Test und Verlässlichkeit Foliensatz 7: Ausfälle und Fehlertoleranz

Prof. G. Kemnitz

Institut für Informatik, TU Clausthal (TV_F7)

April 11, 2022

Inhalt Foliensatz TV_F7: Ausfälle und Fehlertoleranz

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[1] verursacht.

Maßnahmen zum Umgang mit Ausfällen:

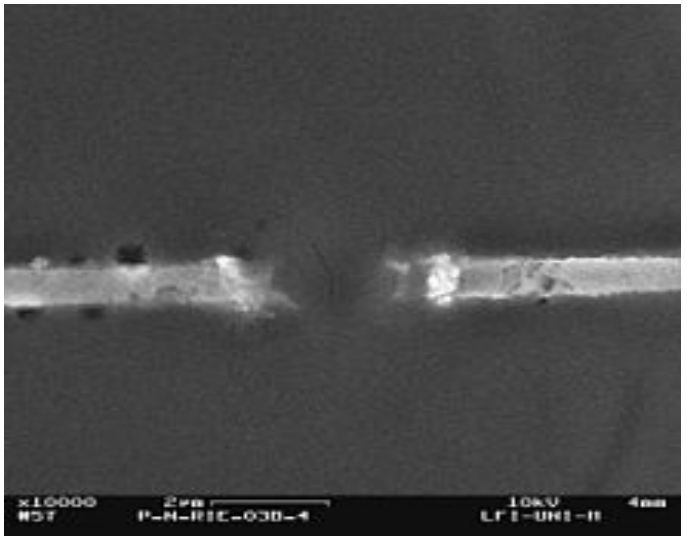
- Voralterung,
- Wartung,
- Redundanz (kalte oder heiße Reserve).

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.

[1] 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:

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

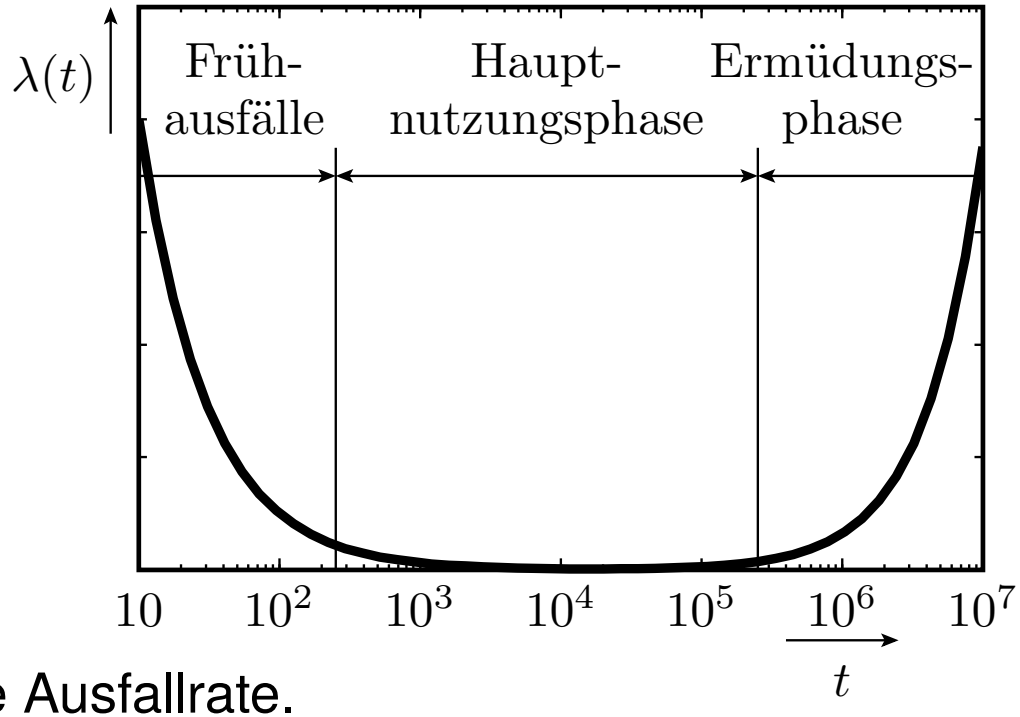
- Ausfallrate λ: Relative Abnahme der Überlebenswahrscheinlichkeit mit der Zeit:

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

- 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:

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

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

(Exponentialverteilung). 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[2]

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.

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

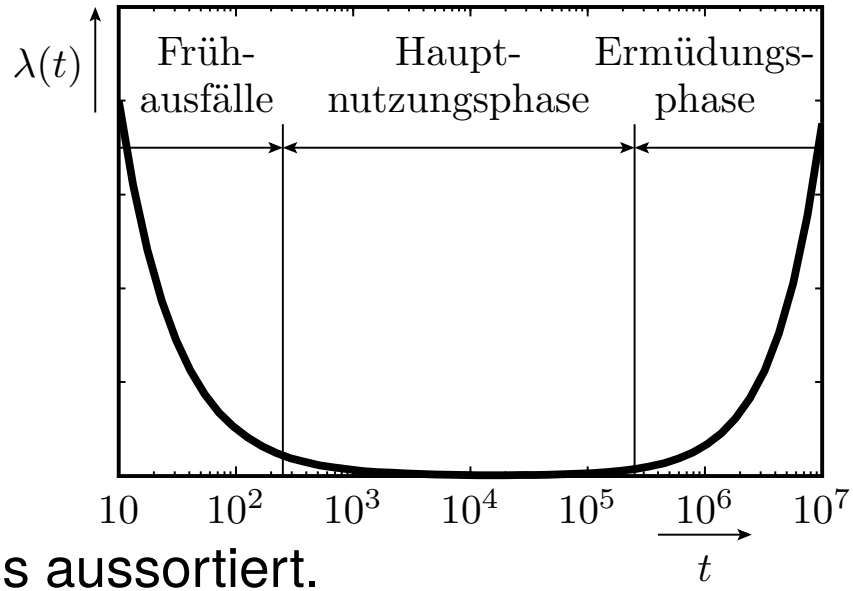
Ausfallrate einer Baugruppe

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

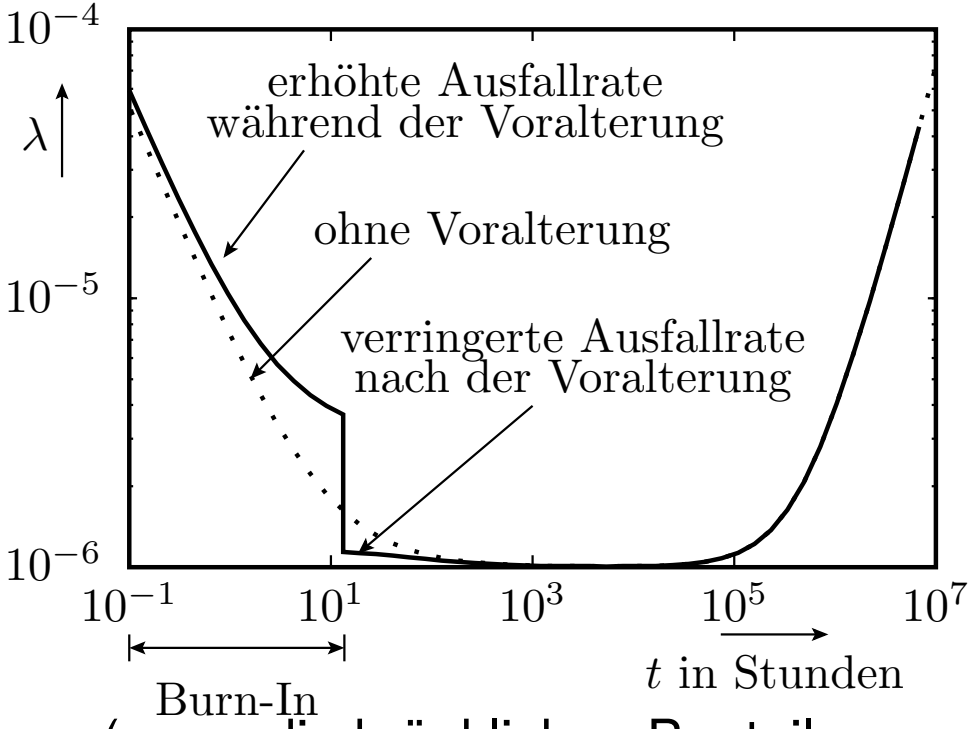
Frühausfälle



- Auf 100 richtige Fehler kommt etwa ein Beinahefehler, der zu einem Frühausfall führt[3].
- 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?

[3] 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).

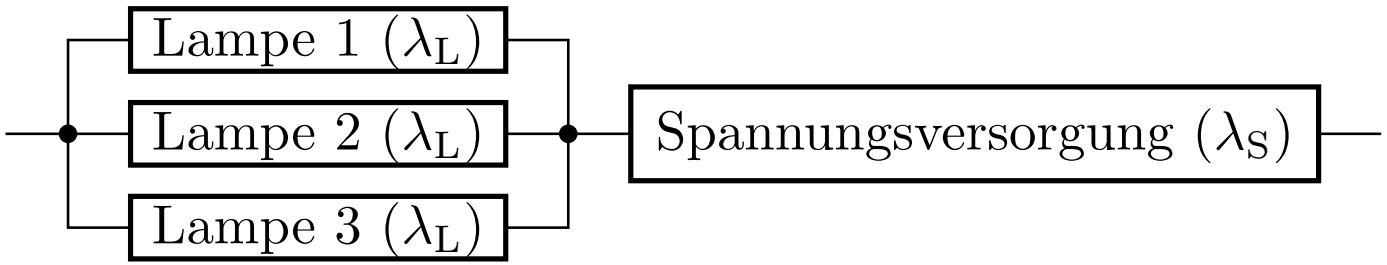
Künstliche Voralterung ist auch in anderen Bereichen, z.B. im Maschinenbau gebräuchlich. Voralterung von Menschen gilt zwar als unmoralisch, aber ...

