



Safety und Fehlertoleranz

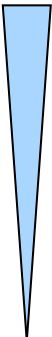
Backup
RAID
Fehlertoleranz

Backup (Datensicherung)

- Bedrohungen (Beispiele)
 - Hardwaredefekte
 - Diebstahl
 - höhere Gewalt
 - versehentliches Löschen
 - Viren u. andere Schadprogramme

- Auswahl der Daten

Nicht wiederbeschaffbare Daten genießen höchste Backup-Priorität:

- 
- selbst erstellte Dateien ++
 - Konfigurationsdateien +
 - Internet-Downloads -/+
 - Programme - (Installations-CD)
 - Betriebssystem -- (Setup-CD)

Backup und Archivierung

- Backup:
 - **Sicherungskopie von Daten als Schutz vor Verlust**
 - einzelne Dateien und Verzeichnisse
 - ganzes Abbild (Image)eines Speichermediums (typ. Festplattenpartition), z.B. sichern inkl. Betriebssystem
 - zur Erfüllung gesetzlicher Auflagen (z.B. KontraG?)
- Archivierung:
 - **Aufbewahrung von Daten in einem bestimmten Zustand**
 - zur Erfüllung gesetzlicher Auflagen
 - zur eigenen Dokumentation
 - zur Versionenkontrolle

Backup-Strategien

- Voll-Backup
 - sichert **alle Daten**
- Inkrementelles Backup
 - sichert alle **seit dem letzten Backup** hinzugekommenen und veränderten Daten
 - mehrfach hintereinander durchführbar
 - alle Zwischenstände zwischen Vollbackups sind rekonstruierbar
 - Restore erfolgt in der Reihenfolge der Sicherungen
 - alle Sicherungen seit dem letzten Voll-Backup erforderlich
- Differenzielles Backup
 - sichert alle **seit dem letzten Voll-Backup** hinzugekommenen und veränderten Daten
 - Restore erfordert nur Voll-Backup und letztes differenzielles Backup

In welchem Format sollte gesichert werden?

- Als Rohdaten (raw)
 - überall lesbar
 - je nach Rohdaten geringe Speichereffizienz
 - In verbreitetem Archivformat (z.B. zip)
 - fast überall lesbar (auch über Plattformen hinweg)
 - bei Komprimierung hohe Speichereffizienz
 - Im proprietärem Format der Backup-Software
 - Abhängigkeit von Betriebssystem und Backup-Software berücksichtigen
-
- Welche Daten müssen gesichert werden?
 - **Archiv-Bit** vom Dateisystem (z.B. NTFS, FAT) verwaltet
 - vom Betriebssystem nach Anlegen oder Verändern einer Datei gesetzt und von Backup-Software zurückgesetzt
 - nur bei inkrementellem Backup nützlich
 - Backup-Software führt Liste der gesicherten Dateien

Auf welchen Medien sollte gesichert werden?

- Externe Standardmedien (Streamer, CD/DVD-R/W)
 - meist überall lesbar
 - empfehlenswert für **Voll-Backup**
 - Haltbarkeitsdauer (DVD 40...200 Jahre) beachten
 - Treiber nicht nur auf Backup sichern
- Festplatten- und Netzlaufwerke
 - sehr effizient für **inkrementelle und differenzielle Sicherungen**
 - Beachte: RAID (Redundant Array of Inexpensive Disks)
 - ersetzt nicht das Backup
 - schützt nicht vor versehentlichem oder böartigem Löschen
- Spezielle Backup-Systeme

Spezielle Backup-Systeme



Bilder: <http://www.ualberta.ca/CNS/vrtour/tsm/>

Vorsichtsmaßnahmen beim Sichern

- **Schutzziel Integrität:** Sicherungskopie sollte nach dem Schreiben mit Originaldaten verglichen werden
- **Schutzziel Verfügbarkeit:** Mehrere Mediensätze verwenden
 - Schutz vor Fehlern während des Sicherns
 - letzten Mediensatz aufbewahren
 - vorletzten (oder besser vorvorletzten) Mediensatz überschreiben
 - Katastrophenschutz:
 - Originaldaten und Backup an verschiedenen Orten sichern
 - Schutz vor Feuer, Wasser, ...
 - Datasafe (Lampertz, Sistec)
- **Schutzziel Vertraulichkeit:** Wer Zugriff auf Backup hat, hat Zugriff auf Daten.
 - sichere Aufbewahrung (Datasafe)
 - Verschlüsselung (Beachte: Schlüsselbackup ggf. notwendig)

Wechselprinzip für inkrementelle Sicherungen

- 1 mal pro Zeiteinheit (z.B. Woche) Voll-Backup (z.B. Montag)
 - auf Medium 1
- n mal inkrementelles Backup (z.B. Di, Mi, Do, Fr)
 - auf Medien 2,3,...,n+1
- Anzahl der benötigten Medien:
 - **1+n+1 Medien**
- nächstes Voll-Backup auf Medium n+2

Mo	Di	Mi	Do	Fr	Mo	Di	Mi	Do	Fr	Mo	Di	Mi
v1	i2	i3	i4	i5	v6	i2	i3	i4	i5	v1	i2	i3

- **Medium 1 und 6:** etwa gleiche (hohe) Kapazität
- **Medien 2-5:** geringere Kapazität als 1 und 6 nötig

Wechselprinzip f. differenzielle Sicherungen

- Anzahl der benötigten Medien:
 - 2+2 Medien
- 1 mal pro Zeiteinheit (z.B. Woche) Voll-Backup (z.B. Montag)
 - auf Medium 1
- differenzielle Backups (z.B. Di, Mi, Do, Fr)
 - abwechselnd auf Medien 2 und 3
- nächstes Voll-Backup auf Medium 4

- falls alle Medien ausreichend groß:
 - 3 Medien genügen
 - vorletztes differenzielles Backup für Voll-Backup

Mo Do Mi Do Fr Mo Di Mi Do Fr Mo Di Mi Do Fr
v1 d2 d3 d2 d3 v2 d3 d1 d3 d1 v3 d1 d2 ...

!!!....bloß nicht durcheinander kommen....!!! :-)



RAID

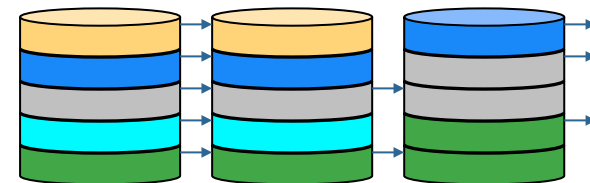
RAID: Einführung

- Akronym für
 - Redundant Array of Inexpensive Disks (1982)
 - Redundant Array of Independent Disks (Neudefinition 1992)
- Steigerung von
 - Leistung (I/O-Durchsatz, Speicherkapazität)
 - Zuverlässigkeit
- 6 klassische RAID-Level

keine Redundanz	RAID-0
Datenreplikation	RAID-1
Fehlerkorrigierende Codes	RAID-2
Paritätsbits	RAID-3, RAID-4, RAID-5

