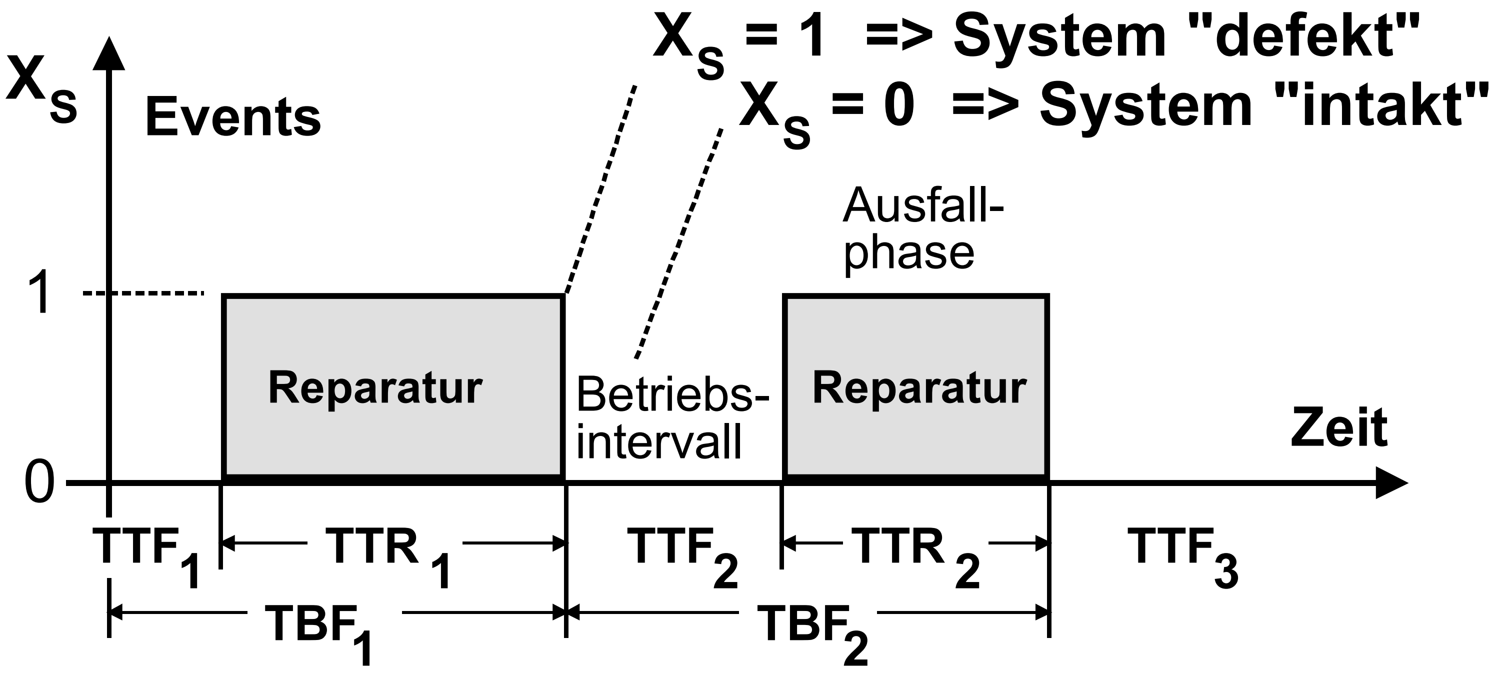
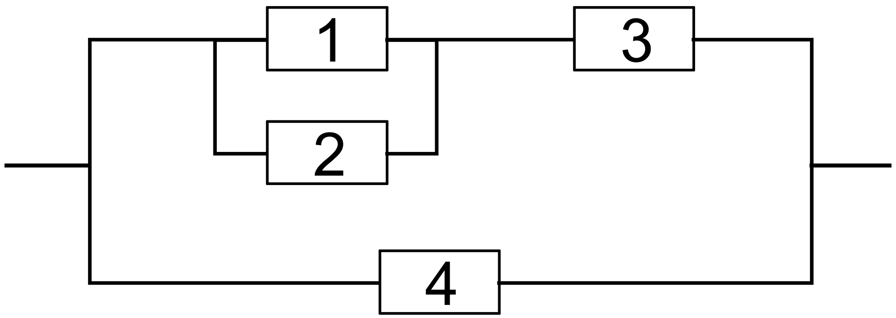
3. Graphische Hilfsmittel und systemtheoretische Grundlagen



TTF = Time To Failure **TTR** = Time To Repair

TBF = Time Between Failure

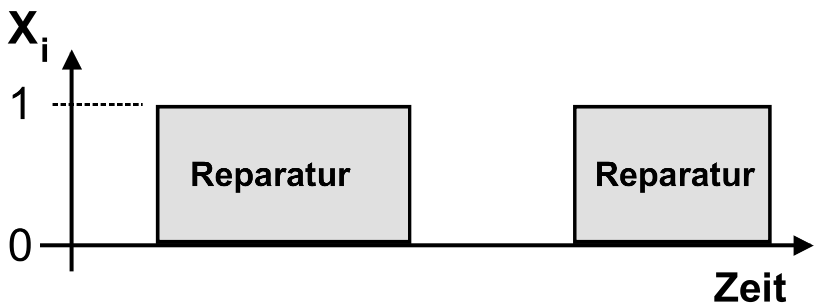
Abschnitt 3.1 — Redundanzstruktur-Funktion



- System **S** besteht aus den Einzelkomponenten $\mathbf{K_1}$, $\mathbf{K_2}$, $\mathbf{K_3}$ und $\mathbf{K_4}$
- Darstellung des Systemzustandes **S** durch den Zustand der Komponenten

Indikatorvariable (der Komponente):

$$\mathbf{X_i(t)} = \begin{cases} \mathbf{1} & \Rightarrow \text{Komponente } K_i \text{ defekt} \\ \mathbf{0} & \Rightarrow \text{Komponente } K_i \text{ intakt} \end{cases}$$



Redundanzstruktur-Funktion:

$$\mathbf{X_S(t)} = \begin{cases} \mathbf{1} & \Rightarrow \text{für alle } \mathbf{X_i}\text{, für die } \mathbf{S} \text{ in } \mathbf{t} \text{ defekt} \\ \mathbf{0} & \Rightarrow \text{für alle } \mathbf{X_i}\text{, für die } \mathbf{S} \text{ in } \mathbf{t} \text{ intakt} \end{cases}$$

