right|_{\mathrm{ACR}} \tag{2.4}$$

Maßeinheiten des Defektanteils dpu (defects per unit), dpm (defects per million):

$$1\,\mathrm{dpu} = 10^6\,\mathrm{dpm}$$

Y, DL	Ausbeute, Defektanteil.
$\#D$, $\#DD$	Anzahl aller defekten Produkte, Anzahl der davon erkannten defekten Produkte.
$\#P$	Anzahl aller getesteten Produkte.
ACR	Brauchbare Schätzwerte nur bei geeigneten Zählwertgrößen.

Defektabdeckung

Die Defektabdeckung ist der Anteil der erkannten defekten Produkte:

$$DC = \left.\frac{\#DD}{\#D}\right|_{\mathrm{ACR}} \tag{2.5}$$

Ausbeute und Defektanteil ungetesteter Produkte:

$$Y = 1 - DL_{\mathrm{M}} \cdot DC \tag{2.6}$$

Ohne Test ($DC = 0$) ist die Ausbeute immer $Y = 1$.

Aussortieren erkannter defekter Produkte verringert Zähler und Nenner in (Gl. 2.6) um die Anzahl der erkannten defekten Produkte:

$$DL = \frac{\#P \cdot DL_{\mathrm{M}} - \#P \cdot DL_{\mathrm{M}} \cdot DC}{\#P - \#P \cdot DL_{\mathrm{M}} \cdot DC}$$

$$DL = \frac{DL_{\mathrm{M}} \cdot (1 - DC)}{1 - DL_{\mathrm{M}} \cdot DC} \tag{2.7}$$

DC	Defektabdeckung (defect coverage), Anteil der erkennbar defekten Produkte.
$\#D$, $\#DD$	Anzahl aller defekten Produkte, Anzahl der davon erkannten defekten Produkte.
Y, DL	Ausbeute, Defektanteil.
DL_{M}	Defektanteil der Fertigung vor Aussortieren der erkannten defekten Produkte.

Erforderliche Defektabdeckung

(2.7) $$DL = \frac{DL_{\mathrm{M}} \cdot (1-DC)}{1-DL_{\mathrm{M}} \cdot DC}$$

eingesetzt in

(2.6) $$Y = 1 - DL_{\mathrm{M}} \cdot DC$$

ergibt einen Defektanteil nach Aussortieren in Abhängigkeit von Defektüberdeckung und Ausbeute:

$$DL = \frac{(1-Y) \cdot (1-DC)}{Y \cdot DC} \tag{2.8}$$

Erforderliche Defektabdeckung zur Erzielung eines Defektanteil DL bei einer Ausbeute Y:

$$DC = \frac{1-Y}{1+(DL-1) \cdot Y} \tag{2.9}$$

Y, DL	Ausbeute, Defektanteil.
DC	Defektabdeckung (defect coverage), Anteil der erkennbar defekten Produkte.

Defektanteil digitaler Schaltkreise

Für Schaltkreise findet man in der Literatur als typische Angaben:

- Ausbaute: $Y = 10\% \ldots 90\%$
- Defektanteil: $DL = 200\,\mathrm{dpm} \ldots 1000\,\mathrm{dpm}$
- Haftfehlerabdeckung: $FC_{\mathrm{SA}} = 80\% \ldots 99\%$..

Erforderliche Defektabdeckung nach

(2.9) $$DC = \frac{1-Y}{1+(DL-1)\cdot Y}$$

	$Y = 10\%$	$Y = 50\%$	$Y = 90\%$
$DL = 200\,\mathrm{dpm}$	$1 - 2{,}2 \cdot 10^{-5}$	$1 - 2 \cdot 10^{-4}$	$1 - 1{,}7 \cdot 10^{-3}$
$DL = 1000\,\mathrm{dpm}$	$1 - 1{,}1 \cdot 10^{-4}$	$1 - 2 \cdot 10^{-3}$	$1 - 8{,}9 \cdot 10^{-3}$

Der Anteil der Schaltkreise, die der Test nicht erkennt, ist laut Abschätzung eine bis zwei Zehnerpotenzen kleiner als der Anteil der nicht nachweisbaren Haftfehler. Daraus resultierende Fragen:

- Gilt für Schaltkreise tatsächlich $1 - DC \ll 1 - FC_{\mathrm{sa}}$ oder
- ist die Dunkelziffen der defekten Schaltkreise so viel größer?

Weitere Frage, wie oft enthalten Rechnern defekte Schaltkreise?

Systeme aus getesteten Teilsystemen

Für Systeme aus Teilsystemen gelten die Grundregeln:

- gründlicher Test der Teilsysteme vor dem Einbau,
- Testfokusierung nach Einbau auf die Verbindungen.

Vor Einbau in Teilsysteme nicht erkannte Fehler bleiben auch im Gesamtsystem unerkannt. Zu erwartende Fehleranzahl Gesamtsystem:

$$\mu_{\mathrm{F}} = \mu_{\mathrm{F.Con}} \cdot (1 - FC_{\mathrm{Con}}) + \sum_{i=1}^{\#Prt} \mu_{\mathrm{F}.i} \tag{2.10}$$

Für den zu erwartenden Fehleranteil folgt später die Abschätzung:

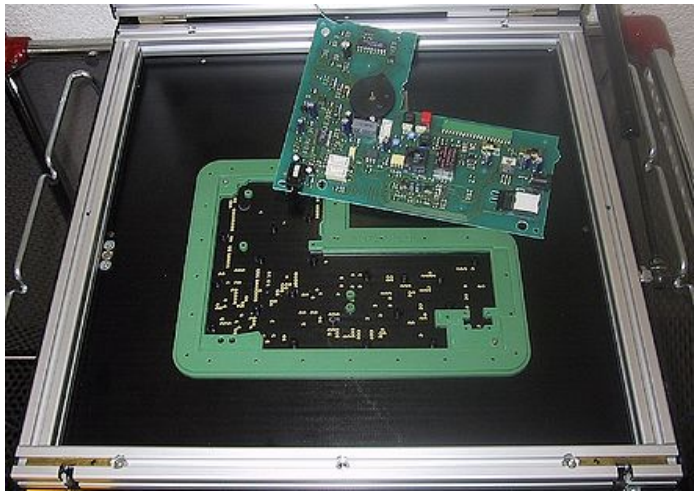
(4.42) $$\mu_{\mathrm{DL}} = 1 - \mathrm{e}^{-\mu_{\mathrm{F}}}$$

Für eine sehr kleine Fehleranzahl $\mu_{\mathrm{F}} \ll 1$ gilt:

(4.43) $$\mu_{\mathrm{DL}} = \mu_{\mathrm{F}}$$

$\mu_{\mathrm{F}}, \mu_{\mathrm{F.Con}}$	Zu erwartende Gesamtfehleranzahl, zu erwartende Anzahl der Verbindungsfehler.
$\mu_{\mathrm{F}.i}$	Zu erwartendender Fehleranzahl Teilsystem i.
FC_{Con}	Fehlerübedeckung für Verbindungsfehler (Fault coverange for connection faults).
$\#Prt$	Anzahl der Bauteile.
μ_{DL}	Zu erwartender Defektanteil.

Leiterplattentest



Bestückte Leiterplatten bestehen aus geprüften Bauteilen und werden für den Test in der Regel auf einem Nadelbett gespannt. Zielfehler: Leitungsunterbrechungen, Kurzschlüsse und Bestückungsfehler.

(Kurzschüsse und Unterbrechungen) und Bestückungsfehler praktisch $FC_{\mathrm{Con}} = 1$ und kein Nachweis für defekte Bauteile und Fehleranteil der Bauteile sehr klein $(\mu_{\mathrm{F}.i} \ll 1 \;\Rightarrow\; \mu_{\mathrm{F}.i} = \mu_{\mathrm{DL}.i})$:

$$\mu_{\mathrm{F}} = \sum_{i=1}^{\#Prt} \mu_{\mathrm{DL}.i} \tag{2.11}$$

Für $\mu_{\mathrm{F}} \ll 1$ ist die abgeschätzte erwartete Fehleranzahl der zu erwartende Fehleranteil der Baugruppe.

μ_{F}	Zu erwartende Fehleranzahl des Gesamtsystems.
$\#Prt$	Anzahl der Bauteile.
$\mu_{\mathrm{DL}.i}$	Zu erwartendender Defektanteil von Bauteil i.

Beispielabschätzung

Leiterplatte mit nachfolgenden Komponenten:

Typ	Anzahl	$\mu_{\mathrm{DL}.i}$
Leiterplatte	1	20 dpm
Schaltkreise	20	200 dpm
diskrete Bauteile	35	10 dpm
Lötstellen	560	1 dpm

$$\begin{aligned}\mu_{\mathrm{DL.Sys}} = \mu_{\mathrm{F}} &= 10\,\mathrm{dpm} + 20 \cdot 200\,\mathrm{dpm} + 35 \cdot 10\,\mathrm{dpm} + 560 \cdot 1\,\mathrm{dpm} \\ &= 5000\,\mathrm{dpm} = 0{,}005\,\mathrm{dpu}\end{aligned}$$

Etwa jedes 200ste Gerät enthält ein nicht erkanntes defektes Bauteil, natürlich nur mit einem kaum nachweisbaren Defekt, der die Zuverlässigkeit nur wenig mindert.

Wenn Defektanteils der Schaltkreisen tatsächlich um Zehnerpotenzen größer (siehe Folie Defektanteil digitaler Schaltkreise, Abschn. 2.1.6)?

$\mu_{\mathrm{DL.Sys}}$ Defektanteil des Systems.

Zusammenfassung

Fehlerbeseitigung

Fehlerbeseitigung: Iteration aus Beseitigungsversuchen für hypothetische Fehler und Erfolgskontrolle durch Testwiederholung:

- Beseitigung aller erkennbaren Fehler.
- Rückbau nach erfolglosen Reparaturversuchen.
- Bei wenigen Bausteinen durch systematisches Tauschen.

Fehlerdiagnose: Abschätzung von Ort-, Ursache und Beseitigungsmöglichkeiten von Fehlern aus Testergebnissen:

- Pareto-Prinzip, Bevorzugungung erfolgsversprechender Fehlerbeseitigungsversuche.
- Rückverfolgung entgegen den Berechnungs- bzw. Signalfluss.

Reparaturgerechter Entwurf:

- Tauschbare Module, deterministische Verhalten,
- gerichteter Berechnungfluss, Fehlerisolation, ...

Bei einer vernünftigen Reparaturtechnologie werden alle erkannten Fehler beseitigt und es entsteht nur eine vernachlässigbar kleine Anzahl neuer nicht nachweisbarer Fehler.

Test und Testvielfalt

IT-Systeme werden einer Vielzahl Tests unterzogen:

- dem Entwurfsfluss folgend nach jeder Entwurfsphase,
- dem Fertigungsfluss folgend bausteinweise und danach das Zusammenwirken der Bausteine im übergeordneten System,
- zur Fehlerbeseitigung vor dem Einsatz und als Wartungstest,
- jeweils statisch (direkte Merkmalskontrolle) und dymamisch (Ausprobieren mit Beispieleingaben).

Kenngrößen:

- Fehlerabdeckung

  (2.1) $$FC = \frac{\#DF}{\#F}\Big|_{\mathrm{ACR}}$$

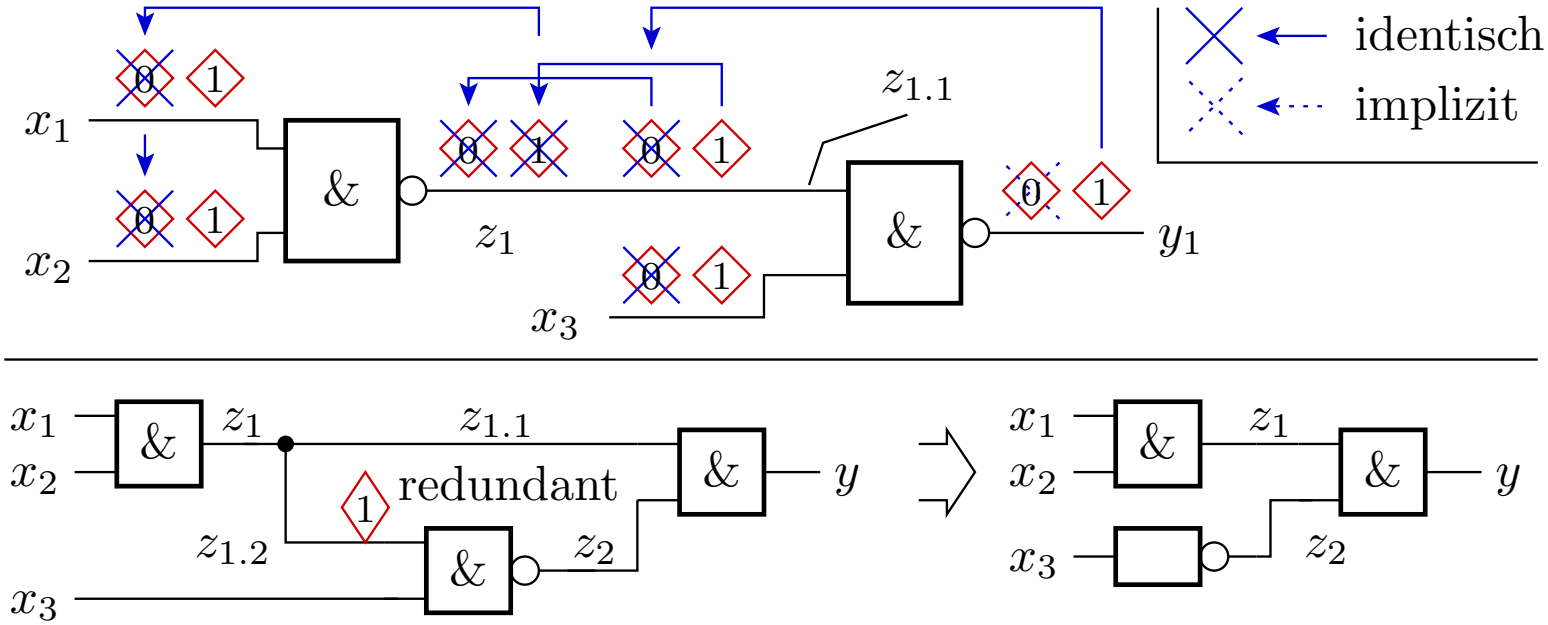
- Phantomfehlerrate

  (2.2) $$\zeta_{\mathrm{PF}} = \frac{\#PM}{N}\Big|_{\mathrm{ACR}}$$

Die Testauswahl und Bewertung erfolgt mit Hilfe von Modellfehlern:

- zielgerichtet (Testsuche für jeden Modellfehler) oder
- zufällig (nur modellfehlerorientierte Bewertung).

Haftfehler



Seit Jahrzehnten wichtigstes Fehlermodell für digitale Schaltungen:

- Initialfehlermenge: je Gatteranschluss sa0 und sa1.
- Zusammenfassen identisch nachweisbarer Fehler, streichen redundanter und implizit nachweisbarer Fehler.
- Daraus, dass sich genau dieses Modell etabliert hat, kann man ableiten, welchen Eigneschaften Fehlermodelle haben sollten.

Defektanteil, Ausbeute

Bei nicht reparierbaren Systemen und tauschbaren Komponenten interessieren statt der Fehleranzahl, Ausbeute und Fehleranteil:

(2.3) $$Y = 1 - \left.\frac{\#DD}{\#P}\right|_{\mathrm{ACR}}$$

(2.4) $$DL = \left.\frac{\#D}{\#P}\right|_{\mathrm{ACR}}$$

Bindeglied ist die Defektabdeckung:

(2.5) $$DC = \left.\frac{\#DD}{\#D}\right|_{\mathrm{ACR}}$$

(2.6) $$Y = 1 - DL_{\mathrm{M}} \cdot DC$$

Defektanteil nach Ersatz der erkannten defekten Produkte:

(2.7) $$DL = \frac{DL_{\mathrm{M}} \cdot (1 - DC)}{1 - DL_{\mathrm{M}} \cdot DC}$$

(2.8) $$DL = \frac{(1 - Y) \cdot (1 - DC)}{DC \cdot Y}$$

Modulare Systeme aus getesteten Bauteilen

Fehleranzahl:

(2.10) $$\mu_{\mathrm{F}} = \mu_{\mathrm{F.Con}} \cdot (1 - FC_{\mathrm{Con}}) + \sum_{i=1}^{\#Prt} \mu_{\mathrm{F}.i}$$

Beziehung Fehleranteil und Fehleranzahl (Vorgriff):

(4.42) $$\mu_{\mathrm{DL}} = 1 - \mathrm{e}^{-\mu_{\mathrm{F}}}$$

Für $\mu_{\mathrm{F}} \ll 1$:

(4.43) $$\mu_{\mathrm{DL}} = \mu_{\mathrm{F}}$$

Für getestete Leiterplatten gilt in der Regel $FC_{\mathrm{Con}} = 1$ und Fehleranzahl gleich Summe der Defektanteile aller Bauteile:

(2.11) $$\mu_{\mathrm{F}} = \sum_{i=1}^{\#Prt} \mu_{\mathrm{DL}.i}$$

Für $\mu_{\mathrm{F}} \ll 1$ gilt auch hier Gl. 4.43.

