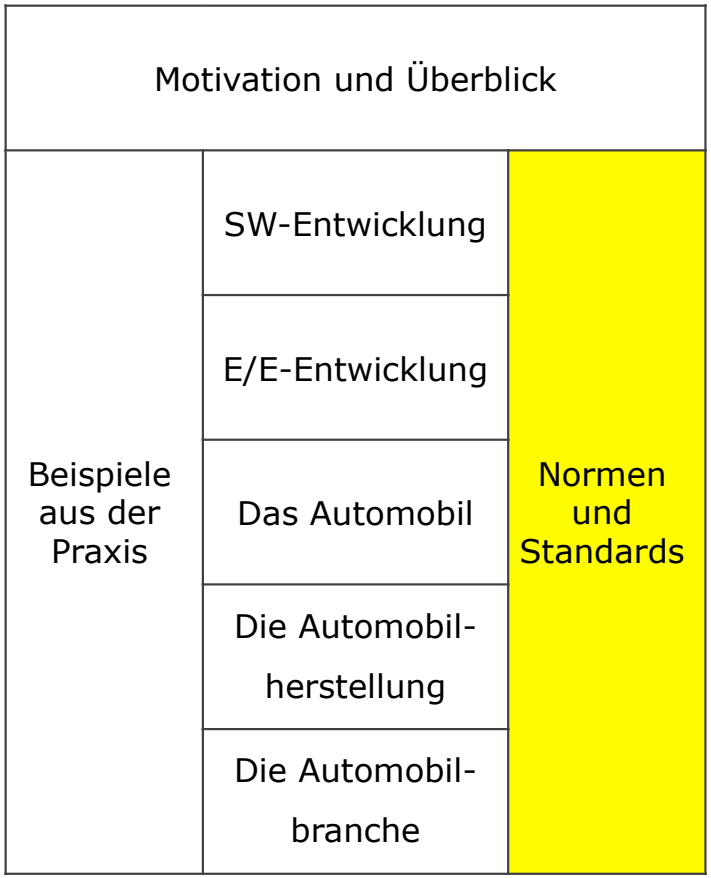
TECHNISCHE UNIVERSITÄT DRESDEN

# Vorlesung
# Automotive Software Engineering
# Teil 7 Normen und Standards (3-0)
# Funktionale Sicherheit - Einleitung

Sommersemester 2015

Prof. Dr. rer. nat. Bernhard Hohlfeld
Bernhard.Hohlfeld@mailbox.tu-dresden.de
Technische Universität Dresden, Fakultät Informatik
Honorarprofessur Automotive Software Engineering

# Vorlesung Automotive Software Engineering




MOST

CAN

AUTOSAR

lin

HIS

OSEK/ VDX

ASAM

**ISO 26262**
**Road vehicles - Functional safety**

FlexRay

# Lernziele Normen und Standards

- Die Bedeutung von Normen und Standards für industrielle Entwicklung verstehen.
- AUTOSAR Automotive Open System Architecture kennenlernen
  - Motivation
  - Technik
  - Beispiele
- ISO 26262 Road Vehicles Functional Safety kennenlernen
- Den Begriff COTS einordnen
- Entwurfs- und Codierstandards kennenlernen

# 7. Normen und Standards

1. AUTOSAR
2. ARTOP
3. ISO 26262 - Road Vehicles - Functional Safety
4. COTS
5. Entwurfs- und Codierstandards

# 7. Normen und Standards

1. AUTOSAR
2. ARTOP
3. **ISO 26262 - Road Vehicles - Functional Safety**
4. COTS
5. Entwurfs- und Codierstandards

# Gliederung

- Funktionale Sicherheit - Einleitung
- ISO 26262

# Funktionale Sicherheit

- Dieser Abschnitt basiert auf dem Vortrag

  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

  
  
  Tagung

  Elektronik im Kraftfahrzeug

  16./17. Juni 2010, Dresden

# Gliederung

# Katastrophen mit technischen Systemen

- 1986 Explosion im Kernkraftwerk Tschernobyl
  - Missachtung von Betriebsvorschriften
- 1987 Explosion des Space Shuttle Challenger
- 1998 ICE-Unglück bei Eschede
  - Radbruch, Weiche, Brücke
- 1999 Feuer im Mont Blanc Tunnel
  - Defektes Fahrzeug, mangelnde Kontrolle bei Einfahrt
- 2000 Absturz der Concorde bei Paris
  - Reifenteile auf Startbahn, Konstruktionsfehler, Freigabe Startbahn
- 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 Verifikation 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

