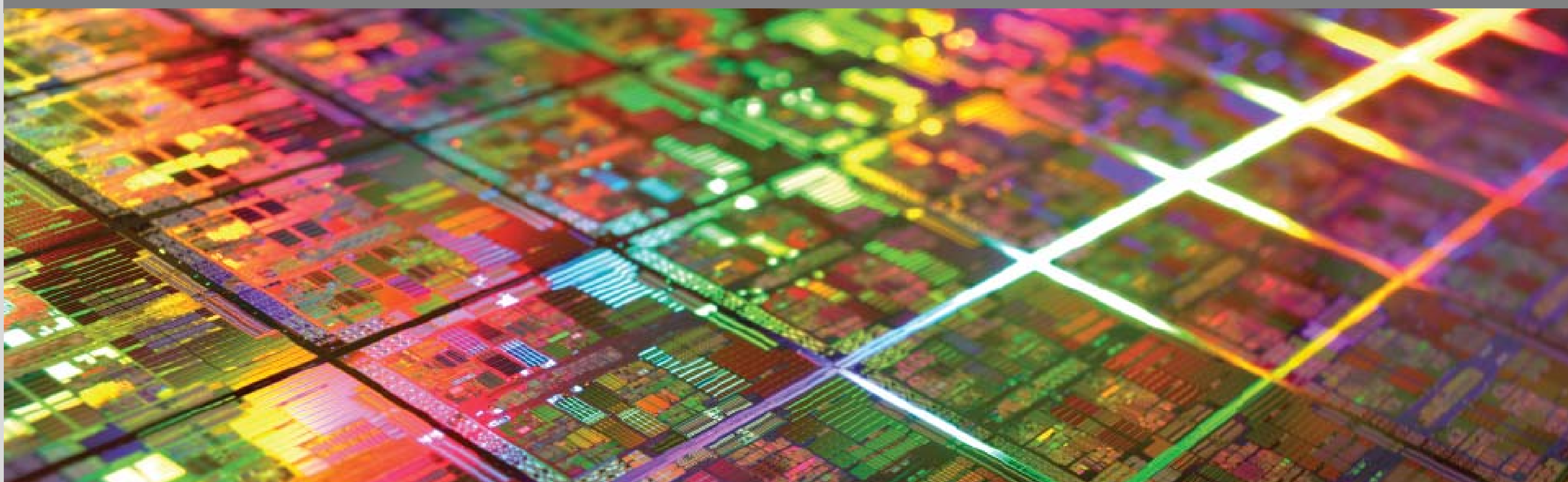
Karlsruher Institut für Technologie

Rechnerstrukturen

Vorlesung im Sommersemester 2010

Prof. Dr. Wolfgang Karl

Fakultät für Informatik – Lehrstuhl für Rechnerarchitektur und Parallelverarbeitung



Vorlesung Rechnerstrukturen

- **Gastvorlesung**
  - **Termin: 13.7.2010, 9:45-11:15 Uhr**
  - **Carl Mayer, IBM Labor Böblingen**
  - **Thema: RAS mit System z**

Vorlesung Rechnerstrukturen

- **Kapitel 5: Fehlertoleranz und Zuverlässigkeit**
- 5.1 Grundlagen

Zuverlässigkeit und Fehlertoleranz

- **Begriffsbildung**
- Zuverlässigkeit (dependability)
  - bezeichnet die Fähigkeit eines Systems, während einer vorgegebenen Zeitdauer bei zulässigen Betriebsbedingungen die spezifizierte Funktion zu erbringen.
  - Ziel
- Fehlertoleranz (fault tolerance)
  - bezeichnet die Fähigkeit eines Systems, auch mit einer begrenzten Anzahl fehlerhafter Subsysteme die spezifizierte Funktion (bzw. den geforderten Dienst) zu erbringen.
  - Technik

Zuverlässigkeit und Fehlertoleranz

- **Begriffsbildung**
- Sicherheit (safety)
  - bezeichnet das Nichtvorhandensein einer Gefahr für Menschen oder Sachwerte. Unter einer Gefahr ist ein Zustand zu verstehen, in dem (unter anzunehmenden Betriebsbedingungen) ein Schaden zwangsläufig oder zufällig entstehen kann, ohne dass ausreichende Gegenmaßnahmen gewährleistet sind.
- Vertraulichkeit (security)
  - betrifft Datenschutz, Zugangssicherheit.

Zuverlässigkeit und Fehlertoleranz

- **Begriffsbildung**
- Zuverlässigkeitskenngrößen:
  - Verfügbarkeit
  - Überlebenswahrscheinlichkeit
  - Ausfallsicherheit
- Wartungsfreundlichkeit
  - System: Instandhaltung notwendig?
  - Komponenten: Ersatz?
  - Datenbestände: langfristig lesbar?
- Nutzungsdauer eines Rechners
  - Mindestens 5 Jahre oder 40000 h, Dauerbetrieb notwendig?
  - Sehr kleine Ausfallraten der Komponenten (< 10-9h-1)
  - Probleme: Nachweisbarkeit, Testmöglichkeiten

