Dynamic Test Center

Funktionale Sicherheit

Felix Iseli
DTC AG
Vauffelin

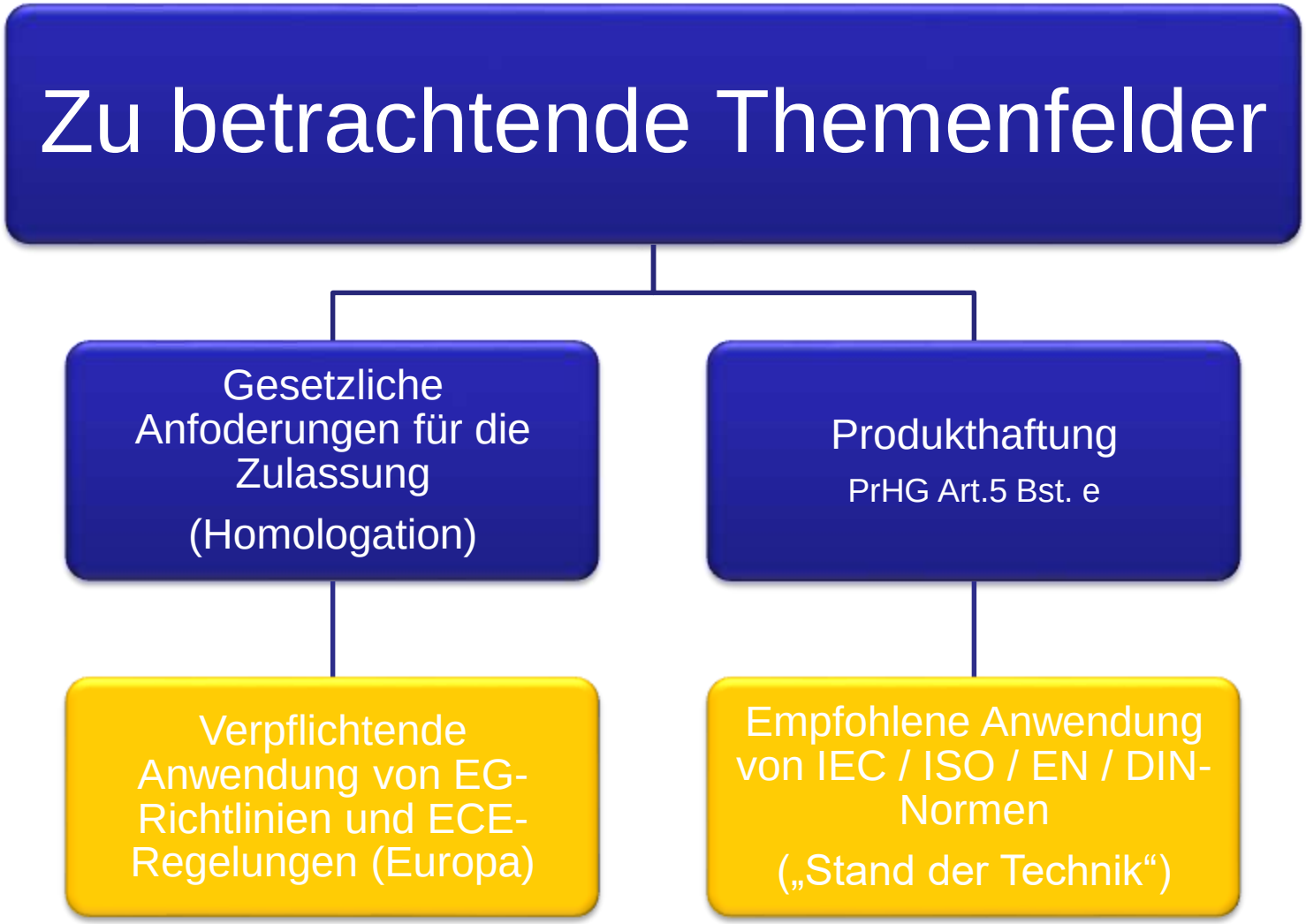
Was ist funktionale Sicherheit?