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

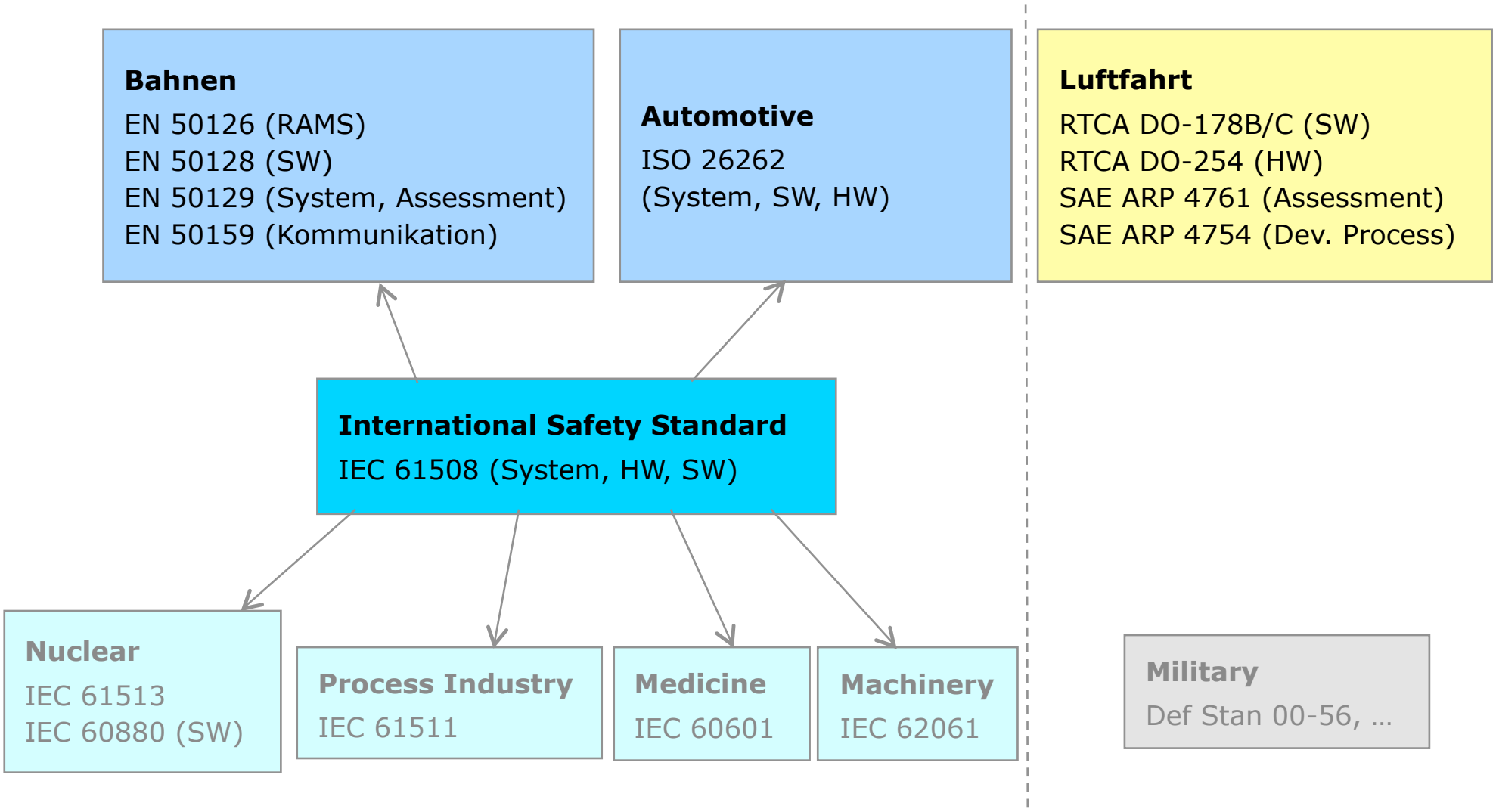
# Ansätze und Prinzipien der Funktionalen Sicherheit

# Ansätze und Prinzipien der Funktionalen Sicherheit

| | **Zufällige Fehler** | **Systematische Fehler** |
|---|---|---|
| Beispiele | • Hardwareausfall<br>• Übertragungsfehler | • Designfehler<br>• Spezifkationsfehler<br>• Programmierfehler |
| Strategie | Beherrschung der Auswirkungen | Fehlervermeidung |
| Ansatz | Quantitative Analysen | Vorgeschriebene Methoden abhängig vom (qualitativen) Safety Integrity Level (SIL) |
| Prinzipien | • Fehlererkennung<br>  • Selbsttests<br>• Fail-safe (Sicherer Zustand bei Ausfall)<br>• Redundanz<br>• Ziel: Beherrschung jedes einzelnen Fehlers | • Entwicklung nach Stand der Wissenschaft und Technik<br>• Umfangreiche Verifikation<br>• Nachvollziehbarkeit<br>• Abdeckung<br>• Unabhängigkeit<br>  • Technisch: Diversität, ...<br>  • Personell: Entwickler und Prüfer verschiedene Personen<br>  • Organisatorisch: Entwickler und Prüfer in verschiedenen Organisationen<br>• Ziel: Vermeidung von Fehlern |

# Sicherheitsstandards im Überblick

# Sicherheitsstandards im Überblick



| | **IEC 61508** | **EN 50126<br>EN 50128<br>EN 50129<br>EN 50159** | **ISO 26262** | **DO-178B<br>DO-254<br>ARP 4761<br>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)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>-- | SIL 4 (hoch)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>SIL 0 (nicht sicherheitsrelevant) | --<br>ASIL D (hoch)<br>ASIL C<br>ASIL B<br>ASIL A (niedrig)<br>(QM) | Level A (hoch)<br>Level B<br>Level C<br>Level D<br>Level E (niedrig)<br>-- |
| Organisatorische Aspekte | Teilweise | Ja | Ja | Nein |
| Werkzeug-qualifizierung | ~~Nein~~ Ja | ~~Nein~~ Ja | Ja | Ja |

| | **IEC 61508** | **EN 50126<br>EN 50128<br>EN 50129<br>EN 50159** | **ISO 26262** | **DO-178B<br>DO-254<br>ARP 4761<br>ARP 4754** |
|---|---|---|---|---|
| Anv Unterschied 1 | 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)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>-- | SIL 4 (hoch)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>SIL 0 (nicht sicherheitsrelevant) | --<br>ASIL D (hoch)<br>ASIL C<br>ASIL B<br>ASIL A (niedrig)<br>(QM) | Level A (hoch)<br>Level B<br>Level C<br>Level D<br>Level E (niedrig)<br>-- |
| Organisatorische Aspekte | Teilweise | Ja | Ja | Nein |
| Werkzeug-qualifizierung | ~~Nein~~ Ja | ~~Nein~~ Ja | Ja | Ja |

