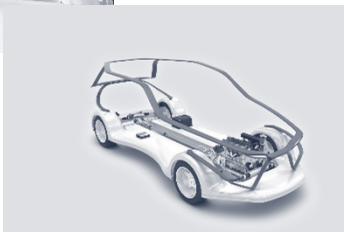
Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH
Dr.-Ing. Marco Schlummer



104. Sicherheitswissenschaftliches Kolloquium

HERAUSFORDERUNGEN DER FUNKTIONALEN SICHERHEIT IM AUTOMOBILBEREICH





IQZ
Ihr Qualitäts-Zulieferer.

MARCO SCHLUMMER

- Studium der Sicherheitstechnik an der Bergischen Universität Wuppertal
  - Schwerpunkt: Verkehrssicherheit
  - Anstellung als SHK am Lehrstuhl „Sicherheitstheorie und Verkehrstechnik“
  - Studien- & Diplomarbeit in der Elektronikforschung der Volkswagen AG
    - erste Berührungspunkte mit Bereich „Funktionale Sicherheit“
    - Anpassung der Risikoanalyse gemäß IEC 61508 an die Automobilindustrie am Beispiel eines elektromechanischen Bremskraftverstärkers
- Wissenschaftlicher Mitarbeiter am Lehrstuhl „Sicherheitstheorie und Verkehrstechnik“
  - Durchführung von Vorlesungen, Übungen und Laborveranstaltungen
  - Bearbeitung von Drittmittelprojekten mit Automobilindustrie
  - Promotionsthema: Beitrag zur Entwicklung einer alternativen Vorgehensweise für eine Proven-in-Use-Argumentation in der Automobilindustrie
- seit Mai 2012: Geschäftsführer der Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH (kurz IQZ)
  - Leiter des Bereichs „Funktionale Sicherheit“
- seit 2012: Lehrauftrag an der BUW für „Funktionale Sicherheit“

Agenda

Vorstellung IQZ

Einführung in die Funktionale Sicherheit

Sicherheitsgrundnorm DIN EN 61508

- Aufbau, Struktur, Inhalte
- Sicherheitslebenszyklus
- Derivate

ISO 26262

- Vorstellung, Allgemeines und Historie
- Grundlegende Konzepte und Ziele
- Aufbau, Struktur und Inhalt
- Automotiver Sicherheitslebenszyklus
- Vorstellung wichtiger Kernaktivitäten

Zusammenfassung

VORSTELLUNG DES IQZ

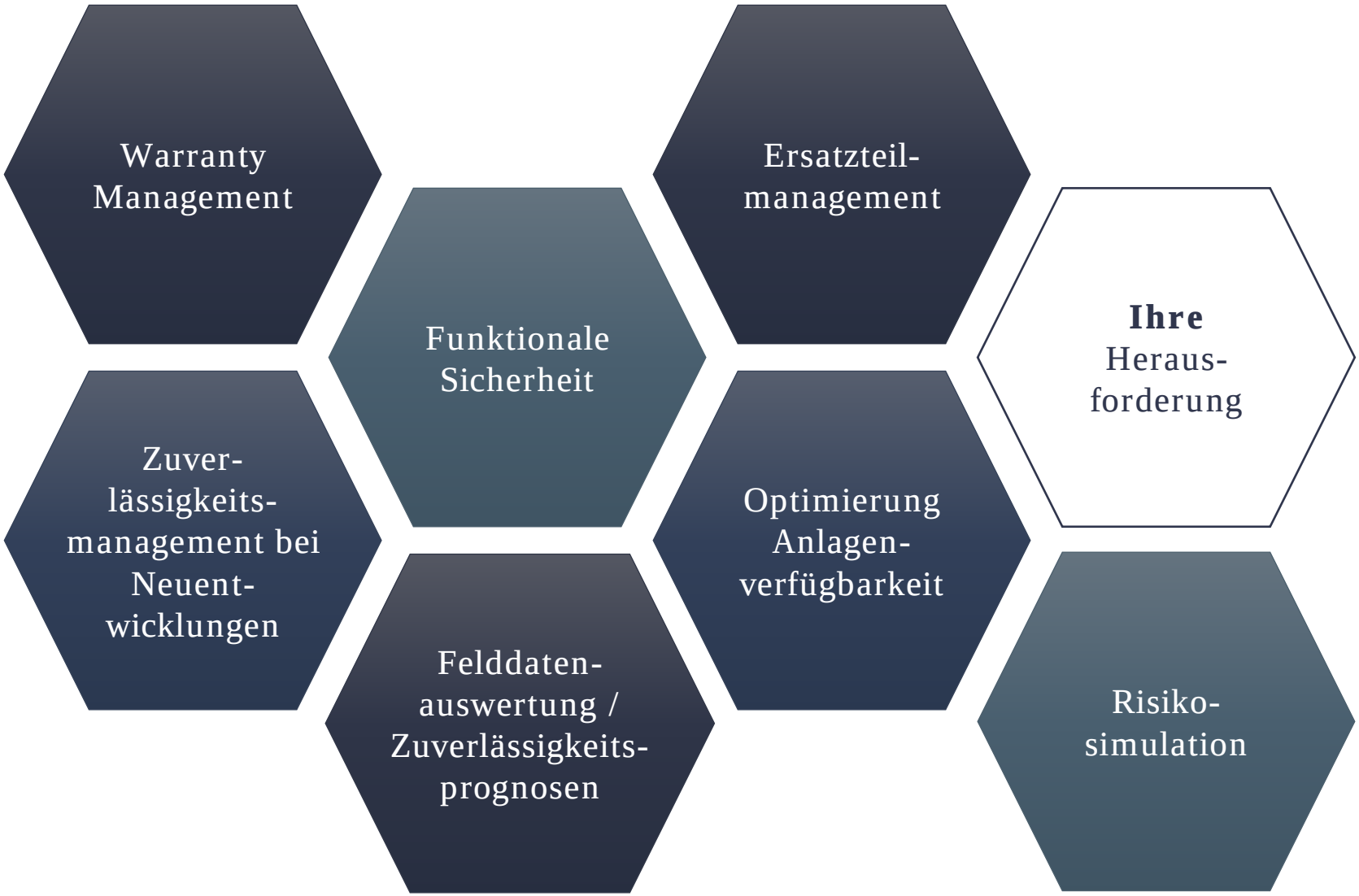
INSTITUT FÜR QUALITÄTS- UND ZUVERLÄSSIGKEITSMANAGEMENT GMBH

Beratungs- und Forschungsdienstleistung auf Stand von Wissenschaft und Technik:

„Wir helfen bei der Entwicklung sicherer und zuverlässiger Produkte und Prozesse.“

Kennen Sie diese Herausforderungen?

Unsere Hauptgeschäftsfelder

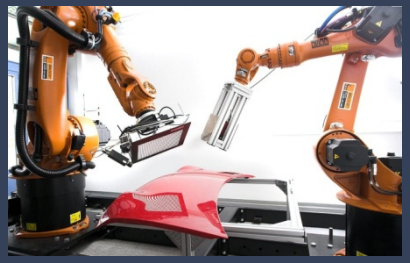


Einige unserer Partner

Einführung in die Funktionale Sicherheit

Warum Funktionale Sicherheit?

- Elektronik unterstützt den Menschen bei verschiedensten Tätigkeiten

Arbeitsmittel	Freizeitgestaltung	Kommunikation	...
			
Quelle: Bogen	Quelle: Acer & Sony	Quelle: Apple	

- Entwicklung spiegelt sich auch im Automobilsektor wider
  - nahezu jeder Bereich und jede Funktion im Kfz beruht auf dem Einsatz von Elektrik und Elektronik (E/E)
  - Bsp.: Fahrerassistenzsysteme, wie ABS oder ESP
    Komfortsysteme, wie Navigationsgeräte
    Motorsteuerung
    Fahrwerksabstimmung

Elektronische Systeme sind unverzichtbarer Bestandteil des täglichen Lebens

Warum Funktionale Sicherheit?

- moderne, technische Systeme, die sicherheitskritische Prozesse steuern und regeln, werden zunehmend komplexer
  - mechanische Systeme werden durch elektronische oder mechatronische ergänzt bzw. abgelöst
  - vielschichtige, verflochtene Systemverbünde
- Anforderungen an ein System werden immer vielfältiger
  - Aspekte wie Kosten, Wettbewerb, Leistungsfähigkeit, Umwelt, Sicherheit und Zuverlässigkeit spielen hierbei eine große Rolle
  - fast nur noch durch Einsatz von Elektronik & Software machbar
- Beispiele für sicherheitskritische Aufgaben
  - Überwachung von Fahrzeugzuständen und Fahrsituationen
  - Steuerung von Zügen
  - Regelung von Prozessen in chemischen Anlagen
  - Roboter-Operationssysteme im medizinischen Bereich

Branchen-unabhängig

Sicherheitskritische Funktionen stellen Herausforderungen an alle Branchen

WARUM FUNKTIONALE SICHERHEIT?

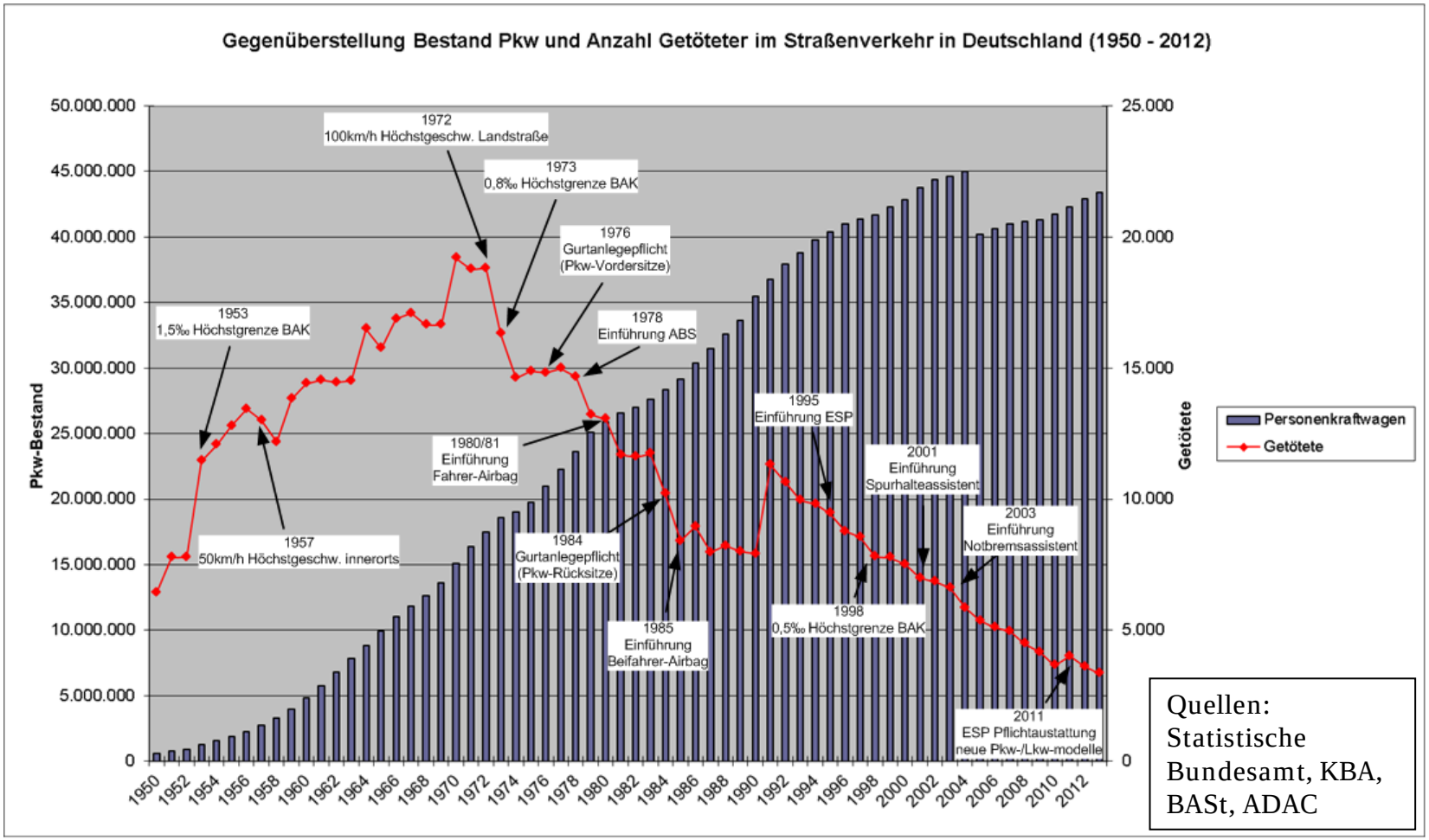
- Fehlfunktionen oder Ausfall beteiligter Systeme können schwerwiegende Folgen nach sich ziehen
  - Sachschäden
  - Gefährdung der Umwelt
  - Gefährdung von Menschenleben im Alltagsleben
- Systeme, die nicht vor Missbrauch geschützt sind oder technische Defizite aufweisen, gelten als nicht sicher
  - erhöhtes Risiko für Personen im Umfeld
  - egal, ob Straßenfahrzeug, Haushaltgerät oder Produktionsanlage

„Funktionale Sicherheit“ oder

„Funktionssicherheit“

(FuSi)

VERKEHRSENTWICKLUNG IN DEUTSCHLAND



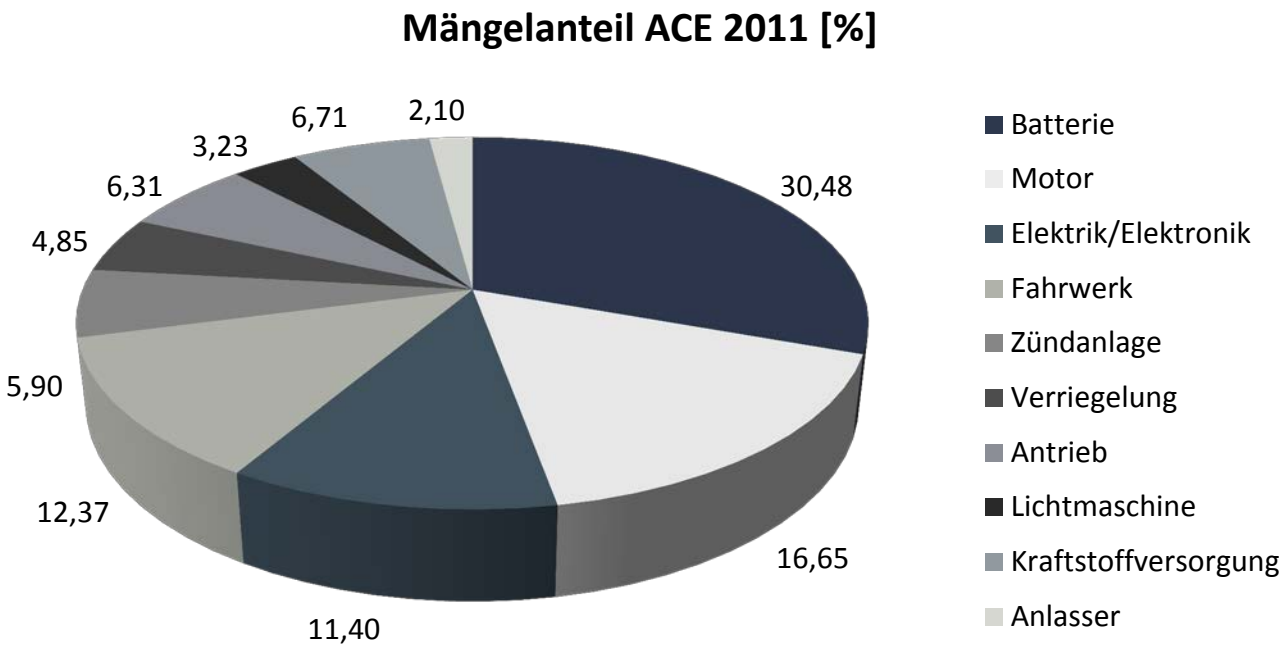
Positive Entwicklung der Zahl der Getöteten im deutschen Straßenverkehr

E/E-Systeme im Kfz

- Erhöhung von Verkehrssicherheit, Komfort, Leistung etc. bei gleichzeitiger Reduzierung von Kosten, Emissionen, Verbrauch etc.
  - Elektronik, Mechatronik und Informationstechnik sind Schlüsselindustrien der Automobilbranche
  - „rund 80% bis 90% aller Innovationen in Maschinen und Autos gehen auf mechatronische und elektronische Erfindungen zurück“ (Prof. Isermann, TU Darmstadt, 2003)
  - Elektronikanteil an Wertschöpfungskette: ~35% (Reiff, 2011)
- Systeme werden zunehmend komplexer
  - heutiges Automobil hat deutlich höhere Rechenleistung als das Raumfahrzeug Apollo 13
  - moderne Oberklasse-Fahrzeuge verfügen über mehr als 80 Steuergeräte (aktuelle A8: ~50 Haupt- und 50 kleinere SG)
  - umfangreiche Systemverbünde, bei denen Funktionen über mehrere Steuergeräte verteilt sind, die intelligent miteinander vernetzt sein müssen
- steigende Komplexität geht oftmals einher mit höheren Fehler- oder Ausfallanfälligkeit