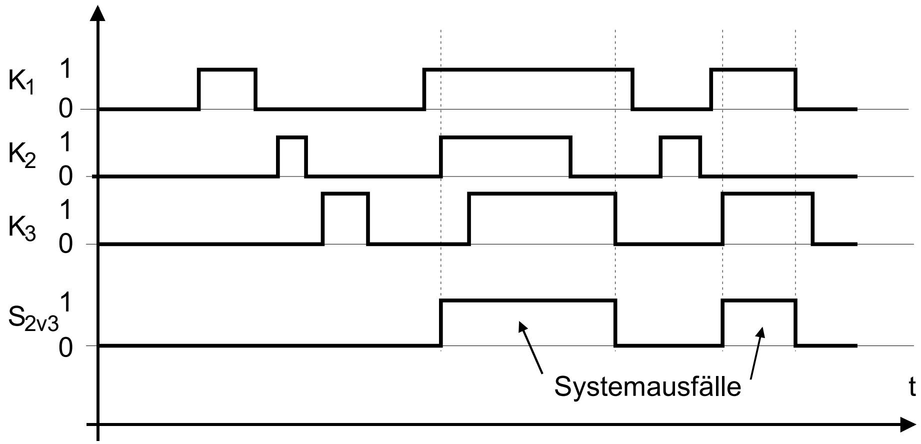
Un- bzw. Verfügbarkeit (der Komponente) im Zeitpunkt t_0:

$$\mathbf{U_i = P\{X_i(t_0) = 1\} \quad V_i = P\{X_i(t_0) = 0\}}$$

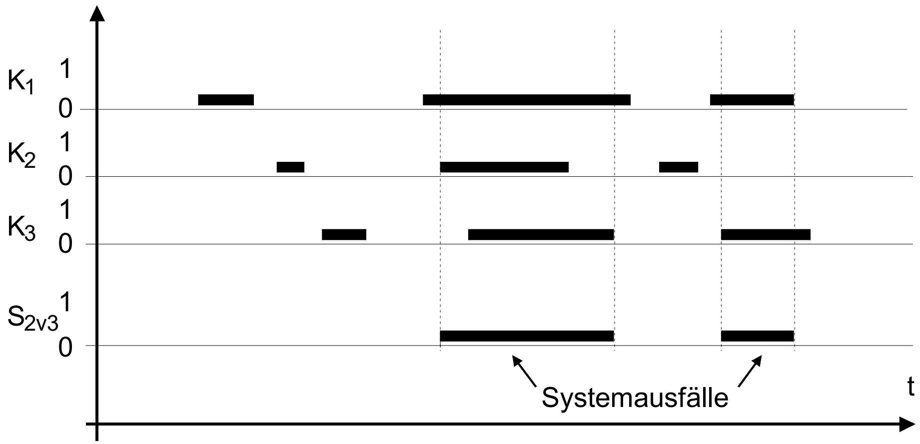
Verfügbarkeit (des System S):

$$\mathbf{V_S = P\{X_S(t_0) = 0\} = f\,(V_1, V_2, V_3, V_4)}$$

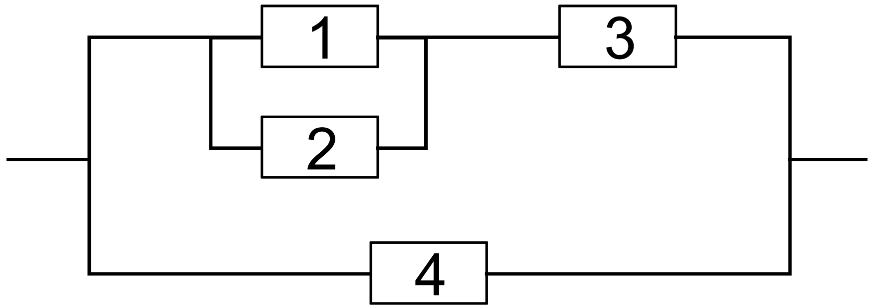
Zeitdiagramm



Balkendiagramm



2v3-System: Zwei von insgesamt drei Komponenten müssen intakt sein, damit das System funktioniert (ansonsten Systemausfall)



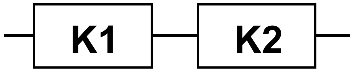
System S intakt, wenn es wenigstens einen Pfad (Kantenzug) mit ausschließlich intakten Komponenten gibt.

- System **S** als Gerichteter Graph
- Komponenten $\mathbf{K_i}$ als Rechtecke mit Nummern oder Namen
- zeigt die Redundanzstruktur des Systems an
- funktionsorientiertes Modell

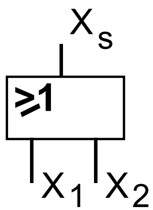
Ergebnis:

$$V_S = (V_1 + V_2 - V_1 \cdot V_2) \cdot V_3 \cdot (1 - V_4) + V_4$$

Serienschaltung:



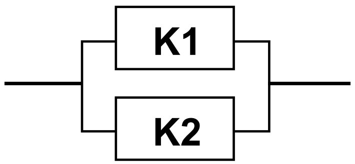
(ODER-Verknüpfung)



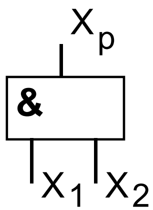
X_1	X_2	X_s
0	0	0
0	1	1
1	0	1
1	1	1

$$\boxed{V_s = V_1 \cdot V_2}$$

Parallelschaltung:



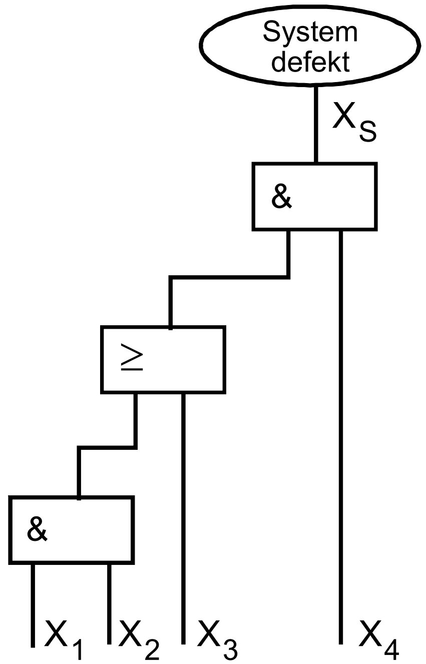
(UND-Verknüpfung)



