Grundlagen zuverlässiger fehlertoleranter Systeme

Quellen:

Eugen Schäfer: "Zuverlässigkeit, Verfügbarkeit und Sicherheit in der Elektronik, Eine Brücke von der Zuverlässigkeittheorie zu den Aufgaben der Zuverlässigkeits-praxis", 1. Auflage, Vogel Verlag, 1979, ISBN 3-0823-0586-8,

Karl-Erwin Großpietsch: "Zuverlässigkeitstheoretische Grundlagen", GMD-Seminar, St. Augustin

Stefan Poledna: "Lecture on Fault-Tolerant Systems", Vorlesungsfolien, Institut für Technische Informatik, TU Wien, SoSe 1996

Grundlagen zuverlässiger Systeme

Verläßlichkeit (Zuverlässigkeit):

Die Verläßlichkeit (Dependability) eines Systems ist die Qualität einer vom System erbrachten Funktion (Service), in die begründbar und berechtigterweise Vertrauen (reliance) gesetzt werden kann.

Die Funktion (Service) ist das an der Schnittstelle zu anderen Systemen, die mit dem betrachteten System interagieren, beobachtbare Systemverhalten. Die Qualität bezieht sich auf die Übereinstimmung der erbrachten mit der spezifizierten Systemfunktion.

Terminologie:

- **Beeinträchtigungen (Impairments) : Fehler**
- **Attribute**
- **Maße**
- **Mechanismen**

Attribute der Zuverlässigkeit (Dependability)

Überlebensfähigkeit (Reliability) bedeutet Zuverlässigkeit in Hinblick auf ununterbrochenes korrektes Systemverhalten. Es ist als die Wahrscheinlichkeit definiert, daß ein zu Beginn fehlerfreies System bis zu einem bestimmten Zeitpunkt fehlerfrei bleibt.

Verfügbarkeit (Availability) bedeutet Zuverlässigkeit in Hinblick auf die momentane Bereitschaft eines Systems zur Erbringung eines Service. Verfügbarkeit wird als quantitaves Maß definiert, das die Ausfalldauer zu der Dauer korrekten Systemverhaltens in Beziehung setzt, d.h. die Wahrscheinlichkeit, das System zu einem beliebigen Zeitpunkt fehlerfrei anzutreffen.

Prozeßsicherheit (Safety) bedeutet Zuverlässigkeit in Hinblick auf das Verhindern katastrophaler Auswirkungen eines Systemverhaltens auf seine Umgebung, wobei mit Umgebung meist die physikalische, reale Umgebung gemeint ist, wie z.B. industrielle Prozeßsteuerungsanlagen, Kraftwerke, Verkehrslenkungssysteme, u.s.w.

Informationssicherheit (Security) bedeutet Zuverlässigkeit in Hinblick auf die Erhaltung der Vertraulichkeit (Confidentiality) und Integrität (Integrity) von Information in einem Computersystem.

Quantitative Ermittlung der Zuverlässigkeit

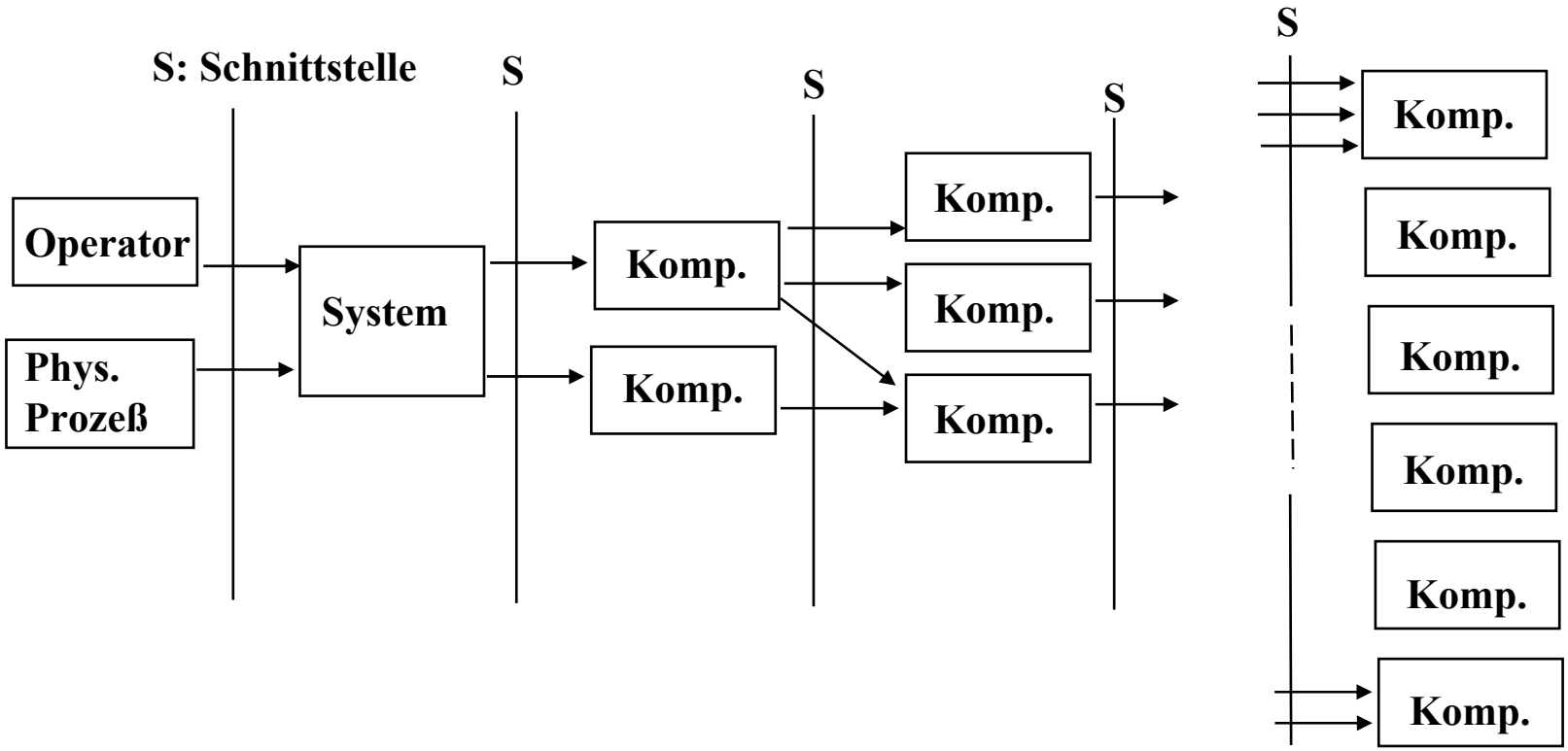
Strukturbasierte Modellierung:

- **identifizierbare unabhängige Komponenten**
- **jede Komponente besitzt eine bestimmte Zuverlässigkeit**
- **die Konstruktion des Modells basiert auf der Verbindungsstruktur zwischen den Komponenten**

Ein System wird definiert durch:

- **seine Struktur, d.h. die Topologie seiner Komponenten**
- **sein Verhalten, d.h. durch die Gesamtheit des Verhaltens seiner Komponenten**

Systemkomponenten sind hierarchisch organisiert. Dadurch ergibt sich eine Abhängigkeitsrelation ($\rightarrow$) zwischen den Systemebenen.



Quantitative Ermittlung der Zuverlässigkeit durch Zuverlässgkeitsschaltbilder

Intaktwahrscheinlichkeiten:

Für jeden Teil eines Systems werden zwei Zustände betrachtet:

• intakt (funktionstüchtig)
• defekt (ausgefallen)

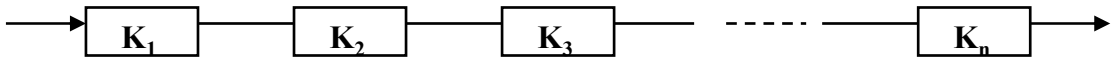
Intakt-Wahrscheinlichkeit einer Komponente oder eines Systems von Komponenten:
Wahrscheinlichkeit, dass die Komponente oder das System das spezifizierte Verhalten zeigen.