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

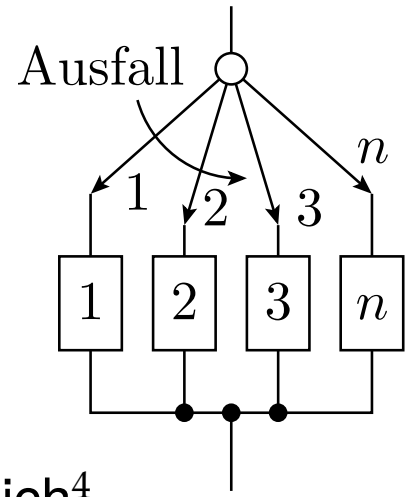
- Heiße Reserve: Reservekomponenten arbeiten parallel (z.B. Mehrversionssystem) und fallen mit derselben Wahrscheinlichkeit wie das aktive System aus.
- Kalte Reserve: Reservekomponenten werden geschont und funktionieren idealerweise noch alle zum Ausfallzeitpunkt der aktiven Komponente.
- Warme Reserve: 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	$\mathbb{E}\left[t_{\mathrm{L}.1}\right]$
2	$\mathbb{E}\left[t_{\mathrm{L}.2}\right]$
3	$\mathbb{E}\left[t_{\mathrm{L}.3}\right]$
...	...
Summe:	$\mathbb{E}\left[t_{\mathrm{L.ges}}\right] = \sum_{i=1}^{n} \mathbb{E}\left[t_{\mathrm{L}.i}\right]$



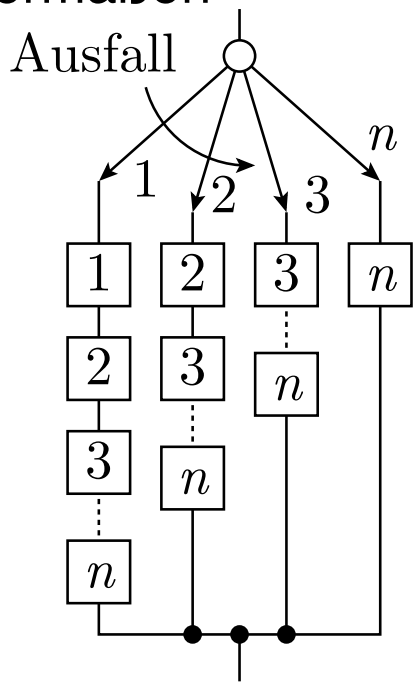
- Die Lebensdauern aller Komponenten addieren sich[4].

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

Heiße Reserve

- Alle noch lebenden Komponenten können gleichermaßen ausfallen:

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

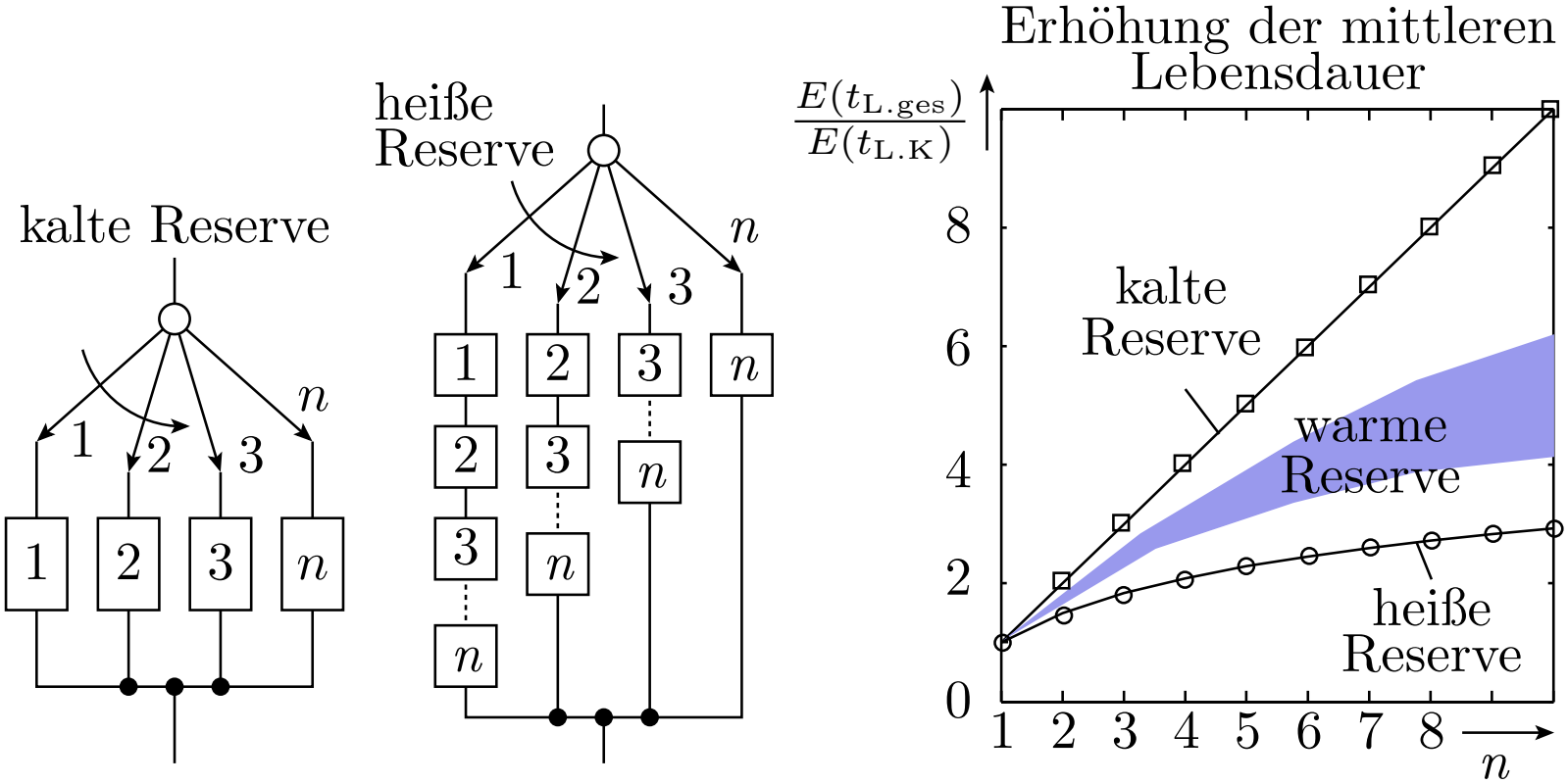


- Komponenten mit gleicher Ausfallrate λ_{K}:

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

- 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

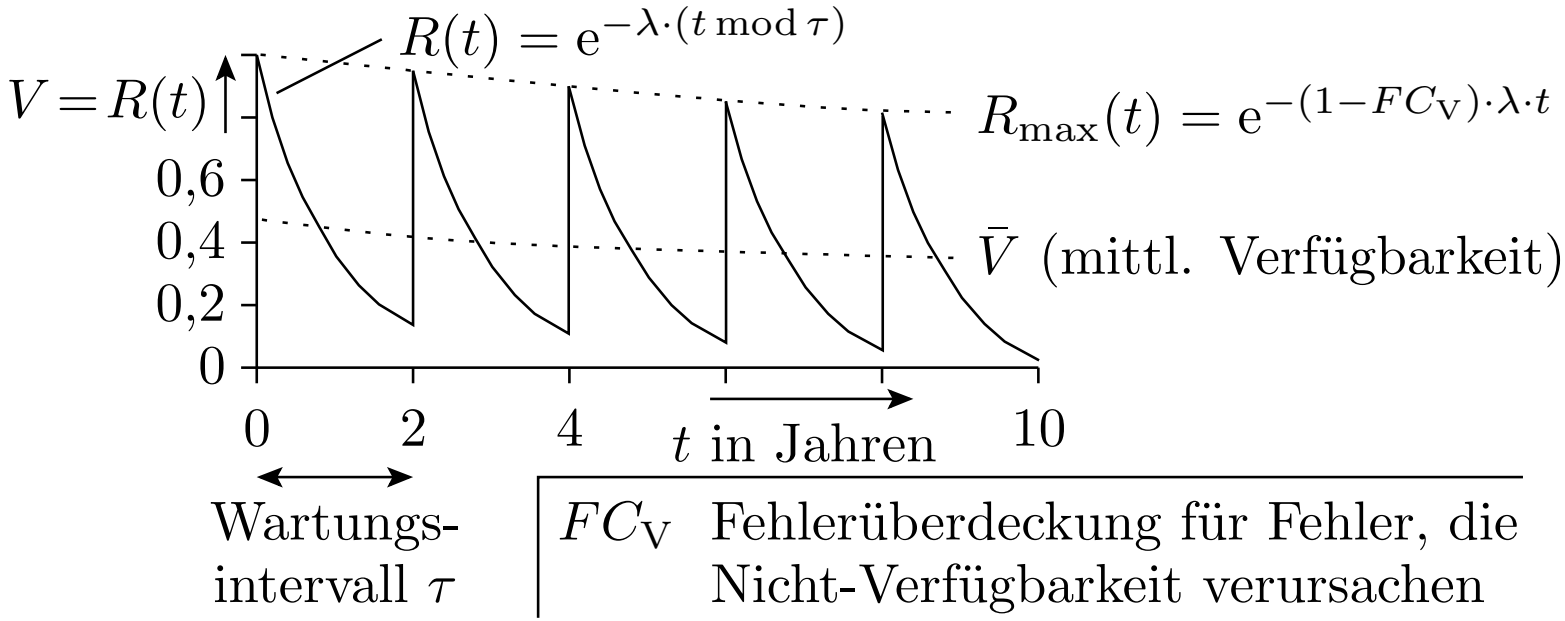
Wartung

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).

