

Wissenschaftliche Vertiefung
Studiengang Technische Informatik

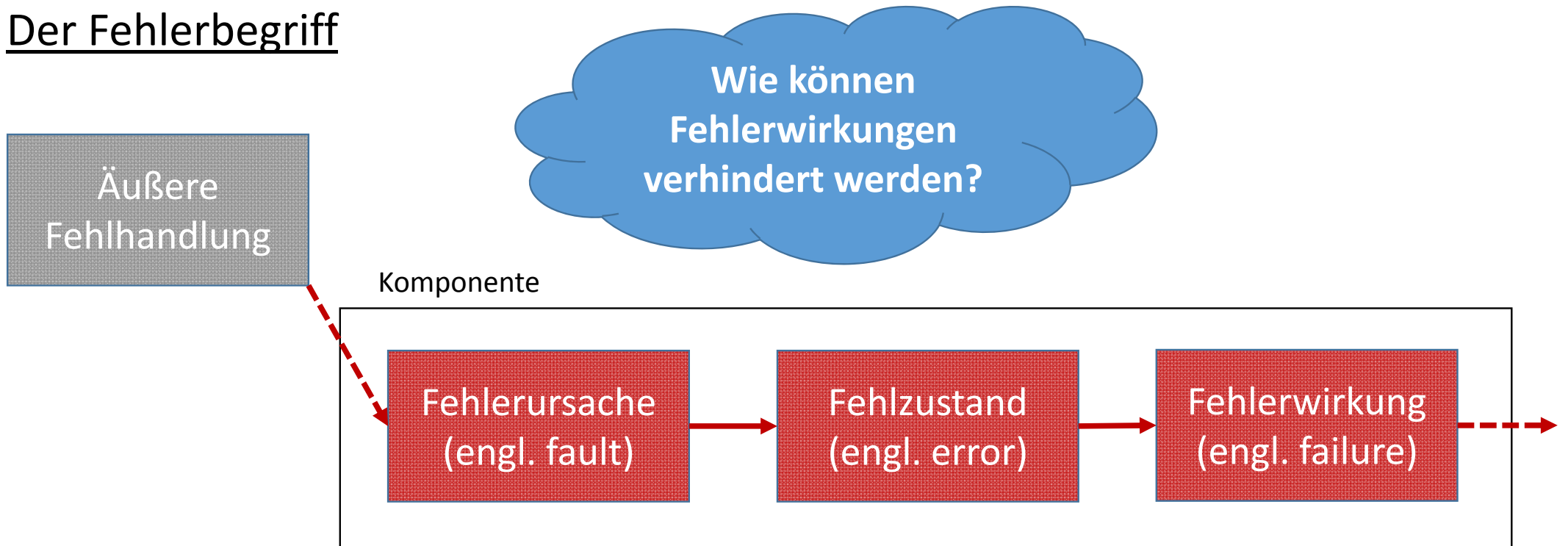
Fehlertolerante Systeme

Philipp Dürnay
22.01.2016

Agenda

- Fehlertoleranz
- Fehlerdiagnose
- Fehlerbehandlung
- Beispielsystem
- Ausblick

Der Fehlerbegriff



Die verschiedenen Aspekte des Fehlers können weit entfernt voneinander auftreten

Fehlertoleranz beschreibt die Fähigkeit eines Systems, trotz einer begrenzten Anzahl fehlerhafter Subsysteme seine spezifizierte Funktion weitestgehend zu erfüllen

Funktionen:

