TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Elektrotechnik & Informationstechnik Institut für Automatisierungstechnik, Professur für Prozessleittechnik

Zuverlässigkeitstechnik

Grundlagen

VL PLT-2
Professur für Prozessleittechnik

Übersicht

- Zuverlässigkeit vs. Verlässlichkeit
- Ziele der Zuverlässigkeitstechnik
- Wiederholung kontinuierliche Zufallsgrößen
  - Verteilungsfunktion
  - Wahrscheinlichkeitsdichtefunktion
- Empirische Bestimmung
- Versagensrate

Zuverlässigkeit

Zuverlässigkeit (engl. Reliability) ist ein Maß für die Fähigkeit des Systems, funktionstüchtig zu bleiben, z.B. die Wahrscheinlichkeit, dass das System während einer bestimmten Zeitdauer t nicht versagt

DIN 40041: Zuverlässigkeit ist die Beschaffenheit bezüglich der Eignung, während oder nach vorgegebenen Zeitspannen bei vorgegebenen Arbeitsbedingungen die Zuverlässigkeitsanforderungen zu erfüllen

Verlässlichkeit (aus der Ecke fehlertolerante Software)

Verlässlichkeit (Dependability):

- Grad der **Vertrauenswürdigkeit** in die vom System erbrachte Leistung
- **Subjektive Bewertung** eines Systems!

Komponenten, die zu Verlässlichkeit beitragen:

- Zuverlässigkeit (reliability) *
- Verfügbarkeit (availiability) *
- Wartbarkeit (maintainability) *
- Sicherheit (safety) **
- Integrität (integrity) **
- Vertraulichkeit (confidentiality) **

* Laprie (1985) Dependable Computing and Fault Tolerance: Concepts and terminology
** Avizienis, Laprie, Randell (2001) Fundamental Concepts of Dependability

Zuverlässigkeitstechnik

Ziel:

Berechnung quantitativer Kenngrößen von reparierbaren oder nicht reparierbaren **Betrachtungseinheiten** zur **Vorhersage der Funktionsfähigkeit** des **Gesamtsystems**

Betrachtungseinheit

- Teilsystem, Software, Baugruppe, Bauelement (je nach Aufgabe)

Achtung! Vereinfachte Betrachtungsweise:

Jede Betrachtungseinheit ist entweder

- **funktionsfähig** – Verhalten entspricht der Anforderungsspezifikation

oder

- **nicht funktionsfähig** – Verhalten entspricht nicht der Anforderungsspezifikation

Fehler und Ausfall

Fehler:

- DIN40041: Nichterfüllung einer Forderung
- Nichterfüllung vorgegebener Forderungen durch einen Merkmalswert (Zustand)
- Eine Komponente ist in einem **nicht funktionsfähigen Zustand.**

Ausfall:

- DIN40041: Beendigung der Funktionsfähigkeit einer materiellen Einheit im Rahmen der zugelassenen Beanspruchung
- Das Aussetzen der Ausführung einer festgelegten Aufgabe.
- Übergang vom fehlerfreien (= funktionsfähigem) in den fehlerhaften (= nicht funktionsfähigem) Zustand (Ereignis).

Fragestellungen der Zuverlässigkeitstechnik

Wie zuverlässig ist eine Funktionseinheit?

Beschaffenheit einer Funktionseinheit bzgl. ihrer Fähigkeit, während oder nach vorgegebenen Zeitspannen bei festgelegten Betriebsbedingungen die Zuverlässigkeitsanforderungen zu erfüllen (DIN 40041, DIN 55350).

Wie hoch ist die Lebensdauer einer Betrachtungseinheit?

für die einzelne **nicht instandsetzbare** Betrachtungseinheit die beobachte **Zeitspanne L** vom Beanspruchungsbeginn t_0 bis zum Ausfallzeitpunkt t_F:
$L := t_F - t_0$

Wie hoch ist die Verfügbarkeit eines Systems?

Wahrscheinlichkeit V, ein System zu einem vorgegebenen Zeitpunkt **t** in einem **funktionsfähigen** Zustand anzutreffen.

