Test und Verlässlichkeit Foliensatz 4: Fehleranzahl, Fehlfunktionsrate und Ausfallverhalten eingesetzter IT-Systeme

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_F4)

June 17, 2020

Inhalt Foliensatz TV_F4: Fehleranzahl, Fehlfunktionsrate, Schadenskosten und Ausfallverhalten eingesetzter IT-Systeme

Nachweislänge

Wiederholung Zufallstest

Nachweiswahrscheinlichkeit

Wenn ein Fehler von allen Testschritten mit derselben Wahrscheinlichkeit $p_i = \zeta_i$ nachgewiesen wird[1], mindestens ein Nachweis bei Testsatzlänge n:

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

Mit der Taylor-Reihe

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

Für den für die Testauswahl interessierender Bereich[2] $p_i \ll 1$:

$$p_i(n) = 1 - \mathrm{e}^{-n \cdot p_i} \tag{1}$$

[1] Das gilt genaugenommen nur für Systeme ohne Gedächtnis, ist aber auch für die meisten Fehler in Systemen mit Gedächtnis und für Fehler, die ein zusätzliches Speicherverhalten bewirken, als Näherung geeignet (vergl. Foliensatz 2, Abschn 2.2. Fehlernachweis mit Gedächtnis).

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

Verteilung

Verteilung der Nachweislänge für bekanntes ζ_i

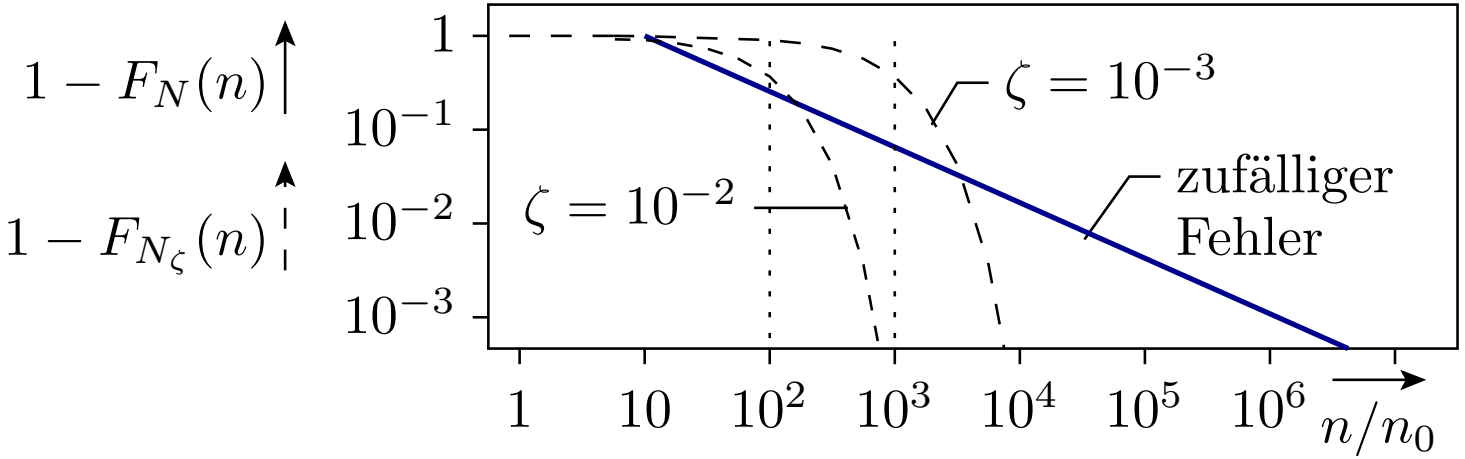
Die Verteilungsfunktion der Nachweislänge N beschreibt die Wahrscheinlichkeit, dass die Anzahl der zufällig ausgewählten Tests N mit einer $\mathrm{FF\text{-}Rate}\ \zeta$ in FF/SL nicht größer als n SL. Für einen Fehler mit FF-Rate $\zeta_i = p_i$ gleich $p_i\,(n)$ nach Gl. 1:

$$F_{N_i}\,(n) = \mathbb{P}\,[N_i \leq n] = 1 - \mathrm{e}^{-\zeta_i \cdot n}$$

Exponentialverteilung $N \sim \mathrm{Exp}\,(\zeta)$ mit Erwartungswert:

$$\mathbb{E}\,[N_i] = \frac{1}{\zeta_i}$$

Verteilung der Nachweislänge realer Systeme



Die Verteilungsfunktion der Nachweislänge realer Fehler in realen Systems tendiert zu einer Pareto-Verteilung (vergl. Foliensatz 1, Abschn. 3.4 Fehlerüberdeckung und FF-Rate):

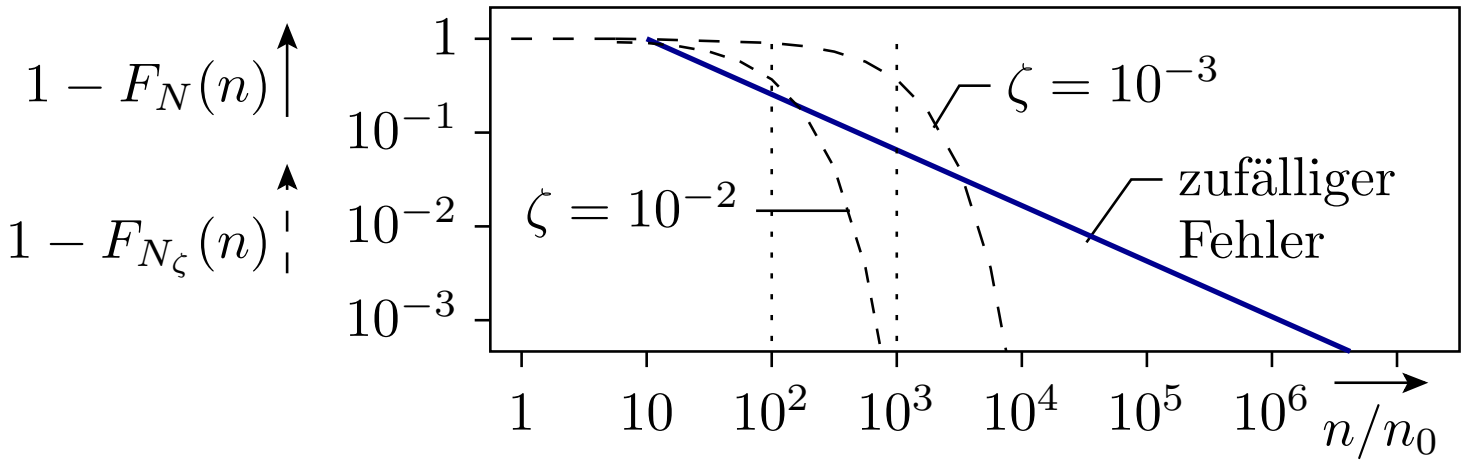
$$F_N(n) = \mathbb{P}[N \leq n] = 1 - \left(\frac{n}{n_0}\right)^{-k} \quad \text{mit } n \geq n_0;\ 0 < k < 1 \tag{2}$$

(n_0 – Mindestnachweislänge vorgelagerter Tests[3]) und ist eine Mischverteilung der Nachweislängen für alle potentiellen Werte von ζ_i, gewichtet mit der Dichtefunktion der FF-Rate $h(\zeta)$.

[3] Fehler mit kürzerer Nachweislänge zählen als vorab beseitigt und n_0 Tests als zusätzlich durchgeführt.

Schätzen der FFR-Dichte

FFR-Dichte bei pareto-verteilter Nachweislänge

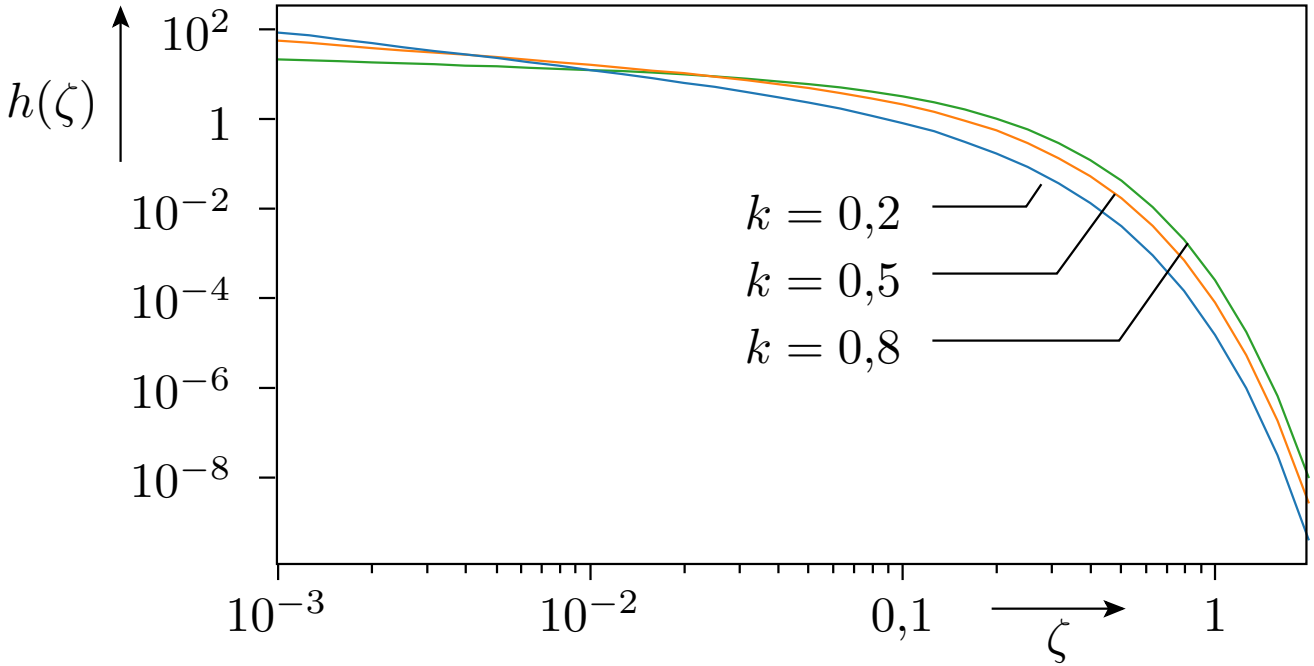


$$F_{N_i}(n) = 1 - \mathrm{e}^{-\zeta_i \cdot n}$$

$$F_N(n) = 1 - \left(\frac{n}{n_0}\right)^{-k} = 1 - \int_0^\infty h(\zeta) \cdot \mathrm{e}^{-(n-n_0)\cdot\zeta} \cdot d\zeta$$

Bezugstestsatzlänge n_0 rechnet hier als bereits durchgeführte Tests.
Die FFR-Dichte $h(\zeta)$ ergibt sich über folgende Bedingung:

$$\left(\frac{n}{n_0}\right)^{-k} = \int_0^\infty h(\zeta) \cdot \mathrm{e}^{-(n-n_0)\cdot\zeta} \cdot d\zeta$$



Lösung: gamma-verteilte FF-Rate $\zeta \sim \mathcal{G}(k, n_0)$. Dichtefunktion:

$$h(\zeta) = \mathrm{e}^{-n_0 \cdot \zeta} \cdot \zeta^{k-1} \cdot \frac{n_0^k}{\Gamma(k)},\ 0 < \zeta \tag{3}$$

Probe:

$$\int_0^\infty e^{-(n-n_0)\cdot\zeta} \cdot \mathrm{e}^{-n_0 \cdot \zeta} \cdot \zeta^{k-1} \cdot \frac{n_0^k}{\Gamma(k)} \cdot \mathrm{d}\zeta \stackrel{!}{=} \left(\frac{n}{n_0}\right)^{-k}$$

$$\int_0^\infty \mathrm{e}^{-(n-n_0)\cdot\zeta} \cdot \mathrm{e}^{-n_0\cdot\zeta} \cdot \zeta^{k-1} \cdot \frac{n_0^k}{\Gamma(k)} \cdot \mathrm{d}\zeta \stackrel{!}{=} \left(\frac{n}{n_0}\right)^{-k}$$

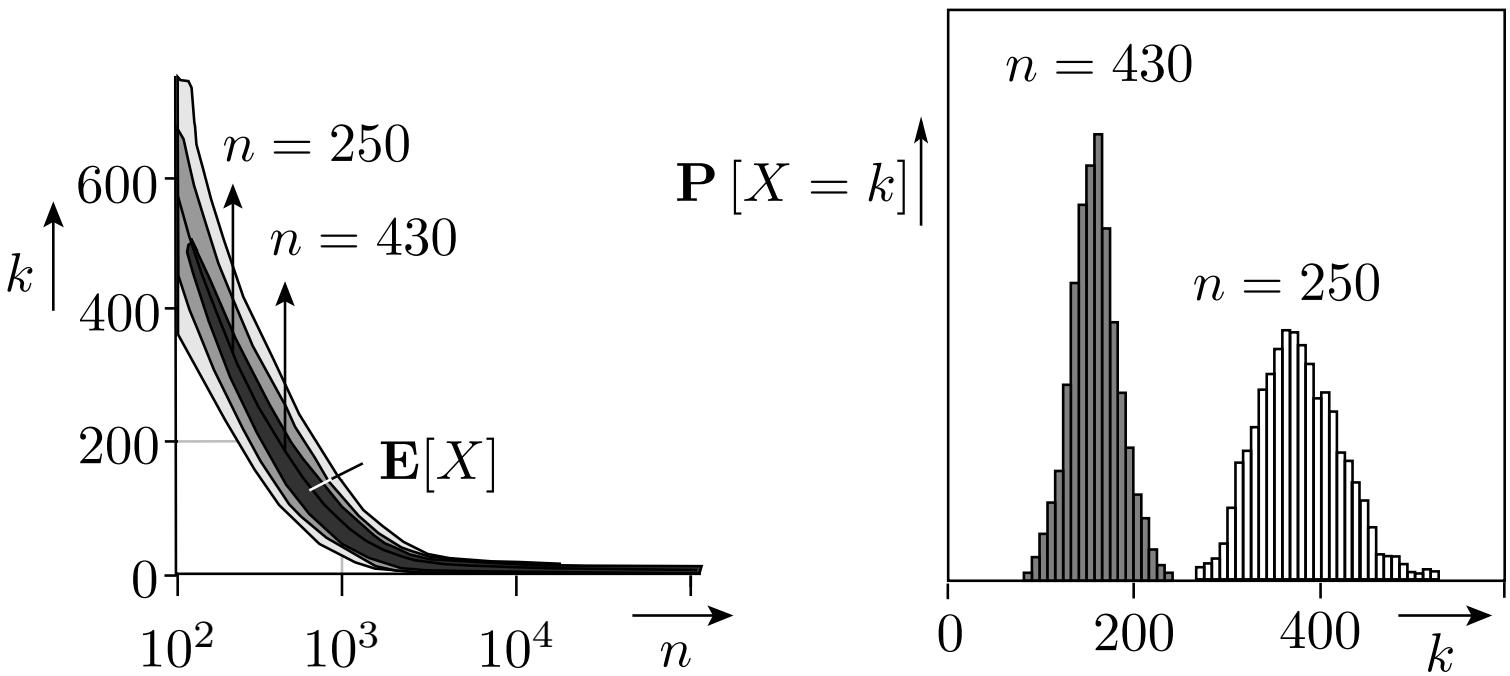
Substitution $z = n \cdot \zeta$, $\mathrm{d}\zeta = \frac{\mathrm{d}z}{n}$

$$\int_n^\infty \mathrm{e}^{-z} \cdot \left(\frac{z}{n}\right)^{k-1} \cdot \frac{n_0^k}{\Gamma(k)} \cdot \frac{\mathrm{d}z}{n} \stackrel{!}{=} \left(\frac{n}{n_0}\right)^{-k}$$