Zuverlässigkeit & Test

Einfache Abschätzung

Beispiel 2.2: Fehleranzahl und Zuverlässigkeit

Programmgröße 10.000 NLOC. 30 ... 100 Fehler je 1000 NLOC.
Fehlerabdeckung der Tests $FC = 70\%$.

a) *Wie groß ist die Fehleranzahl nach Beseitigung aller erkennbaren Fehler?*

$$10.000\,\mathrm{NLOC} \cdot \frac{30\ [\mathrm{F}]\ \ldots\ 100\,[\mathrm{F}]}{1000\,\mathrm{NLOC}} \cdot (1 - 70\%) = 90\,[\mathrm{F}]\ \ldots\ 300\ [\mathrm{F}]$$

b) *Wie zuverlässig ist ein System mit ca. 90 bis 300 Fehlern?*

[F]	Zählwert in Fehlern.
FC	Fehlerabdeckung (fault coverage), Anteil der nachweisbaren Fehler.
NLOC	Netto Lines of Code, Anzahl der Code-Zeilen ohne Kommentar und Leerzeilen.

b) *Wie zuverlässig ist ein System mit ca. 90 bis 300 Fehlern?*

Vorgriff: Bei einem Zufallstest und Beseitigung aller erkannten Fehler verhält sich die fehlerbezogene Teilzuverlässigkeit R_{F} proportional zur Anzahl der dynamischen Tests N und umgekehrt proportional zur zu erwartenden Anzahl der nicht beseitigten Fehler $\mu_{\mathrm{F}}(N)$:

(2.25)
$$R_{\mathrm{F}}(N) = \frac{N}{K \cdot \mu_{\mathrm{F}}(N)}$$

Die Zuverlässigkeit hängt nicht nur von der Fehleranzahl, sondern vom Verhältnis aus Testaufwand und Fehleranzahl ab, vorausgesetzt, dass alle erkennbaren Fehler beseitigt werden.

$R_{\mathrm{F}}(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehler.
N	Anzahl der Tests.
K	Formfaktor der Dichte der Fehlfunktionsrate $(0 < K < 1)$.
$\mu_{\mathrm{F}}(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.

Fehlfunktionsrate durch Fehler

Jeder nicht beseitigte Fehler i verursacht mit der MF-Rate ζ_i (in MF je DS) Fehlfunktionen. Die Summe der MF-Raten aller Fehler

$$\zeta_{\sum} = \sum_{i=1}^{\#F} \zeta_i$$

ist eine Obergrenze $\zeta_{\mathrm{F}} \leq \zeta_{\sum}$ und, wenn fast alle MF nur einen Fehler als Ursache haben, praktisch gleich der MF-Rate durch alle Fehler:

$$\zeta_{\mathrm{F}} = \sum_{i=1}^{\#F} \zeta_i \quad \text{für} \quad \zeta_{\mathrm{F}} \ll 1$$

Im weiteren betrachten wir nur vorgetestete Systeme, in denen die schlimmsten Fehler schon beseitigt sind, so dass im Mittel bereits mehrere Tests korrekt ausgeführt werden, d.h. nur den Fall $\zeta_{\mathrm{F}} \ll 1$.

MF, HW	Fehlfunktion, erbrachte Service-Leistung.
$\#F$	Anzahl der vorhandenen Fehler.
ζ_i	MF-Rate verursacht durch Fehler i.
ζ_{F}	Fehlfunktionsrate durch Fehler.

Unter den Annahmen:

- Beseitigung aller nachweisbaren Fehler,
- mittlere MF-Rate je nicht beseitigten Fehler $\bar{\zeta} < 1/N$
- je Fehlfunktion nur ein Fehler als Ursache

beträgt die MF-Rate für alle nicht beseitigten Fehler zusammen:

$$\zeta_{\mathrm{F}}(N) = \mu_{\mathrm{F}}(N) \cdot \bar{\zeta}(N) \tag{2.12}$$

$$\zeta_{\mathrm{F}}(N) < \frac{\mu_{\mathrm{F}}(N)}{N}$$

Die fehlerbezogene Teilzuverlässigkeit beträgt mindestens:

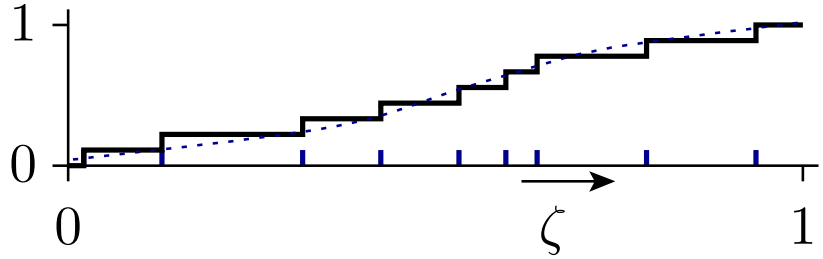
$$R_{\mathrm{F}} > \frac{N}{\mu_{\mathrm{F}}(N)}$$

$\zeta_{\mathrm{F}}(N)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.
$\mu_{\mathrm{F}}(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
$\bar{\zeta}(N)$	Mittlere Fehlfunktionsrate je Fehler als Funktion der Testanzahl N.
N	Anzahl der Tests, für die alle erkannten Fehler beseitigt sind.
$R_{\mathrm{F}}(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehler.

Verbessertes Modell

Verteilung der Fehlfunktionsrate

$$F_Z(\zeta) = \mathbf{P}[Z \leq \zeta]$$



Treppenfunktion für eine endliche Fehleranzahl

Annäherung durch eine stetige Funktion

Die Verteilung $F_Z(\zeta)$ der Zufallsgröße Z beschreibt die Wahrscheinlichkeit, dass diese nicht größer als ζ ist. Die Zufallsgröße $Z \in (0, 1)$ ist hier die Fehlfunktionsrate eines (zufällig ausgewählten) Fehlers. Bei Annäherung von $F_Z(\zeta)$ durch eine stetige Verteilungsfunktion beträgt die Dichte der MF-Rate (siehe später Foliensatz 4):

$$h(\zeta) = f_Z(\zeta) = \frac{\mathrm{d}F_Z(\zeta)}{\mathrm{d}\zeta} \text{ mit } \int_0^1 h(\zeta) \cdot \mathrm{d}\zeta = 1$$

$F_Z(\zeta)$	Verteilungsfunktion der Fehlfunktionsrate, Z – Zufallsvariable, ζ – Wert.
$h(\zeta)$	Dichtefunktion der Fehlfunktionsrate.

Fehlerabdeckung und MF-Rate

Zu erwartende Anzahl der mit N Tests nicht beseitigten Fehler, wenn alle nachweisbaren Fehler beseitigt werden:

$$\mu_{\mathrm{F}}(N) = \mu_{\mathrm{F}} \cdot \int_0^1 p_{\mathrm{FNE}}(\zeta, N) \cdot h(\zeta) \cdot \mathrm{d}\zeta \tag{2.13}$$

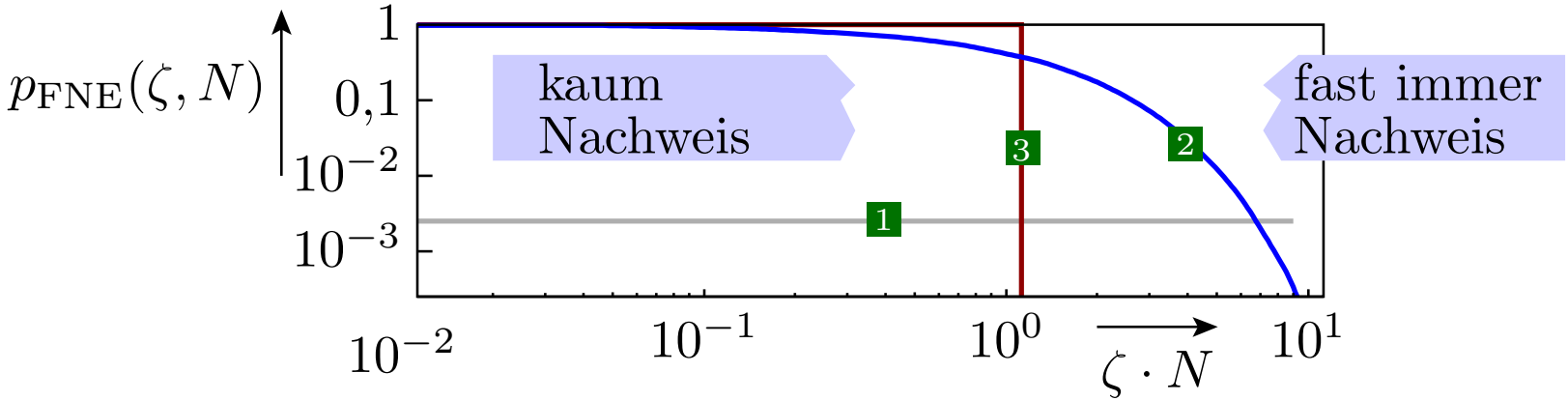
Zu erwartende Fehlfunktionesrate durch die nicht beseitigten Fehler:

$$\zeta_{\mathrm{F}}(N) = \mu_{\mathrm{F}} \cdot \underbrace{\int_0^1 p_{\mathrm{FNE}}(\zeta, N) \cdot h(\zeta) \cdot \zeta \cdot \mathrm{d}\zeta}_{\text{mittlere Fehlfunktionsrate je Fehler}} \tag{2.14}$$

(Integration über die Produkte aus Häufigkeit des Vorhandenseins und Fehlfunktionsrate).

$\mu_{\mathrm{F}}(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
μ_{F}	Zu erwartende Fehleranzahl vor der Iteration aus Test und Fehlerbeseitigung.
$p_{\mathrm{FNE}}(\zeta, N)$	Wahrscheinlichkeit, dass Fehler mit MF-Rate ζ nach N Tests nicht beseitigt sind.
$h(\zeta)$	Dichtefunktion der Fehlfunktionsrate vor der Fehlerbeseitigung.
N	Anzahl der Tests.
$\zeta_{\mathrm{F}}(N)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.

Fehlernachweiswahrscheinlichkeit



Die Nichtbeseitigungswahrscheinlichkeit $p_{\mathrm{FNE}}(\zeta, N)$ eines Fehlers hängt auch von der Art der Testauswahl ab:

1. statische Tests: Keine Abhängigkeit von ζ der Fehler.
2. Zufallstests: Fehler mit $\zeta \ll N^{-1}$ werde nicht und mit $\zeta \gg N^{-1}$ sicher nachgewiesen. Dazwischen (siehe später Gl. 3.9):

$$p_{\mathrm{FNE}}(\zeta, N) = \mathrm{e}^{-\zeta \cdot N}$$

3. Im folgenden verwendete Näherung zur einfacheren Abschätzung:

$$p_{\mathrm{FNE}}(\zeta, N) = \begin{cases} 1 & \zeta \leq \frac{1}{N} \\ 0 & \text{sonst} \end{cases} \tag{2.15}$$

Typische Fehlerabdeckung von Zufallstests

Bei einem Zufallstest erfordert eine Verringerung des Anteils der nicht nachweisbaren Fehler $1 - FC\,(N)$ um eine Dekade eine Erhöhung der Testanzahl N um mehr als eine Dekade. Das ist die Eigenschaft einer Potenzfunktion:

$$\mu_{\mathrm{F}}\,(N_2) = \mu_{\mathrm{F}}\,(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit} \;\; 0 < K < 1 \tag{2.16}$$

K	1	0,5	0,33	0,25
$\frac{N_2}{N_1}$ für $\frac{\mu_{\mathrm{F}}(N_2)}{\mu_{\mathrm{F}}(N_1)} = 0{,}1$	10	100	10^3	10^4

Formfaktor:

$$K = -\log\left(\frac{\mu_{\mathrm{F}}(N_2)}{\mu_{\mathrm{F}}(N_1)}\right) / \log\left(\frac{N_2}{N_1}\right) \tag{2.17}$$

$\mu_{\mathrm{F}}\,(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
K	Formfaktor der Dichte der Fehlfunktionsrate $(0 < K < 1)$.
$N_1\,, N_2$	Testanzahl mit bekannter oder gesuchter zu erwartender Fehleranzahl.

Dichte der MF-Rate

Mit der Vereinfachung, dass ein Zufallstest der Länge N alle Fehler mit $\zeta < \frac{1}{N}$ nicht und ab MF-Rate $\zeta \geq \frac{1}{N}$ sicher nachweist:

$$p_{\mathrm{FNE}}(\zeta, N) = \begin{cases} 1 & \zeta \leq \frac{1}{N} \\ 0 & \text{sonst} \end{cases} \tag{2.15}$$

$$\mu_{\mathrm{F}}(N) = \mu_{\mathrm{F}} \cdot \int_0^1 p_{\mathrm{FNE}}(\zeta, N) \cdot h(\zeta) \cdot \mathrm{d}\zeta \tag{2.13}$$

$$\mu_{\mathrm{F}}(N_2) = \mu_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit } 0 < K < 1 \tag{2.16}$$

Für die Dichte der MF-Rate vor der Beseitigung muss gelten:s

$$\frac{\mu_{\mathrm{F}}(N_2)}{\mu_{\mathrm{F}}(N_1)} = \left(\frac{N_2}{N_1}\right)^{-K} = \frac{\int_0^{\frac{1}{N_2}} h(\zeta) \cdot \mathrm{d}\zeta}{\int_0^{\frac{1}{N_1}} h(\zeta) \cdot \mathrm{d}\zeta}$$

Die passende Dichtefunktion für $\zeta \in (0, 1)$ ist die Potenzfunktion:

$$h(\zeta) = K \cdot \zeta^{K-1} \quad \text{mit } 0 < K < 1 \tag{2.18}$$

Fehlfunktionsrate als Funktion der Testanzahl

Die gefundene Dichtefunktion

(2.18) $$h(\zeta) = K \cdot \zeta^{K-1} \quad \text{mit} \quad 0 < K < 1$$

eingesetzt in

(2.14) $$\zeta_{\mathrm{F}}(N) = \mu_{\mathrm{F}} \cdot \underbrace{\int_0^1 p_{\mathrm{FNE}}(\zeta, N) \cdot h(\zeta) \cdot \zeta \cdot \mathrm{d}\zeta}_{\text{mittlere Fehlfunktionsrate je Fehler}}$$

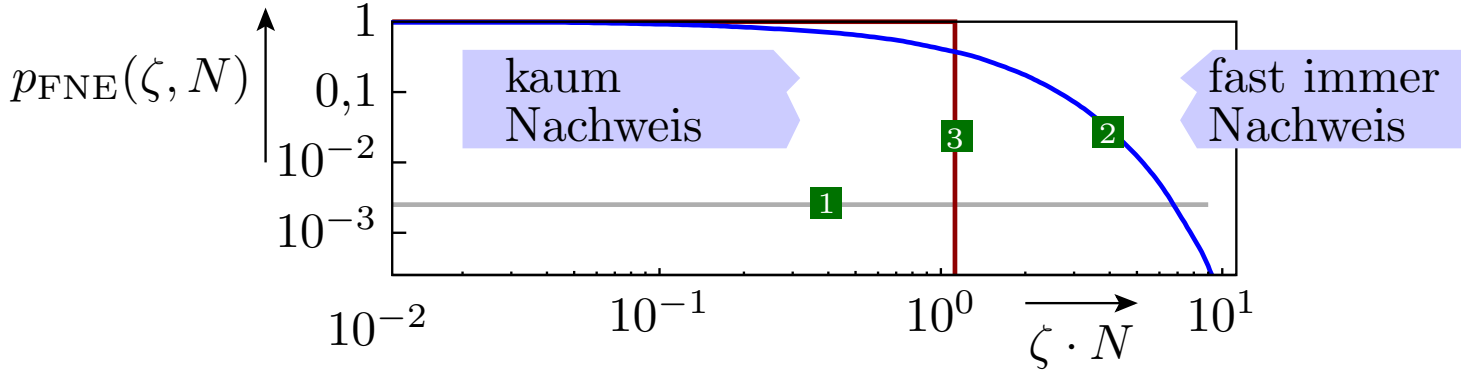
MF-Rate nach Fehlerbeseitigung, wenn ein Zufallstest der Länge N alle Fehler mit $\zeta < \frac{1}{N}$ nicht und ab MF-Rate $\zeta \geq \frac{1}{N}$ sicher nachweist:

$$\zeta_{\mathrm{F}}(N) = \mu_{\mathrm{F}} \cdot \int_0^{\frac{1}{N}} K \cdot \zeta^{K-1} \cdot \zeta \cdot \mathrm{d}\zeta = \mu_{\mathrm{F}} \cdot \tfrac{K}{K+1} \cdot N^{-(K+1)}$$

Abnahme bei Verlängerung der Testanzahl, für die die erkennbaren Fehler beseitigt werden, von N_1 auf N_2 Tests:

$$\zeta_{\mathrm{F}}(N_2) = \zeta_{\mathrm{F}}(N_1) \cdot \left(\tfrac{N_2}{N_1}\right)^{-(K+1)} \tag{2.19}$$

$h(\zeta, N)$	Dichte der Fehlfunktionsrate nach Beseitigung der mit N Tests nachweisbaren Fehler.
K	Formfaktor der Dichte der Fehlfunktionsrate $(0 < K < 1)$.
$\zeta_{\mathrm{F}}(N)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.



Verhältnis zwischen MF-Rate und Fehleranzahl nach Beseitigung aller Fehler für N Tests:

$$\zeta_{\mathrm{F}}(N) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{(K+1) \cdot N} \tag{2.20}$$

Mit Kurve 2 statt 3 für $p_{\mathrm{FNE}}(\zeta, N)$ für einen Zufallstest im Bild oben:

$$\zeta_{\mathrm{F}}(N) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{N} \tag{2.21}$$

(siehe später Abschn. 3.2.1). Achtung: Abschätzungen basieren auf der Annahme $\zeta_{\mathrm{F}}(N) \ll 1$ (siehe Folie Fehlfunktionsrate durch Fehler, Abschn. 2.2.1) und verlangt nach Gl. 2.21 $N \gg \mu_{\mathrm{F}}(N)$.

