

(Miss-) Konzeptionen von Sicherheitsprinzipien

Jan-Tecker Gayen und Hendrik Schäbe

IfEV, TU Braunschweig und TÜV Rheinland InterTraffic

Gliederung

- Einführung
- Sicherer Zustand
- (Sicherheits-)Prinzipien
- Problemfelder
(Wirksamkeit gegen Fehler, Ausfälle)
- Zusammenfassung

Ursachen für Missverständnisse

Bei Auftreten eines **Fehlers** →

System **in einen sicheren Zustand** überführen

(1) Was wird unter Fehler verstanden?

- Hardware-Ausfall
- Fehler in der Software
- Genügt die Unterscheidung?

(2) System in einen sicheren Zustand überführen

- a) War das System vorher nicht in einem sicheren Zustand?
- b) Was charakterisiert einen sicheren Zustand?

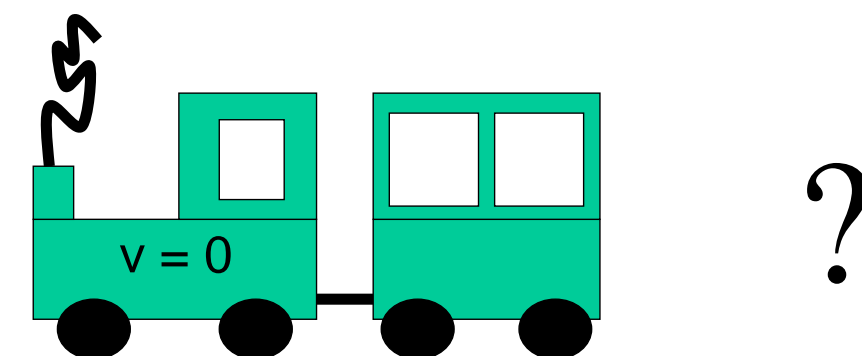
1 Sicherer Zustand

- Sicherer Zustand
Zustand in dem das Risiko, das vom System ausgeht kleiner als das zulässige Risiko ist.
- Sicherer Abschaltzustand/Haltzustand
In der Regel ein gegenüber dem Regelbetrieb relativ energieärmerer Zustand

1 Sichere Zustände

- Jedes Verkehrssystem kennt mindestens 2 sichere Zustände:
 - Regelbetrieb
 - Haltzustand (Abschaltzustand).
- Ein sicheres System geht allenfalls mit tolerierbaren Schäden von einem sicheren Zustand in einen anderen sicheren Zustand über.
- Der sichere Abschaltzustand ist in kurzer Zeit und durch Deaktivieren von Funktionen des Systems erreichbar. Das deaktivieren kann eine aktive Handlung (weitere Funktion des Systems) voraussetzen.

1 Der sichere (Abschalt-)Zustand



Gegenargument:

