INFORMATIK ▪ CONSULTING ▪ SYSTEMS AG

Entwicklung und Zulassung von sicherheitskritischen Systemen -

was kann die Automobilbranche von Bahnen und Luftfahrt lernen?

Dr. Bernhard Hohlfeld, ICS AG, Ulm (Vortragender)
Dr. Paul Linder, ICS AG, Stuttgart
Udo Hipp, ICS AG, Stuttgart

30. Tagung
Elektronik im Kraftfahrzeug
16./17. Juni 2010, Dresden

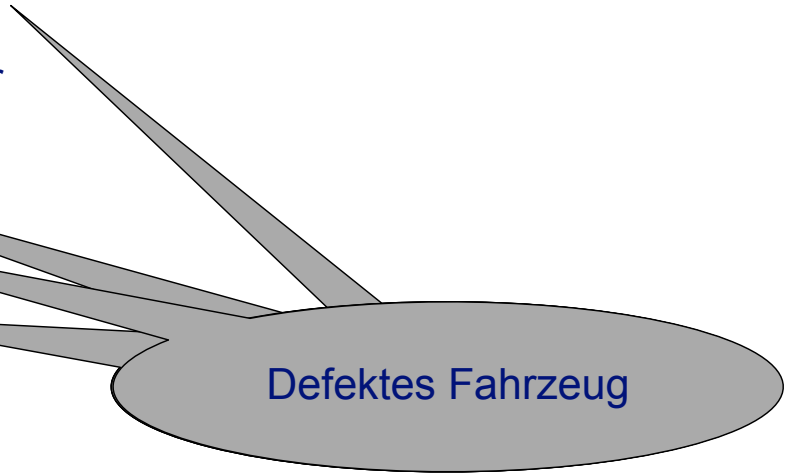
Gliederung

1. Einleitung
2. Normen und Standards für sicherheitskritische Systeme
3. Analyse und Entwicklung sicherheitskritischer Systeme
4. Zusammenfassung

Gliederung

Katastrophen mit technischen Systemen

- 1986 Explosion im Kernkraftwerk Tschernobyl
- 1987 Explosion des Space Shuttle Challenger
- 1998 ICE-Unglück bei Eschede
- 1999 Feuer im Mont Blanc Tunnel
- 2000 Absturz der Concorde bei Paris
- 2010 Absturz der Tupolew 154 bei Smolensk



Igel

Eagle

Unterschiedliche Normen und Standards

Nach Josef Börcsök:
Funktionale Sicherheit,
Hüthig Verlag, Heidelberg, 2008.

Unvollständige Abdeckung

Der automatische Vortriebsregler unserer B737 hatte die Eigenschaft, sich manchmal während des Startvorgangs bei exakt 60 Konten zu verabschieden. Es waren unsere Werkstätten - und nicht etwa der Gerätehersteller -, die anhand des glücklicherweise vorhandenen Listings die Ursache fanden: Der Programmierer hatte festgelegt, was der Vortriebsregler unter und was er über 60 Knoten Fahrt tun sollte. Nur ihm zu sagen, wie er bei 60 Knoten reagieren sollte, dass hatte er vergessen. Wenn der Computer nun bei exakt 60 Knoten die entsprechende Bedingung abfragte, fand er keine Anweisung vor, war verwirrt und schaltete ab.

Nach J.P. Hach:
Digitale Elektronik in Verkehrsflugzeugen, in DGLR (Hrsg.): Test und Verifkation von Software bei digitalen Systemen der Luft- und Raumfahrt, DGLR-Bericht 83-02.

Unvollständige Abdeckung

Der automatische Vortriebsregler unserer B737 hatte die Eigenschaft, sich manchmal während des Startvorgangs bei exakt 60 Konten zu verabschieden. **Es waren unsere Werkstätten** - und nicht etwa der Gerätehersteller -, **die anhand des glücklicherweise vorhandenen Listings die Ursache fanden**: Der Programmierer hatte festgelegt, was der Vortriebsregler unter und was er über 60 Knoten Fahrt tun sollte. Nur ihm zu sagen, wie er bei 60 Knoten reagieren sollte, dass hatte er vergessen. Wenn der Computer nun bei exakt 60 Knoten die entsprechende Bedingung abfragte, fand er keine Anweisung vor, war verwirrt und schaltete ab.

Nach J.P. Hach:
Digitale Elektronik in Verkehrsflugzeugen, in DGLR (Hrsg.): Test und Verifkation von Software bei digitalen Systemen der Luft- und Raumfahrt, DGLR-Bericht 83-02.

Softwarefehler

- Fehlerursache
  Verwechslung von Punkt und Komma in FORTRAN
  - Richtig mit Komma: DO 10 i = 1,3 . . . (Schleife)
  - Falsch mit Punkt: DO 10 i = 1.3 . . . (Zuweisung)
- Fehlerauswirkung:
  Die Mission eines zum Planet Venus gestarteten Satelliten scheiterte (laut NASA).
- Programmierfehler oder ungeeignete Programmiersprache?
- PASCAL
  - for I := 1 to 3 do ...;
  - I := 1.3;
- Nach Rudolf M. Konakovsky:
  Zuverlässigkeit und Sicherheit von Automatisierungssystemen,
  Institut für Automatisierungs- und Softwaretechnik, Universität Stuttgart,
  Vorlesung, 2005.

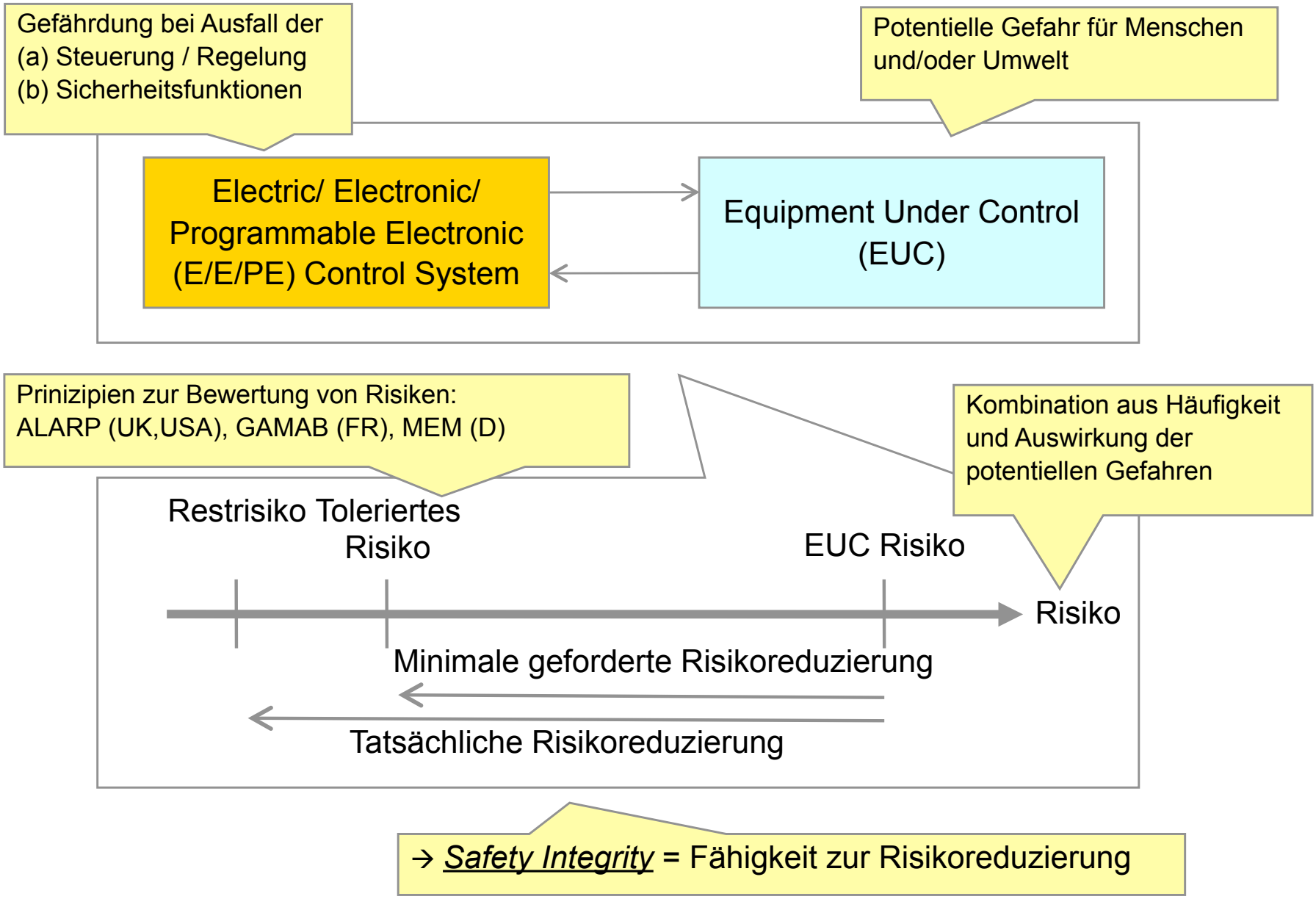
Kein Rosenmontagsscherz

```
if <condition>
then
        ....
        goto L2;
        ....
        L1:
        ....
else
        ....
        L2:
        ....
        goto L1;
        ....
end if;
```

```
while <condition>
do
        ...
        goto L;
        -- irgendwo ausserhalb der
        -- Schleife
        ...
end while;
```

