Institut für Fahrzeugtechnik und Mobilität

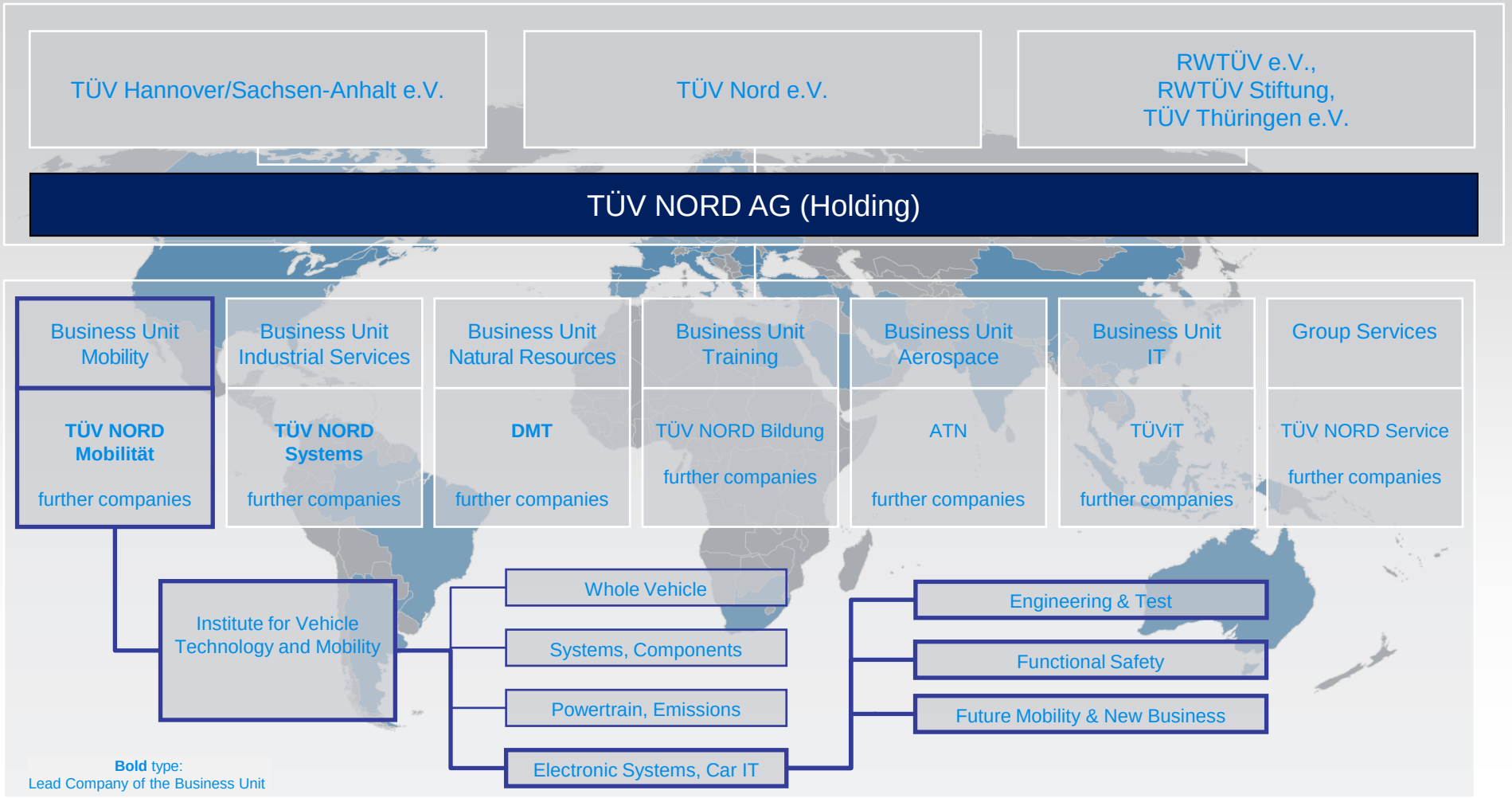
Fachtagung Homologation und Technik, 15.02.2017

Funktionale Sicherheit (ISO 25119) vs. Maschinensicherheit (ISO 12100) – Gegensätze oder Erweiterung?

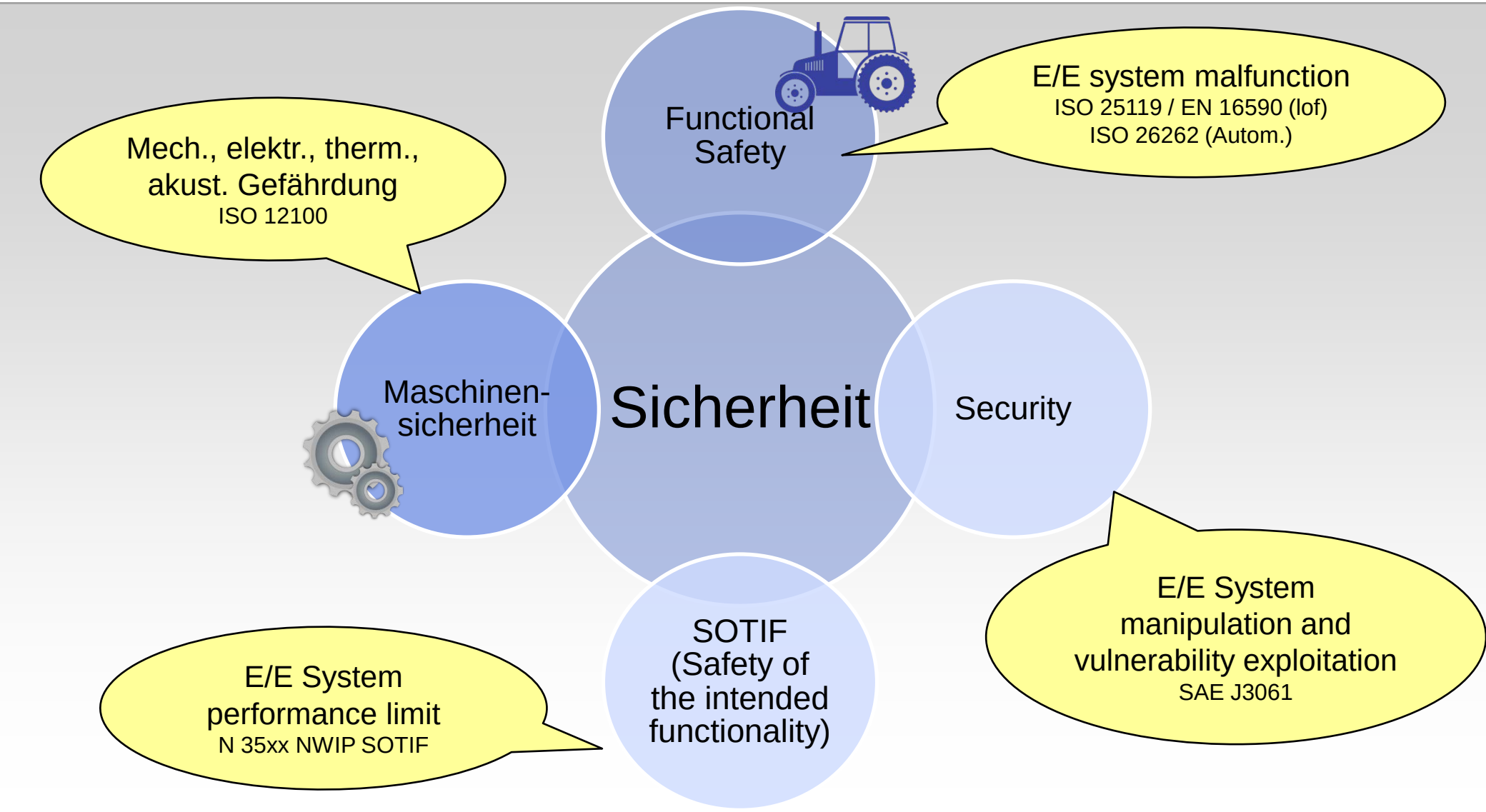
Referent: Dr. Thomas Wenzel

TÜV NORD GROUP
Structure

TÜV NORD operates in more than 70 countries throughout the world.



Grundlagen der funktionalen Sicherheit
(Functional) Safety vs. Machinensicherheit vs. Security vs. SOTIF



Grundlagen der funktionalen Sicherheit

- Sicherstellung, dass ein sicherheitskritisches System* sicher funktioniert
- Überführung des Systems in einen sicheren Zustand falls die sichere Funktionsweise nicht mehr gewährleistet werden kann.

Unterschiedliche Systeme haben unterschiedliche sichere Zustände

Bröckel-Reaktor -Tihange 2
WDR/AFP/Eric Lalmand

- Funktionale Sicherheit unterstützt / beeinflusst:
  - Zuverlässigkeit
  - Verfügbarkeit
  - Wartbarkeit

* sicherheitskritisches System : System, welches im Fehlerfall Menschen töten oder verletzten kann.