Wiederholung Verteilungsfunktion einer Zufallsvariable (ZV) X

- Verteilungsfunktion (VF)
  - für diskrete ZV
  - für stetige ZV

$$F_X(x) = P(X \le x)$$

$$F_X(x) = \sum_{x_i \le x} f_X(x_i)$$

$$F_X(x) = \int_{-\infty}^{x} f_X(y)dy$$

- Wahrscheinlichkeits-dichtefunktion
  - für diskrete ZV
  - für stetige ZV

$$f_X(x) = P(X = x)$$

$$f_X(x) = \frac{dF_X(x)}{dx}; \int_{-\infty}^{+\infty} f_X(y)dy = 1$$

Zuverlässigkeitsfunktion (Überlebenswahrscheinlichkeit)

Zuverlässigkeitsfunktion R(t) = W(T>t)

gibt an, mit welcher Wahrscheinlichkeit Betriebszeiten **T** auftreten, die länger sind als ein vorgegebener Zeitraum **t**

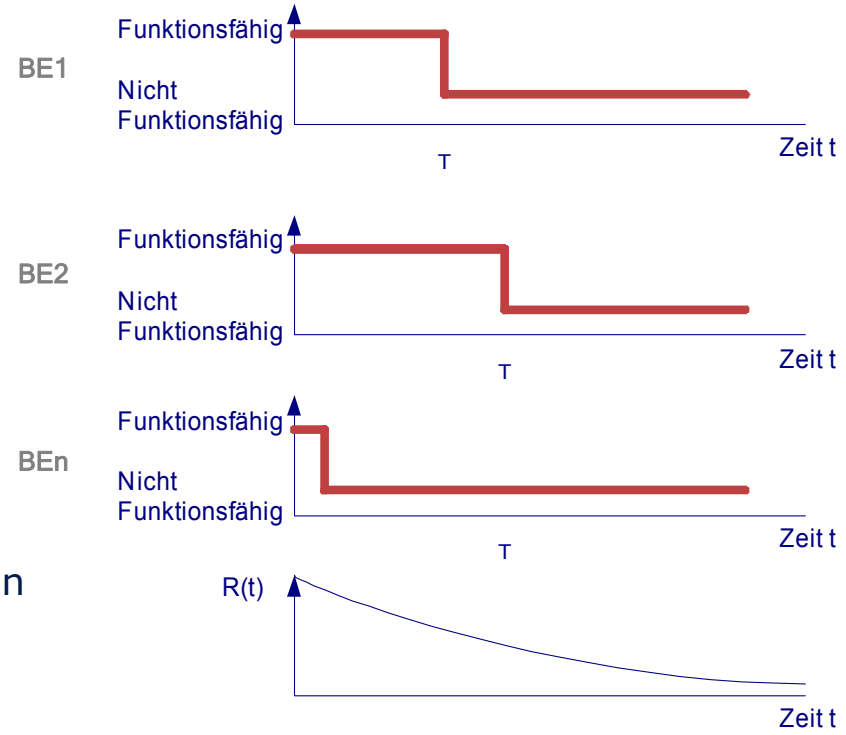
auch

mit welcher Wahrscheinlichkeit ist die Lebensdauer **L := $t_F - t_0$** größer als ein vorgegebener Zeitraum **t**