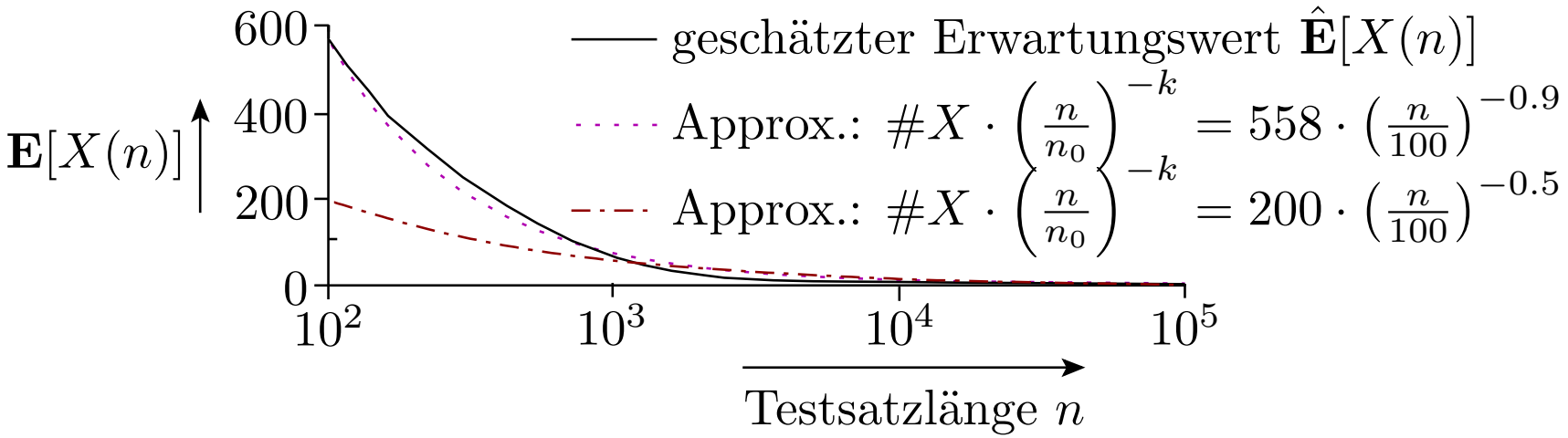
$$\frac{n_0^k}{n^k} \cdot \frac{1}{\Gamma(k)} \cdot \underbrace{\int_0^\infty \mathrm{e}^{-z} z^{k-1} \mathrm{d}z}_{\Gamma(k)} = \left(\frac{n}{n_0}\right)^{-k} \surd$$

Für das Haftfehlerexperiment

Kombinatorische Beispielschaltung (Benchmark c3540). 3606 simulierte, unterschiedlich nachweisbare Haftfehler. Zählwert X ist die Anzahl der nicht nachweisbaren Haftfehler. Abschätzung von $\mathbb{P}[X = k]$ aus einer Stichprobe von $\#w = 1000$ Zählwerten für verschiedenen Zufallstestsätze der Länge n.



Annäherung $\mathbb{E}(X(n))$ durch $\#F \cdot \left(\frac{n}{n_0}\right)^{-k}$



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

Es gibt sicher bessere Approximationen, z.B. Mischverteilungen unterschiedlicher Pareto-Verteilungen, aber das prinzipielle Verhalten lässt sich auch mit einer einfachen Pareto-Verteilung zeigen.

Fehleranzahl

Entstehende Fehler

Entstehende Fehler

- Einfaches Abschätzungsmodell über Metriken, z.B. »Anz_NLOC * Fehler_je_NLOC«.
- Näher am Entstehungsprozess »Anz_Pozessschritte * Prozessgüte«:

$$\mu_{\mathrm{E}} = \mathbb{E}\left[X_{\mathrm{E}}\right] = \#E \cdot \zeta_{\mathrm{E}} \tag{4}$$

(X_{E} – Anzahl der entstehenden Fehler; μ_{E} – Erwartungswert von X_{E}; $\#E$ – Anzahl der Entstehungsschritte; ζ_{E} – Fehlerentstehungsrate je Entstehungsschritt). Entstehungsprozesse reifen vor ihren Einsatz soweit, dass

- die Fehlerentstehungsrate je Prozessschritt sehr klein ist $\zeta_{\mathrm{E}} \ll 1$
- und keine Entstehungsursache stark dominiert.

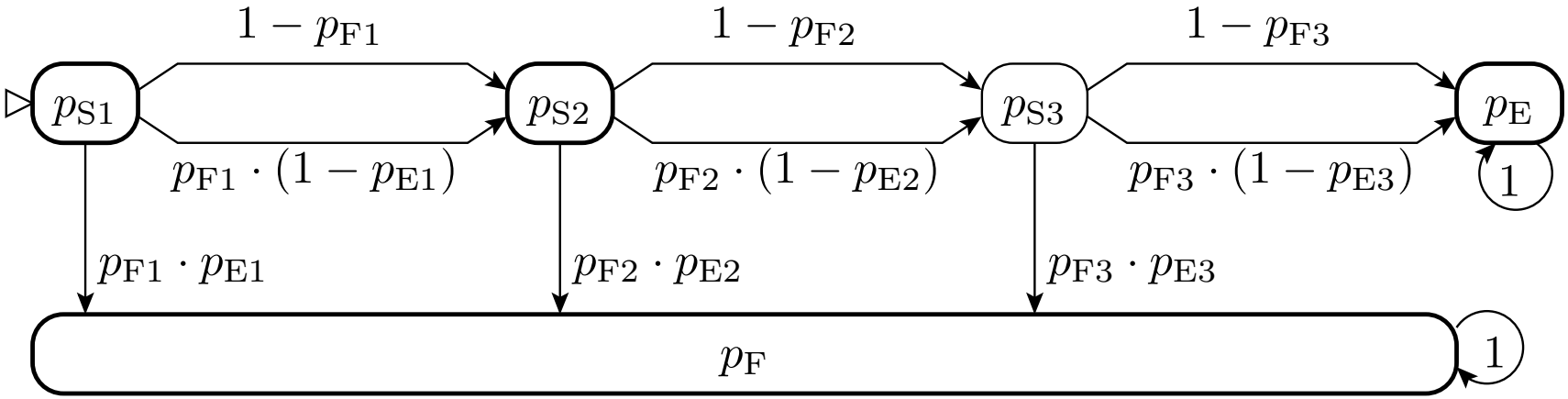
Dadurch ist X_{E} für kleine μ_{E} typisch poisson- und für größere μ_{E} normalverteilt:

$$X_{\mathrm{E}} \sim \begin{cases} \mathrm{Pois}\left(\mu_{\mathrm{E}}\right) & \mu_{\mathrm{E}} < 10 \\ \Phi\left(\mu_{\mathrm{E}}, \sigma = \sqrt{\kappa \cdot \mu_{\mathrm{E}}}\right) & \mu_{\mathrm{E}} \geq 10 \end{cases} \tag{5}$$

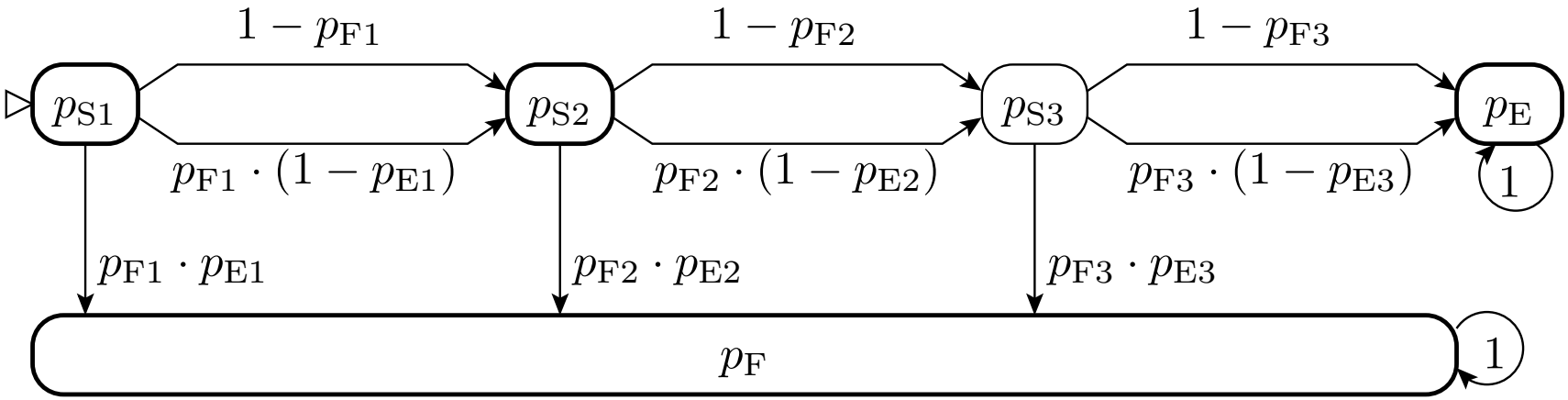
κ – Varianzerhöhung durch Abhängigkeiten bei der Fehlerentstehung.

Entstehungsprozesse mit Kontrollen

Lineare Folge von Entstehungsschritten. Wenn die Kontrolle i einen Fehler erkennt, wird das Objekt aussortiert, sonst Übergang zum nächsten Schritt ohne oder mit nicht erkennbarem entstandenen Fehler:



p_{Si} Wahrscheinlichkeit, dass Schritt i abgearbeitet wird.
p_{Fi} Wahrscheinlichkeit, dass in Schritt i ein Fehler entsteht.
p_{Ei} Fehlererkennungswahrscheinlichkeit der Kontrolle nach Schritt i.
p_E Wahrscheinlichkeit, dass ein als fehlerfrei geltendes Objekt entsteht.
p_F Wahrscheinlichkeit, dass das Objekt als fehlerhaft aussortiert wird.



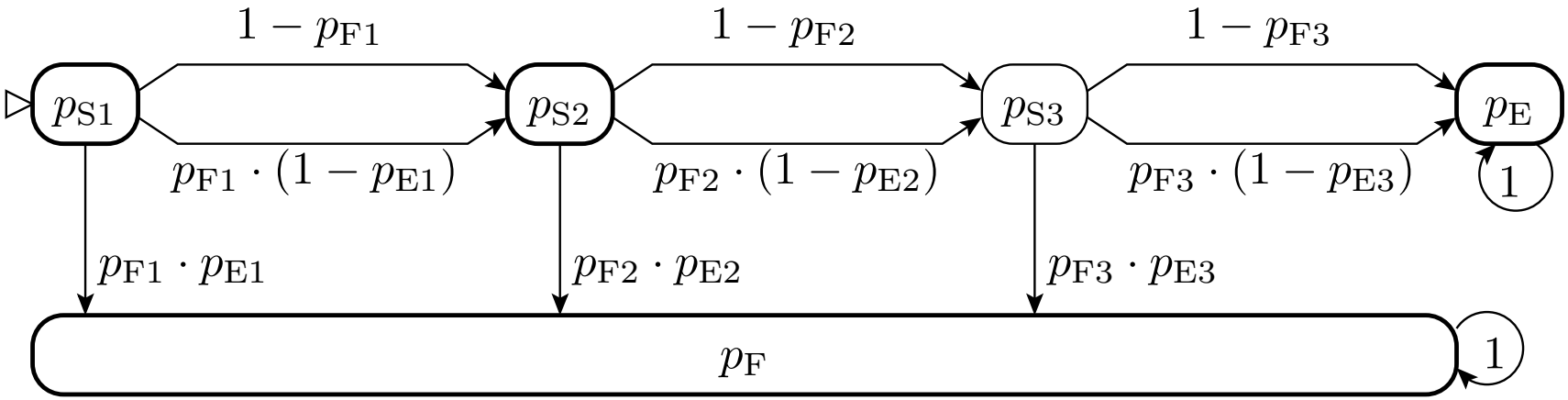
Wahrscheinlichkeit, dass das Objekt nicht aussortiert wird:

$$p_E = \prod_{i=1}^{\#E} (1 - p_{Ei} p_{Fi})$$

Fehleranzahl in den als fehlerfrei geltenden Objekten: Für nicht aussortierte Objekte gilt in Schritt $i \in \{1, 2, 3\}$ $p_{S.i} = 100\%$ und danach $p_E = 100\%$. In Jedem Schritt $i \in \{1, 2, 3\}$ entsteht mit $p_{Fi} \cdot (1 - p_{Ei})$ ein nicht erkennbarer Fehler[4]:

$$\mu_E = \sum_{i=1}^{\#E} (p_{Fi} \cdot (1 - p_{Ei}))$$

[4] Zählen der Kantenübergangswahrscheinlichkeiten unter der Zusatzbedingung $p_{S.i}$ genau in einem Schritt 100 und sonst 0.



