RISIKOABSICHERUNG VON MECHATRONISCHEN SYSTEMEN

Mit neuen Produkten schneller am Markt,
FpF-Veranstaltung, 1. Dezember 2011, 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

Funktionale Sicherheit
Pressevorführung - „Volvo-City-Safety“

Quelle: www.auto.de

Fraunhofer IPA

Funktionale Sicherheit
Beispiele aus der Realität zur „Funktionalen Sicherheit“

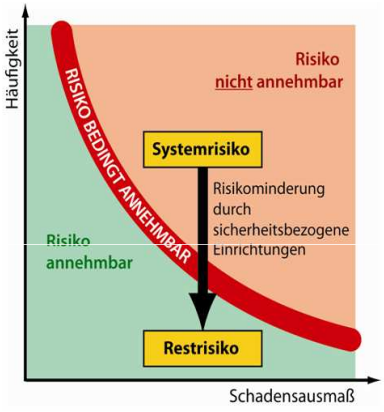
- „Volvo-City-Safety“ versagt 2010 bei Pressevorführung
  - Das City-Safety-System soll Hindernisse auf der Straße erkennen und das Auto automatisch abbremsen, um einen Zusammenstoß zu verhindern. Wie der Autohersteller später angab, war eine nicht funktionierende Batterie schuld am Ausfall des Systems.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

- 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 gezielt 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/

Fraunhofer IPA

Funktionale Sicherheit
Definition und Zielsetzung



Zielsetzung „Risikominderung“

Funktionale Sicherheit ist die Fähigkeit eines elektrischen, elektronischen od. programmierbar elektronischen Systems (E/E/PE-System), beim Auftreten

- systematischer Ausfälle,
  z.B. fehlerhafte Systemauslegung
- zufälliger Hardwareausfälle,
  z.B. Alterung von elektr(on)ischen Bauteilen

mit gefahrbringender Wirkung, einen sicheren Zustand einzunehmen bzw. in einem sicheren Zustand zu bleiben.

Fraunhofer IPA

Funktionale Sicherheit
Vortragsinhalte

- Entwicklung und Normen zur Funktionalen Sicherheit
- Aufbau und Anwendung der ISO 26262
- Risikographen zur ASIL-Klassifizierung
- Failure Modes und Hardware Metriken
- Methoden zur Funktionalen Sicherheit

Fraunhofer IPA

ENTWICKLUNG UND NORMEN ZUR FUNKTIONALEN SICHERHEIT

Fraunhofer IPA

Funktionale Sicherheit
Ursprung der Funktionalen Sicherheit

Chemieunfall in Seveso, Italien 1976:
Hochgiftiges Dioxin mit katastrophalen Folgen für Menschen, Tierwelt und Natur ausgetreten

- Unkontrollierte Reaktion führte zur Überhitzung
- Automatische Kühlsysteme und Warnanlagen waren nicht vorhanden

Unglück löste Normungsbestrebungen für funktionale Sicherheit aus:

- IEC 61508 (allgemein) – 1998/2000
- ISO 26262 (automotive) – 2011

Fraunhofer IPA

Funktionale Sicherheit
Scope der ISO/DIS 26262

- Geltungsbereich der ISO/DIS 26262
  - PKW bis 3,5 Tonnen
  - PKWs, die in Serie produziert werden
  - Elektrische und elektronische Systeme (E/E-Systeme)

- Nicht gültig (weiterhin Geltungsbereich der IEC 61508)
  - Fahrzeuge über 3,5 Tonnen (LKW)
  - Fahrzeuge, die keine PKW darstellen (z.B. Kleintransporter)
  - Sonderfahrzeuge (z.B. Fahrzeuge für Personen mit Behinderungen)

Fraunhofer IPA

BEGRIFFE UND ANFORDERUNG DER FUNKTIONALEN SICHERHEIT

Fraunhofer IPA

Funktionale Sicherheit
Begriffe der funktionalen Sicherheit

- Sicherheitsfunktion bzw. Funktionale Sicherheitsanforderung

  Funktion eines sicherheitsbezogenen Systems, um im Gefahrfall einen Zustand mit tolerierbarem Restrisiko einzunehmen / aufrecht zu erhalten
- Sicherheitsintegrität

  Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen anforderungsgemäß ausführt
- Automotive Sicherheits-Integritätslevel (A)SIL

