STARKES STUDIUM.
PRIMA ZUKUNFT.

HOCHSCHULE HEILBRONN

TECHNIK WIRTSCHAFT INFORMATIK

Sicherheitstechnik, 1. Vorlesung (Safety Technology)

Campus Heilbronn

Campus Künzelsau
Reinhold-Würth-Hochschule

Campus Schwäbisch Hall

Fred Härtelt, Heilbronn

Kontaktdaten

Dipl.-Inf. Fred Härtelt

Fachreferent Zentrales Qualitätsmanagement

Gutachter für die Akkreditierung von Studiengängen

Bosch Engineering GmbH (BEG/QMM)

Postfach 1350

74003 Heilbronn

Telefon: 07062 / 911-7016

E-Mail: fred.haertelt@hs-heilbronn.de

Sicherheitstechnik

- Termin: Montag, 17:30 – 19:00, wöchentlich (2 SWS)
- Vorlesung mit integrierter Übung
- Sicherheitstechnik sowie Sicherheit und Zuverlässigkeit von Systemen
- Prüfung: Belegarbeit + Präsentation (Gruppenarbeit)
- Vorlesungsunterlagen im ILIAS verfügbar (Kurse: 304144 und 194318) H4.4 Sicherheit und Zuverlässigkeit für Studiengänge ASE, ESE, MR
- Kennenlernen der Vorgehensweise bei der Auslegung von sicherheitsgerichteten Systemen (Maschine, Auto)
- Analyse und Entwurf von Sicherheitsrelevanten Systemen

Sicherheitstechnik: zeitlicher Überblick

- **1. V: Definition Sicherheit, Normen und Vorschriften (14.03.2022)**
- 2. V: Festlegung von Grenzen und Gefährdungen (21.03.2022)
- 3. V: Risikobeurteilung, -minimierung, Risikograph (28.03.2022)
- 4. V: Verteilungsfunktion, Ausfallraten, Fehlerbeherrschung (04.04.2022)
- 5. V: Fehlervermeidung, Fehlerentdeckung, FMEA (11.04.2022)
- Keine Vorlesung am 18.04.2022 (Ostermontag)
- Keine Vorlesung am 25.04.2022
- 6. V: Redundanz, Strukturierungsmaßnahmen, FTA (02.05.2022)
- 7. V: Berechnung von Ausfallraten, FMEDA, Aufgabenstellung Belegarbeit, **Einteilung der Gruppen** (09.05.2022)
- 8. V: Prozess vs. Technik, Besonderheiten HW/SW, Zuverlässigkeit SW Entwicklungsprozess, Bsp. Belegarbeit, **Beginn der Gruppenarbeit** (16.05.2022)
- Rückfragen bezüglich Gruppenarbeit am 23.05., 30.05. und 13.06.2022 (WebEx)
- Abgabetermin der Gruppenarbeiten: **20.06.2022** (vor Beginn der Präsentationen)
- Präsentationstermine der Gruppen: **20.06.2022** (vorläufiger Stand)

Sicherheitstechnik
Literatur

- [1] Maschinenbau Praxis: „Risikobeurteilung gemäß 2006/42/EG – Handlungshilfe und Potentiale“ (U. Kessels, S. Muck)
- [2] Bosch Rexroth: „10 Schritte zum Performance Level – Handbuch zur Umsetzung der Funktionalen Sicherheit nach ISO 13849“ (Jürgen Barg, Franz Eisenhut-Fuchsberger)
- [3] Verschiedene Normen (z.B. ISO 26262, ISO 12100)
- [4] Johannes Schild: „Zehn Schritte zur Maschinensicherheit“
- [5] Birolini, A..: Qualität und Zuverlässigkeit technischer Systeme
- [6] Kopetz, H.: Software Relabilty
- [7] Meyna, A.: Einführung in die Sicherheitstheorie
- [8] Reinschke, K,: Zuverlässigkeit von Systemen
- [9] Schäfer, E.: Zuverlässigkeit, Verfügbarkeit und Sicherheit in der Elektronik

Sicherheitstechnik
Inhalte

- Definition Sicherheit
- Aktuelle Normen und Vorschriften
- Methoden und Verfahren
  - Risikobeurteilung und –minderung, Risikograph
  - Verteilungsfunktionen, Ausfallraten, Fehlerbeherrschung und Vermeidung, Fehlerentdeckung, Redundanz
  - Strukturierungsmaßnahmen, FMEA, FTA, FMEDA u.a.
  - Unterscheidung Prozess vs. Technik
- Besonderheiten hinsichtlich Hardware und Software (Zuverlässigkeit SW Entwicklungsprozess)

Definition Sicherheit

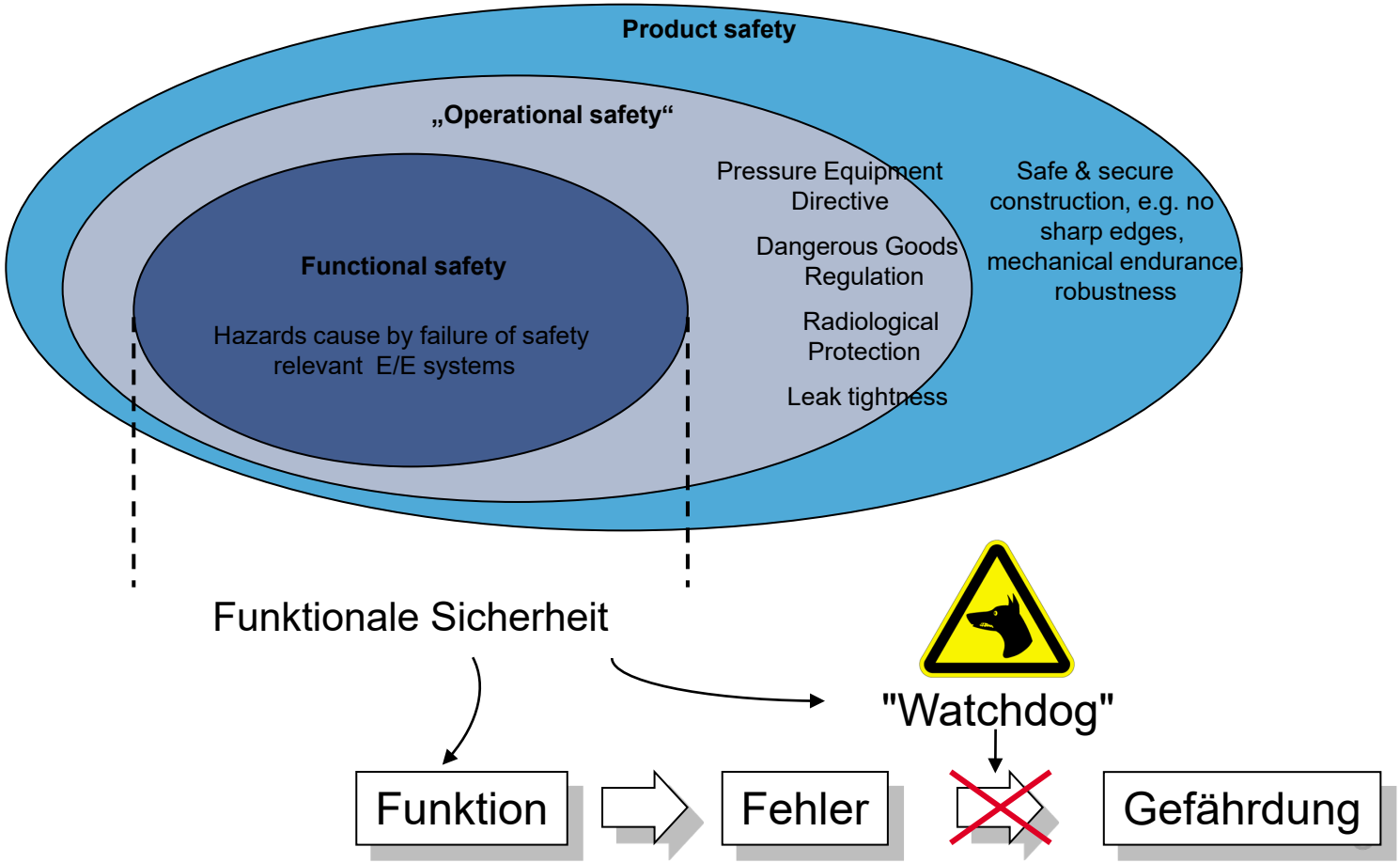
„***Sicherheit*** (von lat. *sēcūritās* zurückgehend auf *sēcūrus* „sorglos“, aus *sēd* „ohne“ und *cūra* „(Für-)Sorge“) *bezeichnet einen Zustand, der frei von unvertretbaren Risiken ist oder als gefahrenfrei angesehen wird*.“ (Allgemeine Definition nach wikipedia)