Ein System ist fehlertolerant, wenn es intakt sein kann, ohne dass alle Komponneten intakt sind.

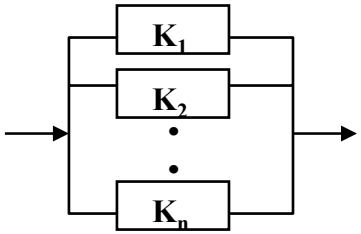
Zuverlässigkeits-Schaltbilder (nicht zu verwechseln mit elektrischen Schaltbildern) :

Abstraktion eines Systems in Komponenten, denen jeweils eine spezifische Zuverlässigkeit zugeordnet wird.

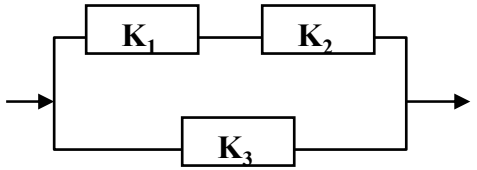
• **Seriensystem:**



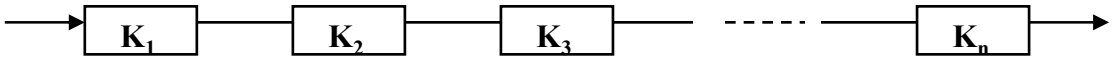
• **Parallelsystem:**



• **Serien/Parallelsystem:**



Intaktwahrscheinlichkeit für ein Seriensystem:



P_{serie} = P (K_1 intakt) und P(K_2 intakt) und .....P(K_n intakt)

Annahme: Die Eigenschaften (K_i intakt) (i=1,..,n) sind unabhängig.

⇒ P_{serie} = P (K_1 intakt) • P(K_2 intakt) • ..... •P(K_n intakt)

mit p_i : Intaktwahrscheinlichkeit der Komponente i:

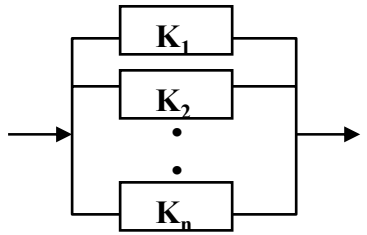
⇒ $P_{serie} = p_1 \bullet p_2 \bullet \ldots\ldots \bullet p_n$

Beispiel:

n identische Komponenten:

$P_{serie} = p_i^n$, n = 5, p_i = 0,99: $P_{serie} = 0{,}99^5 = 0{,}95$
$P_{serie} = p_i^n$, n = 5, p_i = 0,70 : $P_{serie} = 0{,}70^5 = 0{,}16$

Intaktwahrscheinlichkeit für ein Parallelsystem (1-aus-n) :



Defektwahrscheinlichkeit = 1 - Intaktwahrscheinlichkeit
(Intakt und defekt sind zueinander komplementäre Ereignisse).

$P_{parellel}$ = P (K_1 defekt) und P(K_2 defekt) und .....P(K_n defekt)

Annahme: Die Eigenschaften (K_i defekt) (i=1,..,n) sind unabhängig.

⇒ $P_{parellel} = P(K_1 \text{ defekt}) \bullet P(K_2 \text{ defekt}) \bullet ..... \bullet P(K_n \text{ defekt})$

Mit p_i : Defektwahrscheinlichkeit der Komponente i:

⇒ $P_{parellel} = p_1 \bullet p_2 \bullet ..... \bullet p_n$

Beispiel Defektwahrscheinlichkeit:

n identische Komponenten:

$P_{serie} = p_i^n$, n = 5, p_i = 1 - 0,99: $P_{serie} = 0{,}01^5 = 0{,}0000000001$ Intaktw.: 0,9999999999
$P_{serie} = p_i^n$, n = 5, p_i = 1- 0,70 : $P_{serie} = 0{,}30^5 = 0{,}00243$ Intaktw.: 0,99757

K - aus - n - Systeme

Systeme aus n Komponenten von denen mindestens k der Komponenten intakt sind.

Wahrscheinlichkeit, daß genau k ausgewählte Komponenten intakt (die Komponenten 1,..,k), die anderen Komponenten defekt sind (die Komponenten k+1,...,n).

$$P_{k\text{-aus-}n} = p_1 \bullet p_2 \bullet .... \bullet p_k \bullet (1 - p_{k+1}) \bullet (1 - p_{i+2}) \bullet .... \bullet (1- p_n)$$

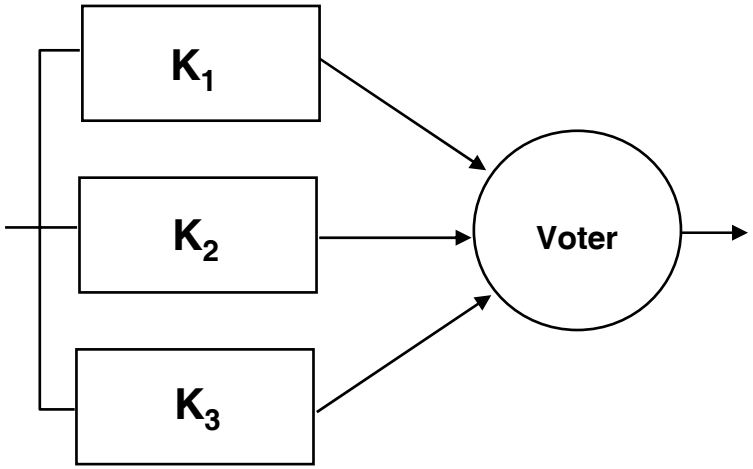
Es gibt $\binom{n}{i}$ Möglichkeiten, i Komponenten aus n Komponenten auszuwählen:

$$P_{k\text{-aus-}n} = \sum_{i=k}^{n} \binom{n}{i} \; p^i \bullet (1 - p)^{n- i}$$

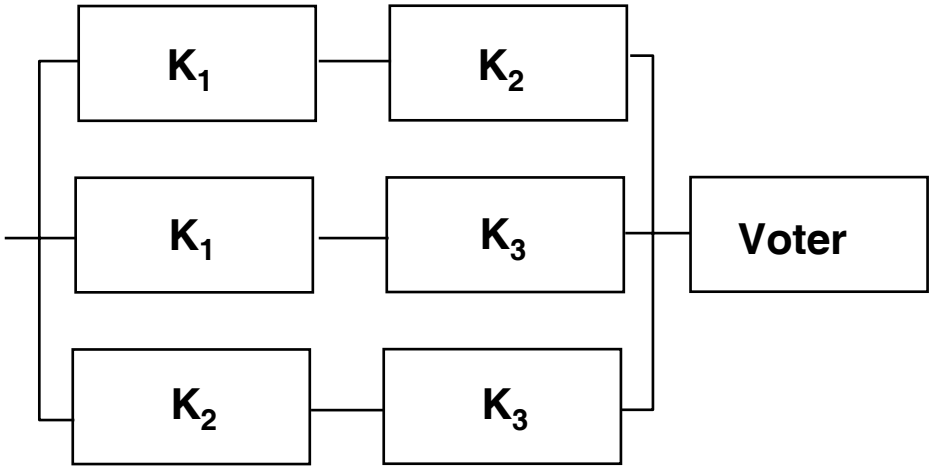
Beisp.: ein 2-aus-3 System: $\binom{3}{2} p^2 \bullet (1 - p)^{3-2} + \binom{3}{3} p^3 \bullet (1 - p)^{3-3} = 3 \bullet p^2 \bullet (1 - p) + p^3 \bullet 1$

Beispiel TMR (Triple Modulare Redundanz: 2-aus-3-System)