  Vier diskrete Stufen zur Festlegung von Anforderungen für die Sicherheitsintegrität der Sicherheitsfunktionen
  - ASIL A bis ASIL D (ISO 26262)
  - SIL 1 bis SIL 4 (IEC 61508)

Fraunhofer IPA

Funktionale Sicherheit
Anforderungen der Norm(en)

Die Norm zur Funktionalen Sicherheit fordert:

- Maßnahmen zum Management der funktionalen Sicherheit
- Maßnahmen gegen systematische Ausfälle
- Maßnahmen gegen zufällige Hardwareausfälle
- Maßnahmen zur Beurteilung der Funktionalen Sicherheit

Fraunhofer IPA

METHODEN ZUR FUNKTIONALEN SICHERHEIT

Fraunhofer IPA

Methoden zur Funktionalen Sicherheit
Methodenübersicht

Methoden zur SIL-Klassifizierung

- Gefahren- und Risikoanalyse
- Risikograph

Methoden zur Analyse systematischer Fehler

- Fehlermöglichkeits- und Einflussanalyse (FMEA)
- Fehlerbasierte System-Reaktionsanalyse (FSR)

Methoden zur Analyse zufälliger Fehler

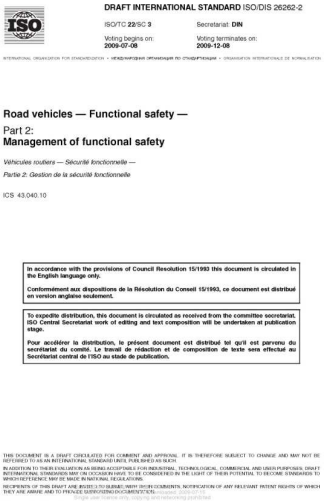
- Berechnungsalgorithmen und Vorgabewerte
- Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse (FMEDA)

Fraunhofer IPA

AUFBAU UND INHALTE DER ISO/DIS 26262

Fraunhofer IPA

ISO/DIS 26262
Aufbau der ISO/DIS 26262



DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-2

ISO/TC 22/SC 3 — Secretariat: DIN

Voting begins on: 2009-07-08 — Voting terminates on: 2009-12-08

Road vehicles — Functional safety —
Part 2:
Management of functional safety

Véhicules routiers — Sécurité fonctionnelle —
Partie 2: Gestion de la sécurité fonctionnelle

ICS 43.040.10

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.
IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.
RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

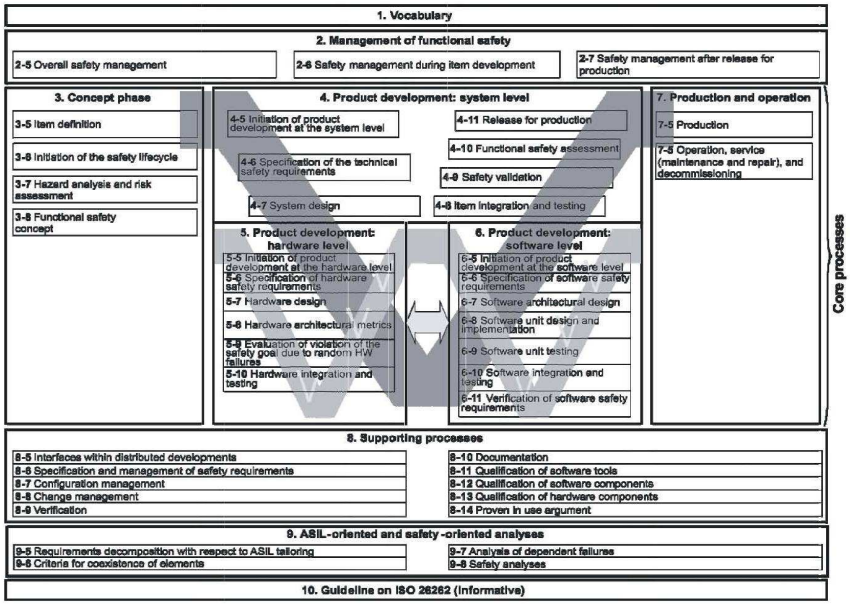
(insgesamt 381 Seiten)

1. Glossar
2. Management der funktionalen Sicherheit
3. Konzeptphase
4. Produktentwicklung: Systemebene
5. Produktentwicklung: Hardwareebene
6. Produktentwicklung: Softwareebene
7. Produktion und Betrieb
8. Unterstützende Prozesse
9. ASIL- und sicherheitsorientierte Analysen
10. Orientierungshilfen

