GRUNDLAGEN DER FUNKTIONALEN SICHERHEIT

Workshop - Methoden der Produktentwicklung

25. 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
- Software in mechatronischen Systemen
- Risikoanalyse und (A)SIL- Einstufung
- Methoden und Werkzeuge der Funktionalen Sicherheit
- 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

Fraunhofer

„Volvo-City- Safety“

Fraunhofer

„Volvo-City- Safety“ - Pressevorführung

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)

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

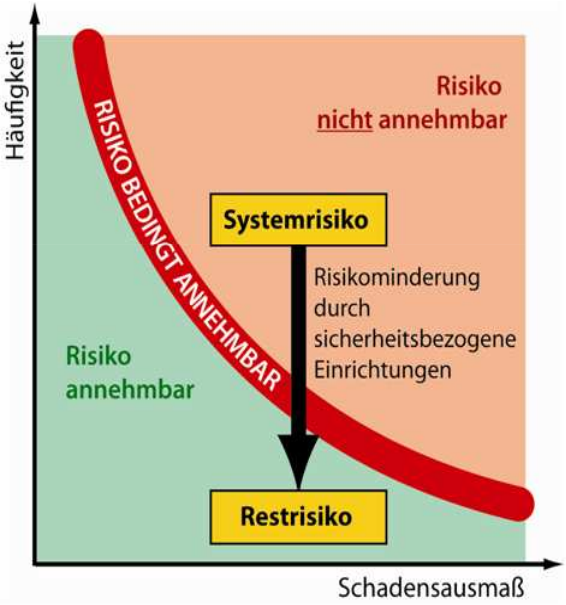
- Fehler/Ausfall mit klarer/eindeutiger Ursache
  - Ursache **eindeutig** identifizierbar
    - → Fehlervermeidung/Fehlerbeherrschung durch
      - Veränderung des Designs
      - Fertigungsprozessänderung

Fraunhofer

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

Fraunhofer

SOFTWARE IN MECHATRONISCHEN SYSTEMEN

Fraunhofer

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?).

Fraunhofer

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.