Grundlagen der funktionalen Sicherheit
Definition der Funktionalen Sicherheit (ISO 25119 / DIN EN 16590)

Funktionale Sicherheit - Ein System, das auf eine Weise funktioniert, welche kein unangemessen hohes Verletzungsrisiko eines Bedieners oder Umstehenden darstellt. (ISO 25119 / EN 16590)

Eine Einheit (Item) oder Subsystem einer Einheit, welches im Fall einer Fehlfunktion in der Lage ist

- Menschen zu verletzen oder
- (Schäden an der Umwelt anzurichten)[1]

kann als sicherheitsbezogenes System definiert werden.

Sicherheitsbezogene Systeme haben ein hohes Potential an unangemessenem Risiko, welches vermieden oder abgeschwächt werden muss.

[1] Nicht im Hauptfokus der ISO 25119

Vergleich ISO 12100 und ISO 25119 / DIN EN 16590
Anwendungsbereich

DIN EN ISO 12100

- „Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung“
- Anwendungsbereich:
  - Maschinen
- Anwendungstechnologie
  - Gesamte Maschine
    - Betriebsteil
    - Steuerungssystem

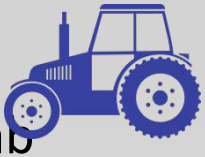
ISO 25119 / DIN EN 16590

- Traktoren und Maschinen für die Land- und Forstwirtschaft — Sicherheitsbezogene Teile von Steuerungen
- Anwendungsbereich:
  - Traktoren
  - etc.
- Anwendungstechnologie
  - SRP/CS

Vergleich ISO 12100 und ISO 25119 / DIN EN 16590
Lebenszyklus

DIN EN ISO 12100

- Risikobetrachtung berücksichtigt kompletten Lebenszyklus
- Prozess in der Norm bildet Lebenszyklus nicht vollständig ab



ISO 25119 / DIN EN 16590

- Deckt Lebenszyklus vollständig ab
- setzt Anwendung der ISO 12100 zur Risikoidentifizierung voraus

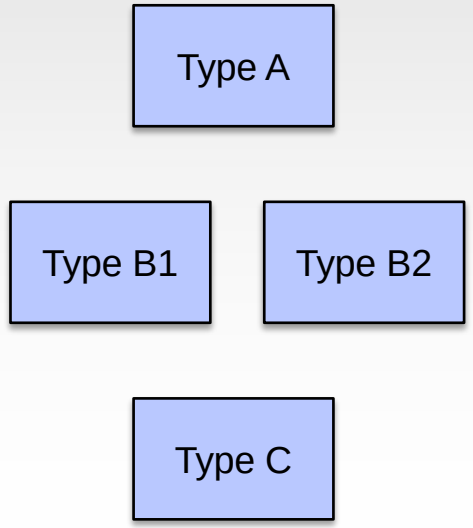
Vergleich ISO 12100 und ISO 25119 / DIN EN 16590
Verbindlichkeit

DIN EN ISO 12100

- Typ A Norm
- Gelistet in Maschinenrichtlinie
- Verweist als Rahmennorm auf spezialisiertere Normen

ISO 25119 / DIN EN 16590

- Optional (ISO 25119 Ed. 1)
- Typ B1 Norm (EN 16590)



Strukturübersicht von Sicherheitsnormen

a) Typ A-Normen (Grundnormen)

enthalten Grundbegriffe, Gestaltungsleitsätze und allgemeine Aspekte, die für alle Maschinen angewandt werden können;

b) Typ B-Normen (Fachgrundnormen)

behandeln einen oder mehrere Sicherheitsaspekte oder eine oder mehrere Arten von Schutzeinrichtungen, die bei einer Reihe von Maschinen angewendet werden können;

Typ B1-Normen behandeln bestimmte Sicherheitsaspekte (z. B. Sicherheitsabstände, Oberflächentemperatur, Geräusch);

Typ B2-Normen behandeln Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungen, Kontaktmatten, trennende Schutzeinrichtungen);

c) Typ C-Normen (Maschinensicherheitsnormen)

behandeln detaillierte Sicherheitsanforderungen für eine bestimmte Maschine oder Gruppe von Maschinen.

Vergleich ISO 12100 und ISO 25119 / DIN EN 16590
Methode - allgemein

DIN EN ISO 12100

- Ziel: Definition von Sicherheitsmaßnahmen, bis ausreichende Sicherheitsminimierung erreicht
- Risikobeurteilung
- 3-Stufen Modell
- Sicherheitsmaßnahmen Produktbezogen (Ausnahme: Anforderungen an Benutzer)

ISO 25119 / DIN EN 16590

- Ziel: Eigensicherheit der sicherheitsrelevanten Funktion
- Risikoanalyse ermittelt Sicherheitsziele und AgPL
- Maßnahmen basierend auf AgPL
  - Prozessanforderungen
  - Produktanforderungen
  - Managementanforderungen

Vergleich ISO 12100 und ISO 25119 / DIN EN 16590
Methode - Konzept

DIN EN ISO 12100:2010

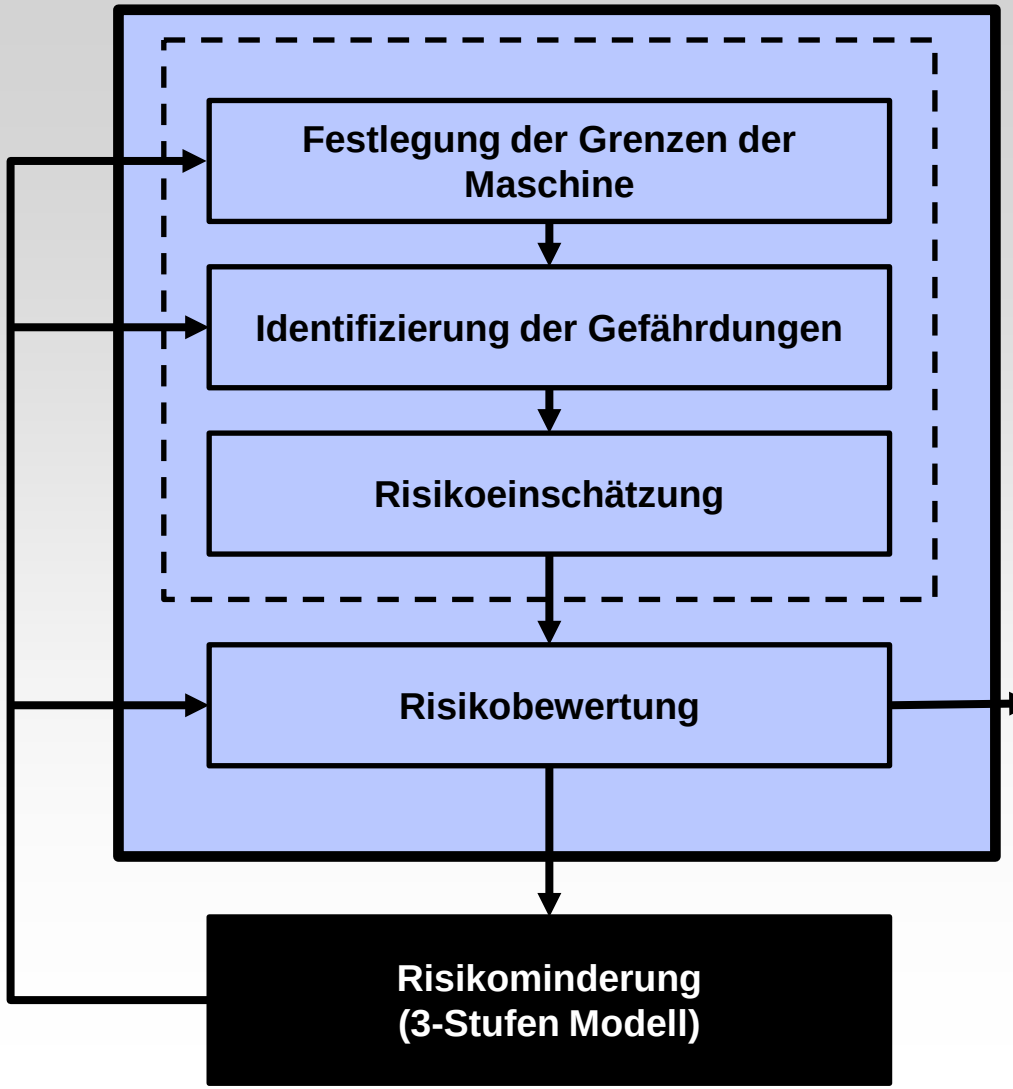
- Risikobeurteilung
  - Risikoanalyse
  - Risikobewertung
- Kein Maß für die Kritikalität (SIL, PL, AgPL, …)
- Spezifischere Normen für bestimmte Teile der Maschine (z.B. Kontrollsystem/IEC 61508/ISO 13849) können eine Bewertung in Form eines SIL oder PL erforderlich machen.

