Grundlagen der funktionalen Sicherheit

Funktionale Sicherheit – Entwicklung sicherer mechatronischer Produkte

18. November 2010, Stuttgart

Dipl.-Ing. Christoph Maier

Wiss. Mitarbeiter Produkt- und Qualitätsmanagement

Telefon: +49(0)711/9 70-1741
Fax: +49(0)711/9 70-1002
E-Mail: christoph.maier@ipa.fraunhofer.de
Internet: www.ipa.fraunhofer.de

Fraunhofer IPA

Vortragsinhalte

- Grundlagen funktionaler Sicherheit
- Unterschiede zwischen IEC 61508 und ISO DIS 26262
- Risikoanalyse und (A)SIL- Einstufung
- Software-Testing
- Fazit

Fraunhofer

GRUNDLAGEN DER FUNKTIONALEN SICHERHEIT

Fraunhofer

Definition der funktionalen Sicherheit aus der Sicht der Norm

- Aus der **DIN EN 61508**
  - **Sicherheit**: Freiheit von unvertretbaren Risiken der physischen Verletzung oder Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt als ein Ergebnis von Schäden an Gütern oder der Umwelt.
  - **Funktionale Sicherheit:** Teil der Gesamtsicherheit, der davon abhängig ist, ob ein System oder ein Betriebsmittel korrekte Antworten auf seine Eingangszustände liefert.
- Aus der **ISO DIS 26262**
  - **Funktionale Sicherheit:** Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems.

Fraunhofer

Beispiele zur „Funktionalen Sicherheit“

Beispiele aus der Realität:

- Renault ruft 2010 weltweit 695.000 Scénic zurück
  - Bei diesem Modell kann es laut Renault zu einem unbeabsichtigten Anziehen der automatischen Parkbremse während der Fahrt kommen.
    Quelle: www.welt.de

- Toyota ruft 2010 373.000 Autos zurück
  - Rückrufaktion auf Grund der Möglichkeit, dass während der Fahrt das Lenkradschloss selbsttätig einrastet. Damit ist das Lenken des Fahrzeugs nicht mehr möglich.
    Quelle: http://www.auto-motor-und-sport.de/