X_1	X_2	X_p
0	0	0
0	1	0
1	0	0
1	1	1

$$\boxed{V_p = V_1 + V_2 - V_1 \cdot V_2}$$

$$U_p = U_1 \cdot U_2 \longrightarrow 1 - V_p = (1 - V_1) \cdot (1 - V_2)$$

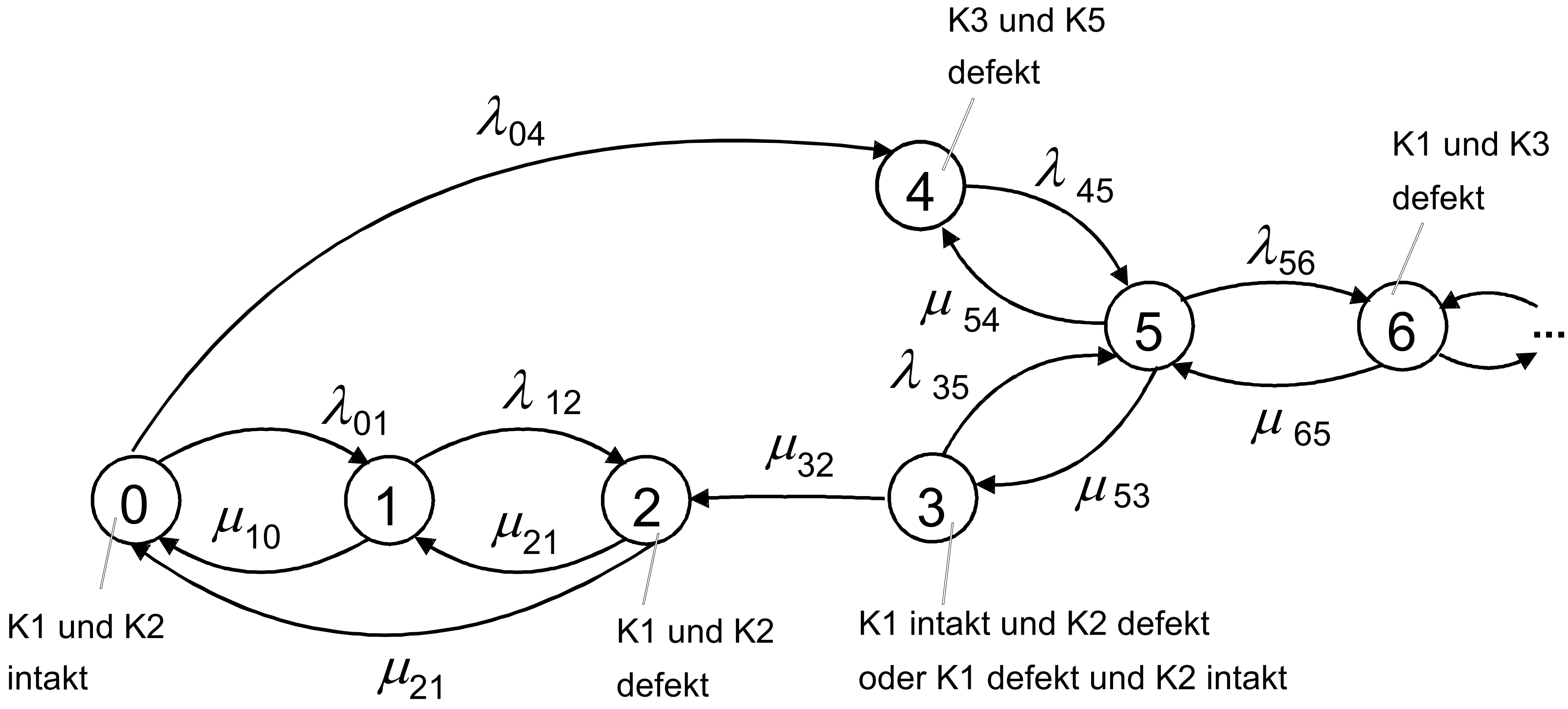


- Baumähnliche graphische Darstellung Boolescher Funktionen
- Komponentenausfälle als Blätter des Baumes
- zeigt die Redundanzstruktur des Systems an
- fehlerorientiertes Modell

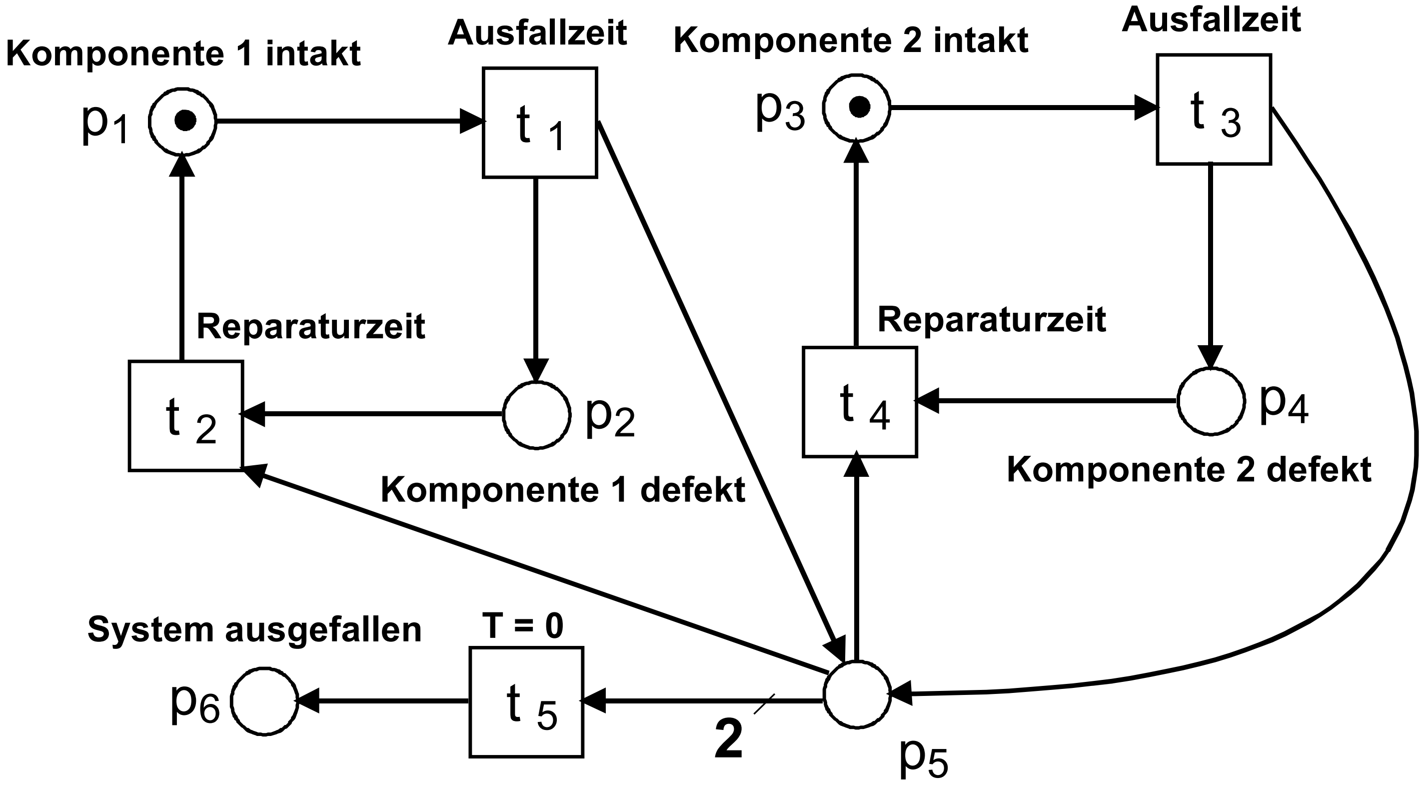
System S defekt, wenn die Wurzel des Baumes ein **aktives** Signal zeigt

Ergebnis (Mathematische Behandlung siehe Absch. 3.5, S. 34 ff.)**:**

$$X_S = \big((X_1 \wedge X_2) \vee X_3 \big) \wedge X_4$$

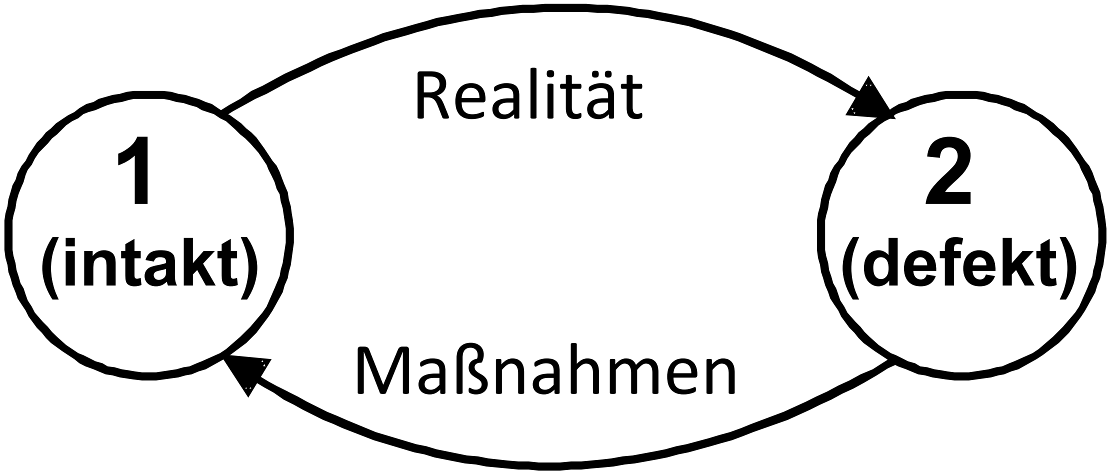

K3 und K5
defekt
λ_{04}
4
λ_{45}
K1 und K3
defekt
λ_{56}
μ_{54}
5
6
...
λ_{35}
μ_{65}
λ_{01}
λ_{12}
μ_{32}
0
1
2
3
μ_{53}
μ_{10}
μ_{21}
K1 und K2
intakt
K1 und K2
defekt
K1 intakt und K2 defekt
oder K1 defekt und K2 intakt
μ_{21}