Fraunhofer

ERMITTLUNG DES (AUTOMOTIVE) SAFETY INTEGRITY LEVELS

Fraunhofer

Risikograph 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

Wahrscheinlichkeit W

[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

Wahrscheinlichkeit W

[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**

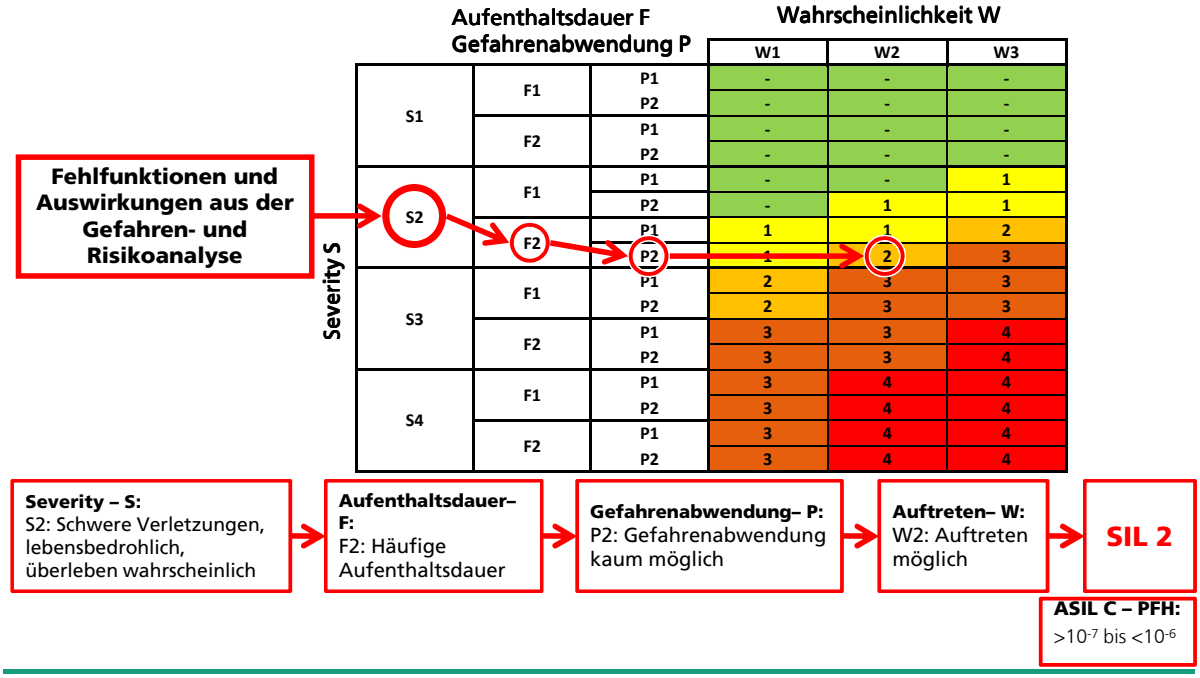
W2: **möglich**

W3: **sehr wahrscheinlich**

[nach IEC 61508 – 5]

Fraunhofer

Möglicher Risikograph gemäß ISO DIS 26262



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

Exposure E Controllability C

Severity S		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

Fehlfunktionen und Auswirkungen aus der Gefahren- und Risikoanalyse

Controllability C / Exposure E / Severity S

Severity S	Exposure E	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

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

Exposure – E:
E4: hohes/ständiges Auftreten

Controllability – C:
C3: schwierig zu kontrollieren, unkontrollierbar
(Weniger als 90% der Fahrer/Verkehrsteilnehmer können die Situation kontrollieren)

ASIL C

ASIL C – PFH:
$>10^{-8}$ bis $<10^{-7}$

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

VORGABEWERTE AUS DER ISO DIS 26262 BZW. DER IEC 61508

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%

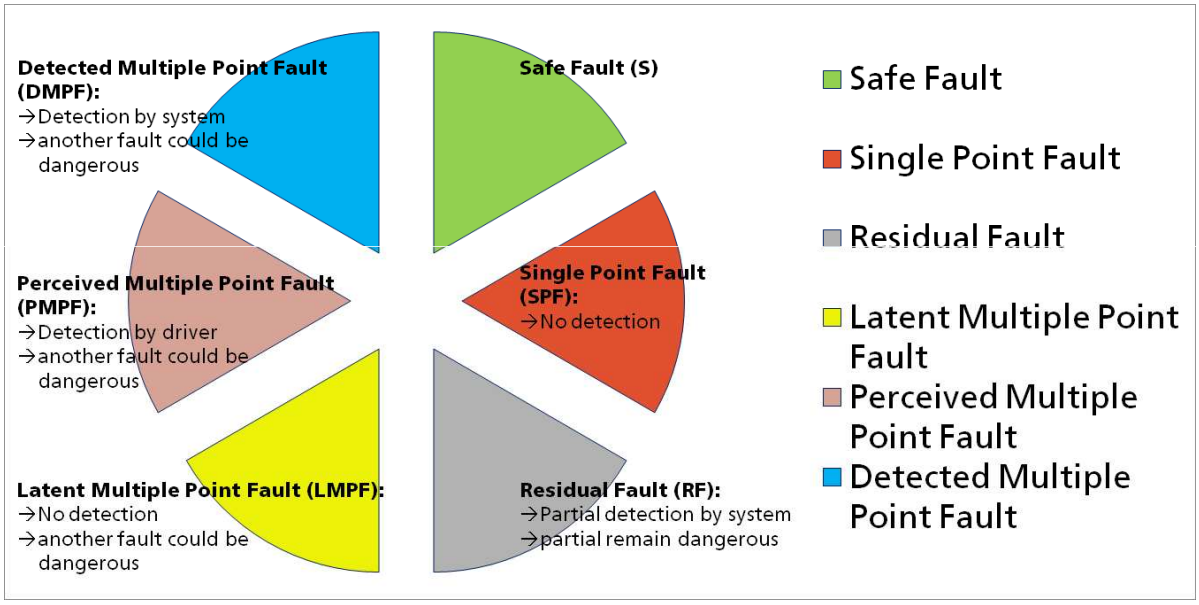
[Quelle: ISO DIS 26262]