Brennender Zug im Tunnel

2 Wirksamkeit von Sicherheitsprinzipien

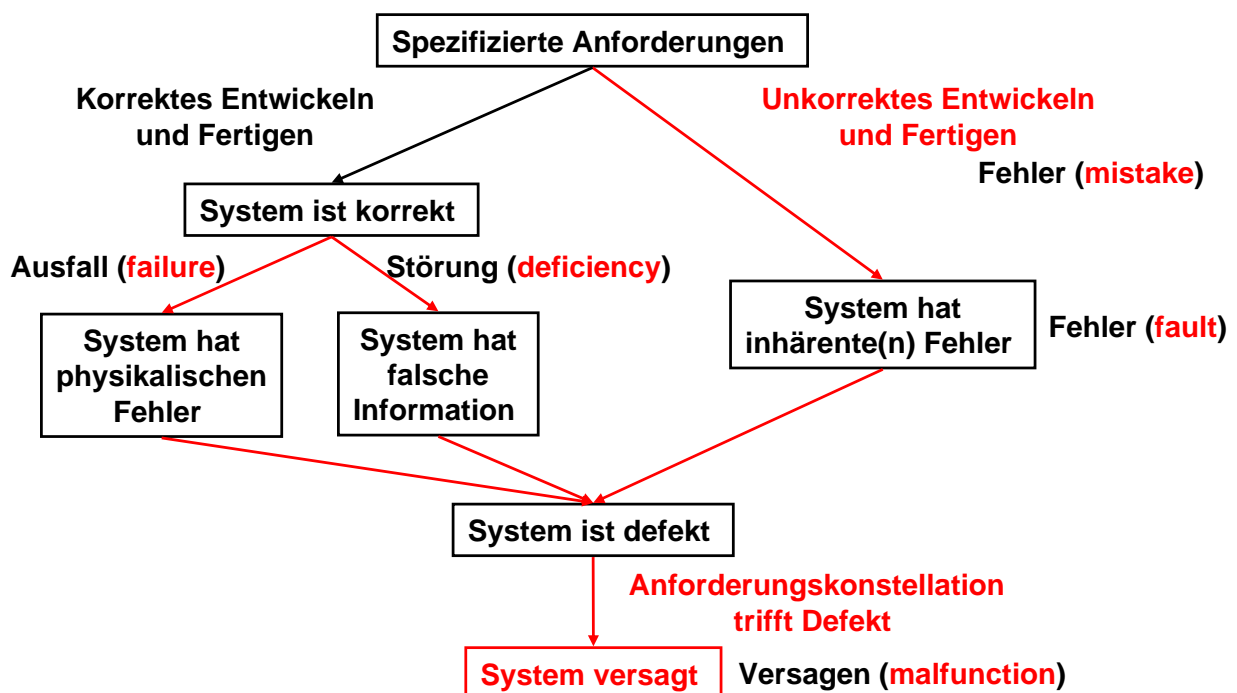
(1) Mit welchem Ziel soll ein bestimmtes Sicherheitsprinzip angewendet werden?

Beherrschung:

- a) Zufälliger Ausfälle
- b) Systematischer Ausfälle
- c) Fehler (in der Hardware)
- d) Fehler (in der Software)

(2) Kann es dieses Ziel erfüllen?

2 Begriffsdefinitionen



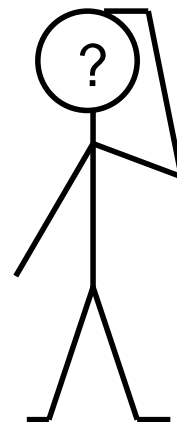
Begriffe nach DIN 40041

2 Begriffsdefinitionen nach DIN 40041

- (1) **Ausfall (failure)** Beendigung der Funktionsfähigkeit einer materiellen Einheit im Rahmen der zugelassenen Beanspruchung.
Anmerkung: Der Ausfall führt zum Versagen sobald die Erfüllung der geforderten Funktion verlangt wird.
- (1) **Fehler** Nichterfüllung einer Forderung. (Planungs-, Realisierungs-, Entwurfs-, Fertigungsfehler)
(Fault?)
(Error?)
- (2) Fehlfunktion
- (3) **Störung** Fehlende, fehlerhafte oder unvollständige Erfüllung einer geforderten Funktion durch die Einheit.
- (4) **Versagen (malfunction)** Entstehen einer Störung bei zugelassenem Einsatz der Einheit aufgrund einer in ihr selbst liegenden Ursache.
Anmerkung 1: Bei einem System kommen alle Ursachen des Versagens ... in Betracht.
Anmerkung 3: Versagen entsteht, wenn ein Fehler der Einheit bei deren zugelassenem Einsatz wirksam wird.

2 Übersicht (Sicherheits-)Prinzipien

- Fail-Safe / Signaltechnisch sicher
- Safe Life
- Redundanz
- Mehrkanaligkeit
- Diversität
- Fail Silent

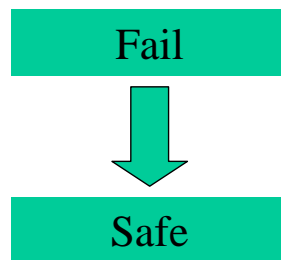


3 Fail-safe (signaltechnisch sicher)

Konzept, das in den Entwurf eines Produktes so einfließt, dass bei Eintreten einer **Fehlfunktion** ein sicherer Zustand eingenommen oder beibehalten wird (EN 50129)

Fähigkeit eines Systems, beim Auftreten eines **Ausfalls** im sicheren Zustand zu bleiben oder unmittelbar in einen anderen sicheren Zustand überzugehen (VDI/VDE 3542 Blatt 1/12.88)

Enge Auslegung



3 Fail-safe (signaltechnisch sicher)

EN 50129 (B.3.1):

Es muss gewährleistet sein, dass das/die System/Teilsystem/Einrichtung bei Eintritt zufälliger **Einzelausfälle** die THR erfüllt.