| | **IEC 61508** | **EN 50126<br>EN 50128<br>EN 50129<br>EN 50159** | **ISO 26262** | **DO-178B<br>DO-254<br>ARP 4761<br>ARP 4754** |
|---|---|---|---|---|
| Anv[illegible] Unterschied 1 | Generisch | Bahnen (1-dimensional) | Automotive (2-dimensional) | Luftfahrt (3-dimensional) |
| Sich[illegible] Unterschied 2 | 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)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>-- | SIL 4 (hoch)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>SIL 0 (nicht sicherheitsrelevant) | --<br>ASIL D (hoch)<br>ASIL C<br>ASIL B<br>ASIL A (niedrig)<br>(QM) | Level A (hoch)<br>Level B<br>Level C<br>Level D<br>Level E (niedrig)<br>-- |
| Organisatorische Aspekte | Teilweise | Ja | Ja | Nein |
| Werkzeug-qualifizierung | ~~Nein~~ Ja | ~~Nein~~ Ja | Ja | Ja |

| | **IEC 61508** | **EN 50126<br>EN 50128<br>EN 50129<br>EN 50159** | **ISO 26262** | **DO-178B<br>DO-254<br>ARP 4761<br>ARP 4754** |
|---|---|---|---|---|
| Anv[Unterschied 1] | Generisch | Bahnen (1-dimensional) | Automotive (2-dimensional) | Luftfahrt (3-dimensional) |
| Sich[Unterschied 2] | 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 | |
| Saf Lev[Unterschied 3] | SIL 4 (hoch)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>-- | SIL 4 (hoch)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>SIL 0 (nicht sicherheitsrelevant) | --<br>ASIL D (hoch)<br>ASIL C<br>ASIL B<br>ASIL A (niedrig)<br>(QM) | Level A (hoch)<br>Level B<br>Level C<br>Level D<br>Level E (niedrig)<br>-- |
| Organisatorische Aspekte | Teilweise | Ja | Ja | Nein |
| Werkzeug-qualifizierung | ~~Nein~~ Ja | ~~Nein~~ Ja | Ja | Ja |

| | **IEC 61508** | **EN 50126<br>EN 50128<br>EN 50129<br>EN 50159** | **ISO 26262** | **DO-178B<br>DO-254<br>ARP 4761<br>ARP 4754** |
|---|---|---|---|---|
| Anv[illegible] | Generisch | Bahnen (1-dimensional) | Automotive (2-dimensional) | Luftfahrt (3-dimensional) |
| Sich[illegible] | 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 | |
| Saf<br>Lev[illegible] | SIL 4 (hoch)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>-- | SIL 4 (hoch)<br>SIL 3<br><br>SIL 2<br>SIL 1 (niedrig)<br>SIL 0 (nicht sicherheitsrelevant) | --<br>ASI[illegible]<br>ASI[illegible]<br>ASIL B<br>ASIL A (niedrig)<br>(QM) | )<br><br><br>Level D<br>Level E (niedrig)<br>-- |
| Organisatorische Aspekte | Teilweise | Ja | Ja | Nein |
| Werkzeug-qualifizierung | ~~Nein~~ Ja | ~~Nein~~ Ja | Ja | Ja |

Unterschied 1

Unterschied 2

Unterschied 3

Weniger Personen

Geringere kinetische Energie

# Gliederung

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

TECHNISCHE UNIVERSITÄT DRESDEN

Beispiel

INTERNATIONAL STANDARD

**ISO 26262-6**

First edition
2011-11-15

# Road vehicles — Functional safety —

## Part 6: Product development at the software level

*Véhicules routiers — Sécurité fonctionnelle —*

*Partie 6: Développement du produit au niveau du logiciel*

# Batterie Management Systems (BMS) (1)

- Electrification of Auxiliary Units contributes to energy efficiency by decoupling energy generation and energy consumption via energy storage in battery
- Battery needs Batterie Management Systems (BMS)
  - Measurement and monitoring of voltage, current, state of charge, temperature, ... for
    - Prediction of range
    - Start / Stop
    - Detection of undesired / dangerous state of battery
    - ...

# Batterie Management Systems (BMS) (2)

- BMS is safety-relevant
  - ISO 26262-6 6.4.1 The software safety requirements shall address each software-based function whose failure could lead to a violation of a technical safety requirement allocated to software.
    EXAMPLE
    Functions whose failure could lead to a violation of a safety requirement can be:
    - functions that enable the system to achieve or maintain a safe state;
    - functions related to the detection, indication and handling of faults of safety-related hardware elements;
- BMS is a software based function which detects, indicates and handles faults of the safety-related hardware element battery
- BMS is classified as ASIL C by German automotive industry
  - ASIL = Automotive Safety Integrity Level according to ISO 26262, from A (low) to D (high)
  - ASIL C implies requirements for development and documentation
  - The line of argumentation (next slide) is not necessarily the same as in the „official" classification but it arrives at the same result