Petrinetze:


Komponente 1 intakt
Ausfallzeit
Komponente 2 intakt
Ausfallzeit
p1
t 1
p3
t 3
Reparaturzeit
Reparaturzeit
t 2
p2
t 4
p4
Komponente 1 defekt
Komponente 2 defekt
System ausgefallen
T = 0
p6
t 5
2
p5

Modellbildung für ein **reparierbares** System:

λ = Ausfallrate



μ = Reparaturrate

Kontinuitätsgleichung:

$$\frac{dP_1(t)}{dt} = -\lambda \cdot P_1(t) + \mu \cdot P_2(t)$$

Normierungsbedingung:

$$P_1(t) + P_2(t) = 1$$

Verfügbarkeit:

$$V_S = \lim_{t \to \infty} P_1(t)$$

Kenngrößen aus wahrscheinlichkeitstechnischer Sicht:

- **Zuverlässigkeit (Reliability):**

  Beschaffenheit einer Funktionseinheit bzgl. ihrer Fähigkeit, während oder nach vorgegebenen Zeitspannen bei festgelegten Betriebsbedingungen die Zuverlässigkeitsanforderungen zu erfüllen (DIN 40 041, DIN 55 350).

- **Verfügbarkeit (Availability):**

  Wahrscheinlichkeit, ein System zu einem vorgegebenen Zeitpunkt **t** in einem **funktionsfähigen** Zustand anzutreffen (DIN 40 042, ISO/IEC 2382, 7498, 9126 und 2003).

Weitere Kenngrößen:

- **Unverfügbarkeit (Unavailability):**

  ... **U** ist das **1er-Komplement** der Verfügbarkeit **V, d. h.:**

  $$\mathbf{U := 1 - V}$$

- **Lebensdauer (Life Time):**

  ... für die einzelne **nicht instandsetzbare** Betrachtungseinheit die beobachte **Zeitspanne L** vom Beanspruchungsbeginn $\mathbf{t_0}$ bis zum Ausfallzeitpunkt $\mathbf{t_F}$:

  $$\mathbf{L := t_F - t_0}$$

Weitere Kenngrößen:

- **Downtime DT in [min/yr]:**

  ... die **Zeitdauer**, für die die Dienste bzw. die Funktionalität eines Systems in einen bestimmten Zeitraum (meistens **bezogen auf ein Jahr**) nicht verfügbar sind. Typisch ist der Durchschnittswert über eine große Zahl von Benutzern.

  $$\mathbf{DT = U * 525.600 \quad [min/yr]}$$

  wobei

  U = Unavailability

  525.600 = 365 * 24 * 60 (**1** Jahr entspricht **525.600** Minuten)

Erwartungs- bzw. Durchschnittswerte:

MTTF = avg $\langle TTF_i \rangle$ Mean Time To Failure
(mittlere ausfallfreie Zeitspanne)

MTTR = avg $\langle TTR_i \rangle$ Mean Time To Repair
(mittlere Ausfalldauer)

MTBF = avg $\langle TBF_i \rangle$ Mean Time Between Failure
(mittlere Zeitdauer zwischen Ausfällen)

Bei uns gilt stets:

MTBF = MTTF + MTTR

Ausfall- und Reparaturrate:

Ausfallrate	λ :	$\lambda = 1 / MTTF$
Reparaturrate	μ :	$\mu = 1 / MTTR$
Mittlere Fehlerhäufigkeit (bzw. durchschnittliche Fehlerrate AFR)	ν :	$\nu = 1 / MTBF$

Demnach gilt der Zusammenhang:

$$\nu = \lambda * \mu / (\lambda + \mu)$$

Kenngrößen eines **reparierbaren** Systems:

- Mit Hilfe von MTTF und MTBF lassen sich die **Verfügbarkeit V**, die **Unverfügbarkeit U** und die **durchschnittliche Fehlerrate AFR** experimentell aus dem Systemverhalten ermitteln.
- Umgekehrt beschreiben **V**, **U** und **AFR** das Systemverhalten eines **reparierbaren** Systems dann, wenn sich **Betriebsintervalle** (***System = intakt***) und **Ausfallphasen** (***System = defekt***) abwechseln.
- Im **stationären Fall** gilt:

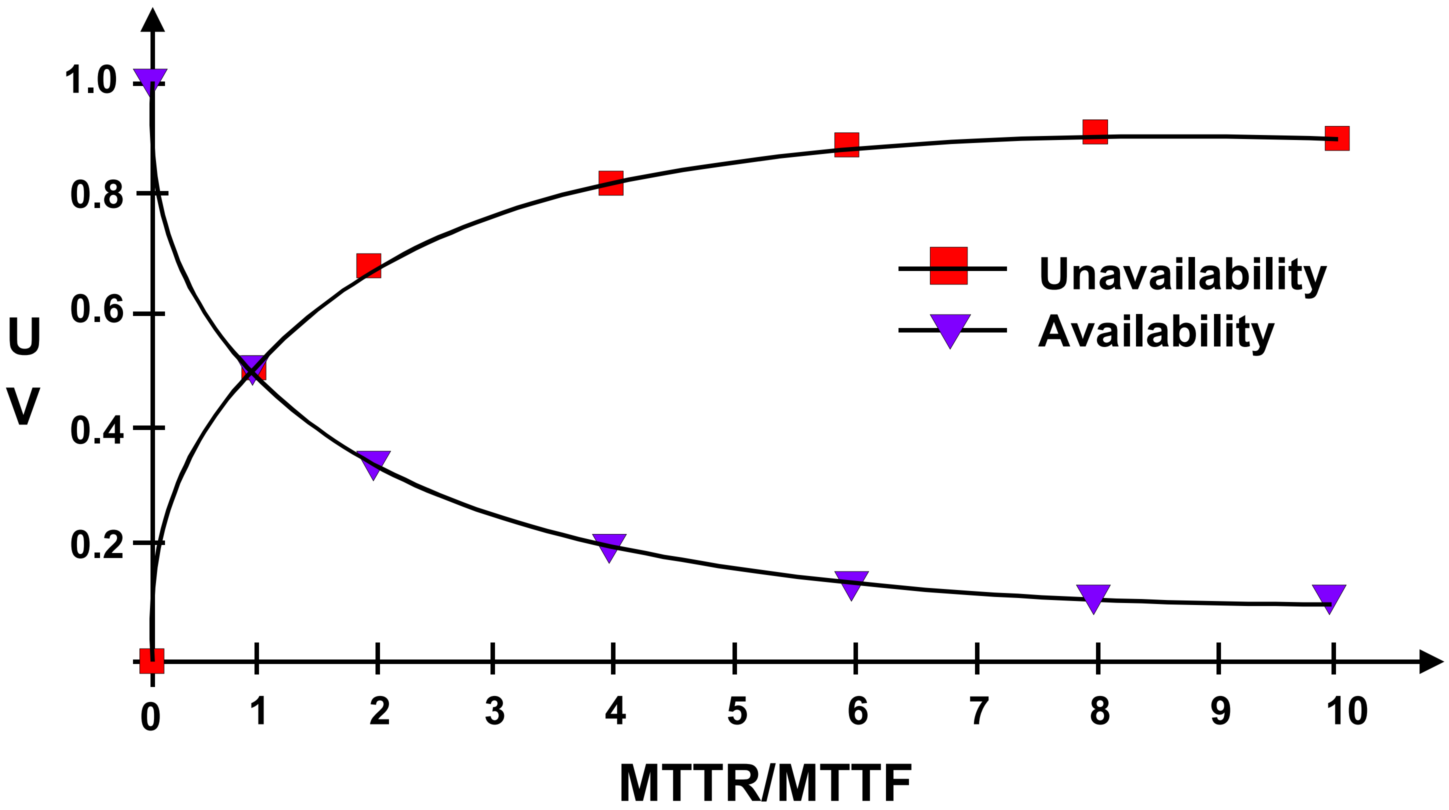
Kenngrößen eines reparierbaren Systems:

$$V = \frac{\mu}{\lambda + \mu} = \frac{MTTF}{MTTF + MTTR} = 1 - U$$

$$U = \frac{\lambda}{\lambda + \mu} = \frac{MTTR}{MTTF + MTTR} = 1 - V$$

$$AFR = \nu = \frac{1}{MTBF} = \frac{\lambda \cdot \mu}{\lambda + \mu}$$

V und U als Funktion von MTTR/MTTF:



Rechenbeispiel:

Verfügbarkeit	Unverfügbarkeit	Downtime
99.99 %	0.01 %	53 min/yr
99.98 %	0.02 %	106 min/yr
99.95 %	0.05 %	265 min/yr
99.90 %	0.10 %	530 min/yr

Kenngrößen eines **nicht-reparierbaren** Systems:

... diese drücken das Systemverhalten bei ununterbrochenem Betrieb **ohne** zwischengeschobenen Reparaturphasen aus.

- Lebensdauer (Life Time) → **L**
- Mittlere Lebensdauer (Mean Life Time) → $\mathbf{T_M := \langle L \rangle}$ = MTTF
- Ausfallwahrscheinlichkeit (Probability Of Failure) → **F(t)**
- Überlebenswahrscheinlichkeit → **R(t) = 1 – F(t)**
- Ausfallrate oder Ausfallhäufigkeitsdichte → **A(t)**

Mittlere Lebensdauer T_M:

$$T_M = E(L) = \langle L \rangle := \int_0^{+\infty} t \cdot f_L(t)\, dt = \int_0^{+\infty} R(t)\, dt$$

wobei

- L = Lebensdauer ($L \geq 0$)
- E(L) = Erwartungswert der Lebensdauer
- f_L = Dichtefunktion der Lebensdauer
- R(t) = Überlebenswahrscheinlichkeit

Ausfallwahrscheinlichkeit:

Wahrscheinlichkeit einer Betrachtungseinheit des Anfangbestandes (die zum Zeitpunkt **t = 0** intakt ist) bis zu einem vorgegebenen Zeitpunkt **t** auszufallen → **F(t)**

⇒ entspricht der **Verteilungsfunktion** der Lebensdauer !

d. h.

$$\mathbf{F(t) = F_L(t)}$$

Ausfallwahrscheinlichkeit:

$$\mathbf{F(t) = P(L \leq t) := F_L\,(t) := \int_0^t f_L(\tau)\, d\tau}$$

wobei

L = Lebensdauer

P = Wahrscheinlichkeit

f_L = Dichtefunktion der Lebensdauer

F_L = Verteilungsfunktion der Lebensdauer

F = Ausfallwahrscheinlichkeit

Überlebenswahrscheinlichkeit:

Die Überlebenswahrscheinlichkeit ist das Komplement der Ausfallwahrscheinlichkeit zu 1 → **R(t)**

d. h.

$$\left.\begin{array}{l}\text{Überleben-}\\ \text{wahrschein-}\\ \text{lichkeit}\end{array}\right\} = 1 - \left\{\begin{array}{l}\text{Ausfall-}\\ \text{wahrschein-}\\ \text{lichkeit}\end{array}\right.$$

bzw.

$$\mathbf{R(t) = 1 - F(t)}$$

Ausfallrate A(t):

Die Ausfallrate ist ein Maß für die temporäre Ausfallhäufigkeit und damit für die Ausfallhäufigkeitsdichte.

