

---

# FUNKTIONALE SICHERHEIT IN DER PRAXIS

2. Osnabrücker FuSi Forum, 29. und 30. November 2011, Osnabrück  
Erfahrungen in der Praxis, offene Punkte und Lösungen

---



## **Dr.-Ing. Alexander Schloske**

Abteilungsleiter Produkt- und Qualitätsmanagement

---

Telefon: +49(0)711/9 70-1890

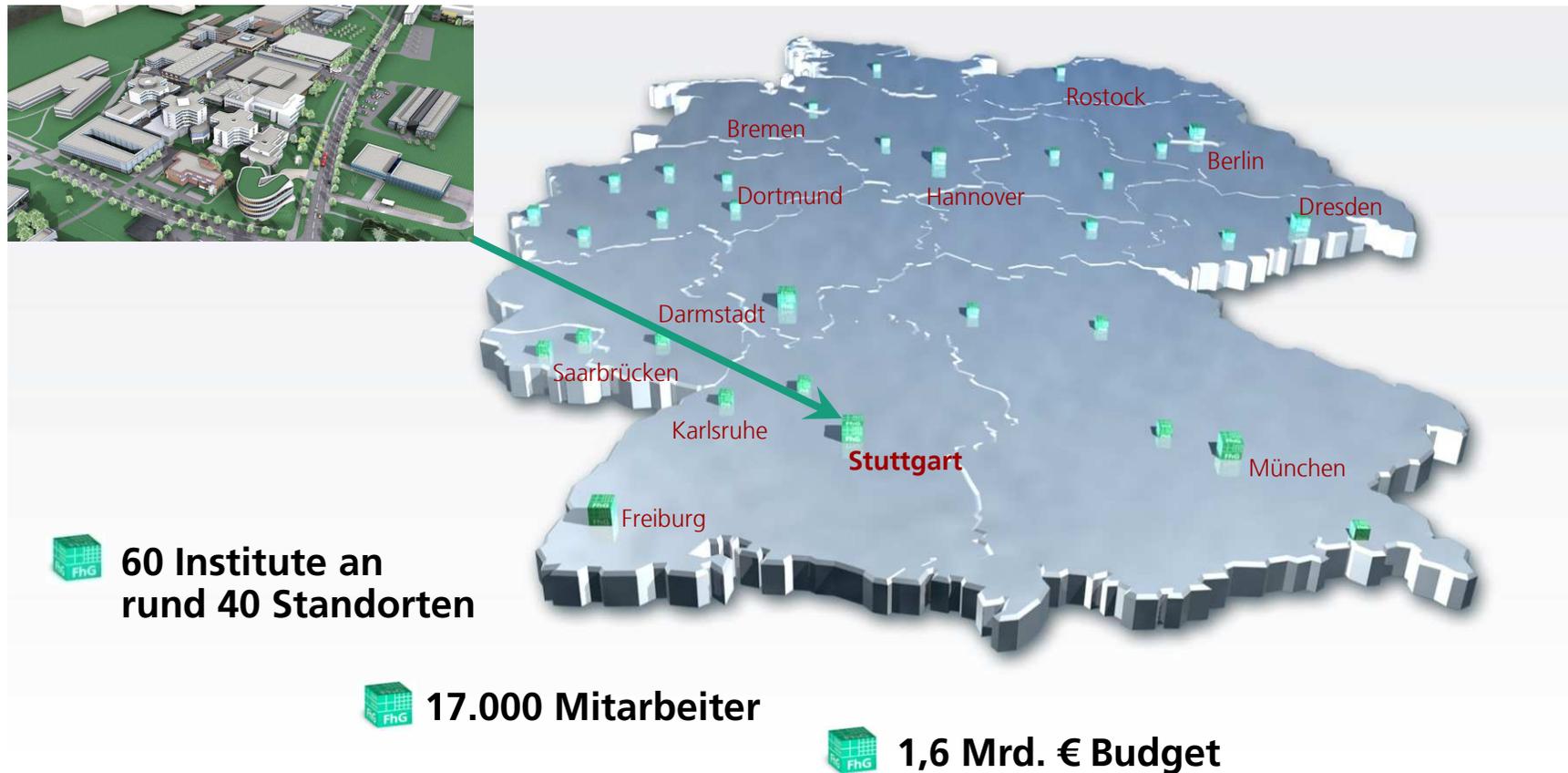
Fax: +49(0)711/9 70-1002

E-Mail: [alexander.schloske@ipa.fraunhofer.de](mailto:alexander.schloske@ipa.fraunhofer.de)

Internet: [www.ipa.fraunhofer.de](http://www.ipa.fraunhofer.de)



# Vorstellung Die Fraunhofer-Gesellschaft



# Vorstellung

## Das Fraunhofer-Institut für Produktionstechnik und Automatisierung (IPA), Stuttgart

<b>Institutsleitung:</b> Prof. Dr.-Ing. Thomas Bauernhansl Prof. Dr.-Ing. Alexander Verl		
<b>Unternehmensorganisation</b>	<b>Automatisierung</b>	<b>Oberflächentechnik</b>
<b>Digitale Fabrik</b> Dr.-Ing. Carmen Constantinescu	<b>Robotersysteme</b> Dipl.-Ing. Martin Hägele M.S.	<b>Lackiertechnik</b> Dipl.-Ing. Dieter Ondratschek
<b>Produkt- und Qualitätsmanagement</b> Dr.-Ing. Alexander Schloske	<b>Orthopädie und Bewegungssysteme</b> Dr. med. Urs Schneider	<b>Pigmente und Lacke</b> Dr.-Ing. Michael Hilt
<b>Fabrikplanung und Produktionsoptimierung</b> Dipl.-Ing. Michael Lickefett	<b>Produktions- und Prozessautomatisierung</b> Dr.-Ing. Jan Stallkamp	<b>Prozessengineering funktionaler Materialien</b> Dipl.-Ing. (FH) Ivica Kolaric, MBA
<b>Unternehmenslogistik und Auftragsmanagement</b> Dipl. oec. soc. Anja Schatz	<b>Reinst- und Mikroproduktion</b> Dr.-Ing. Dipl.-Phys. Udo Gommel	<b>Galvanotechnik</b> Dr.-Ing. Martin Metzner
<b>Refabrikation</b> Prof. Dr.-Ing. Rolf Steinhilper	<b>Technische Informationsverarbeitung</b> Dipl.-Inf. Markus Hüttel	<b>Anwendungszentrum Rostock</b>
	<b>Prüfsysteme</b> Dipl.-Ing. Joachim Montnacher	<b>Projektgruppe Bayreuth</b>
	<b>Generative Fertigung und Digitale Drucktechnik</b> Dipl.-Ing. Andrzej Grzesiak	<b>Fraunhofer Research Austria</b>
		<b>Projektgruppe Zilina</b>
		<b>Projekt Center PMI Budapest</b>

# Abteilung Produkt- und Qualitätsmanagement

## Thematische Ausrichtung

Life-Cycle-Konzepte und Life-Cycle-Methoden zur Optimierung von Produkten und Prozessen nach Qualität, Kosten, Zeit, Umwelt / Energie

Themenschwerpunkte:

- Managementsysteme
- Produktentwicklung
- Prozessoptimierung
- Risikomanagement
- Schadstoff- und Energiemanagement



4

# Tätigkeitsfeld in der Produktentwicklung

## Risikoanalysen mit Fehlermöglichkeits- und Einflussanalyse (FMEA)

Aufgabenstellung:

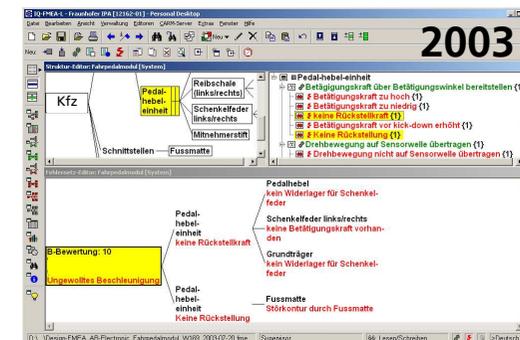
- Risikoabsicherung von Produkten und Prozessen

Tätigkeiten des IPA:

- Durchführung von Gefahren- und Risikoanalysen nach VDA 4 Kapitel 3 (2006) mit IQ-FMEA-RMX
- Definition von Verbesserungsmaßnahmen
- Erarbeitung von Testplänen und Testszenarien

Nutzen für Kunden:

- Sichere und zuverlässige Produkte und Prozesse



# Beispielprojekt zur Funktionalen Sicherheit

## Absicherung einer Sicherheitslogik im automotive Umfeld

Aufgabenstellung:

- Absicherung einer Sicherheitslogik für ein innovatives System in der Automobilindustrie
- Sicherstellung der „Funktionalen Sicherheit“ nach IEC 61508 und ISO 26262

Tätigkeiten des IPA:

- Durchführung von System-Risikoanalysen
- Definition von Software-Requirements
- Erarbeitung von Testplänen und Testszenarien



Bildquelle: [www.automobilrevue.de/detroit2002](http://www.automobilrevue.de/detroit2002)

# **FUNKTIONALE SICHERHEIT**

## **- EINFÜHRUNG -**

# Funktionale Sicherheit

## Pressevorführung - „Volvo-City-Safety“



Quelle: [www.auto.de](http://www.auto.de)

# Funktionale Sicherheit

## Beispiele aus der Realität zur „Funktionalen Sicherheit“

### ■ „Volvo-City-Safety“ versagt 2010 bei Pressevorführung

- Das City-Safety-System soll Hindernisse auf der Straße erkennen und das Auto automatisch abbremsen, um einen Zusammenstoß zu verhindern. Wie der Autohersteller später angab, war eine nicht funktionierende Batterie schuld am Ausfall des Systems.

Quelle: [www.auto.de](http://www.auto.de)



### ■ Renault ruft 2010 weltweit 695.000 Scénic zurück

- Bei diesem Modell kann es laut Renault zu einem unbeabsichtigten Anziehen der automatischen Parkbremse während der Fahrt kommen.

Quelle: [www.welt.de](http://www.welt.de)



### ■ Toyota ruft 2010 gezielt 373.000 Autos zurück

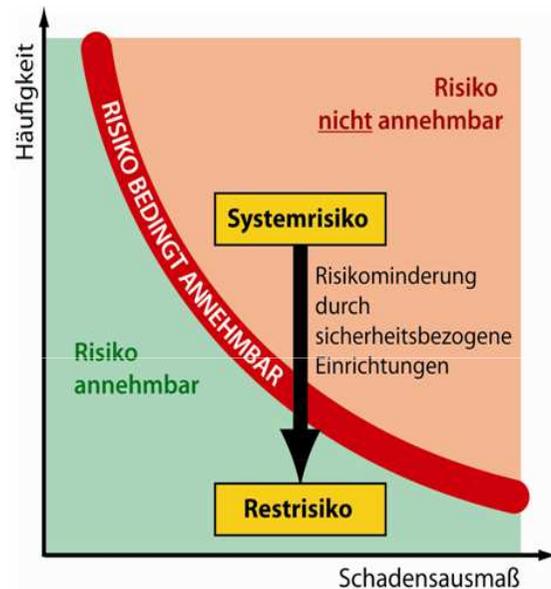
- Rückrufaktion auf Grund der Möglichkeit, dass während der Fahrt das Lenkradschloss selbsttätig einrastet. Damit ist das Lenken des Fahrzeugs nicht mehr möglich.

Quelle: <http://www.auto-motor-und-sport.de/>



# Funktionale Sicherheit

## Definition und Zielsetzung



Zielsetzung  
„Risikominderung“

Funktionale Sicherheit ist die Fähigkeit eines elektrischen, elektronischen od. programmierbarer elektronischen Systems (E/E/PE-System), beim Auftreten

- systematischer Ausfälle, z.B. fehlerhafte Systemauslegung
  - zufälliger Hardwareausfälle, z.B. Alterung von elektr(on)ischen Bauteilen
- mit gefahrbringender Wirkung, einen sicheren Zustand einzunehmen bzw. in einem sicheren Zustand zu bleiben.