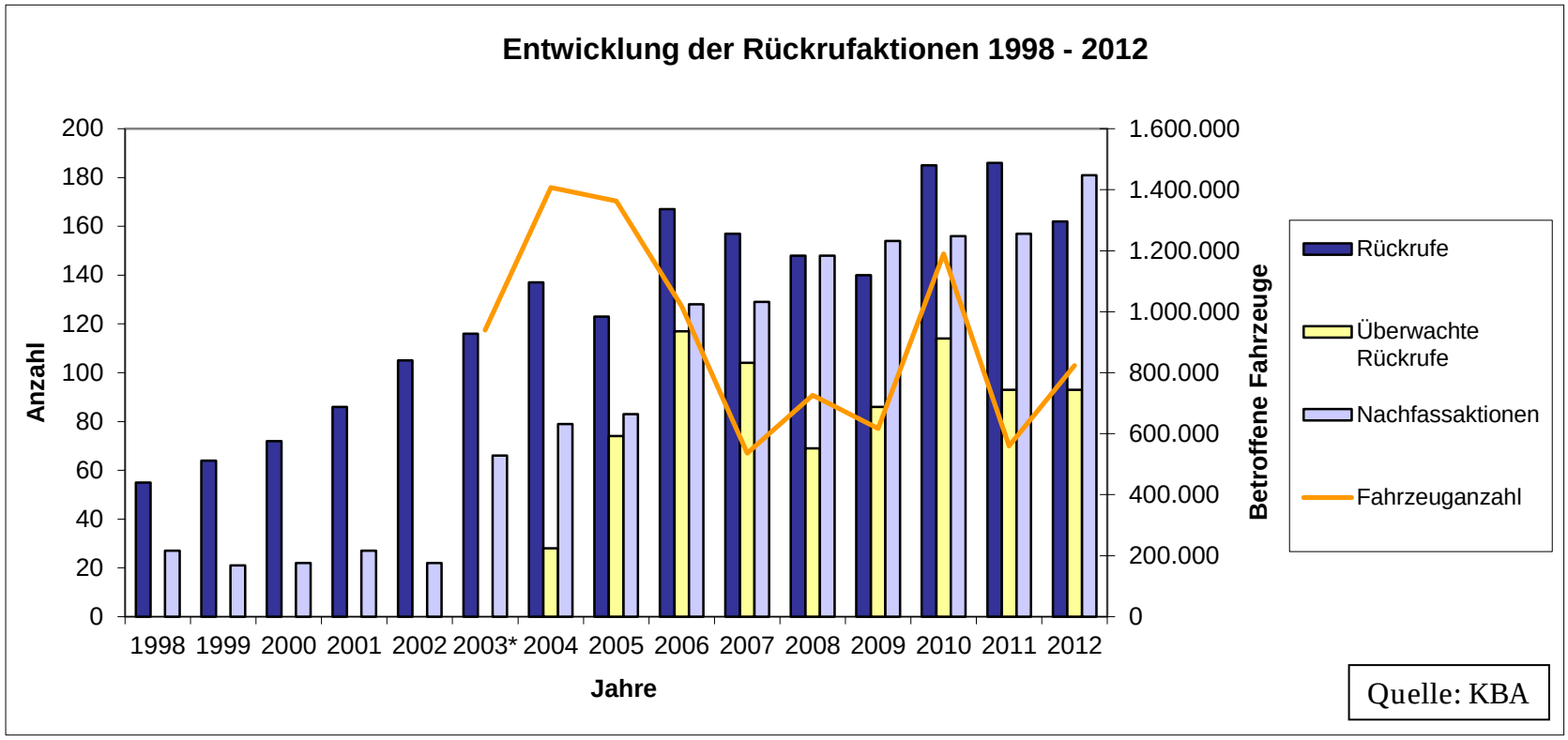
E/E-Systeme im Kfz sind unverzichtbar und werden immer komplexer

ACE-Mängelanteil Deutschland 2011



- störanfällige Elektrik/Elektronik auf Platz 3
  - andere Statistiken (z.B. ADAC) kamen in Vergangenheit auf deutlich höheren Anteil
    → inkl. Batterieproblemen (mittlerweile geändert)
  - kein Problem einzelner Hersteller → Branchenproblem
- oft: Pauschalisierung der Elektronikpannen

Rückrufaktionen in Deutschland 1998 – 2012



- baugruppenbezogene Rückrufursachen 2012:
  - über 70% mechanische Ursachen
  - knapp 20% Elektrik/Elektronik (mech./hydraul. Probleme teils mit einbezogen)

Aktuelle Aktionen der Automobilhersteller

- 2014-02: Toyota startet Prius-Massenrückruf (1,9 Millionen Fahrzeuge weltweit)
  - Softwareprobleme können bei wiederholt starker Beschleunigung zu einer Überbelastung der Hybrid-Regelelektronik führen
- 2014-02: Porsche stoppt Auslieferung des neuen 911 GT3
  - aufgrund von bisher unerfindlichen Gründen sind 2 Neufahrzeuge ausgebrannt
  - bereits verkaufte Modelle werden mit neuen Motoren ausgestattet
- 2014-03: Nissan ruft in den USA fast 1 Million Autos zurück
  - möglicher Defekt des Beifahrer-Airbags aufgrund eines Software-Fehlers

- 2014-02-04: General Motors muss rund 2,6 Millionen Kompaktwagen zurückrufen
  - defektes Zündschloss, das bei Kontakt mit Fahrerknie oder durch Eigengewicht eines Schlüsselbundes in die Stellung „Zündung AUS“ zurückspringen kann
  - Es kann zur Abschaltung des Motors bei voller Fahrt sowie Deaktivierung von Servo-Unterstützung, Bremskraftverstärker und Airbags kommen
  - ➢ Mindestens **13 tödliche Unfälle** werden damit in Verbindung gebracht
  - ➢ direkte Kosten der Rückrufaktionen im ersten Quartal 2014: **750 Mio. $**
  - ➢ Einbruch des Gewinns in den ersten drei Monaten um **90%**

Rückrufaktionen können zu unkalkulierbaren Auswirkungen für den Hersteller führen

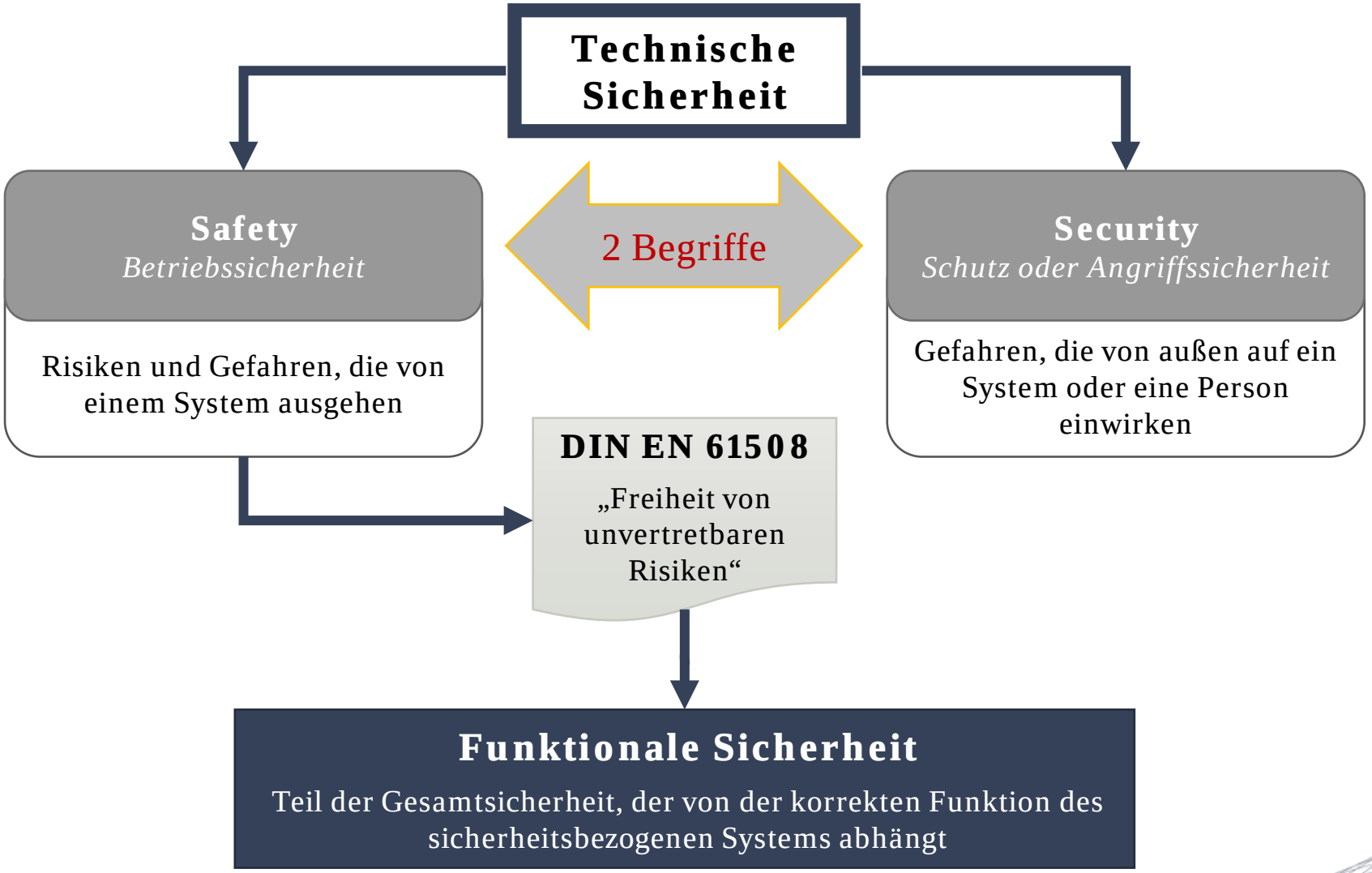
Zusammenfassung E/E im Kfz

- E/E-Systeme leisten erheblichen Beitrag zur Erhöhung der Verkehrssicherheit und Entlastung der Umwelt
- zunehmende Komplexität der Systeme führt zu steigenden Hardware-/Software-Problemen
- Fehler/Ausfall darf nicht zu Gefährdung von Verkehrsteilnehmern führen, wenn E/E-System direkt/indirekt steuernd eingreift
  - gilt nicht nur für so genannte Sicherheitssysteme

➢ **Folgerung**: Funktionale Sicherheit gewinnt immer mehr an Bedeutung
  - insbesondere bei sicherheitsrelevanten Systemen zur aktiven und passiven Sicherheit und deren Verbindung

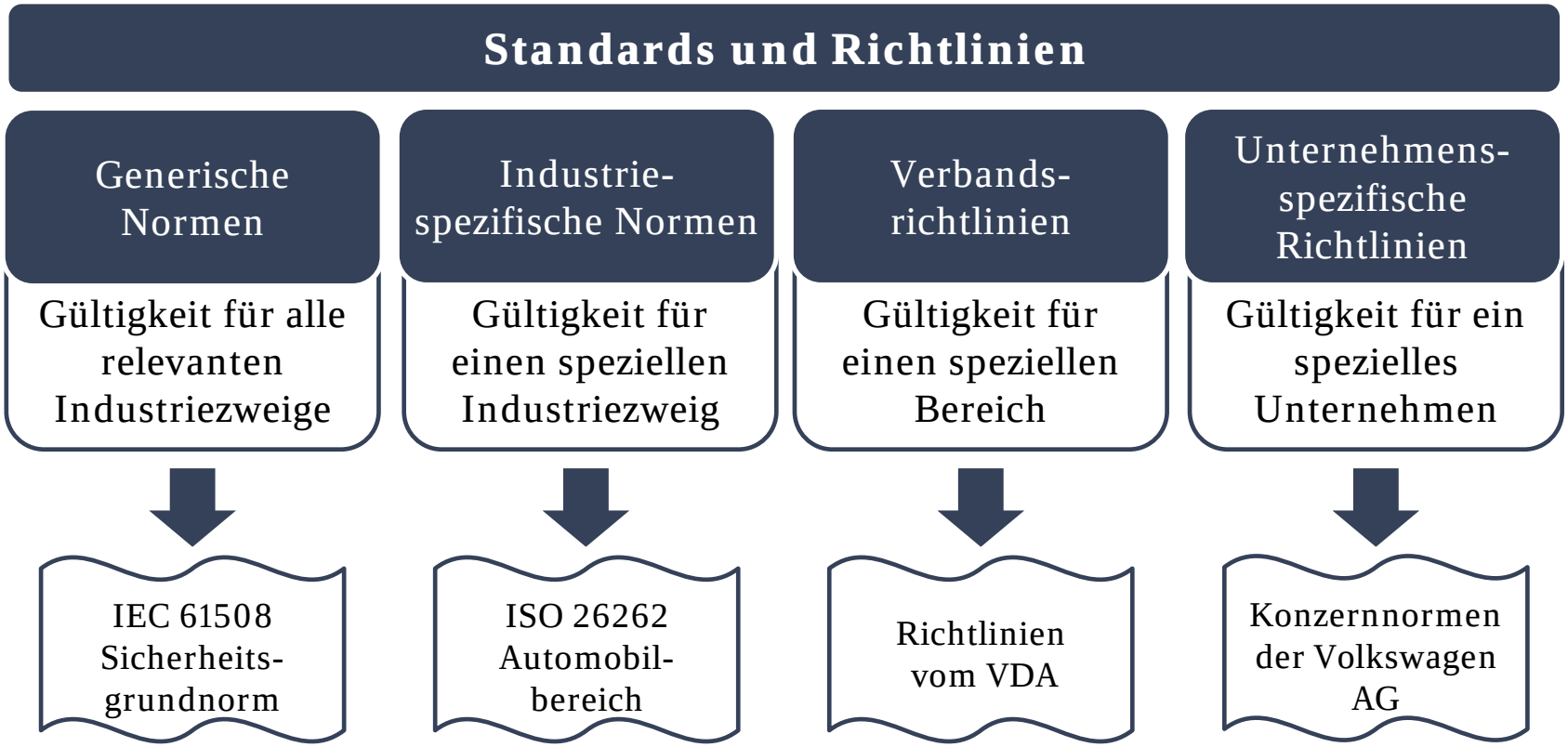
Funktionale Sicherheit im Automobilbereich wird immer wichtiger

Kontext der Funktionalen Sicherheit



Nexus der Funktionalen Sicherheit

- 1980/90er Jahre: erste Standardisierungsversuche



Steigende Bedeutung der Funktionalen Sicherheit in allen technischen Bereichen

DIN EN 61508

Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme

IEC 61508: Allgemeines

- Hintergrund der Normenreihe liegt in Anlagentechnik und Prozessindustrie
  - spiegelt sich in vielen Inhalten und Formulierungen wider
- Gründe für die Entwicklung
  - Schwierigkeiten beim Einsatz rechnerbasierten Systeme → kein international anerkannter Standard
  - bestehende Standards (z.B. EN 954) berücksichtigten die Belange der funktionalen Sicherheit nicht wirklich
- Chronologie
  - 1998: erstmalige Veröffentlichung der IEC 61508
  - Juli 2001: Ratifizierung durch CENELEC und Übernahme als europäische Normenreihe EN 61508
  - November 2002: Übernahme ins deutsche Normenwerk als DIN EN
  - 2010: Veröffentlichung überarbeiteter Versionen aller Teile (Februar 2011 auch auf deutsch)

IEC 61508: Aufbau

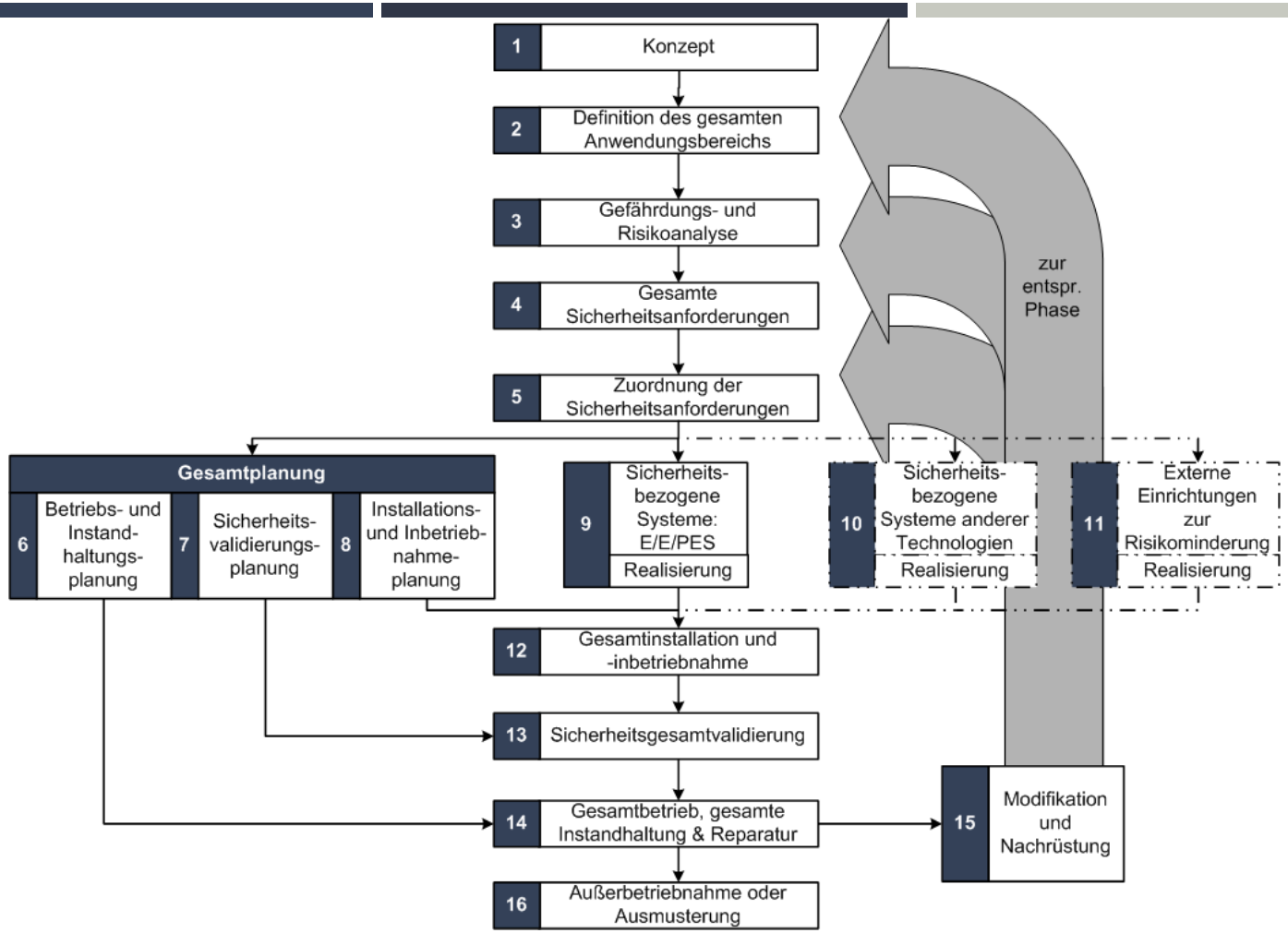
Teil 1	normativ	• Allgemeine Anforderungen
Teil 2		• Anforderungen an sicherheitsbezogene elektrische/ elektronische/programmierbar elektronische Systeme
Teil 3		• Anforderungen an Software
Teil 4		• Begriffe und Abkürzungen
Teil 5	informativ	• Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität
Teil 6		• Anwendungsrichtlinie für die Teile 2 und 3
Teil 7		• Anwendungshinweise über Verfahren und Maßnahmen

