Test and Dependability 3: Stochastics I: Probabilities

Prof. G. Kemnitz

Department of Computer Science, Clausthal University of Technology

November 23, 2026

Contents of Slide Set 3

Probability

1.1 Definition, estimation
1.2 Chained events
1.3 CVA graph
1.4 Fehlerbäume
1.5 Markov-Ketten

Fehlernachweis

2.1 Nachweis & Zuverlässigkeit
2.2 Service mit Gedächtnis
2.3 Fehler und Modellfehler

Fehlerbeseitigung

3.1 Ersatz
3.2 Reparatur
3.3 Reifeprozesse

Fehlerentstehung

Reliability and all its sub-aspects are described in this lecture in terms of counts or frequencies of positive and negative experiences. For large counts, frequencies approach probabilities.

Stochastics is a branch of mathematics that deals with chance and uncertainty. The term originates from Greek and means

> *»the art of guessing«.*

Stochastics provides a wide range of tools for working with probabilities, some of which we have already used.

Probability

Definition, estimation

3.3 Probability

If a random experiment is repeated n times under constant experimental conditions, the relative frequency $\#A/n$ of event A occurring approaches the probability of occurrence:

$$\mathbb{P}[A] = \lim_{n\to\infty} \frac{\#A}{n} \tag{3.1}$$

Many of the metrics introduced so far tend towards probabilities as the count values increase:

- proportion of delivered services η_{DS}
- malfunction rate ζ,
- fault coverage FC, ...

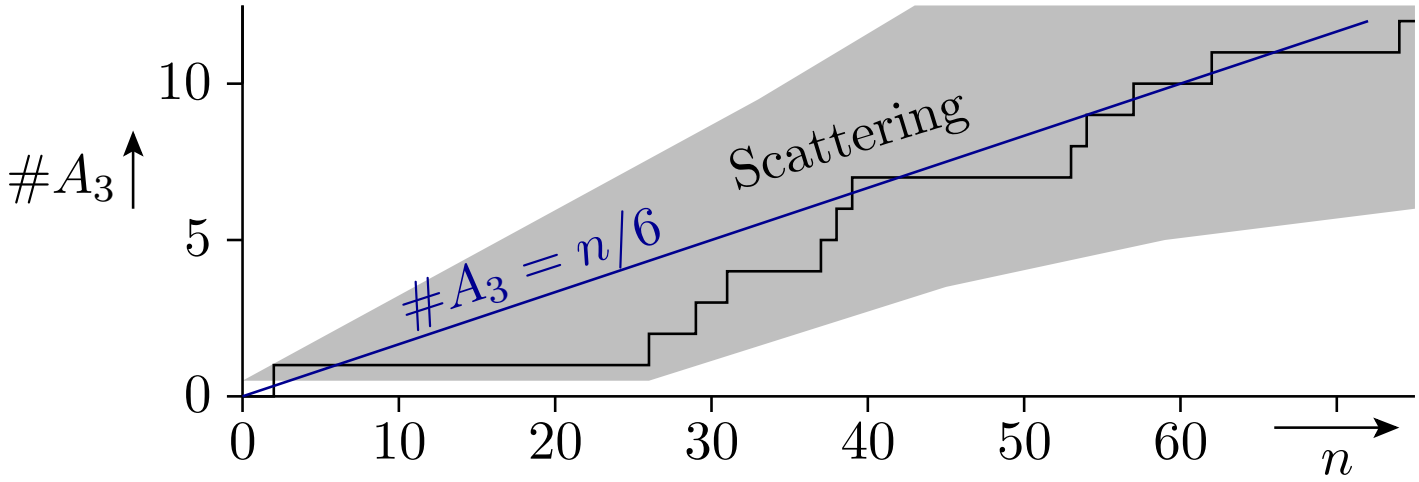
Probability is the best predictor of the expected relative frequency of future trials. That's why here's a subject-specific introduction.

Afterwards, applications for fault detection, fault rectification and fault emergence.

$\mathbb{P}[A]$	Probability of occurrence of event A.
$\#A$	Number of times event A has occurred.

3.4 Example: Rolling a 3

- Possible outcomes: 1, 2, ..., 6; favourable outcome: 3,
- number of trials: n



$$\mathbb{P}[A_3] = \lim_{n\to\infty} \frac{\#A_3}{n} = \frac{1}{6}$$

Theorem 1

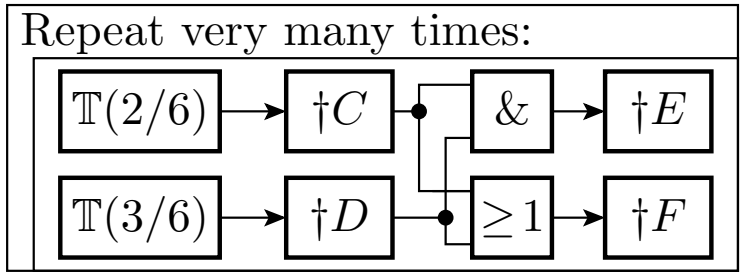
If the possible outcomes of a random experiment are equally likely, the probability is the proportion of favourable outcomes.

Chained events

3.5 Chained events

n	1	2	3	4	5
A	6	1	5	4	1
B	6	5	6	2	1
$C = (A > 3)$	1	0	1	1	0
$D = (B < 3)$	0	0	0	1	1
$E = (C \wedge D)$	0	0	0	1	0
$F = (C \vee D)$	1	0	1	1	1

Included counting experiment:



n	6	7	8	9	10	11	12	13	...	20	...	40
$\#C$	3	3	3	4	5	6	6	6		11		21
$\#D$	2	2	2	2	2	3	3	4		6		9
$\#E$	1	1	1	1	1	2	2	2		5		6
$\#F$	4	4	4	5	6	7	7	8		13		24

Complex events can often be described using logical and other connections between events that are easier to analyse. In the following, the dice are rolled twice in each experiment (events A and B, each with a range of values $\{1, 2, \ldots, 6\}$). From these, the binary events C and D are formed using comparison operators, and these are combined once using AND and once using OR, and then counted.

$\dagger A$ Counting event (triggering or triggered).

$\mathbb{T}(\eta)$ Random event (1 with probability η, otherwise 0).

3.6 Estimation of relative frequencies

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

Of the 6 possible equally probable outcomes of rolling a die, three are favourable for $C = (A > 2)$ and two for $D = (A < 3)$. The compound events E and F have $6^2 = 36$ equally probable possible outcomes, of which six are favourable for $E = C \wedge D$ and 24 for $F = C \wedge D$.

Estimating the proportion of favourable events appears much simpler in this example, but is not always possible.

Counting experiments with only 40 repetitions result in estimation errors of, in the example, $\approx 10\%$ of the probability value (sec.4.2.5).

3.7 Conditional probabilities

In the case of a conditional probability, only those trials and events that satisfy a condition are counted[(1)]; in the example:

$$E = C \vee D \text{ provided that } C \wedge D = 0.$$

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

Events that should not be counted or excluded

Both the number of trials counted and the number of favourable events are reduced by the four events with $C \wedge D = 1$ that are not to be counted.

Not taking into account additional conditions (dependencies), as is often the case in generalised mathematical models, can lead to significant systematic estimation errors. However, it is always possible to check for overly large systematic estimation errors with counting experiments.

(1) In the case of events that are not to be counted, it is irrelevant whether or not they can occur.

3.8 Rules for conditional probabilities

Probability that A occurs given B:

$$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[B]} \tag{3.2}$$

Probability that B occurs given A:

$$\mathbb{P}[B|A] = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[A]}$$

Bayes' theorem:

$$\mathbb{P}[B|A] = \mathbb{P}[A|B] \cdot \frac{\mathbb{P}[B]}{\mathbb{P}[A]} \tag{3.3}$$

A, B	events.
$\mathbb{P}[A\|B]$	Probability of event A under condition B.
$\mathbb{P}[A \wedge B]$	Probability of event A and B.
$\mathbb{P}[A \vee B]$	Probability of event A or B.

Example 3.1: COVID-19 test

Random variable A: a person is infected, $\mathbb{P}[A] = p_{\mathrm{A}} = 10^{-4}$. Random variable B: test result positive (infection detected). Find the probability that a tested person is infected if

a) *the test classifies people as infected regardless of whether they are actually infected with $\mathbb{P}[B] = p_{\mathrm{B}} = 99\%$? (Condition for the validity of Bayes' theorem).*

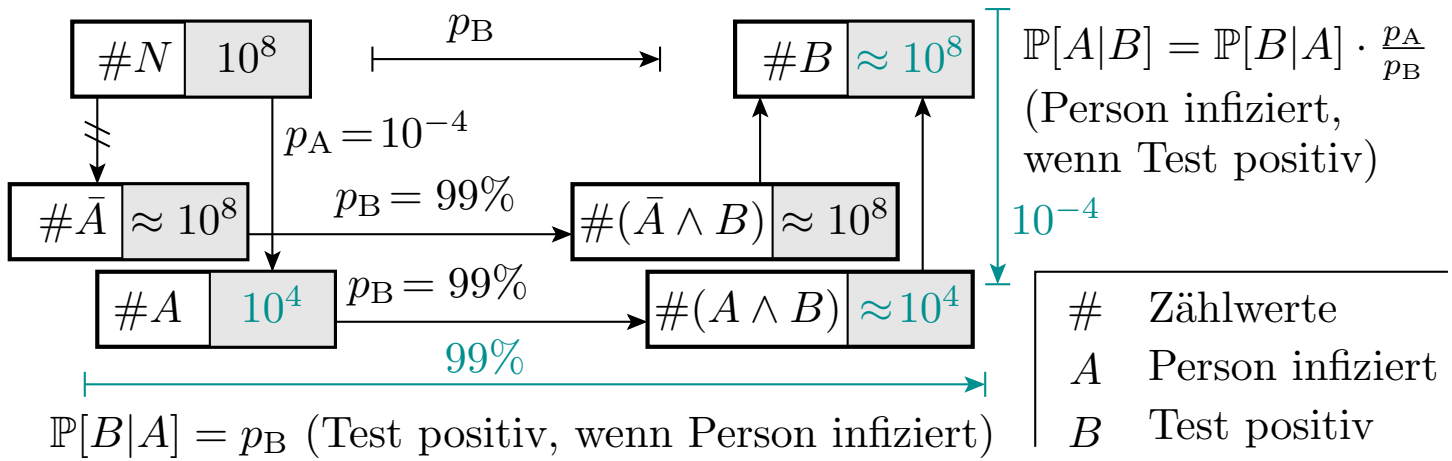
b) *the test classifies infections with $p_{\mathrm{AB}} = 99\%$ and the absence of an infection with $p_{\bar{\mathrm{A}}\mathrm{B}} = 10^{-4}$ as an infection?*

Solve the problems using count-value assignment graphs. Estimate the assignment frequencies and, in addition, the expected counts for a total population of 10^8 people (roughly the population of Germany).

p_{A}	Wahrscheinlichkeit, dass eine Person infiziert ist.
p_{B}	Wahrscheinlichkeit, dass Test positiv ist.
p_{AB}	Wahrscheinlichkeit, Test positiv, wenn Person infiziert ist.
$p_{\bar{\mathrm{A}}\mathrm{B}}$	Wahrscheinlichkeit, Test positiv, wenn Person nicht infiziert ist.

Random variable A: a person is infected, $\mathbb{P}[A] = p_\mathrm{A} = 10^{-4}$. Random variable B: test result positive (infection detected). Find the probability that a tested person is infected if

a) *the test classifies people as infected regardless of whether they are actually infected with $\mathbb{P}[B] = p_\mathrm{B} = 99\%$? (Condition for the validity of Bayes' theorem).*



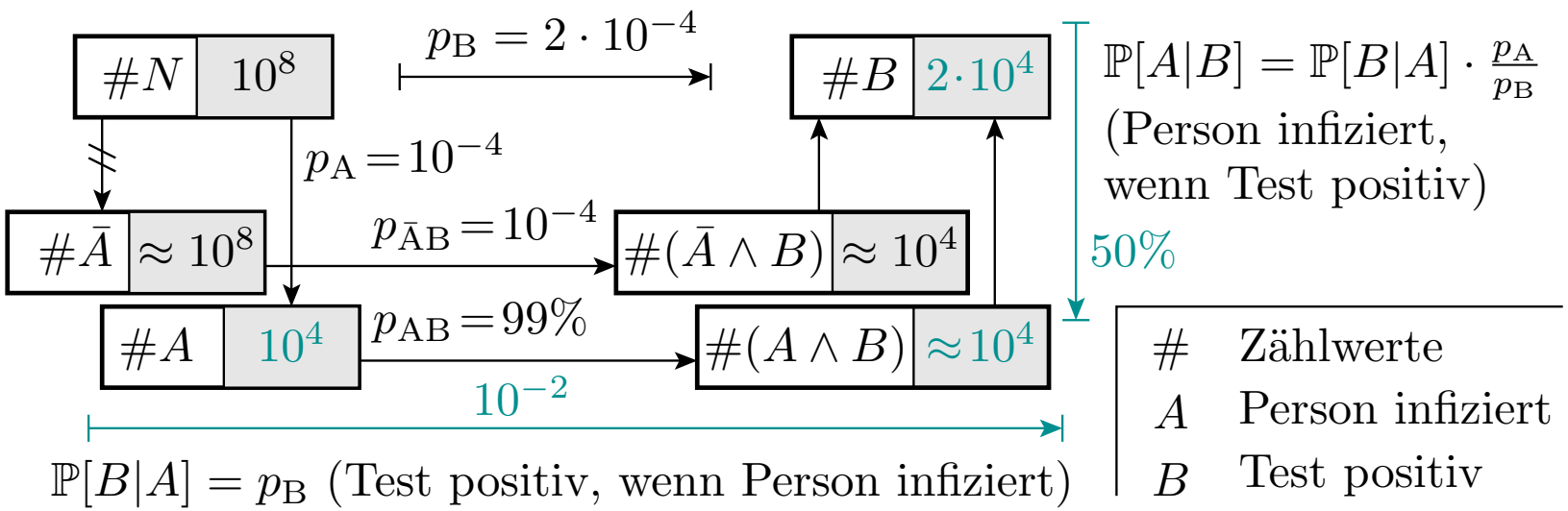
The result also follows from Bayes' theorem:

$$\mathbb{P}[A|B] = \mathbb{P}[B|A] \cdot \frac{\mathbb{P}[B]}{\mathbb{P}[A]} = 99\% \cdot \frac{10^{-4}}{99\%} = 10^{-4}$$

A test result that is independent of the actual outcome is, of course, nonsense, but it illustrates the pitfalls of using stochastic methods.

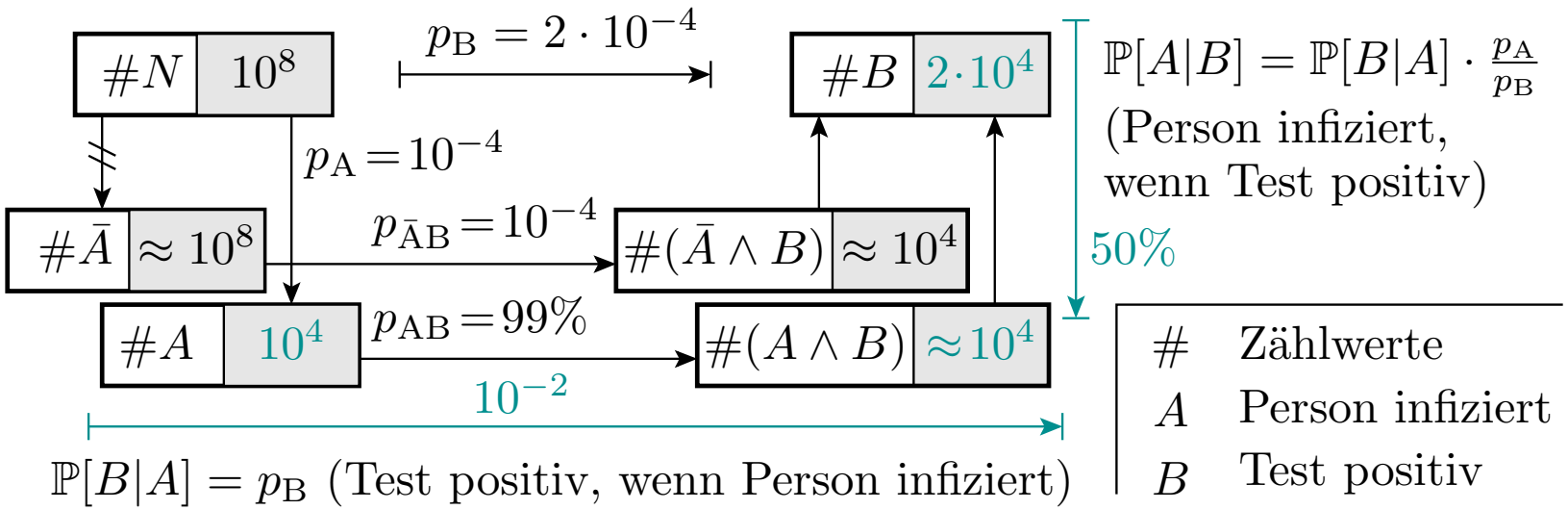
Random variable A: a person is infected, $\mathbb{P}[A] = p_{\mathrm{A}} = 10^{-4}$. Random variable B: test result positive (infection detected). Find the probability that a tested person is infected if

b) *the test classifies infections with $p_{\mathrm{AB}} = 99\%$ and the absence of an infection with $p_{\bar{\mathrm{A}}\mathrm{B}} = 10^{-4}$ as an infection?*



A reliable test has two types of error; in the example

- $p_{\mathrm{A}\bar{\mathrm{B}}} = 1\%$ (masking, or in this case, infection not detected) and
- $p_{\bar{\mathrm{A}}\mathrm{B}} = 10^{-4}$ (false positive, i.e. infection incorrectly detected).

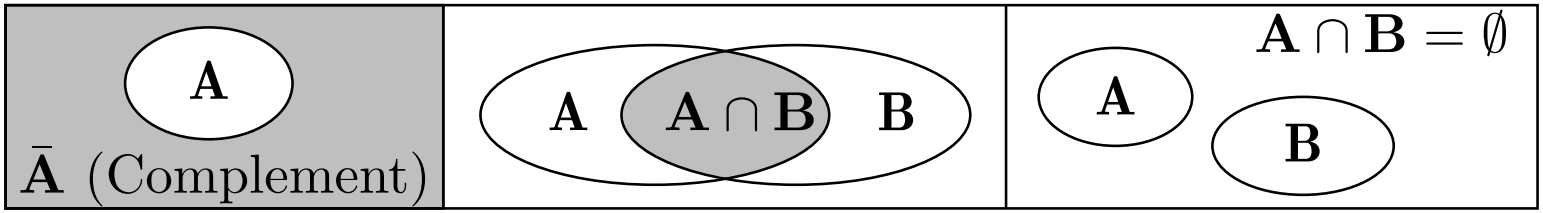


The probability that a randomly selected person who has tested positive is actually infected, using the example values:

$$\left.\frac{\#(A\wedge B)}{\#B}\right|_{\mathrm{SLC}} = \frac{p_{\mathrm{A}}\cdot p_{\mathrm{AB}}}{p_{\mathrm{A}}\cdot p_{\mathrm{AB}}+(1-p_{\mathrm{A}})\cdot p_{\bar{\mathrm{A}}\mathrm{B}}} = 50\%$$

depends primarily on the problem frequency, here p_{A}, and the phantom error rate, here $p_{\bar{\mathrm{A}}\mathrm{B}}$, that good results are classified as bad.

3.10 NOT / AND / OR of events



NOT (probability of non-occurrence):

$$\mathbb{P}\left[\bar{A}\right] = 1 - \mathbb{P}\left[A\right] \tag{3.4}$$

AND (simultaneous occurrence of events A and B):

- Stochastic independence:

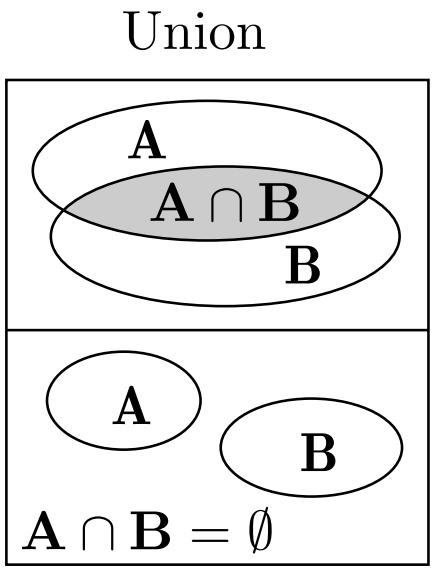
$$\mathbb{P}\left[A|B\right] = \mathbb{P}\left(A\right) = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[B]}$$

$$\mathbb{P}\left[A \wedge B\right] = \mathbb{P}\left[A\right] \cdot \mathbb{P}\left[B\right] \tag{3.5}$$

- Mutually exclusive events:

$$\mathbb{P}\left[A \wedge B\right] = 0 \tag{3.6}$$

$\mathbf{A}$, $\mathbf{B}$	Event sets.
$\cup$, $\emptyset$	Union set. Empty set.
A, B	events.



OR (alternative occurrence of A and B):

$$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B] - \mathbb{P}[A \wedge B]$$

- Stochastic independence:

$$\mathbb{P}[A \wedge B] = \mathbb{P}[A] \cdot \mathbb{P}[B]$$
$$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B] - \mathbb{P}[A] \cdot \mathbb{P}[B] \quad (3.7)$$

- Mutually exclusive events:

$$\mathbb{P}[A \wedge B] = 0$$
$$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B] \quad (3.8)$$

For more than two independent events, it is simpler to first use De Morgan's law to convert OR to AND:

$$A \vee B \vee C = \overline{\bar{A} \wedge \bar{B} \wedge \bar{B}}$$
$$\mathbb{P}[A \vee B \vee C] = 1 - (1 - \mathbb{P}[A]) \cdot (1 - \mathbb{P}[B]) \cdot (1 - \mathbb{P}[C]) \quad (3.9)$$

A, B, C	events.
$\mathbb{P}[\ldots]$	Probability of occurrence of event ...

3.12 Dependent but not mutually exclusive

There is no simple way to estimate dependent, non-mutually exclusive events.

Workaround:

- Rewrite the logical expressions as AND, OR, NOT of independent or mutually exclusive events, e.g.:

$$A \oplus B = \underbrace{\underbrace{\left(A \wedge \bar{B}\right)}_{\text{independent}} \vee \underbrace{\left(\bar{A} \wedge B\right)}_{\text{independent}}}_{\text{mutually exclusive}}$$

$$\mathbb{P}\left[A \oplus B\right] = \mathbb{P}\left[A\right] \cdot \left(1 - \mathbb{P}\left[B\right]\right) + \left(1 - \mathbb{P}\left[A\right]\right) \cdot \mathbb{P}\left[B\right]$$

- A counting experiment, with lots of trials.

Example 3.2: Independent fault detection

A system contains three independently detectable faults with detection probabilities $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

a) *What is the probability that all faults will be detected?*

b) *What is the probability that no fault will be detected?*

c) *What is the probability that at least one fault will be detected?*

d) *What is the probability that exactly two faults will be detected?*

Hint:

- Definition of events F_i for fault i to be detected.
- Definition of events A, B, C and D for the favourable event and describing the events by logical equations.
- Transformation into AND of independent and OR of mutually exclusive terms using Eqs. (3.4), (3.5) and (3.8).

$\mathbb{P}[F_i]$ Probability that fault i is detectable.

A system contains three independently detectable faults with detection probabilities $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

a) *What is the probability that all faults will be detected?*

All faults will be detected if the first fault AND the second fault AND the third faults are detected. AND of independent events:

$$\begin{aligned} \mathbb{P}[F_i] &= p_i \\ A &= F_1 \wedge F_2 \wedge F_3 \\ \mathbb{P}[A] &= \mathbb{P}[F_1] \cdot \mathbb{P}[F_2] \cdot \mathbb{P}[F_3] \\ &= p_1 \cdot p_2 \cdot p_3 = 10\% \cdot 5\% \cdot 20\% = 0.1\% \end{aligned}$$

$\mathbb{P}[A]$ Probability that all three faults are detected.

A system contains three independently detectable faults with detection probabilities $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

b) *What is the probability that no fault will be detected?*

No fault is detected if NOT the first fault AND NOT the second fault AND NOT the third fault are detected:

$$\begin{aligned} B &= \bar{F}_1 \wedge \bar{F}_2 \wedge \bar{F}_3 \\ \mathbb{P}[B] &= (1 - \mathbb{P}[F_1]) \cdot (1 - \mathbb{P}[F_2]) \cdot (1 - \mathbb{P}[F_3]) \\ &= (1 - p_1) \cdot (1 - p_2) \cdot (1 - p_3) = 90\% \cdot 95\% \cdot 80\% = 68.4\% \end{aligned}$$

$\mathbb{P}[B]$ Probability that no fault is detected.

A system contains three independently detectable faults with detection probabilities $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

c) *What is the probability that at least one fault will be detected?*

At least one fault will be detected if NOT no fault is detectable:

$$\begin{aligned} C &= \bar{B} \\ \mathbb{P}[C] &= 1 - \mathbb{P}[B] = 1 - 68{,}4\% = 31.6\% \end{aligned}$$

$\mathbb{P}[C]$ Probability that at least one fault is detected.

A system contains three independently detectable faults with detection probabilities $p_1 = 10\%$, $p_2 = 5\%$ und $p_3 = 20\%$.

d) *What is the probability that exactly two faults will be detected?*

Exactly 2 faults are detected if

- the first two are and the third is not,
- the second two are and the first is not, or
- or the first and the third are and the second is not

detected. All events linked by AND are independent, and the terms linked by OR are mutually exclusive:

$$\begin{aligned} D &= \left(F_1 \wedge F_2 \wedge \bar{F}_3\right) \vee \left(\bar{F}_1 \wedge F_2 \wedge F_3\right) \vee \left(F_1 \wedge \bar{F}_2 \wedge F_3\right) \\ \mathbb{P}\left[D\right] &= p_1 \cdot p_2 \cdot (1 - p_3) + (1 - p_1) \cdot p_2 \cdot p_3 + p_1 \cdot (1 - p_2) \cdot p_3 \\ &= 10\% \cdot 5\% \cdot 80\% + 90\% \cdot 5\% \cdot 20\% + 10\% \cdot 95\% \cdot 20\% = 3.2\% \end{aligned}$$

$\mathbb{P}\left[D\right]$ Probability that exactly two faults are detected.

Example 3.3: Dependent fault detection

The probability of detecting fault 1, independently of the detection of fault 2, is $p_1 = 10\%$. The probability of detecting fault 2, if fault 1 is detected, is $p_2 = 20\%$ and otherwise 0, i.e. the detection of fault 2 implies the detection of fault 1.

$p_1 = 10\%$, $p_2 = 20\%$if fault 1 is detectable, otherwise 0

What are the probabilities that 0, 1 or 2 faults are detectable?

Hint: Define events F_i for fault i is detectable and E_i for the number of detectable faults is i.

$p_1 = 10\%$, $p_2 = 20\%$if fault 1 is detectable, otherwise 0

What are the probabilities that 0, 1 or 2 faults are detectable?

No fault is detectable if fault 1 is not detectable. Detection of fault 2 is by non-detection of fault 1 excluded:

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

One fault is detectable if the first fault is detectable but the second is not:

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

$p_1 = 10\%$, $p_2 = 20\%$if fault 1 is detectable, otherwise 0

What are the probabilities that 0, 1 or 2 faults are detectable?

Two faults are detectable if both faults are detectable:

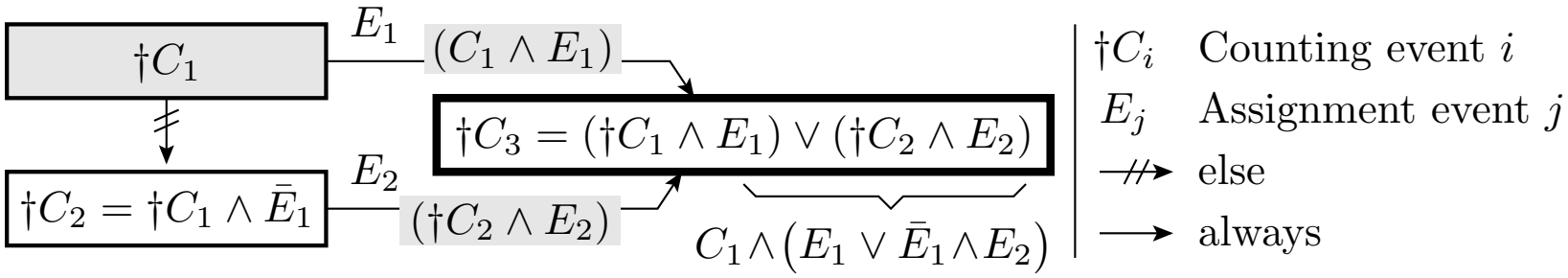
$$\begin{aligned} E_2 &= F_1 \wedge F_2 \\ \mathbb{P}[E_2] &= p_1 \cdot p_2 = 10\% \cdot 20\% = 2\% \end{aligned}$$

Check: The sum of the probabilities of the three possible outcomes must be 1:

$$\mathbb{P}[E_0] + \mathbb{P}[E_1] + \mathbb{P}[E_2] = 90\% + 8\% + 2\% = 100\%\surd$$

CVA graph

3.15 Assignment of count values via events



Directed graph for counting value assignment:

1. Edges pass counting events on if the assignment condition is met (AND).
2. Multiple incoming events forming an OR.

For easy reading of complex assignments:

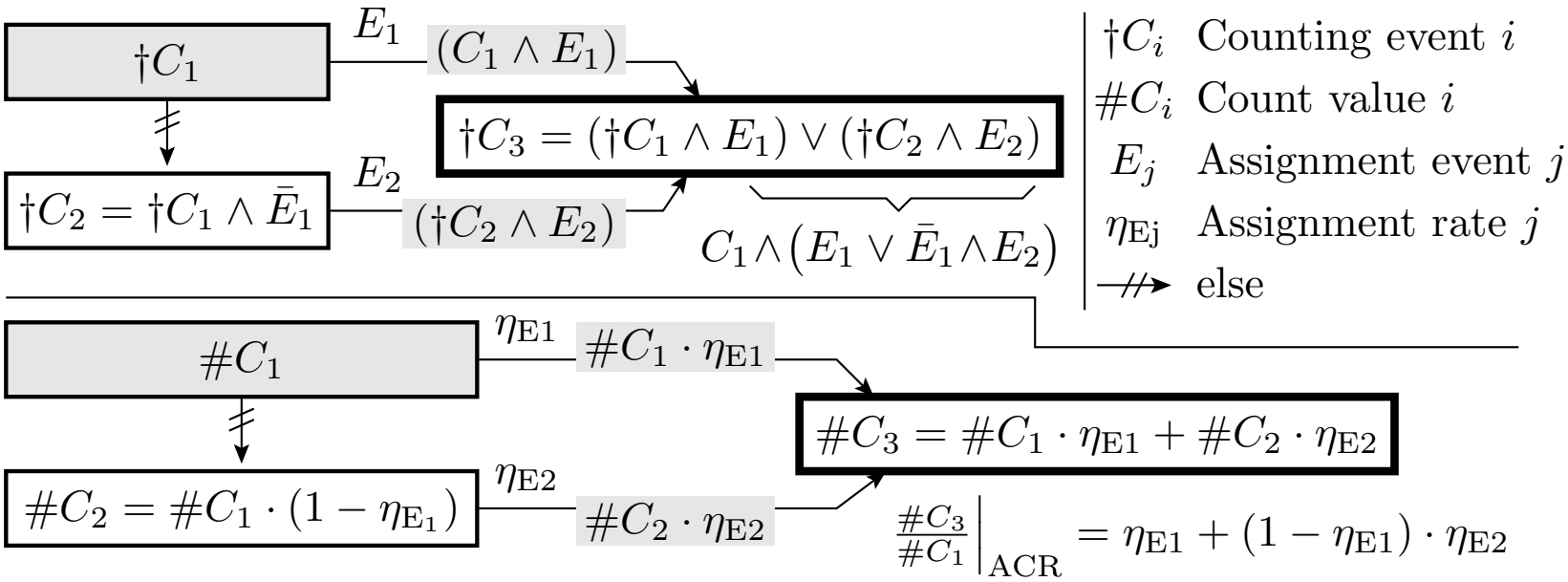
- AND allways with independent assignment events:

(3.5) $$\mathbb{P}[A \wedge B] = \mathbb{P}[A] \cdot \mathbb{P}[B]$$

- OR of counting events allways mutually exclusive by else-edges:

(3.8) $$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B]$$

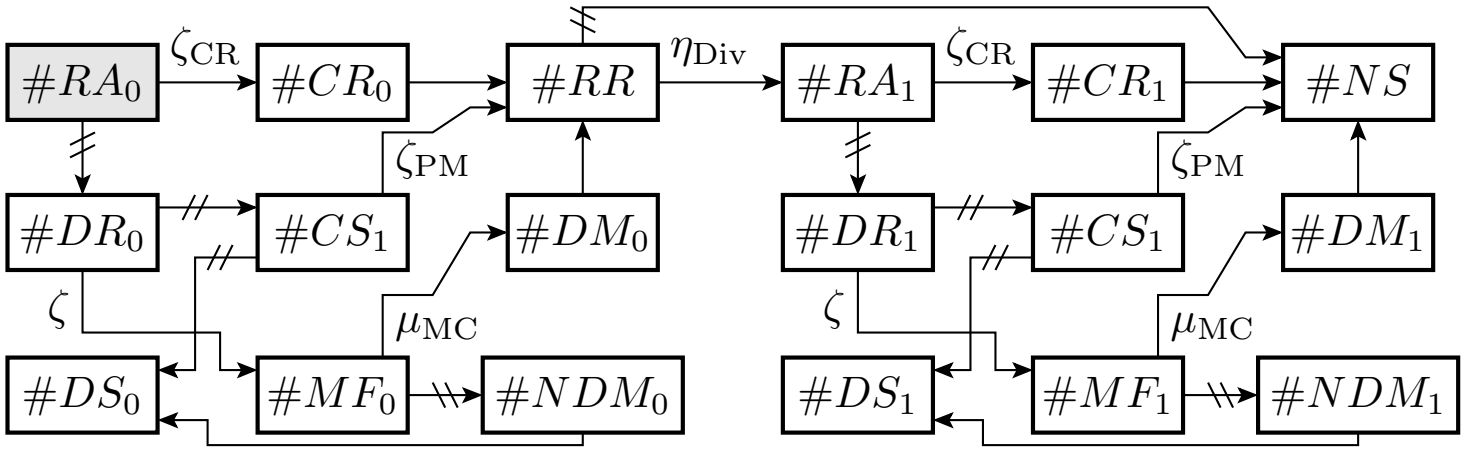
3.16 Transition into a CVA graph



AND of independent assignment events result in multiplication by the assignment rate, whilst mutually exclusive OR assignment rates result in addition.

Precondition: The **counting event** and the **assignment events** must be **independent** of one another. If not, a creative redesign is required. Example: fault correction by majority decision, in which **diversity** may only control one edge transition.