Zuverlässigkeit und Fehlertoleranz

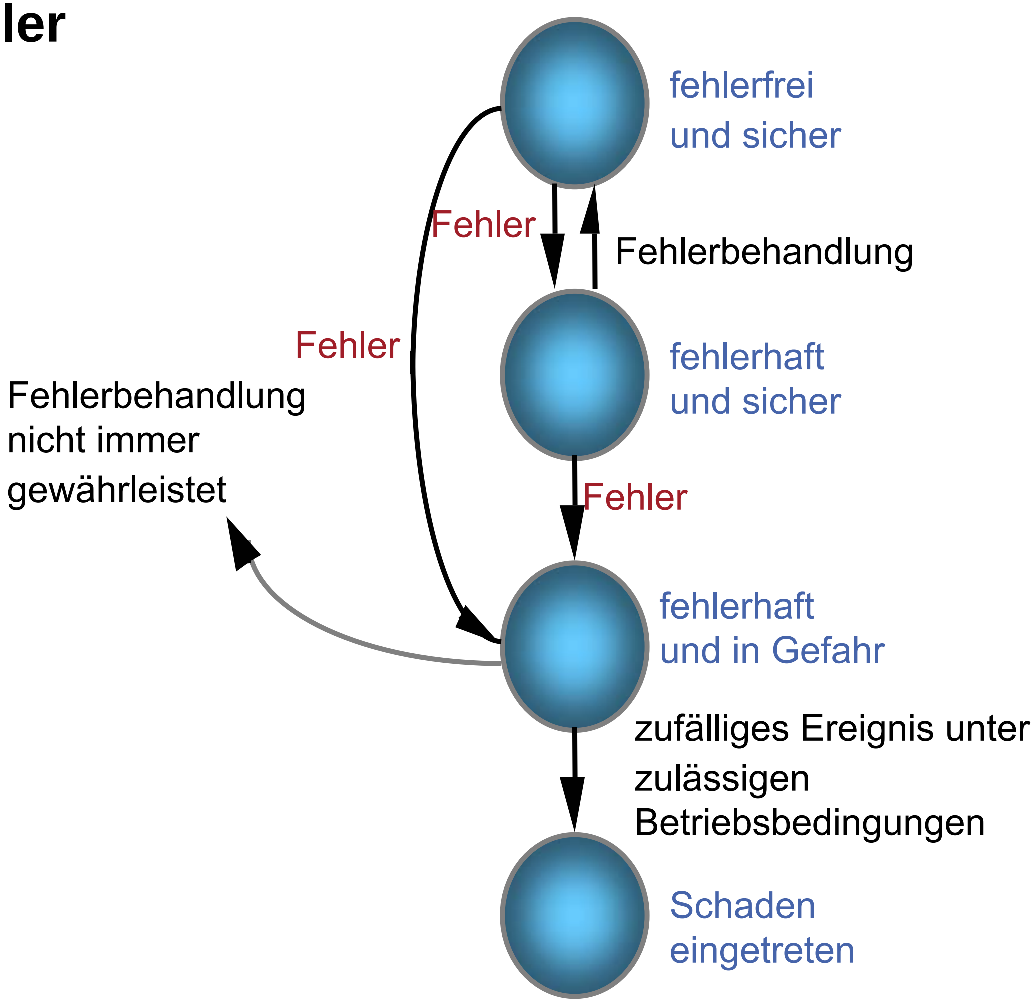
- **Begriffsbildung**
- Ausfall
  - Hardwarekomponenten (Chips, Hintergrundspeicher)
  - Software, durch Programmfehler
  - Menschliche Eingriffe
- Sicherheitsrelevante Anwendungen erfordern eine hohe Verfügbarkeit

Zuverlässigkeit und Fehlertoleranz

- **Fragen:**
  - Wie zuverlässig sind heutige Rechensysteme?
  - Nutzen redundante, also fehlertolerante Strukturen zur Verbesserung der Zuverlässigkeit?
  - Welche Verbesserung der Zuverlässigkeit lässt sich durch derartige Fehlertoleranzmaßnahmen überhaupt erreichen?

Zuverlässigkeit und Fehlertoleranz

- **Fehler**



Zuverlässigkeit und Fehlertoleranz

- **Fehler:**
  - Fehlzustände oder Funktionsausfälle
    - Der Ausfall einer Komponente erzeugt einen Fehlerzustand
    - Ausfall eines Systems: Versagen
  - Wirkungskette:
    - Fehler → Fehlzustand → Ausfall
  - Fehlerausbreitung verhindern!
- Ziel der Fehlertoleranz:
  - Tolerierung der Fehlzustände von Teilsystemen (Komponenten)
  - Erhöhung der Zuverlässigkeit
  - Behebung der Fehlzustände vor dem Ausfall des Systems

Zuverlässigkeit und Fehlertoleranz

- **Fehler:**
- Ursachen
  - Fehler beim Entwurf
    - Spezifikationsfehler
    - Implementierungsfehler
    - Dokumentationsfehler
    - Herstellungsfehler
  - Betriebsfehler
    - Störungsbedingte Fehler
    - Verschleißfehler
    - Zufällige physikalische Fehler
  - Bedienungsfehler
  - Wartungsfehler

Zuverlässigkeit und Fehlertoleranz

- **Fehler:**
  - Dauer und Ort
    - Fehlerentstehungsort
    - Hardware oder Software
  - Fehlerdauer
    - Permanenter Fehler
    - Temporärer Fehler

Zuverlässigkeit und Fehlertoleranz

- **Ausfallverhalten**
  - Teilausfall
    - Von einer fehlerhaften Komponente fallen eine oder mehrere, aber nicht alle Funktionen aus
  - Unterlassungsausfall
    - Eine fehlerhafte Komponente gibt eine Zeit keine Ergebnisse aus. Wenn jedoch ein Ergebnis ausgegeben wird, dann ist dieses korrekt
  - Anhalteausfall
    - Eine fehlerhafte Komponente gibt nie mehr ein Ergebnis aus
  - Haftausfall
    - Eine fehlerhafte Komponente gibt ständig den gleichen Ergebniswert aus
  - Binärstellenausfall
    - Ein Fehler verfälscht eine oder mehrere Binärstellen des Ergebnisses

Zuverlässigkeit und Fehlertoleranz

- **Systemausfallverhalten**
  - Fail-stop-System
    - Ein System, dessen Ausfälle nur Anhalteausfälle sind
  - Fail-silent-System
    - Ein System, dessen Ausfälle nur Unterlassungsausfälle sind
  - Fail-safe-System
    - Ein System, dessen Ausfälle nur unkritische Ausfälle sind

Zuverlässigkeit und Fehlertoleranz

- **Anforderungen**
  - Hohe Überlebenswahrscheinlichkeit
    - kurzzeitige Mission (z.B. 10-stündiger Flug)
  - Hohe mittlere Lebensdauer
    - z.B. bei begrenzten Reparaturmöglichkeiten in unzugänglichen Rechensystemen
  - Hohe Verfügbarkeit
    - z.B. im interaktiven Rechenzentrums- oder Nutzerbetrieb
  - Hohe Sicherheitswahrscheinlichkeit
    - Schutz von Menschen, Maschinen, Daten
  - Hohe Sicherheitsdauer

Zuverlässigkeit und Fehlertoleranz

- **Vorgehensweise**
  - Höchste Präferenz: Fehlervermeidung
    - Perfektionierung, Verwendung von zuverlässigen Komponenten, sorgfältiger Entwurf
  - Fehlertoleranz
    - Erfordert Redundanz und damit Zusatzaufwand