Quelle: ISO/DIS 26262

Fraunhofer IPA

ISO/DIS 26262
Lebenszyklusmodell der ISO/DIS 26262

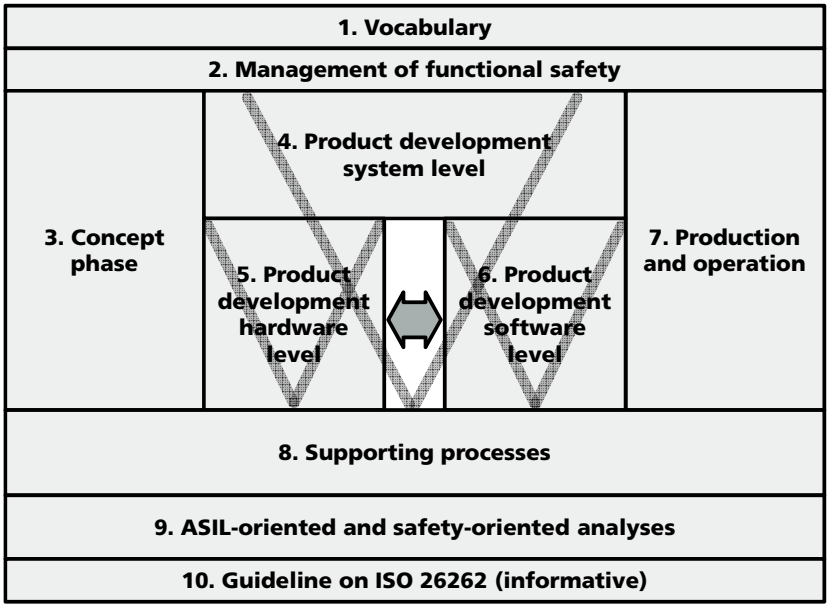


Quelle: ISO/DIS 26262

Fraunhofer IPA

ISO/DIS 26262

Lebenszyklusmodell der ISO/DIS 26262 (vereinfacht)



Quelle: ISO/DIS 26262

Fraunhofer IPA

ANFORDERUNGEN DER ISO/DIS 26262 (KAPITEL 2)

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-2

Definition der Anforderungen der für den Sicherheitslebenszyklus verantwortlichen Organisationen

- Sicherheitskultur
- Kompetenzen
- Qualitätsmanagement

Definition der Rollen, Verantwortlichkeiten und Tätigkeiten für das Sicherheitsmanagement während der Entwicklung der Einheit

- Sicherheitsmanager
- Projektmanager
- Audit, Review, Assessment der Sicherheitsaktivitäten

Quelle: ISO/DIS 26262-2

Fraunhofer IPA

ISO/DIS 26262
Management der Funktionalen Sicherheit (Safety plan)

Der Safety-Plan enthält die zur Sicherstellung der Funktionalen Sicherheit erforderliche Aufbau- und Ablaufplanung (Phasen, Meilensteine, Verantwortlichkeiten, Dokumente) hinsichtlich:

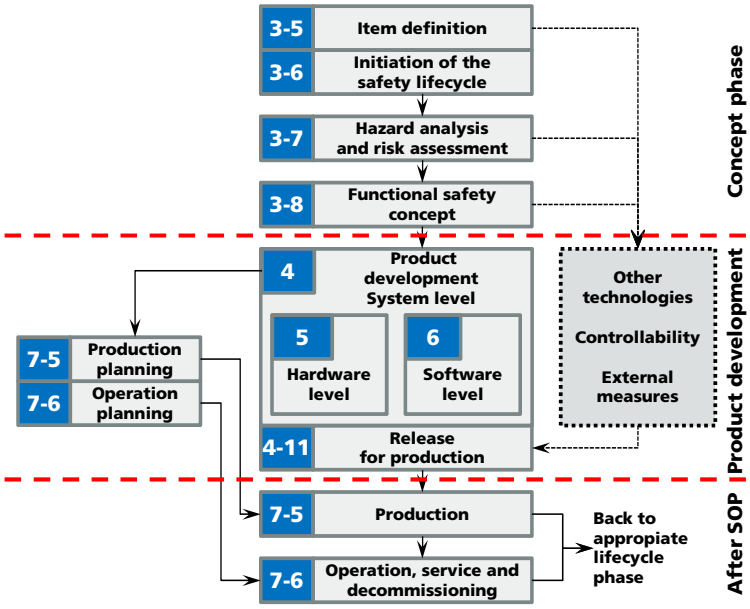
- Strategien und Aktivitäten
- Schnittstellenabstimmung mit Lieferanten
- Unterstützende Prozesse
- Gefahren- und Risikoanalyse
- Entwicklung und Umsetzung der Sicherheitsanforderungen
- Sicherheitsanalysen
- Verifikation und Validation
- Dokumente

