SVT 2006

2. Sachverständigentag
11. und 12. September 2006

Sicherheitsanforderungen an Fahrerassistenzsysteme

Mobilität sicher genießen

- Dr. Tomislav Lovric
- TÜV NORD Mobilität
- IFM - Elektronik & IT

Übersicht über den Vortrag

1. Bedeutung Fahrerassistenzsysteme
2. Erforderliche Sicherheitsbetrachtungen
3. Risikoakzeptanz / Unsicherheiten
4. Beispielhafte Anforderungen (IEC 61508)
5. Stand der Technik
6. Schlussfolgerungen
7. Zusammenfassung und Ausblick

1. Bedeutung FAS

- Rasante Fortschritte
  der Mechatronik erlauben vielfältige Assistenzsysteme
- Steigende Anforderungen
  durch höhere Verkehrsleistung, Verkehrsdichte und Geschwindigkeitsbereiche erfordern intelligente Assistenzfunktionen
- Sinkende Risikoakzeptanz
  neue Systeme zur Steigerung der aktiven und passiven Sicherheit
  - Assistenz bei optimaler Umsetzung des Fahrerwunsches, z.B. ABS
  - Assistenz der normalen Fahrt, z.B. ACC
  - Assistenz bei potentiellen Gefahrensituationen, z.B. LDW
  - Assistenz bei akuter Gefahr, z.B. Emergency Break System
  - Assistenz bei Unfall, z.B. Gurtstraffer
  - Assistenz nach Unfall, z.B. Notruf

Jahr	1950	2000	2010
Verkehrsdichte:	100%	1300%	1???%
Verkehrsopfer:	100%	55%	22,5%

•90% der kommenden Automobil-**Innovation** sind **Elektronik**, davon **80%** **Software**

1. FAS und Sicherheit

Fahrerassistenzsysteme

- erhöhen die Verkehrssicherheit
- unterstützen das EU-Programm: halbieren der Verkehrstotenanzahl bis 2010
- sind mechatronische Systeme mit programmierbarer Elektronik

Herausforderungen:

- Steigende Komplexität / Funktionalität
- Steigende Interoperabilität und Integration der Subsysteme
- Vergleichsweise geringe Erfahrung mit der Technologie
- Steigende Fehlermöglichkeiten
- …

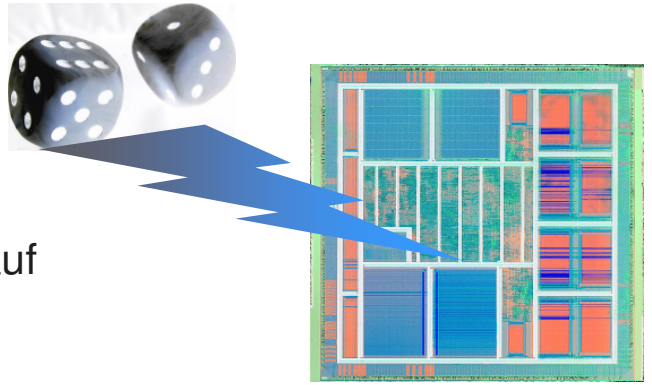
Sicherheitsrelevanz

- Keine / ungewünschte Funktion
- Fehlerhafte Fahrerinformation
- …
- Neue Gefährdungen, die beherrscht werden müssen

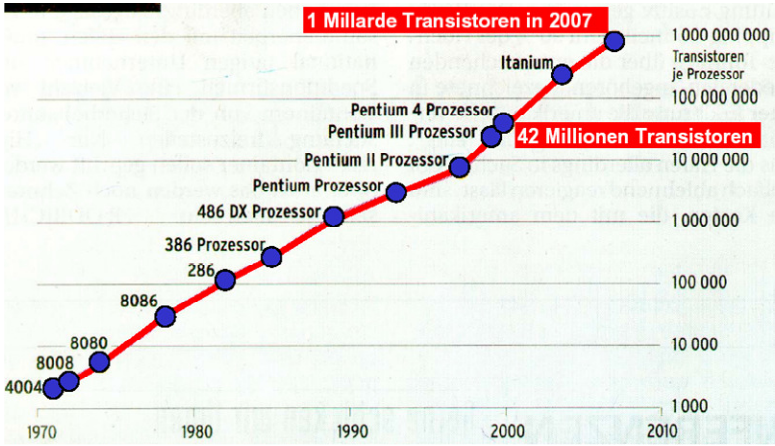
1. Herausforderungen Elektronik

Spezielle Herausforderungen, Beispiele

- Ausfälle der Elektronik
  - sind kein „Materialfehler“ (Mangel, Ermüdung)
  - sind normale physikalische Erscheinungen !
  - treten statistisch zufällig und nicht vorhersehbar auf
  - Ausfallrate der Komponenten (z.B. >>1000 FIT) liegt weit über dem akzeptablen Wert für das System (z.B. 50 FIT)