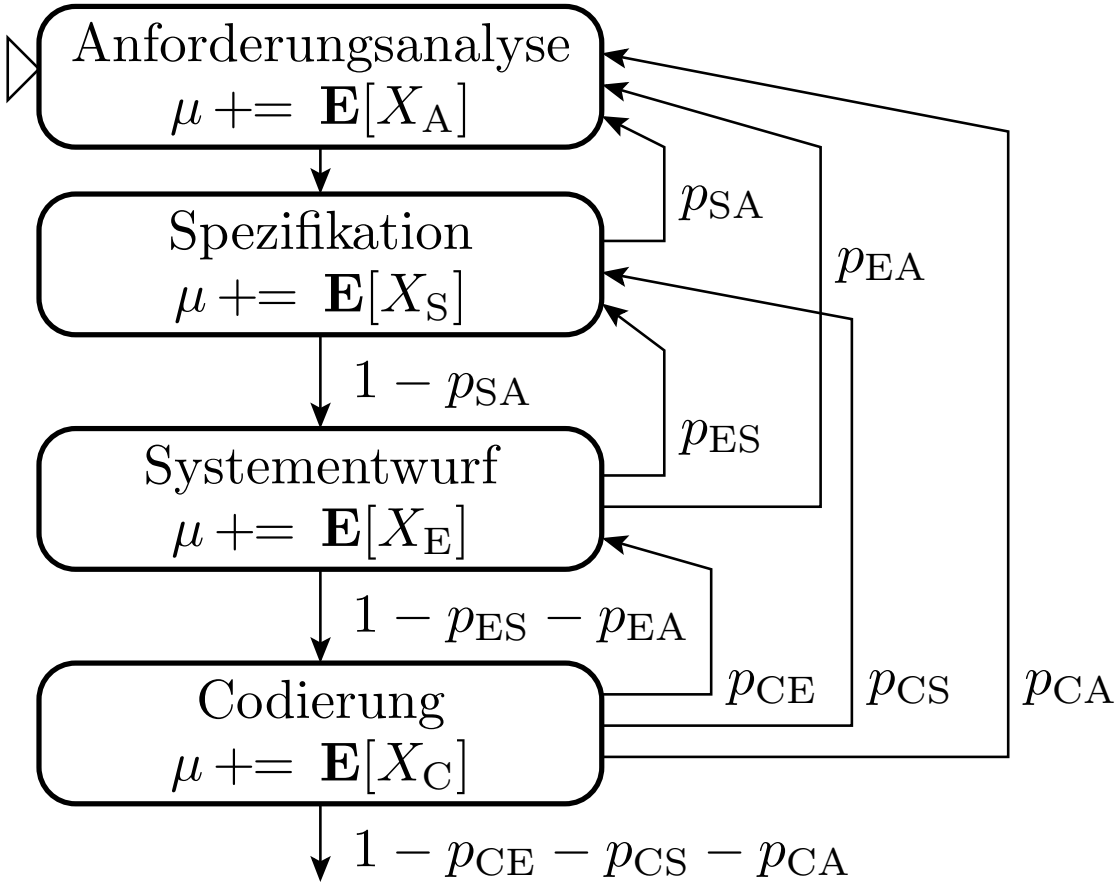
$$\mu_E = \sum_{i=1}^{\#E} (p_{Fi} \cdot (1 - p_{Ei}))$$

Im Vergleich zu Gl. 4 $\#E \cdot \zeta_E$ für eine Abfolge von Entstehungsschritten ohne Kontrolle und Aussortieren, summieren sich hier statt der Fehlerentstehungsraten $\zeta_{Ei} = p_{Fi}$ (mal Fehler je Entstehungsschritt), die Raten der entstehenden und nicht erkennbaren Fehler.

Vorteil von »Kontrolle nach Zwischenschritten und Aussortieren« sind:

- kein weiterer Entstehungsaufwand für erkannten Ausschuss und
- oft höhere erzielbare FC für die gerade entstandenen Fehler.

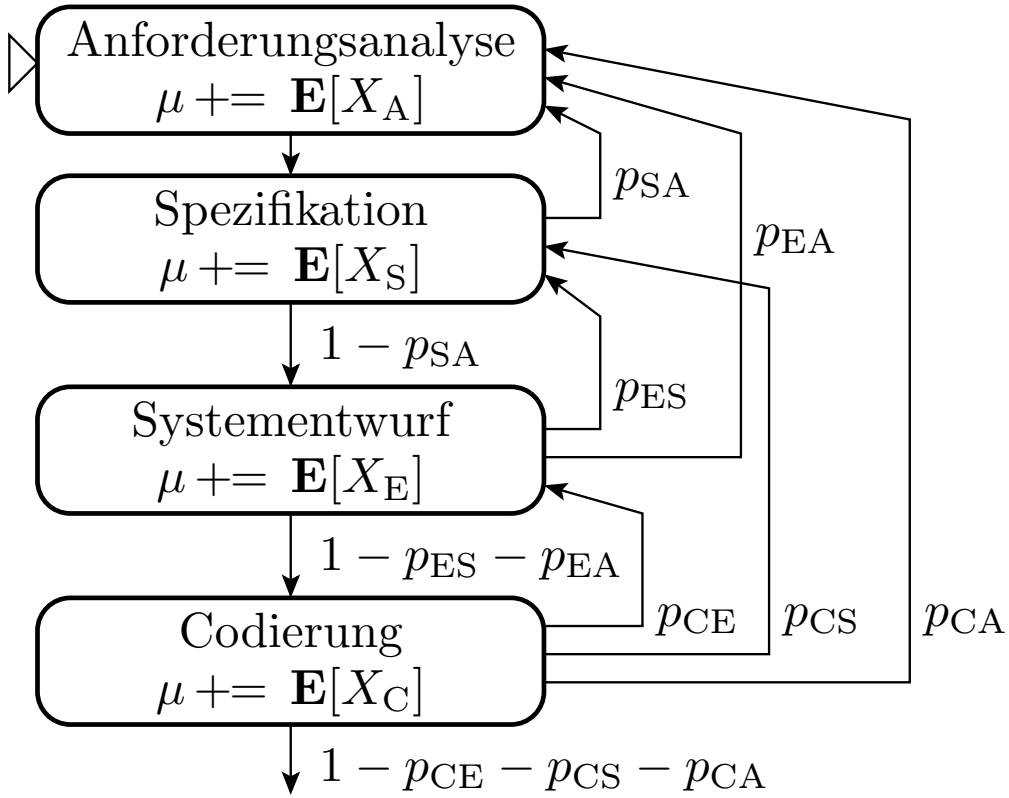
Entstehungsprozesse mit Rückgriffen



μ – Zähler für die zu erwartende Anzahl der entstehenden Fehler; $\mathbb{E}[X_i]$ – zu erwartende Anzahl entstehender Fehler in Entwurfsphase i;
p_{ij} – Rückgriffswahrscheinlichkeiten[4] von i nach j.

[4] Rückgriff: Wiederholung von Entwurfsschritten vorheriger Entwurfsphasen, wenn in späteren Phasen Fehler (oder Unschönheiten) erkannt werden.

Eine Simulation dieser vereinfachten Markov-Kette eines Phasenmodells wird zeigen, dass eine Erhöhung der Rückgriffwahrscheinlichkeiten insbesondere über mehrere Entwurfsphasen die zu erwartende Anzahl der entstehenden Fehler ab einem bestimmten Punkt explosionsartig in die Höhe schnellen lassen.



Dabei haben wir noch nicht berücksichtigt, dass die Rückgriffwahrscheinlichkeiten mit der Anzahl der entstehenden Fehler zunehmen. Vorgehensmodelle schränken deshalb Rückgriffsmöglichkeiten ein (vergl. TV_F1, Abschn. 4.3 Projekte, Vorgehensmodelle).

Fehleranzahl im Einsatz

Statische und fehlerorientiert ausgewählte Tests

Statische und fehlerorientiert ausgewählte dynamische Tests erkennen Fehler mit einer Erkennungswahrscheinlichkeit gleich der Fehlerüberdeckung $p_{\mathrm{E}} = FC_{\mathrm{S}}$. Erkannte Fehler werden beseitigt, aber bei der Beseitigung erkannter Fehler entstehen neue Fehler, und bei der Beseitigung der erkannten neuen Fehler entstehen wieder neue Fehler (vergl. Foliensatz 2, 3.4 Reparaturiteration):

$$\mathbb{E}\left[\#F_{\mathrm{TB}}\right] = \frac{\mathbb{E}\left[\#F\right] \cdot (1 - p_{\mathrm{E}})}{1 - \frac{p_{\mathrm{E}}}{Q_{\mathrm{Rep}}}} \tag{6}$$

(Q_{Rep} – Reparaturgüte in beseitigte Fehler je neu entstehender Fehler). Gezielt für Fehler gesuchte Tests sind für unberücksichtigte Fehlermöglichkeiten Zufallstests. Die Anzahl der fehlerorientiert ausgewählten Tests ist somit die Bezugstestsatzlänge n_0 nach Beseitigung der mit statischen und fehlerorientiert ausgewählten dynamischen Tests erkannten Fehler in Gl. 3:

$$h(\zeta) = \mathrm{e}^{-n_0 \cdot \zeta} \cdot \zeta^{k-1} \cdot \frac{n_0^k}{\Gamma(k)}$$

Zufallstest

Sich an die statischen gezielt berechneten anschließende Zufallstests verringert bei einer parato-verteilten FFR-Dichte nach Gl. 2 die Nichterkennungswahrscheinlichkeit $(1 - p_{\mathrm{E}}) \sim n^{-k}$ auf $(1 - FC_{\mathrm{S}}) \cdot \left(\frac{n}{n_0}\right)^{-k}$. Mit der der Näherung $1 - (1 - p_{\mathrm{E}}) \cdot \left(\frac{n}{n_0}\right)^{-k} = 1$ verringert sich die Anzahl der nicht nachweisbaren Fehler nach Gl. 6 auf:

$$\mathbb{E}\left[\#F_{\mathrm{TB}}\right] = \frac{\mathbb{E}\left[\#F\right] \cdot (1 - FC_{\mathrm{S}}) \cdot \left(\frac{n}{n_0}\right)^{-k}}{1 - Q_{\mathrm{Rep}}^{-1}} \quad \text{mit } n \geq n_0, \quad 0 < k < 1 \qquad (7)$$

und erhöhen die Testsatzlänge in Gl. 3 um $n - n_0$ auf n:

$$h(\zeta) = \mathrm{e}^{-n \cdot \zeta} \cdot \zeta^{k-1} \cdot \frac{n^k}{\Gamma(k)} \qquad (8)$$

(FC_{S} – Fehlerüberdeckung der statischen und fehlerorientiert ausgewählten Tests; n_0– Testsatzlänge der fehlerorientiert ausgewählten Tests; n – effektive Testsatzläge aller Tests zusammen; Q_{Rep} – Reparaturgüte in beseitigte Fehler je neu entstehender Fehler).

Effektive Testsatzlänge und Reifeprozess

Die Anzahl der ganzheitlichen Tests n_{G} geht mit Wichtung 1 und die der Modultests n_{M} tendentiell mit einer Wichtung c$\gg 1$ in die effektive Testsatzlänge ein (vergl. Foliensatz 2, Abschn. 2.4 Isolierter Test):

$$n = n_{\mathrm{G}} + c \cdot n_{\mathrm{M}}$$

Ein sich an die Herstellertests anschließender Reifeprozess verlängert die effektive Testsatzlänge weiter auf:

$$n = n_{\mathrm{G}} + c \cdot n_{\mathrm{M}} + p_{\mathrm{BR}} \cdot n_{\mathrm{U}} \tag{9}$$

(n_{U} – Anzahl genutzter SL durch alle Nutzer zusammen; p_{BR} – Wahrscheinlichkeit, dass eine bei Anwendern beobachtete FF eine Beseitigung des verursachenden Fehlers bewirkt, (vergl. Foliensatz 2, Abschn. 4 Fehlerbeseitigungswahrscheinlichkeit in Reifeprozessen).

Verteilung der Fehleranzahl

Erwartungswert nach Gl. 7;

$$\mu_{\mathrm{T}} = \mathbb{E}\left[\#F_{\mathrm{TB}}\right] = \frac{\mathbb{E}\left[\#F\right] \cdot (1 - FC_{\mathrm{S}}) \cdot \left(\frac{n}{n_0}\right)^{-k}}{1 - Q_{\mathrm{Rep}}^{-1}} \quad \text{mit } n \geq n_0;\ k > 0$$

Abnahme mit $\sim n^{-k}$. Implizit getroffene Annahmen:

- Beseitigung alle durch alle statischen Tests, fehlerorientierten Tests und Zufallstests nachweisbaren Fehler, auch für die bei Reparaturen neu entstehenden Fehler.
- verlangt nach jedem Reparaturschritt die Wiederholung aller Tests. Nur eingeschränkt praktikabel.

Abschätzung wahrscheinlicher Bereiche über Poisson- bzw. Normalverteilung:

$$X_{\mathrm{T}} \sim \begin{cases} \mathrm{Pois}\left(\mu_{\mathrm{T}}\right) & \mu_{\mathrm{T}} < 10 \\ \Phi\left(\mu, \sigma = \sqrt{\kappa \cdot \mu_{\mathrm{T}}}\right) & \mu_{\mathrm{T}} \geq 10 \end{cases}$$

(κ – Varianzehöhung durch Abhängigkeiten bei der Fehlerentstehung und beim Fehlernachweis).

Beispielabschätzung

Softwaresystem 10^5 NLOC, Fehlerentstehungsrate 30 Fehler auf 1000 NLOC, Fehlerüberdeckung der statischen und geziel berechneten Tests $FC_{\mathrm{S}} = 80\%$. Anzahl der gezielt berechneten Tests $n_0 = 100$. Anzahl der zusätzlichen Zufallstests $10^6 - 100$, Reparaturgüte $Q_{\mathrm{Rep}} = 3$ beseitigte Fehler je neu entstehender Fehler. Formfaktor der Pareto-Verteilung der Nachweislänge der Verteilung der Nachweislänge $k = 0{,}2 \ldots 0{,}4$.

a) Zu erwartende Fehleranzahl aus dem Entstehungsprozess.

b) Zu erwartende Fehleranzahl aus dem Reparaturprozess.

c) Zu erwartende Fehleranzahl zum Einsatzbeginn.

d) Wahrscheinlicher Bereich der Fehleranzahl im eingesetzten System bei Irrtumswahrscheinlichkeit $\alpha = 2\%$ ohne Berücksichtigung von Abhängigkeiten im Entstehungsprozess ($\kappa = 1$).