Sicherheit = „*Freiheit von unvertretbaren Risiken*“ (nach IEC 61508)

Definition Sicherheit

- Spannungsfelder
  - Sicherheit vs. Kosten
  - Sicherheit vs. Verfügbarkeit
  - Sicherheit vs. Stand der Technik
  - ...
- Definition
  - Sicherheit vs. Funktionale Sicherheit

Einblick: Abgrenzung zur Funktionalen Sicherheit



Definition Sicherheit

Sicherheitstechnik:

- Untersuchungen von Problemen und Definition von Lösungen in der Sicherheit auf Basis von Normen / Richtlinien und unter Zuhilfenahme ausgewählter Methoden
- Es wird unterschieden zwischen:
  - Unmittelbarer Sicherheit (Verhinderung einer Gefahrenentstehung)
    - Safe-Life, Fail-Safe Ansatz, Redundanz
  - Mittelbarer Sicherheit (zusätzliche Schutzeinrichtungen weisen eine mögliche Gefährdung ab)
    - Zusätzliche Schutzeinrichtungen (Maschinenverkleidung, Sensoren)
  - Hinweisender Sicherheit (Hinweis auf Gefahren)
    - Gefahrenhinweise, Bedienungsanleitungen, Verkehr

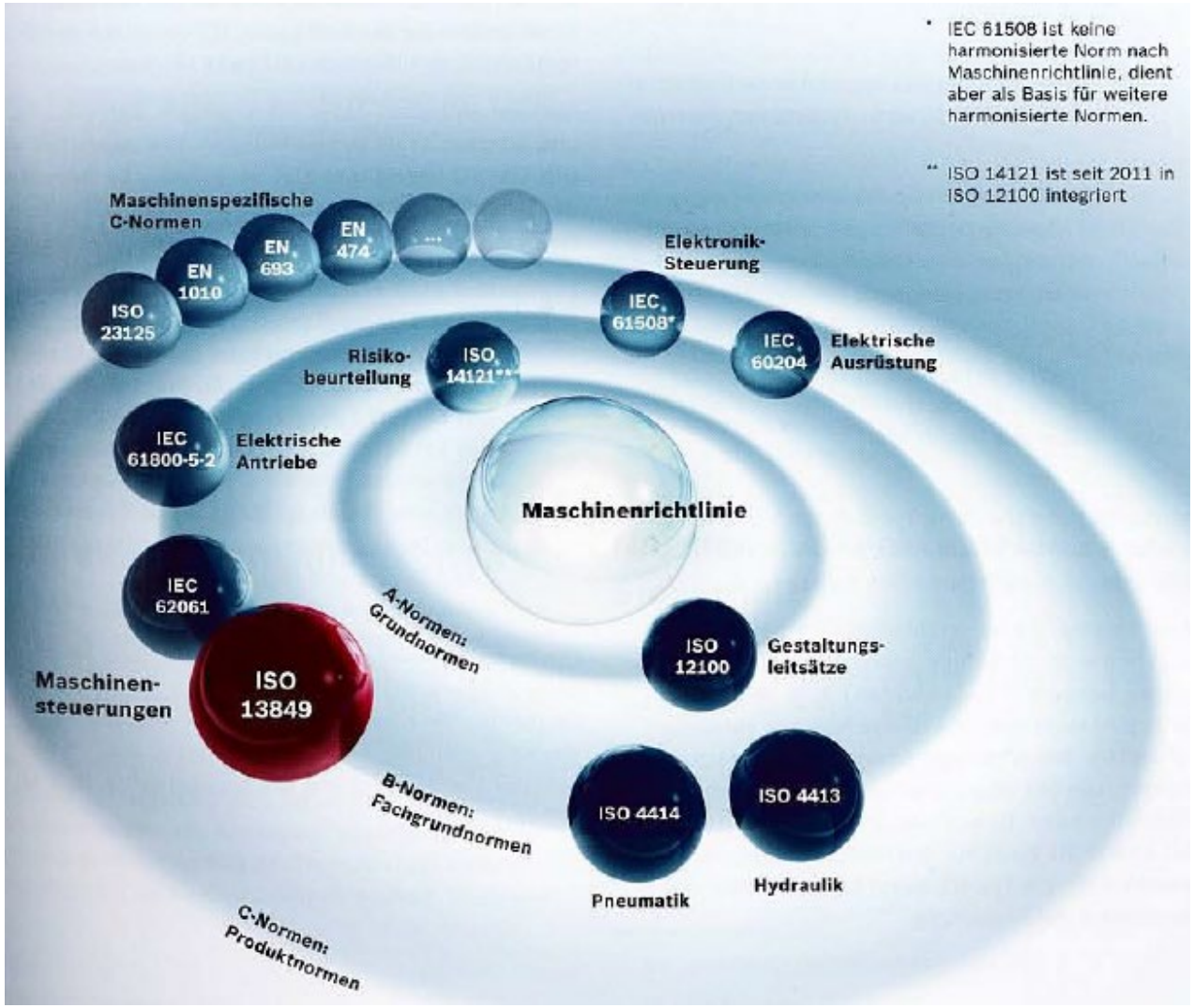
Definition Sicherheit

- Relevant für die Sicherheit von Maschinen ist vor allem die „Maschinenrichtlinie“ (2006/42/EG)
- Umsetzung der Sicherheit neben der „Maschinenrichtlinie“ durch weitere Gesetze / Verordnungen auf nationaler Ebene und Anwendung harmonisierter Normen in der Praxis
- Für die Automobilindustrie gilt die ISO 26262
- Für andere Produkte (z.B. Bahn, Flugzeug) können andere Normen gelten

Sicherheitstechnik
Inhalte

- Definition Sicherheit
- Aktuelle Normen und Vorschriften
- Methoden und Verfahren
  - Risikobeurteilung und –minderung, Risikograph
  - Verteilungsfunktionen, Ausfallraten, Fehlerbeherrschung und Vermeidung, Fehlerentdeckung, Redundanz
  - Strukturierungsmaßnahmen, FMEA, FTA, FMEDA u.a.
  - Unterscheidung Prozess vs. Technik
- Besonderheiten hinsichtlich Hardware und Software (Zuverlässigkeit SW Entwicklungsprozess)