- Funktionale Sicherheit = es muss etwas funktionieren wenn „es“ kritisch wird
- Alternative Sicherheitskonzepte:
  - Mechanische Sicherheit (Abdeckgitter)
  - Elektrische Sicherheit (Isolation)
  - Chemische Sicherheit (Batterien)
  - Andere Massnahmen (z.B. „Unbefugten Zutritt Verboten“)
- Funktionale Sicherheit
  - Ist für den Benutzer nicht erkennbar
  - Ist für die Hardware „teilweise“ prüfbar (Schaltplan)
  - Muss für SW aus dem Entwicklungsprozess kommen

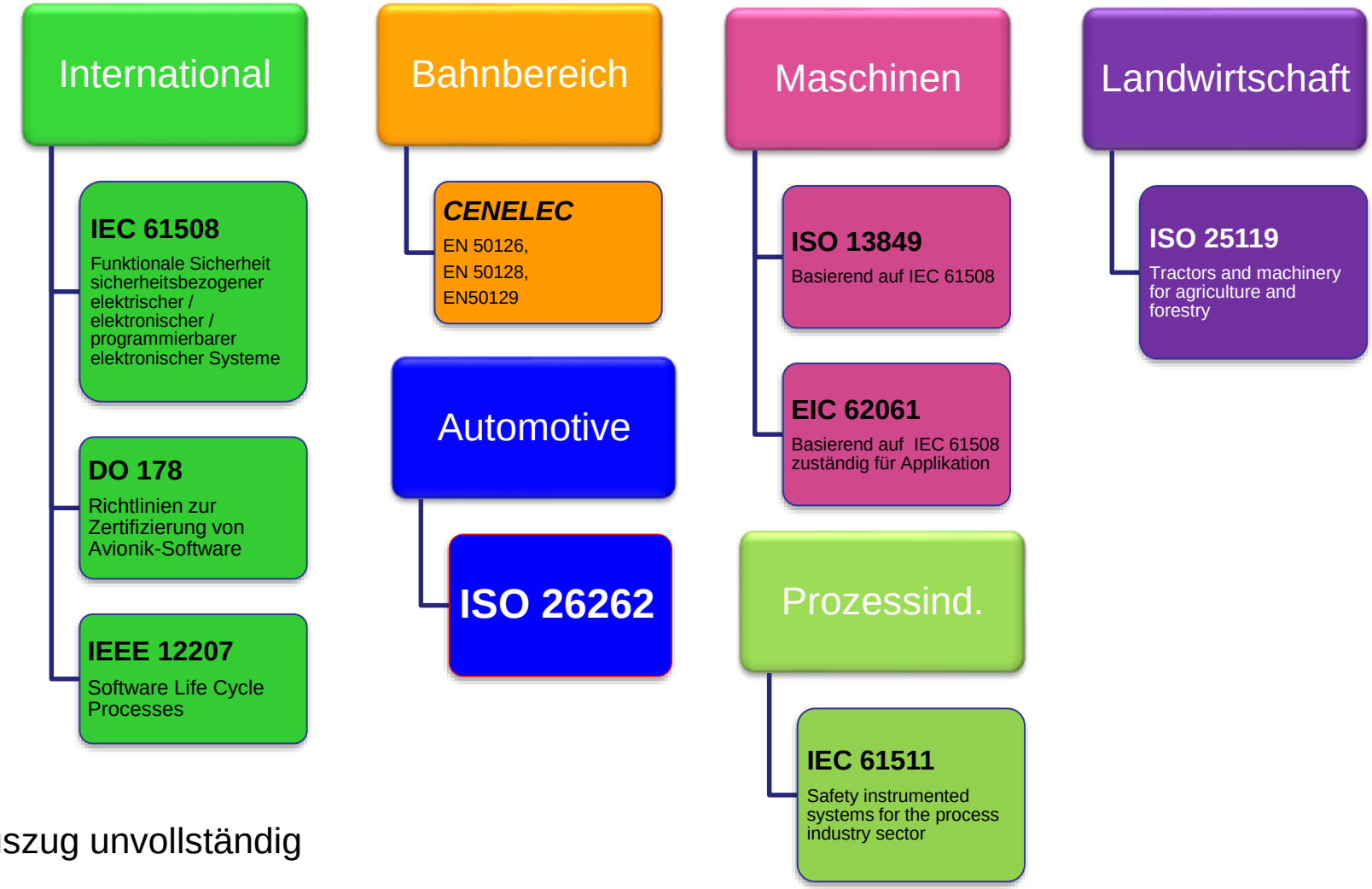
Funktionale Sicherheit = Risikoreduzierung nach ASIL