Fraunhofer IPA

ANFORDERUNGEN DER ISO/DIS 26262 (KAPITEL 3)

Fraunhofer IPA

ISO/DIS 26262
Sicherheits-Lebenszyklus (safety lifecycle)



Quelle: ISO/DIS 26262-2

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-3
Hazard analysis and risk assessment

Identifizierung und Kategorisierung der Gefahren durch den Betrachtungsgegenstand

- Analyse der Betriebsbedingungen und Identifikation der Gefahren
  - Vollständige Auflistung der Betriebsbedingungen
  - Systematische Ableitung und Definition der Gefahren sowie Auswirkungen für alle Betriebsbedingungen
- Bewertung der Gefahren
  - S0-S3: Schwere der potentiellen Gefahr
  - E0-E4: Dauer des Ausgesetzseins in der Betriebssituation
  - C0-C3: Kontrollierbarkeit durch Fahrer und/oder Beteiligte
- Kategorisierung der Gefahren (ASIL)
  - ASIL A - D
  - QM

Quelle: ISO/DIS 26262-3

Fraunhofer IPA

Methoden zur Analyse mechatronischer Systeme
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

Beherrschbarkeit (Controllability)
- **C1:** **einfach beherrschbar:** mehr als 99% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden
- **C2:** **durchschnittlich beherrschbar** : mehr als 90% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden
- **C3:** **schwierig oder gar nicht beherrschbar** : weniger als 90% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden

Fraunhofer IPA

Erläuterung anhand eines Beispielsystems
Beispielsystem (Fahrzeug und Werte zufällig gewählt)

Quelle: http://www.imcdb.org

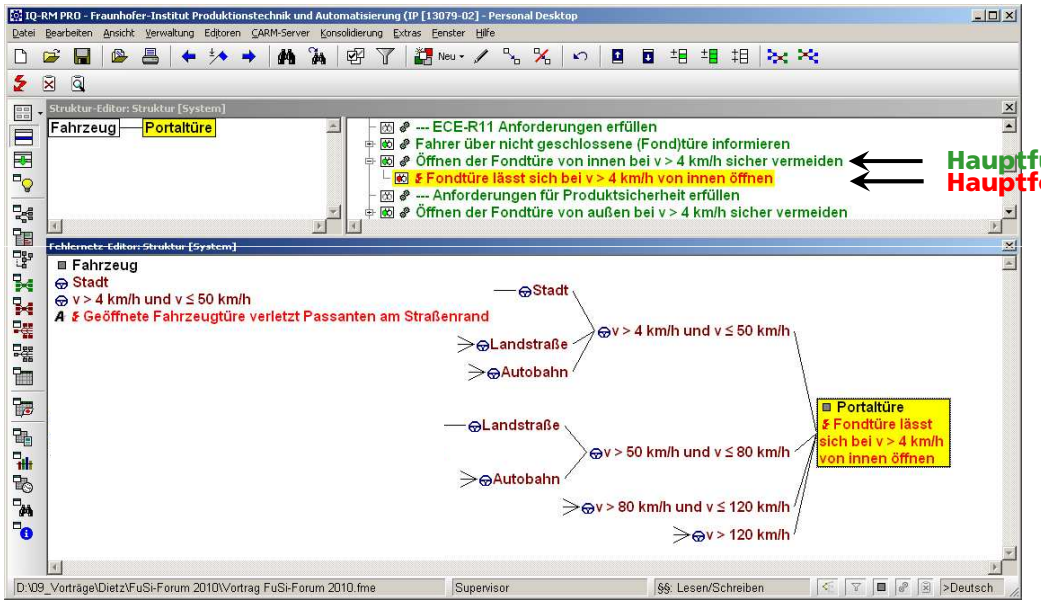
1965

Quelle: http://www.automobilrevue.de/detroit2002.htm

20xx ?