**ASIL = Automotive Safety Integrity Level**

| | Severity (S) | Exposure (E) | Controllability (C): C0 Controllable in general | C1 Simply controllable | C2 Normally controllable | C3 Difficult to control or uncontrollable |
|---|---|---|---|---|---|---|
| lower ↑ | S0 No injuries | -- | QM | | | |
| | S1 Light and moderate injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | |
| | | E3 - Medium probability | QM | | | ASIL A |
| | | E4 - High probability | QM | | ASIL A | ASIL B |
| | S2 Severe injuries, possibly life-threatening, survival probable | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | ASIL A |
| | | E3 - Medium probability | QM | | ASIL A | ASIL B |
| | | E4 - High probability | QM | ASIL A | ASIL B | ASIL C |
| | S3 Life-threatening injuries (survival uncertain) or fatal injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | ASIL A |
| | | E2 - Low probability | QM | | ASIL A | ASIL B |
| | | E3 - Medium probability | QM | ASIL A | ASIL B | ASIL C |
| | | E4 - High probability | QM | ASIL B | ASIL C | ASIL D |

**ASIL = Automotive Safety Integrity Level**

| | Severity (S) | Exposure (E) | Controllability (C): C0 Controllable in general | C1 Simply controllable | C2 Normally controllable | C3 Difficult to control or uncontrollable |
|---|---|---|---|---|---|---|
| lower ↑ | S0 No injuries | -- | QM | | | |
| | S1 Light and moderate injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | |
| | | E3 - Medium probability | QM | | | ASIL A |
| | | E4 - High probability | QM | | ASIL A | ASIL B |
| | S2 Severe injuries, possibly life-threatening, survival probable | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | ASIL A |
| | | E3 - Medium probability | QM | | ASIL A | ASIL B |
| | | E4 - High probability | QM | ASIL A | ASIL B | ASIL C |
| | S3 Life-threatening injuries (survival uncertain) or fatal injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | ASIL A |
| | | E2 - Low probability | QM | | ASIL A | ASIL B |
| | | E3 - Medium probability | QM | ASIL A | ASIL B | ASIL C |
| | | E4 - High probability | QM | ASIL B | ASIL C | ASIL D |

**ASIL = Automotive Safety Integrity Level**

| | Severity (S) | Exposure (E) | Controllability (C): C0 Controllable in general | C1 Simply controllable | C2 Normally controllable | C3 Difficult to control or uncontrollable |
|---|---|---|---|---|---|---|
| lower ↑ | S0 No injuries | -- | QM | | | |
| | S1 Light and moderate injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | |
| | | E3 - Medium probability | QM | | | ASIL A |
| | | E4 - High probability | QM | | ASIL A | ASIL B |
| | S2 Severe injuries, possibly life-threatening, survival probable | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | ASIL A |
| | | E3 - Medium probability | QM | | ASIL A | ASIL B |
| | | E4 - High probability | QM | ASIL A | ASIL B | ASIL C |
| | S3 Life-threatening injuries (survival uncertain) or fatal injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | ASIL A |
| | | E2 - Low probability | QM | | ASIL A | ASIL B |
| | | E3 - Medium probability | QM | ASIL A | ASIL B | ASIL C |
| | | E4 - High probability | QM | ASIL B | ASIL C | ASIL D |

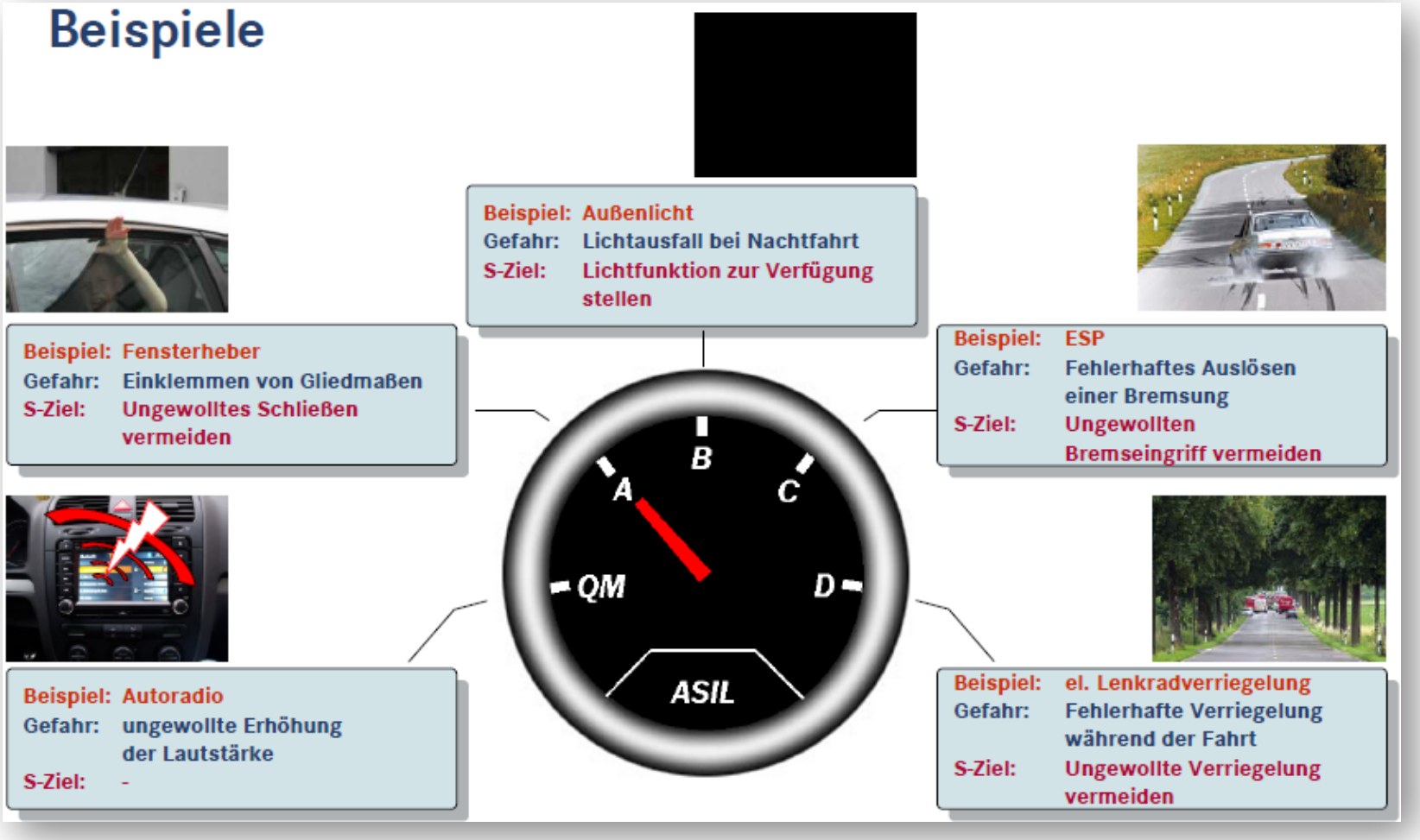
**ASIL = Automotive Safety Integrity Level**