Systeme mit SIL 3 und SIL 4 müssen bei Eintritt jedes anzunehmenden zufälligen Einzelausfalls **sicher bleiben**.

Dieses Prinzip, das als **fail-safety** bekannt ist, kann auf mehreren unterschiedlichen Wegen erreicht werden:

- Fail-safety durch unverlierbare Eigenschaften (**inherent fail-safety**)
- Fail-safety durch sicherheitsgerichtete Ausfallreaktion (**reactive fail-safety**)
- Fail-safety durch Redundanz (← Fehler in deutscher Normversion, eigentlich: **composite fail-safety**)

3 Fail-Safe (signaltechnisch sicher)

Die EN 50129 sagt...

- **Inherent Fail-Safety** ✗
Single item, provided all the credible **failure** modes of the item are non-hazardous
- **Reactive Fail-Safety**
A single item, provided its safe operation is assured by rapid detection and negation of any hazardous **fault**
- **Composite Fail-Safety**
Safety-related function is performed by at least two items. Each of these items shall be independent from all others, to avoid common-cause **failures**. Non-restrictive activities are allowed to progress only if the necessary number of items agree. A hazardous **fault** in one item shall be detected and negated in sufficient time to avoid a co-incident fault in a second item.

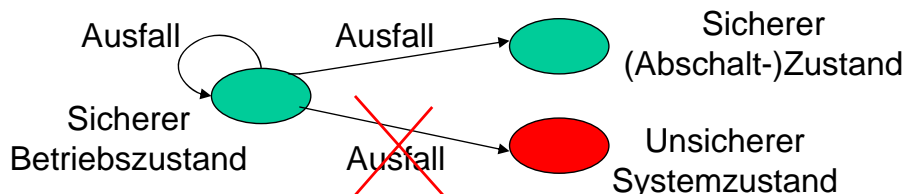
Gayen / Schäbe

10. BieleSchweig Workshop

13

3a Inherent fail-safety

- Voraussetzung: **Alle anzunehmenden Ausfallarten** der Betrachtungseinheit sind ungefährlich
- Physikalische, chemische oder andere Prozesse sorgen dafür, dass jeder Ausfall der Komponente in einen sicheren Zustand führt
- Systemlösungen: Ermöglicht sicheres einkanaliges System



Kein Fail-Safe ohne Übergang in (anderen) sicheren Zustand

Kein Fail-Safe ohne Existenz eines sicheren Abschaltzustandes

Beispiele: Schwerkraftrelais, Gleisstromkreis, (Formsignal)