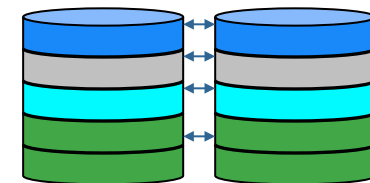
RAID: Grundprinzipien 1/3

- Problem Leistung
 - CPU-Leistung und **Speicherbedarf** wachsen exponentiell
 - **I/O-Performance** wächst dagegen deutlich langsamer
- Ausweg
 - Mehrere Disks und I/O-Kanäle gleichzeitig verwenden
- Verteilung der Daten auf mehrere Disks (Striping, Interleaving)
 - Bit-Interleaving (bitweise Verteilung über mehrere Disks)
 - Sector-Interleaving (Sektor-weise Verteilung)
 - Paralleles Lesen und Schreiben möglich
 - Bei Verlust einer Disk --> Datenverlust



RAID: Grundprinzipien 2/3

- Problem Zuverlässigkeit
 - $MTBF(\text{disk array}) = MTBF(\text{disk}) / \text{Anzahl disks}$
 - Beispiel: (MTBF: Mean Time Between Failure)
 - **MTBF** einer **80GB-Festplatte** sei **>50 000 Stunden (5,7 Jahre)**
 - **MTBF** eines **Disk-Arrays mit 2 Terabyte (25Disks x 80GB)** ist dann **nur 83 Tage**
- Ausweg
 - Einsatz geeigneter Fehlertoleranzmaßnahmen
- Spiegelung (mirroring, shadowing)
 - Doppelung der Daten auf einer zweiten Disk
 - Teuer, aber sehr zuverlässig
- Kompromiss zwischen Zuverlässigkeit und Kosten, je nach RAID-Level auch verwendet:
 - Paritätsbits
 - Fehlerkorrigierende Codes

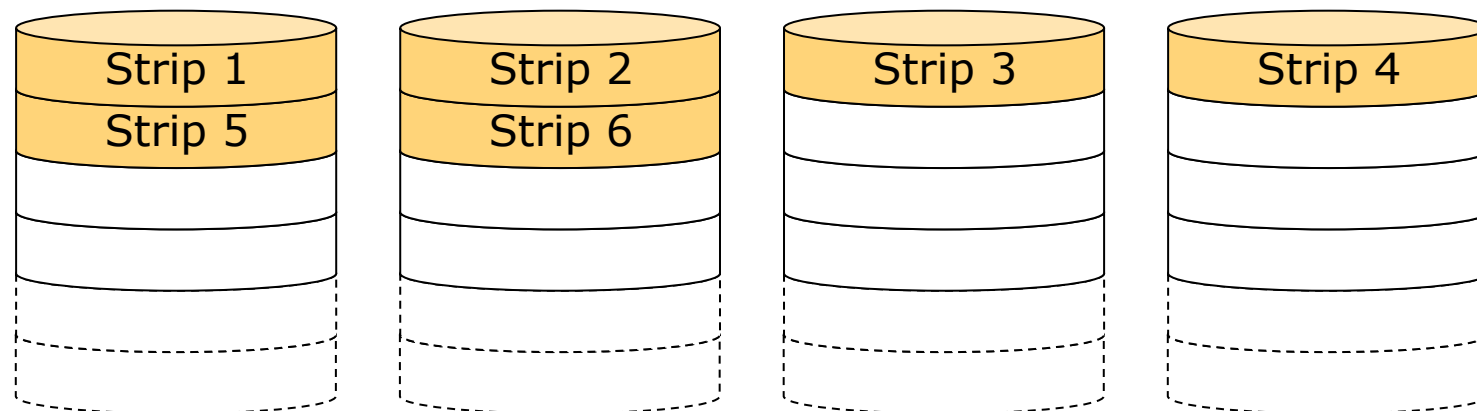


RAID: Grundprinzipien 3/3

- Problem Kosten
 - Einsatz standardisierter, kostengünstiger Komponenten
 - Festplattenlaufwerke (Massenmarkt)
 - Standard-Datenbusse (z.B. SCSI, Firewire, Fibre Channel)
- Teure Alternative:
 - Spezial-Hardware, z.B. Festplattenfarm im Großrechnerbereich
- Einsatzziel von RAID-Technik
 - kostengünstige Erhöhung der Datentransferrate und Ausfallsicherheit von Festplatten

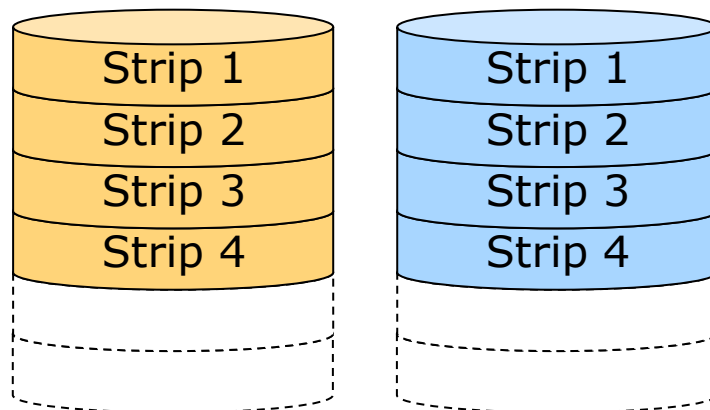
RAID-0

- Merkmale
 - Aufteilung der Daten in Blöcke, paralleles Schreiben auf vorhandene Festplatten (disk striping)
 - keine Redundanz, geringe MTBF
 - **Sehr hohe Datentransferrate (für kleine Strips)**
 - **Sehr geringe I/O-Request-Verarbeitungszeit (für große Strips)**
- Verwendungszweck: Anwendungen mit
 - hohen I/O-Performance-Anforderungen
 - geringen Anforderungen an die Verfügbarkeit



RAID-1

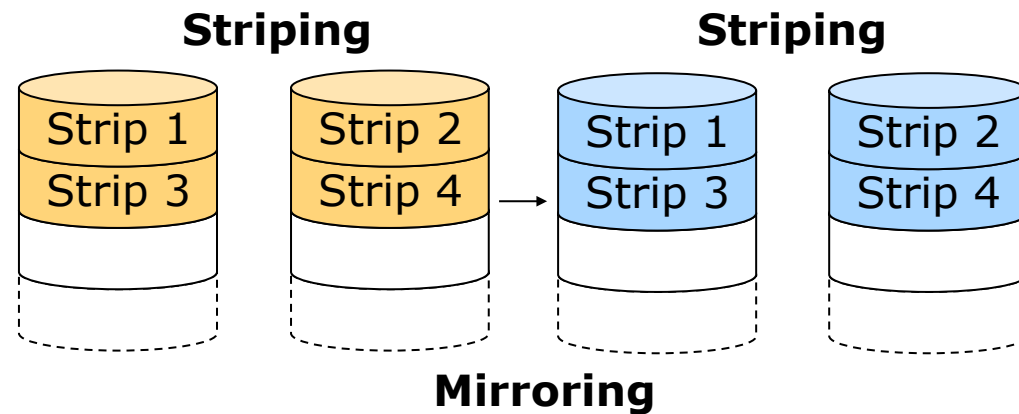
- Merkmale
 - gespiegelte Platten (mirroring, shadowing), gleiche Daten werden gleichzeitig auf unterschiedliche Platten geschrieben
 - bei Datenverlust steht Duplikat der Daten zur Verfügung
 - hohe Kosten
 - **Datentransferrate, I/O-Request-Verarbeitungszeit:**
 - **Lesen:** gut, Platte mit geringerer Zugriffszeit (seek distance)
 - **Schreiben:** mittel, beide Platten müssen schreiben
- Verwendungszweck: Anwendungen mit
 - sehr hohen Anforderungen an die Verfügbarkeit