(Automotive Safety Integrity Level)

Rechtslage


Zu betrachtende Themenfelder
Gesetzliche Anfoderungen für die Zulassung
(Homologation)
Produkthaftung
PrHG Art.5 Bst. e
Verpflichtende Anwendung von EG-Richtlinien und ECE-Regelungen (Europa)
Empfohlene Anwendung von IEC / ISO / EN / DIN-Normen
(„Stand der Technik“)

Normen zur funktionalen Sicherheit



Auszug unvollständig

Übersicht ISO 26262

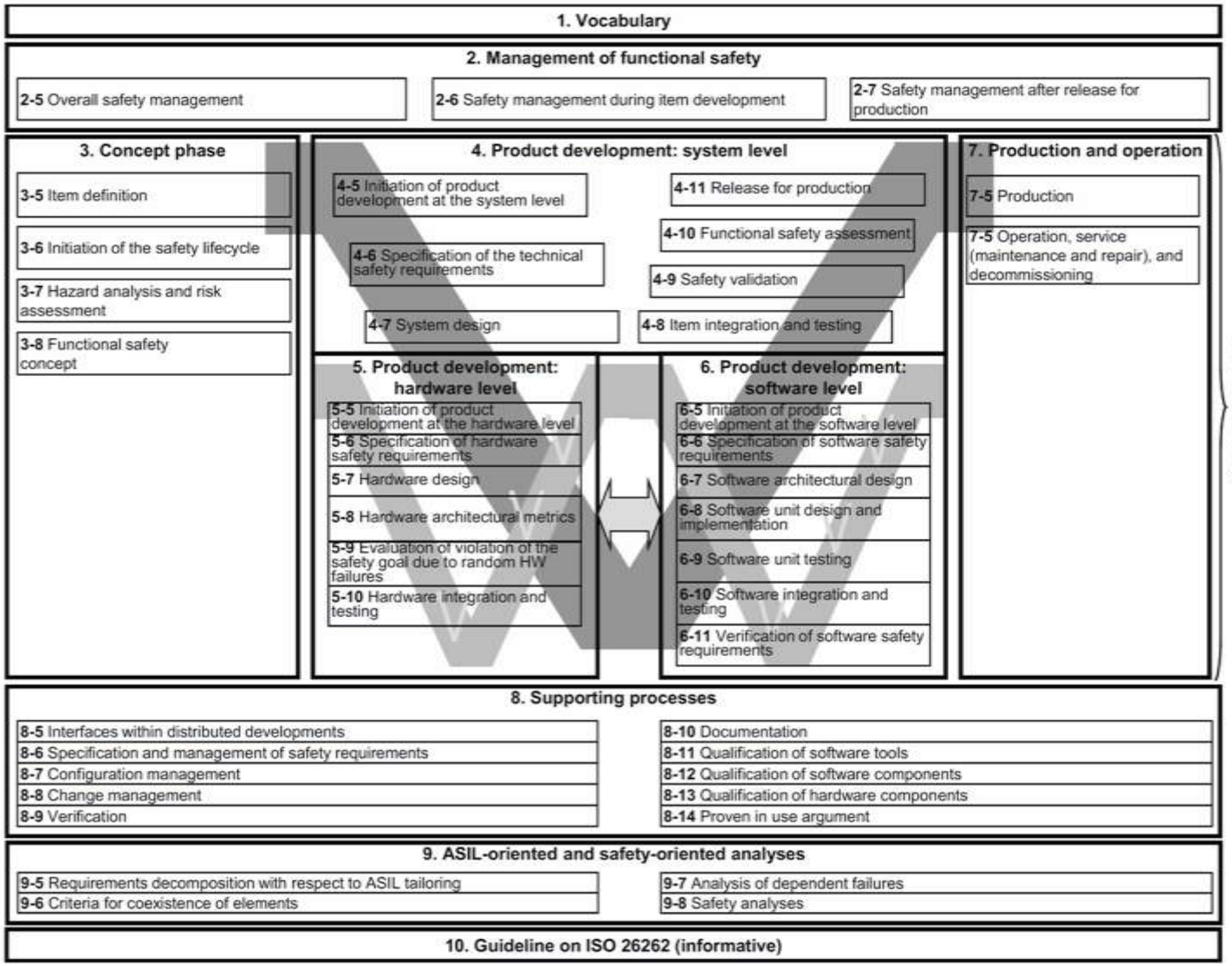


Figure 1 — Overview of ISO 26262

Gefährdungsanalyse: Arbeitsschritte

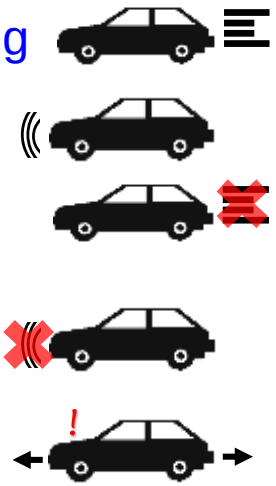
Kapitel 7 in ISO 26262-3

Situationsanalyse und Identifikation der Gefährdungen	• Systematische Aufstellung der Fahrsituationen • Identifikation der zugehörigen möglichen Gefährdungen
Klassifikation der Gefährdungen	• Klassifikation der Gefährdungen (Ableitung der Risikoparameter S, E und C)
ASIL Bestimmung	• Ableitung des ASIL mittels Risikomatrix
Definition der Sicherheitsziele	• Beschreibung der einzuhaltenden Sicherheitsziele
Review	• Überprüfung auf Vollständigkeit, Korrektheit und Konsistenz der Einstufungen

Risiken bedingt durch Fehlfunktionen

Funktionale Risiken

- unbeabsichtigte Beschleunigung
- unbeabsichtigte Verzögerung
- unbeabsichtigter Verlust der Beschleunigung
- unbeabsichtigter Verlust der Verzögerung