Quelle: www.motor-talk.de/

Fraunhofer

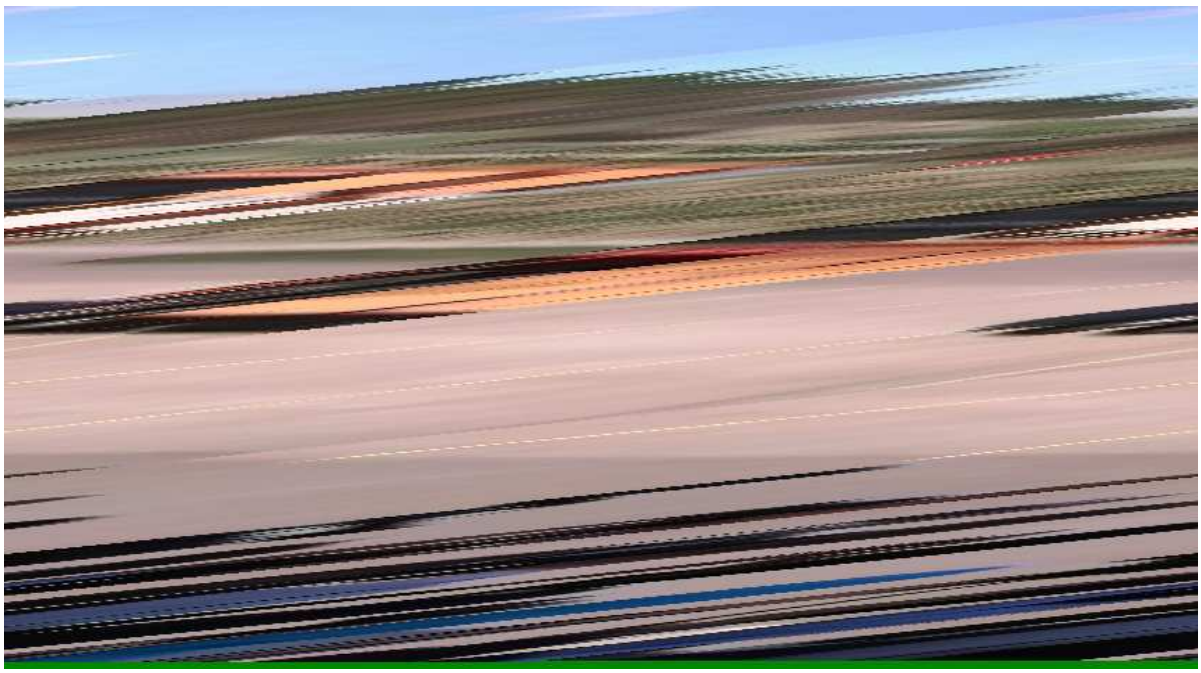
Beispiele zur „Funktionalen Sicherheit“

Beispiele aus der Realität:

- „Volvo-City- Safety“ versagt 2010 bei Pressevorführung
  - Das City-Safety-System soll Hindernisse wie Gegenstände auf der Straße oder Fußgänger erkennen und automatisch das Auto abbremsen, um einen Zusammenstoß zu verhindern.
  - Wie der Autohersteller später angab, war eine nicht funktionierende Batterie schuld am Ausfall des Systems.
    Quelle: www.auto.de

Fraunhofer

„Volvo-City- Safety“ - Pressevorführung



Fraunhofer

„Volvo-City- Safety“ - Funktionsfähig

Fraunhofer

Definition der funktionalen Sicherheit

- **Funktionale Sicherheit** ist die **Fähigkeit eines** elektrischen, elektronischen bzw. programmierbar elektronischen Systems (**E/E/PE-System**) beim **Auftreten**
  - **zufälliger** und/oder
  - **systematischer Ausfälle/Fehler**
  - mit **gefahrbringender Wirkung**

  im **sicheren Zustand** zu **bleiben** bzw. einen **sicheren Zustand einzunehmen.**
- **Ziel der funktionalen Sicherheit**
  - Vermeidung von Personenschäden (1. Priorität)
- **Nebeneffekt**
  - Reduktion/Vermeidung von Maschinen-/Vermögensschäden (2. Priorität)

Scope der ISO DIS 26262 und der IEC 61508

- Geltungsbereich der ISO DIS 26262
  - PKW bis 3,5 Tonnen
  - E/E-Systeme
  - PKWs, die in Serie produziert werden
- Nicht gültig
  - Sonderfahrzeuge (Fahrzeuge für Personen mit Behinderungen)
  - LKW, Pick-ups/Kleintransporter, Motorräder…
  - PE-Systeme

  → Hier gilt die IEC 61508

Scope der ISO DIS 26262 und der IEC 61508

- Welche Norm gilt hier?

Quelle: www.teczilla.de

Fraunhofer

Fault vs. Failure - ISO DIS 26262

Definition aus der ISO DIS 26262

- Fault/Abweichung
  - „abnormal condition that can cause an element or an item to fail"
  - „abnormaler Zustand, der das Versagen eines Elements oder eines ganzen Systems verursachen kann"
- Failure/Fehler
  - „termination of the ability of an element or an item to perform a function as required"
  - „ein Element oder ein ganzes System verliert die Fähigkeit, eine Funktion so auszuführen, wie es verlangt wird"

Ein Fault/eine Abweichung führt zu einem Failure/Fehler

Fraunhofer

Begriffe der funktionalen Sicherheit

- **Sicherheitsfunktion**

  Funktion eines sicherheitsbezogenen Systems, um im Fall einer Gefahr einen Zustand mit tolerierbarem Restrisiko einzunehmen oder aufrecht zu erhalten.

- **Sicherheitsintegrität**

  „Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraums anforderungsgemäß ausführt“. [DIN EN 61508-4]

- **Sicherheits-Integritätslevel (A)SIL**

  Vier diskrete Stufen zur Festlegung von Anforderungen für die Sicherheitsintegrität der Sicherheitsfunktionen (SIL1 bis SIL4 bei IEC 61508 bzw. ASIL A bis ASIL D bei ISO DIS 26262).