Gliederung

Grundlegende Konzepte der Funktionalen Sicherheit



Prinzipien zur Bewertung von Risiken

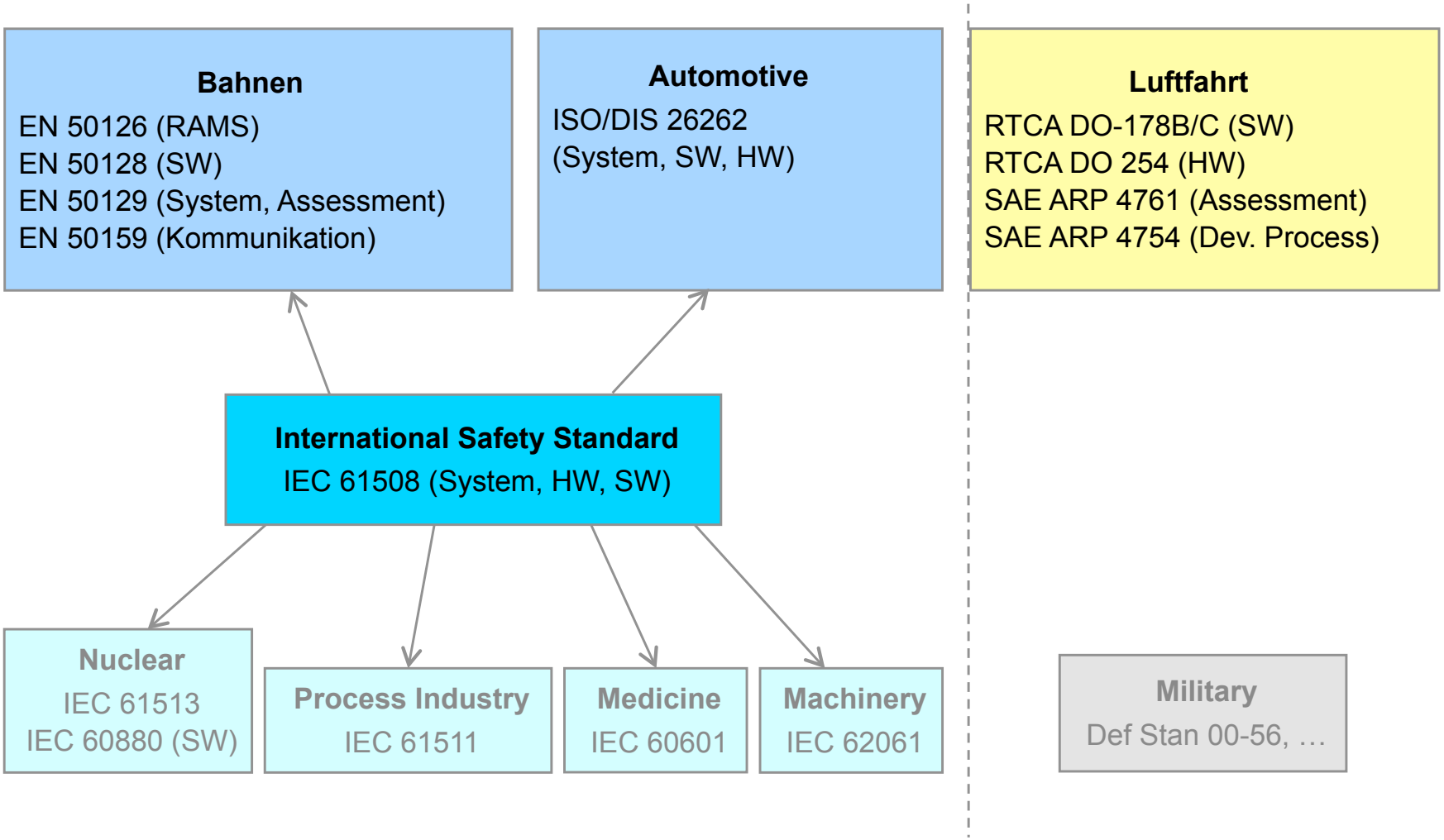
- ALARP - As Low As Reasonably Practicable
  Das ALARP-Prinzip besagt, dass Risiken auf ein Maß reduziert werden sollen, welches den höchsten Grad an Sicherheit garantiert, der vernünftigerweise praktikabel ist (Relevanzmaximalschadenserwartungsbegrenzung).
- GAMAB - Globalement Au Moins Aussi Bon
  Les objectifs de sécurité doivent être d'un ordre de grandeur comparable aux performances de sécurité déjà observées.
- MEM - Minimale Endogene Mortalität
  MEM ist ein Maß für das akzeptierte (unvermeidliche) Risiko, durch die betreffende Technologie zu Tode zu kommen.

Ansätze und Prinzipien der Funktionalen Sicherheit

	Zufällige Fehler	Systematische Fehler
Beispiele	■ Hardwareausfall ■ Übertragungsfehler	■ Designfehler ■ Spezifkationsfehler ■ Programmierfehler
Strategie	Beherrschung der Auswirkungen	Fehlervermeidung
Ansatz	*Quantitative* Analysen	Vorgeschriebene Methoden abhängig vom (*qualitativen)* Safety Integrity Level (SIL)

Prinzipien	■ Fehlererkennung
	  ■ Selbsttests
	■ Fail-safe
	(Sicherer Zustand bei Ausfall)
	■ Redundanz
	■ Ziel: Beherrschung jedes einzelnen Fehlers
		■ Entwicklung nach Stand der Wissenschaft und Technik
		■ Umfangreiche Verifikation
		■ Nachvollziehbarkeit
		■ Abdeckung
		■ Unabhängigkeit
		  ■ Technisch: Diversität, ...
		  ■ Personell: Entwickler und Prüfer verschiedene Personen
		  ■ Organisatorisch: Entwickler und Prüfer in verschiedenen Organisationen

Sicherheitsstandards im Überblick



Sicherheitsstandards Bahnen

- EN 50126: Bahnanwendungen: Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS), 2000.
- EN 50128: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Daten-verarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungsssysteme, 2001.
- EN 50129: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Daten-verarbeitungssysteme, 2003.
- EN 50159: Sicherheitsrelevante Kommunikation, 2001.

Sicherheitsstandards Automotive

- ISO/DIS 26262
  Road vehicles – Functional safety

Sicherheitsstandards Luftfahrt

- RTCA/DO-178B/C: Software Considerations in Airborne Systems and Equipment Certification, RTCA,1992.
- RTCA/DO-254: Design Assurance Guidance for Airbone Electronic Hardware.
- SAE ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.
- SAE ARP 4754: Certification Considerations for Highly-Integrated or Complex Aircraft System

Vergleich der Sicherheitsstandards

	IEC 61508	EN 50126 EN 50128 EN 50129 EN 50159	ISO/DIS 26262	DO-178B DO-254 ARP 4761 ARP 4754
Anwendungsbereich	Generisch	Bahnen (1-dimensional)	Automotive (2-dimensional)	Luftfahrt (3-dimensional)
Sicherheitsansatz	Sicherer Zustand, Fail-safe	Sicherer Zustand, Fail-safe im Fehlerfall	Sicherer Zustand oder sichere Fortsetzung mit Restfunktionalität	Sichere Fortsetzung des Fluges und sichere Landung
Betrachtete Gefahren	Gefährdungen von Menschen und Umwelt		Nur Gefährdungen von Menschen	
Abdeckung	System, Umwelt, Wartung		System	
Safety Integrity Levels (SIL)	SIL 4 (hoch) SIL 3 SIL 2 SIL 1 (niedrig) --	SIL 4 (hoch) SIL 3 SIL 2 SIL 1 (niedrig) SIL 0 (nicht sicherheitsrelevant)	-- ASIL D (hoch) ASIL C ASIL B ASIL A (niedrig) (QM)	Level A (hoch) Level B Level C Level D Level E (niedrig) --
Organisatorische Aspekte	Teilweise	Ja	Ja	Nein
Werkzeug-qualifizierung	Nein	Nein	Ja	Ja

Vergleich der Sicherheitsstandards

	IEC 61508	EN 50126 EN 50128 EN 50129 EN 50159	ISO/DIS 26262	DO-178B DO-254 ARP 4761 ARP 4754
Anwendungsbereich	Generisch	Bahnen (1-dimensional)	Automotive (2-dimensional)	Luftfahrt (3-dimensional)
Sicherheitsansatz	Sicherer Zustand, Fail-safe	Sicherer Zustand, Fail-safe im Fehlerfall	Sicherer Zustand oder sichere Fortsetzung mit Restfunktionalität	Sichere Fortsetzung des Fluges und sichere Landung
Betrachtete Gefahren	Gefährdungen von Menschen und Umwelt		Nur Gefährdungen von Menschen	
Abdeckung	System, Umwelt, Wartung		System	
Safety Integrity Levels (SIL)	SIL 4 (hoch) SIL 3 SIL 2 SIL 1 (niedrig) --	SIL 4 (hoch) SIL 3 SIL 2 SIL 1 (niedrig) SIL 0 (nicht sicherheitsrelevant)	-- ASIL D (hoch) ASIL C ASIL B ASIL A (niedrig) (QM)	Level A (hoch) Level B Level C Level D Level E (niedrig) --
Organisatorische Aspekte	Teilweise	Ja	Ja	Nein
Werkzeug-qualifizierung	Nein	Nein	Ja	Ja