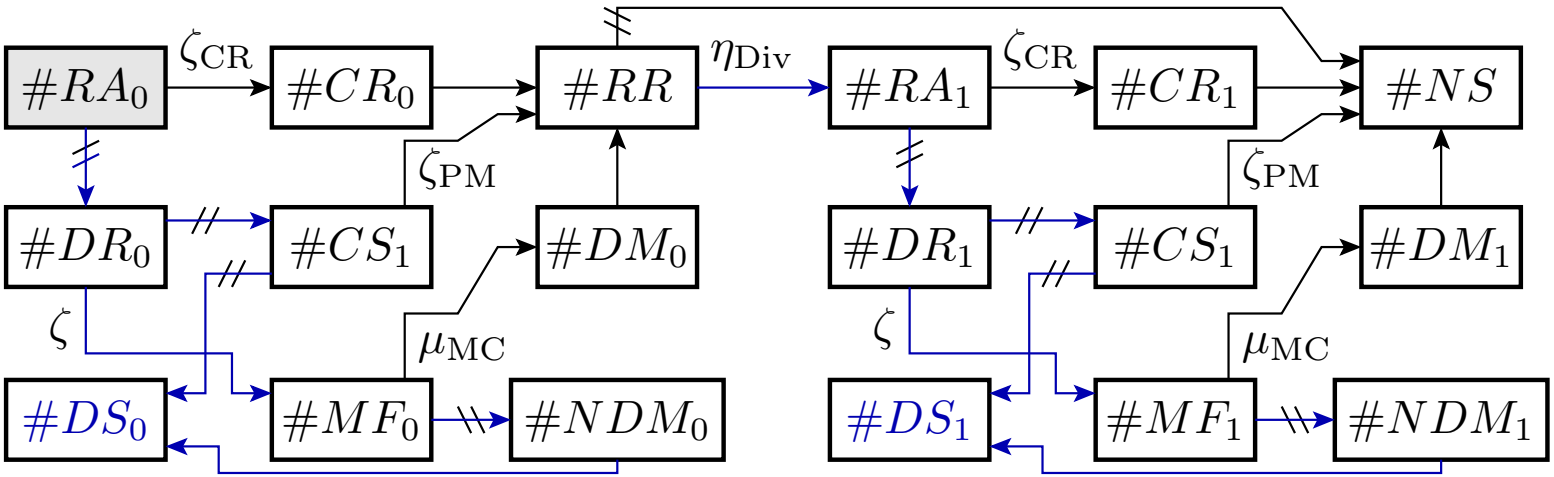
3.17 CVA graph: maximum one repetition



- If crash, detected malfunction or phantom malfunction on first request, rerequest. If although a problem, cancel without service.
- In the case of non-diverse problems, new requests are never successful.

$\zeta_{\mathrm{CR}}, \zeta$	Crash rate. Malfunction rate.
$\mu\mathrm{MC}, \zeta_{\mathrm{PM}}$	Expected malfunction coverage. Phantom malfunction rate.
RA, CR	Accepted request. Crash.
DR, MF	Delivered result. Malfunction.
DM, NDM	Detected malfunction. Undetected malfunction.
CS, DS	Correct service. Delivered service.
NS, RR	Cancellation with no service. Renewed request.

3.18 Delivery rate in the example



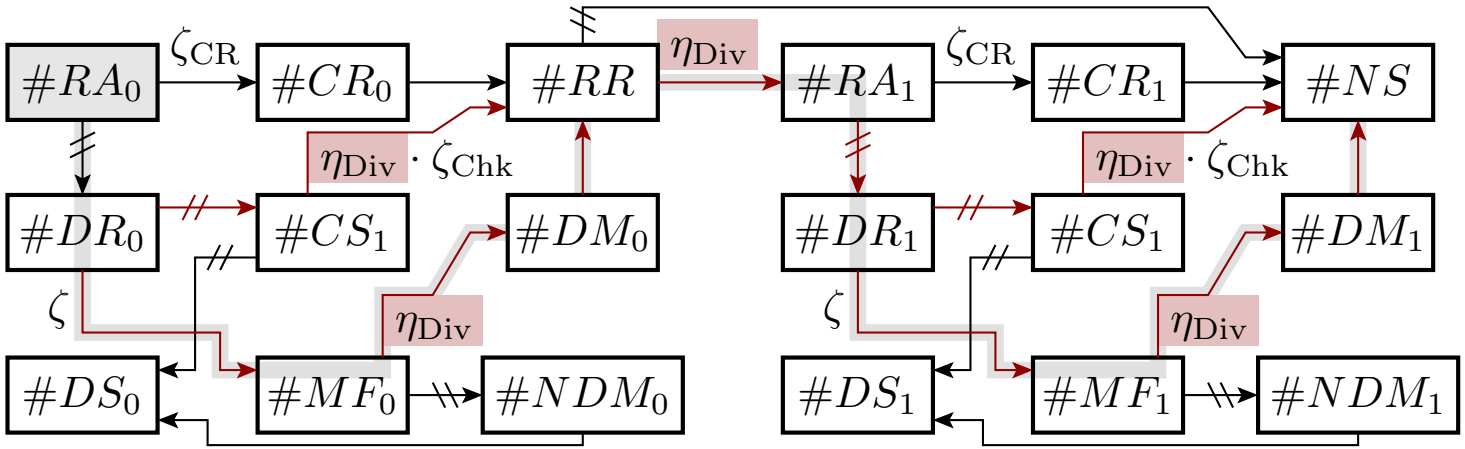
Delivery rate for first attempt and first plus second attempt:

(1.30) $$\eta_{\mathrm{DS}[0]} = \frac{\#DS}{\#RA}\Big|_{\mathrm{ACR}} = (1-\zeta_{\mathrm{CR}}) \cdot (\zeta \cdot (1-MC) + (1-\zeta) \cdot (1-\zeta_{\mathrm{PM}}))$$

(1.52) $$\eta_{\mathrm{DS}[1]} = \frac{\#DS_0+\#DS_1}{\#RA_0}\Big|_{\mathrm{SLC}} = \eta_{\mathrm{DS}[0]} + \left(1-\eta_{\mathrm{DS}[0]}\right) \cdot \eta_{\mathrm{Div}} \cdot \eta_{\mathrm{DS}[0]}$$

Exclusion and independence are ensured if the crash, malfunction and detection events per request are independent of one another. Independence between the first and second request ensures the η_{Div}-edge between the associated subgraphs.

3.19 Special case: majority decision



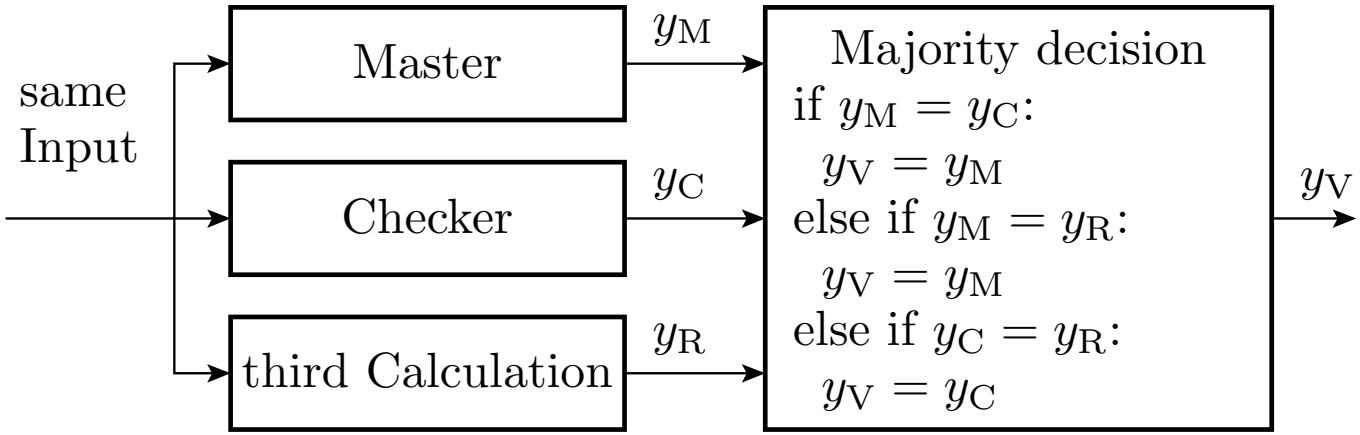
Verification by duplication and comparison. In the case of comparison errors, third-party calculations and service provision, only when two results match. Malfunction coverage and phantom MF rate per requests:

(1.39) $$\mu_{\mathrm{MC}} = \eta_{\mathrm{Div}}$$

(1.40) $$\zeta_{\mathrm{PM}} = \eta_{\mathrm{Div}} \cdot \zeta_{[\mathrm{Chk}]}$$

The path highlighted in grey from RA_0 to DM_1 runs via **three** η_{Div} **edges**, linked to the same event, namely whether the detected problem affects the three results differently or identically. Invalid CVA graph. A **creative redesign** is required

3.20 Modelling as a majority decision

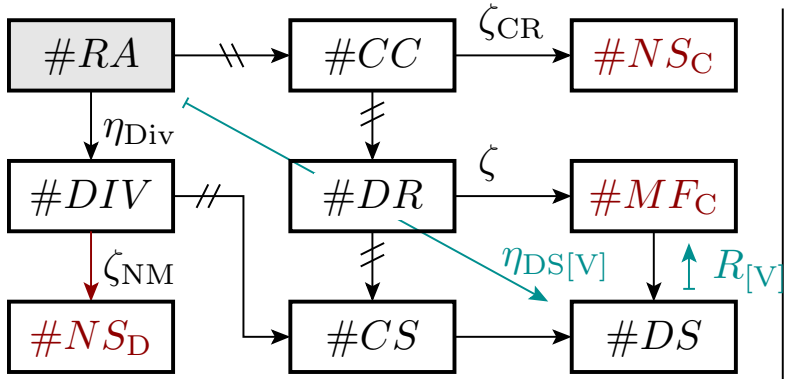


If at least two identical results are produced, the majority result is output; otherwise, no result is produced.

The third calculation is only required if the Master and Checker results differ, and must only be carried out at that point.

The concept was first described by John von Neumann. The earliest computers were three-version systems designed to tolerate frequent hardware failures (see slide »Majority decision with emergency mode«, section 6.6.2).

y_M, y_C Master result. Checker result.



ζ_{NM} Gesamtrate für keine erbrachtes Mehrheitsergebnis, wenn diversitär

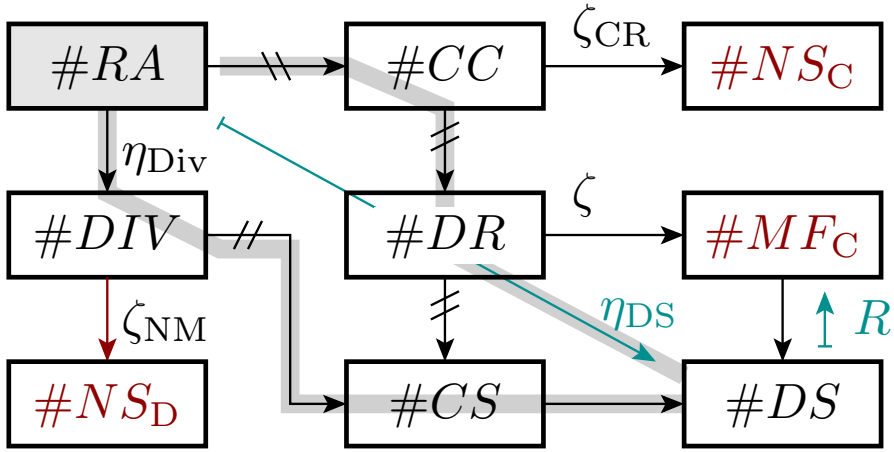
$R_{[\mathrm{V}]}$ Zuverlässigkeit

RA	Anforderungen akzeptiert
CC	gleiche Problemursache
DIV	unabhängige Probleme
NS_{C}	Absturz mit gleicher Ursache
MF_{C}	identische Fehlfunktion
CS	richtiges Mehrheitsergebnis
NS_{D}	zufällig gleichzeitige Probleme
DS	erbrachte Service-Leistung
DR	Erbringung gesicht
ζ_{CR}	CC-Absturzrate
ζ	CC-Fehlfunktionsrate
$\eta_{\mathrm{DS[V]}}$	Erbringungsrate

- Auftretende Probleme (Abstürze, Fehlfunktionen) haben mit Häufigkeit η_{Div} unabhängige Ursachen bzw. unterschiedliche Wirkung.
- Nichterbringung bei Absturz mit gemeinsamer Ursache (NS_{C}) und fehlender Mehrheit (NS_{D}).
- Falsche Mehrheit praktisch nur durch gemeinsame Ursache (MF_{C}). Denn zufällige Übereinstimmung von Datensätzen aus vielen Bits praktisch unmöglich.

Die Rate ζ_{NM} beschreibt die Häufigkeit, dass weniger als zwei der drei Berechnungen das richtige Ergebnis liefern, d.h. max. ein Absturz oder Fehlfunktion je drei Berechnungen. In der Regel vernachlässigbar klein.

3.22 Verfügbarkeit



Erbringungsrate :

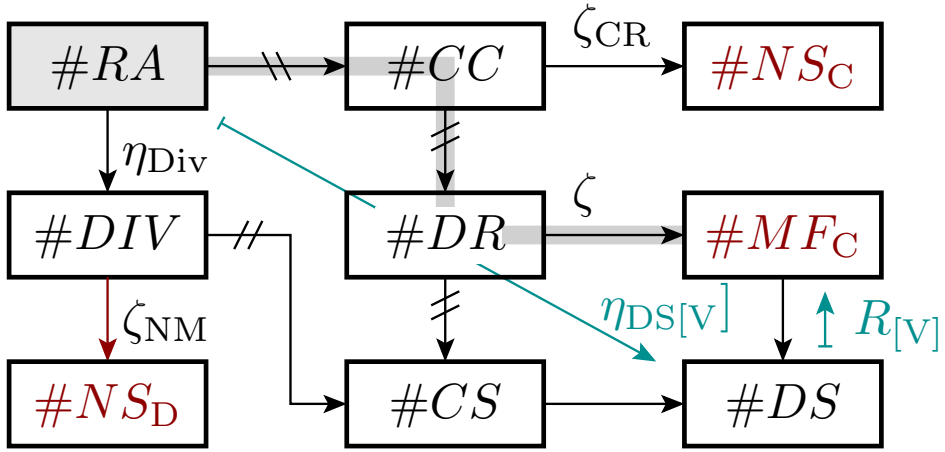
$$\eta_{\mathrm{DS[V]}} = \left.\frac{\#DS}{\#RA}\right|_{\mathrm{SLC}} = \eta_{\mathrm{Div}} \cdot (1 - \zeta_{\mathrm{NM}}) + (1 - \eta_{\mathrm{Div}}) \cdot (1 - \zeta_{\mathrm{CR}}) \tag{3.10}$$

Unter Vernachlässigung des unwahrscheinlichen Falls, dass ohne gemeinsame Ursache zufällig bei zwei der drei Berechnungen ein Problem auftritt (Absturz oder Fehlfunktion) $\zeta_{\mathrm{NM}} = 0$:

$$\eta_{\mathrm{DS[V]}} = \eta_{\mathrm{Div}} + (1 - \eta_{\mathrm{Div}}) \cdot (1 - \zeta_{\mathrm{CR}})$$
$$\eta_{\mathrm{DS[V]}} = 1 - (1 - \eta_{\mathrm{Div}}) \cdot \zeta_{\mathrm{CR}} \tag{3.11}$$

η_{Div}	Diversity rate, defined as fault coverage by doubling and comparison.
ζ, ζ_{CR}	Malfunction rate. Crash rate (individually for each service).
$\eta_{\mathrm{DS[V]}}$	Rate of majority results delivered.
$R_{\mathrm{[V]}}$	Reliability overall sytem with majority voting.

3.23 Zuverlässigkeit



Nicht erkannte Fehlfunktionen nur durch gemeinsame Ursache (MF_C):

$$R_\mathrm{[V]} = \left.\frac{\#DS}{\#MF_\mathrm{C}}\right|_\mathrm{SLC} = \frac{\eta_\mathrm{DS[V]}}{(1-\eta_\mathrm{Div})\cdot(1-\zeta_\mathrm{CR})\cdot\zeta} \tag{3.12}$$

Für hohe Erbringungsrate $\eta_\mathrm{DS[V]} \approx 1$ und seltene Abstürze $\zeta_\mathrm{CR} \ll 1$:

$$R_\mathrm{[V]} = \frac{R}{(1-\eta_\mathrm{Div})} \tag{3.13}$$

$R_\mathrm{[V]}$, R Reliability with majority voting. Reliability single system.

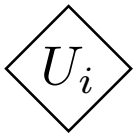
Fehlerbäume

3.24 Fehlerbaumanalyse (FTA)

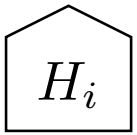
FTA (fault tree analysis) ist eine graphische Darstellung für logische Ereignisbeziehungen (UND, ODER, Nicht*) zur Abschätzung der Eintrittswahrscheinlichkeiten von Gefahrensituationen, Ausfälle, Fehlfunktionen, ... Unterschiedene Ereignistypen:



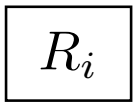
Basisereignis mit bekannter oder auf anderem Wege abgeschätzter Eintrittswahrscheinlichkeit.



unerschlossenes Ereignis, über das nur unzureichende Informationen verfügbar sind.



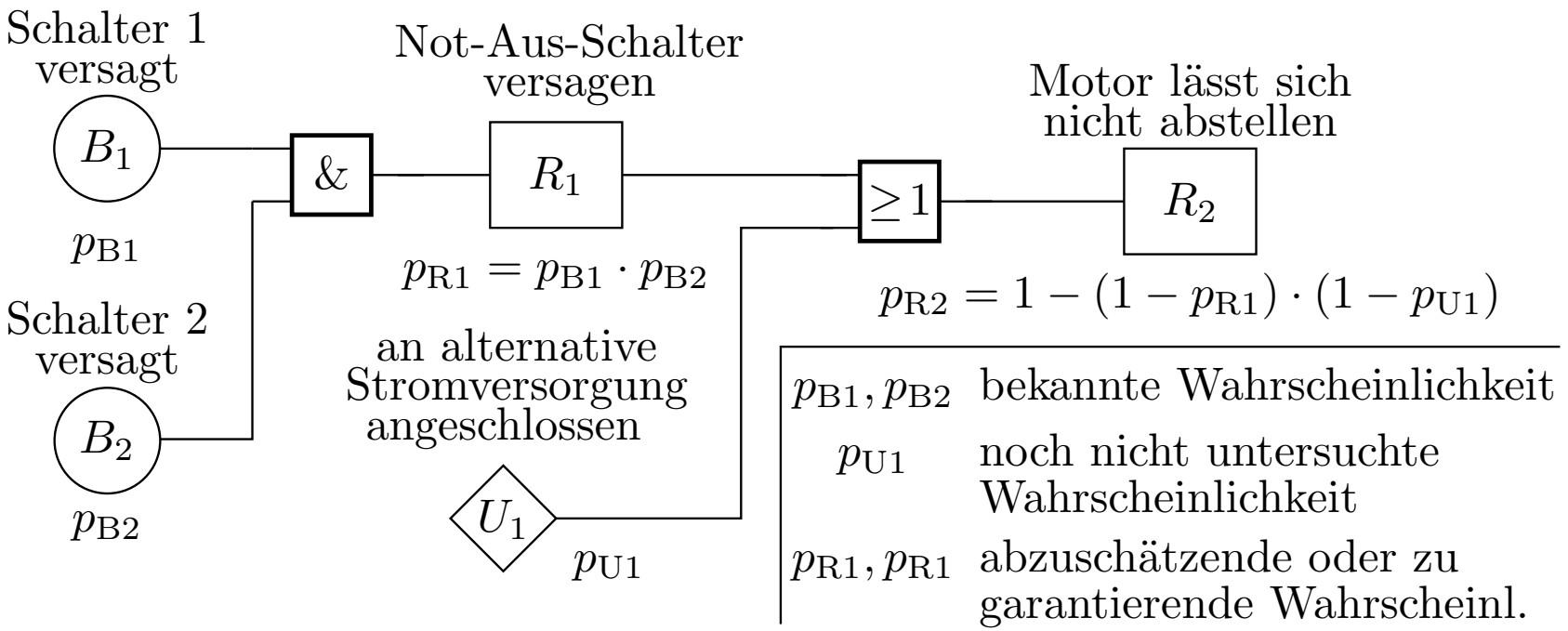
Hausereignis im gewöhnlichen Betrieb, das mit anderen zusammen Probleme verursachen kann.



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

* Abweichend von der klassischen Fehlerbaumdarstellung verwenden wir für logische UND-, ODER- und NICHT die Schaltsymbole aus der Digitaltechnik.

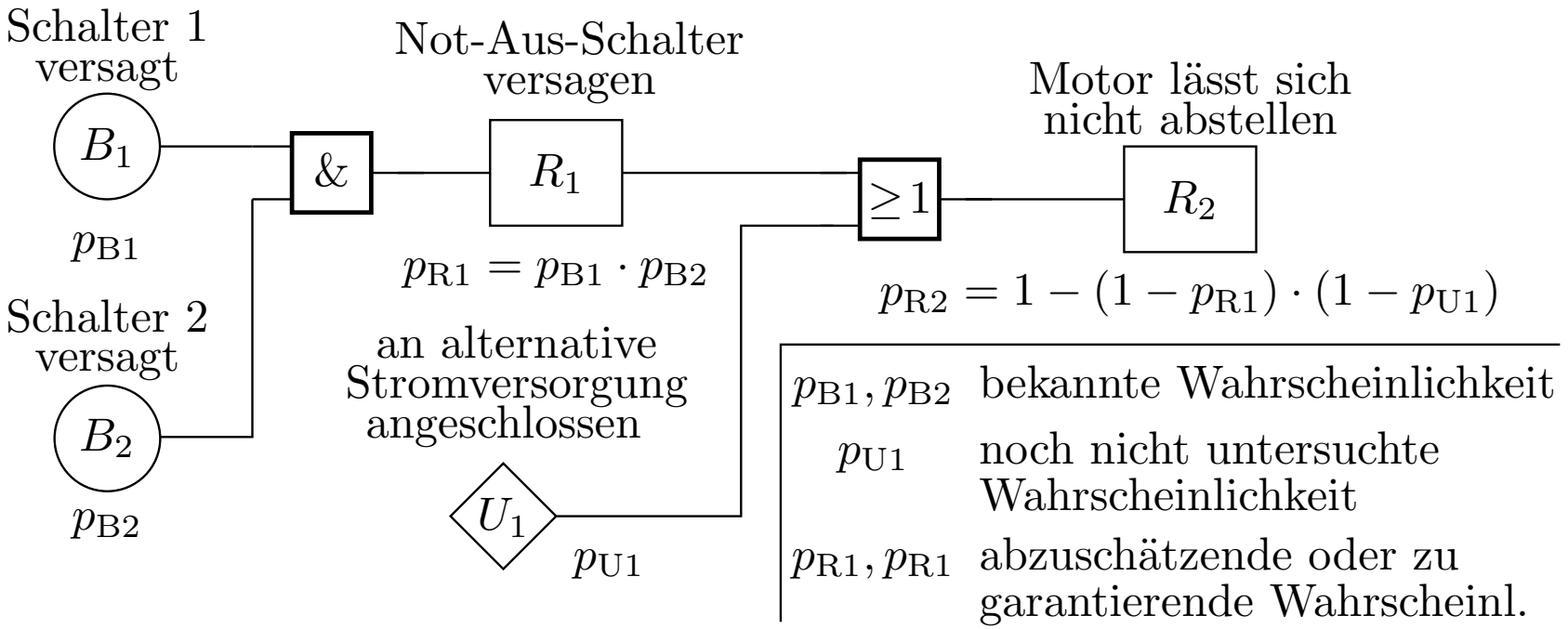
Example 3.4: Motor lässt sich nicht abstellen



Denkbare Aufgabenstellung:

Ist $p_{R2} \leq 10^{-6}$ *erzielbar mit* $p_{B1} = p_{B2} = 10^{-3}$*?*

B_i Base event with known or otherwise estimated probability.
R_i Resulting event whose probability of occurrence is to be estimated.
U_i Undeveloped event about which insufficient information is available.



Ist $p_{R2} \leq 10^{-6}$ erzielbar mit $p_{B1} = p_{B2} = 10^{-3}$?

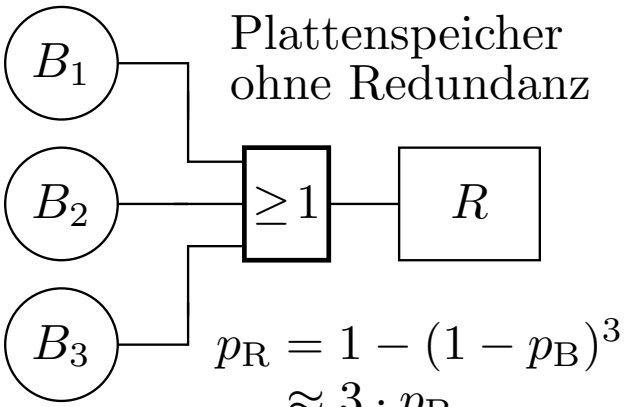
$$p_{R1} = p_{B1} \cdot p_{B2} = 10^{-6}$$

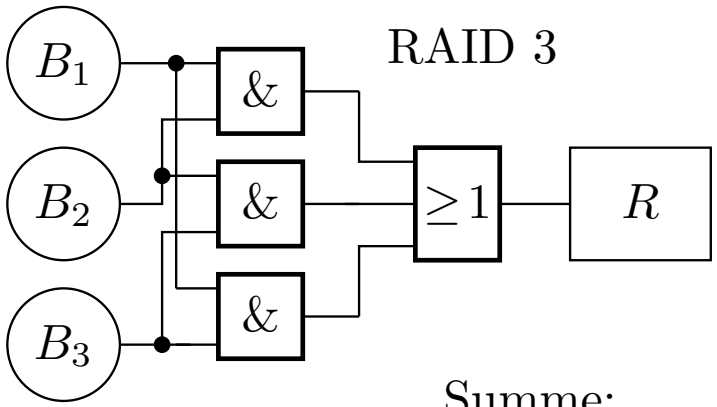
$$p_{R2} = 1 - (1 - p_{R1}) \cdot (1 - p_{U1}) \leq 10^{-6}$$

Es gibt nur die Lösung mit $p_{U1} = 0$. Lässt sich das Risiko einer alternativen Stromversorgung ausschließen oder muss die Gesamtlösung nachgebessert werden?

3.26 Datensicherheit RAID

Ein redundanzfreies Speichersystem aus drei Festplatten verliert Daten, wenn eine der drei Festplatten ausfällt, ein RAID 3 erst, wenn gleichzeitig zwei Platten ausfallen.





B_i	Ausfall Platte i
R	Datenverlust (result. Ereignis)
p_B	Ausfallwahrscheinlichkeit je Zeitschritt für eine Festplatte
p_R	Wahrscheinlichkeit Datenverlust je Zeitschritt Gesamtsystem

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

Summe:

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

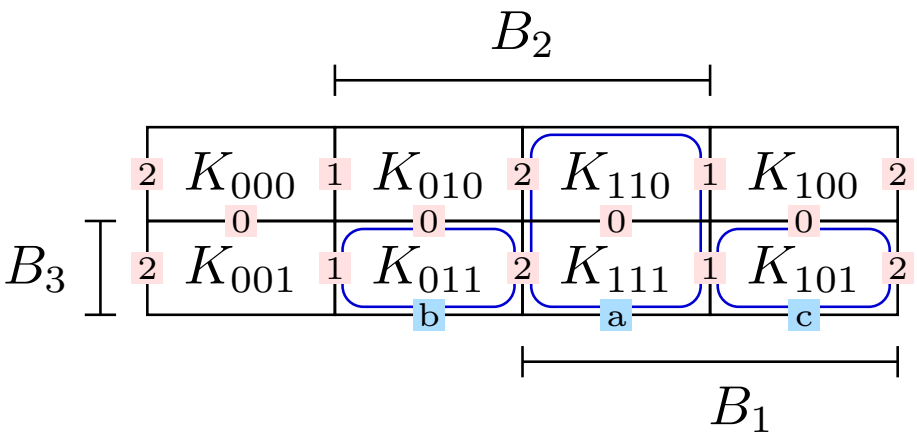
3.27 Rekonvergente Auffächerungen

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

$$R = B_1 B_2 \vee B_2 B_3 \vee B_1 B_3$$

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

Umstellung in Terme sich ausschließender Ereignisse:

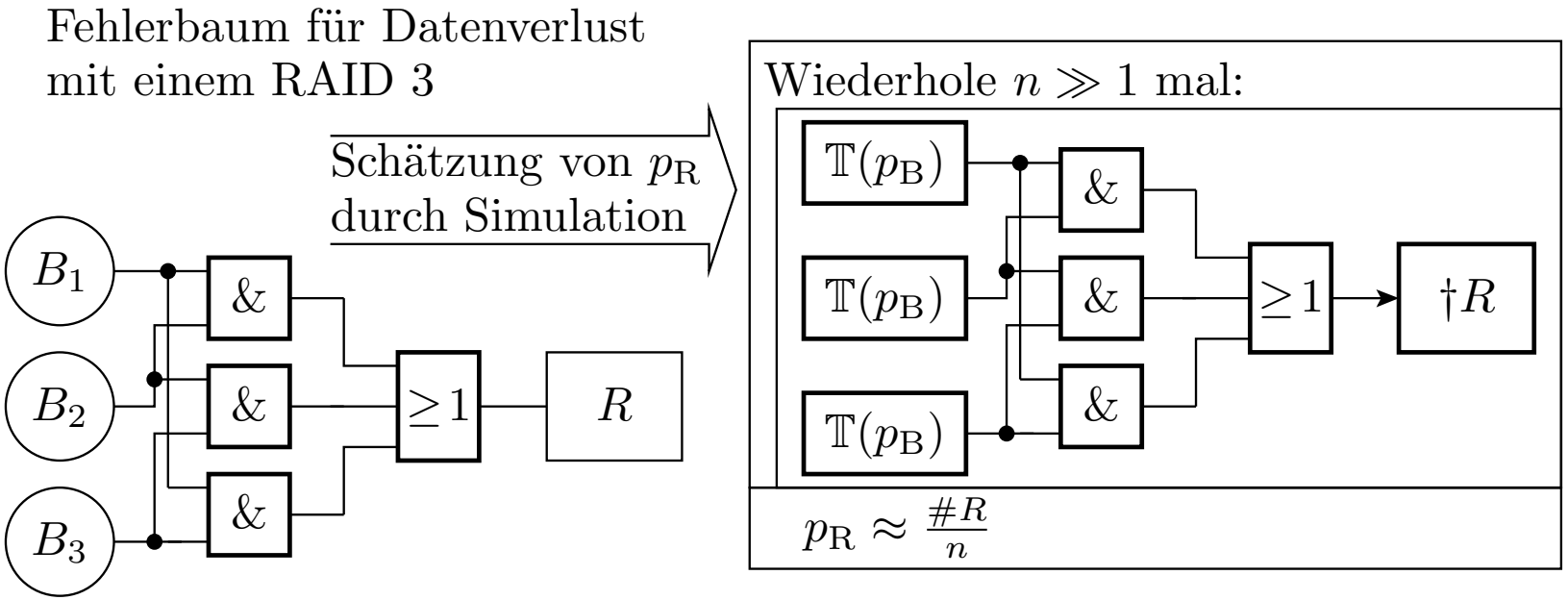


Überdeckungsfreie Konjunktionen:

- a: $B_1 B_2$
- b: $\bar{B}_1 B_2 B_3$
- c: $B_1 \bar{B}_2 B_3$

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

3.28 Notlösung Simulation



Wenn Rekonvergenzen nicht ausschließbar oder zur Kontrolle abgeschätzter Formeln Wahrscheinlichkeitsabschätzung durch Simulation:

- Generierung unabhängiger Eingabeereignisse.
- logische Verknüpfung und Zählen der resultierenden Ereignisse.

$\mathbb{T}(\eta)$ Random event (1 with probability η, otherwise 0).
$\dagger A$ Counting event (triggering or triggered).

3.29 Geschichte der Fehlerbaumanalyse

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

Beim Einsatz zur Sicherheitsbewertung

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

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

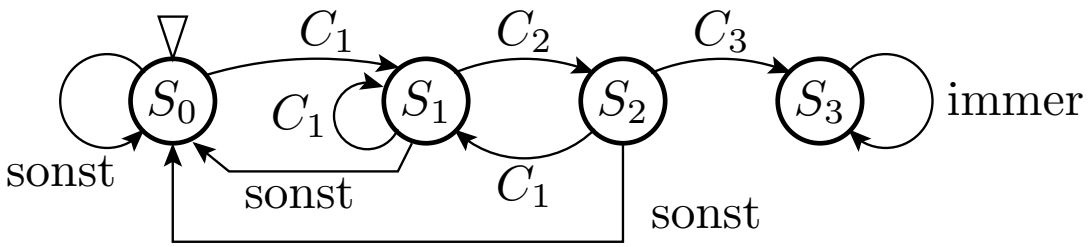
Schätzfehler: unberücksichtigte Schadensereignisse, Einflüsse, ... Für Interkontinentalraketen mit Atomsprengköpfen nicht sehr vertrauenserweckend. **Es gibt aber offensichtlich kein besseres Verfahren**.

Markov-Ketten

3.30 Markov-Ketten$^{(Markov)}$

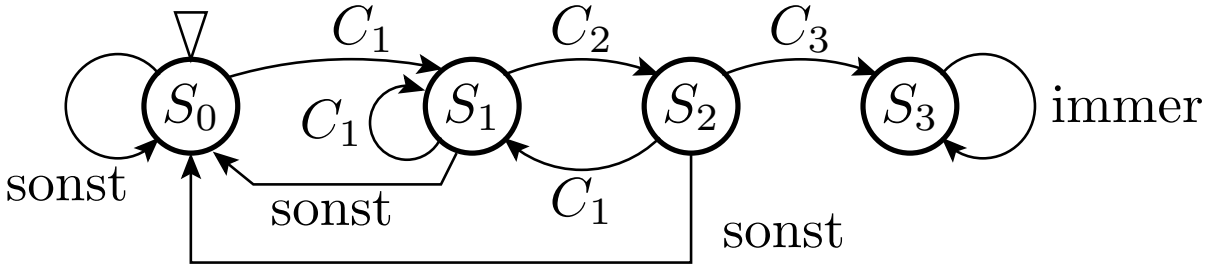
Eine Markov-Kette (MC) ist ein stochastisches Modell für Ereignisfolgen, deren Verarbeitung sich durch einen endlichen Automaten beschreiben lässt.

Zustandsautomat Fehlernachweis mit Eingabefolge $C_1C_2C_3$:

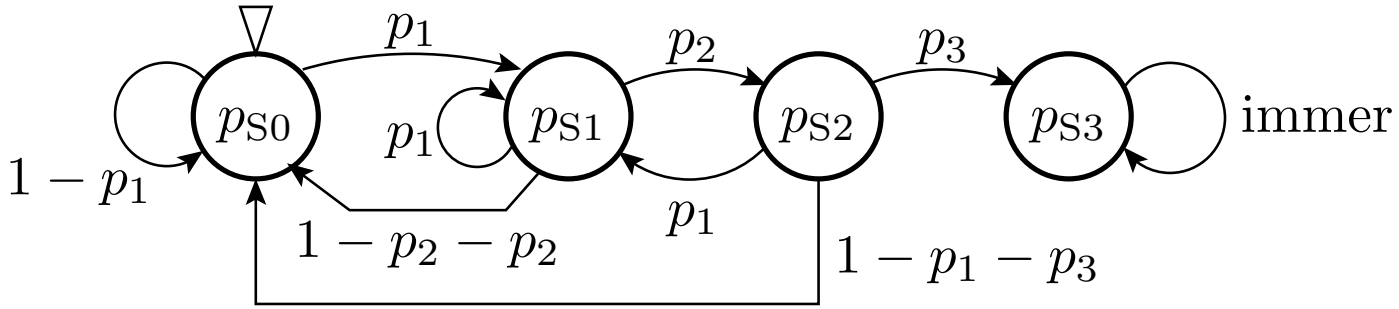


Start im Zustand S_0 »keine richtige Eingabe« und Verbleib nach drei richtigen Eingaben im Zustand S_3 »Fehler nachgewiesen«.