Normenwerk umfasst 7 Teile, wovon die ersten vier normativ sind

IEC 61508: EINFÜHRUNG

- FuSi ist gegeben, wenn jede spezifizierte Sicherheitsfunktion (SIF) ausgeführt wird und der für jede SIF geforderte Erfüllungsgrad erreicht wird
- Sicherheitsbezogenes System
  - Begriff „sicherheitsbezogen“ trifft auf jedes System zu, in dem ein Fehler (allein oder in Kombination mit anderen) zu Verletzung oder Tod von Menschen, katastrophalen Schädigungen der Umwelt oder Zerstörung von Sachgütern führen kann
  - schließt alles ein (Hardware, Software, Versorgungseinrichtungen, Personen), das zur Ausführung einer oder mehrerer SIF erforderlich ist
- Anwendung der Norm auf das gesamte sicherheitsbezogene System, welches die SIF ausführt
  - vom Sensor, über Steuerelektronik und Kommunikationssysteme bis zum Aktuator
  - Berücksichtigung möglicher Fehler des Bedienpersonals

IEC 61508: GESAMTER SICHERHEITSLEBENSZYKLUS



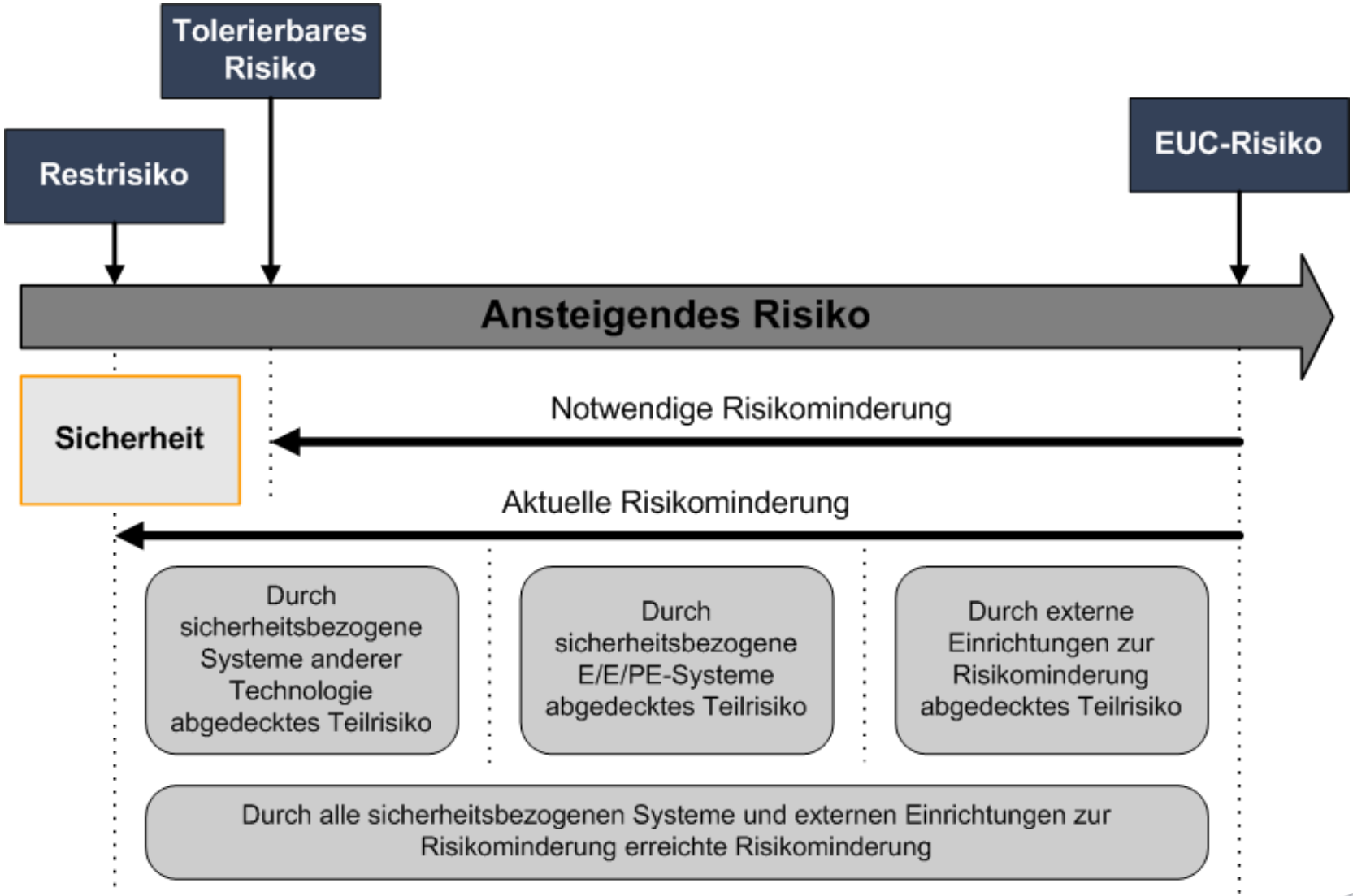
Sicherheitslebenszyklus begleitet Produkt von der ersten Idee bis zur Stilllegung

IEC 61508: RISIKOANALYSE UND SIL

- Gefährdungs- und Risikoanalyse
  - systematische Erfassung der potentiell vom betrachteten System (EUC, Equipment Under Control) ausgehenden Gefährdungen in allen Betriebsarten
- Sicherheitsintegritätslevel (SIL)
  - Ergebnis der Risikoanalyse
  - Sicherheitsintegrität:
    Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderte Sicherheitsfunktion unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraums anforderungsgemäß ausführt
    - ➢ Fähigkeit eines Systems, Fehler während des Betriebs zu erkennen und zu behandeln
  - vier diskrete Stufen (SIL 1 bis SIL 4)
    - SIL 4 stellt die höchste Stufe der Sicherheitsintegrität dar, SIL 1 die niedrigste
  - SIL-Bestimmung über verschiedene Verfahren möglich
    - ALARP
    - Risikomatrix
    - ➢ Risikograph (qualitatives, weit verbreitetes Verfahren)
- SIL-abhängige Anforderungen an den gesamten Sicherheitslebenszyklus

Je höher ein SIL desto geringer die Wahrscheinlichkeit, dass die geforderte Sicherheitsfunktion nicht ausgeführt werden kann

IEC 61508: Allgemeines Konzept der Risikominderung



IEC 61508 : Derivate

Landmaschinen
ISO 25119

Elektrische Antriebe
IEC 61800

Eisenbahnanwendungen
EN 5012x

Medizingeräte
IEC 60601

Straßenfahrzeuge
ISO 26262

IEC 61508

Metanorm

Prozessindustrie
IEC 61511

Medizin Gerätesoftware
IEC 62304

Kerntechnik
IEC 61513

Fertigungsindustrie
Bereich Maschinensicherheit
IEC 62061

Elektrische Ausrüstung
von Feuerungsanalagen
EN 50156

Ein Ziel der IEC 61508 war die Ableitung sektorspezifischer Normen zu ermöglichen

ISO 26262

ROAD VEHICLES - FUNCTIONAL SAFETY

ISO 26262: ALLGEMEINES

- Formulierung eines für die Automobilindustrie tauglichen, handhabbaren und international abgestimmten Sicherheitsstandards als anwendungsspezifische Ableitung der IEC 61508
- Normenwerk umfasst insgesamt 10 Teile, wobei der letzte Teil informativen Charakter hat
- FuSi für sicherheitsrelevante E/E-Systeme im Pkw (Gesamtgewicht bis 3,5t)
  - E/E entspricht E/E/PE aus IEC 61508
  - Pkw sind Fahrzeuge, die primär zum Transport von Personen einschließlich ihres Gepäcks und ihrer Waren konstruiert worden sind und neben dem Fahrersitz nicht mehr als acht Sitz- und keine Stehplätze haben
- Normenwerk sollte ursprünglich für alle Straßenfahrzeuge gelten
  - Anwendungsbereich wurde eingeengt
  - Nutzfahrzeuge, Lastkraftwagen, Busse und Motorräder werden explizit nicht erwähnt
  - formaljuristisch gilt hierfür folglich die IEC 61508

ISO 26262 ist das Derivat der IEC 61508 für die Automobilindustrie

ISO 26262: ALLGEMEINES

- im Geltungsbereich der ISO 26262
  - mögliche Gefährdungen aufgrund von Fehlfunktionen von sicherheitsrelevanten E/E-Systemen
- **nicht** im Geltungsbereich
  - mögliche Gefährdungen durch
    - elektrischen Schlag
    - Feuer
    - Rauch
    - Hitze
    - Entflammbarkeit
    - Strahlung
    - toxische Stoffe
    - Verätzung
    - Energiefreisetzung
  - sofern Gefährdungen nicht unmittelbar durch Fehlfunktion des E/E-Systems ausgelöst werden

Im Fokus sind Fehlfunktionen von E/E-Systemen

ISO 26262: Beteiligte (u.a.)

Deutschland	• u.a. BMW, Daimler, VW, BOSCH, SiemensVDO, ContiTeves, SGS TÜV Saar
Schweden	• u.a. Volvo, Mecel, BAE Systems
Frankreich	• u.a. PSA, RSA, Valeo
Österreich	• MagnaSteyr, ARC Seibersdorf Reasearch
Großbritannien	• Landrover, MIRA
Japan	• u.a. Nissan, JARI
Italien	• Fiat, CRF
USA	• TRW, Delphi, General Motors

An ISO-Arbeiten waren mehr als 80 Unternehmen und Institutionen aus 10 Nationen beteiligt

ISO 26262: HISTORIE

2002: erste Überlegungen hinsichtlich eines eigenen Automobilstandards von BMW angestoßen

2003: Arbeitsgremium des FAKRA nimmt Arbeiten auf (AK16)

2005: Überführung der Arbeiten in Normenausschuss Automobiltechnik des DIN unter Führung des VDA

2005: Überführung der Arbeiten in ISO mit Ziel der Standardisierung

- erste Sitzung Oktober/November 2005 mit den größten Fraktionen aus Deutschland und Frankreich

2007: Veröffentlichung als CD-Standard

- erste weltweite ISO-interne Abstimmung

2009: Veröffentlichung als ISO/DIS 26262

- allgemein zugänglich

seit November 2011 in Kraft (ohne Teil 10)

- Kommentierung hat längere Zeit in Anspruch genommen → seit August 2012 in Kraft

ISO 26262: ZUKÜNFTIGE AUSRICHTUNG

- ISO verbietet Ausweitung der Betrachtung auf **andere Fahrzeugklassen** nicht
  - Task-Force für Zweiräder (ISO/TC22/SC22) hat Arbeiten in 2013 aufgenommen
  - Erweiterung für Lkw ist vorgesehen

- publizierter Standard wird nach ISO-Regularien für 3 Jahre „eingefroren“
  - Arbeit an 2. Edition kann somit offiziell erst im November 2014 starten

- weitere Normenvorhaben in vielen Ländern
  - teils „nur“ Übersetzung (bisher nur Japan mit eigener Übersetzung)
  - teilweise auch Methodenentwicklung zur ISO 26262

Weiterentwicklung der ISO 26262 läuft bereits heute

ISO 26262: Konkrete Ziele

- Unter anderem:

Schaffung einheitlicher Bewertungsmaßstäbe für die sicherheitstechnische Beurteilung und in Produkthaftungsfragen

Schaffung von Transparenz bei Schnittstellen in komplexen Systemen und bei Entwicklungspartnerschaften zwischen OEM und Zulieferer

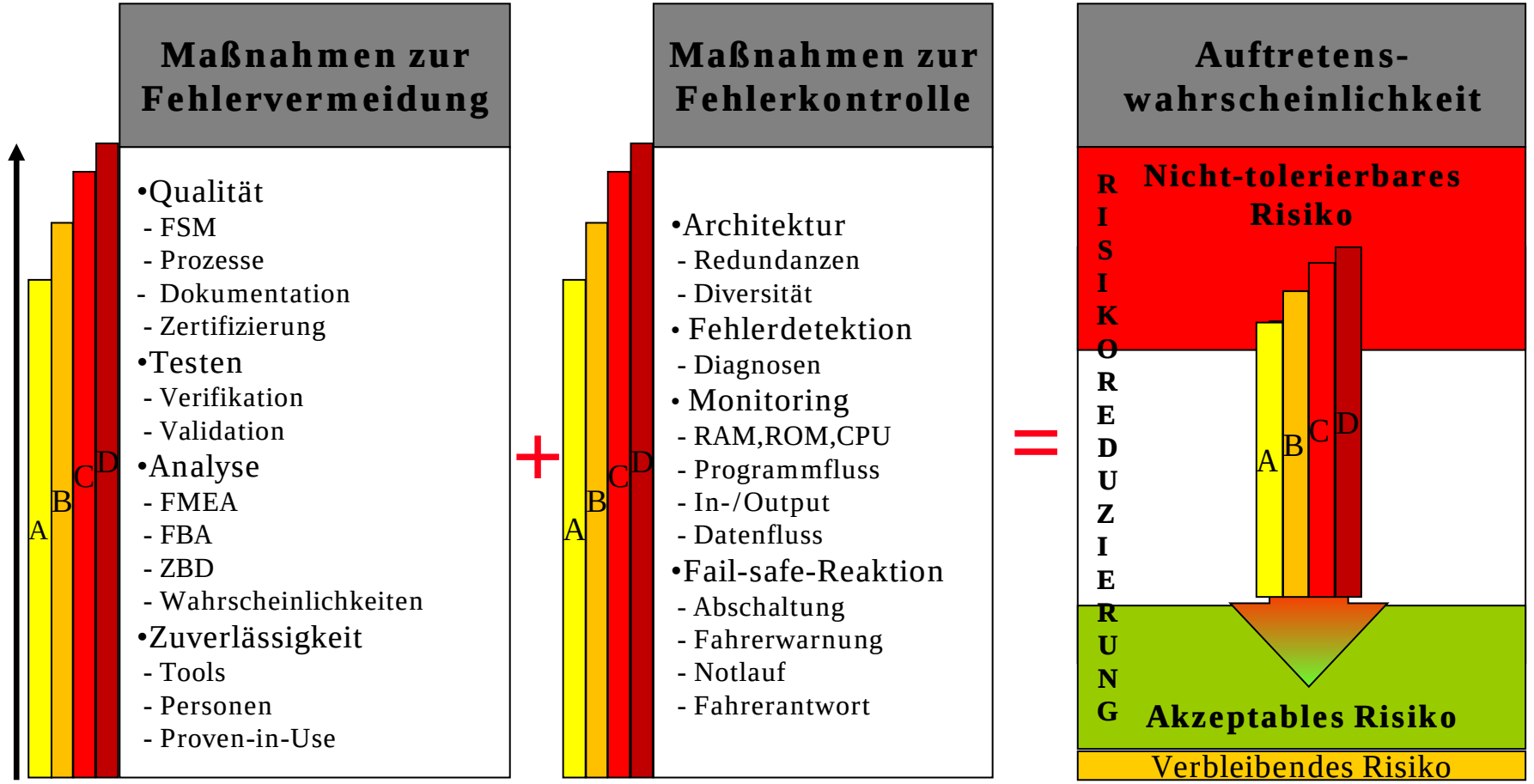
Zurverfügungstellung eines automobilspezifischen risikobasierten Ansatzes zur Ermittlung von Integritätslevel

Festlegung von Anforderungen an den gesamten automotiven Sicherheitslebenszyklus

Unterscheidung zwischen funktionalen („was“) und technischen Sicherheitskonzept („wie“)

Berücksichtigung von Produktion und Betrieb

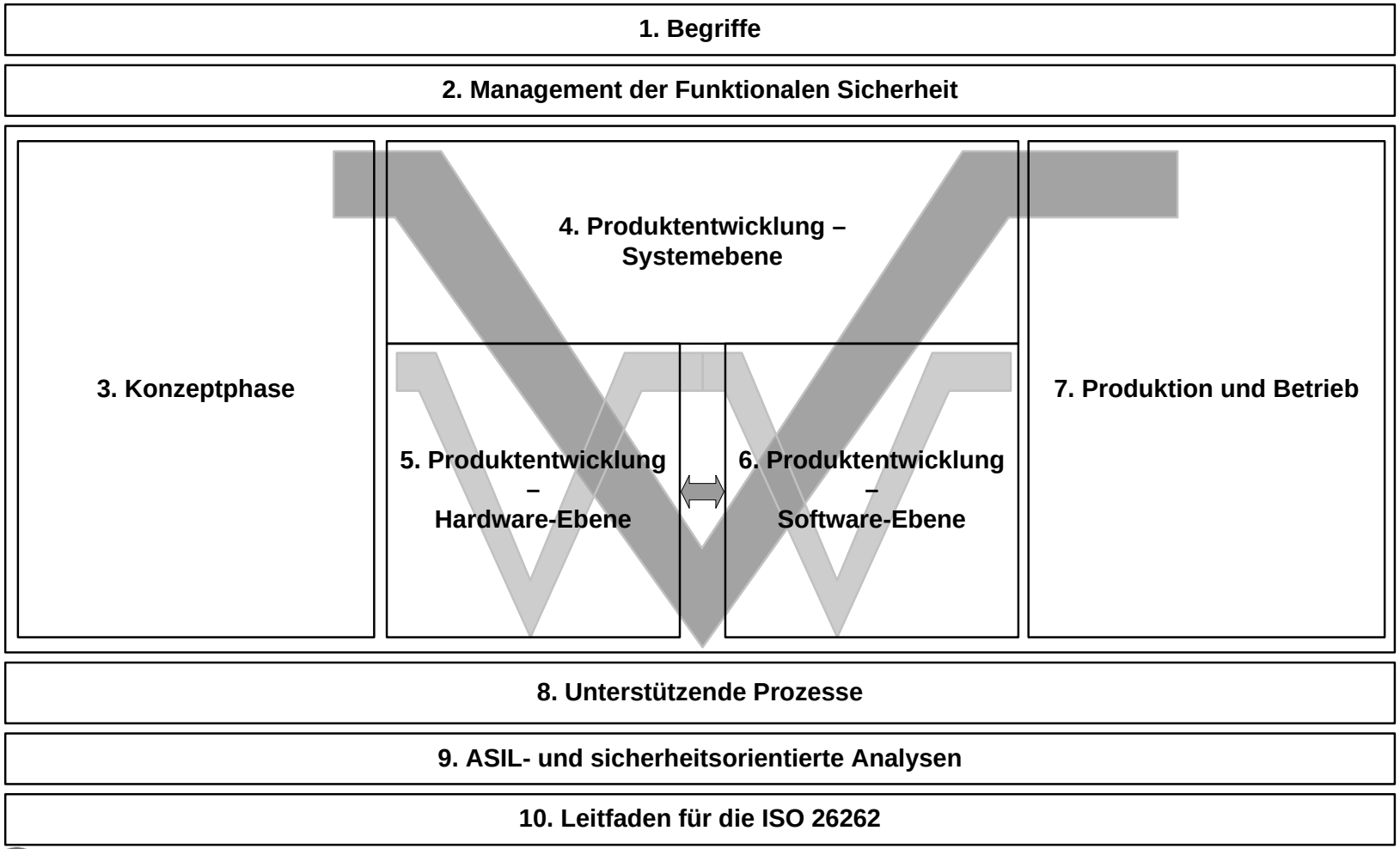
ISO 26262: Grundlegende Konzepte & Ziele