---

a) $\mathbb{E}[\#F] = \frac{10^5 \cdot 30}{1.000} = 3000$

b) Erhöhung von $\mathbb{E}[\#F] = 3000$ auf $\frac{\mathbb{E}[\#F]}{1 - Q_{\mathrm{Rep}}^{-1}} = \frac{3000}{1 - \frac{1}{3}} = 4500$; 1500 zusätzliche bei der Reparatur entstehende Fehler.

Softwaresystem 10^5 NLOC, Fehlerentstehungsrate 30 Fehler auf 1000 NLOC, Fehlerüberdeckung der statischen und geziel berechneten Tests $FC_{\mathrm{S}} = 80\%$. Anzahl der gezielt berechneten Tests $n_0 = 100$. Anzahl der zusätzlichen Zufallstests $10^6 - 100$, Reparaturgüte $Q_{\mathrm{Rep}} = 3$ beseitigte Fehler je neu entstehender Fehler. Formfaktor der Pareto-Verteilung der Nachweislänge der Verteilung der Nachweislänge $k = 0{,}2 \ldots 0{,}4$.

c) Zu erwartende Fehleranzahl zum Einsatzbeginn.

$$\begin{aligned}
\mathbb{E}\left[\#F_{\mathrm{TB}}\right] &= \frac{\mathbb{E}\left[\#F\right] \cdot (1 - FC_{\mathrm{S}}) \cdot \left(\frac{n}{n_0}\right)^{-k}}{1 - Q_{\mathrm{Rep}}^{-1}} \\
&= \frac{3000 \cdot (1 - 80\%) \cdot \left(\frac{10^6}{100}\right)^{-(0{,}2 \ldots 0{,}4)}}{1 - \frac{1}{3}} \\
&= 23 \ldots 143
\end{aligned}$$

Ohne Kenntnis des Formfaktors k sind nur ungenaue Schätzungen möglich.

Softwaresystem 10^5 NLOC, Fehlerentstehungsrate 30 Fehler auf 1000 NLOC, Fehlerüberdeckung der statischen und geziel berechneten Tests $FC_{\mathrm{S}} = 80\%$. Anzahl der gezielt berechneten Tests $n_0 = 100$. Anzahl der zusätzlichen Zufallstests $10^6 - 100$, Reparaturgüte $Q_{\mathrm{Rep}} = 3$ beseitigte Fehler je neu entstehender Fehler. Formfaktor der Pareto-Verteilung der Nachweislänge der Verteilung der Nachweislänge $k = 0{,}2 \ldots 0{,}4$.

d) Wahrscheinlicher Bereich der Fehleranzahl im eingesetzten System bei Irrtumswahrscheinlichkeit $\alpha = 2\%$ ohne Berücksichtigung von Abhängigkeiten im Entstehungsprozess ($\kappa = 1$).

$$x_{\mathrm{min}} = 23 - \Phi^{-1}\left(1 - \frac{\alpha}{2}\right) \cdot \sqrt{23} = 23 - 2{,}33 \cdot \sqrt{23} = 11{,}8$$

$$x_{\mathrm{max}} = 143 + \Phi^{-1}\left(1 - \frac{\alpha}{2}\right) \cdot \sqrt{143} = 143 - 2{,}33 \cdot \sqrt{143} = 162$$

Die zufälligen Streuungen der Werte sind im Vergleich zu denen durch die ungenaue Kenntnis des Formfaktors k der Pareto-Verteilung der Fehlernachweislänge vernachlässigbar.

FF-Rate im Einsatz

FFR-Dichte je Fehler

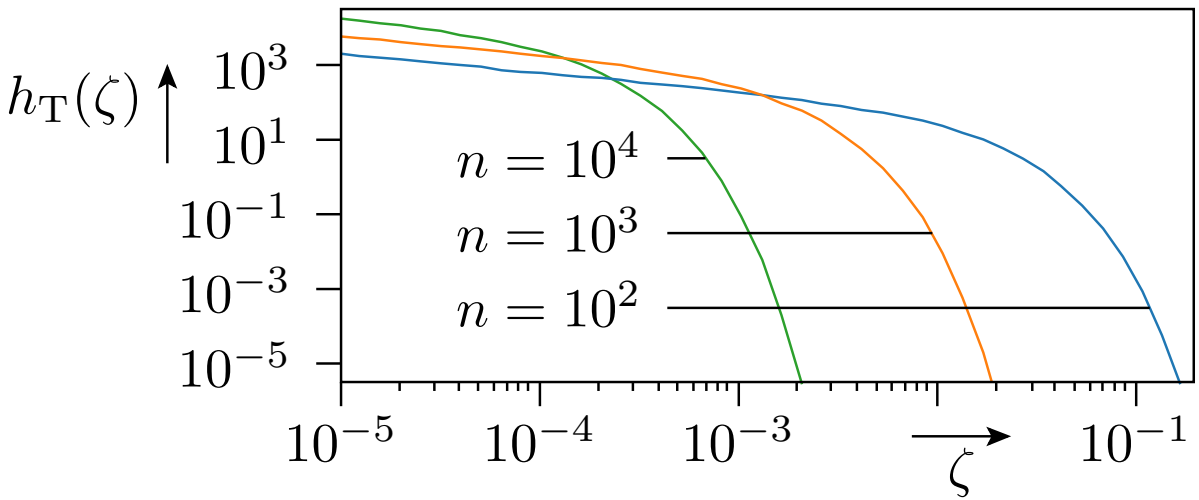
FF-Rate nach Test und Fehlerbeseitigung

FFR-Dichte für eine pareto-verteilte Nachweislänge nach Gl. 8 :

$$h_{\mathrm{T}}(\zeta) = \mathrm{e}^{-n\cdot\zeta} \cdot \zeta^{k-1} \cdot \frac{n^k}{\Gamma(k)}$$

(Gamma-Verteilung) mit der effektiven Testsatzlänge nach Gl. 9

$$n = n_{\mathrm{G}} + c \cdot n_{\mathrm{M}} + p_{\mathrm{BR}} \cdot n_{\mathrm{U}}$$



(k – Formfaktor, $\Gamma(k)$ – Gammafunktion; n_{G} – Anzahl der ganzheitlichen Tests incl. der fehlerorientiert ausgewäglten Tests; ...)

FFR vorhandener Fehler

FFR-Dichte der vorhandenen Fehler im Einsatz

Die Dichte der FF-Rate im Einsatz ist eine Mischverteilung der FFR-Dichten nach der Fehlerbeseitigungsiteration für einen, zwei, ... Fehler gewichtet mit den Wahrscheinlichkeiten, dass das System einen Fehler, zwei Fehler ... enthält:

$$h_{\mathrm{T}}(\zeta) = \sum_{m=1}^{X_{\max}} \mathbb{P}\left[\#F_{\mathrm{TB}} = m\right] \cdot h^{(*m)}(\zeta)$$

Die FFR-Dichte für eine Summe von m Zufallsgrößen ist die m-fache Faltung der Verteilung der Summmanden. Eine Besonderheit der Gamma-Verteilung, dass eine m-fache Faltung wieder eine Gamma-Verteilung ist (verg. Foliensatz 3, Abschn 4.2 Gamma-Verteilung):

$$\mathcal{G}(k,n)^{(*m)} = \mathcal{G}(m \cdot k, n)$$

$$h^{(*m)}(\zeta) = \mathrm{e}^{-n\cdot\zeta} \cdot \zeta^{m\cdot k-1} \cdot \frac{n^{m\cdot k}}{\Gamma(m\cdot k)}$$

$$h_{\mathrm{T}}(\zeta) = \mathrm{e}^{-n\cdot\zeta} \cdot \sum_{m=1}^{X_{\max}} \mathbb{P}\left[\#F_{\mathrm{TB}} = m\right] \cdot \zeta^{m\cdot k-1} \cdot \frac{n^{m\cdot k}}{\Gamma(m\cdot k)}$$

Für die Verteilung der Anzahl der nicht nachweisbaren Fehler kann je nach Erwartungswert eine Poisson-Verteilung oder eine diskrete Annäherung einer Normalverteilung eingesetzt werden ...

Zumindest für die Abschätzung des Erwartungswertes gibt es einen anschaulicheren Weg.

Abschätzung der Varianz, der Verteilung, ... finden Sie in speziellen Mathematikvorlesungen z.B. über Versicherungsmathematik[5].

[5] z.B. Albrecher: Finanz- und Versicherungsmathematik. TU Graz

Zu erwartende FF-Rate

Zu erwartende FF-Rate

Die Anzahl der FF ist die Summe der FF aller $\#F_{\mathrm{TB}}$ Fehler:

$$\zeta = \sum_{i=1}^{\#F_{\mathrm{TB}}} \zeta_i$$

ζ_i hat für alle Fehler dieselbe Verteilung $\Gamma(k,n)$ mit dem Erwartungswert (verg. Foliensatz 3, Abschn 4.2 Gamma-Verteilung)

$$\mathbb{E}\left[\zeta_i\right] = \frac{k}{n}$$

Der Erwartungswert einer zufälligen Anzahl von Zufallsgrößen ist das Produkt der Erwartungswerte:

$$\mathbb{E}\left[\zeta\right] = \mathbb{E}\left[\#F_{\mathrm{TB}}\right] \cdot \frac{k}{n}$$

Mit der zu erwartenden Anzahl den nicht nachweisbaren Fehler in einem eingesetzten System nach Gl. 7

$$\mathbb{E}\left[\zeta\right] = \frac{k \cdot \mathbb{E}\left[\#F\right] \cdot (1 - FC_{\mathrm{S}}) \cdot \left(\frac{n}{n_0}\right)^{-k}}{n \cdot \left(1 - Q_{\mathrm{Rep}}^{-1}\right)}$$

Beispielaufgabe

Die mittlere FF-Rate eines Systems beträgt nach einer Reparaturiteration mit einer effektiven Testlänge von $n = 10^5$ zufälligen SL $\mathbb{E}(\zeta) = 10^{-4}$ FF/SL. Schätzen Sie unter Annahme einer gamma-verteilten FF-Rate mit den Formfaktoren $k \in \{0{,}3, 0{,}4, 0{,}5, 0{,}6, 0{,}7\}$:

1. die zu erwartende Anzahl der nicht beseitigten Fehler für die aktuelle effektive Testlänge von $n = 10^5$,
2. die zu erwartende Anzahl der nicht beseitigten Fehler für die zehnfache effektive Testlänge $n = 10^6$,
3. die zu erwartende FF-Rate für die zehnfache effektive Testlänge $n = 10^6$.

$$\mathbb{E}[\zeta] = \mathbb{E}[\#F_{\mathrm{TB}}] \cdot \frac{k}{n}$$

$$\mathbb{E}[\#F_{\mathrm{TB}}(n)] = \mathbb{E}[\#F_{\mathrm{TB}}(n_0)] \cdot \left(\frac{n}{n_0}\right)^{-k}$$

$$\mathbb{E}[\zeta(n)] = \mathbb{E}[\zeta(n_0)] \cdot \left(\frac{n}{n_0}\right)^{-(k+1)}$$

Lösung

1. Für $\mathbb{E}[\zeta] = \mathbb{E}[\#F_{\mathrm{TB}}] \cdot \frac{k}{n}$ sind gegeben $\mathbb{E}(\zeta) = 10^{-4}$ für $n = 10^5$ und $k \in \{0{,}3, 0{,}4, 0{,}5, 0{,}6, 0{,}7\}$:

$$\mathbb{E}\left[\#F_{\mathrm{TB}},\, n = 10^5\right] = \mathbb{E}\left[\zeta_i,\, n = 10^5\right] \cdot \frac{n}{k} = \frac{10}{k}$$

2. Die zu erwartende Fehleranzahl nimmt mit der Erhöhung der effektiven Testlänge mit Exponent k ab:

$$\mathbb{E}\left[\#F_{\mathrm{TB}}, n = 10^6\right] \quad = \quad \mathbb{E}\left[\#F_{\mathrm{TB}}, n = 10^5\right] \cdot \left(\frac{10^6}{10^5}\right)^{-k} = \frac{10}{k} \cdot 10^{-k}$$

3. Die zu erwartende Fehleranzahl nimmt mit der Erhöhung der effektiven Testlänge mit Exponent $-(k+1)$ ab:

$$\mathbb{E}\left[\zeta, n = 10^6\right] \quad = \quad \mathbb{E}\left[\zeta, n = 10^5\right] \cdot \left(\frac{10^6}{10^5}\right)^{-(k+1)} = 10^{-4} \cdot 10^{-(k+1)}$$

	k=0,3	k=0,4	k=0,5	k=0,6	k=0,7
$\mathbf{E}[\zeta, n = 10^5]$	10^{-4}	10^{-4}	10^{-4}	10^{-4}	10^{-4}
$\mathbf{E}[\#F_{\mathrm{TB}}, n = 10^5]$	26,7	20	16	13,3	11,2
$\mathbf{E}[\#F_{\mathrm{TB}}, n = 10^6]$	13,4	7,96	5,06	3,45	2,28
$\mathbf{E}[\zeta, n = 10^6]$	$5{,}01 \cdot 10^{-6}$	$3{,}98 \cdot 10^{-6}$	$3{,}16 \cdot 10^{-6}$	$2{,}51 \cdot 10^{-6}$	$2{,}00 \cdot 10^{-6}$

- Die FF-Rate eines Systems ist eine auch für den Anwender gut beobachtbare Größe.
- Mit einem Schätzwert für die bisherige effektive Testlänge lässt sich aus der FF-Rate auf die Anzahl der noch vorhandenen Fehler schließen, auch wenn über die Verteilung der FF-Rate wenig bekannt ist.
- Eine Verzehnfachung der effektiven Testlänge, z.B. durch Erhöhung der Reifedauer von 6 Monaten auf 5 Jahre reduziert die Fehlerzahl auf $\frac{1}{2} \ldots \frac{1}{5}$ und die FF-Raten auf $\frac{1}{20} \ldots \frac{1}{50}$.