S_i State i of Markov chain.
C_j Transitional condition j.
$(Markov)$ Andrej Andreevič Markov, Russian mathematician, 1856-1922.



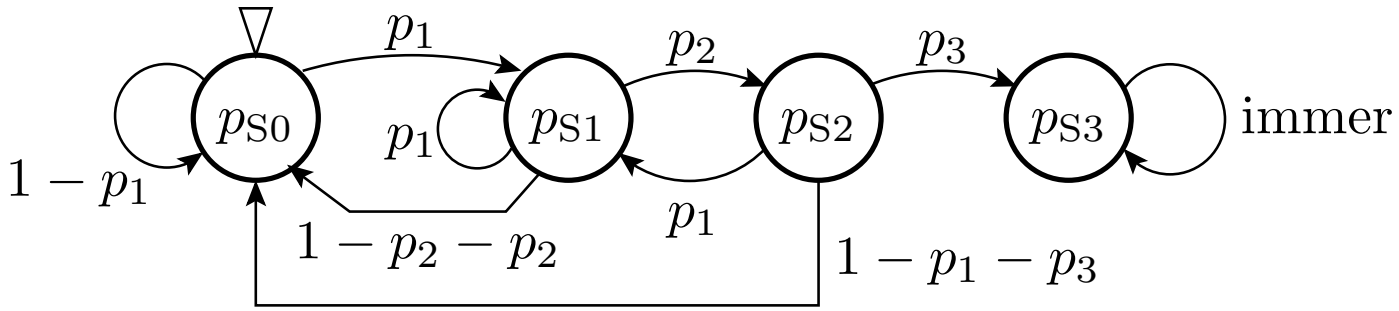
In der Markov-Kette werden Übergangsbedingungen durch die Übergangswahrscheinlichkeiten und Zustände durch Zustandswahrscheinlichkeiten ersetzt.



Zu Beginn hat der Startzustand S_0 die Wahrscheinlichkeit $p_{S0} = 1$ und die anderen Zustände haben die Wahrscheinlichkeit $p_{S.i}|_{i \neq 0} = 0$.

In jedem Schritt verteilt jeder Knoten seine Wahrscheinlichkeit über seine abgehenden Kanten auf Zielknoten. $\sum p_{S.i}$ bleibt immer 100%.

p_{Si} Probability that the Markov chain is in state S_i.
p_j Probability of transition C_j.



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

$$\begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_1-p_2 & 1-p_1-p_3 & 0 \\ p_1 & p_1 & p_1 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_{n-1}$$

mit $\begin{pmatrix} p_{S0} & p_{S1} & p_{S2} & p_{S3} \end{pmatrix}_0^T = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^T$.

Kontrollkriterien für Gleichungssystem und Simulationsergebnis:

- Summe der Wahrscheinlichkeiten je Matrixspalte eins.
- Summe aller $p_{S.i}$ nach jedem Schritt eins.

$(\ldots)^T$ Transposed matrix (exchange of rows and columns).
n Step number of the Markov chain simulation.

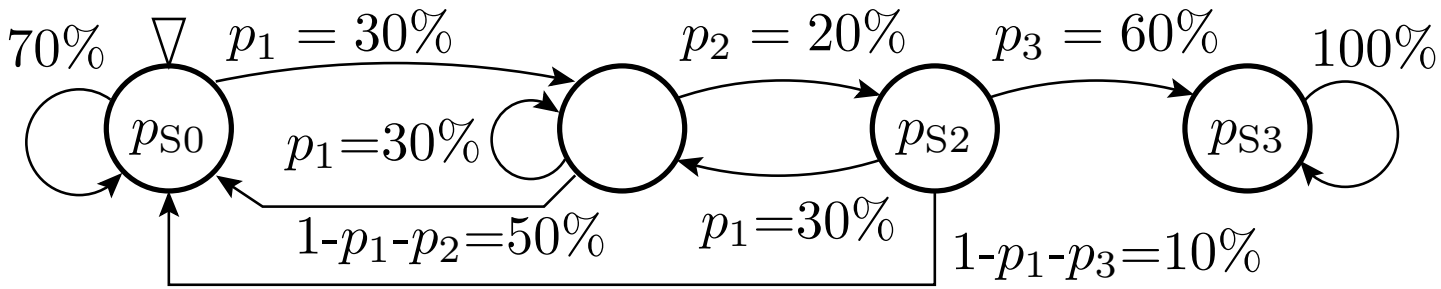
$$\begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_n = \begin{pmatrix} 1-p_1 & 1-p_1-p_2 & 1-p_1-p_3 & 0 \\ p_1 & p_1 & p_1 & 0 \\ 0 & p_2 & 0 & 0 \\ 0 & 0 & p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \end{pmatrix}_{n-1}$$

Simulation mit Octave bzw. Matlab:

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

3.34 Beispielsimulation

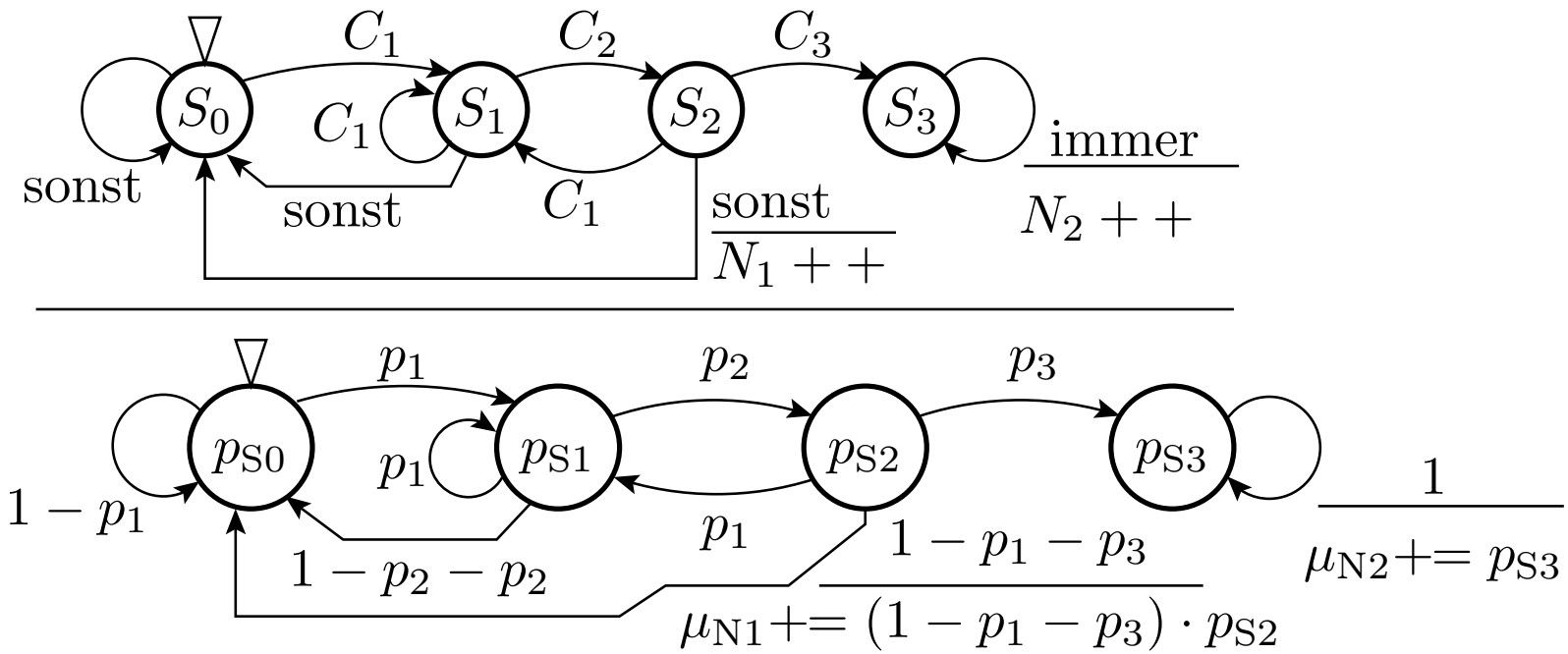
Übergangswahrscheinlichkeiten: $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$:



Schritt	p_{S0}	p_{S1}	p_{S2}	p_{S3}	$\sum_{i=0}^{3} p_{Si}$
0	100,00%	0	0	0	100%
1	70,00%	30,00%	0	0	100%
2	64,00%	30,00%	6,00%	0	100%
3	60,40%	28,20%	7,80%	3,60%	100%
4	57,16%	26,58%	7,89%	8,28%	100%
...	...	...	...	...	...
10	41,08%	19,06%	5,90%	33,96%	100%
...	...	...	...	...	...
50	4,54%	2,11%	0,65%	92,71%	100%
...	...	...	...	...	...
100	0,29%	0,13%	0,04%	99,44%	100%

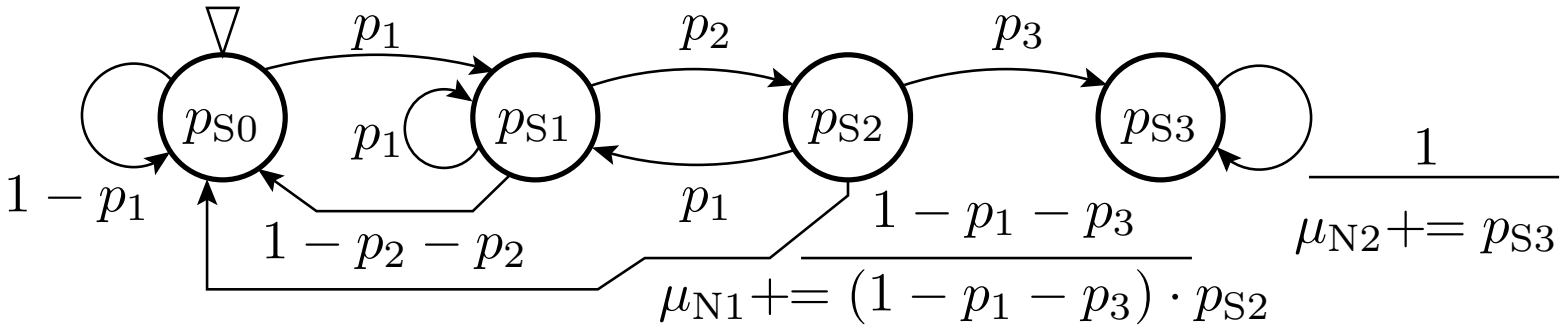
3.36 Kantenzähler

Mit Zählern an den Kanten lässt sich die Anzahl bzw. die zu erwartende Anzahl der Kantenübergänge, bestimmen:



n	Step number of the Markov chain simulation.
N_1	Counter, how often two correct entries are followed by a wrong one.
N_2	Counter for the number of steps after fault detection.
μ_{Ni}	Expected edge transition count.
$n - \mu_{N2}$	Expected number of steps until fault detection.

In den Variablen $\mu_{\mathrm{N}\ldots}$ werden die Wahrscheinlichkeiten der Kantenübergänge aufsummiert. Das sind die Erwartungswerte der Anzahl der Übergänge. μ_{N2} summiert die Häufigkeit, wie oft das System in S_3 bleibt bzw. sich in S_3 befindet.

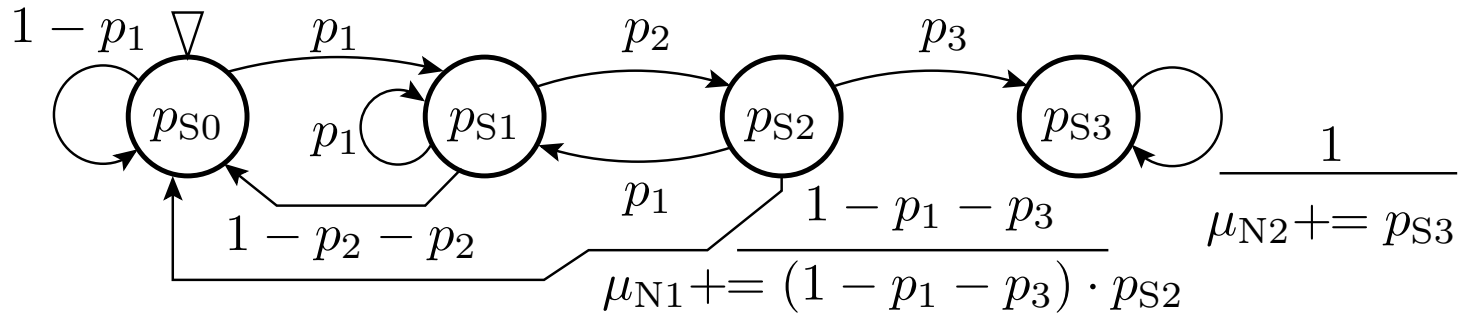


Erweiterung des Simulationsprogramms:

```
...
N1=0; N2=0;

for idx=1:100
 Z = M * Z;
 N1 = N1+Z(3)*(1-p1-p3);
 N2 = N2+Z(4);
 printf('%3i %6.2f%% %6.2f%% %6.2f%% %6.2f%%',idx,100*Z);
 printf('%6.2f %6.2f\n', N1, N2);
end;
```

3.38 Beispielsimulation

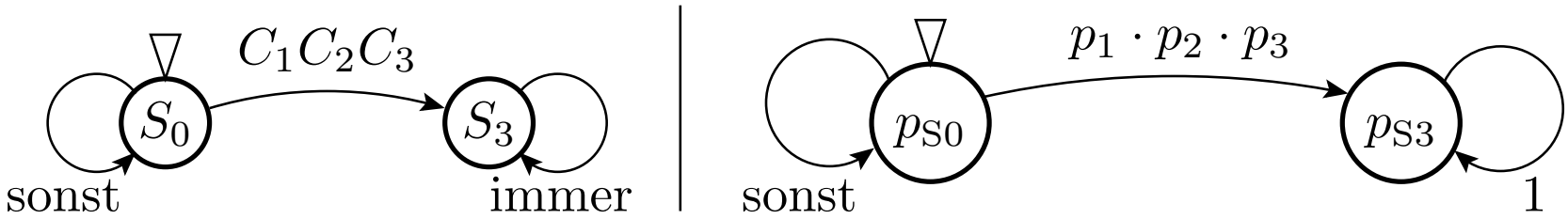
Übergangswahrscheinlichkeiten: $p_1 = 30\%$, $p_2 = 20\%$ und $p_3 = 60\%$



Schritt	p_{S0}	p_{S1}	p_{S2}	p_{S3}	μ_{N1}	μ_{N2}
1	70,00%	30,00%	0	0	0	0
2	64,00%	30,00%	6,00%	0	0,01	0
3	60,40%	28,20%	7,80%	3,60%	0,01	0,04
4	57,16%	26,58%	7,89%	8,28%	0,02	0,12
...	...	...	...	...	...	...
10	41,08%	19,06%	5,90%	33,96%	0,06	1,55
...	...	...	...	...	...	...
50	4,54%	2,11%	0,65%	92,71%	0,16	31,18
...	...	...	...	...	...	...
100	0,29%	0,13%	0,04%	99,44%	0,17	79,79

Zu erwartende Anzahl der Schritte bis zum Nachweis: $n - \mu_{N2} \approx 20$

3.39 Drei richtige Eingaben als Einzelereignis



Gleichungssystem der modifizierten Markov-Kette:

$$\begin{pmatrix} p_{S0} \\ p_{S3} \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_1 \cdot p_2 \cdot p_3 & 0 \\ p_1 \cdot p_2 \cdot p_3 & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{S0} \\ p_{S3} \end{pmatrix}_n \text{ mit } \begin{pmatrix} p_{S0} \\ p_{S3} \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

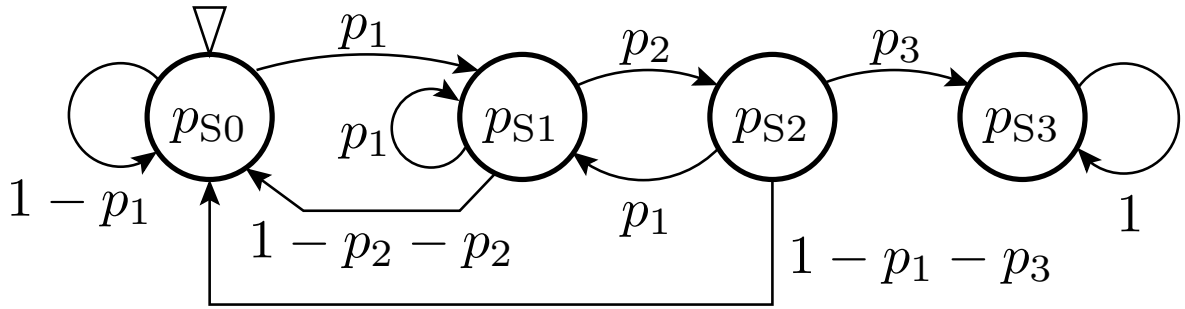
$$\begin{aligned} p_{S0}(n) &= (1 - p_1 \cdot p_2 \cdot p_3) \cdot p_{S0}(n-1) = (1 - p_1 \cdot p_2 \cdot p_3)^n \\ p_{S3}(n) &= 1 - p_{S0}(n) = 1 - (1 - p_1 \cdot p_2 \cdot p_3)^n = 1 - \mathrm{e}^{\ln(1-p_1 \cdot p_2 \cdot p_3) \cdot n} \end{aligned}$$

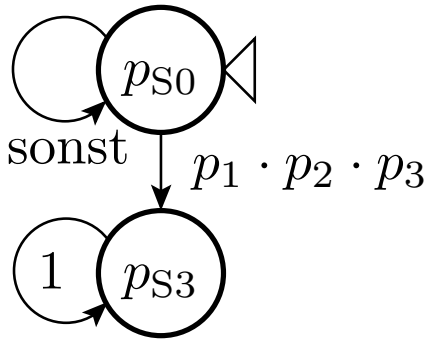
Für $p_1 \cdot p_2 \cdot p_3 \ll 1$*:

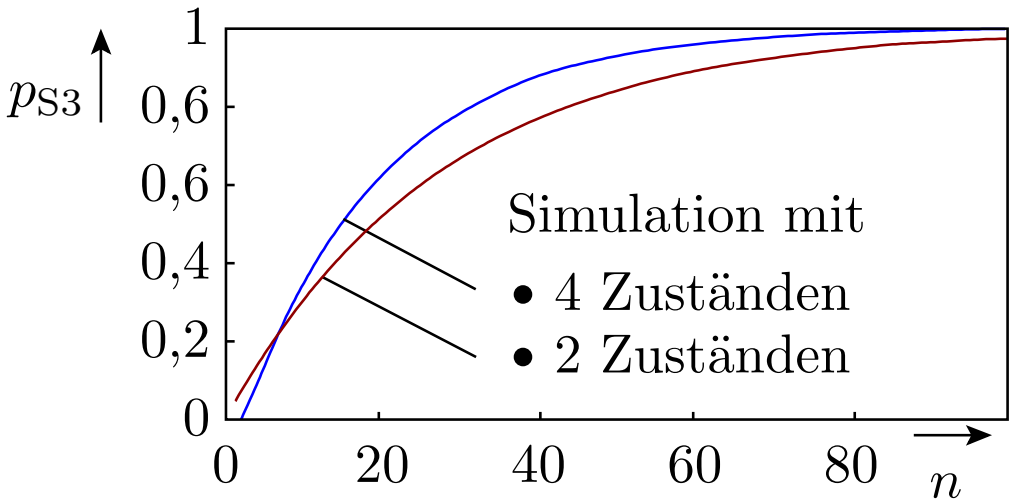
$$\begin{aligned} p_{S0}(n) &= \mathrm{e}^{-p_1 \cdot p_2 \cdot p_3 \cdot n} \\ p_{S3}(n) &= 1 - \mathrm{e}^{-p_1 \cdot p_2 \cdot p_3 \cdot n} \end{aligned}$$

* Approximation by first member Taylor series: $\ln(1-x) = -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots\right)$.

3.40 Unterschied zwischen den Markov-Ketten



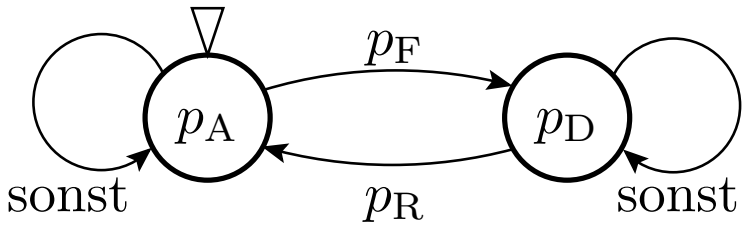




Die Vermutung, dass die rechte Markov-Kette den Endzustand »drei Richtige in Folge« zwischen null und drei Schritten schneller erreicht, offenbar aus einem nicht offensichtlichen Grund unzutreffend.

3.41 Abschätzung einer Verfügbarkeit

Ein System sei zu Beginn funktionsfähig (Zustand A), fällt in jedem Zeitschritt, wenn es ganz ist, mit einer Wahrscheinlichkeit p_F aus (Übergang in Zustand D) und wird, wenn es kaputt ist, innerhalb des Zeitschritts mit einer Wahrscheinlichkeit p_R repariert (Übergang in Zustand A):

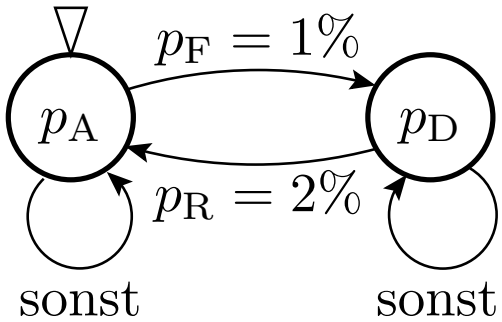


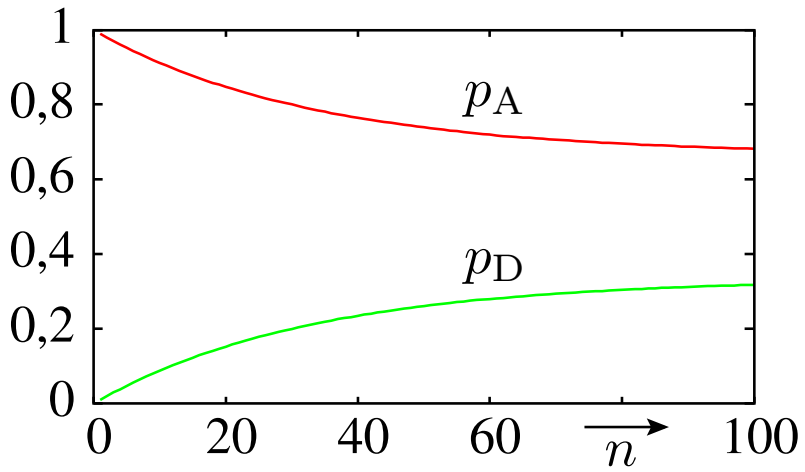
Modellierung als simulierbares Gleichungssystem:

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

p_A	Probability that the system is available.
p_D	Probability that the system is defect.
p_F	Probability that the system will fail in the time step.
p_R	Probability that the system will be repaired in the time step.
n	Step number of the Markov chain simulation.

3.42 Beispielsimulation





Stationärer Zustand (Zufluss von Wahrscheinlichkeit gleich Abfluss):

$$p_A \cdot p_F = p_D \cdot p_R \quad \text{with} \quad p_A + p_D = 1$$

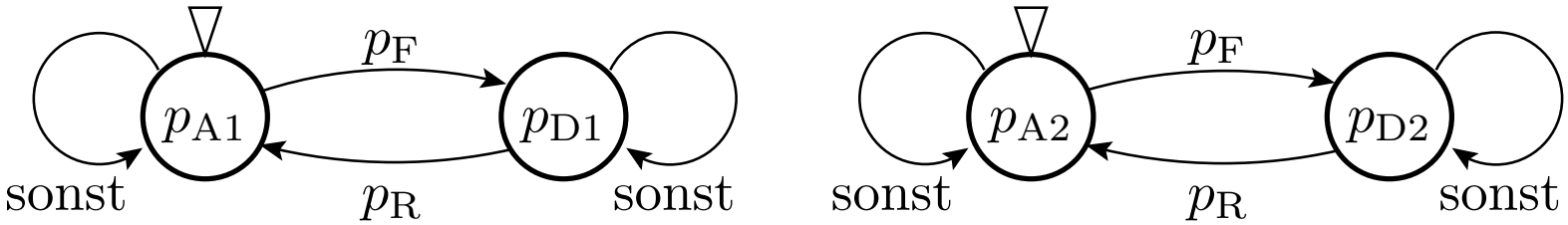
$$p_A = \frac{p_R}{p_R + p_F} = \frac{2\%}{1\% + 2\%} = 66{,}7\%$$

$$p_D = \frac{p_F}{p_R + p_F} = \frac{1\%}{1\% + 2\%} = 33{,}3\%$$

p_A	Probability that the system is available.
p_D	Probability that the system is defect.
p_F	Probability that the system will fail in the time step.
p_R	Probability that the system will be repaired in the time step.

3.43 Reparaturprozess für ein 1oo2 System

System aus zwei gleichartigen Teilsystemen, das solange funktioniert, wie 1 von (**o**ut **o**f) 2 Teilsystemen funktioniert (sec. 6.6.2):

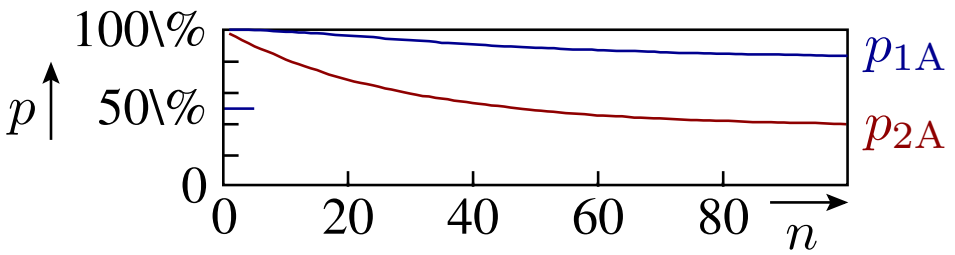



```
pF=0.01; pR=0.02;
M=[1-pF  pR; pF  1-pR];
S=[1; 0];
for n=1:100
  S = M * S;
  p1A(n)=1-S(1)**2; % min. eine Einheit verfügbar
  p2A(n)=S(2)**2; % beide Einheiten verfügbar
end;
plot(1:100, p1A, 1:100, 1-p2A)
```

$k$oo$n$ Ssystem of n identical subsystems, available as long as k components are available.

3.44 Beispielsimulation

Simulation
mit $p_{\mathrm{F}} = 1\%$
und $p_{\mathrm{R}} = 2\%$



		für sehr große n
mindestens eins verfügbar	$p_{1\mathrm{A}} = 1 - p_{\mathrm{D}}^2$	$1 - (1/9)$
beide Systeme verfügbar	$p_{2\mathrm{A}} = p_{\mathrm{A}}^2$	$(2/3)^2$

- **1oo2-Reserve nur für hoch verfügbare Einzelsystem sinnvoll.**
- Im Beispiel wäre ein $p_{\mathrm{R}} \gg p_{\mathrm{F}}$ zielführender.

n	Step number of the Markov chain simulation.
p_{F}	Probability that the system will fail in the time step.
p_{R}	Probability that the system will be repaired in the time step.
$p_{2\mathrm{D}}$	Probability that both systems are defect.
$p_{\geq 1\mathrm{A}}$	Probability that at least one system is availablee.
$p_{2\mathrm{A}}$	Probability that both systems are available.

Zusammenfassung

3.45 Wahrscheinlichkeit (𝕃)

Unter konstanten Versuchbedingungen strebt die Eintrittshäufigkeit von Zählversuchen gegen die Eintrittswahrscheinlichkeit:

(3.1) $$\mathbb{P}[A] = \lim_{n\to\infty} \frac{\#A}{n}$$

Die Wahrscheinlichkeit ist die beste Vorhersage der zu erwartenden relativen Häufigkeit künftiger Versuche.

Bei gleichhäufigen möglichen Ereignissen ist die Wahrscheinlichkeit der Anteil der günstigen Ereignisse.

Komplexe Ereignisse lassen sich oft durch logische Verknüpfungen einfacher zu untersuchender Ereignisse beschreiben. Zusatzbedingungen mit Einfluss auf die Eintrittshäufigkeit sind zu berücksichtigen.

Für logische Ereignisverknüpfungen bietet die Mathematik nur Lösungen für UND, ODER und NOT unabhängiger und sich ausschließender Ereignisse. Für andere Abhängigkeiten müssen die logischen Beziehungen entsprechend umgestellt werden.

Abschätzung durch Simulation funktioniert immer.

3.46 Werkzeugkasten für verkettete Ereignisse

Bedingte Wahrscheinlichkeit:

(3.2) $$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \wedge B]}{\mathbb{P}[B]}$$

Satz von Bayes: $(\mathbb{B})$

(3.3) $$\mathbb{P}[B|A] = \mathbb{P}[A|B] \cdot \frac{\mathbb{P}[B]}{\mathbb{P}[A]}$$

Gegenwahrscheinlichkeit: $(\mathbb{L})$

(3.4) $$\mathbb{P}\left[\bar{A}\right] = 1 - \mathbb{P}[A]$$

UND unabhängiger Ereignisse: $(\mathbb{L})$

(3.5) $$\mathbb{P}[A \wedge B] = \mathbb{P}[A] \cdot \mathbb{P}[B]$$

UND sich ausschließerder Ereignisse: $(\mathbb{L})$

(3.6) $$\mathbb{P}[A \wedge B] = 0$$

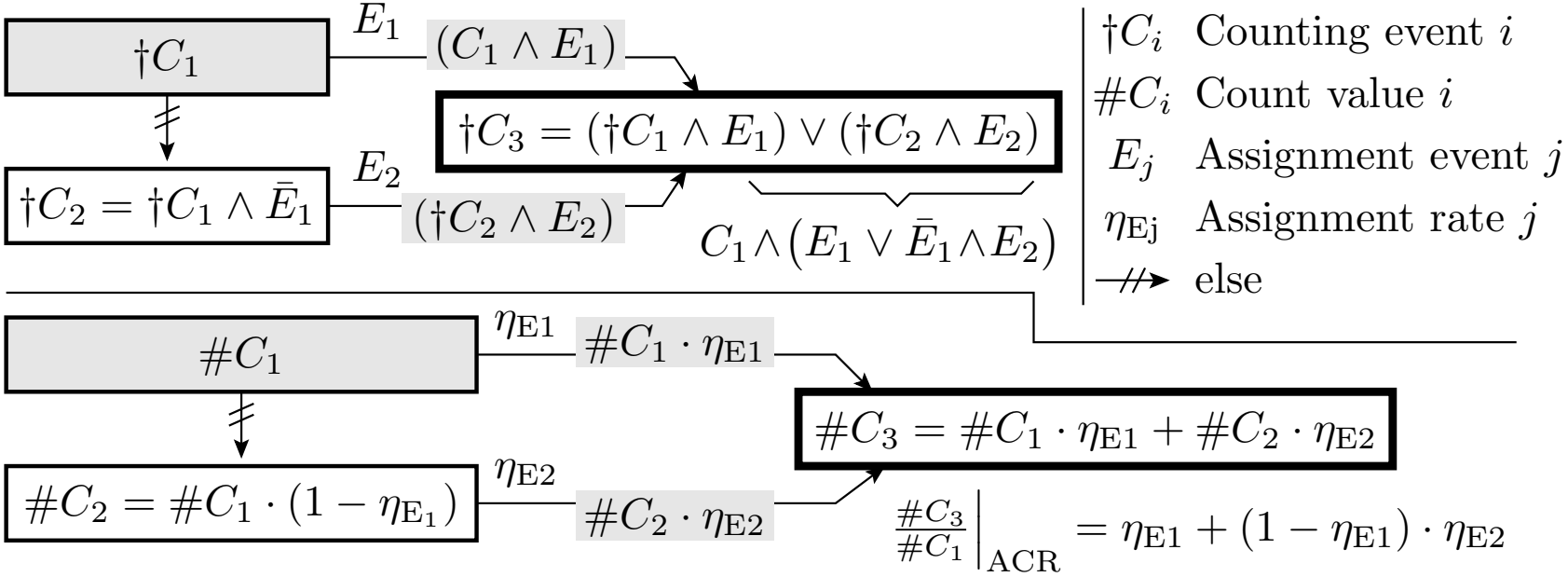
ODER unabhängiger Ereignisse: $(\mathbb{L})$

(3.7) $$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B] - \mathbb{P}[A] \cdot \mathbb{P}[B]$$

ODER sich ausschließender Ereignisse: $(\mathbb{L})$

(3.8) $$\mathbb{P}[A \vee B] = \mathbb{P}[A] + \mathbb{P}[B]$$

3.47 Zählwertzuordnungsgraph (𝕃)

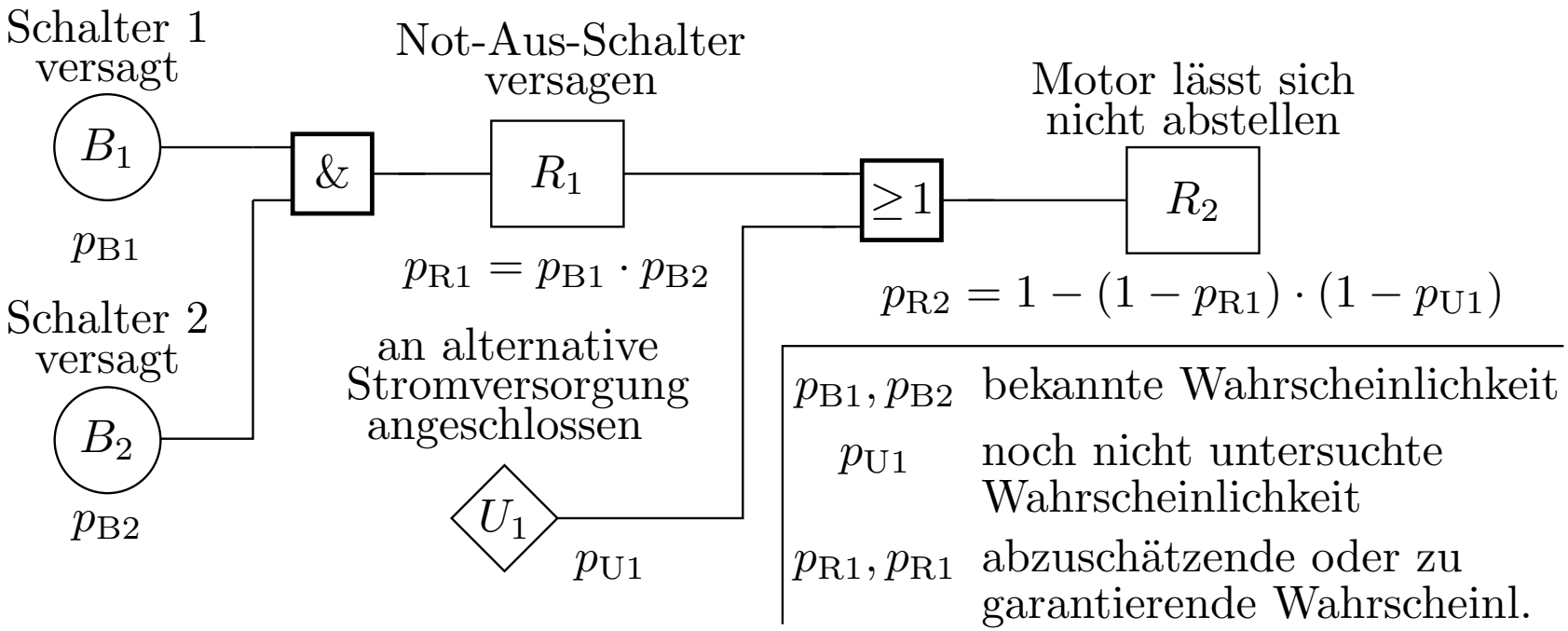


Beschreibung von Zählwertzuordnungen

- über Kanten durch unabhängige und
- bei Zusammenführung über sich ausschließende Ereignisse.