Abschätzung Formfaktor K aus der Abnahme der MF-Rate:

$$K = \log\left(\frac{\zeta_{\mathrm{F}}(N_1)}{\zeta_{\mathrm{F}}(N_2)}\right) / \log\left(\frac{N_2}{N_1}\right) - 1 \tag{2.22}$$

Vortests

Aufteilung in Vortest und Zufallstest

Vor einem gründlichen Zufallstest erfolgen Vortests:

- statische Tests: Reviews, Syntax, ...
- Grobtests, ob überhaupt etwas funktioniert und
- gezielt gesuchte Tests für Grenz- und Sonderfälle.

Bei statischen und fehlerorientiert gesuchten Tests hängt $p_{\mathrm{FNE}}(\zeta, N)$ weniger von ζ als beim Zufallstest ab. Pauschalannahme, dass alle Vortests zusammen einen Anteil von FC_{PT} Fehler erkennen, die alle beseitigt werden und $N_0 \geq 1$ dynamische Tests enthalten:

$$\mu_{\mathrm{F}}(N_0) = \mu_{\mathrm{FCR}} \cdot (1 - FC_{\mathrm{PT}}) \tag{2.23}$$

$$\zeta_{\mathrm{F}}(N_0) = \frac{K \cdot \mu_{\mathrm{F}}(N_0)}{N_0} \ll 1 \tag{2.24}$$

$p_{\mathrm{FNE}}(\zeta, N)$	Wahrscheinlichkeit, dass Fehler mit MF-Rate ζ nach N Tests nicht beseitigt sind.
$\mu_{\mathrm{F}}(N_0)$	Zu erwartende Anzahl der Fehler, die nach N_0 Tests nicht erkannt und beseitigt sind.
N_0	Anzahl der dynamischen Tests aller Vortests zusammen.
μ_{FCR}	Zu erwartende Fehleranzahl aus den Entstehungs- und Reparaturprozessen insgesamt.
FC_{PT}	Fehlerabdeckung aller Vortests zusammen.
$\zeta_{\mathrm{F}}(N_0)$	Fehlfunktionsrate nach Beseitigung der von Vortests erkannten Fehler.

Der Zufallstest nach dem Vortest

... erhöht die Testanzahl auf $N > N_0$. Für jede Testanzahl $N > N_0$ bzw. $N_1 \geq N_0$ und $N_2 > N_0$ gelten die Gleichungen:

(2.16) $$\mu_F(N_2) = \mu_F(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit} \quad 0 < K < 1$$

(2.19) $$\zeta_F(N_2) = \zeta_F(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-(K+1)}$$

(2.21) $$\zeta_F(N) = \frac{\mu_F(N) \cdot K}{N}$$

Fehlerbezogenen Teilzuverlässigkeit als Kehrwert der MF-Rate:

$$R_F(N) = \frac{N}{K \cdot \mu_F(N)} \tag{2.25}$$

$$R_F(N_2) = R_F(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{K+1} \tag{2.26}$$

$\zeta_F(N)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.
N_1, N_2	Testanzahl mit bekannter / gesuchter Fehlfunktionsrate oder Fehleranzahl.
$\mu_F(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
$R_F(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehler.

Zuverlässigkeit [mit Fehlfunktionsbehandlung]

(2.21) $$\zeta_{\mathrm{F}}(N) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{N}$$

(2.26) $$R_{\mathrm{F}}(N_2) = R_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{K+1}$$

Zuverlässigkeit mit MF-Behandlung und MF durch Störungen:

$$R_{\mathrm{MT}}(N) = \frac{1}{(\zeta_{\mathrm{F}}(N) + \zeta_{\mathrm{D}}) \cdot (1 - MC)} \tag{2.27}$$

Wenn Fehlfunktionen durch Störungen vernachlässigbar sind:

$$R_{\mathrm{MT}}(N) = \frac{N}{K \cdot \mu_{\mathrm{F}}(N) \cdot (1 - MC)} \tag{2.28}$$

$$R_{[\mathrm{MT}]}(N_2) = R_{[\mathrm{MT}]}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{K+1} \tag{2.29}$$

$R_{\mathrm{F}}(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehler.
$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
ζ_{D}	Fehlfunktionsrate durch Störungen (Malfunction rate due to disturbance).
MC	Fehlfunktionsabdeckung (malfunction coverage), Anteil nachweisbare Fehlfunktionen.
N_1, N_2	Testanzahl mit bekannter oder gesuchter Zuverlässigkeit.
K	Formfaktor der Dichte der Fehlfunktionsrate $(0 < K < 1)$.

Beispiel 2.3: Zuverlässigkeit dreifacher Testaufwand

a) *Um welchen Faktor verringern sich MF-Rate $\zeta_{\mathrm{F}}(N)$ und Fehleranzahl $\mu_{\mathrm{F}}(N)$, wenn die Anzahl der dynamischen Tests verdreifacht wird? Formfaktoren der Verteilung der MF-Rate $K \in \{0{,}3,\ 0{,}5\}$.*

b) *Welche Erhöhung der Zuverlässigkeit ist unter Vernachlässigung der Fehlfunktionen durch Störungen zu erwarten, wenn das Personal der Testabteilung verdreifacht wird?*

$\zeta_{\mathrm{F}}(N)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Testanzahl.
$\mu_{\mathrm{F}}(N)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
K	Formfaktor der Dichte der Fehlfunktionsrate $(0 < K < 1)$.
$R(N)$	Zuverlässigkeit nach Beseitigung aller mit den N Tests nachweisbaren Fehler.

a) *Um welchen Faktor verringern sich MF-Rate $\zeta_{\mathrm{F}}(N)$ und Fehleranzahl $\mu_{\mathrm{F}}(N)$, wenn die Anzahl der dynamischen Tests verdreifacht wird? Formfaktoren der Verteilung der MF-Rate $K \in \{0{,}3,\ 0{,}5\}$.*

Geschätzte Reduzierung der MF-Rate und der Fehlerzahl sowie die Erhöhung der Zuverlässigkeit als Kehrwert der MF-Rate:

$$\frac{\mu_{\mathrm{F}}(3\cdot N)}{\mu_{\mathrm{F}}(N)} = 3^{-K};\quad \frac{\zeta_{\mathrm{F}}(3\cdot N)}{\zeta_{\mathrm{F}}(N)} = 3^{-(K+1)};\quad \frac{R_{\mathrm{F}}(3\cdot N)}{R_{\mathrm{F}}(N)} = 3^{K+1}$$

	$\frac{\mu_{\mathrm{F}}(3\cdot N)}{\mu_{\mathrm{F}}(N)}$	$\frac{\zeta_{\mathrm{F}}(3\cdot N)}{\zeta_{\mathrm{F}}(N)}$	$\frac{R_{\mathrm{F}}(3\cdot N)}{R_{\mathrm{F}}(N)}$
$K = 0{,}3$	0,72	0,24	4,17
$K = 0{,}5$	0,56	0,19	5,19

Die Fehleranzahl verringert sich auf 56% bis 72% und die Fehlfunktionsrate durch nicht beseitigte Fehler auf 19% bis 24%.
Die Rechengröße K kennen wir in der Regel nicht so genau. Für die Abnahme der Fehleranzahl hat K einen großen, aber für die Abnahme die Zuverlässigkeitsverbesserung nur moderaten Einfluss.

Geschätzte Reduzierung der MF-Rate und der Fehlerzahl sowie die Erhöhung der Zuverlässigkeit als Kehrwert der MF-Rate:

$$\frac{\mu_{\mathrm{F}}(3\cdot N)}{\mu_{\mathrm{F}}(N)} = 3^{-K}; \quad \frac{\zeta_{\mathrm{F}}(3\cdot N)}{\zeta_{\mathrm{F}}(N)} = 3^{-(K+1)}; \quad \frac{R_{\mathrm{F}}(3\cdot N)}{R_{\mathrm{F}}(N)} = 3^{K+1}$$

	$\frac{\mu_{\mathrm{F}}(3\cdot N)}{\mu_{\mathrm{F}}(N)}$	$\frac{\zeta_{\mathrm{F}}(3\cdot N)}{\zeta_{\mathrm{F}}(N)}$	$\frac{R_{\mathrm{F}}(3\cdot N)}{R_{\mathrm{F}}(N)}$
$K = 0{,}3$	0,72	0,24	4,17
$K = 0{,}5$	0,56	0,19	5,19

b) *Welche Erhöhung der Zuverlässigkeit ist unter Vernachlässigung der Fehlfunktionen durch Störungen zu erwarten, wenn das Personal der Testabteilung verdreifacht wird?*

Wenn 3-facher Personaleinsatz den dreifachen Testaufwand impliziert, zu erwartende Erhöhung der Zuverlässigkeit auf etwa das 4- bis 5-fache.

Effektive Testanzahl

Effektive Testanzahl

In den bisherigen Abschätzungen ist N die Anzahl der Tests, für die alle erkennbaren Fehler beseitigt werden. Es gibt jedoch Fehlerbeseitigungsiterationen, bei denen ein Fehler

- erst beseitigt wird, wenn er im Mittel $c \gg 1$ Fehlfunktionen verursach (Reifeprozesse),
- bereits erkannt und beseitigt wird, wenn er im Mittel $c \ll 1$ Fehlfunktion verursacht (modularer Test) oder
- die mittlere MF-Rate je Fehler beim Test größer oder kleiner als in der Anwendung sein kann (FC-Abschätzung mit Modellfehlern).

Modellierung durch Umrechnung der tatsächlichen Testanzahl N_T in die effektive Testanzahl N, für die alle erkannten Fehler beseitigt werden:

$$N = c \cdot N_\mathrm{T} \tag{2.30}$$

N	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
N_T	Tatsächliche Testanzahl.
c	Testskalierung, Verhältnis von effektiver und tatsächlicher Testanzahl.

In den Abschätzungen

(2.16) $$\mu_{\mathrm{F}}\left(N_2\right) = \mu_{\mathrm{F}}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit} \;\; 0 < K < 1$$

(2.19) $$\zeta_{\mathrm{F}}\left(N_2\right) = \zeta_{\mathrm{F}}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{-(K+1)}$$

(2.29) $$R_{[\mathrm{MT}]}\left(N_2\right) = R_{[\mathrm{MT}]}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{K+1}$$

ist das Verhältnis der effektiven Testanzahl gleich dem der tatsächlichen Testanzahl:

$$\frac{N_2}{N_1} = \frac{c \cdot N_{\mathrm{T}.2}}{c \cdot N_{\mathrm{T}.1}} = \frac{N_{\mathrm{T}.2}}{N_{\mathrm{T}.1}} \tag{2.31}$$

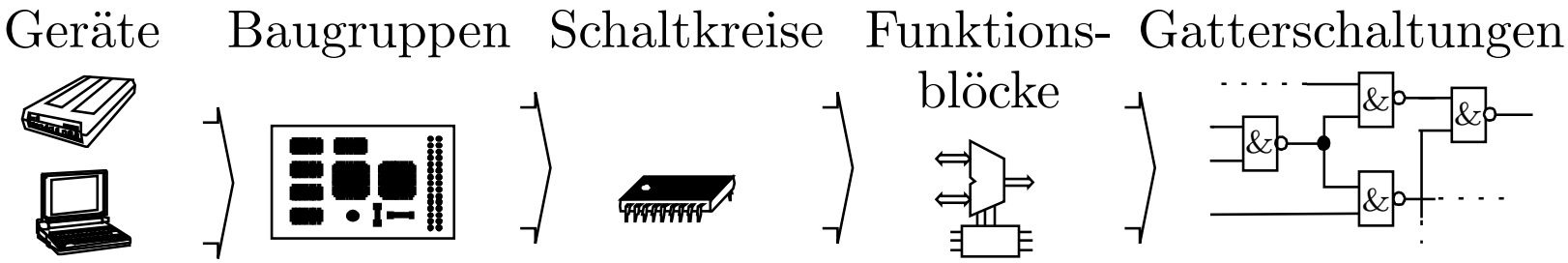
Nur in (Gl. 2.21) hat die Testskalierung Einfluss:

$$\zeta_{\mathrm{F}}\left(N_{\mathrm{T}}\right) = \frac{K \cdot \mu_{\mathrm{F}}(N)}{N} = \frac{K \cdot \mu_{\mathrm{F}}(c \cdot N_{\mathrm{T}})}{c \cdot N_{\mathrm{T}}} \tag{2.32}$$

$\mu_{\mathrm{F}}\left(N\right)$	Zu erwartende Anzahl der Fehler, die nach N Tests nicht erkannt und beseitigt sind.
N_1, N_2	(Effektive) Testanzahl mit bekannter / gesuchter Fehlfunktionsrate oder Fehleranzahl.
$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
N, N_{T}	Effektive Testanzahl, tatsächliche Testanzahl.
c	Testskalierung, Verhältnis von effektiver und tatsächlicher Testanzahl.

Modularer Test

Modularer Test

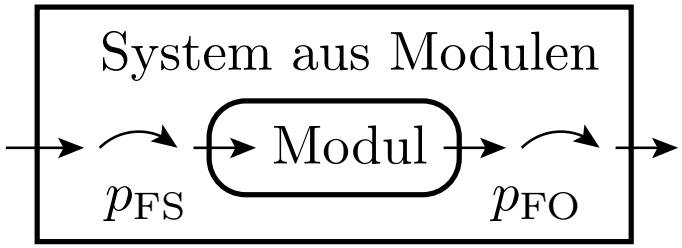


- Rechner-Systeme bestehen aus Rechnern, EA-Geräten, Druckern, Netzwerkkomponenten, diese aus ...
- Die Hardware stellt der SW Grundfunktionen (Maschinenbefehler, EA-Einheiten, ...).
- Software gliedert sich in Teilsysteme, Module, Bibliotheken, ...

Die durchgeführten Tests folgen der Hierarchie. Wenn möglich, werden die Bausteine vor Übernahme in das übergeordnete System gründlich getestet (siehe Abschn. 2.1.4 *Vielfalt der Tests*).

Der übergeordnete Test zielt hauptsächlich nur Fehler beim Zusammenwirken (siehe Folie Leiterplattentest, Abschn. 2.1.6).

Der Grund ist deutlich größere effektive Testanzahl von Modultests.



Modulinterne Fehler werden bei Einbettung in ein übergeordnetes System im Mittel um eine Anregungswahrscheinlichkeit p_{FS} seltener angeregt und fehlerverursachte Verfälschungen am Modulausgang verfälschen nur mit einer Beobachtbarkeit $p_{\mathrm{FO}} \leq 1$ die Systemausgabe. Die zu erwartende Anzahl der Fehlfunktionen beim Modultests und damit die effektive Testanzahl sind $\frac{1}{p_{\mathrm{FS}} \cdot p_{\mathrm{FO}}}$ mal größer als nach Einbettung:

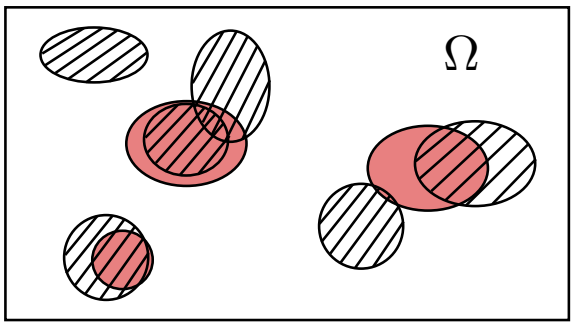
$$N = c \cdot N_{\mathrm{M}} \quad \text{mit} \quad c = \frac{1}{p_{\mathrm{FS}} \cdot p_{\mathrm{FO}}} \gg 1 \tag{2.33}$$

Hierarchische Tests erzielen mit demselben Gesamttestaufwand in der Regel deutlich höhere Fehlerüberdeckungen.

p_{FS}	Fehleranregungswahrscheinlichkeit (Probability of fault stimulation).
p_{FO}	Fehlerbeobachtbarkeitswahrscheinlichkeit (Probability of fault observation).
N	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
c, N_{M}	Testskalierung, Anzahl der Modultests.

Fehlermodellskalierung

Fehler und Modellfehler



Ω Ereignisraum, hier Menge der möglichen Eingaben bzw. Eingabefolgen.

Nachweismenge eines Modellfehlers

Nachweismenge eines tatsächlichen Fehlers

Ein gutes Fehlermodell generiert für (fast) alle zu erwartenden Fehler Mengen ähnlich nachweisbare Modellfehler, die sich Anregungs- und Beobachtungsbedingungen teilen. Effektive Testanzahl:

$$N = c \cdot N_{\mathrm{MF}}$$

- $c < 1$: Modellfehler tendentiell schlechter,
- $c \approx 1$: Modellfehler tendentiell ähnlich gut,
- $c > 1$: Modellfehler tendentiell besser

nachweisbar als die tatsächlich zu erwartenden Fehler möglich.

N, c	Effektive Testanzahl, Testskalierung.
N_{MF}	Testanzahl, mit der die Modellfehlerüberdeckung bestimmt wird.

Die zu erwartende Fehlerabdeckung tendiert zur zu erwartenden Modellfehlerabdeckung der c-fachen Testanzahl:

$$N = c \cdot N_{\mathrm{MF}} \quad \text{für } \mu_{\mathrm{FC}}(N) = \mu_{\mathrm{FCM}}(N_{\mathrm{MF}}) \tag{2.34}$$

Auf die Abnahme der MF-Rate (Gl. 2.29) und der Fehleranzahl (Gl. 2.16) und auch die Abnahme der zu erwartenden Fehlerabdeckung mit einer relativen Erhöhung der Testanzahl $\frac{N_2}{N_1}$ hat die Testanzahlskalierung c wieder keinen Einfluss.