# Vortragsinhalte

- Methoden zur Funktionalen Sicherheit
- Ermittlung von Kenngrößen zur Funktionalen Sicherheit
- Eingesetzte Methoden und deren Zusammenhang
- Erläuterung anhand von Beispielen

# METHODEN ZUR FUNKTIONALEN SICHERHEIT

---

12

# Methoden zur Funktionalen Sicherheit

## Methodenübersicht

### Methoden zur SIL-Klassifizierung

- Gefahren- und Risikoanalyse
- Risikograph

### Methoden zur Analyse systematischer Fehler

- Fehlermöglichkeits- und Einflussanalyse (FMEA)
- Fehlerbasierte System-Reaktionsanalyse (FSR)

### Methoden zur Analyse zufälliger Fehler

- Berechnungsalgorithmen und Vorgabewerte
- Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse (FMEDA)

# METHODEN ZUR SIL-KLASSIFIZIERUNG

---

14



# Methoden zur SIL-Klassifizierung

## Risikograph zur ASIL-Klassifizierung nach ISO 26262

		Exposure E		Controllability C			
		E0	E1	C0	C1	C2	C3
Severity S	S0	E0 – E4	QM	QM	QM	QM	QM
	S1	E0	QM	QM	QM	QM	QM
		E1	QM	QM	QM	QM	QM
		E2	QM	QM	QM	QM	QM
		E3	QM	QM	QM	QM	A
		E4	QM	QM	A	B	
	S2	E0	QM	QM	QM	QM	QM
		E1	QM	QM	QM	QM	QM
		E2	QM	QM	QM	QM	A
		E3	QM	QM	A	B	
		E4	QM	A	B	C	
	S3	E0	QM	QM	QM	QM	QM
		E1	QM	QM	QM	QM	A
		E2	QM	QM	A	B	
		E3	QM	A	B	C	
		E4	QM	B	C	D	

[nach ISO DIS 26262]

### Zielsetzung:

- Systematische Ermittlung des ASIL-Levels auf Basis der Gefahren- und Risikoanalyse

### Methodisches Vorgehen:

- Bestimmung des ASIL-Levels anhand
  - der Schwere (Severity)
  - der Häufigkeit des Ausgesetztseins (Exposure)
  - der Beherrschbarkeit (Controllability)

### Nutzen/Anmerkung:

- Systematisches und nachvollziehbares Vorgehen
- Basis für Vorgaben zur Methodenanwendung und für Zielwerte der weiteren Entwicklung

16

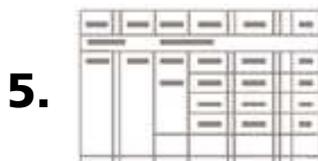
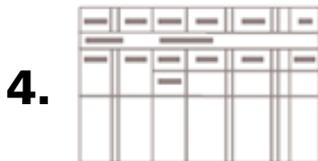
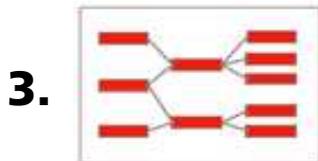
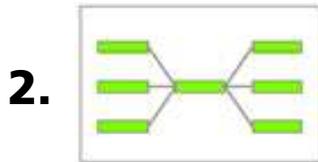
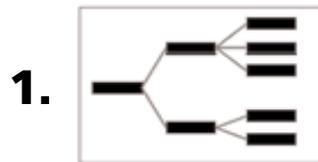
# METHODEN ZUR ANALYSE SYSTEMATISCHER FEHLER

---

17

# Methoden zur Analyse systematischer Fehler

## Fehlermöglichkeits- und Einflussanalyse (FMEA)



### Zielsetzung:

- Systematische Ermittlung potentieller Fehlfunktionen des betrachteten Systems

### Methode nach VDA 4 Kapitel 3 (2006):

- 1: Strukturanalyse (Strukturbaum)
- 2: Funktionsanalyse (Funktionsnetze)
- 3: Fehleranalyse (Fehlernetze)
- 4: Maßnahmenanalyse und Bewertung
- 5: Optimierung (falls notwendig)

### Nutzen/Anmerkung:

- Frühzeitige Ermittlung von Fahrsituationen, Funktionen und Erstellung von Funktionsnetzen
- Präzise Benennung der Fehlfunktionen
- Detaillierte Übersicht über Fehlfunktionen



# BERECHNUNGSALGORITHMEN UND VORGABEWERTE

---

20

# Kennwerte und Berechnungsalgorithmen der DIN 61508 für zufällige Fehler in Abhängigkeit vom SIL

## DIN EN 61508

Sicherheits-Integritätslevel SIL	Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (Wahrscheinlichkeit eines gefährbringenden Ausfalls pro Stunde) PFH
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

### Ausfallwahrscheinlichkeit

- PFH = Probability of Failures per Hour

Anteil ungefährlicher Ausfälle SFF	Fehlertoleranz der Hardware (siehe Anmerkung 2) HFT		
	0	1	2
< 60 %	nicht erlaubt	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
$\geq 99$ %	SIL3	SIL4	SIL4

ANMERKUNG 1 Siehe 7.4.3.1.1 bis 7.4.3.1.4 zu Einzelheiten bezüglich der Interpretation dieser Tabelle.

ANMERKUNG 2 Eine Fehlertoleranz der Hardware von N bedeutet, dass N + 1 Fehler zu einem Verlust der Sicherheitsfunktion führen können.

### Strukturelle Anforderungen

- SFF = Safe Failure Fraction
- HFT = Hardware Failure Tolerance

$$SFF = \frac{\Sigma\lambda_S + \Sigma\lambda_{DD}}{\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU}}$$

Anteil ungefährlicher Ausfälle (safe failure fraction)

- (D)angerous
- (S)afe
- (D)etected
- (U)ndetected

Quelle: DIN EN 61508<sub>21</sub>

# Kennwerte und Berechnungsalgorithmen der ISO 26262 für zufällige Fehler in Abhängigkeit vom ASIL

## ISO 26262-5, Annex E und G

$$\text{Single Point Fault metric} = 1 - \frac{\sum (\lambda_{\text{SPF}} + \lambda_{\text{RF}})}{\sum \lambda} = \frac{\sum (\lambda_{\text{MPF}} + \lambda_{\text{S}})}{\sum \lambda}$$

$$\text{Latent Fault metric} = 1 - \frac{\sum (\lambda_{\text{MPF Latent}})}{\sum (\lambda - \lambda_{\text{SPF}} - \lambda_{\text{RF}})} = \frac{\sum (\lambda_{\text{MPF perceived or detected}} + \lambda_{\text{S}})}{\sum (\lambda - \lambda_{\text{SPF}} - \lambda_{\text{RF}})}$$

where  $\sum_{\text{safety related HW elements}} \lambda_x$  is the sum of  $\lambda_x$  of the safety-related hardware elements of the item.

ASIL	PMHF	SPFM	LFM
A	< 10 <sup>-6</sup>	-	-
B	< 10 <sup>-7</sup>	≥ 90%	≥ 60%
C	< 10 <sup>-7</sup>	≥ 97%	≥ 80%
D	< 10 <sup>-8</sup>	≥ 99%	≥ 90%

### Legende:

PMHF = Probabilistic Metric for random Hardware Failures (PMHF)

SPFM = Single-point fault metric

LFM = Latent-fault metric

Quelle: ISO/DIS 26262-5<sub>22</sub>

# METHODEN ZUR ANALYSE ZUFÄLLIGER FEHLER

---

23

# Methoden zur Analyse zufälliger Fehler

## Failure Modes, Effects and Diagnostic Analysis (FMEDA)

**Sicherheitsziel 1: Keine ungewollte Aktivierung der EPS während der Fahrt**

**Komponenten der Sicherheitsfunktion**

Component	Failure Mode	Effect	Severity	Occurrence	Detection	Diagnosis	Reference for FIT	Remarks
IC-303M	20.00	IC-303M	20.00	IC-303M	20.00	IC-303M	IC-303M	IC-303M
IC-303M	20.00	IC-303M	20.00	IC-303M	20.00	IC-303M	IC-303M	IC-303M
IC-303M	20.00	IC-303M	20.00	IC-303M	20.00	IC-303M	IC-303M	IC-303M
IC-303M	20.00	IC-303M	20.00	IC-303M	20.00	IC-303M	IC-303M	IC-303M
IC-303M	20.00	IC-303M	20.00	IC-303M	20.00	IC-303M	IC-303M	IC-303M
IC-303M	20.00	IC-303M	20.00	IC-303M	20.00	IC-303M	IC-303M	IC-303M
IC-303M	20.00	IC-303M	20.00	IC-303M	20.00	IC-303M	IC-303M	IC-303M
IC-303M	20.00	IC-303M	20.00	IC-303M	20.00	IC-303M	IC-303M	IC-303M
IC-303M	20.00	IC-303M	20.00	IC-303M	20.00	IC-303M	IC-303M	IC-303M

**Komponenten der Sicherheitsfunktion**

5 - Failure Mode (S-scale / D-dangerous / H-hort care)  
 7 - Number of components in identical function  
 8 - Diesel FIT Rate  
 9 - Contribution of Failure Mode to FIT Rate  
 10 - Failure rate for failure mode  
 11 - Detectable (F-fyes)  
 12 - Diagnostic method  
 13 - Detection Level

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	
NAME	Value	Type	Function	Failure Mode	Effect	M	FT	% die	PM	FIT	Die	Diagnostic Level	SD	SU	DD	SU	Reference for FIT	Remarks	
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M
IC-303M	20.00	OK	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M	IC-303M

### Zielsetzung:

- Analyse der Fehlermodi der an der Sicherheitsfunktion beteiligten Komponenten

### Methode:

- Auflistung aller Abweichungen der an der Sicherheitsfunktion beteiligten Komponenten
- Bewertung der Abweichungen/Ausfälle
- Ermittlung der Fehlerraten

### Nutzen/Anmerkung:

- Tabellarisches Verfahren zur Berechnung der FuSi-Parameter (z.B. PMHF, Fault-Metriken)
- Pro Sicherheitsziel Erstellung einer FMEDA

# ERLÄUTERUNG ANHAND VON BEISPIELEN

---

25

# Erläuterung anhand von Beispielen

## Methoden zur Analyse systematischer und zufälliger Fehler



Bildquelle: [www.automobilrevue.de/detroit2002](http://www.automobilrevue.de/detroit2002)

Systematische Fehler mit der FMEA und FSR

- Fragestellungen:
  - Welche Fehler können in den Baugruppen und Bauteilen auftreten und wie wird darauf reagiert?
  - Wie gut funktionieren die Sicherheitsmechanismen?



Bildquelle: [www.seuffer.de](http://www.seuffer.de)

Zufällige Fehler mit der FMEA, FSR und FMEDA

- Fragestellungen:
  - Welche Fehlermodi haben die E/E-Komponenten und wie häufig können diese im Betrieb auftreten?
  - Wie wird auf die Fehlermodi im Betrieb reagiert?
  - Wie gut funktionieren die Sicherheitsmechanismen?