Zufälliger vs. Systematischer Fehler

Zufälliger Fehler

- Fehler/Ausfall, der zu einem zufälligen Zeitpunkt auftritt und keine klare/eindeutige Ursache aufweist
  - Ursache **nicht eindeutig** identifizierbar
    - → Fehlerbeherrschung
      - Bauteilversagen (Widerstand, Kondensator …)
      - Bit-Kipper im RAM

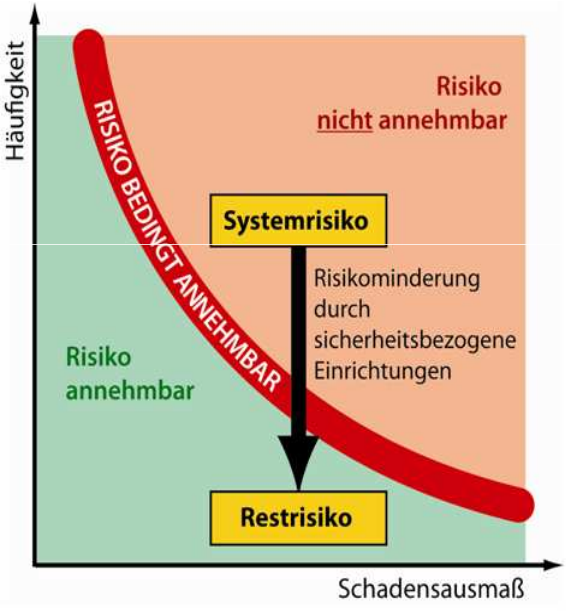
Systematischer Fehler

- Fehler/Ausfall mit klarer/eindeutiger Ursache
  - Ursache **eindeutig** identifizierbar
    - → Fehlervermeidung/Fehlerbeherrschung durch
      - Veränderung des Designs
      - Fertigungsprozessänderung

Voraussetzungen für funktional sichere Produkte

Fraunhofer

Grundprinzip der funktionalen Sicherheit: „Risikominderung“



Fraunhofer

Was ist funktionale Sicherheit?

- **Nicht** bloßes **Erreichen** der **geforderten Grenzwerte**
  - Warum nur 99% Sicherheit, wenn man für ein paar Cent mehr 100% Sicherheit erreichen kann?
- **Aktive Sicherheitsmaßnamen**
- **Passive Sicherheitsmaßnahmen einbeziehen**
  - Positionierung von Tastern/Schaltern
    - Vertikal vs. horizontal
  - Sicherheitsorientierte Auslegung der Taster/Schalter-Funktion
    - Ziehen von Taster schließt Fenster
    - Drücken von Taster öffnet Fenster

SOFTWARE IN MECHATRONISCHEN SYSTEMEN

Charakteristika von Software im mechatronischen System

Die Software / Steuerung muss

- das System in allen Systemzuständen sicher steuern.
- das System in allen Systemzuständen beim Auftreten von Fehlfunktionen in einen sicheren Zustand überführen.
- relevante Fehlfunktionen und unplausible Zustände dem Benutzer melden.

Die Software / Steuerung muss mit Hilfe von Sensoren und Algorithmen

- Fehlfunktionen an den Systemkomponenten erkennen.
- Fehlfunktionen und unplausible Zustände an den Informations-schnittstellen erkennen.
- Fehlfunktionen im Diagnosesystemen erkennen (kann ich meinem Diagnosesystem noch trauen?).

Testen von Software

Software /Steuerung muss getestet werden.

- Gezielte Simulation eines Bauteil-Ausfalls (zufälliger Fehler)
  - auf der Schaltung (invasiver Eingriff)
    - einen Widerstand überbrücken (Kurzschluss)
    - einen Widerstand auslöten (unendlich großer Widerstand)
    - einen Sensor deaktivieren (Stuck at „0“)
    - einen Sensor dauerhaft auf „an“ schalten (Stuck at „1“)

→Prüfen, ob die Software korrekt reagiert bzw. der Fehler erkannt wird.

ERMITTLUNG DES (AUTOMOTIVE) SAFETY INTEGRITY LEVELS

Fraunhofer

Risikograph zur SIL-Klassifizierung gemäß IEC 61508

Severity S	Aufenthaltsdauer F	Gefahrenabwendung P	W1	W2	W3
S1	F1	P1	-	-	-
		P2	-	-	-
	F2	P1	-	-	-
		P2	-	-	-
S2	F1	P1	-	-	1
		P2	-	1	1
	F2	P1	1	1	2
		P2	1	2	3
S3	F1	P1	2	3	3
		P2	2	3	3
	F2	P1	3	3	4
		P2	3	3	4
S4	F1	P1	3	4	4
		P2	3	4	4
	F2	P1	3	4	4
		P2	3	4	4

[nach ISO DIS 26262]

Zielsetzung:

- Systematische Ermittlung des SIL-Levels auf Basis der Gefahren- und Risikoanalyse.