Unser bereits schon vorher benutztes Werkzeug zur eindeutige Beschreibung von Kenngrößen. Einfaches Ablesen auch weniger offensichtlicher Beziehungen zwischen Kenngrößen.

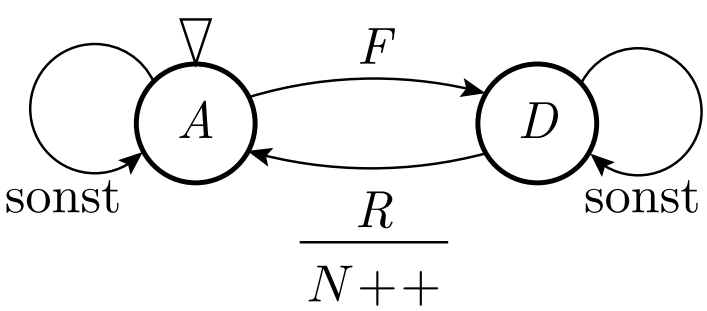
3.48 Fehlerbäume (𝔹)

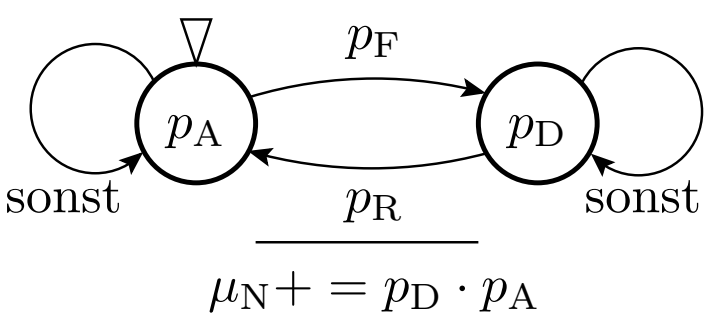


Graphische Darstellung logisch verketteter Ereignisse zur Abschätzung der Eintrittswahrscheinlichkeiten von Gefahren, Ausfällen, ...

Wenn Abhängigkeiten, aber nicht Ausschluss, Umstellung der ogischen Beziehungen in UND/ODER-Verknüpfungen unabhängiger oder sich ausschließender ereignisse und Inverierungen. Alternative bzw. Kontrolle auch hier Simulation als Zählexperiment.

3.49 Markov-Ketten (𝕃)





$$\begin{pmatrix} p_A \\ p_D \end{pmatrix}_{n+1} = \begin{pmatrix} 1-p_F & p_R \\ p_F & 1-p_R \end{pmatrix} \cdot \begin{pmatrix} p_A \\ p_D \end{pmatrix}_n \text{ mit } \begin{pmatrix} p_A \\ p_D \end{pmatrix}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\mu_N = \mu_N + p_D \cdot p_A$$

Berechnung von Zustandswahrscheinlichkeit für stochastische Prozesse, die sich durch endliche Automaten beschreiben lassen:

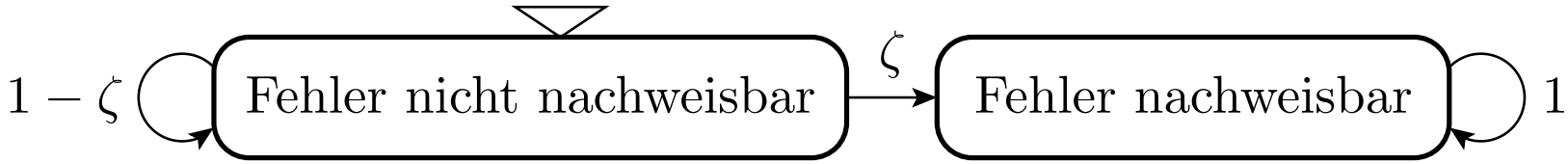
- Fehlernachweis,
- Fehlerentstehung,
- Verfügbarkeit, ...

Kantenzähler für die zu erwartende Anzahl der Übergänge.

Fehlernachweis

Nachweis & Zuverlässigkeit

3.50 Nachweiswahrscheinlichkeit



Ein Fehler verursacht mit einer Rate ζ Fehlfunktionen, an denen er erkannt wird. Mindesten ein Nachweis bei N Tests:

$$p_{\mathrm{FD}}\left(\zeta, N\right) = 1 - \left(1 - \zeta\right)^{N} = 1 - \mathrm{e}^{\ln(1-\zeta)\cdot N}$$

Für Zuverlässigkeitstests gilt praktisch immer$^{(1)}$ $\zeta_i \ll 1$. Fehlernachweiswahrscheinlichkeit:

$$p_{\mathrm{FD}}\left(\zeta, N\right) = 1 - \mathrm{e}^{-\zeta\cdot N} \tag{3.14}$$

Durchlasswahrscheinlichkeit je Fehler mit N Tests:

$$p_{\mathrm{FP}}\left(\zeta, N\right) = \mathrm{e}^{-\zeta\cdot N} \tag{3.15}$$

$p_{\mathrm{FD}}\left(\zeta, N\right)$ Probability of detecting of a fault with MF rate ζ and N tests.

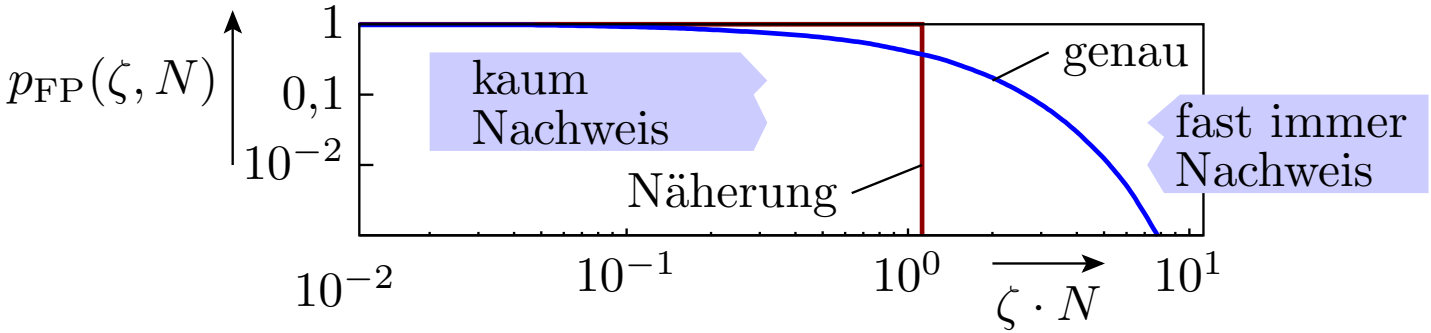
$p_{\mathrm{FP}}\left(\zeta, N\right)$ Probability of passage for faults with an MF rate ζ and N tests.

ζ Malfunction rate of the fault.

(1) Approximation by first member Taylor series: $\ln\left(1-x\right) = -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots\right)$.

3.51 Rückblick

Durchlasswahrscheinlichkeit je Fehler in Abhängigkeit von Fehlfunktionsrate des Fehlers und der Testanzahl:



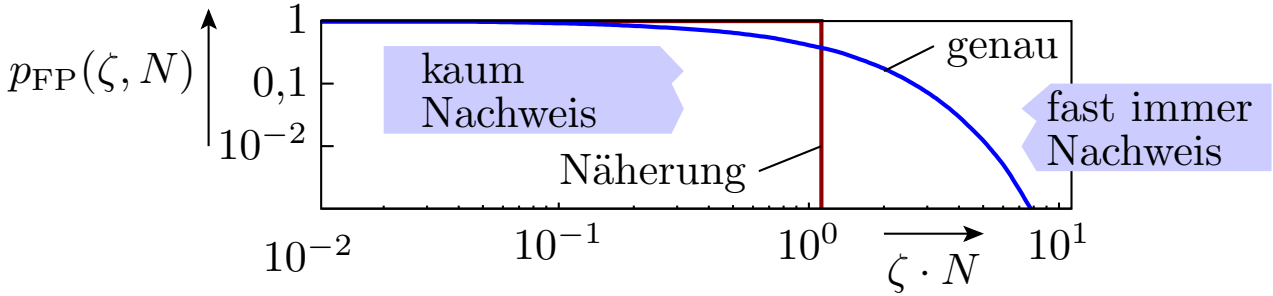
In Abschn. 2.3.2 hatten wir für die Fehlerdurchlasswahrscheinlichkeit p_{FT} eine Sprungfunktion angenommen:

(2.18)
$$p_{\mathrm{FP}}(\zeta, N) = \begin{cases} 1 & \zeta \leq \frac{1}{N} \\ 0 & \text{else} \end{cases}$$

Nachweis und Beseitigung aller Fehler $\zeta \cdot N \geq 1$ und sonst nicht. Für die typische Abnahme der Fehlerdurchlässigkeit

(2.19)
$$\mu_{\mathrm{FP}}\left(\frac{N}{N_0}\right) = \left(\frac{N}{N_0}\right)^{-K} \quad \text{with } 0 < K < 1$$

ergab sich daraus eine Dichte der Fehlfunktionsrate ...



... ergab sich daraus eine Dichte der Fehlfunktionsrate:

(2.21) $$h(\zeta) = N_0^K \cdot K \cdot \zeta^{K-1} \quad \text{for } 0 < \zeta \leq \frac{1}{N_0} \quad \text{else } 0$$

Mit der e-Funktion für die Durchlasswahrscheinlichkeit

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

ist nach den Vortests folgende Dichte zu erwarten:

$$h(\zeta) = \frac{1}{\int_0^1 \mathrm{e}^{-\zeta \cdot N_0} \cdot \zeta^{K-1} \cdot \mathrm{d}\zeta} \cdot \mathrm{e}^{-\zeta \cdot N_0} \cdot \zeta^{K-1}$$

Die nächsten Folien zeigen, dass die wesentlichen Zusammenhänge,

- Abnahme der Fehleranzahl mit Exponent $0 \leq K \leq 1$ und
- Abnahme der mittleren Fehlfunktionsrate je Fehler $\sim N^{-1}$

auch mit dieser Dichte der Fehlfunktionsrate gelten.

$p_{FP}(\zeta, N)$	Probability of passage for faults with an MF rate ζ and N tests.
$h(\zeta)$	Density function of the malfunction rate at the start of the reliability test.
K, N_0	Shape parameter. Number of preliminary tests for which detected faults are eliminated.

3.53 Gammafunktion

Substitution: $\zeta = \frac{z}{N_0}$, $\mathrm{d}\zeta = \frac{\mathrm{d}z}{N_0}$:

$$\int_0^1 \mathrm{e}^{-\zeta \cdot N_0} \cdot \zeta^{K-1} \cdot \mathrm{d}\zeta = \int_0^{N_0} \mathrm{e}^{-z} \cdot \left(\frac{z}{N_0}\right)^{K-1} \cdot \frac{\mathrm{d}z}{N_0} = N_0^{-K} \cdot \underbrace{\int_0^{N_0} \mathrm{e}^{-z} \cdot z^{K-1} \cdot \mathrm{d}z}_{*} = \frac{1}{K \cdot N_0^K}$$

$$h(\zeta) = K \cdot N_0^K \cdot \mathrm{e}^{-\zeta \cdot N_0} \cdot \zeta^{K-1} \tag{3.16}$$

Integral * für $N_0 \gg 1$ näherungsweise Gamma-Funktion:

$$\Gamma(K) = \int_0^{\infty} \mathrm{e}^{-z} \cdot z^{K-1} \cdot \mathrm{d}z \tag{3.17}$$

Für $0 < K < 1$ gilt:

$$\Gamma(K) \approx \frac{1}{K} \tag{3.18}$$

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

Für $K > 1$ gilt:

$$\Gamma(K+1) = K \cdot \Gamma(K) \tag{3.19}$$

$\Gamma(K)$) Gamma function of the shape parameter K.

3.54 Abnahme der Fehlerdurchlässigkeit

(3.20) $$h(\zeta, N) = K \cdot N^K \cdot \mathrm{e}^{-\zeta \cdot N} \cdot \zeta^{K-1}$$

Abnahme der Fehlerdurchlässigkeit durch $N - N_0$ zusätzliche Tests:

$$\begin{aligned}\mu_{\mathrm{FP}}\left(\tfrac{N}{N_0}\right) &= \int_0^1 p_{\mathrm{FP}}(\zeta, N - N_0) \cdot h(\zeta) \cdot \mathrm{d}\zeta \\ &= \int_0^1 \mathrm{e}^{-\zeta \cdot (N - N_0)} \cdot K \cdot N_0^K \cdot \mathrm{e}^{-\zeta \cdot N_0} \cdot \zeta^{K-1} \cdot \mathrm{d}\zeta \\ &= K \cdot N_0^K \cdot \int_0^1 \mathrm{e}^{-\zeta \cdot N} \cdot \zeta^{K-1} \cdot \mathrm{d}\zeta\end{aligned}$$

Substitution: $\zeta = \frac{z}{N}$, $\mathrm{d}\zeta = \frac{\mathrm{d}z}{N}$:

$$\mu_{\mathrm{FP}}\left(\tfrac{N}{N_0}\right) = K \cdot N_0^K \cdot \int_0^N \mathrm{e}^{-z} \cdot \left(\tfrac{z}{N}\right)^{K-1} \cdot \tfrac{\mathrm{d}z}{N} = K \cdot \left(\tfrac{N}{N_0}\right)^{-K} \cdot \underbrace{\int_0^N \mathrm{e}^{-z} \cdot z^{K-1} \cdot \mathrm{d}z}_{\Gamma(K) \approx \frac{1}{K}} \surd$$

Auch mit Fehlfunktionsdichte (eq. 3.16) gilt:

(2.19) $$\mu_{\mathrm{FP}}\left(\tfrac{N}{N_0}\right) = \left(\tfrac{N}{N_0}\right)^{-K} \quad \text{with } 0 < K < 1$$

$\mu_{\mathrm{FP}}\left(\frac{N}{N_0}\right)$ Expected fault permeability of a test extension N/N_0.

3.55 Mittlere Fehlfunktionsrate je Fehler

Eine Testverlängerung um $N - N_0$ zusätzliche zufällige Tests und Beseitigung alle damit nachweisbaren Fehler erhöht die Testanzahl, für die alle Fehler beseitigt sind, von N_0 auf N in (eq. 3.16):

$$h\left(\zeta, N\right) = K \cdot N^K \cdot \mathrm{e}^{-\zeta \cdot N} \cdot \zeta^{K-1} \tag{3.20}$$

Mittlere Fehlfunktionsrate je Fehler:

$$\bar{\zeta} = \int_0^1 h\left(\zeta, N\right) \cdot \zeta \cdot \mathrm{d}\zeta = \int_0^1 K \cdot N^K \cdot \mathrm{e}^{-\zeta \cdot N} \cdot \zeta^{K-1} \cdot \zeta \cdot \mathrm{d}\zeta$$

Substitution $\zeta = \frac{z}{N}$, $\mathrm{d}\zeta = \frac{\mathrm{d}z}{N}$:

$$\bar{\zeta} = K \cdot N^K \cdot \int_0^N \mathrm{e}^{-z} \cdot \left(\tfrac{z}{N}\right)^{K-1} \cdot \tfrac{z}{N} \cdot \tfrac{\mathrm{d}z}{N} = \tfrac{K}{N} \cdot \int_0^N \mathrm{e}^{-z} \cdot z^K \cdot \mathrm{d}z$$

$$\bar{\zeta} = \tfrac{K \cdot \Gamma(K+1)}{N^{K+1}} = \tfrac{K^2 \cdot \Gamma(K)}{N^{K+1}}$$

$$\bar{\zeta} = \tfrac{K}{N} \tag{3.21}$$

Um Faktor $K + 1$ größer als mit der Sprungfunktion als Durchlasswahrscheinlichkeit je Fehler.

3.56 Wesentliche Zusammenhänge unverändert

(2.19) $$\mu_{\mathrm{FP}}\left(\frac{N}{N_0}\right) = \left(\frac{N}{N_0}\right)^{-K} \quad \text{with } 0 < K < 1$$

(3.21) $$\bar{\zeta} = \frac{K}{N}$$

Abnahme der zu erwartenden Fehleranzahl proportional zur Fehlerdurchlässigkeit mit Exponent $0 \leq K \leq 1$:

(2.24) $$\mu_{\mathrm{F}}(N) = \mu_{\mathrm{F}}(N_0) \cdot \left(\frac{N}{N_0}\right)^{-K}$$

Abnahme der Fehlfunktionsrate durch Fehler mit Exponent $K + 1$:

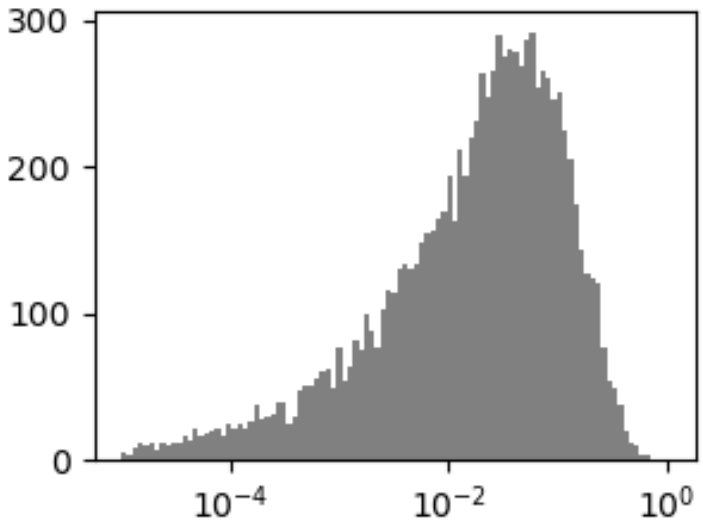
(2.25) $$\zeta_{\mathrm{F}}(N) = \frac{K \cdot \mu_{\mathrm{F}}(N)}{N}$$

(2.26) $$\zeta_{\mathrm{F}}(N) = \zeta_{\mathrm{F}}(N_0) \cdot \left(\frac{N}{N_0}\right)^{-(K+1)}$$

$\mu_{\mathrm{FP}}\left(\frac{N}{N_0}\right)$	Expected fault permeability of a test extension N/N_0.
K	Shape parameter of the distribution of the malfunction rate $(0 < K < 1)$.
N, N_0	Total number of tests. Number of tests for which all detected faults are eliminated.
$\mu_{\mathrm{F}}(N)$	Expected number of faults not detected and eliminated after N tests.
$\zeta_{\mathrm{F}}(N)$	Malfunction rate caused by faults depending on the number of tests.
$\bar{\zeta}$	Mean malfunction rate per fault.

3.57 Einer Stichprobe von Fehlfunktionsraten

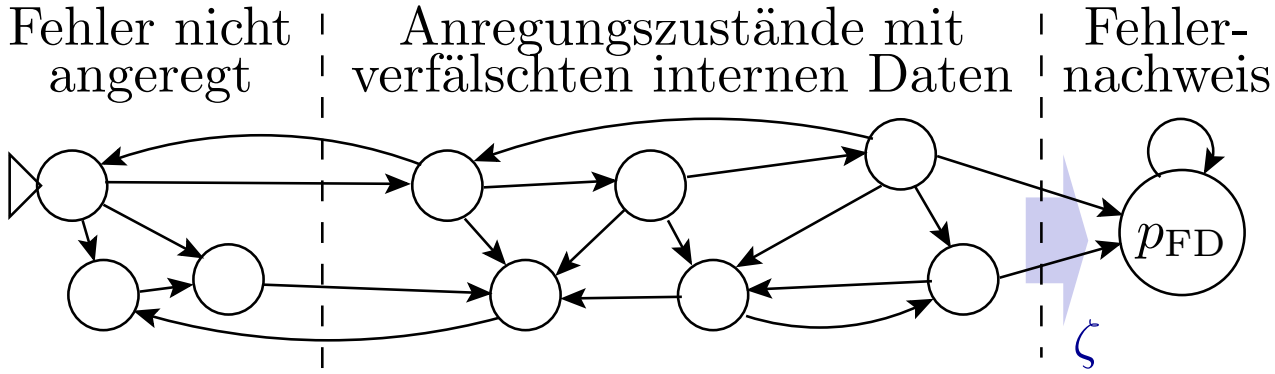
```
import numpy as np
import matplotlib.pyplot as plt

# Parameter definieren
shape = 0.5 # Formfaktor
scale = 0.1 # Skalenparameter
n = 10000   # Stichprobengröße

# Daten generieren
data = np.random.gamma(shape, scale, n)
print(data[:8])

# Visualisierung
bins=np.logspace(start=np.log10(0.00001),
    stop=np.log10(1), num=100)
plt.hist(data, bins=bins, color='grey')
plt.gca().set_xscale("log")
plt.show()
```



Beispielwerte:
0.11240502
0.00043902
0.04227980
0.08142087
0.10094599
0.32683308
0.21336941
0.00621701

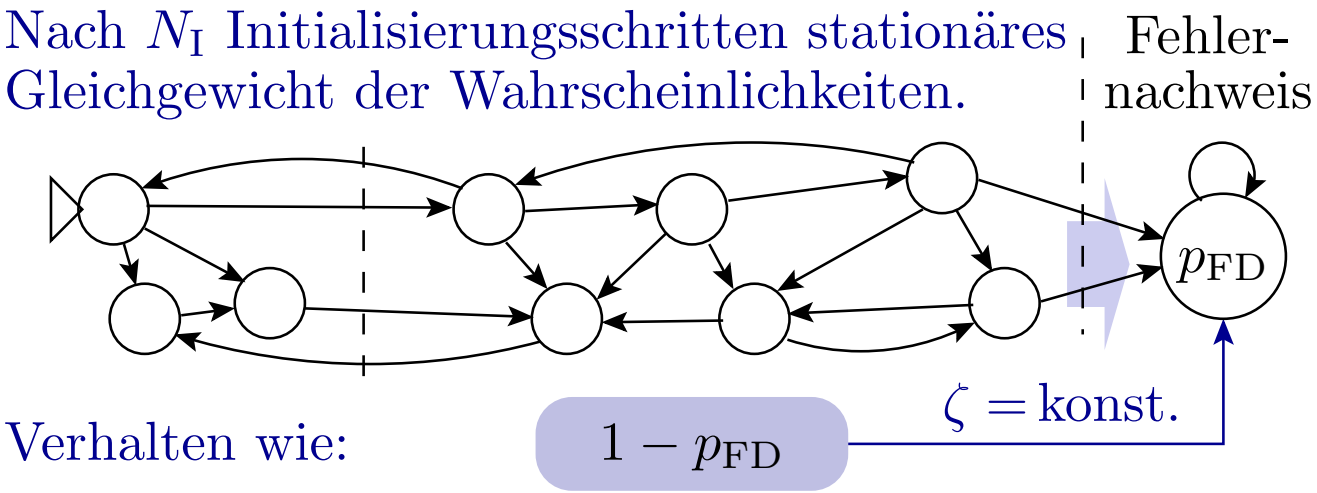
Service mit Gedächtnis

3.58 Service mit Gedächtnis



In Systemen mit internen Speicherzuständen (Gedächtnis) verlangt der Fehlernachweise zum Teil mehrere Zustandsübergänge über Anregungszustände mit verfälschten internen Daten bis zum Nachweis.

Eine genaue Modellierung des Zusammenhangs zwischen Nachweiswahrscheinlichkeit und Testanzahl verlangt für jeden Fehler einen individuellen Beobachterautomaten, aus dem sich eine fehlerspezifische Markov-Kette ableitet. Oft mehr als zwei Zustände, testschrittabhängige Fehlfunktionsrate ζ.



An einem Beispielfehler wird gezeigt, dass solche Beobachterautomaten dazu tendieren, sich für lange Testsätze nahzu wie der Zweizustands-Beobachterautomat mit der abklingenden Exponentialfunktion als Nachweiswahrscheinlichkeit zu verhalten.

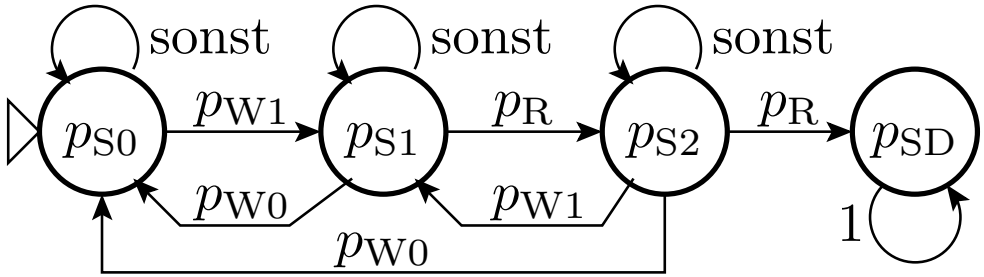
Und zwar stellt sich **nach N_I Initialisierungsschritten** ein stationäres Gleichgewicht zwischen den Zustandswahrscheinlichkeiten der linken Zustände und darüber eine **konstante Fehlfunktionsrate** ζ für den »Abfluss von Wahrscheinlichkeit« in den Zustand »Fehlernachweis« ein.

3.60 Beispiel: RAM-DR1-Fehler

Zustände:

S0: Wert 0 oder unbekannt
S1: Wert 1 geschrieben
S2: 1 zerstörend gelesen
SD: Fehler nachgewiesen

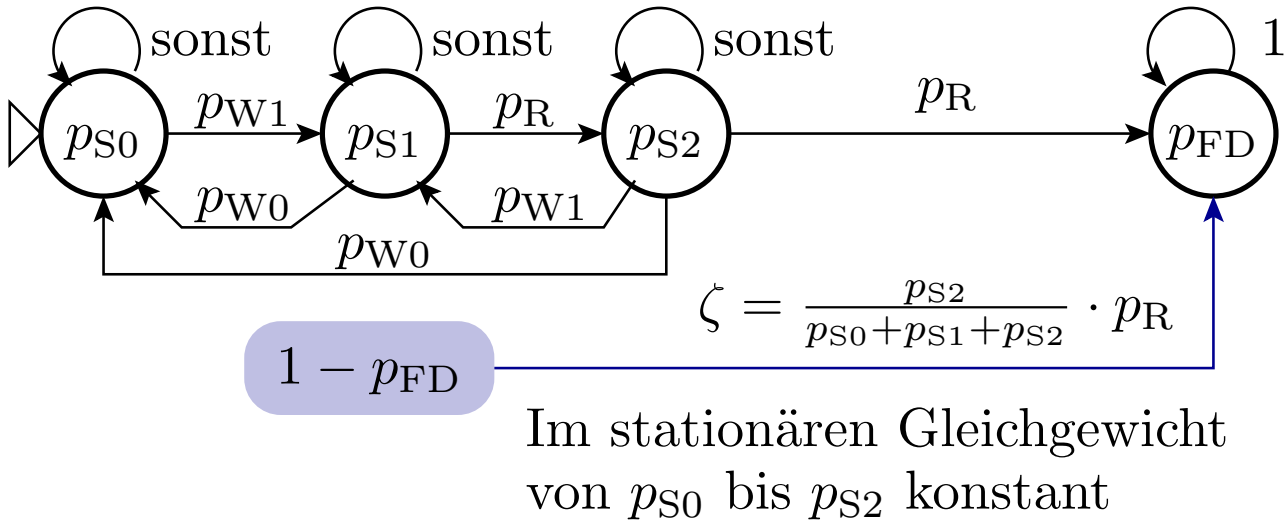
Nachweisfolge: Schreibe 1 → Lesen → Lesen



Fehler bewirkt, dass beim Lesen der fehlerhaften Speicherzelle eine gespeicherte 1 in eine 0 verfälscht wird. Der Nachweis erfordert:

- Schreibe 1 auf Adresse a (Übergang in Zustand S1),
- Lese Wert von Adresse a (Übergang in Anregungszustand S2),
- Lese Wert von Adresse a ohne zwischenzeitlichen Schreibzugriff auf a (Übergang in den Nachweiszustand SD).

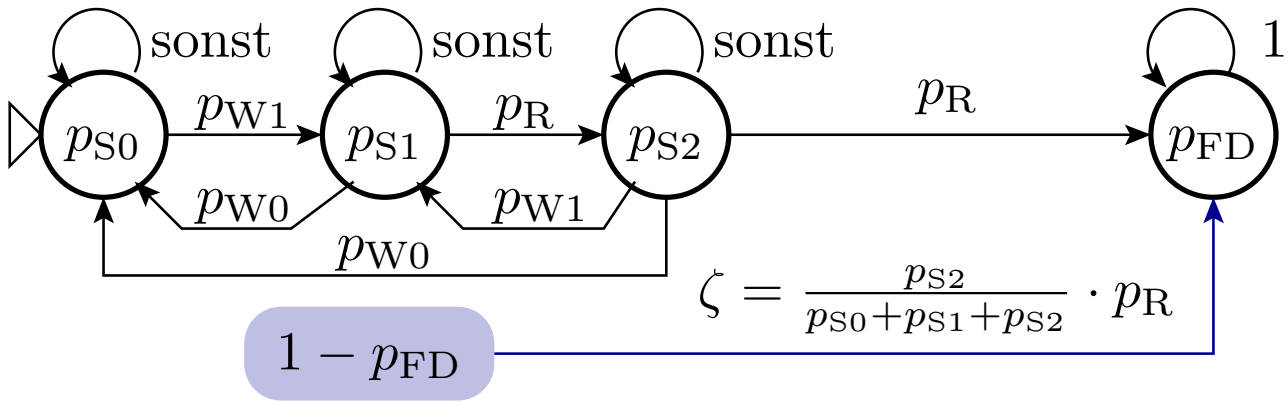
p_{W0}	Probability that a 0 is written into the memory cell.
p_{W1}	Probability that a 1 is written into the memory cell.
p_R	Probability that the memory cell is read.
p_{FD}	Probability of fault detection.
DR1	Destructive reading of one.



Die äquivalente Fehlfunktionsrate für die Zweizustands-Markov-Kette ist hier die bedingte Wahrscheinlichkeit, dass der Beobachterautomat im Zustand S2 ist, wenn er nicht im Zustand FD, also in einem der Zustande S1, S2 oder S3 ist, und die defekte Speicherzelle gelesen wird.

Es folgt eine Beispielrechnung mit:

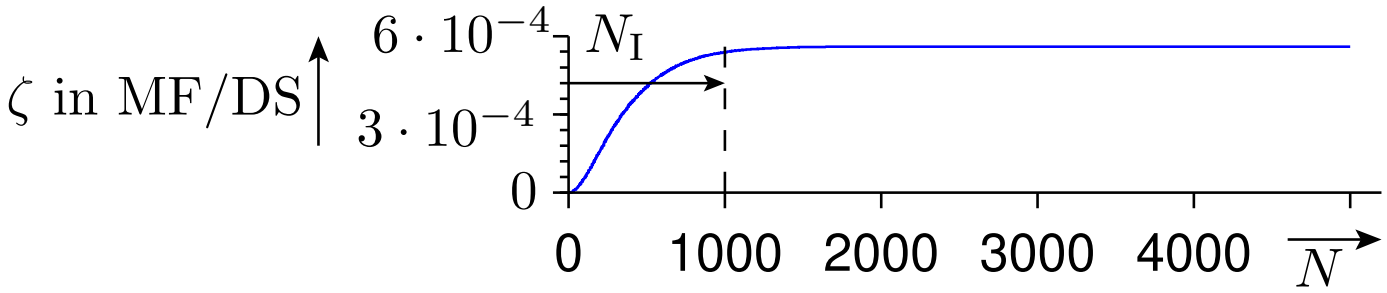
- RAM: 128×1 Speichplätze. Zugriffswahrscheinlichkeit auf eine bestimmte Zelle: 1/128.
- Lesewahrscheinlichkeit der Zelle: $p_R = \frac{50\%}{128}$
- Schreibwahrscheinlichkeit eins und null: $p_{W1} = p_{W0} = \frac{25\%}{128}$




```
pS0=1; pS1=0; pS2=0; pSD(1)=0; N=5000;
NA=128; pR = 1/(2*NA); pW0 = pW1 = 1/(4*NA);
for n=1:N
  p0   = pS0 * (1-pW1) + pS1*pW0          + pS2*pW0;
  p1   = pS0 *    pW1  + pS1*(1-pW0-pR)  + pS2*pW1;
  p2   = pS1 *    pR   + pS2*(1-pW1+pW0-pR);
  pFD   = pSD(n) + pS2 * pR;
  zeta  = pS2*pR / (pS0+pS1+pS2); % MF rate
  pS0 = p0; pS1 = p1; pS2 = p2;
end
plot(1:N, zeta);
```

p_{Si}	Probability that the Markov chain is in state S_i.
p_R	Probability that the memory cell is read.
ζ	Malfunction rate by the DR1 fault.
N	Number of tests.

3.63 Simulation



Die durch den Fehler verursachte MF-Rate ζ nimmt anfangs mit der Testanzahl N zu und bleibt ab $N_\mathrm{I} \approx 1000$ konstant $\zeta \approx 5{,}7 \cdot 10^{-4}$. Ab $N > N_\mathrm{I}$ beträgt die Nachweiswahrscheinlichkeit mindestens:

$$p_\mathrm{FD}\left(\zeta, N\right) \geq 1 - \mathrm{e}^{-\zeta \cdot (N - N_\mathrm{I})} \tag{3.22}$$

und für lange Zufallstests $N \gg N_\mathrm{I}$ gilt wie für Systeme ohne Gedächtnis:

(3.14) $$p_\mathrm{FD}\left(\zeta, N\right) = 1 - \mathrm{e}^{-\zeta \cdot N}$$

$p_\mathrm{FD}\left(N\right)$	Detection probability of the DR1 fault as a function of the number of tests.
ζ	Malfunction rate by the DR1 fault.
N_I	Number of initialisation steps.
N	Number of tests, for worst-case estimates without the N_I initialisation steps.

Fehler und Modellfehler

3.64 Fehler und Modellfehler (sec.2.1.3)

Bekannt sind nur gefundene Fehler, nicht die zu suchenden.

Testauswahl und Testbewertung verwenden für Hardware-Fertigungsfehler Modellfehler und für Software Abdeckungskriterien.

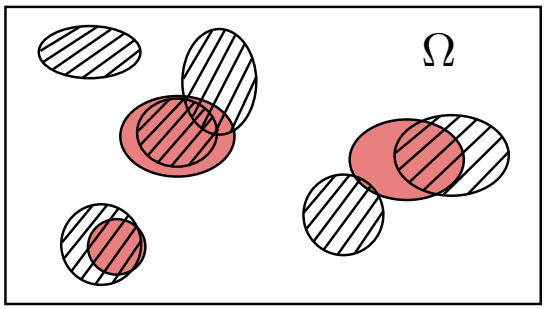
Modellfehler: Fehlerannahmen, in der Regel eine kleine Änderung (Mutation) der Testobjektbeschreibung, z.B. Haftfehler »Gateranschluss ständig null oder ständig eins«.