# SYSTEMATISCHE FEHLER ANHAND EINES BEISPIELS

27

# Erläuterung anhand eines Beispielsystems

## Beispielsystem (Fahrzeug und Werte zufällig gewählt)



**1965**



**20xx ?**

# Erläuterung anhand eines Beispielsystems

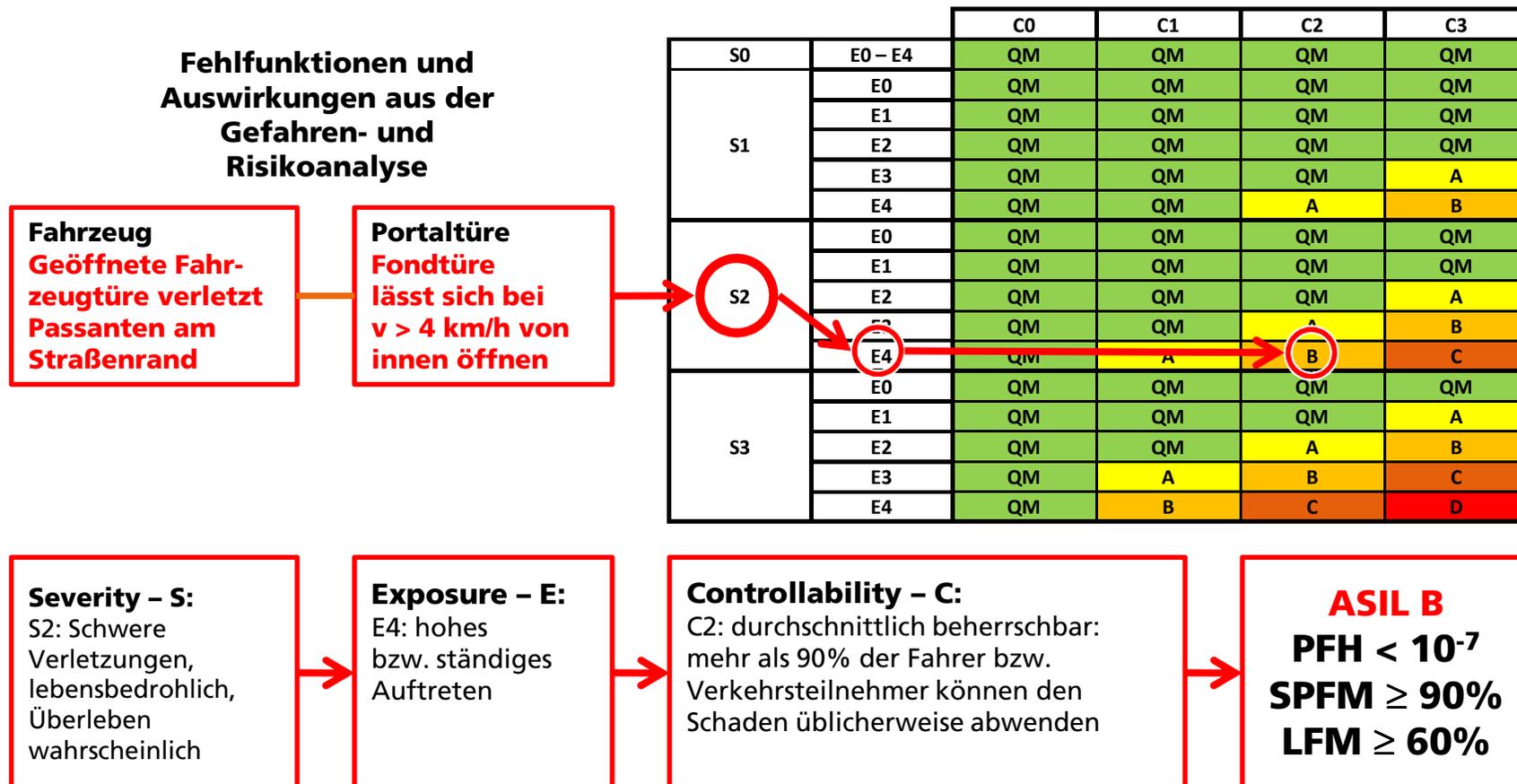
## Gefahren- und Risikoanalyse

The screenshot shows the IQ-RM PRO software interface. The top panel, 'Struktur-Editor: Struktur [System]', lists requirements for the 'Fahrzeug' system, with 'Portalüre' as a sub-component. The requirement 'Fondtüre lässt sich bei v > 4 km/h von innen öffnen' is highlighted in yellow. The bottom panel, 'Fehlernetz-Editor: Struktur [System]', displays a fault tree diagram. The top event is 'A ⚠️ Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand'. This event branches into two main conditions: 'v > 4 km/h und v ≤ 50 km/h' and 'v > 50 km/h und v ≤ 80 km/h'. The first condition branches into 'Landstraße' and 'Autobahn'. The second condition branches into 'Landstraße' and 'Autobahn'. A third condition, 'v > 80 km/h und v ≤ 120 km/h', also branches into 'Landstraße' and 'Autobahn'. A fourth condition, 'v > 120 km/h', is shown at the bottom. A yellow box highlights the requirement 'Fondtüre lässt sich bei v > 4 km/h von innen öffnen' in the fault tree diagram.

Hauptfunktion  
Hauptfehlfunktion

# Erläuterung anhand eines Beispielsystems

## Möglicher Risikograph gemäß ISO/DIS 26262



# Erläuterung anhand eines Beispielsystems

## Gefahren- und Risikoanalyse mit ASIL-Klassifizierung

The screenshot displays the IQ-RM PRO software interface. The top pane, 'Struktur-Editor: Struktur [System]', shows a tree view with 'Fahrzeug' and 'Portaltüre'. The middle pane, 'Fehlernetz-Editor: Struktur [System]', shows a fault tree diagram for the 'Portaltüre' function. The diagram includes nodes for 'Stadt', 'Landstraße', and 'Autobahn' with associated ASIL values and velocity conditions. A yellow box highlights the top event: 'Portaltüre & Fondtüre lässt sich bei v > 4 km/h von innen öffnen (ASIL-Max=B)'. The bottom pane shows the file path and system information.

**Struktur-Editor: Struktur [System]**

- ECE-R11 Anforderungen erfüllen
- Fahrer über nicht geschlossene (Fond)türe informieren
- Öffnen der Fondtüre von innen bei  $v > 4$  km/h sicher vermeiden
- ! Fondtüre lässt sich bei  $v > 4$  km/h von innen öffnen**
- Anforderungen für Produktsicherheit erfüllen
- Öffnen der Fondtüre von außen bei  $v > 4$  km/h sicher vermeiden
- Zuverlässigkeits-Anforderungen erfüllen
- Fahrer über Fehler im System sicher informieren

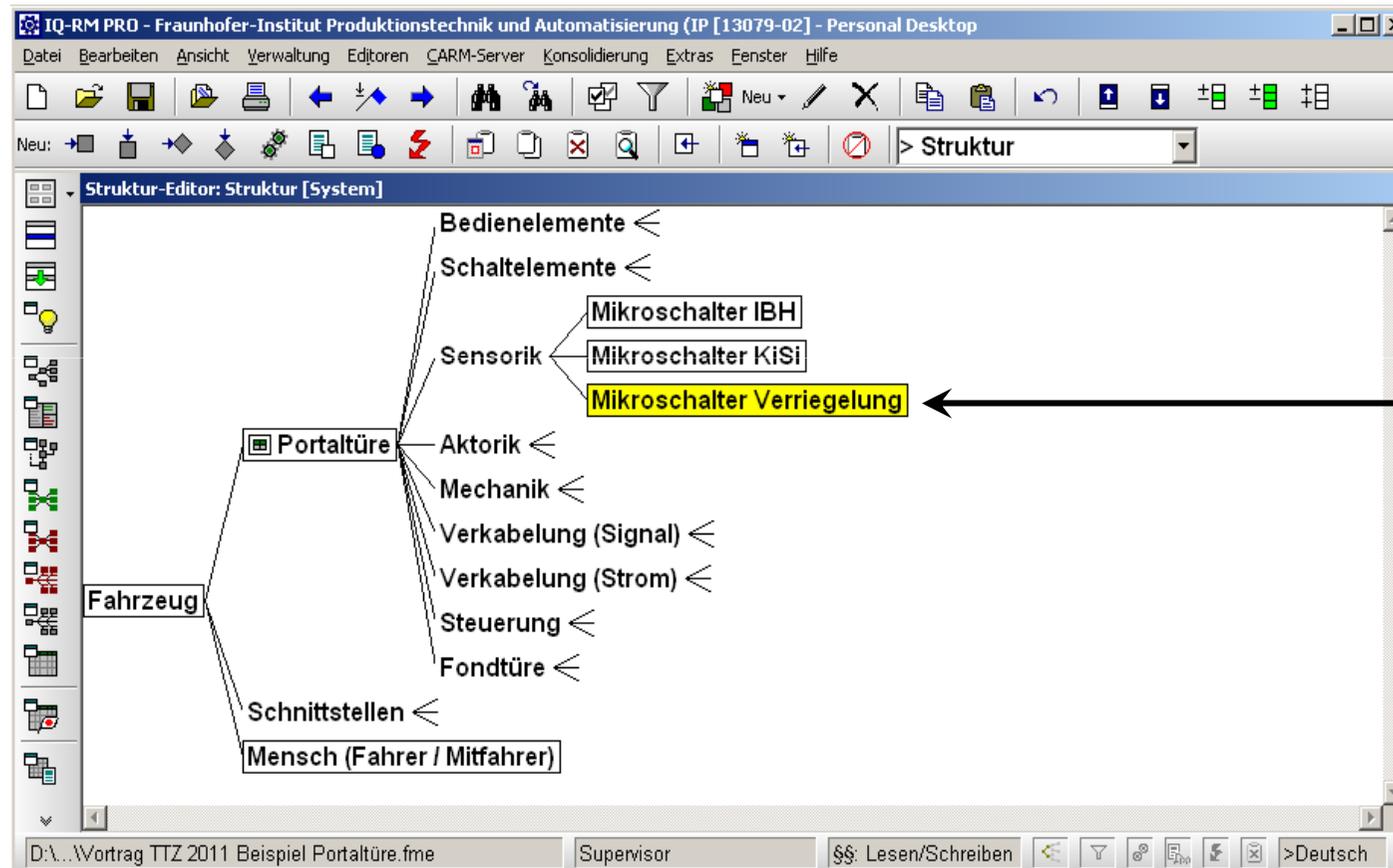
**Fehlernetz-Editor: Struktur [System]**

- Fahrzeug
  - Stadt
    - $v > 4$  km/h und  $v \leq 50$  km/h
      - 1. Schwere: S2
      - 2. Häufigkeit: E4
      - 3. Kontrollierbarkeit: C2
      - ! Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand (ASIL-Max=B)**
    - Landstraße (ASIL-Max=B)
    - Autobahn
  - Landstraße (ASIL-Max=A)
    - $v > 50$  km/h und  $v \leq 80$  km/h (ASIL-Max=A)
    - Autobahn
  - $v > 80$  km/h und  $v \leq 120$  km/h
    - $v > 120$  km/h (ASIL-Max=B)
- Portaltüre
  - ! Portaltüre & Fondtüre lässt sich bei  $v > 4$  km/h von innen öffnen (ASIL-Max=B)**

# **ANALYSE SYSTEMATISCHER FEHLER**

# Erläuterung anhand eines Beispielsystems

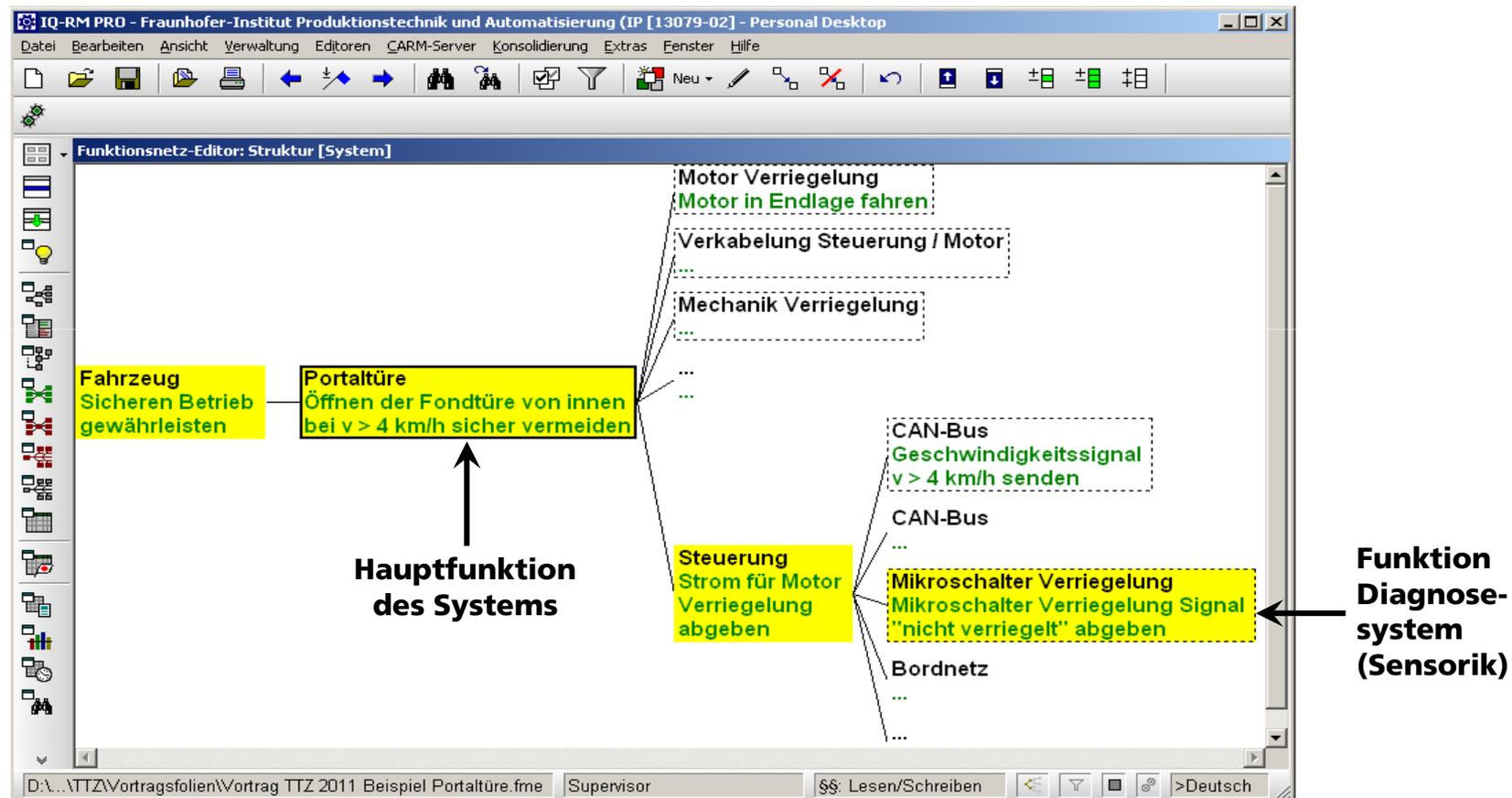
## Mögliche Systemstruktur einer „Portaltüre“