| | Severity (S) | Exposure (E) | Controllability (C): C0 Controllable in general | C1 Simply controllable | C2 Normally controllable | C3 Difficult to control or uncontrollable |
|---|---|---|---|---|---|---|
| lower ↑ | S0 No injuries | -- | QM | | | |
| | S1 Light and moderate injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | |
| | | E3 - Medium probability | QM | | | ASIL A |
| | | E4 - High probability | QM | | ASIL A | ASIL B |
| | S2 Severe injuries, possibly life-threatening, survival probable | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | ASIL A |
| | | E3 - Medium probability | QM | | ASIL A | ASIL B |
| | | E4 - High probability | QM | ASIL A | ASIL B | ASIL C |
| | S3 Life-threatening injuries (survival uncertain) or fatal injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | ASIL A |
| | | E2 - Low probability | QM | | ASIL A | ASIL B |
| | | E3 - Medium probability | QM | ASIL A | ASIL B | ASIL C |
| | | E4 - High probability | QM | ASIL B | ASIL C | ASIL D |

**ASIL = Automotive Safety Integrity Level**

| | Severity (S) | Exposure (E) | C0 Controllable in general | C1 Simply controllable | C2 Normally controllable | C3 Difficult to control or uncontrollable |
|---|---|---|---|---|---|---|
| | | | Controllability (C) — better → | | | |
| lower ↑ | S0 No injuries | -- | QM | | | |
| | S1 Light and moderate injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | |
| | | E3 - Medium probability | QM | | | ASIL A |
| | | E4 - High probability | QM | | ASIL A | ASIL B |
| | S2 Severe injuries, possibly life-threatening, survival probable | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | ASIL A |
| | | E3 - Medium probability | QM | | ASIL A | ASIL B |
| | | E4 - High probability | QM | ASIL A | ASIL B | ASIL C |
| | S3 Life-threatening injuries (survival uncertain) or fatal injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | ASIL A |
| | | E2 - Low probability | QM | | ASIL A | ASIL B |
| | | E3 - Medium probability | QM | ASIL A | ASIL B | ASIL C |
| | | E4 - High probability | QM | ASIL B | ASIL C | ASIL D |

# Beispiel ASIL-Einstufung - Automotive




Vortrag Dr. Jürgen Schwarz, Daimler AG

# Bewerten der Risiken in allen Fahrsituationen (1)

- Das Risiko jedes funktionalen Fehlers wird bei ISO 26262 für alle Fahrsituationen mit folgenden drei Attributen bewertet:
- Schwere eines möglichen Schadens (Severity S)
  - Maß für den erwarteten Schädigungsgrad einer gefährdeten Person in einer bestimmten Situation
  - S0: Keine Verletzung
  - S1: Leichte und mittlere Verletzung
  - S2: Schwere Verletzung - Überleben wahrscheinlich
  - S3: Lebensgefährliche Verletzung - Überleben unwahrscheinlich
- Häufigkeit der Fahrsituation (Exposure E)
  - Häufigkeit der  Situation, die in Kombination mit einem betrachteten Versagen gefährlich sein kann.
  - E0: Unwahrscheinlich
  - E1: Sehr niedrige Wahrscheinlichkeit
  - E2: Niedrige Wahrscheinlichkeit
  - E3: Mittlere Wahrscheinlichkeit
  - E4: Hohe Wahrscheinlichkeit

# Bewerten der Risiken in allen Fahrsituationen (2)

- Das Risiko jedes funktionalen Fehlers wird bei ISO/DIS 26262 für alle Fahrsituationen mit folgenden drei Attributen bewertet:
- Schwere eines möglichen Schadens (Severity S)
- Häufigkeit der Fahrsituation (Exposure E)
- Beherrschbarkeit durch den Fahrer (Controllability C)
- Beherrschbarkeit: Vermeidung des Eintretens einer Schädigung durch rechtzeitige Reaktion der beteiligten Personen (Fahrer, andere Verkehrsteilnehmer)
  - C0: Im Allgemeinen beherrschbar
  - C1: Einfach beherrschbar
  - C2: Normalerweise beherrschbar
  - C3: Schwierig oder nicht beherrschbar

