2. Grundlagen fehlertoleranter Rechensysteme

- **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).

- ***Sicherheit:***

  Sachlage, bei der das zulässige Grenzrisiko nicht überschritten wird, d. h. eines vereinbarten Wertes, der sich aus der Häufigkeit für den Eintritt eines Schadensereignisses sowie dem möglichen Schadensmaß zusammensetzt (DIN 31 000).

- ***Ausfall:***

  Aussetzen der Ausführung der festgelegten Aufgabe einer Betrachtungseinheit aufgrund einer in ihr selbst liegenden Ursache und im Rahmen der zulässigen Beanspruchung (DIN 40 041, Teil 3).

- ***Redundanz:***

  Vorhandensein von mehr als für die Ausführung der vorgesehenen Aufgaben an sich notwendigen Mitteln (DIN 40 041, Teil 4). Betrachtungseinheiten, für die diese Eigenschaft zutrifft, heißen **fehlertolerant**.

- ***Fehlertoleranz:***

  Fähigkeit eines Systems, auch mit einer begrenzten Zahl fehlerhafter Teilsysteme seine spezifizierten Funktionen zu erfüllen.

- ***Statische Redundanz:***

  ... erlaubt eine Aktivierung von redundanten Komponenten von vornherein (z. B. Vervielfachung der HW oder Duplizierung von Programmen) $\rightarrow$ Fehlerkompensation

- ***Dynamische Redundanz:***

  ... erlaubt eine Aktivierung nur bzw. erst bei Bedarf. Solange kein Bedarf vorliegt, können von den redundanten Komponenten aber andere Aufgaben übernommen werden $\rightarrow$ Fehlerbehebung

- ***Heiße (aktive) Redundanz:***

  Redundanz, bei der die zusätzlichen Mittel nicht nur ständig in Betrieb sind, sondern auch an der Ausführung der vorgesehenen Aufgabe beteiligt sind → Funktionsbeteiligung

- ***Passive (Standby-) Redundanz:***

  Redundanz, bei der die zusätzlichen Mittel eingeschaltet, aber erst bei Störung oder Ausfall an der Ausführung der vorgesehenen Aufgabe beteiligt sind → Funktionsbeteiligung

- ***Kalte Redundanz:***

  Redundanz, bei der die zusätzlichen Mittel zur Ausführung der vorgesehenen Aufgabe erst bei Störung oder Ausfall eingeschaltet werden.

- ***Homogene und diversitäre Redundanz:***

  Redundanz mit gleichartigen bzw. ungleichartigen (z. B. andere physikalische Prinzipien, andere Lösungswege, andere Aufbauweise usw.) Mitteln.

- ***Vorwärtsfehlerkorrektur:***

  … versucht weiterzumachen, als läge kein Fehler vor. Fehlerhafte Eingabewerte werden durch Erfahrungswerte aus der Vergangenheit ausgeglichen oder es wird mit korrekt funktionierenden Ersatzsystemen gearbeitet.

