# Grundlagen der funktionalen Sicherheit

# GRUNDLAGEN DER FUNKTIONALEN SICHERHEIT

Vertiefungsseminar der Stuttgarter Produktionsakademie
07.-08. Mai 2014, Stuttgart

**Dipl.-Ing. Stefan Gerstmayr**
Functional Safety Engineer (TÜV Rheinland, Automotive)
Wissenschaftl. Mitarbeiter
Abteilung Nachhaltige Produktion und Qualität

Telefon: +49(0)711/9 70-1337
Fax: +49(0)711/9 70-1002
E-Mail: stefan.gerstmayr@ipa.fraunhofer.de
Internet: www.ipa.fraunhofer.de

© Fraunhofer

Fraunhofer IPA

## Funktionale Sicherheit
## Beispiele aus der Realität zur „Funktionalen Sicherheit“

- Rückruf 12/2013 – Infiniti Q50 Probleme mit der Kabel-Lenkung
  - Es gibt Probleme mit der Software des Systems, wenn die Kälte im Motorraum Frosttemperatur erreicht, so die Angaben der NHTSA.
    Die Software-Version der betroffenen Modelle könnte in diesem Fall die vollelektronische Lenkung deaktivieren und auch das Einsetzen des Sicherheitssystems verzögern.
  - Für den Notfall gibt es - so will es auch der Gesetzgeber - noch eine Kupplung, die automatisch schließt und eine mechanische Verbindung herstellt, so dass der Fahrer in jedem Fall eingreifen kann. Bei den vom Rückruf betroffenen Modellen kann sich der Einsatz dieses Notfallmodus verzögern.
    Quelle: http://www.auto.de/magazin/showArticle/article/122149/Drive-by-wire-im-Infiniti-Q50-Probleme-mit-der-Kabel-Lenkung

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit
## Beispiele aus der Realität zur „Funktionalen Sicherheit“

- Rückruf 01/2014 – Range Rover Airbag-Verkabelung
  - So können sich bei 3.912 Range Rover-Modellen des Jahrgangs 2013/2014 die Verbindungskabel der vorderen Seiten-Airbags in den Sitzen gelöst haben.
    Quelle: http://www.kfz-auskunft.de/rueckruf/387.html
- Rückruf 01/2014 – Defekter Öldrucksensor beim Volvo S60 (30.929 Fzg.)
  - Wegen des fehlerhaften Sensors warnt die Elektronik den Fahrer nicht vor einem zu geringen Öldruck. Dadurch kann der Motor während der Fahrt unvermittelt absterben, was das Unfallrisiko erhöht.
    Quelle: http://www.kfz-auskunft.de/rueckruf/386.html
- Rückruf 02/2014 – Toyota Prius Fehlerteufel Software (~1,9 Mio Fzg.)
  - Bei starken Beschleunigungsmanövern kann eine Überlastung der Hybrid-Regel-Elektronik auftreten. Aufgetreten ist der Fehler weltweit bisher aber nur bei 400 Fahrzeugen (weltweit), die wegen der Überlastung in das Notlaufprogramm geschaltet haben. Dadurch verursachte Unfälle hat es keine gegeben.
    Quelle: http://www.kfz-auskunft.de/rueckruf/391.html

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit
## Vortragsinhalte

- Entwicklung und Normen zur Funktionalen Sicherheit
- Definition und Zielsetzung der Funktionalen Sicherheit
- Grundlagen der Funktionalen Sicherheit
- Aufbau und Inhalte der ISO 26262
- Fazit

© Fraunhofer

Fraunhofer IPA

# ENTWICKLUNG UND NORMEN ZUR FUNKTIONALEN SICHERHEIT

© Fraunhofer

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

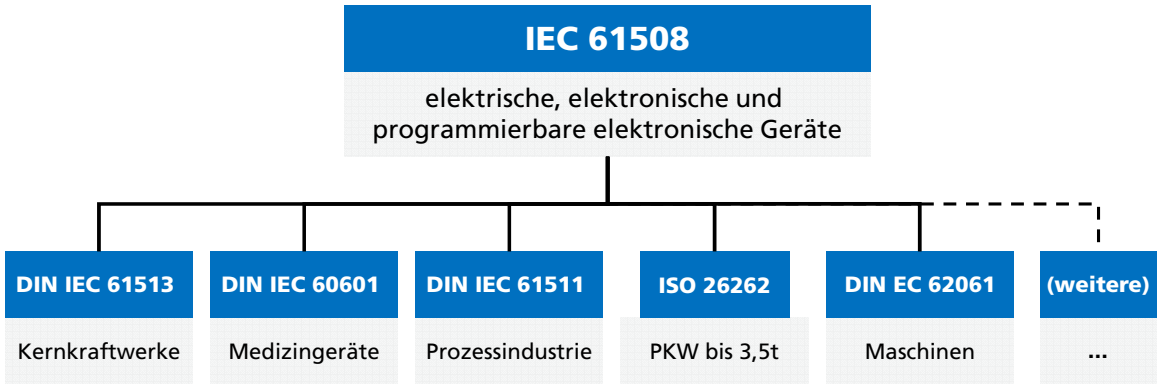
Unglück löste Normungsbestrebungen für funktionale Sicherheit aus:

- IEC 61508 (allgemein) – 1998/2000
- ISO 26262 (automotive) – 11/2011

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit
## Normenlandschaft




© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit
## Gültigkeitsbereich der ISO 26262

**Geltungsbereich der ISO 26262**

- PKW bis 3,5 Tonnen
- PKWs, die in Serie produziert werden
- Elektrische und elektronische Systeme (E/E-Systeme)
- Programmierbare elektronische Systeme (PE-Systeme)

**Nicht gültig (weiterhin Geltungsbereich der IEC 61508)**

- Fahrzeuge über 3,5 Tonnen (LKW)
- Fahrzeuge, die keine PKW darstellen (z.B. Kleintransporter, Motorräder)
- Sonderfahrzeuge (z.B. Fahrzeuge für Personen mit Behinderungen)

© Fraunhofer

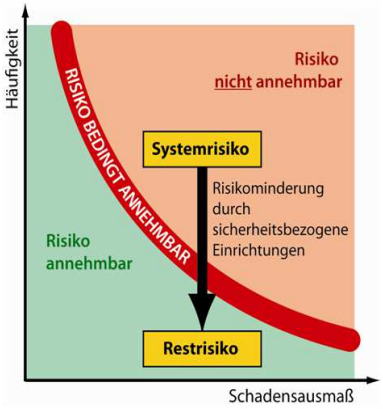
Fraunhofer IPA

# DEFINITION UND ZIELSETZUNG DER FUNKTIONALEN SICHERHEIT

© Fraunhofer

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

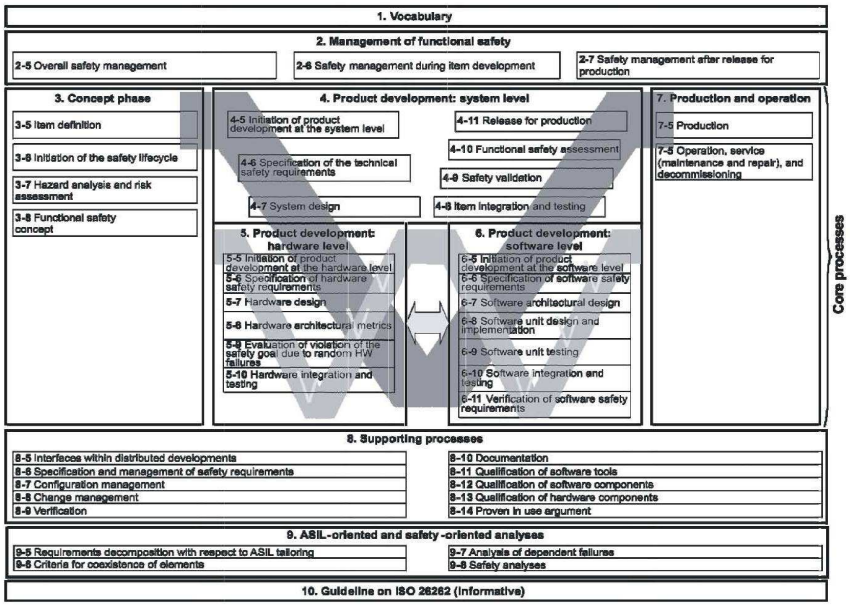
mit gefahrbringender Wirkung, einen sicheren Zustand einzunehmen bzw. in einem sicheren Zustand zu bleiben.