# Bestimmung der Schadensschwere - Severity

| Class | S0 | S1 | S2 | S3 |
|---|---|---|---|---|
| Description | No injuries | Light and moderate injuries | Severe injuries, possibly life-threatening (survival probable) | Life-threatening injuries (survival uncertain), fatal injuries |
| Reference for single injuries (AIS - Abbreviated Injury Scale) | AIS 0<br>Damage that cannot be classified safety-related, e.g. limited to material demage | More than 10% probability of AIS 1-6 (and not S2 or S3) | More than 10% probability of AIS 3-6 (and not S3) | More than 10% probability of AIS 5 and 6 |
| Rear/front collision between two Passenger cars | | $\Delta v < 20$km/h | $20 < \Delta v < 40$ km/h | $\Delta v > 40$ km/h, |

# AIS - Abbreviated Injury Scale

| AIS-Code | AIS-Verletzungsschwere (englisch) | AIS-Verletzungsschwere |
|---|---|---|
| 1 | Minor | Gering |
| 2 | Moderate | Ernsthaft |
| 3 | Serious | Schwer |
| 4 | Severe | Sehr Schwer |
| 5 | Critical | Kritisch |
| 6 | Maximum | Maximal (nicht behandelbar) |

# Bestimmung der Häufigkeit - Exposure

| Class | E0 | E1 | E2 | E3 | E4 |
|---|---|---|---|---|---|
| Description | Incredible | Very low probability | Low probability | Medium probability | High probability |
| Definition of frequency | -- | Situations that occur less often than once a year for the great majority of drivers | Situations that occur a few times a year for the great majority of drivers | Situations that occur once a month or more often for the great majority of drivers | All situations that occur during almost every drive on average |
| Definition of duration / probability of exposure | -- | Not specified | < 1% of average operating time | 1% - 10% of average operating time | > 10% of average operating time |

# Bestimmung der Beherrschbarkeit - Contollability

| Class | C0 | C1 | C2 | C3 |
|---|---|---|---|---|
| Description | Controllable in general | Simply controllable | Normally controllable | Difficult to control or uncontrollable |
| Definition | Distracting (störend) | More than 99% of average drivers or other traffic participants are usually able to control the damage. | More than 90% of average drivers or other traffic participants are usually able to control the damage. | The average driver or other traffic participant is usually unable, or barely able, to control the damage. |

**ASIL = Automotive Safety Integrity Level**

| | Severity (S) | Exposure (E) | Controllability (C): C0 Controllable in general | C1 Simply controllable | C2 Normally controllable | C3 Difficult to control or uncontrollable |
|---|---|---|---|---|---|---|
| lower ↑ | S0 No injuries | -- | QM | | | |
| | S1 Light and moderate injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | |
| | | E3 - Medium probability | QM | | | ASIL A |
| | | E4 - High probability | QM | | ASIL A | ASIL B |
| | S2 Severe injuries, possibly life-threatening, survival probable | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | |
| | | E2 - Low probability | QM | | | ASIL A |
| | | E3 - Medium probability | QM | | ASIL A | ASIL B |
| | | E4 - High probability | QM | ASIL A | ASIL B | ASIL C |
| | S3 Life-threatening injuries (survival uncertain) or fatal injuries | E0 - Unusual or incredible | QM | | | |
| | | E1 - Very low probability | QM | | | ASIL A |
| | | E2 - Low probability | QM | | ASIL A | ASIL B |
| | | E3 - Medium probability | QM | ASIL A | ASIL B | ASIL C |
| | | E4 - High probability | QM | ASIL B | ASIL C | ASIL D |