Aktuelle Normen und Vorschriften

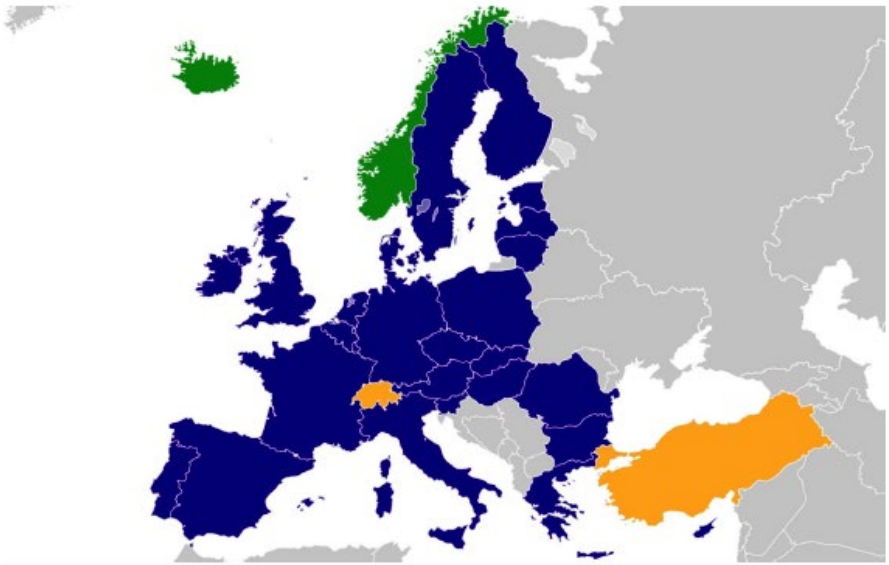


Quelle:

Nach [2], S. 25

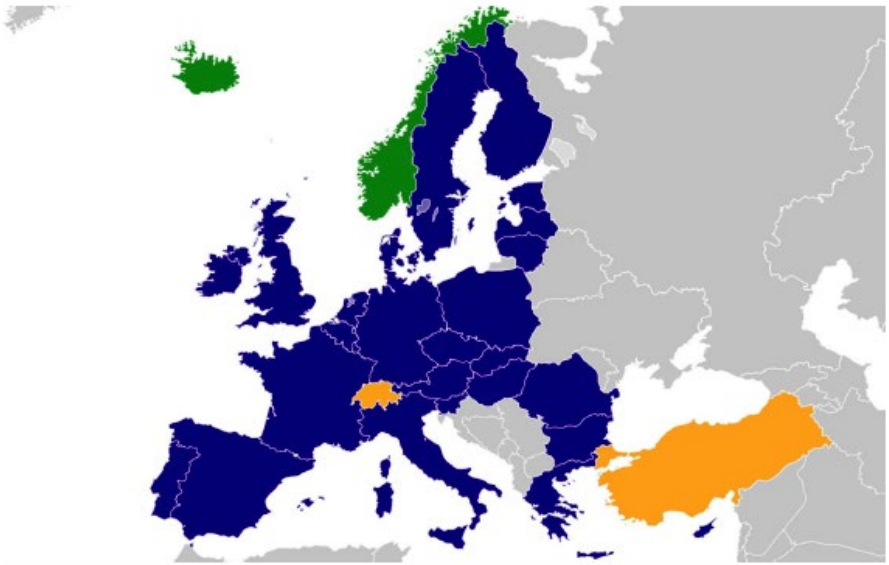
Aktuelle Normen und Vorschriften
Maschinenrichtlinie (2006/42/EG)

- Gültigkeitsbereich
  - Import aus Ländern, die nicht dem Gültigkeitsbereich angehören: Maschinenrichtlinie hat Gültigkeit
  - Export aus dem Gültigkeitsbereich: Bestimmungen des importierenden Landes gelten



Aktuelle Normen und Vorschriften
Maschinenrichtlinie (2006/42/EG)

- Anwendungsbereich:
  - Maschinen
  - Auswechselbare Ausrüstungen
  - Sicherheitsbauteile
  - Lastaufnahmemittel
  - Ketten, Seile und Gurte
  - Abnehmbare Gelenkwellen
  - Unvollständige Maschinen

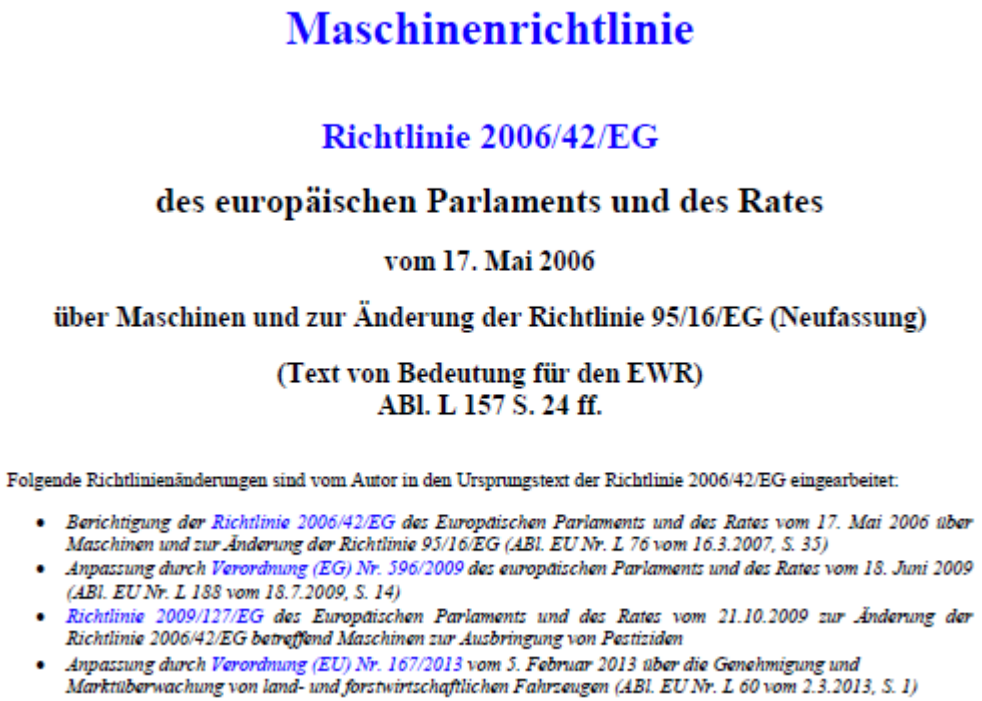


- Definition Maschine:
  - Keine Menschliche Kraft
  - Mindestens eine Bewegung

Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)

- Vollständige Übersicht über die Maschinenrichtline

  www.maschinenrichtline.de



Maschinenrichtlinie

Richtlinie 2006/42/EG

des europäischen Parlaments und des Rates

vom 17. Mai 2006

über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung)

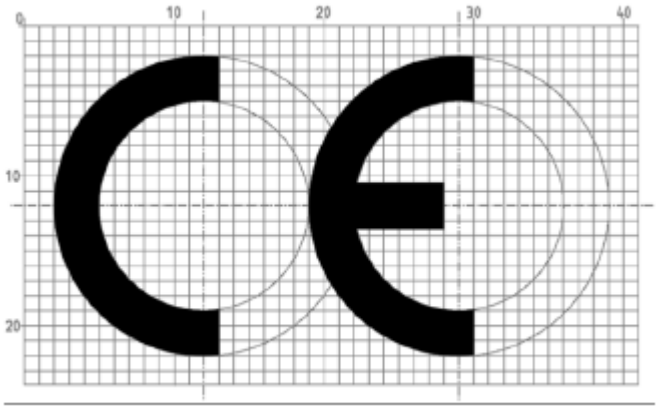
(Text von Bedeutung für den EWR)
ABl. L 157 S. 24 ff.