Methodisches Vorgehen:

- Bestimmung des SIL-Levels anhand
  - des Schadensausmaßes
  - der Aufenthaltsdauer im Gefahrenbereich
  - der Möglichkeit zur Gefahrenabwendung
  - der Wahrscheinlichkeit des unerwünschten Ereignisses

Nutzen/Anmerkung:

- Systematisches und nachvollziehbares Vorgehen

Fraunhofer

Risikograph zur SIL-Klassifizierung nach IEC 61508

Schadensausmaß S	Aufenthaltsdauer F	Gefahrenabwendung P	W1	W2	W3
S1	F1	P1	-	-	-
		P2	-	-	-
	F2	P1	-	-	-
		P2	-	-	-
S2	F1	P1	-	-	1
		P2	-	1	1
	F2	P1	1	1	2
		P2	1	2	3
S3	F1	P1	2	3	3
		P2	2	3	3
	F2	P1	3	3	4
		P2	3	3	4
S4	F1	P1	3	4	4
		P2	3	4	4
	F2	P1	3	4	4
		P2	3	4	4

[nach IEC 61508]

Schadensausmaß
S1: **leichte Verletzung** einer Person**; kleinere** schädliche **Umwelteinflüsse**
S2: **schwere irreversible Verletzung** einer oder mehrerer Personen oder **Tod** einer **Person; vorübergehende größere** schädliche **Umwelteinflüsse**
S3: **Tod mehrerer Personen; langandauernde größere** schädliche **Umwelteinflüsse**
S4: **katastrophale Auswirkungen, sehr viele Tote**
Aufenthaltsdauer von Personen
F1: **selten bis öfter**
F2: **häufig bis dauernd**
Gefahrenabwendung
P1: **möglich unter bestimmten Bedingungen**
P2: **kaum möglich**
Wahrscheinlichkeit des unerwünschten Ereignisses
W1: **eher unwahrscheinlich**
W2: **möglich**
W3: **sehr wahrscheinlich**

[nach IEC 61508 – 5]

Fraunhofer

Möglicher Risikograph gemäß IEC 61508

Fehlfunktionen und Auswirkungen aus der Gefahren- und Risikoanalyse

Severity S	Aufenthaltsdauer F	Gefahrenabwendung P	W1	W2	W3
S1	F1	P1	-	-	-
		P2	-	-	-
	F2	P1	-	-	-
		P2	-	-	-
S2	F1	P1	-	-	1
		P2	-	1	1
	F2	P1	1	1	2
		P2	1	2	3
S3	F1	P1	2	3	3
		P2	2	3	3
	F2	P1	3	3	4
		P2	3	3	4
S4	F1	P1	3	4	4
		P2	3	4	4
	F2	P1	3	4	4
		P2	3	4	4

Severity – S:
S2: Schwere Verletzungen, lebensbedrohlich, Überleben wahrscheinlich

Aufenthaltsdauer– F:
F2: Häufige Aufenthaltsdauer

Gefahrenabwendung– P:
P2: Gefahrenabwendung kaum möglich

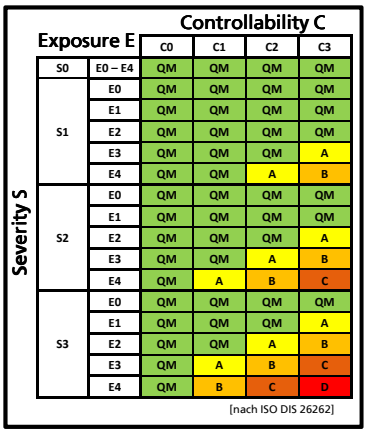
Auftreten– W:
W2: Auftreten möglich

SIL 2

ASIL C – PFH:
$>10^{-7}$ bis $<10^{-6}$

Fraunhofer

Risikograph zur ASIL-Klassifizierung nach ISO DIS 26262



Severity S	Exposure E	Controllability C: C0	C1	C2	C3
S0	E0 – E4	QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
S3	E0	QM	QM	QM	QM
	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