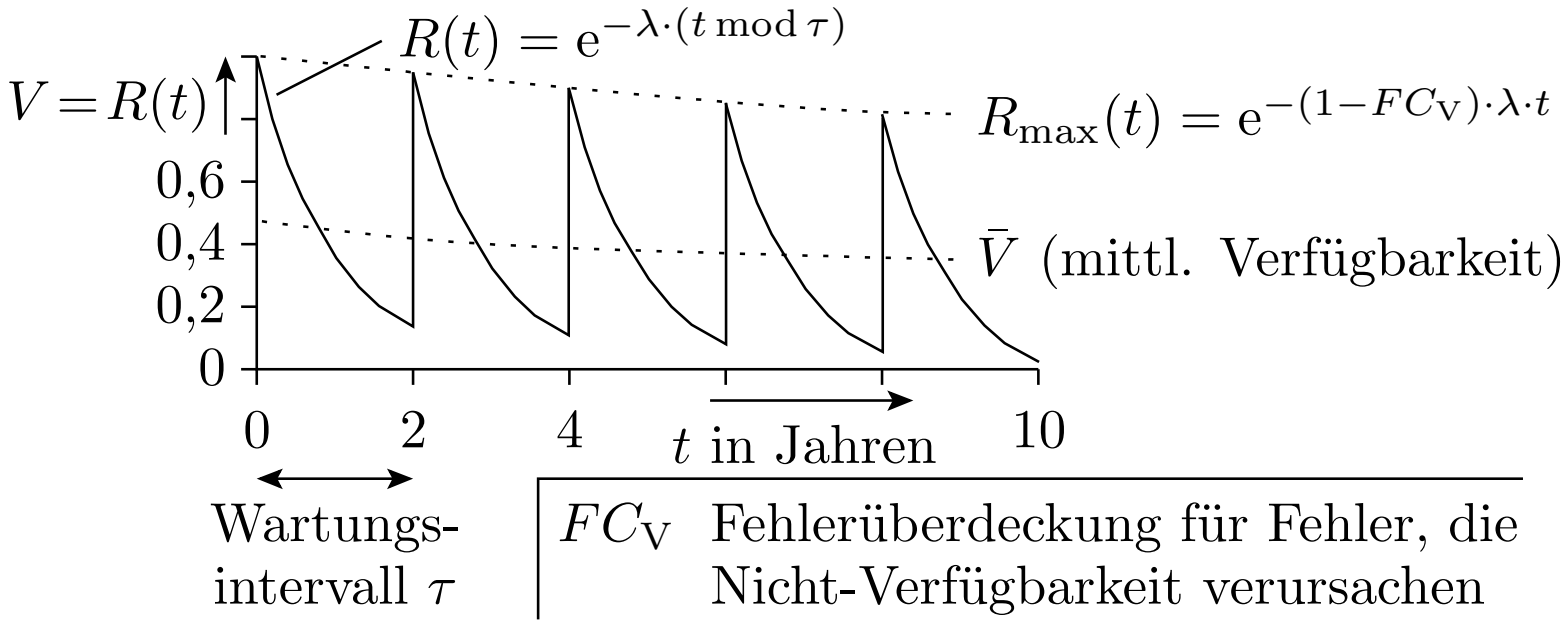
Wartungsintervall τ: Zeit zwischen den Wartungen, z.B. 1 Jahr.

Verfügbarkeit und Wartung



Die Verfügbarkeit ist gleich der Überlebenswahrscheinlichkeit.

Zwischen den Wartungen sinkt die Überlebenswahrscheinlichkeit in der Hauptnutzungsphase entsprechend Gl. 1 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

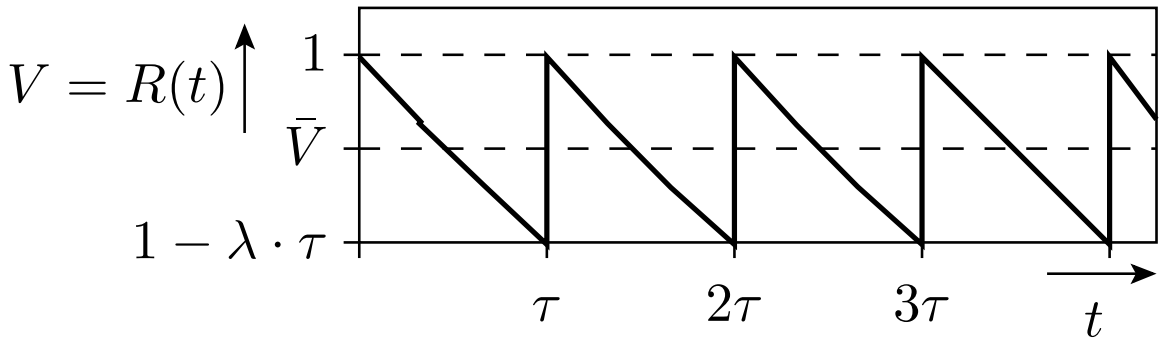
$$FC_{\mathrm{V}} < 1$$

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 $\lambda \cdot \tau \ll 1$:

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

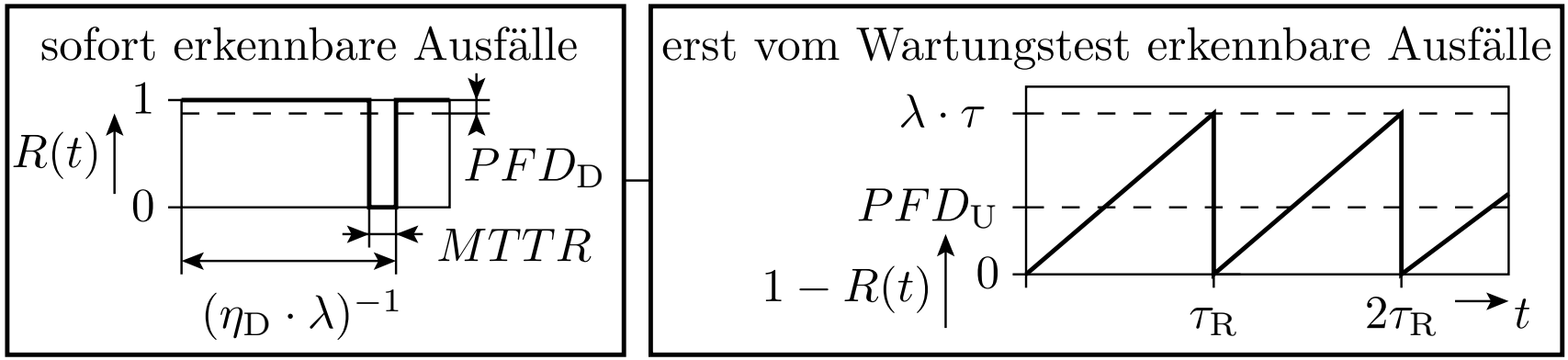
mit

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

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

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

Beseitigung sofort bemerkter Ausfälle

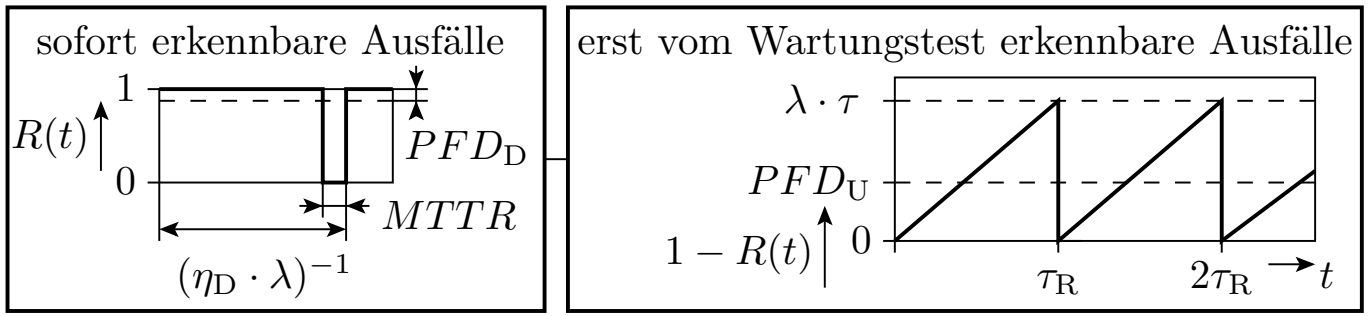


Ein Anteil η_D der Ausfälle wird sofort bemerkt und mit der $MTTR$ (Mean Time to Repair) beseitigt. Modellierung als Reihenschaltung

- eines Systems mit den sofort erkennbaren Ausfällen. Mittlere Zeit zwischen zwei Ausfällen $1/\left(\eta_\mathrm{D} \cdot \lambda\right)$. Mittler Wahrscheinlichkeit, dass dieses 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.