**Diagnose-  
system  
(Sensorik)**

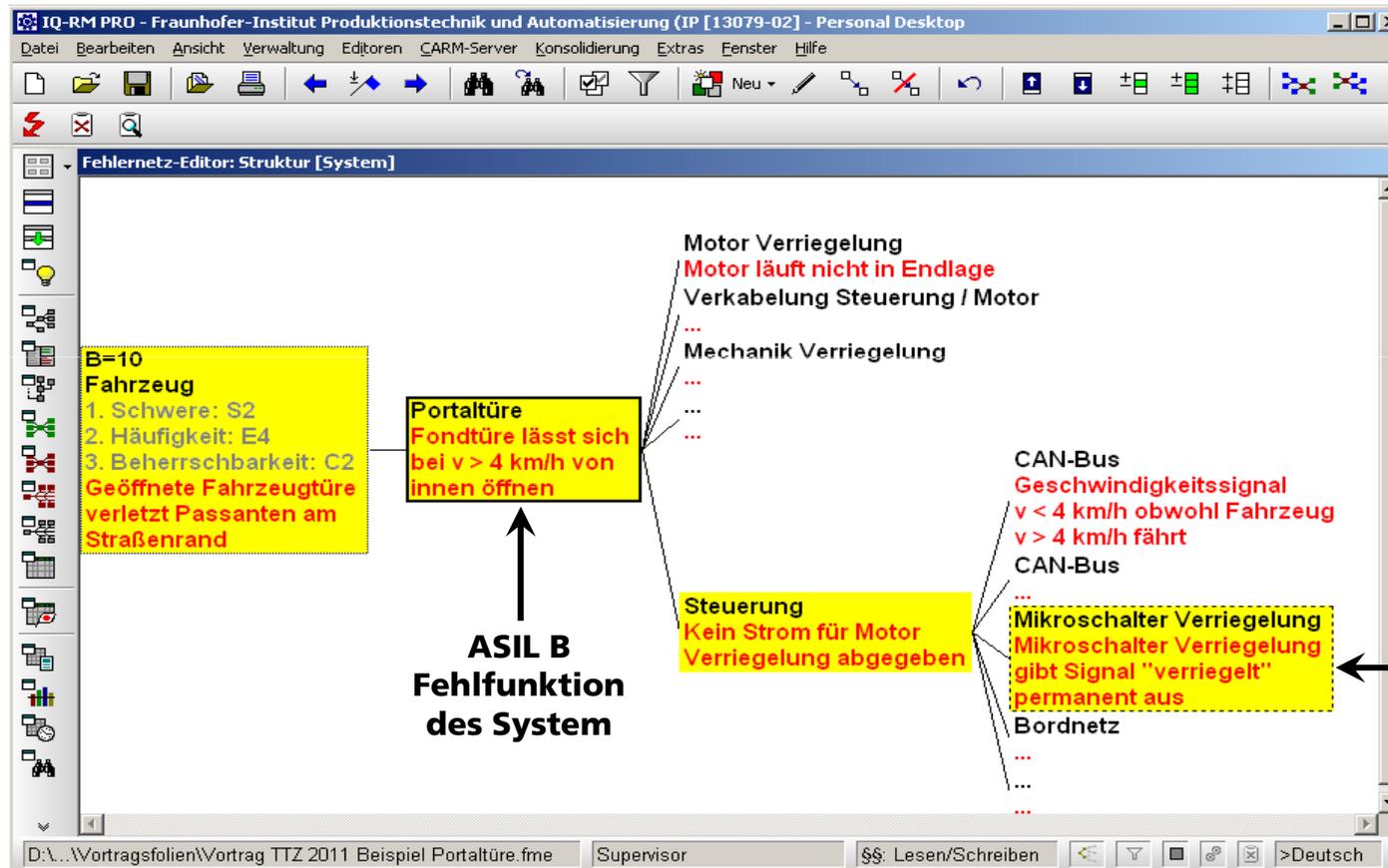
# Erläuterung anhand eines Beispielsystems

## Mögliches Funktionsnetz einer „Portaltüre“



# Erläuterung anhand eines Beispielsystems

## Mögliches Fehlernetz einer „Portaltüre“



# Erläuterung anhand eines Beispielsystems

## Mögliche FSR eines Diagnosesystems der „Portaltüre“

Microsoft Excel - FSR-Analyse ohne Diagnosecheck 2008-08-16.xls

Diagnosecheck

**Regeln:**

1. Elemente können nur ausfallen, wenn sie belastet sind
3. Elemente, die in einer vorgelagerten Phase unentdeckt ausfallen, werden in den nächsten Phasen weiter betrachtet

**Farben**

Kritisch / Unentdeckt  
 Kritisch / Entdeckt  
 Unkritisch / Unentdeckt  
 Unkritisch / Entdeckt

	B	E	F	G	J	K	L	M	N	S	T	Y
1	Auftreten aus FMEA	Motorstart	Einsteigen (hinten)	Verriegelung bei v > 4 km/h	Fahrt	v < 4 km/h ohne Türöffnung	v < 4 km/h mit Türöffnung	Aussteigen (hinten)	Verriegelung bei v > 4 km/h	Fahrt	Abstellen, Zündung aus	schlafender Fehler möglich
3												
4												
5												

Mikroschalter Verriegelung

Mikroschalter Verriegelung permanent auf "verriegelt"

Mikroschalter Verriegelung permanent auf "nicht verriegelt"

Mikroschalter Verriegelung

Bereit

# Erläuterung anhand eines Beispielsystems

## Mögliches Formblatt einer „Portaltüre“

Formblatt-Editor VDA 96 / VDA 06: Steuerung (Struktur [System])

Fehlerfolge	B	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RPZ	V/T		
Funktion: [Steuerung] Strom für Motor Verriegelung abgeben											
« 1/5 » [Portaltüre] Fondtüre lässt sich bei v > 4 km/h von innen öffnen		[Steuerung] Kein Strom für Motor Verriegelung abgeben	« 2/0 » [Mikroschalter Verriegelung] Mikroschalter Verriegelung gibt Signal "verriegelt" permanent aus	Maßnahmenstand - Anfang: Entwicklung		Widerstandskodierter Mikroschalter	3	Keine Entdeckung und keine Warnung im Betrieb möglich	10	300	
>> (ASIL=B) « 0/1 » [Fahrzeug] A Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand	10			Maßnahmenstand: Software-Requirements		Software-Requirement ID=SR120: Nach jeder Öffnung (Fondtüre) ist bei Überschreitung von v>4 km/h an beiden Fondtüren ein Verriegelungszyklus durchzuführen. Sollte dabei ein Mikroschalter keinen Signalwechsel haben ist die Warneinheit zu aktivieren.	1		10	(100) Schloske Software-Requirements in Umsetzung	
				Maßnahmenstand: Softwaretest		Test-Bench ID=TB080: Test, ob bei ausgefallenem Mikroschalter (li / re) während bzw. nach Türöffnung die Warneinheit aktiviert wird.	1		1	10	Mannuß Softwaretest abgeschlossen
				Maßnahmenstand: Betrieb		Sichere Entdeckung im Betrieb und Information des Kunden bei ausgefallenem Mikroschalter Verriegelung in allen Systemzuständen	1		1	10	Kunde Betrieb abgeschlossen

**Keine Erkennung der Fehlfunktion an der Sensorik im Betrieb und keine Information des Fahrers**

# Erläuterung anhand eines Beispielsystems

## Mögliches Formblatt einer „Portaltüre“

Formblatt-Editor VDA 96 / VDA 06: Steuerung (Struktur [System])

Fehlerfolge	B	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RPZ	V/T
Funktion: [Steuerung] Strom für Motor Verriegelung abgeben									
« 1/5 » [Portaltüre] Fondtüre lässt sich bei v > 4 km/h von innen öffnen		[Steuerung] Kein Strom für Motor Verriegelung abgeben	« 2/0 » [Mikroschalter Verriegelung] Mikroschalter Verriegelung gibt Signal "verriegelt" permanent aus	Maßnahmenstand - Anfang: Entwicklung					
>> (ASIL=B) « 0/1 » [Fahrzeug] A Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand	10			Widerstandskodierter Mikroschalter	3	Keine Entdeckung und keine Warnung im Betrieb möglich	10	300	
				Maßnahmenstand: Software-Requirements					
				Software-Requirement ID=SR120: Nach jeder Öffnung (Fondtüre) ist bei Überschreitung von v>4 km/h an beiden Fondtüren ein Verriegelungszyklus durchzuführen. Sollte dabei ein Mikroschalter keinen Signalwechsel haben ist die Warneinheit zu aktivieren.	1		10	(100)	Schloske Software-Requirements in Umsetzung
				Maßnahmenstand: Softwaretest					
				Test-Bench ID=TB080: Test, ob bei ausgefallenem Mikroschalter (li / re) während bzw. nach Türöffnung die Warneinheit aktiviert wird.	1		1	10	Mannuß Softwaretest abgeschlossen
				Maßnahmenstand: Betrieb					
				Sichere Entdeckung im Betrieb und Information des Kunden bei ausgefallenem Mikroschalter Verriegelung in allen Systemzuständen	1		1	10	Kunde Betrieb abgeschlossen