ISO 25119 / DIN EN 16590

- Risikoanalyse führt zu
  - AgPL
  - Systemdesign
  - funktionalem Sicherheitskonzept
- Kritikalität: AgPL
- Top-Down-Prinzip
- Validation der Sicherheit am Ende des Konstruktionsprozesses (V-Modell)

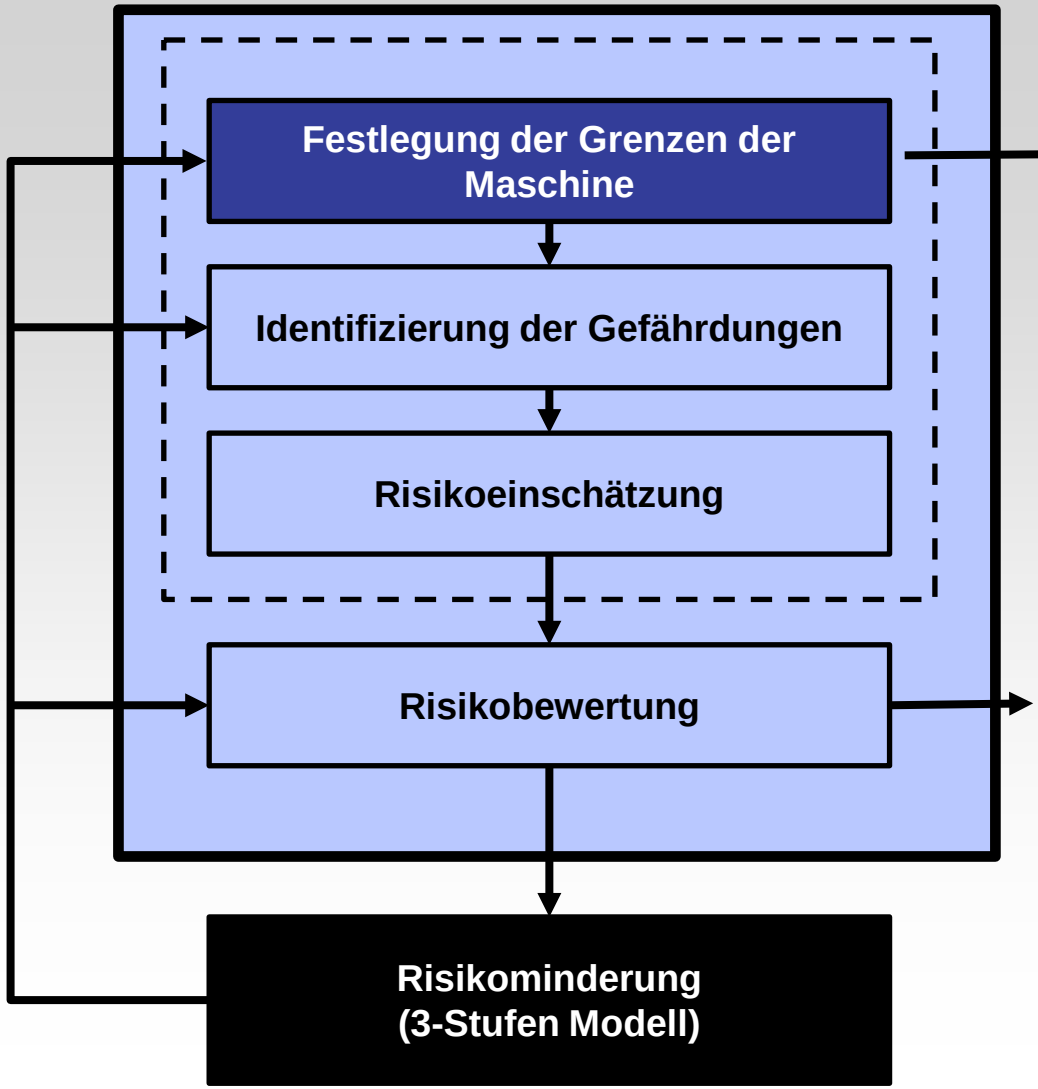
Vorstellung
DIN EN ISO 12100

Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 - Risikobeurteilung



Abbruch, falls Risiko ausreichend vermindert

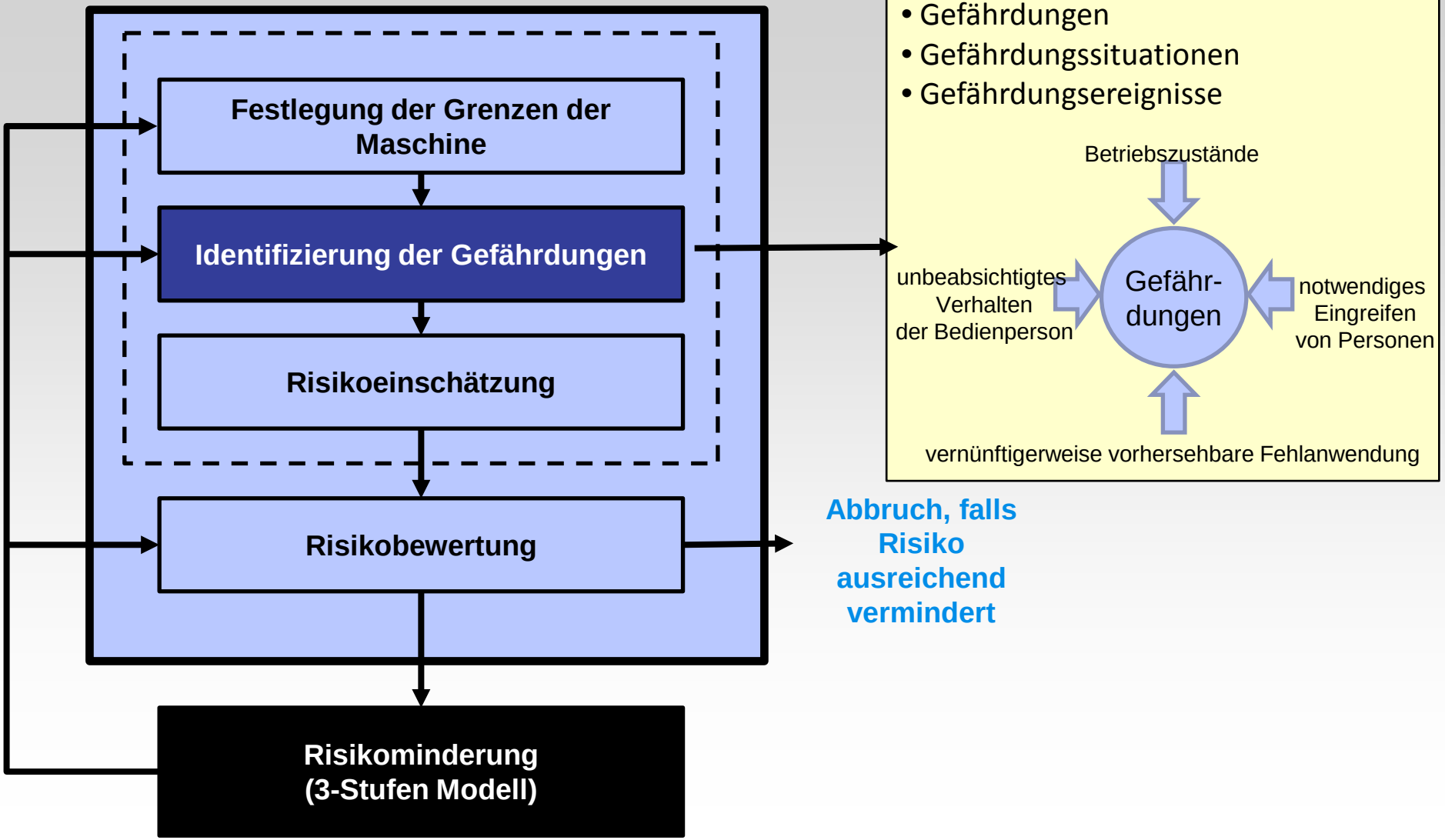
Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 - Risikobeurteilung