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit nach ISO26262
## Umfang der Norm

- Management
- Prozess
  - Konzept
  - System-Design
  - HW-Entw.
  - SW-Entw.
- Lifecycle
- Rollen
- Methoden
- Templates
- Beispiele




© Fraunhofer

Fraunhofer IPA

# BEGRIFFE DER FUNKTIONALEN SICHERHEIT

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit nach ISO26262
## Begriffe

**Sicherheit**

- "Safety: absence of unreasonable risk"
- Abwesenheit von unakzeptablen Risiken

**Risiko**

- "Risk: combination of the probability of occurrence of harm and the severity of that harm"
- "Harm: physical injury or damage to the health of persons"
- Wahrscheinlichkeit für das Auftreten einer Gefährdung

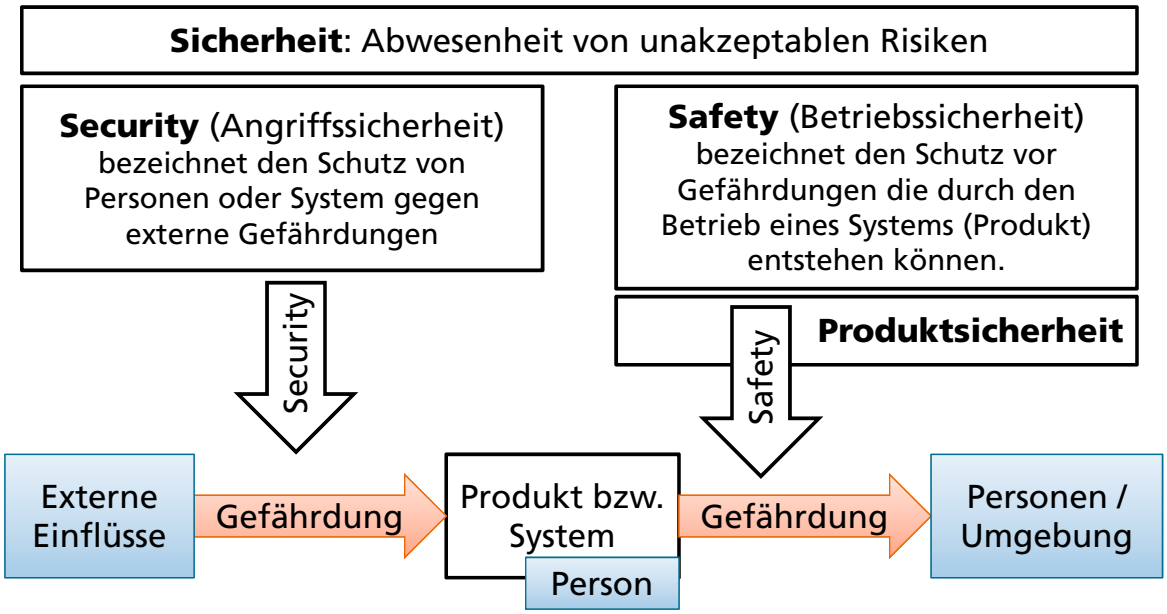
**Gefährdung**

- "Hazard: potential source of harm caused by malfunctioning behaviour of the item"

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit nach ISO26262
## Sicherheitsbegriffe




© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit nach ISO26262
## Begriffsklärung und Scope

### Funktionale Sicherheit

- "absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems"

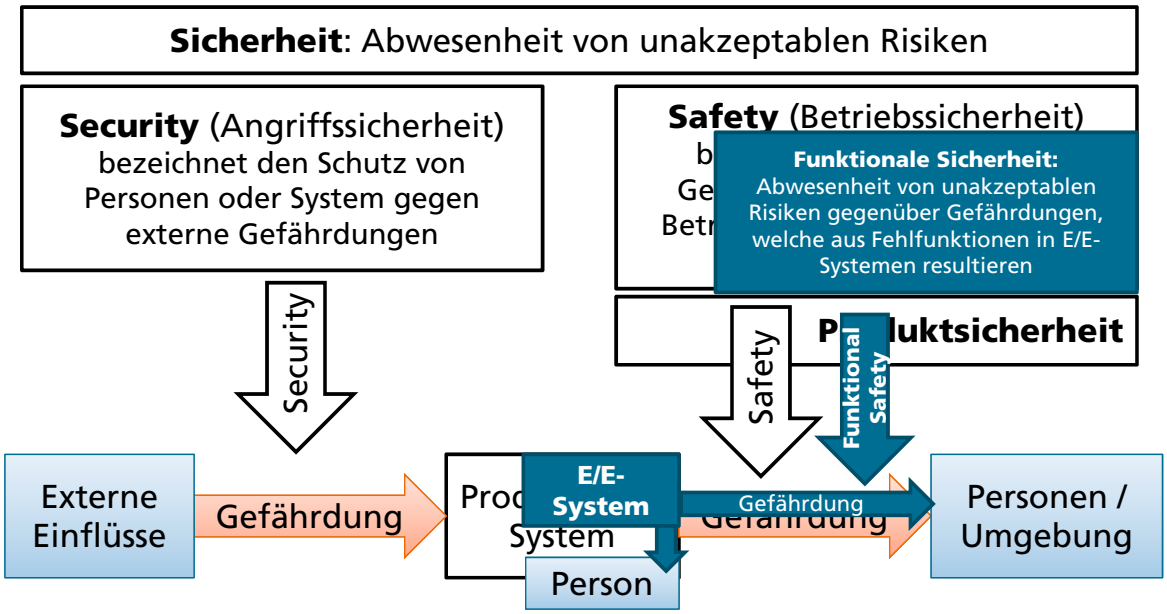
### System Scope der ISO26262

- "ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, <u>including interaction of these systems.</u> "
- "It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems."
- "ISO 26262 does not address the nominal performance of E/E systems"

© Fraunhofer



# Funktionale Sicherheit nach ISO26262
## Abgrenzung der Funktionalen Sicherheit




© Fraunhofer

# Funktionale Sicherheit nach ISO26262
## Sicherheit vs. Verfügbarkeit

**Zuverlässigkeit**

- Wahrscheinlichkeit, mit welcher ein System die geforderte Funktion innerhalb eines gegeben Zeitraums erfüllt.

**Verfügbarkeit**

- Wahrscheinlichkeit eines Systems funktionsfähig zu sein (Kehrwert der Ausfallwahrscheinlichkeit)

**Perspektive der ISO26262**

- Diejenigen Ausfälle, welche zu Gefährdung führen können, durch Überführung in sichern Zustand zu beherrschen.
- Das bedeutet i.d.R. immer eine Form der Abschaltung (Verfügbarkeitsverlust).

© Fraunhofer



# 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 (ASIL)**

- Vier diskrete Stufen zur Festlegung von Anforderungen für die Sicherheitsintegrität der Sicherheitsfunktionen
- ASIL A bis ASIL D

© Fraunhofer

# Funktionale Sicherheit
## Fault versus Failure (Definition gemäß ISO 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(e) **Fault / Abweichung** kann zu einem **Failure / Fehler** führen

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit
## Fehlerarten

### Systematische Fehler

- Ausfall mit eindeutiger Ursache, wie z.B. fehlerhafte Systemauslegung
- Maßnahmen zur Fehlervermeidung und Fehlerbeherrschung erforderlich

### Zufällige Fehler

- Ausfall, der zu einem zufälligen Zeitpunkt auftritt und dessen Ursache nicht eindeutig definiert werden kann, wie z.B. Alterung von Bauteilen
- Maßnahmen zur Fehlerbeherrschung erforderlich

### Fehler gemeinsamer Ursache

- Ausfall aufgrund einer gemeinsamen Ursache, z.B. Spannungsausfall
- Maßnahmen zur Fehlervermeidung und Fehlerbeherrschung erforderlich

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit
## Fehlermodelle

### Einfaches Fehlermodell = Stuck-at Fehlermodell

- Kontinuierlich „0“ oder „1“ oder „On“ oder „Off“ oder „Active“ oder „Inactive“ am Pin eines an der Sicherheitsfunktion beteiligten Teilsystems

### Mittleres Fehlermodell = Direct Current (DC) Fehlermodell

- Schließt Stuck-at Fehlermodell ein
- Zusätzlich Stuck-at „open“ oder „high impedance“ oder „Short circuit“ zwischen Signalen

### Komplexes Fehlermodell

- Schließt Stuck-at Fehlermodell und DC-Fehlermodell ein.
- Zusätzliche Betrachtung von „Drift“ und „Oszillation“

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit
## Fehlermodi der HAZOP-Studie (IEC 61882)

| Deviation type | Guide word | Example interpretation for process industry | Example interpretation for a Programmable Electronic System, PES |
|---|---|---|---|
| Negative | NO | No part of the intention is achieved, e.g. no flow | No data or control signal passed |
| Quantitative modification | MORE | A quantitative increase, e.g. higher temperature | Data is passed at a higher rate than intended |
| | LESS | A quantitative decrease e.g. lower temperature | Data is passed at a lower rate than intended |
| Qualitative modification | AS WELL AS | Impurities present Simultaneous execution of another operation/step | Some additional or spurious signal is present |
| | PART OF | Only some of the intention is achieved, i.e. only part of an intended fluid transfer takes place | The data or control signals are incomplete |
| Substitution | REVERSE | Covers reverse flow in pipes and reverse chemical reactions | Normally not relevant |
| | OTHER THAN | A result other than the original intention is achieved, i.e. transfer of wrong material | The data or control signals are incorrect |
| Time | EARLY | Something happens early relative to clock time, e.g. cooling or filtration | The signals arrive too early with reference to clock time |
| | LATE | Something happens late relative to clock time, e.g. cooling or filtration | The signals arrive too late with reference to clock time |
| Order or sequence | BEFORE | Something happens too early in a sequence, e.g. mixing or heating | The signals arrive earlier than intended within a sequence |
| | AFTER | Something happens too late in a sequence, e.g. mixing or heating | The signals arrive later than intended within a sequence |

Quelle: IEC 61882 – August 2001, Table 3

© Fraunhofer

Fraunhofer IPA

# Funktionale Sicherheit
## Redundanzen

**Homogene Redundanz**

- Redundanz mit dem gleichen Wirkprinzip
- “homogeneous redundancy: multiple but identical implementations of a requirement”
- Beherrschung von zufälligen Fehlern

**Diversitäre Redundanz**

- Redundanz mit unterschiedlichen Wirkprinzipen
- Beherrschung von systematischen Fehlern
- Beherrschung von zufälligen Fehlern