In Abschn. 6.1.3 wird später beispielhaft gezeigt, dass zu erwartende Schaltkreisfehler (Kurzschlüsse, Unterbrechungen, Transistorfehler) tendentiell doppelt so große Nachweismengen wie die ähnlich nachweisbaren Haftfehler haben. Das lässt als grober Richtwert Testskalierung $c \approx 0{,}5$ erwarten, d.h. für dieselbe echte Fehlerüberdeckung genügen halb so viele Tests wie über eine Fehlersimulation abgeschätzt. (Mehr Testen, als unbedingt erforderlich, ist natürlich immer erlaubt.)

N, c	Effektive Testanzahl, Testskalierung.
N_{MF}	Testanzahl, mit der die Modellfehlerüberdeckung bestimmt wird.
μ_{FC}	Zu erwartende Fehlerabdeckung.
μ_{FCM}	Zu erwartende Modellfehlerabdeckung.

Reifen von Produkten

Das Problem immer größerer IT-Systeme

Die zu erwartende Fehleranzahl wächst proportional zur Systemgröße bzw. zum Entstehungsaufwand (siehe später Abschn. 2.3.1):

(2.45) $$\mu_{\mathrm{CF}} = \xi_{<\mathrm{C}>} \cdot C$$

Nach Beseitigung der von den Vor- und Zufallstest gefundenen Fehler:

(2.23) $$\mu_{\mathrm{F}}\left(N_0\right) = \mu_{\mathrm{FCR}} \cdot \left(1 - FC_{\mathrm{PT}}\right)$$

(2.16) $$\mu_{\mathrm{F}}\left(N_2\right) = \mu_{\mathrm{F}}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit} \quad 0 < K < 1$$

(2.21) $$\zeta_{\mathrm{F}}\left(N\right) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{N}$$

Zuverlässigkeitsabnahme mit Systemgröße / Entstehungsaufwand:

$$R_{\mathrm{F}}\left(N\right) = \frac{N}{K \cdot \mu_{\mathrm{F}}(N_0)} \cdot \left(\frac{N}{N_0}\right)^{K} = \ldots \sim \frac{N^{K+1}}{C}$$

$\xi_{<\mathrm{C}>}$	Fehlerentstehungsrate in Fehlern je Bezugsgröße der Metrik C.
μ_{CF}	Zu erwartende Anzahl der Fehler aus den Entstehungsprozessen.
C	Metrik für den Entstehungsaufwand oder die Größe des Produkts.
μ_{FCR}	Zu erwartende Fehleranzahl aus den Entstehungs- und Reparaturprozessen insgesamt.
Aussprache:	ξ: xi, μ: my.

Zuverlässigkeitsabnahme mit der Systemgröße C:

$$R_{\mathrm{F}}(N) \sim \frac{N^{K+1}}{C}$$

Die Kompensation des Zuverlässigkeitsverlust durch den immer größeren Entstehungsaufwand bzw. die wachsende Systemgröße, beschrieben durch die Metrik C, verlangt eine immer größere effektive Testanzahl N.

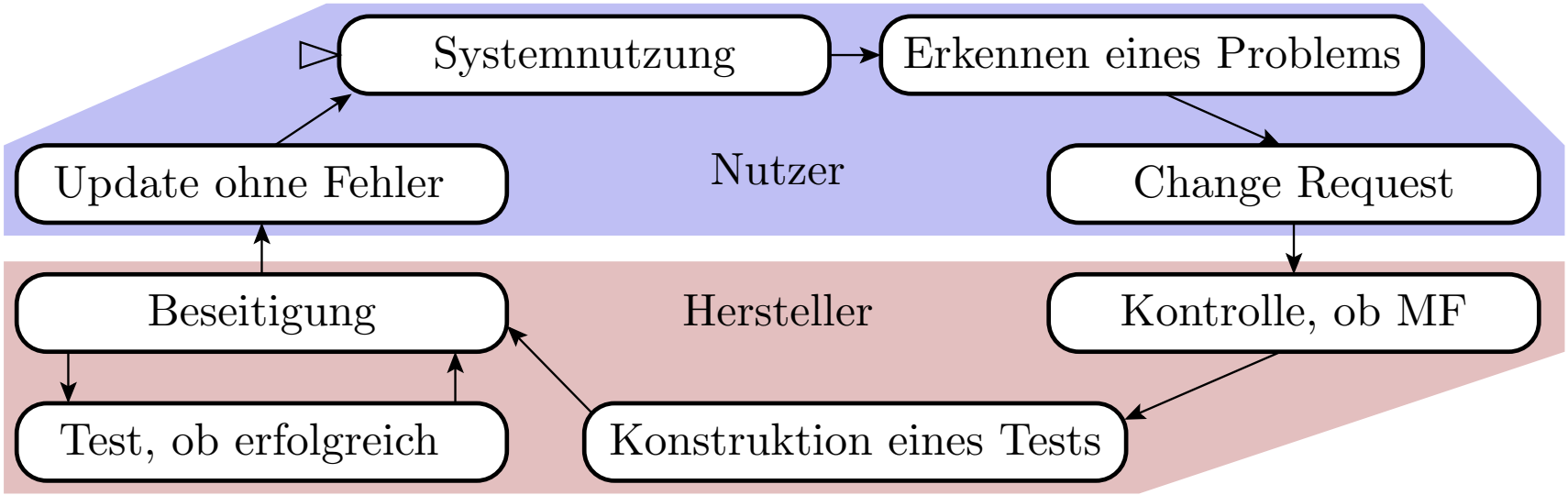
Die Größe C der IT-Systeme nimmt über die Jahre exponentiell zu, der erbringbare Testaufwand N ist durch Zeit und Personal begrenzt.

Was tun gegen den drohenden Zuverlässigkeitsverlust?

$R_{\mathrm{F}}(N)$	Fehlerbezogene Teilzuverl. nach Beseitigung aller mit N Tests nachweisbaren Fehler.
N	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
K	Formfaktor der Dichte der Fehlfunktionsrate $(0 < K < 1)$.
C	Metrik für den Entstehungsaufwand oder die Größe des Produkts.

Reifen der Produkte in der Einsatzphase

Alternative zu immer längeren Testzeiten vor dem Einsatz ist die Fortsetzung der Fehlerbeseitigung im Einsatz mit den Nutzern als Tester.



- Erfassen der MF in der Einsatzphase.
- Sammeln der Daten, um die MF nachzustellen.
- Übermittlung an den Hersteller.
- Suche von Tests für einen reproduzierbaren Fehlernachweis.
- Beseitigung durch experimentelle Reparatur.
- Herausgabe und Installieren von Updates.

Fehlerbeseitigungswahrscheinlichkeit

Die Fehlerbeseitigungswahrscheinlichkeit p_{FE} ist die bedingte Wahrscheinlichkeit, dass, wenn eine Fehlfunktion (MF) auftritt,

1. Nutzer oder System diese erkennen,
2. an den Hersteller einen MF-Report bzw. Änderungswunsch (Change Request) senden,
3. die vermeindliche MF vom Hersteller als solche bestätigt und für die Beseitigung priorisiert wird,
4. der Hersteller Tests für den Nachweis der MF findet,
5. den verursachenden Fehler findet und beseitigt und
6. der Anwender das Update, in dem der Fehler beseitigt ist, übernimmt.

Zu 3: MF-Reports werden in Schubladen vermuteter gleicher Ursache gesammelt. Der Hersteller bevorzugt für die Beseitigung Schubladen, die Fehler mit häufigen schwerwiegenden MF vermuten lassen.

Die Wahrscheinlichkeit p_{FE}, dass ein Fehler beseitigt wird, wenn er eine MF verursacht, ist gering.

Effektive Testanzahl

Reifende Produkte werden von vielen Nutzern über lange Zeit mit unzähligen Beispieleingaben genutzt. Geschätze effektive Testanzahl:

$$N = p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot (t_{\mathrm{M}} + t_{\mathrm{V0}}) \quad \text{mit} \quad t_{\mathrm{V0}} = \frac{N_{\mathrm{V0}}}{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}}} \tag{2.35}$$

Genau genommen nimmt die effektive Testanzahl nicht kontinuierlich mit der Reifedauer zu, sondern zeitdiskret mit den Versionsfreigaben. Zunahme der effektiven Testanzahl mit der Versions-Anzahl bei gleich langen Release-Intervallen:

$$N = \underbrace{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot t_{\mathrm{VR}}}_{N_{\mathrm{MV}}} \cdot (u + u_{\mathrm{V0}}) \quad \text{mit} \quad u_{\mathrm{V0}} = \frac{N_{\mathrm{V0}}}{N_{\mathrm{VM}}} \tag{2.36}$$

N	Effektive Testanzahl, für die alle erkannten Fehler beseitigt werden.
p_{FE}	Wahrscheinlichkeit, dass ein Fehler beseitigt wird, wenn er eine MF verursacht.
μ_{NU}	Zu erwartende Nutzeranzahl (Expected **n**umber of **u**ser).
η_{SU}	Mittlere Anzahl der **S**ervice-Leistungen pro Nutzer (**u**ser) und Nutzungszeit.
t_{M}	Reifedauer (Maturing time).
N_{V0}	Effektive Testanzahl von Version 0, d.h. der Fehlerbeseitigungsiteration vor dem Einsatz.
t_{VR}	Versionsintervall, Zeit zwischen der Freigabe aufeinanderfolgender Version.
N_{MV}	Erhöhung der effektive Testanzahl mit jeder Version.
u	Versionsnummer des reifenden Objekts, Zählweis 0, 1, 2, ...
Aussprache:	μ: my, η: eta.

Abnahme der Fehleranzahl mit der Reifedauer

Der Abschnitt betrachtet nur der vereinfachte Fall, dass bei der Fehlerbeseitigung keine neuen Fehler entstehen bzw. neue entstandene Fehler vor Versionsfreigabe gefunden und beseitigt werden. Ausgehend von

(2.16) $$\mu_\mathrm{F}\left(N_2\right) = \mu_\mathrm{F}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit} \;\; 0 < K < 1$$

mit Gl. 2.35 bzw. 2.36 nimmt die zu erwartende Fehleranzahl mit der K-ten Potenz der Reifedauer bzw. bei gleich langen Release-Intervallen Versionsanzahl ab:

$$\mu_\mathrm{F}\left(t_\mathrm{M}\right) = \mu_\mathrm{F}\left(t_\mathrm{M0}\right) \cdot \left(\frac{t_\mathrm{M}+t_\mathrm{V0}}{t_\mathrm{M0}+t_\mathrm{V0}}\right)^{-K} \tag{2.37}$$

$$\mu_\mathrm{F}\left(u\right) = \mu_\mathrm{F}\left(v\right) \cdot \left(\frac{u+u_\mathrm{V0}}{v+u_\mathrm{V0}}\right)^{-K} \tag{2.38}$$

$\mu_\mathrm{F}\left(t_\mathrm{M}\right)$	Zu erwartende Anzahl der nicht beseitigten Fehler in Abhängigkeit von der Reifedauer.
t_M0	Bezugsreifedauer.
t_V0	Equivalente Reifedauer vor Freigabe von Version null.
K	Formfaktor der Dichte der Fehlfunktionsrate $(0 < K < 1)$.
$\mu_\mathrm{F}\left(u\right)$	Zu erwartende Fehleranzahl in Version u.
$u,\, v$	Versionnummern und Bezugsversionsnummer des reifenden Objekts.
u_V0	Verhältnis der Reifedauer vor Versionsfreigabe zur Reifedauererhöhung je Version.

Fehlfunktionsrate und Zuverlässigkeit

Die Fehlfunktionsrate durch Fehler nimmt mit der $K+1-$ten Potenz der Reifedauer ab:

$$\zeta_{\mathrm{F}}\left(t_{\mathrm{M}}\right) = \zeta_{\mathrm{F}}\left(t_{\mathrm{M0}}\right) \cdot \left(\frac{t_{\mathrm{M}}+t_{\mathrm{V0}}}{t_{\mathrm{M0}}+t_{\mathrm{V0}}}\right)^{-K} \tag{2.39}$$

$$\zeta_{\mathrm{F}}\left(u\right) = \zeta_{\mathrm{F}}\left(v\right) \cdot \left(\frac{u+u_{\mathrm{V0}}}{v+u_{\mathrm{V0}}}\right)^{-K} \tag{2.40}$$

Durch digitale Verarbeitung, elektromagnetische Verträglichkeit, Datenübertragung und Speicherung mit Prüfkennzeichen, ... sind Fehlfunktionen durch Störungen oft vernachlässigbar. Wenn das der Fall, ist Zuverlässigkeit der Kehrwert der Fehlfunktionsrate durch Fehler:

$$R_{[\mathrm{MT}]}\left(t_{\mathrm{M}}\right) = R_{[\mathrm{MT}]}\left(t_{\mathrm{M0}}\right) \cdot \left(\frac{t_{\mathrm{M}}+t_{\mathrm{V0}}}{t_{\mathrm{M0}}+t_{\mathrm{V0}}}\right)^{K+1} \tag{2.41}$$

$$R_{[\mathrm{MT}]}\left(u\right) = R_{[\mathrm{MT}]}\left(v\right) \cdot \left(\frac{u+u_{\mathrm{V0}}}{v+u_{\mathrm{V0}}}\right)^{K+1} \tag{2.42}$$

$\zeta_{\mathrm{F}}\left(t_{\mathrm{M}}\right)$	Fehlfunktionsrate durch Fehler in Abhängigkeit von der Reifedauer.
$\zeta_{\mathrm{F}}\left(u\right)$	Gesamte Fehlfunktionsrate durch alle Fehler in Version u.
$R_{\mathrm{F}}\left(t_{\mathrm{M}}\right)$	Fehlerbezogene Teilzuverlässigkeit in Abhängigkeit von der Reifedauer.
$R_{\mathrm{F}}\left(u\right)$	Fehlerbezogene Teilzuverlässigkeit in Abhängigkeit von der Versionszahl.

Sicherheit

Wenn bei allen erkannten Problemen ein sicherer Zustand hergestellt wird, ist die Raten der sicherheitsgefährdenden Fehlfunktionen ein Anteil ρ der nicht erkannten Fehlfunktionen:

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

In dem Fall wächst die Sicherheit genau wie die Zuverlässigkeit mit der $K+1$-ten Potenz der Reifedauer:

$$S\left(t_{\mathrm{M}}\right) = S\left(t_{\mathrm{M0}}\right) \cdot \left(\frac{t_{\mathrm{M}}+t_{\mathrm{V0}}}{t_{\mathrm{M0}}+t_{\mathrm{V0}}}\right)^{K+1} \tag{2.43}$$

$$S\left(u\right) = S\left(v\right) \cdot \left(\frac{u+u_{\mathrm{V0}}}{v+u_{\mathrm{V0}}}\right)^{K+1} \tag{2.44}$$

S	Sicherheit (Safety or security).
$R_{[\mathrm{MT}]}$	Zuverlässigkeit mit bzw. ohne Fehlfunktionsbehandlung.
ρ	Anteil sicherheitskritischer Fehlfunktionen an den nicht erkannten Fehlfunktionen.
t_{M0}	Bezugsreifedauer.
t_{V0}	Equivalente Reifedauer vor Freigabe von Version null.
$u,\ v$	Versionnummern und Bezugsversionsnummer des reifenden Objekts.
u_{V0}	Verhältnis der Reifedauer vor Versionsfreigabe zur Reifedauererhöhung je Version.

Systeme mit hoher Zuverlässigkeit

Hohe Zuverlässigkeit und Sicherheit verlangen:

- hohe Zuverlässigkeit bei Produktfreigabe,
- hohe MC der Fehlerfunktionsbehandlung und eine
- eine hohe effektive Testanzahl

(2.35) $$N = p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot (t_{\mathrm{M}} + t_{\mathrm{V0}}) \quad \text{mit} \quad t_{\mathrm{V0}} = \frac{N_{\mathrm{V0}}}{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}}}$$

  - hohe Wahrscheinlichkeit p_{FE}, dass, wenn eine MF beobachtet wird, der verursachenden Fehler beseitigt wird,
  - eine große zu erwartende Anzahl von Nutzern μ_{NU},
  - viele genutzte Service-Leistungen je Nutzer und Zeit η_{ST} und
  - eine lange Reifezeit t_{M}.

Systeme, die viele Jahre gereift sind, haben hohe, auf anderem Wege unerreichbare Zuverlässigkeiten und Sicherheiten. Schwer ersetzbar durch neue Systeme (siehe Jahr2000-Problem).

Neue / alternative Systeme sind in den ersten Nutzungsjahren vielfach viel unzuverlässer als die Systeme, die sie ersetzen. Wenn das die Akzeptanz beeinträchtigt, reifen sie auch nicht.

MF-Vermeidung – Lernprozesse der Nutzer

Bei der Einarbeitung in ein neues IT-System ist es typisch, dass zu Beginn häufig und mit zunehmender Nutzung immer seltener Fehlfunktionen auftreten, weil die Nutzer lernen, die Fehler und Schwachstellen im System zu umgehen (siehe Folie Fehlerumgehung, Abschn. 1.2.3). Auch hier ist ein Zuverlässigkeitswachtum mit der Nutzungdauer zu beobachten.