Abdeckungskriterien: Nur Kontrolle Erreichbarkeit Fehlerort und optional Infektionsbedingung.

Fehlermodell: Algorithmus zur Erzeugung einer Modellfehlermenge aus einer Testobjektbeschreibung. Abdeckungsmodell analog.

> *Wie und wie gut kann von einer als Zahlenwert bestimmten Modellfehler- bzw. Kriterienabdeckung auf die tatsächliche Fehlerabdeckung geschlussfolgert werden?*

3.65 Nachweismengen, Nachweisbeziehungen



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

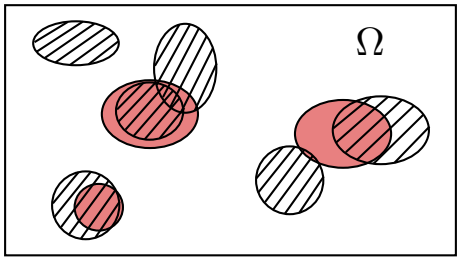
Nachweismenge eines Modellfehlers

Nachweismenge eines tatsächlichen Fehlers

Die Nachweisbeziehungen zwischen Fehlern und Modellfehlern lassen sich über die Mengenbeziehungen veranschaulichen:

- Der Ereignisraum Ω umfasst alle Möglichkeiten der Eingaben bzw. der Eingabefolgen.
- Günstig sind die, die einen betrachteten Fehler bzw. Modellfehler nachweisen.
- Idealerweise generiert ein Fehlermodell für alle tatsächlichen Fehler mehrere Modellfehler mit ähnlichen Anregungs- und Beobachtungsbedingungen.
- Gemeinsame Nachweisbedingungen bilden sich auf mehr oder weniger große Schnittmengen der Nachweismengen ab.

3.66 Zufallstest



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

Nachweismenge eines Modellfehlers

Nachweismenge eines tatsächlichen Fehlers

Die Modellfehler teilen sich mit den zu erwartenden tatsächlichen Fehlern Eingabemengen für den Nachweis. Ähnliche Verteilung der Größe der Nachweismengen und der Fehlfunktionsraten, wobei die Nachweismengen der Modellfehler in Abhängigkeit vom Fehlermodell im Mittel um einen Faktor C größer oder kleiner sind als die der Modellfehler. Die zu erwartende Fehlerabdeckung (und -durchlässigkeit) ist abschätzungsweise die für Modellfehler der C-fachen Testanzahl (slide 2.95):

(2.41) $$\mu_{\mathrm{FC}}(N) = \mu_{\mathrm{FCM}}(N_{\mathrm{T}}) \quad \text{for } N = C \cdot N_{\mathrm{T}}$$

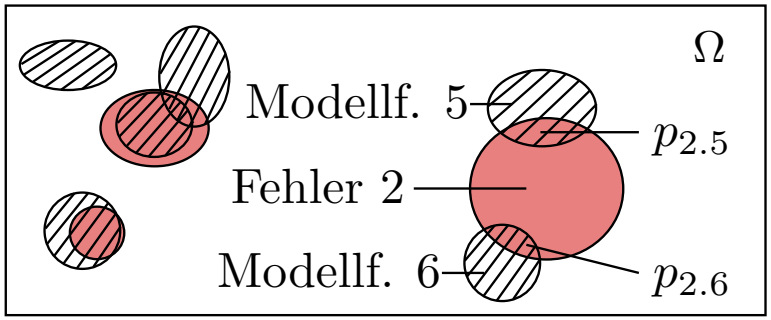
(2.42) $$\mu_{\mathrm{FP}}(N) = \mu_{\mathrm{FPM}}(N_{\mathrm{T}}) \quad \text{for } N = C \cdot N_{\mathrm{T}}$$

$\mu_{\mathrm{FC}}, \mu_{\mathrm{FCM}}$ Expected fault coverage for actual fault or modelled faults.

$\mu_{\mathrm{FP}}, \mu_{\mathrm{FTM}}$ Expected fault permeability, for actual fault or modelled faults.

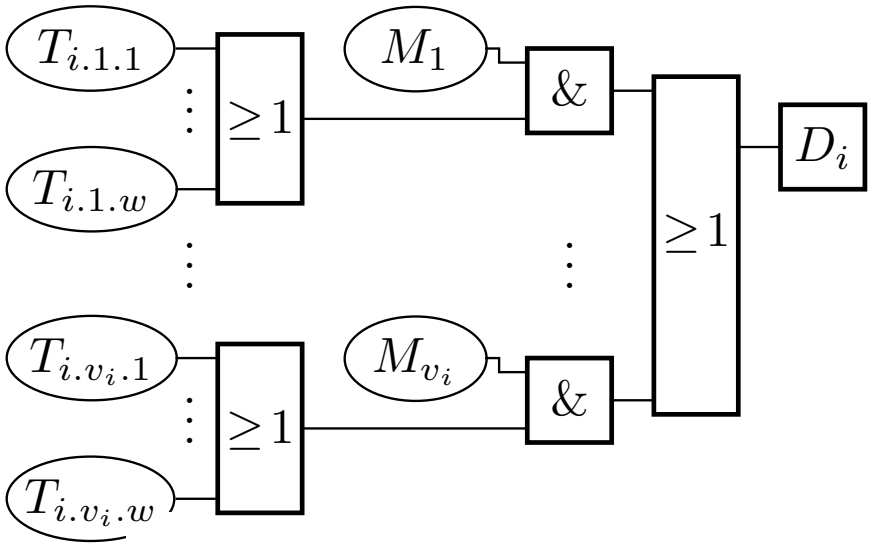
N_{T}, C Number of tests carried out to determine coverage. Test scaling.

3.67 Gezielte Testsuche



Nachweismenge eines tatsächlichen Fehlers

Nachweismenge eines Modellfehlers

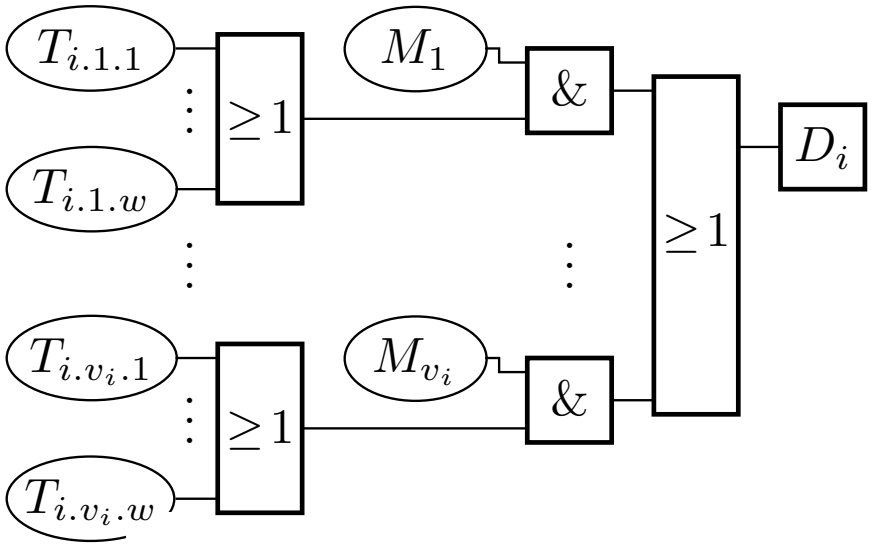


M_j für Modellfehler j werden w Tests gefunden
$\mathbb{P}[M_j] = FC_{\mathrm{M}} \neq f(i,j)$

T_{ijk} wenn für Modellfehler j w Tests gefunden werden, weist Test k Fehler i nach
$\mathbb{P}[T_{i.j.k}] = p_{ij} \neq f(k)$

D_i Nachweis Fehler i

Für jeden Fehler i enthält die Modellfehlermenge $j = 1$ bis v_i ähnlich nachweisbare Modellfehler, für die jeweils $w \geq 1$ Tests gesucht und mit Wahrscheinlichkeit $\mathbb{P}[M] = FC_{\mathrm{M}}$ gefunden werden.



M_j für Modellfehler j werden w Tests gefunden
$\mathbf{P}\left[M_j\right] = FC_{\mathrm{M}} \neq f(i,j)$

T_{ijk} wenn für Modellfehler j w Tests gefunden werden, weist Test k Fehler i nach
$\mathbf{P}\left[T_{i.j.k}\right] = p_{ij} \neq f(k)$

D_i Nachweis Fehler i

Testsuche ist nur für FC_{M} Modellfehler erfolgreich (sec.6.2). Wenn sich ein Test finden lässt, werden auch $w \geq 1$ zufällige Tests aus der Nachweismenge gefunden (in der Regel zutreffende Vereinfachung):

$$D_i = \bigvee_{j=1}^{v_i} \left(\left(\bigvee_{k=1}^{w} T_{ijk} \right) \wedge M_j \right) = \overline{\bigwedge_{j=1}^{v_i} \left(\left(\overline{\bigwedge_{k=1}^{w} \bar{T}_{ijk}} \right) \wedge M_j \right)}$$

w	Number of randomly selected test inputs per model fault detection set.
v_i	Number of similarly detectable model faults per fault i.
FC_{M}	Fault Coverage for model faults.
p_{ij}	Probability that a test for model fault j detects fault i.

3.69 Nachweiswahrscheinlichkeit

$$D_i = \overline{\bigwedge_{j=1}^{v_i} \overline{\left(\left(\overline{\bigwedge_{k=1}^{w} \bar{T}_{ijk}}\right) \wedge M_j\right)}}$$

$$p_i = \mathbb{P}(D_i) = 1 - \prod_{j=1}^{v_i} \left(1 - \left(FC_{\mathrm{M}} \cdot \left(1 - (1 - p_{ij})^w\right)\right)\right) \tag{3.23}$$

Beispielwerte: $p_{\mathrm{ij}} = 25\%$, $v_i = 5$ und $w = 1 \ldots 5$:

$p_i\,(w,\, FC_{\mathrm{M}})$	$w = 1$	$w = 2$	$w = 3$	$w = 4$	$w = 5$
$FC_{\mathrm{M}} = 90\%$	72,0%	91,8%	97,5%	99,15%	99,70%
$FC_{\mathrm{M}} = 95\%$	74,2%	93,2%	98,1%	99,47%	99,84%

Wesentliche Kenngröße zur Charakterisierung der Nachweiswahrsch. p_i für FC_{M} nahe 1 ist offenbar nicht die FC_{M}, sondern die Anzahl der Tests w, die je Modellfehler (bei SW Abeckungskriterium) gesucht werden.

D_i, p_i	Detection event of fault i. Detection probability of fault i.
w	number of verificationsper model fault or, in the case of software, per coverage criterion.
v_i	Number of similarly detectable model faults per fault i.
FC_{M}	Fault Coverage for model faults.
p_{ij}	Probability that a test for model fault j detects fault i.

3.70 Modellrechnung für Fehlerabdeckung eins

$$p_i = 1 - \prod_{j=1}^{v_i} (1 - (1 \cdot (1 - (1 - p_{ij})^w))) = 1 - \prod_{j=1}^{v_i} (1 - p_{ij})^w$$

$$p_i = 1 - \prod_{j=1}^{v_i} (1 - p_{ij})^w = 1 - \mathrm{e}^{\mathrm{w} \cdot \sum_{\mathrm{j}=1}^{\mathrm{v_i}} \ln(1-\mathrm{p_{ij}})}$$

$$p_i = 1 - \mathrm{e}^{-w \cdot \zeta_{\mathrm{C}.i}} \quad \text{with} \quad \zeta_{\mathrm{C}.i} = \sum_{j=1}^{v_i} \ln(1 - p_{ij})$$

Nachweiswahrscheinlichkeit, wie bei Zufallstest (eq. 3.14), nur

- das ζ_C die bedingte Fehlfunktionsrate ist, wenn die gewählten Eingaben ähnlich nachweisbare Kriterin abdecken und
- als Tests nur solche zählen, die ähnlich nachweisbare Kriterien abdecken.

$\zeta_{\mathrm{C}.i}$ Malfunction rate per test due to fault i when tests are searched for modelled faults.

Die individuellen ζ_C können wie beim Zufallstest um Zehnerpotenzen auseinander liegen. Wir orientieren uns an der Dichtefunktion für den Zufallstest

(3.20) $$h\left(\zeta, N\right) = K \cdot N^K \cdot \mathrm{e}^{-\zeta \cdot N} \cdot \zeta^{K-1}$$

und passen nur den Formfaktor K und den Skalenparameter N an:

$$h_\mathrm{C}\left(\zeta_\mathrm{C}, w\right) = K_\mathrm{C} \cdot w^{K_\mathrm{C}} \cdot \mathrm{e}^{\zeta_\mathrm{C} \cdot w} \cdot \zeta_\mathrm{C}^{K_\mathrm{C}-1} \quad \text{with} \quad 0 < K_\mathrm{C} < 1$$

mit $0 < \zeta_\mathrm{C} \leq 1$. **Offenbar dieselben Funktion mit anderen Parametern**. Analog zu

(2.24) $$\mu_\mathrm{F}\left(N\right) = \mu_\mathrm{F}\left(N_0\right) \cdot \left(\frac{N}{N_0}\right)^{-K}$$

nimmt die Fehleranzahl bei Erhöhung der Abdeckungsanzahl auch nach einer Potenzfunktion auch mit einem Exponenten $0 < K_\mathrm{C} < 1$ ab, der aber von K abweichen kann:

$$\mu_\mathrm{F}\left(w\right) = \mu_\mathrm{F}\left(w_0\right) \cdot \left(\frac{w}{w_0}\right)^{-K_\mathrm{C}} \quad \text{with} \quad 0 < K_\mathrm{C} < 1$$

$\zeta_{\mathrm{C}.i}$	Malfunction rate per test due to fault i when tests are searched for modelled faults.
K_C	Shape parameter of the distribution of the malfunction rate ζ_C for targeted tests.
$h\left(\zeta_\mathrm{K}\right)$	Distribution of the malfunction rate ζ_C for targeted tests.
w, w_0	Distribution of the malfunction rate ζ_C for targeted tests.
$\mu_\mathrm{FT}\left(w/w_0\right)$	Expected fault permeability of a cover increase w/w_0.

3.72 Verbesserung gegenüber W1-Test

Für Software gilt nach aktuellen Regularien W1-Tests als ausreichend (Anweisungs-, Zweig- oder Bedingungsabdeckung mit $w = 1$, vergl. Folie 2.37). Verringerung der Fehleranzahl durch Erhöhung der Abdeckungsanzahl von $w_0 = 1$ auf $w > 1$:

$$\mu_{\mathrm{F}}(w) = \mu_{\mathrm{F}}(1) \cdot w^{-K_{\mathrm{C}}} \tag{3.24}$$

Unter der plausibel Annahme, dass die Anzahl der gefundenen abdeckungsverbessernden Tests proportional mit der geforderten zunimmen:

$$w \sim N$$

Abnahme der Fehlfunktionsrate durch Fehler und unter Vernachlässigung der Fehlfunktionen durch Störungen, Zunahme der Zuverlässigkeit mit Exponent $K_{\mathrm{C}} + 1$:

$$\zeta(w) = \zeta(1) \cdot w^{-(K_{\mathrm{C}}+1)} \tag{3.25}$$

$$R(w) = R(1) \cdot w^{K_{\mathrm{C}}+1} \tag{3.26}$$

$\mu_{\mathrm{FT}}(w)$	Expected fault permeability at an increase in the coverage ratio from $w = 1$ to $w > 1$.
w	number of verificationsper model fault or, in the case of software, per coverage criterion.
K_{C}	Shape parameter of the distribution of the malfunction rate ζ_{C} for targeted tests.
$R(w)$	Reliability depending on the number of coverings w.

3.73 Erforderliche Abdeckungsanzahl

Erforderlich Abdeckungsanzahl für eine zulässige Fehlerdurchlässigkeit bzw. gewünschte Zuverlässigkeitsverbesserung:

$$w \geq \left(\frac{\mu_{\mathrm{FT}}(1)}{\mu_{\mathrm{FT}}} \right)^{\frac{1}{K_{\mathrm{C}}}} \tag{3.27}$$

$$w \geq \left(\frac{R}{R(1)} \right)^{\frac{1}{K_{\mathrm{C}}+1}} \tag{3.28}$$

Beispielabschätzungen für die erforderliche Kriterienabdeckung für eine gewünschte Durchlässigkeit von 10% bis 0,5% bei einer W1-Durchlässigkeit $\mu_{\mathrm{FT}}(1) = 40\%$ bzw. $\mu_{\mathrm{FT}}(1) = 10\%$ sowie $K_{\mathrm{C}} = 0{,}5$:

$K_{\mathrm{C}} = 0{,}5$	$\mu_{\mathrm{FT}} = 10\%$	$= 5\%$	$= 1\%$	$= 0{,}5\%$
$\mu_{\mathrm{FT}}(1) = 40\%$	$w = 16$	$w = 64$	$w = 256$	$w = 1024$
$\mu_{\mathrm{FT}}(1) = 10\%$	$w = 1$	$w = 4$	$w = 16$	$w = 64$

μ_{FT}	Expected or permitted fault permeability.
w	number of verificationsper model fault or, in the case of software, per coverage criterion.
$\mu_{\mathrm{FT}}(1)$	Fault permeability for coverage number $w = 1$.
K_{C}	Shape parameter of the distribution of the malfunction rate ζ_{C} for targeted tests.
R, $R(1)$	Erforderliche Zuverlässigkeit. Mit W1-Tests erzielte Zuverlässigkeit.

Zusammenfassung

3.74 Zufallstests (𝕃)

Nachweiswahrscheinlichkeit und Durchlasswahrscheinlichkeit je Fehler für kleine Fehlfunktionsraten:

(3.14) $$p_{\mathrm{FD}}(\zeta, N) = 1 - \mathrm{e}^{-\zeta \cdot N}$$

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

- für Fehler mit hoher Fehlfunktionsrate ist p_{FP} obere Schranke,
- für Systeme mit Gedächtnis brauchbare Näherung.

Zu erwartende Fehlerdurchlässigkeit: (𝕎)

- Zunahme mit Exponent $0 < K < 1$ mit der Testanzahl:

  (2.19) $$\mu_{\mathrm{FP}}\left(\frac{N}{N_0}\right) = \left(\frac{N}{N_0}\right)^{-K} \quad \text{with } 0 < K < 1$$

- gleich der Modellfehler bzw. Kriterien der C-fachen Testanzahl:

  (2.41) $$\mu_{\mathrm{FC}}(N) = \mu_{\mathrm{FCM}}(N_{\mathrm{T}}) \quad \text{for } N = C \cdot N_{\mathrm{T}}$$

  - Erreichbarkeitskriterien Software $C \gg 1$.
  - Modellfehler ähnlich großen Nachweismengen[1] $C \approx 1$ und
  - für strenge (praxisuntaugliche Fehlermodelle) $C \ll 1$.

(1) z.B. Fertigungs- und Haftfehler.

3.75 Fehlerorientierte Suche (𝕃)

Suchschema: Finde für alle abzudeckten Modellfehler bzw. Abdeckungskriterien w Tests. Die tatsächlich Fehlerabdeckung hängt dabei weniger von der Modellfehler- bzw. Kriterianabdeckung, als von der Anzahl der je Kriterium gefundenen Tests ab.

Abdeckung aller nicht redundanten Modellfehler/Kriterien ($FC_{\mathrm{M}} = 1$):

(3.24) $$\mu_{\mathrm{F}}(w) = \mu_{\mathrm{F}}(1) \cdot w^{-K_{\mathrm{C}}}$$

(3.26) $$R(w) = R(1) \cdot w^{K_{\mathrm{C}}+1}$$

Erforderlich Abdeckungsanzahl für zulässige Fehlerdurchlässigkeit:

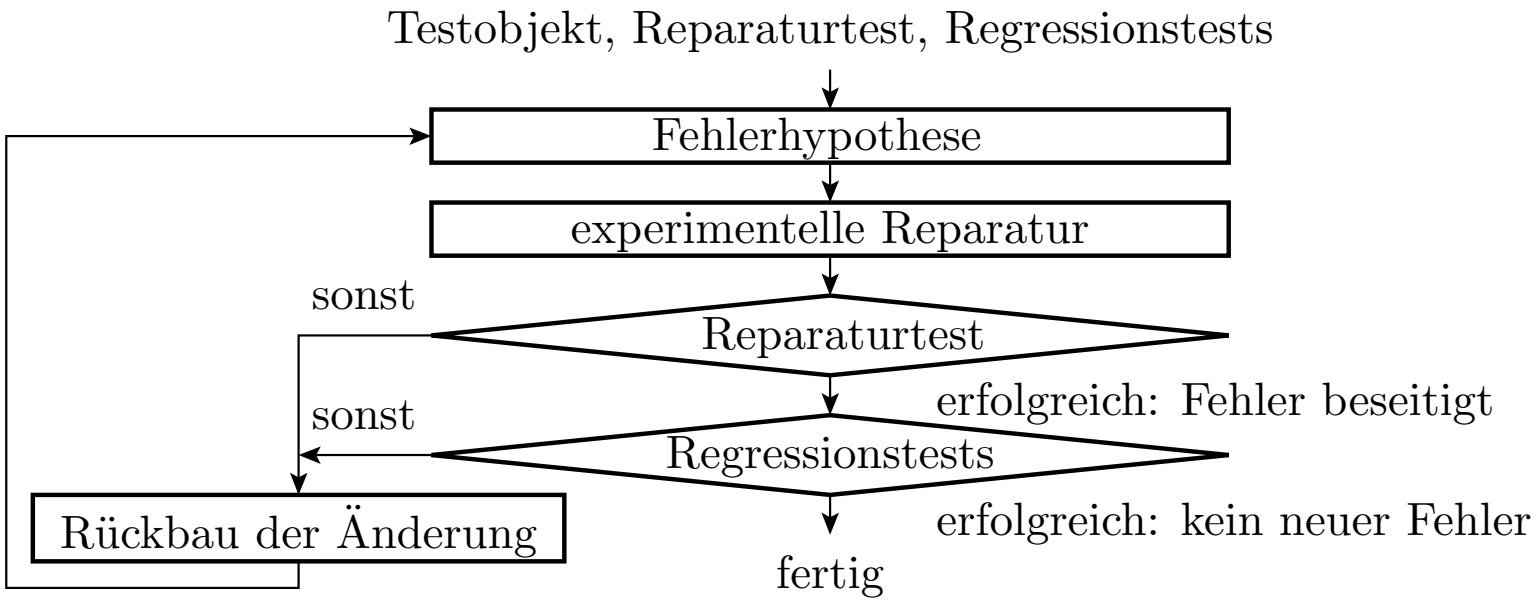
(3.27) $$w \geq \left(\frac{\mu_{\mathrm{FT}}(1)}{\mu_{\mathrm{FT}}}\right)^{\frac{1}{K_{\mathrm{C}}}}$$

(3.28) $$w \geq \left(\frac{R}{R(1)}\right)^{\frac{1}{K_{\mathrm{C}}+1}}$$

Geringere Fehlerdurchlässigkeit und höhere Zuverlässigkeit verlangt ein Vervielfachung der Testanzahl. Das dürfen auch smarte Zufallstests, die sich Kriterienabdeckungen teilen, sein, wobei das Testgütemass dann die Abdeckungsanzahl w je Kriterium ist.

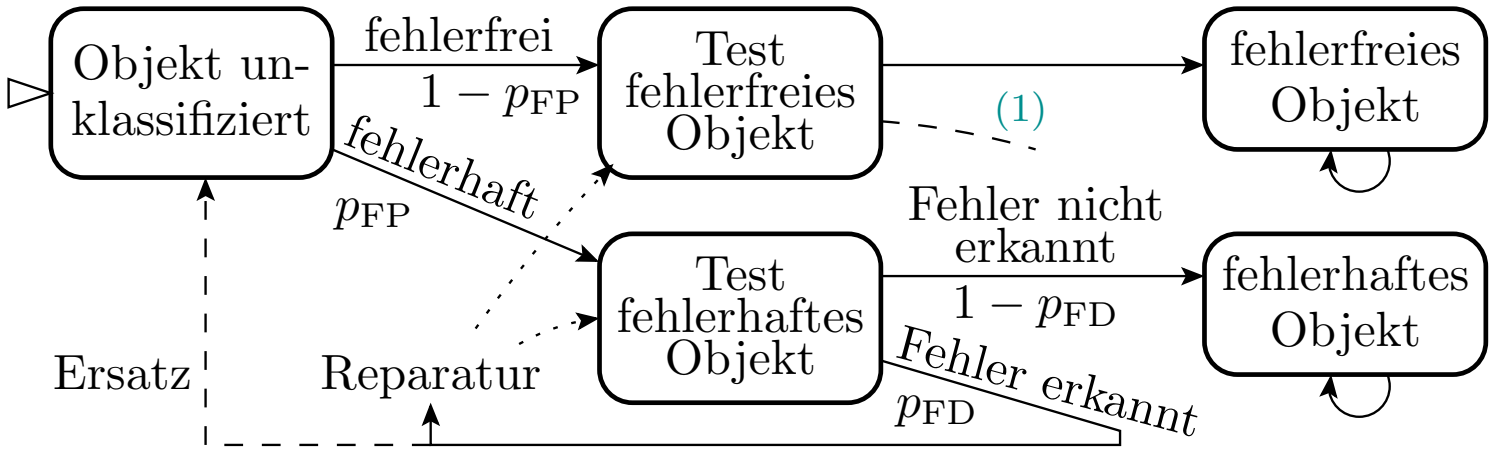
Fehlerbeseitigung

3.76 Experimentelle Reparatur nach Absch. 2.2.1



- Iteration aus Beseitigungsversuchen für hypothetische Fehler und Erfolgskontrolle durch Testwiederholung.
- Beseitigt alle vom Test nachweisbaren Fehler.
- Zur Vermeidung neu entstehender Fehler bei der Reparatur, Rückbau nach erfolglosen Reparaturversuchen.
- Regessionstest zum Nachweis neuer nicht beseitigter Fehler.

3.77 Beseitigung eines Fehlers als Markov-Kette



Fehlerbeseitigung als durch einen Automaten beschreibaren Ablauf, der sich in eine Markov-Kette überführen lässt. Ein Fehler i

- ist mit einer Wahrscheinlichkeit p_{FP} vorhanden und
- wird mit einer Wahrscheinlichkeit p_{FD} erkannt.

Für die Fehlerbeseitigung sind zwei Ansätze zu unterscheiden:

- Ersatz Gesamtsystem,
- Reparatur z.B. durch Ersatz fehlerhafter Teilsysteme.

p_{FP} Probability that fault is present.
p_{FD} Probability of fault detection.
(1) Zusatzkante für Phantomfehler zur Vereinfachung vernachlässigt.

3.78 Ersatz oder Reparatur

Beim Ersatz erkannter defekter Systeme vor dem Einsatz aus demselben Fertigungsprozess

- haben Orginal- und Ersatzteile dieselbe Ausbeute Y und
- muss das Originalteil im Mittel μ_{Repl} mal ersetzt werden:

$$\mu_{\mathrm{Repl}} = \frac{1}{Y} - 1 \tag{3.29}$$

- Fertigungskosten pro verkauftes System $\approx \frac{1}{Y}$ mal so hoch wie die Kosten für die Fertigung eines einzelnen Systems.

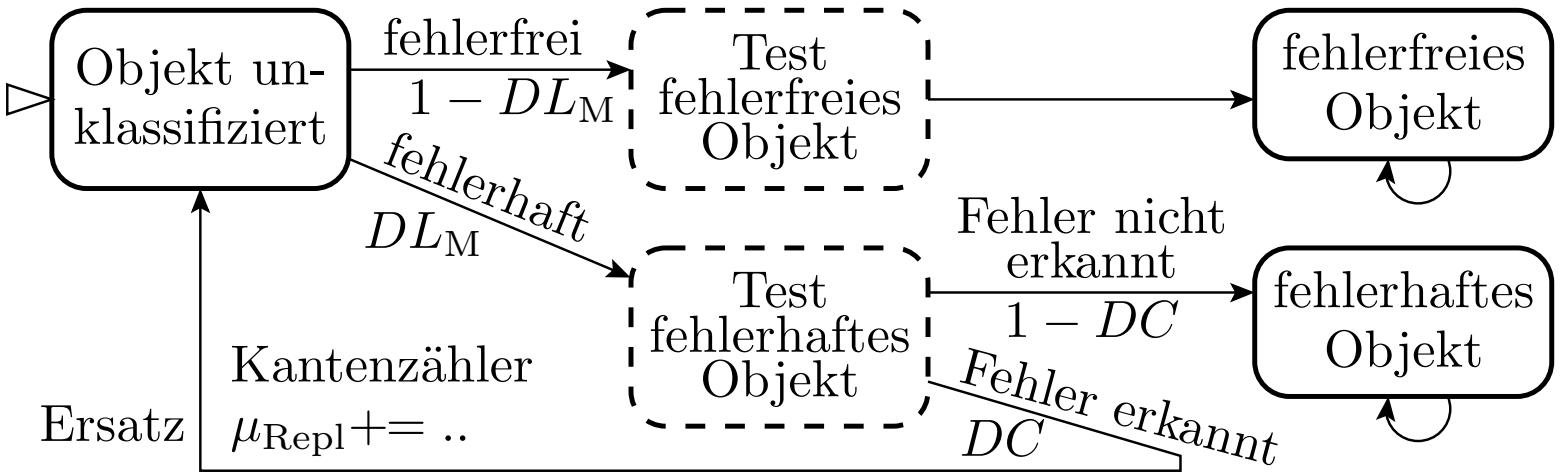
Reparatur: Tausch kleinerer Bausteine, die mit geringerem Risiko defekt sind. Dafür Zusatzaufwand für Lokalisierung, Reparatur, Ersatzteile, ...

Ersatz ist kostengünstigster bei hoher und Reparatur bei geringer Ausbeute.

μ_{Repl}	Expected number of replacements.
Y	Yield.

Ersatz

3.79 Fehlerbeseitigung durch Ersatz



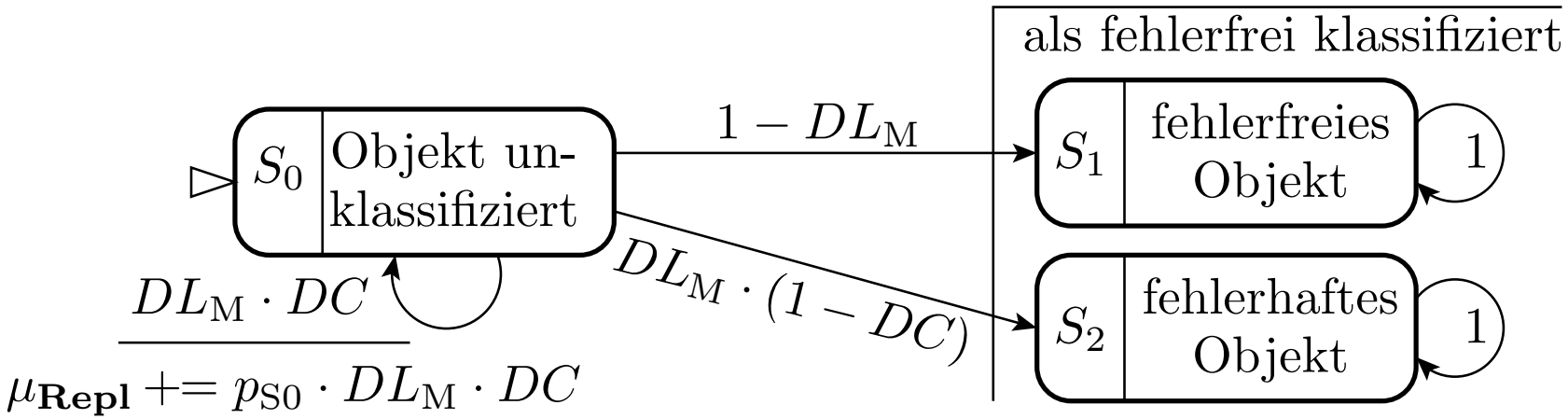
Original- und Ersatzobjekte sind mit Wahrscheinlichkeit DL_{M} defekt.

Je Schritt wird aus unklassifizierten Objekten mit Wahrscheinlichkeit

- $1 - DL_{\mathrm{M}}$ ein fehlerfreies Objekt oder
- $DL_{\mathrm{M}} \cdot (1 - DC)$ ein nicht erkanntes defektes Objekt,
- sonst wird es ersetzt und ist damit wieder unklassifiziert.

DL_{M}	Defect level after manufacturing before discarding detected defective parts.
DC	Defect coverage, percentage of detectable defective devices.
μ_{Repl}	Edge counter for the expected number of replacements.

3.80 Vereinfachte Markov-Kette



Nach Ersatz aller erkennbar defekten Objekte:

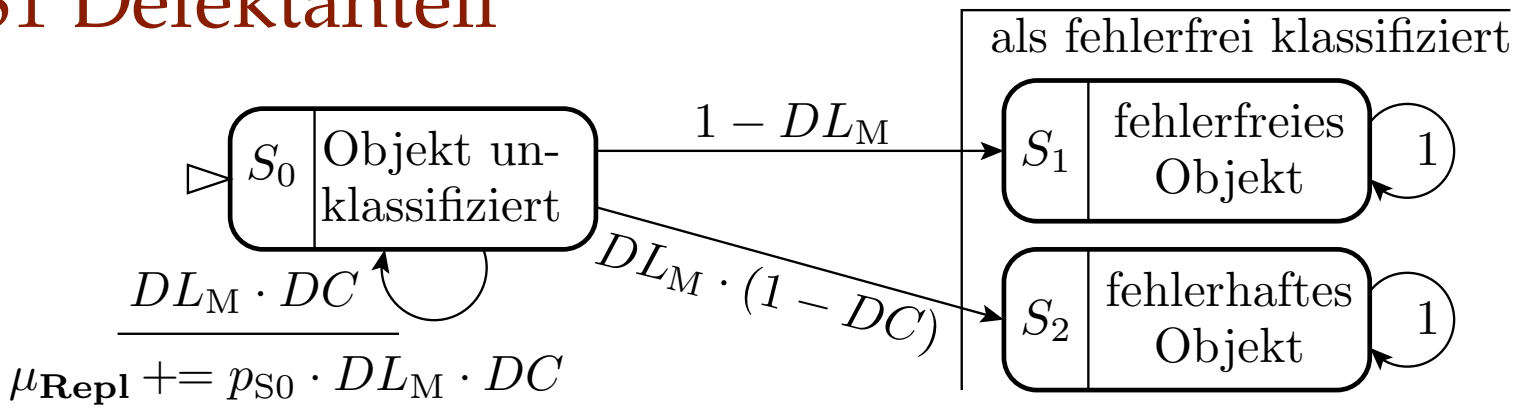
$$\lim_{\#Repl \to \infty} (p_{\mathrm{S0}}) = \lim_{\#Repl \to \infty} (DL_{\mathrm{M}} \cdot DC)^{\#Repl} = 0$$

$$\lim_{\#Repl \to \infty} (p_{\mathrm{S1}}) = (1 - DL_{\mathrm{M}}) \cdot \sum_{\#Repl=0}^{\infty} (DL_{\mathrm{M}} \cdot DC)^{\#Repl} \overset{(\mathrm{SGS})}{=} \frac{1-DL_{\mathrm{M}}}{1-DL_{\mathrm{M}} \cdot DC}$$

$$\lim_{\#Repl \to \infty} (p_{\mathrm{S2}}) = DL = 1 - \lim_{\#Repl \to \infty} (p_{\mathrm{S1}}) = \frac{DL_{\mathrm{M}} \cdot (1-DC)}{1-DL_{\mathrm{M}} \cdot DC}$$

DC	Defect coverage, percentage of detectable defective devices.
DL_{M}	Defect level after manufacturing before discarding detected defective parts.
$\#Repl$	Number of replacements.
SGS	Summation formula of the geometric series: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

3.81 Defektanteil



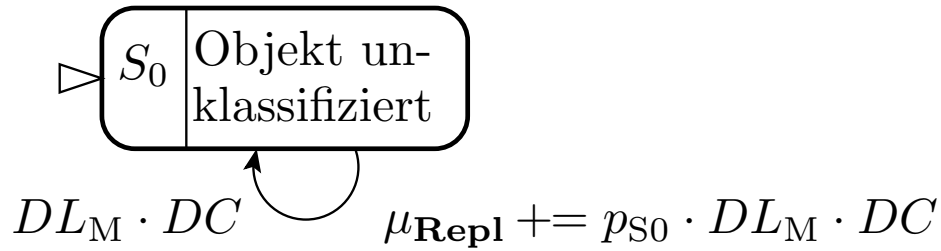
Der Defektanteil nach Aussortieren als Wahrscheinlichkeit, dass ein als fehlerfrei ausgewiesenes Objekt fehlerhaft ist $\lim_{\#Repl \to \infty} (p_{\mathrm{S2}})$ wurde in Abschn. 2.1.5 durch Subtraktion der Anzahl der erkannten defekten Produkte von der Anzahl der defekten und aller Produkte in Zähler und Nenner hergeleitet:

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

Vorherige Abschätzung hier mit Markov-Kette bestätigt.