Zuverlässigkeit und Fehlertoleranz

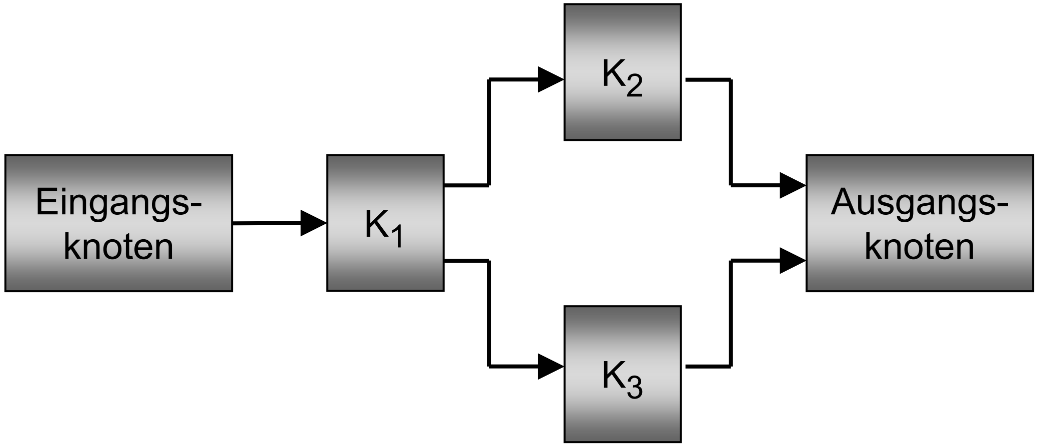
- **Weitere Gesichtspunkte**
  - Fehlervorgabe
    - Nicht alle Fehler sind tolerierbar
  - Menge der zu tolerierenden Fehler
    - Gibt an, welche im Fehlermodell vorgesehenen Fehler tolerierbar sind
  - Fehlerbereichsannahme
    - Die Menge der zu tolerierenden Fehler wird bezüglich einer Fehlerannahme formuliert
  - Festlegung:
    - wie viele Einzelfehlerbereiche können gleichzeitig fehlerhaft werden
    - Welche Fehlfunktionen sind zu behandeln

Zuverlässigkeit und Fehlertoleranz

- **Zusätzliche Anforderungen**
  - Nachweis der Fehlertoleranz
    - Verifikation, Validierung, Durchführung einer Anfälligkeitsanalyse
  - Geringer Betriebsmittelbedarf (geringe Kosten)
  - Schnelle Ausführung von Fehlertoleranzverfahren (Leistung)
  - Unabhängigkeit von der Anwendungssoftware (Transparenz)
  - Unabhängigkeit vom Rechensystem

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Ausgangspunkt
  - Zuverlässigkeitsblockdiagramm
    - Die Systemfunktion lässt sich grafisch durch ein Zuverlässigkeitsblockdiagramm darstellen:
    - Gerichteter Graph mit einem Eingangs- und einem Ausgangsknoten



$$S = K_1 \wedge \left(K_2 \vee K_3 \right)$$

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitskenngrößen
  - Zuverlässigkeit, Sicherheit einer Rechensystems
    - Quantifizierbar mittels stochastischer Modelle
    - Man betrachtet die kontinuierliche Variable Zeit zwischen dem Zeitpunkt, ab dem die Zuverlässigkeitsbetrachtung beginnen soll (Zeitpunkt Null), bis zum Auftreten eines betrachteten Effekts
    - Nichtnegative Zufallsvariablen:
      - Lebensdauer L – besitzt die Dichte $f_L(t)$
      - Fehlerbehandlungsdauer B – besitzt die Dichte $f_B(t)$
      - Sicherheitsdauer D – *besitzt die Dichte* $f_D(t)$

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitskenngrößen
  - Zuverlässigkeit, Sicherheit einer Rechensystems
    - Verteilungsfunktion

$$F_x(t) := \int_0^t f_x(s)ds$$

      - mit x = L, D, B

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitskenngrößen
  - Fehlerwahrscheinlichkeit $F_L(t)$
    - Bezeichnet die Wahrscheinlichkeit, dass ein zu Beginn fehlerfreies System im Zeitintervall [0,t] fehlerhaft wird
  - Überlebenswahrscheinlichkeit

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

    - System ist von t=0 bis zum Zeitpunkt t ununterbrochen fehlerfrei.
    - $F_L(t)=0$ und $\lim_{t \to \infty} F_L(t) = 1$
      - damit folgt: R(0)=1,
      - und R ist in t monoton fallend $\lim_{t \to \infty} R(t) = 0$

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitskenngrößen
  - Mittlere Lebensdauer

$$E(L) = \int_0^\infty R(t)dt$$

    - bezeichnet für ein zu Beginn fehlerfreies System den Erwartungswert der Zeitdauer bis zum Eintreffen des ersten Fehlers

  - Ausfallrate

$$z(t) := \frac{f_L(t)}{R(t)}$$

    - bezeichnet den Anteil der in einer Zeiteinheit ausfallenden Komponenten bezogen auf den Anteil der noch fehlerfreien Komponenten

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitskenngrößen
  - Fehlerwahrscheinlichkeit
    - Ist die Ausfallrate bekannt, so ergibt sich die Fehlerwahrscheinlichkeit aus der Anfangswertaufgabe

$$\frac{d}{dt} F_L(t) = f_L(t) = z(t) \cdot (1 - F_L(t))$$

    - mit der Anfangsbedingung $F_L(0)=0$.
    - Die Anfangswertaufgabe hat die Lösung

$$F_L(t) = 1 - e^{-\int_0^t z(s)ds}$$

    - Bei einer konstanten Ausfallrate $z(t)=\lambda$ ist die Fehlerwahrscheinlichkeit

$$F_L(t) = 1 - e^{-\lambda t}$$

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitskenngrößen
  - Verfügbarkeit

$$v := \frac{E(L)}{E(L) + E(B)}$$

    - Wahrscheinlichkeit, ein System zu einem beliebigen Zeitpunkt fehlerfrei anzutreffen
    - D.h., der zeitliche Anteil der Benutzbarkeit des Systems an der Summe der Erwartungswerte von Lebensdauer L und Behandlungsdauer B, wenn während B das System repariert und wieder funktionsfähig wird.