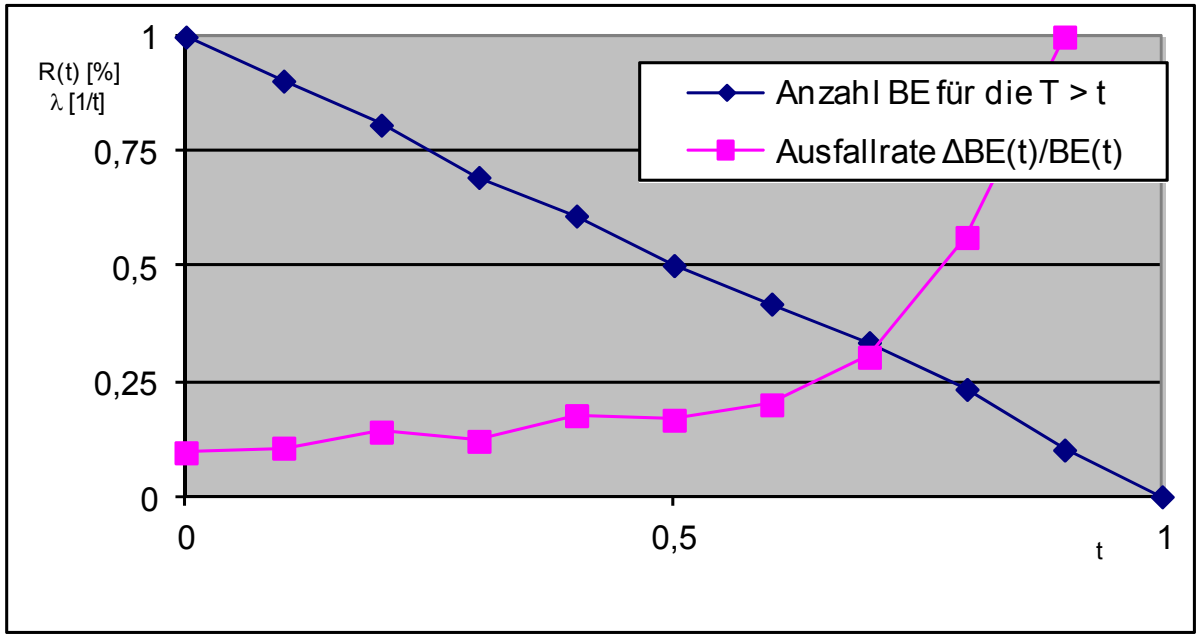
Empirische Bestimmung der Zuverlässigkeitsfunktion

- Mehrere baugleiche Betrachtungseinheiten
- Gleichzeitige Inbetriebsetzung
- **Zufällige** Ausfallmechanismen führen zu **unterschiedliche** Ausfallzeiten T
  - Model gilt nicht für Software!

- Gemessen wird der Zeitpunkt der beobachteten Ausfälle für die Betrachtungseinheiten.
- Daraus wird eine Verteilungsfunktion abgeleitet → R(t)



Beispiel (→ Excel)



Versagenswahrscheinlichkeit

Versagenswahrscheinlichkeit

- Die Wahrscheinlichkeit, dass die Betriebszeiten T bis zum Versagen nicht länger sind als t

- $Q(t) = W(T \leq t) = 1 - R(t)$

MTTF (mittlere Lebensdauer)

- En ISO 13849-1: Mittlere Betriebsdauer bis zum Ausfall
- Bei konst. Ausfallrate zum Zeitpunkt MTTF etwa 63 % der Einheiten ausgefallen!

Versagensrate

Versagensrate / Ausfallrate

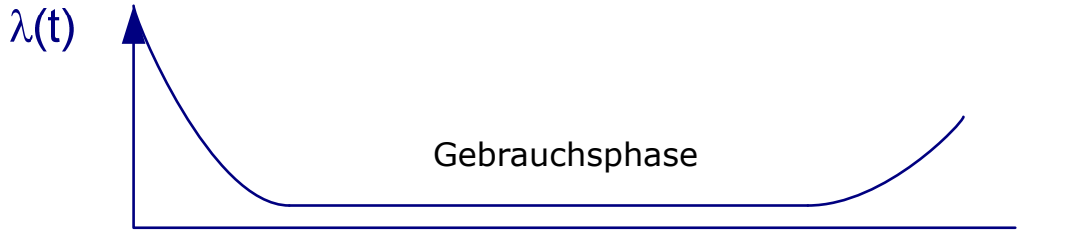
- Negativer Wert der Ableitung der logarithmischen Zuverlässigkeitsfunktion
- $$\lambda(t) = -\frac{d}{dt}\left[\ln R(t)\right] = -\frac{1}{R(t)}\,\frac{dR(t)}{dt} \qquad R(t) = e^{-\int_{\tau=0}^{t} \lambda(\tau)\, d\tau}$$

Gleichung hat einfache Lösung für mittlere Versagensrate $\lambda(t) = \text{const.}$