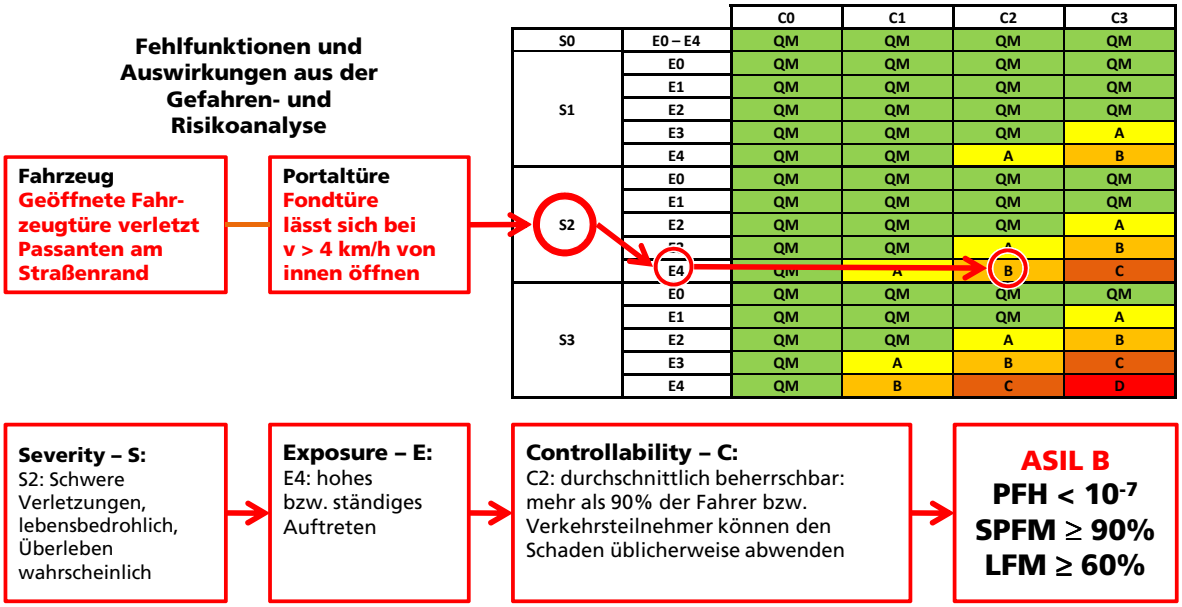
Fraunhofer IPA

Erläuterung anhand eines Beispielsystems
Gefahren- und Risikoanalyse



Fraunhofer IPA

Erläuterung anhand eines Beispielsystems
Möglicher Risikograph gemäß ISO/DIS 26262



		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
	[illegible]	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

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-3
Functional safety concept

Formulierung von Sicherheitszielen zur Vermeidung oder Abschwächung der Gefahren und Review des Schrittes

- Definition der Sicherheitsziele

Nachvollziehbare Ableitung und Spezifikation der funktionalen Sicherheitsanforderungen sowie Zuordnung zur Systemarchitektur

- Funktionale Sicherheitsanforderungen
- Zustandsbeschreibung
- Warn- und Degradationskonzept
- Notbetriebskonzept
- Reaktionskonzept durch Fahrer

Quelle: ISO/DIS 26262-3

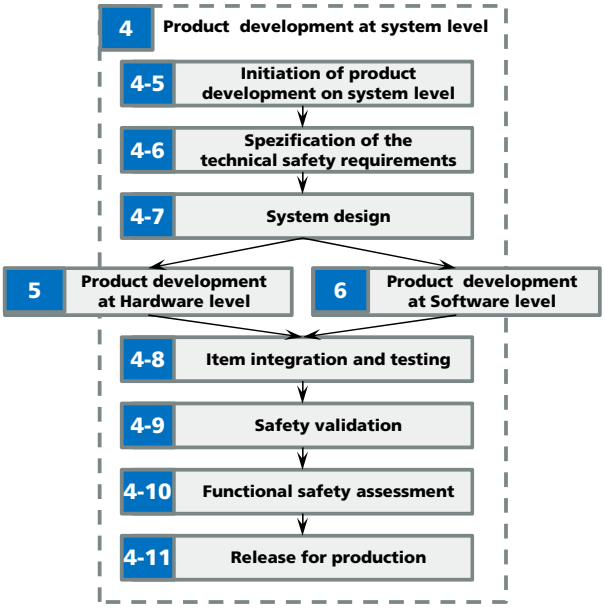
Fraunhofer IPA

ANFORDERUNGEN DER ISO/DIS 26262 (KAPITEL 4)