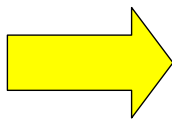
Gayen / Schäbe

10. BieleSchweig Workshop

14

3b Reactive fail-safety

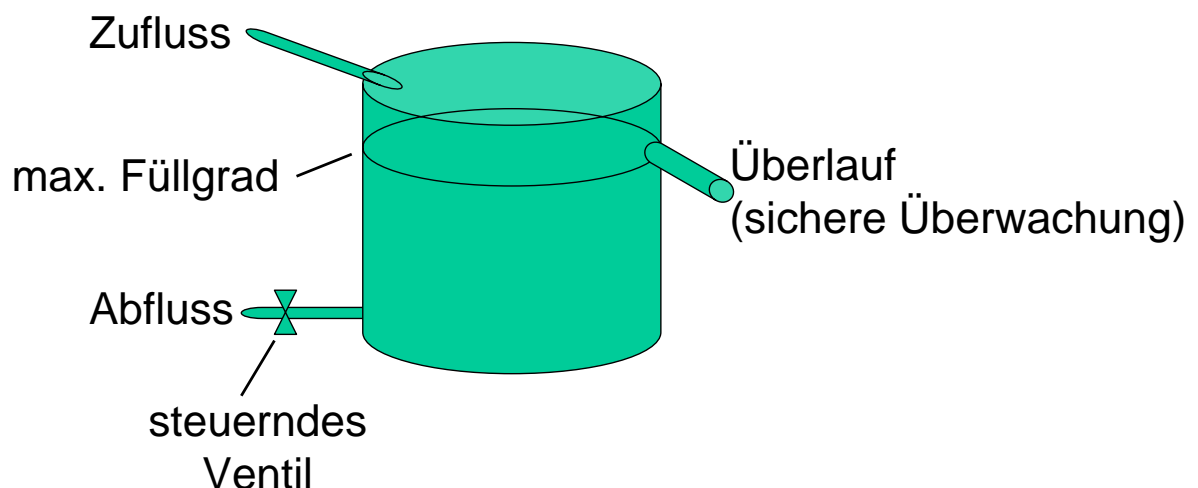
- Voraussetzung:
Sichere Funktion wird durch schnelles Erkennen und eine sicherheitsgerichtete **Ausfall**reaktion jeder gefährlichen Fehlfunkt erreicht
- Obgleich nur eine Betrachtungseinheit die tatsächliche sicherheitsrelevante Funktion erbringt, kann die Überprüfungs-/Test-/Erkennungs-Funktion als zweite Betrachtungseinheit angesehen werden.
- Systemlösungen: System mit sicherer Überwachungsfunktion, ...



Detektion jedes (gefährlichen) Ausfalls nötig.
Detektion muss hinreichend schnell erfolgen
Aktive Handlung nötig (Überführung in (anderen) sicheren Zustand).

3b Beispiel für reactive fail-safety

Sichere Füllstandsüberwachung eines Wasserbehälters



3b Erkenntnisse

- Zuverlässigkeit, Güte usw. des Detektors
- Zuverlässigkeit und Güte des eingreifenden Systems
- Zuverlässigkeit und Güte des Aktors

- Hier gibt es überall Versagenswahrscheinlichkeiten
- Der sichere Abschaltzustand muss existieren

3c Composite fail-safety

- Mehrere (mindestens 2) Kanäle (Subsysteme), die die identische Sicherheitsfunktion ausführen
- Kanäle müssen unabhängig voneinander sein
- Übereinstimmung der notwendigen Anzahl der Subsysteme (aller oder Mehrheit) → **Vergleich oder Mehrheitsentscheid**
- Detektion von **Ausfällen** einzelner Kanäle und Reaktion (Detektion muss sicher sein und relativ schnell, bevor weiterer Kanal ausfällt)

Prinzip der Mehrkanaligkeit

3c Vergleich / Mehrheitsentscheid

Konfigurationen:

- Mehrkanaligkeit mit Vergleich
- Mehrkanaligkeit mit Mehrheitsentscheid
- Mehrkanaligkeit mit adaptivem Mehrheitsentscheid

Anforderungen:

- Vergleich muss sicher und schnell sein
- Mehrheitsentscheid muss sicher und schnell sein

3c Erkenntnisse Mehrheitsentscheid

- Abstimmungssystem k-aus-n mit $k \geq (n+1)/2$
- Der sichere Voter (auch mehrkanalig?)
- Detektion von **Ausfällen** einzelner Kanäle
- Was passiert, wenn keine Mehrheit zustande kommt? Ungerade Anzahl von Kanälen verwenden.
- Es muss ein sicherer (Abschalt-)Zustand existieren.

3d Diskussion fail-safety

Gelten die fail-safety Prinzipien nur für Ausfälle?

Wie sieht es mit Fehlern aus?