Folgende Richtlinienänderungen sind vom Autor in den Ursprungstext der Richtlinie 2006/42/EG eingearbeitet:

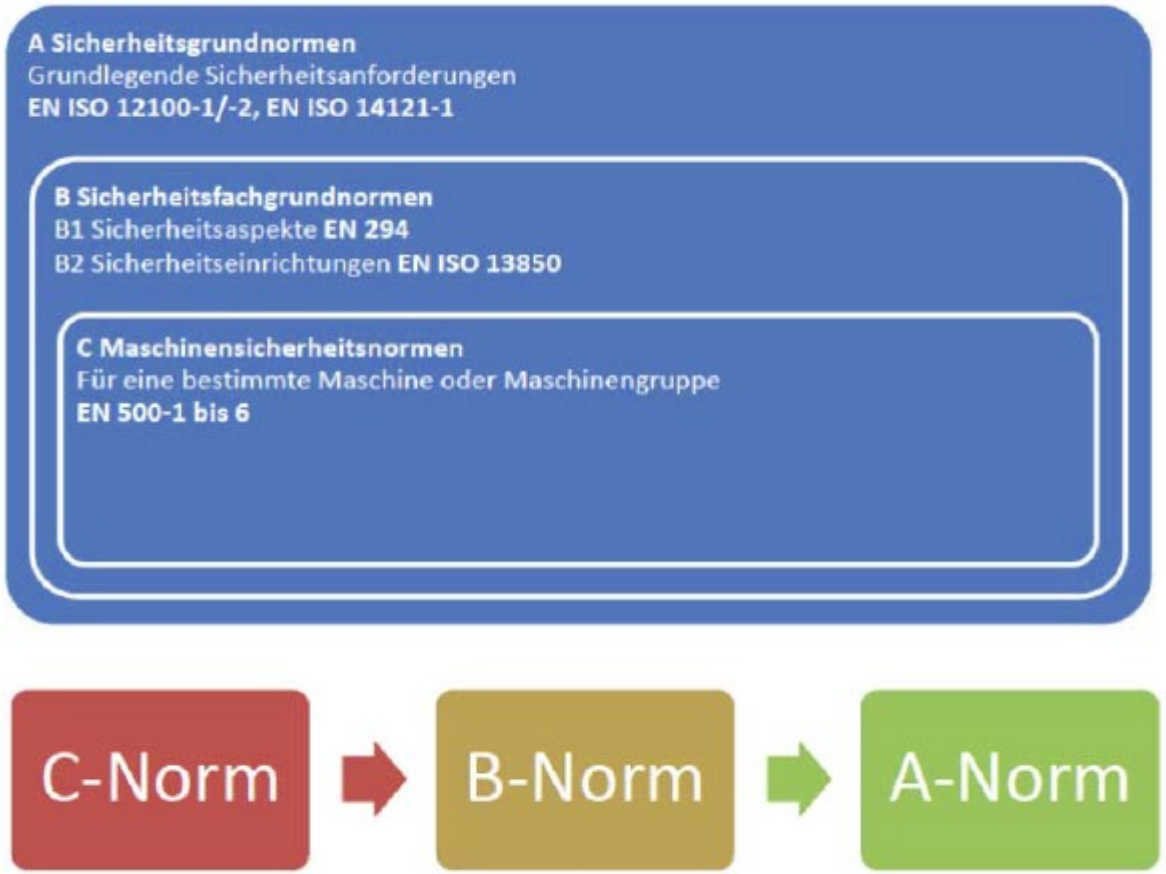
- *Berichtigung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (ABl. EU Nr. L 76 vom 16.3.2007, S. 35)*
- *Anpassung durch Verordnung (EG) Nr. 596/2009 des europäischen Parlaments und des Rates vom 18. Juni 2009 (ABl. EU Nr. L 188 vom 18.7.2009, S. 14)*
- *Richtlinie 2009/127/EG des Europäischen Parlaments und des Rates vom 21.10.2009 zur Änderung der Richtlinie 2006/42/EG betreffend Maschinen zur Ausbringung von Pestiziden*
- *Anpassung durch Verordnung (EU) Nr. 167/2013 vom 5. Februar 2013 über die Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen Fahrzeugen (ABl. EU Nr. L 60 vom 2.3.2013, S. 1)*

Aktuelle Normen und Vorschriften
Maschinenrichtlinie (2006/42/EG)

- Inverkehrbringen von Maschinen
  - Einhalten der Maschinenrichtlinie
  - Konformitätsbewertungsverfahren
  - Anbringen der **CE-Kennzeichnung**



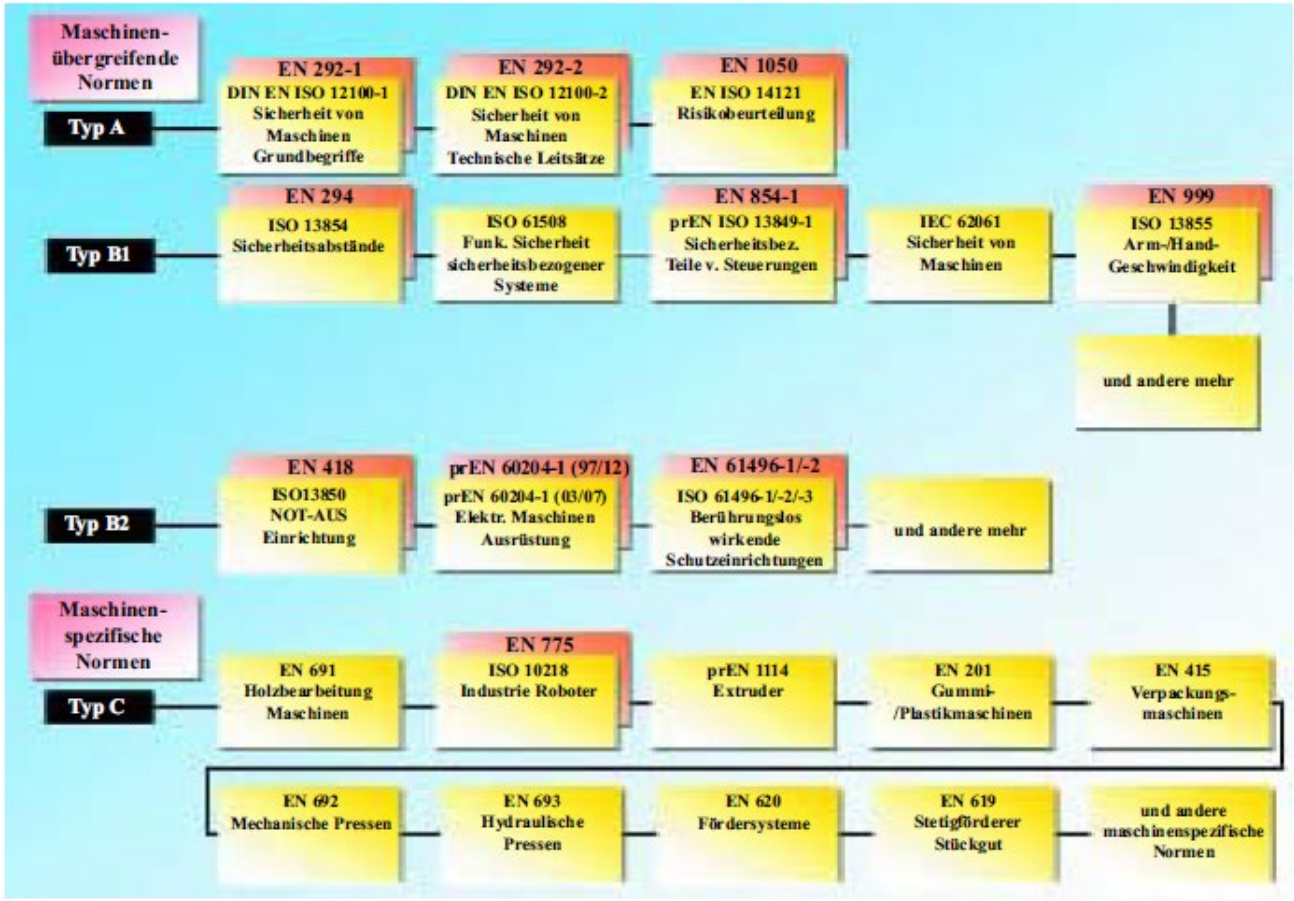
Aktuelle Normen und Vorschriften
Maschinenrichtlinie (2006/42/EG)