(Elektr.) Schaltbild



Zuverlässigkeits-Schaltbild



$$P_{TMR} = (p^3 + 3\,p^2 \bullet (1-p)\ ) \bullet p_{voter}$$

$$p = 0{,}9,\ p_{voter} = 0{,}99: P_{TMR} = (0{,}9^3 + 3 \bullet 0{,}9^2 \bullet (1-0{,}9)) \bullet 0{,}99$$

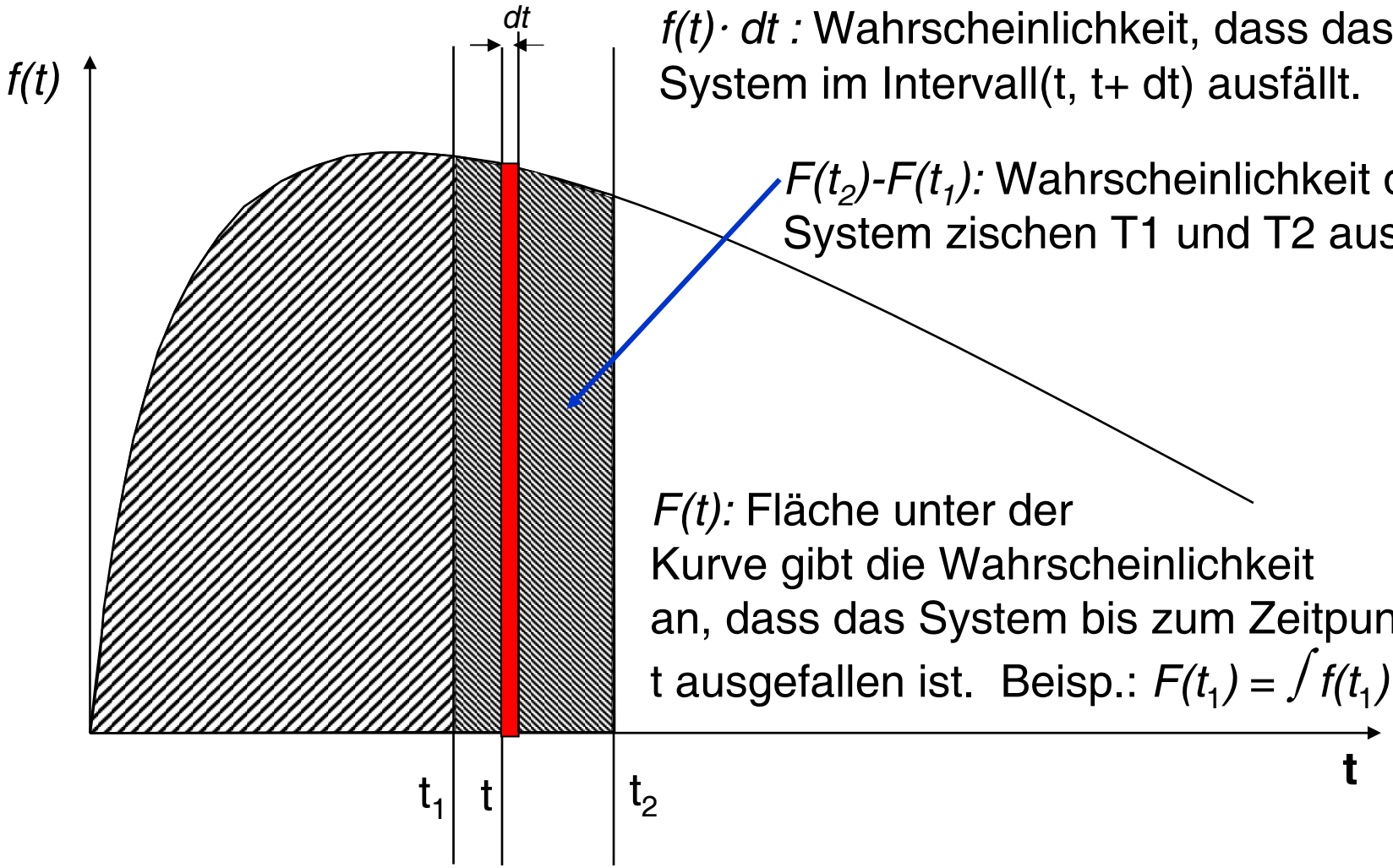
$$= (0{,}729 + 3 \bullet 0{,}81 \bullet (1-0{,}9)) \bullet 0{,}99$$

$$= (0{,}729 + 2{,}43 \bullet 0{,}1) \bullet 0{,}99 = 0{,}972 \bullet 0{,}99$$

$$= 0{,}96228$$

Wie werden die Wahrscheinlichkeiten für eine intakte oder defekte Komponente über die Zeit ermittelt ?

Lebensdauer-Modellierung



f(t)· dt : Wahrscheinlichkeit, dass das System im Intervall(t, t+ dt) ausfällt.

$F(t_2)$-$F(t_1)$: Wahrscheinlichkeit das das System zischen T1 und T2 ausfällt

F(t): Fläche unter der Kurve gibt die Wahrscheinlichkeit an, dass das System bis zum Zeitpunkt t ausgefallen ist. Beisp.: $F(t_1) = \int f(t_1)$

f(t): PDF: Probability Distribution Function

F(t): CDF: Cumulative Distribution Function. Für $t_{\rightarrow\infty}$: $F(t) = 1$

Maße der Fehlertoleranz

Lebensdauer T

Zeit vom Beanspruchungsbeginn (DIN 40 042) bis zum Totalausfall (nicht mehr reparierbar)

Ausfallwahrscheinlichkeit F(t)

ist die Wahrscheinlichkeit für eine Komponente bis zum Zeitpunkt $T < t_i$ auszufallen.

Überlebenswahrscheinlichkeit R(t) (Reliability)

Wahrscheinlichkeit, daß eine Komponente zum Zeitpunkt t_i noch nicht ausgefallen ist. F(t) ist das Komplement zu R(t).

$$R(t) = 1 - F(t)$$

Für nicht reparierbare Systeme ist R(t) eine monoton fallende Funktion. $R(0) \leq 1$, $R(\infty) = 0$

Ausfallwahrscheinlichkeitsdichte f(t)

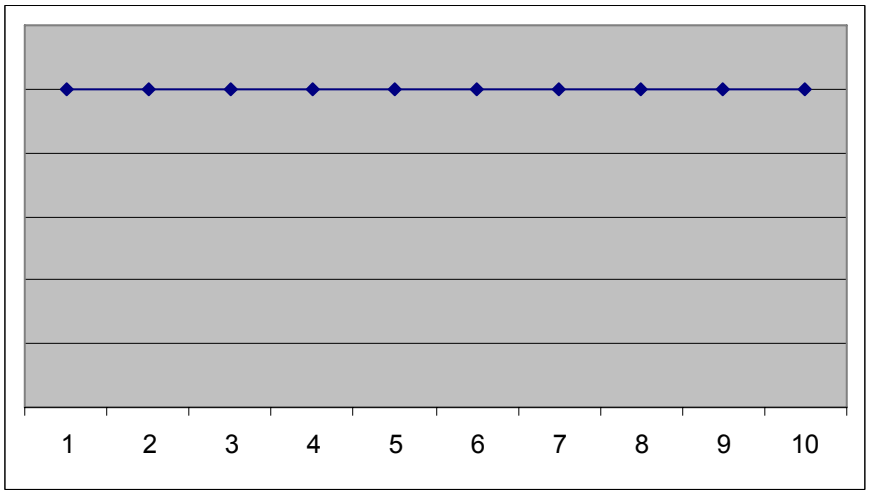
f(t) • dt ist die Wahrscheinlichkeit, daß der Ausfall einer Komponente im Zeitintervall (t, t+dt) auftritt.

f(t) ist dann die Wahrscheinlichkeit, mit der in diesem Zeitintervall Ausfälle erwartet werden können.