**Sichere Fehlererkennung der Sensorik im Betrieb und Information des Fahrers**

# Erläuterung anhand eines Beispielsystems

## Mögliches Formblatt einer „Portaltüre“

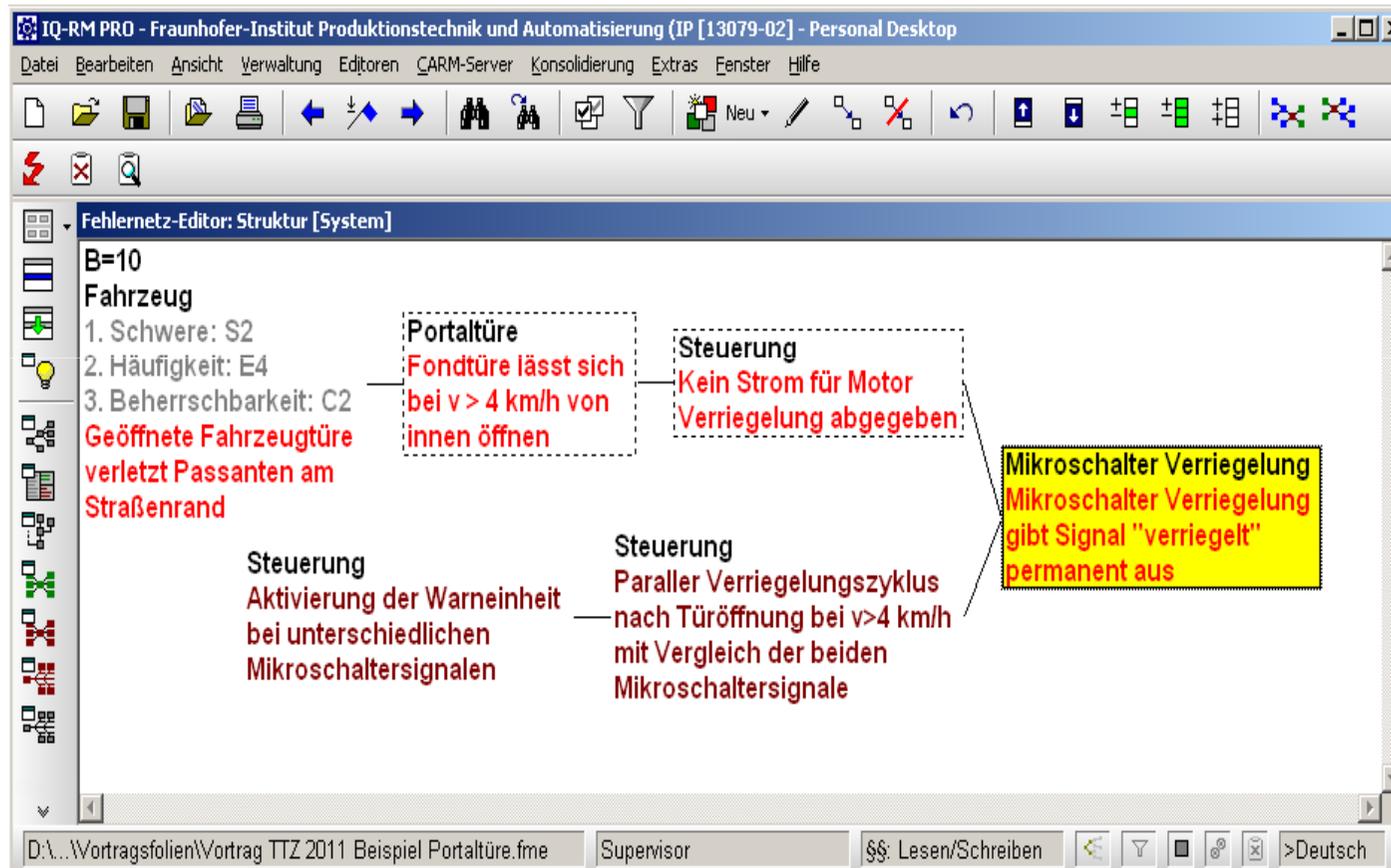
Formblatt-Editor VDA 96 / VDA 06: Steuerung (Struktur [System])

Fehlerfolge	B	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RPZ	V/T
<b>Funktion: [Steuerung]</b> <b>Strom für Motor Verriegelung abgeben</b>									
« 1/5 » [Portaltüre] Fondtüre lässt sich bei v > 4 km/h von innen öffnen		[Steuerung] Kein Strom für Motor Verriegelung abgeben	« 2/0 » [Mikroschalter Verriegelung] Mikroschalter Verriegelung gibt Signal "verriegelt" permanent aus	Maßnahmenstand - Anfang: Entwicklung					
>> (ASIL=B) « 0/1 » [Fahrzeug] A Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand	10			Widerstandskodierter Mikroschalter	3	Keine Entdeckung und keine Warnung im Betrieb möglich	10	300	
				Maßnahmenstand: Software-Requirements					
				Software-Requirement ID=SR120: Nach jeder Öffnung (Fondtüre) ist bei Überschreitung von v>4 km/h an beiden Fondtüren ein Verriegelungszyklus durchzuführen. Sollte dabei ein Mikroschalter keinen Signalwechsel haben ist die Warneinheit zu aktivieren.	1		10	(100)	Schloske Software-Requirements in Umsetzung
				Maßnahmenstand: Softwaretest					
				1 Test-Bench ID=TB080: Test, ob bei ausgefallenem Mikroschalter (li / re) während bzw. nach Türöffnung die Warneinheit aktiviert wird.	1		1	10	Mannuß Softwaretest abgeschlossen
				Maßnahmenstand: Betrieb					
				1 Sichere Entdeckung im Betrieb und Information des Kunden bei ausgefallenem Mikroschalter Verriegelung in allen Systemzuständen	1		1	10	Kunde Betrieb abgeschlossen

**Nachweis erbracht!**  
**Sichere Fehlererkennung an der Sensorik im Betrieb und Information des Fahrers**

# Erläuterung anhand eines Beispielsystems

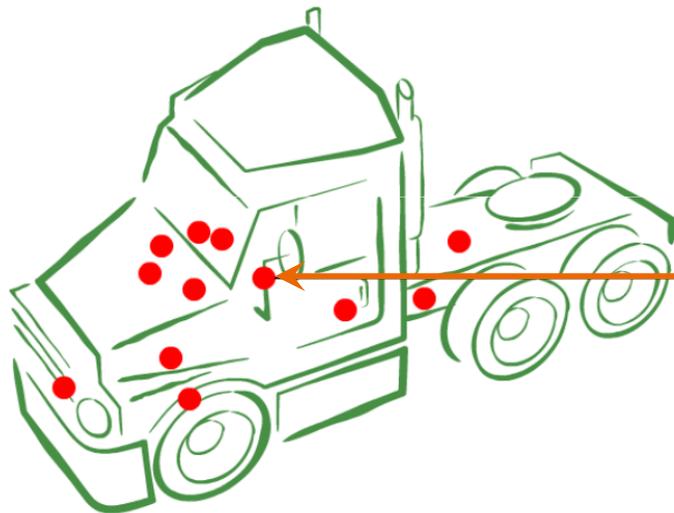
## Analyse und Bewertung von Fehlfunktionen, Fehlererkennung / Fehlerreaktion im System „Portaltüre“



# ANALYSE ZUFÄLLIGER FEHLER

# Erläuterung anhand eines Beispielsystems

## Drehschalter



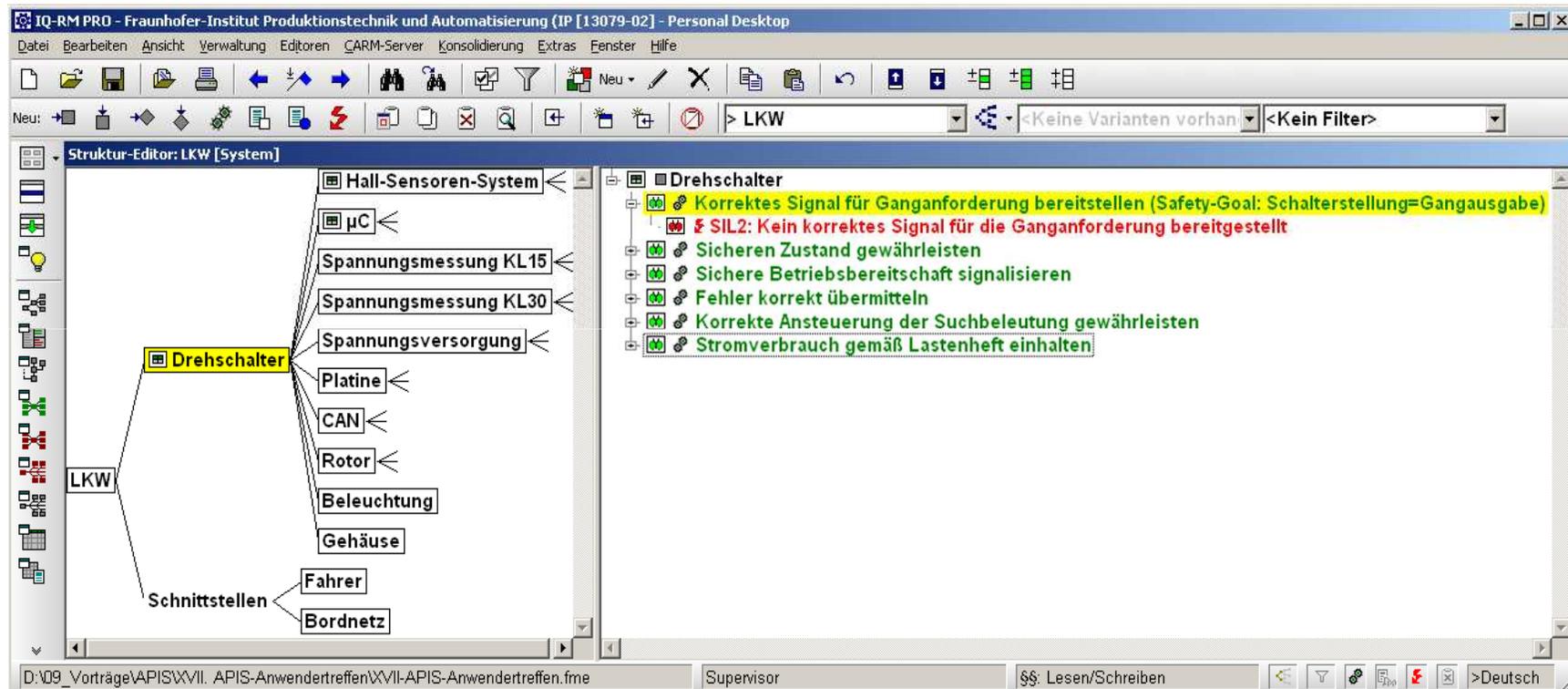
**Schaltechnologie  
mit Hall-Sensoren**

Projekt Drehschalter SIL 2  
PFH = 2% von PFH (SIL2) = 20 FIT  
SFF = 90%

Quelle: [www.seuffer.de](http://www.seuffer.de)<sub>42</sub>

# Erläuterung anhand eines Beispielsystems

## Systemstruktur Drehschalter und Safety Goal



# ERMITTLUNG DER FUSI-KENNWERTE FIT-WERTE / DIAGNOSEDECKUNG

# Erläuterung anhand eines Beispielsystems

## Ermittlung der Fehlermodi und Fehlerraten (zufällige Fehler) von E/E-Komponenten



Ermittlung der Fehlermodi und FIT-Werte von Systemelementen:

- Literatur zur Zuverlässigkeit
- Firmennormen (z.B. SN 29500)
- Zuverlässigkeitsbücher (z.B. MIL-Handbook 217)
- Herstellerangaben und Datenblätter
- Felderfahrungswerte
- Umrechnung auf Umgebungstemperaturen

**FIT = Failure in Time:**

Ausfallrate technischer Komponenten (Anzahl Bauteile, welche in  $10^9$  Stunden ausfallen). 1 FIT = 1 Ausfall in ca. 114.000 Jahren

# Erläuterung anhand eines Beispielsystems

## Ermittlung der Fehlermodi und Fehlerraten (zufälliger Fehler) von E/E-Komponenten

Seite/page 5  
SN 29500-4 : 2004-03

Tabelle 2 Ausfallraten für Widerstände  
Table 2 Failure rates for resistors

Widerstand / Resistor	$\lambda_{\text{ref}}$ in FIT	$\theta_1^{1)}$ in °C
Kohleschicht / Carbon film	≤100 kOhm	55
	>100 kOhm	
Metallschicht / Metal film	0,2	55
Netzwerke (Schichtschaltung) je Widerstandselement Networks (film circuits) per resistor element	Standard	55
	kundenspezifische / Custom design	
Metalloxidschicht / Metal-oxide	5	85
Draht / Wire-wound	5	85
Veränderbare / Variable	30	55
1 FIT = $1 \times 10^{-9}$ 1/h (ein Ausfall pro $10^9$ Bauelementestunden) 1) Oberflächentemperatur		1 FIT equals one failure per $10^9$ component hours 1) Resistor element temperature

Fehlermodi für Widerstände:

Open = 40%

Drift = 60%

**0,4 FIT (open)**

**0,6 FIT (drift)**

Quellen:  
SN 29500-4 (2004)  
Biolini (2007)<sup>46</sup>

# Erläuterung anhand eines Beispielsystems

## Ermittlung der Fehlermodi und Fehlerraten (zufälliger Fehler) von E/E-Komponenten



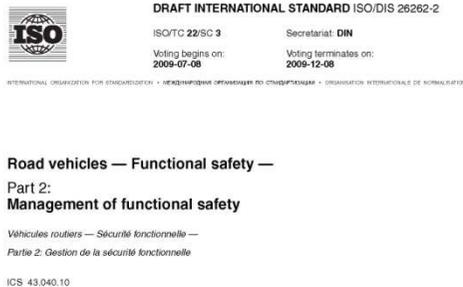
Verfahren zur Aufteilung von FIT-Werten bei komplexen Bauteilen (Typ B gemäß DIN EN 61508):

- 50/50-Aufteilung
- Aufteilung auf Funktionsgruppen
- Aufteilung nach Chipflächen
- Aufteilung nach Empfehlungen (z.B. Birolini, SN 29500)

Bildquelle: [www.kurz-elektronik.de](http://www.kurz-elektronik.de)<sup>47</sup>

# Erläuterung anhand eines Beispielsystems

## Ermittlung und Realisierung der Diagnosedeckungsgrade



### Ermittlung und Realisierung der Diagnosedeckungsgrade:

- Einfache Systeme und Fehlerfälle
  - Empfehlungen der IEC 61508
  - Empfehlungen der ISO 26262-5
- Komplexe Systeme und Fehlerfälle
  - Fehlerbasierte-Systemreaktionsanalyse (FSR)

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.  
Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.  
IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.  
RECORDS OF THIS DRAFT ARE KEPT TO BE AVAILABLE FOR INFORMATION TO ALL INTERESTED PARTIES. NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO TAKE APPROPRIATE ACTION IN THIS REGARD SHOULD BE REFERRED TO THE SECRETARIAT OF THE ORGANIZATION.

© International Organization for Standardization, 2009

# Erläuterung anhand eines Beispielsystems

## ISO 26262-5, Annex D (informative)

### Ermittlung von Diagnosedeckungsgraden (DC)

Ermittlung und Realisierung der Diagnosedeckungsgrade kann auf Basis von Empfehlungen der ISO/DIS 26262-5, Annex D (Tabelle 1-12 und Erläuterung D 2.1-D 2.11) erfolgen (z.B. ROM und Block replication)

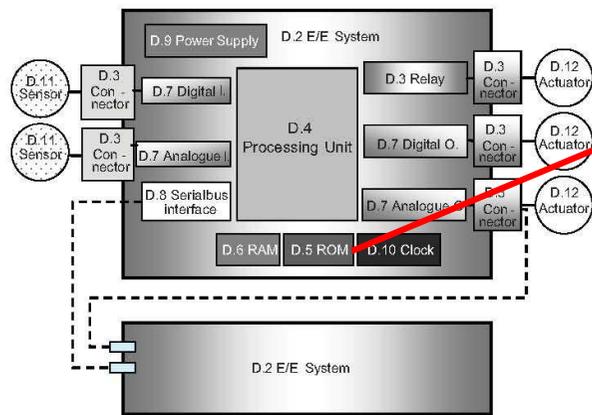


Table D.5 — Invariable memory ranges

Diagnostic technique/measure	See overview of techniques	Maximum diagnostic coverage considered achievable	Notes
Parity bit	-	Low	
Detection of memory data failures with error-detection-correction codes (EDC)	D.2.4.1	High	The effectiveness depends on the number of redundant bits.
Modified checksum	D.2.4.2	Low	-
Signature of one byte (8-bit) (CRC)	D.2.4.3	Medium	The effectiveness of the signature depends on the polynomial in relation to the block length of the information to be protected.
Signature of a double byte (16-bit) (CRC)	D.2.4.4	High	The effectiveness of the signature depends on the polynomial in relation to the block length of the information to be protected.
Block replication	D.2.4.5	High	-

#### D.2.4.5 Block replication (for example double memory with hardware or software comparison)

NOTE This technique/measure is referenced in Table D.5 and D.6.

Aim: To detect each bit failure.

Description: The address space is duplicated in two memories. The first memory is operated in the normal manner. The second memory contains the same information and is accessed in parallel to the first. The outputs are compared and a failure message is produced if a difference is detected. In order to detect certain kinds of bit errors, the data is to be stored inversely in one of the two memories and inverted once again when read.

Quelle: ISO/DIS 26262-5<sup>49</sup>

# BEISPIEL FIT-/DC-ERMITTLUNG FÜR EINEN EINFACHEN FEHLERFALL

---

50

Bit-Kipper 😊



# FIT-/DC-Ermittlung

## Einfacher Fehlerfall „Bit-Kipper im RAM“

The screenshot shows the IQ-RM PRO software interface. The main window displays a system structure editor for a truck (LKW) with components like RAM, EEPROM, Flash, CPU, Timer, CAN-Controller, PWM, Quarz, Latch, Datenrichtungsregister, AD-Wandler, Abblockkondensatoren, and Reset-Leitung. A yellow callout box highlights the failure rate for a bit flip in RAM:

**µC:**

- 86,94 FIT
- 27 Funktionen

**Ausfall je Funktion**

- 50% Safe
- 50% Dangerous

**-> 1,61 FIT je Ausfall**

# Einfacher Fehlerfall „Bit-Kipper im RAM“

## FMEA-Formblattinhalte (Beispiel nach DIN EN 61508)

The screenshot shows the 'Formblatt-Editor VDA 96 / VDA 06: µC (LKW [System])' window. The table contains the following data:

Fehlerfolge	B	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RP	Z	V/T
Funktion: [µC] Signale aller Hall-Sensor korrekt einlesen (Hall-Sensor) und auslesen (RAM)										
[Drehschalter] SIL2: Kein korrektes Signal für die Ganganforderung bereitgestellt	10	[µC] Signale der Hall-Sensoren werden nicht korrekt ausgelesen (RAM)	[RAM] (DCSPF=99,0%) (FR-Ist=1,6100 FIT) Bit-Kipper (der sicherheitsrelevanten Daten) im RAM	Maßnahmenstand - Anfang: Software-Requirement S-FMEA-V000830: Check des RAM (Test jeder Zelle mit den Bitmustern 0X55 und 0XAA) bei der Initialisierung Diagnose in der Initialisierungsphase	1		10	100		Schloske, Alexander 31.03.2011 SW-Freeze - C1-Muster abgeschlossen
>> (SIL=2) (SFF-Soll=90%) (PFH-Soll=20.000 FIT) [LKW] SIL2-Fehlfunktion				S-FMEA-V000720: Sicherheitsrelevante Daten werden doppelt in verschiedenen Adressbereichen und die Kopie zusätzlich invertiert abgelegt. Beim Einlesen und Zugriff erfolgt ein Vergleich. Diagnose im Betrieb, IEC 61508-7: Verfahren A.4.5						
				S-FMEA-V000730: Zyklischer CPU-Test des XOR-Befehls vor RAM-Check. IEC 61508-7: Verfahren A.3						
				S-FMEA-V000740: Bei Auftreten eines Fehlers im RAM erfolgt ein time-out. Diagnose im Betrieb						
				Maßnahmenstand: Software Test						
				S-FMEA-E000290: Test des CPU-Tests für den XOR-Befehl.	1		1	10		Maier, Christoph 22.04.2011 Modultest - C1 abgeschlossen
				S-FMEA-E000050: Modultest der RAM-Check-Routine sowie der Sicherstellung der Einnahme des sicheren Zustandes (time-out).						

Annotations and Labels:

- Komp./ Funktion Software-Requirements**: Points to the function row.
- Requirement ID**: Points to the ID 'S-FMEA-V000830'.
- Verfahren**: Points to 'IEC 61508-7: Verfahren A.4.5'.
- Maßnahmen zum Test der Software**: Points to the test measures section.
- Test-ID**: Points to 'S-FMEA-E000050'.
- Verifizierung im Rahmen der Entwicklung**: A central label with arrows pointing to the development phase measures.
- Erkennung / Reaktion Beherrschung im Betrieb (DC = High = 99%)**: A central label with arrows pointing to the operational phase measures.
- SFF-Soll** and **PFH-Soll**: Labels pointing to the failure rate columns.
- DC-Ist** and **FIT-Ist**: Labels pointing to the current failure rate columns.

# Einfacher Fehlerfall „Bit-Kipper im RAM“

## Fehlererkennung und Fehlerreaktion im Betrieb durch die Software

**Struktur-Editor: LKW [System]**

- Hall-Sensoren-System
  - Software
    - Sicherheitsrelevante Daten werden doppelt in verschiedenen Adressbereichen und die Kopie zusätzlich invertiert abgelegt.
    - Bei Auftreten eines Fehlers im RAM erfolgt ein time-out.
    - RAM
      - Korrekte Datenhaltung (der sicherheitsrelevanten Daten) während der Laufzeit ermöglichen
      - (DCSPF=99,0%) (FR-Ist=1,6100 FIT) **Bit-Kipper (der sicherheitsrelevanten Daten) im RAM**
      - (DCSPF=99,0%) (FR-Ist=1,6100 FIT) **Zeitdefekt (der sicherheitsrelevanten Daten) im RAM**
      - (FR-Ist=1,6100 FIT) **QM: Korrekte Datenhaltung wird während der Laufzeit durchgeführt**

**Fehlernetz-Editor: LKW [System]**

- LKW
  - SIL2-Fehlfunktion (SIL=2) (SFF-Soll=90%) (PFH-Soll=20,000 FIT) **1%**
  - Drehschalter
    - SIL2: Kein korrektes Signal für die Ganganforderung bereitgestellt
  - µC
    - Signale der Hall-Sensoren werden nicht korrekt ausgelesen (RAM)
  - Software
    - Bei Auftreten eines Fehlers im RAM erfolgt ein time-out. **99%**
  - RAM
    - Bit-Kipper (der sicherheitsrelevanten Daten) im RAM (DCSPF=99,0%) (FR-Ist=1,6100 FIT)

**Erkennung / Reaktion im Betrieb (DC = High = 99%)**

**Reaktion im Betrieb**

**Erkennung im Betrieb**

# BEISPIEL FIT-/DC-ERMITTLUNG FÜR EINEN KOMPLEXEN FEHLERFALL

---

55

# FIT-/DC-Ermittlung

## Komplexer Fehlerfall „Fehler im Hall-Sensoren-System“

The screenshot displays the IQ-RM PRO software interface. The main window is titled "Struktur-Editor: LKW [System]". On the left, a hierarchical tree structure shows the system components:

- Hall-Sensoren-System (highlighted in yellow)
  - µC
  - Spannungsmessung KL15
  - Spannungsmessung KL30
  - Spannungsversorgung
  - Drehschalter
    - Platine
    - CAN
    - Rotor
    - Beleuchtung
    - Gehäuse
  - Schnittstellen
    - Fahrer
    - Bordnetz

On the right, a list of detected faults is shown under the heading "Position der Magneten korrekt erkennen". The faults are:

- (DCSPF=99.0%) (FR-Ist=2,0400 FIT) ⚠ Wechsel von N zu einer Fahrstufe (D od. R) wird nicht korrekt erkannt
- (DCSPF=99.0%) (FR-Ist=2,0400 FIT) ⚠ Wechsel von einer Fahrstufe (D od. R) zu N wird nicht korrekt erkannt
- ⚠ Wechsel von einem Schleichgang (DC od. RC) zu einer Fahrstufe (D oder R) wird nicht korrekt erkannt
- ⚠ Wechsel von einer Fahrstufe (D od. R) in einen Schleichgang (DC oder RC) wird nicht korrekt erkannt

The status bar at the bottom shows the file path "D:\09\_Vorträge\APIS\XVII. APIS-Anwendertreffen\XVII-APIS-Anwendertreffen.fme", the user "Supervisor", and the language "Deutsch".