# 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) Gefährdungsanalyse

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“

# Qualitätssicherung: Standards und Methoden

## 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)

FMEA:
Fehler-Möglichkeits- und Einflussanalyse
Failure Mode and Effect Analysis

# Qualitätssicherung: Standards und Methoden

## 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)

FMEA:
Fehler-Möglichkeits- und Einflussanalyse
Failure Mode and Effect Analysis

# Qualitätssicherung: Standards und Methoden

## Beispiel FMEA - Motorenentwicklung


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

RPZ: Risiko-Prioritätszahl

| 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 |

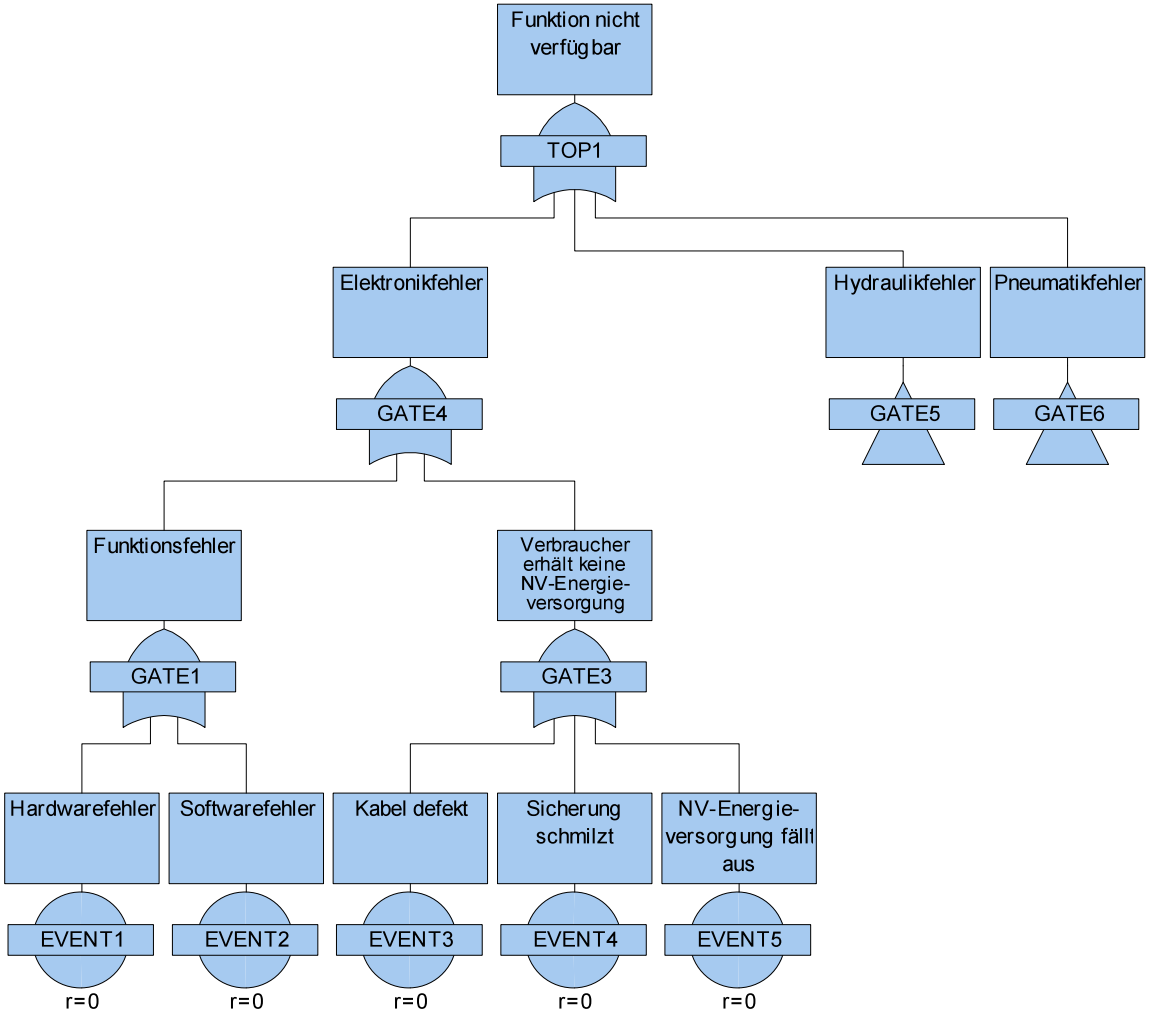
Bewertungszahlen:

**A - Auftretenswahrscheinlichkeit**
1 (unwahrscheinlich)
10 (hoch)

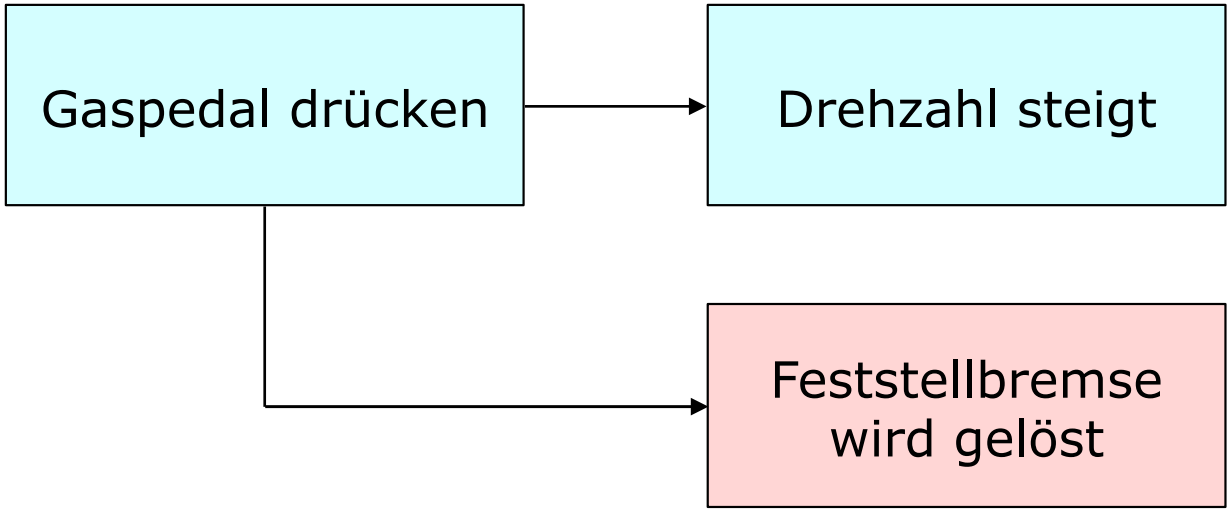
**B - Bedeutung**
1 (keine Bedeutung)
10 (sehr hohe Bedeutung)