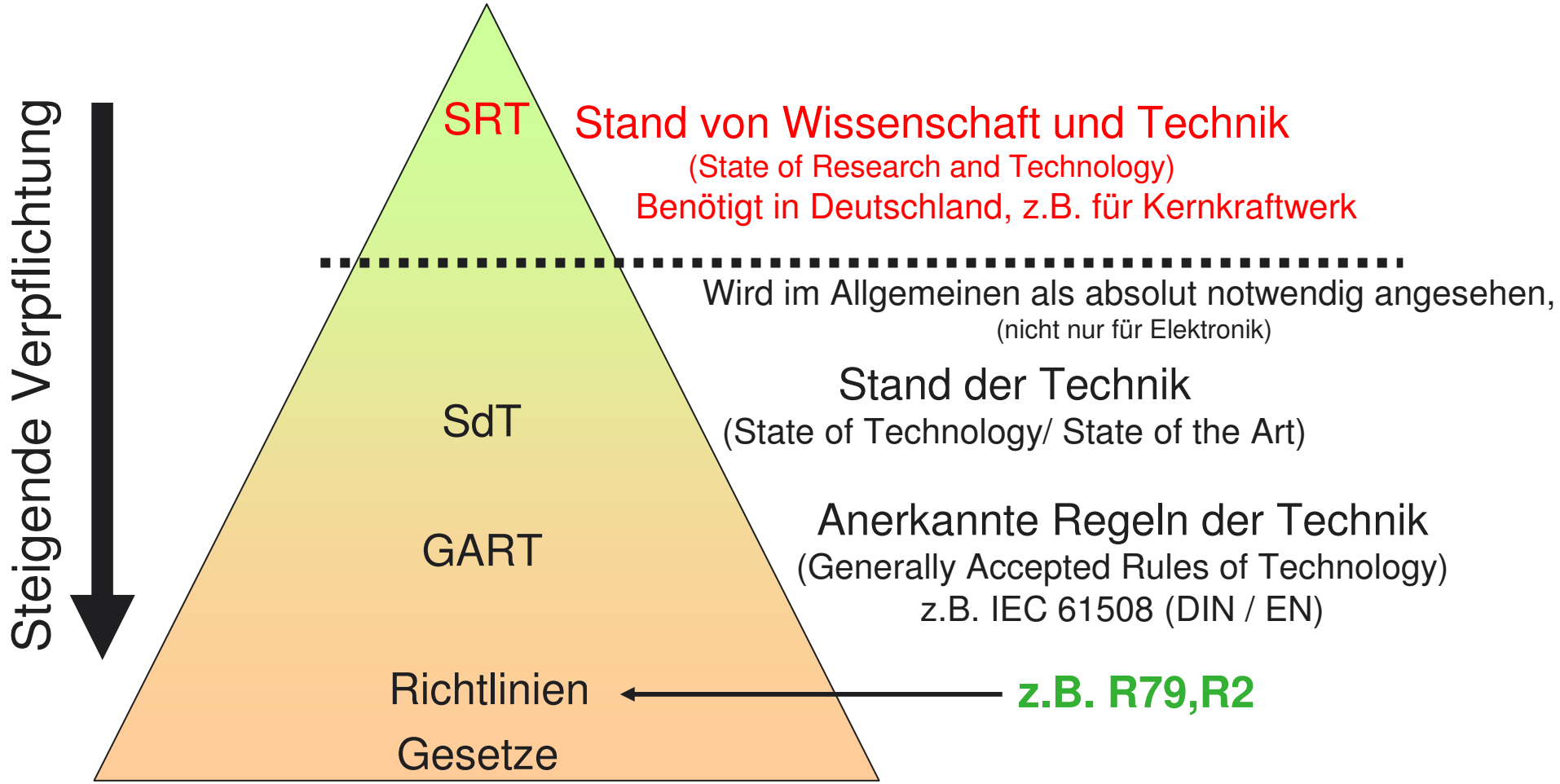


- Komplexität:
  - „Moore‘s Law“ (1965, kurz nach der Erfindung des IC) alle 18 Monate: Verdopplung der Transistoren
  - Moderne Halbleiter haben Millionen Transistoren
  - Software hat Milliarden Zustände