© Fraunhofer

Fraunhofer IPA

# AUFBAU UND INHALTE DER ISO 26262

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Aufbau der ISO 26262

INTERNATIONAL STANDARD

ISO 26262-5

First edition 2011-11-15

Road vehicles — Functional safety —

Part 5:
Product development at the hardware level

Véhicules routiers — Sécurité fonctionnelle —

Partie 5: Développement du produit au niveau du matériel

Reference number ISO 26262-5:2011(E)

© ISO 2011

(insgesamt 486 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 26262

© Fraunhofer



# ISO 26262
## Aufbau der Einzelnormen der ISO 26262-#

INTERNATIONAL STANDARD

ISO 26262-5

First edition 2011-11-15

Road vehicles — Functional safety —

Part 5:
Product development at the hardware level

Véhicules routiers — Sécurité fonctionnelle —

Partie 5: Développement du produit au niveau du matériel

Reference number ISO 26262-5:2011(E)

© ISO 2011

1. Scope
2. Normative reference
3. Terms, definitions, abbreviated terms
4. Requirements for compliance
5. Content
   - Objectives
   - General
   - Inputs for this clause
   - Requirements and recommendations
   - Work products
6. Annex (informative)
7. Bibliography

Quelle: ISO 26262

© Fraunhofer

# ISO 26262
## Anforderungen an compliance (Kapitel 4 in ISO 26262-#)

INTERNATIONAL STANDARD

ISO 26262-5

First edition 2011-11-15

**Road vehicles — Functional safety —**

Part 5:
**Product development at the hardware level**

*Véhicules routiers — Sécurité fonctionnelle —*
*Partie 5: Développement du produit au niveau du matériel*

Reference number ISO 26262-5:2011(E)

© ISO 2011

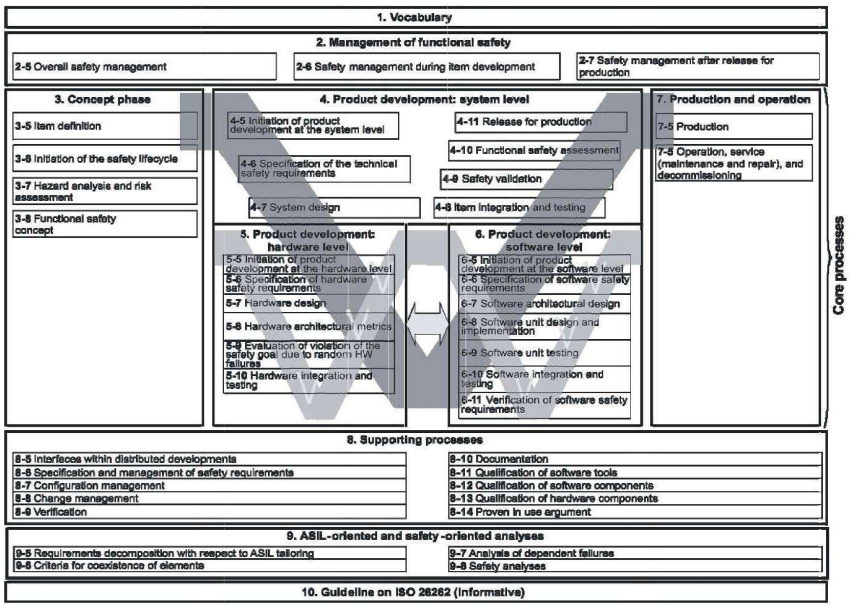
- 4.1 Allgemeine Anforderungen
  - Geplante Anpassungen
  - Begründungen bei Abweichungen
- 4.2 Interpretation der Tabellen
  - ++ Methode für ASIL stark empfohlen
  - \+ Methode für ASIL empfohlen
  - 0 Keine Aussage (für / wider) zur Methode
- 4.3 ASIL-abhängige Anforderungen und Empfehlungen
  - ASIL Anwendung
  - (ASIL) Empfehlung

Quelle: ISO 26262-2

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Lebenszyklusmodell der ISO 26262



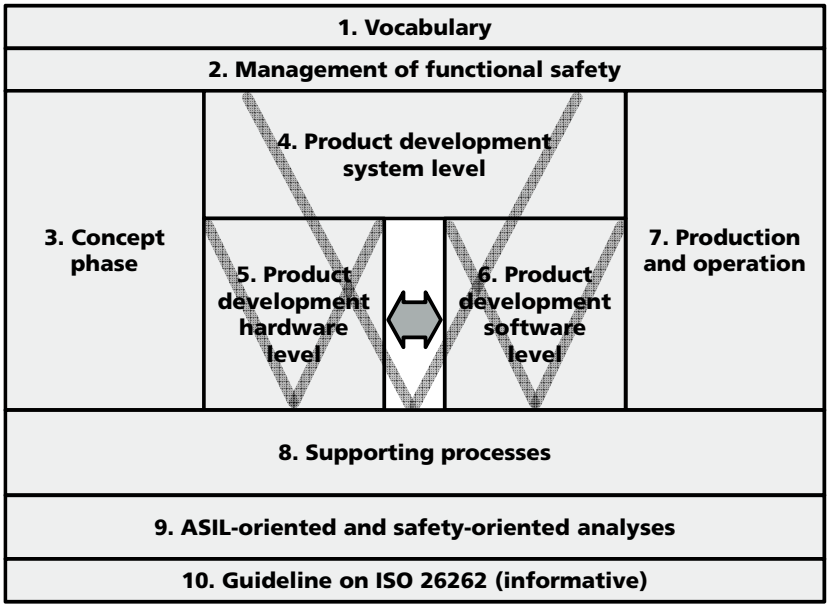

Quelle: ISO 26262

© Fraunhofer

Fraunhofer IPA

# ISO 26262

## Lebenszyklusmodell der ISO 26262 (vereinfacht)




Quelle: ISO 26262

© Fraunhofer

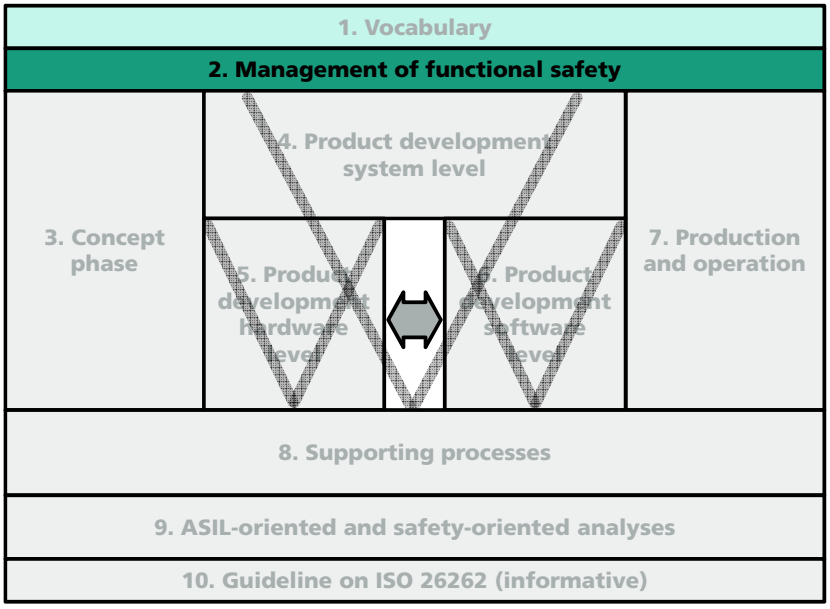
Fraunhofer IPA

# ANFORDERUNGEN DER ISO 26262 (PART 2)

© Fraunhofer

Fraunhofer IPA

# ISO 26262-2
## Management of functional safety




Quelle: ISO 26262

© Fraunhofer

Fraunhofer IPA

# ISO 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 26262-2

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Management der Funktionalen Sicherheit (Safety plan)

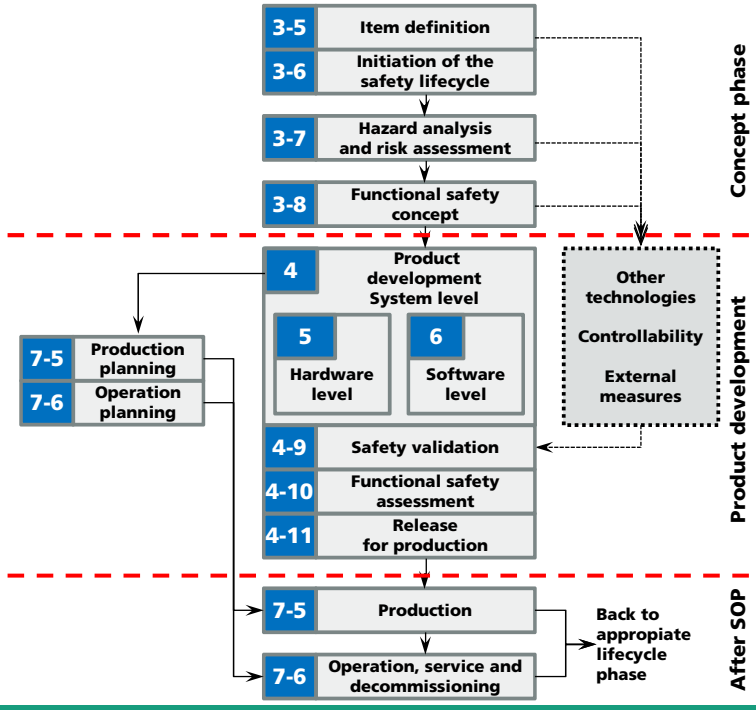
Der Safety-Plan enthält die zur Sicherstellung der Funktionalen Sicherheit erforderliche Aufbau- und Ablaufplanung (Phasen, Meilensteine, Verantwortlichkeiten, Dokumente) hinsichtlich:

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

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Sicherheits-Lebenszyklus (safety lifecycle)




Quelle: ISO 26262-2

© Fraunhofer

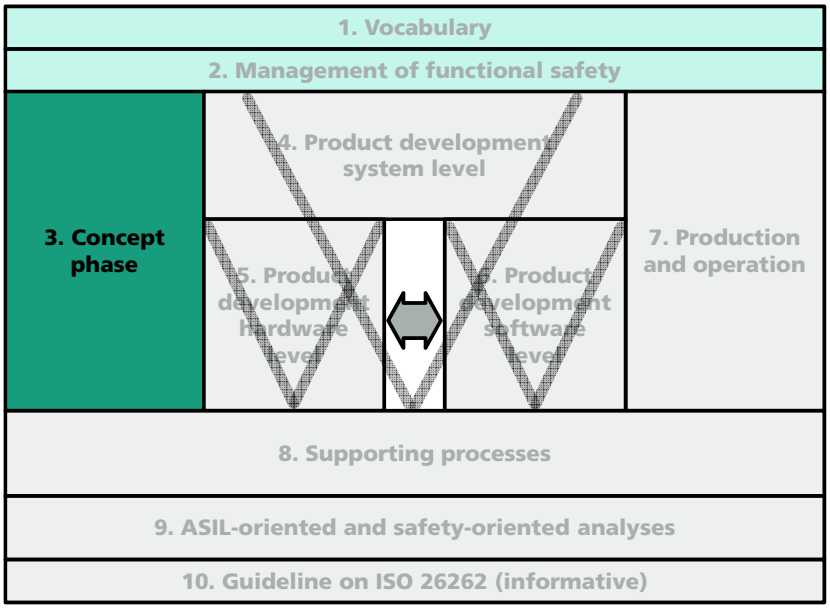
Fraunhofer IPA

# ANFORDERUNGEN DER ISO 26262 (PART 3)

© Fraunhofer

Fraunhofer IPA

## ISO 26262-3
## Concept phase




Quelle: ISO 26262

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Anforderungen der ISO 26262-3
## Item definition 3-5

Definition und Beschreibung des “Item”, inklusive seinen Abhängigkeiten zur Umgebung sowie der Interaktion mit dieser und mit anderen Systemen.

Notwendiges Verständnis über das System generieren, damit die nachfolgenden Aktivitäten ausgeführt werden

### Inhalte der Item Definition

- Funktionale und nicht-funktionale Anforderungen an das Item sowie die Abhängigkeiten und Interaktionen mit der Umgebung
- Die Grenzen des Items, die Schnittstellen zu anderen Systemen, und die Annahmen zur Interaktion mit diesen
- Mögliche Konsequenzen von Verhaltensdefiziten sowie bekannte Fehlermodi und Gefährdungen

Quelle: ISO 26262-3

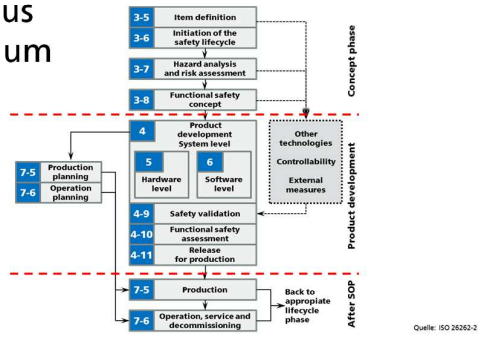
© Fraunhofer



# ISO 26262
## Anforderungen der ISO 26262-3
## Initiation of safety lifecycle 3-6

In der Initialisierung des Sicherheitslebenszyklus soll vorrangig entschieden werden, ob es sich um eine Neuentwicklung oder eine Änderungen handelt.

In zweitem Fall soll definiert werden, welche Phasen des Safety Lifecycle für diese Modifikation auszuführen sind.




Ergebnis

- Impact Analyse und Safety Plan im Falle von Änderungen

Quelle: ISO 26262-3

© Fraunhofer

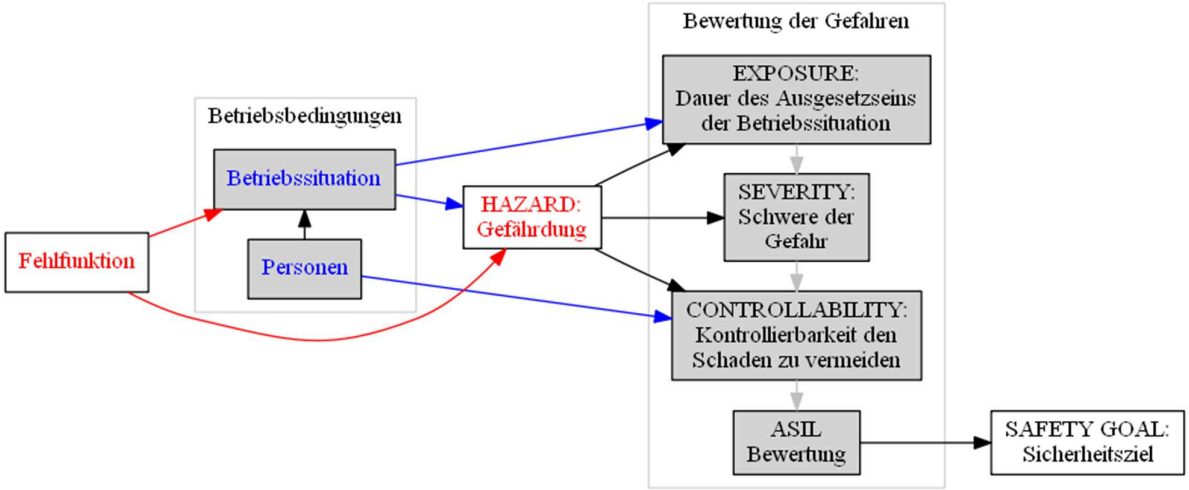
# ISO 26262
## Anforderungen der ISO 26262-3
## Hazard analysis and risk assessment

- Analyse der Betriebsbedingungen und Identifikation der Gefahren
  - Vollständige Auflistung der Betriebsbedingungen
  - Systematische Ableitung und Definition der Gefahren (Auswirkungen) von Systemfehlfunktion 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: explizite Sicherheitsanforderungen sind zu definieren
  - QM: keine Sicherheitsmaßnahmen notwendig
- Ableitung von Sicherheitszielen für Gefahren mit ASIL A – D

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Anforderungen der ISO 26262-3
## Hazard analysis and risk assessment




© Fraunhofer

Fraunhofer IPA

# Gefahren- und Risikoanalyse

## Bewertungstabellen für Schwere in Folge eines Fehlers

| Class | S0 | S1 | S2 | S3 |
|---|---|---|---|---|
| Description | No injuries | light and moderate injuries | Severe injuries, possibly life-threatening, survival probable | Life-threatening injuries (survival uncertain) or fatal injuries |
| Reference for single injuries (from AIS scale) | AIS 0<br>Damage that cannot be classified safety-related, e.g. bumps with roadside infrastructure<br>AIS 0 | more than 10% probability of AIS 1-6 (and not S2 or S3)<br>AIS 1-6 | more than 10% probability of AIS 3-6 (and not S3)<br>AIS 3-6 | more than 10% probability of AIS 5-6<br>AIS 5-6 |
| Informative examples | -Pushing over roadside infrastructure, e.g. post or fence<br>-Light collision<br>-Light grazing damage<br>-Damage while entering or leaving a parking space<br>-Leaving the road without collision or rollover | | | |
| -Side collision, e.g. crashing into a tree (impact to passenger cell) 15 < Δv < 25 km/h | | Δv <15km/h | 15 < Δv <25 km/h | Δv >25 km/h |
| Side collision with a passenger car (impact to passenger cell) | | Δv <15km/h | 15< Δv <35 km/h | Δv >35 km/h |
| Rear/front collision between two passenger cars | | Δv < 20km/h | 20< Δv <40 km/h | Δv>40 km/h, |
| Other collisions | | -Scrape collision with little vehicle to vehicle overlap (< 10%) | | -Roof or side collision with considerable deformation |
| Under riding a truck | | Without deformation of the passenger cell | | With deformation of the passenger cell |
| Pedestrian/bicycle accident | | | E.g. during a turning manoeuvre inside built-up area | Outside built-up area |

Quelle: ISO 26262-3 (Annex B)

**Abbreviated Injury Scale (AIS98-Code)**

- **AIS 0:** **keine** Verletzungen (unverletzt)
- **AIS 1:** **geringe** Verletzungen
- **AIS 2:** **ernsthafte** Verletzungen
- **AIS 3:** **schwere** Verletzungen
- **AIS 4:** **sehr schwere** Verletzungen
- **AIS 5:** **kritische** Verletzungen
- **AIS 6:** **maximale** (nicht behandelbare) Verletzungen

**Unfallkategorien**

Personenschäden

- **UK 1:** **tödliche** Verletzungen (Tod innerhalb von 30 Tagen nach dem Unfall)
- **UK 2:** **schwere** Verletzungen (Krankenhausaufenthalt von mehr als 24 Stunden erforderlich)
- **UK 3:** **leichte Verletzungen** (ärztliche Behandlung oder Krankenhausaufenthalt von weniger als 24 Stunden)

Sachschäden

- **UK 4-6:** **Sachschäden** in Abhängigkeit der Unfallumstände (Alkohol, Drogen, Fahrtüchtigkeit des Fahrzeugs etc.)