- ***Rückwärtsfehlerkorrektur:***

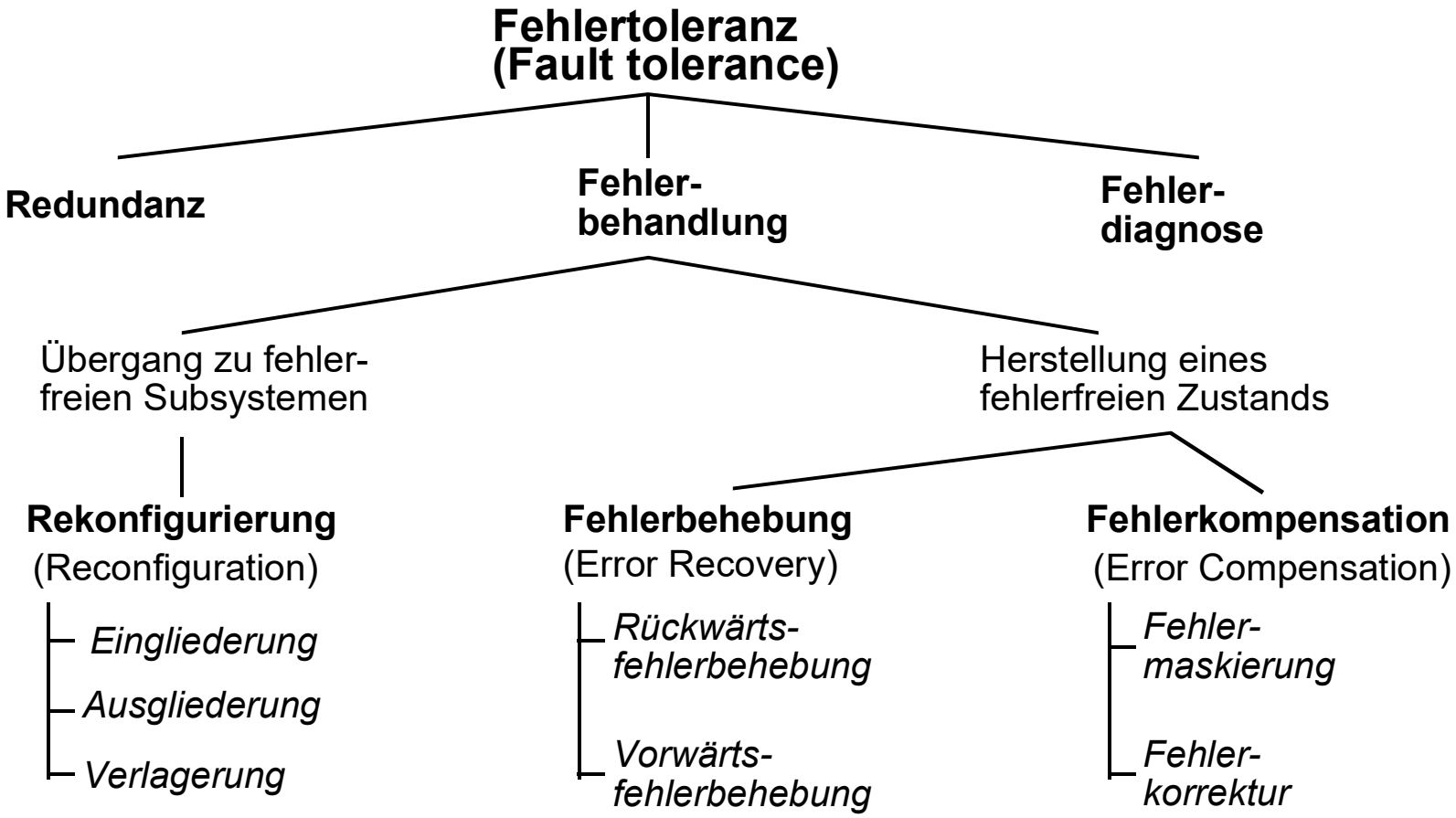
  Zurückkehr in einen Zustand vor dem Auftreten eines Fehlers. Genauso ist aber auch ein Zustandswechsel in einen Notbetrieb oder ein Neustart des Systems möglich.

- ***Fehlermaskierung (fault masking):***

  … ist die dynamische Korrektur von Fehlern aus mehreren Ergebniswerten, die jeweils von redundanten Systemexemplaren (statisch) zur Verfügung gestellt werden, z. B. anhand einer Mehrheitsentscheidung.

- ***Fehlerkorrektur (error correction):***

  … geht nur von einem Ergebniswert bzw. nur einem Systemexemplar aus. Ist dieser Ergebniswert fehlerhaft, so wird aus diesem anschließend ein fehlerfreier Wert errechnet.


Fehlertoleranz
(Fault tolerance)
Redundanz
Fehler-
behandlung
Fehler-
diagnose
Übergang zu fehler-
freien Subsystemen
Herstellung eines
fehlerfreien Zustands
Rekonfigurierung
(Reconfiguration)
Eingliederung
Ausgliederung
Verlagerung
Fehlerbehebung
(Error Recovery)
Rückwärts-
fehlerbehebung
Vorwärts-
fehlerbehebung
Fehlerkompensation
(Error Compensation)
Fehler-
maskierung
Fehler-
korrektur

- Fehlervermeidung
  versucht, die Fehlerursachen zu verhindern
- Fehlermaskierung
  versucht, die Fehlerauswirkung zu verhindern
- Fehlertoleranz
  wirkt sich auf die Fehlerzustände im System aus, so dass bei entsprechender Gegenmaßnahme ein Systemausfall vermieden werden kann
- Wartung und Reparatur
  periodische Prüfungen und Austausch defekter Komponenten