- Raue Automobil-Umgebung
- Hoher Wettbewerbsdruck

2. Sicherheitsbetrachtungen



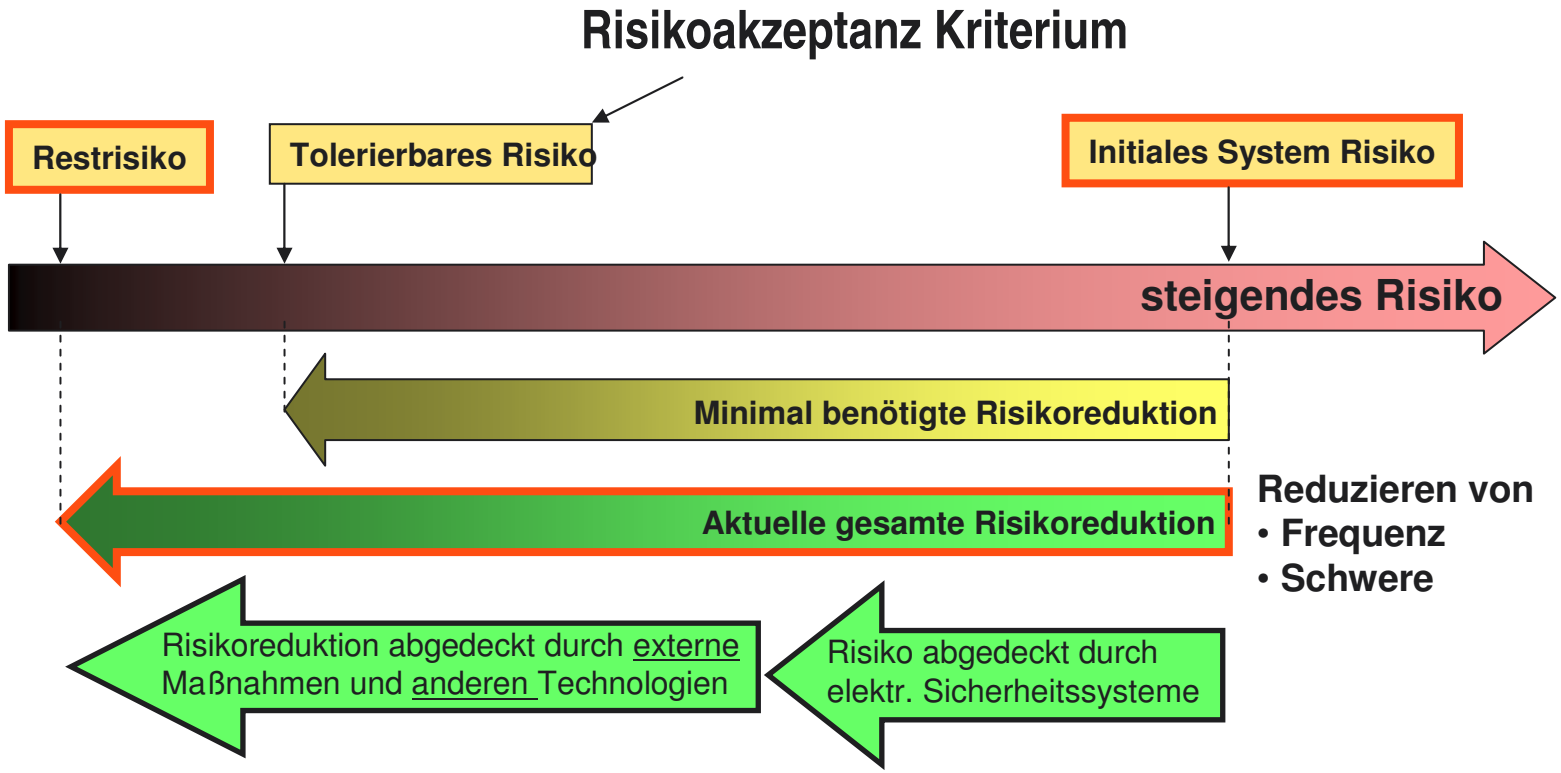
2. Sicherheitsbetrachtungen

- Anerkannte Regeln der Technik
  - in D: DIN,
  - in EU: EN

- Im Automobilbereich (Sicherheitsrelevante Elektronik):
  - DIN EN 61508 (Identisch: IEC 61508)
  - Zukünftig die „61508 Automotive Ableitung“ ISO 26262

- IEC 61508 erfordert u.a.
  - Gefährdungs- und Risikoanalyse (erfordert „Risikoakzeptanz“ Kriterien)
  - Risikobasierten Entwicklungsansatz
  - Sicherheitsorganisation und -Management
  - Sicherheitslebenszyklus
  - Probabilistische Sicherheitsbetrachtungen und Sicherheitsnachweise