Fraunhofer IPA

ISO/DIS 26262

Anforderungen der ISO 26262-4
Produktentwicklung auf Systemebene



Quelle: ISO/DIS 26262-4

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-4

Entwicklung und Verifizierung der technischen Sicherheitsanforderungen

- Sicherheitsmechanismen und Systemreaktionen
  - Maßnahmen zur Entdeckung, Anzeige und Beherrschung von Abweichungen innerhalb der Betrachtungseinheit bzw. in externen Einheiten
  - Maßnahmen zur Erreichung und Aufrechterhaltung des sicheren Zustandes
  - Maßnahmen zur Warnung und Degradation
  - Maßnahmen zur Vermeidung latenter Fehler
- Sicherheitsmechanismen (safe state)
  - Übergang in den sicheren Zustand (inkl. Anforderungen zur Regelung der Aktoren)
  - Fehlertoleranzintervall (Zeitintervall, in dem das Fahrzeug mit Abweichungen betrieben werden kann, bevor ein Gefahrenzustand eintritt)
  - Notfallbetriebsintervall (Zeitintervall, vom Auftreten der Abweichung bis zum Übergang in den sicheren Zustand)
  - Maßnahmen zur Aufrechterhaltung des sicheren Zustandes

Quelle: ISO/DIS 26262-4

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-4

Entwicklung und Verifizierung der technischen Sicherheitsanforderungen

- Vermeidung schlafender (latent) Abweichungen
  [Empfohlen bei A und B / Gefordert bei C und D]
  - Spezifizierung des Zeitintervalls zur Entdeckung schlafender Fehler (Berücksichtigung von Zuverlässigkeit der Komponente und der Exposure)
  - On-board tests (z.B. bei „Zündung an“ / „Zündung aus“)
  - Test im Betrieb
  - Test während Service / Wartung
- Entwicklung von Sicherheitsmechanismen zur Vermeidung/Diagnose schlafender Doppelfehler
  - ASIL B für ASIL D Sicherheitsziele
  - ASIL A für ASIL B und ASIL C Sicherheitsziele

Quelle: ISO/DIS 26262-4

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-4

Entwicklung und Verifizierung des Systems und des technischen Sicherheitskonzepts

- Systemspezifizierung
- Systemarchitektur
- Maßnahmen zur Vermeidung von systematischen Fehlern
- Vermeidung von Fehlern durch zu hohe Komplexität
- Maßnahmen zur Beherrschung zufälliger HW-Fehler im Betrieb
- Zuordnung der Sicherheitsanforderungen auf Hardware und Software
- Spezifikation der Hardware- und Software-Schnittstellen (HSI)
- Spezifikation der Diagnose der HSI
- Verifizierung des System Designs

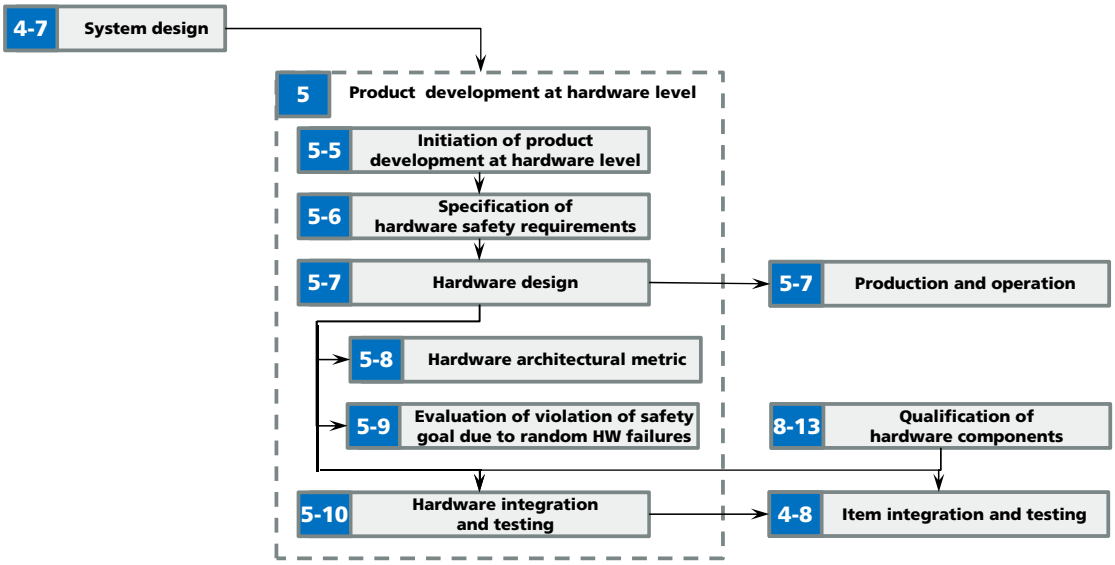
Quelle: ISO/DIS 26262-4

Fraunhofer IPA

ANFORDERUNGEN DER ISO/DIS 26262 (KAPITEL 5)