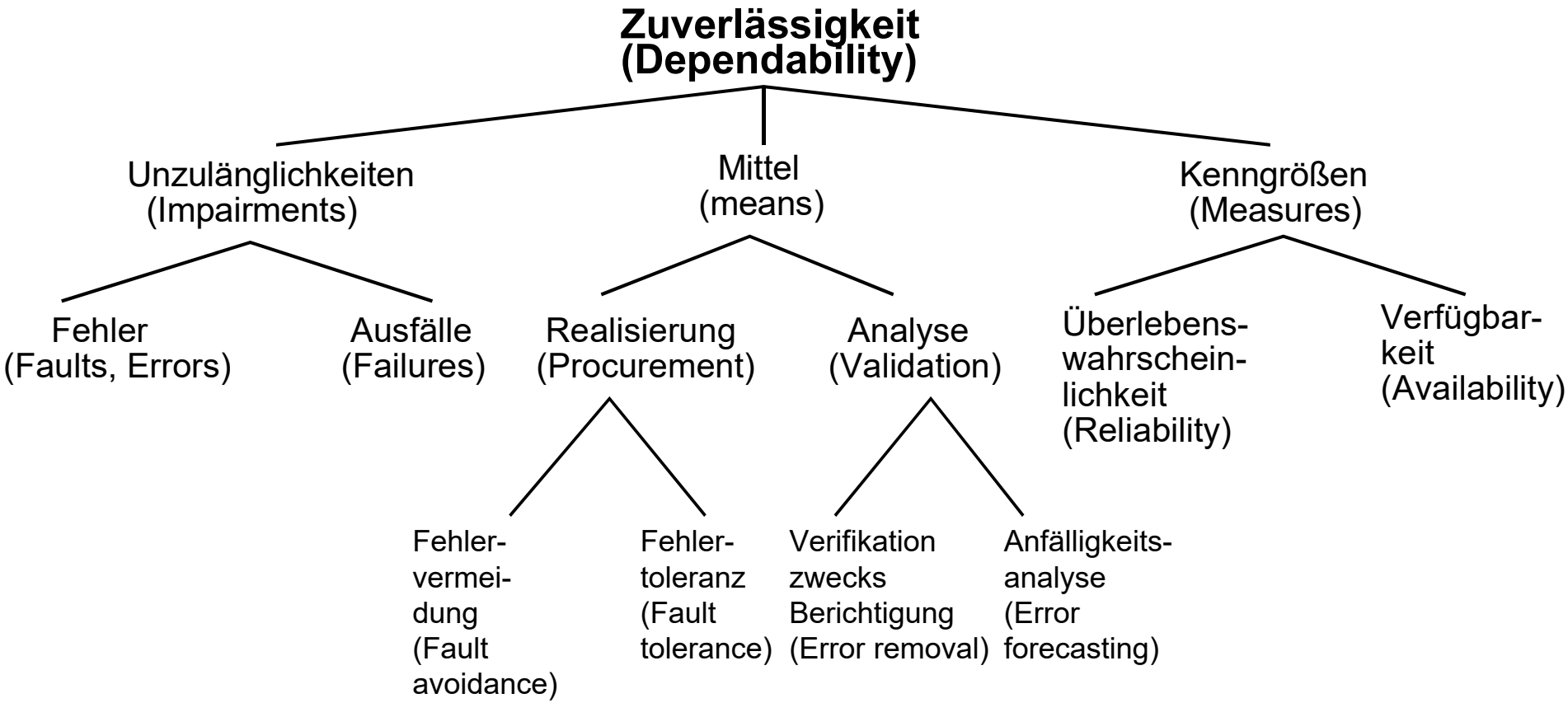
- ***Fehler (fault, error, defect, mistake):***

  eher die Auswirkung eines Ausfalls auf die erbrachte Funktion und damit eine unzulässige Abweichung vom wahren Wert eines Merkmals $\rightarrow$ Zustand