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

und

- $\lambda = 1/MTTF$



Mittel zur Erhöhung der Zuverlässigkeit

- Konstruktion zuverlässigerer Komponenten
  - Material
  - Herstellungstechnologie
  - Konstruktion/Gestaltung
  - Auswahl geeigneter Komponenten (Eingangskontrolle, Burn-in)
  - Überdimensionierung, Unterlastung
  - Störfestigkeit, Schutz gegen Umwelteinflüsse
  - Verwendung von Selbsttestverfahren
- Redundanzmaßnahmen
  - Idee: „Doppelt genäht hält besser"
    - wenn eine Komponente ausfällt, dann übernimmt eine andere die Aufgabe
    - wenn es zwei tun, dann fällt's nicht auf wenn einer wegfällt

Erhöhung der Redundanz

- Redundanz (DIN40041): Funktionsbereites Vorhandensein **zusätzlicher** technischer Mittel
- Passive Redundanz:
  - (*nicht funktionsbeteiligte*, *kalte*, *dynamische*, *heißer/kalter stand-by*)
  - Zusätzliche Mittel sind bereitgestellt, werden aber erst bei Ausfall an der Aufgabe beteiligt.
- Aktive Redundanz:
  - (*funktionsbeteiligte*, *heiße*, *statische*)
  - Mehrere technische Mittel führen die Aufgabe gleichzeitig aus.

- **Frage:** Welche grundlegende Voraussetzung muss erfüllt sein, dass das überhaupt funktioniert?

Passive Redundanz

Prinzip:

- Ein gleiches technisches Mittel steht eingeschaltet (hot standby) oder ausgeschaltet (cold standby) zur Verfügung.
- Im Falle eines Ausfalls muss es „nur" stoßfrei aktiviert werden.

Prozedur:

- Schritt 1: Erkenne, dass es einen Ausfall gab
- Schritt 2: Lokalisiere die ausgefallene Einheit
- Schritt 3: Wähle eine geeignete redundante Einheit aus
- Schritt 4: Bringe die redundante Einheit auf Stand
- Schritt 5: Schalte auf die redundante Einheit um
- Schritt 6: Isoliere die ausgefallene Einheit
- Schritt 7: Redundante Einheit hat all Fkt. der ausgefallenen übernommen

Jeder Schritt ist selbst fehleranfällig!

Aktive Redundanz

Prinzip:

- Gleiche Mittel werden mehrfach eingesetzt und geeignet verschaltet

Beispiel: Kontakt am Relais

Zwei Ausfallarten:

- FSN (Kontakt schließt nicht, Kontakt abgebrannt) und
- FÖN (Kontakt öffnet nicht, Kontakt verklebt)

	Ausfallart FSN	Ausfallart FÖN
Serienschaltung --| |--| |-- S1 S2	Ausfall System	**Funktion System**
Parallelschaltung --| |--+---- S1 | --| |--+ S2	**Funktion System**	Ausfall System

Aktive Redundanz

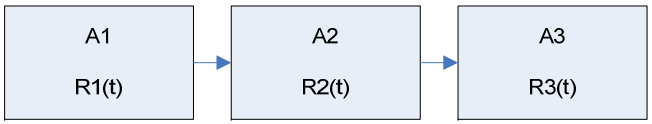
Komplexere Strukturen

	Ausfallart FSN (Einfachfehler)	Ausfallart FÖN (Einfachfehler)
Serienparallelschaltung --| |---+--+--| |--+-- S1 | | S2 | --| |---+ +--| |--+ S3 S4	Funktion System	Funktion System
Parallelserienschaltung --| |-----------| |--+-- S1 S2 | --| |-----------| |--+ S3 S4	Funktion System	Funktion System