[nach ISO DIS 26262]

Zielsetzung:

- Systematische Ermittlung des ASIL-Levels auf Basis der Gefahren- und Risikoanalyse

Methodisches Vorgehen:

- Bestimmung des ASIL-Levels anhand
  - der Schwere (Severity)
  - der Häufigkeit des Ausgesetztseins (Exposure)
  - der Kontrollierbarkeit (Controllability)

Nutzen/Anmerkung:

- Systematisches und nachvollziehbares Vorgehen

Fraunhofer

Risikograph zur ASIL-Klassifizierung nach ISO DIS 26262

Severity S	Exposure E	Controllability C: C0	C1	C2	C3
S0	E0 – E4	QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
S3	E0	QM	QM	QM	QM
	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

[nach ISO DIS 26262]

Schwere (Severity)

S0: **keine** Verletzungsgefahr
S1: **geringe** und **mäßige** Verletzungen
S2: **ernste** und **möglicherweise tödliche** Verletzungen
S3: **schwere** und **wahrscheinlich tödliche** Verletzungen

Häufigkeit des Ausgesetztseins (Exposure)

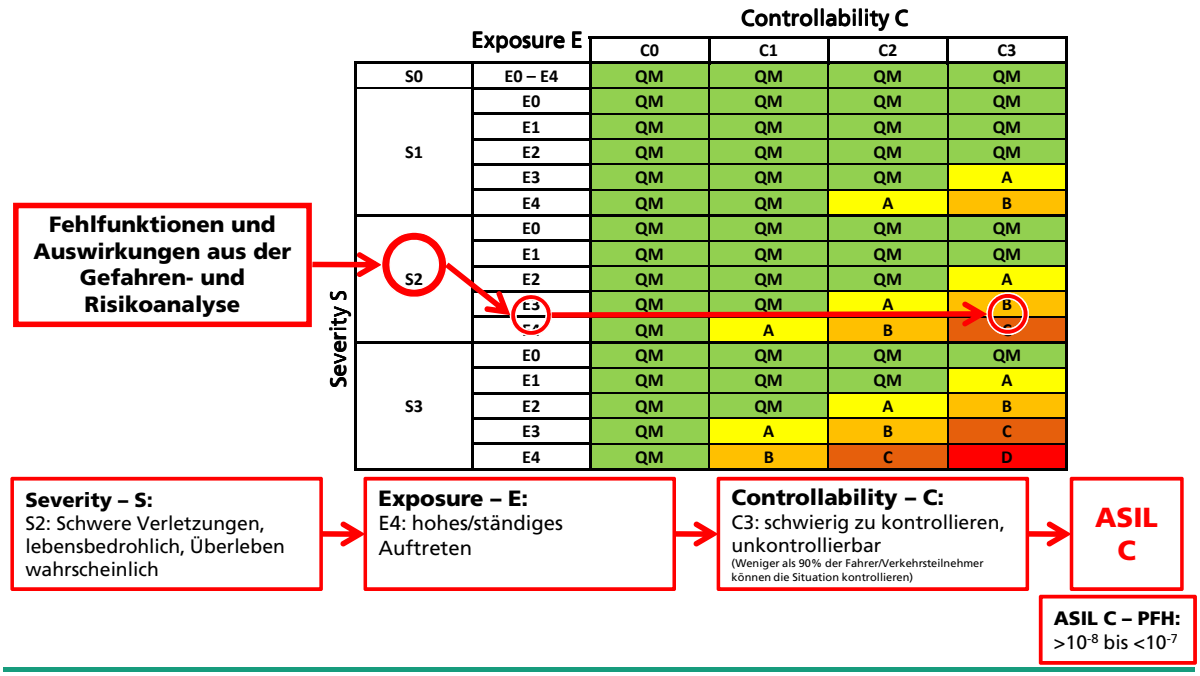
E1: **selten:** Situation tritt für die meisten Fahrer seltener als einmal pro Jahr auf
E2: **gelegentlich:** Situation tritt für die meisten Fahrer wenige Male pro Jahr auf
E3: **ziemlich oft:** Situation tritt für Durchschnittsfahrer einmal im Monat oder öfter auf
E4: **oft:** Situation, die bei nahezu jeder Fahrt auftritt