© Fraunhofer

Fraunhofer IPA

# Gefahren- und Risikoanalyse

## Bewertungstabellen für Exposure (Dauer des Ausgesetztseins in einer potentiell gefährlichen Fahrsituation)

| Class | E1 | E2 | E3 | E4 |
|---|---|---|---|---|
| **Description** | Very low probability | Low probability | Medium probability | High probability |
| Definition of duration/ probability of exposure | Not specified | < 1% of average operating time | 1% - 10% of average operating time | > 10% of average operating time |
| Informative examples | Highway – lost cargo/obstacle on road<br>Mountain pass – driving down hill with the engine off<br>Jump start<br>Garage – vehicle on roller rig | Pulling a trailer<br>Driving with roof rack<br>Driving on a mountain pass with an unsecured steep slope<br>Snow and ice<br>Driving backwards<br>Fuelling<br>Overtaking<br>Car wash<br>City driving – driving backwards<br>City driving – parking situation<br>Country road – crossing<br>Country road – snow and ice<br>Country road – slippery/leaves<br>Highway – entering<br>Highway – exit<br>Highway – approaching end of congestion<br>Parking – sleeping person in the vehicle<br>Parking – parking with trailer<br>Garage – diagnosis<br>Garage – vehicle on auto lift | Tunnels<br>Hill hold<br>Night driving on roads without streetlights<br>Wet roads<br>Congestion<br>City driving – one way street<br>Highway – heavy traffic/stop and go | Accelerating<br>Braking<br>Steering<br>Parking<br>Driving on highways<br>Driving on secondary roads<br>City driving – changing lane<br>City driving – stopping at traffic lights<br>Country road – free driving<br>Highway – free driving<br>Highway – changing lane<br>Parking – parking lot |

Quelle: ISO 26262-3 (Annex B)

**Exposure**

- **E0:** **Sehr unwahrscheinlich:** bspw. landendes Flugzeug auf Straße
- **E1:** **geringe** Aufenthaltsdauer keine spezifizierte Betriebs-/Aufenthaltszeit
- **E2:** **gelegentlich:** Situation tritt für die meisten Fahrer wenige Male pro Jahr auf (<1% der Betriebszeit)
- **E3:** **ziemlich oft:** Situation tritt für Durchschnittsfahrer einmal im Monat oder öfter auf (1%-10% der Betriebszeit)
- **E4:** **oft:** Situation die bei nahezu jeder Fahrt auftritt (>10% der Betriebszeit)

© Fraunhofer

Fraunhofer IPA

# Gefahren- und Risikoanalyse

## Bewertungstabellen für Exposure (Dauer des Ausgesetzt-seins in einer potentiell gefährlichen Fahrsituation)

| Class | E1 | E2 | E3 | E4 |
|---|---|---|---|---|
| Description | Very low probability | Low probability | Medium probability | High probability |
| Definition of frequency | Situations that occur **less often than once a year** for the great majority of drivers | Situations that occur **a few times a year** for the great majority of drivers | Situations that occur **once a month or more often** for an average driver | All situations that occur during **almost every drive on average** |
| Informative examples | Stop at railway crossing, which requires the engine to be restarted<br>Towing<br>Jump start | Pulling a trailer, driving with a roof rack<br>Driving on a mountain pass with an unsecured steep slope<br>Driving situation with a deviation from the desired path<br>Snow and ice | Fuelling<br>Overtaking<br>Tunnels<br>Hill hold<br>Car wash<br>Wet roads<br>Congestion | Starting<br>Shifting gears<br>Accelerating<br>Braking<br>Steering<br>Using indicators<br>Parking<br>Driving backwards |

Quelle: ISO 26262-3 (Annex B)

**Exposure**

**E0:** **Sehr unwahrscheinlich:** bspw. landendes Flugzeug auf Straße

**E1:** **geringe** Aufenthaltsdauer keine spezifizierte Betriebs-/Aufenthaltszeit

**E2:** **gelegentlich:** Situation tritt für die meisten Fahrer wenige Male pro Jahr auf (<1% der Betriebszeit)

**E3:** **ziemlich oft:** Situation tritt für Durchschnittsfahrer einmal im Monat oder öfter auf (1%-10% der Betriebszeit)

**E4:** **oft:** Situation die bei nahezu jeder Fahrt auftritt (>10% der Betriebszeit)

© Fraunhofer

Fraunhofer IPA

# Gefahren- und Risikoanalyse

## Bewertungstabellen für Beherrschbarkeit einer Situation in Folge eines Fehlers

| Class | C0 | C1 | C2 | C3 |
|---|---|---|---|---|
| Description | Controllable in general | Simply controllable | Normally controllable | Difficult to control or uncontrollable |
| Definition | Controllable in general | 99% or more of all drivers or other traffic participants are usually able to avoid a specific harm. | 90% or more of all drivers or other traffic participants are usually able to avoid a specific harm. | Less than 90% of all drivers or other traffic participants are usually able, or barely able, to avoid a specific harm. |
| Informative examples | Unexpected increase in radio volume<br>Situations that are considered distracting<br>Unavailability of a driver assisting system | When starting the vehicle with a locked steering column, the car can be brought to stop by almost all drivers early enough to avoid a specific harm to persons nearby.<br>Faulty adjustment of seats while driving can be controlled by almost all drivers by bringing the vehicle to a stop. | Driver can normally avoid departing from the lane in case of a failure of ABS during emergency braking.<br>Driver is normally able to avoid departing from the lane in case of a motor failure at high lateral acceleration (motorway exit).<br>Driver is normally able to bring the vehicle to a stop in case of a total lighting failure at medium or high speed on an unlighted country road without departing from the lane in an uncontrolled manner.<br>Driver is normally able to avoid hitting an unlit vehicle on an unlit country road. | Wrong steering with high angular speed at medium or high vehicle speed can hardly be controlled by the driver.<br>Driver normally cannot avoid departing from the lane on snow or ice on a bend in case of a failure of ABS during emergency braking.<br>Driver normally cannot bring the vehicle to a stop if a total loss of braking performance occurs.<br>In the case of faulty airbag release at high or moderate vehicle speed, the driver usually cannot prevent vehicle from departing from the lane. |

Quelle: ISO 26262-3 (Annex B)

**Beherrschbarkeit (Controllability)**

**C0:** von **jedem** Verkehrsteilnehmer beherrschbar

**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

Fraunhofer IPA

# ISO 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
  - Fehlerentdeckung und Fehlerabschwächung
  - Überführung in sichere Zustände
  - Fehlertoleranz-Mechanismen
  - Fehlerentdeckung und Warnung des Fahrers
  - Entscheidungslogiken

Quelle: ISO 26262-3

© Fraunhofer



# ISO 26262
## Anforderungen der ISO 26262-3
## Functional safety concept

Nachvollziehbare Ableitung und Spezifikation der funktionalen Sicherheitsanforderungen sowie Zuordnung zur Systemarchitektur

- Zustandsbeschreibung
  - Betriebsmodi
  - Fehlertoleranzintervall
  - Sichere Zustände
  - Notfall Betriebsmodus
  - Funktionale Redundanzen
- Warn- und Degradationskonzept
- Notbetriebskonzept
- Reaktionskonzept durch Fahrer

Quelle: ISO 26262-3

© Fraunhofer

# ISO 26262
## Anforderungen der ISO 26262-3
## Functional safety concept

Verifizierung, Bewertung, Validierung und Review des Sicherheitskonzepts

- Verifizierung des funktionalen Sicherheitskonzepts auf Übereinstimmung mit den Sicherheitszielen
- Bewertung der Effektivität des Sicherheitskonzepts (z.B. Versuche mit Mustern und/oder Prototypen, Simulationen)
- Definition der Kriterien zur Validierung
- Review des Sicherheitskonzepts

Quelle: ISO 26262-3

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Tabelle der Anforderungen an die Unabhängigkeit der Personen, die Maßnahmen und Ergebnisse bestätigen

**Table 1 — Required confirmation measures, including required independence**

| Confirmation measures | | | | | |
|---|---|---|---|---|---|
| Confirmation review of the hazard analysis & risk assessment, of the item that is dealt with in accordance with ISO°26262 (see ISO°26262-3, Clause 7 and if applicable, ISO 26262-8, Clause 5)<br>- independent from the developers of the item | I3 | | | | For all ASILs, and including hazards rated as QM |
| | applies to ASIL | | | | of the |
| | A | B | C | D | |
| Confirmation review of the safety plan (see Clause 6)<br>- independent from the developers of the item / project management | - | I1 | I2 | I3 | highest ASIL among safety goals of the item |
| Confirmation review of the integration and testing plan (see ISO°26262-4, Clause 5)<br>-independent from the developers of the item / project management | I0 | I1 | I2 | I2 | highest ASIL among safety goals of the item |
| Confirmation review of the validation plan (see ISO°26262-4, Clause 5)<br>-independent from the developers of the item / project management | I0 | I1 | I2 | I2 | highest ASIL among safety goals of the item |
| Confirmation review of the safety analyses (FMEA, FTA): (see ISO°26262-9, 8.4.8) | I1 | I1 | I2 | I3 | highest ASIL among safety goals of the item |
| Confirmation review of the qualification of software tools (see ISO°26262-8, Clause 11)<br>- independent from the person performing the qualification of the software tool | - | I0 | I1 | I1 | highest ASIL among safety goals of the item |
| Confirmation review of the proven in use arguments (analysis, data and credit), of the candidates. See ISO°26262-8, Clause 14.<br>-independent from the supplier of the argument | I0 | I1 | I2 | I3 | ASIL of the safety goal or requirement related to the considered behaviour, or function, of the candidate |
| Confirmation review of the completeness of the safety case (see 6.4.5)<br>- independent from authors of safety case | I0 | I1 | I2 | I3 | highest ASIL among safety goals of the item |
| Audit of functional safety processes (see 6.4.6)<br>- independent from the persons working in accordance with the processes required for functional safety | - | I0 | I2 | I3 | highest ASIL among safety goals of the item |
| Functional safety assessment (see 6.4.6.7)<br>-independent from the supplier of the safety case | - | I0 | I2 | I3 | highest ASIL among safety goals of the item |

- no requirement, and no recommendation for or against, regarding this confirmation measure

I0 the confirmation measure should be performed

I1 the confirmation measure shall be performed

I2 the confirmation measure shall be performed, by a person from a different team, i.e. not reporting to the same direct superior

I3 the confirmation measure shall be performed, by a person from a different department or organization, i.e. independent from the relevant department, regarding management, resources, and responsibility for release for production.