$$\mathbf{A(t) \;=\; -\;1 \,/\, R(t) * dR(t) \,/\, dt}$$

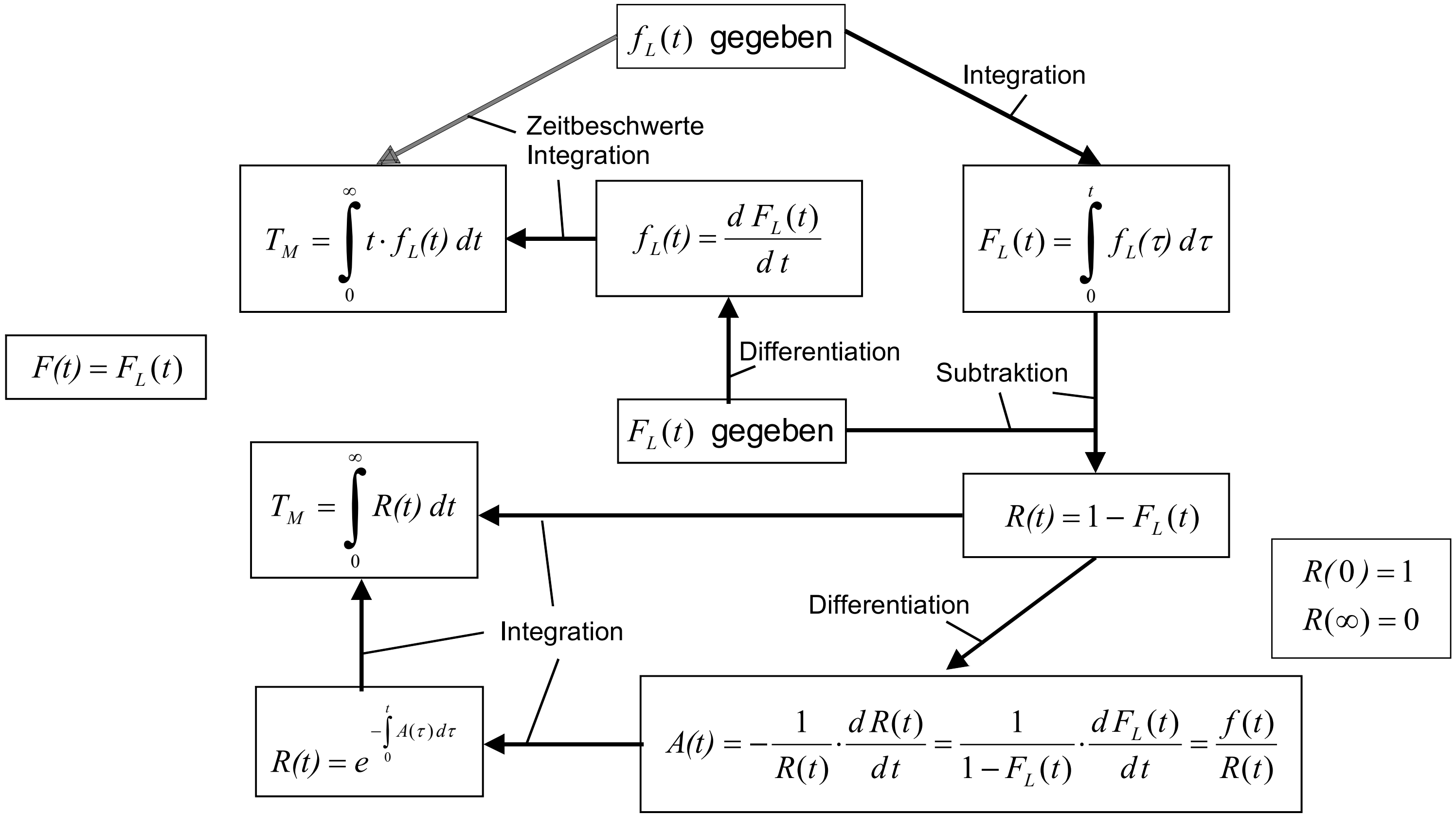
wobei

R(t) = Überlebenswahrscheinlichkeit

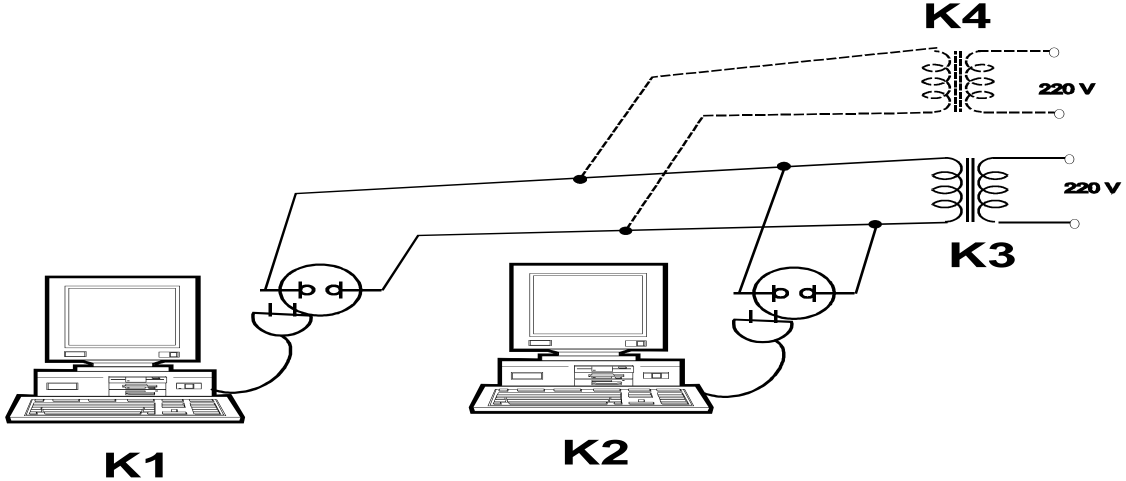
d / dt = Ableitung nach der Zeit t

A(t) = Ausfallrate in [Ausfälle / Zeiteinheit]

Kenngrößen eines **nicht-reparierbaren** Systems:



Doppelrechnersystem (K1 und K2)
an kritischer Stromversorgung (K3 bzw. K4)



- Welche Systemverfügbarkeit V_S ergibt sich für die vorliegende Anordnung?
- Ist die Systemverfügbarkeit höher als die Verfügbarkeit der Einzelrechner?
- Schafft Redundanz tatsächlich immer eine höhere Systemverfügbarkeit?

Grundlagen der Aussagenlogik:

Es seien **a**, **b** logische Aussagen. Dann folgen wir nachstehender **Notation**:

Negation:	$\bar{\mathbf{a}}$, $\bar{\mathbf{b}}$,	Komplementbildung
Konjunktion:	**a** ∧ **b** = **a** and **b** = **a** & **b**	UND-Verknüpfung
Disjunktion:	**a** ∨ **b** = **a** or **b** = **a** I **b**	ODER-Verknüpfung

Boolesche Algebra:

Wir definieren auf der Menge **M** = {**a**, **b**, ...} der logischen Aussagen **a**, **b**, ... ∈ {0, 1} zwei binäre Operatoren ∧ und ∨ sowie eine unäre Operation ¯ (Komplementbildung) und schreiben hierfür [**M**, ∧, ∨, ¯]. Die Algebra [**M**, ∧, ∨, ¯] heißt **Boolesche Algebra**.

Boolesche Funktion:

Auf **B** = {0, 1} definieren wir Funktionen **f** mit endlich vielen Argumenten (Variablen) $\mathbf{x_1}$, $\mathbf{x_2}$, ..., $\mathbf{x_n}$ aus **B** mit den Funktionswerten $\mathbf{y_m}$ = f ($\mathbf{x_1}$, $\mathbf{x_2}$, ..., $\mathbf{x_n}$) in **B**. **f** heißt **Boolesche Funktion**.

Unter der Funktion f ($\mathbf{x_1}$, $\mathbf{x_2}$, ..., $\mathbf{x_n}$) versteht man somit die Abbildung

$$\mathbf{f} : \mathbf{B}^n \rightarrow \mathbf{B}^1 = \{0, 1\} ,$$

wobei

$\mathbf{B}^n$ der **n-dimensionale Binärraum** aller n-Tupel aus Nullen und Einsen ist.

Bei **n** Variablen gibt es **m** = $2^{2^{\mathbf{n}}}$ (sprich: 2 hoch 2 hoch **n**) nicht äquivalente Boolesche Funktionen (im Falle n = 2 also 16).

Satz:

Jede Boolesche Funktion lässt sich unter ausschließlicher Verwendung der Operatoren $\wedge$ und $\vee$ sowie der Komplementbildung $\overline{}$ erzeugen. Man sagt auch:

$\wedge$, $\vee$ und $\overline{}$ bilden ein vollständiges System (Verknüpfungsbasis).

Wir ersetzen im folgenden die **Booleschen** Operatoren $\wedge$, $\vee$ und $\overline{}$ durch äquivalente **arithmetische** +, – (Addition und Subtraktion) und • (Multiplikation). Es seien **a**, **b** $\in$ {0, 1}. Dann gilt offensichtlich:

Verknüpfung	Boolesche Operation	Arithmetischer Ausdruck
Negation	$\overline{\mathbf{a}}$	$1 - \mathbf{a}$
Konjunktion	$\mathbf{a} \wedge \mathbf{b}$	$\mathbf{a} \bullet \mathbf{b}$
Disjunktion	$\mathbf{a} \vee \mathbf{b}$	$\mathbf{a} + \mathbf{b} - \mathbf{a} \bullet \mathbf{b}$

Gesetzmäßigkeiten und Verknüpfungsregeln:

Distributivgesetz

$$\mathbf{a} \wedge (\mathbf{b} \vee \mathbf{c}) = (\mathbf{a} \wedge \mathbf{b}) \vee (\mathbf{a} \wedge \mathbf{c})$$
$$\mathbf{a} \vee (\mathbf{b} \wedge \mathbf{c}) = (\mathbf{a} \vee \mathbf{b}) \wedge (\mathbf{a} \vee \mathbf{c})$$

Absorption / Redundanz

$\mathbf{a} \wedge (\mathbf{a} \vee \mathbf{b}) = \mathbf{a}$ sowie $\mathbf{a} \vee (\mathbf{a} \wedge \mathbf{b}) = \mathbf{a}$

Idempotenzgesetze

$1 \vee \mathbf{a} = 1$ $0 \vee \mathbf{a} = \mathbf{a}$ $0 \wedge \mathbf{a} = 0$ $1 \wedge \mathbf{a} = \mathbf{a}$

Vereinfachungen

$\mathbf{a} \cdot \mathbf{a} = \mathbf{a}^2 = a$ $\mathbf{a} \cdot \mathbf{a} \ldots \cdot \mathbf{a} = \mathbf{a}^n = a$

$\mathbf{a} \cdot \overline{\mathbf{a}} = 0$

Anwenden auf Fehlerbaummethode:

Berechnung der System-Verfügbarkeit V_S oder der System-Unverfügbarkeit U_S aus der Redundanzstruktur-Funktion $X_S = f(X_1, X_2, ..., X_n)$ – abgeleitet aus dem Fehlerbaum.