DC	Defect coverage, percentage of detectable defective devices.
DL_{M}	Defect level after manufacturing before discarding detected defective parts.
DL	Defect level after sorting out or replacing detected defective parts.

3.82 Zu erwartende Anzahl der Ersetzungen



$$\mu_{\mathrm{Repl}} = DL \cdot DC \cdot \sum_{n=0}^{\infty} \underbrace{(DL \cdot DC)^n}_{p_{\mathrm{S0}}()} = \frac{DL_{\mathrm{M}} \cdot DC}{1 - DL_{\mathrm{M}} \cdot DC} \tag{3.30}$$

(n– Nummer der Ersetzung). Zur Kontrolle, es muss gelten:

(3.29) $$\mu_{\mathrm{Repl}} = \frac{1}{Y} - 1$$

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

$$Y = \frac{1}{\mu_{\mathrm{Repl}} + 1} = \frac{1}{\frac{DL_{\mathrm{M}} \cdot DC}{1 - DL_{\mathrm{M}} \cdot DC} + 1} = 1 - DL \cdot DC \surd$$

Auch hier vorherige Abschätzung aus Abschn. 2.1.5 bestätigt.

Example 3.5: Ausbeute und Defektanteil nach Ersatz

Schaltkreisausbeuten Y: 10%, 30%, 50%, 80% und 90%, Defektabdeckung DC: 90%, 99%, 99,5% und 99,9%.

a) *Wie groß ist der Defektanteil DL_{M} der Schaltkreise nach der Fertigung vor dem Aussortieren?*

b) *Wie groß ist der Defektanteil DL nach Aussortieren (Ersatz) der als defekt erkannten Schaltkreise in Abhängigkeit von der Ausbeute und der Defektabdeckung?*

Y	Yield.
DC	Defect coverage, percentage of detectable defective devices.
μ_{Repl}	Expected number of replacements.
DL_{M}	Defect level after manufacturing before discarding detected defective parts.
DL	Defect level after sorting out or replacing detected defective parts.

Schaltkreisausbeuten Y: 10%, 30%, 50%, 80% und 90%, Defektabdeckung DC: 90%, 99%, 99,5% und 99,9%.

a) *Wie groß ist der Defektanteil DL_{M} der Schaltkreise nach der Fertigung vor dem Aussortieren?*

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

Umstellung nach dem Defektanteil DL_{M} vor dem Aussortieren der als derfekt erkannten Schaltkreise:

$DL_{\mathrm{M}} = \frac{1-Y}{DC}$ ↘	$Y = 10\%$	...=30%	...=50%	...=80%	...=90%
$DC = 90{,}0\%$	100,0%	77,8%	55,6%	22,2%	11,1%
$DC = 99{,}0\%$	90,9%	70,7%	50,50%	20,2%	10,1%
$DC = 99{,}9\%$	90,1%	70,1%	50,1%	20,0%	10,0%

100% Für $Y = 1 - DC$ sind alle gefertigten Schaltkreise defekt.

Schaltkreisausbeuten Y: 10%, 30%, 50%, 80% und 90%, Defektabdeckung DC: 90%, 99%, 99,5% und 99,9%.

b) *Wie groß ist der Defektanteil DL nach Aussortieren (Ersatz) der als defekt erkannten Schaltkreise in Abhängigkeit von der Ausbeute und der Defektabdeckung?*

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

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

$DL \searrow$	$DC = 90\%$	$DC = 99\%$	$DC = 99,5\%$	$DC = 99,9\%$
$Y = 10\%$	100%	9,09%	4,52%	9.009 dpm
$Y = 30\%$	25,9%	2,36%	1,17%	2.336 dpm
$Y = 50\%$	11,1%	1,01%	5.025 dpm	1.001 dpm
$Y = 80\%$	2,78%	2.525 dpm	1.256 dpm	250 dpm
$Y = 90\%$	1,23%	1.122 dpm	558 dpm	111 dpm

Haben Schaltkreistests wirklich so hohe Defektabdeckung oder ist die ausgewiesenen der Defektanteil getesteter Schaltkreise nur die Anteil der reklamierten Schaltkreise? ... siehe (slide 2.41).

dpm Defecs per million, number of defective products per one million.

Reparatur

3.84 Fehlerbeseitigung durch Reparatur

Bei Reparatur werden nur die als defekt diagnostizierten Teile getauscht oder modifiziert. Zu ersetzende Teilsysteme:

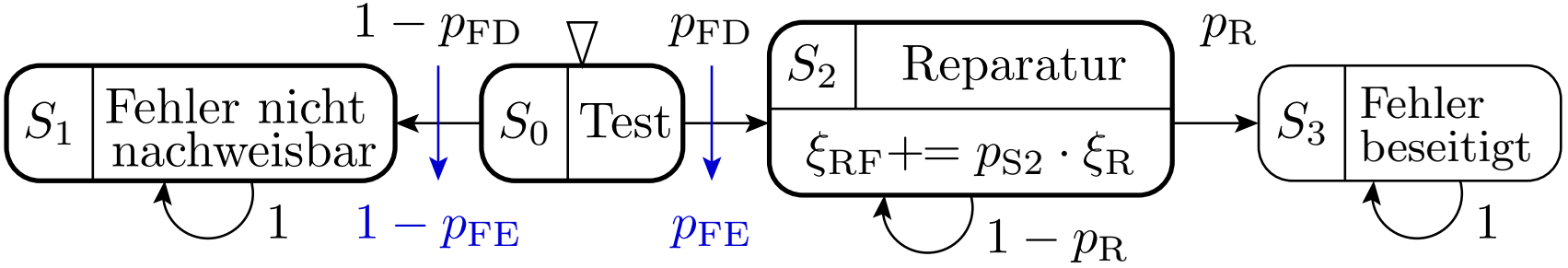
- sind billiger als zu ersetzende Gesamtsysteme und
- haben einen kleineren Defektanteil (weniger Mehrfachersetzungen durch defekte Ersatzteile).

Dafür verlangt Reparatur Zusatzaufwändungen:

- Vorhaltung von Organisationseinheiten + Personalkapazität für Wartung und Reparatur.
- Reparaturgerechter Entwurf (modulare Austauschbarkeit),
- aufwändigere Fehlerlokalisierung und mehr Reparaturversuche durch Fehldiagnose.

Bei hoher Ausbeute $Y \gg 50\%$ unrentabel.

3.85 Markov-Kette für einen vorhandenen Fehler



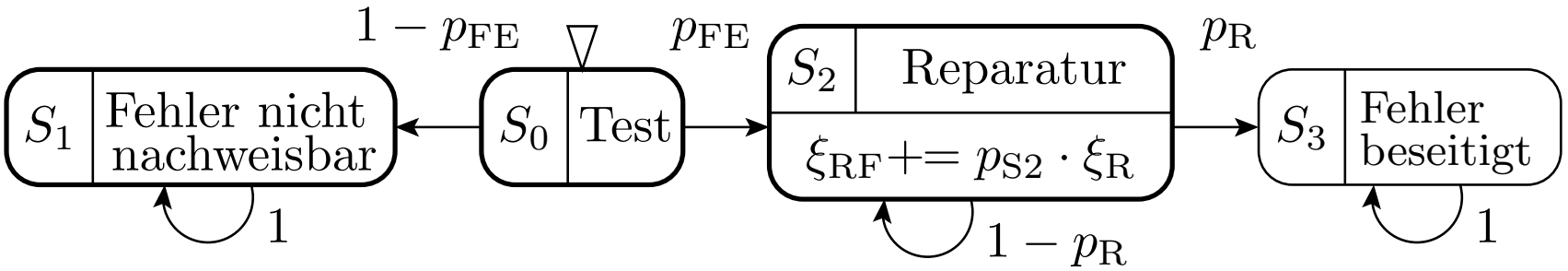
Jeder erkannte Fehler wird beseitigt:

$$p_{\mathrm{FE}} = p_{\mathrm{S3}} = p_{\mathrm{FD}} \cdot p_{\mathrm{R}} + p_{\mathrm{FD}} \cdot (1 - p_{\mathrm{R}}) \cdot p_{\mathrm{R}} + p_{\mathrm{FD}} \cdot (1 - p_{\mathrm{R}})^2 \cdot p_{\mathrm{R}} + \ldots$$

$$p_{\mathrm{FE}} = p_{\mathrm{FD}} \cdot p_{\mathrm{R}} \cdot \sum_{n=0}^{\infty} (1 - p_{\mathrm{R}})^n \overset{(\mathrm{SGS})}{=} p_{\mathrm{FD}}$$

Bei der Beseitigung können jedoch neue Fehler entstehen ...

p_{FD}	Probability of fault detection.
p_{FE}	Probability of fault detection and elimination.
p_{R}	Probability of repair success.
$p_{\mathrm{S}i}$	Probability that the Markov chain is in state S_i.
ξ_{RF}	Fault emergence rate in new faults per existing fault.
ξ_{R}	Fault emergence rate in new faults per repair attempt.
SGS	Summation formula of the geometric series: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.



Im Zustand S_2 werden die Wahrscheinlichkeiten für die Entstehung neuer Fehler für alle Reparaturversuche eines zu beseitigenden Fehlers aufsummiert:

$$\xi_{\mathrm{RF}} = p_{\mathrm{FE}} \cdot \sum_{n=0}^{\infty} \xi_{\mathrm{R}} \cdot (1 - p_{\mathrm{R}})^n \overset{(\mathrm{SGS})}{=} p_{\mathrm{FE}} \cdot \frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}} \tag{3.31}$$

Die Entstehungsrate je beseitigter Fehler ist um den Kehrwert der Beseitigungswahrscheinlichkeit größer:

$$\xi_{\mathrm{RE}} = \frac{\xi_{\mathrm{RF}}}{p_{\mathrm{FE}}} = \frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}} < 1 \tag{3.32}$$

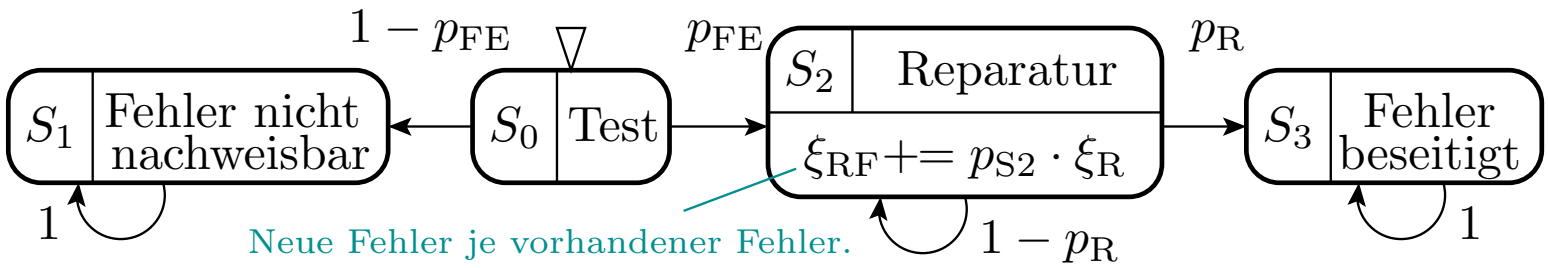
ξ_{RF}	Fault emergence rate in new faults per existing fault.
p_{FE}	Probability of fault detection and elimination.
p_{R}	Probability of repair success.
ξ_{R}	Fault emergence rate in new faults per repair attempt.
ξ_{RE}	Fault emergence rate in new faults per eliminated fault.
SGS	Summation formula of the geometric series: $\sum_{n=0}^{\infty} a_0 \cdot q^n = \frac{a_0}{1-q}$.

3.87 Mehrere zu beseitigende Fehler

$\mu_F = \mu_{CF}$

μ_F Zu erwartende Anzahl der zu beseitigenden Fehler.
μ_{CF} Zu erwartende Fehleranzahl aus Entstehungsprozessen.

Wiederhole für alle Fehler aus Entstehungs- und Reparaturprozessen



$\mu_F += \xi_{RF}$ // Plus neue Fehler.

- Je zu beseitigender Fehler eine Markov-Kette.
- Jeder erkennbare Fehler wird beseitigt.

Beim Beseitigung eines Fehler entstehen im Mittel ξ_{RE} neue Fehler, bei deren Beseitigung wieder im Mittel ξ_{RE} neue Fehler entstehen, ...

$$\xi_{RER} = \xi_{RE} \cdot (1 + \xi_{RE} \cdot (1 + \ldots)) = \sum_{i=1}^{\infty} (\xi_{RE})^i \overset{(SGS)}{=} \frac{1}{1-\xi_{RE}} - 1$$

ξ_{RE} Fault emergence rate in new faults per eliminated fault.
ξ_{RER} Fault emergence rate in new faults per original fault eliminated.

$$\xi_{\mathrm{RER}} = \frac{1}{1-\xi_{\mathrm{RE}}} - 1 = \frac{\xi_{\mathrm{RE}}}{1-\xi_{\mathrm{RE}}} \tag{3.33}$$

Neuentstehungsrate je vorhandener ursprünglicher Fehler:

$$\xi_{\mathrm{RFR}} = p_{\mathrm{FE}} \cdot \xi_{\mathrm{RER}} = p_{\mathrm{FE}} \cdot \left(\frac{\xi_{\mathrm{RE}}}{1-\xi_{\mathrm{RE}}} \right) \text{ for } \xi_{\mathrm{RE}} < 1 \tag{3.34}$$

Ersatz der Entstehungsrate je vorhandener Fehler in (eq. 3.34) durch:

(3.32) $$\xi_{\mathrm{RE}} = \frac{\xi_{\mathrm{RF}}}{p_{\mathrm{FE}}} = \frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}} < 1$$

$$\xi_{\mathrm{RFR}} = p_{\mathrm{FE}} \cdot \left(\frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}-\xi_{\mathrm{R}}} \right) \text{ for } p_{\mathrm{R}} > \xi_{\mathrm{R}} \tag{3.35}$$

ξ_{RE}	Fault emergence rate in new faults per eliminated fault.
ξ_{RER}	Fault emergence rate in new faults per original fault eliminated.
ξ_{RFR}	Fault emergence rate in new faults per existing original fault.
$p_{\mathrm{R}}, \xi_{\mathrm{R}}$	Probability of repair success. Fault emergence rate per repair attempt.
p_{FE}	Probability of fault elimination.
Pronounce:	ξ: xi, η: eta, μ: my.

Zu erwartende Anzahl aller zu beseitigender Fehler:

$$\mu_{\mathrm{FCR}} = \mu_{\mathrm{CF}} \cdot (1 + \xi_{\mathrm{RFR}}) \tag{3.36}$$

Zu erwartende Anzahl der nicht beseitigten Fehler:

$$\mu_{\mathrm{F}} = \mu_{\mathrm{CF}} \cdot (1 + \xi_{\mathrm{RFR}}) \cdot (1 - p_{\mathrm{FE}}) \tag{3.37}$$

$$\mu_{\mathrm{F}} = \mu_{\mathrm{CF}} \cdot \left(1 + p_{\mathrm{FE}} \cdot \left(\frac{\xi_{\mathrm{RE}}}{1-\xi_{\mathrm{RE}}}\right)\right) \cdot (1 - p_{\mathrm{FE}}) \text{ for } \xi_{\mathrm{RE}} < 1 \tag{3.38}$$

Wir brauchen die komplizierte Formel, um zu zeigen, dass es bei Reparaurprozessen so ewas wie Kipppunkte gibt:

- gute Prozesse, die die Fehleranzahl praktisch auf den Anteil der nicht nachweisbaren Fehler reduzieren,
- Prozess, die Fehler nur versteckt, statt sie zu beseitigt und
- Prozesse, die zu keinem Abschluss kommen.

μ_{FCR}	Total expected number of faults from creation and repair processes.
μ_{CF}	Expected number of faults from the creation processes.
ξ_{RFR}	Fault emergence rate in new faults per existing original fault.
μ_{F}	Expected number of faults after testing and elimination of all detectable faults.
p_{FE}	Probability of fault elimination.
ξ_{RE}	Fault emergence rate in new faults per eliminated fault.
Pronounce:	ξ: xi, η: eta, μ: my.

3.90 Fallunterscheidung nach η_{RE} in (eq. 3.38)

(3.38) $$\mu_{\mathrm{F}} = \mu_{\mathrm{CF}} \cdot \left(1 + p_{\mathrm{FE}} \cdot \left(\frac{\xi_{\mathrm{RE}}}{1-\xi_{\mathrm{RE}}}\right)\right) \cdot (1 - p_{\mathrm{FE}}) \text{ for } \xi_{\mathrm{RE}} < 1$$

- Wenig neu entstehende Fehler: ($\xi_{\mathrm{RE}} \ll 1$):

  $$\mu_{\mathrm{F}} \approx \mu_{\mathrm{CF}} \cdot (1 - p_{\mathrm{FE}}) \cdot (1 + p_{\mathrm{FE}} \cdot \eta_{\mathrm{RE}})$$

  Die Fehleranzahl μ_{F} nach der Beseitigungsiteration erhöht sich nur prozentual um $p_{\mathrm{FE}} \cdot \eta_{\mathrm{RE}}$.
- Beseitigung aller erkennbaren Fehler, ohne dass sich die zu erwartende Fehleranzahl verringert:

  $$(1 - p_{\mathrm{FE}}) \cdot \left(1 + p_{\mathrm{FE}} \cdot \frac{\xi_{\mathrm{RE}}}{1-\xi_{\mathrm{RE}}}\right) = 1 \Rightarrow \xi_{\mathrm{RE}} = \frac{1}{2-p_{\mathrm{FE}}}$$

Kontrolle:

$$p_{\mathrm{FE}} = p;\ (1-p) \cdot \left(1 - p \cdot \frac{\frac{1}{2-p}}{\frac{2-p-1}{2-p}}\right) = (1-p) \cdot \left(1 - \frac{p}{2-p-1}\right) = (1-p) \cdot \frac{1-p-p}{1-p} = 1$$

ξ_{RE}	Fault emergence rate in new faults per eliminated fault.
μ_{F}	Expected number of faults after testing and elimination of all detectable faults.
p_{FE}	Probability of fault detection and elimination.
Pronounce:	ξ: xi, η: eta, μ: my.

- Erhöhung der zu erwartenden Fehleranzahl bei Beseitigung aller erkennbaren Fehler: $\frac{1}{2-p_{\mathrm{FE}}} < \xi_{\mathrm{RE}} < 1$
- Erkennbar mehr neu entstehende als beseitigte Fehler ($\xi_{\mathrm{RE}} \geq 1$). Das Reparaturziel, die Beseitigung aller erkennbaren Fehler, ist nicht erreichbar.

Einen vernünftiger Reparaturprozess sollte

- alle erkennbaren Fehler beseitigen,
- eine hohe Fehlernachweis- und Beseitigungswahrscheinlichkeit p_{FE} und
- eine geringe Fehlerentstehungsrate $\xi_{\mathrm{RE}} < 0{,}1$ in neue je beseitigter Fehler

anstreben.

ξ_{RE} Fault emergence rate in new faults per eliminated fault.
p_{FE} Probability of fault detection and elimination.

3.92 Gute studentische Programmierleistung

- Fehlerarme Programmierung, z.B. $\mu_{\mathrm{CF}} = 5$ (ohne Syntaxfehler).
- Gründlicher Test, z.B. $p_{\mathrm{FE}} = 50\%$ mit $N = 10$ Tests.
- Brauchbare Fehlerbeseitigung: etwa 2,5 Reparaturversuche je Fehler ($p_{\mathrm{R}} = 40\%$), ein neuer Fehler je 10 Reparaturversuche ($\xi_{\mathrm{R}} = 0{,}1$).
- Formfaktor der Verteilung der MF-Rate $K = 0{,}4$.

Gl. 3.35:	ξ_{RFR}	$= \frac{p_{\mathrm{FE}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}} - \xi_{\mathrm{R}}}$	$= \frac{0{,}5 \cdot 0{,}1}{0{,}4 - 0{,}1}$	$= 0{,}167$
Gl. 3.37:	μ_{F}	$= \mu_{\mathrm{CF}} \cdot (1 - p_{\mathrm{FE}}) \cdot (1 + \xi_{\mathrm{RFR}})$	$= 5 \cdot (1 - 50\%) \cdot 1{,}167$	$= 2{,}92$
Gl. 2.25:	ζ_{F}	$\overset{(\leq 1)}{=} \frac{K \cdot \mu_{\mathrm{F}}(N)}{N}$	$= \frac{0{,}4 \cdot 2{,}92}{10}$	$= 0{,}11$

- Im Mittel 2,5 ursprüngliche plus 0,42 bei der Reparatur entstehende nicht erkennbare Fehler.
- Ein weiteres zufälliges Testbeispiel wird mit einer Wahrscheinlichkeit von $1 - \zeta = 89\%$ korrekt abgearbeitet.

Gut genug für die Abnahme bei einem Programmierkurs.

3.93 Schlechte Programmierleistung

- Mehr Entwurfsfehler: $\mu_{\mathrm{CF}} = 7$ Fehler (ohne Syntaxfehler).
- Weniger Tests: $p_{\mathrm{FE}} = 30\%$ mit $N = 5$ Tests.
- Etwa 4 Reparaturversuche je Fehler ($p_{\mathrm{R}} = 25\%$), ein neuer Fehler je 5 Reparaturversuche $\xi_{\mathrm{R}} = 0{,}2$.
- Formfaktor der Verteilung der MF-Rate $K = 0{,}4$:

Gl. 3.35:	ξ_{RFR}	$= \frac{p_{\mathrm{FE}} \cdot \xi_{\mathrm{R}}}{p_{\mathrm{R}} - \xi_{\mathrm{R}}}$	$= \frac{0{,}3 \cdot 0{,}2}{0{,}25 - 0{,}2}$	$= 1{,}2$
Gl. 3.37:	μ_{F}	$= \mu_{\mathrm{CF}} \cdot (1 - p_{\mathrm{FE}}) \cdot (1 + \xi_{\mathrm{RFR}})$	$= 7 \cdot (1 - 30\%) \cdot 2{,}2$	$= 10{,}8$
Gl. 2.25:	ζ	$\overset{(\leq 1)}{=} \frac{K \cdot \mu_{\mathrm{F}}(N)}{N}$	$= \frac{0{,}4 \cdot 10{,}8}{5}$	$\to 1$

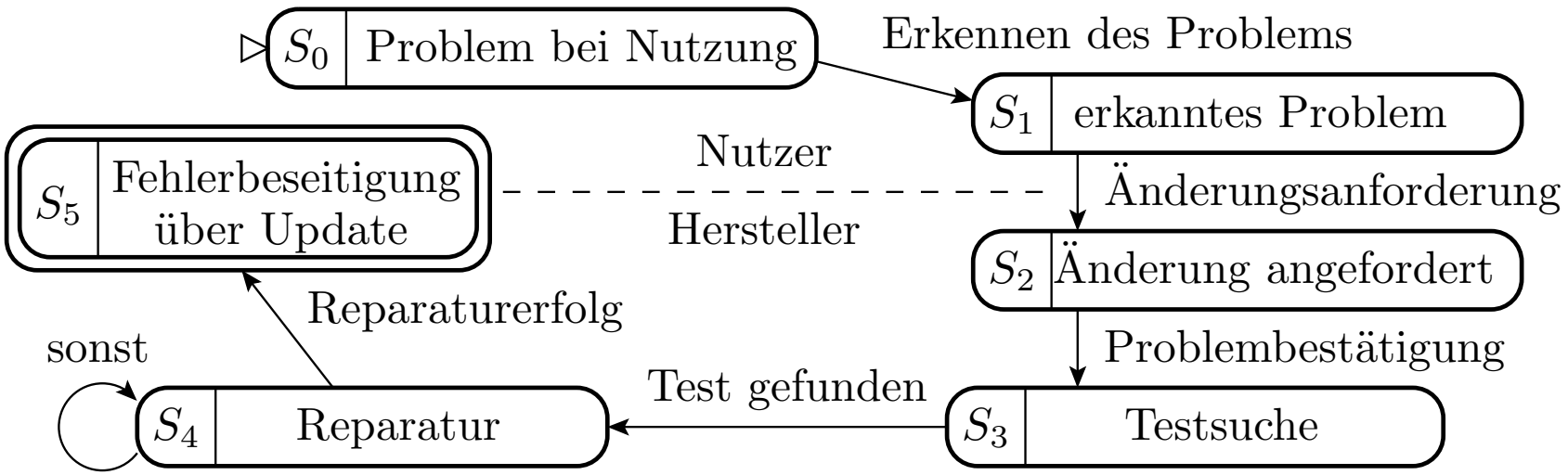
- Im Mittel 4,9 ursprüngliche plus 5,9 bei der Reparatur entstehende nicht erkennbare Fehler.
- Ein weiteres zufälliges Testbeispiel liefert garantiert MF.

Wie Programmierkursabnahme schaffen? Mehr Testen und Rückbau!

μ_{F}, ζ Expected number of faults. Malfunction rate.
(≥ 1) The calculated value is an upper limit. The actual value is max. one.

Reifeprozesse

3.94 Reifen von Produkten (sec.2.3.7)



- Bei einer vermuteten Fehlfunktion stellt der Nutzer eine Änderungsanforderung (Change Request). Alternativ sendet das System einen MF-Report. Change Requests und MF-Reports werden in Schubladen vermuteter gleicher Ursache gesammelt.
- Der Hersteller beseitigt bevorzugt Fehler, die mit großer Häufigkeit und/oder schwerwiegende Fehlfunktionen verursachen.
- Suche von Tests, die den Fehler reproduzierbar nachweisen.
- Experimentelle Reperatur. Fehlerbeseitigung über Updates.

3.95 Beseitigungswahrsch., effektive Testanzahl

Die Wahrscheinlichkeit, dass ein bei der Nutzung nachweisbares Problem erkannt, der Hersteller informiert, ... (bedingte Beseitigungswahrscheinlichkeit, wenn Problem erkennbar) ist gering:

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

aber die effektive Testanzahl ist, weil sich dafür die genutzten Service-Leistung aller Nutzer addieren, viel größer, als die Anzahl der Regessionstests der Hersteller vor der Produkt- und Versionsfreigabe:

(2.46)
$$N = \underbrace{p_{\mathrm{FE}} \cdot \mu_{\mathrm{NU}} \cdot \eta_{\mathrm{SS}} \cdot t_{\mathrm{VR}}}_{N_{\mathrm{MV}}} \cdot (u + u_{\mathrm{V0}}) \quad \text{with} \quad u_{\mathrm{V0}} = \frac{N_{\mathrm{V0}}}{N_{\mathrm{MV}}}$$

N	Effective number of tests: the number of tests required to eliminate all detected faults.
p_{FE}	Probability that a fault will be eliminated if it causes a MF.
μ_{NU}	Expected **n**umber of **u**ser.
η_{SS}	System utilisation rate, percentage of available service time used.
t_{VR}	Version interval, time between the release of successive versions.
N_{MV}	Increase the effective number of tests in each version interval.
N_{V0}	Effective number of tests prior to version release; approx. number of regression tests.
$u,\ v$	Version number and reference version number of the maturing object.
u_{V0}	Ratio of the maturing time before version release to maturing time increase per version.
K	Shape parameter of the distribution of the malfunction rate $(0 < K < 1)$.

3.96 Fehleranzahl, Zuverlässigkeit, Sicherheit

Abnahme der zu erwartenden Fehleranzahl ohne Fehlerneuentstehung für gleich lange Versionsintervalle, ...:

(2.48)
$$\mu_{\mathrm{F}}(u) = \mu_{\mathrm{F}}(v) \cdot \left(\frac{u+u_{\mathrm{V0}}}{v+u_{\mathrm{V0}}}\right)^{-K}$$

Bei geeigneter Systemgestaltung und Problembehandlung

- ist die Fehlfunktionsrate durch Störungen vernachlässigbar und
- wächst die Sicherheit proportional mit der Zuverlässigkeit.

Zunahme von Zuverlässigkeit und Sicherheit mit Exponent $K+1$ mit der Reifedauer und bei gleich langen Versionsintervallen auch etwa mit der Versionsnummer:

(2.52)
$$\frac{R(u)}{R(v)} = \frac{S(u)}{S(v)} = \left(\frac{u+u_{\mathrm{V0}}}{v+u_{\mathrm{V0}}}\right)^{K+1}$$

$\mu_{\mathrm{F}}(u)$	Expected number of faults in version u.
u, v	Version number and reference version number of the maturing object.
u_{V0}	Ratio of the maturing time before version release to maturing time increase per version.
R, S	Reliability, safety or security, each under ideal conditions.
K	Shape parameter of the distribution of the malfunction rate $(0 < K < 1)$.

3.97 Fortsetzung / Modellerweiterung

Zu den Idealisierungen in (sec.2.3.7) zählte, dass bei der Repartur keinen neuen Fehler entstehen, bzw. dass die neuen Fehler von den Regressionstests des Herstellers alle erkannt werden.

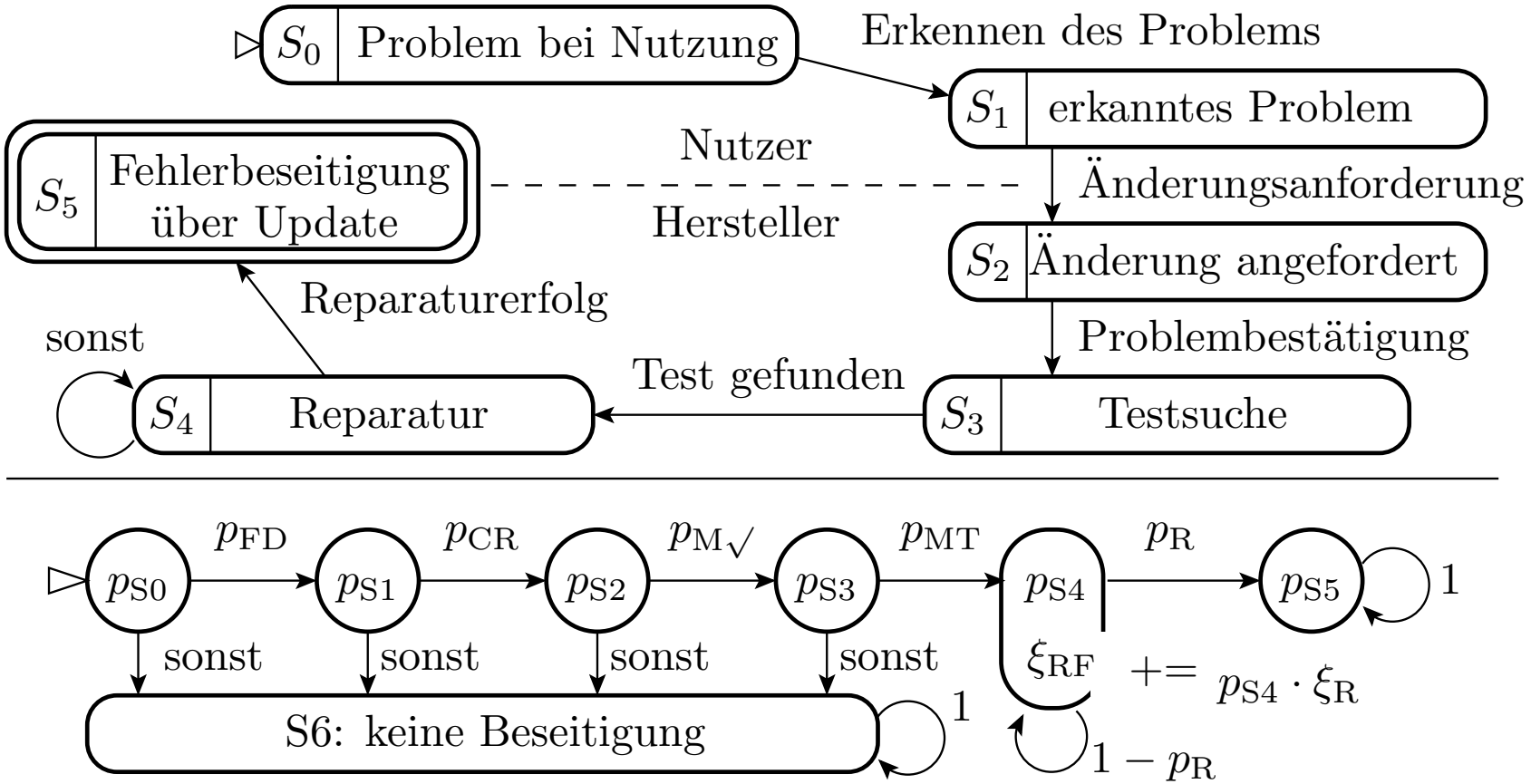
Die praktischen Erfahrungen sind anders. Nach jedem Update banges Hoffen auf:

- keine schwerwiegenden neuen Fehler, die wieder
- eine mühevolle Suche neue Workarouns verlangen.

Geplante Modellerweiterung: Modellierung der Fehlerbeseitigung als Markov-Prozess mit Fehlerneuentstehung. Untersuchung, wie sich die Fehlerneuentstehung auf die zu erwartende Zuverlässigkeit auswirkt.

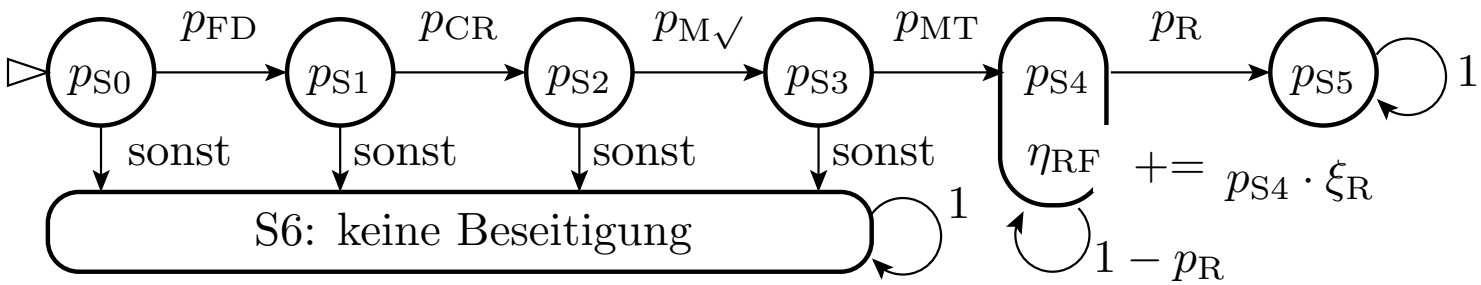
Demonstrieren, warum die Nutzer die Fehlerneuentstehung so drastisch spühren und Aufzeigen, was die Hersteller dagegen tun müssten.