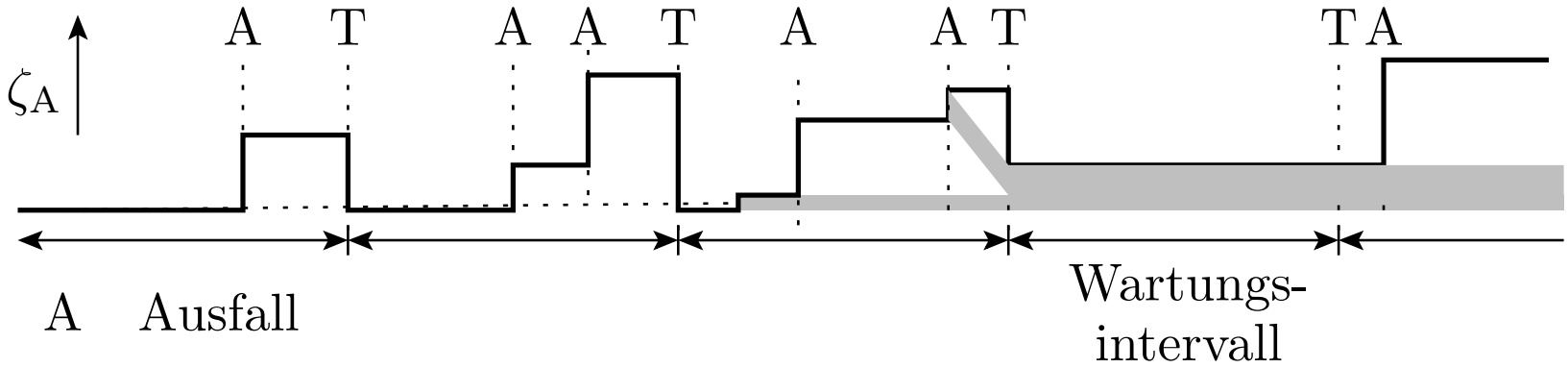
Beispiel 1

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



A Ausfall

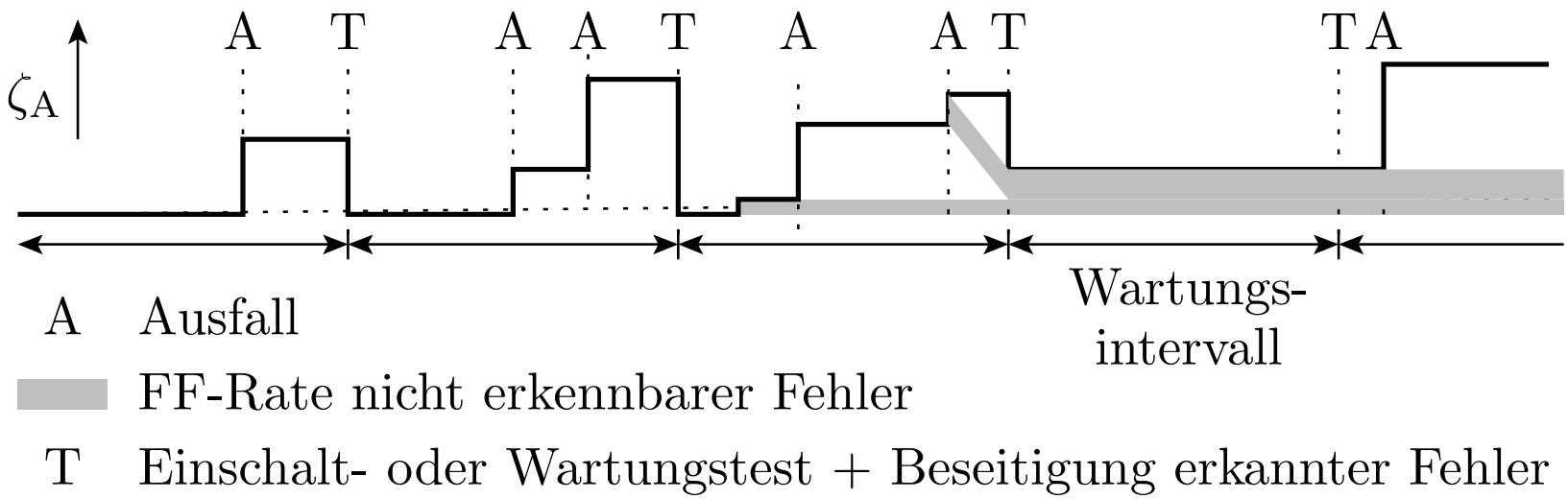
FF-Rate nicht erkennbarer Fehler

T Einschalt- oder Wartungstest + Beseitigung erkannter Fehler

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.

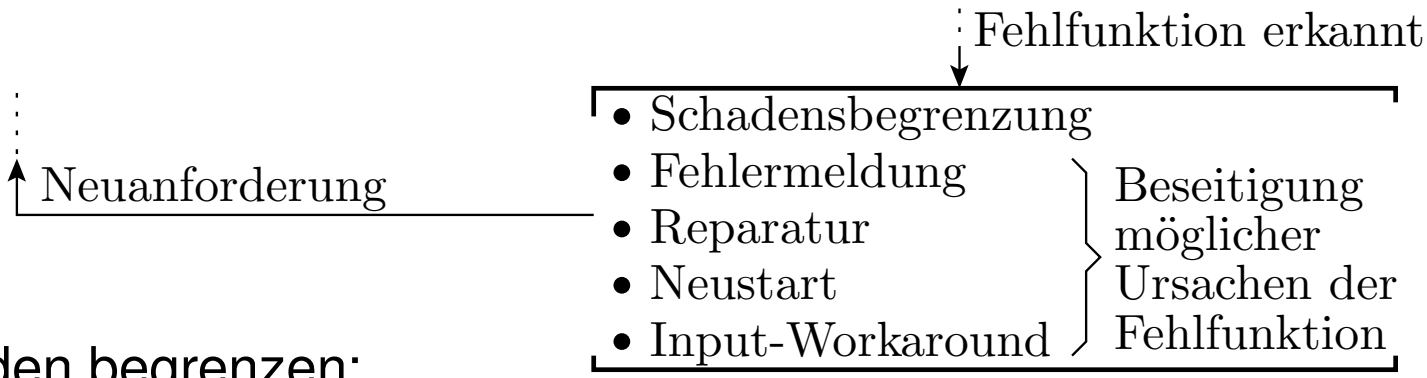
Fehlertoleranz

Fehlertoleranz

Von lateinisch tolerare »erleiden«, »erdulden«. In der Technik, aufrechterhalten der Funktion bei unvorhergesehene Eingaben oder oder internen FF. Stufen der Fehlertoleranz:

- go: System reagiert sicher und korrekt.
- fail-operational: Verbleib in einem betriebsfähigem Zustand.
- fail-soft: Systembetrieb sicher, aber Leistung vermindert
- fail-safe: Nur Systemsicherheit gewährleistet
- fail-unsafe: unvorhersehbares Systemverhalten

Maßnahmen FF-Behandlung / Fehlertoleranz



Schaden begrenzen:

- Bearbeitungsabbruch, Daten sichern, ...
- Herstellen eines sicheren Zustands, z.B. Notausschaltung.

Daten zur Fehlerlokalisierung erfassen:

- Fehlermeldung, Core-Dump, Cap-Datei (Windows) erzeugen.

Wiederholung / Vermeidung desselben Versagens:

- Fehlerbeseitigung: Hardware-Tausch, Updates einspielen,
- Rekonfiguration mit/ohne verringerte Leistung, ...
- Neuinitialisierung.
- Diversitäre Service-Anforderung / Berechnung: Geänderte Service-Reihung, Eingaben, Berechnungsfluß, ...

Kenngrößen der FF-Behandlung

- Robustheit (Anteil der FF ohne unvorhersehbares Systemverhalten):

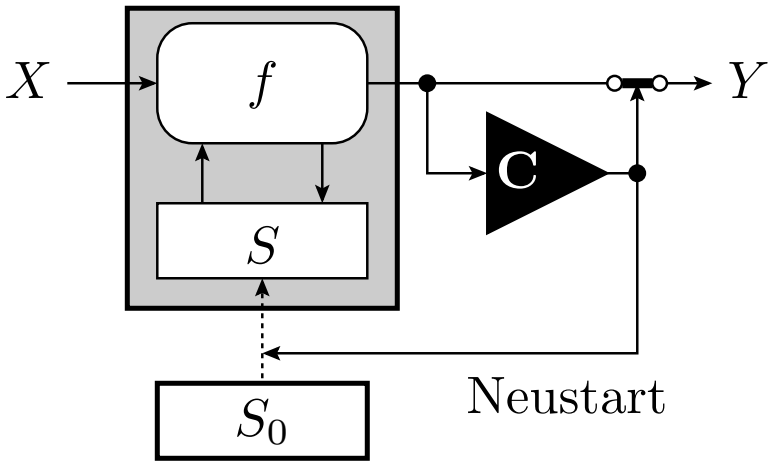
$$ROB = \frac{\#FFR}{\#FF} \tag{2}$$

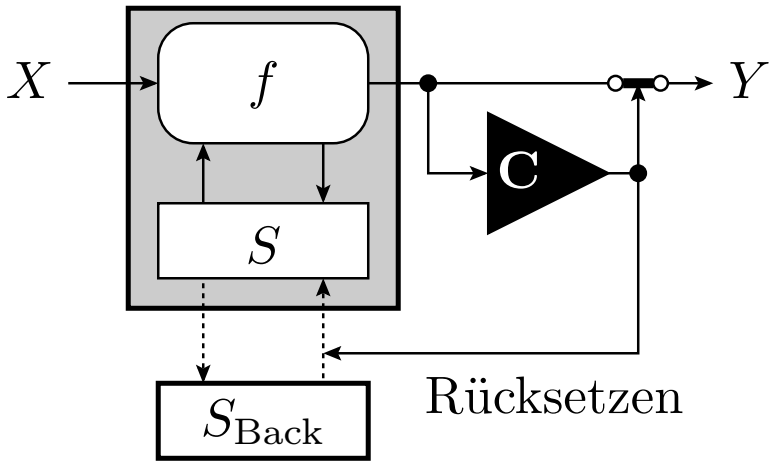
- Fehlertoleranz (Anteil der FF, die das System selbst korrigiert):

$$FT = \frac{\#FFT}{\#FF} \tag{3}$$

($\#FFR$ – Anzahl der internen FF ohne unvorhersehbares Systemverhalten; $\#FFS$ – Anzahl der tolerierten internen FF). Fehlertoleranz setzt Robustheit und Robustheit Nachweisbarkeit der FF voraus.

Neuinitialisierung





Systeme mit internen Daten nach jeder FF neu initialisieren:

- Statische Neuinitialisierung (Reset): fester Anfangszustand,
- Dynamische Neuinitialisierung: Regelmäßiges Backup wärend des Betriebs. Laden des letzten Backups nach Crash.

  Oft werden nur Daten gesichert, die sich nicht problemlos neu berechnen lassen, bei Editoren, Logistiksysteme, Datenbanken, ... die Eingaben seit dem letzten kompletten Backup.

  Berechnungswiederholung vom letzten Backup bis Versagen.