Inherent fail-safety: Ausfälle

Reactive fail-safety: Ausfälle

Composite fail-safety: Ausfälle und Fehler¹

¹Fehler (Hardware, Software bei entsprechender Diversität in den Kanälen)

4 Safe Life

- Während eines Lebensdauerabschnitts darf das System nicht ausfallen

Lösung:

- Dimensionierung (keine Schädigung)
→ Bauwerke (z.B. Brücke)
- Redundanz
→ Flugzeug (z.B. mehr als ein Triebwerk)

Redundanz: Mehrere Komponenten führen dieselbe Funktion aus, sind dazu aber nicht alle erforderlich

4 Fail-safe versus Safe Life

- Wahl des Prinzips ist abhängig vom Prozess
- Kann jederzeit der sichere (Abschalt-)Zustand eingenommen werden?
 - Eisenbahn → ja → fail-safe
(Ausnahme: Brand im Tunnel)
 - Flugzeug → nein → safe life
 - Kerntechnik → ja → fail-safe

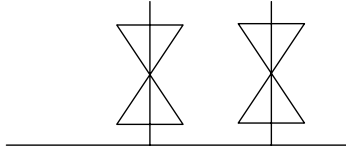
5 Redundanz

Vorhandensein von mehr als für die Ausführung der vorgesehenen Aufgaben an sich notwendigen Mittel (VDI/VDE 3542 Blatt 1/12.88)

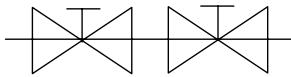
- Mehrere Komponenten führen dieselbe Funktion aus (eine Komponente würde z. B. genügen)
- Varianten: hot standby, warm standby, cold standby
- Ziel der Redundanz:
 - Erhöhung der Zuverlässigkeit, Verfügbarkeit,
jedoch nicht der Sicherheit

5 Akademisches Beispiel

Wo ist hier Redundanz?



2 Sicherheits-
abblaseventile



2 Absperrventile eines
Behältnisses mit
giftiger Flüssigkeit /
Gas

6 Unterschied Redundanz / Mehrkanaligkeit

Mehrkanaligkeit	Redundanz
Sicherheitsfunktion durch mehrere Subsysteme mit derselben Aufgabe erfüllt	Mehrere Subsysteme realisieren dieselbe Funktion
Sicherheit nur bei Funktion aller Systeme gegeben, Aufdeckung von Fehlern durch Mehrkanaligkeit	Es sind mehr Subsysteme vorhanden als zur Erfüllung der Aufgabe erforderlich
Vergleich	Kein Vergleich → Mehrheitsentscheid
Mehrkanaligkeit erhöht Sicherheit	Redundanz erhöht Zuverlässigkeit und Verfügbarkeit

6 Mehrkanaligkeit **und** Redundanz

- Sicherheitsfunktion nur durch mehrere Subsysteme mit derselben Aufgabe erfüllt
- Sicherheit nur bei Funktion einer Mehrheit dieser Subsysteme gegeben
- Es sind mehr dieser Subsysteme vorhanden als zur Erfüllung der Sicherheitsfunktion erforderlich
- Mehrheitsentscheid
- Höhere Zuverlässigkeit und Verfügbarkeit

Beispiel m-von-n System:

- m Kanäle zur sicheren Funktion notwendig
- (m-n) Kanäle aus Redundanzgründen (Verfügbarkeit)

7 Diversität

- Mehrere Subsysteme realisieren dieselbe Funktion auf unterschiedliche Art
- Diversitär kann der Entwicklungsprozess, der Algorithmus, die Software oder die Hardware sein
- Anwendbar bei mehrkanaligen und bei redundanten Systemen
- Vergleiche und Mehrheitsentscheide nur auf Funktionsebene

Ziel:

Common-mode-failure weitgehend ausschließen

7 Arten der Diversität

- Diversitäre Entwicklungsteams
- Entwurfsdiversität
- Hardwarediversität
- Softwarediversität
 - Diversitäre Betriebssysteme
 - Diversitäre Programmiersprachen
 - Diversitäre Algorithmen
 - ...