Aktuelle Normen und Vorschriften
Maschinenrichtlinie (2006/42/EG)

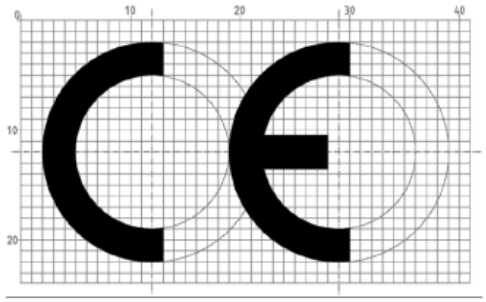
- 1. Soll eine Maschine konstruiert werden, wird zuerst die passende C-Norm gesucht -> wenn vorhanden: Anwendung der C-Norm (Prioriät vor B- und A-Norm)
- 2. Ist keine C-Norm vorhanden wird nach einer passenden B-Norm gesucht -> wenn vorhanden: Anwendung der B-Norm (Priorität vor A-Norm)
- 3. Ist keine C- und B-Norm vorhanden ist die zugehörige A-Norm anzuwenden

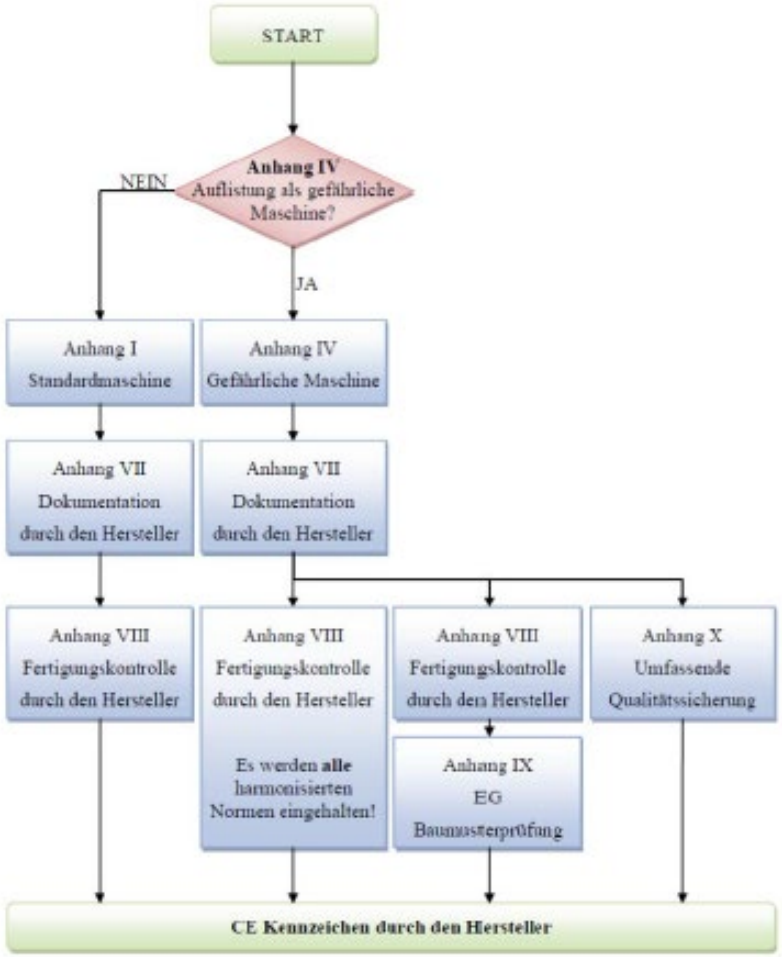
Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)



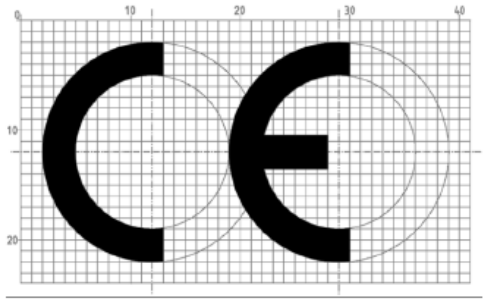
Quelle: Dietz, Normenheft Sicherheit für Maschinen

Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)



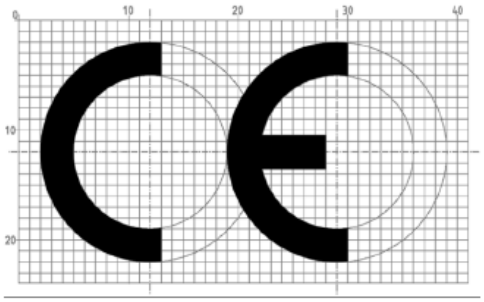


Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)



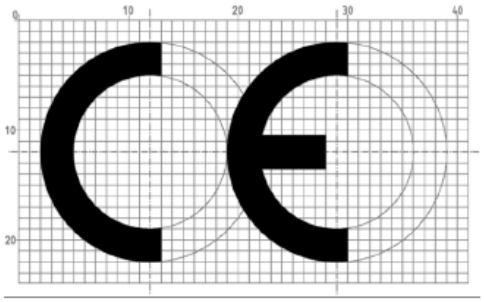
- Anhang I – Grundlegende Anforderungen
  - Allgemeine Grundsätze
  - Grundlegende Sicherheits- und Gesundheitsschutz Anforderungen an Standardmaschinen
    - Allgemeines, Steuerungen und Befehlseinrichtungen, Schutzmaßnahmen gegen mechanische Gefährdungen, Anforderungen an Schutzeinrichtungen, Risiken durch sonstige Gefährdungen, Instandhaltungen, Informationen, ….
  - Zusätzliche grundlegende Sicherheits- und Gesundheitsschutz Anforderungen an bestimmte Maschinengattungen
    - Nahrungsmittelmaschinen, Maschinen für kosmetische Erzeugnisse, für pharmazeutische Erzeugnisse, für die Holzbearbeitung, Handgehaltene und / oder handgeführte tragbare Maschinen
  - …

Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)



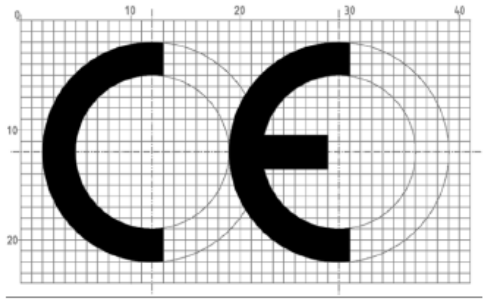
- Anhang I – Grundlegende Anforderungen
  - Zusätzliche grundlegende Sicherheits- und Gesundheitsschutzanforderungen zur Ausschaltung von Gefährdungen, die von der Beweglichkeit von Maschinen ausgeht.
  - Zusätzliche grundlegende Sicherheits- und Gesundheitsschutzanforderungen zur Ausschaltung der durch Hebevorgänge bedingten Gefährdungen.
  - Zusätzliche grundlegende Sicherheits- und Gesundheitsschutzanforderungen an Maschinen, die zum Einsatz unter Tage bestimmt sind.
  - Zusätzliche grundlegende Sicherheits- und Gesundheitsschutzanforderungen an Maschinen, von denen durch das Heben von Personen bedingte Gefährdungen ausgehen.

Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)



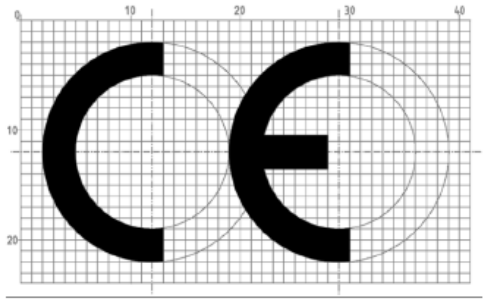
- Anhang II – Erklärungen
  - Teil 1:
    - EG Konformitätserklärung für eine Maschine
    - EG Erklärung für den Einbau einer unvollständigen Maschine
  - Teil 2: Aufbewahrungsfrist

Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)



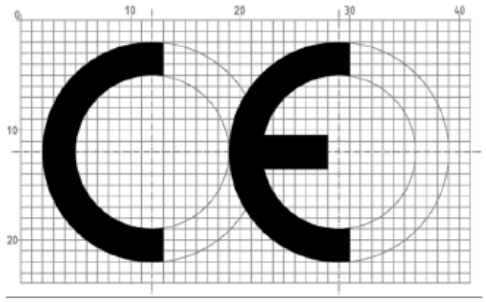
- Anhang IV – Sonderverfahren für spezielle Maschinen/Bauteile
  - Die im Anhang IV gelisteten Maschinen zählen zu den gefährlichen Maschinen
  - Die im Anhang IV gelisteten Maschinen und Bauteile unterliegen hohen Anforderungen, da ein Versagen zu gravierenden gefahrenbringenden Zuständen führen kann.
  - Beispiele: Sägemaschinen, Hobelmaschinen, Bandsägen, Fräsmaschinen, Handkettensägen, Pressen, Spritzgießmaschinen, Formpressmaschinen, Lokomotiven und Bremswagen unter Tage, …

Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)



- Anhang V – Sicherheitsbauteile (z.B.)
  - Not – Halt Befehlsgeräte
  - Zweihandschaltungen
  - Schutzeinrichtung für abnehmbare Gelenkwellen
  - Schutzeinrichtungen für Personendetektion (Lichtvorhang, Trittmatten, …)
  - Kraftbetriebene, bewegliche, trennend Schutzeinrichtungen
  - Logikeinheiten zur Gewährung der Sicherheitsfunktionen
  - Ventile mit Ausfallerkennung
  - Systeme zur Beseitigung von Emissionen
  - Trennende Schutzeinrichtungen zum Schutz für Personen vor beweglichen Teilen
  - Nichttrennende Schutzeinrichtungen zum Schutz für Personen vor beweglichen Teilen
  - Einrichtungen zur Überlastsicherung und Bewegungsbegrenzung bei Hebezeugen
  - Personen Rückhalteeinrichtungen für Sitze
  - Ableitsysteme für gefährliche elektrostatische Aufladungen
  - Energiebegrenzer und Entlastungseinrichtungen
  - Systeme zur Verminderung von Lärm und Vibration

Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)



- Anhang VII – Technische Unterlagen für Maschinen
  - Für die Definition von Sicherheitsfunktionen sind die Unterlagen über die Risikobewertung entscheidend, denn sie müssen auch

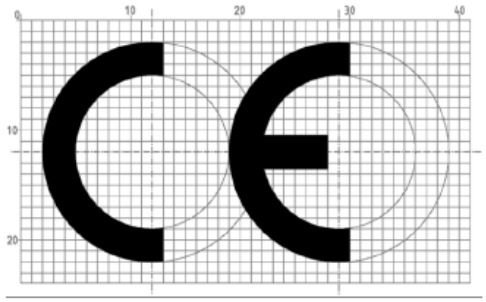
    „…eine Beschreibung der zur Abwendung ermittelnder Gefährdungen oder zur Risikominderung ergriffenen Schutzmaßnahmen und ggf. eine Angabe der von der Maschine ausgehenden Restrisiken…“

    enthalten.

Technische Unterlage	VM	UM
Allgemeine Beschreibung	■	
Übersichtszeichnung	■	■
Schaltpläne	■	■
Funktionsbeschreibungen	■	■
Vollständige Detailzeichnungen mit Berechnungen, Versuchsergebnissen und Bescheinigungen, die für die Überprüfung der Übereinstimmung der Maschine mit den grundlegenden Sicherheits– und Gesundheitsschutzanforderungen erforderlich sind.	■	■
Die Unterlagen der Risikobeurteilung aus denen hervorgeht welches Verfahren angewandt wurde. (Konstruktive Maßnahmen, Schutzmaßnahmen, Restrisiken)	■	■
Die angewandten Normen und sonstige technische Spezifikationen.	■	■
Alle technischen Berichte mit den Ergebnissen der Prüfungen, die von Hersteller oder einer Stelle seiner Wahl durchgeführt wurden.	■	■
Betriebsanleitung	■	
Einbauerklärung		■
Montageanleitung		■
EG Konformitätserklärung	■	

(Vollständige Maschine **VM** / Unvollständige Maschine **UM**)

Aktuelle Normen und Vorschriften Maschinenrichtlinie (2006/42/EG)



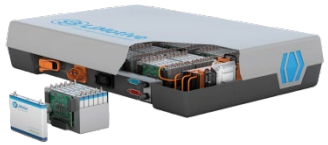
- Folgende Punkte müssen erfüllt sein:
  - Gefahrenanalyse (EN 12100, EN14121)
  - Risikobewertung (EN 14121)
  - Technische Dokumentation
  - Betriebsanleitung

Sicherheitstechnik
Inhalte

- Definition Sicherheit
- Aktuelle Normen und Vorschriften
- Methoden und Verfahren
  - Risikobeurteilung und –minderung, Risikograph
  - Verteilungsfunktionen, Ausfallraten, Fehlerbeherrschung und Vermeidung, Fehlerentdeckung, Redundanz
  - Strukturierungsmaßnahmen, FMEA, FTA, FMEDA u.a.
  - Unterscheidung Prozess vs. Technik
- Besonderheiten hinsichtlich Hardware und Software (Zuverlässigkeit SW Entwicklungsprozess)