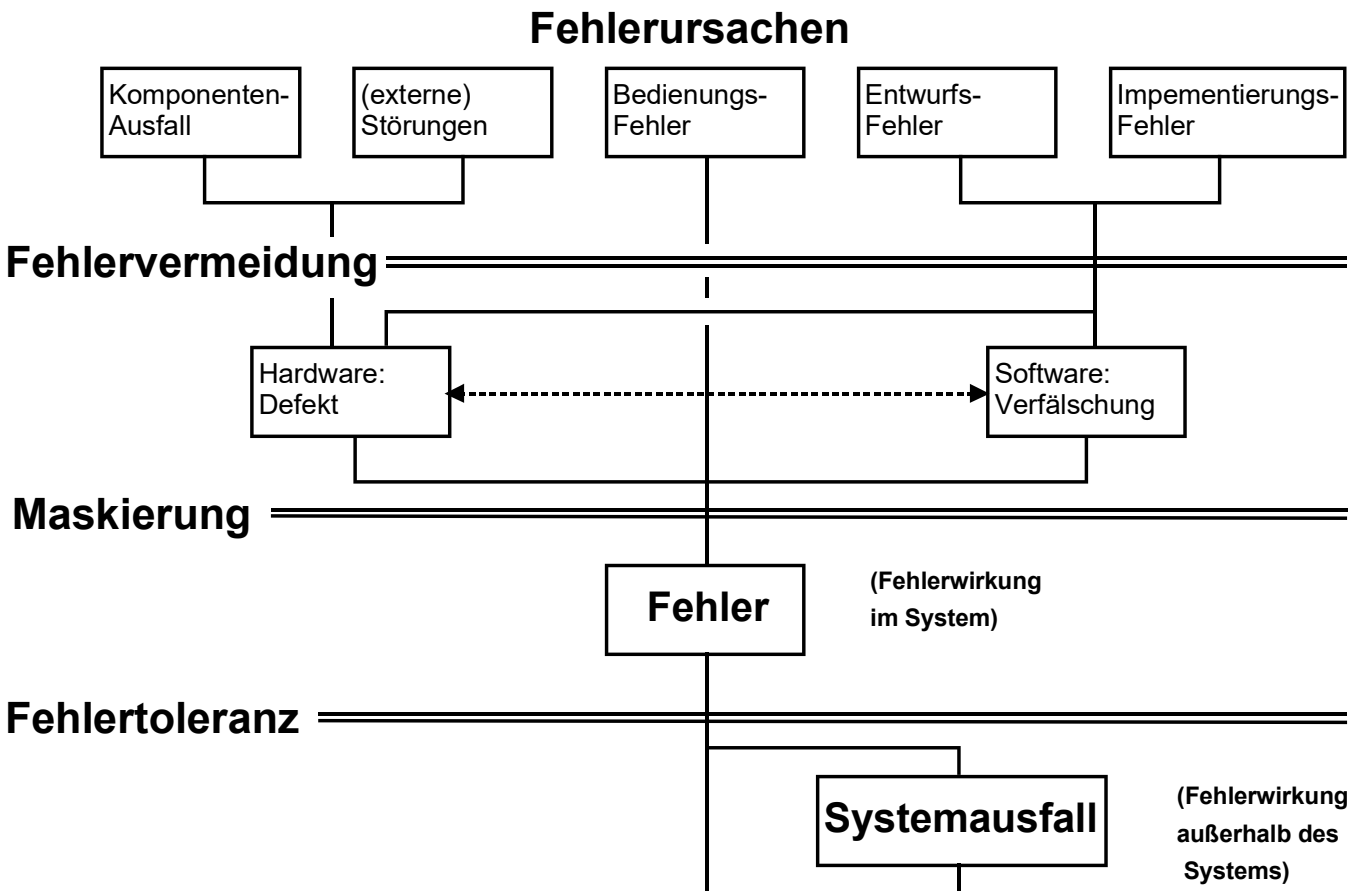
- ***Ausfall (failure):***

  dagegen das Ereignis der nicht erfolgten Funktionserbringung und damit der Übergang in den nicht funktionsfähigen Zustand $\rightarrow$ Ereignis