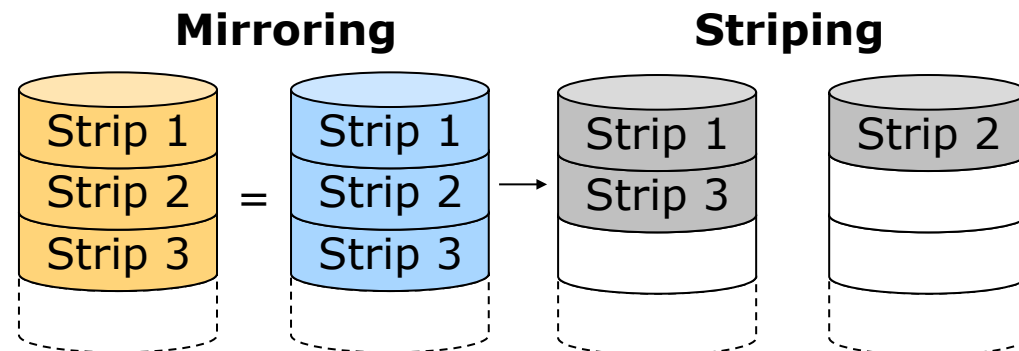
1 Logischer Schreibzugriff =
2 physische Schreibzugriffe

Kombination von RAID-0 und RAID-1

gespiegelte Verteilung
Mirrored Strips
RAID 0+1 oder RAID 01

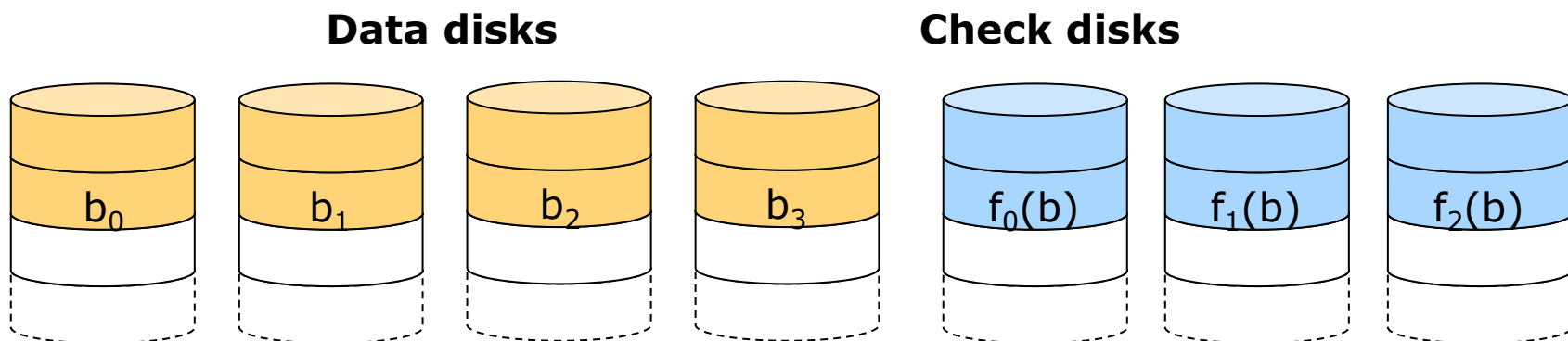


verteilte Spiegelung
Striped Mirrors
RAID 1+0 oder RAID 10



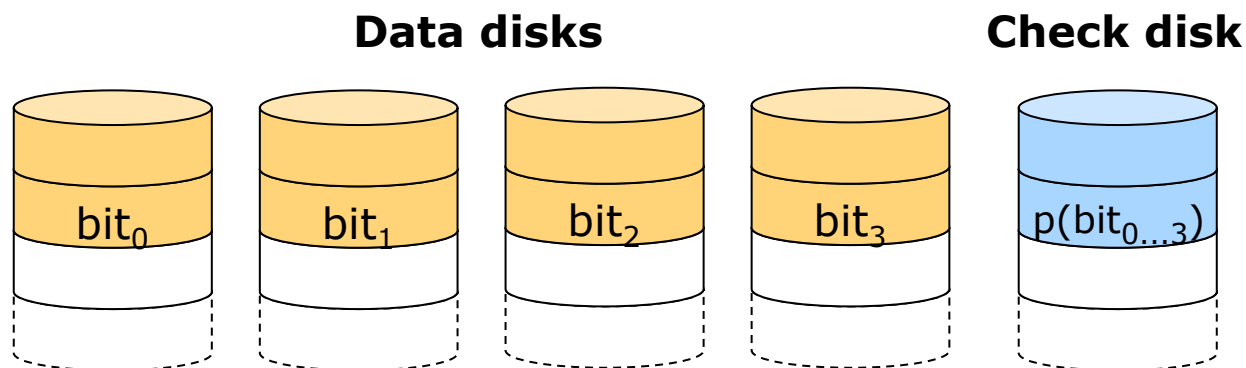
RAID-2

- Merkmale
 - Verteilung (striping)
 - fehlerkorrigierender Hamming-Code (20-40 Prozent Overhead)
 - **Datentransferrate**
 - hervorragend für große Datensätze
 - gering für kleine Datensätze, da gesamter Strip gelesen werden muss
 - **I/O-Request-Verarbeitungszeit**
 - gering: keine parallelen I/O-Requests verarbeitbar, da alle Laufwerke mit einem Request befasst sind
 - geringe praktische Bedeutung