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitskenngrößen
  - Sicherheit einer Rechensystems
      - Geht man Ausfällen aus, die die Sicherheit beeinträchtigen, dann ergeben sich analog zu den bisher betrachteten Größen solche mit Sicherheitsrelevanz
    - Gefährdungswahrscheinlichkeit $F_D(t)$
      - Wahrscheinlichkeit, dass ein zu Beginn sicheres System im Zeitintervall [0,t] in einen gefährlichen Zustand gerät
    - Sicherheitswahrscheinlichkeit $S(t):=1- F_D(t)$
      - Wahrscheinlichkeit, dass ein zu Beginn sicheres System bis zum Zeitpunkt t ununterbrochen in einem sicheren Zustand bleibt
    - Mittlere Sicherheitsdauer

$$E(D) = \int_0^\infty t \cdot f_D(t)dt = \int_0^\infty S(t)dt$$

      - Erwartungswert der Zeitdauer, bis ein gefährlicher Zustand auftritt

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitskenngrößen
  - Funktionswahrscheinlichkeit der Komponenten und Systemfunktionen

$$\varphi(S) = \sum_{(K_1,\ldots,K_n)\in f^{-1}(wahr)} \varphi(\wedge_{i=1}^{n} K_i)$$

    - (als Oberbegriff für Überlebenswahrscheinlichkeit und Verfügbarkeit)

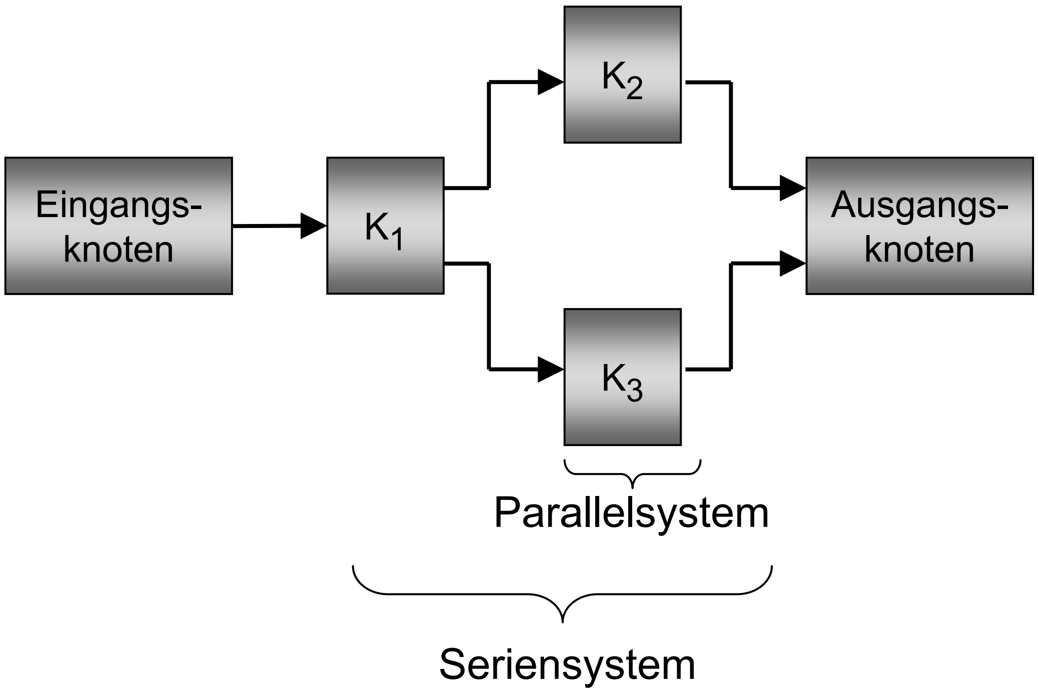
  - Nichtfunktionswahrscheinlichkeit

$$\varphi(\neg K) = 1 - \varphi(K)$$

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitsdiagramm

$$S = K_1 \wedge \left(K_2 \vee K_3\right)$$



Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitskenngrößen
  - Funktionswahrscheinlichkeit eines Seriensystems

$$\varphi(\wedge_{K\in\Lambda}) = \prod_{K\in\Lambda} \varphi(K)$$

  - Funktionswahrscheinlichkeit eines Parallelsystems

$$\varphi(\vee_{K\in\Lambda}) = \sum_{\emptyset\neq A\in\Lambda} (-1)^{1+\# A} \cdot \varphi(\wedge_{K\in A} K)$$

Zuverlässigkeit und Fehlertoleranz

- **Bewertung**
- Zuverlässigkeitsverbesserung
  - Für ein System $S = K_1 \vee K_2$
    - Gilt demnach:

$$\varphi(S) = \varphi(K_1 \vee K_2) = \varphi(K_1) + \varphi(K_2) - \varphi(K_1 \wedge K_2)$$

    - Mit bedingten Wahrscheinlichkeiten erhält man:

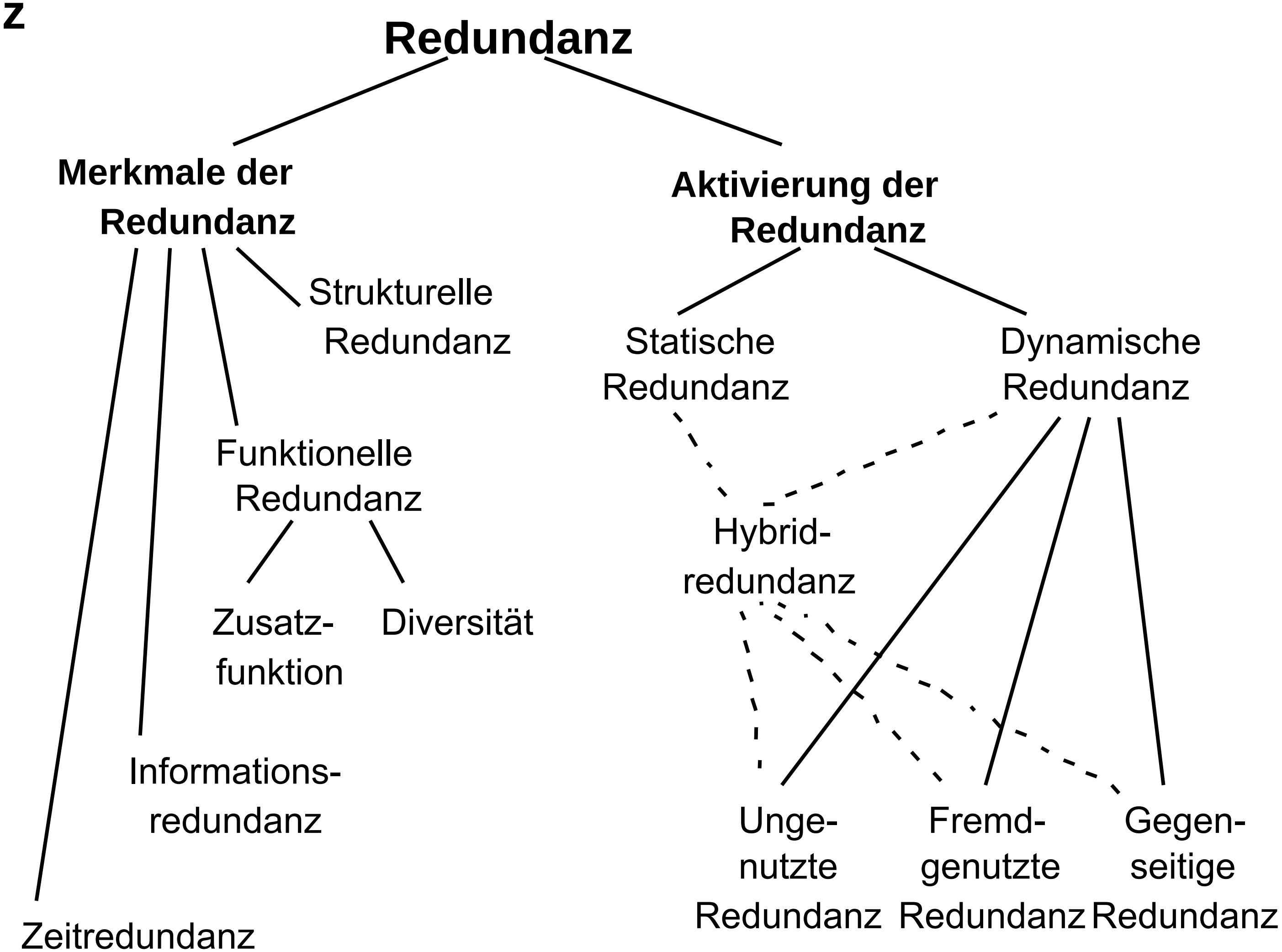
$$\varphi(S) = \varphi(K) \cdot \varphi(S | K) + \varphi(\neg K) \cdot \varphi(S | \neg K)$$

    - Verbesserungsfaktor:

$$\Phi_{S_1 \rightarrow S_2} = \frac{\varphi(\neg S_1)}{\varphi(\neg S_2)} = \frac{1 - \varphi(S_1)}{1 - \varphi(S_2)}$$

Zuverlässigkeit und Fehlertoleranz

- **Redundanz**



Zuverlässigkeit und Fehlertoleranz

- **Redundanz**
- Dynamische Redundanz (dynamic redundancy)
  - bezeichnet das Vorhandensein von redundanten Mitteln, die erst nach Auftreten eines Fehlers aktiviert werden, um eine ausgefallene Nutzfunktion zu erbringen.
  - Typisch für dynamische strukturelle Redundanz ist die Unterscheidung in Primär- und Ersatzkomponenten
(bzw. Sekundär- oder Reservekomponenten).
  - Grundstruktur eines dynamisch strukturell redundanten Systems

Zuverlässigkeit und Fehlertoleranz

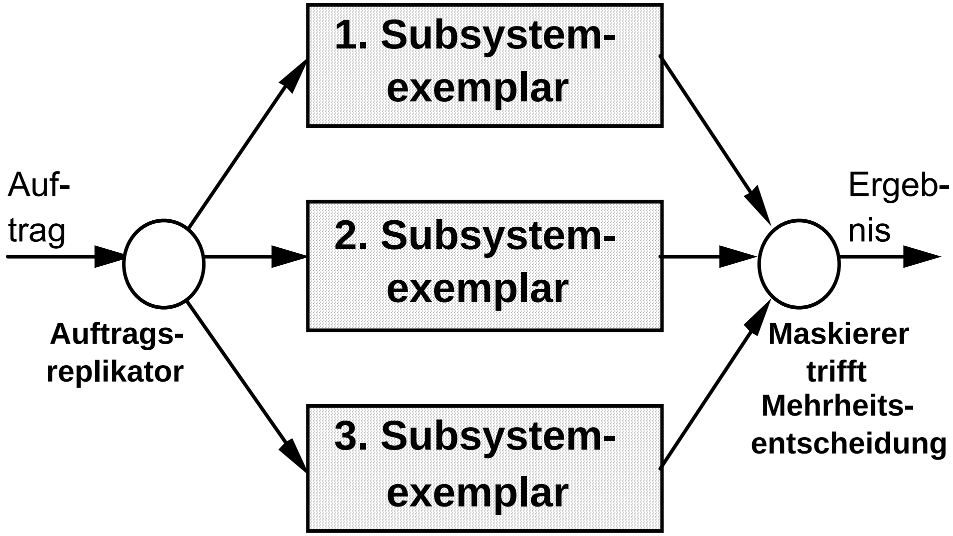
- **Redundanz**
- Dynamische Redundanz (dynamic redundancy)
  - bezeichnet das Vorhandensein von redundanten Mitteln, die erst nach Auftreten eines Fehlers aktiviert werden, um eine ausgefallene Nutzfunktion zu erbringen.
  - Typisch für dynamische strukturelle Redundanz ist die Unterscheidung in Primär- und Ersatzkomponenten
    (bzw. Sekundär- oder Reservekomponenten).
  - Grundstruktur eines dynamisch strukturell redundanten Systems

Zuverlässigkeit und Fehlertoleranz

- **Redundanz**
- Dynamische Redundanz (dynamic redundancy)
  - Bevor Ersatzkomponenten aktiviert werden, lassen diese sich auf eine der folgenden Arten verwenden:
  - Ungenutzte Redundanz
    - Ersatzkomponenten führen keine sonstigen Funktionen aus und bleiben bis zur fehlerbedingten Aktivierung passiv.
  - fremdgenutzte Redundanz:
    - Ersatzkomponenten erbringen nur Funktionen, die nicht zum betreffenden Subsystem gehören und im Fehlerfall bei niedrigerer Priorisierung ggf. verdrängt werden.
  - gegenseitige Redundanz:
    - Ersatzkomponenten erbringen die von einer anderen Komponente zu unterstützenden Funktionen, die Komponenten stehen sich gegenseitig als Reserve zur Verfügung.
      Dies ermöglicht einen abgestuften Leistungsabfall (graceful degradation).