Vergleich der Sicherheitsstandards

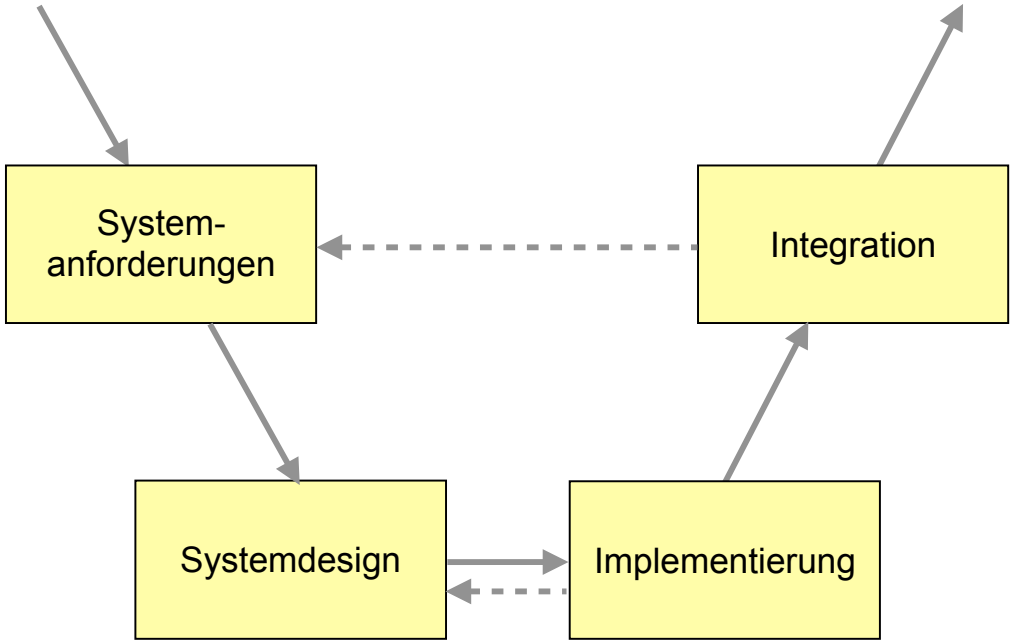
	IEC 61508	EN 50126 EN 50128 EN 50129 EN 50159	ISO/DIS 26262	DO-178B DO-254 ARP 4761 ARP 4754
Anwendungsbereich	Generisch	Bahnen (1-dimensional)	Automotive (2-dimensional)	Luftfahrt (3-dimensional)
Sicherheitsansatz	Sicherer Zustand, Fail-safe	Sicherer Zustand, Fail-safe im Fehlerfall	Sicherer Zustand oder sichere Fortsetzung mit Restfunktionalität	Sichere Fortsetzung des Fluges und sichere Landung
Betrachtete Gefahren	Gefährdungen von Menschen und Umwelt		Nur Gefährdungen von Menschen	
Abdeckung	System, Umwelt, Wartung		System	
Safety Integrity Levels (SIL)	SIL 4 (hoch) SIL 3 SIL 2 SIL 1 (niedrig) --	SIL 4 (hoch) SIL 3 SIL 2 SIL 1 (niedrig) SIL 0 (nicht sicherheitsrelevant)	-- ASIL D (hoch) ASIL C ASIL B ASIL A (niedrig) (QM)	Level A (hoch) Level B Level C Level D Level E (niedrig) --
Organisatorische Aspekte	Teilweise	Ja	Ja	Nein
Werkzeug-qualifizierung	Nein	Nein	Ja	Ja

Vergleich der Sicherheitsstandards

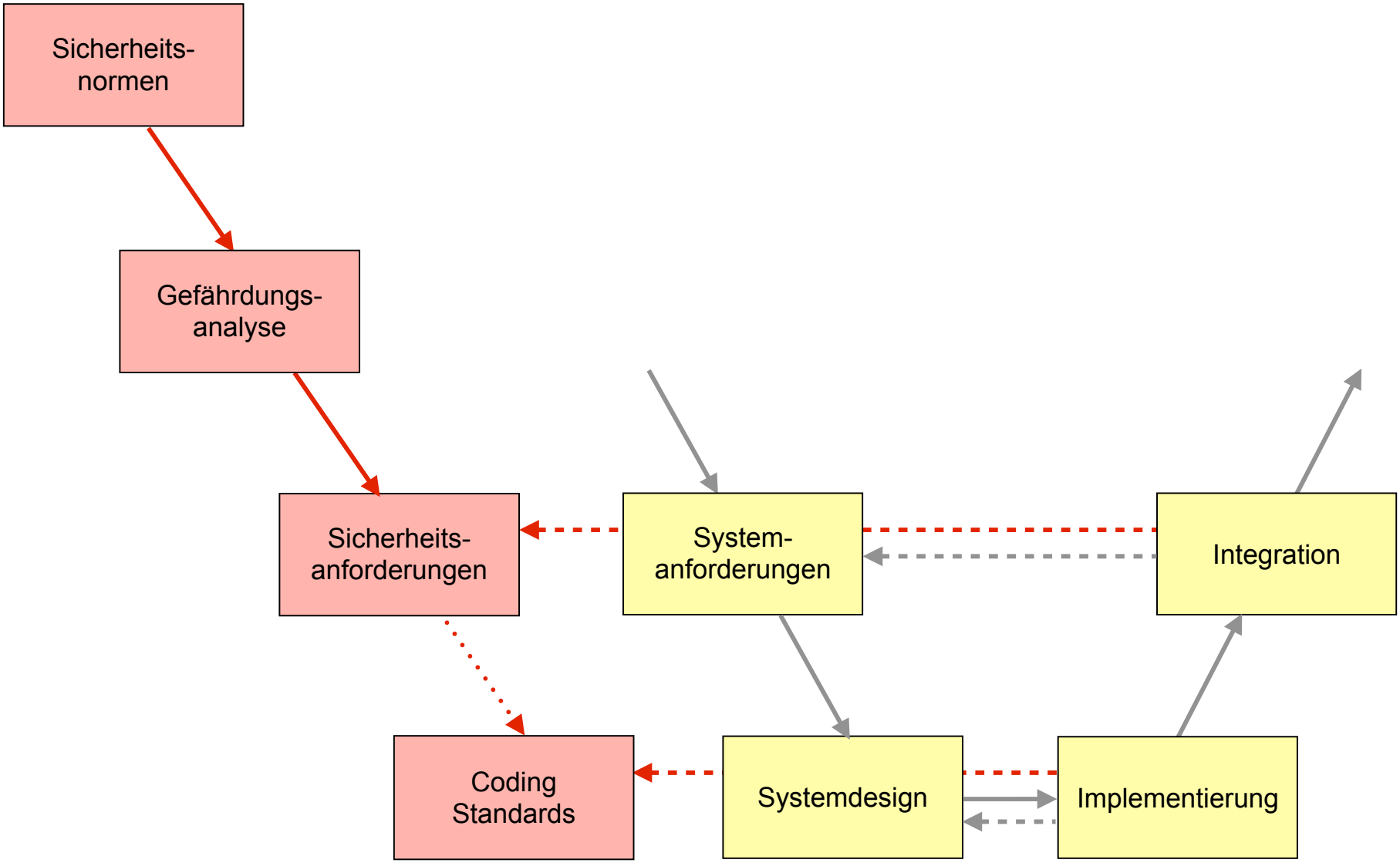
	IEC 61508	EN 50126 EN 50128 EN 50129 EN 50159	ISO/DIS 26262	DO-178B DO-254 ARP 4761 ARP 4754
Anwendungsbereich	Generisch	Bahnen (1-dimensional)	Automotive (2-dimensional)	Luftfahrt (3-dimensional)
Sicherheitsansatz	Sicherer Zustand, Fail-safe	Sicherer Zustand, Fail-safe im Fehlerfall	Sicherer Zustand oder sichere Fortsetzung mit Restfunktionalität	Sichere Fortsetzung des Fluges und sichere Landung
Betrachtete Gefahren	Gefährdungen von Menschen und Umwelt		Nur Gefährdungen von Menschen	
Abdeckung	System, Umwelt, Wartung		System	
Safety Integrity Levels (SIL)	SIL 4 (hoch) SIL 3 SIL 2 SIL 1 (niedrig) --	SIL 4 (hoch) SIL 3 SIL 2 SIL 1 (niedrig) SIL 0 (nicht sicherheitsrelevant)	-- ASIL D (hoch) ASIL C ASIL B ASIL A (niedrig) (QM)	Level A (hoch) Level B Level C Level D Level E (niedrig) --
Organisatorische Aspekte	Teilweise	Ja	Ja	Nein
Werkzeug-qualifizierung	Nein	Nein	Ja	Ja