Wenn Wissen über Fehlerumgehungsmöglichkeiten weitergegeben wird, z.B. über Foren oder FAQ-Seiten, lernt die gesamte Nutzergemeinschaft. Summierung der Nutzungsdauern vieler Nutzer.

Zusammenfassung

Entstehung, Vor- und Zuverlässigkeitstest

In den Entstehungs- und Fehlerbeseitigungsprozesse entehen insgesamt im Mittel μ_{FCR} Fehler. Davon erkennt ein Vortests aus

- statisch Tests (Reviews, Syntax, ...)
- dynamischen Grobtests, ob überhaupt etwas funktioniert,
- fehlerorientierten Tests z.B. für Grenzwerte, ...

mit N_0 enthaltenen dynamischen Tests einen Anteil FC_{PT}, der beseitigt beseitigt wird. Verbleibende Fehleranzahl und Fehlfunktionsrate:

(2.23) $$\mu_{\mathrm{F}}\left(N_0\right) = \mu_{\mathrm{FCR}} \cdot \left(1 - FC_{\mathrm{PT}}\right)$$

(2.24) $$\zeta_{\mathrm{F}}\left(N_0\right) = \frac{K \cdot \mu_{\mathrm{F}}(N_0)}{N_0} \ll 1$$

Eine Fortsetzung der Fehlerbeseitigungsiteration verlängert die effektive Testanzahl vom Bezugswerte N_0 auf ein Wert N. Abnahme der Fehleranzahl mit Exponent $0 < K < 1$:

(2.16) $$\mu_{\mathrm{F}}\left(N_2\right) = \mu_{\mathrm{F}}\left(N_1\right) \cdot \left(\frac{N_2}{N_1}\right)^{-K} \quad \text{mit } \; 0 < K < 1$$

(Der Zuwachs $\frac{N_2}{N_1}$ ist hier im Kontext der Zuwachs $\frac{N}{N_0}$).

Fehlfunktionsrate, Formfaktor, Zuverlässigkeit

(2.21) $$\zeta_{\mathrm{F}}(N) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{N}$$

(2.19) $$\zeta_{\mathrm{F}}(N_2) = \zeta_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{-(K+1)}$$

Der Formfaktor der Verteilung der Fehlfunktionsrate kann sowohl aus der Abnahme der Fehleranzahl als auch aus der Abnahme der Fehlfunktionsrate abgeschätzt werden:

(2.17) $$K = -\log\left(\frac{\mu_{\mathrm{F}}(N_2)}{\mu_{\mathrm{F}}(N_1)}\right) / \log\left(\frac{N_2}{N_1}\right)$$

(2.22) $$K = \log\left(\frac{\zeta_{\mathrm{F}}(N_1)}{\zeta_{\mathrm{F}}(N_2)}\right) / \log\left(\frac{N_2}{N_1}\right) - 1$$

Die fehlerbezogene Teilzuverlässigkeit ist der Kehrwert der Fehlfunktionsrate durch Fehler:

(2.20) $$\zeta_{\mathrm{F}}(N) = \frac{\mu_{\mathrm{F}}(N) \cdot K}{(K+1) \cdot N}$$

(2.26) $$R_{\mathrm{F}}(N_2) = R_{\mathrm{F}}(N_1) \cdot \left(\frac{N_2}{N_1}\right)^{K+1}$$

Störungen, Fehlfunktionsbehandlung

In die Gesamtzuverlässigkeit fließen zusätzlich die MF-Rate durch Störungen und die Verbesserung durch die Fehlfunktionsbehandlung mit ein:

(2.27) $$R_{\mathrm{MT}}(N) = \frac{1}{(\zeta_{\mathrm{F}}(N)+\zeta_{\mathrm{D}})\cdot(1-MC)}$$

Wenn die MF-Rate durch Störungen vernachlässigbar ist, wächst die Zuverlässigkeit mit der $K+1$-ten Potenz der Testanzahl:

(2.28) $$R_{\mathrm{MT}}(N) = \frac{N}{K\cdot\mu_{\mathrm{F}}(N)\cdot(1-MC)}$$

(2.29) $$R_{[\mathrm{MT}]}(N_2) = R_{[\mathrm{MT}]}(N_1)\cdot\left(\frac{N_2}{N_1}\right)^{K+1}$$

Effektive Testanzahl

Äquivalente Testanzahl, für alle erkannten Fehler beseitigt werden, um einen Skalierungsfaktor c größer oder kleiner als die tatsächliche Testanzahl:

(2.30) $$N = c \cdot N_{\mathrm{T}}$$

- Für modulinteren Fehler ist die effektive Testanzahl der Modultests viel größer als die der Tests in den Systemumgebung:

  (2.33) $$N = c \cdot N_{\mathrm{M}} \quad \text{mit} \quad c = \frac{1}{p_{\mathrm{FS}} \cdot p_{\mathrm{FO}}} \gg 1$$

  Deshalb werden Module vor Einbau gründlich getestet.

- Fehlermodellspezifische Skalierung. Zu erwartende Fehlerabdeckung tendiert zur Modellfehlerabdeckung der c-fachen Testanzahl:

  (2.34) $$N = c \cdot N_{\mathrm{MF}} \quad \text{für } \mu_{\mathrm{FC}}(N) = \mu_{\mathrm{FCM}}(N_{\mathrm{MF}})$$

  - tendentiell besser nachweisbare Modellfehler: $c > 1$
  - tendendtiell schlechter nachweisbare Modellfehler: $c < 1$.
  - Für Haftfehler wird später der Richtwert $c \approx 0{,}5$ abgeschätzt.

- Reifeprozess:

$$c = p_{\mathrm{FE}} \ll 1$$

Reifeprozess

Fortsetzung der Fehlerbeseitigungsiteration in der Einsatzphase mit den Nutzern als Tester.

- Zunahme der effektive Testanzahl mit der Reifedauer:

(2.35) $$N = p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot (t_{\mathrm{M}} + t_{\mathrm{V0}}) \quad \text{mit} \quad t_{\mathrm{V0}} = \frac{N_{\mathrm{V0}}}{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}}}$$

- Zunahme der effektive Testanzahl mit Versionsnummer:

(2.36) $$N = \underbrace{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SU}} \cdot t_{\mathrm{VR}}}_{N_{\mathrm{MV}}} \cdot (u + u_{\mathrm{V0}}) \quad \text{mit} \quad u_{\mathrm{V0}} = \frac{N_{\mathrm{V0}}}{N_{\mathrm{VM}}}$$

- Abnahme der Fehleranzahl mit Exponent K:

(2.37) $$\mu_{\mathrm{F}}(t_{\mathrm{M}}) = \mu_{\mathrm{F}}(t_{\mathrm{M0}}) \cdot \left(\frac{t_{\mathrm{M}} + t_{\mathrm{V0}}}{t_{\mathrm{M0}} + t_{\mathrm{V0}}} \right)^{-K}$$

(2.38) $$\mu_{\mathrm{F}}(u) = \mu_{\mathrm{F}}(v) \cdot \left(\frac{u + u_{\mathrm{V0}}}{v + u_{\mathrm{V0}}} \right)^{-K}$$

Zuverlässigkeit und Sicherheit

Wenn Fehlfunktionen durch Störungen und Ausfälle vernachlässigbar selten sind, nimmt auch die Zuverlässigkeit mit Exponent $K+1$ der Reifedauer zu. Desselbe gilt für die Sicherheit, wenn für alle im laufenen Betrieb erkannten Probleme ein sicherer Zustand hergestellt wird.

- Lange Reifeprozesse über Jahre und Jahrzehnte erzielen auf andere Weise unerreichbare Zuverlässigkeiten und Sicherheiten.
- Alte, lange gereifte Software ist schwer zu ersetzen, weil gleichwertiger Ersatz zuerst lange bei vielen Nutzern reifen muss.

Fehlervermeidung

Fehlerentstehung und -vermeidung

MF-Behandlung	Fehlerbeseitigung	Fehlervermeidung
Überwachung, robuste Reaktion auf erkannte Probleme	Test und Beseitigung erkannter Fehler	Beseitigung von Fehlerentstehungsursachen

- Fehler entstehen in den Entwurf-, Fertigungs- und Reparaturprozessen zusammen mit dem Produkt.
- Entstehungsprozesse sind wie IT-Systeme als Service-Leister modellierbar mit Erbringungsraten ($\Rightarrow$ Ausbeute), Fehlfunktionsraten ($\Rightarrow$ Fehlerenstehungsrate), ...
- Fehlervermeidung ist Problembehandlung (Lernen aus Fehlern) für Entstehungsprozesse auch auf drei Ebenen:
  - Überwachung und robuste Reaktion auf akute Prozessprobleme.
  - Test und Fehlerbeseitigung vor und während der Prozessnutzung.
  - Fehlervermeidung bei der Schaffung neuer Prozessfähigkeiten*.

* Prozessfähigkeiten: Möglichkeiten, was mit den Prozess geschaffen werden kann und Leistungsmerkmale, wie gut, billig, genau, ... das möglich ist (Werkzeuge, Wissen, ...).

Schaffung und Nutzung von Prozessfähigkeiten

Der wissenschaftlich-technische Fortschritt lässt sich als Prozess aus Schaffung und Nutzung von Prozessfähigkeiten modellieren:

- Schaffung: (Weiter-) Entwicklung von Werkzeuge, Verfahren, Kontrollen (incl. Messverfahren), Programmiersprachen, Theorien, Modellen, ... getrennt von der Prozessnutzung.
- Nutzung: Neuer Fähigkeiten »kauft man«, kann sie aber erst schrittweise in einen Lernprozess nutzen. Für die Fehlervermeidung bedeuten neue Prozessfähigkeiten neue Probleme, die in einem Prozess »Lernen aus Fehlern« umgangen oder beseitigt werden.
- Die Erfahrungen bei der Prozessnutzung fließen in die Zielstellungen für die Weiterentwicklung der Prozessfähigkeiten ein.

Kontrollfragen:

- Wie funktioniert die Fehlerumgehung für IT-Systeme?
- Wie und unter welchen Voraussetzungen reifen IT-Systeme?
- Gibt es IT-Entstehungsschritte, die aus Verlässlichkeitssicht wie IT-Systeme modelliert werden können?

Fähigkeiten zum »Lernen aus Fehlern«

MF-Behandlung	Fehlerbeseitigung	Fehlervermeidung

Maßnahmen zur Fehlervermeidung auf allen drei Ebenen

- Überwachung und robuste Reaktion auf erkannte akute Probleme.
- Fehlerbeseitigung vor und **während der Nutzung*** und
- Fehlervermeidung bei der Schaffung der Prozessfähigkeiten.

setzen selbst spezielle Prozessfähigkeiten voraus:

- Kontrolle und Erfassung von Problemen,
- Diagnose- und Änderungsmöglichkeiten, Erfolgskontrollen, ...

Lernen aus Fehlern selbst ist ein extrem arbeitsintensiver stochastischer Prozess, der irgendwann die Prozessfähigkeiten zum Erkennen und Beheben von Problemen ausschöpft.

Ergänzung unserer idealisierten Fehlerkultur**:

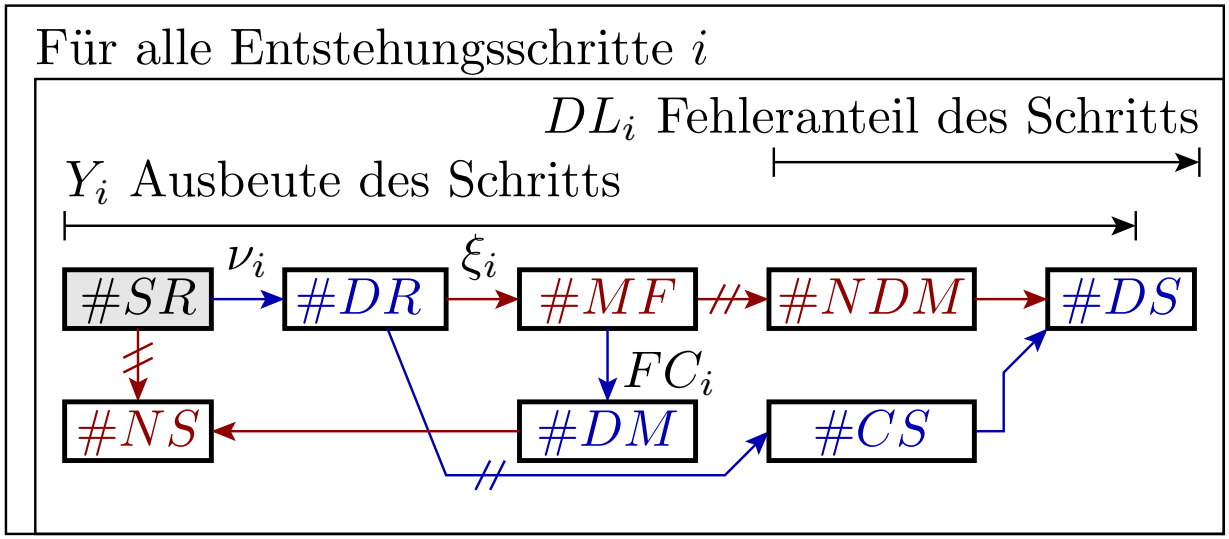
Nutzung aller vorhandenen Fähigkeiten zum »Lernen aus Fehlern.

* Reifeprozess für Prozessfähigkeiten. Darauf wird sich der Abschnitt konzentrieren.

** Vernachlässigung Kosten, Verkaufsaspekte, ... zur Vereinfachung der Modellierung.

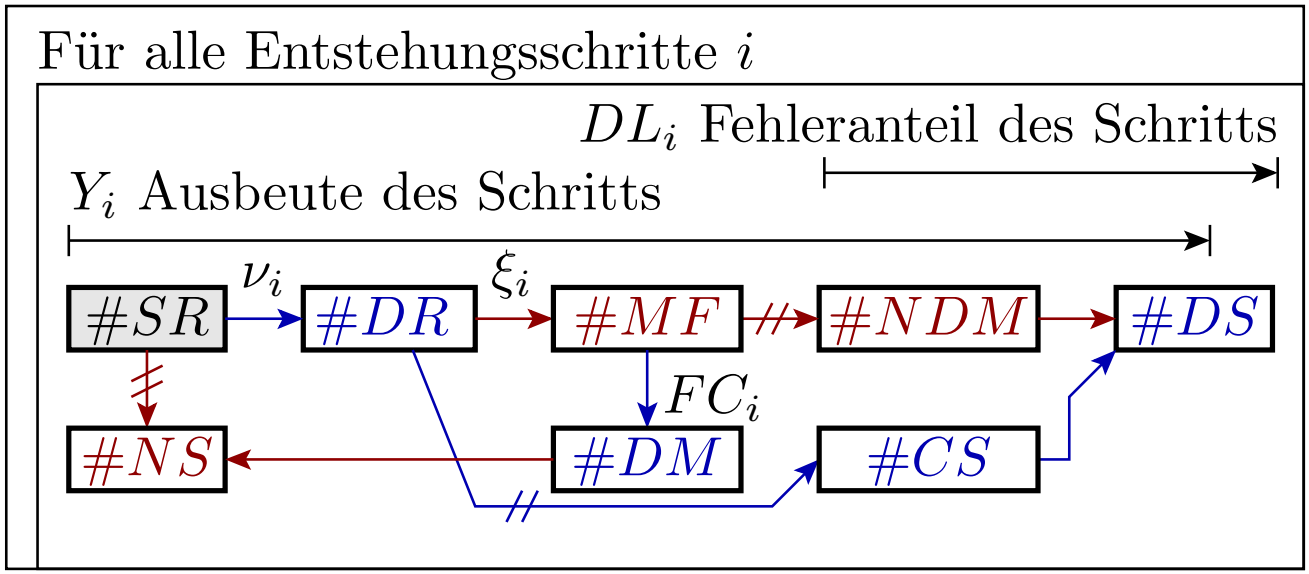
Fehlerentstehung

Fehler als MF der Entstehungsprozesse



SR	Schritt-Anforderung	MF	Fehlfunktion (Prozessfehler)
NS	verweigerte Leistung	DM	erkannter Prozessfehler
DR	erbrachtes Ergebnis	NDM	nicht erkannter Prozessfehler
CS	korrekte Leistung	DS	erbrachte Leistung
ν_i	Erfolgsrate	FC_i	Prozessfehlerabdeckung
ξ_i	Fehlerentstehungsrate	Aussprache: ν: ny, ξ: xi	

Ein Entstehungsprozess besteht aus vielen Schritten, in denen Leistungen erbracht und Fehler entstehen, erkannt und beseitigt werden.