3.98 Reifeprozess als Markov-Kette



p_{Si}	Probability that the Markov chain is in state S_i.
ξ_{RF}	Fault emergence rate in new faults per existing fault.
p_{FD}, ...	siehe nächste Folie.

3.100 Fehlerbeseitigungswahrscheinlichkeit



Unter der Annahme, dass so lange repariert wird, bis der Fehler beseitigt ist, beträgt die Wahrscheinlichkeit, dass ein Fehler, wenn er eine Fehlfunktion verursacht, letztendlich beseitigt wird:

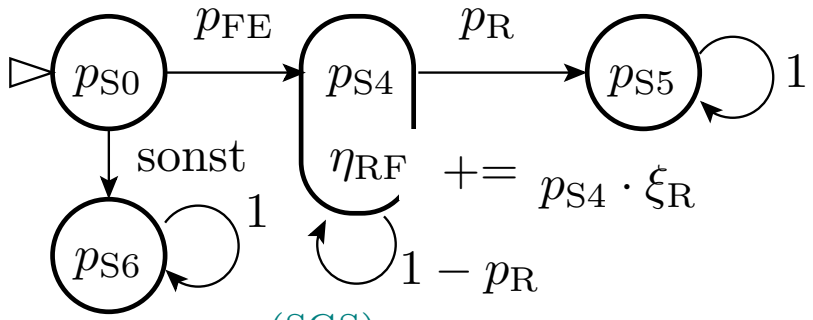
$$p_{\mathrm{FE}} = \lim_{n \to \infty} p_{\mathrm{S5}}(n) = p_{\mathrm{FD}} \cdot p_{\mathrm{CR}} \cdot p_{\mathrm{M}\surd} \cdot p_{\mathrm{MT}} \tag{3.39}$$

In S_4 (Reparatur) verbleibt der Automat bis zur Fehlerbeseitigung. Je Beseitigungsversuch entsteht mit der Rate ξ_{R} ein neuer Fehler.

p_{FE}	Probability that a fault will be eliminated if it causes a MF.
p_{FD}	Probability of fault detection.
p_{CR}	Probability of a change request being made for an observed MF.
$p_{\mathrm{M}\surd}$	probability that manufacturer can reconstruct the MF.
p_{MT}	Probability that the manufacturer will find a test for fault detection.
p_{R}	Probability of repair success.
ξ_{R}	Fault emergence rate in new faults per repair attempt.

3.101 Fehlerentstehungsrate

Dieselbe Markov-Kette wie für die Fehlerbeseitigung durch Reparatur (sec.3.3.2). Entstehungsrate neuer je vorhandener Fehler:



(3.31) $$\xi_{RF} = p_{FE} \cdot \sum_{n=0}^{\infty} \xi_R \cdot (1 - p_R)^n \overset{(SGS)}{=} p_{FE} \cdot \frac{\xi_R}{p_R}$$

Die Fehlerentstehungsrate je beseitigter Fehler ist um den Kehrwert der Beseitigungswahrscheinlichkeit größer:

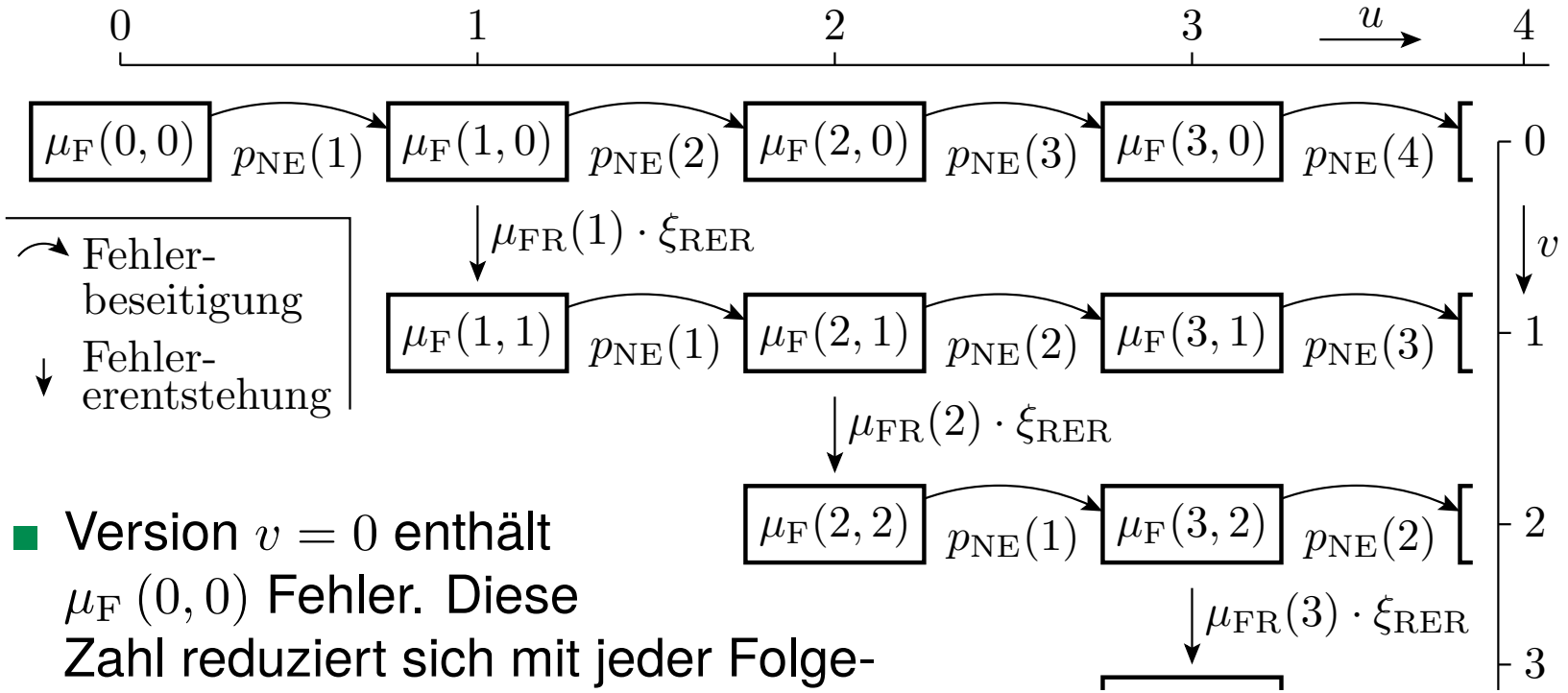
(3.32) $$\xi_{RE} = \frac{\xi_{RF}}{p_{FE}} = \frac{\xi_R}{p_R} < 1$$

Rekursiv unter Berücksichtigung »neuer Fehler durch neue Fehler«

(3.33) $$\xi_{RER} = \frac{1}{1-\xi_{RE}} - 1 = \frac{\xi_{RE}}{1-\xi_{RE}}$$

p_{FE}	Probability that a fault will be eliminated if it causes a MF.
p_R	Probability of repair success.
ξ_R	Fault emergence rate in new faults per repair attempt.
ξ_{RF}	Fault emergence rate in new faults per existing fault.
ξ_{RE}	Fault emergence rate in new faults per eliminated fault.
ξ_{RER}	Fault emergence rate in new faults per original fault eliminated.

3.103 Reifeprozess mit Fehlerneuentstehung



- Version $v = 0$ enthält $\mu_F(0,0)$ Fehler. Diese Zahl reduziert sich mit jeder Folgeversionen $u > 0$ um eine Nichtbeseitigungswahrscheinlichkeit $p_{NE}(u - v)$ auf $\mu_F(u, 0)$.
- In jeder Version $u > 0$ entstehen neue Fehler. Deren zu erwartende Anzahl nimmt mit jeder Folgeversionen $u > v$ um eine Nichtbeseitigungswahrscheinlichkeit $p_{NE}(u - v)$ ab auf $\mu_F(u, v)$.

3.104 Nichtbeseitigungswahrscheinlichkeit

Für gleichlange Update-Intervalle beträgt die effektive Testanzahl für Fehler in Version u, die in Version v entstanden sind, nach (eq. 2.46):

$$N(u,v) = N_{\mathrm{VM}} \cdot (u - v + u_{\mathrm{V0}}) \tag{3.40}$$

Die zu erwartende Fehleranzahl aus jeder Version v nimmt mit Version $u \geq v$ seit der Vorversion $u-1$ nach (eq. 2.48) ab:

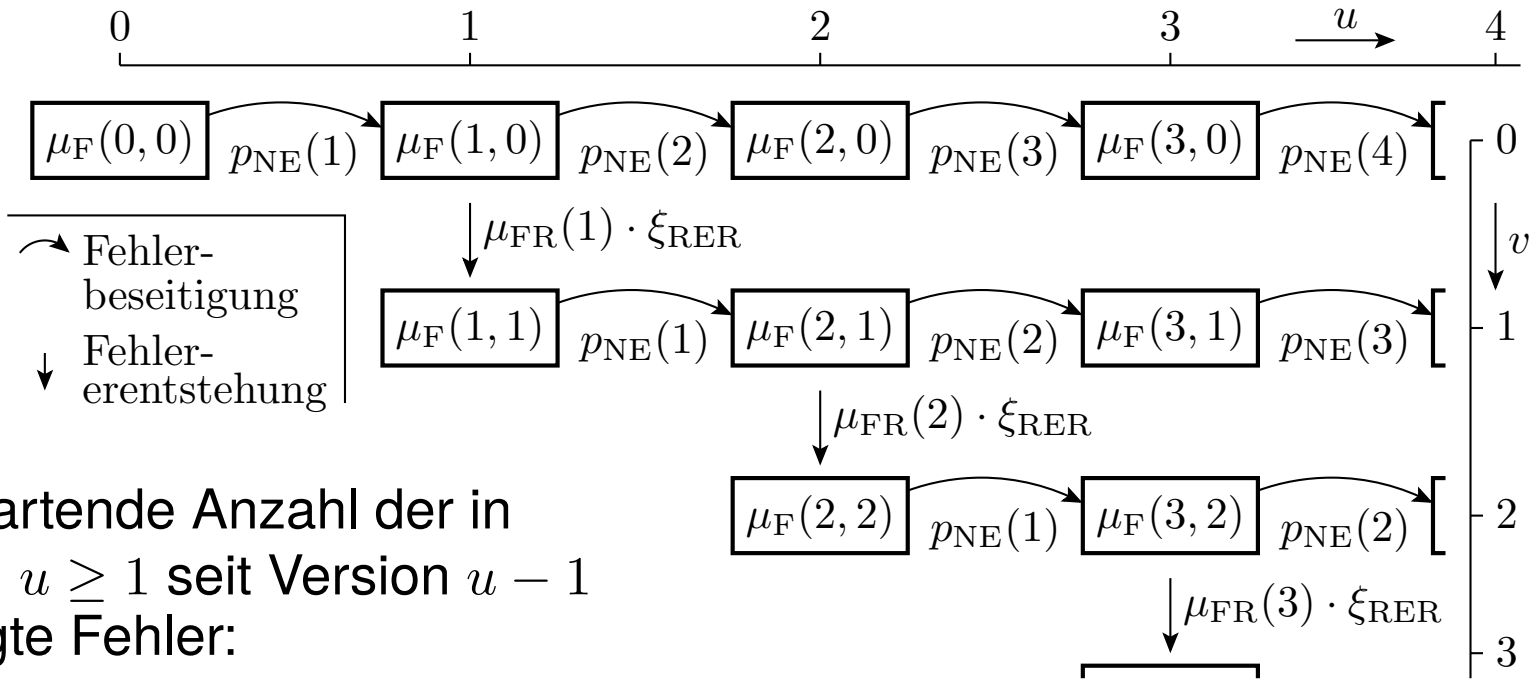
$$\mu_{\mathrm{F}}(u,v) = \mu_{\mathrm{F}}(u-1,v) \cdot \left(\frac{u-v+u_{\mathrm{V0}}}{u-1-v+u_{\mathrm{V0}}}\right)^{-K} \tag{3.41}$$

Nichtbeseitigungswahrscheinlichkeit $p_{\mathrm{NE}}(u)$ als relative Verringerung der zu erwartenden Fehleranzahl gegenüber Vorversion:

$$p_{\mathrm{NE}}(u-v) = \frac{\mu_{\mathrm{F}}(u,v)}{\mu_{\mathrm{F}}(u-1,v)} = \left(\frac{u-v+u_{\mathrm{V0}}}{u-v-1+u_{\mathrm{V0}}}\right)^{-K} \tag{3.42}$$

$N(u,v)$	Effective test count in version u for faults from version v.
N_{MV}	Increase the effective number of tests in each version interval.
u, v	Version number and reference version number of the maturing object.
u_{V0}	Ratio of the maturing time before version release to maturing time increase per version.
$p_{\mathrm{NE}}(u-v)$	Non-elimination probability for errors from version v in the subsequent version of u.
K	Shape parameter of the distribution of the malfunction rate $(0 < K < 1)$.

3.105 Neu entstehende Fehler



Zu erwartende Anzahl der in Version $u \geq 1$ seit Version $u-1$ beseitigte Fehler:

$$\mu_{FR}(u) = \sum_{v=0}^{u-1} \left(\mu_F(u-1,v) - \mu_F(u,v)\right) \tag{3.43}$$

Die Anzahl der neu entstehenden Fehler ist ξ_{RER} mal so groß:

$$\mu_F(u,u) = \xi_{RER} \cdot \mu_{FR}(u) \tag{3.44}$$

ξ_{RER} Fault emergence rate in new faults per original fault eliminated.

3.106 Zu erwartende Fehleranzahlen insgesamt

$\mu_{\mathrm{F}}(0,0)$ gleich erwartetet Fehleranzahl in Version 0

Wiederhole für jede Versionsnummer ab $u = 1$

- Wiederhole für Fehlerentstehungsversion $v = 0$ bis $u - 1$
  - Zu erwartende Anzahl der nicht beseitigten Fehler:

$$\mu_{\mathrm{F}}(u,v) = \mu_{\mathrm{F}}(u-1,v) \cdot \left(\frac{u-v+u_{\mathrm{V0}}}{u-1-v+u_{\mathrm{V0}}}\right)^{-K} \tag{3.41}$$

- Erwartete Zahl der beseitigten und neu entstehenden Fehler:

$$\mu_{\mathrm{FR}}(u) = \sum_{v=0}^{u-1} \left(\mu_{\mathrm{F}}(u-1,v) - \mu_{\mathrm{F}}(u,v)\right) \tag{3.43}$$

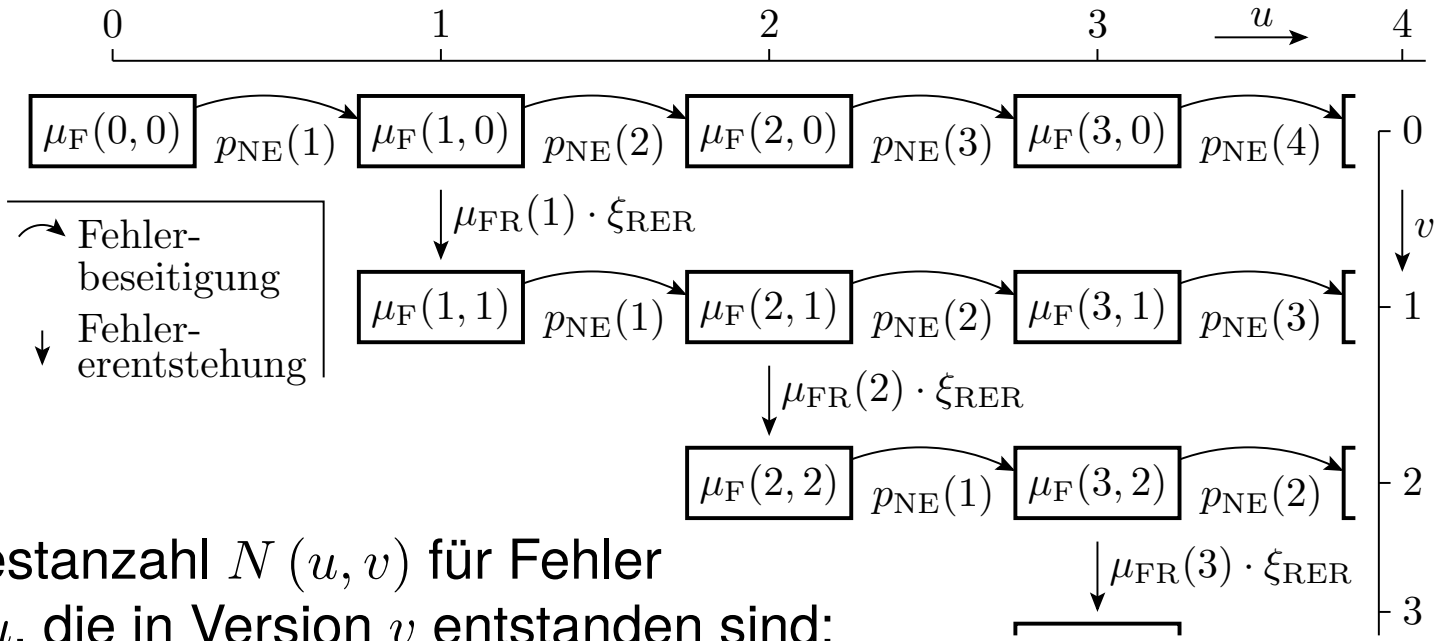
$$\mu_{\mathrm{F}}(u,u) = \xi_{\mathrm{RER}} \cdot \mu_{\mathrm{FR}}(u) \tag{3.44}$$

- Alle Fehler:

$$\mu_{\mathrm{F}}(u) = \sum_{v=0}^{u} \mu_{\mathrm{F}}(u,v) \tag{3.45}$$

$\mu_{\mathrm{F}}(u,v)$	Expected number of faults in version u that originate in version v.
$u,\ v$	Version number and reference version number of the maturing object.
u_{V0}	Ratio of the maturing time before version release to maturing time increase per version.
$\mu_{\mathrm{FE}}(u)$	Expected number of faults eliminated in version u from version $u-1$.
ξ_{RER}	Fault emergence rate in new faults per original fault eliminated.

3.107 Fehlfunktionsrate durch Fehler



Effektive Testanzahl $N(u,v)$ für Fehler in Version u, die in Version v entstanden sind:

(3.40) $$N(u,v) = N_{VM} \cdot (u - v + u_{V0})$$

Wiederhole für jede Versionsnummer ab $u = 0$ (vergl. Gl. 2.25):

$$\zeta_F(u) = K \cdot \sum_{v=0}^{u} \frac{\mu_F(u,v)}{N(u,v)} \tag{3.46}$$

$\zeta_F(u)$	Total malfunction rate due to all faults in version u.
K	Shape parameter of the distribution of the malfunction rate $(0 < K < 1)$.

Example 3.6: Reifeprozess mit neu entstehenden Fehlern

$\mu_{\mathrm{F}}(0,0) = 100$, $N_{\mathrm{MV}} = 10^6$, $u_{\mathrm{V0}} = 0{,}1$, $\eta_{\mathrm{RER}} = 0{,}1$, $K = 0{,}4$.

a) *Zu erwartende Fehleranzahlen $\mu_{\mathrm{F}}(u,v)$ für $u = 0$ bis 5 gereifte Versionen je Entstehungsversion v und insgesamt?*

b) *MF-Raten $\zeta_{\mathrm{F}}(u,v)$ einzeln und Summe $\zeta_{\mathrm{F}}(u)$?*

c) *Relative Erhöhung der zu erwartenden Fehleranzahl durch die bei der Beseitigung neu entstehenden Fehler?*

d) *Relative Erhöhung der MF-Rate durch die neuen Fehler?*

$\mu_{\mathrm{F}}(0,0)$	Expected number of faults in version 0 (first released version).
N_{MV}	Increase the effective number of tests in each version interval.
u_{V0}	Ratio of the maturing time before version release to maturing time increase per version.
ξ_{RER}	Fault emergence rate in new faults per original fault eliminated.
K	Shape parameter of the distribution of the malfunction rate $(0 < K < 1)$.
u, v	Version number and reference version number of the maturing object.
$\mu_{\mathrm{F}}(u,v)$	Expected number of faults in version u that originate in version v.
$\mu_{\mathrm{F}}(u)$	Expected total number of faults in version u.

$\mu_{\mathrm{F}}(0,0) = 100$, $N_{\mathrm{MV}} = 10^6$, $u_{\mathrm{V0}} = 0{,}1$, $\eta_{\mathrm{RER}} = 0{,}1$, $K = 0{,}4$.

a) *Zu erwartende Fehleranzahlen $\mu_{\mathrm{F}}(u,v)$ für $u = 0$ bis 5 gereifte Versionen je Entstehungsversion v und insgesamt?*

(3.41) $$\mu_{\mathrm{F}}(u,v) = \mu_{\mathrm{F}}(u-1,v) \cdot \left(\frac{u-v+u_{\mathrm{V0}}}{u-1-v+u_{\mathrm{V0}}}\right)^{-K}$$

(3.43) $$\mu_{\mathrm{FR}}(u) = \sum_{v=0}^{u-1} \left(\mu_{\mathrm{F}}(u-1,v) - \mu_{\mathrm{F}}(u,v)\right)$$

(3.44) $$\mu_{\mathrm{F}}(u,u) = \xi_{\mathrm{RER}} \cdot \mu_{\mathrm{FR}}(u)$$

$\mu_{\mathrm{F}}(u,v)$	$u=0$	$u=1$	$u=2$	$u=3$	$u=4$	$u=5$
$v=0$	100	38,32	29,59	25,32	22,64	20,75
$v=1$	0	6,17	2,36	1,82	1,56	1,40
$v=2$	0	0	1,25	$4{,}80 \cdot 10^{-1}$	$3{,}71 \cdot 10^{-1}$	$3{,}17 \cdot 10^{-1}$
$v=3$	0	0	0	$5{,}58 \cdot 10^{-1}$	$2{,}14 \cdot 10^{-1}$	$1{,}65 \cdot 10^{-1}$
$v=4$	0	0	0	0	$3{,}40 \cdot 10^{-1}$	$1{,}30 \cdot 10^{-1}$
$v=5$	0	0	0	0	0	$2{,}37 \cdot 10^{-1}$
$\mu_{\mathrm{F}}(u)$	100	44,49	33,21	28,18	25,13	22,99

$\mu_{\mathrm{F}}(0,0) = 100$, $N_{\mathrm{MV}} = 10^6$, $u_{\mathrm{V0}} = 0{,}1$, $\eta_{\mathrm{RER}} = 0{,}1$, $K = 0{,}4$.

b) *MF-Raten $\zeta_{\mathrm{F}}(u,v)$ einzeln und Summe $\zeta_{\mathrm{F}}(u)$?*

(3.40) $$N(u,v) = N_{\mathrm{VM}} \cdot (u - v + u_{\mathrm{V0}})$$

(3.46) $$\zeta_{\mathrm{F}}(u) = K \cdot \sum_{v=0}^{u} \frac{\mu_{\mathrm{F}}(u,v)}{N(u,v)}$$

Tabelle $\zeta_{\mathrm{F}}(u,v) = \frac{\mu_{\mathrm{F}}(u,v)}{N(u,v)}$:

$\zeta_{\mathrm{F}}(u,v)$	$u=0$	$u=1$	$u=2$	$u=3$	$u=4$	$u=5$
$v=0$	$4{\cdot}10^{-4}$	$1{,}39{\cdot}10^{-5}$	$5{,}64{\cdot}10^{-6}$	$3{,}27{\cdot}10^{-6}$	$2{,}21{\cdot}10^{-6}$	$1{,}63{\cdot}10^{-6}$
$v=1$	0	$2{,}47{\cdot}10^{-5}$	$8{,}59{\cdot}10^{-7}$	$3{,}48{\cdot}10^{-7}$	$2{,}02{\cdot}10^{-7}$	$1{,}36{\cdot}10^{-7}$
$v=2$	0	0	$5{,}02{\cdot}10^{-6}$	$1{,}75{\cdot}10^{-7}$	$7{,}07{\cdot}10^{-8}$	$4{,}10{\cdot}10^{-8}$
$v=3$	0	0	0	$2{,}23{\cdot}10^{-6}$	$7{,}78{\cdot}10^{-8}$	$3{,}14{\cdot}10^{-8}$
$v=4$	0	0	0	0	$1{,}36{\cdot}10^{-6}$	$4{,}73{\cdot}10^{-8}$
$v=5$	0	0	0	0	0	$9{,}48{\cdot}10^{-7}$
$\zeta_{\mathrm{F}}(u)$	$4{\cdot}10^{-4}$	$3{,}86{\cdot}10^{-5}$	$1{,}15{\cdot}10^{-5}$	$6{,}02{\cdot}10^{-6}$	$3{,}92 \cdot 10^{-6}$	$2{,}83{\cdot}10^{-6}$

$\zeta_{\mathrm{F}}(u,v)$ MF rate in version u caused by faults emerged in version v.
$\zeta_{\mathrm{F}}(u)$ Total malfunction rate in version u.

$\mu_\mathrm{F}(0,0) = 100$, $N_\mathrm{MV} = 10^6$, $u_\mathrm{V0} = 0{,}1$, $\eta_\mathrm{RER} = 0{,}1$, $K = 0{,}4$.

c) *Relative Erhöhung der zu erwartenden Fehleranzahl durch die bei der Beseitigung neu entstehenden Fehler?*

$\mu_\mathrm{F}(u,v)$	$u=0$	$u=1$	$u=2$	$u=3$	$u=4$	$u=5$
$v=0$	100	38,32	29,59	25,32	22,64	20,75
$v=1$	0	6,17	2,36	1,82	1,56	1,40
$v=2$	0	0	1,25	$4{,}80 \cdot 10^{-1}$	$3{,}71 \cdot 10^{-1}$	$3{,}17 \cdot 10^{-1}$
$v=3$	0	0	0	$5{,}58 \cdot 10^{-1}$	$2{,}14 \cdot 10^{-1}$	$1{,}65 \cdot 10^{-1}$
$v=4$	0	0	0	0	$3{,}40 \cdot 10^{-1}$	$1{,}30 \cdot 10^{-1}$
$v=5$	0	0	0	0	0	$2{,}37 \cdot 10^{-1}$
$\mu_\mathrm{F}(u)$	100	44,49	33,21	28,18	25,13	22,99
$\frac{\mu_\mathrm{F}(u)}{\mu_\mathrm{F}(u,0)}$		1,161	1,122	1,113	1,110	1,108

Erhöhung etwa um die zu erwartende Fehlerentstehungsrate η_RER in bei der Beseitigung neu enstehende Fehler je beseitigter Fehler.

$\mu_\mathrm{F}(u,0)$ Expected number of faults from version 0, which are not eliminated in version u.

$\mu_\mathrm{F}(0,0) = 100$, $N_\mathrm{MV} = 10^6$, $u_\mathrm{V0} = 0{,}1$, $\eta_\mathrm{RER} = 0{,}1$, $K = 0{,}4$.

d) *Relative Erhöhung der MF-Rate durch die neuen Fehler?*

$\zeta_\mathrm{F}(u,v)$	$u=0$	$u=1$	$u=2$	$u=3$	$u=4$	$u=5$
$v=0$	$4\cdot10^{-4}$	$1{,}39\cdot10^{-5}$	$5{,}64\cdot10^{-6}$	$3{,}27\cdot10^{-6}$	$2{,}21\cdot10^{-6}$	$1{,}63\cdot10^{-6}$
$v=1$	0	$2{,}47\cdot10^{-5}$	$8{,}59\cdot10^{-7}$	$3{,}48\cdot10^{-7}$	$2{,}02\cdot10^{-7}$	$1{,}36\cdot10^{-7}$
$v=2$	0	0	$5{,}02\cdot10^{-6}$	$1{,}75\cdot10^{-7}$	$7{,}07\cdot10^{-8}$	$4{,}10\cdot10^{-8}$
$v=3$	0	0	0	$2{,}23\cdot10^{-6}$	$7{,}78\cdot10^{-8}$	$3{,}14\cdot10^{-8}$
$v=4$	0	0	0	0	$1{,}36\cdot10^{-6}$	$4{,}73\cdot10^{-8}$
$v=5$	0	0	0	0	0	$9{,}48\cdot10^{-7}$
$\zeta_\mathrm{F}(u)$	$4\cdot10^{-4}$	$3{,}86\cdot10^{-5}$	$1{,}15\cdot10^{-5}$	$6{,}02\cdot10^{-6}$	$3{,}92\cdot10^{-6}$	$2{,}83\cdot10^{-6}$
$\frac{\zeta_\mathrm{F}(u)}{\zeta_\mathrm{F}(u,0)}$		2,78	2,04	1,84	1,77	1,74

Erhöhung um Größenordnung $\eta_\mathrm{RFR}/u_\mathrm{V0}$. Es sind zwar insgesamt nur grob geschätzt $\xi_\mathrm{RFR} = 10\%$ mehr Fehler. Aber die jüngsten Fehler davon haben nur eine effektive Testanzahl $N(u,u) = 0{,}1 \cdot N_\mathrm{MV}$ und alle anderen Fehler von mindesten von N_MV.

$\zeta_\mathrm{F}(u,0)$ MF rate in version u due to faults from version 0 (first released version.

Zusammenfassung

3.109 Fehlerbeseitigung, Ersatz (𝕎)

Fehlerbeseitigung mit Erfolgskontrolle beseitigt alle erkennbaren Fehler. Bei hoher Ausbeute ist Ersatz und bei geringer Ausbeute Reparatur günstiger.

Für Ersatz, Anzahl der Ersetzungen

(3.29) $$\mu_{\mathrm{Repl}} = \frac{1}{Y} - 1$$

Fehleranteil nach Ersatz der erkannten defekten Teile, siehe auch Abschn. 2.1.5:

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

𝕃, 𝔹, 𝕎 Key message. Illustrative examples. Key message from previous sections.

3.110 Reparatur (𝔹)

Bei einer Reparaturiteration bis Erfolg werden auch alle nachweisbaren Fehler beseitigt, aber statt der Reduzierung der Objektanzahl im Nenner um die aussortierten Objekte entstehen neue Fehler.

- Fehlerentstehungsrate je vorhandener Fehler:

(3.31) $$\xi_{\mathrm{RF}} = p_{\mathrm{FE}} \cdot \sum_{n=0}^{\infty} \xi_{\mathrm{R}} \cdot (1-p_{\mathrm{R}})^n \overset{(\mathrm{SGS})}{=} p_{\mathrm{FE}} \cdot \frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}}$$

- Fehlerentstehungsrate je beseitigter Fehler:

(3.32) $$\xi_{\mathrm{RE}} = \frac{\xi_{\mathrm{RF}}}{p_{\mathrm{FE}}} = \frac{\xi_{\mathrm{R}}}{p_{\mathrm{R}}} < 1$$

- Fehlerentstehungsrate je beseitigter ursprünglicher Fehler:

(3.33) $$\xi_{\mathrm{RER}} = \frac{1}{1-\xi_{\mathrm{RE}}} - 1 = \frac{\xi_{\mathrm{RE}}}{1-\xi_{\mathrm{RE}}}$$

- Fehlerentstehungsrate je vorhandener ursprünglicher Fehler:

(3.34) $$\xi_{\mathrm{RFR}} = p_{\mathrm{FE}} \cdot \xi_{\mathrm{RER}} = p_{\mathrm{FE}} \cdot \left(\frac{\xi_{\mathrm{RE}}}{1-\xi_{\mathrm{RE}}} \right) \text{ for } \xi_{\mathrm{RE}} < 1$$

Zu erwartende Anzahl der nicht beseitigten Fehler:

(3.37) $$\mu_{\mathrm{F}} = \mu_{\mathrm{CF}} \cdot (1+\xi_{\mathrm{RFR}}) \cdot (1-p_{\mathrm{FE}})$$

3.111 Regeln für eine vernünftige Reparatur (𝕃)

Vernünftige Reparaturtechnologie:

- geringe Fehlerentstehungsrate (z.B. $\xi_{\mathrm{RE}} \lesssim 0{,}1$ neuer je beseitigter Fehler) und
- hoher Fehlererkennungswahrscheinlichkeit p_{FD}.

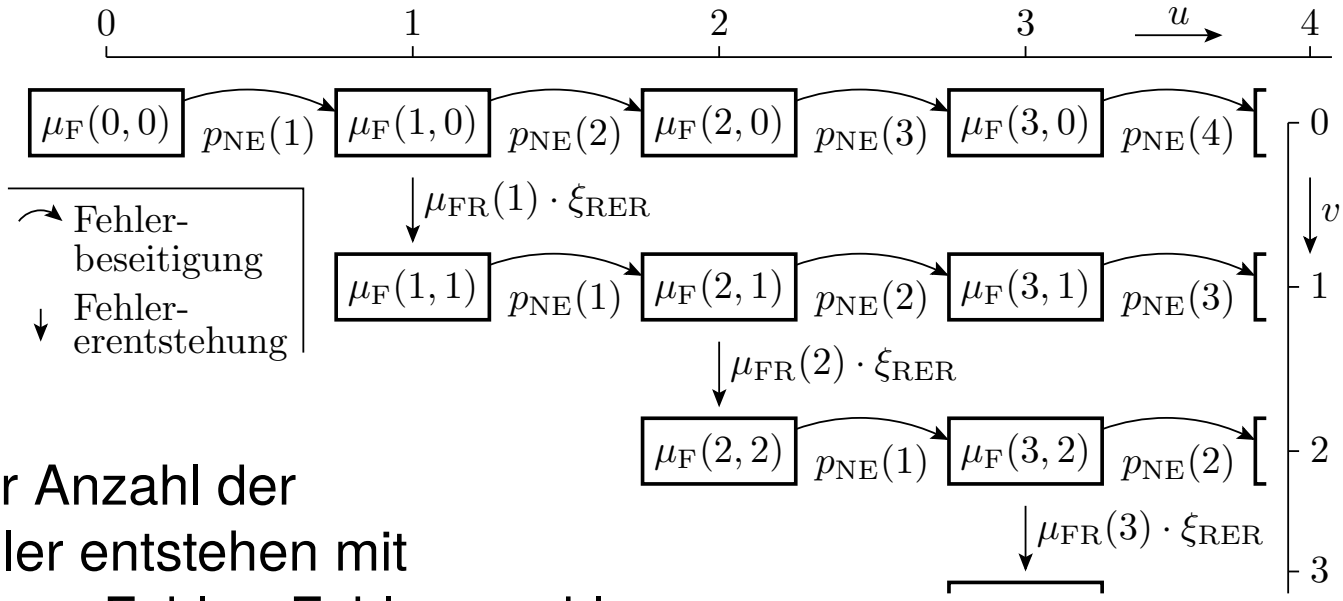
  Erhöhung der Fehleranzahl gegenüber der Anzahl der ursprünglichen nicht erkennbaren Fehler nur prozentual um $p_{\mathrm{FD}} \cdot \xi_{\mathrm{RE}}$.

Kenngrößen und Symtome schlechter Reparaturtechnologie:

- Kleine Erkennungswahrscheinlichkeit p_{FD} und deutlich mehr als ein neu entstehender je 10 beseitigte Fehler. Kaum Verringung oder sogar Vergrößerung der Fehleranzahl durch die Reparaturiteration. Auch deshalb Rückbau nach erfolglosen Reperaturversuchen.
- Wenn die Testanzahl nicht deutlich größer als die zu erwartende Fehleranzahl nach der Beseitigungsiteration ist, wird oft nicht einmal ein neues zufällig gewähltes Testbeispiel richtig abgearbeitet.