Gliederung

(Vereinfachtes) V-Modell der Softwareentwicklung



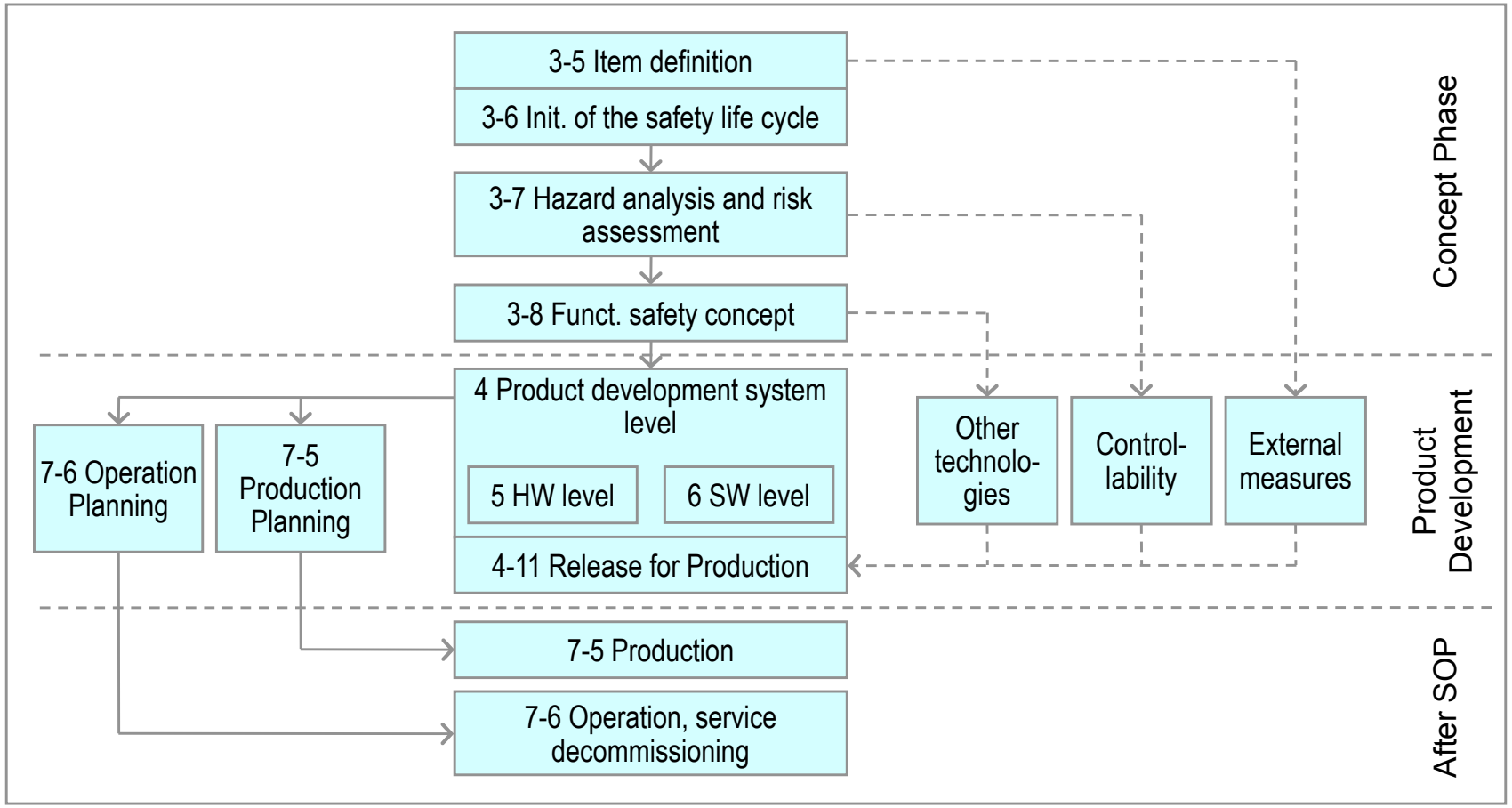
(Vereinfachtes) V-Modell der Softwareentwicklung bei sicherheitskritischen Systemen



Funktionssicherheit Fahrdynamik: Entwicklung eines Sicherheitskonzeptes

- Bestätigung der Sicherheitsziele
  - Durchführung der Gefahren & Risikoanalyse auf Basis der System-FMEA
  - Bewertung von Fahrmanövern nach Auftretenswahrscheinlichkeit, Kritikalität und Beherrschbarkeit für die Einstufung nach ASIL
- Erstellung des Sicherheitskonzeptes
  - Zuordnung von Sicherheitsanforderungen auf Systemelemente (Allokation)
  - Erarbeitung und Abstimmung der Degradationsebenen des Funktionalen Sicherheitskonzeptes
- Sicherheitsarchitektur
  - Erstellung einer FuSi-Architektur
- Sicherheitsanalysen
  - Erweiterung der System-FMEA
  - Mitarbeit an FTA für TOP-Sicherheitsziele

Safety Life Cycle und Prozesse

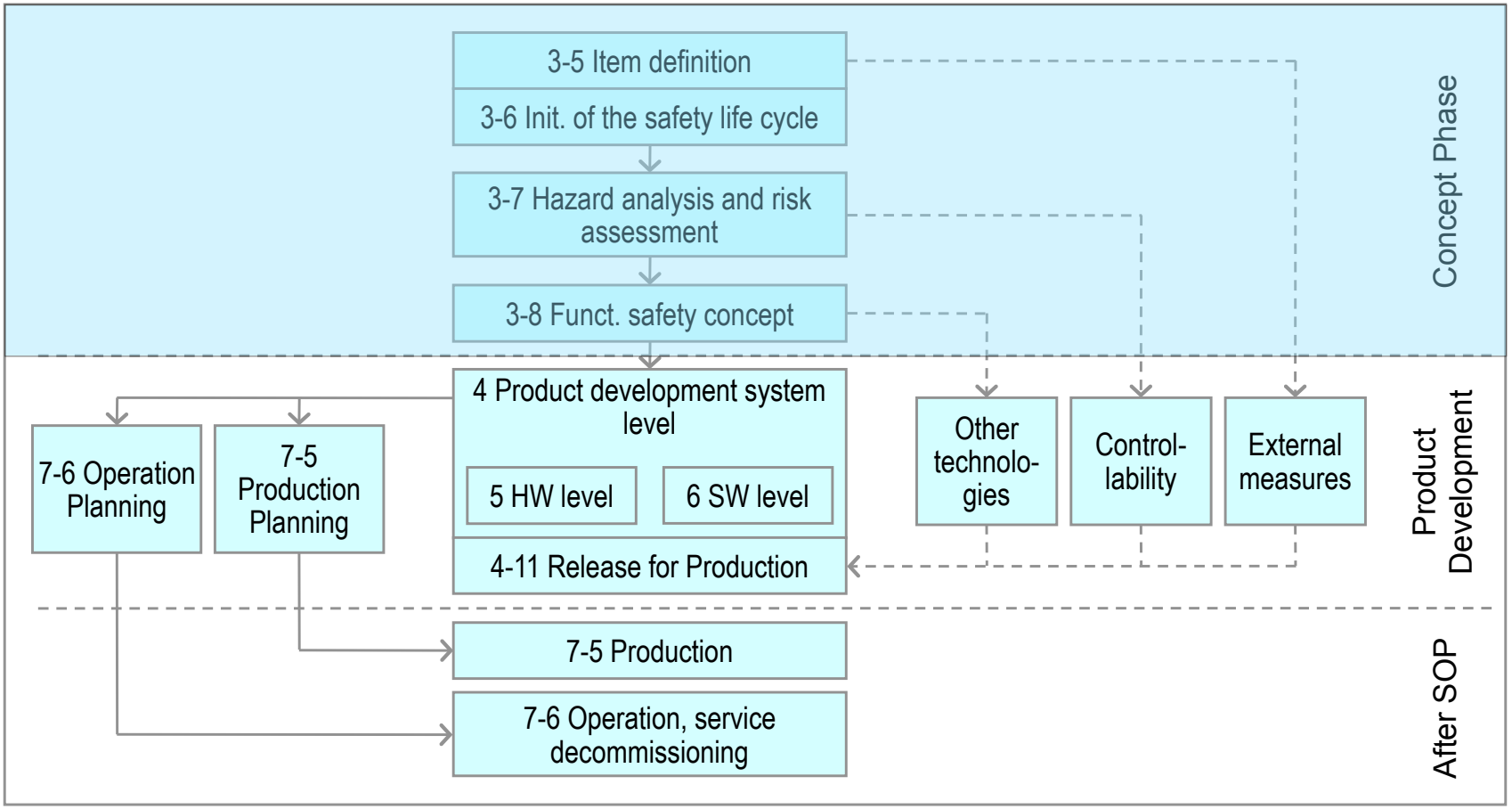


Safety Life Cycle nach ISO/DIS 26262

Prozesse im life cycle (Auswahl):

- Entwicklung
- Verifikation und Validation
- Sicherheitsmanagement
- Qualitätsmanagement
- Assessment / Bewertung