Fraunhofer

UNTERTEILUNG DER MÖGLICHEN FEHLERARTEN

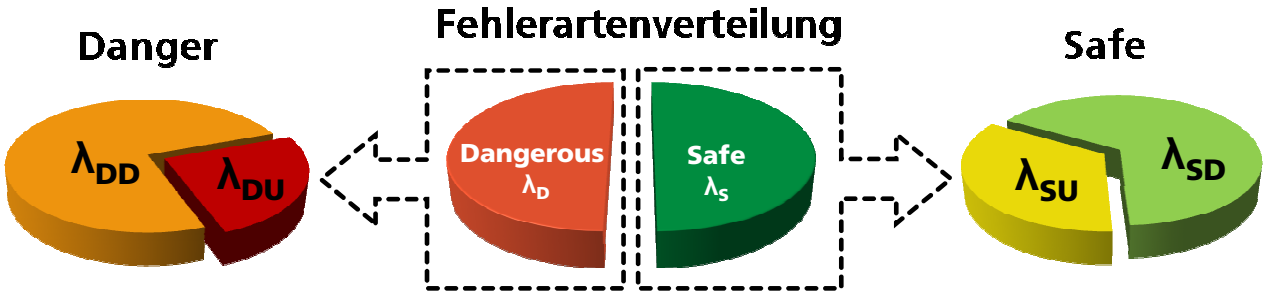
Fraunhofer

Unterteilung der verschiedenen Fehlerarten gemäß ISO DIS 26262



Fraunhofer

Unterteilung der verschiedenen Fehlerarten gemäß IEC 61508



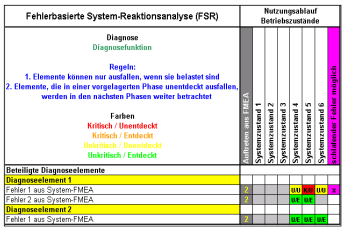
Abkürzung und Formel	Bedeutung
DC	Diagnostic coverage – Diagnosedeckungsgrad (0-100%)
$\lambda_S = \lambda_{SD} + \lambda_{SU}$	Sichere Fehler
$\lambda_{SD} = \lambda_S * DC$	Sicherer Fehler, der entdeckt werden kann (SD = Safe Detected)
λ_{SU}	Sicherer Fehler, der nicht entdeckt werden kann (SU = Safe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

METHODEN UND WERKZEUGE DER FUNKTIONALEN SICHERHEIT

Fraunhofer

Fehlerbasierte System-Reaktionsanalyse (FSR)



Zielsetzung:

- Analyse der Diagnose- und Absicherungsmaßnahmen auf systematische Fehler

Methode:

- Übernahme der Fehlfunktionen aus der System-FMEA für alle beteiligten Komponenten
- Bewertung der Entdeckbarkeit von Ausfallarten unter Berücksichtigung von nutzerbedingten Interaktionen und Systemzuständen

Nutzen/Anmerkung:

- Hinweise auf „schlafende Fehler“ im System
- Kompakte Darstellung komplexer Systeme

Fraunhofer

Paarvergleichsmatrix für schlafende Fehler

	Fehlfunktion 1	Fehlfunktion 2	Fehlfunktion 3	Fehlfunktion 4	Fehlfunktion 5	Fehlfunktion 6
Fehlfunktion 1						
Fehlfunktion 2						
Fehlfunktion 3						
Fehlfunktion 4						
Fehlfunktion 5						
Fehlfunktion 6						