Quelle: Smuszynski, 2013

Kombination aus Maßnahmen zur Fehlervermeidung und Fehlerkontrolle

ISO 26262: Struktur und Inhalt (einfach)



Standard basiert in Teilen stark auf bekanntem V-Modell

ISO 26262: Struktur und Inhalt (detailliert)

1. Begriffe

2. Management der Funktionalen Sicherheit

- 2-5 Gesamtsicherheitsmanagement
- 2-6 Sicherheitsmanagement während Entwicklung
- 2-7 Sicherheitsmanagement nach Produktionsfreigabe

3. Konzeptphase

- 3-5 Identifikation des Gegenstands
- 3-6 Initiierung des Sicherheitslebenszyklus
- 3-7 Gefahrenanalyse und Risikobewertung
- 3-8 Funktionales Sicherheitskonzept

4. Produktentwicklung – Systemebene

- 4-5 Initiierung der Produktentwicklung auf System-Ebene
- 4-6 Spezifikation der technischen Sicherheitsanforderungen
- 4-7 Systementwurf
- 4-8 Gegenstandsintegration und -test
- 4-9 Sicherheitsvalidierung
- 4-10 Beurteilung der Funktionalen Sicherheit
- 4-11 Produktionsfreigabe

5. Produktentwicklung – Hardware-Ebene

- 5-5 Initiierung der Produktentwicklung auf Hardware-Ebene
- 5-6 Spezifikation der Hardware-Sicherheitsanforderungen
- 5-7 Entwurf der Hardware
- 5-8 Architektonische Hardware-Metriken
- 5-9 Bewertung der Verletzung von Sicherheitszielen durch zufällige HW-Ausfälle
- 5-10 HW-Integration und Test

6. Produktentwicklung – Software-Ebene

- 6-5 Initiierung der Produktentwicklung auf Software-Ebene
- 6-6 Spezifikation der Software-Sicherheitsanforderungen
- 6-7 Architektonischer Entwurf der Software
- 6-8 Entwurf und Implementierung der Software-Einheit
- 6-9 Test der Software-Einheit
- 6-10 SW-Integration und Test
- 6-11 Verifikation der SW-Sicherheitsanforderungen

7. Produktion und Betrieb

- 7-5 Produktion
- 7-6 Betrieb, Service (Instandhaltung und Reparatur) und Außerbetriebnahme

8. Unterstützende Prozesse

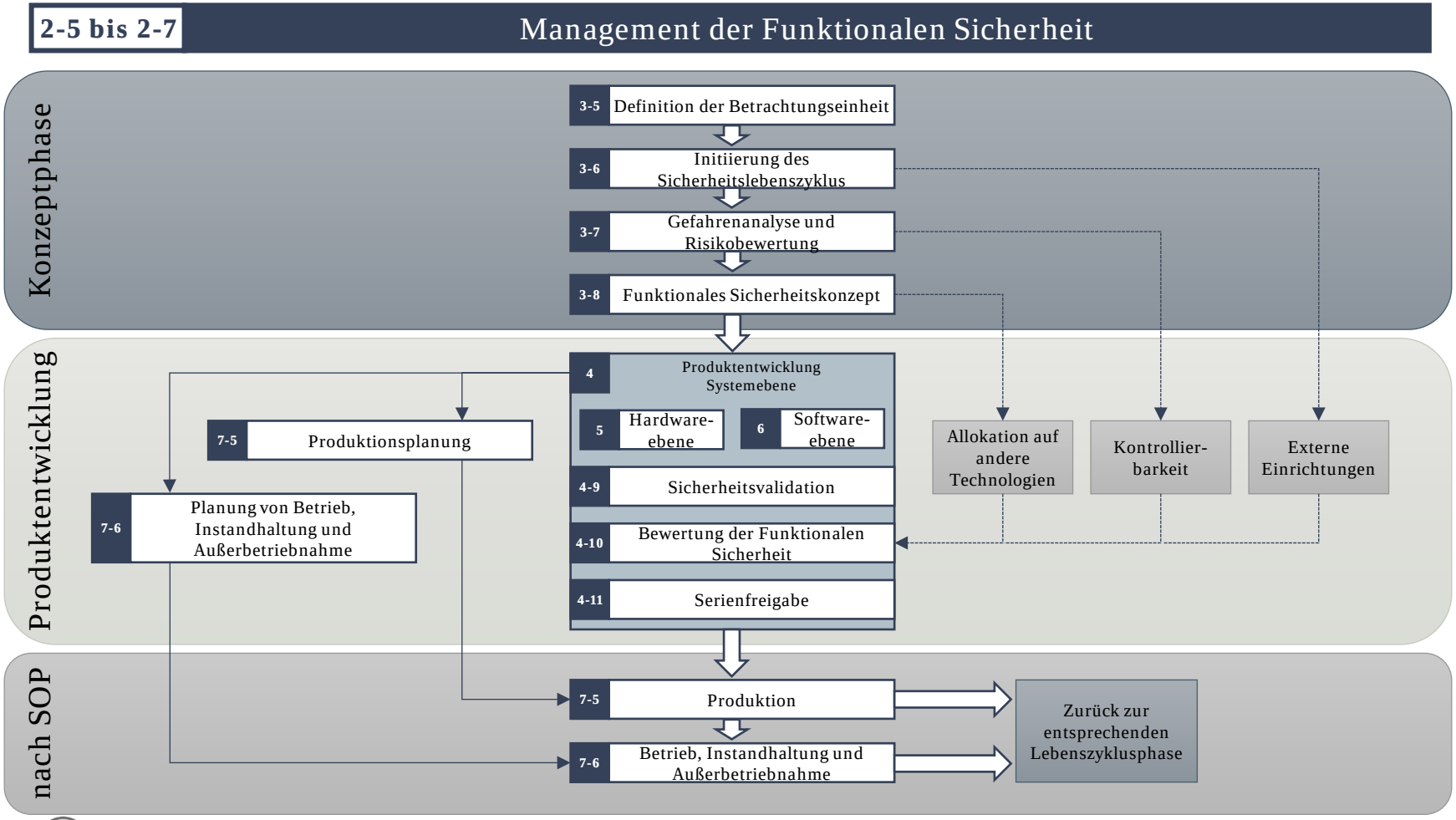
- 8-5 Schnittstellen innerhalb der verteilten Entwicklungen
- 8-6 Spezifikation und Management der Sicherheitsanforderungen
- 8-7 Konfigurationsmanagement
- 8-8 Änderungsmanagement
- 8-9 Verifikation
- 8-10 Dokumentation
- 8-11 Konfidenz in die Nutzung von SW-Tools
- 8-12 Qualifikation der SW-Komponenten
- 8-13 Qualifikation der HW-Komponenten
- 8-14 Proven-in-Use-Argumentation

9. ASIL- und sicherheitsorientierte Analysen

- 9-5 Dekomposition der Anforderungen nach ASIL-Tailoring
- 9-6 Merkmale einer Koexistenz von Elementen
- 9-7 Analyse abhängiger Ausfälle
- 9-8 Sicherheitsanalysen

10. Leitfaden für die ISO 26262

ISO 26262: Automotiver Sicherheitslebenszyklus



ISO 26262 gibt eigenen automotiven Sicherheitslebenszyklus vor

Allgemeine Informationen

- Vorwort
- Einleitung
- Kapitel 1: Anwendungsbereich
- Kapitel 2: Normative Referenzen
- Kapitel 3: Vokabular
- Kapitel 4: Anforderungen zur Normenerfüllung
  - Interpretation der Anforderungstabellen
  - Gültigkeit der Einzelanforderungen

Normenteile haben gleichen Aufbau

Spezifischer Inhalt

- Kapitel 5ff
  - Beschreibung Arbeitsschritte gemäß Entwicklungsmodell
- Kapitelstruktur
  - X.1: Ziele
  - X.2: Allgemeines
  - X.3: Input und Informationen
  - X.4: Anforderungen und Empfehlungen
  - X.5: Arbeitsergebnisse
- Anhänge

Anforderungskapitel sind gleich strukturiert

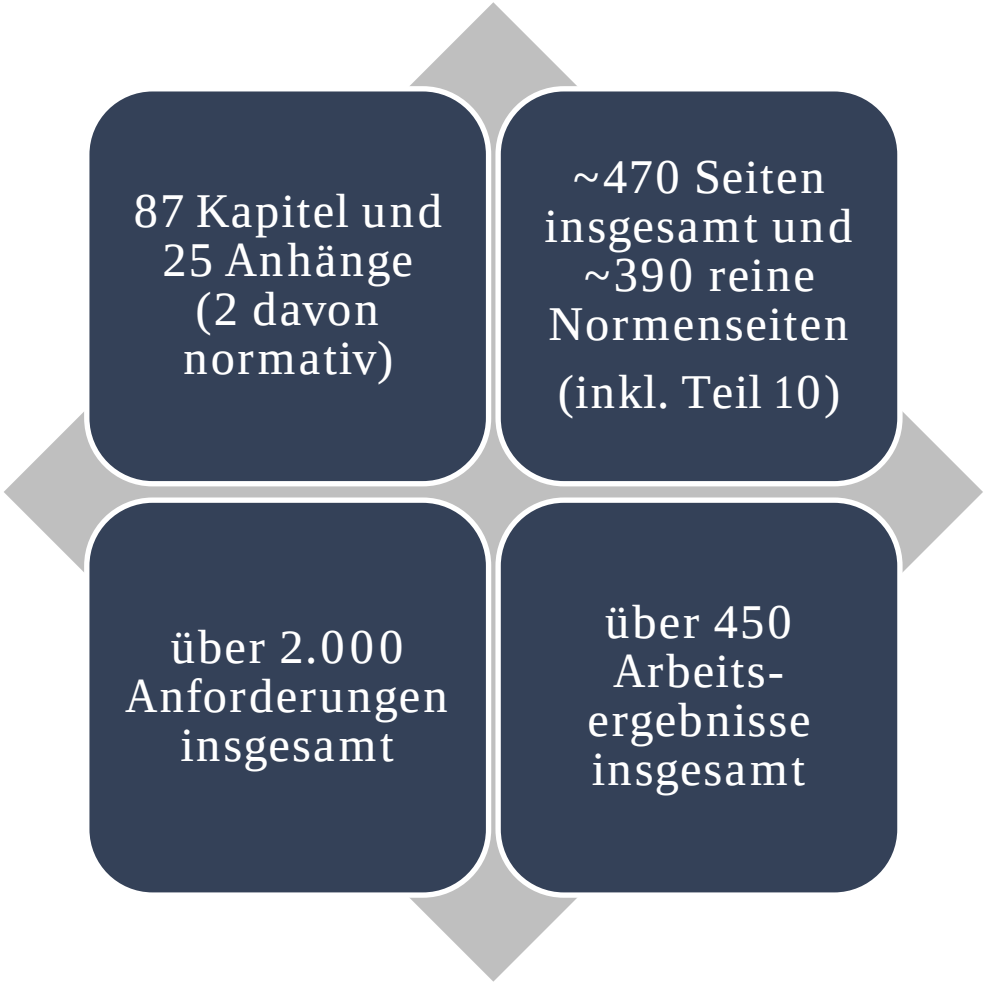
ISO 26262: Interpretation Anforderungstabellen

- Tabellen mit ASIL-abhängigen Methoden
- jede Methode hat
  - fortlaufende Nummerierung (z.B. 1, 2, 3, 4) → **Alle anwenden!**
  - alternative Nummerierung (z.B. 2a, 2b, 2c) → **Angemessene Auswahl!**
- Kategorisierung der Empfehlungen
  - „++“ *method is highly recommended*
  - „+“ *method is recommended*
  - „o“ *no recommendation for or against the method*

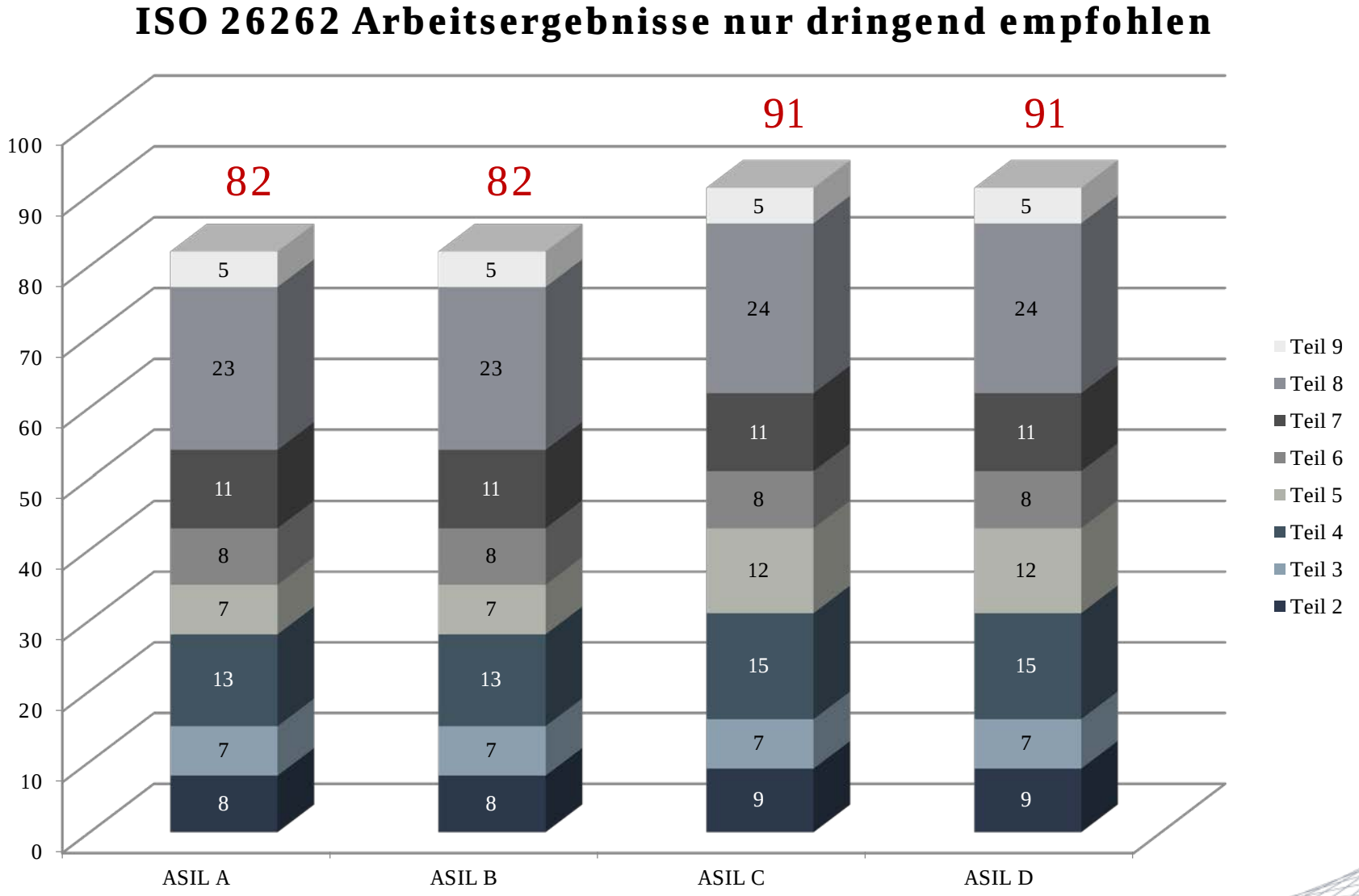
	Method	ASIL A	ASIL B	ASIL C	ASIL D
1a	**Hardware design walk-through**	++	++	o	o
1b	**Hardware design inspection**	+	+	++	++
2	**Safety analysis**	in accordance with 7.4.3			
3a	**Simulation**	o	+	+	+
3b	**Development by hardware prototyping**	o	+	+	+