8 Fail Silent

- (Unerkannter) Ausfall einer unterstützenden Funktion
- Nur bei Systemen mit unterstützenden Funktionen anwendbar → z.B. Fahrerassistenzsysteme
- Versagen der unterstützenden Funktion als Folge eines Ausfalls ist nicht gefährlich, wohl aber eine Fehlfunktion als Folge eines Ausfalls
- Forderung, dass gefährliche Ausfälle erkannt werden und das System abgeschaltet wird

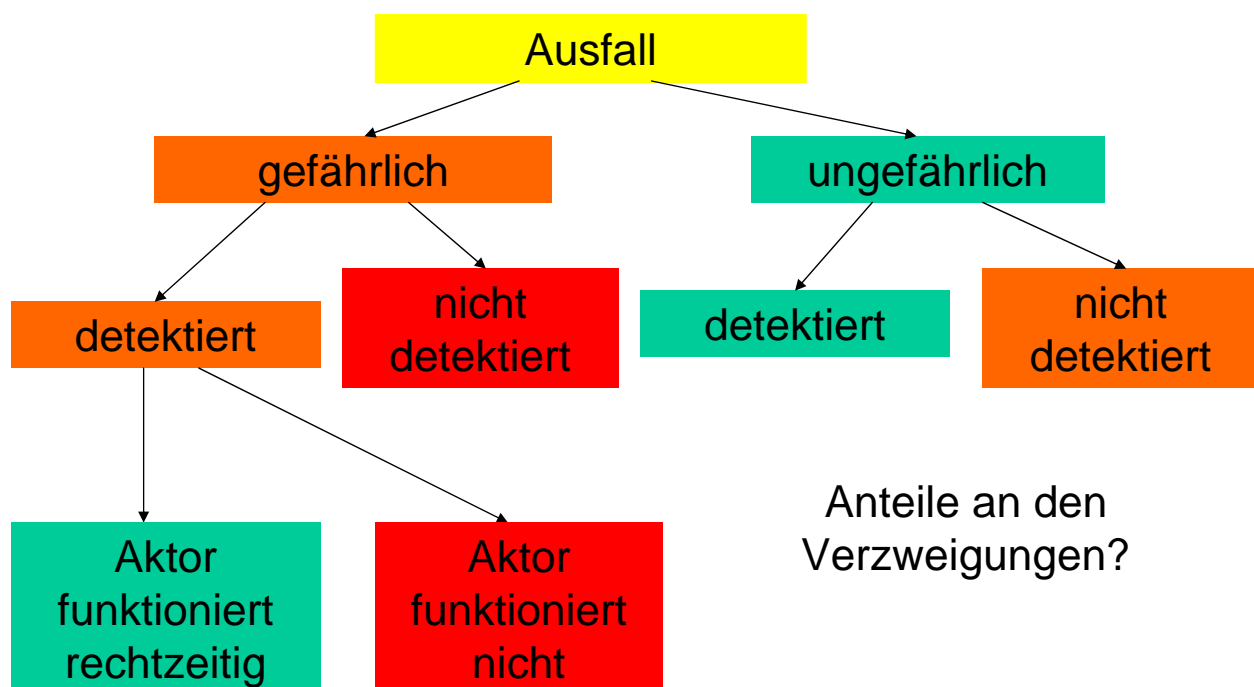
8 Erkenntnisse

- Es existiert ein sicherer Zustand ?
- Abschaltung des Systems ähnlich zu reactive fail-safety (Überwachungssystem), jedoch kann das System selbst an Diagnose und Abschaltung beteiligt sein
- Zuverlässigkeit und Güte von Diagnose, Steuerung und Aktor
- Fahrer verlässt möglicherweise sich auf fail-silent System

9 Problemfelder

- Ausfalloffenbarung (Grad)
- Mehrkanaligkeit und Common-Mode Ausfälle
- Diversität
- Vergleich, Mehrheitsentscheid
- Ausfälle zur sicheren Seite
- Fail-safe Betrachtung gegen Risikobetrachtung
- Aktoren

9a Ausfalloffenbarung



9b Common Mode Failures

Ein common-mode failure (CMF) ist das (gleichzeitige) Auftreten eines gleichartigen Ausfalls von Komponenten in zwei oder mehr gleichen Kanälen eines mehrkanaligen Systems verursacht und dadurch zu einem Ausfall des Systems führt.