Zuverlässigkeit und Fehlertoleranz

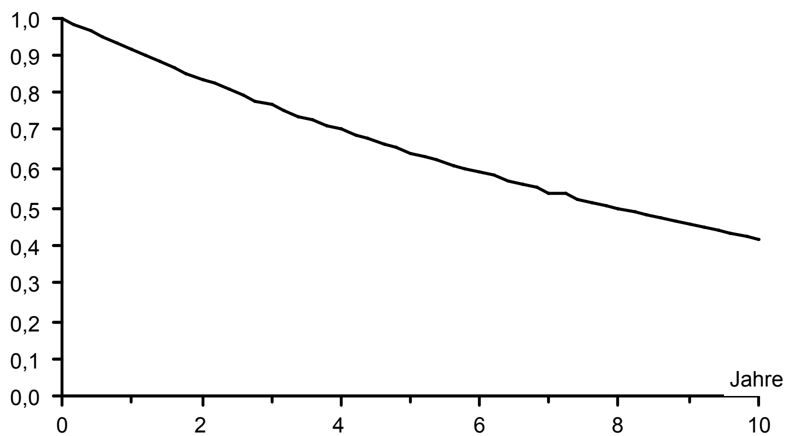
- **Redundanz**
- Statische Redundanz (static redundancy)
  - bezeichnet das Vorhandensein von redundanten Mitteln, die während des gesamten Einsatzzeitraums die gleiche Nutzfunktion erbringen.
  - Beispiel der statischen strukturellen Redundanz: n-von-m-System
    - 2-von-3-System:



Zuverlässigkeit und Fehlertoleranz

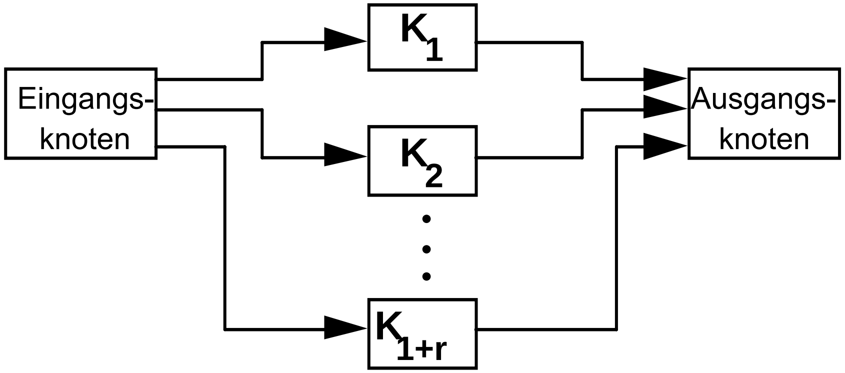
- **Verbesserung der Zuverlässigkeit durch Redundanz**
  - Nichtredundantes Einfachsystem: S1=K1
  - Bei konstanter Ausfallrate beschreibt man die Zeitabhängigkeit der Funktionswahrscheinlichkeit φ (S_1, t) durch eine Exponentialverteilung
    - mit $z(t)=\lambda$, $\varphi(S_1, t) = e^{-\lambda \cdot t}$.

  - Beispiel:
    - Funktionswahrscheinlichkeit φ (S_1, t) mit $\lambda=10^{-5/h}$



Zuverlässigkeit und Fehlertoleranz

- **Verbesserung der Zuverlässigkeit durch Redundanz**
- Parallelsystem (Einfachsystem mit ungenutzter oder fremdgenutzter Redundanz)



Systemfunktion $S_{1+r} = K_1 \vee \ldots \vee K_{1+r}$

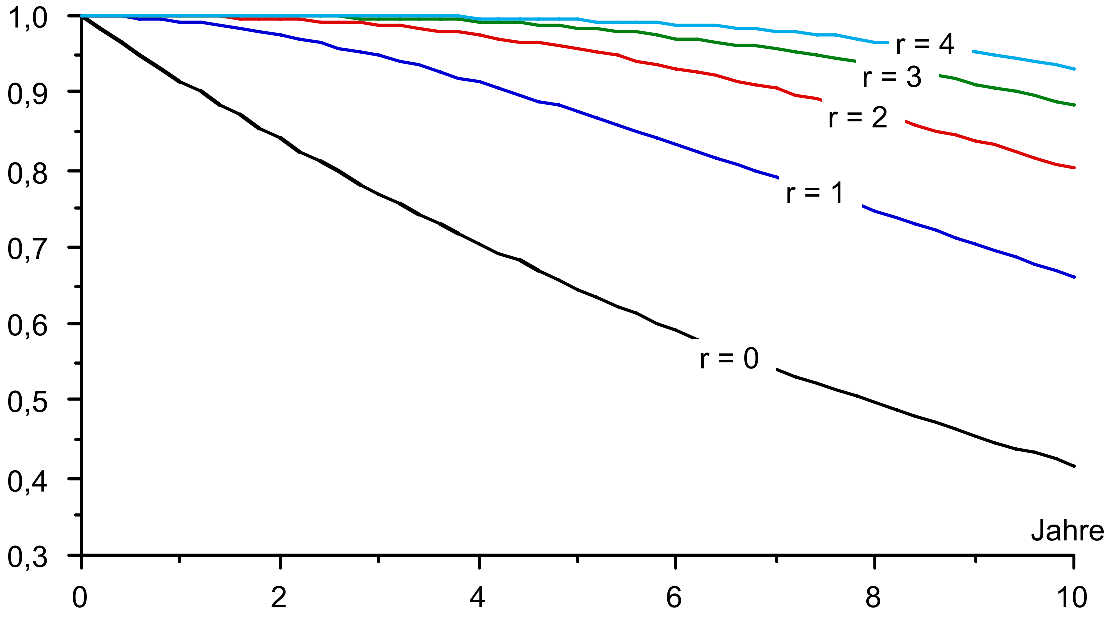
Funktionswahrscheinlichkeit $\varphi(S_{1+r}, t) = 1 - \prod_{i=1}^{1+r} (1 - \varphi(K_i, t))$

gleiche konstante Ausfallrate λ $\varphi(S_{1+r}, t) = 1 - (1 - e^{-\lambda \cdot t})^{1+r}$