Kontrollierbarkeit (Controllability)

C1: **einfach kontrollierbar:** mehr als 99% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden
C2: **durchschnittlich kontrollierbar**: mehr als 90% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden
C3: **schwierig kontrollierbar oder unkontrollierbar**: weniger als 90% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden

Fraunhofer

Möglicher Risikograph gemäß ISO/DIS 26262



Fraunhofer

Unfallkategorien

UK 1: Unfall mit Getöteten

- Als Getöteter gilt ein Verunglückter, der innerhalb von 30 Tagen nach einem Verkehrsunfall an den Unfallfolgen verstirbt.

UK 2: Unfall mit Schwerverletzten

- Als Schwerverletzter gilt ein Verunglückter, bei dem durch die Unfalleinwirkung ein Krankenhausaufenthalt von mehr als 24 Stunden erforderlich war und der 30 Tage nach dem Unfall noch am Leben war.

UK 3: Unfall mit Leichtverletzten

- Als Leichtverletzter gilt ein Verunglückter, bei dem durch die Unfalleinwirkung ärztliche Behandlung oder ein Krankenhausaufenthalt von unter 24 Stunden erforderlich war.

Quelle: www.wikipedia.de

Fraunhofer

VORGABEWERTE AUS DER ISO DIS 26262 BZW. IEC 61508

Fraunhofer

Vorgabewerte der IEC 61508 in Abhängigkeit vom SIL

Sicherheits-Integritätslevel SIL	**Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung** (Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

Anteil ungefährlicher Ausfälle	**Fehlertoleranz der Hardware (siehe Anmerkung 2)**		
	0	**1**	**2**
< 60 %	nicht erlaubt	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4
ANMERKUNG 1 Siehe 7.4.3.1.1 bis 7.4.3.1.4 zu Einzelheiten bezüglich der Interpretation dieser Tabelle.			
ANMERKUNG 2 Eine Fehlertoleranz der Hardware von N bedeutet, dass N + 1 Fehler zu einem Verlust der Sicherheitsfunktion führen können.			

[nach IEC 61508]

Fraunhofer

Vorgabewerte ISO DIS 26262 in Abhängigkeit vom ASIL

Automotive Safety Integrity Level – ASIL	**Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung** (PFH – Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
D	$< 10^{-8}$
C	$< 10^{-7}$
B	$< 10^{-7}$
A	$< 10^{-6}$

Metrik	**ASIL A**	**ASIL B**	**ASIL C**	**ASIL D**
Single point faults metric	Nicht relevant	>90%	>97%	>99%
Latent faults metric	Nicht relevant	>60%	>80%	>90%

[Quelle: ISO DIS 26262]

Fraunhofer

UNTERTEILUNG DER MÖGLICHEN FEHLERARTEN

Fraunhofer

Verschiedene Fault-Arten

Definition aus der ISO DIS 26262

- **Single point fault**: fault in an element that is not covered by a safety mechanism and that leads directly to the violation of a safety goal.
  - „Abweichung in einem Element, welche durch keinen Sicherheitsmechanismus abgedeckt ist und direkt zur Verletzung eines Sicherheitsziels führt."
- **Residual fault:** portion of a fault that by itself leads to the violation of a safety goal, occurring in a hardware element, where that portion of the fault is not covered by safety mechanisms.
  - „Der Anteil einer Abweichung, der in einem Hardware Element auftritt und zu einer Verletzung eines Sicherheitsziels führt, wobei dieser Anteil der Abweichung durch keine Sicherheitsmechanismen abgedeckt ist."

Verschiedene Fault-Arten

Definition aus der ISO DIS 26262

- **Safe fault:** fault whose occurrence will not significantly increase the probability of violation of a safety goal.
  - „Abweichung, deren Auftreten unwesentlich die Wahrscheinlichkeit der Verletzung eines Sicherheitsziels erhöht."
- **Latent fault:** multiple point fault whose presence is not detected by a safety mechanism nor perceived by the driver within the multiple point fault detection interval.
  - „ Eine Einzelabweichung, deren Eintritt nicht innerhalb des Multiple point fault-Entdeckungsintervalls von den Sicherheitsmechanismen detektiert oder vom Fahrer wahrgenommen wurde."