Safety Life Cycle und Prozesse



Safety Life Cycle nach ISO/DIS 26262

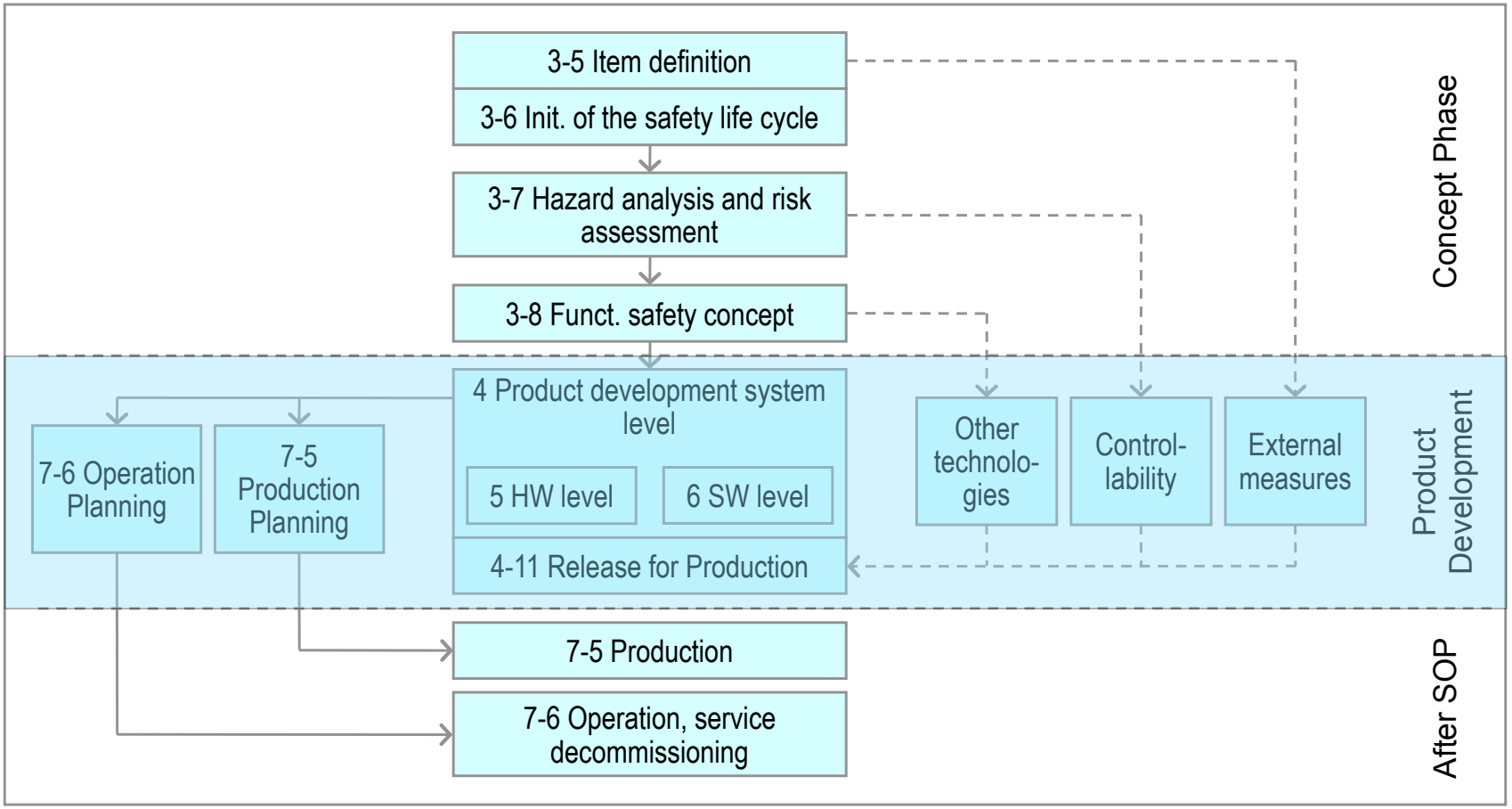
Prozesse im life cycle (Auswahl):

- Entwicklung
- Verifikation und Validation
- Sicherheitsmanagement
- Qualitätsmanagement
- Assessment / Bewertung

Sicherheitskonzept Aktive Frontlenkung – Concept Phase

- 3-5 Item Definition
  - Brief description of the item (main functions)
  - General requirements (e.g. ECE-R 79)
  - Functional, non-functional and legal requirements
  - Boundaries
  - Preliminary known hazards
- 3-6 Initiation of the safety lifecycle
  - Mapping ISO CD 26262 requirements to existing OEM Development process
  - Creation of the Safety Plan
- 3-7 Hazard analysis and risk assessment
  - Preliminary hazard analysis, HAZOP
  - FMEA
  - Risk assessment: Severity – Exposure – Controllability
  - ASIL determination
  - Definition of safety goals
- 3-8 Functional safety concept
  - Preliminary architectural assumptions
  - Functional concept
  - Specification of operation modes and system states
  - FTA
  - Warning and back-up concept
  - Safety architecture concept
  - Functional safety concept
  - Safety requirements specification

Safety Life Cycle und Prozesse

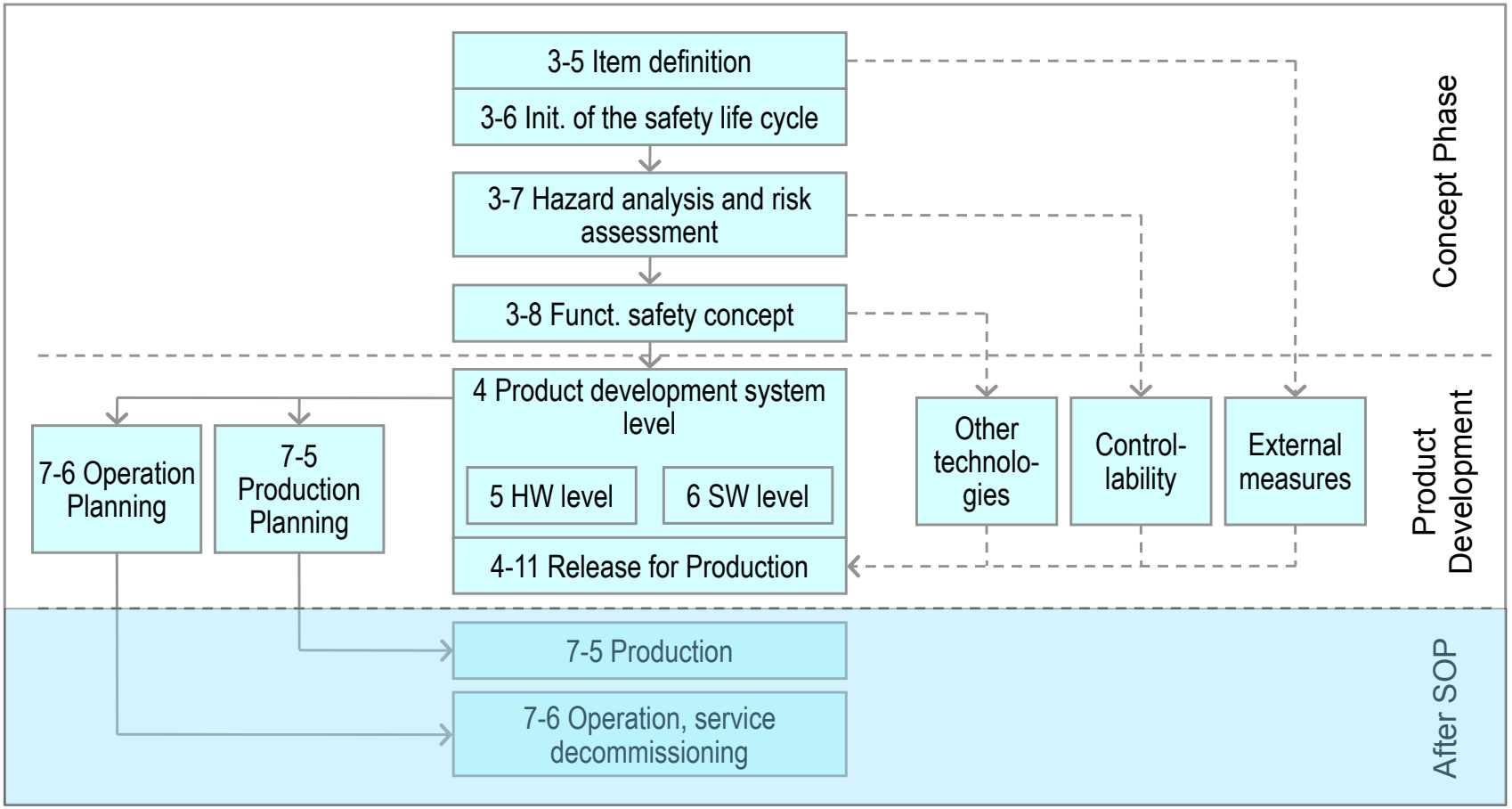


Safety Life Cycle nach ISO/DIS 26262

Prozesse im life cycle (Auswahl):

- Entwicklung
- Verifikation und Validation
- Sicherheitsmanagement
- Qualitätsmanagement
- Assessment / Bewertung