# Komplexer Fehlerfall „Fehler im Hall-Sensoren-System“

## DC-Ermittlung über FSR für Hall-Sensoren-System

Nr.	Ausgangsstellung					Sensorensignale							Endstellung					Sensorensignale							Gangausgabe			Fehlerentdeckung					
	RC	R	N	D	DC	RC	R'	R	N'	N	D'	D	DC	RC	R	N	D	DC	RC	R'	R	N'	N	D'	D	DC	Ausgabe	SIL-kritisch	Regel	nein	sofort	nächstes N	nächstes D/R
1			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	1	1	1	N	nein	1	x			
2			x			1	1	1	0	0	1	1	1			X			1	1	1	0	0	1	1	1	N	nein	1	x			
3			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	1	1	1	N	nein	1	x			
4			x			1	1	1	0	0	1	1	1			x			1	1	1	0	1	1	1	1	k.A.	nein	2				x
5			x			1	1	1	0	0	1	1	1			x			1	1	1	1	0	1	1	1	k.A.	nein	2				x
6			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	1	1	1	N	nein	1	x			
7			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	1	1	1	N	nein	1	x			
8			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	1	1	1	N	nein	1	x			
9			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	1	1	0	k.A.	nein	3		x		
10			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	1	0	1	k.A.	nein	3				R
11			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	0	1	1	k.A.	nein	3				R
12			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	1	1	1	N	nein	1				x
13			x			1	1	1	0	0	1	1	1			x			1	1	1	0	0	1	1	1	N	nein	1				x
14			x			1	1	1	0	0	1	1	1			x			1	1	0	0	0	1	1	1	k.A.	nein	3				D
15			x			1	1	1	0	0	1	1	1			x			1	0	1	0	0	1	1	1	k.A.	nein	3				D
16			x			1	1	1	0	0	1	1	1			x			0	1	1	0	0	1	1	1	k.A.	nein	3		x		

**Legende:**

0	Sensor aktiv	0	Sensor fehlerhaft aktiv
1	Sensor inaktiv	1	Sensor fehlerhaft inaktiv

$$DC = \frac{\Sigma DD}{\Sigma DD + \Sigma DU}$$

# Komplexer Fehlerfall „Fehler im Hall-Sensoren-System“

## FMEA-Formblattinhalte

Formblatt-Editor VDA 96 / VDA 06: Hall-Sensoren-System (LKW [System])

Fehlerfolge	B	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RP Z	V/T
Systemelement: Hall-Sensoren-System									
Beteiligt an SIL-Funktion									
Funktion: [Hall-Sensoren-System]									
Position der Magneten korrekt erkennen									
[Dreheschalter] SIL2: Kein korrektes Signal für die Ganganforderung bereitgestellt	10	[Hall-Sensoren-System] (DCSPF=99,0%) (FR-Ist=2,0400 FIT) <b>Wechsel von einer Fahrstufe (D od. R) zu N wird nicht korrekt erkannt</b>	[Hall-Sensor] (DCSPF=99,0%) (FR-Ist=4,2000 FIT) Stuck at 0, Stuck at 1 und Drift	Maßnahmenstand - Anfang: Software-Requirement	1		10	100	Schloske, Alexander 31.03.2011 SW-Freeze - C1-Muster abgeschlossen
>> (SIL=2) (SFF-Soll=90%) (PFH-Soll=20,000 FIT) [LKW] SIL2-Fehlfunktion				S-FMEA-V000690: Regeln zum Fahrstufenwechsel (siehe Dokument xyz: Regeln zum Fahrstufenwechsel.PPTX) Diagnose im Betrieb	1				
				S-FMEA-V000700: Fehlerbasierte System-Reaktionsmatrix (FSR) zur sofortigen Erkennung bzw. Erkennung innerhalb des Diagnoseintervalls mit zusätzlicher Sensorsignalsplausibilisierung (siehe Dokument FSR YY-MM-DD.XLSX) Diagnose im Betrieb	1				
				Maßnahmenstand: Software-Test	1		1	10	Maier, Christoph 22.04.2011 Modul-test - C1 abgeschlossen

**Sichere Fehlererkennung der Hallensoren im Betrieb und Information des Fahrers (DC = High = 99%)**

**Nachweis erbracht!**  
**Sichere Fehlererkennung der Hallensoren im Betrieb**

58

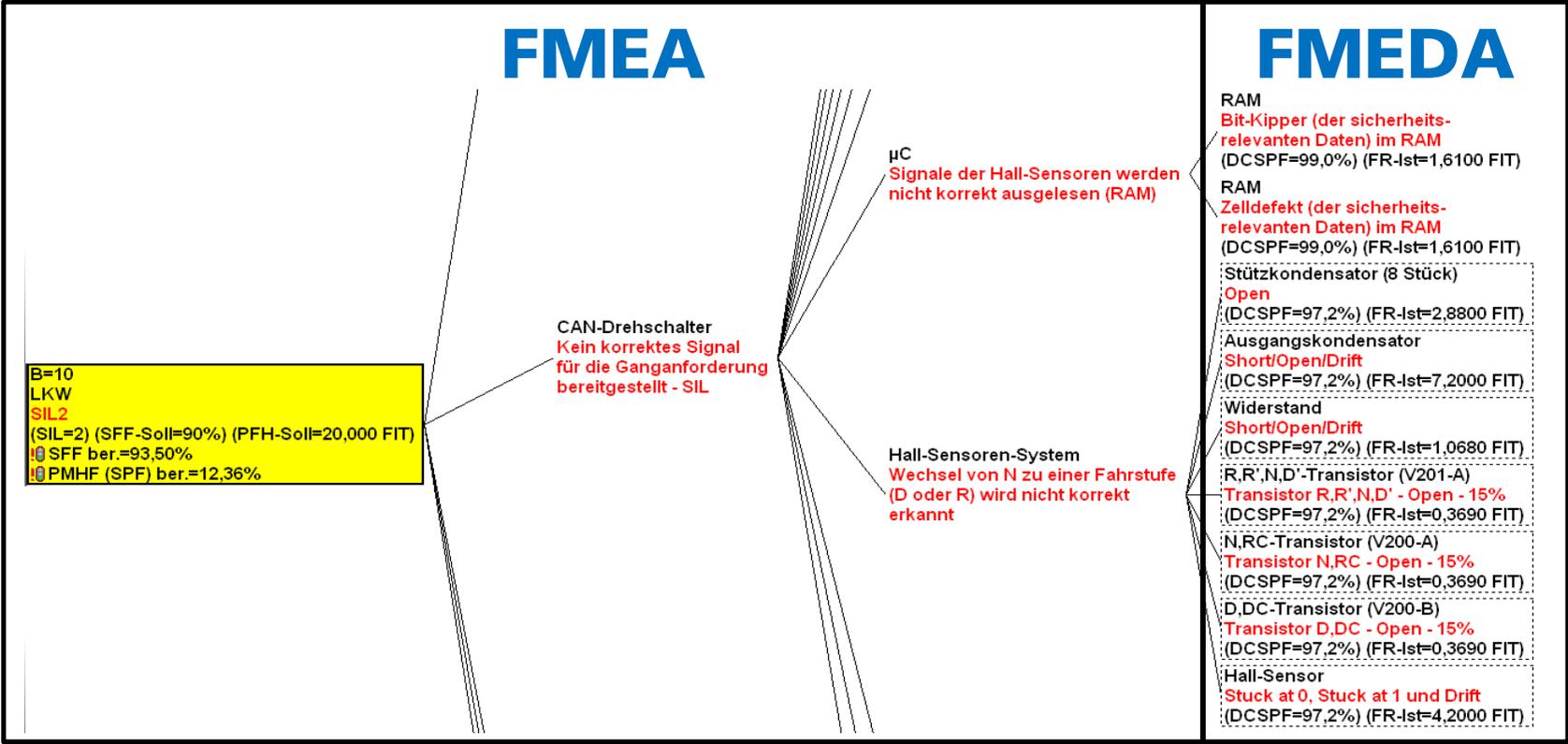
# FMEA UND FMEDA

# Analyse systematischer und zufälliger Fehler

## Aufgabenteilung zwischen FMEA (systematische Fehler) und FMEDA (zufällige Fehler)

### Systematische Fehler

### Zufällige Fehler



# Analyse zufälliger Fehler

## FMEDA

IQ-RM PRO - Fraunhofer-Institut Produktionstechnik und Automatisierung (IP [13079-02] - Personal Desktop)

Datei Bearbeiten Ansicht Verwaltung Editoren CARM-Server Konsolidierung Extras Fenster Hilfe

Neu: > LKW <Keine Varianten vorhanden> <Kein Filter>

FMEDA-Formblatt: LKW [System]

Systemelement	Funktion	Fehlerart	FA FIT	Entdeckbar	Diagnose	DC	SD	SU	DD	DU
RAM	Korrekte Datenhaltung (der sicherheitsrelevanten Daten) während der Laufzeit ermöglichen	Zelldefekt (der sicherheitsrelevanten Daten) im RAM	1,6100	Ja	<p>S-FMEA-V000830: Check des RAM (Test jeder Zelle mit den Bitmustern 0X55 und 0XAA) bei der Initialisierung</p> <p>S-FMEA-V000720: Sicherheitsrelevante Daten werden doppelt in verschiedenen Adressbereichen und die Kopie zusätzlich invertiert abgelegt. Beim Einlesen erfolgt ein Vergleich. Des Weiteren erfolgt ein Vergleich beim Zugriff auf die Daten.</p> <p>S-FMEA-V000730: Zyklischer CPU-Test des XOR-Befehls vor RAM-Check.</p> <p>S-FMEA-V000740: Bei Auftreten eines Fehlers im RAM wird der sichere Zustand eingenommen (Time-out).</p> <p>S-FMEA-E000290: Test des CPU-Tests für den XOR-Befehl.</p> <p>S-FMEA-E000050: Modultest der RAM-Check-Routine sowie der Sicherstellung der Einnahme des sicheren Zustandes.</p>	99,0			1,59	0,02

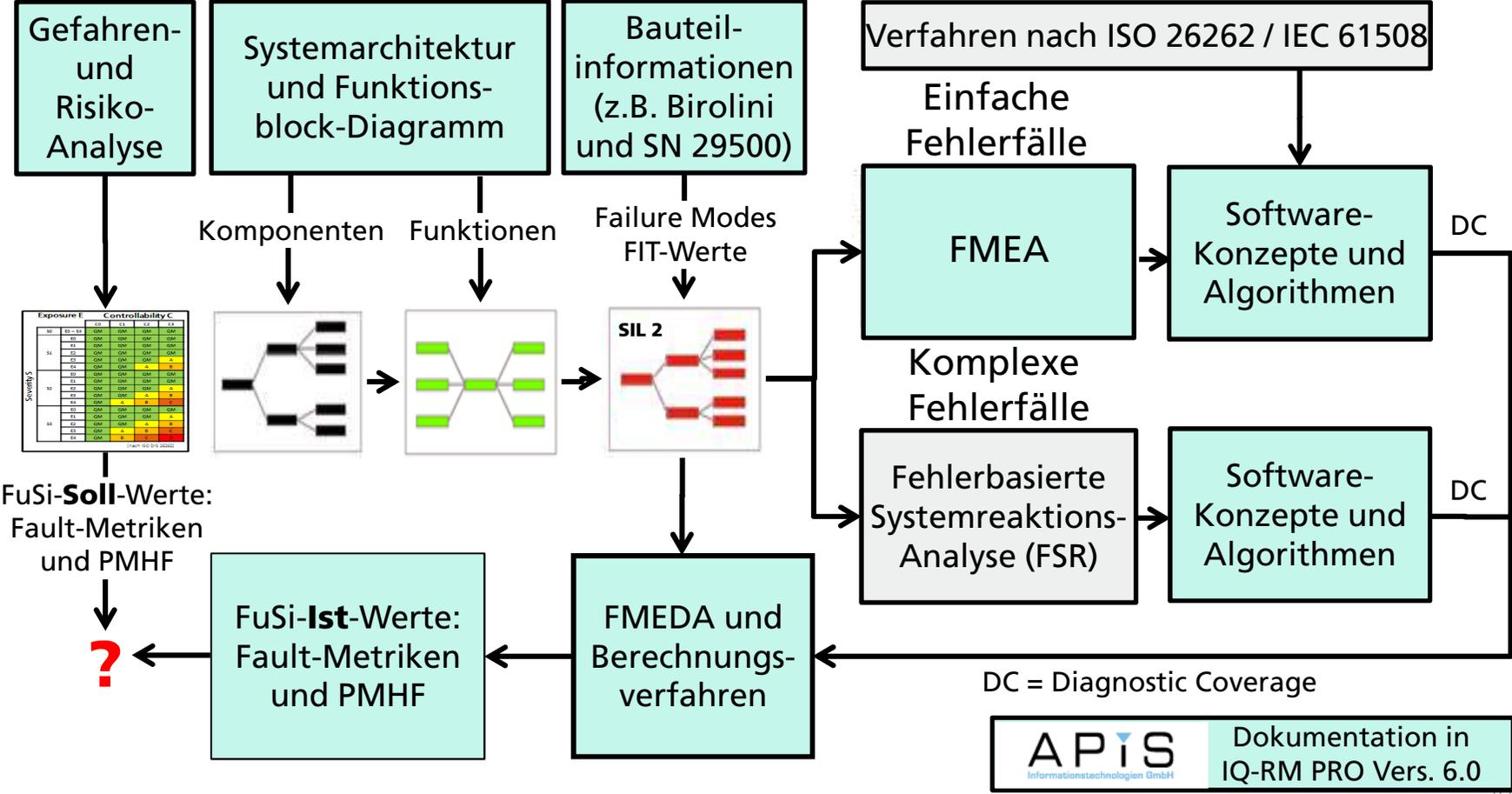
D:\... \APIS\XVII. APIS-Anwendertreffen\XVII-APIS-Anwendertreffen.fme 99 Systemelemente Supervisor §§ Lesen/Schreiben >Deutsch