Vorgehensweise

1. Entwickle einen Fehlerbaum mit den Indikatorvariablen $X_1, X_2, ..., X_n$.
2. Ermittle die Redundanzstruktur-Funktion $X_S = f(X_1, X_2, ..., X_n)$ aus dem Fehlerbaum (logische Funktion):

   gfs. Vereinfachung unter Beachtung der Verknüpfungsregeln, z. B.

$$X_i \wedge \overline{X}_i = 0 \qquad X_i \wedge X_i = X_i$$

Fortsetzung:

3. Ersetze Boolesche Operationen durch äquivalente arithmetische Ausdrücke gemäß obiger Tabelle:

   gfs. Vereinfachung unter Beachtung von z. B.

   $$X_i \cdot X_i = X_i$$

4. Wenn alle Potenzen $X_i^n = X_i$ für die Variablen X_i verschwunden, ersetze X_i durch U_i und $1 - X_j$ durch $V_j = 1 - U_j$ $(i, j = 1, 2, ..., n)$.

Beispiel

Siehe Fehlerbaum Absch. 3.3, S. 7.

geg.: $X_S = f(X_1, X_2, ..., X_n) = \big((X_1 \wedge X_2) \vee X_3\big) \wedge X_4$

ges.: $V_S = ?$

Lösung

1. $(X_1 \wedge X_2) = X_1 \cdot X_2$
2. $(X_1 \wedge X_2) \vee X_3 = X_1 \cdot X_2 + X_3 - X_1 \cdot X_2 \cdot X_3$
3. $\big((X_1 \wedge X_2) \vee X_3\big) \wedge X_4 = (X_1 \cdot X_2 + X_3 - X_1 \cdot X_2 \cdot X_3) \cdot X_4$

$\rightarrow X_S = X_1 \cdot X_2 (1 - X_3) \cdot X_4 + X_3 \cdot X_4$

Nun ersetzen wir:

$X_i \rightarrow 1 - V_i$ und $1 - X_j \rightarrow V_j$

$\rightarrow \quad 1 - V_S = (1 - V_1) \cdot (1 - V_2) \cdot V_3 \cdot (1 - V_4) + (1 - V_3) \cdot (1 - V_4)$

und somit

$$V_S = (V_1 + V_2 - V_1 \cdot V_2) \cdot V_3 \cdot (1 - V_4) + V_4$$

Entwicklungssatz von Shannon:

Jede Boolesche Funktion $\mathbf{f} \ : \ \mathbf{B}^n \rightarrow \mathbf{B}^1 = \{0, 1\}$ kann für jede ihrer Variablen X_i durch

$$
\begin{aligned}
f(X_1, \ldots, X_i, \ldots, X_n) \ = \ & X_i \cdot f(X_1, \ldots, X_{i-1}, \mathbf{1}, X_{i+1}, \ldots, X_n) \\
\vee \ & \overline{X}_i \cdot f(X_1, \ldots, X_{i-1}, \mathbf{0}, X_{i+1}, \ldots, X_n)
\end{aligned}
$$

dargestellt werden. Hierin ist $X_i \cdot f$ die Abkürzung für $X_i \wedge f$.

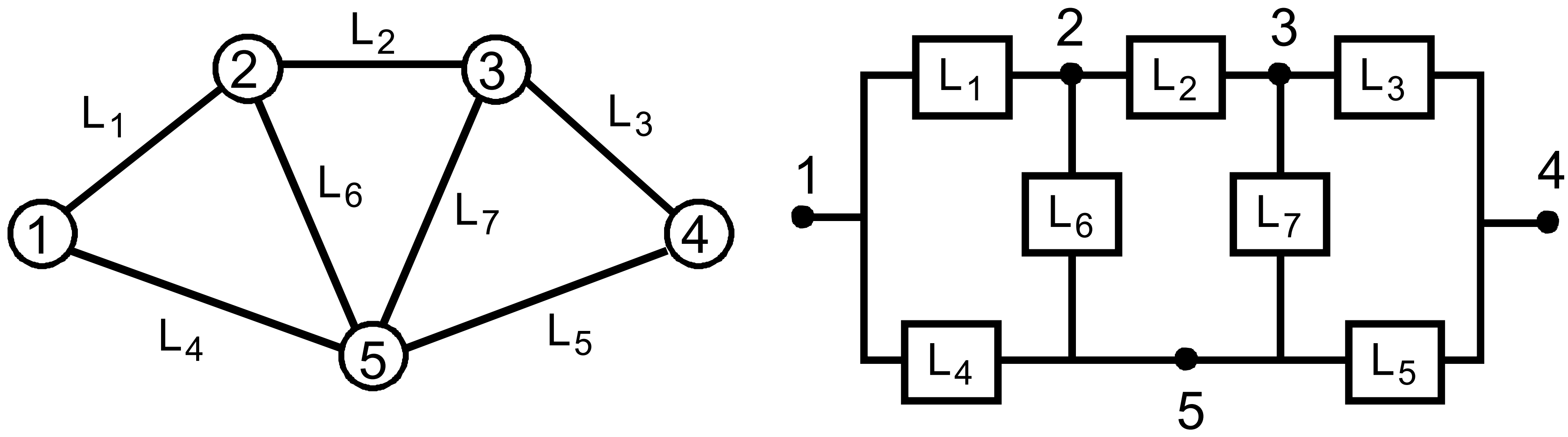
Kurzform: ($\wedge$ = UND-Verknüpfung!)

$$
f = X_i \cdot f|_{X_i = 1} \vee \overline{X}_i \cdot f|_{X_i = 0}
$$

Bei **rekursiver** Anwendung des **Shannonschen Entwicklungssatzes** erhält man eine binär-baumartige Klammerstruktur, aus der man leicht die sogenannte **disjunktive Normalform** (DNF) bilden kann.

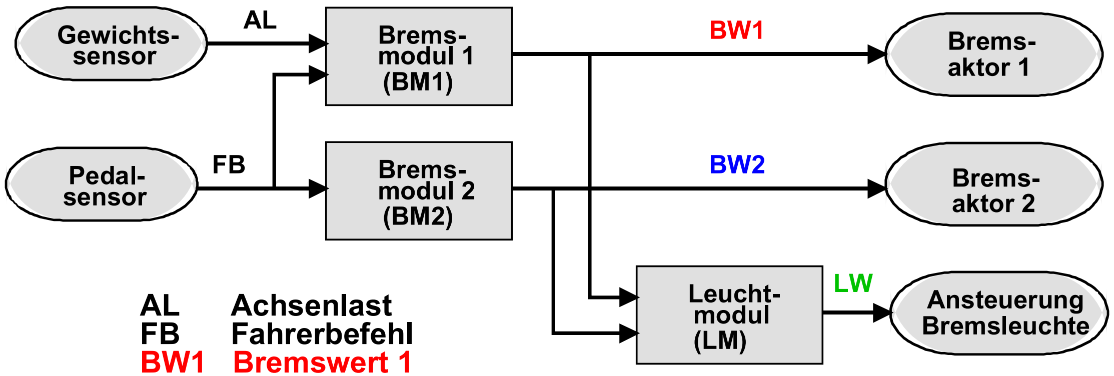
Anwendung des Entwicklungssatzes:

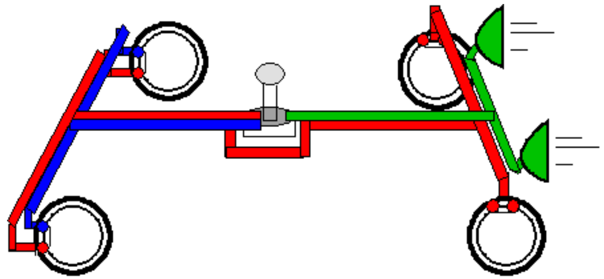
Überführung einer komplexen Netzwerkstruktur in einfachere Serien- bzw. Parallelredundanzstrukturen.