Quelle: ISO 26262-2

© Fraunhofer

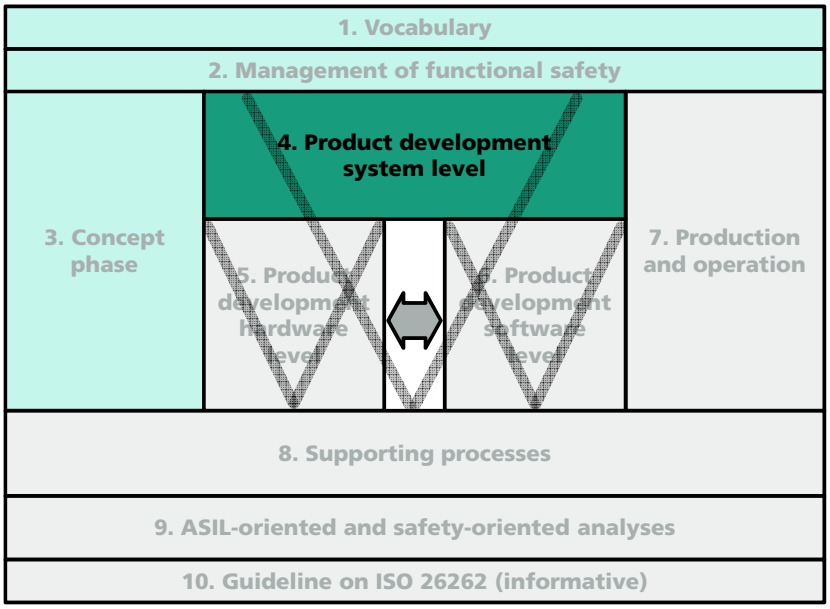
Fraunhofer IPA

# ANFORDERUNGEN DER ISO 26262 (KAPITEL 4)

© Fraunhofer

Fraunhofer IPA

## ISO 26262-4
## Product development system level

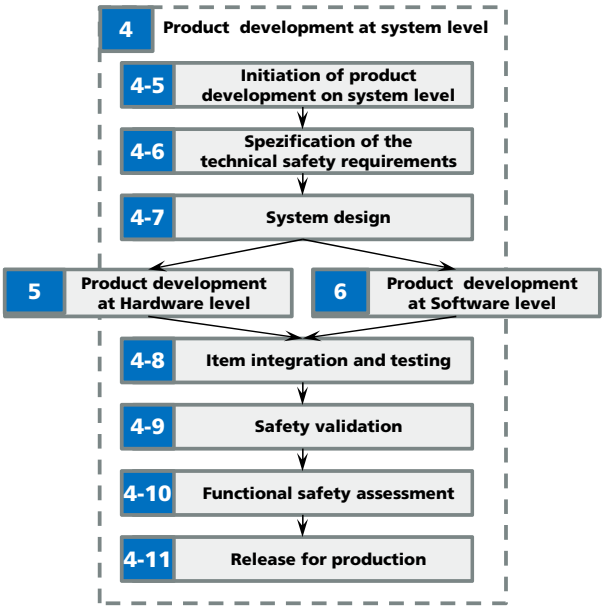



Quelle: ISO 26262

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Anforderungen der ISO 26262-4
## Produktentwicklung auf Systemebene




Quelle: ISO 26262-4

© Fraunhofer

Fraunhofer IPA

# ISO 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 26262-4

© Fraunhofer

Fraunhofer IPA

# ISO 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/startup Tests (z.B. bei „Zündung an“ / „Zündung aus“)
  - Test im Betrieb (online Tests)
  - Test während Service / Wartung
- Entwicklung von Sicherheitsmechanismen zur Vermeidung/Diagnose schlafender Doppelfehler
  - ASIL B für ASIL D Sicherheitsanforderungen
  - ASIL A für ASIL B und ASIL C Sicherheitsanforderungen
  - „Engineering judgement“ für ASIL A Sicherheitsanforderungen

Quelle: ISO 26262-4

© Fraunhofer

Fraunhofer IPA

# ISO 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 26262-4

© Fraunhofer

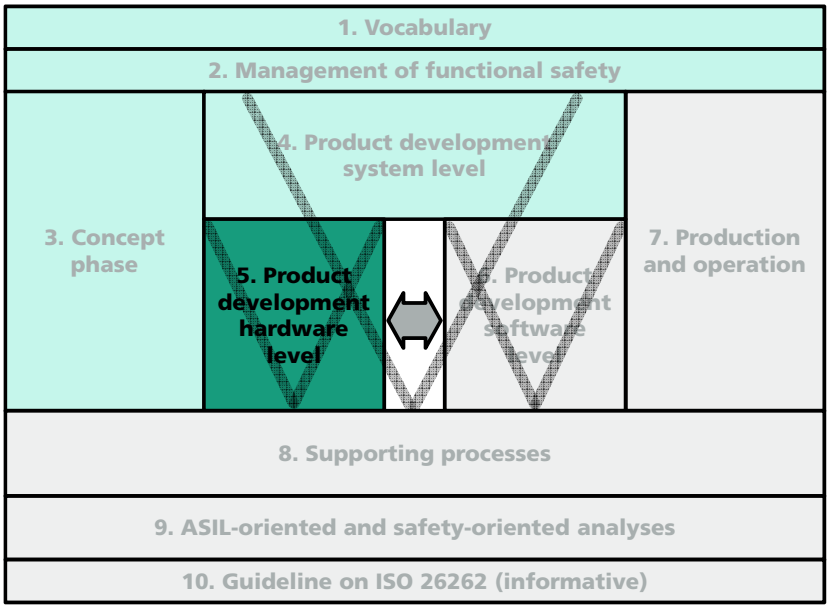
Fraunhofer IPA

# ANFORDERUNGEN DER ISO 26262 (KAPITEL 5)

© Fraunhofer

Fraunhofer IPA

## ISO 26262-5
## Product development hardware level

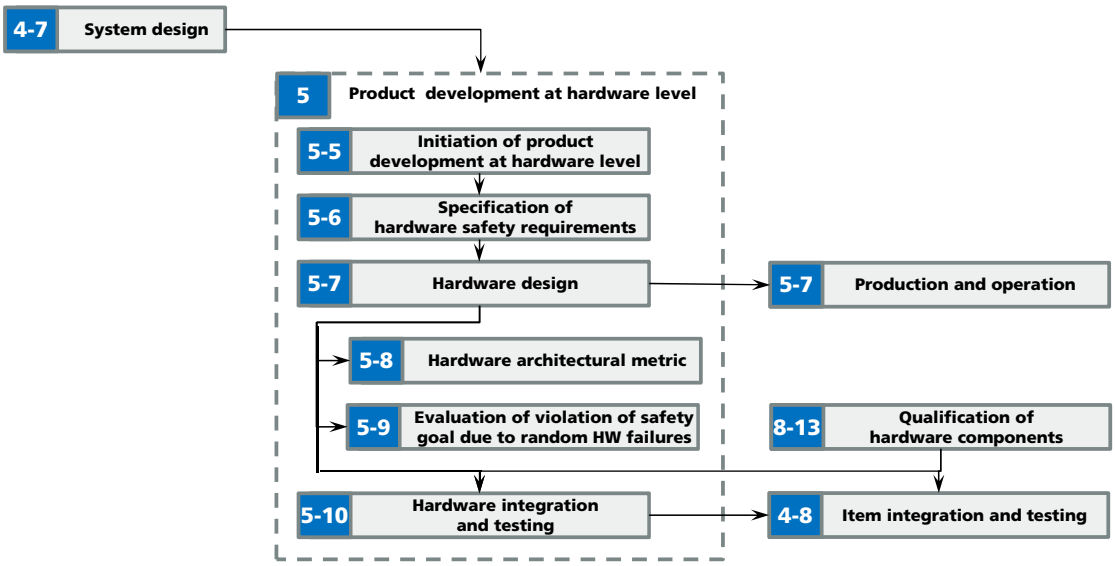



Quelle: ISO 26262

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Anforderungen der ISO 26262-5
## Produktentwicklung auf Hardwareebene




Quelle: ISO 26262-5

© Fraunhofer

Fraunhofer IPA

# ISO 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 26262-5

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Fault-Arten gemäß ISO 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 Sicherheits-mechanismus abgedeckt ist und direkt zur Verletzung eines Sicherheitsziels führt."
- **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."