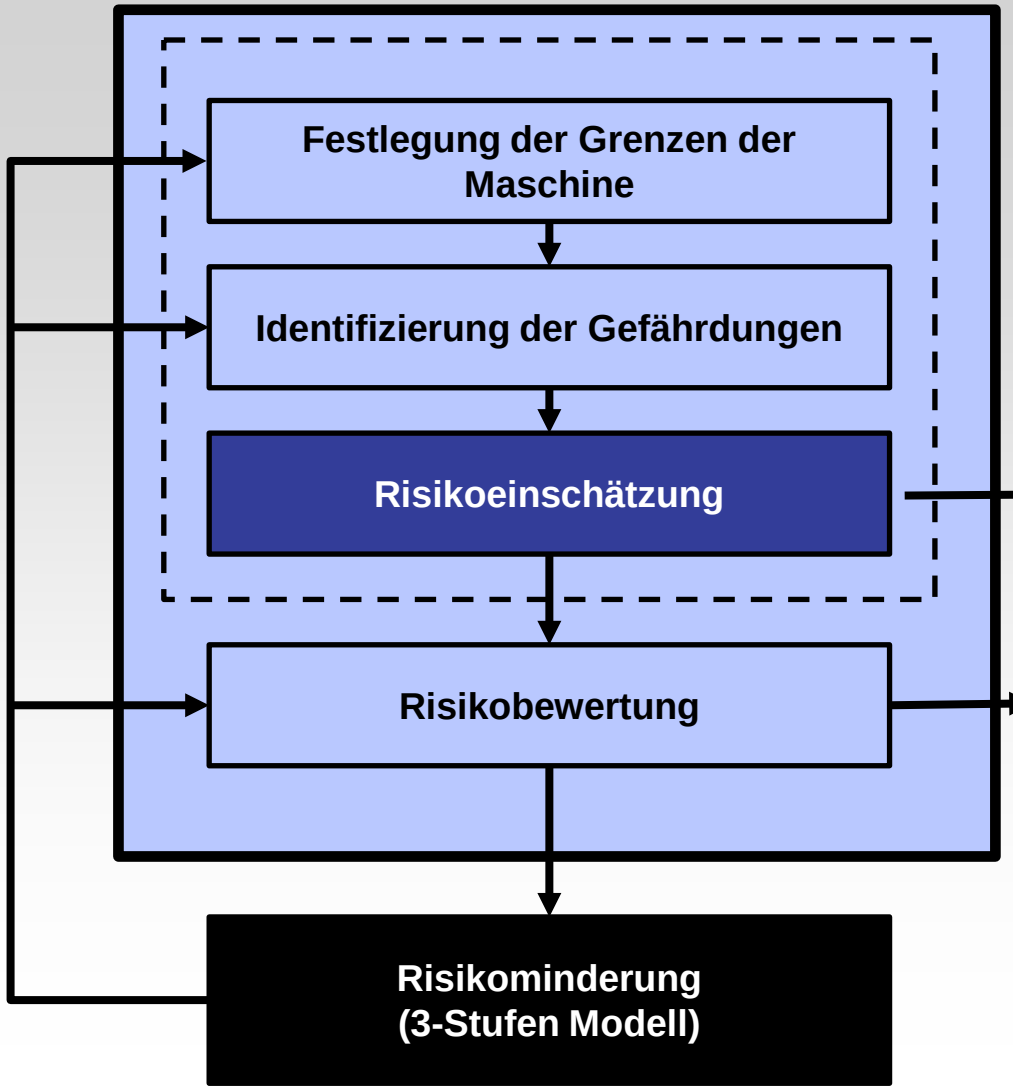
- räumliche Grenzen
- zeitliche Grenzen
- gesamter Lebenszyklus
- Verwendungsgrenzen:
  - Betriebsarten,
  - Einsatzbereich,
  - Ausbildung, …

Abbruch, falls Risiko ausreichend vermindert

Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 - Risikobeurteilung



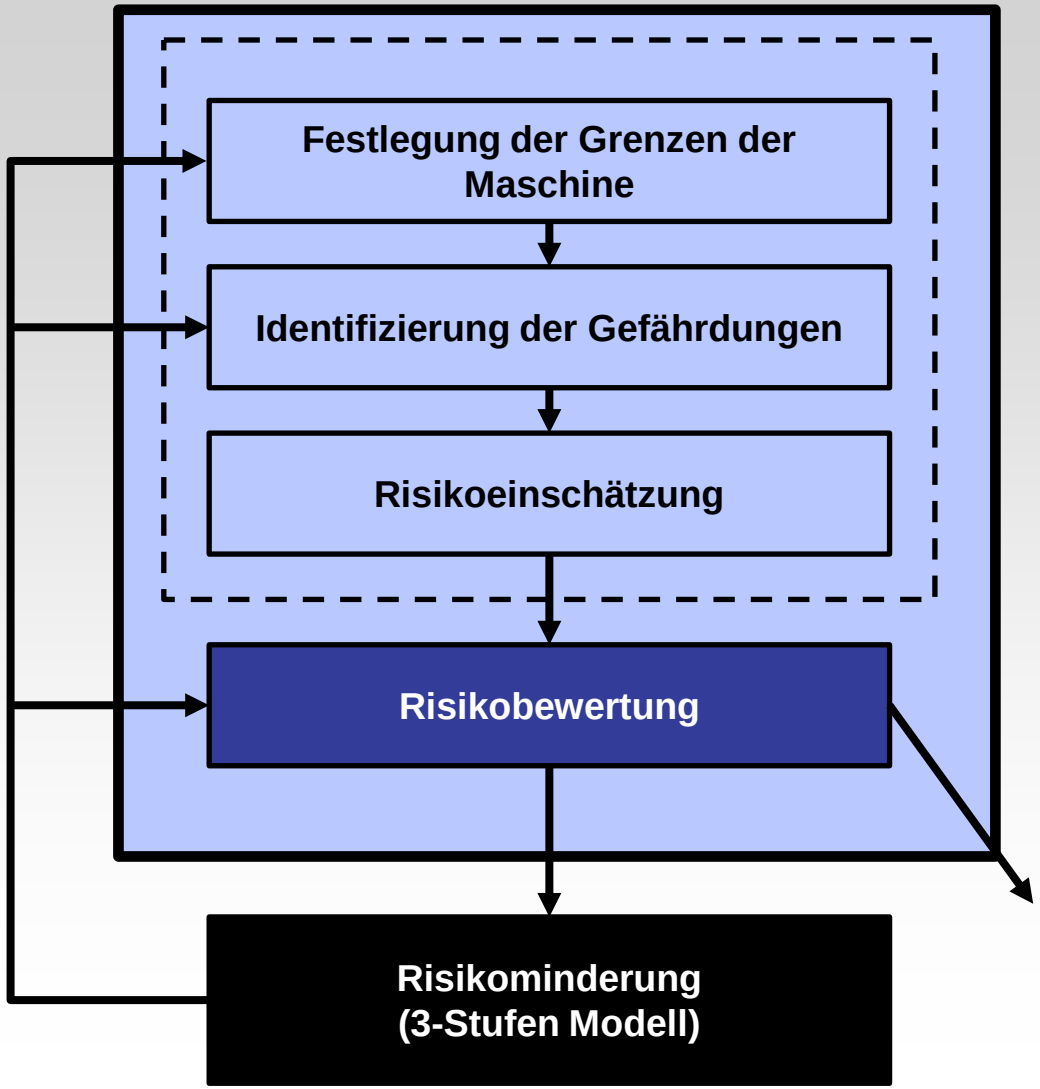
Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 - Risikobeurteilung



- Risiko, Funktion aus
  - Schadensausmaß und
  - Eintrittswahrscheinlichkeit
    - Gefährdungsexposition
    - Eintritt des Gefährdungsereignisses
    - Möglichkeiten zur Vermeidung oder Begrenzung des Schadens

Abbruch, falls Risiko ausreichend vermindert

Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 - Risikobeurteilung



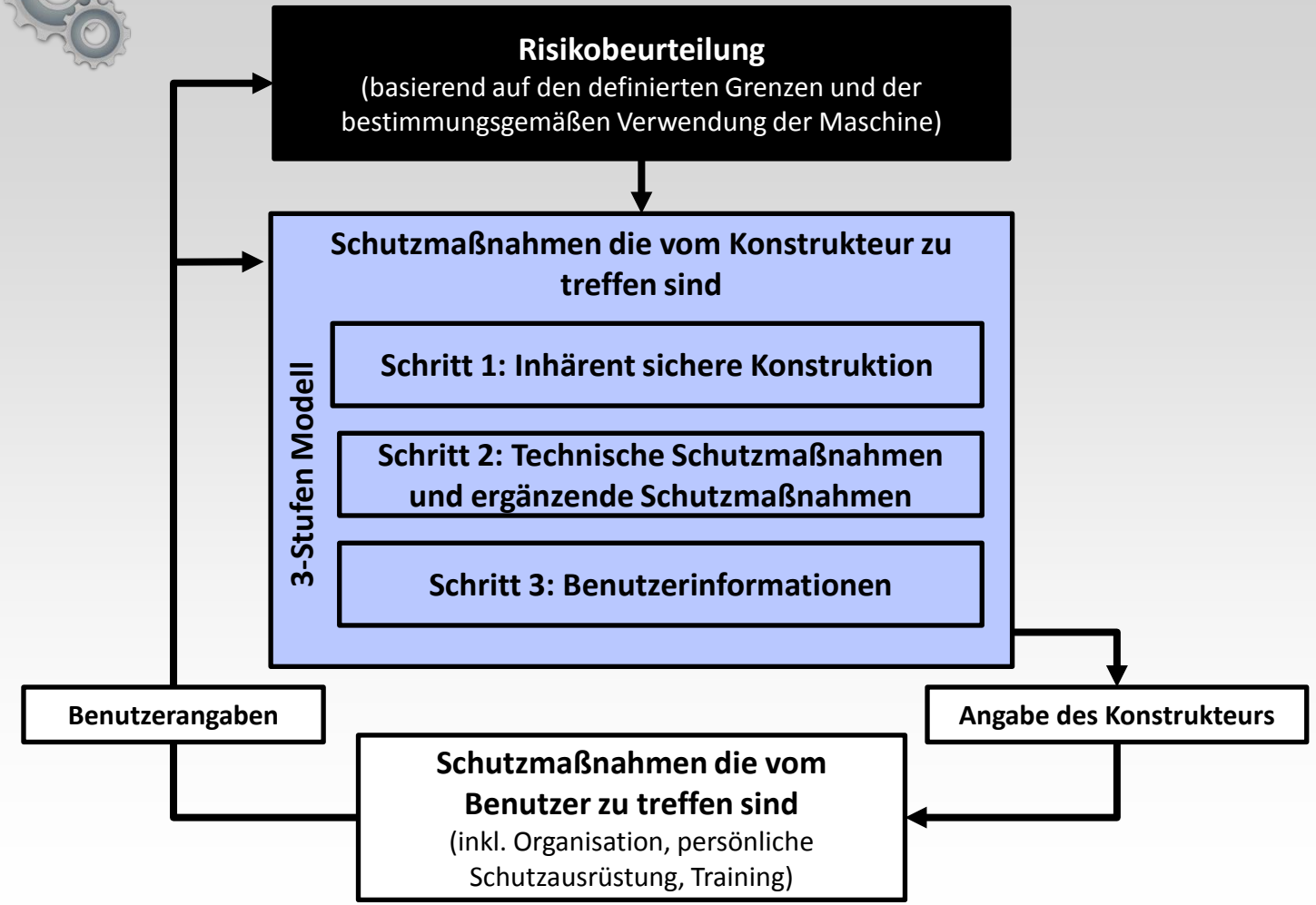
Kriterien zur Erreichung einer hinreichende Risikominderung