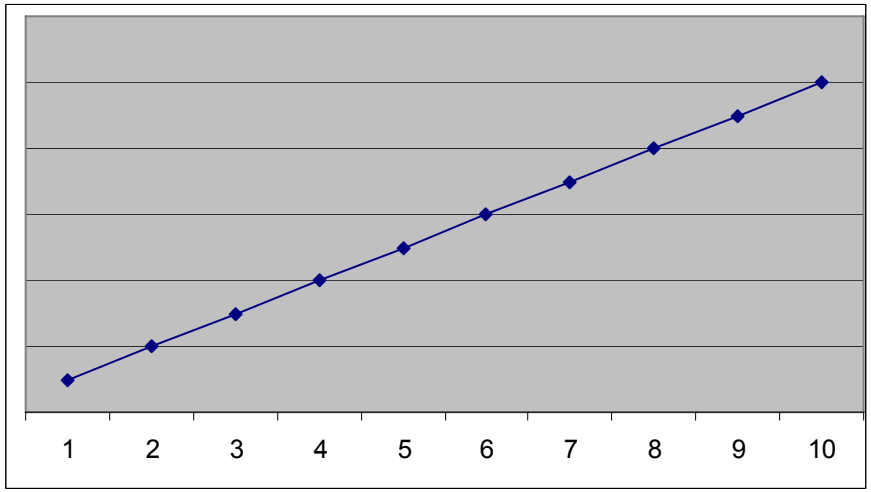
$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt}$$

Konstante Ausfallwahrscheinlichkeitsdichte

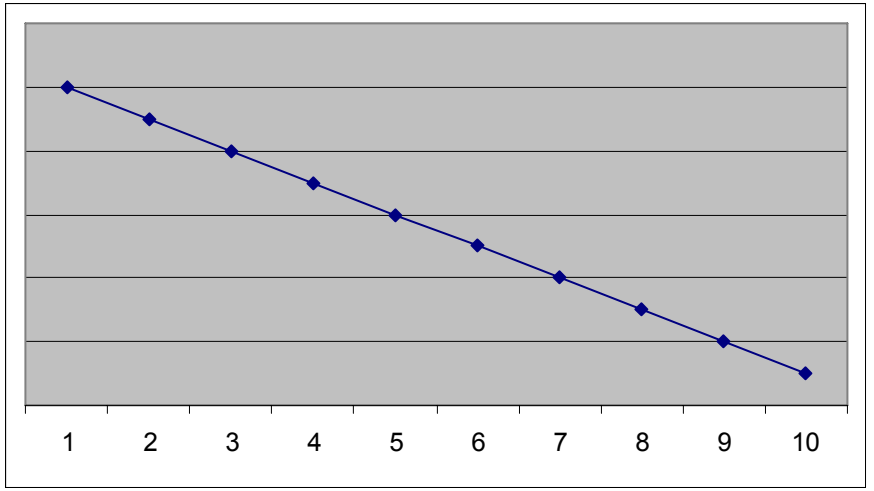
f(t)



F(t)



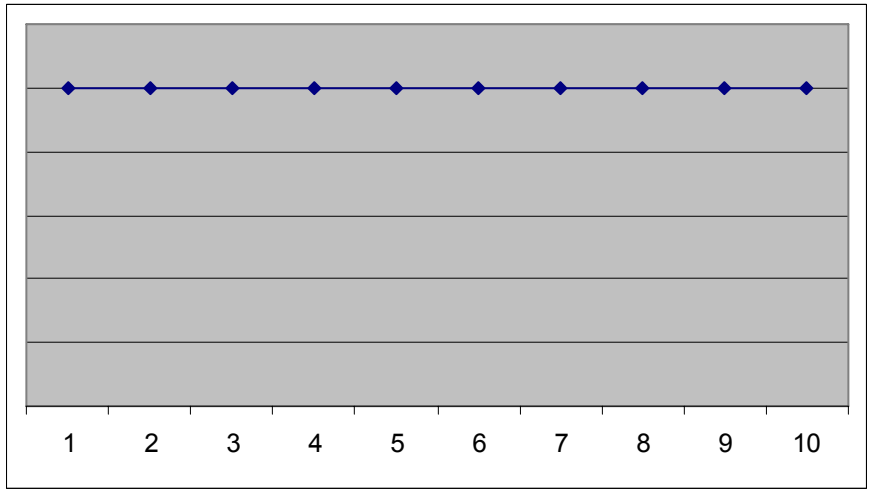
R(t)



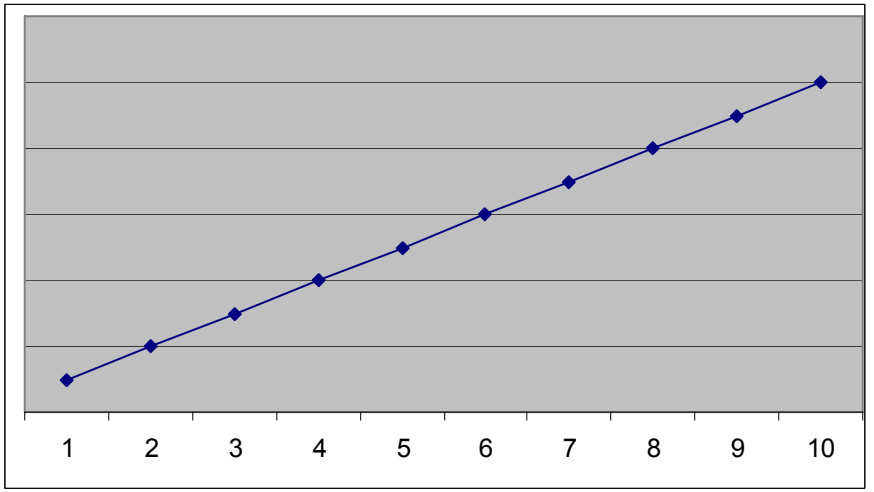
$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt}$$

Konstante Ausfallwahrscheinlichkeitsdichte

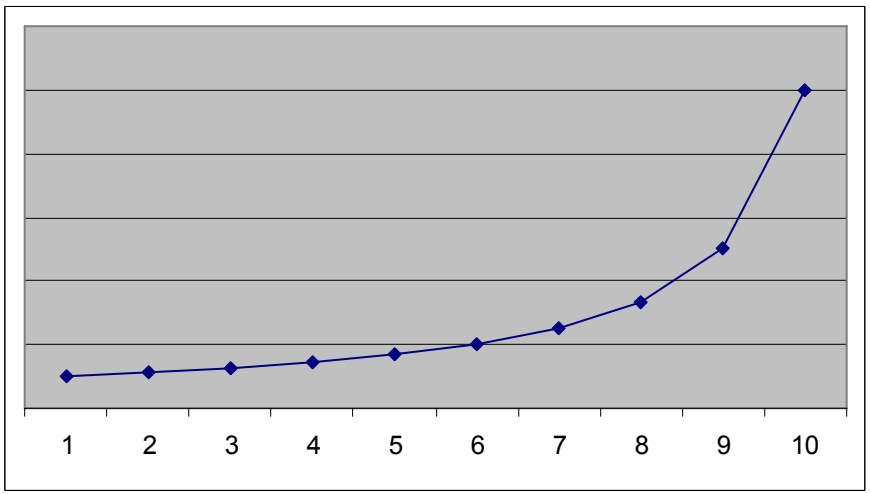
f(t)