- Wenn ein System reift, ohne dass dabei mehr neue Fehler eingebaut als alte beseitigt werden (z.B. bei der Einprogrammierung neuer Features), sollte die beobachtbare Fehlerrate deutlich überproportional mit der Nutzungsdauer abnehmen.
- Lange gereifte Systeme erreichen Fehlfunktionsraten / Zuverlässigkeiten, mit denen eine Neuentwicklung nicht konkurieren kann.

Schaden durch FF

Verteilung von Haftpflichtschäden

Haftpflichtschäden über 100.000 SF (SF – Schweizer Franken) einer Schweizer Autoversicherung[6]:

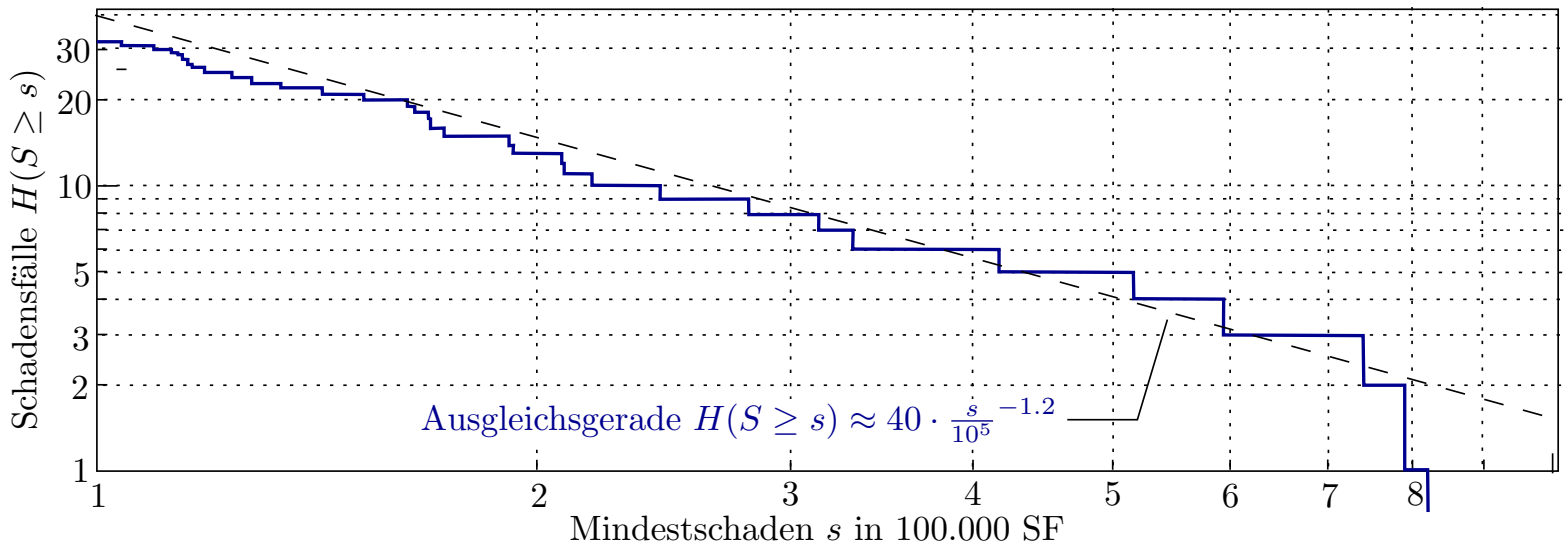
```
103.765, 109.168, 112.341, 113.800, 114.791, 115.731, 118.264,
123.464, 127.611, 133.504, 142.821, 152.270, 163.491, 164.968,
168.915, 169.346, 172.668, 191.954, 193.102, 208.522, 209.070,
219.111, 243.910, 280.302, 313.898, 330.461, 418.074, 516.218,
595.310, 742.198, 791.874, 822.787, 1.074.499

33 Schadensfälle mit einer Gesamtschadenssum-
me: 9.458.208 SF
```

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

Annäherung durch eine Pareto-Verteilung

Schadenshäufigkeit in Abhängigkeit von der Schadenshöhe:



Verteilung der Schadenshöhe S für Schäden $S > 10^5$ ist hier eine Pareto-Verteilung mit Formfaktor $k = 1{,}2$ und Skalenparameter $x_{\min} = 10^5$:

$$F_S(s) = \mathbb{P}[S \leq s] = 1 - \left(\frac{s}{s_{\min}}\right)^{-k} = 1 - \left(\frac{s}{10^5}\right)^{-1{,}2}$$

Dichtefunktion:

$$f(s) = k \cdot \frac{s_{\min}^{k}}{s^{k+1}} = 1{,}2 \cdot \frac{10^{5 \cdot 1{,}2}}{s^{2{,}2}}$$

Erwartungswert

$$\mathbb{E}[S] = x_{\min} \cdot \frac{k}{k-1} = 5 \cdot x_{\min}$$

Eine Varianz besitzt eine Pareto-Verteilung erst ab Formfaktor $k > 2$ (vergl. Foliensatz 3, Abschn. Abschn. 4.1 Pareto-Verteilung).

Schaden durch FF

Mindestschaden eine erkannten FF sind die Kosten für Datenwiederherstellung, Neustart und Wiederholung:

$$\mathbb{E}\left[S_1\right] = \mathbb{E}\left[\zeta\right] \cdot \mathbb{E}\left[K_{\mathrm{W}}\right]$$

Hinzu kommen für einen Anteil von $\eta_{\mathrm{R}} \ll 1$ Kosten für Fehlersuche und Reparatur:

$$\mathbb{E}\left[S_2\right] = \mathbb{E}\left[\zeta\right] \cdot \eta_{\mathrm{R}} \cdot \mathbb{E}\left[K_{\mathrm{R}}\right]$$

Für nicht erkannte FF kommen die Kosten für »kleinere« Folgeschäden hinzu:

$$\mathbb{E}\left[S_3\right] = \mathbb{E}\left[\zeta\right] \cdot (1 - FFC) \cdot \mathbb{E}\left[K_{\mathrm{F}}\right]$$

Für erkannte sicherheitskritische FF kommen Kosten für Schadensabwehr hinzu:

$$\mathbb{E}\left[S_4\right] = \mathbb{E}\left[\zeta\right] \cdot \eta_{\mathrm{g}} \cdot FFC_{\mathrm{S}} \cdot \mathbb{E}\left[K_{\mathrm{A}}\right]$$

(FFC – Fehlfunktionsüberdeckung der Überwachung; η_{R} – Anteil der FF, für die Reparaturiterationen gestartet werden; η_{g} – Anteil der FF, für die Schaden abzuwehren ist; FFC_{S} – siehe nächste Folie).

Für nicht erkannte sicherheitskritische FF kommen die dann in der Regel erheblichen Schadenskosten hinzu:

$$\mathbb{E}\left[S_5\right] = \mathbb{E}\left[\zeta\right] \cdot \eta_{\mathrm{g}} \cdot (1 - FFC_{\mathrm{S}}) \cdot \mathbb{E}\left[K_{\mathrm{S}}\right]$$

Zu erwartender Gesamtschaden je SL:

$$\mathbb{E}[S]/\mathbb{E}[\zeta] = \mathbb{E}\left[K_{\mathrm{W}}\right] + \eta_{\mathrm{R}} \cdot \mathbb{E}\left[K_{\mathrm{R}}\right] + (1 - FFC) \cdot \mathbb{E}\left[K_{\mathrm{F}}\right] + \eta_{\mathrm{g}} \cdot ((1 - FFC_{\mathrm{S}}) \cdot \mathbb{E}\left[K_{\mathrm{A}}\right] + FFC_{\mathrm{S}} \cdot \mathbb{E}\left[K_{\mathrm{S}}\right])$$

($K_{\ldots}$ – Kosten für ...: K_{W} – Datenherstellung und Wiederholung, K_{R} – Fehlersuche und Reparatur; K_{F} – Folgeschäden; K_{A} – Schadensabwehr; K_{S} – sicherheitskritische Schäden; η_{R} – Anteil der FF, deren Korrektur Fehlersuche und Repartur erfordert; FFC – Fehlfunktionsüberdeckung für eingebaute Überwachungsfunktionen und Benutzer zusammen; $FFC_{\mathrm{S}} \gg FFC$ – Fehlfunktionsüberdeckung für sicherheitskritische FF; η_{g} – Anteil der sicherheitskritischen (gefährdenden) FF, die ohne Gegenmaßnahmen großen Schaden verursachen.)

Die Kosten für die überwiegend anfallenden kleineren Schäden sind Betriebskosten, die der Anwender trägt oder die z.T. auch durch Wartungsverträge abgedeckt sind.

Im Straßenverkehr die großen, selten auftretenden Schadensfälle durch FF durch Fahrer und Fahrzeug über Haftpflichtversicherungen abgedeckt. Schäden durch sicherheitskritische IT-FF haben heute ähnliche Verteilungen wie große KFZ-Haftpflichschäden.

Zukunftsmodell ist auch sicher hier eine Haftpflichtversicherung.

Ausfälle

Ausfälle

Hardware und Mechanik unterliegt einem Verschleiß, der zu Ausfällen führen kann. Bei einem Ausfall entsteht ein Fehler, der oft mehr FF als alle vom Test nicht erkannten Fehler zusammen oder ein komplettes Versagen[7] verursacht.

Maßnahmen zum Umgang mit Ausfällen:

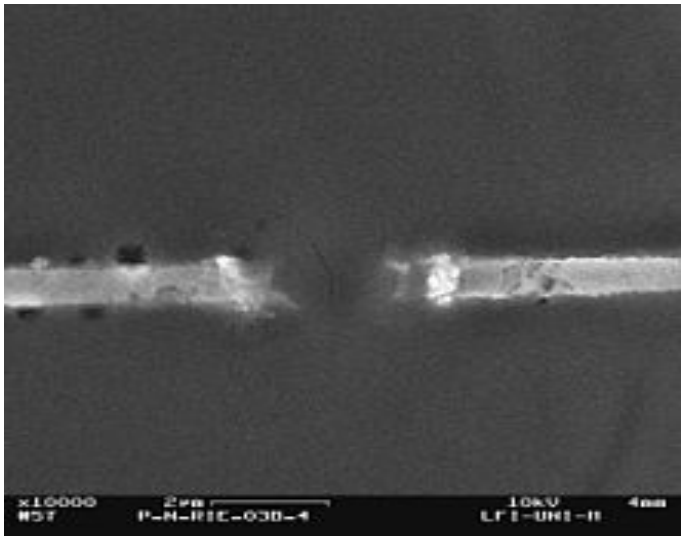
- Voralterung,
- Wartung,
- Redundanz (kalte oder heiße Reserve).

In Software entstehen während des Betriebs keine neuen Fehler, ausgenommen

- einprogrammiertes Ausfallverhalten (geplante Obsoleszenz)
- und wenn Verfälschungen von (Programm-) Daten durch Fehler oder Störungen als Ausfälle gezählt werden.

[7] Keine weiteren SL bis zur Reparatur.

Verschleiß elektronischer Bauteile



Physikalische Verschleißmechanismen für elektronische Bauteile:

- Korrosion (Stecker, Schalter, Isolationen, Leiterbahnen, ...).
- Elektromigation: strombedingte Wanderung von Metallatomen bei hohen Stromdichten.
- Gateoxiddurchschlag: Hochschaukelnde Tunnelströme, Ladungseinlagerung bis zum lokalen Schmelzen des Oxids. Bildung von Kurzschlüssen. Phänomen: Zunahme des Stromverbrauchs über Monate bis zum Ausfall.
- Parameterdrift: Widerstandswerte, Kapazitäten, Schwellspannungen etc.

Verbesserung Fertigung, Material etc. $\Rightarrow$ weniger Ausfälle

Kenngrößen

Kenngrößen des Ausfallverhaltens

- Lebensdauer t_L: Zeit vom Beanspruchungsbeginn bis zum Ausfall. Verteilungsfunktion:

$$F(t) = \mathbb{P}[t_\mathrm{L} \leq t]$$

- Überlebenswahrscheinlichkeit:

$$R(t) = \mathbb{P}[t_\mathrm{L} > t] = 1 - F(t)$$

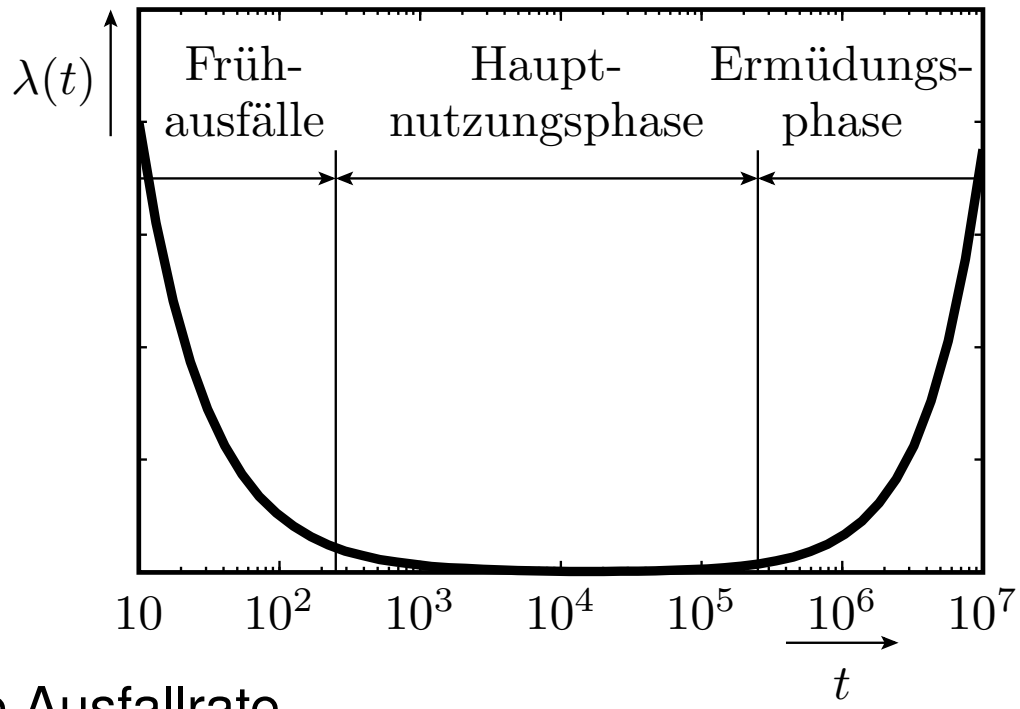
- Ausfallrate λ: Relative Abnahme der Überlebenswahrscheinlichkeit mit der Zeit:

$$\lambda(t) = -\frac{1}{R(t)} \cdot \frac{\mathrm{d}\,R(t)}{\mathrm{d}t}$$

- Mittlere Lebensdauer:

$$\mathbb{E}[t_\mathrm{L}] = \int_0^\infty R(t) \cdot \mathrm{d}t$$

Ausfallphasen



- Frühausfälle (infant mortalities): Erhöhte Ausfallrate durch Schwachstellen (Materialrisse, lokal stark überhöhte Feldstärke oder Stromdichte, ...).
- Hauptnutzungsphase: Näherungsweise konstante Ausfallrate.
- Ermüdungsphase: Anstieg der Ausfallrate: Materialermüdung, ...