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-5
Produktentwicklung auf Hardwareebene



Quelle: ISO/DIS 26262-5

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-5
Hardware architectural metrics

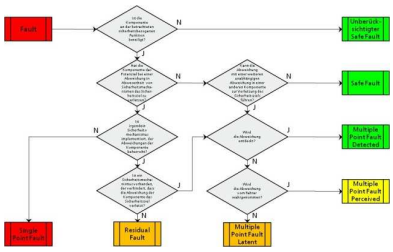
Bewertung der Hardwarearchitektur in Bezug auf Behandlung zufälliger Hardwarefehler

- ASIL (B), C, D: Anwendung Hardwaremetriken
  - Single point faults metric
    (Bewertet die Robustheit gegenüber Single Point Faults und Residual Faults)
  - Multiple point faults metric
    (Bewertet die Robustheit gegenüber Multiple Point Faults)
- ASIL (B), C, D: Einhaltung von Zielwerten
  - Single point faults metric
  - Multiple point faults metric
- ASIL (B), C, D: Review der Bewertung

Quelle: ISO/DIS 26262-5

Fraunhofer IPA

ISO/DIS 26262
ISO 26262-5, Annex C
Zufällige Hardwarefehler



- **Single point fault (SPF)**
  Abweichung, die durch keinen Sicherheitsmechanismus abgedeckt ist und sofort zur Verletzung eines Sicherheitsziels führt
- **Residual fault (RF)**
  Teil einer Abweichung, der nicht durch einen Sicherheitsmechanismus abgedeckt wird und welcher zur Verletzung eines Sicherheitsziels führt
- **Multiple point fault (MPF)**
  Abweichung unter mehreren unabhängigen Abweichungen, welcher in Kombination zu einem Mehrfachfehler führt
  - Perceived (MPF P)
    bemerkt
  - Detected (MPF D)
    entdeckt
  - Latent (MPF L)
    schlafend

Quelle: ISO/DIS 26262-5

Fraunhofer IPA

Kennwerte und Berechnungsalgorithmen der ISO 26262 für zufällige Fehler in Abhängigkeit vom ASIL
ISO 26262-5, Annex E und G

$$\text{Single Point Fault metric} = 1 - \frac{\sum_{\text{Safety related HW elements}} (\lambda_{SPF} + \lambda_{RF})}{\sum_{\text{Safety related HW elements}} \lambda} = \frac{\sum_{\text{Safety related HW elements}} (\lambda_{MPF} + \lambda_{S})}{\sum_{\text{Safety related HW elements}} \lambda}$$

$$\text{Latent Fault metric} = 1 - \frac{\sum_{\text{safety related HW elements}} (\lambda_{\text{MPF Latent}})}{\sum_{\text{safety related HW elements}} (\lambda - \lambda_{SPF} - \lambda_{RF})} = \frac{\sum_{\text{safety related HW elements}} (\lambda_{\text{MPF perceived or detected}} + \lambda_{S})}{\sum_{\text{safety related HW elements}} (\lambda - \lambda_{SPF} - \lambda_{RF})}$$

where $\sum_{\text{safety related HW elements}} \lambda_x$ is the sum of λ_x of the safety-related hardware elements of the item.

ASIL	PMHF	SPFM	LFM
A	$< 10^{-6}$	-	-
B	$< 10^{-7}$	≥ 90%	≥ 60%
C	$< 10^{-7}$	≥ 97%	≥ 80%
D	$< 10^{-8}$	≥ 99%	≥ 90%

Legende:
PMHF = Probabilistic Metric for random Hardware Failures (PMHF)
SPFM = Single-point fault metric
LFM = Latent-fault metric

Quelle: ISO/DIS 26262-5

Fraunhofer IPA

Funktionale Sicherheit
Ermittlung der Fehlermodi und Fehlerraten von Systemelementen