RAID-3

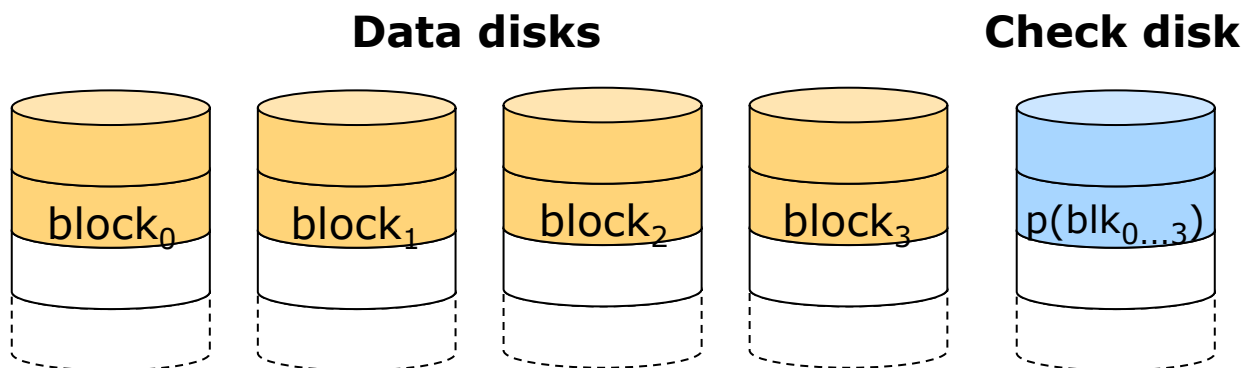
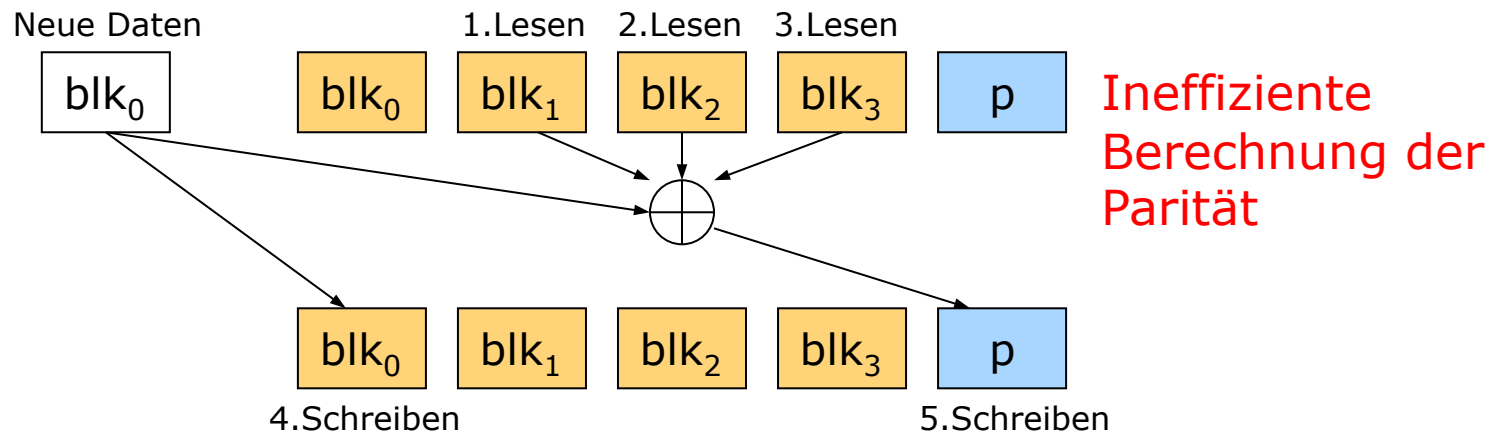
- Merkmale
 - Verteilung (striping): bit interleaving
 - Paritätsinformation auf zusätzlicher Platte
 - bei Ausfall genau einer Platte Rekonstruktion der Daten möglich
 - geringfügig zuverlässiger als RAID-2, da weniger Platten
 - **Datendurchsatz: geringfügig besser als RAID-2**
 - **I/O-Request-Verarbeitungszeit: geringfügig besser als RAID-2 wg. bitweiser Verarbeitung, aber immer noch schlecht**
- Verwendungszweck:
 - Anwendungen mit wenigen großen Dateien (z.B. Bildverarb.)
 - nicht geeignet für Transaktionssysteme und Direktzugriff



RAID-4

- Merkmale

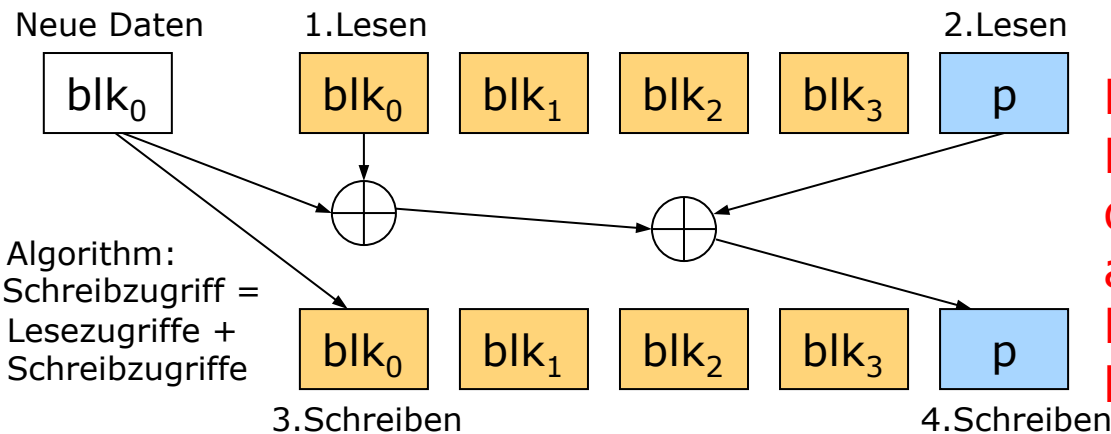
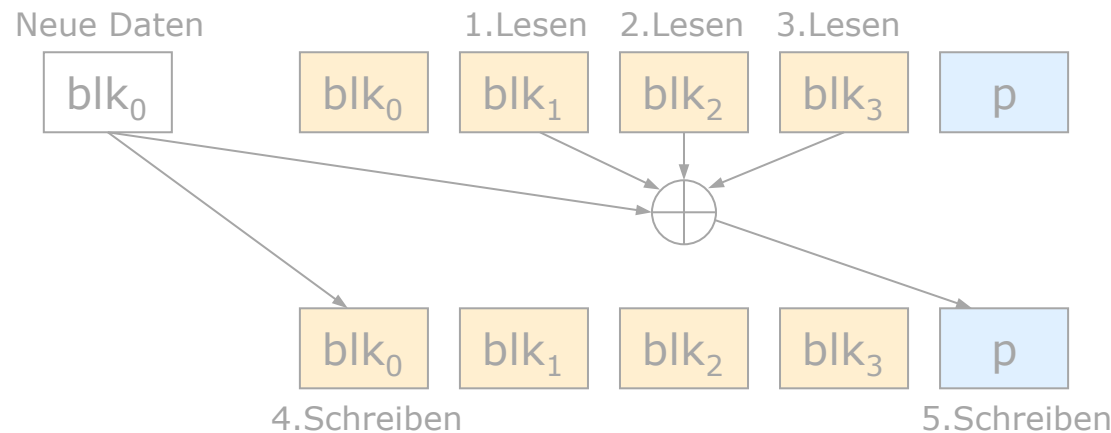
- Verteilung (striping): sector interleaving
- Paritätsinformation auf zusätzlicher Platte



RAID-4

- Merkmale

- Verteilung (striping): sector interleaving
- Paritätsinformation auf zusätzlicher Platte

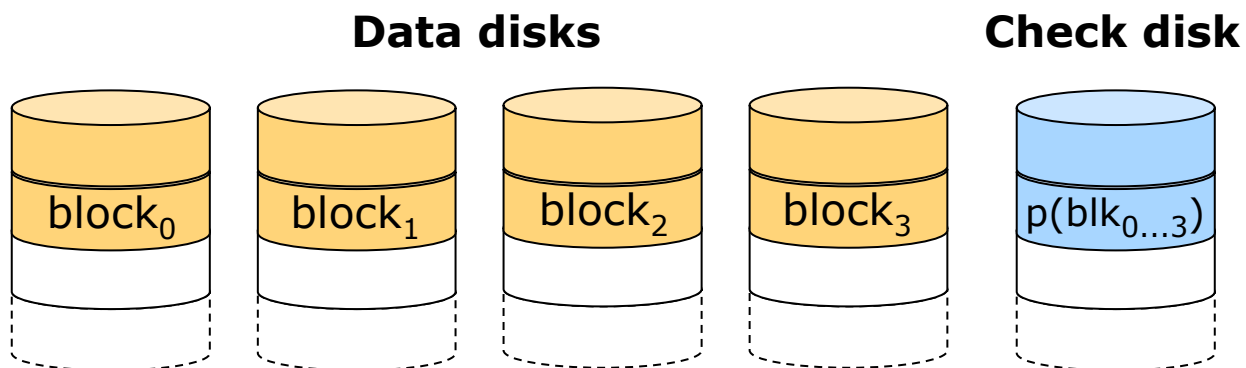


Small-Write Algorithm:
 1 Logischer Schreibzugriff =
 2 physische Lesezugriffe +
 2 physische Schreibzugriffe