Überlebenswahrscheinlichkeit in der Hauptnutzungsphase:

$$R(t) = \mathrm{e}^{-\lambda \cdot t}$$

$$F(t) = 1 - \mathrm{e}^{-\lambda \cdot t}$$

$$\lambda(t) = -\frac{1}{R(t)} \cdot \frac{\mathrm{d}\,R(t)}{\mathrm{d}t} = \lambda = \text{konst.}$$

Hauptnutzungsphase

Hauptnutzungsphase

Konstante Ausfallrate:

$$\lambda(t) = -\frac{1}{R(t)} \cdot \frac{\mathrm{d}\,R(t)}{\mathrm{d}t} = \lambda = \text{konst.}$$

verlangt für Überlebenswahrscheinlichkeit und Vert. Lebensdauer:

$$R(t) = \mathrm{e}^{-\lambda \cdot t} \tag{10}$$

$$F(t) = 1 - \mathrm{e}^{-\lambda \cdot t}$$

Mittlere Lebensdauer:

$$\mathbb{E}[t_\mathrm{L}] = \int_0^\infty R(t) \cdot \mathrm{d}t = \frac{1}{\lambda}$$

Maßeinheit der Ausfallrate: fit (failure in time)

$$1\,\text{fit} = 1\,\text{Ausfall in } 10^9\,\text{Stunden}$$

System mit mehreren Komponenten

Das Gesamtsystem überlebt, solange alle Komponenten überleben:

$$R(t) = \prod_{i=1}^{\#K} R(t)_i$$

($\#K$ – Anzahl der Komponanten). Mit einer konstanten Ausfallrate λ_i für alle Komponenten:

$$R(t) = \prod_{i=1}^{\#K} \mathrm{e}^{-\lambda_i \cdot t} = \mathrm{e}^{-\left(\sum_{\mathrm{i}=1}^{\mathrm{n}} \lambda_{\mathrm{i}}\right) \cdot \mathrm{t}}$$

Die Ausfallrate des Gesamtsystems ist die Summe der Ausfallraten aller Komponenten:

$$\lambda_{\mathrm{Sys}} = \sum_{i=1}^{\#K} \lambda_i$$

Ausfallraten in der Hauptnutzungsphase nach[8]

Bauteil	Ausfallrate in fit	Bauteil	Ausfallrate in fit
diskrete HBT	1 bis 100	Widerstände	1 bis 20
digitale IC	50 bis 200	Kondensatoren	1 bis 20
ROM	100 bis 300	Steckverbinder	1 bis 100
RAM	bis 500	Lötstellen	0,1 bis 1
analoge IC	20 bis 300		

(HBT – Halbleiterbauteile; IC – Schaltkreise)

- Ausfallrate = Ausfallanzahl / Bauteilanzahl
- Bei mehreren Bauteilen und konstanten Ausfallraten addieren sich die Ausfallraten.

[8] Kärger, R.: Diagnose von Computern, Teubner 1996, S. 68

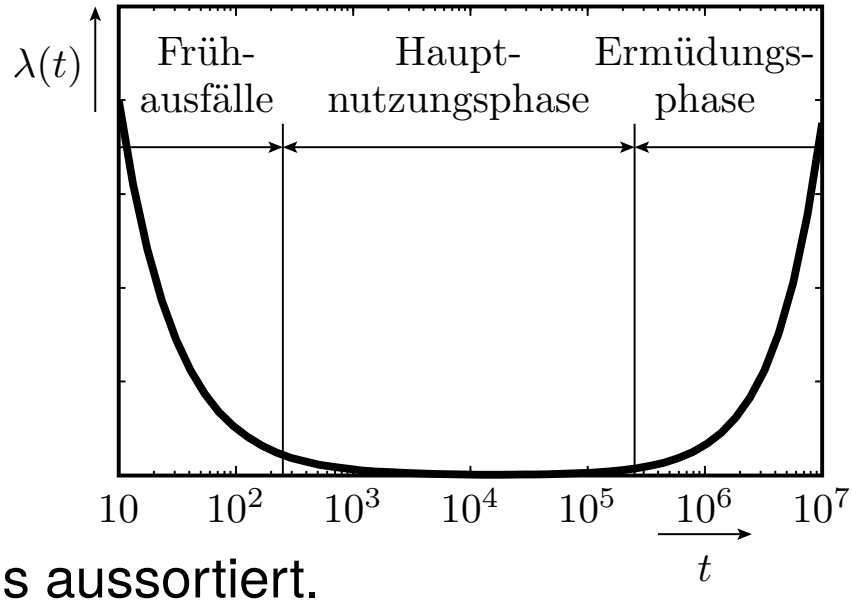
Ausfallrate einer Baugruppe

Bauteiltyp	Anzahl n	Ausfallrate λ	$n \cdot \lambda$
Schaltkreise	20	150 fit	3000 fit
diskrete BT	15	30 fit	450 fit
Kondensatoren	15	10 fit	250 fit
Widerstände	30	10 fit	300 fit
Lötstellen	2000	0,5 fit	1000 fit
Baugruppe			5000 fit

- Im Mittel 1 Ausfall in $2 \cdot 10^5$ Stunden ($\approx$23 Jahre) Betriebsdauer.
- Von den heutigen PCs, Handys, ... fallen pro Jahr und hundert Stück nur wenige aus. Nach 2 ... 5 Jahren Ermüdungsausfälle, z.B. durch Austrocknung von Elektrolytkondensatoren.

Voralterung

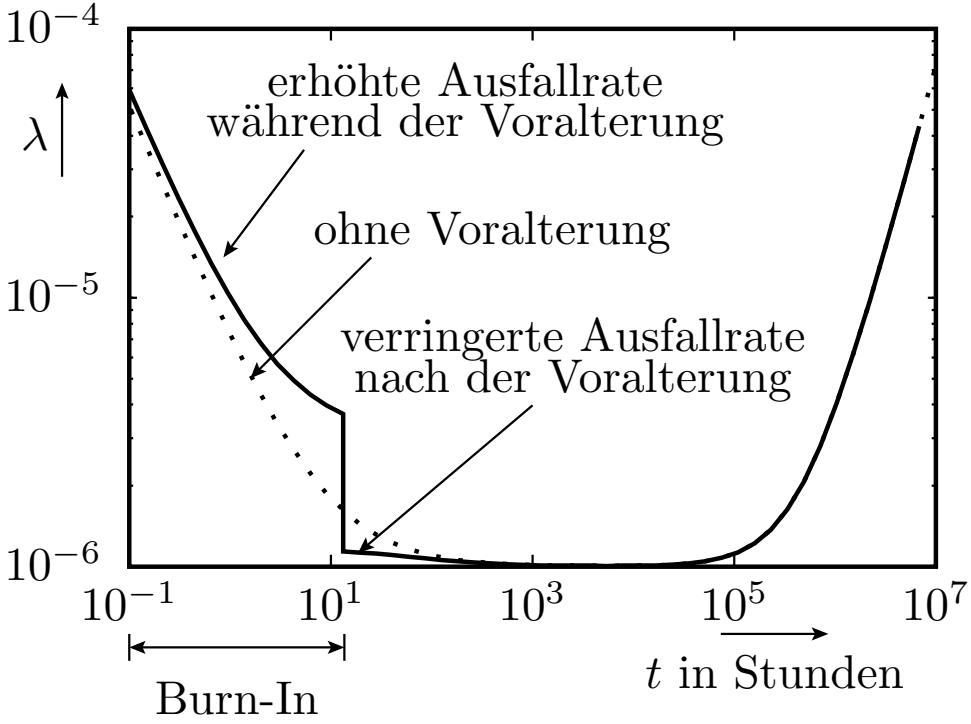
Frühausfälle



- Auf 100 richtige Fehler kommt etwa ein Beinahefehler, der zu einem Frühausfall führt[9].
- Bei 50% fehlerfreien und 50% aussortierten Schaltkreisen $50\%/100 = 0{,}5\%$ Beinahefehler.
- Die Hälfte wird mit dem Ausschuss aussortiert.
  - $\approx 0{,}25\%$ (jeder 400ste) Schaltkreis verursacht ein Frühausfall.
  - Bei 20 Schaltkreisen pro Gerät jedes zwanzigste Gerät.
  - Bei großen Systemen fast jedes System.
- Frühausfälle sind Garantiefälle und verursachen Kosten für Reparatur, Ersatz, Auftragsabwicklung, ... Was tun?

[9] Barnett, T. S., Singh, A. D.: Relating Yield Models to Burn-In Fall-Out in Time. ITC, 12/2003, S.77-84.

Voralterung (Burn-In)



- Beschleunigung der Alterung vor dem Einsatz durch »harte« Umgebungsbedingungen
  - überhöhte Spannung,
  - überhöhte Temperatur,
  - Stress.
- Einsatz erst nach der Frühphase (wenn die kränklichen Bauteile gestorben und ausgetauscht sind).

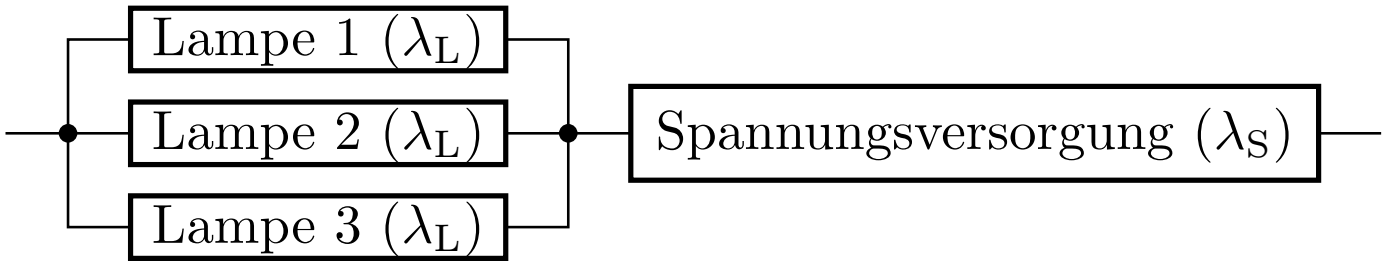
Künstliche Voralterung ist auch in anderen Bereichen, z.B. im Maschinenbau gebräuchlich. Voralterung von Menschen gilt zwar als unmoralisch, aber ...

Redundanz

Ausfallplan mit Redundanzen

Im Ausfallplan werden notwendige Komponenten für die Verfügbarkeit des Services als Reihenschaltung und Reserveeinheiten (Redundanzen) als Parallelschaltung dargestellt.

Eine Flurbeleuchtung sei verfügbar, wenn mindestens eine von drei Lampen und die Spannungsversorgung funktioniert:



Systeme ohne Reparaturmöglichkeit, die lange verfügbar sein müssen (z.B. in einem Satelliten)

- erhalten Ersatzkomponenten und
- Funktionen zur automatischen Rekonfiguration nach Ausfall.

Kalte, warme und heiße Reserve

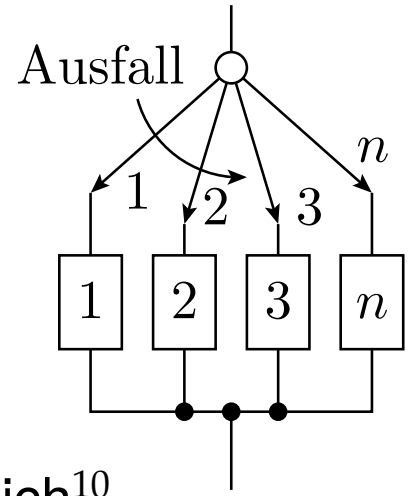
- Heiße Reserve: Reservekomponenten arbeiten parallel (z.B. Mehrversionssystem) und fallen mit derselben Wahrscheinlichkeit wie das aktive System aus.
- Kalte Reserve: Reservekomponenten werden geschont und funktionieren idealerweise noch alle zum Ausfallzeitpunkt der aktiven Komponente.
- Warme Reserve: Reserveeinheiten (z.B. das Reserverad im Auto) altern auch bei Nichtnutzung, nur langsamer.

Die beiden zusätzlichen Lampen auf der Folie zuvor, die für die Verfügbarkeit der Treppenbeleuchtung nicht unbedingt funktionieren müssen, bilden eine heiße Reserve, Ersatzlampen, die erst nach Ausfall der »Hauptlampe« eingeschaltet werden, eine kalte Reserve, ein Ersatzrad im Auto eine warme Reserve, weil der Gummi auch ohne Beanspruchung altert.

Kalte Reserve

Für jede Komponente beginnt die Belastung erst nach Ausfall der vorherigen Komponente.