**E - Entdeckungswahrscheinlichkeit**
1 (hoch)
10 (unwahrscheinlich)

# Fehlerbaum - Fault Tree

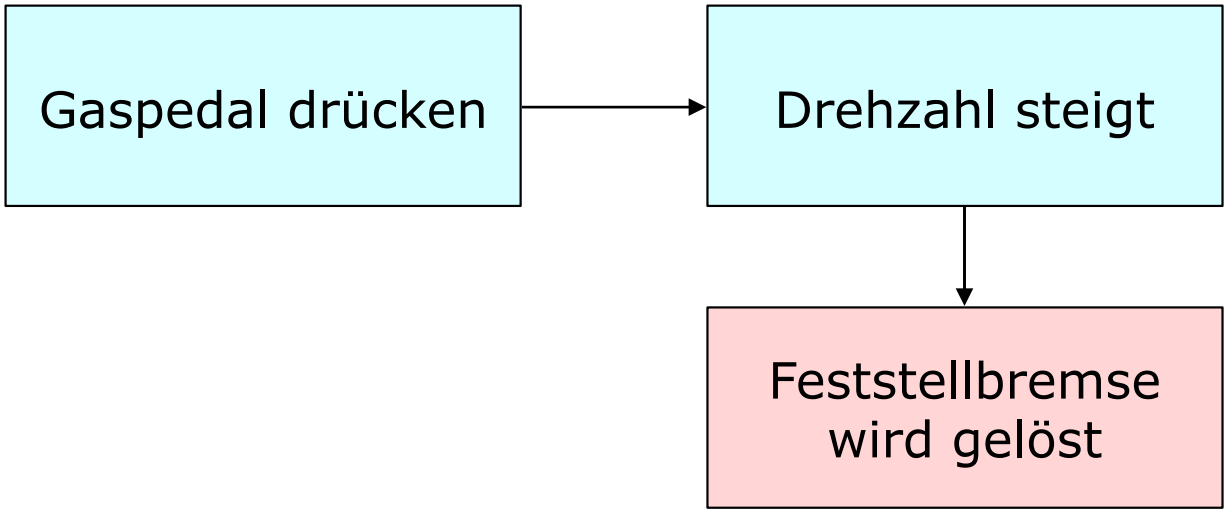


# Was der System-Entwickler dachte

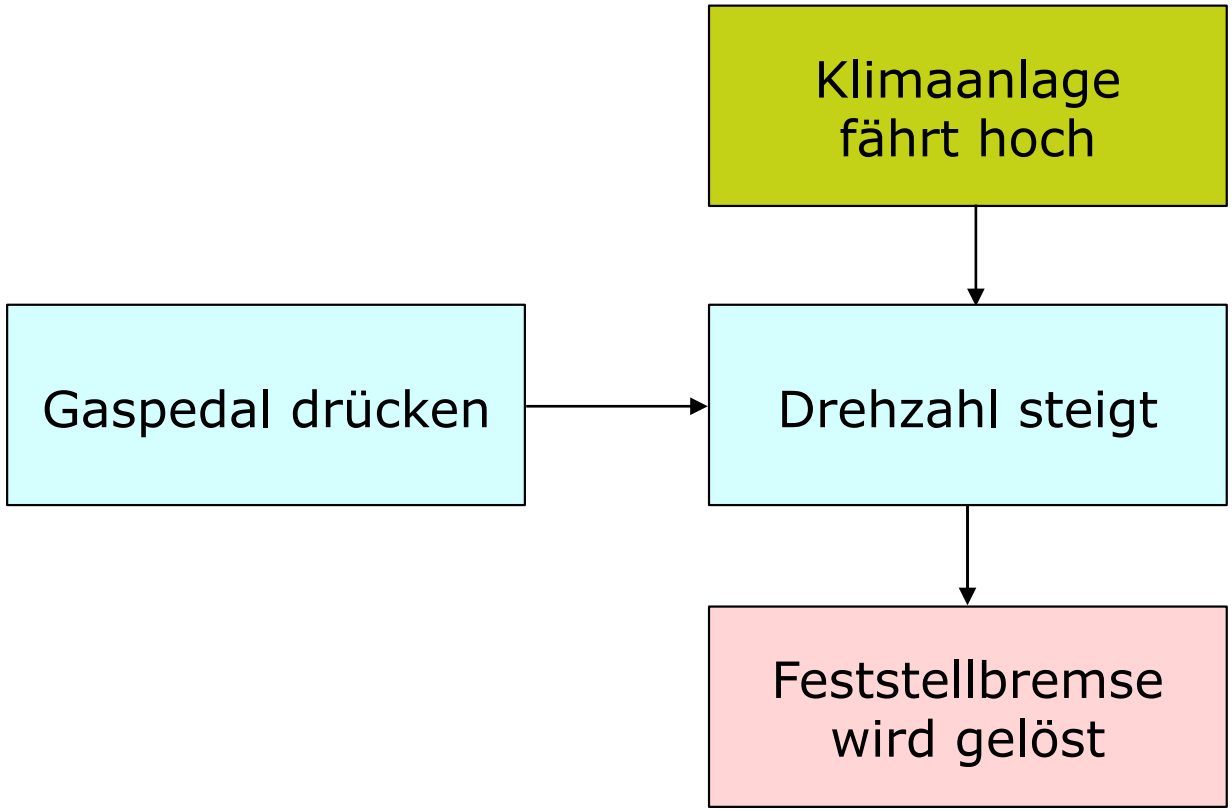


# Was der SW-Entwickler realisierte

- Kostenziel
- Gewichtssziel
- Drehzahl liegt schon auf CAN



# Was passierte

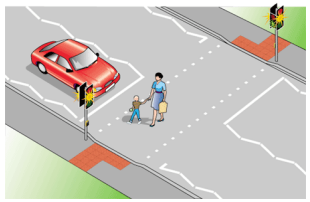


# Beispiel Micro-Hybrid Stop-Start Feature

- 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** 7

**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

Research & Advanced Engineering Thomas Rambow [19 Nov 2009]

# 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)
  - ...