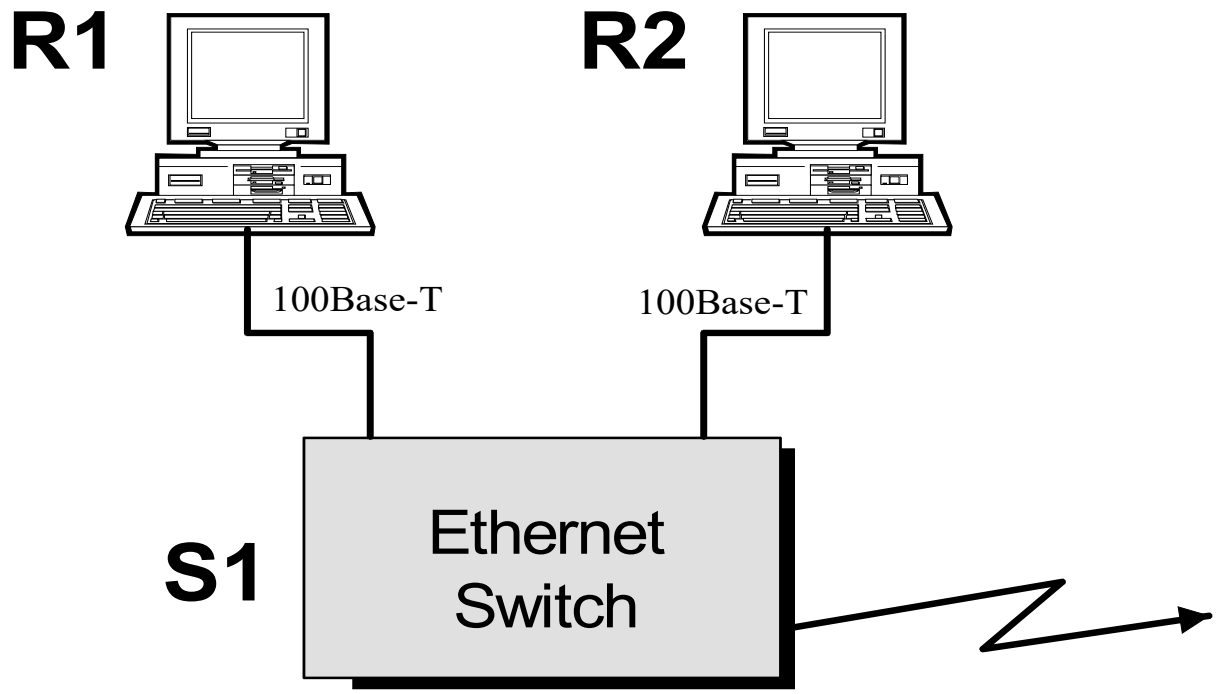
- Permanente Fehler
  ... eine Fehlermaskierung oder Ausgliederung der betroffenen Komponente sowie anschließende Reparatur
- Transiente Fehler
  ... eine Reparatur ist hier sinnlos, da gar keine Komponente im engeren Sinn ausgefallen ist
  ... eine Fehlerbehebung oder Fehlerkompensation notwendig
- Intermittierende Fehler (pseudo-transient)
  ... lassen sich als Sonderfall permanenter oder transienter Fehler behandeln


Zuverlässigkeit
(Dependability)
Unzulänglichkeiten
(Impairments)
Mittel
(means)
Kenngrößen
(Measures)
Fehler
(Faults, Errors)
Ausfälle
(Failures)
Realisierung
(Procurement)
Analyse
(Validation)
Überlebens-
wahrschein-
lichkeit
(Reliability)
Verfügbar-
keit
(Availability)
Fehler-
vermei-
dung
(Fault
avoidance)
Fehler-
toleranz
(Fault
tolerance)
Verifikation
zwecks
Berichtigung
(Error removal)
Anfälligkeits-
analyse
(Error
forecasting)