- Software (Betriebssystem, Bibliotheken, Compiler, Linker)
- Hardware (Prozessoren, Layouts)
- Stromversorgung
- Äußere Einflüsse (EMV, Temperatur, Druck, Strahlung usw.)
- Prozesse (Konzepte, Entwurf, Herstellung)

9b Common Cause Failures

Systematischer Fehler, bei dem die einzelnen Merkmalabweichungen aufgrund einer gemeinsamen Ursache entstanden sind (DIN/VDE 0801),

d.h. eine Ursache führt zu mehreren Ausfällen

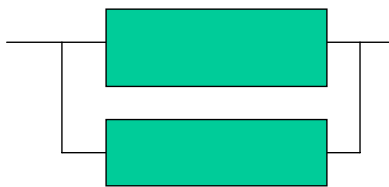
- Software (Betriebssystem, Bibliotheken, Compiler, Linker)
- Hardware (Prozessoren, Layouts)
- Stromversorgung
- Äußere Einflüsse (EMV, Temperatur, Druck, Strahlung usw.)
- Prozesse (Konzepte, Entwurf, Herstellung)

9b CCF versus CMF

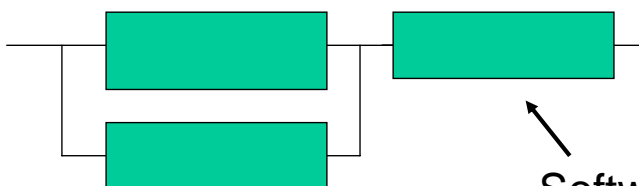
	CCF	CMF
Software (Betriebssystem, Bibliotheken, Compiler, Linker)	X	bei identischen
Algorithmus		bei identischen
Hardware (Prozessoren, Layouts, ..)	X	bei identischen
Stromversorgung	X	bei identischen
Äußere Einflüsse (EMV, Temperatur, Druck, Strahlung usw.)	X	
Prozesse (Konzepte, Entwurf, Herstellung)	X	

9b Konsequenzen

?



Zweikanaliges System
mit identischer
Hardware und Software
→ CMF und CCF



Software oder Hardware
~~CMF~~ CCF

9c Diversität gegen CMF

- Durch Diversität keine CMF mehr?
- Welche Art Diversität ist dann notwendig?
- Welche Diversität gegen welche CMF?
- ARP 4761 Aerospace Recommended Practice, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996-12

9d Aktoren

- Fallen aus bei Anforderung
- Reagieren ungewollt und können dadurch Probleme verursachen
- Potential für schlafende Fehler

9e Ausfälle zur sicheren Seite

- Identifizierung aller Ausfälle (Ausfallarten)
- Bewerten der Ausfälle (abhängig von der Funktion der Komponente im Gesamtsystem) in gefährlich / ungefährlich
- Nachweis der Beherrschung (Ausschluss) gefährlicher Ausfälle
- Voraussetzung: sicherer Abschaltzustand existiert
- Beispiel: Gleisstromkreis (Ruhestromprinzip)

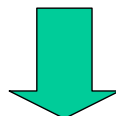
9f Fail-Safe versus Risikobetrachtung

Fail safe: deterministisch



Risiko: probabilistisch

- Gibt es fail-safe überhaupt? Wie groß ist die Wahrscheinlichkeit, dass Fail-Safe nicht funktioniert (besonderes bei reactive fail-safety und Mehrkanaligkeit)?



In den meisten Fällen gibt es das reine fail-safe nicht. Da man Überwachungssysteme oder mehrkanalige Systeme hat mit den o.g. Problemen, verbleibt ein gewisses Risiko.

Deshalb: Risikobetrachtung ist immer nötig. Vor der leichtfertigen Verwendung des Begriffes „Fail-Safe“ wird gewarnt.

10 Zusammenfassung

- Eine saubere Unterscheidung der Begriffe und Sicherheitsprinzipien ist notwendig
- Ermittlung der sicheren Systemzustände
- Prozess analysieren und geeignete Sicherheitsprinzipien identifizieren
- Identifizierung der möglichen Ausfallarten
- Klar unterscheiden, wogegen die geplanten Sicherheitsmaßnahmen wirken sollen und ob sie das leisten können

Danke für Ihre Aufmerksamkeit