Besser: Neue Parität wird aus der Differenz des alten und neuen Datenblocks berechnet

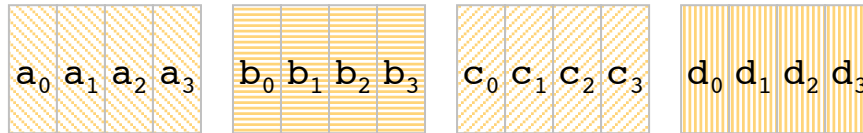
RAID-4

- Merkmale
 - Verteilung (striping): sector interleaving
 - Paritätsinformation auf zusätzlicher Platte
 - große Lese- und Schreibzugriffe parallel möglich
 - **Datendurchsatz: etwa wie RAID-3**
 - **I/O-Request-Verarbeitungszeit: sehr gut für Lesen, etwas besser als RAID-3 für Schreiben**
 - Paritätsplatte bleibt Flaschenhals
- Anwendungen wie RAID-3

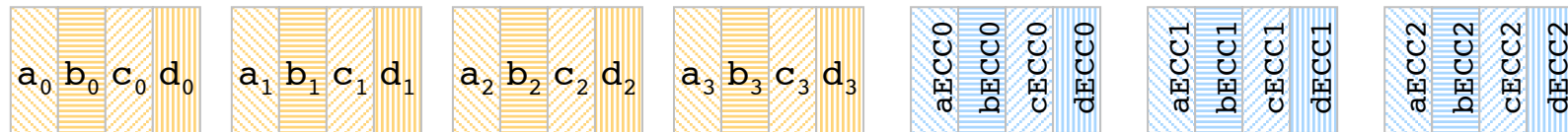


Vergleich der RAID-Levels 2, 3 und 4

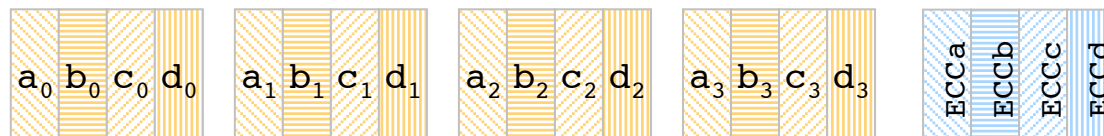
**4 Dateneinheiten
a, b, c, d sind zu
speichern**



RAID-2

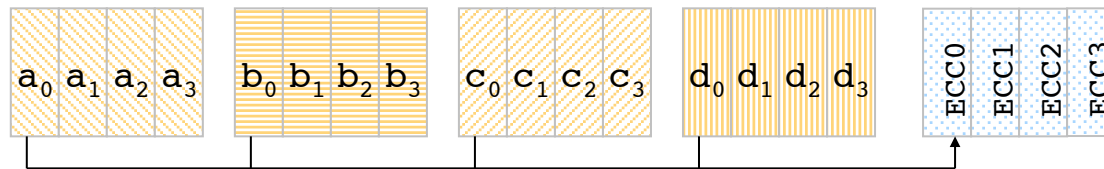


RAID-3



**Parität wird über
jeder Dateneinheit
berechnet**

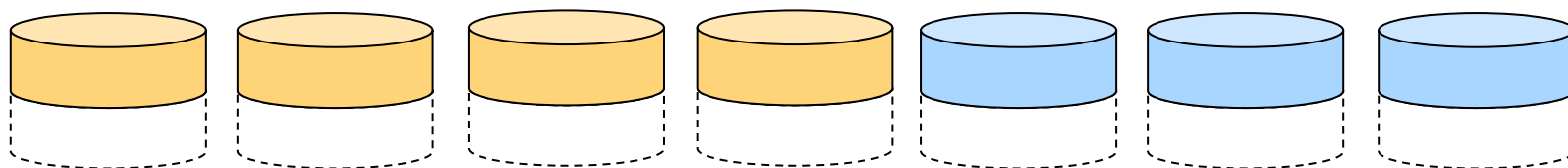
RAID-4



**Parität wird über
einem Teil jeder
Dateneinheit
berechnet**

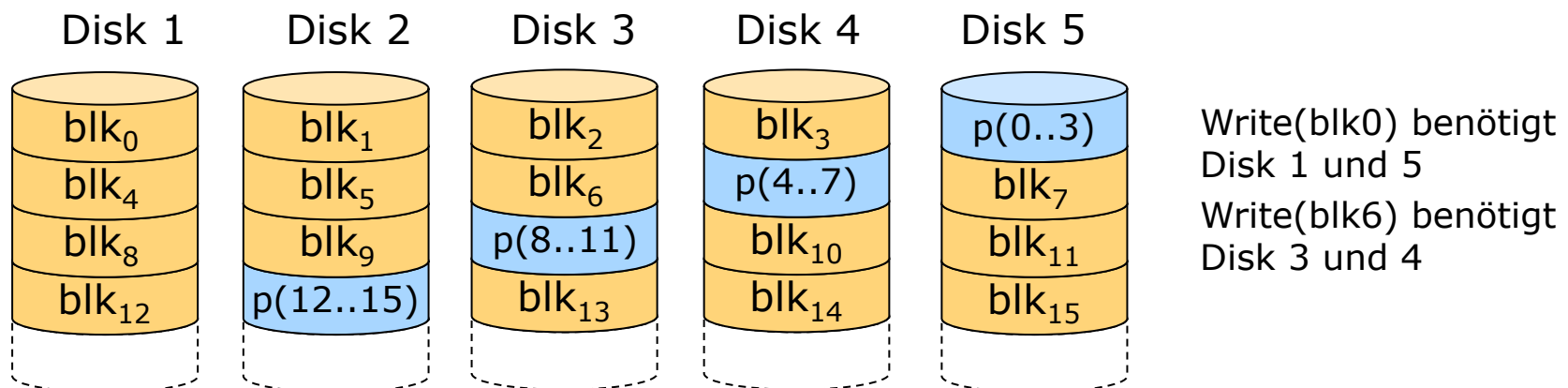
Data disks

Check disk(s)