Zuverlässigkeitsmodelle für Hardwaresysteme

Serienanordnung

- System lebt, solange alle Komponenten leben

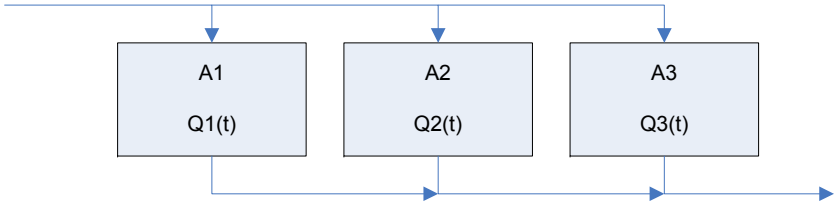


$$R_{ges}(t) = \prod_{i=1}^{n} R_i(t)$$

$$MTBF_{ges} = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTBF_i}}$$

Parallelanordnung

- System fällt aus, wenn alle Komponenten ausfallen



$$Q_{ges}(t) = \prod_{i=1}^{n} Q_i(t)$$

$$R_{ges}(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t))$$

Redundanzstrukturen

Beispiel 1)

- Systemkomponenten: 2 Server c_1,c_2; 1 Netzwerk c_3
- System funktionsfähig, wenn mindestens ein Server und das Netzwerk funktionieren.

- Redundanzstruktur Φ
  - Boolscher Ausdruck mit der semantischen Belegung des Wahrheitswerts „Komponente/System ist verfügbar"
  - Hier: $\Phi = (c_1 \vee c_2) \wedge c_3$

- Wenn Ereignisse **statistisch unabhängig** sind, dann gilt:
  $Pr(\Phi_1 \wedge \Phi_2) = Pr(\Phi_1) * Pr(\Phi_2)$
  $Pr(\Phi_1 \vee \Phi_2) = Pr(\Phi_1) + Pr(\Phi_2) - Pr(\Phi_1 \wedge \Phi_2)$
  $Pr(\neg\Phi_1) = 1 - Pr(\Phi_1)$

Redundanzstrukturen (Forts. 1)

- Mit:
  $\Phi = (c_1 \vee c_2) \wedge c_3$
- und
  $Pr(c_i) = a_i$

  $Pr(\Phi) = Pr(((c_1 \vee c_2) \wedge c_3)$

Wenn Ereignisse **statistisch unabhängig** sind, dann gilt

- $Pr(\Phi_1 \wedge \Phi_2) = Pr(\Phi_1) * Pr(\Phi_2)$
- $Pr(\Phi_1 \vee \Phi_2) = Pr(\Phi_1) + Pr(\Phi_2) - Pr(\Phi_1 \wedge \Phi_2)$
- $Pr(\neg\Phi_1) = 1 - Pr(\Phi_1)$

Berechnung Beispiel → Tafelbild

Redundanzstrukturen / Forts

Beispiel 2)

- **Drei** Systemkomponenten c_1,c_2,c_3
- System funktionsfähig, wenn mindestens zwei Komponenten funktionieren.

- $\Phi = (c_1 \wedge c_2) \vee (c_1 \wedge c_3) \vee (c_2 \wedge c_3)$

- Achtung! Terme sind **nicht stochastisch unabhängig** voneinander

- Shannon Dekomposition: Substition von redundanten Variablen c_i durch Zerlegung in Teilausdrücke mit c_i=true und c_i=false bis keine Variablen in den Termen mehrfach auftreten!

  $Pr(\Phi) = a_1 * Pr(\Phi_{c1=ture}) + (1-a_1) * Pr(\Phi_{c1=false})$

Berechnung Beispiel → Tafelbild

Literatur

Lehrbücher

Schneeweiß, W.G. (1992) Zuverlässigkeitstechnik. von den Komponenten zum System. Köln:Datakontext-Verlag. (SLUB)

…

Bertsche, Göhner, Jensen, Schinköthe, Wunderlich (2009) Zuverlässigkeit mechatronischer Systeme. Grundlagen und Bewertung in frühen Entwicklungsphasen. Berlin:Springer

Normen

DIN 40041 Zuverlässigkeit; Begriffe

DIN 55350 Begriffe zum Qualitätsmanagement

EN 13849 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen

Verlässlichkeit von Fehlertoleranten Rechnersystemen

- Laprie (1985) Dependable Computing and Fault Tolerance: Concepts and terminology
- Avizienis, Laprie, Randell (2001) Fundamental Concepts of Dependability