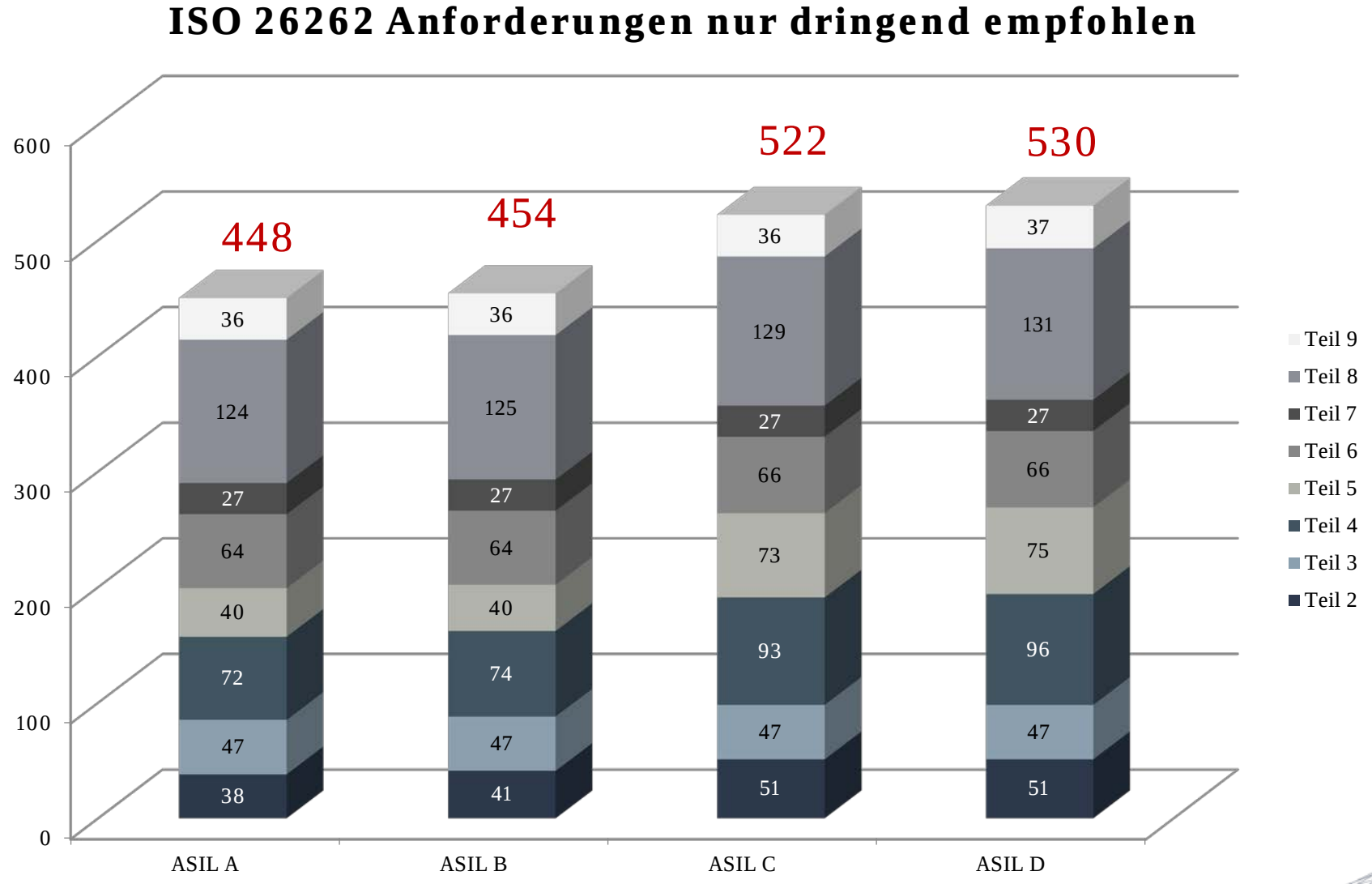
Auf fortlaufende und alternative Nummerierung bei Anforderungstabellen achten!

ISO 26262: Zahlen



ISO 26262 ist durchaus umfangreich und stellt Beteiligte vor Herausforderungen





ISO 26262-2

Management of Functional Safety

ISO 26262-2: MANAGEMENT

1. Begriffe

2. Management der Funktionalen Sicherheit

- 2-5 Gesamtsicherheitsmanagement
- 2-6 Sicherheitsmanagement während Entwicklung
- 2-7 Sicherheitsmanagement nach Produktionsfreigabe

3. Konzeptphase

- 3-5 Identifikation des Gegenstands
- 3-6 Initiierung des Sicherheitslebenszyklus
- 3-7 Gefahrenanalyse und Risikobewertung
- 3-8 Funktionales Sicherheitskonzept

4. Produktentwicklung – Systemebene

- 4-5 Initiierung der Produktentwicklung auf System-Ebene
- 4-6 Spezifikation der technischen Sicherheitsanforderungen
- 4-7 Systementwurf
- 4-8 Gegenstandsintegration und -test
- 4-9 Sicherheitsvalidierung
- 4-10 Beurteilung der Funktionalen Sicherheit
- 4-11 Produktionsfreigabe

5. Produktentwicklung – Hardware-Ebene

- 5-5 Initiierung der Produktentwicklung auf Hardware-Ebene
- 5-6 Spezifikation der Hardware-Sicherheitsanforderungen
- 5-7 Entwurf der Hardware
- 5-8 Architektonische Hardware-Metriken
- 5-9 Bewertung der Verletzung von Sicherheitszielen durch zufällige HW-Ausfälle
- 5-10 HW-Integration und Test

6. Produktentwicklung – Software-Ebene

- 6-5 Initiierung der Produktentwicklung auf Software-Ebene
- 6-6 Spezifikation der Software-Sicherheitsanforderungen
- 6-7 Architektonischer Entwurf der Software
- 6-8 Entwurf und Implementierung der Software-Einheit
- 6-9 Test der Software-Einheit
- 6-10 SW-Integration und Test
- 6-11 Verifikation der SW-Sicherheitsanforderungen

7. Produktion und Betrieb

- 7-5 Produktion
- 7-6 Betrieb, Service (Instandhaltung und Reparatur) und Außerbetriebnahme

8. Unterstützende Prozesse

- 8-5 Schnittstellen innerhalb der verteilten Entwicklungen
- 8-6 Spezifikation und Management der Sicherheitsanforderungen
- 8-7 Konfigurationsmanagement
- 8-8 Änderungsmanagement
- 8-9 Verifikation
- 8-10 Dokumentation
- 8-11 Konfidenz in die Nutzung von SW-Tools
- 8-12 Qualifikation der SW-Komponenten
- 8-13 Qualifikation der HW-Komponenten
- 8-14 Proven-in-Use-Argumentation

9. ASIL- und sicherheitsorientierte Analysen

- 9-5 Dekomposition der Anforderungen nach ASIL-Tailoring
- 9-6 Merkmale einer Koexistenz von Elementen
- 9-7 Analyse abhängiger Ausfälle
- 9-8 Sicherheitsanalysen

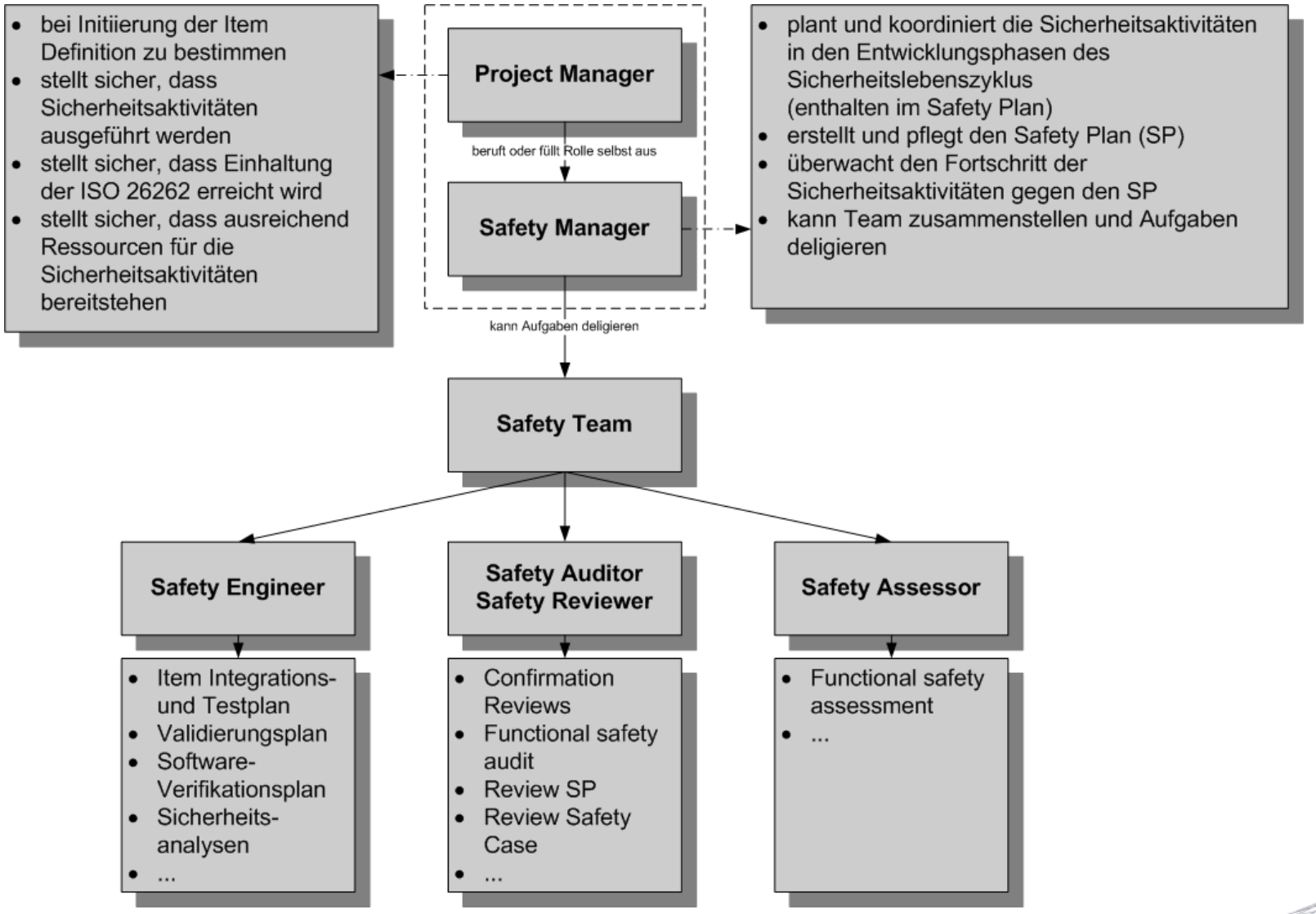
10. Leitfaden für die ISO 26262

Anforderungen werden u.a. gestellt an

die **Organisation**	das **Projektmanagement** über den gesamten Produktlebenszyklus hinweg	die **Absicherungs-maßnahmen** zum Nachweis der Normkonformität
Einführung einer Sicherheitskultur in das Unternehmen	Rollen und Verantwortlichkeiten (Project Manager, Safety Manager)	Functional Safety Audit
gelebtes Qualitätsmanagement gemäß ISO/TS 16949 oder ISO 9001	Planung und Koordinierung der Sicherheits-aktivitäten (Safety Plan, Safety Case)	Functional Safety Assessment

Die Management-Anforderungen lassen sich drei Bereichen zuordnen

ISO 26262-2: ROLLEN / VERANTWORTLICHKEITEN



„Confirmation Measures“ werden in 3 Aktivitäten unterteilt

- **Review**
  - Überprüfung der Ergebnisse von Arbeitsaktivitäten
- **Audit**
  - Untersuchung und Bewertung der implementierten Prozesse (Entwicklung, Unterstützung), die für die Funktionale Sicherheit erforderlich sind
- **Assessment**
  - Beurteilung der Funktionalen Sicherheit

Bei der Ausführung von Bestätigungsmaßnahmen sind ASIL-abhängige Unabhängigkeitslevel zu berücksichtigen

ISO 26262-2: BESTÄTIGUNGSMAßNAHMEN

- Bestätigungsmaßnahme darf grundsätzlich nicht von der erstellenden Person des Arbeitsergebnisses durchgeführt werden
- Unabhängigkeitsgrad

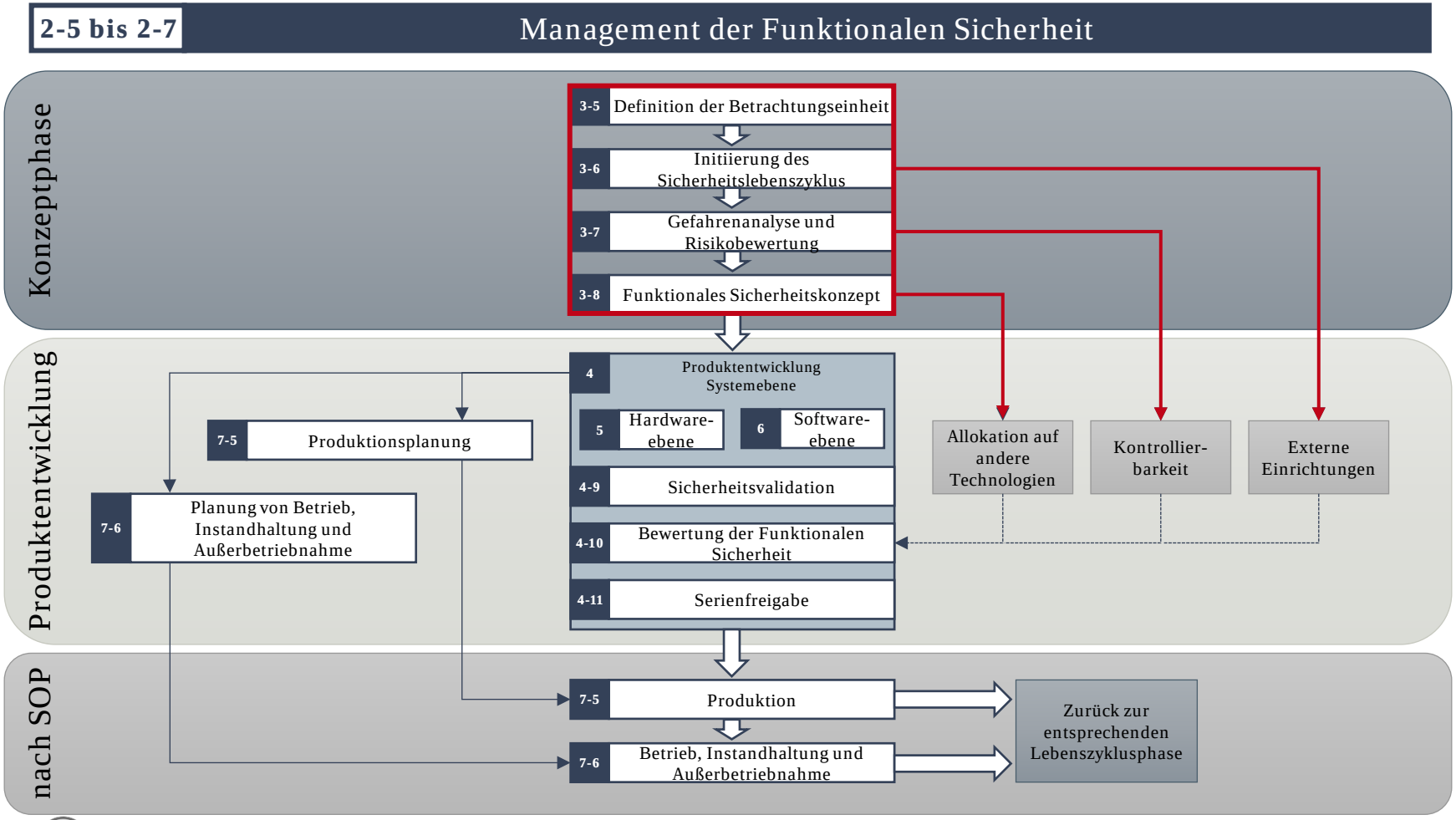
Level of Independence	Anforderungen
-	Keine Anforderung
I0	Bestätigungsmaßnahme sollte durchgeführt werden
I1	Bestätigungsmaßnahme soll durchgeführt werden
I2	Bestätigungsmaßnahme soll von einer Person aus einem anderen Team durchgeführt werden (unterschiedlicher direkter Vorgesetzter)
I3	Bestätigungsmaßnahme soll von einer Person aus einer anderen Abteilung oder Organisation durchgeführt werden (Unabhängigkeit bzgl. Management, Ressourcen und Verantwortung für Produktionsfreigabe)

Bestätigungsmaßnahmen werden für Arbeitsergebnisse gefordert, die spezifiziert sind und gemäß Sicherheitsplan gefordert werden