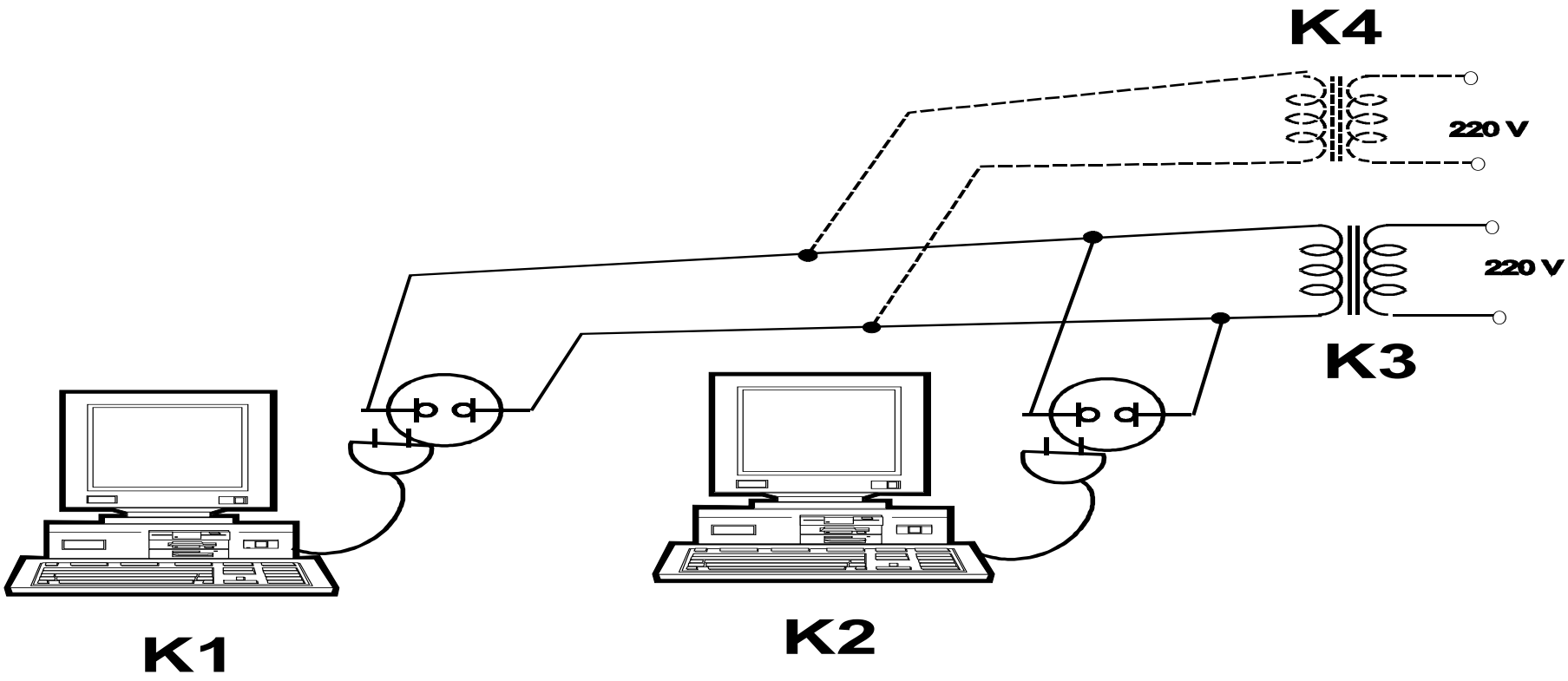
- Strukturelle Redundanz (HW- oder Modul-Redundanz)
  $\rightarrow$ Maskierung, Duplizierung, Lokalisierung, hybride Formen
- Funktionelle Redundanz (SW-Redundanz)
  $\rightarrow$ Gültigkeitstests, Selbsttests, vervielfachte Programme etc.
- Informationsredundanz (Code-Redundanz)
  $\rightarrow$ Codierung, Prüfsummen, Signaturen etc.
- Zeitredundanz
  $\rightarrow$ ARQ (automatic repeat request), Recovery Block etc.


Fehlerursachen
Komponenten-Ausfall
(externe) Störungen
Bedienungs-Fehler
Entwurfs-Fehler
Impementierungs-Fehler
Fehlervermeidung
Hardware: Defekt
Software: Verfälschung
Maskierung
Fehler
(Fehlerwirkung im System)
Fehlertoleranz
Systemausfall
(Fehlerwirkung außerhalb des Systems)