3. Risikoakzeptanz



- Fahrgastzelle Energieaufnahme
- Hydraulische Backup
- Training…

- Leitplanken
- Notrufsäulen
- Organisatorische Maßnahmen
- …

- Robuste Sensoren, Komponenten
- Inhärente Eigenschaften
- **Funktionen mit hoher Sicherheitsintegrität**
- …

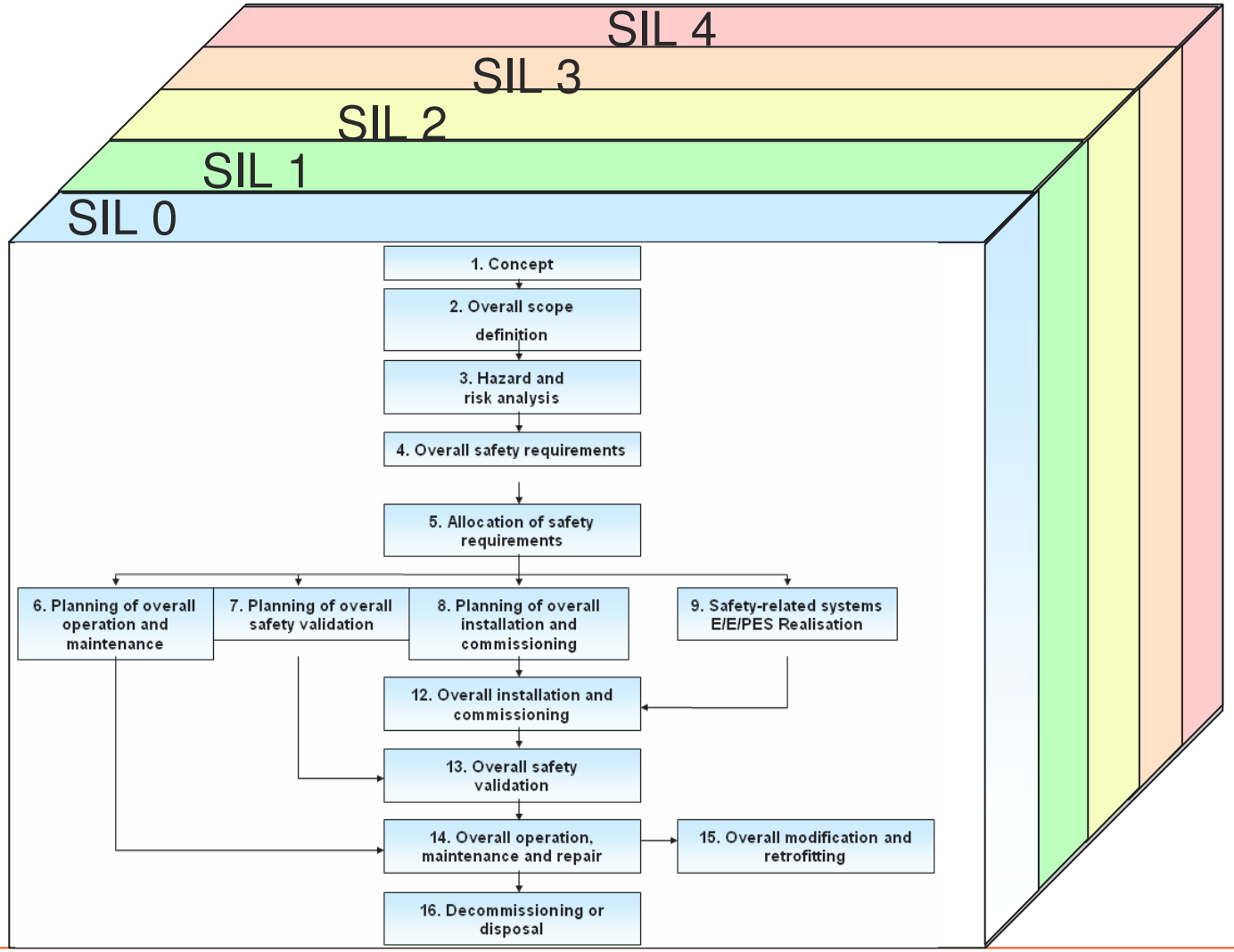
3. Risikoakzeptanz

Unsicherheiten:

- IEC 61508 ist „generische“ Norm
- Kein Risikobeurteilungsverfahren in IEC 61508 vorgeschrieben
- Keine Grenzwerte als Akzeptanzkriterium in IEC 61508
- Jede Industrie hat ihre eigenen Grenzwerte
- Festlegung der Akzeptanzkriterien sind politische Entscheidungen
- Verbindliche Festlegungen werden selten getroffen
- Insbesondere für Automotive sind diese noch nicht festgelegt