Safety Life Cycle und Prozesse

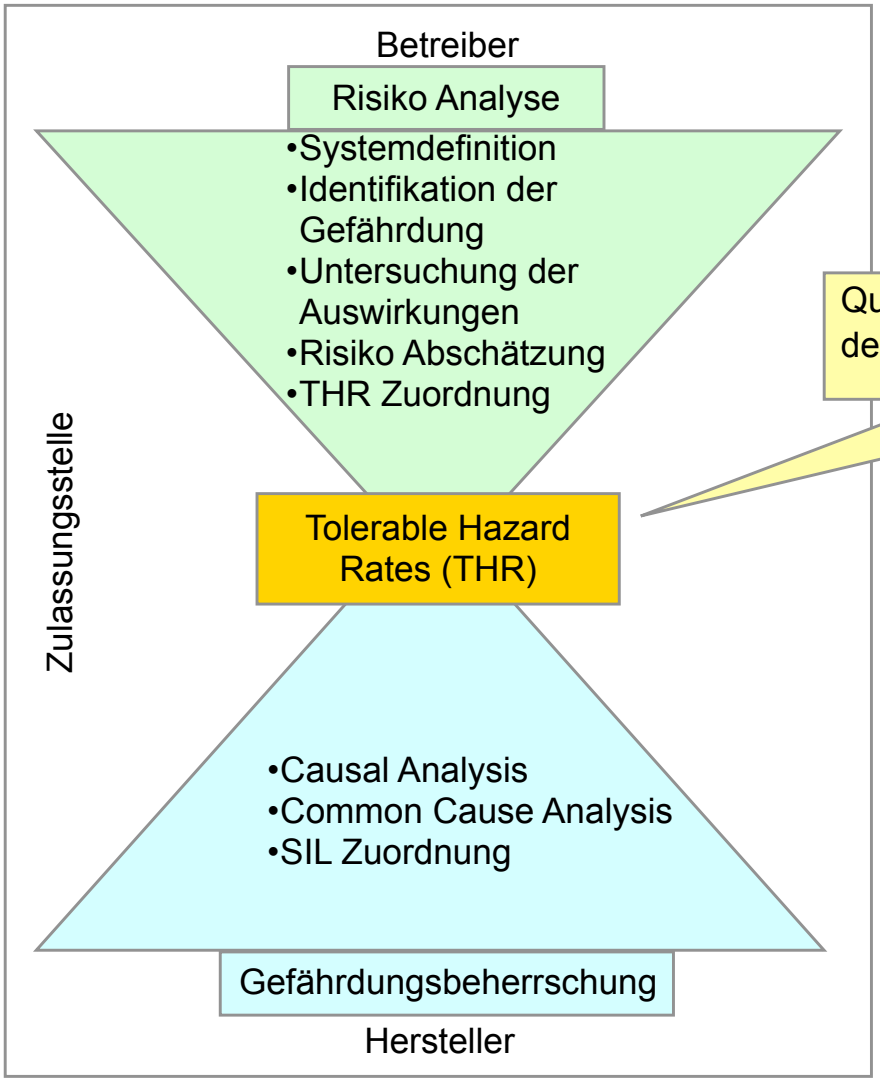


Safety Life Cycle nach ISO/DIS 26262

Prozesse im life cycle (Auswahl):

- Entwicklung
- Verifikation und Validation
- Sicherheitsmanagement
- Qualitätsmanagement
- Assessment / Bewertung

Analyse sicherheitskritischer Systeme nach EN 50129

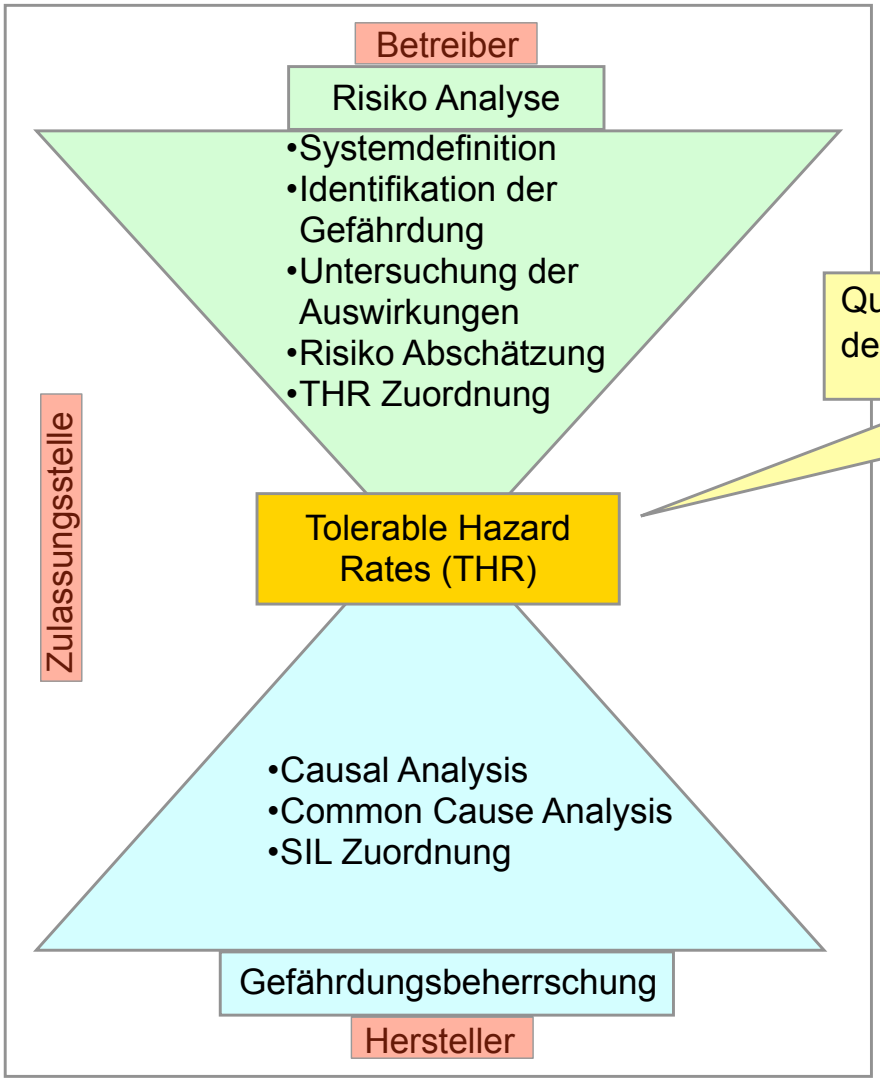


Quantitative oder qualitative Bestimmung des Safety Integrity Level (SIL)

Methods:

- Hazard and Operability Studies (HAZOP)
- Functional Hazard Assessment (FHA)
- Failure Mode and Effects Analysis (FMEA)
- Event Tree Analysis (ETA)
- Reliability Block Diagrams (RBD)
- Fault Tree Analysis (FTA)
- Hidden Markov Models
- Sneak Circuit Analysis

Analyse sicherheitskritischer Systeme nach EN 50129



Quantitative oder qualitative Bestimmung des Safety Integrity Level (SIL)

Methods:

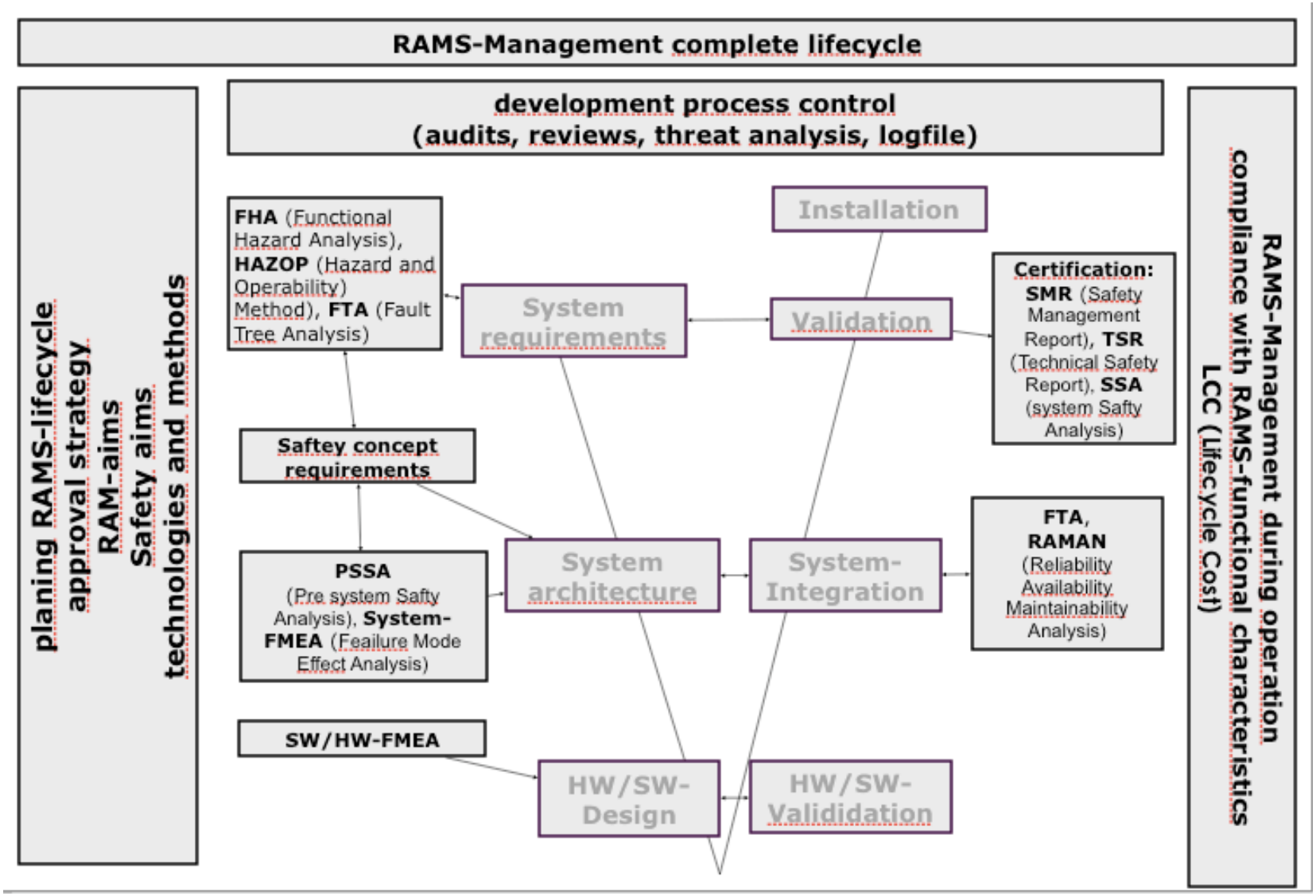
- Hazard and Operability Studies (HAZOP)
- Functional Hazard Assessment (FHA)
- Failure Mode and Effects Analysis (FMEA)
- Event Tree Analysis (ETA)
- Reliability Block Diagrams (RBD)
- Fault Tree Analysis (FTA)
- Hidden Markov Models
- Sneak Circuit Analysis