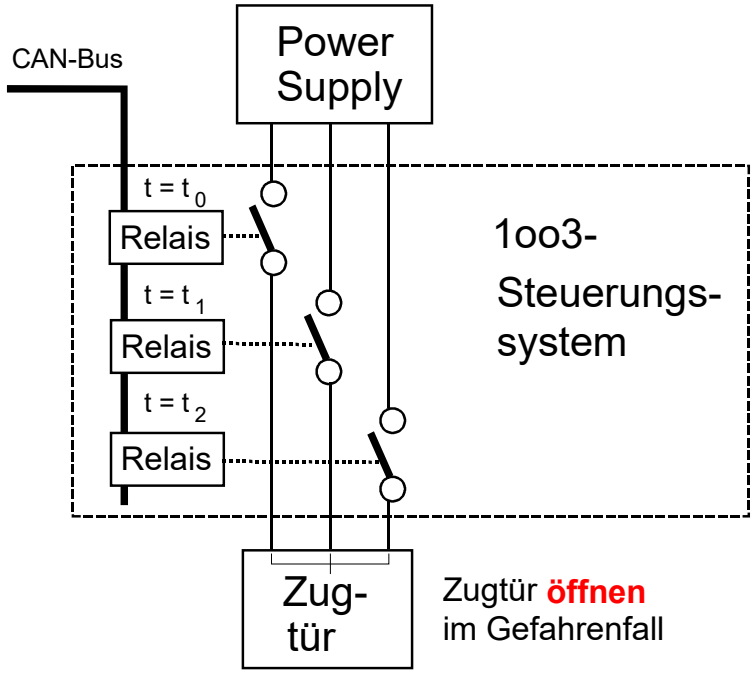
Zwei redundante Rechner in einem Netzwerk

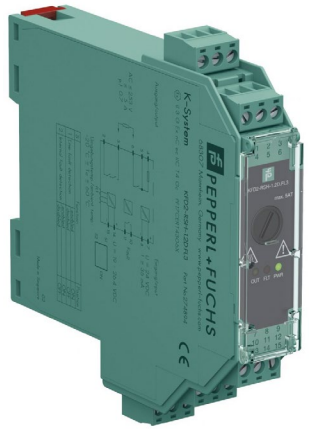


Redundante Rechner an redundanter Stromversorgung

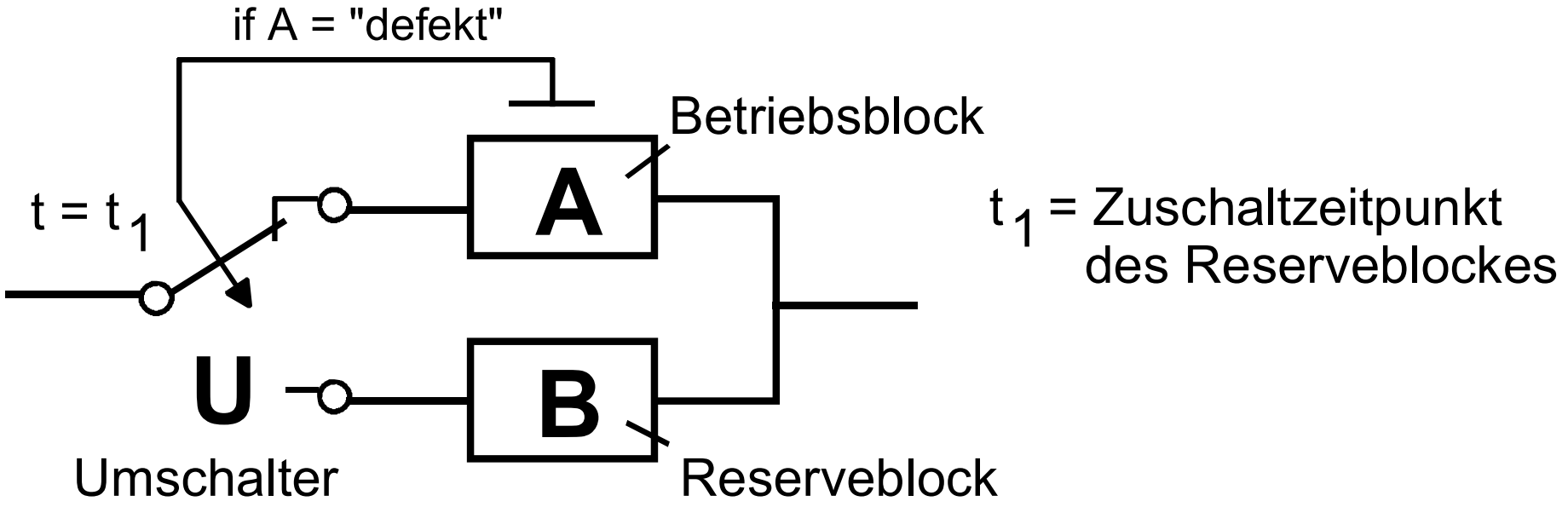


Automatisches Öffnen der Zugtüren bei einem Schnellzug im Bedarfsfalle (beispielsweise bei Ausbruch eines Feuers im Zug)