- alle Betriebsbedingungen berücksichtigt
- alle Risiken vermindert, soweit praktisch umsetzbar
- neue Gefährdungen berücksichtigt
- Benutzerinfo über Restrisiken
- durchgeführte Schutzmaßnahmen miteinander vereinbar
- Folgen durch Gebrauch ausreichend berücksichtigt
- Schutzmaßnahmen beeinflussen die Arbeitsbedingungen nicht negativ

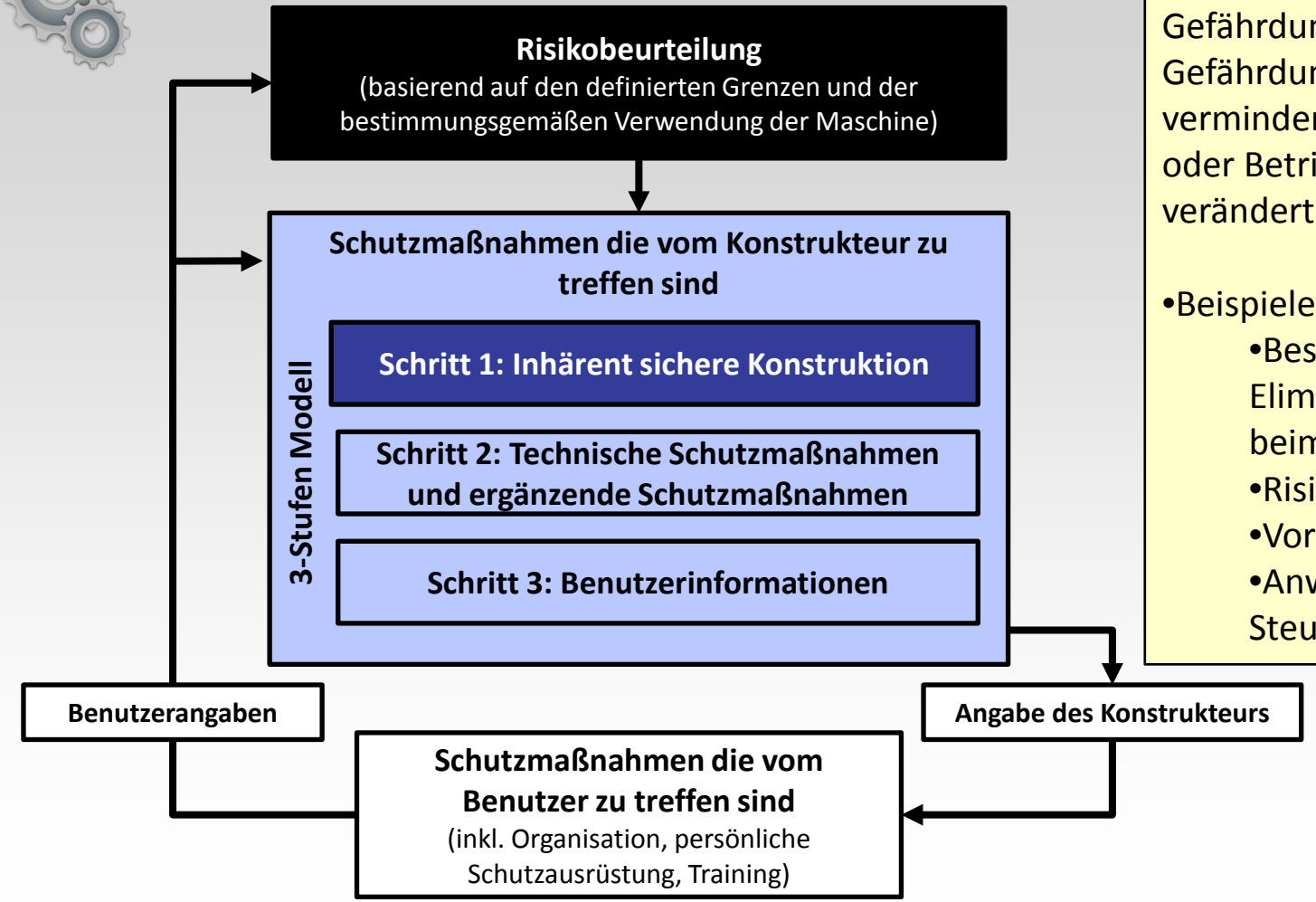
Risikovergleich

Abbruch, falls Risiko ausreichend vermindert

Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 – Risikominderung – 3-Stufen Modell



Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 – Risikominderung – 3-Stufen Modell



- Schutzmaßnahme, die entweder Gefährdungen beseitigt oder die mit den Gefährdungen verbundenen Risiken vermindert, indem [...] die Konstruktions- oder Betriebseigenschaften der Maschine verändert werden

- Beispiele
  - Beseitigung von Gefährdungen: Eliminierung von scharfen Kanten beim Design
  - Risikominderung:
  - Vorrichtungen für Standsicherheit
  - Anwendung der ISO 13849 für Steuerungen

Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 – Risikominderung – 3-Stufen Modell

Risikobeurteilung
(basierend auf den definierten Grenzen und der bestimmungsgemäßen Verwendung der Maschine)

Schutzmaßnahmen die vom Konstrukteur zu treffen sind

3-Stufen Modell

- **Schritt 1: Inhärent sichere Konstruktion**
- **Schritt 2: Technische Schutzmaßnahmen und ergänzende Schutzmaßnahmen**
- **Schritt 3: Benutzerinformationen**

Benutzerangaben

Angabe des Konstrukteurs

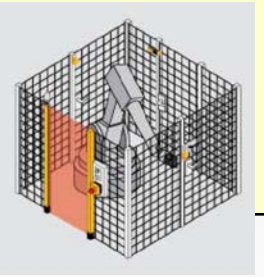
Schutzmaßnahmen die vom Benutzer zu treffen sind
(inkl. Organisation, persönliche Schutzausrüstung, Training)