Begriffe

- Common Cause Analysis
  Die Common Cause Analyse (CCA) sucht nach singulären Fehlerursachen (Common Cause Failure – CCF), durch die funktional unabhängige Pfade in einem System gleichzeitig beeinflusst werden können.
  http://www.systema-gmbh.de/methoden/methoden-des-safety-engineering/common-cause-analysis.html

- causal analysis
  identifying cause and effect

V-Modell der Softwareentwicklung bei sicherheitskritischen Systemen (Beispiel)



Systemfunktion „Anfahren“

Als einfaches Beispiel wird die Systemfunktion „Anfahren“ bei einem PKW mit Automatikgetriebe genommen. Gewolltes Anfahren bei laufendem Motor wird durch die folgenden Bedienschritte erreicht:

- Auf die Betriebsbremse („Fussbremse“) treten und diese gedrückt halten.
- Den Wählhebel in die Stellung „D“ oder „R“ bringen.
- Ggf. die Feststellbremse („Handbremse“) lösen.
- Die Betriebsbremse lösen.
- Gas geben.

Fehlverhalten der Systemfunktion „Anfahren“ wäre „nicht gewolltes Anfahren“.

Functional Hazard Assessment (FHA)

Bei der FHA wird der Systementwurf aus funktionaler Sicht analysiert. Ziel ist die Identifikation von

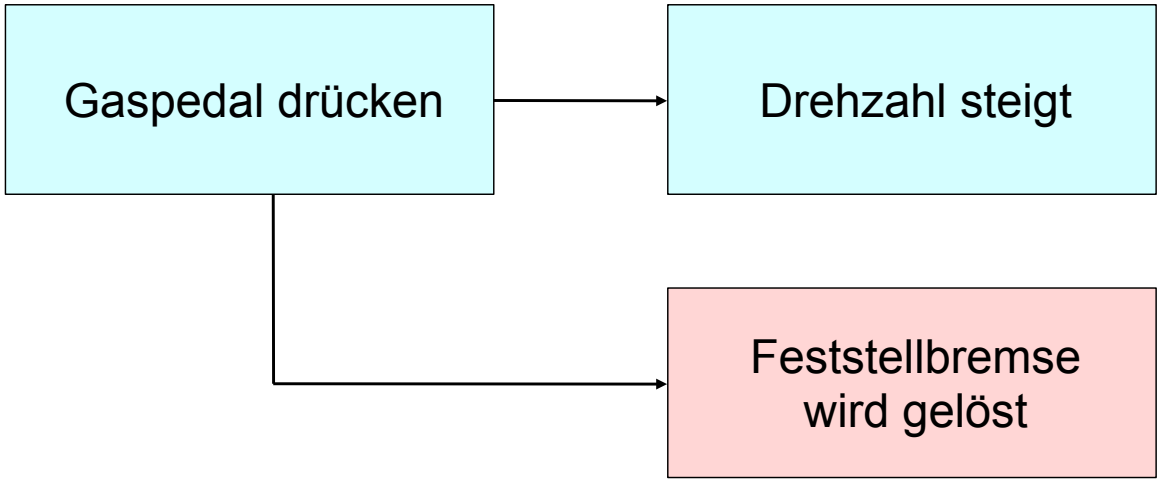
- Möglichem Fehlverhalten
- Betriebszustand, in dem das Fehlverhalten auftritt
- Auswirkung des Fehlverhaltens
- Klassifizierung der Auswirkungen (z.B. gefährlich, bedeutend, ungefährlich)
- Gegenmassnahmen (wenn sinnvoll)
- Überprüfungsmethode

Das Ergebnis der FHA wird meist in Tabellenform dokumentiert. Abbildung 3 zeigt das Ergebnis der FHA für das Beispiel „Anfahren“ (in Anlehnung an [2]).

Systemfunktion	Fehlverhalten	Betriebszustand	Auswirkung der Fehlerbedingung	Klassifizierung	Gegenmassnahmen	Überprüfungsmethode
Anfahren	Nicht gewolltes Anfahren	Motor aus, Bremsen gelöst, Stellung "N"	Fahrzeug kann anfahren (je nach Strassenneigung)	bedeutend	Schlüssel kann nur bei Stellung "P" abgezogen werden, evtl. Warnsignal	
	Nicht gewolltes Anfahren	Motordrehzahl über Grenzwert, Bremsen gelöst, Stellung "D" oder "R"	Fahrzeug fährt an	gefährlich		FMEA

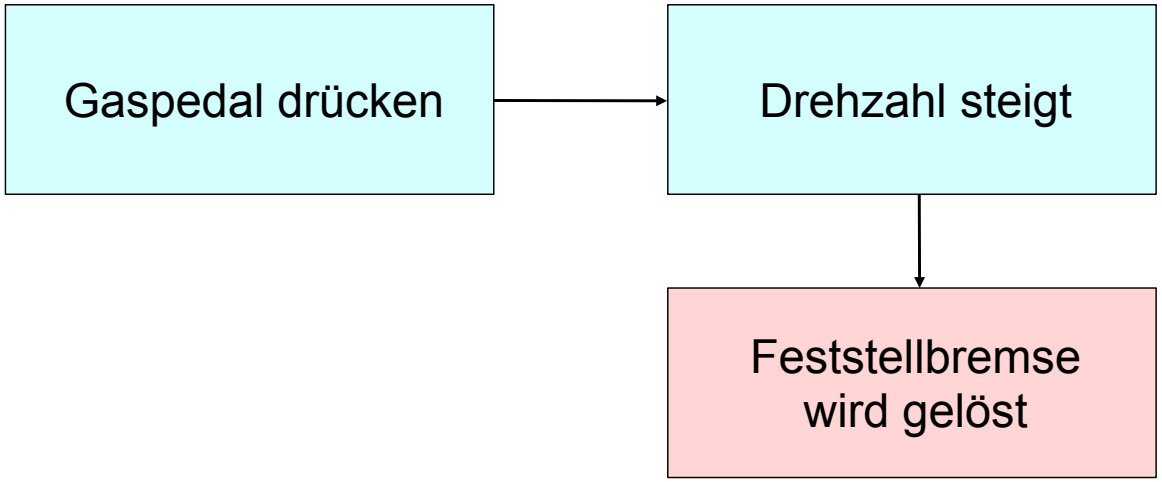
Abbildung 3: Ergebnis der FHA für die Systemfunktion „Anfahren“