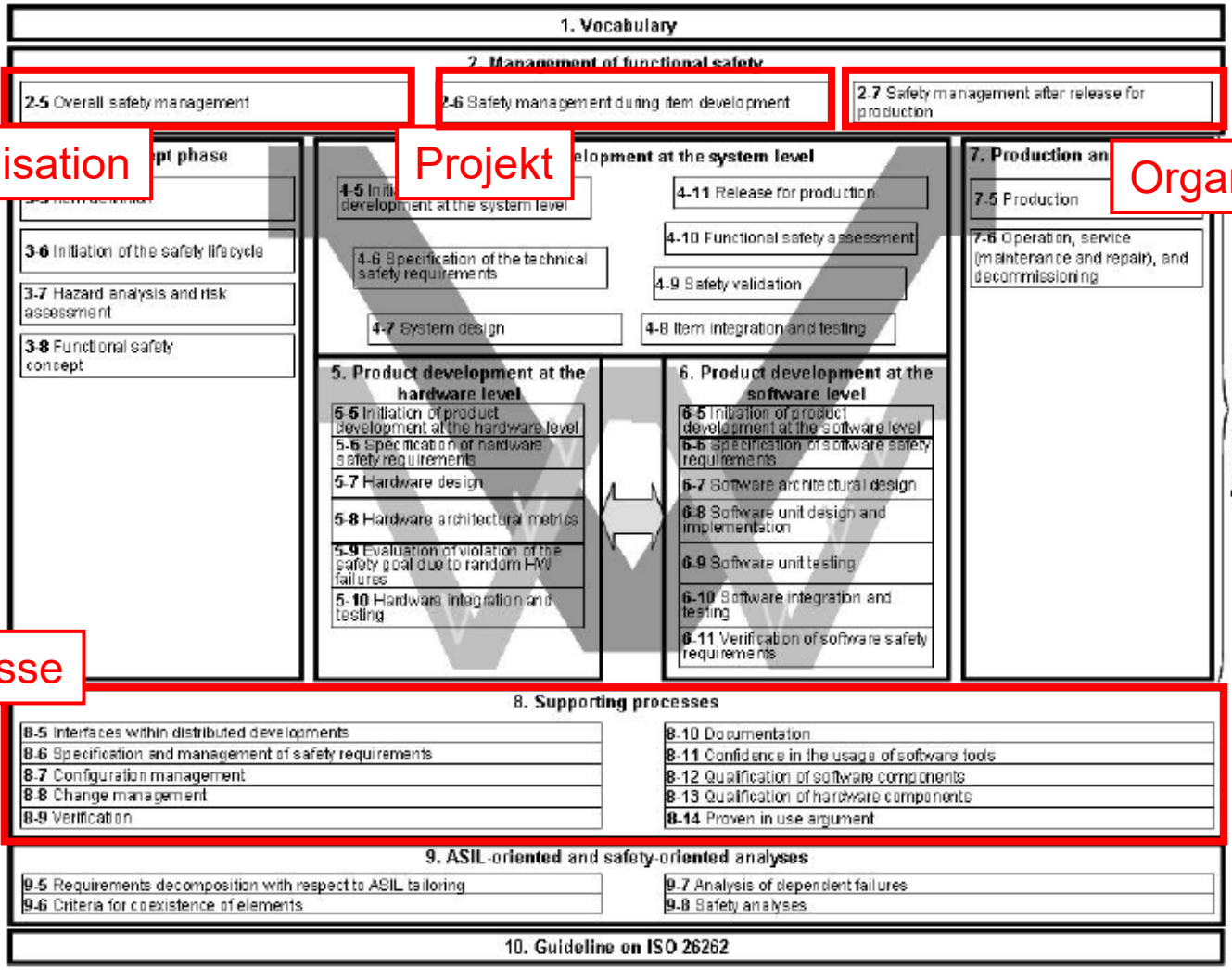
ISO 26262



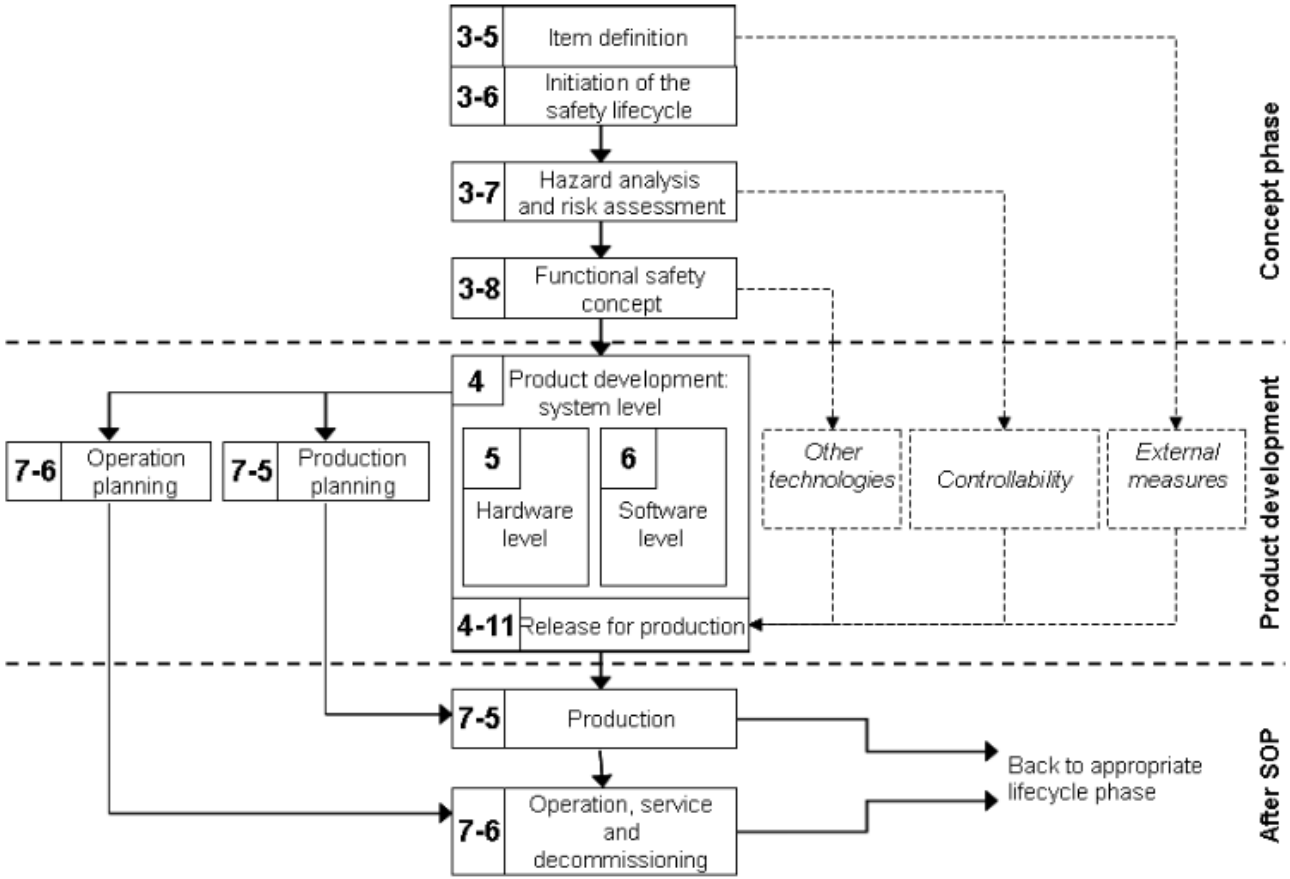


- Norm in der Automobilindustrie, die im November 2011 in Kraft getreten ist
- Vorgängernorm (Basis): IEC 61508
- Einteilung in Sicherheitsstufen QM, ASIL A – D
- Relevant für Autohersteller und Zulieferer weltweit (für Autos < 3,5t)
- Norm ist für elektrische und elektronische Systeme sowie Komponenten anzuwenden, die sicherheitsrelevante Funktionen unterstützen bzw. einen Einfluss darauf haben