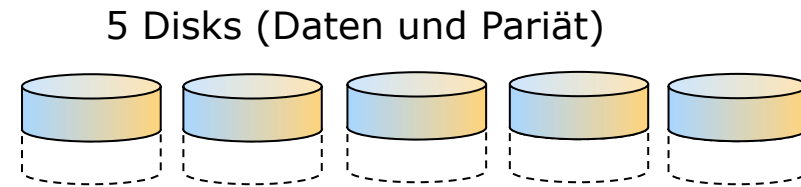
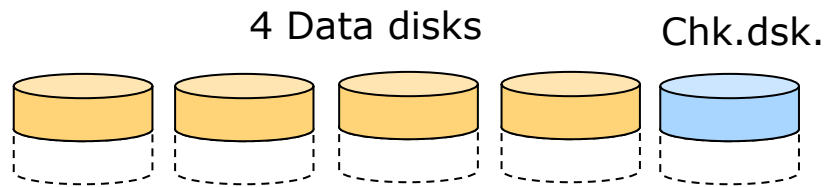


RAID-5

- Merkmale
 - Verteilung (striping) der Daten (sector interleaving) und Paritätsinformation zur Verbesserung der Performance
 - Ziel: Verteilen der Last auf Paritätsplatte, Schreibzugriffe können simultan erfolgen
 - **Datendurchsatz: gut für Lesen und Schreiben**
 - **I/O-Request-Verarbeitungszeit: sehr gut für Lesen, sehr gut für Schreiben**
- Verwendungszweck:
 - Transaktionsorientierte Anwendungen, Datenbanken



Vergleich von RAID-4 und RAID-5 (Schreiben von Daten)



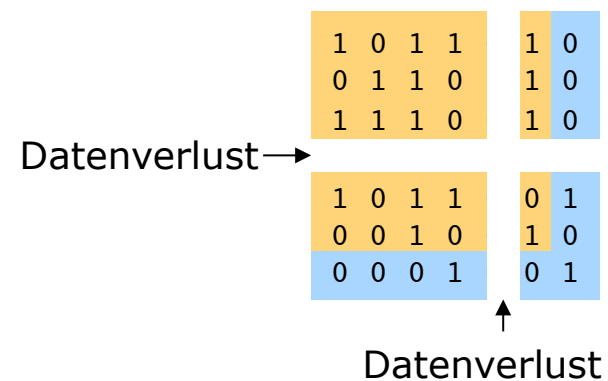
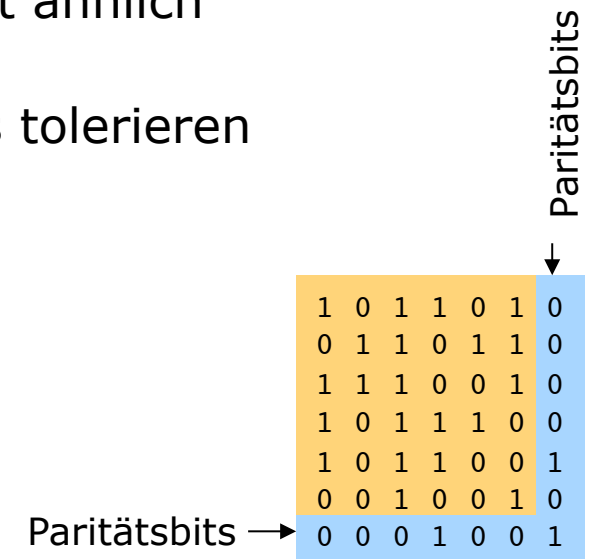
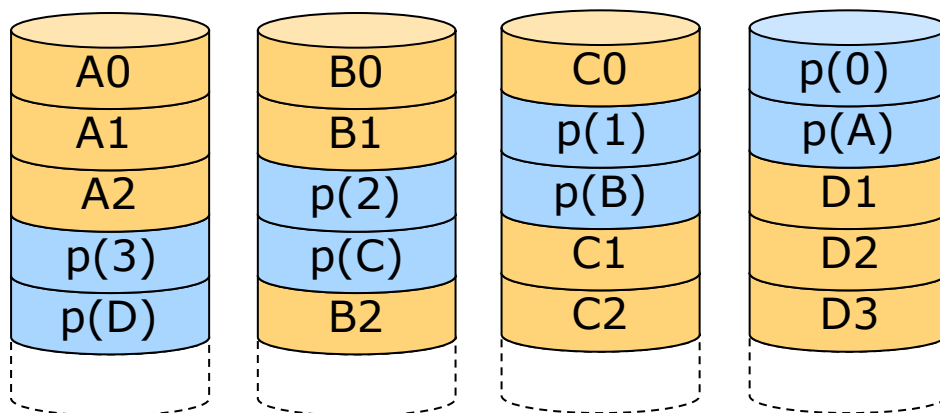
RAID-4

RAID-5

RAID-6

- Merkmale
 - Verwendung zweidimensionaler Parität ähnlich Kreuzsicherungsverfahren
 - kann zwei gleichzeitige Plattencrashes tolerieren
 - recht aufwändige Elektronik
 - Schreiben ist langsam

- Schematisch





Fehlertoleranz

Arten von Fehlern

Nicht-reparierbare Systeme

Reparierbare Systeme

Redundanztechniken

Aspekte der Bewertung eines fehlertoleranten
Systems

Anwendungsbeispiele für fehlertolerante Systeme

Fehlertoleranz durch redundante Systeme

- Ziel
 - Verbesserung der Zuverlässigkeit (Ausfallsicherheit) von Systemkomponenten

- Typische Kenngrößen
 - Mean Time To Failure (MTTF)
 - Erwartungswert für die Zeit (von der Inbetriebnahme) bis zum (ersten) Ausfall eines Systems
 - Mean Time To Repair (MTTR)
 - Erwartungswert für die Zeit zur Ersetzung des Systems und ggf. der Rekonstruktion der Daten

- ferner
 - Mean Time To Data Loss (MTTDL)
 - Erwartungswert für die Zeit bis zu einem nicht-maskierbaren Fehler (hauptsächlich verwendet in Speicherkomponenten)

Arten von Fehlern

1. Hardware-Fehler

- betreffen *physische* Teile des Systems

Software-Fehler

- betreffen *logische* Teile des Systems

2. Transiente Fehler

- vorübergehende Fehler, evtl. nicht reproduzierbar, z.B. Übertrag.fehler
- können behoben werden durch wiederholte Ausführung der fehlerhaften Operation

Permanente Fehler

- dauerhaft
- leicht erkennbar

3. Einzel-Fehler

- betreffen einzelne Komponenten
- unabhängig von der Funktion anderer Systemteile

Mehrfach-Fehler

- betreffen mehrere Komponenten des Systems gleichzeitig
- durch *Fehlerfortpflanzung* oder gemeinsame Fehlerquellen hervorgerufen

Nicht-reparierbare Systeme

- Zuverlässigkeit (reliability): $R(t)$
 - bedingte Wahrscheinlichkeit, dass ein System das Zeitintervall $[0, t]$ überlebt, wenn es in $t=0$ funktionstüchtig war