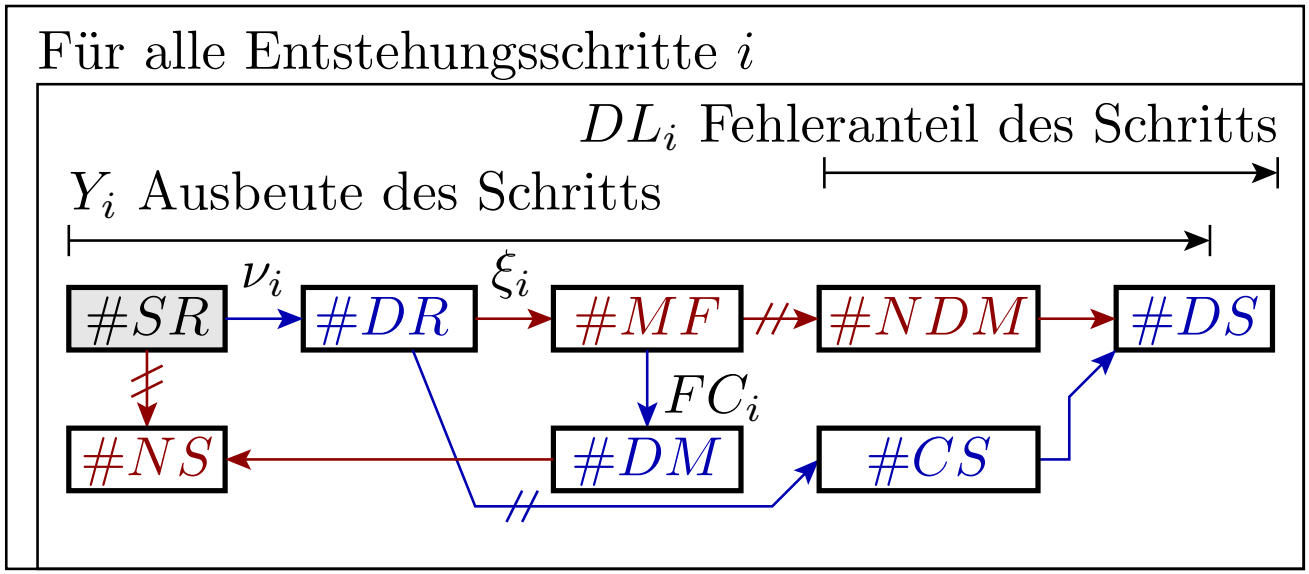
Wenn alle Leistungen mit erkannten Problemen aussortiert werden, hat jeder Schritt eine Ausbeute und einen Fehleranteil:

$$Y_i = \frac{\#DS}{\#SR}\Big|_{\text{ACR}} = \nu_i \cdot ((1-\xi_i) + \xi_i \cdot (1-FC_i)) = \nu_i \cdot (1 - FC_i \cdot \xi_i)$$

$$DL_\text{i} = \frac{\#NDM}{\#DS}\Big|_{\text{ACR}} = \frac{\nu_i \cdot \xi_i \cdot (1-FC_i)}{\nu_i \cdot (1-FC_i \cdot \xi_i)} = \frac{\xi_i \cdot (1-FC_i)}{1-FC_i \cdot \xi_i}$$

- Ein Produkt entsteht, wenn alle Schritte erbracht werden.
- Ein fehlerhaftes Produkt entsteht, wenn in mindestens einem Schritt ein Fehler entsteht.

Fehlerentstehung ist prinzipiell ist wie ein System aus vielen Komponenten modellierbar.



Praktisch setzt die Modellierung von Entstehungsprozessen

- als Folgen von Teilschritten mit zählbaren Problemen und
- bestimmbaren Eintrittsraten, Erkennungsraten, ...

Prozessfähigkeiten voraus, z.B. Determinismus, die nicht da sind.

Keine weitere Vertiefung der Modellierung der Fehlerentstehung durch Zählwertzuordnungsgraphen hier. Ein Beispiel folgt erst auf dem nächsten Foliensatz nach der themenspezifischen Einführung in das Rechnen mit Wahrscheinlichkeiten.

Fehlerentstehungsraten und Metriken

Statt aus den Fehlerentstehungs, -erkennung und -korrekturraten der einzelnen Entstehungsschritte wird die zu erwartende Fehleranzahl in der Regel über Metriken für die Produkt- oder Prozessgröße abgeschätzt:

$$\mu_{\mathrm{CF}} = \xi_{<\mathrm{C}>} \cdot C \tag{2.45}$$

Die verwendeten Metriken sind gut bestimmbare Kenngrößen, z.B.:

- Entwurfsaufwand in Arbeitsstunden,
- Entwurfsumfang in NLOC, Transistoren, Dokumentationsseiten, ...
- Fertigungsaufwand in Arbeitsschritten,
- ...

Die Entstehungsraten ergeben sich umgekehrt aus dem Verhältnis experimentell abgeschätzter Erwartungswerte zum Zahlenwert der Metrik:

$$\xi_{<\mathrm{C}>} = \frac{\mu_{\mathrm{CF}}(C)}{C} \tag{2.46}$$

$\xi_{<\mathrm{C}>}$	Fehlerentstehungsrate in Fehlern je Bezugsgröße der Metrik C.
μ_{CF}	Zu erwartende Anzahl der Fehler aus den Entstehungsprozessen.
C	Metrik für den Entstehungsaufwand oder die Größe des Produkts.
Aussprache:	μ: my, ξ: xi.

Beispiel 2.4: Programmfehler

$\xi_{\mathrm{NLOC}} = 30$ Fehler / 1000 NLOC, Programm mit $C = 2000$ NLOC.

Wie groß ist die zu erwartende Anzahl der Programmierfehler vor Test und Fehlerbeseitigung?

$$\mu_{\mathrm{CF}} = \xi_{\mathrm{NLOC}} \cdot C = \frac{30\,\mathrm{Fehler} \cdot 2000\,\mathrm{NLOC}}{1000\,\mathrm{NLOC}} = 60\,\mathrm{Fehler}$$

Beispiel 2.5: Schaltkreisfehler

$\xi_{\#\mathrm{Tr}} = 1$ Fehler je 10^6 Transistoren. Schaltkreis mit $C = 10^5$ Transistoren.

Wie groß ist die zu erwartende Anzahl der Fehler je Schaltkreis vor dem Aussortieren der erkennbar defekten Schaltkreise?

$$\mu_{\mathrm{CF}} = \xi_{\#\mathrm{Tr}} \cdot C = \frac{1\,\mathrm{Fehler} \cdot 10^5\,\mathrm{Transistoren}}{10^6\,\mathrm{Transistoren}} = 0{,}1\mathrm{Fehler}$$

NLOC Netto Lines of Code, Anzahl der Code-Zeilen ohne Kommentar und Leerzeilen.

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

Wir nehmen in unsere idealisierte Fehlerkultur mit auf*:

Entstehungsprozesse sind so zu gestalten, dass

- offenkundige negative Einflüsse auf die Fehlerentstehungsrate, wie die Zunahme der Fehlerentstehungsrate mit dem Entstehungsaufwand, durch die Prozessgestaltung vermieden werden,
- so dass tatsächlich gilt:

(2.45) $$\mu_{\mathrm{CF}} = \xi_{<\mathrm{C}>} \cdot C$$

(2.46) $$\xi_{<\mathrm{C}>} = \frac{\mu_{\mathrm{CF}}(C)}{C}$$

* Unsere idealisierte Fehlerkultur dient der Modellvereinfachung.

Aussprache: μ: my, ξ: xi.

Metriken sind praktisch bestimmbar. Ihre Brauchbarkeit hängt davon ab, wie gute sie auf die interessierenden Größen

- Problementstehungsraten
- Problemerkennungsraten und
- Problemvermeidungsraten

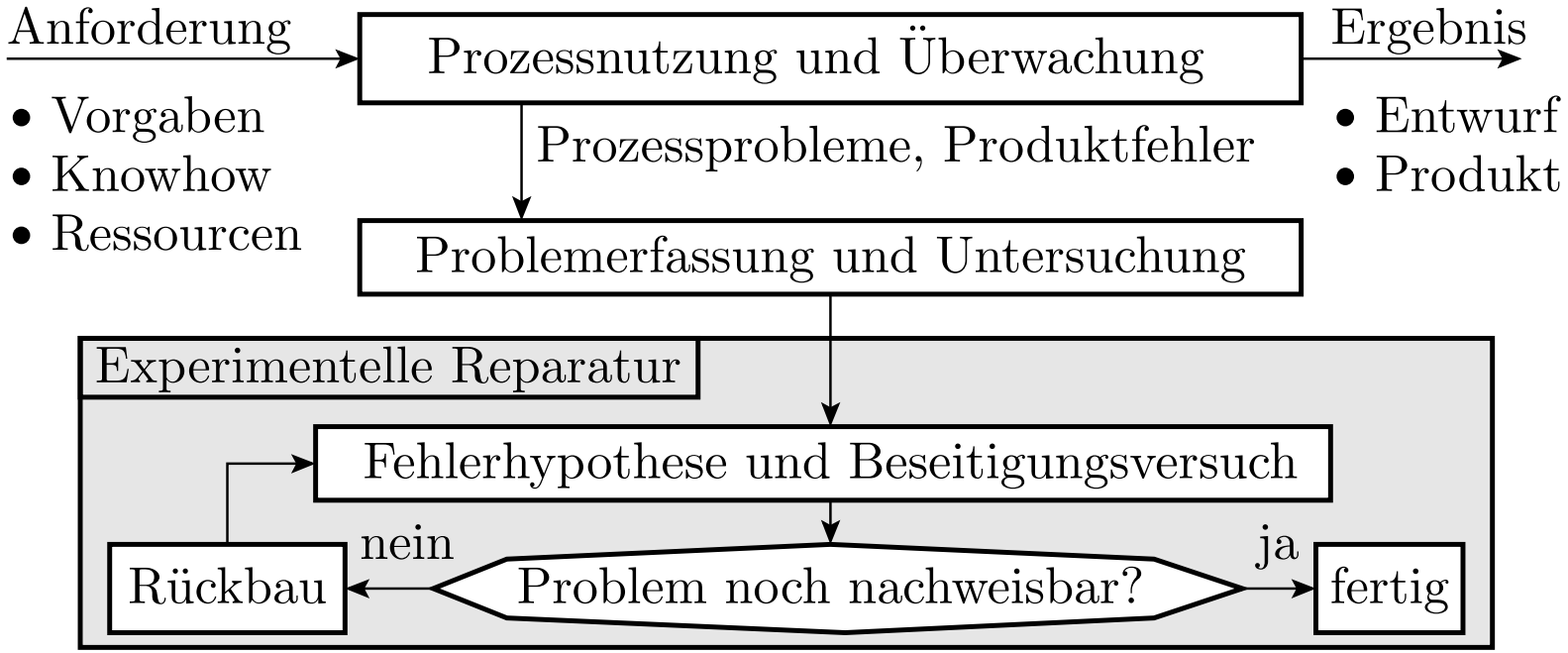
schließen lassen.

Umgekehrt sind bestimmbare Metriken mit Aussagewert, an denen sich Verbesserungen oder Verschlechterungen erkennen lassen, notwendige Prozessfähigkeiten zur Fehlervermeidung, die erst einmal da sein müssen.

Im weiteren werden wir uns auf die Prozessfähigkeiten zur Fehlervermeidung konzentrieren und konkrete Massnahmen nur beispielhaft betrachten.

Reifen von Prozessen

Das Reifen von Entstehungsprozessen

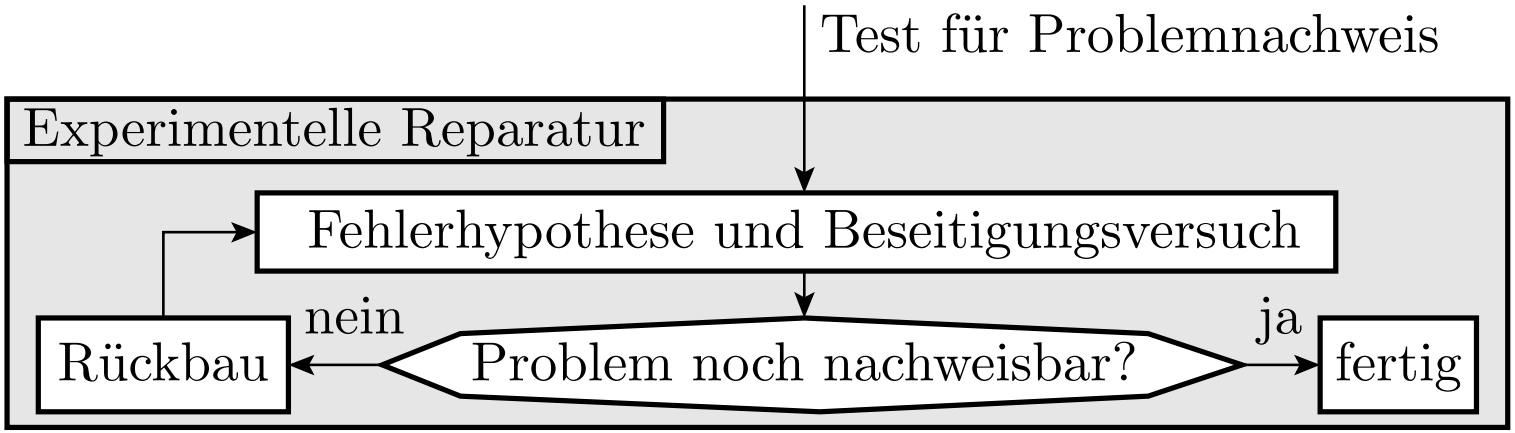


Nach Einführung neuer / verbesserter Fähigkeiten reift ein Entstehungsprozess. Das erfordert Prozessfähigkeiten:

- Große Wiederholrate vergleichbarer Entstehungsleistungen.
- Prozessüberwachung und Problemerfassung.
- Möglichkeite für Erfolgskontrolle, Rückbau, ...

die die Absenkung Fehlerentstehungsraten begrenzen.

Determinismus und Erfolgskontrolle



Insbesondere Fertigungsprozesse und kreative Teile von Entwurfsprozessen sind nicht deterministisch. Auch ohne Fehler entstehen bei Wiederholung mit gleichen Eingaben abweichende Ergebnisse.

Ohne Determinismus fehlen die Prozessfähigkeiten:

- Erfolgskontrolle durch eine einzelne Testwiederholung und
- Rückbau nach allen erfolglosen Beseitigungsversuchen,

Diese müssen durch andere Prozessfähigkeiten ersetzt werden.

Erfolgskontrolle bei fehlendem Determinismus

- Bestimmung von Metriken über viele Prozesswiederholungen und
- Abschätzung von Wahrscheinlichkeiten für besser /schlechter.

Im Vergleich zu deterministischen Prozessen

- Erfolgskontrollen nach jedem Beseitigungsversuch kann statt einem sehr viele Prozessdurchläufe erfordern,
- bei positivem Erfolgskontrollergebnis Beseitigungserfolg unsicher,
- Rate der neu entstehenden je beseitigter Fehler höher.

Die Fähigkeit zur Minimierung der Fehlerentstehungsrate korreliert mit der Fähigkeit, Verbesserungen zu erkennen und diese mit der Fähigkeit Prozessergebnisse vorherzusagen.

Je besser Prozessergebnisse vorhersagbar, je einfacher und aussagekräftig die Erfolgskontrollen, ... desto geringere Fehlerentstehungsraten kann ein Reifeprozess erzielen*.

* Unsere idealisierte Fehlerkultur unterstellt, dass die Fähigkeiten genutzt werden und die Fehlerentstehungsrate ohne Rücksicht auf Zeit und Kosten auf das erreichbare Minimum abgesenkt wird.

Prozesszentrierung

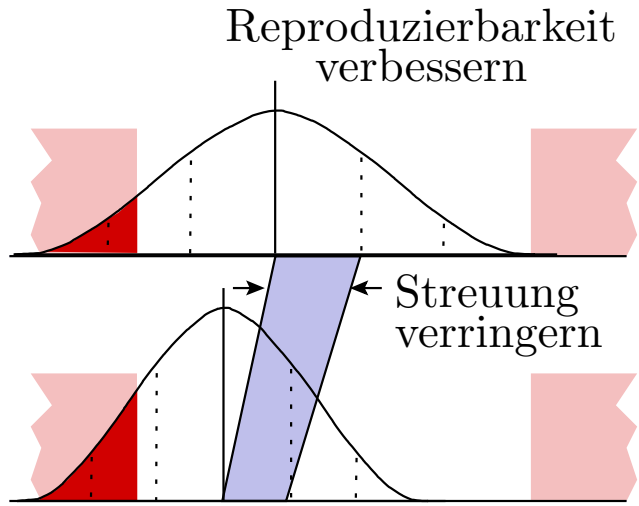
Einfaches Beispiel für die komplexen Zusammenhänge zwischen

- Fähigkeiten und
- Fehlerentstehungsrate

ist ein mechanischer Fertigungsschritt mit einem streuenden Parameter z.B. dem Durchmesser einer Bohrung.

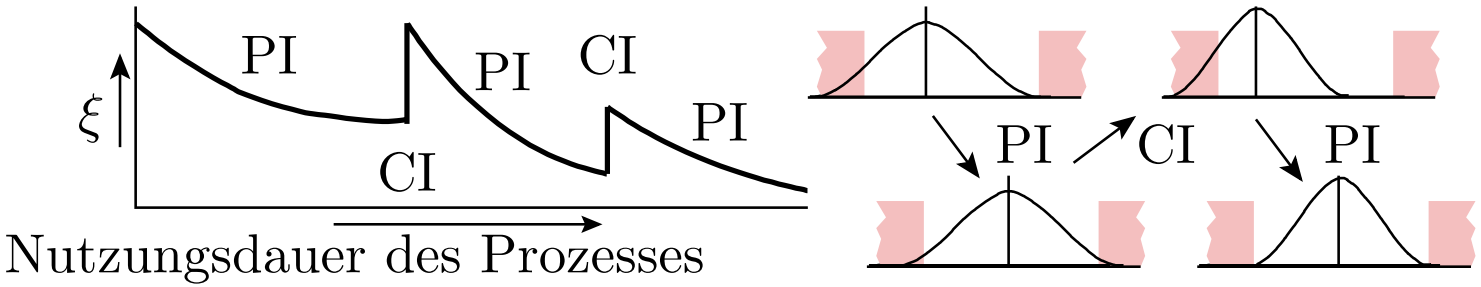
Die Fehlerentstehungsrate ist hier die Wahrscheinlichkeit, dass der Parameterwert nicht im Toleranzbereich liegt:

- Prozesszentrierung: Verschiebung der Verteilung mit Hilfe von Einstelloptionen in die Mitte des Toleranzbereichs.
- Fähigkeitsverbesserung: Verringerung der Streuung durch technologische Neuerungen neue Maschinen, Verfahren, ...