© Fraunhofer



# ISO 26262
## Fault-Arten gemäß ISO 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 Zweifachfehler 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 Mehrfachfehler führt."
  - **Detected:** by safety mechanism
  - **Perceived:** detected by the driver
  - **Latent** (schlafend)**:** not detected nor perceived

© Fraunhofer

# ISO 26262
## Fault-Arten gemäß ISO 26262

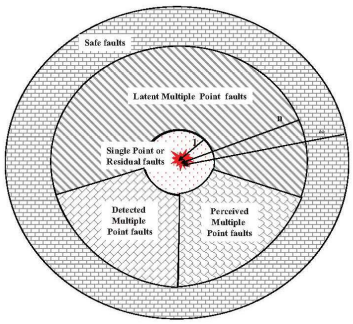
- **Latent fault:** multiple point fault whose presence is not detected by a safety mechanism nor perceived by the driver within the multiple point fault detection interval.
  - „ Eine Einzelabweichung deren Eintritt nicht innerhalb des Multiple point fault-Entdeckungsintervalls von den Sicherheitsmechanismen detektiert oder vom Fahrer wahrgenommen wurde.“

- **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."

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## ISO 26262-5, Annex C
## Zufällige Hardwarefehler




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

Quelle: ISO 26262-5

© Fraunhofer

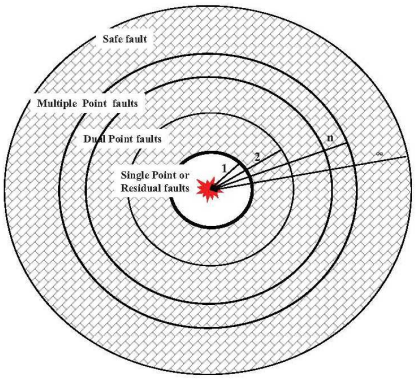
Fraunhofer IPA

# ISO 26262

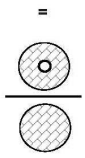
## ISO 26262-5, Annex C (normative)
## Hardwarefehlermetrik für Single Point Fault (SPF)

$$\boldsymbol{SPFM} = 1 - \frac{\sum_{SR,HW}(\lambda_{SPF} + \lambda_{RF})}{\sum_{SR,HW}\lambda} = \frac{\sum_{SR,HW}(\lambda_{MPF} + \lambda_{S})}{\sum_{SR,HW}\lambda}$$

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




**Single Point Fault Metric**




*Graphical representation*

Quelle: ISO 26262-5

© Fraunhofer

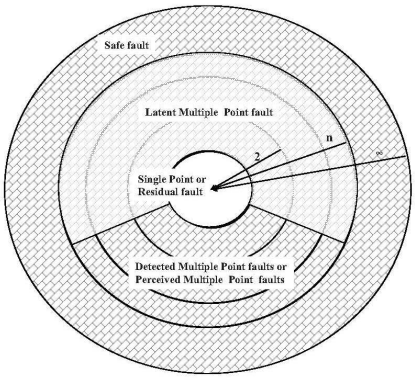
Fraunhofer IPA

# ISO 26262

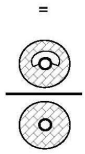
## ISO 26262-5, Annex C (normative)
## Hardwarefehlermetrik für Latent Fault

$$\boldsymbol{LFM} = 1 - \frac{\sum_{SR,HW}(\lambda_{MPF,latent})}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})} = \frac{\sum_{SR,HW}(\lambda_{MPF,perceived\ or\ detected} + \lambda_{S})}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})}$$

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




**Latent Fault metric**




*Graphical representation*

Quelle: ISO 26262-5

© Fraunhofer

Fraunhofer IPA

# ISO 26262

## Fault-Metriken und gefahrbringende Ausfälle
## ISO 26262-5, Annex E und G, Zielwerte

$$\boldsymbol{LFM} = 1 - \frac{\sum_{SR,HW}(\lambda_{MPF,latent})}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})} = \frac{\sum_{SR,HW}(\lambda_{MPF,perceived\ or\ detected} + \lambda_S)}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})}$$

$$\boldsymbol{SPFM} = 1 - \frac{\sum_{SR,HW}(\lambda_{SPF} + \lambda_{RF})}{\sum_{SR,HW}\lambda} = \frac{\sum_{SR,HW}(\lambda_{MPF} + \lambda_S)}{\sum_{SR,HW}\lambda}$$

$$\boldsymbol{\lambda_{SR,HW}} = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_S$$

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

**SPFM:** Single Point Faults Metric

**LFM:** Latent Faults Metric

**PMHF:** Probabilistic Metric for random Hardware Failures

**SR,HW:** Safety Related HardWare

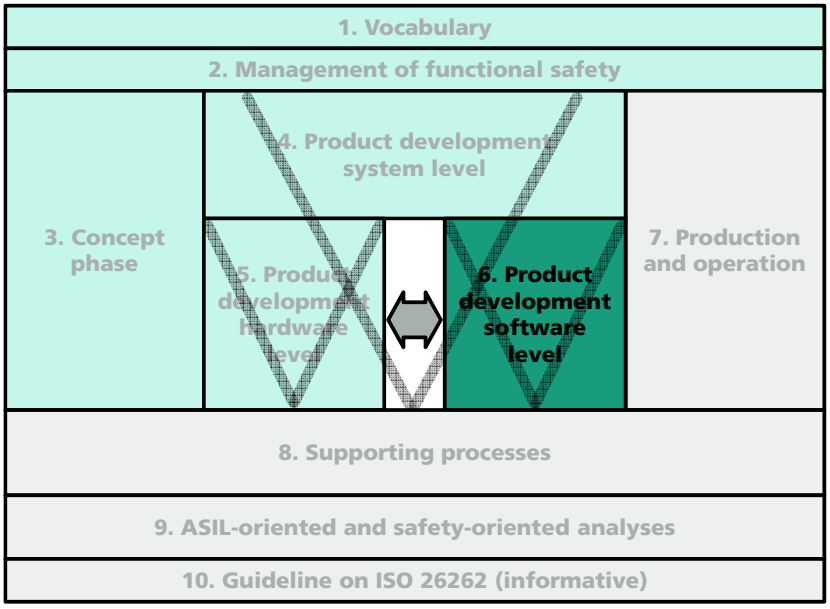
© Fraunhofer



# ANFORDERUNGEN DER ISO 26262 (KAPITEL 6)

© Fraunhofer

# ISO 26262-6
## Product development software level

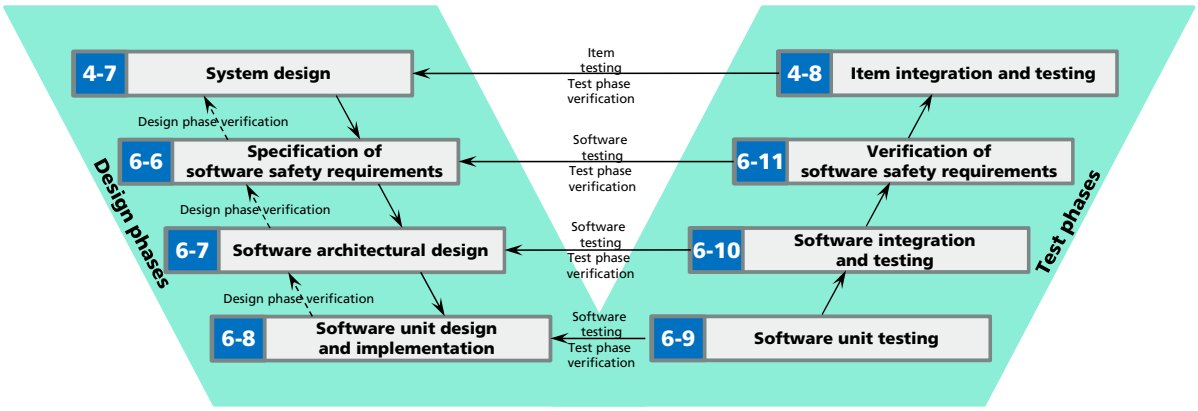



Quelle: ISO 26262

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Anforderungen der ISO 26262-6
## Produktentwicklung auf Softwareebene




Quelle: ISO 26262-6

© Fraunhofer

Fraunhofer IPA

# ISO 26262

## Anforderungen der ISO 26262-6
## Priciples for software architectural design

| Methods | | ASIL | | | |
|---|---|---|---|---|---|
| | | A | B | C | D |
| 1a | Hierarchical structure of software components | ++ | ++ | ++ | ++ |
| 1b | Restricted size of software components[a] | ++ | ++ | ++ | ++ |
| 1c | Restricted size of interfaces[a] | + | + | + | + |
| 1d | High cohesion within each software component[b] | + | ++ | ++ | ++ |
| 1e | Restricted coupling between software components[a, b, c] | + | ++ | ++ | ++ |
| 1f | Appropriate scheduling properties | ++ | ++ | ++ | ++ |
| 1g | Restricted use of interrupts[a, d] | + | + | + | ++ |

[a] In methods 1b, 1c, 1e and 1g "restricted" means to minimise in balance with other design considerations.

[b] Methods 1d and 1e can, for example, be achieved by separation of concerns which refers to the ability to identify, encapsulate, and manipulate those parts of software that are relevant to a particular concept, goal, task, or purpose.

[c] Method 1e addresses the limitation of the external coupling of software components.

[d] Any interrupts used have to be priority-based.

Quelle: ISO 26262-6

© Fraunhofer

Fraunhofer IPA

# Software in mechatronischen System

## Charakteristika von Software

Die Software / Steuerung muss

- das System in allen Systemzuständen sicher steuern
- das System in allen Systemzuständen bei 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 Informationsschnittstellen erkennen
- Fehlfunktionen im Diagnosesystemen erkennen (kann ich meinem Diagnosesystem noch trauen?)