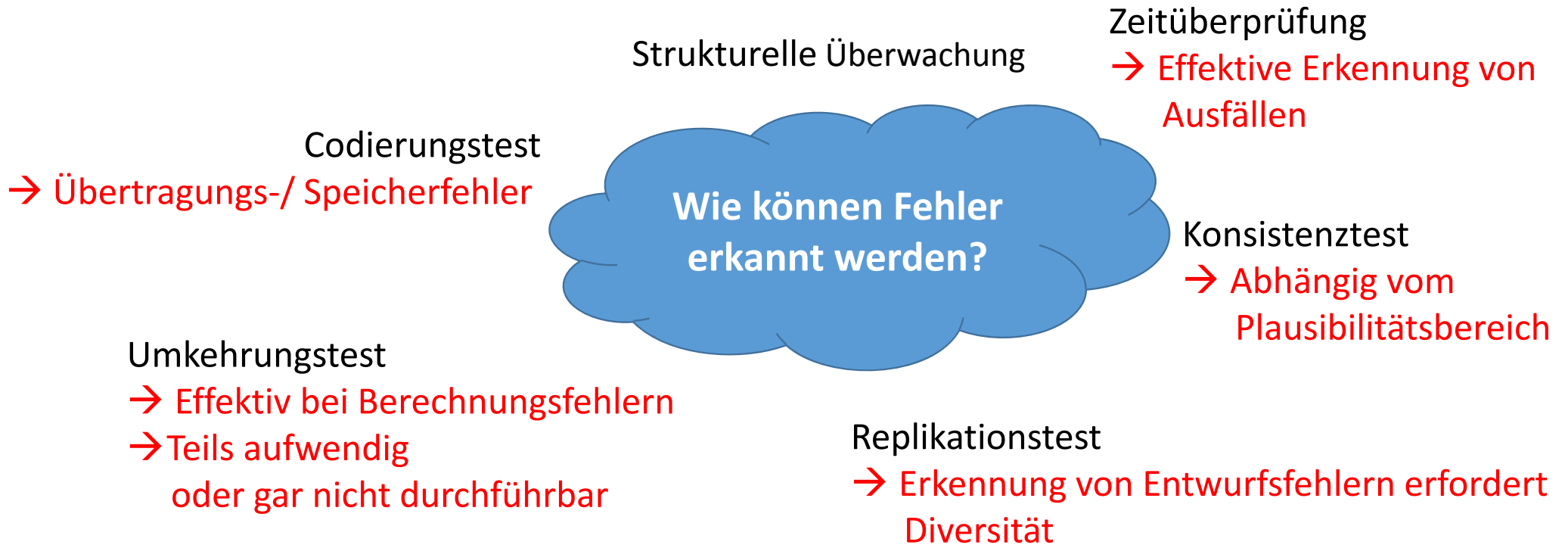
- 1) Fehlerdiagnose
- 2) Fehlerbehandlung

Zusätzliche Betriebsmittel

Redundanzarten:

- Strukturelle Redundanz
- Funktionale Redundanz
- Informationsredundanz
- Zeitredundanz

Fehlertoleranz erfordert Redundanz



Ein Ausfall ist leichter zu erkennen als eine Fehlfunktion

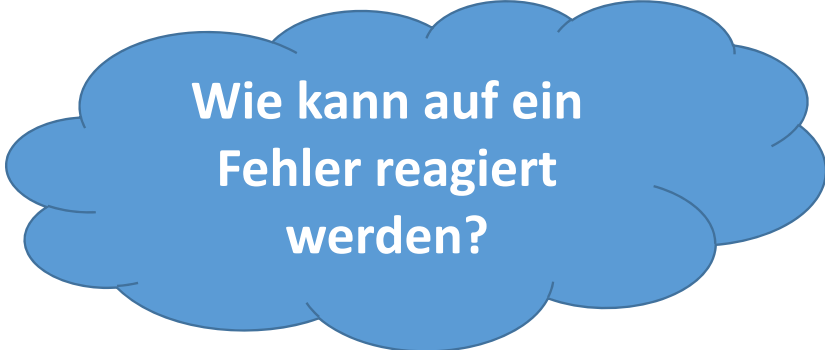
Modellbasierte Verfahren

- Basiert auf Modell des Zielsystems
- Präzises Modell ermöglicht detaillierte Diagnose
- Diagnose stark abhängig vom Modell

Beobachtungsbasierte Verfahren

- Basiert auf Beobachtung des Zielsystems
- Kann universeller und dynamischer entwickelt werden
- Benötigt viele Daten zur effektiven Diagnose

Diagnoseverfahren können in zwei Gruppen unterschieden werden



Wie kann auf ein Fehler reagiert werden?