Phase	mittlere Dauer
1	$\mathbb{E}[t_{\mathrm{L}.1}]$
2	$\mathbb{E}[t_{\mathrm{L}.2}]$
3	$\mathbb{E}[t_{\mathrm{L}.3}]$
...	...
Summe:	$\mathbb{E}[t_{\mathrm{L.ges}}] = \sum_{i=1}^{n} \mathbb{E}[t_{\mathrm{L}.i}]$



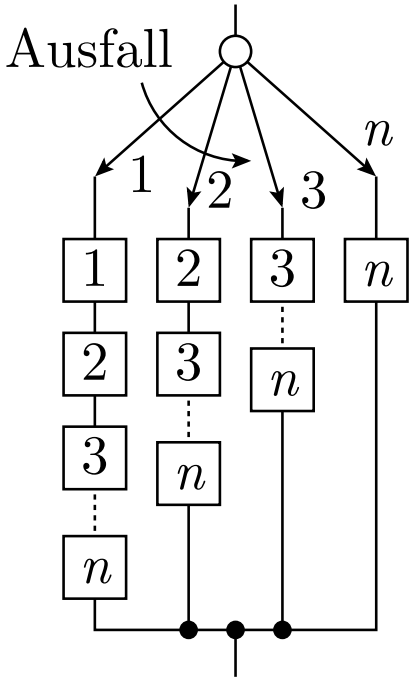
- Die Lebensdauern aller Komponenten addieren sich[10].

[10] Unter der Annahme, dass die Umschalter und die ungenutzten Reserveeinheiten Ausfallrate null haben.

Heiße Reserve

- Alle noch lebenden Komponenten können gleichermaßen ausfallen:

$$\mathbb{E}\left[t_{\mathrm{L}.i}\right] = \frac{1}{\sum_{j=1}^{i} \lambda_j}$$

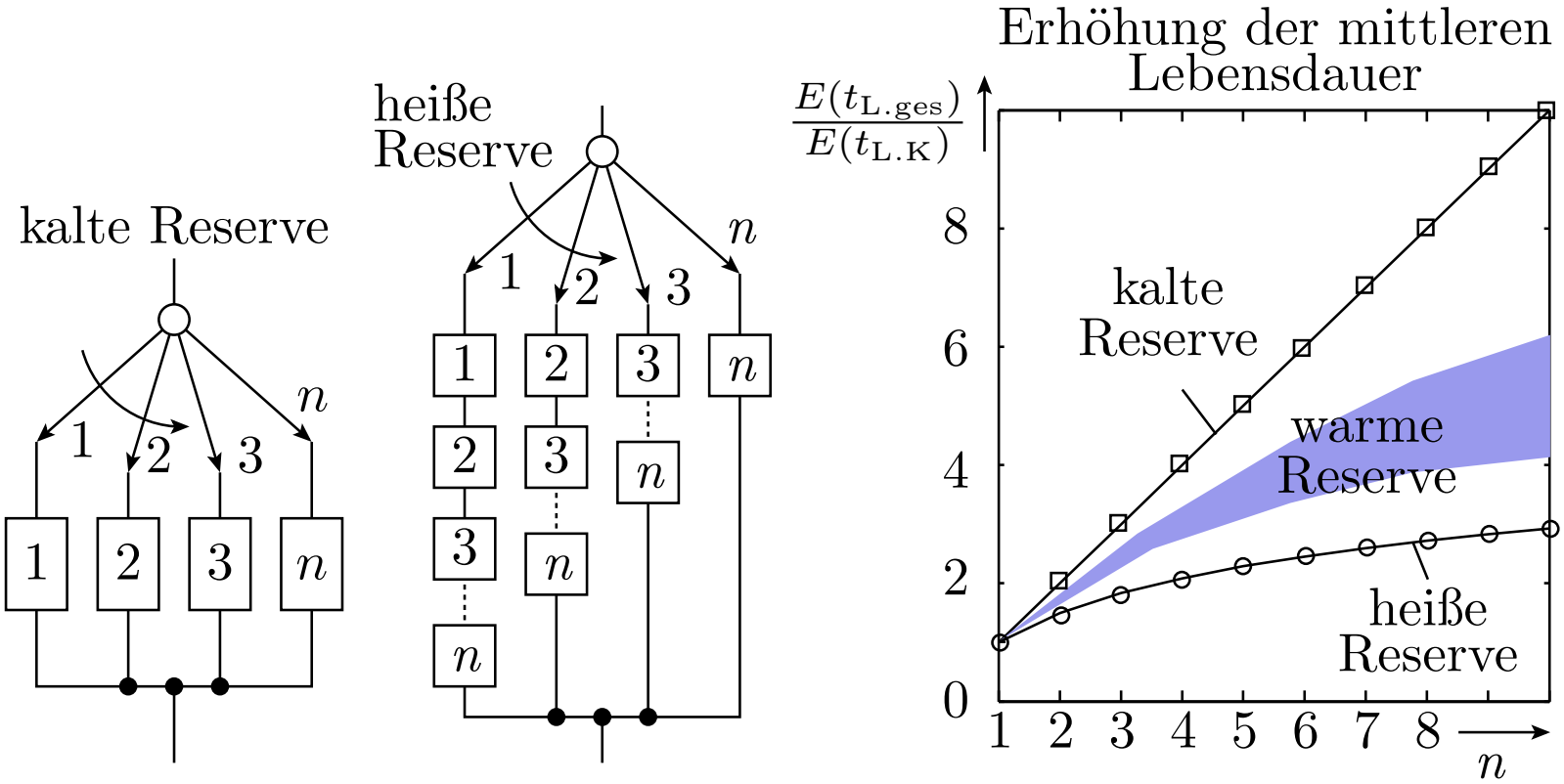


- Komponenten mit gleicher Ausfallrate λ_{K}:

Phase	mittlere Dauer
1	$\frac{1}{n \cdot \lambda_{\mathrm{K}}} = \frac{\mathbb{E}[t_{\mathrm{L.K}}]}{n}$
2	$\frac{1}{(n-1) \cdot \lambda_{\mathrm{K}}} = \frac{\mathbb{E}[t_{\mathrm{L.K}}]}{n-1}$
...	...
Summe:	$\mathbb{E}\left[t_{\mathrm{L.ges}}\right] = \mathbb{E}\left[t_{\mathrm{L.K}}\right] \cdot \sum_{i=1}^{n} \frac{1}{i}$

- Die erste Reservekomponente erhöht die mittlere Lebensdauer um die Hälfte, die zweite um ein Drittel etc.

Warme Reserve



- Die Ausfallrate der »kalten« Ersatzkomponenten ist kleiner als im aktiven Zustand, aber größer null.
- »Warme« Reserveeinheiten verlängert die Lebensdauer mehr als »heiße« und weniger als »kalte«.

Wartung

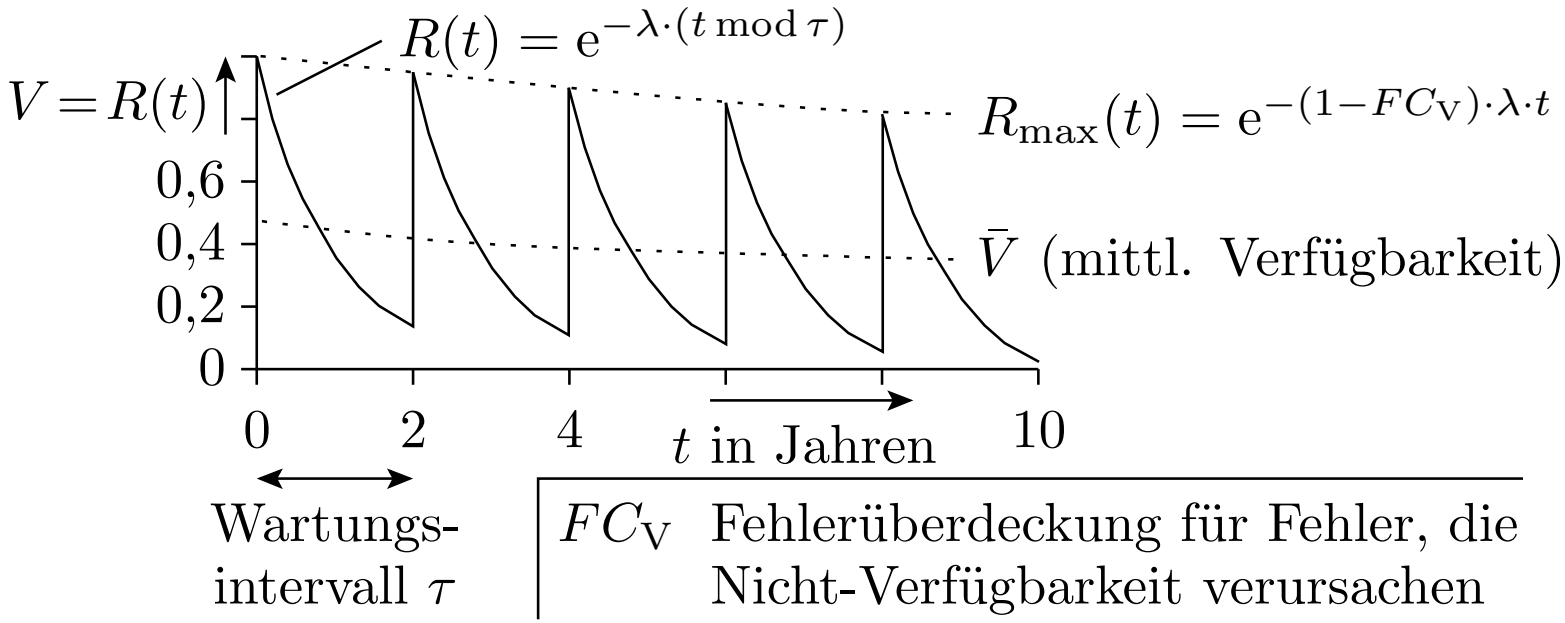
Wartung

Wartung:

- Test und die Beseitigung aller erkennbaren Fehler, die seit der letzten Wartung entstanden sind, insbesondere auch der durch Ausfälle.
- Ergänzen und Ersatz von Betriebsstoffen und Verbrauchsmitteln (Getrieben Schmierstoffe, bei Druckern Papier und Toner).
- Planmäßiger Austausch von Verschleißteilen vor der Ermüdungsphase, in der die Ausfallrate stark zunimmt (in PCs die Batterien für den BIOS-RAM, in Servern die Festplatten).

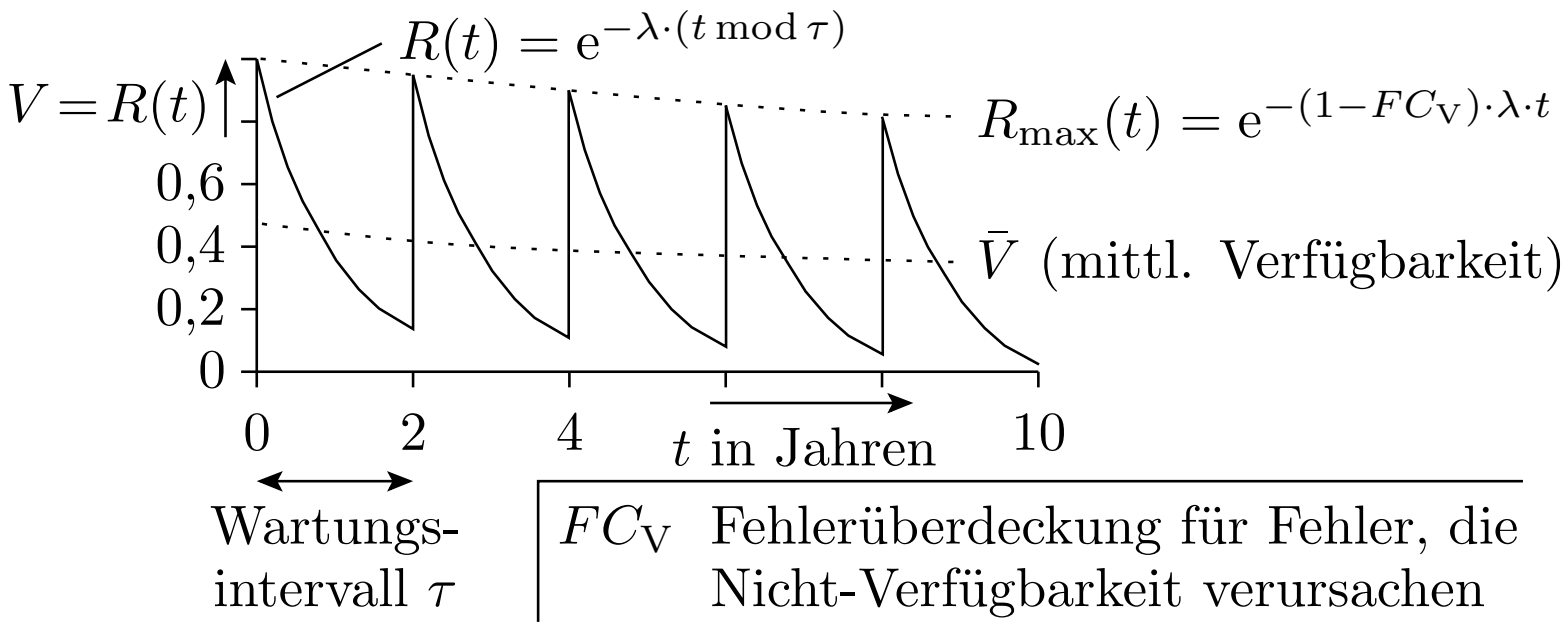
Wartungsintervall τ: Zeit zwischen den Wartungen, z.B. 1 Jahr.

Verfügbarkeit und Wartung



Die Verfügbarkeit ist gleich die Überlebenswahrscheinlichkeit.

Zwischen den Wartungen sinkt die Überlebenswahrscheinlichkeit in der Hauptnutzungsphase entsprechend Gl. 10 und wird zum Wartungszeitpunkt durch Beseitigung der möglicherweise entstandenen Fehler idealerweise auf 1 zurückgesetzt (τ – Wartungsintervall; $t \bmod \tau$ – t modulo τ).