ISO 26262-3

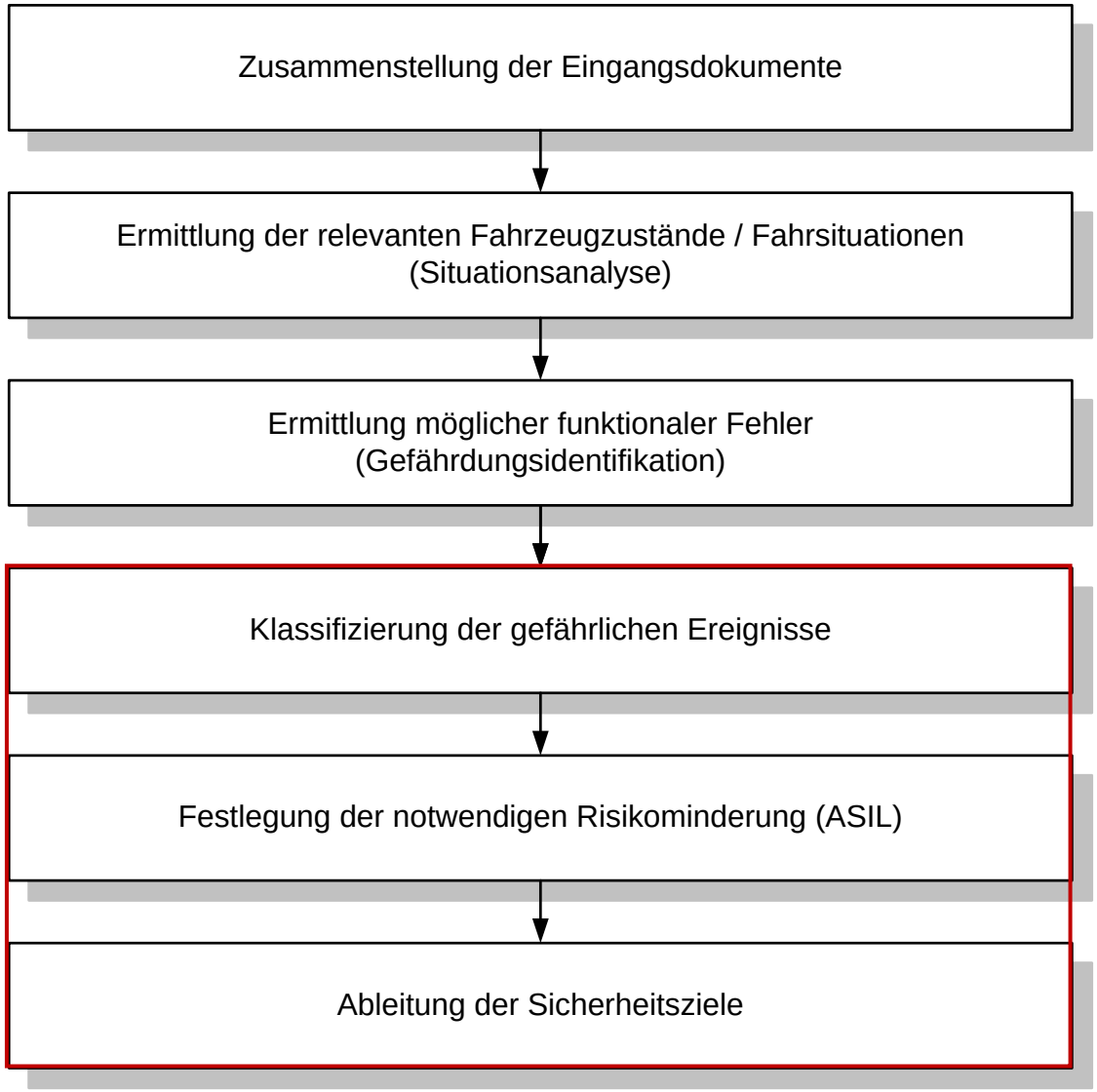
Concept Phase

ISO 26262: Automotiver Sicherheitslebenszyklus



ISO 26262 gibt eigenen automotiven Sicherheitslebenszyklus vor

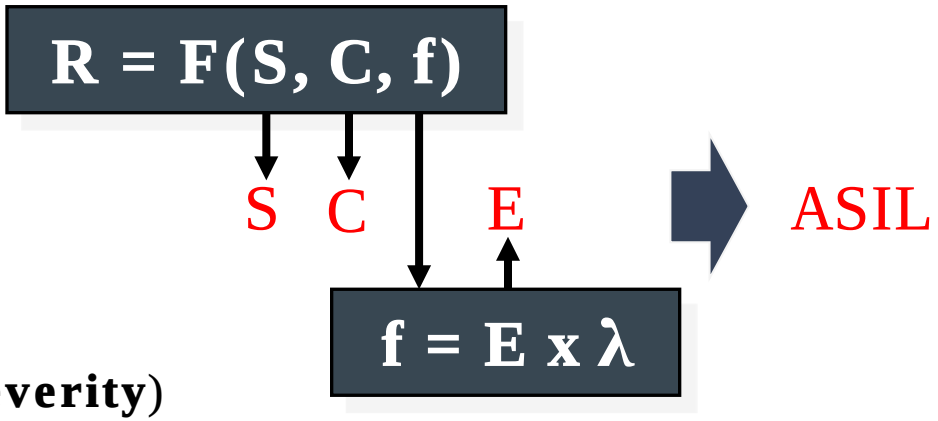
ISO 26262-3: Gefahrenanalyse und Risikobewertung (G+R)



Ziel:
Ermittlung des unerwünschten Verhaltens des Betrachtungsgegenstands, das zu einem gefährlichen Ereignis führen kann

Wichtig:
Jede Funktion des Item ist Gegenstand der G+R

Quelle: Löw, 2010



- R: Risiko
- S: Schadensausmaß (**Severity**)
- C: Möglichkeit der Gefahrenabwehr (**Controllability**)
- f: Auftretenshäufigkeit eines gefährlichen Ereignisses (Frequency of Occurrence)
- E: Wahrscheinlichkeit der Exposition (**Exposure**)
- λ: Ausfallrate des Betrachtungsgegenstands (charakterisiert durch zufällige HW-Ausfälle und systematische Systemfehler)

➢ Risikoparameter beschreiben Gefährdungssituation
  - Zuordnung von Parametereinstufungen zur Erleichterung der Festlegung

Risikobewertung basiert auf der allgemeinen Risikodefinition
Gefährdungssituation wird durch drei Risikoparameter S, C und E beschrieben

ISO 26262-3: G+R – SCHADENSSCHWERE (S)

Stufe	Beschreibung	Referenz
S0	Keine Verletzungen; nur Materialschaden Schaden kann nicht als sicherheitsrelevant angesehen werden	AIS 0
S1	Leichte und mäßige Verletzungen	AIS 1-2
S2	Schwere bis lebensgefährliche Verletzungen (Überleben wahrscheinlich)	AIS 3-4
S3	Lebensgefährliche Verletzungen (Überleben ungewiss), Fatale Verletzungen	AIS 5-6

Risikoparameter S beschreibt die mögliche Schadensschwere

ISO 26262-3: G+R – SCHADENSSCHWERE (S)

- AIS: Abbreviated Injury Scale
  - Klassifizierung der Verletzungsschwere bei Unfällen über sechs Schweregrade

Stufe	Beschreibung
AIS 0	Keine Verletzungen
AIS 1 …	Leichte Verletzungen, wie oberflächliche Wunden, Muskelschmerzen oder Schleudertrauma
AIS 3 …	Schwere Verletzungen (nicht lebensbedrohlich), wie Schädelfrakturen ohne Gehirnverletzungen, mehr als eine Rippenfraktur ohne paradoxische Atmung
AIS 6	Extrem kritische oder fatale Verletzungen

AIS-Klassifizierung unterstützt bei Einstufung des Risikoparameters S

ISO 26262-3: G+R – KONTROLLIERBARKEIT (C)

Stufe	Beschreibung	Definition
C0	Allgemein beherrschbar	Ablenkung
C1	Einfach beherrschbar	Mehr als 99% der durchschnittlichen Fahrer oder anderen Verkehrsteilnehmer sind in der Lage den Schaden abzuwenden
C2	In der Regel / Normal beherrschbar	Mehr als 90% der durchschnittlichen Fahrer oder anderen Verkehrsteilnehmer sind in der Lage den Schaden abzuwenden
C3	Schwer oder nicht beherrschbar	Der durchschnittliche Fahrer oder andere Verkehrsteilnehmer sind kaum in der Lage oder außerstande den Schaden abzuwenden

Risikoparameter C beschreibt die Kontrollierbarkeit einer Gefährdungssituation

ISO 26262-3: G+R – Aufenthaltshäufigkeit in Ausgangssituation (E)

Stufe	Beschreibung	Definition der Häufigkeit	Definition der Dauer
E0	Unvorstellbar	-	-
E1	Sehr geringe Wahrscheinlichkeit	Weniger als einmal pro Jahr	Nicht spezifiziert
E2	Geringe Wahrscheinlichkeit	Ein paar Mal im Jahr	Weniger als 1% der Betriebszeit
E3	Mittlere Wahrscheinlichkeit	Einmal pro Monat oder öfter	1% bis 10% der Betriebszeit
E4	Hohe Wahrscheinlichkeit	Fast bei jeder Fahrt	Mehr als 10% der Betriebszeit

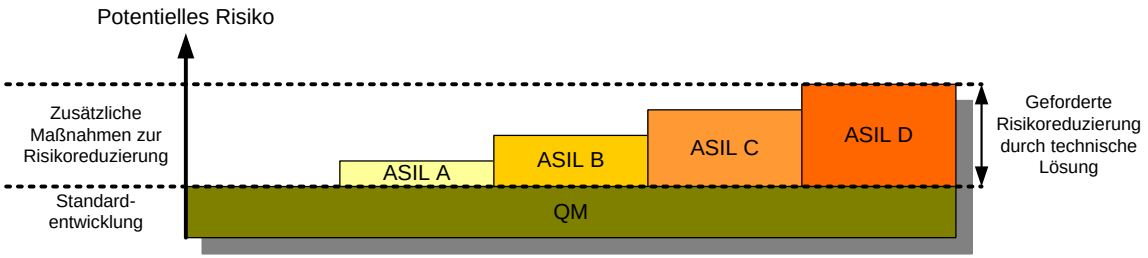
Risikoparameter E beschreibt die Exposition in der Gefährdungssituation

ISO 26262-3: ASIL-MATRIX

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
S3	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Bewertung	Summe
ASIL D	10
ASIL C	9
ASIL B	8
ASIL A	7
QM	≤6

- ASIL-Klassifizierung ist Ergebnis eines analytischen Vorgehens, um Risiken einer Funktion zu bewerten
- ASIL A ist die niedrigste und ASIL D die höchste Einstufung
- weitere Einstufungsmöglichkeit QM (Qualitätsmanagement)
  - keine besonderen Anforderungen
  - Schritte der Standardentwicklung sind ausreichend



Quelle: Dold, 2008

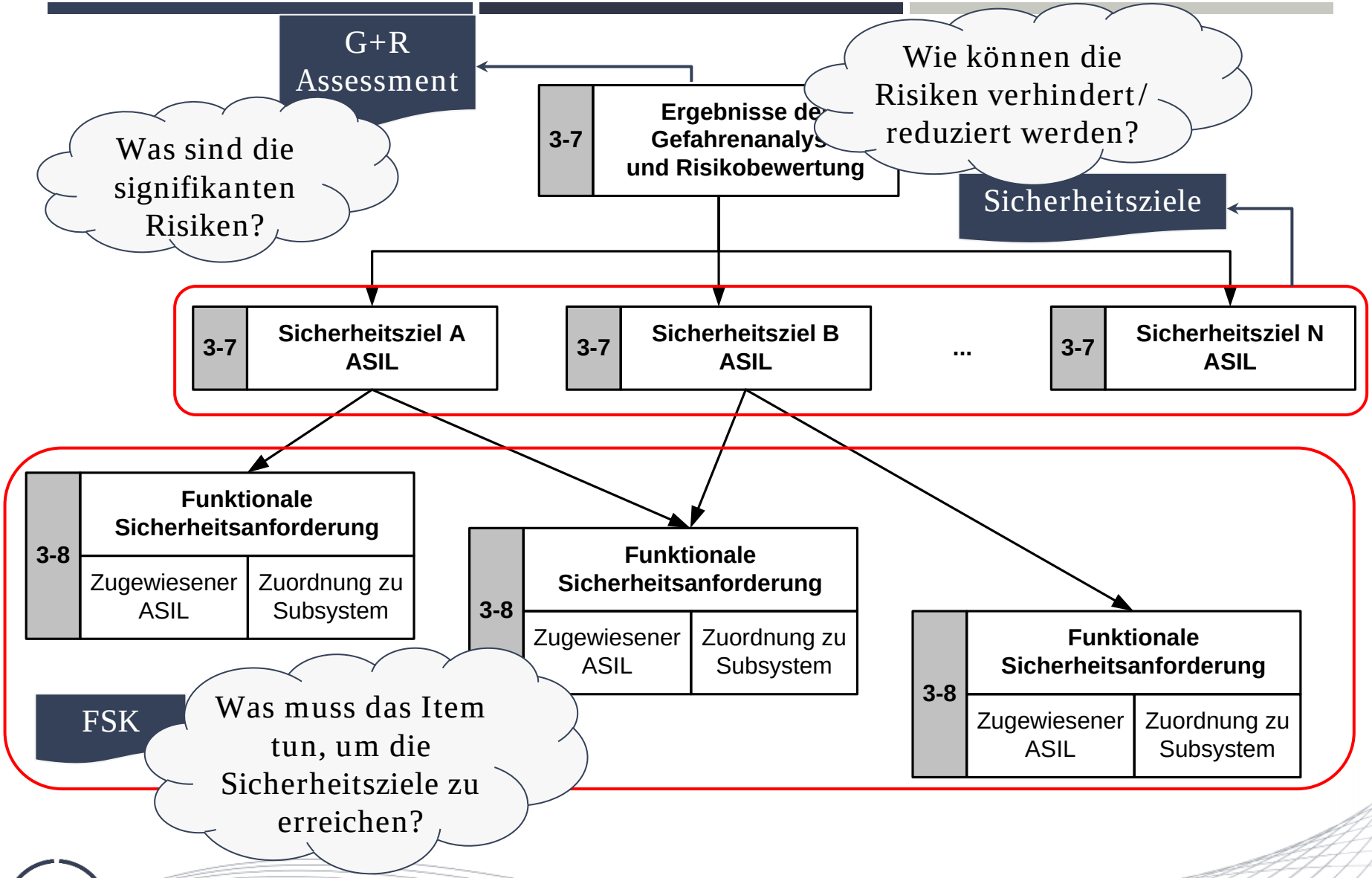
Kombination der Risikoparameter ergibt ASIL
Je höher die ASIL-Einstufung, desto höher die geforderte Risikoreduzierung

ISO 26262-3: SICHERHEITSZIEL

- Ableitung von Sicherheitszielen für jede mit einem ASIL eingestufte Gefährdungssituation
  - **Top-Level-Sicherheitsanforderungen**
    → alle anderen Sicherheitsanforderungen werden hiervon abgeleitet
  - werden auf Fahrzeugebene definiert
  - ähnliche Sicherheitsziele können zu einem Sicherheitsziel zusammengefasst werden
    → höchste ASIL gilt
  - funktionale, keine technischen Vorgaben
- Formulierung eines Sicherheitsziel:
  - *„Vermeide, dass mögliche Fehlfunktion zu einer Gefährdung führt“*
- Sicherheitsziele führen zu funktionalen Sicherheitsanforderungen, die zur Vermeidung von unzumutbaren Risiken erforderlich sind
- Sicherheitsziele sind Input für **funktionales Sicherheitskonzept**
  - mindestens eine funktionale Sicherheitsanforderung für jedes Sicherheitsziel

Sicherheitsziele sind die Top-Level-Sicherheitsanforderungen

ISO 26262-3: Sicherheitsziele & Funktionale Sicherheitsanforderungen



Funktionales Sicherheitskonzept (FSK)

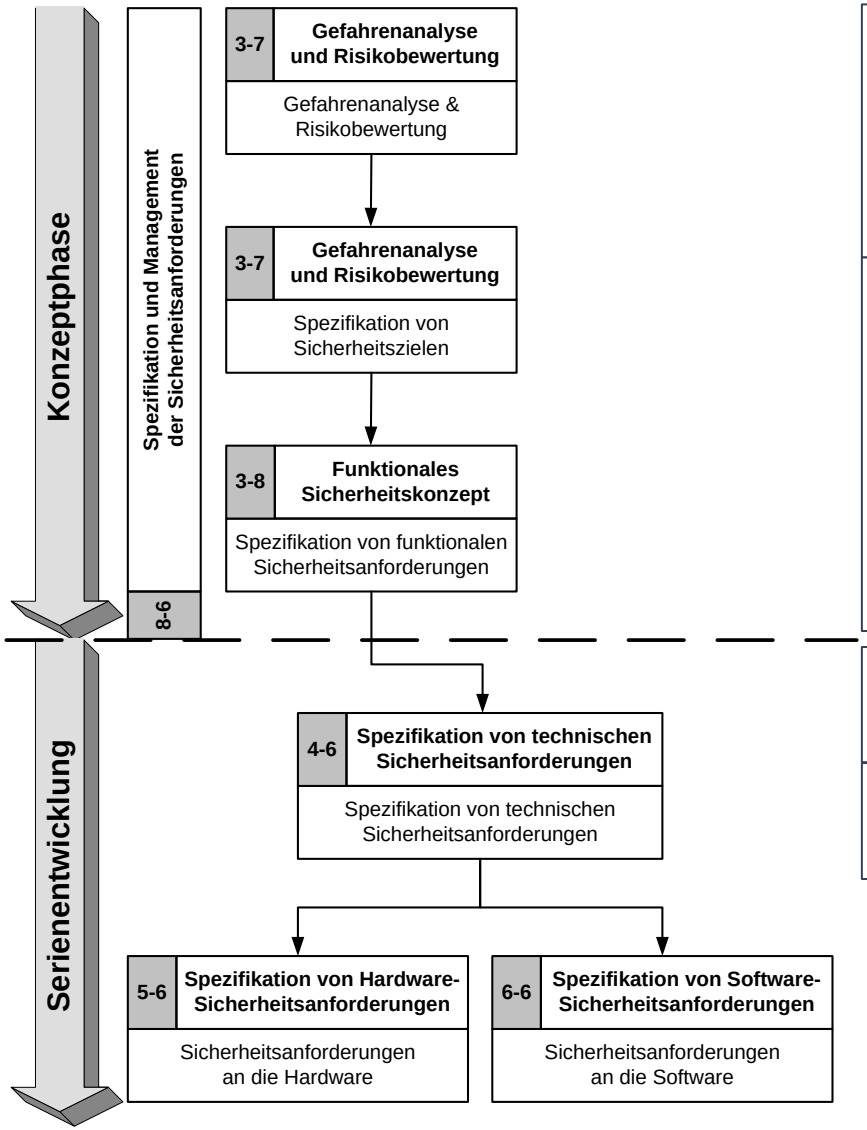
- spezifiziert in Form von funktionalen Sicherheitsanforderungen die grundlegende Funktionsweise des Sicherheitskonzepts, mit dem die Sicherheitsziele erfüllt werden sollen
- „Beschreibt, **was** getan werden muss“
- Funktionale Sicherheitsanforderungen sind prüfbare Anforderungen

Technisches Sicherheitskonzept (TSK)

- spezifiziert in Form von Sicherheitskonzeptanforderungen die grundlegende Verteilung der funktionalen Sicherheitsanforderungen auf die Systemarchitektur (Hard- und Software)
- „Beschreibt, **wie** es technisch implementiert werden muss“