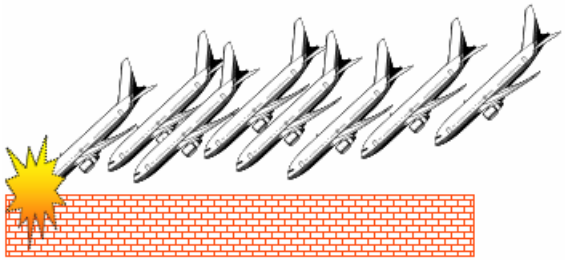
- Abhängig von Risikobewertung ergibt sich der erforderliche Sicherheits-Integritäts-Level (SIL) für die Elektronik-Entwicklung
- Der SIL bestimmt maßgeblich den Entwicklungsaufwand

3. Anforderungstiefe nach SIL



3. Risikoakzeptanz

- Weltweit über 1,2 Millionen Verkehrstote pro Jahr
  D.h. über 8 Jumbo Jets pro Tag
  (2004; WHO)



EU: über 40.000 Opfer/Jahr (200 Mio Fahrzeuge)
  - 1,6 Millionen Verletzte

- EU-Programm für Risikoakzeptanz:
  - Die Zahlen bis zum Jahr 2010 um die Hälfte reduzieren
    (durch aktive Sicherheit)

Fragen:
- Wie viele Opfer wären ohne Fahrerassistenzsysteme aufgekommen?
- Wie viele Opfer gab es durch Fehler in Fahrerassistenzsystemen?

3. Methoden Integritätslevel

Bestimmung der benötigten Integrität kann auf verschiedenen Wegen erfolgen.

- Durch Festlegen der Risikoakzeptanzkriterien, z.B. durch
  - ALARP
  - GAMAB
  - MEM
- Durch Anwenden einer skalierten Risikobewertungsmethode, z.B.
  - Risikograph
  - Risk Matrix

3. Eigenschaften Risikograph

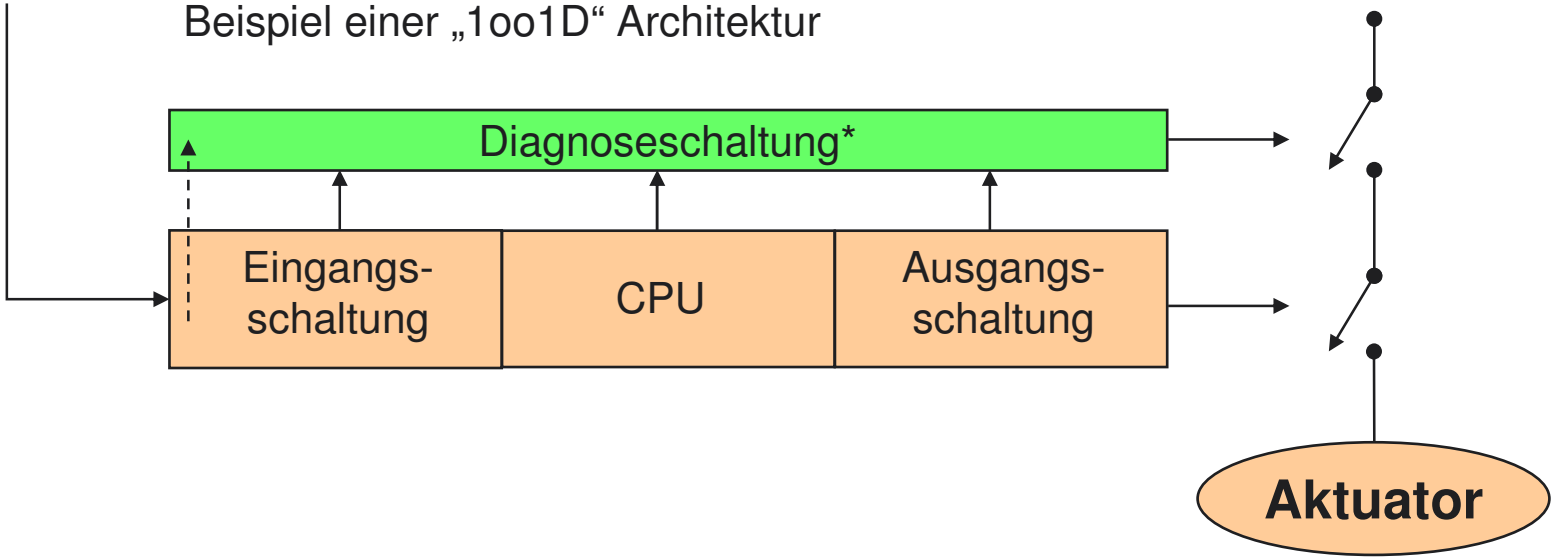
- Ansatz ist beliebt und weit verbreitet
- Leicht und intuitiv zu benutzen
- Wird in der IEC 61508 erwähnt
  …jedoch NICHT im normativen Teil