Trennende Schutzeinrichtung

•Ein Maschinenteil, das Schutz mittels einer physischen Barriere bietet

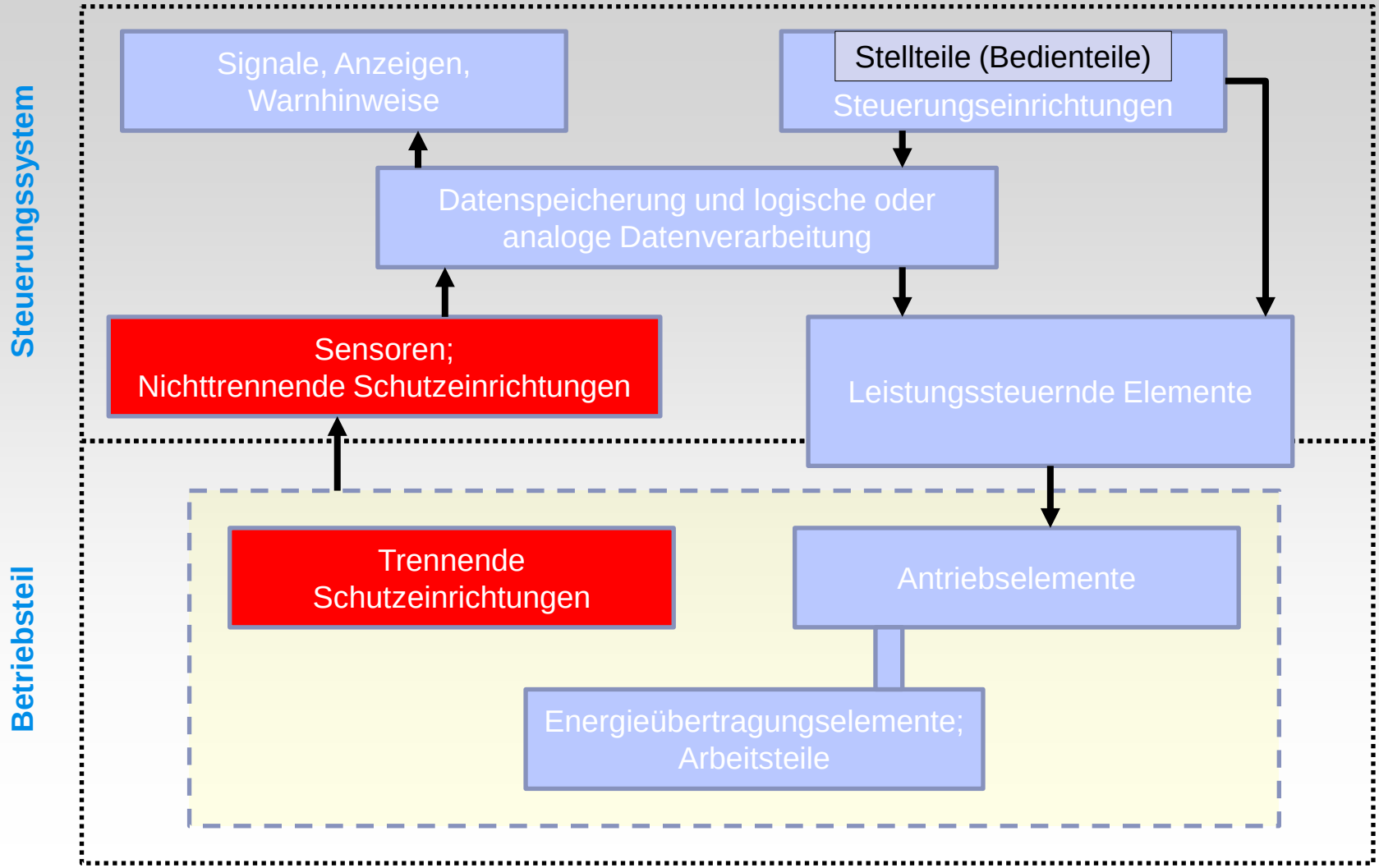
Nichttrennende Schutzeinrichtung

•Eine Einrichtung ohne trennende Funktion, die allein oder in Verbindung mit einer trennenden Schutzeinrichtung das Risiko vermindert (Maschinenrichtlinie 2006/42/EG)



Risikominderung II:

Technische und/oder ergänzende Schutzmaßnahme



Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 – Risikominderung – 3-Stufen Modell

Risikobeurteilung
(basierend auf den definierten Grenzen und der bestimmungsgemäßen Verwendung der Maschine)

Schutzmaßnahmen die vom Konstrukteur zu treffen sind

3-Stufen Modell

- **Schritt 1: Inhärent sichere Konstruktion**
- **Schritt 2: Technische Schutzmaßnahmen und ergänzende Schutzmaßnahmen**
- **Schritt 3: Benutzerinformationen**

Benutzerangaben

Angabe des Konstrukteurs

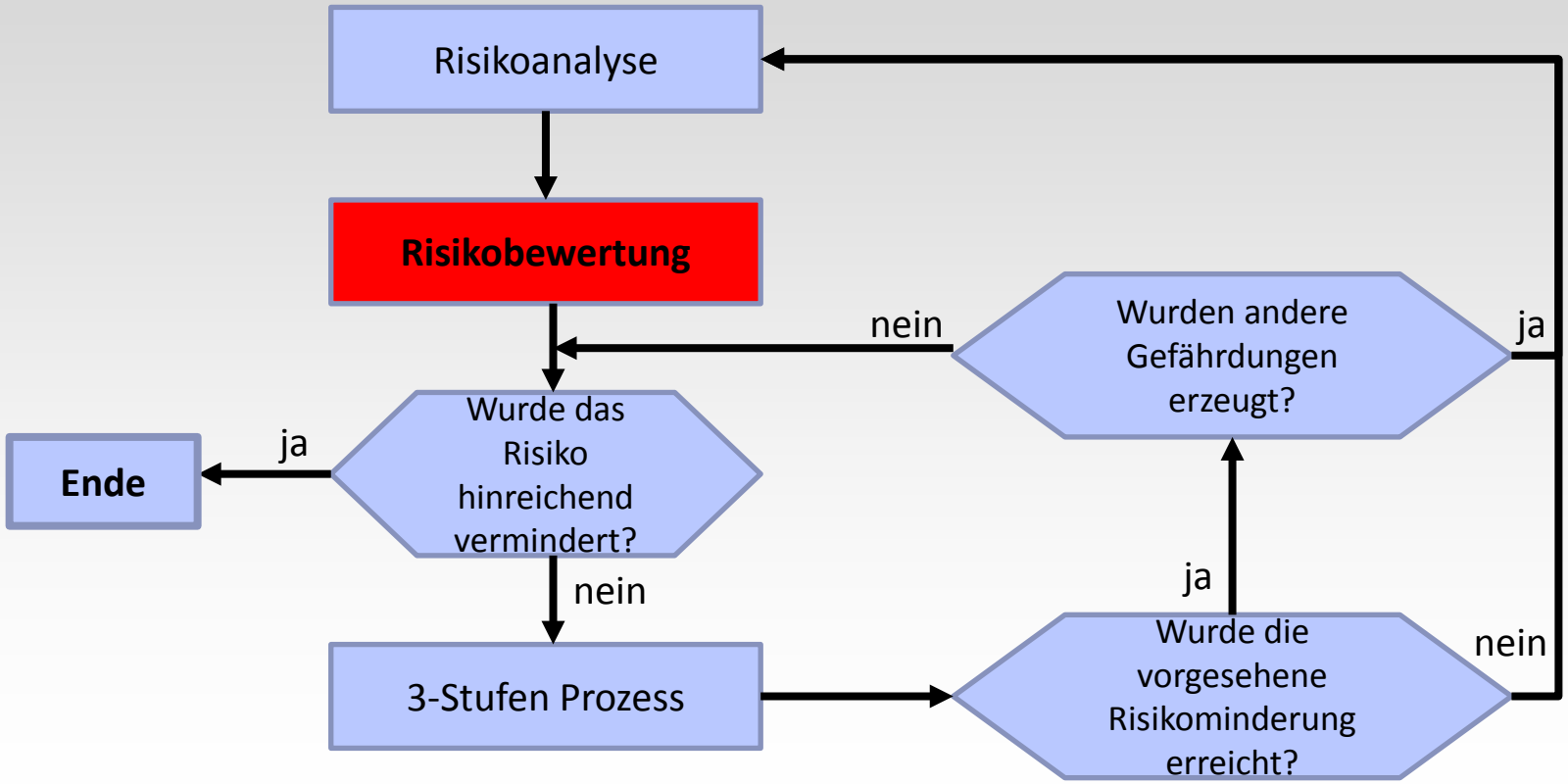
Schutzmaßnahmen die vom Benutzer zu treffen sind
(inkl. Organisation, persönliche Schutzausrüstung, Training)

- Benutzerhandbuch

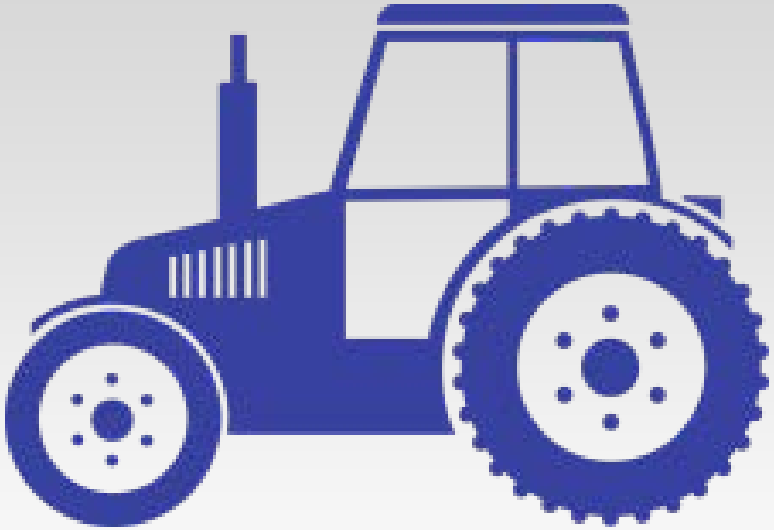
- Piktogramme

Methode: Definition von Sicherheitsmaßnahmen
ISO 12100 – Risikobewertung

„auf der Risikoanalyse beruhende Beurteilung, ob die Ziele zur Risikominderung erreicht wurden“



Vorstellung
ISO 25119 / DIN EN 16590



Funktionale Sicherheit - Konzepte und neue Basisansätze
ISO 25119 - Klassifikation und Reduzierung von Risiken (tech. Ansatz)

Systemrisiko

Risiko-freiheit

Vertretbares Risiko (gesellschaftlich akzeptiert)
Hinweis: kann schwanken

Gesellschaftlich akzeptiertes Restrisiko

Mindestens benötigte Risikoreduzierung um vertretbare Akzeptanz zu erreichen

Weitere Technologien für sicherheitsrelevante Systeme z.B. mechanisches Design oder Komponentensicherheit	Elektrische / elektronische sicherheitsrelevante Systeme, z. B. Überwachungssystem	Externe Maßnahmen zur Risikominimierung z. B. Gesetze, Richtlinien, Maßnahmen

Angewandte Maßnahmen zur Risikoreduzierung

Restrisiko | Sicherheitsmarge

Virtuelles Beispiel:
Elektrisches Bremssystem

Ein fehlerbedingter Bremseingriff mit maximaler Bremskraft führt zum ….