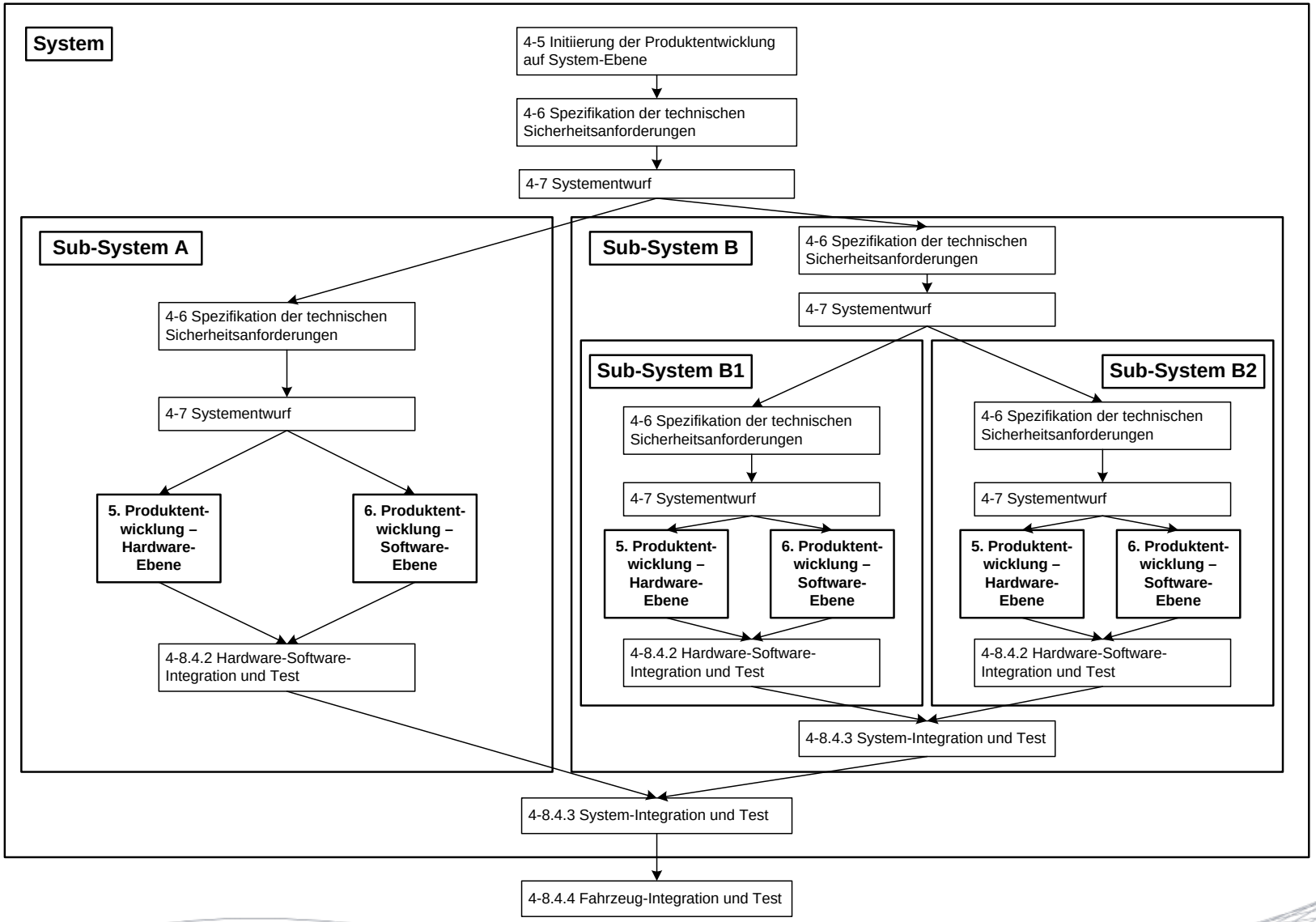
FSK = „Was“ / TSK = „Wie“

ISO 26262-4: FSK & TSK



- Gefährdungsidentifikation & Zuordnung der Risikoparameter
  - Selbstlenker
  - E4, S3, C3 → ASIL D
- Spezifikation der Sicherheitsanforderungen
  - Kein falscher Output darf Lenkung beeinflussen
  - Sicherheitsmaßnahmen einführen, die sicherheitsrelevante Fehler detektieren (z.B. Drehmomentüberwachung, Spannungsdiagnose)
- Realisierung der Sicherheitsmaßnahmen im Item
- Spezifikation der technischen Sicherheitsanforderungen
- Spezifikation des Systementwurfs
- Spezifikation von detaillierten HW- und SW-Sicherheitsanforderungen (aus TSK)

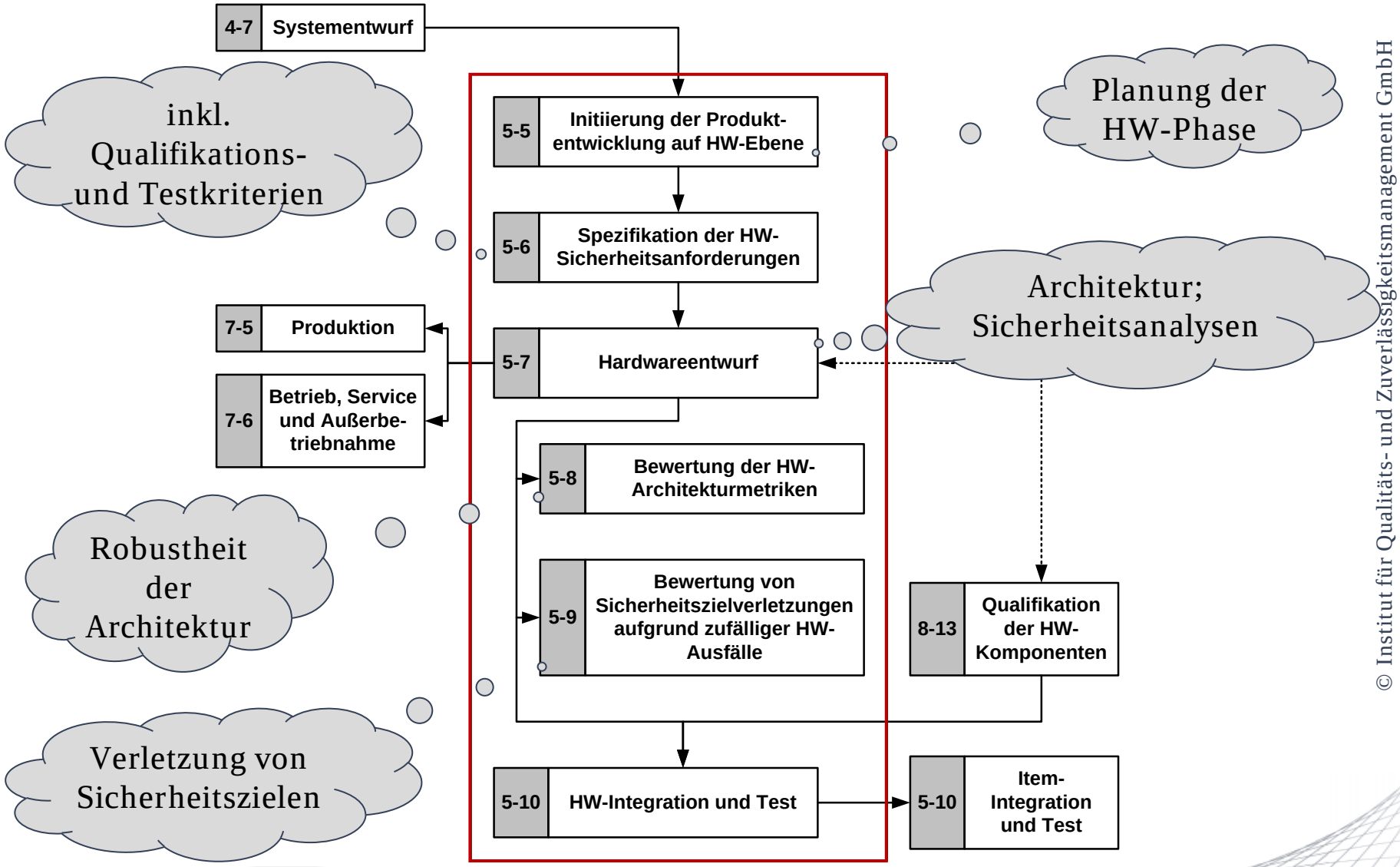
ISO 26262-4: PRODUKTENTWICKLUNG SYSTEMEBENE



ISO 26262-5

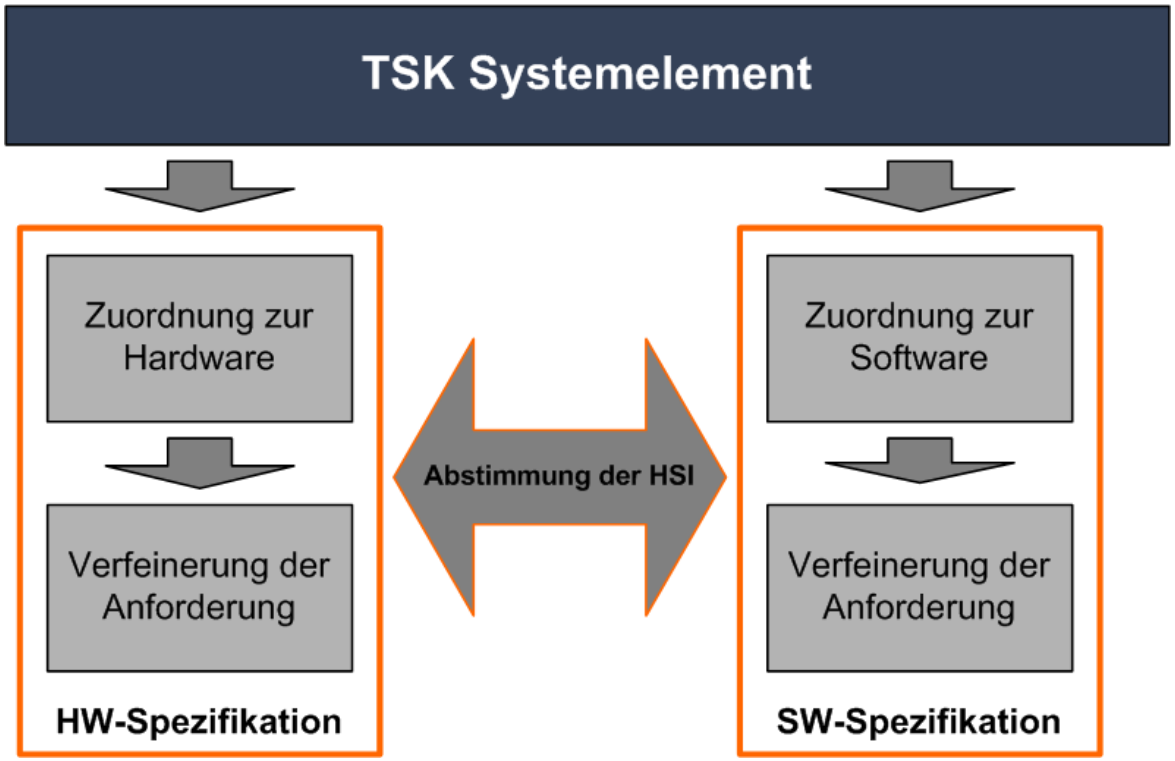
Product Development at the Hardware Level

ISO 26262-5: Produktentwicklung HW-Ebene



ISO 26262-5: HW-Spezifikation und -Design

1. Allokation der Anforderungen aus TSK auf Hardware- und/oder Softwareelemente
2. Verfeinerte Spezifikation der Anforderungen der HW-Elemente in Abstimmung mit SW-Spezifikation
3. Auswahl der HW-Bauteile und Entwurf des HW-Designs



Quelle: SGS TÜV Saar, 2013

Systematischer Ausfall

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

Zufälliger Ausfall

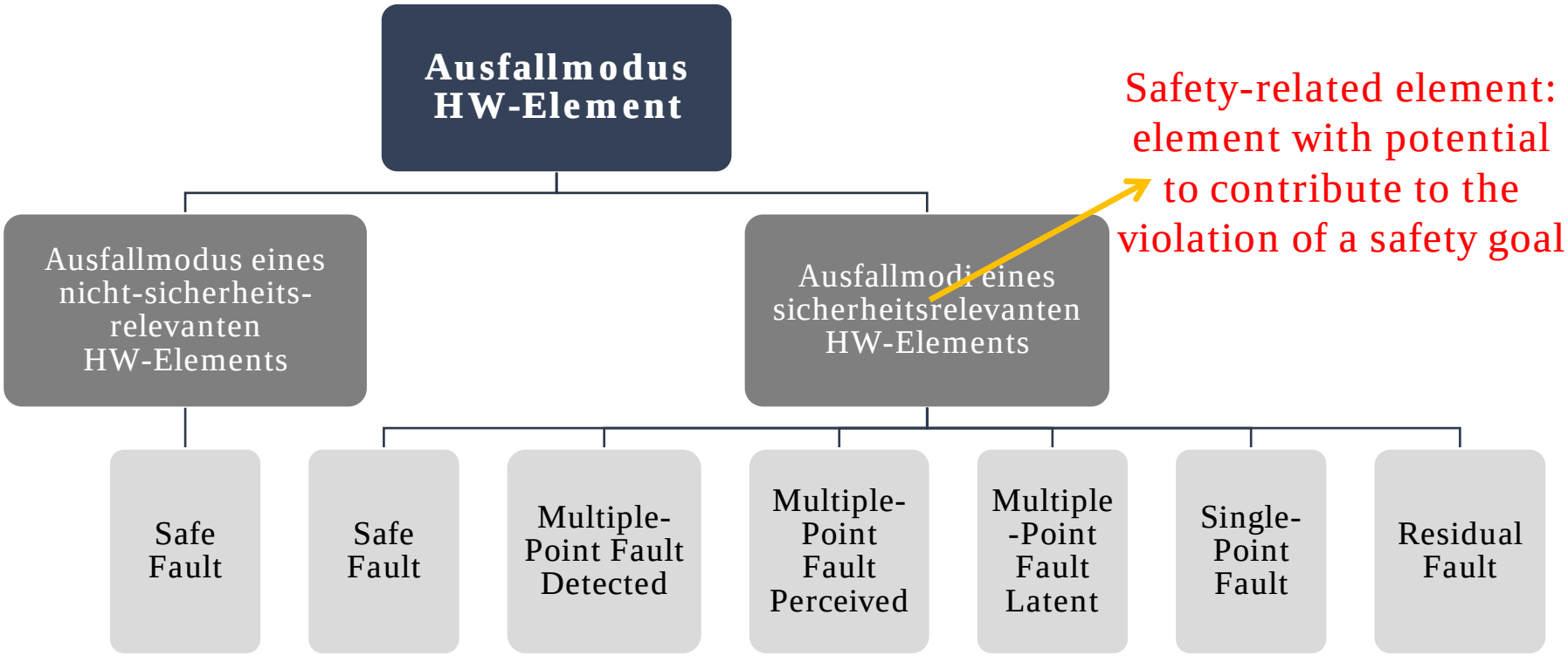
- Ausfall, der zu einem zufälligen Zeitpunkt auftritt und dessen Ursache nicht eindeutig definiert werden kann, wie z.B. Bauteilalterung
- Maßnahmen zur Fehlerbeherrschung erforderlich

Ausfall gemeinsamer Ursache

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

ISO unterscheidet zwischen systematischen und zufälligen Ausfällen

ISO 26262-5: KLASSIFIKATION AUSFALLMODI



ISO unterscheidet in eine Reihe unterschiedlicher Ausfallmodi von Hardware-Elementen

ISO 26262-5 verfolgt zweigeteilten Ansatz bei der Beurteilung der HW-Sicherheit eines Systems:

Bewertung der Effektivität der HW-Architektur des Items in Bezug auf die Behandlung folgender zufälliger Fehlerarten

- Einfachfehler
- (schlafende) Mehrfachfehler

Ansatz 1

SPFM, LFM

Bewertung, ob das verbleibende Risiko einer Verletzung eines Sicherheitsziels aufgrund von zufälligen HW-Ausfällen des Items hinreichend niedrig ist

Ansatz 2

PMHF

ISO definiert drei verschiedene Metriken für die Hardware

Ansatz 1

- Bewertung der Hardwarearchitektur in Bezug auf die Behandlung zufälliger HW-Fehler
  - bei elektromechanischer HW werden nur die E/E-Fehlermodi betrachtet

für ASIL (B), C, D: Anwendung der Konzepte

Diagnosedeckung

- Wahrscheinlichkeit, einen auftretenden Fehler zu entdecken (z.B. durch Diagnose, Testen)

Ausfallraten

- Angabe möglicher Quellen

Hardware-metriken

- SPFM
- LFM

Drei Konzepte müssen bei der HW-Architektur beachtet werden

Ansatz 1

- Architekturmetriken haben Aufgabe, die Sicherheitsarchitektur bewertbar und vergleichbar zu machen
- für ASIL (B), C, D: Anwendung der Hardwaremetrik **„Single-Point Fault Metric“ (SPFM)**

Empfehlung, keine Anforderung

	ASIL B	ASIL C	ASIL D
Single-Point Fault Metric	≥90%	≥97%	≥99%

- $SPFM = 1 - \frac{\sum_{SR,HW}(\lambda) - \sum_{SR,HW}(\lambda)}{\sum_{SR,HW}(\lambda)}$

  mit $\sum_{SR,HW} \lambda_x$: Summe der Ausfallraten des sicherheitsrelevanten HW-Elements
- hohe SPFM bedeutet geringer Anteil der Einfachfehler
- Redundanzen verringern Anteil der Einfachfehler

Architekturmetrik SPFM kann über FMEDA bestimmt werden

Ansatz 1

- Architekturmetriken haben Aufgabe, die Sicherheitsarchitektur bewertbar und vergleichbar zu machen
- für ASIL (B), C, D: Anwendung der Hardwaremetrik **„Latent Fault Metric“ (LFM)**

Empfehlung, keine Anforderung

	ASIL B	ASIL C	ASIL D
Latent Fault Metric	≥60%	≥80%	≥90%

- $SPFM = 1 - \frac{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})} = \frac{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})}$
  mit $\sum_{SR,HW} \lambda_x$: Summe der Ausfallraten des sicherheitsrelevanten HW-Elements
- hohe LFM bedeutet geringer Anteil schlafender Fehler
- Diagnosefähigkeiten verringern Anteil schlafender Einfachfehler