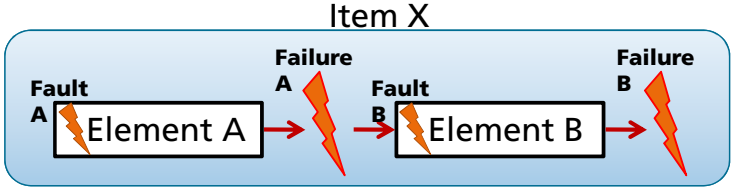
Verschiedene Fault-Arten

Definition aus der ISO DIS 26262

- **Dual point fault:** individual fault that, in combination with another independent fault, leads to a dual point failure.
  - „Eine Einzelabweichung, die in Verbindung mit einer weiteren, unabhängigen Abweichung zu einem Dual Point Failure führt."
- **Multiple point fault:** individual fault that, in combination with other independent faults, leads to a multiple point failure.
  - „Eine Einzelabweichung, die in Verbindung mit mehreren weiteren, unabhängigen Abweichungen zu einem Multiple Point Failure führt."

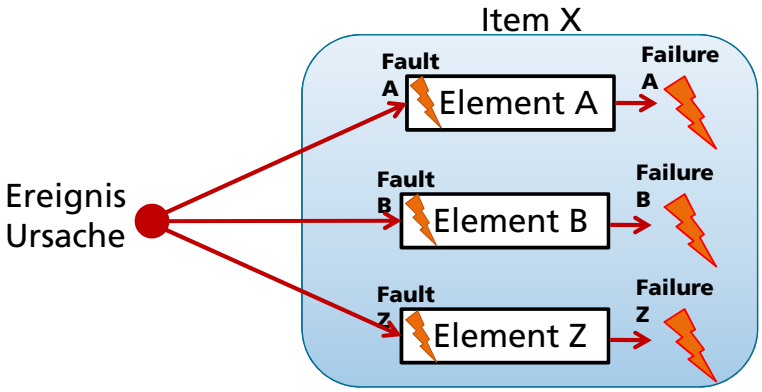
Fehlerarten im betrachteten System

- **Cascading failure**
  - Die Fehlfunktion/Abweichung A eines Elements/Bauteils in dem System/Produkt X führt zu einem Fehler A der zu einer Fehlfunktion/Abweichung B führt. Daraus resultiert im selben System/Produkt X ein Fehler B.