- Die Parameter sind nicht auf Automotive bezogen
- Es existieren unterschiedliche Versionen
- Beurteilung erfolgt auf Grund unscharfer Parameter
- Die Bedeutung der Parameter werden unterschiedlich interpretiert

- Wie bei allen Risikoakzeptanzkriterien gilt auch hier:
  - Die Auswahl eines Risikographen und deren Parameter definieren das von einer Firma vorgegebene tolerierbare Risikolevel
  - Entscheidungen sollen auf politischer Firmenebene getroffen werden und nicht Aufgabe eines einzelnen Entwicklers sein
  - Zur Zeit gibt es keine normative Grundlage für die Entscheidungen

4. Anforderungen (IEC 61508)

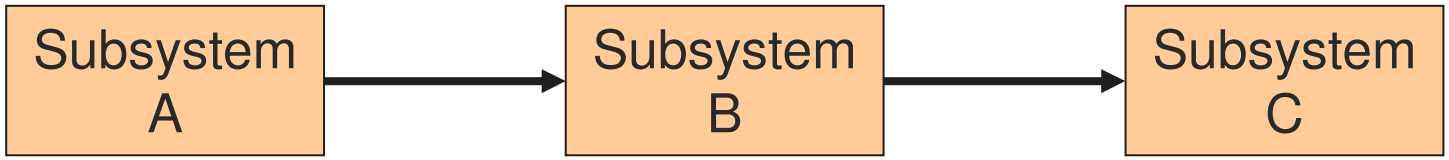
- Anforderungen für eine robuste HW-Architektur
  - Begrenzung des höchst erreichbaren SILs für HW durch Parameter
  - Anteil sicherer Ausfälle (Safe Failure Fraction – SFF)
  - Grad der Fehlertoleranz des HW-Subsystems



4. Anforderungen (IEC 61508)

- Anforderungen um zufällige HW-Ausfälle gering zu halten
  - Einhaltung probabilistischer Werte muss nachgewiesen werden
  - Pro Sicherheitsfunktion einzuhaltende Wahrscheinlichkeitswerte
    - Probability of failure on demand (PFD)
    - Probability of dangerous failure per hour (PFH)
  - Die gesamte PFD ergibt sich aus der Summe der Teilsystem-PFDs (s.u.)

$$PFD_{ges} = PFD_A + PFD_B + PFD_C$$



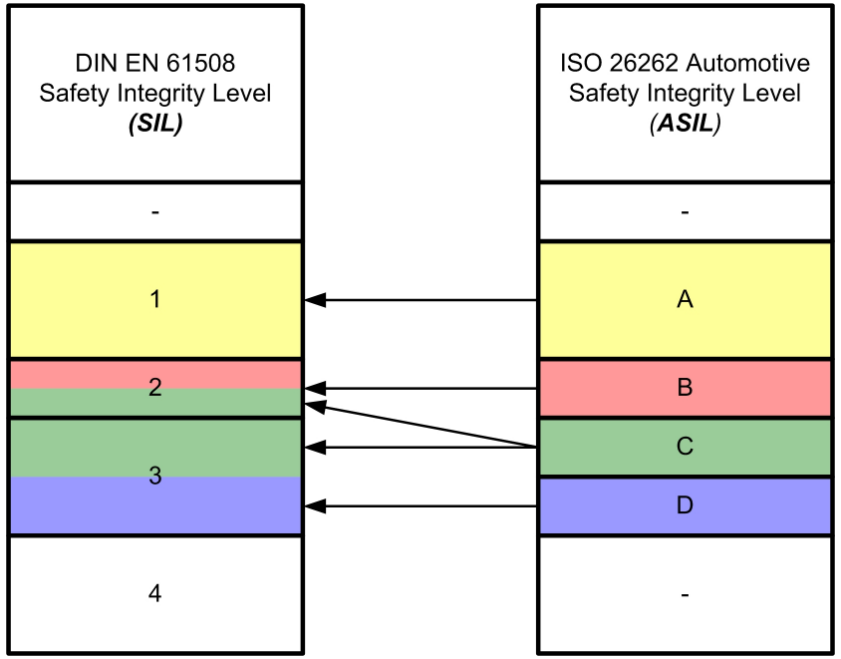
5. Stand der Technik

- IEC 61508 ist generisch und wird zur Zeit zugeschnitten auf automotive
  - **ISO 26262** : Straßenfahrzeuge — Funktionale Sicherheit durch ISO-TC 22 - SC 3 - WG 16
- Die Draft Version beinhaltet bereits ausgereifte Prozeduren zur Herleitung des "Automotive Sicherheits-Integritäts-Levels (ASIL)"