Fail-Fast, Fail-Slow und Ruhestromprinzip

- Fail Fast: Abbruch bei erkannten FF, üblich in der Testphase zur Fehlersuche.
- Fail-Slow: Funktion so lange wie möglich aufrechterhalten, z.B
  - Ersatz fehlerhafter Daten durch sinnvolle Standardwerte,
  - Bei WB-Überlauf Begrenzung auf zulässige Werte,
  - Suche fehlender Dateien an anderen Orten,
  - ...
- Ruhestromprinzip: Konstruktionsprinzip, bei dem das System bei Versagen automatisch in einen sicheren Zustand übergeht.
  - Eisenbahnsignaltechnik: bei fehlendem Ruhestrom Störungsmeldung.
  - Brandmeldeanlage: bei Drahtbruch Alarm.
  - Fahrzeugbremse: Bremsen, wenn Bremsschlauch platzt.
  - ...

Fehlerisolation

Fehlerisolation

Eine sinnvolle automatische Reaktion auf eine FF benötigt

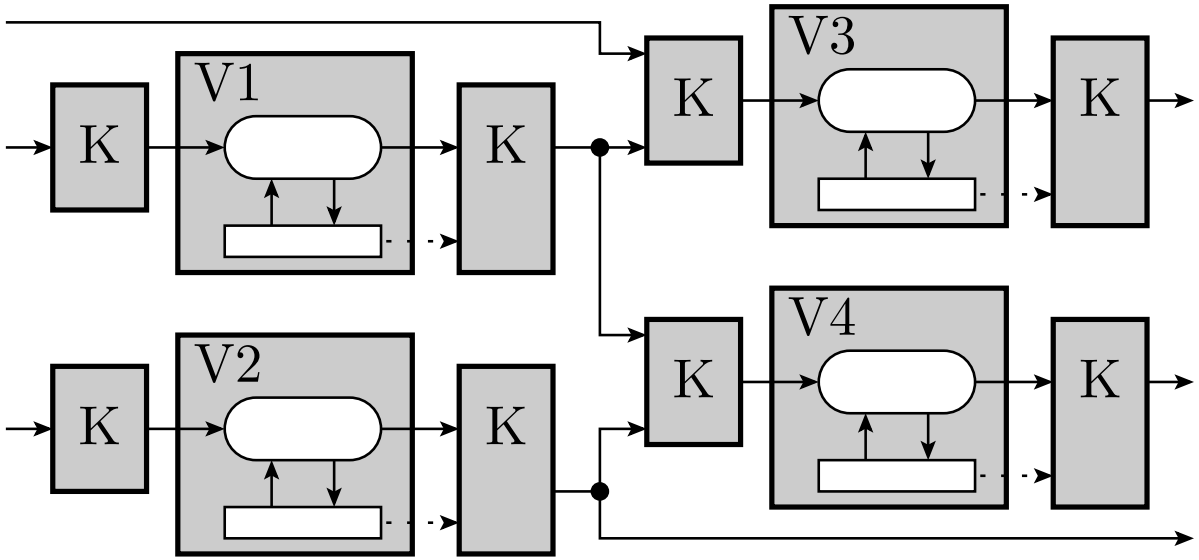
- von der FF nicht kontaminierte Daten und
- von der Entstehungsursache der FF unbeeinträchtigte Systemteile.

Techniken zur Fehlerisolation:

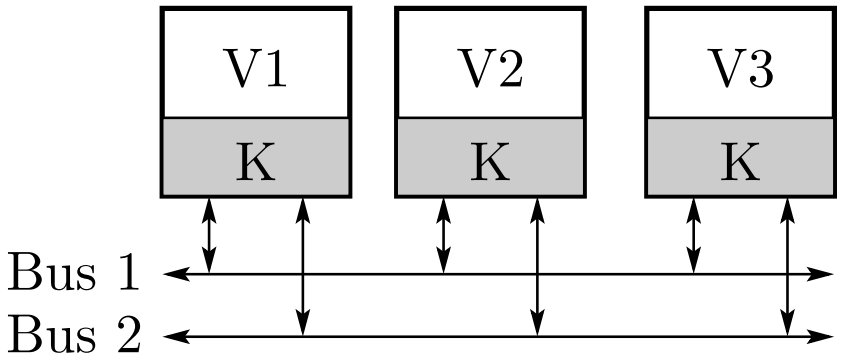
- Datenkontrolle an Schnittstellen zwischen Teilsystemen. Keine Weitergabe erkannter verfälschter Daten.
- Keine Zugriffmöglichkeit auf interne Daten fremder Funktionseinheiten.
- Physikatisch und räumlich getrennte Systeme (Risikominderung gleicher Fehler, zeitgleicher Ausfälle, ...).
- ...

Architekturen zur Fehlerisolation

- Berechnungskonoten mit gerichtetem Datenfluss



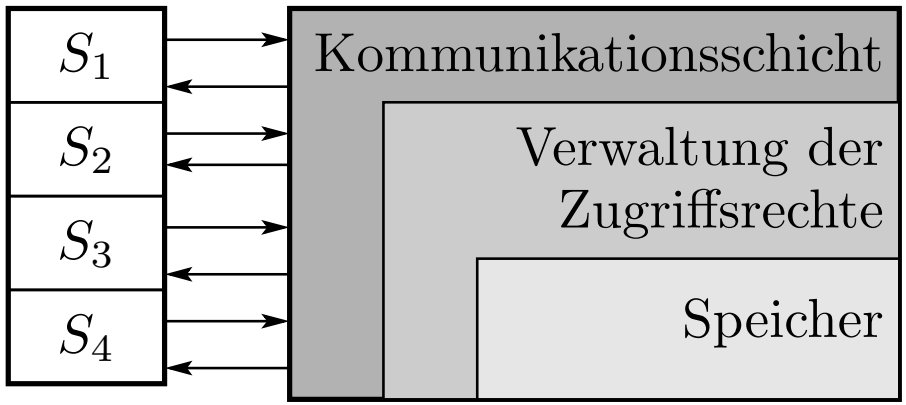
- Steuergeräte an einem redundanten Bussystem



V Verarbeitungs-baustein

K Überwachung und Fehler-isolation

Fehlerisolation in Betriebssystemen



Die zu isolierenden Teilsysteme sind die Prozesse S_i.

- Jeder Prozess sieht nur seinen eigenen virtuellen Speicher,
- die ihm zugeordneten Ein- und Ausgabegeräte und
- bekommt den Prozessor zeitscheibenweise zugeteilt.

Resourcen-Zuordnung (physikalischer Speicher, Ein- und Ausgabegeräte, Kommunikation zu anderen Prozessen, ...) nur über Systemrufe möglich. Nur der Betriebssystemkern hat Universalzugriff (und kann alle Daten kontaminieren).

Redundanz

Gleichschrittsysteme

- Gleichschrittsysteme: Parallele Ausführung der SL auf replizierten Funktionsbausteinen. Im fehlerfreien Fall übereinstimmende SL und übereinstimmende interne Zustände.
- Sanfter Leistungsabfall (Graceful degradation): Nach Ausfall von Systemkomponenten Fortsetzung (eines Notbetriebs) mit verlängerter Verarbeitungszeit oder vermindertetem Service.

Noo$M$ (N out of M): N benötigte von M vorhandenen Replik.:

- 1oo1: Einfaches System. Nach Ausfall Reparatur.
- 1oo2: Überwachung durch Vergleich. Ab Teilsystemausfall bis Reparatur Betrieb als 1oo1.
- 2oo2: Überwachung durch Vergleich. Ab Teilsystemausfall bis Reparatur optional Betrieb als 1oo1 mit reduzierter Leistung.
- 2oo3: Mehrheitsentscheid. Ab Teilsystemausfall bis Reparatur Betrieb als 2oo2.

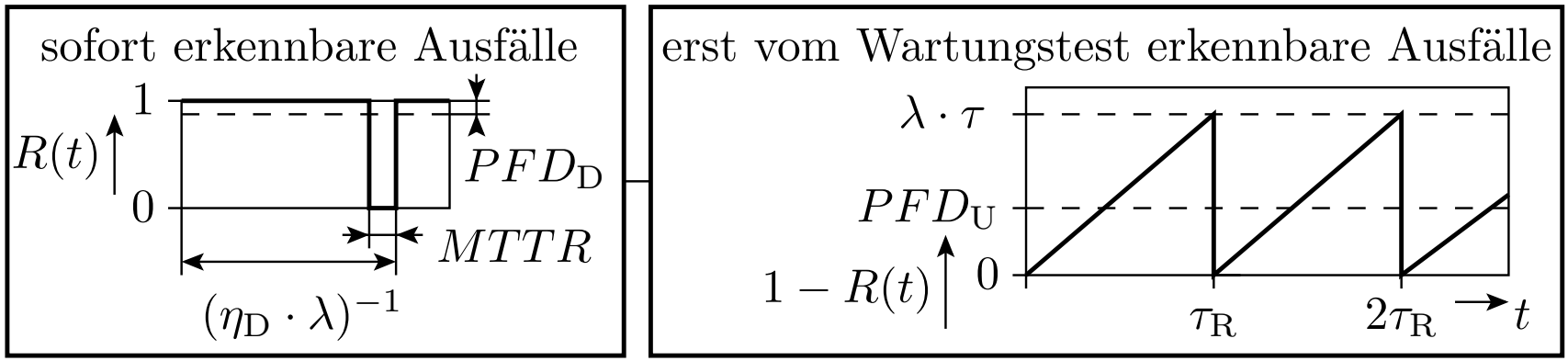
- Alle redundanzfreien Systeme, die regelmäßig gewartet werden, z.B. wie Autos zum TÜV müssen, sind 1oo1.
- Im Maschinenbau je nach Sicherheitsstufe: 1oo1- oder 1oo2.
- Prozessindustrie und Systeme ohne einen in kurzer Zeit erreichbaren sicheren Zustand (z. B.: Flugzeugsteuerungen, Atomkraftwerke, Chemiereaktoren) auch höhere Redundanzen 2oo2, 2oo3 oder 2oo4 üblich.

Sanfter Leistungsabfall

- Bei Komponentenausfall Umverteilung von Aufgaben auf andere Systembestandteile.
- Bei Notstromversorgung Abschalten von Systemteilen.
- Transmission Control Protocol (TCP): auch dann noch eine sichere Punkt-zu-Punkt-Verbindung, wenn einzelne Knoten im Netzwerk überlastet, falsch eingestellt sind oder Daten verfälschen.
- HTML ist aufwärtskompatibel so aufgebaut, dass älterer Browser neue HTML-Einheiten, die sie nicht kennen, ignorieren und den Rest des Dokuments trotzdem dargestellen.
- Ausschluss / Ersatz fehlerhafter Rechner-Knoten und Aufgabenumverteilung auf die verringerte Anzahl.

Verfügbarkeit 1oo1 mit Wartungsintervall τ

1oo1 ist ein System ohne Redundanz. Verfügbarkeit und PFD (Probability of Failure on Demand) siehe Foliensatz 7, Abschnitt 1.5 Wartung.



Sofort erkennbare Ausfälle treten mit einer Rate $\eta_{\mathrm{D}} \cdot \lambda$ im mittleren Abstand von $(\eta_{\mathrm{D}} \cdot \lambda)^{-1}$ auf, haben eine mittlere Beseitigungszeit $MTTR \ll \lambda_{\mathrm{DD}}^{-1}$ und sind im Mittel mit Wahrscheinlichkeit:

$$PFD_{1001\mathrm{D}} = \eta_{\mathrm{D}} \cdot \lambda \cdot MTTR$$

vorhanden. Ausfälle, die erst bei der Wartung beseitigt werden ...

Ausfälle, die erst vom Wartungstest erkannt werden, sind im Mittel mit Wahrscheinlichkeit

$$PFD_{1001\mathrm{U}} = \frac{(1-\eta_{\mathrm{D}}) \cdot \lambda \cdot \tau}{2}$$

vorhanden. System nicht verfügbar, wenn wegen sofort erkennbarem ODER erst vom Wartungstest erkennbarem Ausfall nicht verfügbar. Für kleine $PFD_{\ldots} \ll 1$ mit guter Näherung:

$$\begin{aligned} PFD_{1\mathrm{oo}1} &= PFD_{1001\mathrm{D}} + PFD_{1001\mathrm{U}} \\ &= \eta_{\mathrm{D}} \cdot \lambda \cdot MTTR + \frac{(1-\eta_{\mathrm{D}}) \cdot \lambda \cdot \tau}{2} \end{aligned}$$

(τ – Wartungsintervall incl. mittlere Reparaturzeit; $MTTR$ – mittlere Reparaturzeit außerhalb der Wartung). Verfügbarkeit als Gegenwahrscheinlichkeit:

$$V_{1\mathrm{oo}1} = 1 - PFD_{1\mathrm{oo}1}$$

Beispiel 2

KFZ: Wartungsintervall $\tau = \frac{10.000\text{km}}{50\,\text{km/h}} = 200\text{h}$, $\lambda = 10^{-3}\,\text{h}^{-1}$, $\eta_\text{D} = 80\%$, $MTTR = 2\,\text{h}$. Gesucht:

- PFD (Probability of Failure on Demand) und
- mittlere Wahrscheinlichkeit, dass das KFZ sicher verfügbar ist:

$$\begin{aligned} PFD_\text{KFZ} &= \eta_\text{D} \cdot \lambda \cdot MTTR + \frac{(1-\eta_\text{D}) \cdot \lambda \cdot \tau}{2} \\ &= 0{,}8 \cdot 10^{-3}\,\text{h}^{-1} \cdot 2\,\text{h} + \frac{0{,}2 \cdot 10^{-3}\,\text{h}^{-1} \cdot 200\text{h}}{2} \\ &= 2{,}16\% \\ V_\text{KFZ} &= 1 - PFD_\text{KFZ} = 97{,}84\% \end{aligned}$$

Verfügbarkeit redundanter 1oo2-Systeme

Wahrscheinlichkeit, dass mindestens eine von zwei unabhängig ausfallenden Komponenten mit Überlebenswahrscheinlichkeit $e^{\lambda t}$ nicht ausgefallen ist:

$$\begin{aligned} R(t)_{1\text{oo}2\text{U}} &= 1 - \left(1 - e^{\lambda t}\right)^2 \\ &= 2 \cdot e^{\lambda t} - e^{2\lambda t} \end{aligned}$$

Verfügbarkeit als mittlere Überlebenswahrscheinlichkeit in einem Wartungsintervall τ:

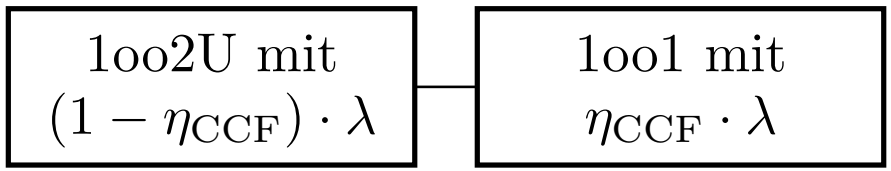
$$\begin{aligned} \bar{V}_{1\text{oo}2\text{U}} &= \frac{1}{\tau} \int_0^\tau \left(2 \cdot e^{\lambda t} - e^{2\lambda t}\right) \cdot \mathrm{d}\tau \\ &= \frac{2}{\lambda\tau} \cdot \left(1 - e^{\lambda t}\right) - \frac{1}{2\lambda\tau} \cdot \left(1 - e^{2\lambda t}\right) \end{aligned}$$

Mit der Näherung:

$$e^{-x} = 1 - x + \frac{x^2}{2} - \frac{x^3}{6}$$

$$\bar{V}_{1oo2U} = \frac{2}{\lambda\tau} \cdot \left(1 - \left(1 - \lambda\tau + \frac{(\lambda\tau)^2}{2} - \frac{(\lambda\tau)^3}{6}\right)\right)$$
$$- \frac{1}{2\lambda\tau} \cdot \left(1 - \left(1 - 2\lambda\tau + \frac{(2\lambda\tau)^2}{2} - \frac{(2\lambda\tau)^3}{6}\right)\right) = 1 - \frac{(\lambda\tau)^2}{3}$$

$$PFD_{1oo2U} = 1 - \bar{V}_{1oo2U} = \frac{(\lambda\tau)^2}{3}$$



Ein Anteil η_{CCF} der Ausfälle verursacht wegen gemeinsamer Ursachen (Common Cause Failurs) den gleichzeitigen Ausfall beider Systeme. Modellierung als Reihenschaltung:

- 1oo2-System für alle unabhängigen Ausfälle und

$$PFD_{1oo2U} = \frac{(1 - \eta_{CCF}) \cdot (\lambda\tau)^2}{3}$$

- ein 1oo1-System für die gleichzeitigen Ausfälle ...

- ein 1oo1-System für die gleichzeitigen Ausfälle:

$$PFD_{1oo1} = \eta_{CCF} \cdot \eta_D \cdot \lambda \cdot MTTR + \frac{\eta_{CCF} \cdot (1 - \eta_D) \cdot \lambda \cdot \tau}{2}$$

Gesamt-PDF für $PFD_{\ldots} \ll 1$ für Reparatur, solange noch eine Komponente verfügbar ist, erst zum Wartungstermin:

$$PFD_{1oo2} = \frac{((1 - \eta_{CCF}) \cdot \lambda \cdot \tau)^2}{3} + \eta_{CCF} \cdot \eta_D \cdot \lambda \cdot MTTR + \frac{\eta_{CCF} \cdot (1 - \eta_D) \cdot \lambda \cdot \tau}{2}$$

Weitere N aus M Systeme

- 2oo2: Zwei identische Systeme (Master und Checker) im Gleichschritt mit Ergebnisvergleich. Sobald ein System versagt, nicht mehr sicher verfügbar. Verfügbarkeit und PFD wie 1oo1 mit der doppelten Ausfallrate:

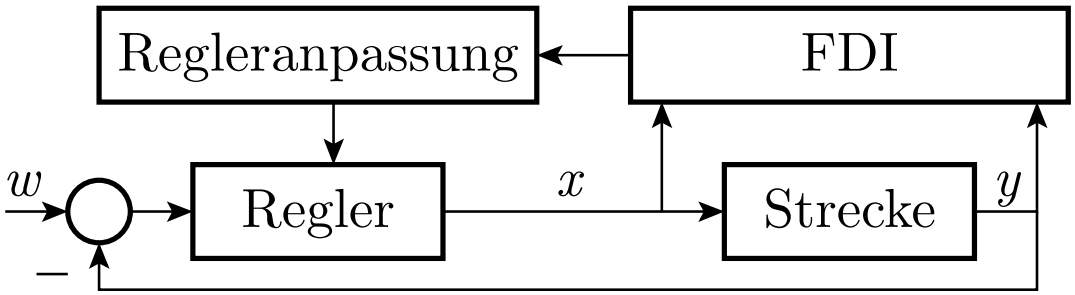
$$PFD_{2oo2} = 2 \cdot \eta_D \cdot \lambda \cdot MTTR + (1 - \eta_D) \cdot \lambda \cdot \tau$$

- PFD nach [3] für N von M funktionierende mit Ausfallrate λ unabhängig voneinander ausfallende identische Komponenten; Reparaturintervall τ:

N	Noo1	Noo2	Noo3	Noo4
1	$\frac{\lambda \cdot \tau}{2}$	$\frac{(\lambda \cdot \tau)^2}{3}$	$\frac{(\lambda \cdot \tau)^3}{4}$	$\frac{(\lambda \cdot \tau)^4}{5}$
2	-	$\lambda \cdot \tau$	$(\lambda \cdot \tau)^2$	$(\lambda \cdot \tau)^3$
3	-	-	$\frac{3 \cdot \lambda \cdot \tau}{2}$	$2 \cdot (\lambda \cdot \tau)^2$
4	-	-	-	$2 \cdot \lambda \cdot \tau$

Anwendungsspez. Lösungen

Fehlertolerantes Regelsystem

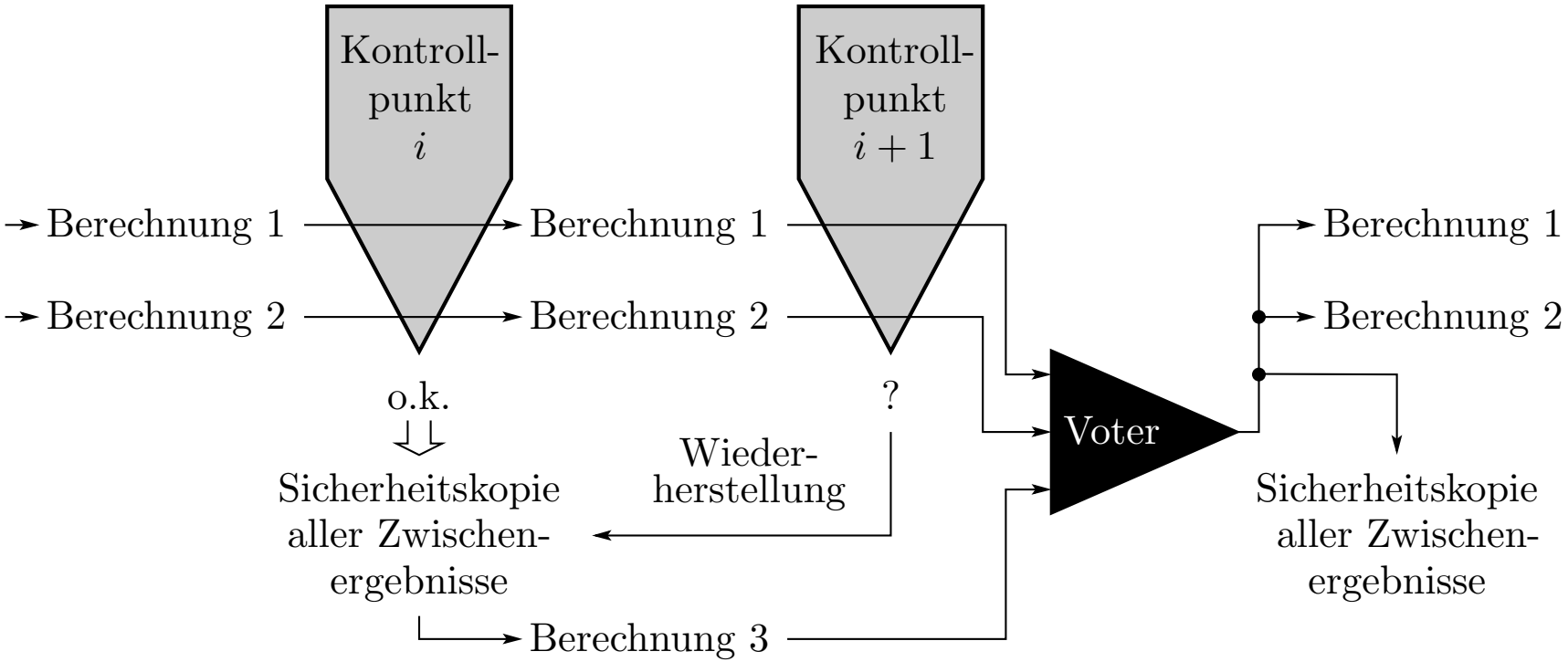


In einem Reglersystem wird vom Sollwert w der zu regelnde Ist-Wert y abgezogen. Aus der Differenz bildet der Regler den Stellwert x für die Regelstrecke (z.B. eine Heizung, wenn y eine Temperatur ist).

Fehlertoleranz gegenüber FF von Regler und Strecke:

- Zusatzmodul zur Fehlerdiagnose (Fehler Detektion, Isolation und Identifikation, FDI) überwacht Stellwert und Ist-Wert.
- Regleranpassung: Bei signalisierter FF, Änderung der Reglerfunktion so, dass eine Mindestfunktionalität gewährleistet bleibt.

Check-Point-Roll-Back-Recovery [2]



- Nur zwei parallel ausgeführte Berechnungen.
- An einprogrammierten Kontrollpunkten im Programm werden die Bearbeitungszustände[5] verglichen.

[5] Werte der Variablen, Register, ...

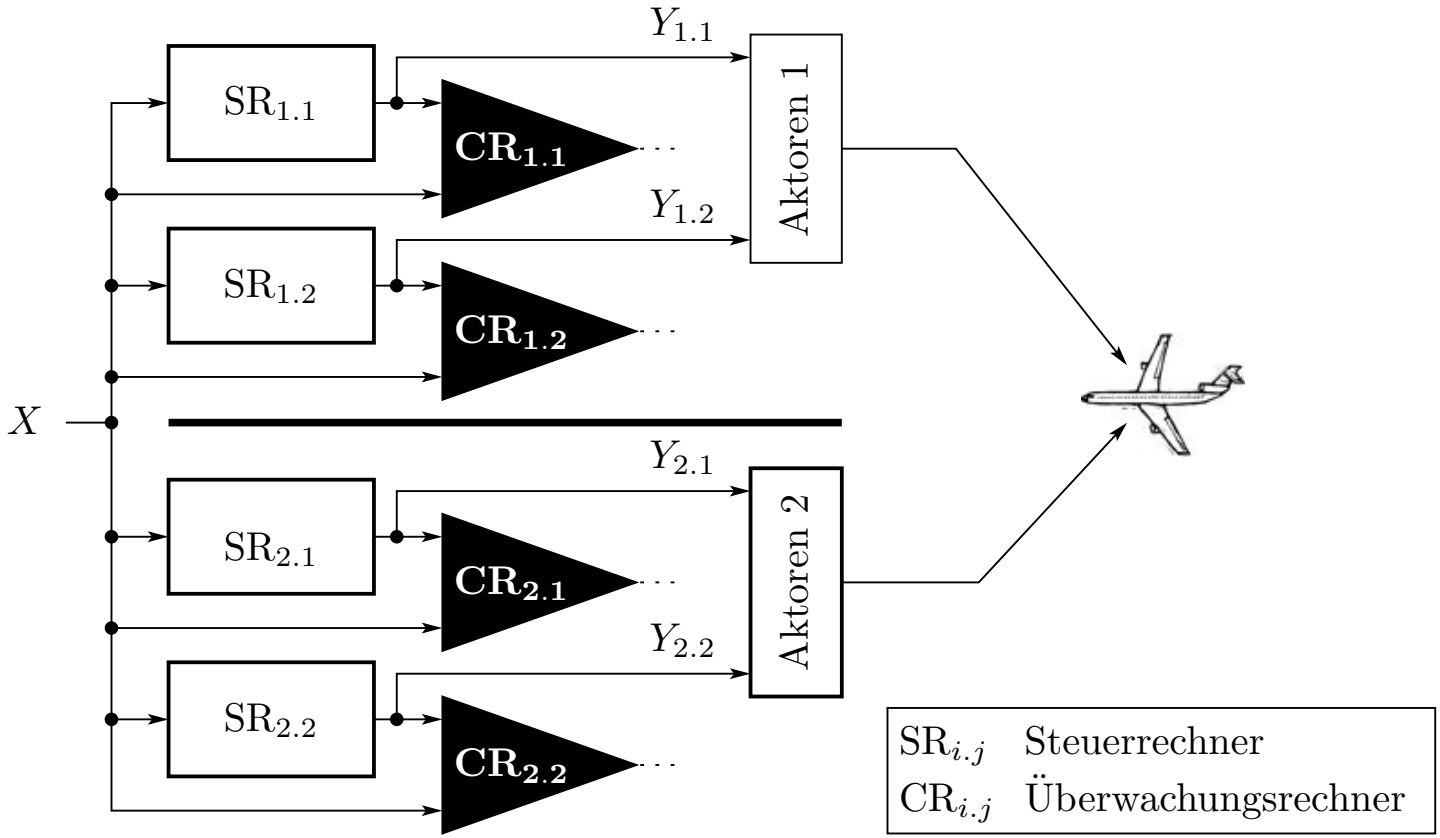
- Bei Übereinstimmung Speicherung des Bearbeitungszustands in einem geschützten Speicher.
- Bei Abweichung, Laden der letzten Sicherheitskopie und Berechnungswiederholung (Roll-Back Recovery).
- Nach Roll-Back Recovery am nächsten Kontrollpunkt wieder Vergleich.
- Wenn Übereinstimmung, diesen als gesicherten Zustand speichern, sonst Abbruch.

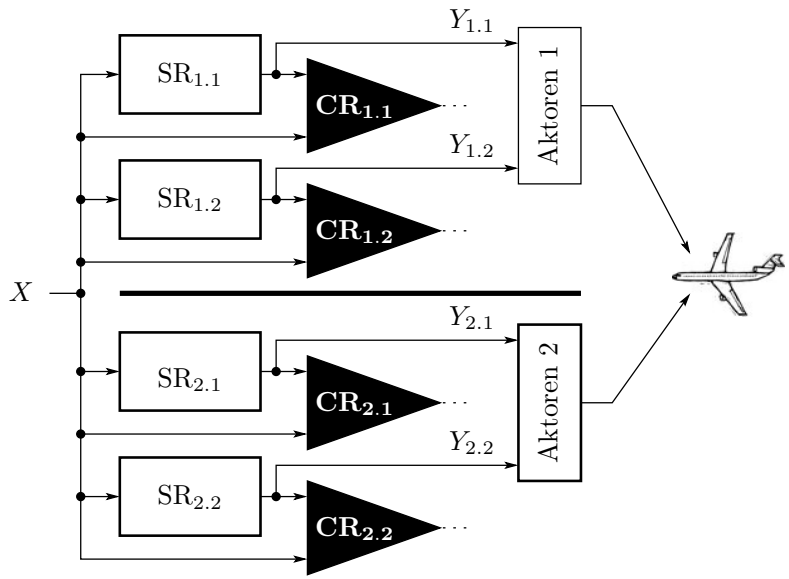
Sequoia-System [1]:

- Berechnung auf zwei Prozessoren mit eigenem Write-Back-Cache.
- Vergleich in jedem Takt.
- Zustands-Backup bei Ereignissen wie Stack-Überlauf und Prozesswechsel.
- Hauptspeicher hat die Funktion des stabilen Speichers.

Flugsteuersystem Airbus A3XX [4]

Hochsicherheitskritische Anwendungen müssen möglichst alle Fehlfunktionen, auch solche durch nicht erkannte Entwurfsfehler, nicht erkannte Fertigungsfehler und Ausfälle tolerieren.





- Zwei identische Systeme mit allen Sensoren, Aktoren und zwei Rechnerpaaren.
- Jedes Rechnerpaar besteht aus einem Steuerrechner $SR_{i.j}$, der die Aktoren ansteuert, und einem Überwachungsrechner $CR_{i.j}$.
- Normalzustand Rechner $SR_{1.1}$ steuert und $CR_{1.1}$ überwacht. Zweites Rechnerpaar Stand-By. System 2 abgeschaltet.
- Bei Ausfall übernimmt Rechnerpaar 1 von Rechnerpaar 2. Bei Komplett-, Sensor- oder Aktorausfällen übernimmt System 2 von System 1.

Diversität: Rechner unterschiedlicher Hersteller, getrennte Software-Entwicklung nach Spezifikationen, die unabhängig von einer gemeinsamen Basisspezifikation abgeleitet wurden.

RAID und Backup

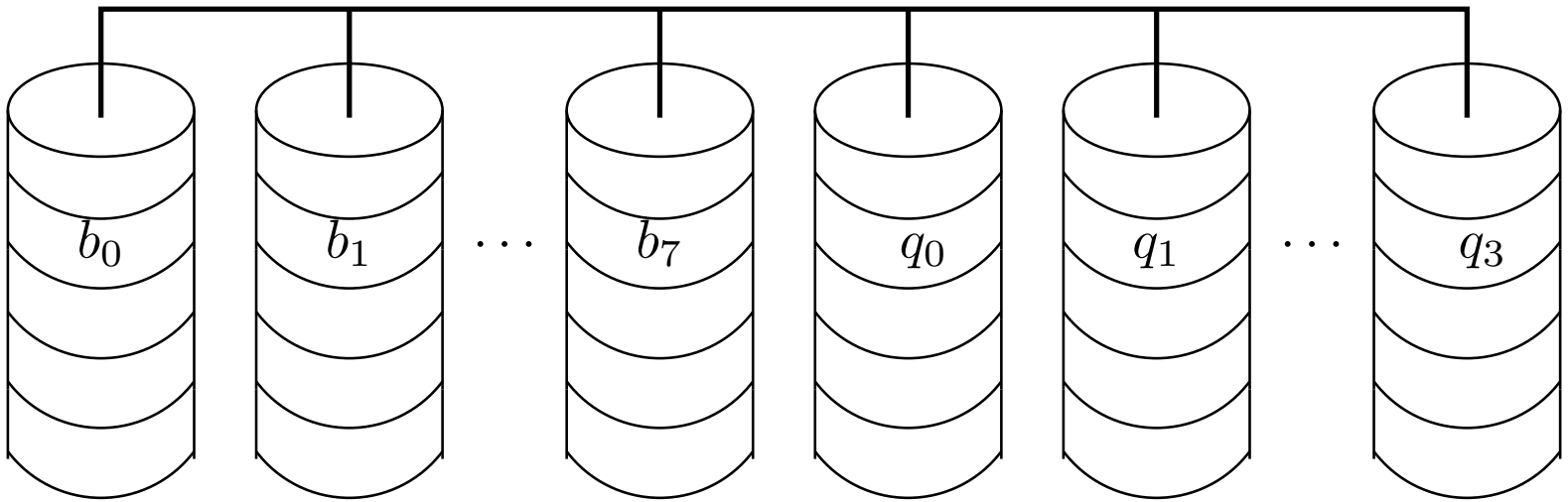
RAID, RAID Level 1

RAID – **R**edundant **A**rray of **I**ndependent **D**isks. Anwendung der behandelten Codes zur Korrektur bei Datenspeicherung auf Festplatten.

RAID Level 1: Zwei gespiegelte Festplatten. Die Daten werden versetzt geschrieben, so dass das Schreiben etwas länger dauert, aber mit nahe doppelter Geschwindigkeit gelesen werden kann. Bei Ausfall einer Platte existieren alle Daten noch auf der zweiten Festplatte. Die Lesegeschwindigkeit reduziert sich, aber das System bleibt funktionsfähig.

RAID Level 2

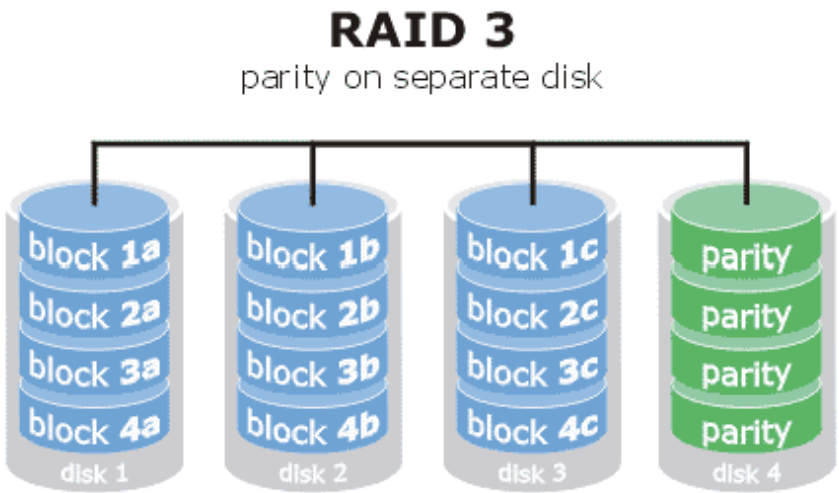
Bei RAID Level 2 werden die Daten in einem 1-Bit-korrigierenden Hamming-Code gespeichert, und zwar jedes der w Daten- und der r Kontrollbits auf einer anderen Platte, z.B. $w = 8$ Datenbit- und $r = 4$ Kontrollbitplatten. Im Vergleich zu RAID 1 werden statt der doppelten Plattenanzahl nur 50% mehr Platten benötigt.



Gilt als aufwändig und ungebräuchlich.

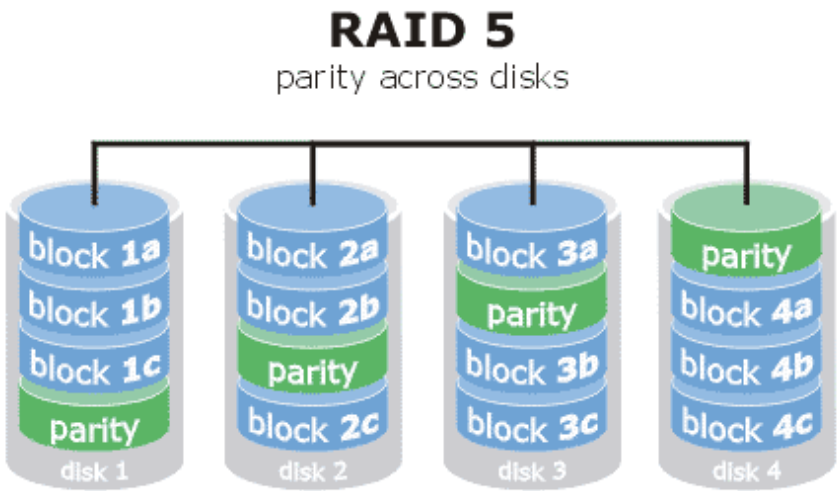
RAID Level 3

Auf einer Extra-Platte wird bitweise die Querparitätsbit der anderen Platten gebildet. Zusätzlich werden auf jeder Platte die Längsparitätsbits (oder Prüfkennzeichen) gespeichert. Mit einer zusätzlichen Blockparität ist eine 1-Bit-Fehlerkorrektur nach dem Prinzip der Kreuzparität. Erlaubt die Tolerierung eines einzelnen Plattenausfalls.



RAID Level 5

Fehlertoleranz ähnlich wie Level 3, nur dass Datenzugriffe durch unabhängige Lese- und Schreiboperationen (statt ausschließlich parallel) erlaubt sind. Größere schreibbare Datenblöcke. Die Paritätsinformation verteilt sich auf alle Platten. Gleichfalls tolerant gegenüber einem einzelnen Plattenausfall. Am häufigsten genutzte RAID-Struktur.



RAID ist kein Backup-Ersatz

Backup: Sicherungskopien von (wichtigen / aufwändig neu zu erzeugenden) Daten. Typisch:

- Tägliche automatische Erstellung durch das Rechenzentrum.
- Nur Änderungen zum letzten Backup.
- Aufbewahrung mehrerer Versionen an einem getrennten Ort.

Wird benötigt zur Datenwiederherstellung nach

- gleichzeitiger Zerstörung aller Platten z.B. durch Überspannungsspitzen, Feuer, ...
- Diebstahl von Datenträgern,
- einem versehentlichen Löschen, das erst nach Stunden oder Wochen bemerkt wird.

Literatur

3. Literatur

[1] P.A. Bernstein.
Sequoia: a fault-tolerant tightly coupled multiprocessor for transaction processing.
Computer, 21(2):37–45, 1988.

[2] D. K. Pradhan, D. D. Sharma, and N. H Vaidya.
Roll-forward checkpointing schemes.
In *Lecture Notes in Computer Science 744*, pages 93–116. Springer Verlag, 1994.

[3] Marvin Rausand and Arnljot Hsyland.
Systems Reliability Theory, Models, Statistical Methods, and Applications.
Wiley-Interscience, 2004.

[4] Pascal Traverse.
Dependability of digital computers on board airplanes.
Dependable Computing for critical applications, 4:134–152, 1991.