Zielsetzung:

- Bewertung des Risikos schlafender Fehler unter Berücksichtigung des zeitlichen Auftretens

Methode:

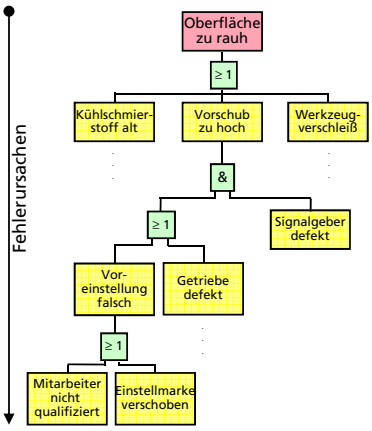
- Gegenüberstellung schlafender Fehler in der Paarvergleichsmatrix
- Bewertung der Auswirkungen und Entdeckbarkeit in Abhängigkeit des zeitlichen Auftretens

Nutzen/Anmerkung:

- Hilfsmittel zur Entwicklung des Sicherheitskonzepts für zeitlich unabhängig auftretende Mehrfachfehler (latent und multiple faults)

Fraunhofer

Fehlerbaumanalyse (FTA)



$$\dot{H}_i(\propto) = \lambda_i(1 - U_i(\propto))$$

Zielsetzung:

- Ermittlung und Visualisierung aller Fehlerursachen, die zum unerwünschten Ereignis führen

Methode:

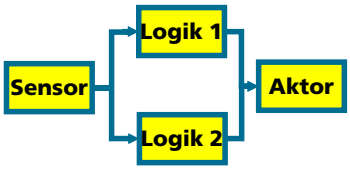
- Systemanalyse und Erstellung des Fehlerbaums
- Qualitative bzw. quantitative Auswertung des Fehlerbaums

Nutzen/Anmerkung:

- Visualisierung von Ausfällen und deren Zusammenhänge und Wahrscheinlichkeiten
- Beurteilung von Systemen und Produkten bzgl. Sicherheit und Zuverlässigkeit

Fraunhofer

Reliability Block Diagramm



Teilsysteme der Sicherheitsfunktion

Zielsetzung:

- Hilfsmittel zur Zerlegung der an der Sicherheitsfunktion beteiligten Teilsysteme

Methode:

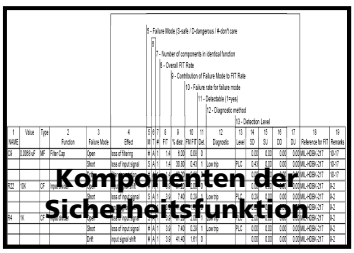
- Abbildung der an der Sicherheitsfunktion beteiligten Teilsysteme entsprechend der Architektur
  - Seriell
  - Parallel
  - Common cause

Nutzen/Anmerkung:

- Voraussetzung zur Berechnung der FuSi-Parameter (z.B. PFH, Fault-Metrik) in der FMEDA

Fraunhofer

Failure Modes, Effects and Diagnostic Analysis (FMEDA)



FMEDA

Zielsetzung:

- Analyse der Fehlermodi der an der Sicherheitsfunktion beteiligten Komponenten

Methode:

- Auflistung aller Fehlerarten der an der Sicherheitsfunktion beteiligten Komponenten
- Bewertung der Ausfälle in „Sichere Ausfälle“ und „Gefährliche Ausfälle“
- Ermittlung der Kennwerte λ, λ_S, λ_D, λ_{DD}, λ_{DU}

Nutzen/Anmerkung:

- Tabellarisches Verfahren zur Vorbereitung der Berechnung der FuSi-Parameter (z.B. PFH, SFF)

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
- Kritische Betrachtung der Risiken unabhängig von Zahlenwerten

Fraunhofer

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Fraunhofer