- ISO WD 26262
  ASIL A bis ASIL D

  entspricht

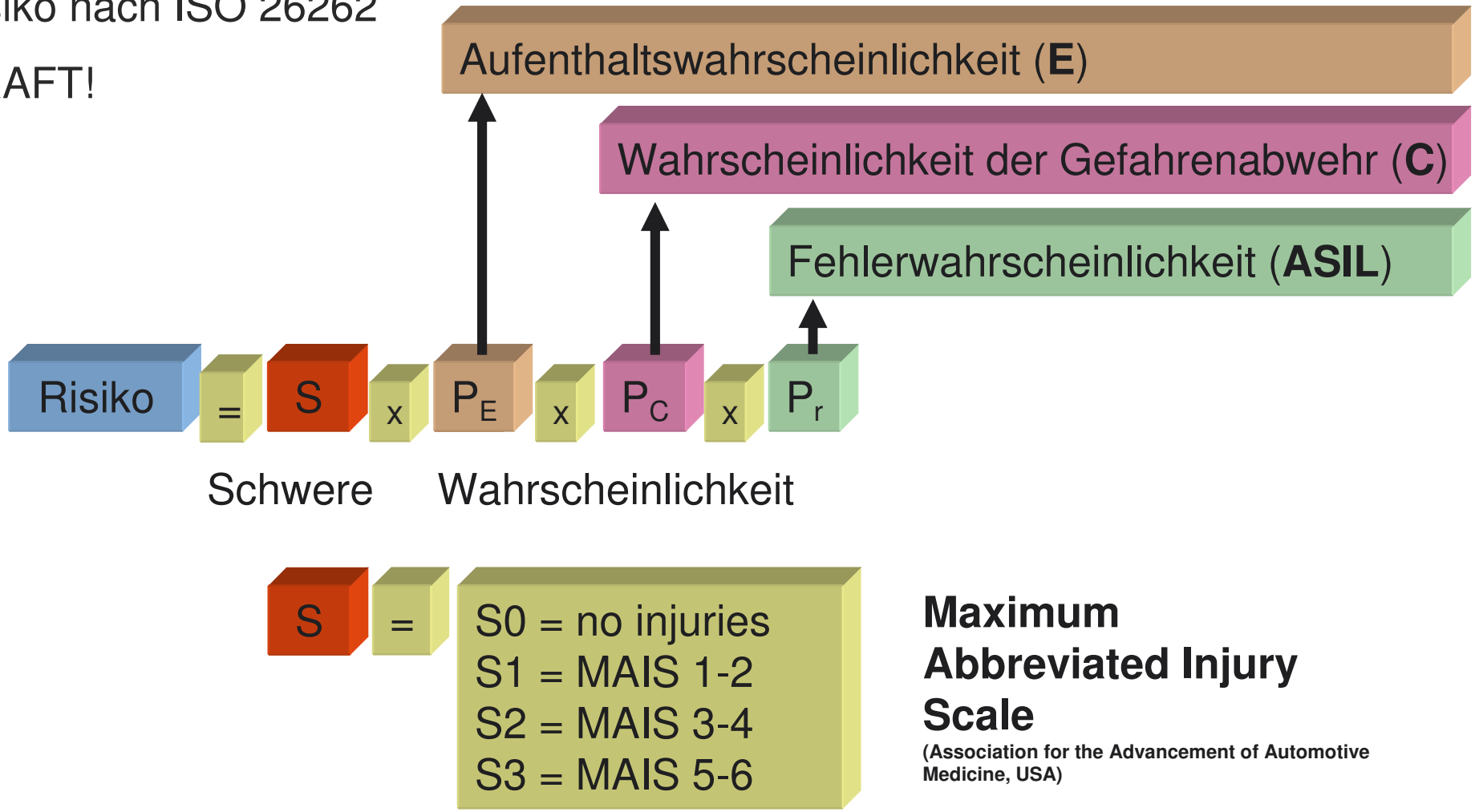
  IEC 61508
  SIL1 bis SIL3



5. Stand der Technik

Risiko nach ISO 26262

DRAFT!