- Es gilt

$$\lim_{t \rightarrow \infty} R(t) = 0$$

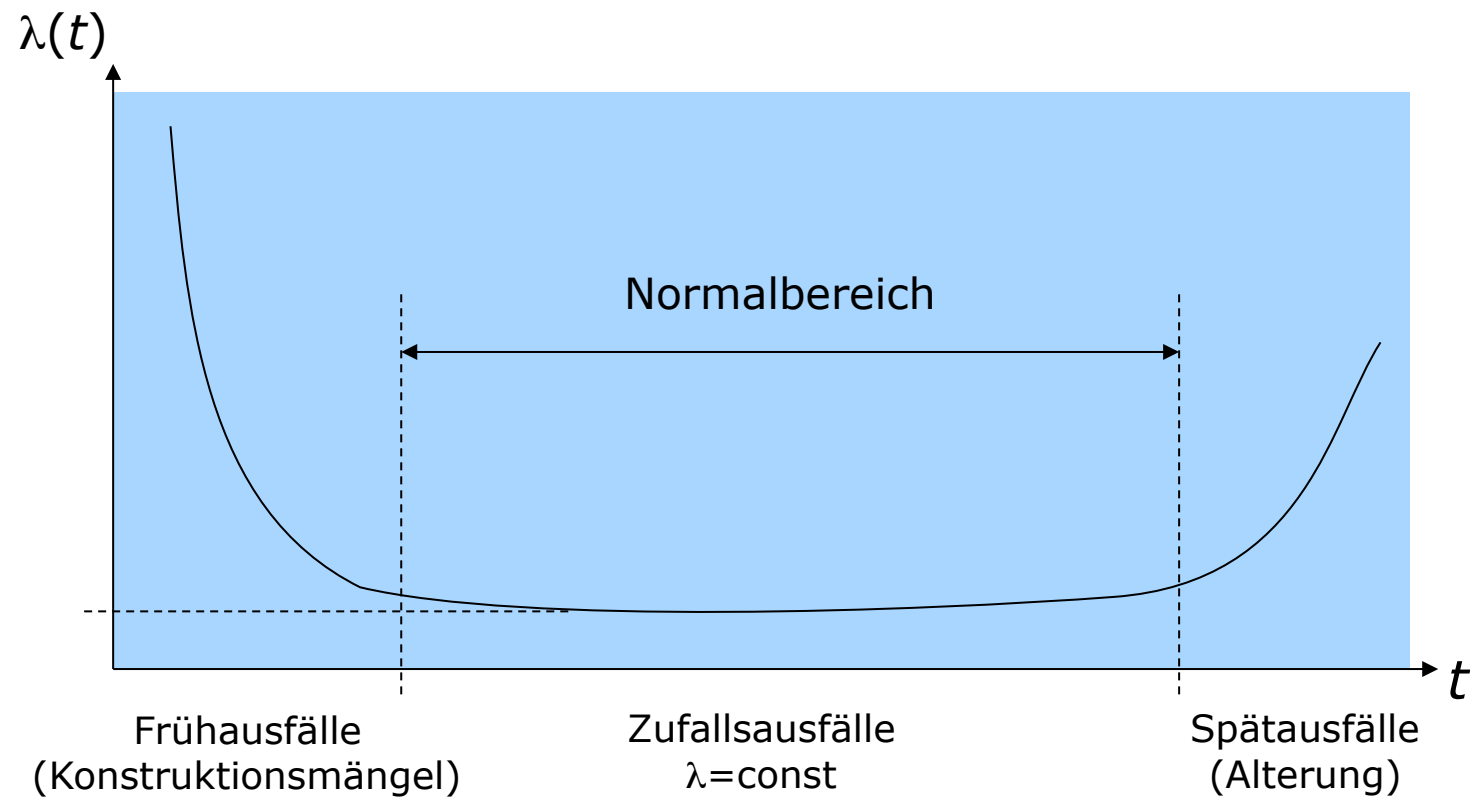
- Ausfallrate: $\lambda(t)$
 - bedingte Wahrscheinlichkeit, dass das System im differentiellen Zeitintervall $[t+dt]$ ausfällt

- Typischerweise gilt im "Normalbereich" der Nutzung eines Systems (z.B. Halbleiter-Bausteine)

$$\lambda(t) = \text{const}$$

"Badewannenkurve"

- gilt für Halbleiter,
- nicht jedoch für bewegliche Teile (z.B. Lüfter, Festplatten etc.)



Nicht-reparierbare Systeme

- Mit $\lambda = \lambda(t) = \text{const}$ gilt

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

- Mittlere Zeit bis zu einem Fehler (MTTF)

$$MTTF = \int_{t=0}^{\infty} R(t) dt = \frac{1}{\lambda}$$

Reparierbare Systeme

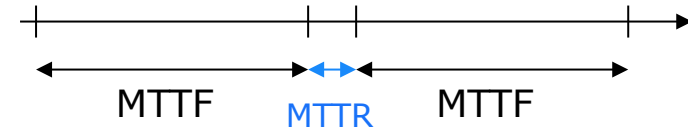
- Verfügbarkeit (availability): $A(t)$
 - Wahrscheinlichkeit, dass ein System zu einem vorgegebenen Zeitpunkt t bzw. in einem Zeitraum $[0,t]$ in einem funktionsfähigen Zustand angetroffen wird
- Für Nicht-reparierbare Systeme gilt:
 $A(t) = R(t)$
- Für reparierbare Systeme Ermittlung der stationären Verfügbarkeit

$$A = \lim_{t \rightarrow \infty} A(t)$$

Reparierbare Systeme

- Stationäre Verfügbarkeit

$$A = \frac{\mu}{\lambda + \mu} = \frac{MTTF}{MTTF + MTTR}$$



- Mit

$\lambda = \lambda(t) = \text{const}$ (Ausfallrate)

$$\longrightarrow \lambda = \frac{1}{MTTF}$$

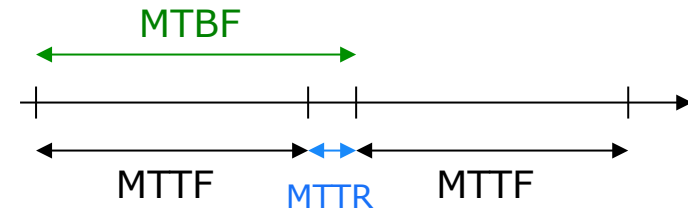
Mittlere Zeit bis zum Ausfall

$\mu = \mu(t) = \text{const}$ (Reparaturrate)

$$\longrightarrow \mu = \frac{1}{MTTR}$$

Mittlere Reparaturzeit

Reparierbare Systeme



- Bei reparierbaren Systemen findet man auch häufig die Kenngröße
 - Mean Time Between Failure (MTBF)
 - Erwartungswert für die Zeit zwischen zwei Ausfällen
 - Achtung! (z.B. Lexikon Informatik und Kommunikationstechnik, VDI Verlag, 1990, S. 419)
 - Manchmal wird definiert: $MTBF = MTTF + MTTR$
 - Manchmal auch: $MTBF \equiv MTTF$ (umgangssprachlich)
 - Beispiel Festplatten: Wenn Platte defekt, wird sie üblicherweise ausgetauscht, trotzdem wird MTBF angegeben, gemeint ist aber MTTF

Verlässlichkeit von Datenbanken und Transaktionssystemen

- Fehlerrate

$$\frac{\text{nicht erkannte fehlerhaft durchgeführte Transaktionen}}{\text{Gesamtzahl durchgeführter Transaktionen}}$$

- irrelevant:

- Transaktionen, die aufgrund eines Fehlers abgebrochen wurden

- Zusammenhang zur Verfügbarkeit

- Maßnahmen zur Reduzierung der Fehlerrate können zu Verschlechterung der Verfügbarkeit führen