* Arbeitsaufwändiger Prozess, bei dem nach dem Prinzip der experimentellen Reparatur viele Prozesseinstellungen durchprobiert werden (Ameisarbeit).

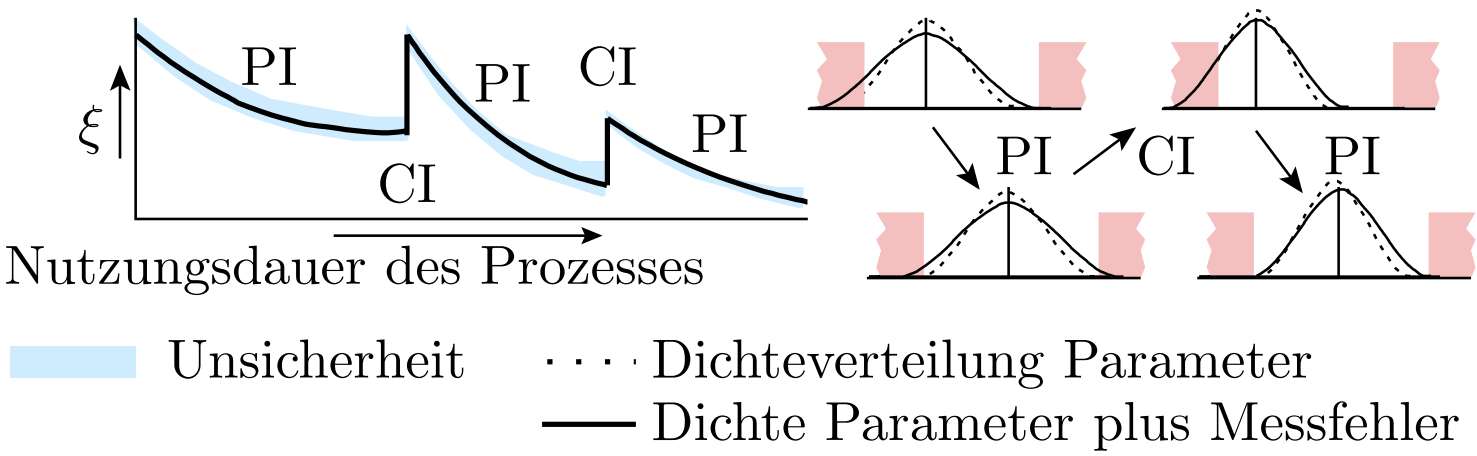
Sägzahnverlauf der Fehlerentstehungsrate



- Die Fähigkeitsverbesserung schafft die Möglichkeit, Toleranzen besser einzuhalten, aber bei Neuerungen geht die Zentrierung verloren. Sprunghafte Zunahme der Fehlerenstehungsrate.
- Während der Prozessnutzung Nachjustierung an den Einstellmöglichkeiten zur Verschiebung des Erwartungswerts in die Mitte des Toleranzfensters. Abnahme der Fehlerenstehungsrate.

CI, PI Fähigkeitsverbesserung, Prozessverbesserung.

Schätz- und Messgenauigkeiten

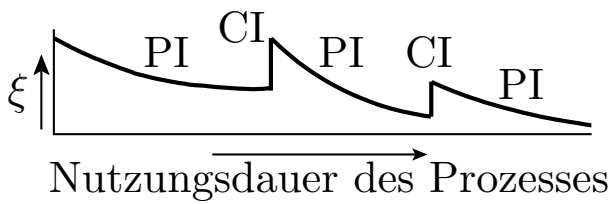


Schätzwerte von Fehlerentstehungsraten, aber auch einzelne Messergebnisse sind eine Summe aus Wert und Schätz- bzw. Messfehlern (siehe Abschn. 4.1.4). Schätz- und Messfehler verursachen Fehleinschätzungen:

- Beibehaltung von Verschlechterungen oder
- Rückbau nach Verbessserungen.

Je geringer die Schätz- und Messfehler, desto größer die Fähigkeit des Prozesses zur Fehlervermeidung.

CI, PI Fähigkeitsverbesserung, Prozessverbesserung.



- Fähigkeitsverbesserung in größeren Zeitschritten und
- Reifen durch »Lernen aus Fehlern« in kleinen Schritten

ist typisch für alle technologischen Prozesse* incl. für Entwurfs- und Fertigungsprozesse von IT-Systeme.

Fähigkeitsverbesserung beinhaltet neben Funktionalität, Rechenleistung, Kosten auch die für geringe erzielbare Fehlerentstehungsraten wichtigen Fähigkeiten Vorhersagbarkeit und Kontrollierbarkeit.

Das Modell der alternierenden Abfolge von Fähigkeitsverbesserung und Reifen liefert auch zahlreiche nützliche weitere Einblicke:

- Ausreichend Reifezeit zwischen Fähigkeitverbesserungen,
- Nur was kontrollierbar ist, lässt sich zielgerichtet verbessern,
- Falsche Zielgrößen führen zur »Verschlimmbesserung«,
- Am qualitativ hochwertigsten sind oft die Produkte, die kurz vor einer technologischen Neuerung gefertigt wurden, ...

Reifegrade nach CMMI

Prozessfähigkeiten großes Thema, nicht nur für Informatik. Das CMMI (Capability Maturity Model Integration) definiert u.a. fünf Fähigkeitsstufen* zur Klassifikation von Prozessen, Organisationen, ...:

1. Wiederholte Abläufe, undokumentiert. Ermöglicht individuelles Lernen aus Fehlern.
2. Dokumentation der Abläufe und beobachteten Probleme. Ermöglicht personenübergreifendes Lernen aus Fehlern.
3. Verwaltung und Steuerung der Abläufe. Ermöglicht Fokusierung auf das sichere Erreichen angestrebter Ziele (Dauer, Qualität, ...).
4. Quantitatives Management: Definition und Erfassung von Leistungskennzahlen. Ermöglicht Beobachtung des Reifeverhaltens.
5. Kontinuierliche Prozessverbesserung durch quantitatives Feedback aus dem Prozess, d.h. gezielter Reifeprozess**.

Je höher der Reifegrad, um so größer die Fähigkeit zu reifen und desto geringer die erzielbaren Fehlerentstehungsrate der Prozesse.

* Abstufung als Vorstufe einer Metrik charakterisiert den aktuellen Entwicklungsstand.

** Fähigkeit zum Reifen sind nicht selbstverständlich.

Vorgehensmodelle

Der Technologiegedanke und Projekte

Reproduzierbare Entstehungsabläufe werden auch als Technologie bezeichnet*. Technologien reifen dadurch, dass ähnliche Abläufe oft wiederholt, dabei überwacht und erkannte Probleme beseitigt werden.

Wie verhält es sich mit Projekten:

- Manuelle kreative Teile der Entwurfsprozesse und
- Fertigung von Prototypen, Demonstratoren, ... ?

Ein Projekt ist ein zielgerichtetes, einmaliges Vorhaben, das aus einem Satz von abgestimmten, gelenkten Tätigkeiten besteht. ...

Projekten fehlt aus Sicht der Fehlervermeidung die häufige Wiederholung ähnlicher Abläufe, um aus erkannten Fehlern lernen zu können.

Schließt das Projekte von der Fehlervermeidung aus?

* Der Begriff *Technologie* wurde erstmals vom Göttinger Professor Johann Beckmann (1739-1811) im Lehrbuch "Grundsätze der teutschen Landwirthschaft" verwendet.

Vorgehensmodelle

Vereinheitlichung des Vorgehens für große Klassen von Projekten

- zur Aufwandsminimierung, besseren Vorhersagbarkeit und
- zur Fehlervermeidung durch »Lernen aus Fehlern«.

Typische Vorgehensmodelle für den Entwurf und die Fertigung von IT-Komponenten umfassen:

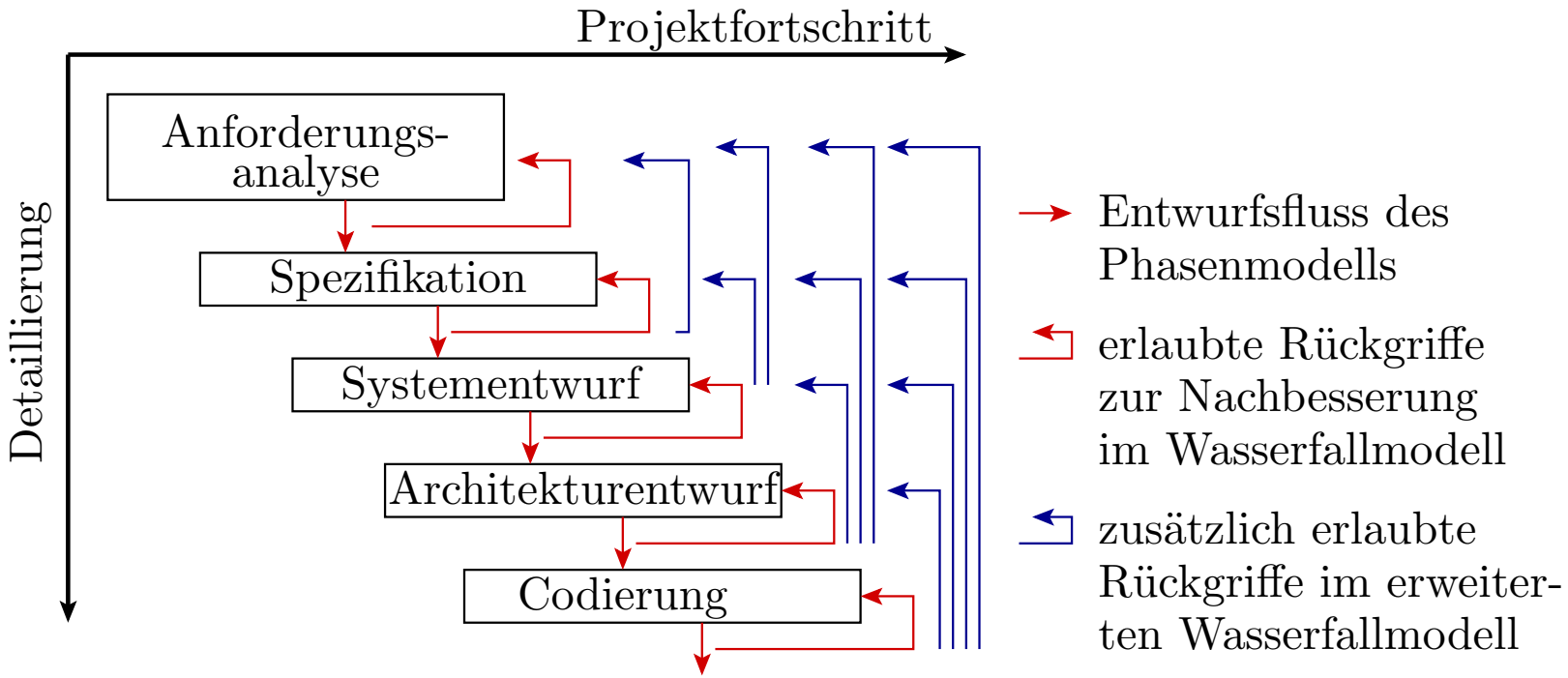
- Aufteilung in Schritte und Phasen,
- Referenzabläufe,
- Definition von Zwischen- und Endkontrollen, ...

Die klassischen Vorgehensmodelle für den Software-Entwurf sind Stufenmodelle. Sie unterteilen Entstehungsprozesse in Phasen:

- Anforderungsanalyse,
- Spezifikation der Ziele,
- Architekturentwurf, Codierung, Test, ...

Fehlervermeidung bei Projektarbeit ist die kontinuierliche empirische Verbesserung, d.h. das Reifen des Vorgehens- [modells].

Stufenmodelle

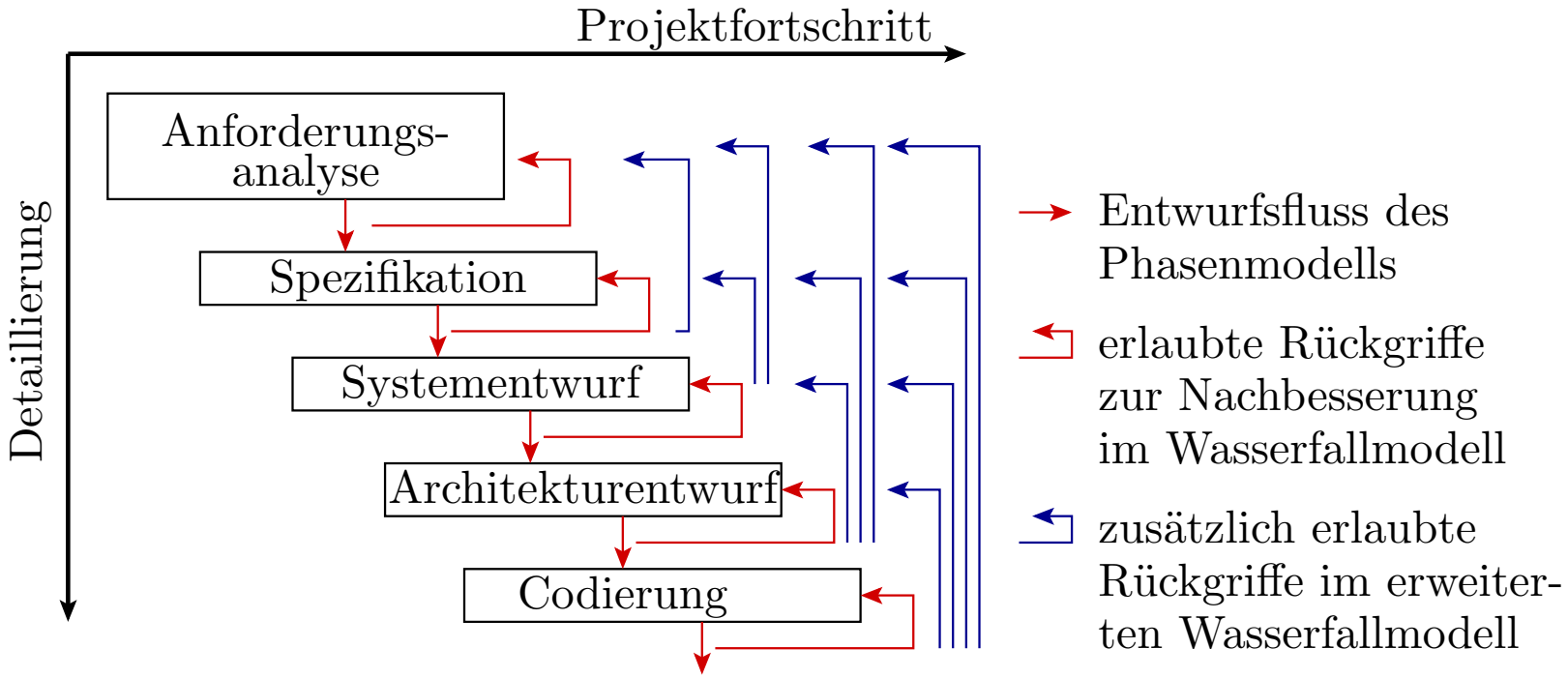


Weiterentwicklung der Fähigkeiten:

- Programmiersprache, Tools,
- Organisationsrahmen, Rundregeln der Qualitätssicherung, ...

Prozesseinstellungungen zum Durchprobieren:

- praktische Arbeitsgestaltung,
- Abgrenzungen der Entwurfsphasen, ...



Prozesseinstellungungen zum Durchprobieren (Fortsetzung):

- Arbeitsorganisation der Phasen,
- geforderte Tests, Dokumentation, ... bei Phasenübergängen,
- Genehmigungsverfahren für Rückgriffe über mehrere Stufen*,
- ...

* Rückgriffe verlängern die Anzahl der Entstehungsschritte für einen Entwurf, und darüber die Anzahl der Fehler. Ein Workaround um einen Fehler kann jedoch auch den Arbeitsaufwand erheblich erhöhen und darüber die Fehleranzahl. Schwieriger Kompromiss.

Bewertung von Vorgehensmodellen

Reifen als komplexer arbeitsintensiver stochastische Prozess schafft nur Verbesserungen, wenn diese überprüfbar sind.

Daraus resultierende Frage

An welchen mess- oder abschätzbaren Parametern ist eine Verbesserung eines Vorgehensmodells erkennbar?