© Fraunhofer

Fraunhofer IPA

Testplan

- Auf Basis der Ergebnisse der System-FMEA, der Konstruktions-FMEA und der Fehlerbasierten System-Reaktionsanalyse (FSR) lassen sich detaillierte Testpläne ableiten mit deren Hilfe das korrekte Funktionieren der Diagnose- und Absicherungsmaßnahmen (im Allgemeinen durch die Software realisiert) unter allen nutzerbedingten Interaktionen und Systemzuständen analysiert werden kann

Anmerkung:

- Detaillierte und für den Testingenieur verständliche Beschreibung der Testfälle
- Durchführung der Testfälle auf der Test-Bench mit der Zielsoftware
- Verwendung von speziellen Fehlermustern und Break-Out-Boxen zur Simulation der Fehlerfälle (neue Testverfahren)

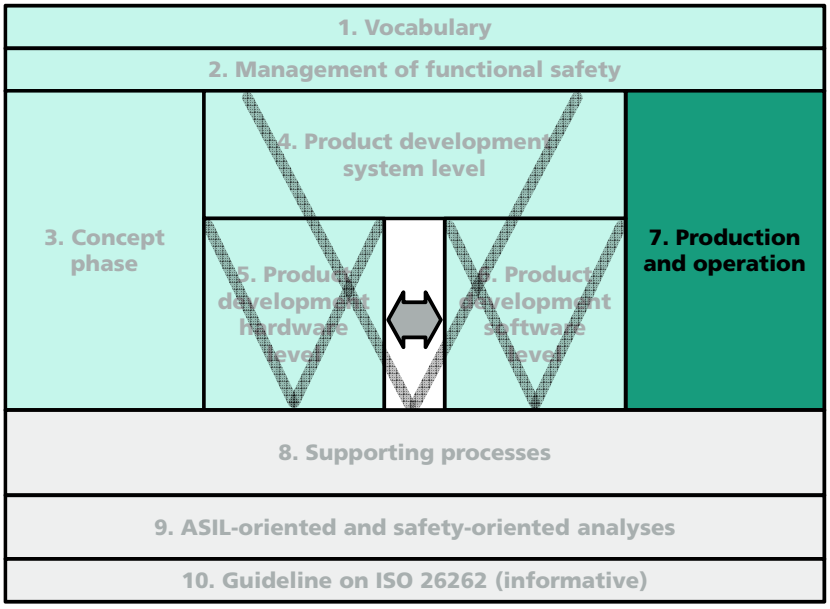
© Fraunhofer



# ANFORDERUNGEN DER ISO 26262 (KAPITEL 7)

© Fraunhofer

# ISO 26262-7
## Production and operation




Quelle: ISO 26262

© Fraunhofer

Fraunhofer IPA

# ISO 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 26262-7

© Fraunhofer

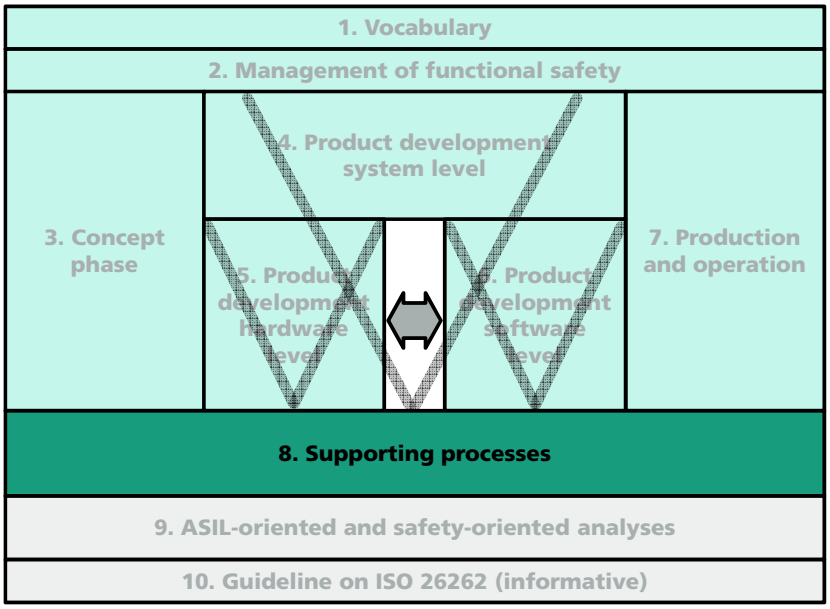
Fraunhofer IPA

# ANFORDERUNGEN DER ISO 26262 (KAPITEL 8)

© Fraunhofer

Fraunhofer IPA

## ISO 26262-8
## Supporting processes




Quelle: ISO 26262

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Anforderungen der ISO 26262-8
## Supporting processes

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

Quelle: ISO 26262-8

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Dokumentation

- Safety Plan
  - Planungsdokument analog eines Projekthandbuchs
  - Wichtigstes Instrument des Safety Managers um die geforderten Aktivitäten der ISO26262 zu planen
- Safety Case
  - Sammlung aller relevanten Unterlagen zur Funktionalen Sicherheit
  - Zum Zeitpunkt eines Release zu erstellen
  - Soll wie eine Art „Koffer" jedem Release beiliegen

© Fraunhofer

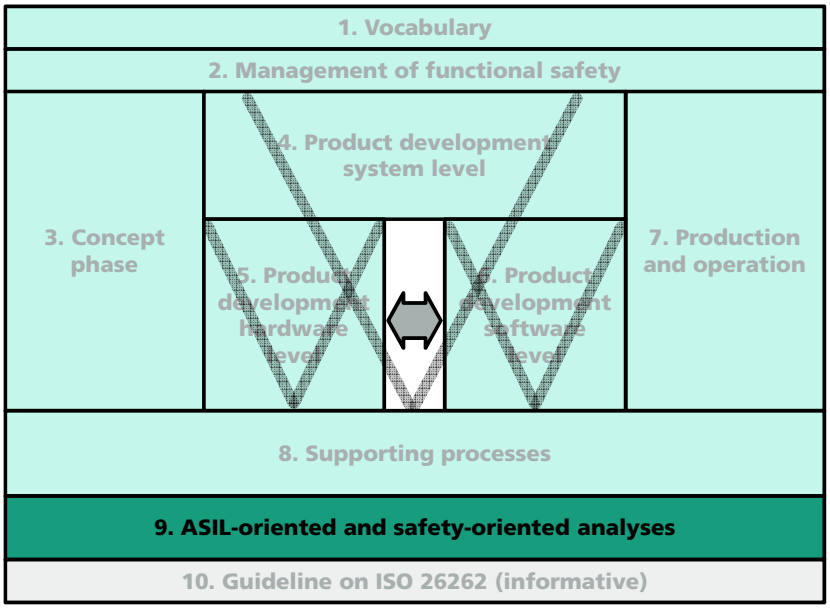
Fraunhofer IPA

# ANFORDERUNGEN DER ISO 26262 (KAPITEL 9)

© Fraunhofer

Fraunhofer IPA

## ISO 26262-9
## ASIL-oriented and safety-oriented analyses




Quelle: ISO 26262

© Fraunhofer

Fraunhofer IPA

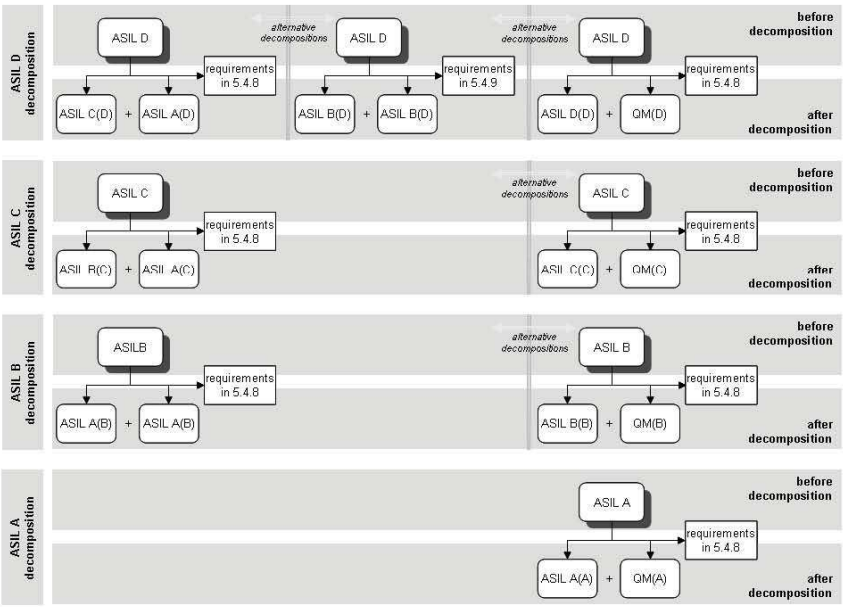
# ISO 26262-9
## ASIL-oriented and safety-oriented analyses

- Regeln zur ASIL-Dekomposition
  - Safety Requirements können in redundante Safety Requrirements auf niedrigerer System-Detaillierungsstufe dekomponiert werden.
  - Voraussetzung: unabhängige Element in der System-Architektur
  - Einschränkung: Vorgaben für „Confirmation Measures“ (Reviews, Audits und Assessments) gelten nach wie vor anhand des ursprünglichen ASIL
- Criteria for coexistance of elements (freedom of interferance)
- Analysis of dependant failures
- Safety Analysis
  - Qualitative und quantitative FMEA, FTA, etc.

© Fraunhofer

Fraunhofer IPA

# ISO 26262
## Anforderungen der ISO 26262-9
## ASIL-Dekomposition




Quelle: ISO 26262-9

© Fraunhofer

Fraunhofer IPA

# FAZIT

© Fraunhofer

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

Fraunhofer IPA

Stuttgarter
Produktionsakademie

# FUNKTIONALE SICHERHEIT

## NACH ISO 26262

Seminar **SPA 082**
7. und 8. Mai 2014
Stuttgart