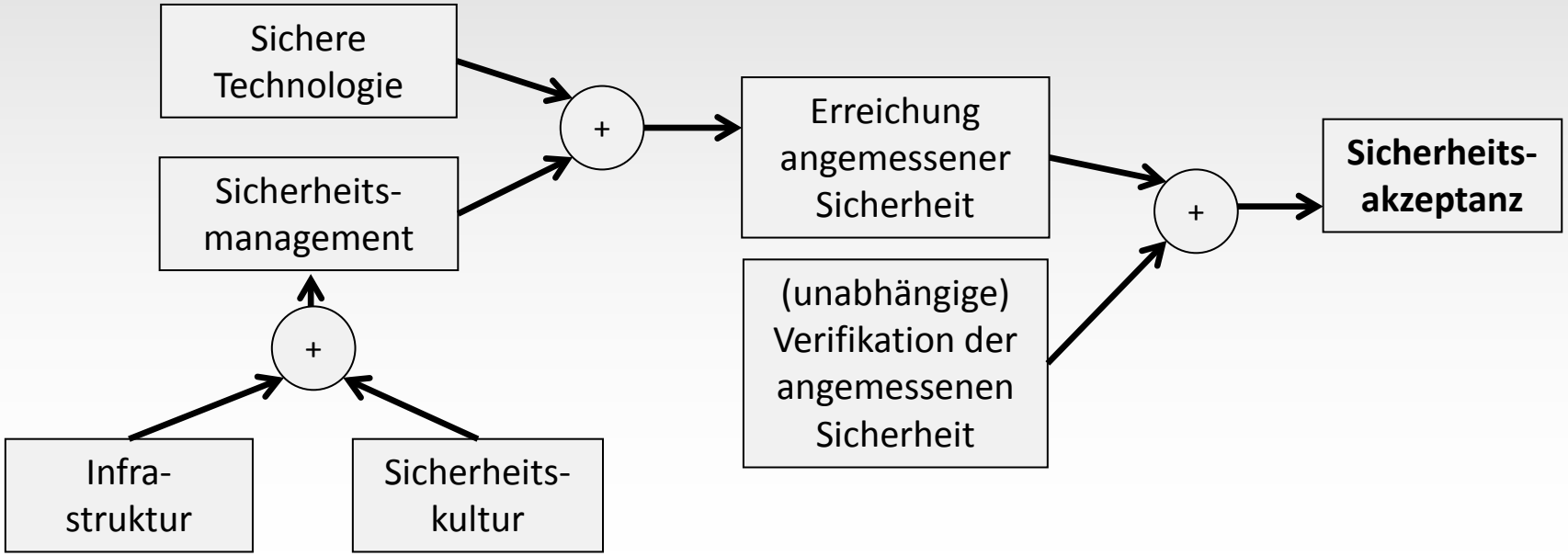
… Verlust der Fahrzeugkontrolle mit Unfallfolge.

Frage:
Würden Sie Fehler in Ihrer Bremsanlage akzeptieren?

Funktionale Sicherheit - Konzepte und neue Basisansätze
ISO 25119 - Basiskonzept – Fokus auf dem Sicherheitsmanagement

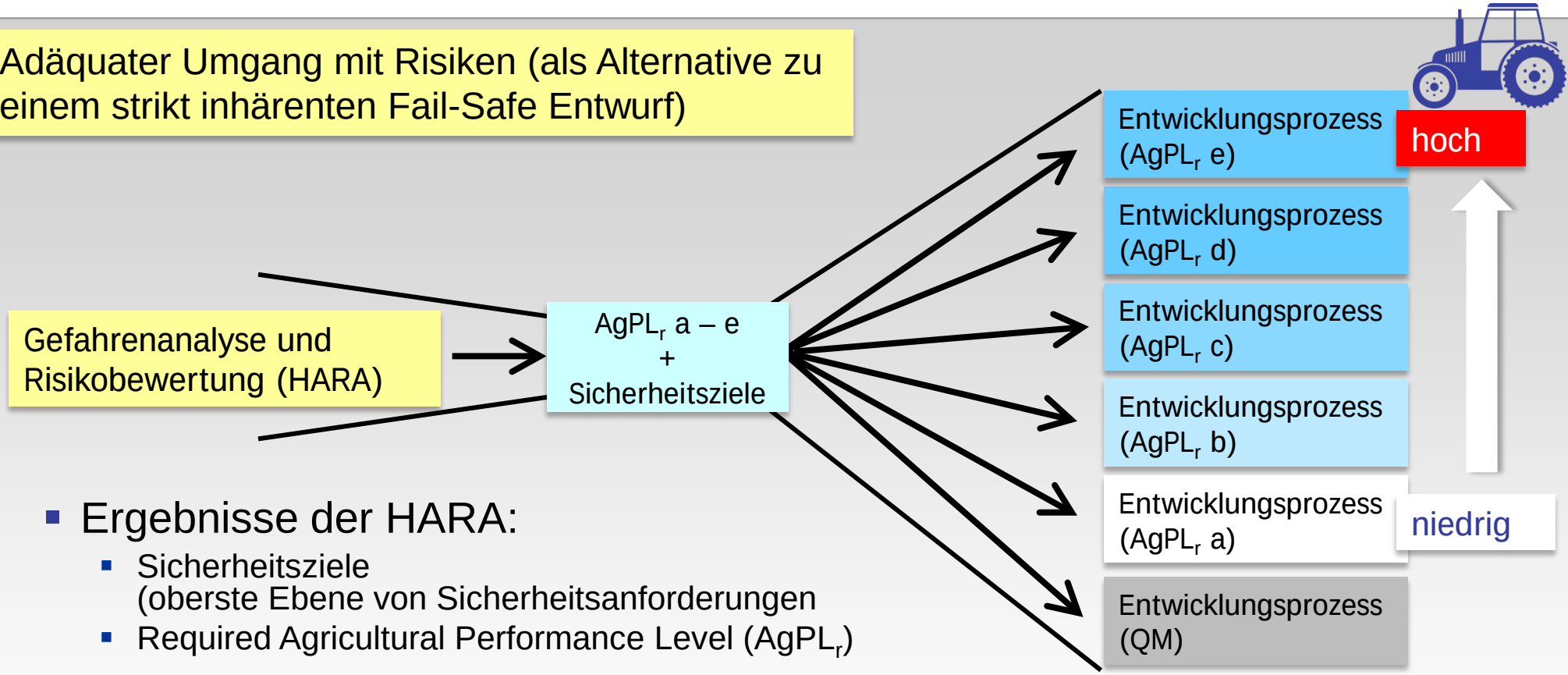
Falsche Annahme:
"Sicherheit ist eine Frage der Technologie!"

Realität:
Je größer die Komplexität eines technischen Systems, umso strenger sind die Anforderungen an das Management!



ISO 25119 - Grundkonzept – Agricultural Performance Level

Adäquater Umgang mit Risiken (als Alternative zu einem strikt inhärenten Fail-Safe Entwurf)



- Ergebnisse der HARA:
  - Sicherheitsziele
    (oberste Ebene von Sicherheitsanforderungen
  - Required Agricultural Performance Level (AgPL$_r$)
- Übereinstimmung zu den Sicherheitsanforderungen zeigen (AgPL$_r$ bezogen) durch angemessene:
  - Prozesse
  - Architektur
  - Entwurf, …

ISO 25119 definiert entsprechende Maßnahmen um eine ausreichende Funktionale Sicherheit zu erreichen

ISO 25119 - Systementwurf

Vorgesehene Architekturen
B, 1, 2, 3, 4

Von einkanalig über einkanalig mit Überwachung bis zu komplett redundant zweikanalig

Kategorie

Diagnosedeckungsgrad
(Diagnostic Coverage)

Niedrig	DC < 60%
Mittel	60% ≤ DC < 90%
Hoch	90% ≤ DC

$MTTF_d$

$AgPL_r$

DC

Mittlere Zeit bis zum gefährlichen Ausfall (Mean Time to dangerous failure)

Kurz	3 Jahre <	$MTTF_d$ < 10 Jahre
Mittel	10 Jahre <	$MTTF_d$ < 30 Jahre
Hoch	30 Jahre <	$MTTF_d$