Zuverlässigkeitsverbesserung $\Phi_{S_1 \to S_{1+r}} = (1 - e^{-\lambda \cdot t})^{-r}.$

Zuverlässigkeit und Fehlertoleranz

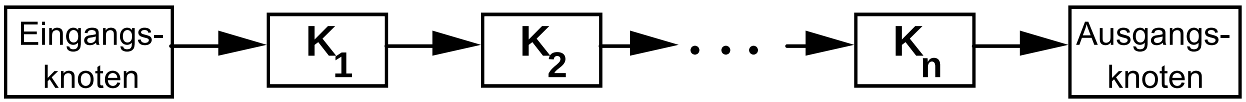
- **Verbesserung der Zuverlässigkeit durch Redundanz**
- Funktionswahrscheinlichkeit für Parallelsystem



Annahme einer Komponentenausfallrate von $\lambda = 10^{-5}/\mathrm{h}$

Zuverlässigkeit und Fehlertoleranz

- **Verbesserung der Zuverlässigkeit durch Redundanz**
- Seriensystem

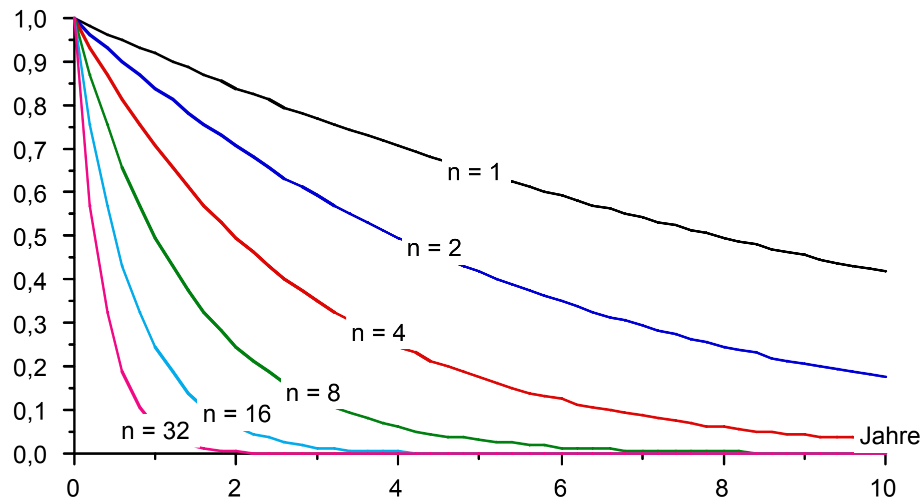


Seriensystem $$S_n = K_1 \wedge \ldots \wedge K_n$$

Zuverlässigkeit $$\varphi(S_n, t) = \prod_{i=1}^{n} \varphi(K_i, t)$$

Funktionswahrschein-lichkeit $\varphi\,(S_n, t)$

für $\lambda = 10^{-5}/h$



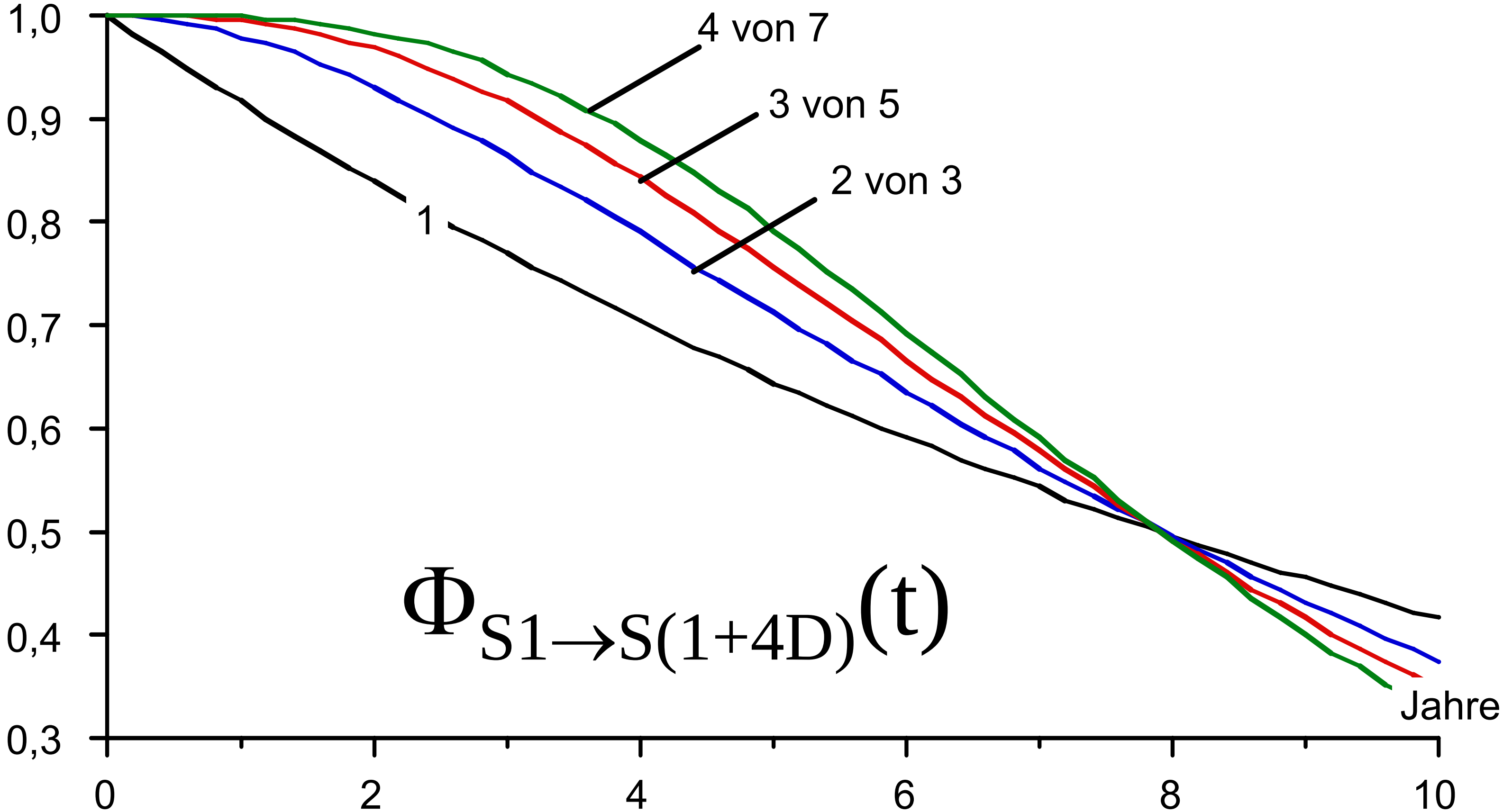
Zuverlässigkeit und Fehlertoleranz

- **Statisch redundantes System**
  - Ist die Fehlererfassung zu gering oder verbieten sich wiederholte Berechnungen wegen den geforderten maximalen Antwortzeiten, so kann statische Redundanz eingesetzt werden.