Wenn der Wartungstests nicht alle Fehler erkennt, die die Verfügbarkeit beeinträchtigen

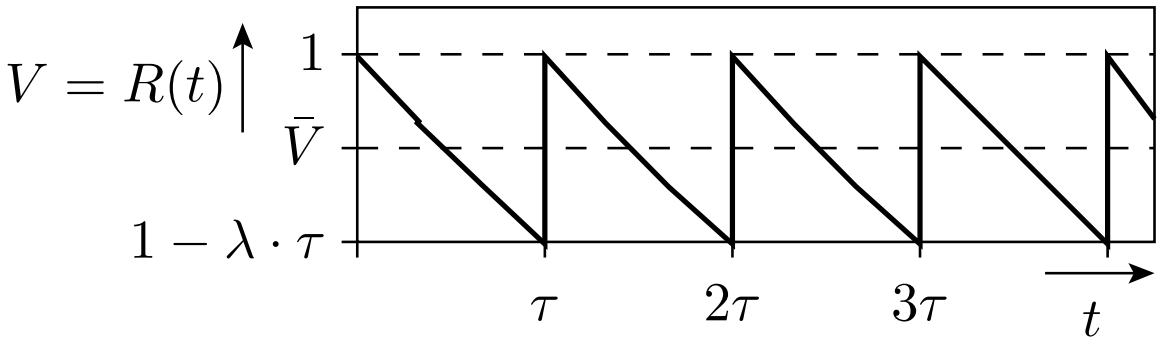
$$FC_{\mathrm{V}} < 1$$

steigt die Überlebenswahrscheinlichkeit nur auf einen mit der Nutzungsdauer abnehmenden Wert $R_{\max}(t) < 1$.

Eine hohe (mittlere) Verfügbarkeit verlangt ein Wartungsintervall:

$$\tau \ll \lambda^{-1}$$

Mittlere Verfügbarkeit und PFD



Mittlere Verfügbarkeit (Überlebenswahrscheinlichkeit), wenn der Wartungstest alle Ausfälle erkennt und $\lambda \cdot \tau \ll 1$:

$$\bar{V} = \frac{1}{\tau} \cdot \int_0^\tau R\,(t) \cdot \mathrm{d}\tau = \int_0^\tau \mathrm{e}^{-\lambda \cdot t} \cdot \mathrm{d}\tau = \frac{1 - \mathrm{e}^{-\lambda \cdot \tau}}{\lambda}$$

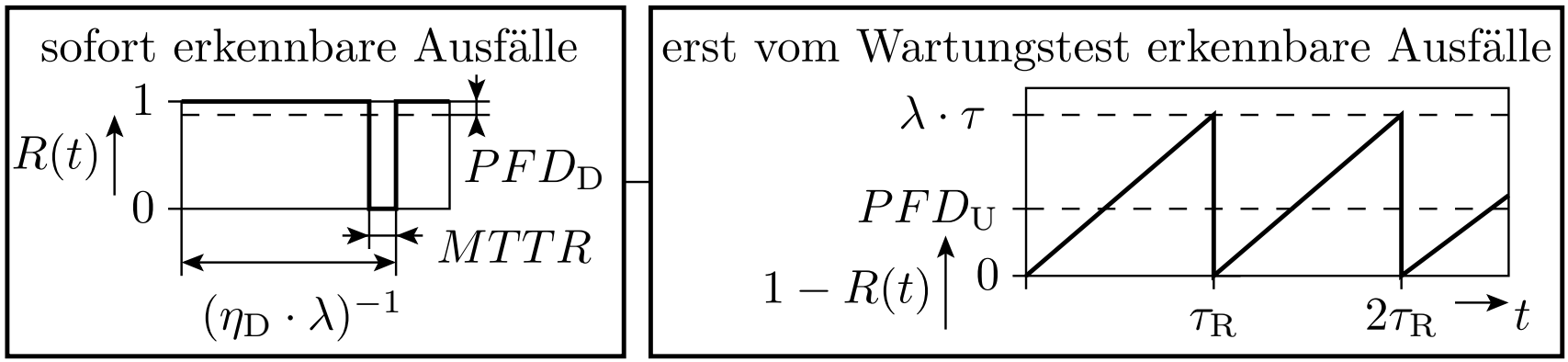
mit

$$\mathrm{e}^{-\lambda \cdot \tau} \approx 1 - \lambda \cdot \tau + \frac{(\lambda \cdot \tau)^2}{2}$$

$$\bar{V} = 1 - \frac{\lambda \cdot \tau}{2}; \quad PFD = 1 - \bar{V} = \frac{\lambda \cdot \tau}{2}$$

(τ – Wartungsintervall; λ – Ausfallrate; PFD – Probability of Failure on Demand, Wahrscheinlichkeit der Nichtverfügbarkeit, zu einem zufälligen Zeitpunkt).

Beseitigung sofort bemerkter Ausfälle

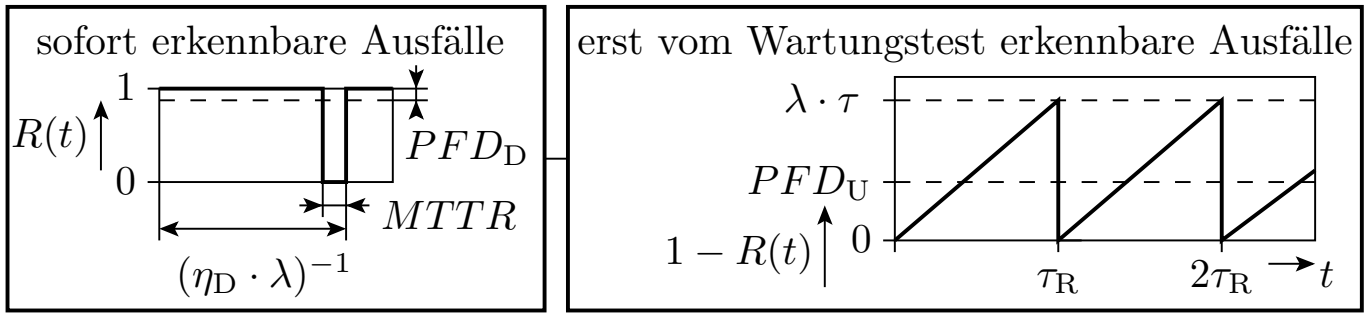


Ein Anteil η_{D} der Ausfälle wird sofort bemerkt und mit der $MTTR$ (Mean Time to Repair) beseitigt. Modellierung als Reihenschaltung

- eines Systems mit den sofort erkennbaren Ausfällen. Mittlere Zeit zwischen zwei Ausfällen $1/(\eta_{\mathrm{D}} \cdot \lambda)$. Mittler Wahrscheinlichkeit, dass diese Teilsystem ausgefallen ist:

$$PFD_{\mathrm{D}} = \eta_{\mathrm{D}} \cdot \lambda \cdot MTTR$$

- und eines Systems mit den Ausfällen, die erst beim der Wartung bemerkt und beseitigt werden ...



- ... erst bei der Wartung bemerkt und beseitigt werden:

$$PFD_{\mathrm{U}} = \frac{(1-\eta_{\mathrm{D}}) \cdot \lambda \cdot \tau}{2}$$

Ein System ist nicht verfügbar, wenn

- es wegen der Beseitigung eines sofort erkennbaren ausfallbedingten Fehler **ODER** (sich ausschließender Ereignisse)
- wegen eines nicht sofort bemerkbaren Fehlers, der erst bei der Wartung erkannt und beseitigt wird

nicht verfügbar ist. Wahrscheinlichkeit, dass das System insgesamt zu einem zufälligen Anforderungszeitpunkt ausgefallen ist:

$$PFD = PFD_{\mathrm{D}} + PFD_{\mathrm{U}} = \eta_{\mathrm{D}} \cdot \lambda \cdot MTTR + \frac{(1-\eta_{\mathrm{D}}) \cdot \lambda \cdot \tau}{2}$$

$$\bar{V} = 1 - PDF = 1 - \eta_{\mathrm{D}} \cdot \lambda \cdot MTTR + \frac{(1-\eta_{\mathrm{D}}) \cdot \lambda \cdot \tau}{2}$$

Sicherheitsstufen für Industriegeräte nach IEC 61508, Mindest-$MTBF$ und Maximal-PFD:

SIL	1	2	3	4
$MTBF_{\min}$ in Jahren	10	10^2	10^3	10^4
$PFD_{\max}$	10^{-1}	10^{-2}	10^{-3}	10^{-4}

(SIL – **S**afety **I**ntegrity **L**evel). Aus den $MTBF$ und PFD leiten sich die Wartungsintervalle, erforderliche Redundanzen etc. ab.

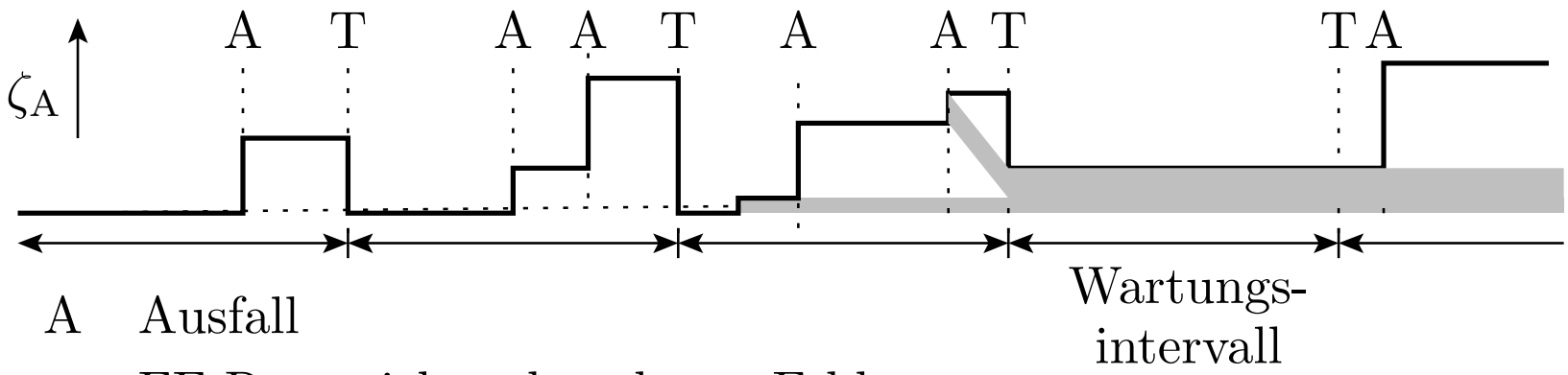
Beispiel 1

Ausfallrate $\lambda = 10^{-6}\,\mathrm{h}^{-1}$, Anteil der Ausfälle, die sofort beseitigt werden $\eta_\mathrm{D} = 75\%$. Wartungsintervall $\tau = 2 \cdot 10^3\,\mathrm{h}$, mittlere Reparaturzeit $MTTR = 4\,\mathrm{h}$. Gesucht PFD:

$$PFD = \eta_\mathrm{D} \cdot \lambda \cdot MTTR + \frac{(1-\eta_\mathrm{D}) \cdot \lambda \cdot \tau}{2}$$

$$= 0{,}75 \cdot 10^{-6}\,\mathrm{h}^{-1} \cdot 4\,\mathrm{h} + \frac{0{,}25 \cdot 10^{-6}\,\mathrm{h}^{-1} \cdot 2 \cdot 10^3\mathrm{h}}{2} = 2{,}53 \cdot 10^{-4}$$

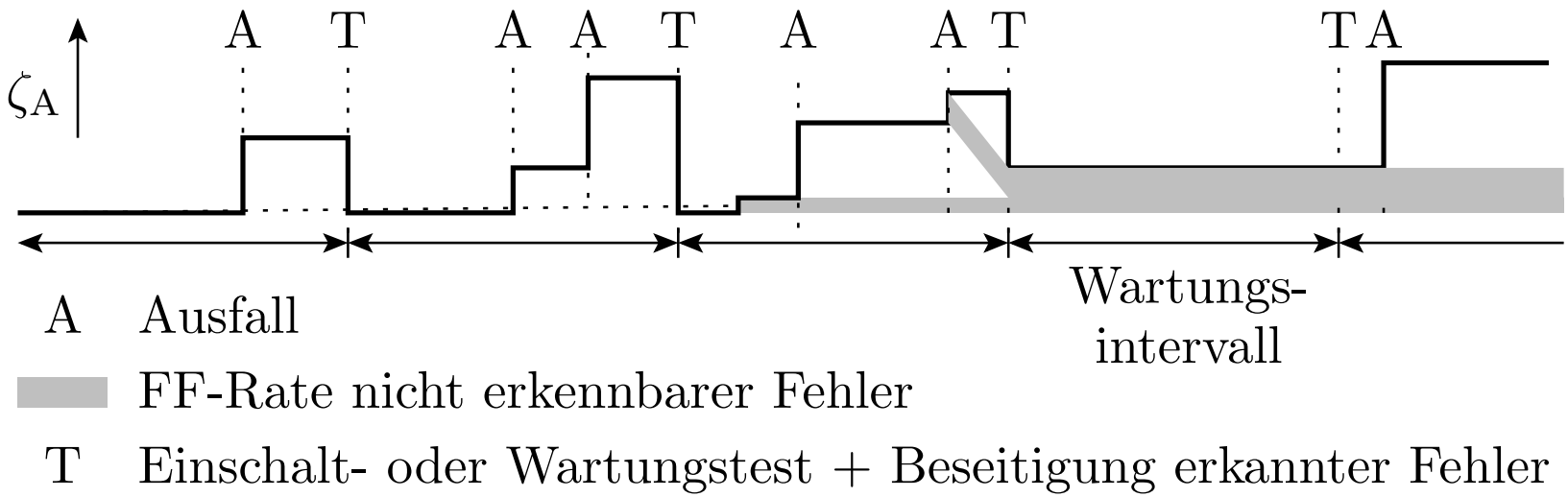
Zuverlässigkeitsverlust durch Ausfälle



Fehler durch Ausfälle mit kleiner FF-Rate

- beeinträchtigen statt der Verfügbarkeit die Zuverlässigkeit,
- werden von Wartungs- und Einschalttests nur mit $FC < 1$ erkannt,
- ihre zu erwartende Anzahl und die Häufigkeit der FF durch sie nehmen proportional zur Nutzungsdauer t, zur Nicht-Nachweiswahrscheinlichkeit $1 - FC$ und zum Kehrwert der Ausfallrate λ zu

$$\zeta_A \sim \mathbb{E}[X_A] \sim \frac{(1 - FC) \cdot t}{\lambda}$$



Auch bei regelmäßiger Wartung nimmt die FF-Rate über die Nutzungsdauer zu und die Zuverlässigkeit ab.

Gegenmaßnahmen:

- Ersatz des Gesamtsystems oder
- experimentelle Reparatur durch Tausch der potentiell ausgefallenen Komponenten und statistische Erfolgkontrolle anhand der FF-Rate.
- Suche von Tests für der Fehlernachweis und normale experimentelle Reparatur.