Redundanztechniken

- Zeitredundanz
 - *Berechnungen werden mehrfach durchgeführt*
 - + transiente Hardware-Fehler erkennbar
 - keine Erkennbarkeit von Konstruktionsmängeln und permanenten Hardwarefehlern
- Informationsredundanz
 - *Daten werden mehrfach gespeichert oder übertragen oder Prüfinformation gebildet*
 - + transiente Fehler werden toleriert

Redundanztechniken

- Funktionelle Redundanz

→ *Hinzufügen speziell entworfener Komponenten*

Beispiele:

- Selbsttest-Komponente
- N-Version-Programming:

N verschiedene Versionen eines Programms lösen Aufgabe, Mehrheitslogik vergleicht Ergebnisse

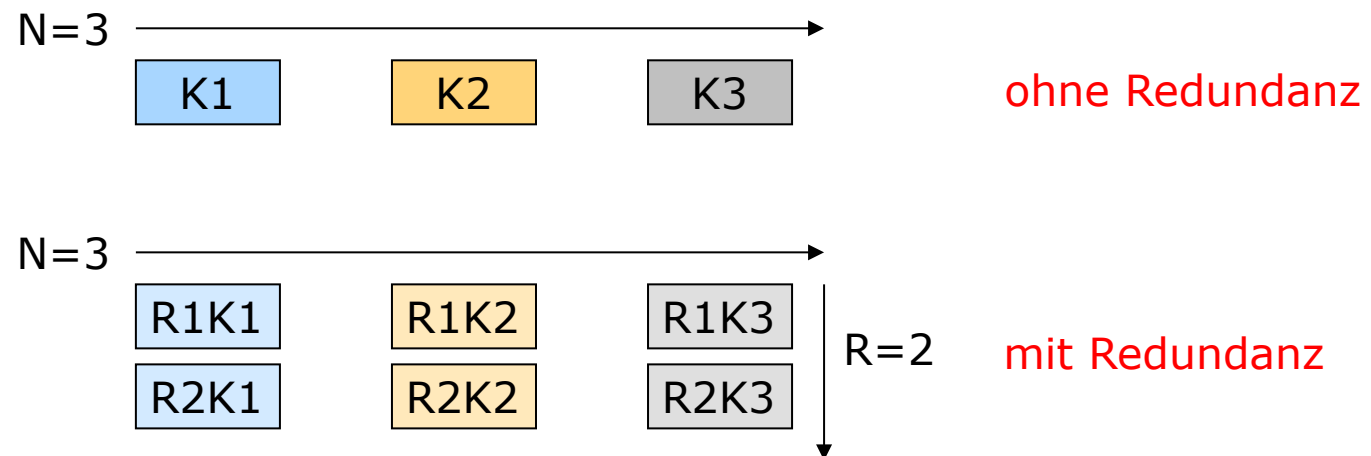
+ Tolerierung von Konstruktionsmängeln

→ *Verwandt: Spezielle Überwachungsdienste*

- externe Abfrage von Systemzuständen
- Plausibilitätsprüfungen

Redundanztechniken

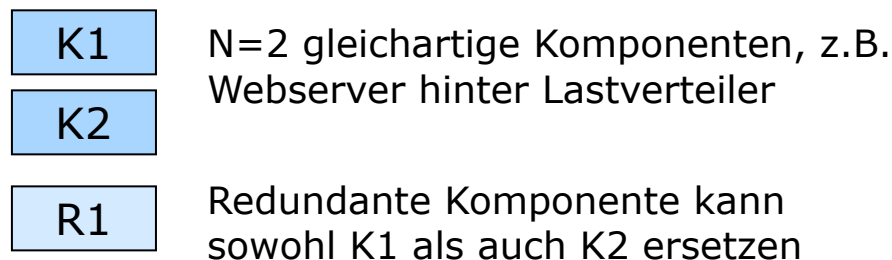
- Strukturelle Redundanz
 - *System oder Teile davon werden mehrfach ausgelegt*
 - + Tolerierung von permanenten Hardwarefehlern
 - *Unterscheidungen*
 - **RN-Redundanz:** Jede der N Komponenten wird **ver-R-facht**.
 - R-1 Komponenten stehen jeder der N Komponenten *exklusiv* zur Verfügung



- Meist 2N-Redundanz: System wird gedoppelt

Redundanztechniken

- Strukturelle Redundanz
 - *System oder Teile davon werden mehrfach ausgelegt*
 - + Tolerierung von permanenten Hardwarefehlern
 - *Unterscheidungen*
 - **R+N-Redundanz:** Dem System
 - bestehend aus **N gleichartigen Komponenten**
 - werden **R redundante Komponenten hinzugefügt.**
 - Jede der R Komponenten kann eine *beliebige* der N Komponenten ersetzen.
 - Bsp: 1+2-Redundanz



- Mit R=1 auch: "1:N-Redundanz"
 - » 1:1-Redundanz entspricht Doppelung

Redundanztechniken

- Statische und dynamische Redundanz

↓
Alle Komponenten sind ständig in Betrieb.

In Kombination mit funktioneller Redundanz: Triple-Modular-Redundancy (TMR) oder allgemein N-Modular-Redundancy (NMR): Hardware-Komponenten werden 3- bzw. N-fach ausgeführt, Mehrheitslogik ermittelt Ergebnis

↓
Redundante Komponente wird erst bei Ausfall in Betrieb genommen (Standby-Verfahren).



- erzeugt meist niedrigere Verfügbarkeit als statische R.
- + redundante Komponenten können im fehlerfreien Betrieb für andere Aufgaben verwendet werden
- + höhere MTTF, da redundante Komponenten sich nicht abnutzen

Aspekte der Bewertung eines fehlertoleranten Systems

- Überdeckungsgrad (coverage factor)

$$\frac{\text{Anzahl der durch FT-Maßnahmen tolerierbaren Fehler}}{\text{Anzahl der überhaupt spezifizierten Fehler}}$$

- Schutz vor Mehrfachfehlern
 - Ausfall der redundanten Komponente (z.B. weil sie gleichen Fehler ebenfalls enthält)
 - Schutz vor gegenseitiger Fehlerfortpflanzung (**Diversität**)
 - z.B. geograph. getrennte Aufstellung, Hard- und Software verschiedener Hersteller
- Gesamtverfügbarkeit richtet sich nach schwächster Stelle
 - Produkt der Einzelverfügbarkeiten
 - z.B. TMR: Vergleichslogik nur einmal vorhanden
 - **single-point-of-failure**
→ selbst hochverfügbar auslegen

Anwendungsbeispiele für fehlertolerante Systeme

- Bereiche
 - Raumfahrt, Medizintechnik, Luftfahrt
 - Kritische Infrastrukturen
 - Signalsysteme (**fail-stop**)
 - Systeme mit erheblicher wirtschaftlicher Bedeutung
- Mit Schwerpunkt auf Integrität
 - Datenbanksysteme von Banken, Versicherungen etc.
- Mit Schwerpunkt auf Verfügbarkeit
 - Telefonvermittlungsanlagen
 - Buchungssysteme
 - lebenserhaltende Systeme
 - eingebettete Systeme (z.B. im Auto)