Maximum Abbreviated Injury Scale
(Association for the Advancement of Automotive Medicine, USA)

6. Schlussfolgerungen

Erfordernisse der Norm

- sind nicht direkt gesetzlich geregelt
- bestehen als Regeln der Technik, somit dringend zu empfehlen
  - zur Realisierung der angemessenen Funktionalen Sicherheit
  - Zur Absicherung der Sorgfaltspflicht des Herstellers
- werden nicht abgedeckt durch andere bestehende Standards
- sind durchgreifend, betreffen z.B.
  - Aufbau und Ablauf
  - Management und Entwickler
  - System Konzept bis Entsorgung
  - Produkt und Prozess
- werden angewandt, sind aber schwierig voll umzusetzen …
- werden nicht einheitlich umgesetzt
- bedürfen der Erfahrung in Spezialkenntnissen

6. Handlungsbedarf

Die Komplexität und Sicherheitsrelevanz moderner FAS erfordert

- Intelligente Absicherungsverfahren und Prüfkonzepte
  - Detailprüfung ist nicht abgedeckt durch Homologation
  - „Prüfung am Schluss“ ist nicht möglich
  - Entwicklungsbegleitung
  - Wiederkehrende Prüfungen sollten einbezogen werden

- Starke Partner bei der Umsetzung des Standards
  - Kompetent, erfahren
  - Unabhängig und vertrauenswürdig
  - Schulung, Einführung
  - Prüfung und Ergänzung bestehender Prozesse (Gap Analyse)
  - Umsetzung der Maßnahmen
  - Absicherung der einzelnen Entwicklungsphasen
  - Bewertung der Umsetzung
  - Bewertung der Produkte

7. Zusammenfassung / Ausblick

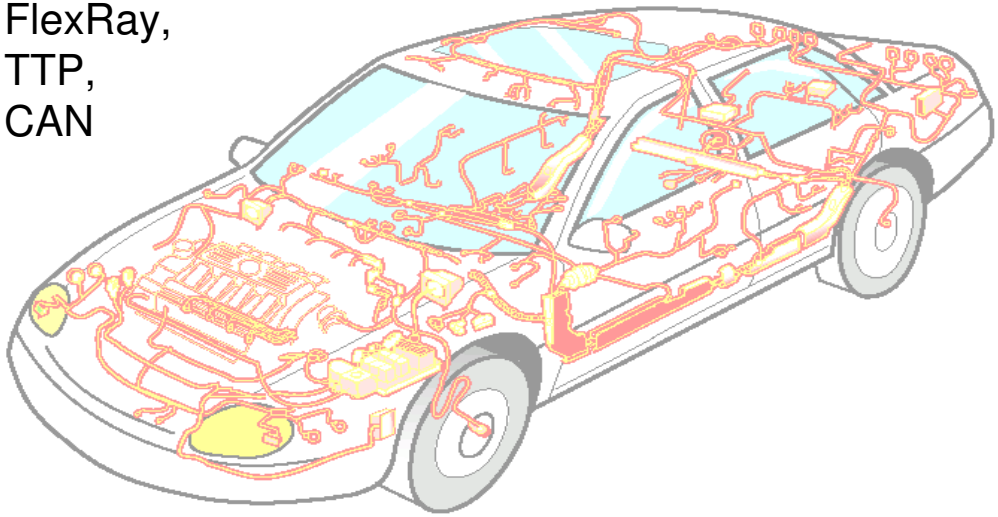
- Sicherheitsanforderungen an Fahrerassistenzsysteme sind anspruchsvoll
- Anerkannte Regeln der Technik regeln das mindestens erforderliche Maß der Sorgfalt bei der Entwicklung
- Die Angemessenheit der Entwicklung kann durch unabhängige Experten abgesichert werden
- Dies erlaubt dem Hersteller
  - Produktrisiken angemessen zu minimieren
  - Mögliche Entwicklungsrisiken frühzeitig zu behandeln
  - Vertrauen zu schaffen in die Sicherheit der neuen Technik

Kontakt - Vielen Dank

TÜV NORD MOBILITY, IFM (Institut für Fahrzeugtechnik und Mobilität)
Abteilung **„Elektronik & IT“**

1: Communication Engineering

Datenbus Kommunikation
FlexRay,
TTP,
CAN



2: Functional Safety

Assessment, Staff Training,
Beratung, Technischer Support,
Sicherheits-Management System,
Quantitative Sicherheitsanalyse
(FMEDA, FTA)
IEC 61508, ISO WD 26262,
ICE TR 62380
prEN ISO 13849 / 954, etc.

3: Software Tools für Validation und Standardisierung

ASAM Corp.: FIBEX Checker
FlexRay: Conformance Tester; AUTOSAR: WP4

Dr.rer.nat., Dipl.-Inform.

Tomislav Lovric

Telefon + 49 (0) 201 – 825 4112
Fax + 49 (0) 201 – 825 4204
e-mail TLovric@tuev-nord.de
Internet: www.tuev-nord.de/26544.asp
www.ift.rwtuev.de