Diese Parameter müssen zwischen unterschiedlichen realen Projekten und Vorgehensmodellen vergleichbar sein:

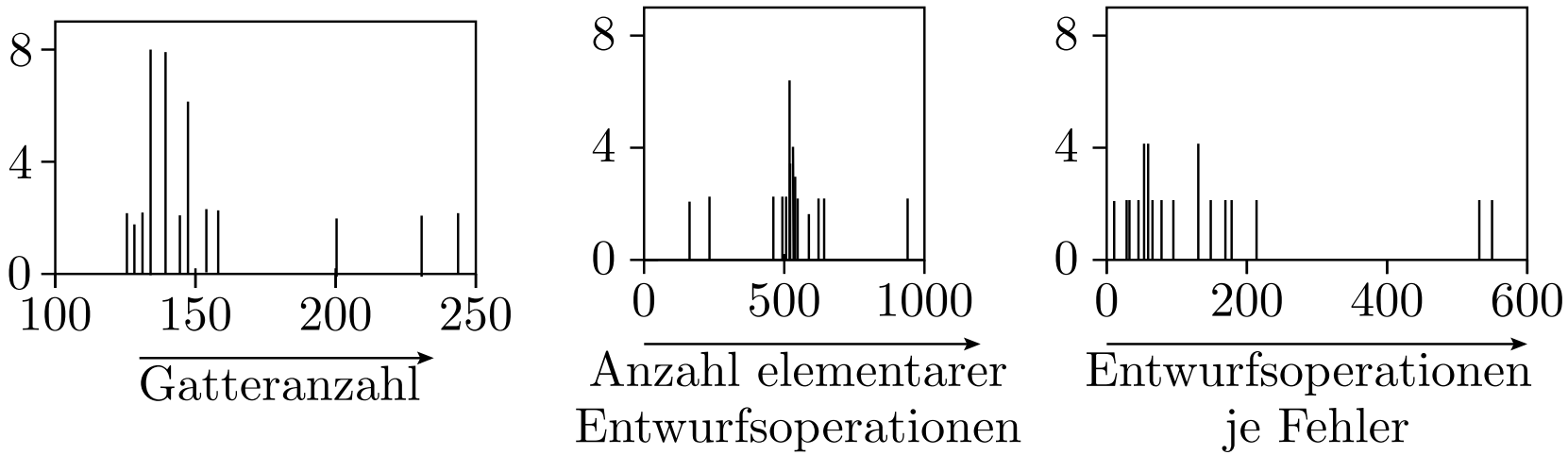
- Dauer, Kosten bezogen auf die Projektgröße,
- Arbeitsschritte je entstehender Fehler, Umfrageergebnisse, ...

Erwartungswerte, Streuungen, Skalierbarkeit auf Projektgröße, ...

Signifikante Aussagen über Vorgehensmodelle verlangen die Beobachtung tausender Projekte mit vergleichbarem Vorgehen.

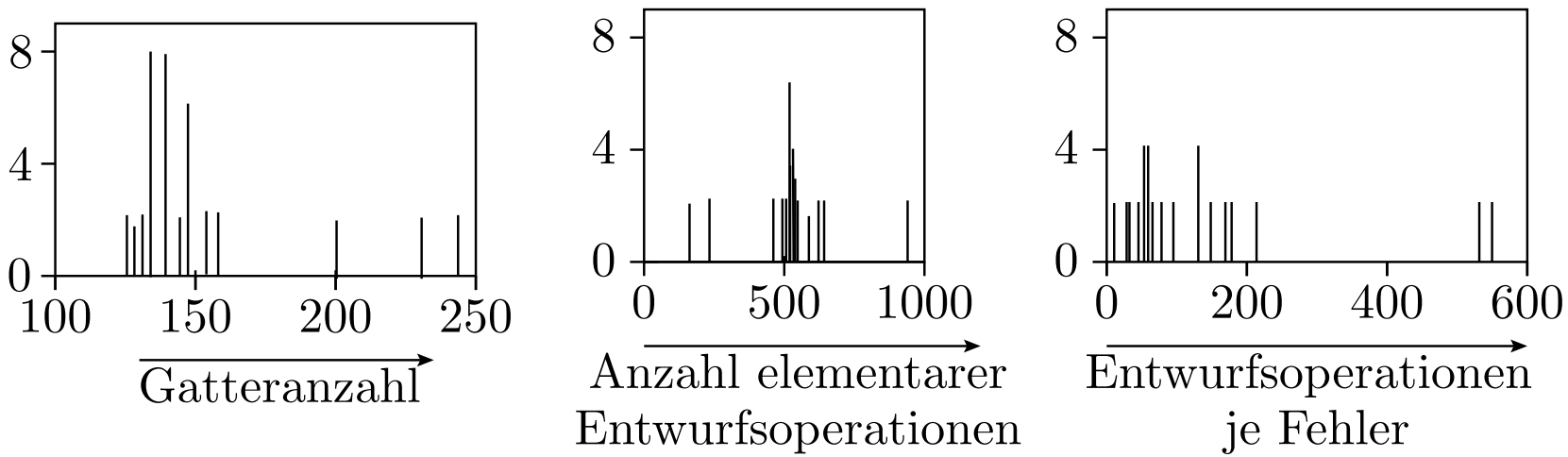
Ein Experiment [1]

Eine Gruppe von 72 Studenten sollte aus einer PLA- (**P**rogrammable **L**ogic **A**rray) Beschreibung eine Gatterschaltungen entwickeln und diese über eine GUI in ein CAD-System eingeben. Für jeden Entwurf wurden die elementaren Entwurfsoperationen, die Gatteranzahl und die Entwurfsfehler gezählt. Als elementare Entwurfsoperationen galten das Anordnen eines Gatters auf dem Bildschirm, das Zeichnen einer Verbindung, ...



[1] Aas, J. E., Sundsbo, I.: Harnessing the Human Factor for Design Quality, IEEE Circuits and Devices Magazine, 3/1995, S. 24-28

Welche Rückschlüsse erlaubt das Experiment?



Angenommen, der Versuch wird genauso an anderen Hochschulen wiederholt:

- auch hier dieselben Kenngrößen je Student bestimmt und
- Verteilung, Erwartungswert und Varianz verglichen.
- Unterschiede statistisch signifikant?

Aus den Vergleichergebnissen ließe sich bei signifikannten Unterschieden schlussfolgern, an welcher Hochschule Studierende für diese Aufgabe besser ausgebildet werden.

Qualität und Kreativität

Qualität und Kreativität

Qualität verlangt Fehlervermeidung. Fehlervermeidung verlangt:

- eine hohe Wiederholrate gleicher oder ähnlicher Tätigkeiten,
- einzuhaltende Arbeitsabläufe mit reproduzierbaren Ergebnissen,
- Protokollierung aller Unregelmäßigkeiten und Probleme, ...

Kreativität verlangt »Einzigartigkeit«:

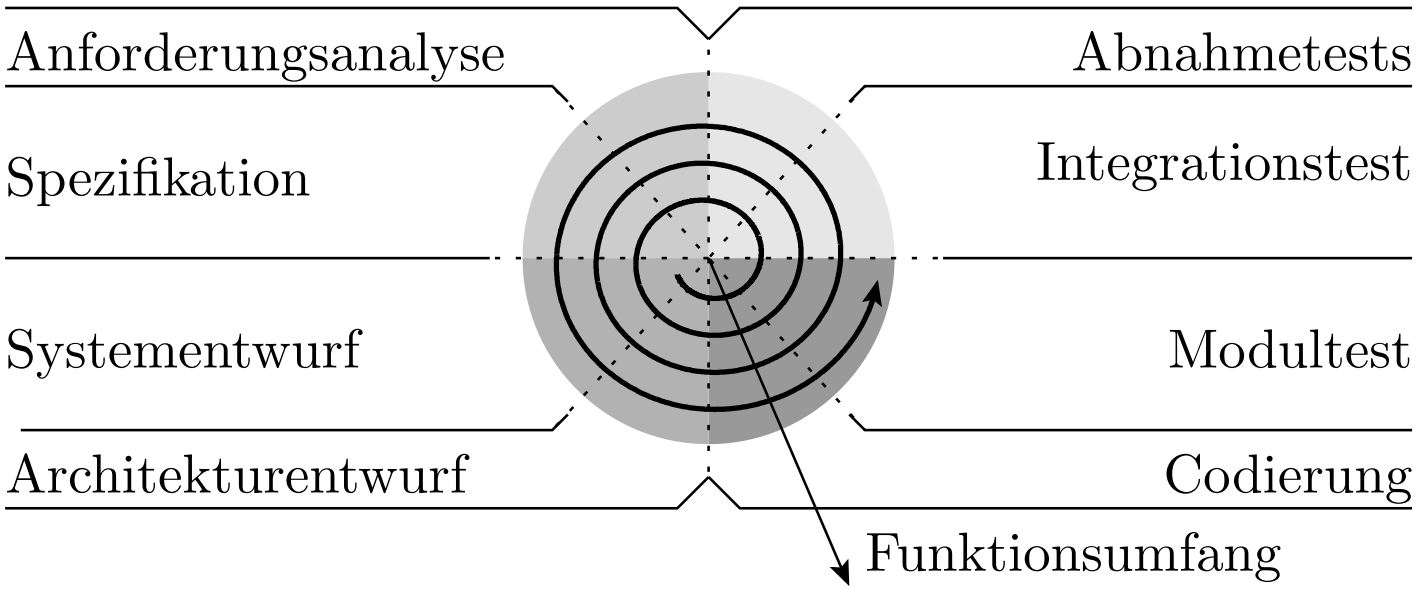
- Einbringen neuer Konzepte,
- Ausprobieren neuer Lösungswege,
- flexible Anpassung an sich ändernde Anforderungen.

Daraus resultierende Fragestellung

Qualität und Kreativität haben entgegengesetzte Anforderungen an die Gestaltung von Arbeitsabläufen. IT-Entwurf verlangt Qualität und Kreativität. Wie lässt sich beides in einem Vorgehensmodell vereinen?

Spiralmodell als Beispiel evolutionärer Modelle

Evolutionäre Vorgehensmodelle versuchen einen Rahmen für Projekte zu bieten, bei denen sich Kundenwünsche, Ziele, Vorgehen, ... mit dem Projekt weiterentwickeln. Weniger starre Abläufe. Mehr kreativer Gestaltungsspielraum. Beispiel Spiralmodell:



- Aufteilung einer Entwicklung auf ein mehrmaliges Durchlaufen eines Stufenmodells.

Aufteilung auf mehrmalige Durchläufe eines Stufenmodells.

- Durchlauf 1: Spezifikation von Grundanforderungen, Entwurf, Codierung, Test, ..., Abnahme und Einsatz.
- Durchlauf 2 bis n: Ideensammlung und Auswahl gewünschter Zusatzanforderungen und Änderungen. Entwurf bis Einsatz.

Ziel:

- Minimierung der Anzahl der Entstehungsschritte und der Anzahl der entstehenden Fehler je Stufenmodelldurchlauf.
- Kreativer Freiraum in Form einer Ideensammlung für den nächsten Stufenmodelldurchlauf.

Idealerweise dürften nach jedem Stufenmodelldurchlauf im entstandenen Code nur noch Fehler beseitigt werden.

Neue Features, Ideen und Werkzeuge können aber nachträglich grundlegende Änderungen an existierenden Systemteilen, Architekturentscheidungen, Modularisierung, ... ratsam erscheinen lassen.

Grundidee gut, tatsächlicher Nutzen steckt in den Umsetzungsdetails.

Ein Abstecher zu Lernprozessen

In der Schule und beim Erlernen praktischer Tätigkeiten werden zum erheblichen Teil Vorgehensmodelle vermittelt und trainiert:

- Rechnen, Schreiben, Handwerkern, Programmieren, ...
- Bewertung in Service-Leistungen pro MF und Zeit.

Da steckt über Jahrhunderte gereiftes Knowhow drin.

Lernphasen an einer Hochschule:

1. Wissenvermittlung: anlesen, erklärt bekommen, ...
   Vorlesung, Seminare, Selbststudium, ...
2. Training, bis Ergebnisse vorhersagbar.
   Übung, Klausurvorbereitung*, Praktika.
3. Professionalisierung: Prozessüberwachung; Beseitigung von Schwachstellen und Problemen in den Abläufen.
   Aus Zeitgründen erst in der Berufspraxis für den eigenen eingeschränkten Tätigkeitsbereich möglich.

* Auch Bewertung in Arbeitsmenge pro Klausurdauer und Fehlern pro Arbeitsmenge.

Querverbindung Drittmittelprojekte

- Die Professionalisierungsphase durchlaufen erst die Absolventen in der Praxis.
- Akademiker und Studenten sind noch nicht für fehlerarme Arbeitsabläufe trainiert.
- In industriellen Software-Projekten entstehen durch Akademiker tendenziell mehr Fehler je Aufgabengröße.
- Die Kosten für die Fehlerbeseitigung trägt der Industriepartner.
- Deshalb rechnet es sich normalerweise für die Industrie nicht, Hochschulen und Studenten in ihr Tagesgeschäft einzubinden.
- Industrielle Studenten-Projekte dienen der Ausbildung.
- Drittmittelforschung ist wertvoll für den Knowhow-Transfer, Literaturstudien, Demonstratoren, ... aber im IT-Bereich ungeeignet für die Einbindung in die Produktentwicklung.

Qualitätssicherung an unser Hochschule

Die Master-Bachelor-Einführung (Bolonia-Prozess) strebt nach Referenzabläufen, vergleichbare Abschlüsse, ...

Das ist eine Etablierung grundlegender Prozessfähigkeiten:

- große Wiederholanzahl vergleichbarer Abläufe,
- Prozesseinstellungen zum Durchprobieren,
- Kenngrößenerhebung für die Erfolgskontrolle.

um ein Reifen der Ausbildungqualität zu ermöglichen.

Wie ist das an unserer Uni:

- Welche Prozessüberwachungen gibt es?
- Wo sind Vorgehensmodelle erkennbar?
- Was für Ressourcen bindet der angestoßene Reifeprozess?
- Wie wird verhindert, dass die Kreativität nicht darunter leidet?

Fehlervermeidung eröffnet interessante Blickwinkel auf Technologien, Institutionen, Behörden bis hin zu unserer gesamten wissenschaftlich-technische Weiterentwicklung.

Zusammenfassung

Fehlerentstehung

- Fehler entstehen in den Entwurf-, Fertigungs- und Reparaturprozessen mit dem Entwurf oder Produkt.
- Entstehungsprozesse sind wie IT-Systeme als Service-Leister modellierbar mit Erbringungsraten ($\Rightarrow$ Ausbeute), Fehlfunktionsraten ($\Rightarrow$ Fehlerenstehungsrate), ...
- In der Praxis werden die Fehlerentstehungsraten auf Zählwerte von Metriken bezogen:

(2.45) $$\mu_{\mathrm{CF}} = \xi_{<\mathrm{C}>} \cdot C$$

(2.46) $$\xi_{<\mathrm{C}>} = \frac{\mu_{\mathrm{CF}}(C)}{C}$$

Fehlervermeidung, Determinismus

Fehlervermeidung ist Fehlerbeseitigung in den Entstehungsprozessen. Fokus Reifen der Prozesse, d.h. Fehlerbeseitigung in der Nutzungsphase mit seinen Bestandteilen:

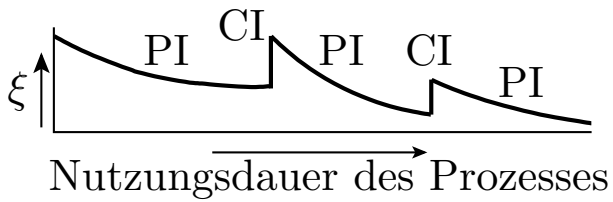
- Prozessnutzung und Überwachung,
- Problemerfassung und Untersuchung,
- Problembeseitigung durch experimentelle Reparatur als Iteration aus Beseitigungsversuchen und Erfolgskontrolle.

Das erfordert Fähigkeiten:

- große Wiederholrate, große Problemerkennungsrate,
- Stellschrauben zur Prozessnachbesserung,
- Kontrollmöglichkeiten für den Beseitigungserfolg, ...

Problematisch oft fehlender Determinismus, insbesondere bei kreativen Arbeiten. Kein Determinismus erschwert Lernen aus Fehlern, dabei insbesondere die Erfolgskontrolle nach Problembeseitigungsversuchen.

Fähigkeitsverbesserung und Reifen



Fähigkeiten, auch die für eine geringere Fehlerentstehungsrate werden »Offline«, d.h. getrennt vom Prozess entwickelt und in größeren Zeitschritten übernommen. Dabei geht die »Zentrierung« verloren, d.h. es kommen neue Probleme in den Prozess. Die Fehlerenstehungsrate steigt sprunghaft.

Reifen umfasst viele kleine Verbesserungsversuche mit Erfolgkontrolle. Abnehmende Fehlerentstehungsrate, bis das Potential der neuen Fähigkeiten ausgereizt ist.

Unter Einbeziehung der Fähigkeitsverbesserung in größeren Zeitschritten nimmt die Fehlerentstehungsrate tendentiell sägezahnförmig ab*.

* Für IT-Service-Leistungen hatten wir das Abnahmeverhalten der Fehlfunktionsrate, beim Reifen als IT-Entstehungsleistungen die Fehlerentstehungsrate, genauer untersucht, Abnahme mit Exponent 1 bis 2.

Projekte, Vorgehensmodelle, Kreativität

Reifeprozess benötigen eine große Wiederholanzahl gleicher Abläufe. Um auch bei Projekten aus erkannten Fehlern lernen zu können, erfolgt Projektarbeit nach Vorgehensmodellen.

Klassiker sind die Stufenmodelle, die Entwürfe in Phasen teilen und Kontrollen und Aktivitäten beim Stufenübergang definieren. Problematisch ist die Überprüfung, ob eine Änderung einer Verbesserung bewirkt hat.

Vorgehensmodelle findet man überall dort, wo ein beständiges Lernen aus Fehlern angestrebt wird, also auch in Verwaltungen, Schulen, ... Es gibt anwendungsunabhängige Gemeinsamkeiten:

- erforderliche Fähigkeiten, Aufwand für den Reifeprozess,
- Phasenaufteilung, Beschränkung der Kreativität, ...

Allein diese anwendungsunabhängige Gemeinsamkeiten eröffnet interessante Blickwinkel, wie und wohin die Entwicklung von Technologien, Arbeitsabläufen in Institutionen und Behörden und auch die Ausbildung an Schulen verläuft.