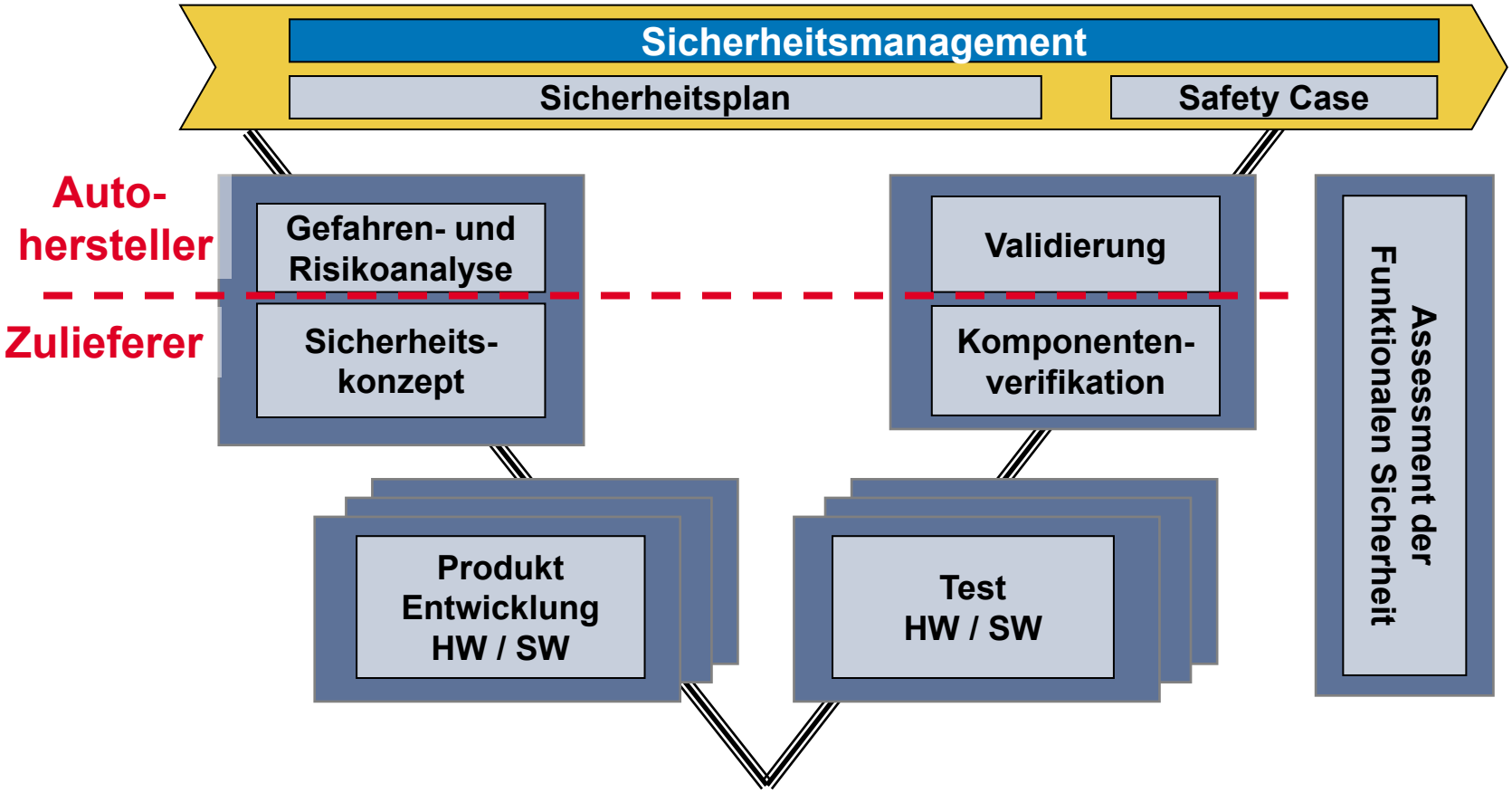
ISO 26262: Überblick



ISO 26262: Sicherheitslebenszyklus



ISO 26262: Verantwortlichkeiten



ISO 26262: Item Definition

- Item beschreiben und definieren
- Abhängigkeiten, Interaktion, Umgebung (Grenzen)
- Funktionalitäten
- Voraussetzung für Durchführung einer Gefahren- und Risikoanalyse (z.B. Festlegung einer Motorsteuerung usw.)

ISO 26262: Gefahren- und Risikoanalyse

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASILA
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASILB	ASIL C
	E4	ASIL B	ASIL C	ASIL D

S: Estimation of potential severity

Class	SO	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life threatening injuries (survival probable)	Life threatening injuries (survival uncertain), fatal injuries

E: Estimation of probability of exposure in driving and operating situation

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability

C: Estimation of controllability

Class	CO	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Sicherheitstechnik
Inhalte

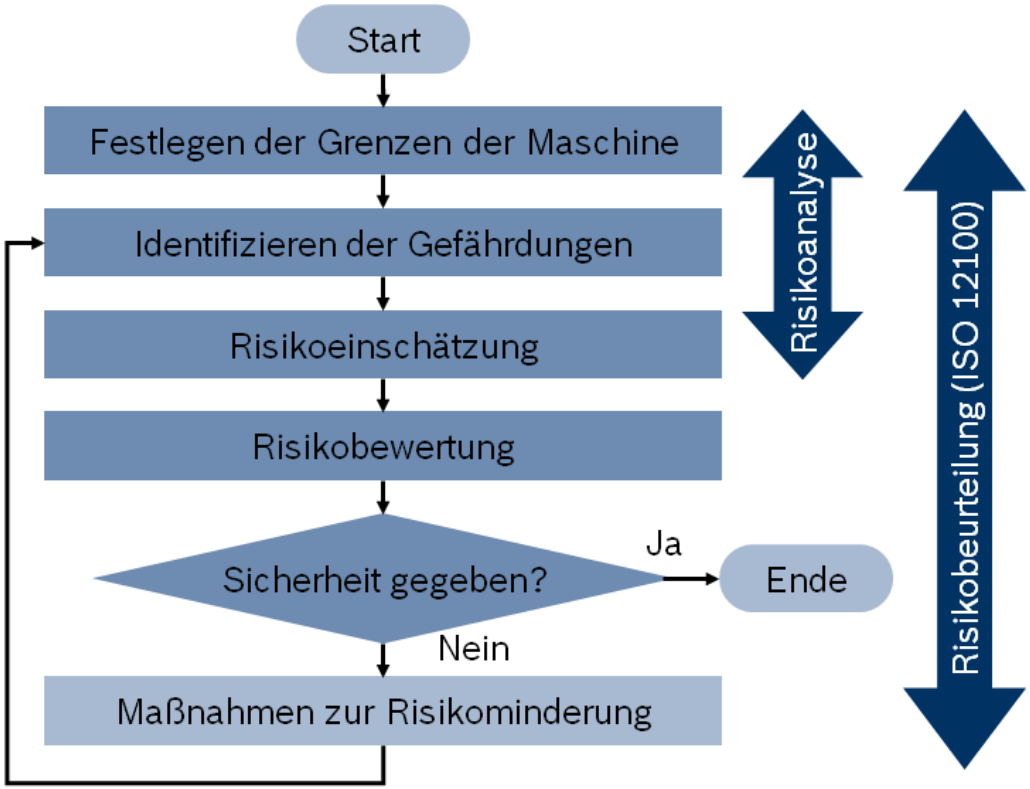
- Definition Sicherheit
- Aktuelle Normen und Vorschriften
- Methoden und Verfahren
  - Risikobeurteilung und –minderung, Risikograph
  - Verteilungsfunktionen, Ausfallraten, Fehlerbeherrschung und Vermeidung, Fehlerentdeckung, Redundanz
  - Strukturierungsmaßnahmen, FMEA, FTA, FMEDA u.a.
  - Unterscheidung Prozess vs. Technik
- Besonderheiten hinsichtlich Hardware und Software (Zuverlässigkeit SW Entwicklungsprozess)

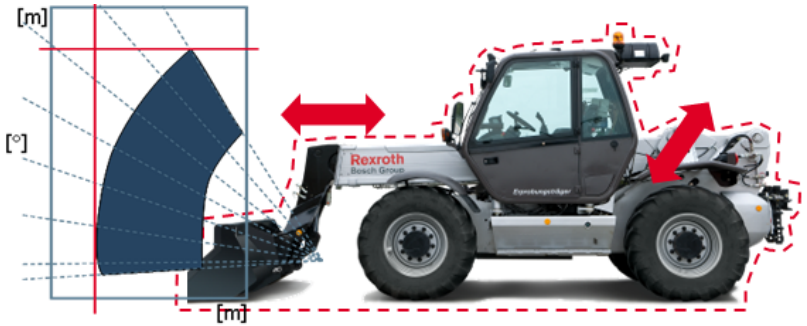
Beispiel

1. **Risikobeurteilung und –minderung**
2. Identifikation der Sicherheitsfunktionen
3. Bestimmen des PL_r
4. Auswahl der Systemarchitektur
5. Modellieren des Systems als Blockdiagramm
6. Fehler und Diagnose
7. Bestimmen des PL
8. Bewerten der Robustheit der Steuerung - Fehlervermeidung
9. Software-Anforderungen
10. Verifizieren und Validieren

Quelle: Nach [4]

Beispiel





DEUTSCHE NORM Juni 2012

DIN EN 1459 DIN

ICS 53.060 Ersatz für DIN EN 1459:2010-05

Sicherheit von Flurförderzeugen – Kraftbetriebene Stapler mit veränderlicher Reichweite; Deutsche Fassung EN 1459:1998+A3:2012

Safety of industrial trucks –

- Gibt es eine **C-Norm** für die Maschine? Diese als Vorlage nutzen.
- Beispiel: Schwere Verletzung durch unerwartete teleskopische Bewegung

Quelle: Nach [4]