Architekturmetrik LFM kann über FMEDA bestimmt werden

ISO 26262-5: Nachweis der HW-Metriken SPFM & LFM

Ansatz 1

1. Auflistung aller HW-Elemente
2. Ermittlung der entsprechenden Basisausfallraten
3. Identifikation, ob Element sicherheitsrelevant ist oder nicht
4. Ermittlung der Fehlermodi jedes Bauteils inkl. der statistischen Verteilung
5. Klassifikation der Fehlermodi hinsichtlich Sicherheitsziel
6. Bestimmung DC für RF und MPF
7. Aufsummierung der Ausfallraten
8. Berechnung der Architektur-Metriken gemäß Formeln

ISO 26262-5: NACHWEIS DER HW-METRIKEN

- Siemens-Norm SN29500
  - weltweit anerkannte Hausnorm der Siemens AG zu Ausfallraten von vielen elektronischen Bauelementen, wie z.B.
    - Integrierte Schaltkreise
    - Diskrete Halbleiter (Transistoren, Dioden etc.)
    - Passive Bauelemente (Kondensatoren, Widerstände, Induktivitäten)
    - Relais
    - Schalter und Taster
  - 13 Teile, die kontinuierlich überarbeitet werden (aktuell: 2004 – 2013)

  - Prozedur: $\lambda = \lambda_{ref} \times \lambda_U \times \lambda_I \times \lambda_T$

    λ_{ref}: Ausfallrate bei Referenzbedingungen

    λ_U: Faktor für Spannungsabhängigkeit

    λ_I: Faktor für Stromabhängigkeit

    λ_T: Faktor für Temperaturabhängigkeit
    - Faktoren werden über entsprechende Formalismen ermittelt
    - ggf. Einsatz weiterer Korrekturfaktoren

Ansatz 1 Schritt 4

- Ermittlung der Fehlermodi und deren statistischer Verteilung
  - z.B. Widerstand: Kurzschluss
    Unterbrechung
    Drift
  - Quellen für die Fehlermodi und den Verteilungen
    - Alessandro Birolini: *Reliability Engineering – Theory and Practice*
    - DIN EN 62061, Anhang D

Relais	alle Kontakte verbleiben im angezogenen Zustand, wenn die Spule entregt ist	25
	alle Kontakte verbleiben im nicht angezogenen Zustand, wenn die Spule erregt ist	25
	Nichtöffnen von Kontakten	10
	Nichtschließen von Kontakten	10
	gleichzeitiger Kurzschluss zwischen drei Kontakten eines Wechselkontaktes	10
	gleichzeitiges Geschlossensein von Schließer- und Öffnerkontakten	10
	Kurzschluss zwischen zwei Kontaktpaaren und/oder zwischen Kontakten und Spulenklemme	10

ISO 26262-5: Nachweis der HW-Metriken

Schritt 7/8 Ansatz 1

Component Name	Failure rate/FIT	Safety-related component to be considered in the calculation?	Failure Mode	Failure rate distribution	Failure mode that has the potential to violate the safety goal in absence of safety mechanisms?	Safety mechanism(s) allowing to prevent the failure mode from violating the safety goal?	Failure mode coverage wrt. violation of safety goal	Residual or Single-Point Fault failure rate/FIT	Failure mode that may lead to the violation of safety goal in combination with an independent failure of another component?	Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent?	Failure mode coverage wrt. Latent failures	Latent Multiple-Point Fault failure rate/FIT
R11 note 1, note 6 and note 7	2	YES	open	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			closed	10 %	X		99 %	0,002	X		100 %	0
R12 note 1, note 6 and note 7	2	YES	open	90 %	X	SM2	99 %	0,018	X	SM2	100 %	0
			closed	10 %	X		99 %	0,002	X		100 %	0
L1	10	NO	open	90 %								
			closed	10 %								
µC	100	YES	All	50 %	X	SM4	90 %	5	X	SM4	100 %	0
			All	50 %								
								∑ 5,48			∑ 12,80	

Total failure rate 176
Total Safety Related 157
Total Not Safety Related 19

Single-Point Fault Metric = 1-(5,48/157) = 96,5 %

Latent Fault Metric = 1-(13,99/(157-5,48)) = 91,6 %

SPFM < 97% → ASIL B

LFM > 90% → ASIL D

Ansatz 2

Ziel

- Begründung, dass das verbleibende Risiko einer **Verletzung eines Sicherheitsziels** aufgrund von zufälligen HW-Ausfällen (SPF, RF, DPF – MPF wenn relevant) des Items hinreichend niedrig ist

2 Methoden für ASIL (B), C, D

- Nutzung einer probabilistischen Metrik für zufällige Hardwareausfälle (PMHF)
- Individuelle Bewertung der Ausfallmodi über „Failure Rate Classes“ (FRC)

Zufällige HW-Ausfälle müssen betrachtet werden

Methode 1 Ansatz 2

- für ASIL (B), C, D: Quantitative Zielwerte aus folgenden Quellen
  -

ASIL	Zielwerte für zufällige HW-Ausfälle	
B	Empfehlung, keine Anforderung	$< 10^{-7}\frac{1}{h}$
C		$< 10^{-7}\frac{1}{h}$
D		$< 10^{-8}\frac{1}{h}$

„Average Probability per Hour over the Operational Lifetime

  - abgeleitet aus Felddaten ähnlich gut gesicherter Entwurfsprinzipien
  - abgeleitet aus quantitativen Analysen (unter Verwendung von Ausfallraten) für ähnliche gut gesicherte Entwurfsprinzipien

➢ quantitative Zielwerte haben keine absolute Signifikanz
  ➢ sinnvoller Vergleich neuer Entwurf mit existierendem Entwurf

- Aufteilung des PMHF-Werts muss klar kommuniziert werden

Metrik kann über quantitative Fehlerbaumanalyse bestimmt werden

ZUSAMMENFASSUNG

ISO 26262: Zusammenfassung

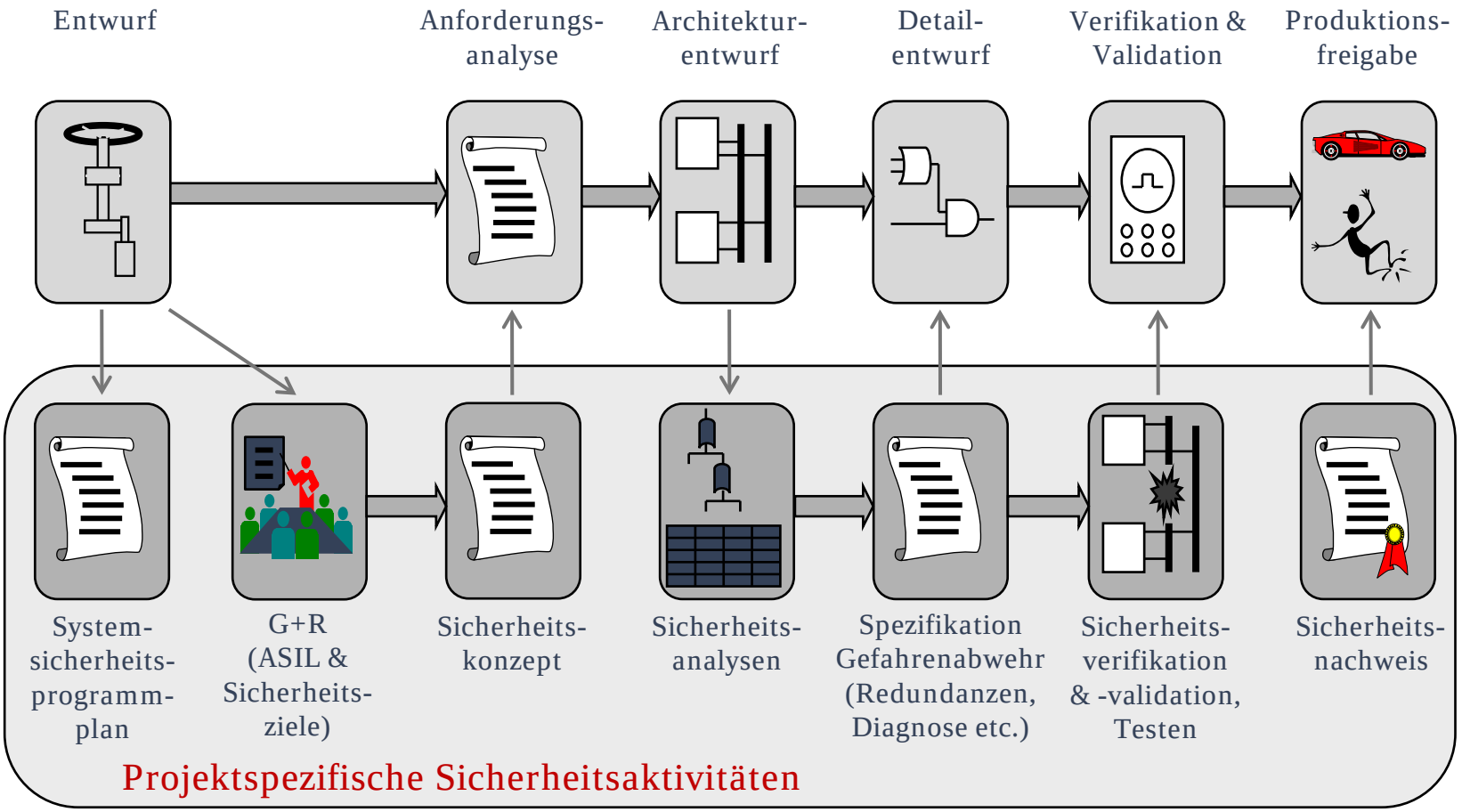
- ISO 26262 gibt das Rahmenwerk vor, um Funktionale Sicherheit von automotiven E/E-Systemen zu gewährleisten

- hauseigene Entwicklungsprozess muss um Aspekte der Funktionalen Sicherheit erweitert werden
  - Unterstützung vom Management und Akzeptanz aller Beteiligter ist unerlässlich
  - „FuSi wird nicht schnell nebenher erreicht“

- Anforderungen sind teils sehr allgemein gehalten und beziehen sich zum Großteil auf prozessuale Aspekte
  - unternehmensinterne Guidelines zur Umsetzung für Entwickler sind wichtig
  - Herausforderungen durch neue Aspekte (z.B. HW-Metriken) wollen gemeistert werden

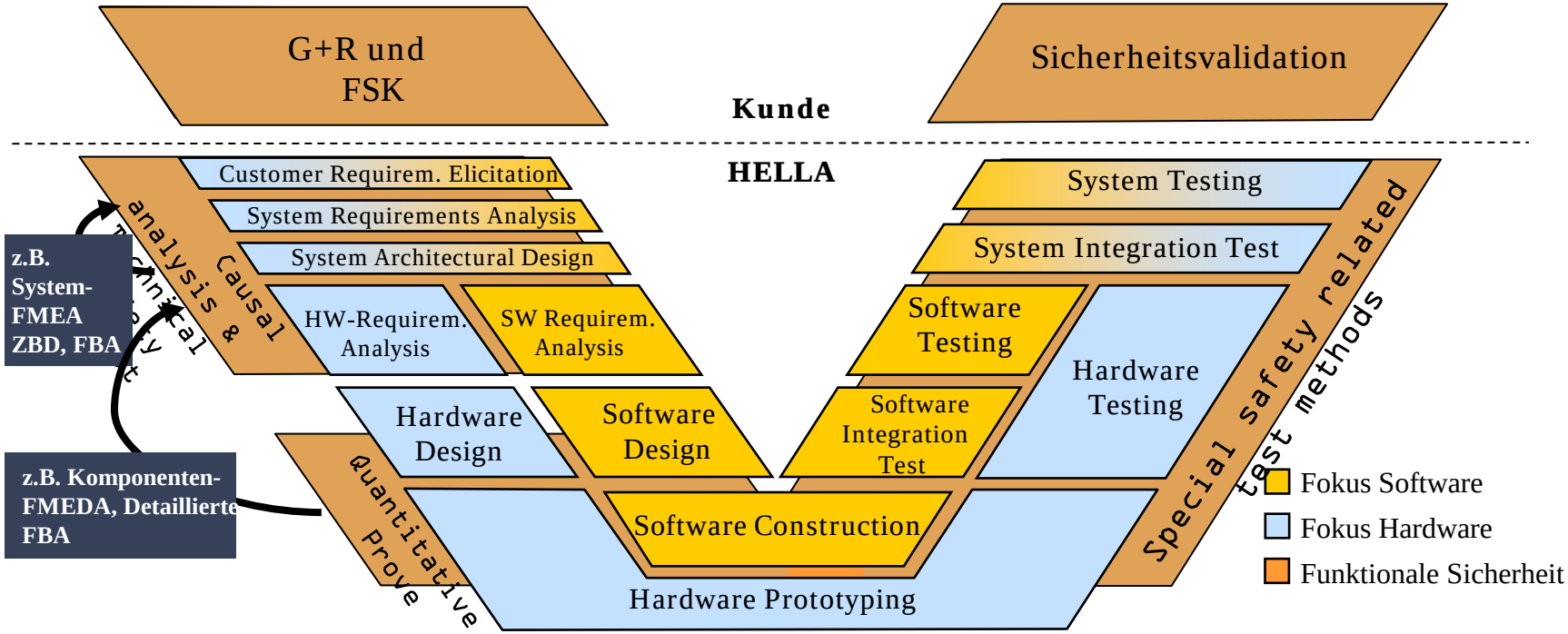
- Normenwerk wird überarbeitet und um weitere Anwendungsbereiche erweitert werden

ISO 26262: Zusammenfassung – Systemsicherheitsprozess



Quelle: Smuszynski, 2013

ISO 26262: FuSi-Integration in Entwicklungsprozess (Bsp. Hella)

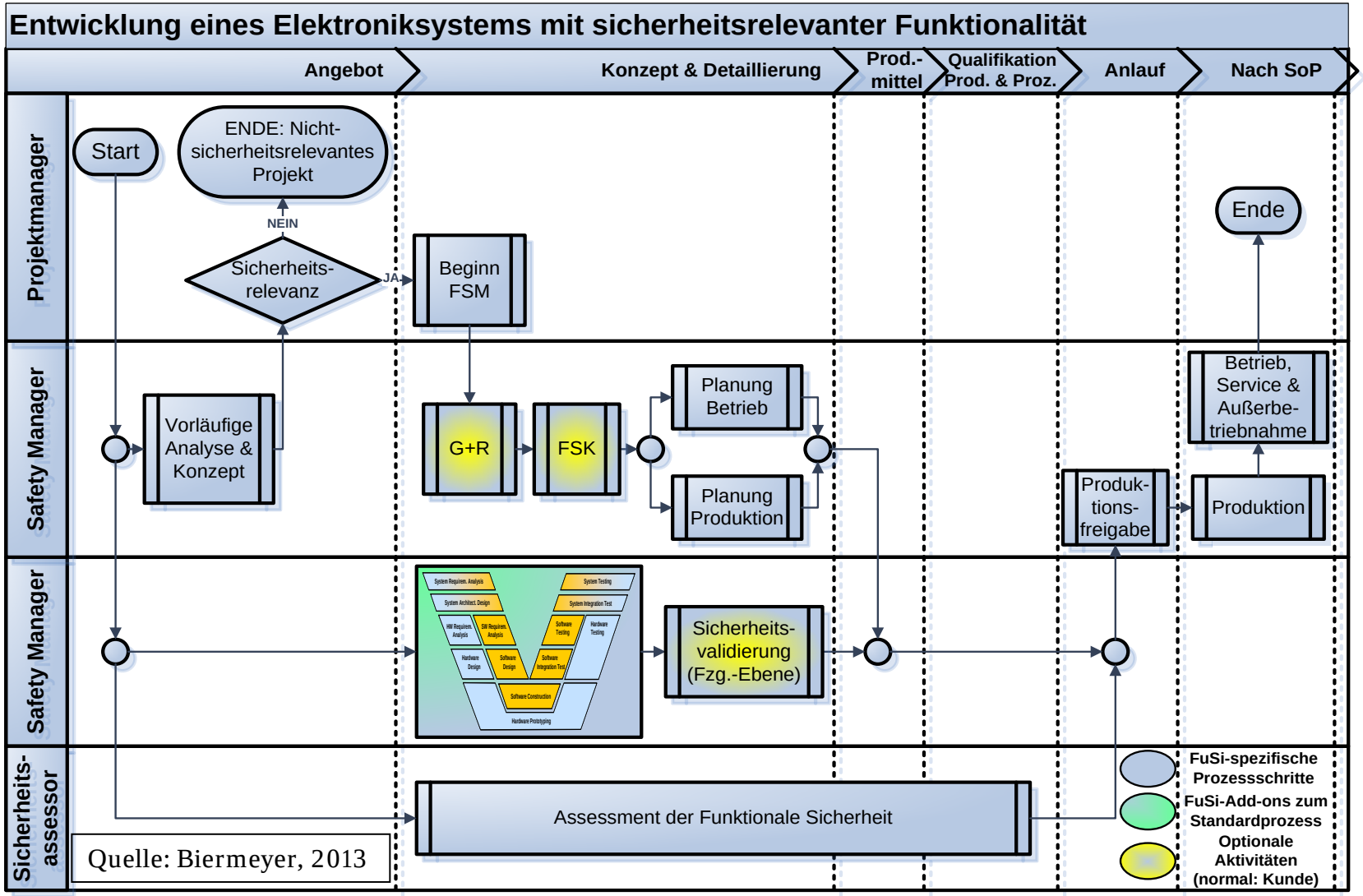


Supporting Processes:

HW-/SW-Project Management	Safety planning
HW-/SW-Quality Assurance	Safety Support activities during Development
HW-/SW-Configuration Management	
HW-/SW-Problem Resolution Management	
HW-/SW-Change Request Management	
HW-/SW-Supplier Monitoring	
ReUse program management	

Quelle: Biermeyer, 2013

ISO 26262: Integration FSM in Entwicklungsprozess (Bsp: Hella)



VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Kontakt

Mail: schlummer@iqz-wuppertal.de

Tel.: +49 (0)202 – 515 616 93

Fax: +49 (0)202 – 515 616 89

www.iqz-wuppertal.de

Dr.-Ing. Marco Schlummer|Dr.-Ing. Andreas Braasch|Prof. Dr.-Ing. Arno Meyna|Dr.-Ing. Dirk Althaus