ξ_{RE} Fault emergence rate in new faults per eliminated fault.

3.112 Reifeprozess mit Fehlerentstehung



Proportional zur Anzahl der beseitigten Fehler entstehen mit jeder Version neue Fehler. Fehleranzahl insgesamt grob abgeschätzt etwa um η_{RER} größer als ohne Fehlerneuentstehung.

Fehlerfunktionsrate proportional zur Fehleranzahl geteilt durch die Reifedauer seit Entstehungsversion. Erhöhung der Fehlerfunktionsrate insgesamt gegenüber ohne Neuentstehung etwa um $\approx \eta_{RFR} / u_{V0}$.

u_{V0} Ratio of the maturing time before version release to maturing time increase per version.
ξ_{RER} Fault emergence rate in new faults per original fault eliminated.

... Erhöhung der Fehlerfunktionsrate insgesamt gegenüber ohne Neuentstehung etwa um $\approx \eta_{\mathrm{RFR}}/u_{\mathrm{V0}}$.

Bei geringem relativen Testaufwand u_{V0} beobachtet der Nutzer in jeder Version hauptsächlich Fehlfunktionen durch neue Fehler.

Die Wahrnehmung neuer Fehler wird durch die Nutzerlernprozesse verstärkt. Nutzer müssen für die schlimmsten neuen Fehler jeder Version Workarounds suchen, die in der Folgeversion wieder überflüssig sind.

Nutzerakzeptanz von Reifeprozessen verlangt, die Nutzer nicht zu oft mit neu entstehenden Fehlern zu konfrontieren, d.h. einen ausreichenden Testaufwand u_{V0} vor jeder Versionsfreigabe.

Fehlerentstehung

3.114 Modelle für die Fehlerentstehung

Einfacher Zufallsprozess, bei dem mit einer Raten $\xi_{<\mathrm{C}>}$ bezogen auf eine Metrik M_C Fehler entstehen.

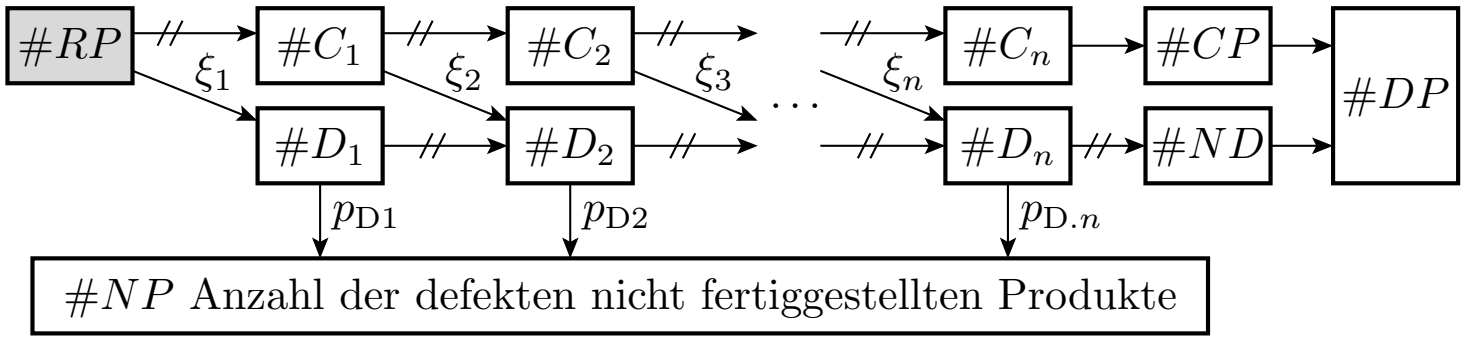
- Programmgröße: $M_\mathrm{C} = 800\,\mathrm{NLOC}$
- Fehlerentstehungsrate: $\xi_\mathrm{NLOC} = 20 \ldots 80\,\frac{\mathrm{F}}{1.000\,\mathrm{NLOC}}$
- zu erwartende Anzahl der entstehenden Fehler: 16 bis 64

Detaillierter: Modellierung wie ein IT-Systeme **als Service**, der auf Anforderung aus Eingaben Ergebnisse erzeugen. Nur mit Produkten als Ausgabe und Produktfehlern statt Fehlerfunktionen (sec.1.1.1).

Genauere Berücksichtigung der Entstehungsteilschritte, Kontrollen, ... bei den **Vorhersagen** der Zählwerte, Raten und Wahrscheinlichkeiten entstehender, vermiedener und beseitigter Fehler.

μ_CF	Expected number of faults from the creation processes.
ξ_NLOC	Fault emergence rate in faults per NLOC.
M_C	Metric for the effort of creation or the size of the product.
Pronounce:	ξ: xi.

3.115 Lineare Schrittfolge mit Kontrollen



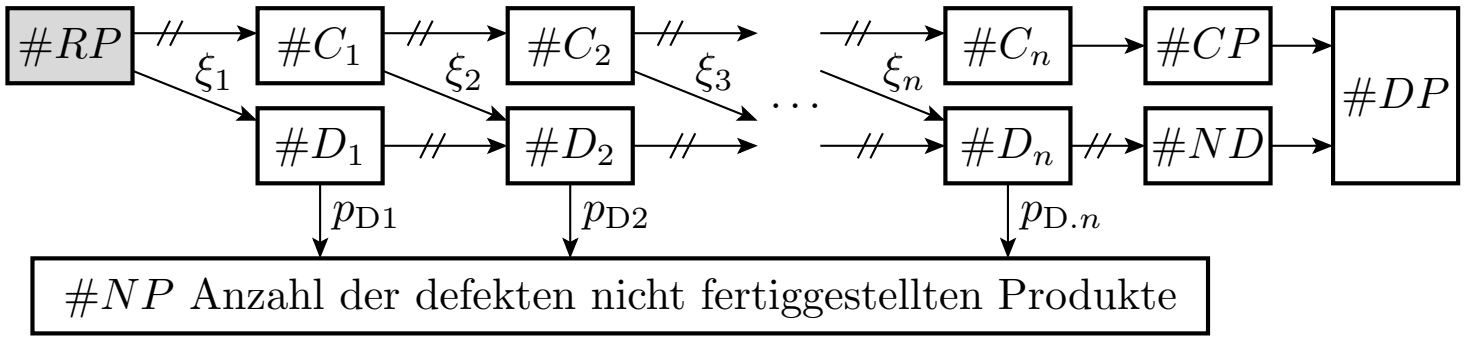
Folge von Entstehungsschritten und Kontrollen. In jedem Schritt

- werden Entstehungsleistungen erbracht, bei denen mit einer kleinen Rate $\xi_i \ll 1$ Fehler entstehen.
- Entstandene Fehler werden mit Wahrscheinlichkeit $p_{\mathrm{D}.i}$ erkannt.

Schleifenfreie Zuordnung von Entstehungsanforderung zu Teil- und weiter zu Endergebnisses $\Rightarrow$ Zählwertzuordnungsgraph

RP	Request to manufacture a product.
C_i, D_i	Steps 1 to i have been carried out correctly. The product after step i is incorrect.
CP, ND	Fault-free product. Product with undetected faults.
PD, NP	Product delivered. No product.
ξ_i, $p_{\mathrm{D}.i}$	Fault emergence rate and fault detection probability step i.

3.116 Prozesserbringungsrate



Der skizzierte Entstehungsprozess bricht bei erkanntem Fehler ab.
Erbringungsrate für korrekte Produkte:

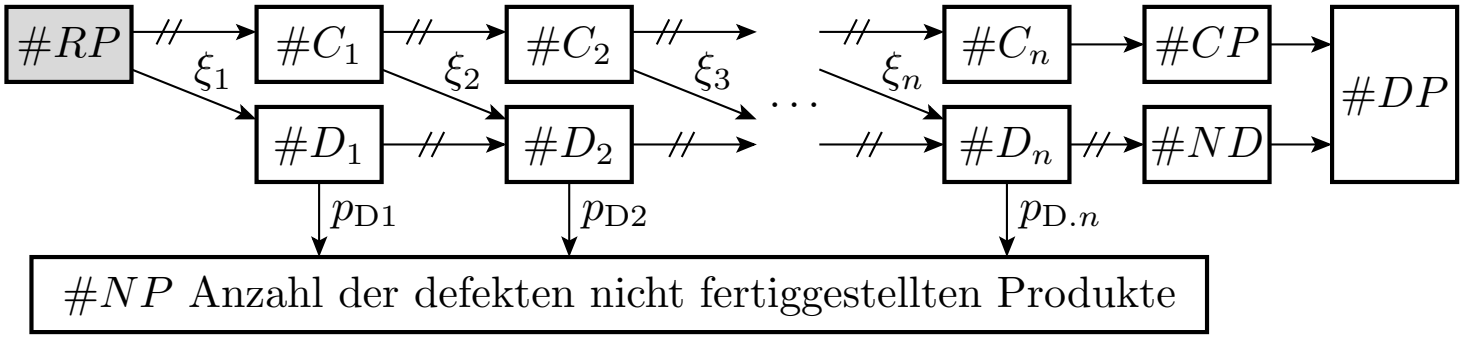
$$\eta_{\mathrm{CP}} = \left.\frac{\#CP}{\#RP}\right|_{\mathrm{ACR}} = \prod_{i=1}^{n}(1-\xi_i)$$

Erbringungsrate für Produkte mit nicht erkannten Fehlern:

$$\eta_{\mathrm{ND}} = \xi_1 \cdot \prod_{i=1}^{n}(1-p_{\mathrm{D}.i}) + \sum_{i=1}^{n-1}\left(\prod_{j=1}^{i}(1-\xi_j)\cdot\xi_{i+1}\cdot\prod_{j=i+1}^{n}(1-p_{\mathrm{D}.i})\right) \qquad (3.47)$$

$\eta_{\mathrm{CP}}, \eta_{\mathrm{ND}}$	Delivery rate of products without and with unrecognised faults.
$\xi_i, p_{\mathrm{D}.i}$	Fault emergence rate and fault detection probability step i.
Pronounce:	η: eta, ξ: xi.

3.117 Ausbeute und Fehleranteil



Die Ausbeute ist die gesamte Erbringungsrate:

$$Y = \frac{\#DP}{\#RP}\Big|_{\mathrm{SLC}} = \eta_{\mathrm{CP}} + \eta_{\mathrm{ND}}$$

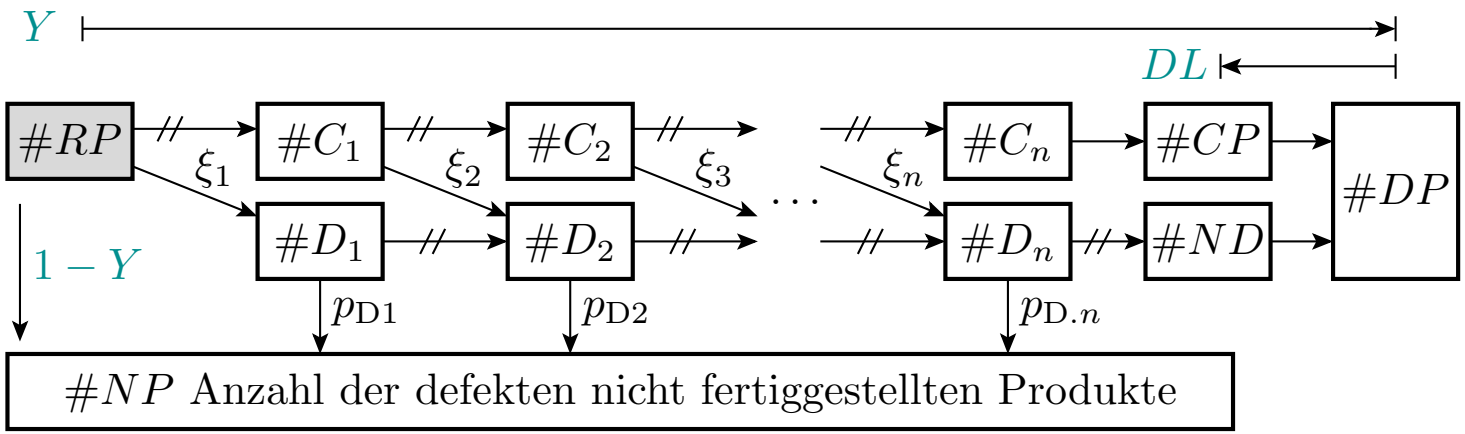
Fehleranteil der fertiggestellten Produkte:

$$DL = \frac{\#ND}{\#DP}\Big|_{\mathrm{SLC}} = \frac{\eta_{\mathrm{ND}}}{Y}$$

Für $\#DP \to \infty$ ist der Fehleranteil DL die bedingte Wahrscheinlichkeit, das ein fehlerfreies Produkt entsteht, wenn ein Produkt entsteht.

$\eta_{\mathrm{CP}}, \eta_{\mathrm{ND}}$ Delivery rate of products without and with unrecognised faults.
Y, DL Yield. Defect level.

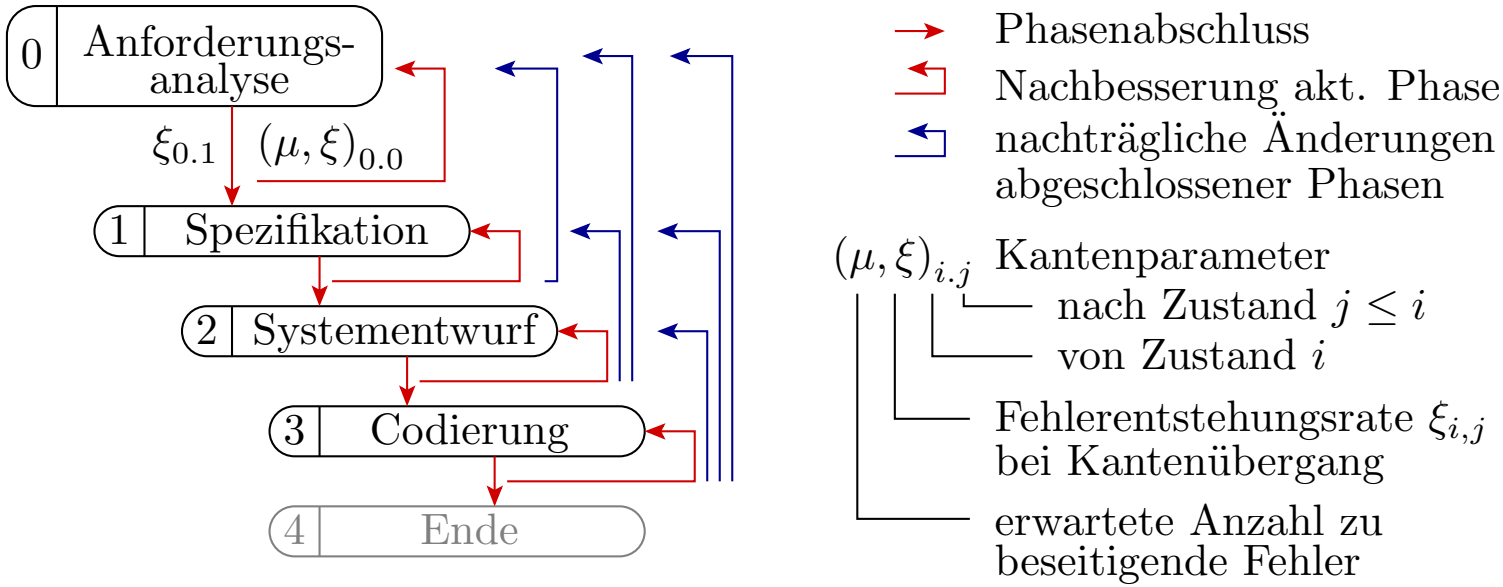
3.118 Modellnutzung und -verbesserung



Ein Modell, wie das skizzierte, erlaubt auch Rückschlüsse von bekannten Ausgaben (hier Y und DL) auf mögliche oder erforderliche Parameterwerte (hier ξ_i und $p_{\mathrm{D}.i}$), die Lokalisierung von Schwachstellen im Prozess und und darüber eine Verbesserung der Entstehungsabläufe.

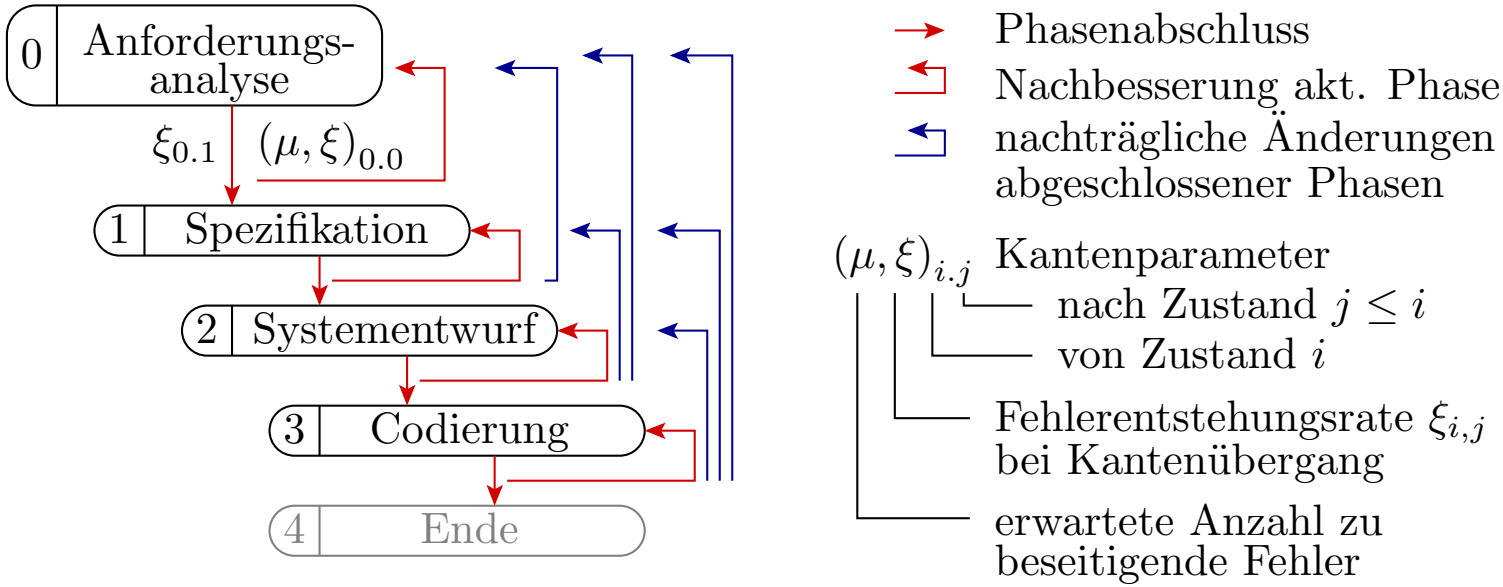
Entstehungsabläufe **mit Rückgriffen zur Problembeseitigung** kann man versuchen, mit **Markov-Ketten** zu beschreiben. Die Entstehungszustände müssen sich dabei wie die Zustände eines endlichen Automaten gegenseitig ausschließen. Den Schritten und Übergängen können **akkumulierende Fehlerentstehungsraten** zugeordnet werden (sec.3.3.2).

3.119 Phasenmodell als Markov-Kette



Entstehungsablauf als Folge von Entstehungsphasen. Die Abschlusskontrolle nach jeder Phase entdeckt Fehler, die Korrekturen der Ergebnisse derselben oder einer bereits abschlossenen Phase verlangen. Ohne nachweisbare Fehler Übergang zu nächsten Phase.

Den Rückgriffkanten ist je eine zu erwartende Übergangsanzahl μ je Vorwärtsübergang zugeordnet, aus denen sich die Übergangshäufigkeiten aller Kanten ergeben.



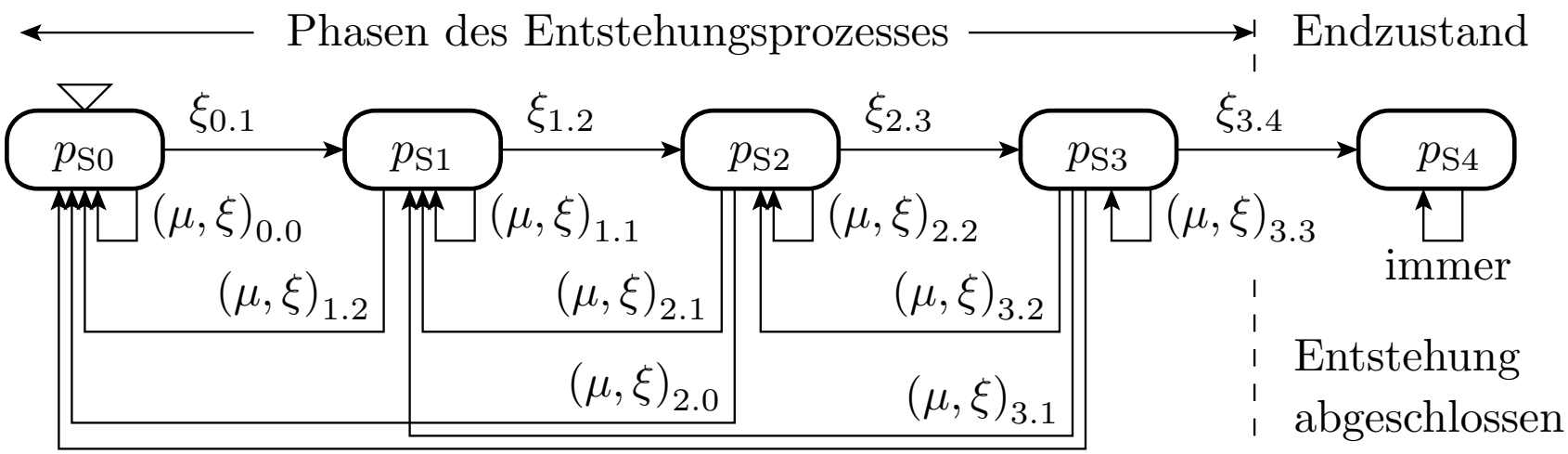
Die Übergangswahrscheinlichkeiten je abgehende Kante von Phase i nach Phase j ergibt sich aus den Anteilen der über die Kanten zu beseitigenden Fehler:

$$p_{i,j} = \frac{\mu_{i,j}}{1+\sum_{j=0}^{i} \mu_{i,j}}$$

Die den Kanten zugeordneten Fehlerentstehungsrate ξ sind die der nicht erkennbaren Fehler:

- für Rückwärtskanten je Fehlerbeseitigung und
- für Vorwärtskanten die der in Phase i entstehenden.

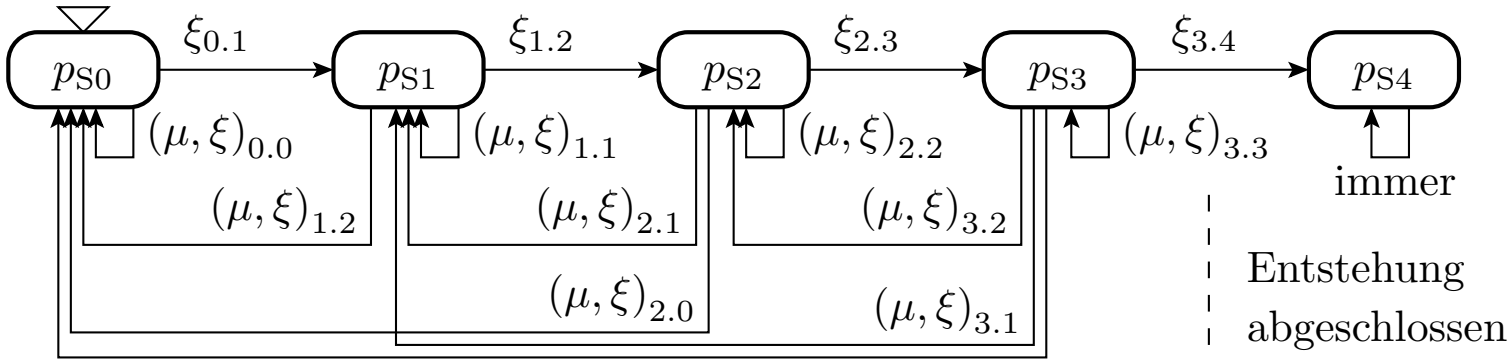
3.121 Modellierung als Markov-Kette



Vorgabe geschätzte Kantenübergangsanzahl $\mu_{i,j}$, für Phasenübergang $\mu_{i.i+1} = 1$. Kantenübergangswahrscheinlichkeiten

$$p_{i,j} = \frac{\mu_{i,j}}{1+\sum_{j=0}^{i} \mu_{i,j}}$$

$p_{S.i}$	Probability that process phase i will be processed.
$(\mu,\xi)_{i,j}$	Expected transition number b_{ij} and fault emergence rate ξ_{ij}.
$\xi_{i,j}$	Generation rate of undetected faults counted on the edge transition $i \rightarrow j$.
$\mu_{i,j}$	Expected number of fallbacks from phase i to phase $j \leq i$ per forward step.
$\#PS$	Number of process phases to be processed.



Die zu erwartende Anzahl der entstehenden Fehler je Simulationsschritt k ist Summe für alle Kanten und je Kante Produkt aus Zustandswahrscheinlichkeit, Übergangswahrscheinlichkeit und Fehlerentstehungsrate:

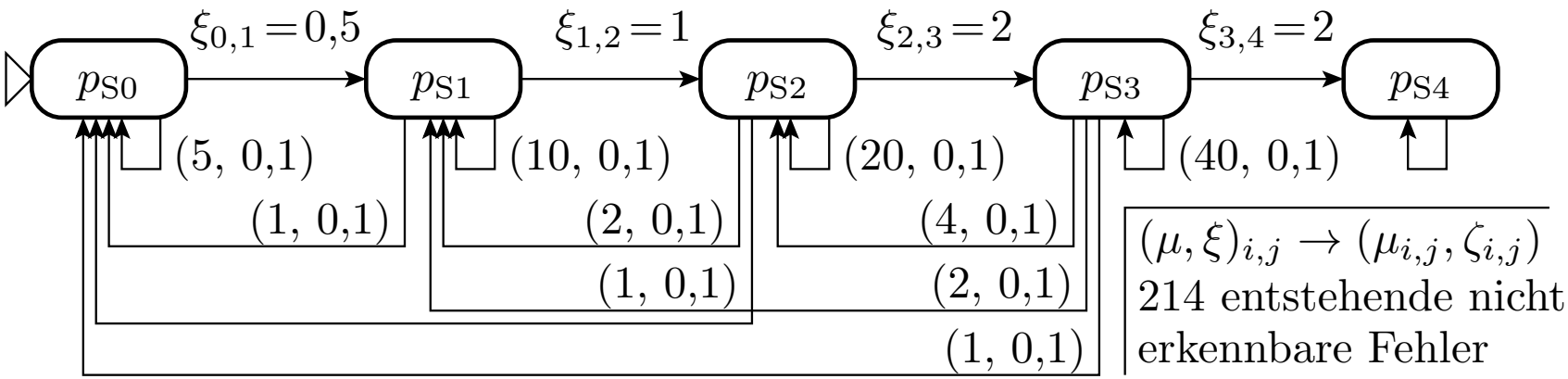
$$\mu_{\mathrm{FS}}(k) = \sum_{i=0}^{\#PS-1} p_{\mathrm{S}.i}(k) \cdot \sum_{j=0}^{i} \xi_{i,j} \cdot p_{i,j}$$

Aufsummiert für alle n Simulationsschritte:

$$\mu_{\mathrm{FS}} = \sum_{k=1}^{n} \mu_{\mathrm{FS}}(k)$$

$\mu_{\mathrm{FS}}(k)$	Expected number of all faults emerging in simulation step k.
μ_{FS}	Expected total number of emerging faults.

3.123 Beispiel

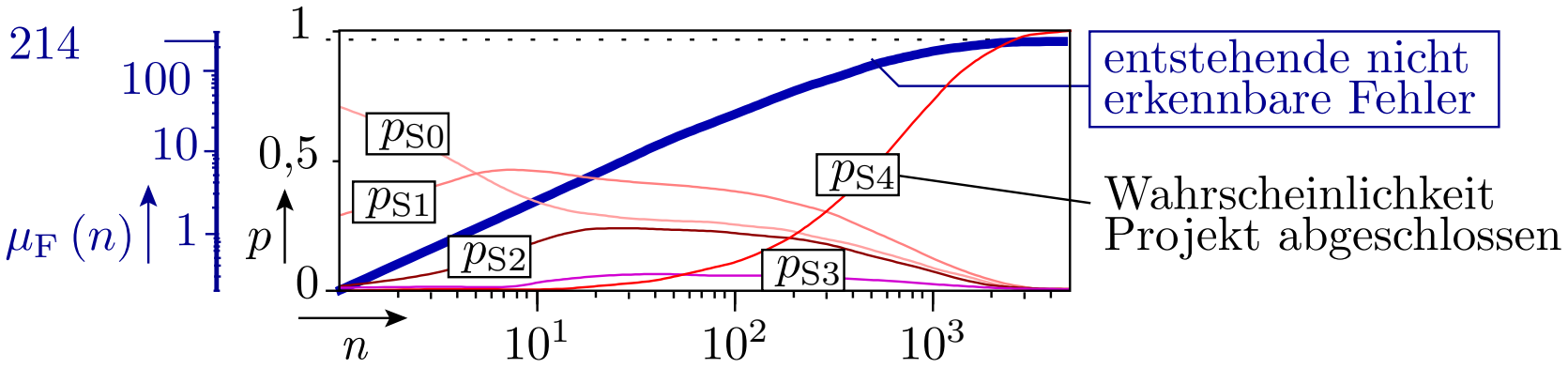


Übergangsmatrix der Markov-Kette und Zunahme der Fehleranzahl:

$$\begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \\ p_{S4} \end{pmatrix}_{n+1} = \begin{pmatrix} \frac{5}{6} & \frac{1}{12} & \frac{1}{24} & \frac{1}{48} & 0 \\ \frac{1}{6} & \frac{10}{12} & \frac{2}{24} & \frac{2}{48} & 0 \\ 0 & \frac{1}{12} & \frac{20}{24} & \frac{4}{48} & 0 \\ 0 & 0 & \frac{1}{24} & \frac{40}{48} & 0 \\ 0 & 0 & 0 & \frac{1}{48} & 1 \end{pmatrix} \cdot \begin{pmatrix} p_{S0} \\ p_{S1} \\ p_{S2} \\ p_{S3} \\ p_{S4} \end{pmatrix}_{n}$$

$p_{S.i}$ Probability that process phase i will be processed.
n Step number of the Markov chain simulation.

3.124 Ergebnis der Beispielsimulation

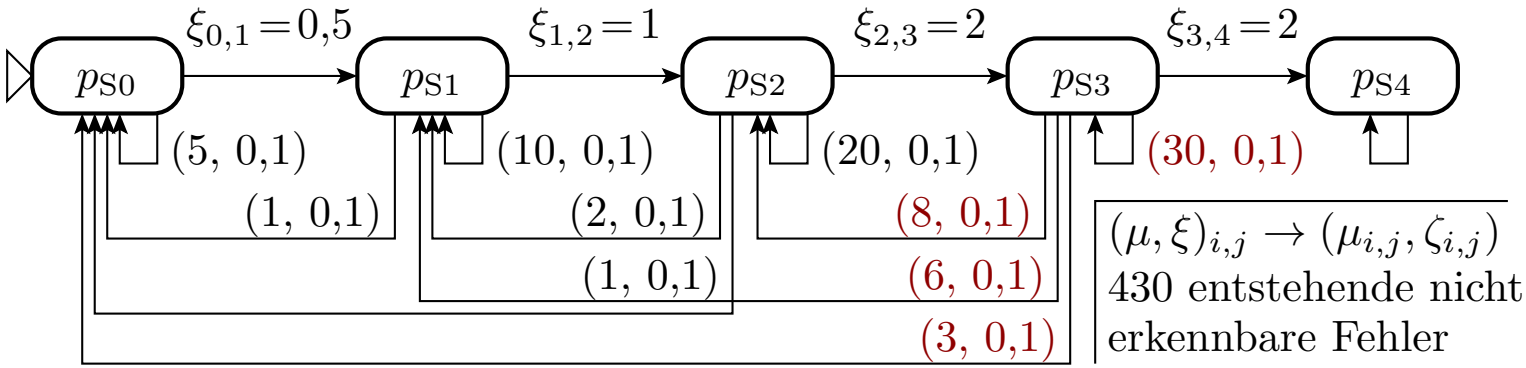


Die berechneten Zustandswahrscheinlichkeiten als Funktions des Projektfortschritts n sind die Wahrscheinlichkeiten, welche Phase gerade bearbeitet oder nachbearbeitet wird. Das sind für reale Projektabläufe zuverlässig bestimmbare Größen.

Praktisch könnte man die Zeiten für die (Nach-) Bearbeitung der Phasen über die Projektdauer mitschreiben und die Markov-Kette so anpassen, dass sie ähnliche Werte liefert. In einem zweiten Schritt könnten die Fehlerentstehungsraten an die Anzahlen der beseitigten und nicht beseitigten Fehler in den Phasenergebnisse angepasst werden.

p_{Si} Probability that the creation process is in stage i.
$\mu_F(n)$ Accumulated number of all faults emerging up to simulation step n.

3.125 Erhöhung der Rückgrifftiefe und Anzahl



Erhöhung der Häufigkeit nachträglicher Änderungen nach Stufe S_3:

$p_{3.3}$:	$\frac{40}{48}$	$\to$	$\frac{30}{48}$	
$p_{3.2}$:	$\frac{4}{48}$	$\to$	$\frac{8}{48}$	(verdoppelt)
$p_{3.1}$:	$\frac{2}{48}$	$\to$	$\frac{6}{48}$	(verdreifacht)
$p_{3.0}$:	$\frac{1}{48}$	$\to$	$\frac{3}{48}$	(verdreifacht)
μ_{CF} :	214	$\to$	450	(mehr als verdoppelt)

Mehr als doppelte zu erwartenden Anzahl entstehender Fehler. Untermauerung der empirischen Annahme, dass die fehlerbezogenen Kosten (fehlgeleiteter Entwicklungsaufwand, Beseitigungskosten, ...) **exponentiell mit der Phasenanzahl** zwischen Fehlerentstehung und Erkennen zunehmen (slide 7.139).

3.126 Zusammenfassung

An zwei Beispielen wurde gezeigt, wie sich Wissen über den Entstehungsfluss für eine genauere Modellierung der Fehlerentstehung und letztendlich auch der Fehlervermeidung nutzen lässt.

Für lineare Entstehungsabläufe aus Schritten und Kontrollen eignen sich **Zählwertzuordnungsgraphen**, aus denen sich Fehleranteil und Ausbeute abschätzen lassen.

Prozesse mit Nachbesserungsiterationen lassen sich durch **Markov-Ketten mit Kantenzählern** beschreiben. Damit simulierbar, wie nachträgliche Änderung den Entwurfsfortschritt bremsen und die zu erwartende Fehleranzahl erhöhen.

Auch wenn das beispielhafte Modell noch erheblicher Nachbesserungen bedarf, um Projektfortschritt und Fehlerentstehung wirklichkeitsnahe nachzubilden, veranschaulicht es schon recht gut, wie und warum sich der Nacharbeitsaufwand und die Anzahl der dabei neu entstehenden Fehler mit der **Anzahl der Phasen** zwischen Fehlerentstehung und Erkennen erhöht.