  - Dabei führen mehrere Komponenten die gleiche Berechnung aus, um anschließend die errechneten Ergebnisse zu vergleichen und ein mehrheitliches auszuwählen.
  - Bis zu f fehlerhafte Komponenten können überstimmt werden, wenn mindestens n=f+1 fehlerfreie, insgesamt also m=2·f+1 Komponenten vorhanden sind.

$$S_{m\,von\,m} = \bigvee_{1 \le i_1 < \ldots < i_n \le m} K_{i_1} \wedge \ldots \wedge K_{i_n}$$

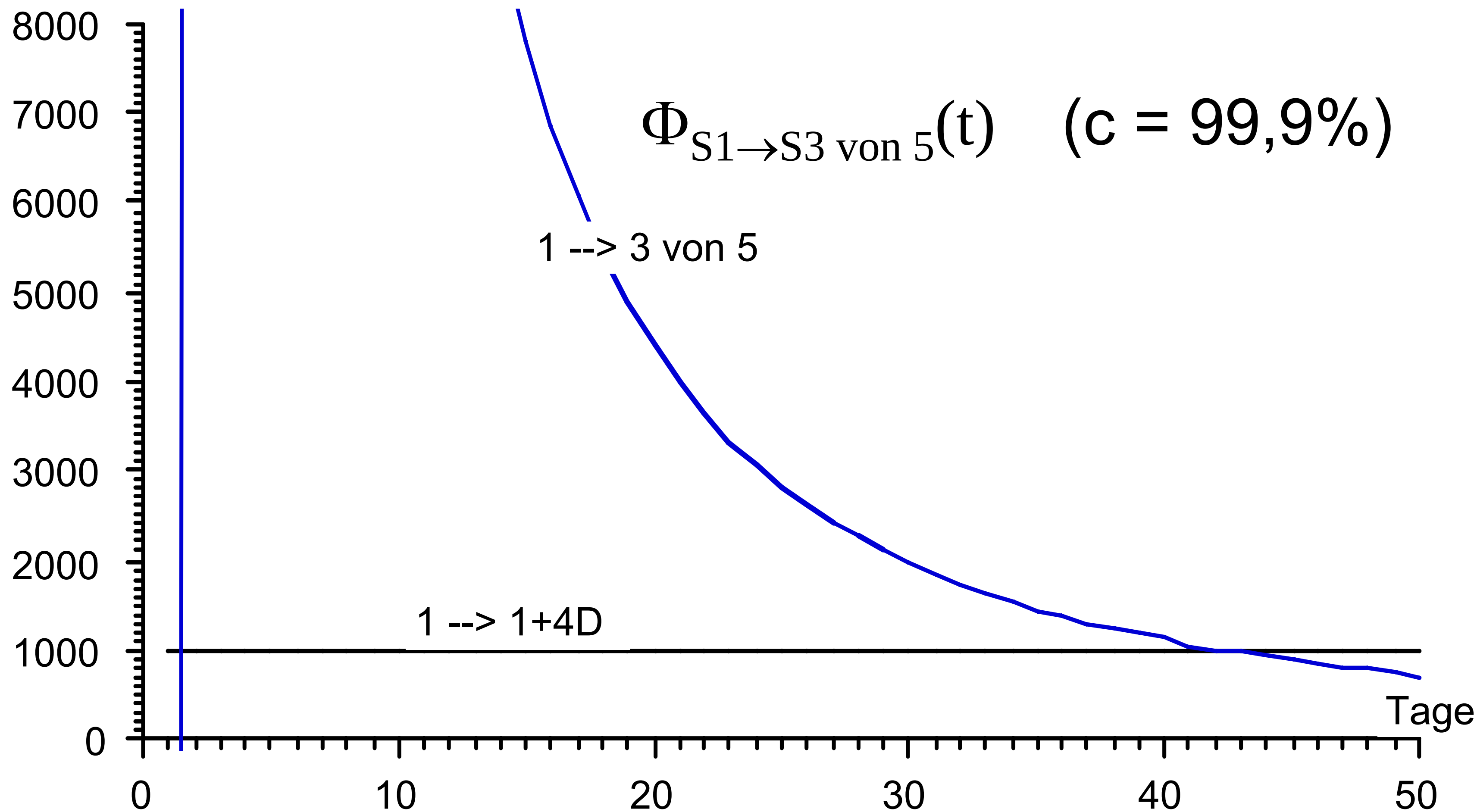
Zuverlässigkeit und Fehlertoleranz

- **Statisch redundantes System**



Zuverlässigkeit und Fehlertoleranz

- **Statisch redundantes System**



Zuverlässigkeit und Fehlertoleranz

- **Statisch redundantes System**
- Zuverlässigkeitsengpass
  - Maskierer M trifft in einem statisch redundanten System die Mehrheitsentscheidung. Dies verändert Systemfunktion und Zuverlässigkeit:

$$S_{n\,von\,mM} = M \wedge \left(\bigvee_{1 \le i_1 < \ldots < i_n \le n+r} K_{i_1} \wedge \ldots \wedge K_{i_n} \right)$$

  - Funktionswahrscheinlichkeit ist durch die des "Zuverlässigkeitsengpasses" M beschränkt:

    $\varphi\,(S_{n\ von\ mM}) \le \varphi\,(M)$.