# VORGEHENSWEISE ZUR ANALYSE ZUFÄLLIGER FEHLER

---

62

# Zusammenhang zwischen den eingesetzten Methoden Vorgehensweise zur Analyse und Absicherung funktional sicherer mechatronischer Systeme



# Analyse funktional sicherer mechatronischer Systeme

## Vergleich zwischen Soll-Werten und Ist-Werten in der IQ-RM PRO Version 6.0.0.7.0

**Fehlernetz-Editor: LKW [System]**

**Fehlfunktion: SIL2-Fehlfunktion**

FTA | Klassifikation | Bemerkung | Info | Ratgeber | ppm pro Zeiteinheit

Name | Bewertung | Attribute | Benutzerdefinierte Attribute | Funktionale Sicherheit

SOLL-Werte (Anforderungen):

SIL/ASIL: **SIL 2**

SEF/SPFM/LFM (0-100%): 90

PFH (FIT): 20,0  
(1 FIT = 1\*10e-3 pro Stunde)

Ist-Werte:

DCSPF (0-100%):

DQLF (0-100%):

FR = Fehlerrate (FIT):

Fehlertoleranzzeit (FTT) in ms:

Lambda-Werte:

Anteil entdeckbarer Ausfälle:

Anteil nicht entdeckter Ausfälle:

Werte zurücksetzen

OK | Abbruch | Hilfe

**B=10  
LKW  
SIL2  
(SIL=2) (SFF-Soil=90%) (PFH-Soil=20,000 FIT)  
SFF ber.=93,50%  
PMHF (SPF) ber.=12,36%**

**µC**  
Signale der Hall-Sensoren werden nicht korrekt ausgelesen (RAM)

**Hall-Sensoren-System**  
Wechsel von N zu einer Fahrstufe (D oder R) wird nicht korrekt erkannt (DCSPF=97,2%)

**RAM**  
Bit-Kipper (der sicherheitsrelevanten Daten) im RAM (DCSPF=99,0%) (FR-Ist=1,6100 FIT)

**RAM**  
Zelldefekt (der sicherheitsrelevanten Daten) im RAM (DCSPF=99,0%) (FR-Ist=1,6100 FIT)

Stützkondensator (8 Stück)  
**Open** (DCSPF=97,2%) (FR-Ist=2,8800 FIT)

Ausgangskondensator  
**Short/Open/Drift** (DCSPF=97,2%) (FR-Ist=7,2000 FIT)

Widerstand  
**Short/Open/Drift** (DCSPF=97,2%) (FR-Ist=1,0680 FIT)

R,R',N,D'-Transistor (V201-A)  
**Transistor R,R',N,D' - Open - 15%** (DCSPF=97,2%) (FR-Ist=0,3690 FIT)

N,RC-Transistor (V200-A)  
**Transistor N,RC - Open - 15%** (DCSPF=97,2%) (FR-Ist=0,3690 FIT)

D,DC-Transistor (V200-B)  
**Transistor D,DC - Open - 15%** (DCSPF=97,2%) (FR-Ist=0,3690 FIT)

Hall-Sensor  
**Stuck at 0, Stuck at 1 und Drift** (DCSPF=97,2%) (FR-Ist=4,2000 FIT)

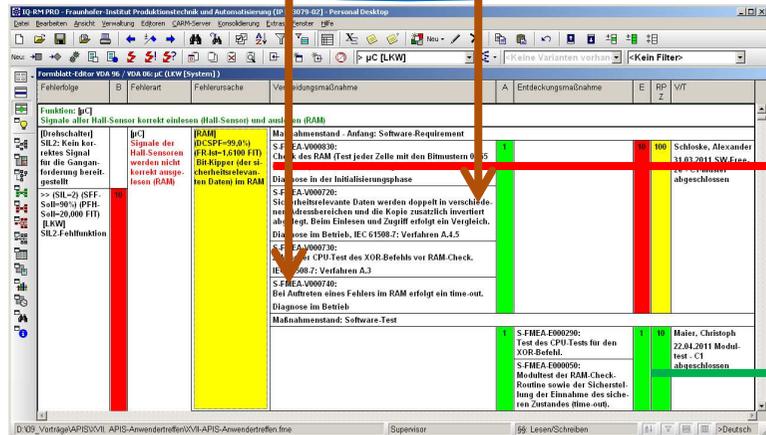
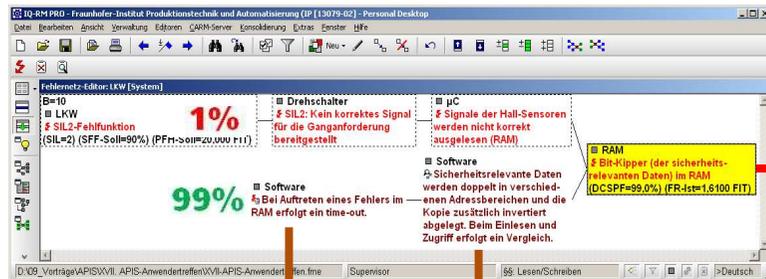
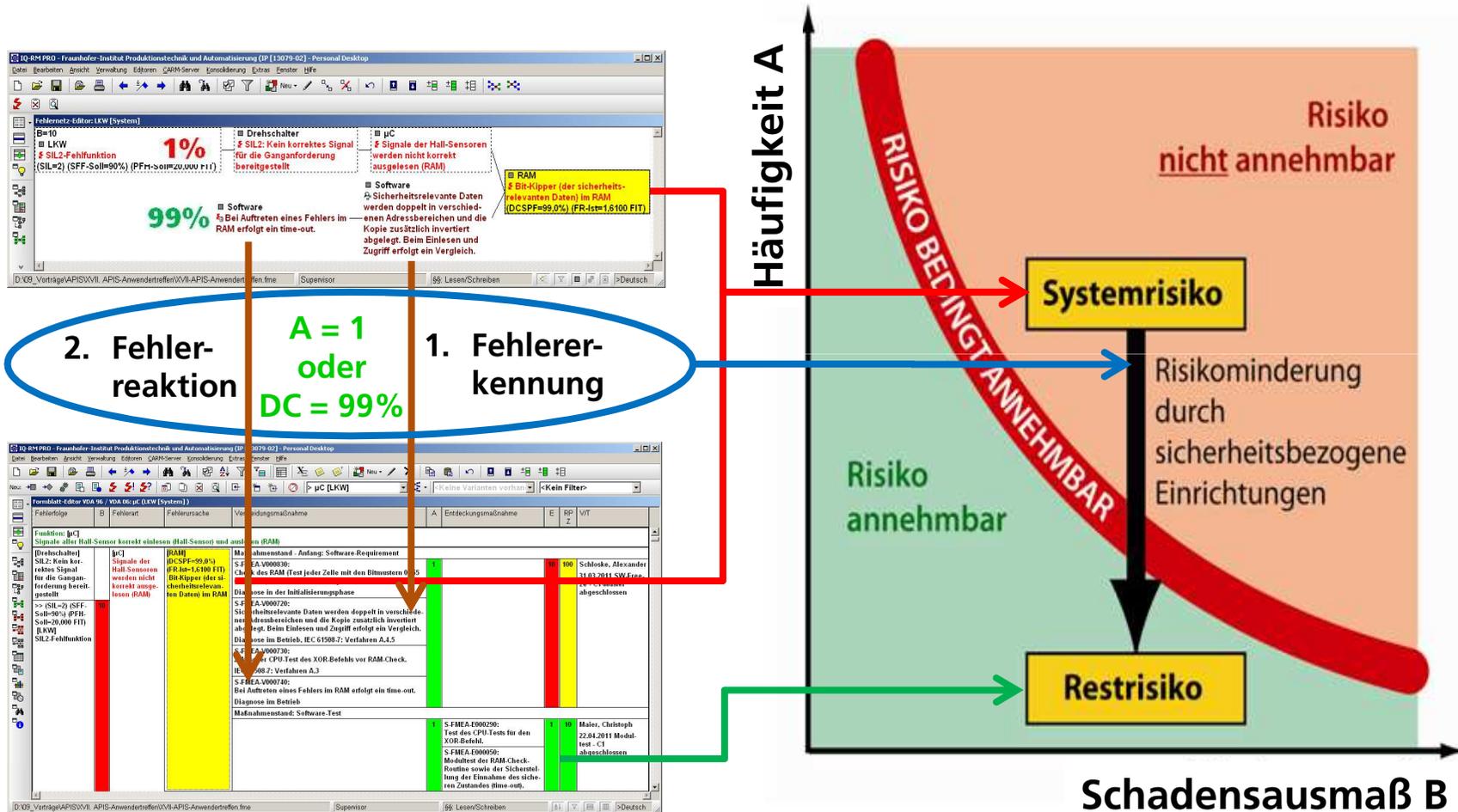
D:\09\_Vorträge\DietsFuSi-Forum\FuSi-Forum 2011\Beispiel Drehschalter - 2011-10-31.tme | Supervisor | §§: Lesen/Schreiben | < > >Deutsch

# ANWENDUNG DER FMEA, FSR UND FMEDA ZUR „RISIKOMINDERUNG“

---

65

# FMEA, FSR und FMEDA zur „Risikominderung“ Analyse und Bewertung von Fehlfunktionen, Fehlererkennungen und Fehlerreaktionen im Betrieb



# FAZIT

# Funktionale Sicherheit in der Praxis (Erfahrungen)

## Fazit

- Analyse systematischer Fehler mit der FMEA und FSR
  - Frühzeitige Analyse der Funktionen und Erstellung der Funktionsnetze
  - Detaillierte Risikoanalyse mit präziser Bezeichnung der Fehlfunktionen
- Analyse zufälliger Fehler mit der FMEA, FSR und FMEDA
  - Ermittlung von FIT-Werten anhand Zuverlässigkeitsnormen (SN 29500)
  - Ermittlung von Diagnosedeckungsgraden anhand Vorgaben aus den FuSi-Normen (einfache Fehlerfälle) und der FSR (komplexe Fehlerfälle)
- Integrierte Analyse und Darstellung
  - Abbildung der Fehlerzusammenhänge (Fehlernetze) inkl. FIT-/DC-Werte in der IQ-RM PRO 6.0 der APIS Informationstechnologien GmbH
  - Integrierte Anwendung erleichtert die durchgängige Betrachtung und Aktualisierung der Informationen und Daten

No risk – no fun



**Vielen Dank für Ihre Aufmerksamkeit !**

Bildquelle: <http://www.extr3m3.de/>69