Angedachte Lösung

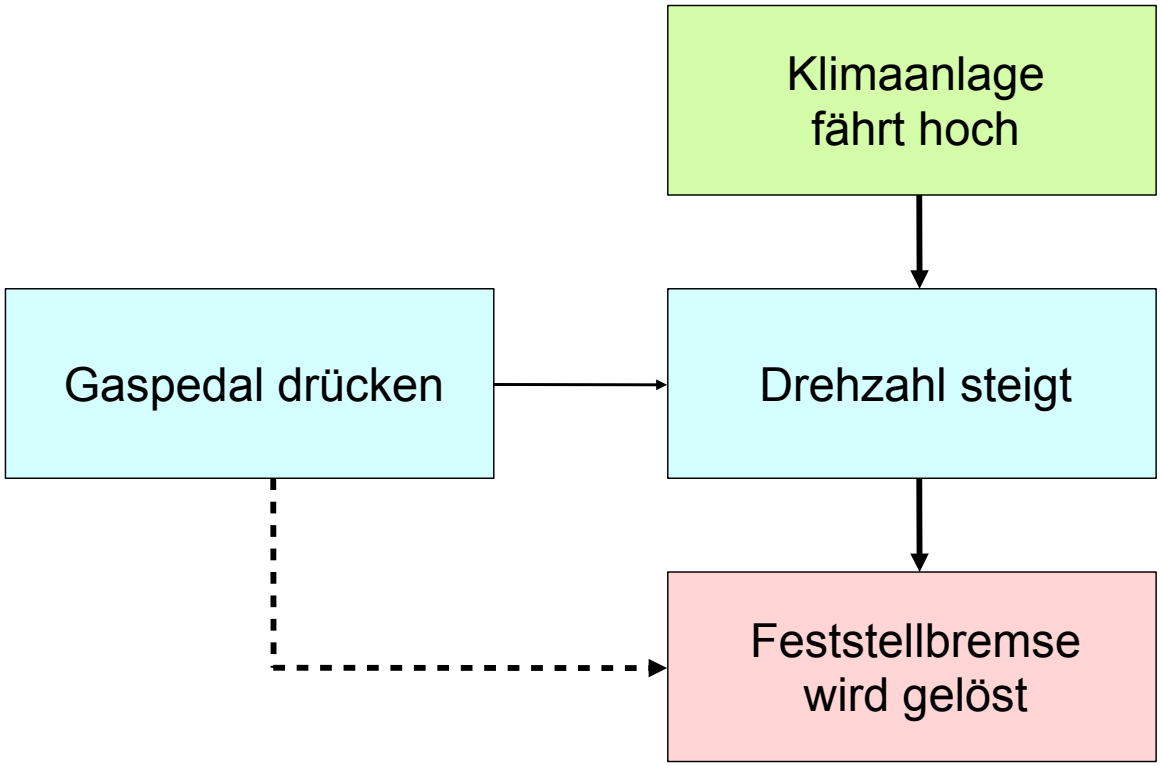


Realisierte Lösung

- Kostenziel
- Gewichtsszie l
- Drehzahl liegt schon auf CAN



Auswirkung

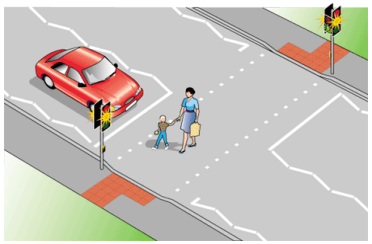

Klimaanlage
fährt hoch
Gaspedal drücken
Drehzahl steigt
Feststellbremse
wird gelöst

Beispiel Micro-Hybrid Stop-Start Feature

- Verifikation einer sicherheitskritischen Anwendung im Automobilbau
  Dr. Thomas Rambow, Ford Forschungszentrum Aachen GmbH
  7. SafeTRANS Industrial Day am 19. November 2009 bei EADS in Friedrichshafen

Example

Hazard: Unintended vehicle lurch



Safety Goal:

- Cranking the engine by the Micro-Hybrid Stop-Start Feature shall not contribute to vehicle movement (transfer torque to wheels) in other than vehicle pull-away maneuvers.

Functional and Technical Safety Concept

SW Safety Requirement:

- If the starter command is CRANK and the gear state is not NEUTRAL then the starter command shall be reset

Hybrid Antrieb

Ladestrategien

- Mindestladung der Batterie erhalten
- Ab definierter Motordrehzahl laden
- Nur Bremsenergie laden
- Konstanter Ladestrom
- Mindestreichweite
- ...

Zuschaltung Elektromotor

- Bis Richtgeschwindigkeit
- Ortsbezogen
- Ladungsbezogen
- Booster (siehe SPIEGEL 13.02.2010)
- ...

Beispiel ASIL-Levels für Antriebsstrang

- Halbleiter ermöglichen effiziente Lösungen in Elektrofahrzeugen
  Hans Adlkofer, Infineon Technologies AG München
  Moderne Elektronik im Kraftfahrzeug V, 16. - 17. Juni 2010, Dresden

- clustered to application segments

"For information only"
Subject to modification

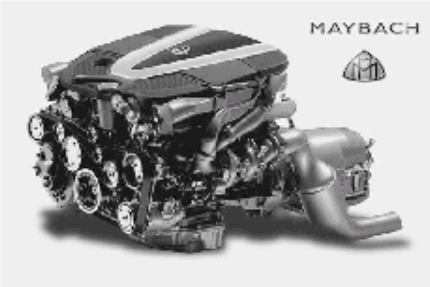
Application	ASIL level	Failure Reaction Time	Percentage for safty critical task
Gasoline Engine w/o ETC	QM	-	-
Gasoline Engine w ETC + GDI/DDI	C	100ms	10%
Transmission - ECAT with mechanical Backup	B	100ms	5%
Transmission - ECAT by wire	C	20ms	10%
DCT/CVT by wire	C	20ms	10%
accessories - water pump	QM	-	-
accessories - cooling fan	QM	-	-
accessories - fuel pump	QM	-	-
accessories - oil pump	QM	-	-
accessories - valve control (electronic)	D	4ms	30%
accessories - standard alternator	QM	-	-
Starter Alternator	B	20ms	10%
Hybrid or EV (Motor Drive)	D	10ms	30%
Battery Management	D	10ms	30%
Charger (PHEV-Range Extenter & EV)	A	10ms	5%
Infrastructure Power Plug	A	10ms	5%
DC/DC - HV to LV	D	10ms	30%
HV Accessories (air conditioning compressor)	A	10ms	5%

ASIL levels for Powertrain

Gliederung

1. Einleitung
2. Normen und Standards für sicherheitskritische Systeme
3. Analyse und Entwicklung sicherheitskritischer Systeme
4. **Zusammenfassung**

Beispiel FMEA - Motorenentwicklung



- **Motor „Typ 12“**
- **Biturbo-System mit mit zwei Ladeluftkühlern**
- **405 kW / 550 PS**
- **900 Nm**

Failure Mode and Effects Analysis									Blatt Nr.:		
Produkt-feature	Möglicher Fehler	Mögliche Folgen	Mögliche Fehler-ursache	Aktueller Status: Aktuelle Maß-nahme	Auftreten	Bedeutung	Entdeckung	RPZ	Maß-nahmen	Ver-ant-wortlich	Termin
Feder Nr. 103-5	Bruch	Zylinder-ausfall	Ermüdung	Festigkeits-test	6	7	10	420	versch.	R.B.Shaw	08/07/01
Öldicht-schraube	Leck	Ölverlust, Über-hitzung	Dichtung nicht fest genug	Höheres Montage-moment	7	9	9	567	dickere Dichtung	R.Frost	05/09/01

Bewertungszahlen:

A - Auftretenswahrscheinlichkeit
1 (unwahrscheinlich)
10 (hoch)

B - Bedeutung
1 (keine Bedeutung)
10 (sehr hohe Bedeutung)

E - Entdeckungswahrscheinlichkeit
1 (hoch)
10 (unwahrscheinlich)

Was bringt uns das?

- „Wir machen doch schon FMEA und haben einen ordentlichen Entwicklungsprozess.“
- Dann bringt die Anwendung der Sicherheitsnormen lokal und kurzfristug gesehen u. U. keinen Gewinn.

Aber:

- Die Anwendung der Sicherheitsnormen bringt Vergleichbarkeit.
- Die Anwendung der Sicherheitsnormen kann vom Gesetzgeber oder vom Auftraggeber vorgegeben sein.
- Mit der Anwendung der Sicherheitsnormen kann die Einhaltung des Standes von Wissenschaft und Technik belegt werden.
- Und schliesslich: Professionelle Neugier
  - Vergleich des eigenen Vorgehens mit den Sicherheitsnormen
  - Bewusstes Anpassen
  - Bewusstes Beibehalten
  - Vorbereitung für spätere Anpassung

Erfahrungen

- Standards müssen von Anfang an berücksichtigt werden
  - Der nachträgliche Nachweis der Befolgung von Standards ist kaum möglich
  - Die Anwendung von Standards muss bekannt sein und gelebt werden
- Methods und Werkzeuge sollten betriebsbewährt sein
  - Breiter Einsatz mit guten Erfahrungen
  - Stabiler Hersteller mit etabliertem Fehlermanagement
  - Leading edge“, nicht „bleeding edge“
- Aufwände für Kommunikation, Dokumentation und Verifikation nicht unterschätzen
- CMMI, SPICE etc.: Unterschiedliche Schwerpunkte, aber Überschneidungen
  - Gleiche Grundlagen: Stand der Wissenschaft und Technik
  - CMMI: Prozessorientiert
  - Sicherheitsstandards: Produktorientiert

Zusammenfassung

- Die funktionale Sicherheit ist durch anwendungsspezifische Standards geregelt:
  - Generischer Standard: IEC 61508
  - Bahnen: EN 50126, EN 50128, EN 50129
  - Luftfahrt: DO-178B/C, DO-254, ARP 4761, ARP 4754
  - Automotive: ISO/DIS 26262
- Grundlegende Konzepte der Sicherheitsstandards sind:
  - Risikoanalyse und Gefährdungsbeherrschung auf Systemebene
  - Sicherheitsmanagement und Sicherheitskultur
  - Einhaltung von vorgeschriebenen Methoden und Vorgehensweisen basierend auf dem Stand der Wissenschaft und Technik
- Unterschiede zwischen Sicherheitsstandards durch anwendungsspezifische Interpretation und Umsetzung der Sicherheitskonzepte
  - Betrachtung der Umwelt (IEC 61508, EN501xy)
  - Sicherer Zustand (Bahnen), kein sicherer Zustand (Luftfahrt)
  - Betrachtung der Produktion (ISO/DIS 26262)
  - Personelle oder organisatorische Unabhängigkeit von Entwickler und Prüfer (EN501xy, DO-178B)
  - ...

Dr. Bernhard Hohlfeld
Business Unit MPT
Methods, Processes & Tools
ICS AG
Geschäftsstelle Ulm
Sedanstrasse 14
D-89077 Ulm

Tel.: +49 731 392 8320
Mobile: +49 172 7280510

Email: bernhard.hohlfeld@ics-ag.de
Web: www.ics-ag.de