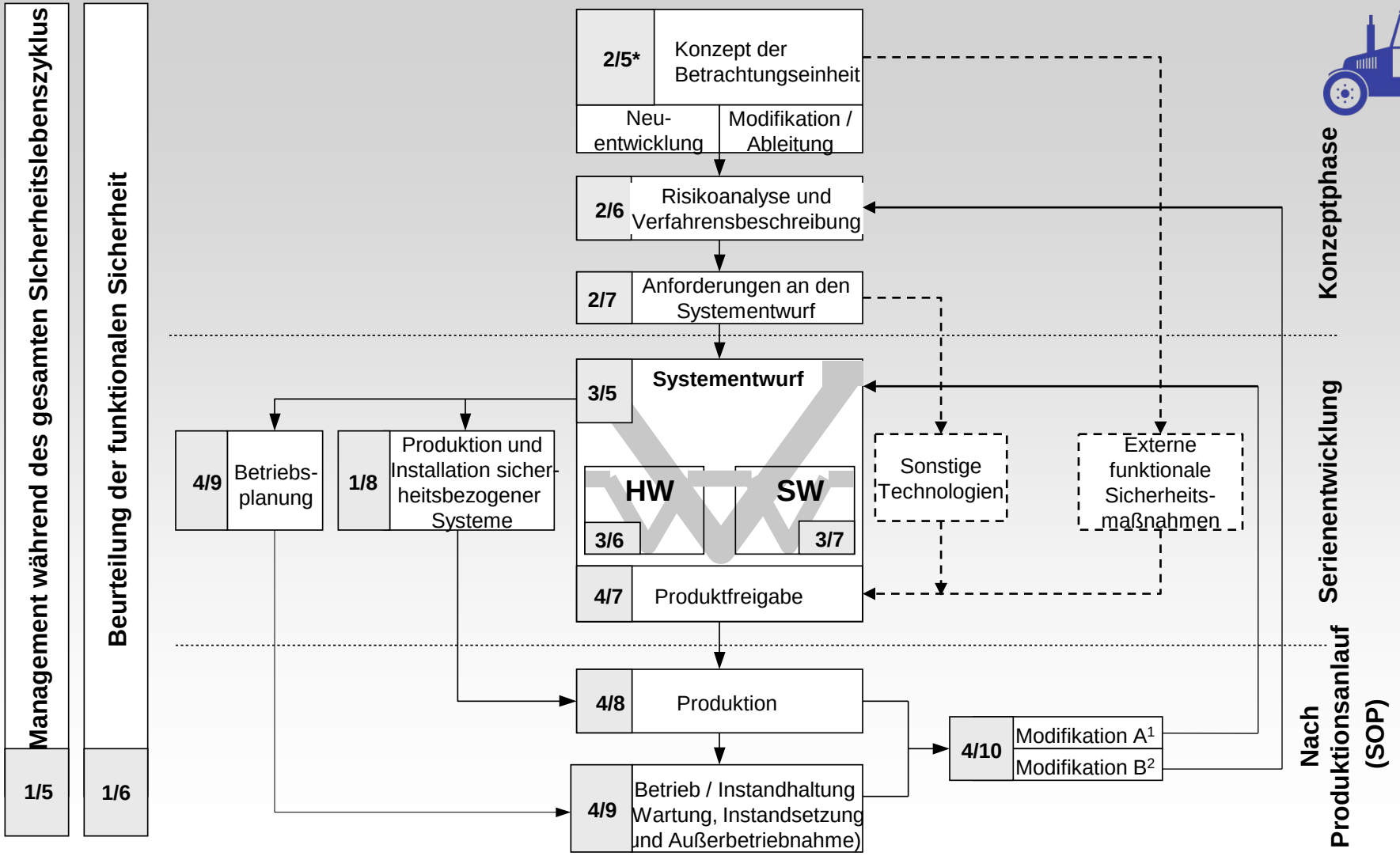
SRL

Anforderungsniveau an die Software
(Software Requirement Level)
B, 1, 2, 3

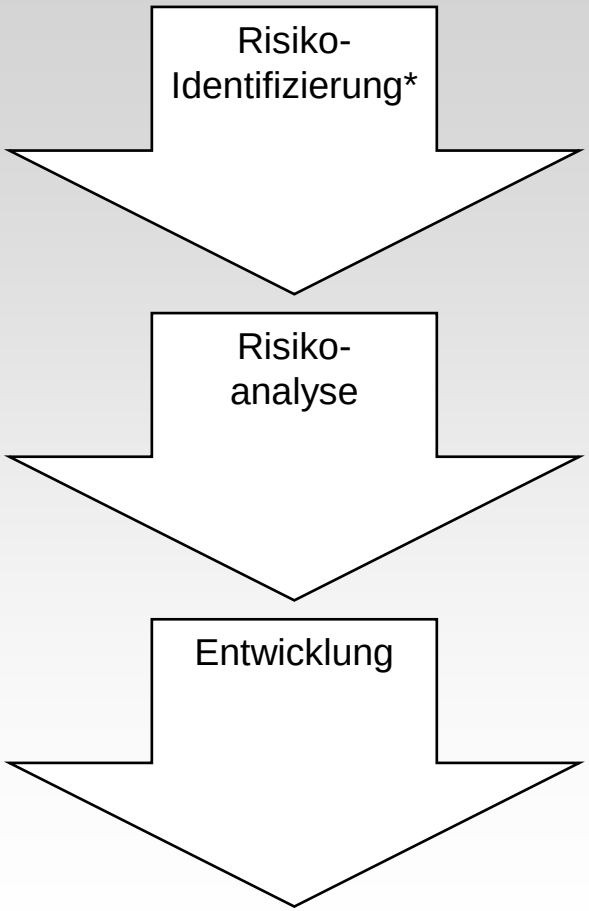
Methode: Eigensichere Konstruktion
ISO 25119 / DIN EN 16590

- Zerlegung des AgPLr in Faktoren MTTFd, Cat, DC, SRL und CCF.
  - Definition von Sicherheitsanforderungen an sicherheitsrelevante Funktion (funktionales/ technisches Sicherheitskonzept)
  - Sicherheitsanforderungen an HW und SW (Verfeinerung)
- zusätzlich Prozess- und methodische Anforderungen vor allem an die Entwicklung von SW
  - Verifikation/Validation
  - Unterstützung der funktionalen Sicherheit durch Managementanforderungen

Konzept des Sicherheitslebenszyklus
ISO 25119 / DIN EN 16590



Anwendung in der Praxis
Kombination der einzelnen Sicherheitsstandards



Steuersystem

DIN EN ISO 12100

ISO 25119 / EN 16590

ECU, Sensoren	Ventile	Leiter, Hydraulik, Reling, …
ISO 25119	ISO 13849, ISO 4254, …	ISO 4254, ISO 4413, …

* ISO 25119 Ed. 2 setzt Anwendung der ISO 12100 zur Risikoidentifizierung voraus

Zusammenfassung

- Funktionale Sicherheit von elektronischen Systemen ist in allen Branchen notwendig, einschließlich der Landwirtschaft
- ISO 12100 und ISO 25119 ergänzen sich (Typ A Norm und Typ B1 Norm)
- ISO 25119 Ed. 2 wird die ISO 12100 voraussetzen
- ISO 25119 wurde veröffentlicht und …
  - ist gegenüber IEC 61508 vereinfacht, hat aber einen ähnlichen Ansatz .
  - wurde auch als EN 16590 als harmonisierte Norm veröffentlicht.
  - ist auf die Bedürfnisse für landwirtschaftlichen Maschinen zugeschnitten und angepasst.
  - muss für andere Technologien durch andere Standards (wird nicht allein die Maschinenrichtlinie erfüllen) ergänzt werden.
  - enthält ein normatives Verfahren zur Risikobeurteilung und Annahmekriterien.
  - definiert einen risikobasierten Ansatz für Sicherheitsentwicklung und -nachweis.
  - basiert auf AgPl a bis e.
  - enthält Risikoanalyse-Ansatz vergleichbar Automobilindustrie.
  - legt Leitlinien für ein Ansatz mit ganzheitlichem Sicherheitslebenszyklus.
  - definiert Anforderungen an das Sicherheitsmanagement.
  - deckt Software-Sicherheitsanforderungen ab.
  - wird den Stand der Technik im Bereich FS für landwirtschaftliche Maschinen definieren.
- Änderungen erwartet für ISO 25119 Ed. 2 in 2018

Vielen Dank für Ihre Aufmerksamkeit!

TÜV NORD Mobilität GmbH & Co KG

Institut für Fahrzeugtechnik & Mobilität (IFM)

Electronic Systems & Car IT

Dr. Thomas Wenzel
Kompetenzfeldleiter Funktionale Sicherheit
Adlerstraße 7
45307 Essen
Germany
Tel.: +49 (0)201 825 4197
Fax: +49 (0)201 825 4109
E-Mail: twenzel@tuev-nord.de

Weitere Informationen unter:
www.tuev-nord.de/ifm