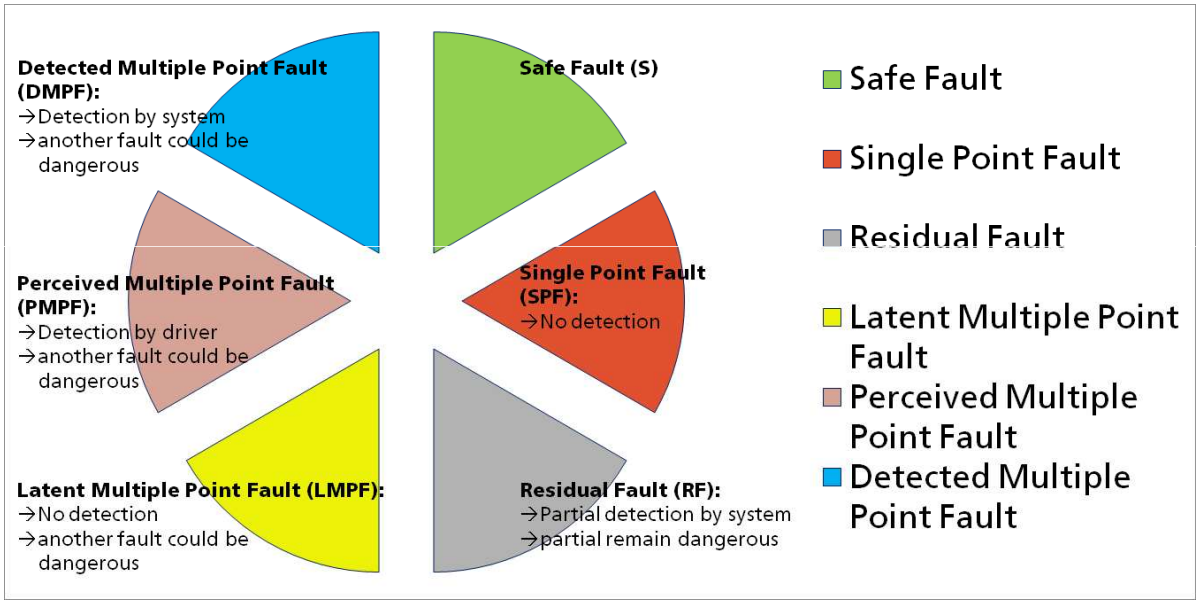
Fehlerarten im betrachteten System

- **Common cause failure (CCF)**
  - Das Auftreten eines Ereignisses/einer Ursache („root cause“) führt dazu, dass zwei oder mehr Elemente/Bauteile Abweichungen aufweisen. Diese Abweichungen führen ihrerseits zu zwei oder mehr Fehlern.



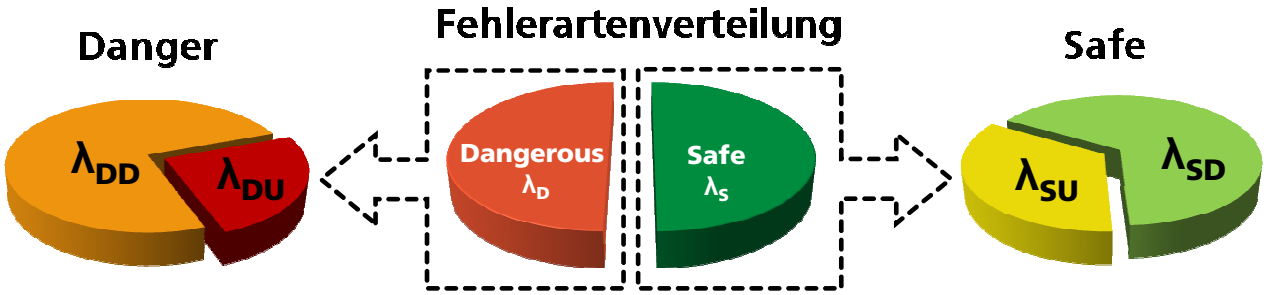
Fraunhofer

Unterteilung der verschiedenen Fehlerarten gemäß ISO DIS 26262



Fraunhofer

Unterteilung der verschiedenen Fehlerarten gemäß IEC 61508



Abkürzung und Formel	Bedeutung
DC	Diagnostic coverage – Diagnosedeckungsgrad (0-100%)
$\lambda_S = \lambda_{SD} + \lambda_{SU}$	Sichere Fehler
$\lambda_{SD} = \lambda_S * DC$	Sicherer Fehler, der entdeckt werden kann (SD = Safe Detected)
λ_{SU}	Sicherer Fehler, der nicht entdeckt werden kann (SU = Safe Undetected)
$\lambda_D = \lambda_{DD} + \lambda_{DU}$	Gefährlicher Fehler
$\lambda_{DD} = \lambda_D * DC$	Gefährlicher Fehler, der entdeckt werden kann (DD = Dangerous Detected)
λ_{DU}	Gefährlicher Fehler, der nicht entdeckt werden kann (DU = Dangerous Undetected)

Fraunhofer

FAZIT

Fraunhofer

Fazit

Bewertung

Funktionale Sicherheit stellt eine neue Herausforderung an das technische Risikomanagement dar (von Industrie geschätzter Mehraufwand: 10-20%).

Voraussetzungen zur Sicherstellung der funktionalen Sicherheit sind

- Funktionierende Managementsysteme (z.B. TS 16949, SPICE, CMMI)
- Organisatorische Erweiterungen für das Safety Management entsprechend den Anforderungen der IEC 61508 bzw. ISO DIS 26262
- Detaillierte und präzise Systemanalysen über den Produktlebenszyklus durch den OEM sowie Weitergabe der Anforderungen an die Lieferanten
- Integrierte Anwendung vorhandener technischer Risikoanalysen
- Kritische Betrachtung der Risiken unabhängig von Zahlenwerten

Fraunhofer

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

© Fraunhofer

Fraunhofer