SIEMENS

SIEMENS NORM
SN
29500-1
HINWEIS 1 / NOTE 1
Ausgabe / Edition 2010-09

Ausfallraten Bauelemente
Hinweis 1 zu Teil 1: Erwartungswerte, Allgemeines, Ausgabestand

Failure rates of components
Note 1 on Part 1: Expected values, General, Date of issue

Fortsetzung Seite 2
Continued on page 2

CT SR Corporate Standardization & Regulation, Muenchen and Erlangen

Ermittlung der Fehlermodi und FIT-Werte von Systemelementen:

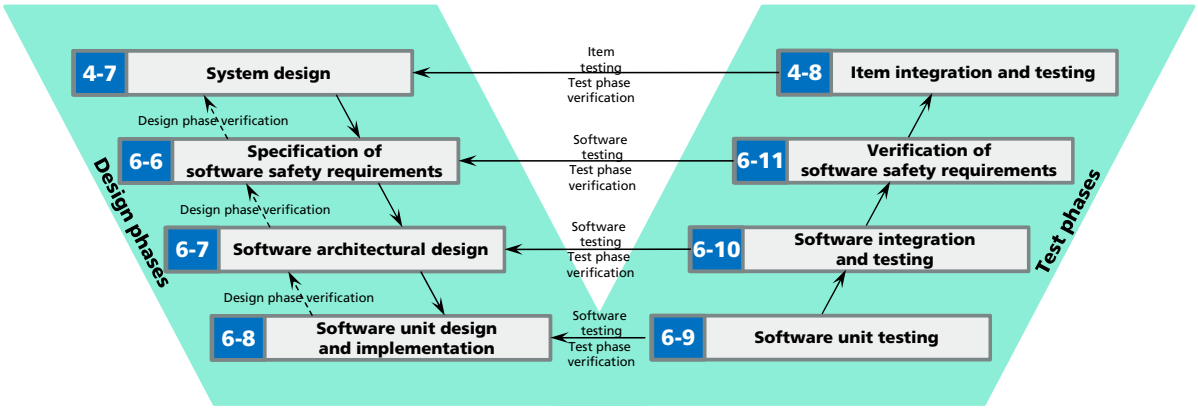
- Literatur zur Zuverlässigkeit (z.B. Birolini)
- Firmennormen (z.B. SN 29500)
- Zuverlässigkeitshandbücher (z.B. MIL-Handbook 217)
- RDF 2000 (IEC TR 62380)
- Datenblätter
- Felderfahrungswerte

Fraunhofer IPA

ANFORDERUNGEN DER ISO/DIS 26262 (KAPITEL 6)

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-6
Produktentwicklung auf Softwareebene



Quelle: ISO/DIS 26262-6

Fraunhofer IPA

ANFORDERUNGEN DER ISO/DIS 26262 (KAPITEL 7)

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-7

Planung und Sicherstellung der Produktion sicherheitsbezogener Produkte

- Planung der Produktion
- Beschreibung der Produktion
- Software und Kalibrierung
- Prüfmaßnahmen
- Risikoanalysen
- Abweichungsmanagement
- Planung der Prozesse für Benutzer, Service, Reparatur und Außerbetriebnahme
- Erstellung der Benutzerdokumentation
- Feldbeobachtung

Quelle: ISO/DIS 26262-7

Fraunhofer IPA

ANFORDERUNGEN DER ISO/DIS 26262 (KAPITEL 8)

Fraunhofer IPA

ISO/DIS 26262
Anforderungen der ISO 26262-8
Supporting processes

- Schnittstellenmanagement bei verteilter Entwicklung
- Management von Sicherheitsanforderungen
- Konfigurationsmanagement
- Änderungsmanagement
- Verifizierung
- Dokumentation
- Softwarequalifizierung
- Qualifizierung von Softwarekomponenten
- Qualifizierung von Hardwarekomponenten
- Argumentation „Proven in use“

Quelle: ISO/DIS 26262-8

Fraunhofer IPA

FAZIT

Fraunhofer IPA

Funktionale Sicherheit
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 26262
- Detaillierte und präzise Systemanalysen durch den OEM sowie effektives Schnittstellenmanagement/Kommunikation mit den Lieferanten
- Integrierte Anwendung vorhandener technischer Risikoanalysen
- Kritische Betrachtung der Risiken unabhängig von Zahlenwerten

Fraunhofer
IPA

METHODEN DER PRODUKTENTWICKLUNG

Mit neuen Produkten schneller am Markt

Fraunhofer IPA Workshop
1. Dezember 2011
Stuttgart