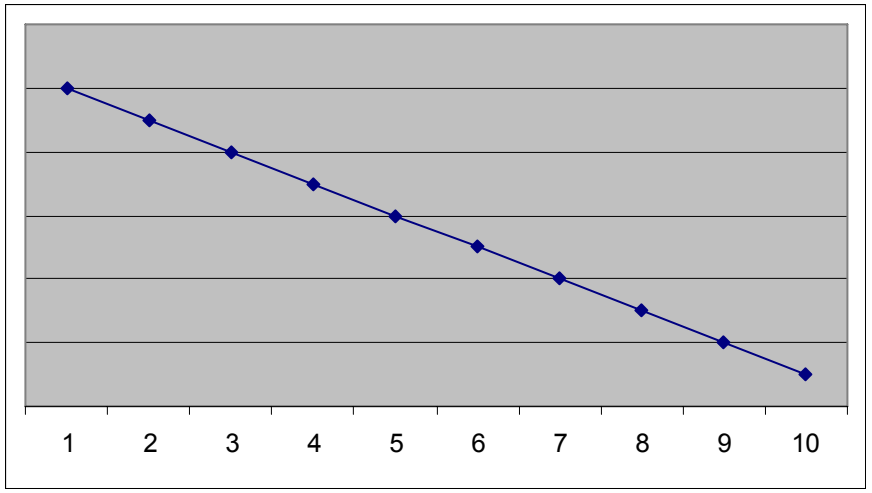
F(t)



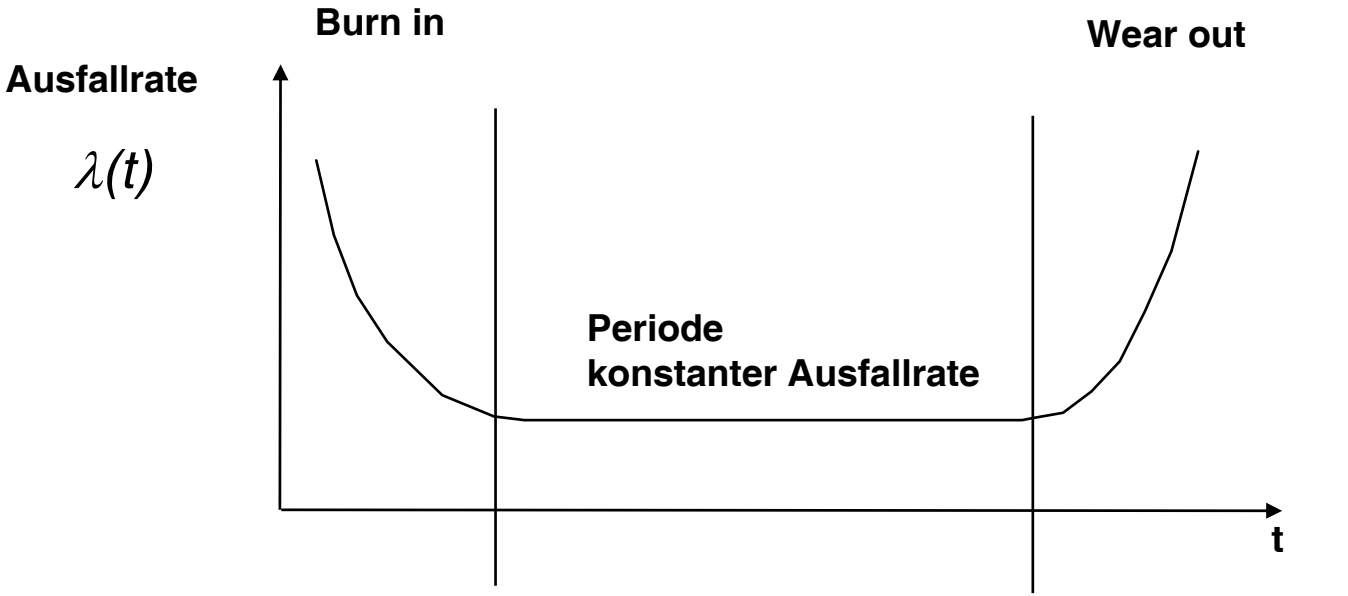
Ausfallrate: λ



R(t)



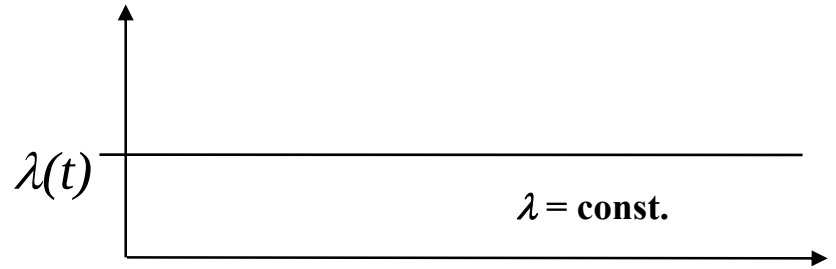
Die "Badewannenkurve"

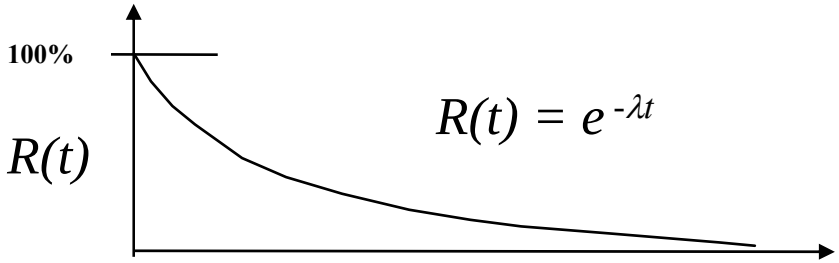


Typische Ausfallrate:
VLSI-Chip: 10^{-8} Ausfälle/h = 1 Ausfall in 115000 Jahren

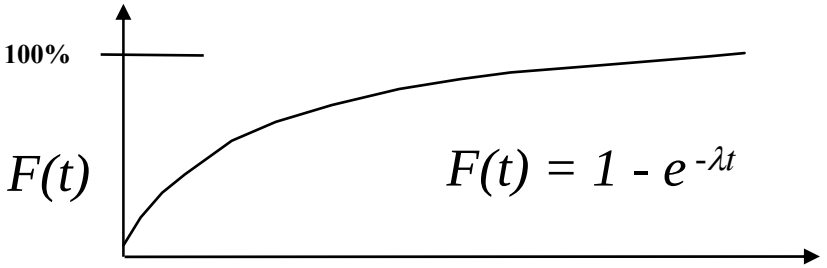
Maße der Fehlertoleranz

Ausfallrate λ (t)
Anzahl der Ausfälle pro Zeiteinheit

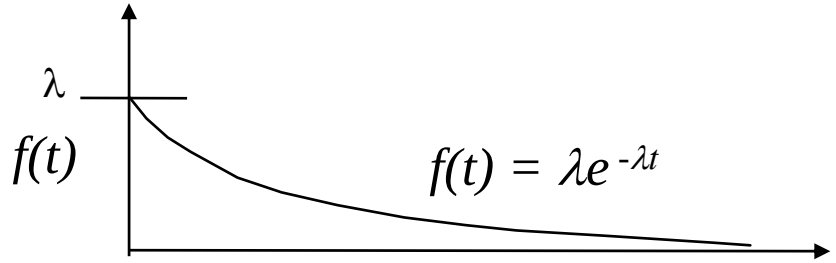




Bemerkung: **Die Ausfallrate ist relativ zum Bestand definiert. Fallen pro Zeiteinheit immer gleich viele Komponenten aus, steigt die Ausfallrate relativ zum Bestand an, der ja immer kleiner wird.**

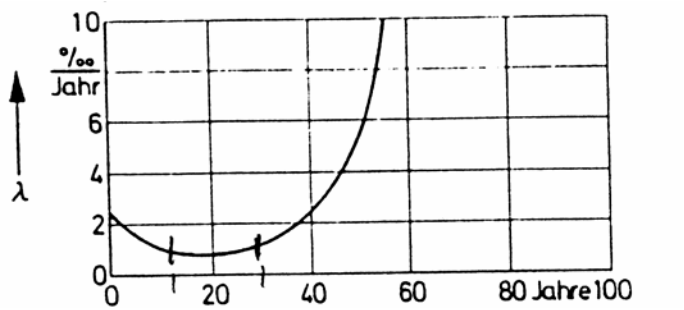


Bleibt die Ausfallrate relativ zum Bestand konstant, ergibt sich daraus eine Exponentialverteilung für die Überlebenswahrscheinlichkeit R(t).