Steuerungssystem einer Zweikreisbremsanlage:

Sensoren **Controller** **Aktoren**

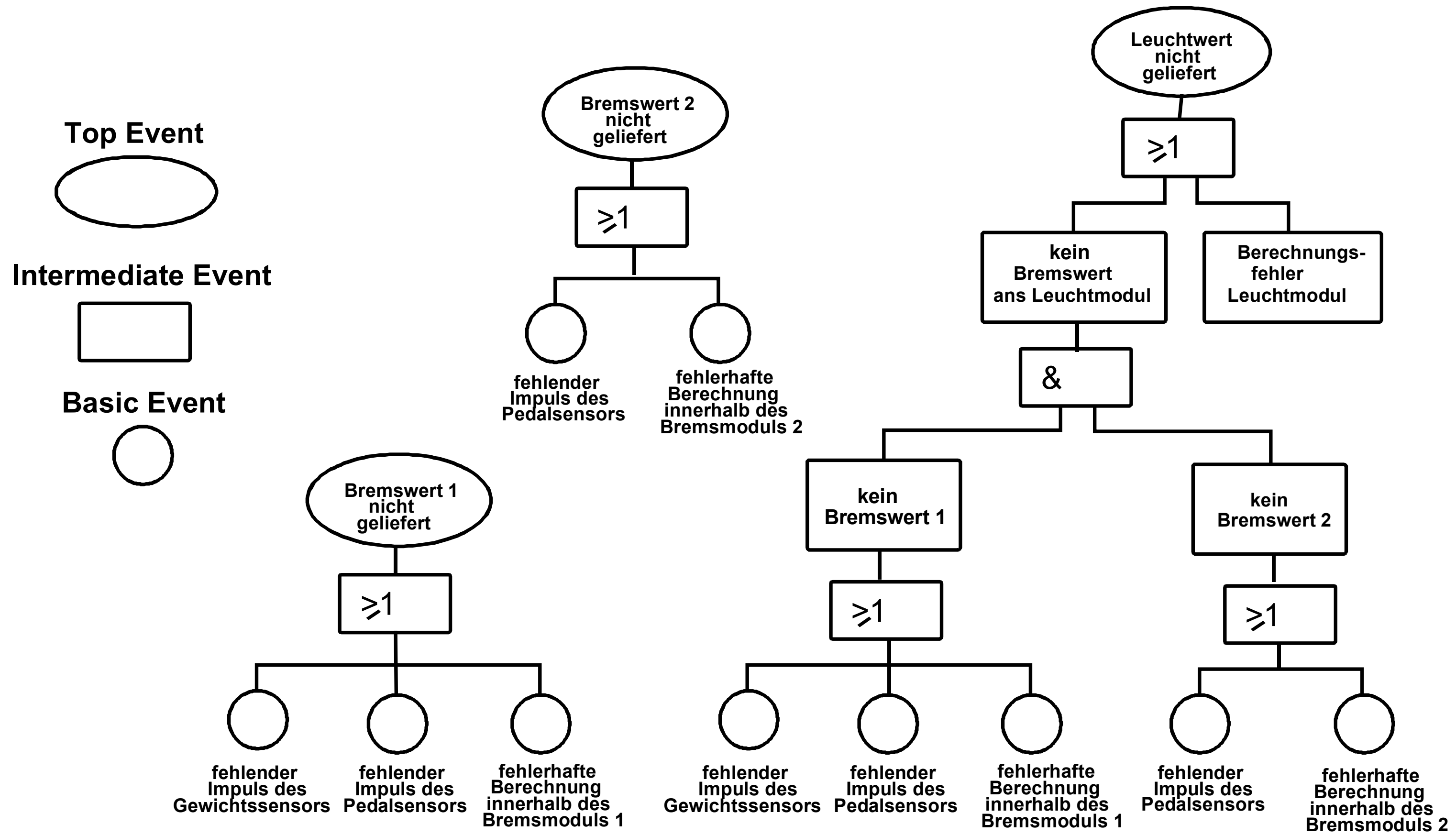




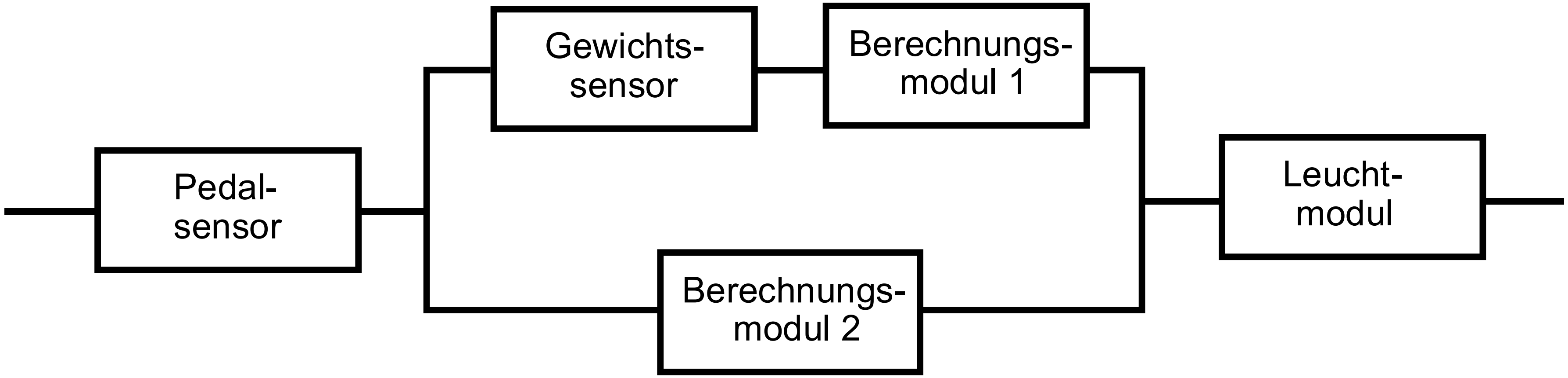
AL	Achsenlast
FB	Fahrerbefehl
BW1	Bremswert 1
BW2	Bremswert 2
LW	Leuchtwert

- Fahrer tritt das Bremspedal, aber das Fahrzeug wird nicht oder zu spät gebremst.
- Fahrzeug wird korrekt gebremst, aber die Bremsleuchten leuchten nicht auf.
- Fahrzeug wird gebremst, obwohl das Bremspedal nicht getreten wurde.

Fehlerbäume:



Zuverlässigkeitsblockdiagramm für fehlenden Leuchtwert:



Unverfügbarkeit $\Rightarrow$ **max. $\approx 1.8 \cdot 10^{-4}$**