- unbeabsichtigte Fahrzeugbewegung



Nicht funktionale Risiken (Beispiele)

- hohe Spannung
- Feuer / Explosion

Massnahmen zur Risikoreduzierung

Funktionale Sicherheit

- Überwachende Funktionen (Sicherheitsfunktion, z.B. Einklemmschutz)
- Zuverlässigkeit der Zielfunktion

Sonstige Massnahmen

- Designmassnahmen (z.B. Isolation)
- Organisatorische Massnahmen (z.B. Arbeitsvorschriften)

Gefährdungsanalyse: Risikomatrix

Kapitel 7 in ISO 26262-3

Summe = S+E+C

6 und kleiner = ASIL QM
7 = ASIL A
8 = ASIL B
9 = ASIL C
10 = ASIL D

Schadensausmass S=Severity	*Wahrscheinlichkeit E=Exposure*	*Gefahrenabwendung C=Controllability*		
		C1	*C2*	*C3*
S1	*E1*	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	*E1*	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	*E1*	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	**D**

Wenn S,E oder C = 0 dann ASIL = QM

Gefährdungsanalyse: Unabhängiges Review

Bestätigungsmassnahme	Unabhängig vom ermittelten ASIL
Review der Gefährdungsanalyse (H&R)	I3

Auszug aus ISO 26262-2, Table D.1

I3: die Bestätigungsmassnahme soll von einer Person aus einer anderen Abteilung oder Organisationseinheit durchgeführt werden (unabhängig von der relevanten Abteilung bezüglich Management, Ressourcen und Verantwortung für die Produktionsfreigabe)