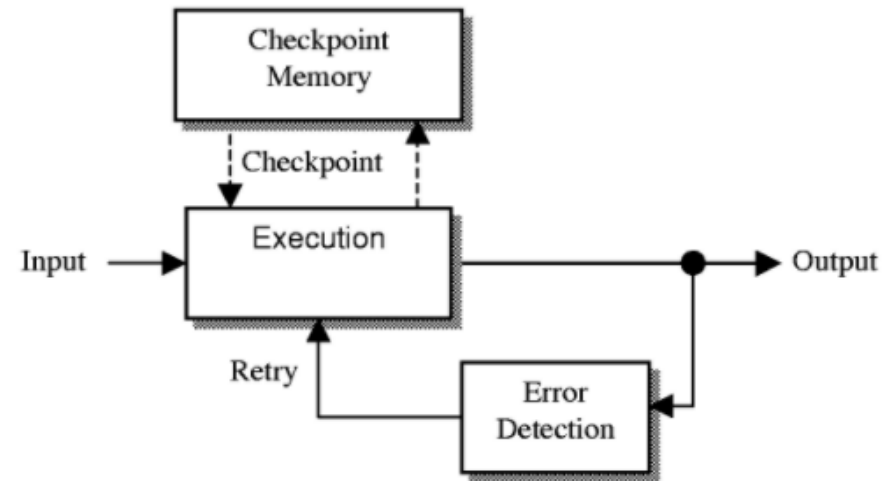
- Fehlerbehebung → Entfernen des Fehlzustandes
- Rekonfiguration → Ersetzen des fehlerhaften Subsystems
- Fehlerkompensation → Ausgleichen der Fehlerwirkung

Behandlungsmethoden unterscheiden sich in drei Gruppen

Fehlerbehandlung

Beispiel für Fehlerbehebung:

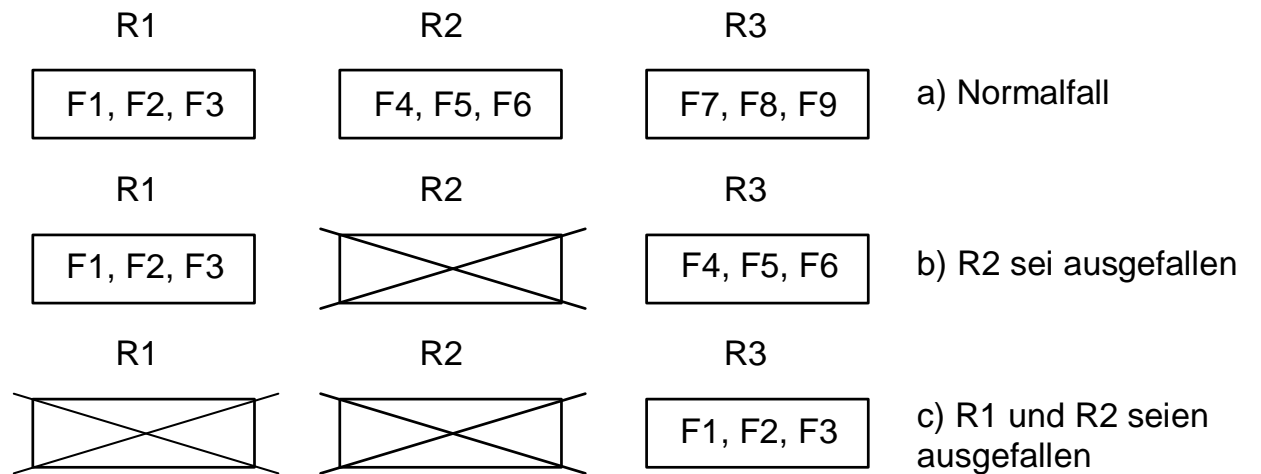
„Checkpoint and Restart“



Fehlzustand soll durch Neustart des (Sub-) Systems behoben werden

Beispiel für Rekonfiguration:

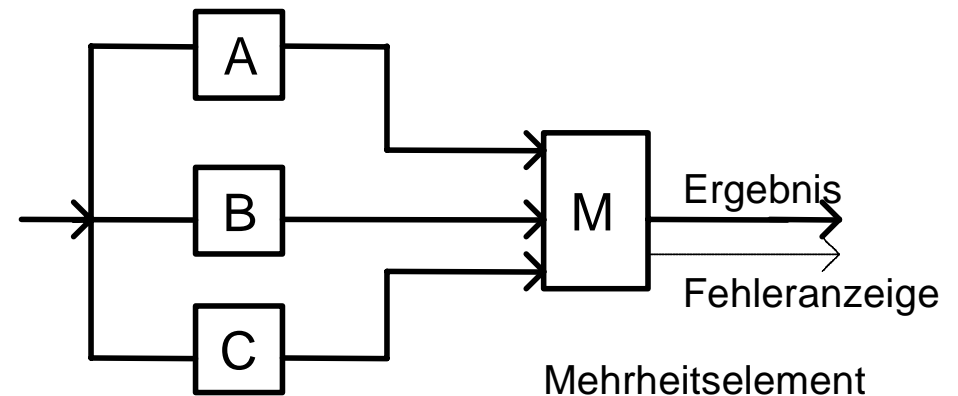
„Graceful Degradation“



Wichtige Prozesse werden auf verbleibende Ressourcen verteilt

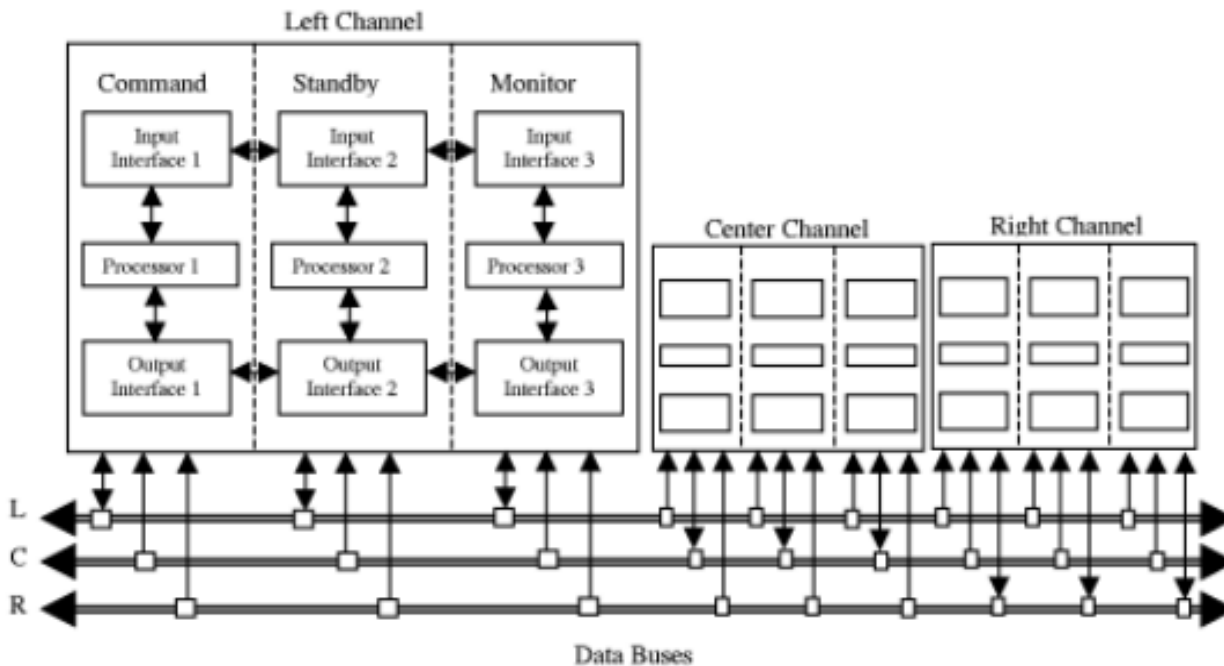
Beispiel für Fehlerkompensation:

„N-aus-M-Systeme“



Fehler wird nicht entfernt sondern ausgeglichen

Beispielsystem – Flugcomputer B777

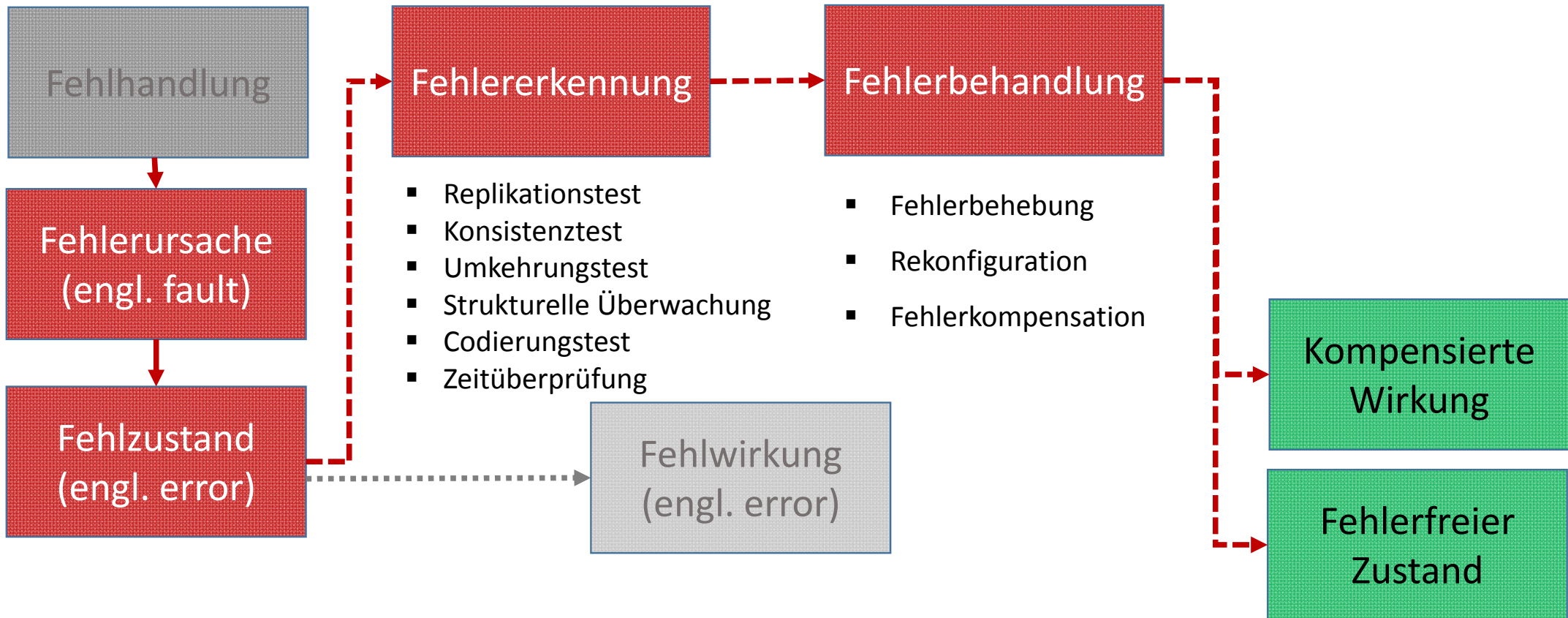


- Standby-System innerhalb der Kanäle
- Ergebnis ist Mittelwert aller Kanäle
- Hardwarediversität durch verschiedene Prozessoren
- Softwarediversität durch verschiedene Compiler

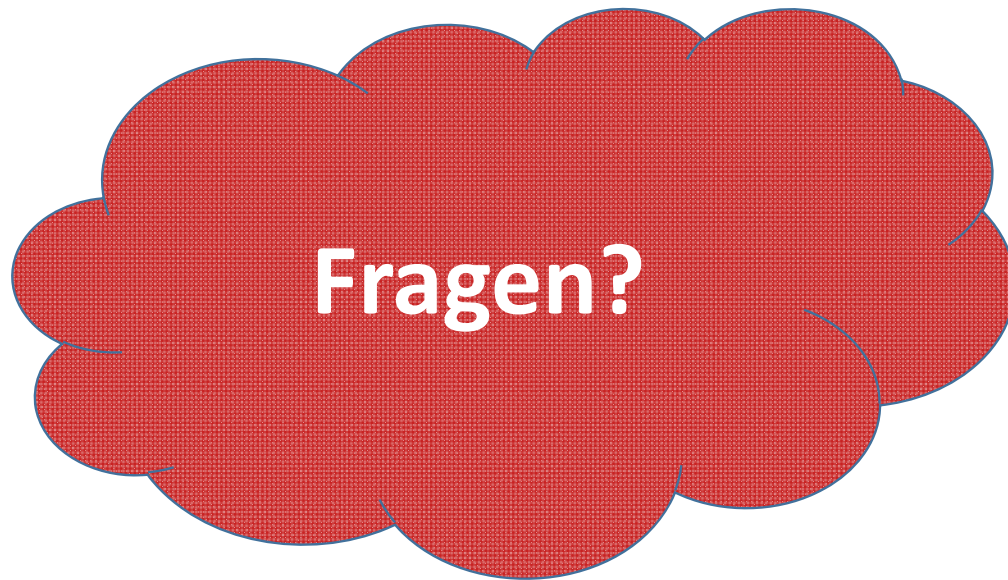
- Fehlerursachen können nicht entfernt werden
- Systeme, die hohe Zuverlässigkeit benötigen, erfordern viele zusätzliche Ressourcen

Je mehr Toleranz, desto mehr Redundanz erforderlich

Zusammenfassung



Ende



Quellen:

[1] DIN 400041

[2]

[3]

[4]

Danke für die Aufmerksamkeit