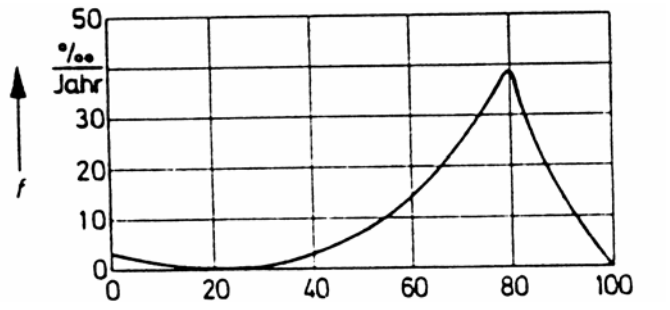


Lebensdauerverteilung beim Menschen

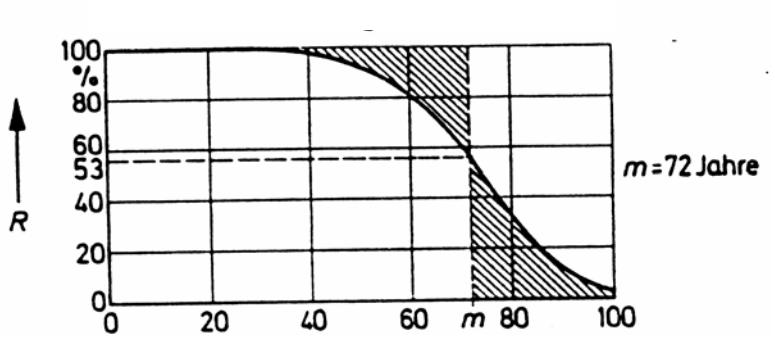
Ausfallrate λ (t)



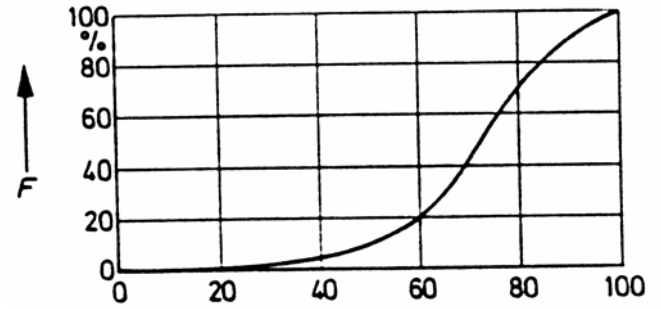
Ausfallwahrscheinlichkeitsdichte f(t)



Überlebenswahrscheinlichkeit R(t) (Reliability)



Ausfallwahrscheinlichkeit F(t)



Kenngröße	Symbol	Einheit
Lebensdauer	T	h
Ausfallwahrscheinlichkeit	F	%
Überlebenswahrscheinlichkeit	R	%
Ausfallwahrscheinlichkeitsdichte	f	%/h
Ausfallrate	λ	1/h

Anforderungen an die Autoelektronik

Anfangszuverlässigkeit:	**(0 *km* / 0 *h*) Fehler: $< 500 \cdot 10^{-9}$**
	im 1. Jahr Fehler: $< 1000 \cdot 10^{-9}$
System-Lebenszeit:	**3500 *h* (ca. 5Jahre bei 2*h*/Tag)**
Garantie:	**≥ 1 Jahr, Ersatzteile ≥ 10 Jahre**
Umgebungsbedingungen:	**-40 bis +85 ^oC**
Vibration:	**10 *Hz* bis 1 *kHz*, zufällig 5*g*, Sinus 2-5*g***
Shock:	**30 *g***
Versorgungsspannung:	**8-16*V***
	Motorstart mit 6*V* (-40 bis +85 ^oC), 18*V* für 2*h*, 24*V* für 1 *min*
	umgekehrte Polarität 13,5*V* für 1 *min*

Streßtest für Autoelektronik

- **Funktionstest: 8, 13.5, 16 *V* bei -40, 25, 85 ^oC**
- **Hitzetest: 85 ± 2 ^oC für 16*h* bei 16 *V* und 6000 *upm***
- **Kältetest: -40 ± 3 ^oC für 2*h***
- **Lagerung: 85 ± 2 ^oC für 504*h***
- **Temperaturschock: -40 bis 85 ^oC Übergang in 30 *sek.* 25 mal**
- **Temperaturänderung: -40 bis 85 ^oC , 3 ± 0.6 ^oC /*min* für 2 Zyklen**

Maße der Fehlertoleranz

Unter der Annahme von $\lambda(t) = \text{const.}$ gilt:

$$\frac{1}{\lambda} = \text{MTBF} = \text{MTTFF} = \text{MTTF}$$

MTBF : Mean Time Between Failures

MTTFF: Mean Time To First Failure

MTTF : Mean Time To Failure

Maße der Fehlertoleranz

Verfügbarkeit (Availability)

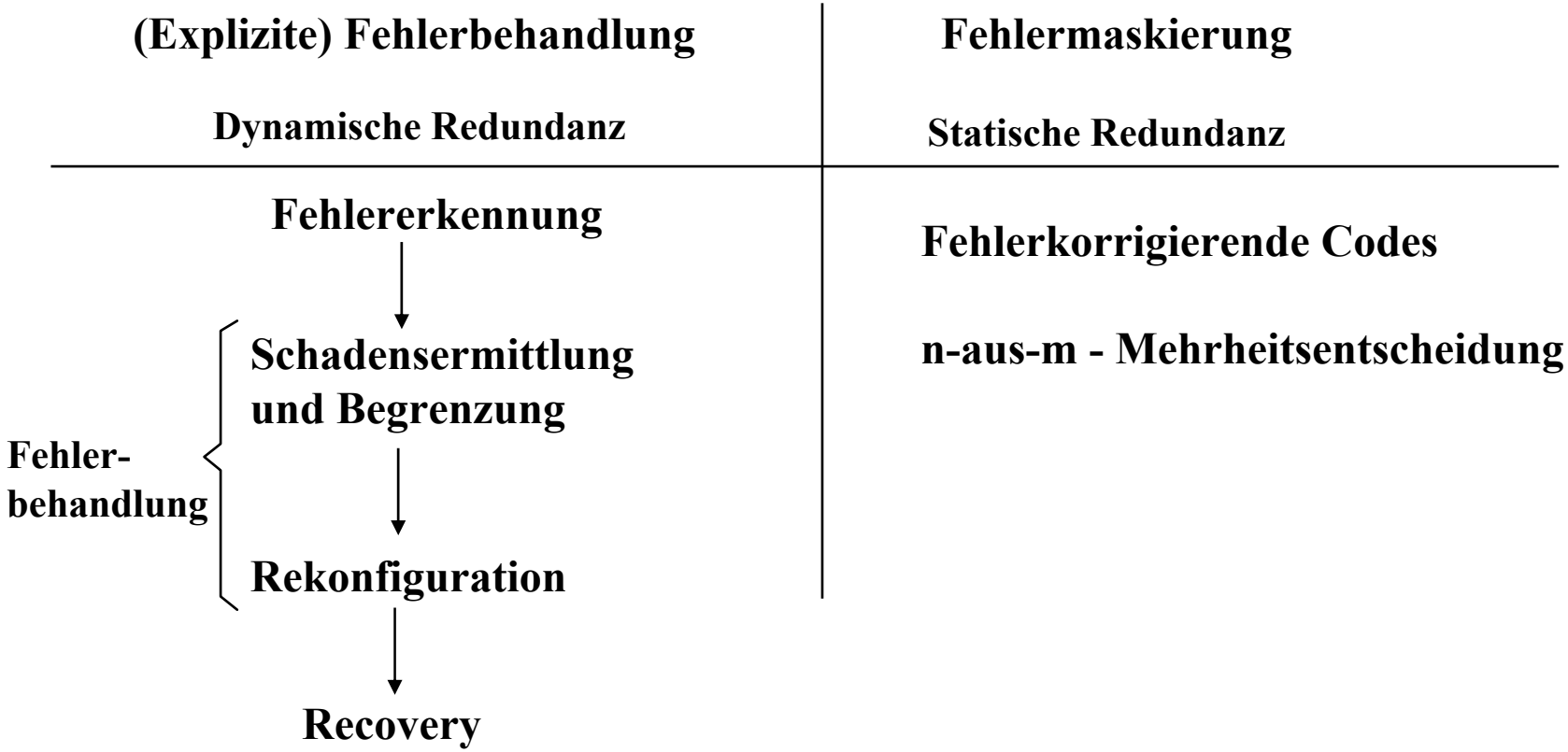
Zeit in der ein System intakt ist bezogen auf die gesamte Missionszeit

$$A = \frac{\text{U (Up time)}}{\text{M (Mission time)}}$$

$$\text{M} = \text{U} + \text{TR (Repair time)}$$

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

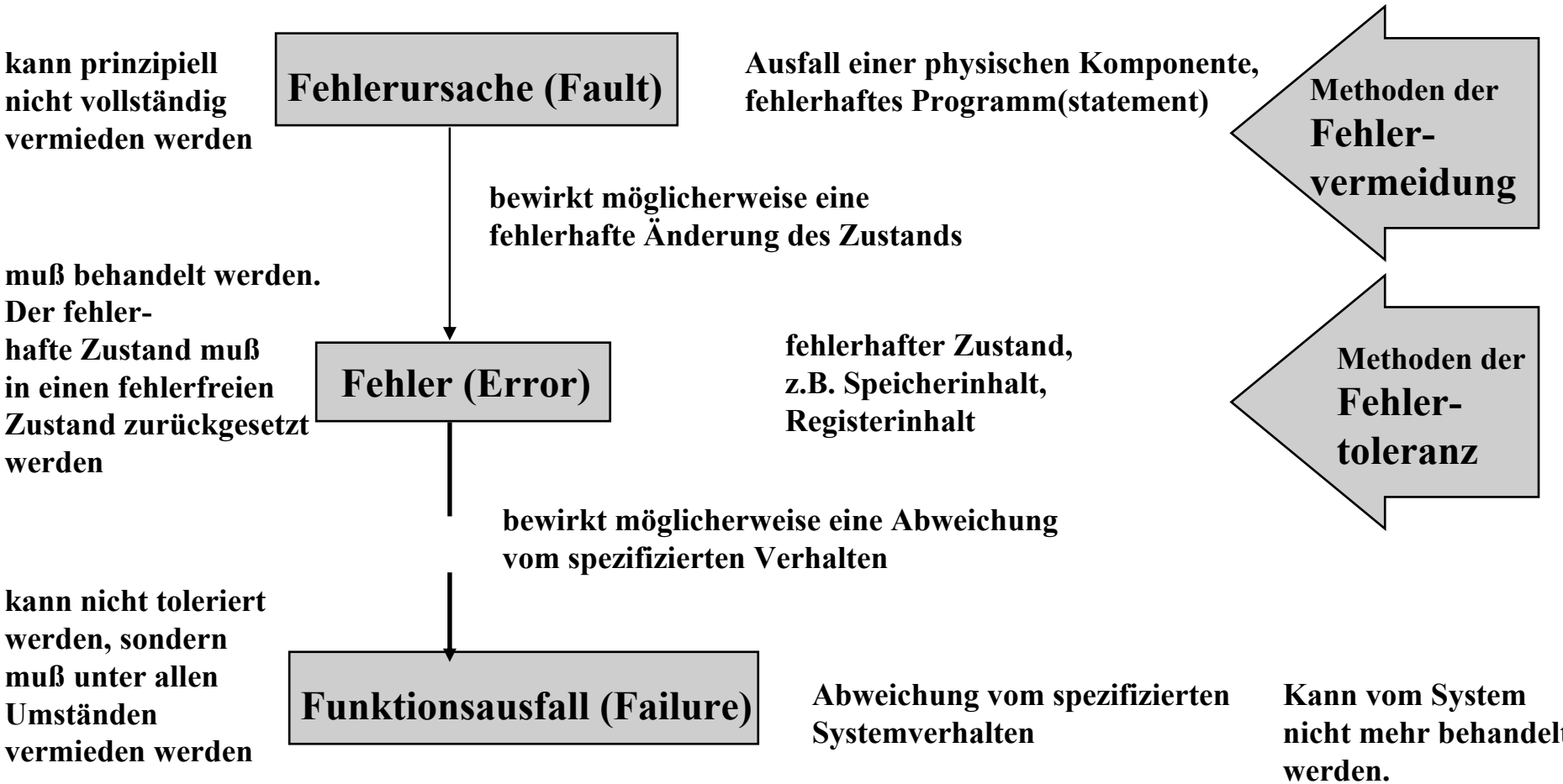
Mechanismen der Fehlertoleranz



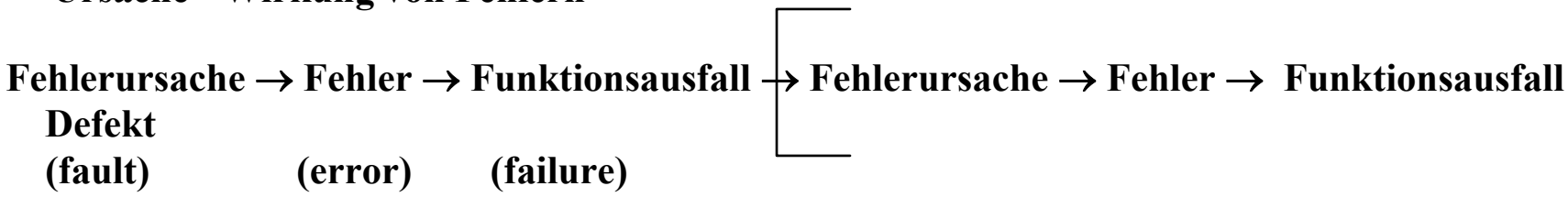
Alle Mechanismen der Fehlertoleranz beruhen auf Redundanz

- **Informationsredundanz**
- **Komponentenredundanz**
- **Zeitredundanz**

Fehlerklassifizierung



Ursache - Wirkung von Fehlern



Defekt: Ereignis
Fehler: Auswirkungen der Fehlerursache auf den Systemzustand
Funktionsausfall: Abweichung des Systems von seinem spezifizierten Verhalten

Defekt → Fehler

- ein Defekt, der durch den Berechnungsvorgang (noch) nicht aktiviert wurde, heißt *ruhend (dormant)*.
- Ein Defekt ist *aktiv*, wenn er einen Fehler verursacht.

Fehler → Funktionsausfall

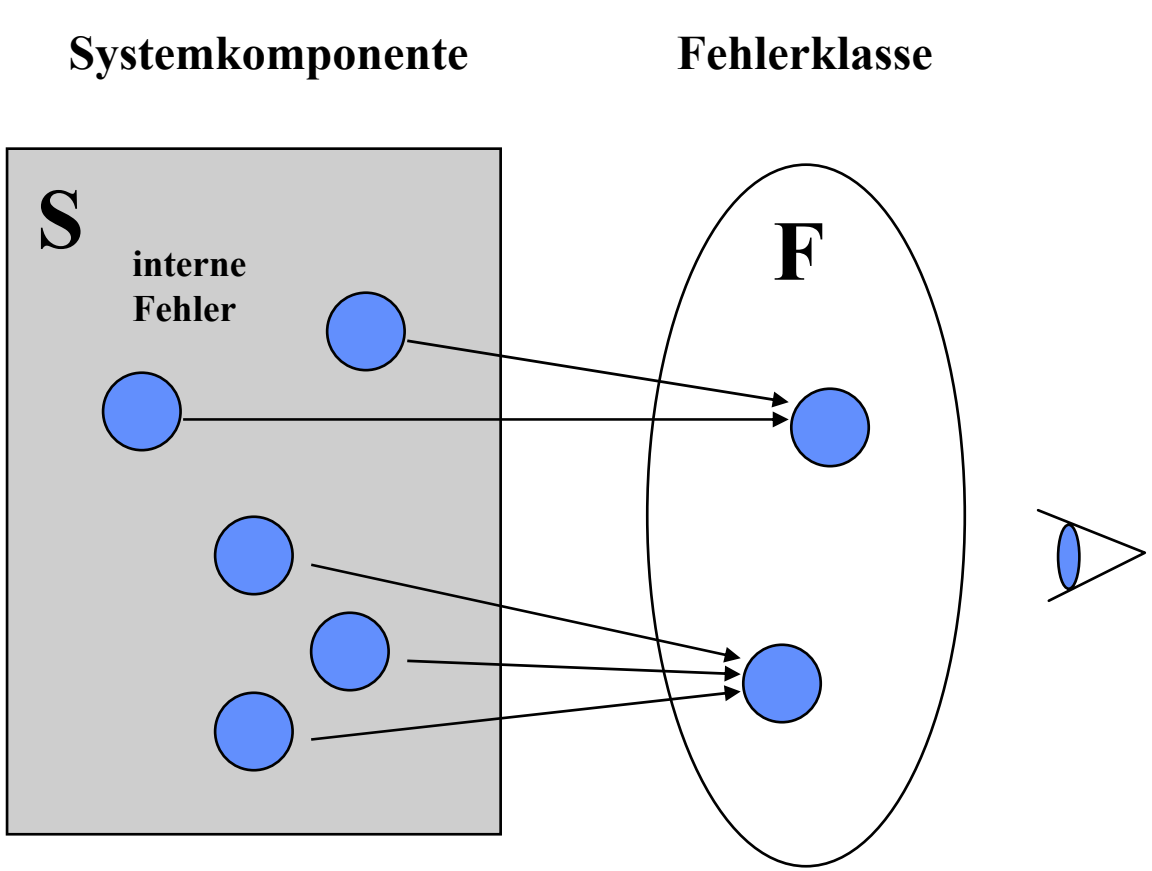
- ein Fehler heißt *latent*, wenn er noch nicht zu einem Funktionsausfall geführt hat (oder durch Erkennungsmaßnahmen entdeckt wurde).
- ein Fehler heißt *effektiv* , wenn er zu einem Funktionsausfall führt.

Funktionsausfall → Defekt

- ein Funktionsausfall tritt ein, wenn ein Fehler effektiv wird und den erbrachten Service verfälscht.
- ein Funktionsausfall kann die Fehlerursache für eine höhere Systemebene darstellen.

Fehlersemantik

Die Fehlersemantik beschreibt die Annahmen über die Auswirkungen interner Fehler auf das beobachtbare Verhalten einer Systemkomponente (Abstraktion interner Fehler).



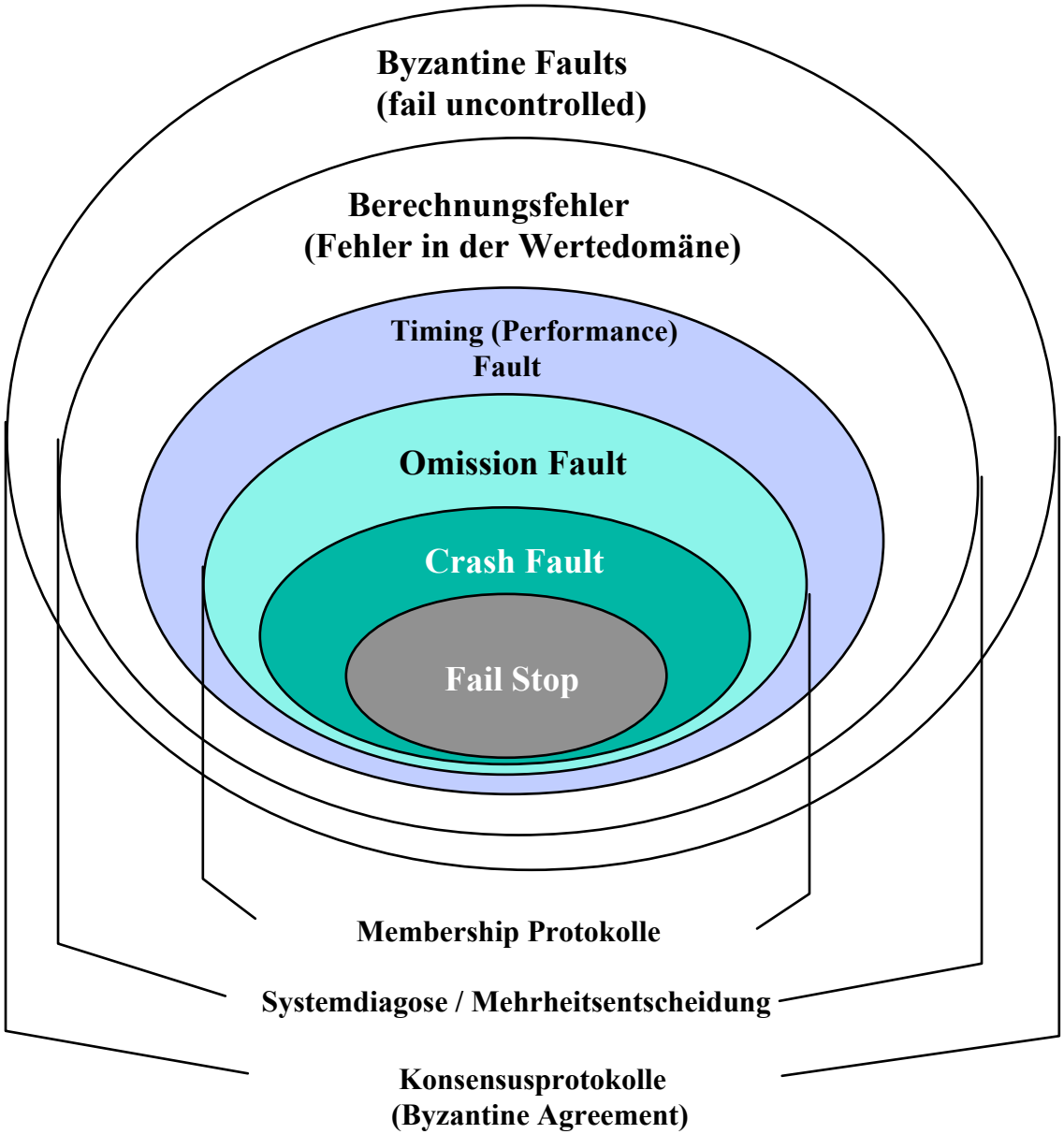
Problem:
Die Mechanismen zur Fehlerbehandlung beziehen sich auf die antizipierte Fehlerklasse.

Es muss gewährleistet werden, dass die Fehlersemantik F im System auch durchgesetzt wird.

Beispiele:
Omission-Fehlersemantik
Crash-Fehlersemantik

S hat die Fehlersemantik F

Hierarchie der Fehlermodi



Byzantinische Fehler:
Beliebige, unkontrollierbare Fehler

Zeitfehler.
Korrekte Resultate in der Wertedomäne, aber zu früh oder zu spät.

Omission (Unterlassungs-) Fehler:
Spezielle Klasse der Zeitfehler. Die (korrekten) Resultate kommen entweder zur richtigen Zeit oder gar nicht.

Crash Fehler:
Komponente liefert keine Resultate mehr.

Fail Stop:
Andere Komponenten können den Crash Fehler korrekt diagnostizieren.