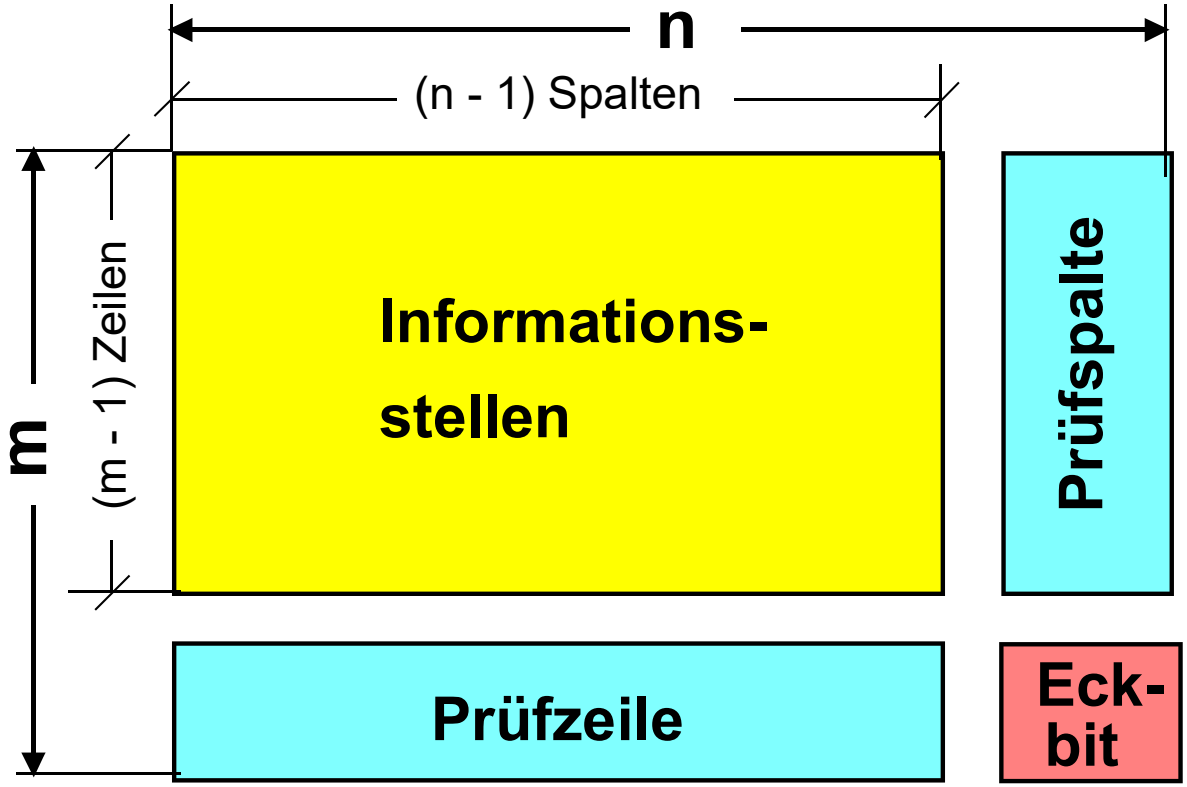




Umschaltung auf einen Reserveblock im Bedarfsfall



Redundante Prüfinformationen (Rechteckcode)



Zeitredundanz

… über den Zeitbedarf des Normalbetriebs hinausgehende ***zusätzliche*** Zeit, die einem funktionell redundantem System zur Funktionsausführung zur Verfügung steht.

Beispiele:

- Wiederholungsbetrieb
- Zeitbedarf für Konsistenzmechanismen in verteilten Dateisystemen und Netzwerken (TCP/IP)
- Store-and-Forward Switching ()
- Packet switching networks (Datex P, X.25, Frame Relay)

Verlust einer Nachricht: