

NEUE UND BEWÄHRTE METHODEN ZUR SICHERSTELLUNG DER FUNKTIONALEN SICHERHEIT

Dr. Alexander Schloske

NEUE UND BEWÄHRTE METHODEN ZUR SICHERSTELLUNG DER FUNKTIONALEN SICHERHEIT

Neue Herausforderungen – Erfolg versprechende Lösungsansätze
FpF-Seminar, 03.-04. Juli 2012, Stuttgart



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
Internet: www.ipa.fraunhofer.de



© Fraunhofer



Vortragsinhalte

- Methoden und Werkzeuge zur Gefahren- und Risikoanalyse
- Methoden und Werkzeuge zur Analyse systematischer Fehler
- Methoden und Werkzeuge zur Analyse zufälliger Fehler
- Zusammenspiel der Methoden
- Erläuterung anhand von Beispielen

© Fraunhofer



METHODEN ZUR ANALYSE MECHATRONISCHER SYSTEME

© Fraunhofer



Funktionale Sicherheit **Methoden zur Analyse mechatronischer Systeme**

Methoden zur SIL-Klassifizierung

- Gefahren- und Risikoanalyse
- Risikograph

Methoden zur Analyse systematischer Fehler

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

Methoden zur Analyse zufälliger Fehler

- Fehlerbaumanalyse (FTA)
 - Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse (FMEDA)
 - Berechnungsalgorithmen
-

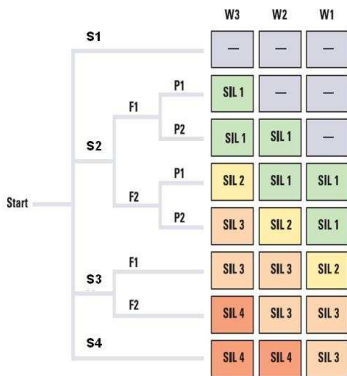
© Fraunhofer



© Fraunhofer

Methoden zur Analyse mechatronischer Systeme

Risikograph zur SIL-Klassifizierung nach DIN EN 61508



Zielsetzung:

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

Methodisches Vorgehen:

- Bestimmung des SIL-Levels anhand der
 - Schwere (S)
 - Häufigkeit des Ausgesetztseins (F)
 - Beherrschbarkeit (P)
 - Wahrscheinlichkeit des Auftretens (W)

Nutzen/Anmerkung:

- Systematisches und nachvollziehbares Vorgehen
- Basis für Methodenanwendung und Zielwerte

Methoden zur Analyse mechatronischer Systeme

Risikograph zur ASIL-Klassifizierung nach ISO/DIS 26262

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

[nach ISO DIS 26262]

[nach ISO DIS 26262]

Zielsetzung:

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

Methodisches Vorgehen:

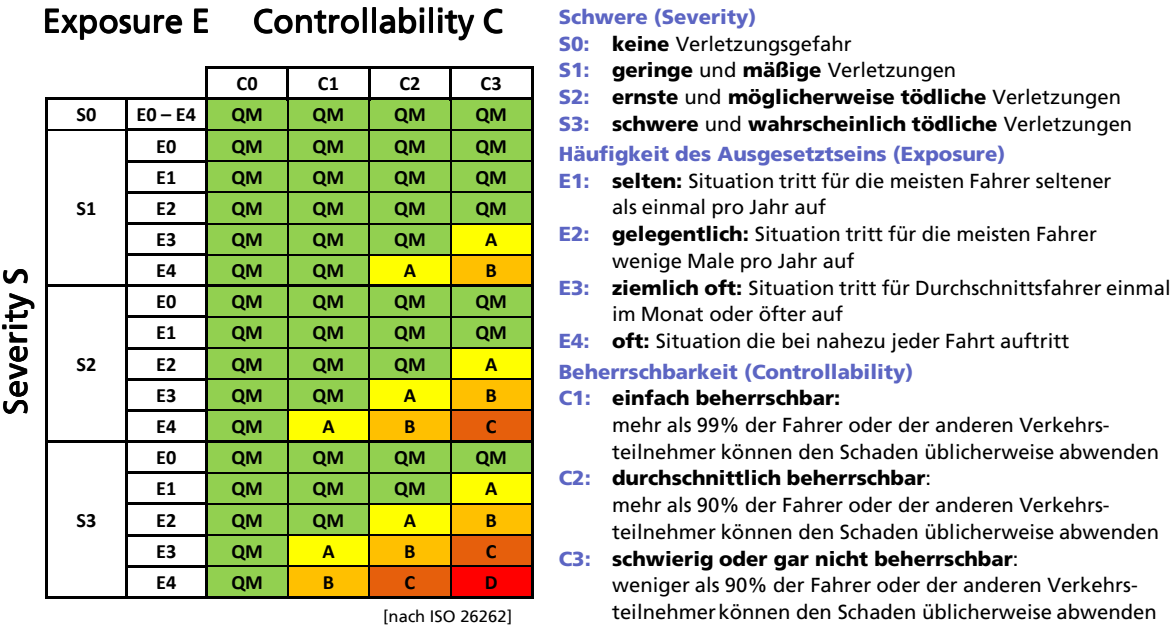
- Bestimmung des ASIL-Levels anhand
 - der Schwere (Severity)
 - der Häufigkeit des Ausgesetztseins (Exposure)
 - der Beherrschbarkeit (Controllability)

Nutzen/Anmerkung:

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

Methoden zur Analyse mechatronischer Systeme

Risikograph zur ASIL-Klassifizierung nach ISO 26262



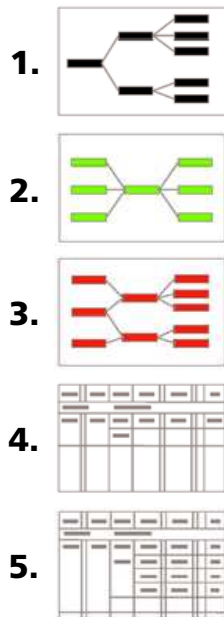
[nach ISO 26262]

METHODEN ZUR ANALYSE

SYSTEMATISCHER FEHLER

Methoden zur Analyse mechatronischer Systeme

Fehlermöglichkeits- und Einflussanalyse (FMEA)



Zielsetzung:

- Systematische Ermittlung potentieller Fehlfunktionen des betrachteten Systems

Methode nach VDA 4 Kapitel 3 (2006):

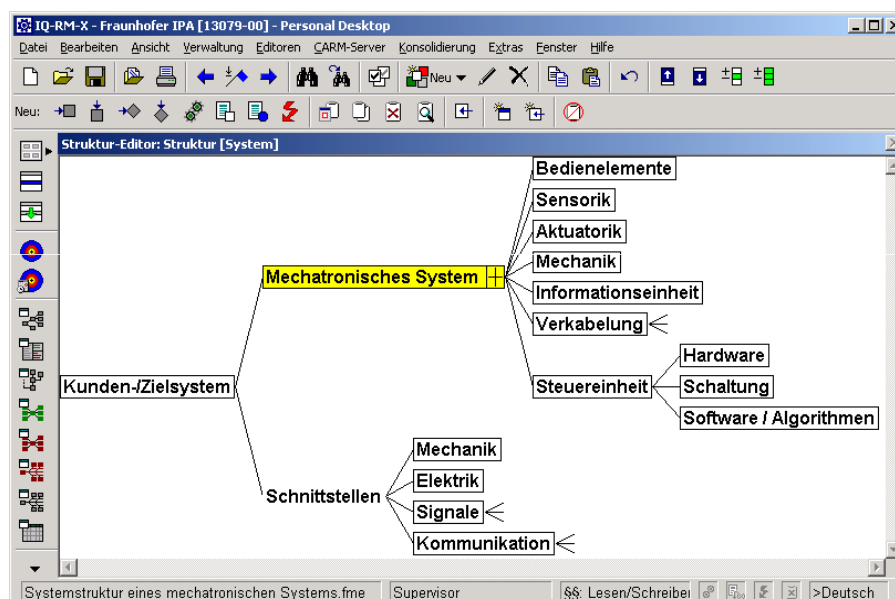
- 1: Strukturanalyse (Strukturbaum)
- 2: Funktionsanalyse (Funktionsnetze)
- 3: Fehleranalyse (Fehlernetze)
- 4: Maßnahmenanalyse und Bewertung
- 5: Optimierung (falls notwendig)

Nutzen/Anmerkung:

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

Methoden zur Analyse mechatronischer Systeme

Mögliche Systemstruktur eines mechatronischen Systems



Methoden zur Analyse mechatronischer Systeme

Mögliche Maßnahmenstruktur eines mechatronischen Systems

IQ-RM-X - Fraunhofer IPA [13079-00] - Personal Desktop									
Formblatt-Editor VDA 96: Mechatronisches System (Struktur [System])									
Fehlerfolge	B	K	Fehlerart	Fehlerursache	Vermeidungs maßnahme	A	Entdeckungs maßnahme	E	RPZ V/T
Funktion: Mechatronische Funktion									
[Kunden-/Zielsystem] Fehlerfolge im Zielsystem	10	YC	[Mechatroni- sches System] Fehlfunction des mechatroni- schen Systems	[Mechatronische Komponente] Fehlerursache einer mechatronischen Komponente	Maßnahmenstand - Anfang: Entwicklung				
					Konzeptionelle Maßnahmen zur Vermeidung der Fehlerursache				
						2		10	200
					Maßnahmenstand: Hardwaretest				
					Bestätigung der Auftretenswahrscheinlichkeit des Hardwarefehlers				
					4	Maßnahmen zum Test der korrekten Funktion der Hardware	2	80	Versuch Hardwaretest abgeschlossen
					Maßnahmenstand: Software-Requirement				
					Anforderungen an die Software bzw. Steuerung zur Überführung des Systems trotz des Hardwarefehlers in einen sicheren Zustand				
					4		10	(400)	Entwicklung Software-Requirement in Bearbeitung
					Maßnahmenstand: Softwaretest				
					Bestätigung der Auftretenswahrscheinlichkeit des Hardwarefehlers unter Berücksichtigung der Absicherung durch die Software bzw. Steuerung				
					4	Maßnahmen zum Test der korrekten Funktion der Absicherung durch die Software bzw. Steuerung	3	(120)	Versuch Softwaretest in Bearbeitung
					Maßnahmenstand: Gesamttest				
					4	Tests im Gesamtsystem	2	(80)	Entwicklung Gesamttest in Bearbeitung
					Maßnahmenstand: Service				
					Maßnahmen zur präventiven Instandhaltung im Service				
					4	Maßnahmen zur Entdeckung der Fehlfunction im Service	3	(120)	Service Service unbearbeitet
					Maßnahmenstand: Betrieb				
					4	Maßnahmen zur Information des Benutzers über Fehlfunctionen im System	1	(40)	Kunde Betrieb in Bearbeitung

- Maßnahmen zur Vermeidung in der Entwicklung
- Maßnahmen zur Entdeckung in der Entwicklung
- Software-Requirements zur Überführung in sicheren Zustand
- Maßnahmen zum Test der korrekten Software-Funktion
- Maßnahmen zur Entdeckung im Gesamtsystem
- Maßnahmen zur Entdeckung im Service
- Maßnahmen zur Entdeckung im Betrieb

Methoden zur Analyse mechatronischer Systeme

Fehlerbasierte System-Reaktionsanalyse (FSR)

Fehlerbasierte System-Reaktionsanalyse (FSR)		Nutzungsablauf Betriebszustände				
Diagnose Diagnosefunktion						
Regel: 1. Elemente können nur ausfallen, wenn sie belastet sind 2. Elemente, die in einer vorgelagerten Phase unentdeckt ausfallen werden in den nächsten Phasen weiter betrachtet						
Farben Kritisch / Unentdeckt Kritisch / Entdeckt Unkritisch / Unentdeckt Unkritisch / Entdeckt						
Geteilte Diagnoseelemente						
Diagnoseelement 1						
Fehler 1 aus System-FMEA						
Fehler 2 aus System-FMEA						
Diagnoseelement 2						
Fehler 1 aus System-FMEA						

Zielsetzung:

- Analyse komplexer Fehlermodelle
- Definition von Diagnose- und Absicherungsmaßnahmen für komplexer Fehlermodelle
- Ermittlung von Diagnosedeckungsgraden

Methode:

- Übernahme Fehlfunktionen der System-FMEA
- Bewertung Entdeckbarkeit von Ausfallarten unter Berücksichtigung von Systemzuständen

Nutzen/Anmerkung:

- Diagnosedeckungsgrade für komplexe Fehler
- Hinweise auf „schlafende Fehler“ im System

Methoden zur Analyse mechatronischer Systeme

Paarvergleichsmatrix für schlafende Fehler

	Fehlfunktion 1	Fehlfunktion 2	Fehlfunktion 3	Fehlfunktion 4	Fehlfunktion 5	Fehlfunktion 6
Fehlfunktion 1						
Fehlfunktion 2						
Fehlfunktion 3						
Fehlfunktion 4						
Fehlfunktion 5						
Fehlfunktion 6						

Zielsetzung:

- Bewertung des Risikos schlafender Fehler unter Berücksichtigung des zeitlichen Auftretens

Methode:

- Gegenüberstellung schlafender Fehler in der Paarvergleichsmatrix
- Bewertung der Auswirkungen und Entdeckbarkeit in Abhängigkeit des zeitlichen Auftretens

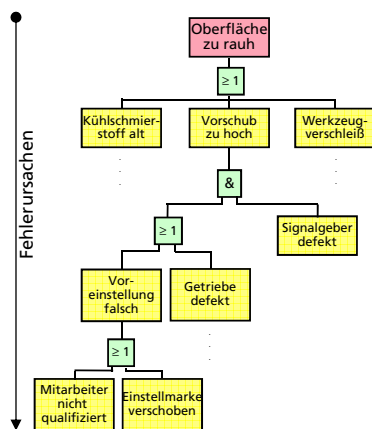
Nutzen/Anmerkung:

- Hilfsmittel zur Entwicklung des Sicherheitskonzepts für zeitlich unabhängig auftretende Mehrfachfehler (latent und multiple faults)

METHODEN ZUR ANALYSE ZUFÄLLIGER FEHLER

Methoden zur Analyse mechatronischer Systeme

Fehlerbaumanalyse (FTA)



Zielsetzung:

- Ermittlung und Visualisierung aller Fehlerursachen, die zum unerwünschten Ereignis führen

Methode:

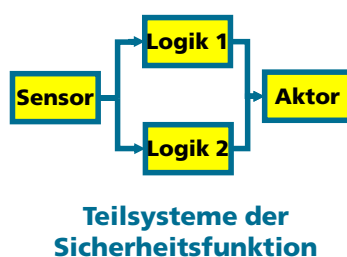
- Systemanalyse und Erstellung des Fehlerbaums
- Quantitative Auswertung des Fehlerbaums

Nutzen/Anmerkung:

- Visualisierung von Ausfällen und deren Zusammenhänge und Wahrscheinlichkeiten
- Beurteilung von Systemen und Produkten bzgl. Sicherheit und Zuverlässigkeit

Methoden zur Analyse mechatronischer Systeme

Reliability Block Diagramm



Zielsetzung:

- Hilfsmittel zur Zerlegung der an der Sicherheitsfunktion beteiligten Teilsysteme

Methode:

- Abbildung der an der Sicherheitsfunktion beteiligten Teilsysteme entsprechend der Architektur
 - Seriell
 - Parallel
 - Common cause

Nutzen/Anmerkung:

- Voraussetzung zur Berechnung der FuSi-Parameter (z.B. PMHF, Fault-Metrik) in der FMEDA

Methoden zur Analyse mechatronischer Systeme

Failure Modes, Effects and Diagnostic Analysis (FMEDA)

[illegible]

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Zielsetzung:

- Analyse der Fehlermodi der an der Sicherheitsfunktion beteiligten Komponenten

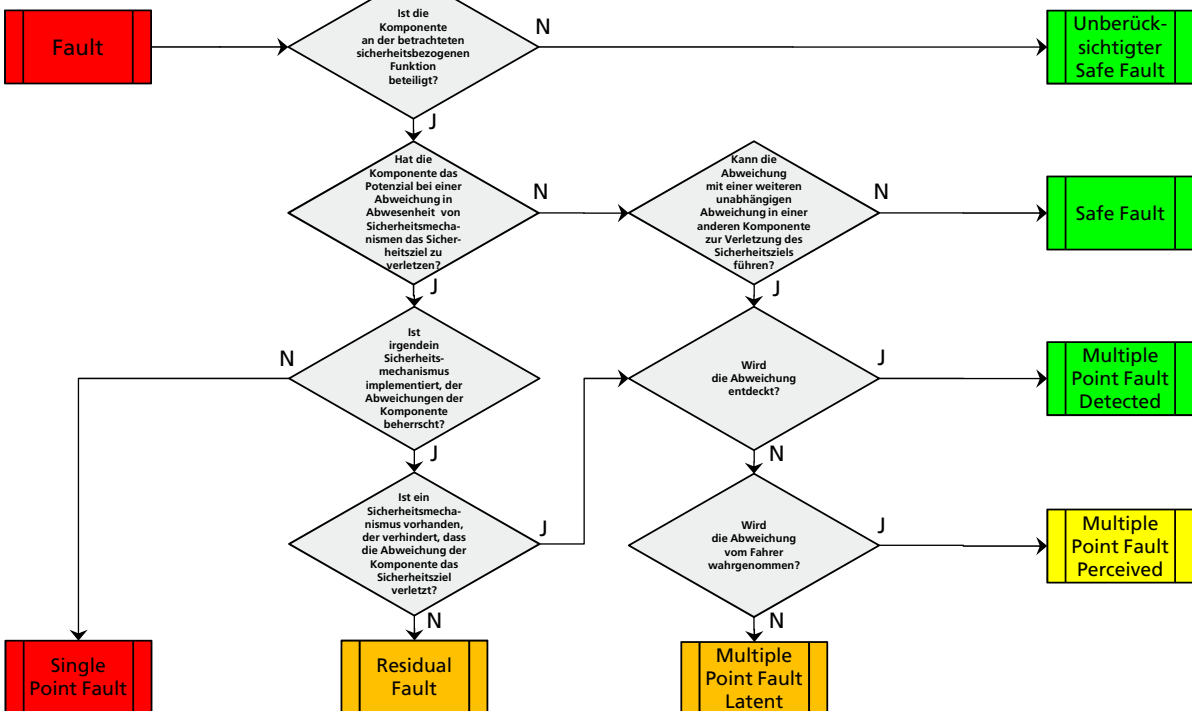
Methode:

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

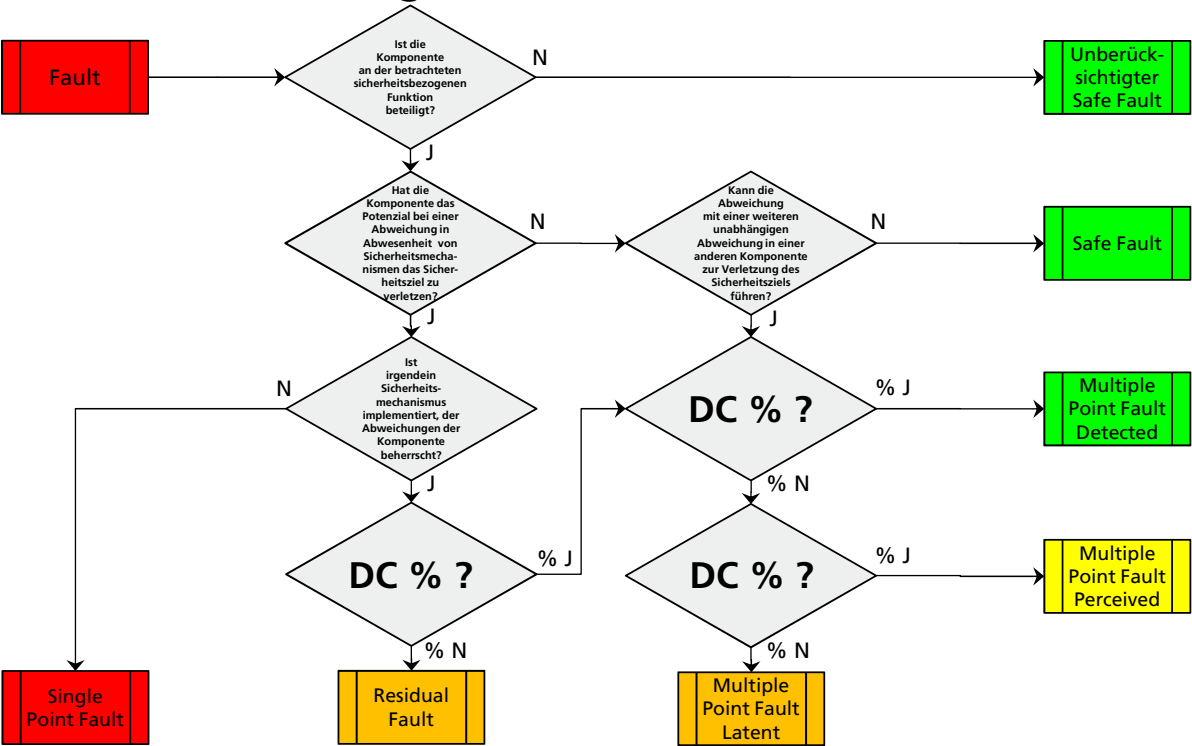
Nutzen/Anmerkung:

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

Fault-Klassifizierung nach ISO 26262



Fault-Klassifizierung nach ISO 26262



Berechnungsmodell Residual, Detected, Perceived und Latent Multiple Faults

Abweichung Bauteil mit Möglichkeit zur Verletzung des Sicherheitsziels	Sicherheitsmechanismus 1 (DC = 90%)	Sicherheitsmechanismus 2 (DC = 50%)
100 FIT	90 FIT	Detected MPF 45 FIT
		DC Nutzer (DC = 30%) Perceived MPF 27 FIT
		Latent MPF 18 FIT
	Residual Fault 90 FIT	

Methoden zur Analyse mechatronischer Systeme

Berechnungsalgorithmen für Fault-Metriken und gefahrbringende Ausfälle nach 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 $\sum \lambda_x$ is the sum of λ_x of the safety-related hardware elements of the item.

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

Legende:
 PMHF = Probabilistic Metric for random Hardware Failures (PMHF)
 SPFM = Single-point fault metric
 LFM = Latent-fault metric

Quelle: ISO 26262-5

ERLÄUTERUNG ANHAND EINES BEISPIELSYSTEMS

Erläuterung anhand eines Beispielsystems

Beispielsystem (Fahrzeug und Werte zufällig gewählt)



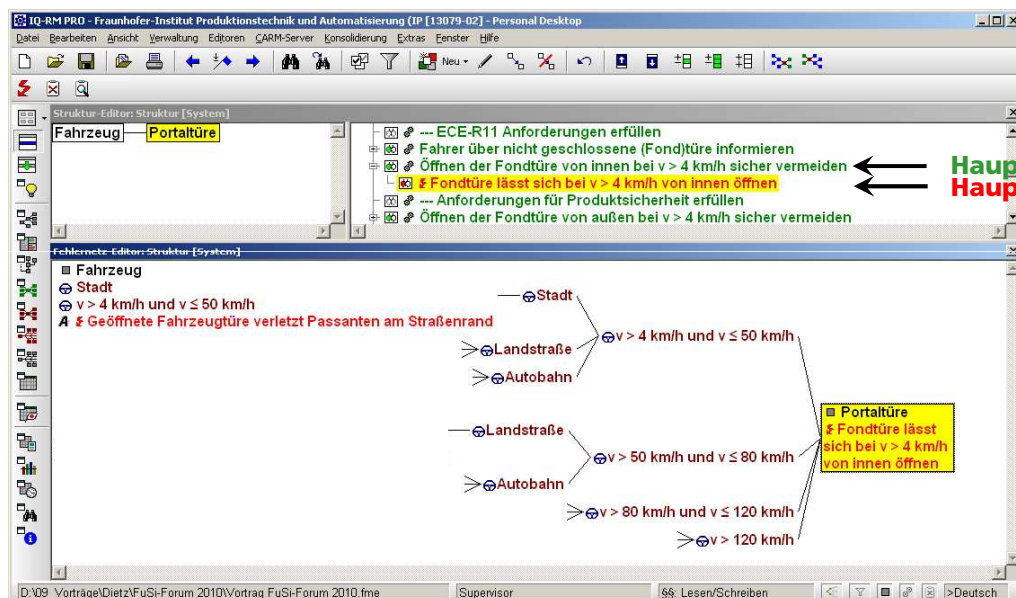
1965



20xx ?

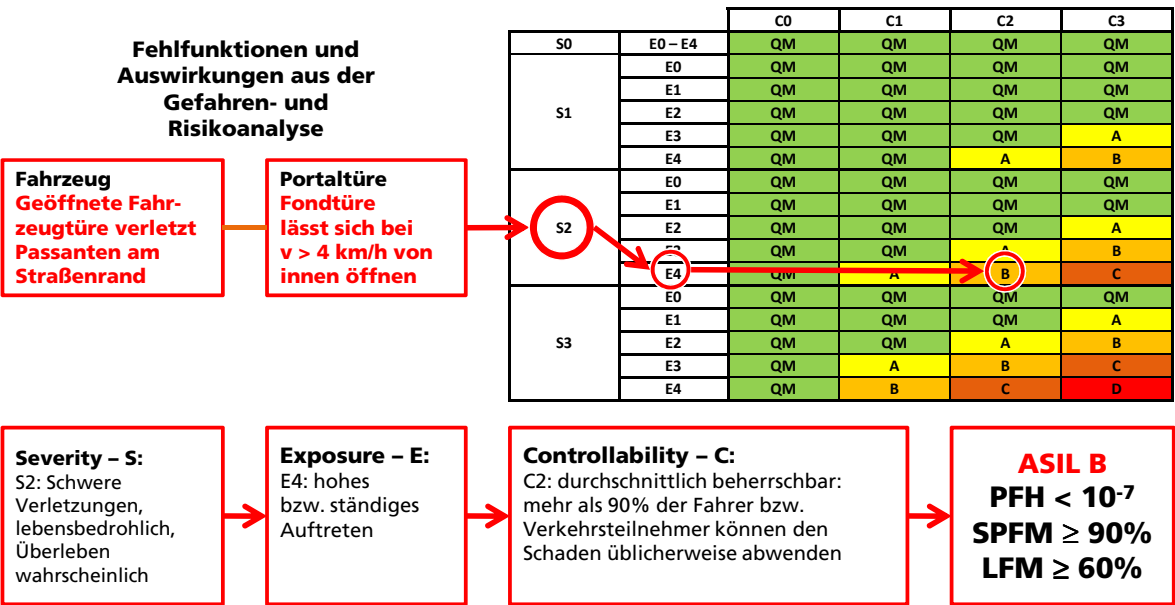
Erläuterung anhand eines Beispielsystems

Gefahren- und Risikoanalyse



Erläuterung anhand eines Beispielsystems

Möglicher Risikograph gemäß ISO/DIS 26262

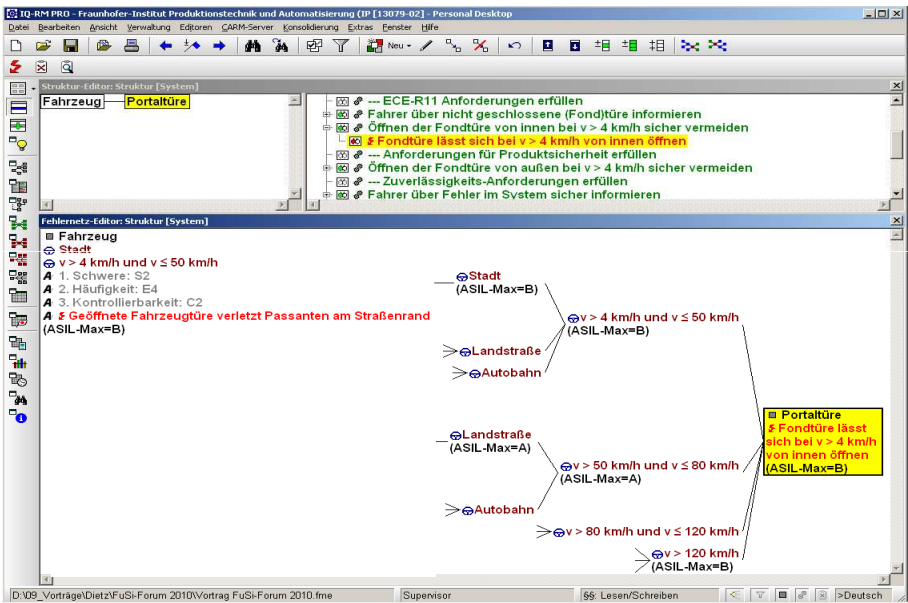


© Fraunhofer



Erläuterung anhand eines Beispielsystems

Gefahren- und Risikoanalyse mit ASIL-Klassifizierung



© Fraunhofer

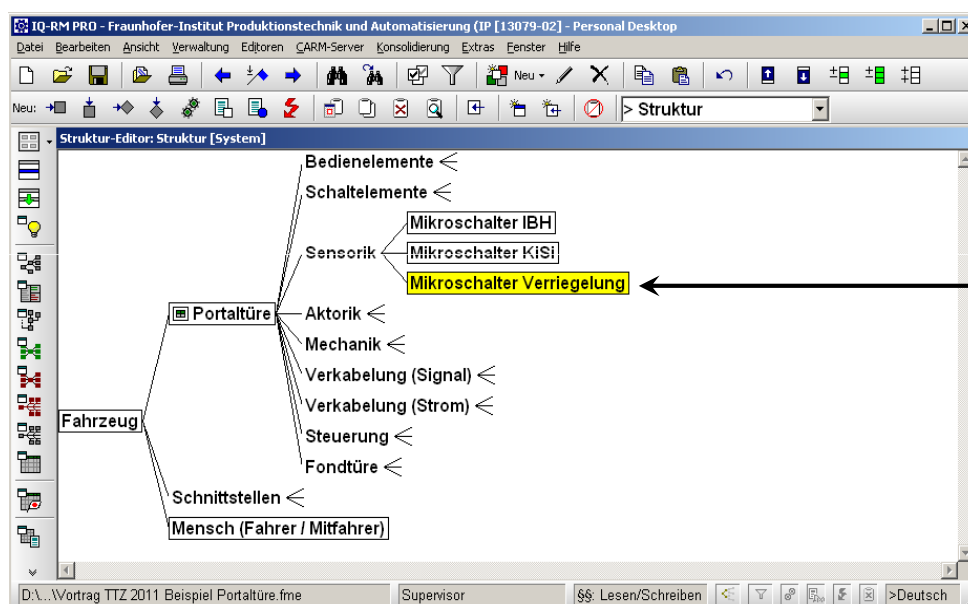


ANALYSE SYSTEMATISCHER FEHLER

© Fraunhofer



Erläuterung anhand eines Beispielsystems Mögliche Systemstruktur einer „Portaltüre“



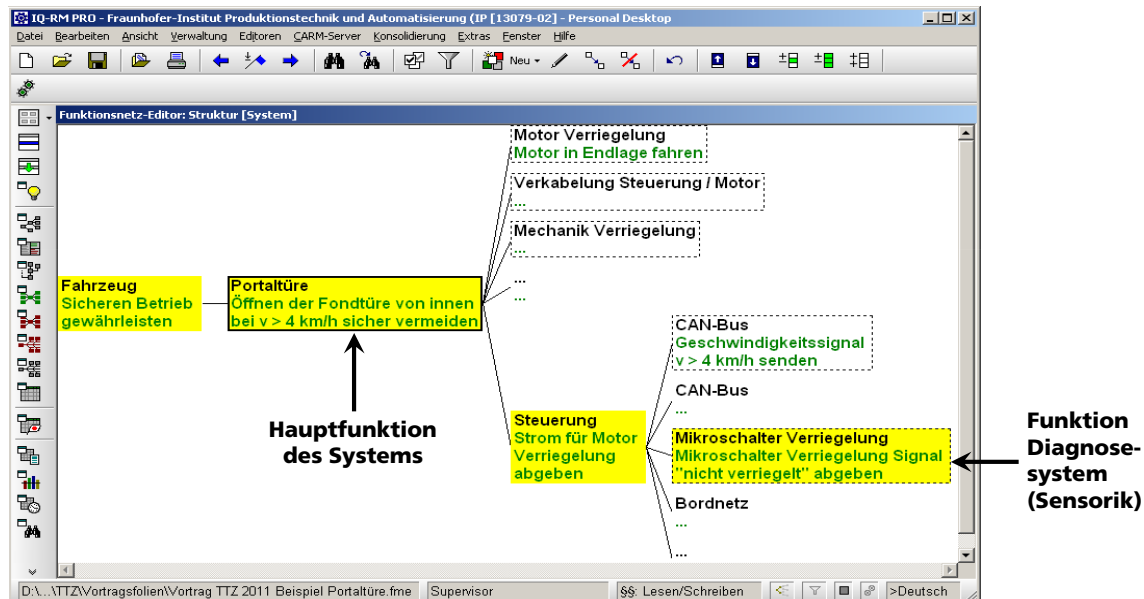
**Diagnose-
system
(Sensorik)**

© Fraunhofer



Erläuterung anhand eines Beispielsystems

Mögliches Funktionsnetz einer „Portaltüre“

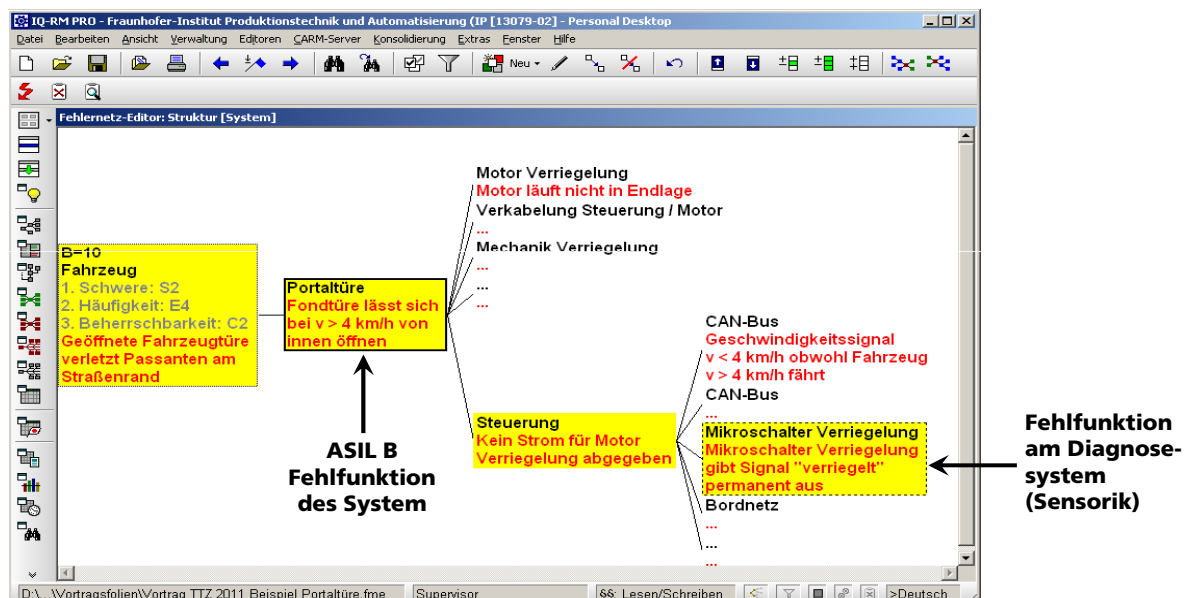


© Fraunhofer

Fraunhofer

Erläuterung anhand eines Beispielsystems

Mögliches Fehlernetz einer „Portaltüre“



© Fraunhofer

Fraunhofer

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	Mikroschalter Verriegelung											
4	Mikroschalter Verriegelung permanent auf "verriegelt"	2		U/U	U/U	U/U	U/U	U/U	K/U	K/U	U/U	x
5	Mikroschalter Verriegelung permanent auf "nicht verriegelt"	2		K/E	U/U	U/U	U/U	U/U	K/E	U/U	U/U	

© Fraunhofer



Erläuterung anhand eines Beispielsystems

Mögliches Formblatt einer „Portaltüre“

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

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									
>> (ASIL=B) « 0/1 » [Fahrzeug] A Geöffnete Fahrgasttüre verletzt Passanten am Straßenrand									
[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	1000	
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	1000	Schlosse Software-Requirements in Umsetzung
Maßnahmenstand: Softwaretest									
Test-Bench ID=TB080: Test, ob bei ausgefallenem Mikroschalter (li/ra) 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

© Fraunhofer



Erläuterung anhand eines Beispielsystems

Mögliches Formblatt einer „Portaltüre“

Fehlerfolge	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RPZ	VT
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 abgegeben	« 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	
Maßnahmenstand: Software-Requirements								
>> (ASIL=B) « 0/1 » [Fahrzeug] A Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand			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)	Schlosse 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

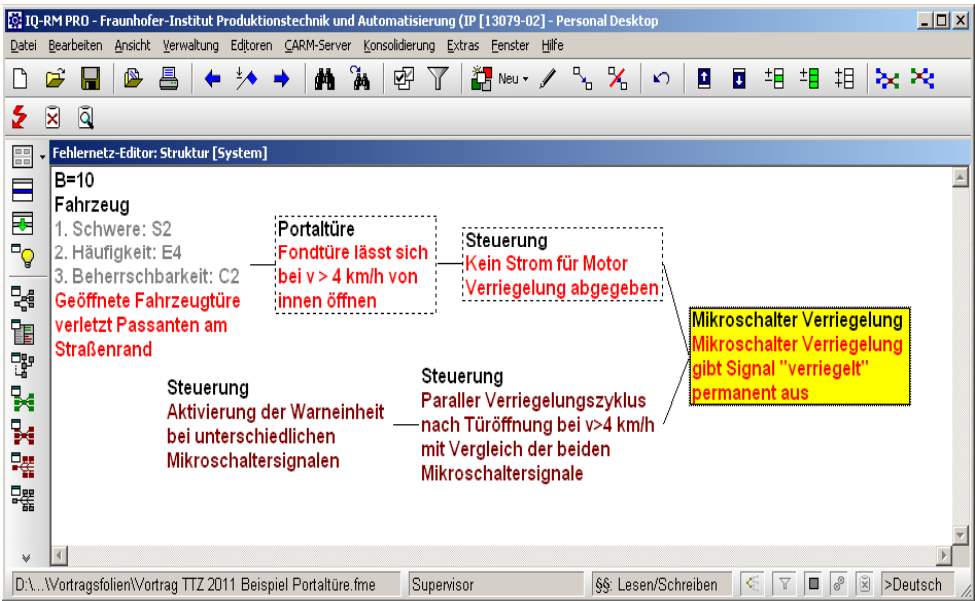
Erläuterung anhand eines Beispielsystems

Mögliche FSR eines Diagnosesystems der „Portaltüre“

	B	C	F	G	H	I	J	K	L	M	N	O	T	U	V	AA
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																
Diagnoseelemente																
1																
2																
3	Mikroschalter Verriegelung															
4	Mikroschalter Verriegelung permanent auf "verriegelt"															
5	Mikroschalter Verriegelung permanent auf "nicht verriegelt"															
6	Mikroschalter Verriegelung / Inform															
Bereit																

Erläuterung anhand eines Beispielsystems

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



Erläuterung anhand eines Beispielsystems

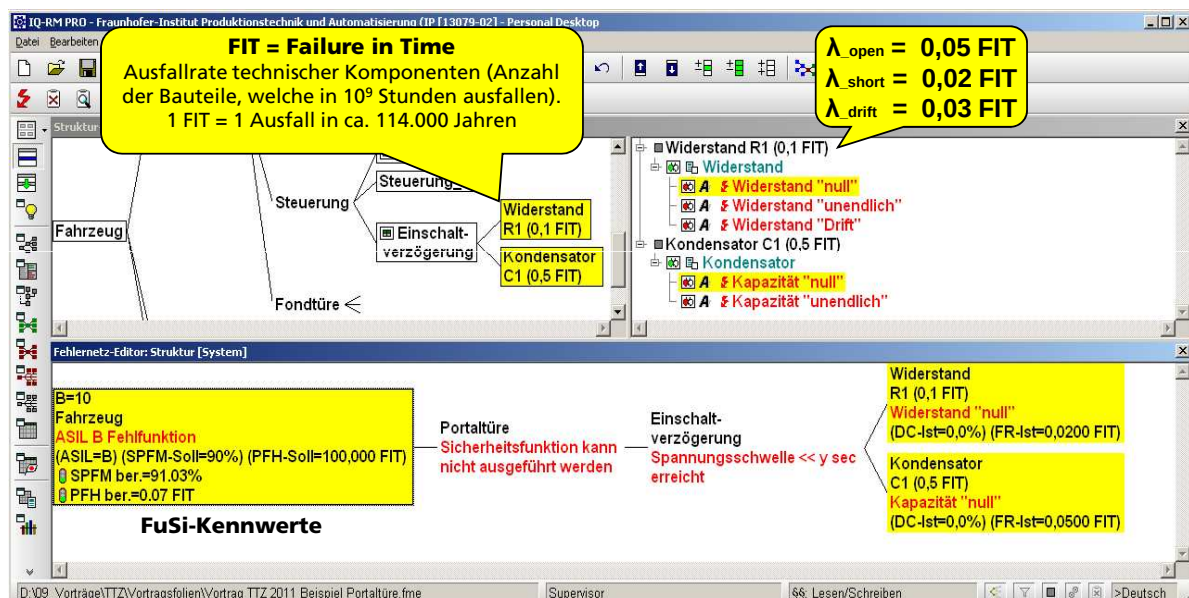
Mögliches Formblatt einer „Portaltüre“

Formblatt-Editor VDA 96 / VDA 06: Steuerung (Struktur [System])			
Fehlerfolge	Fehlerart	Fehlerursache	Vermeidungsmaßnahme
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 abgegeben	« 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
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.			
Maßnahmenstand: Softwaretest			
1 Test-Bench ID=TB090: Test, ob bei ausgefallenem Mikroschalter (li / re) während bzw. nach Türöffnung die Warneinheit aktiviert wird.			
Maßnahmenstand: Betrieb			
1 Sichere Entdeckung im Betrieb und Information des Kunden bei ausgefallenem Mikroschalter Verriegelung in allen Systemzuständen			

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

ANALYSE ZUFÄLLIGER FEHLER

Erläuterung anhand eines Beispielsystems FuSi-Kennwerte anhand von Fehlernetzen und Ausfall- raten bis auf die Ebene der elektr(on)ischen Bauteile



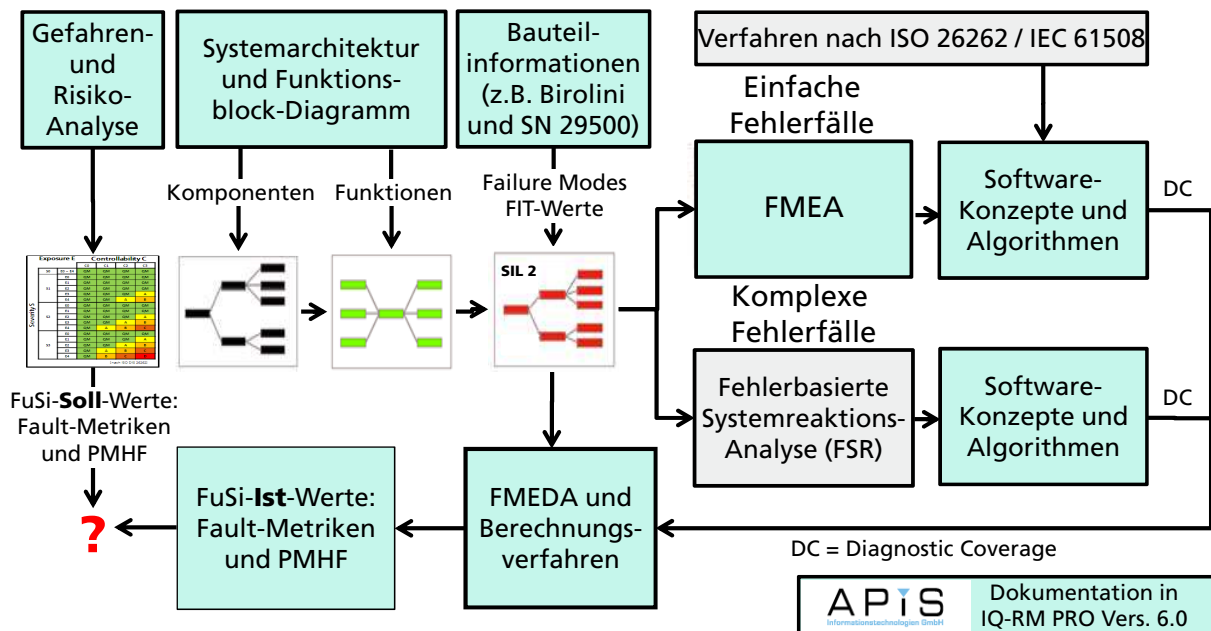
Failure Modes, Effects and Diagnostic Analysis (FMEDA)

FMEDA für ein System (gemäß ISO/DIS 26262)

Sicherheitsziel 1: Keine ungewollte Aktivierung der EPB während der Fahrt											
Komponente	FT-Wert	Sicherheitsniveau	Fehlerrate / Abweichung	Fehlerrateentwicklung (FIT)	Potential zur Verletzung des Sicherheitsziels in Abwesenheit eines Sicherheitsmechanismus	Sicherheitsmechanismus zur Vermeidung der Verletzung des Sicherheitsziels	Nachweis der Fehlerrate / Abweichung zur Verletzung des Sicherheitsziels	Restrisiko oder Single Point Fault (Fehlerrate / FIT)	Fehlerrate / Abweichung, welche zusammen mit einer anderen unabhängigen Fehlerrate / Abweichung zu einer Verletzung des Sicherheitsziels führen können	Sicherheitsmechanismus zur Vermeidung eines latenten Fehlers / Abweichung	Reduktion der Fehlerschweregrade (z.B. durch Redundanz, Latente Mehrfach-Point Fault (Fehlerrate / FIT))
Spannungsversorgung	30,00	ja	Ausfall während der Fahrt	2.4750							
			Ausfall im Stand	0,0250							
			Reduzierte Spannung während der Fahrt	47,0250	x	Überwachung durch externe ECU	99%	0,4709			
Quarz	5,00	ja	Reduzierte Spannung im Stand	0,4750							
			Ausfall während der Fahrt	2.4750	x	Überwachung durch Hardware-Watchdog	90%	0,2475			
			Ausfall im Stand	0,0250							
Balais	300,00	ja	Drift während der Fahrt	2.4750	x	Überwachung durch Hardware-Watchdog	90%	0,2475			
			Drift im Stand	0,0250							
			Stuck at ON während der Fahrt	0,2250							
Taster	40,00	ja	Stuck at OFF während der Fahrt	0,0750							
			Stuck at ON im Stand	124,7750							
			Stuck at OFF im Stand	74,9250							
Hardware-Watchdog	10,00	nein	Stuck at ON während der Fahrt	0,0200							
			Stuck at OFF während der Fahrt	0,0200							
			Stuck at ON im Stand	19,9800							
µC-Logik	20,00	ja	Stuck at OFF im Stand	19,9800							
			Ausfall	10,0000					x	Check bei Zündung "ON"	60% 4,0000
			Ausfall zu Stuck at ON während der Fahrt	9,9000	x	keine	0%	9,9000			
µC-RAM	20,00	ja	Ausfall zu Stuck at ON während der Fahrt	9,9000							
			Ausfall zu Stuck at ON im Stand	0,1000							
			Ausfall zu Stuck at OFF im Stand	0,1000							
µC-IO	20,00	ja	Bitkipper oder Zelldefekt	10,0000	x	Checksummenprüfung beim Einlesen	99%	0,1000			
			Bitkipper oder Zelldefekt	10,0000							
			Bitkipper oder Zelldefekt während der Fahrt	9,9000	x	Checksummenprüfung beim Ein-/Auslesen	99%	0,0990			
µC-Watchdog	20,00	nein	Bitkipper oder Zelldefekt während der Fahrt	9,9000							
			Bitkipper oder Zelldefekt im Stand	0,1000							
			Bitkipper oder Zelldefekt während der Fahrt	9,9000							
µC-Watchdog	20,00	ja	Bitkipper oder Zelldefekt im Stand	0,1000							
			Bitkipper oder Zelldefekt während der Fahrt	9,9000	x	keine	0%	9,9000			
			Ausfall zu Stuck at ON während der Fahrt	9,9000							
µC-Watchdog	20,00	nein	Ausfall zu Stuck at ON im Stand	0,1000							
			Ausfall zu Stuck at OFF im Stand	0,1000							
			Ausfall	20,0000					x		20,0000

ZUSAMMENSPIEL DER METHODEN

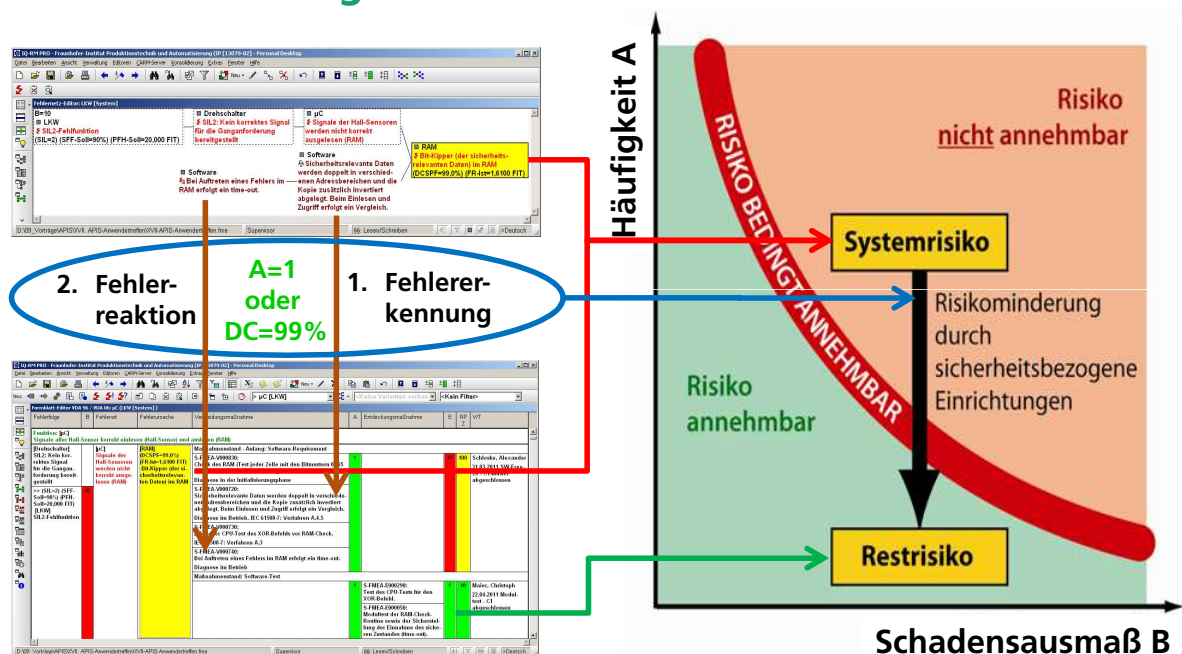
Zusammenhang zwischen den eingesetzten Methoden Vorgehensweise zur Analyse und Absicherung funktional sicherer mechatronischer Systeme



© Fraunhofer

Fraunhofer

FMEA und FMEDA Analyse und Bewertung von Fehlfunktionen, Fehlererkennungen und Fehlerreaktionen im Betrieb



© Fraunhofer

Fraunhofer

FAZIT

Methoden zur Sicherstellung der Funktionalen Sicherheit Fazit

- Zur Analyse und Beurteilung der Funktionalen Sicherheit existieren bereits effektive Methoden und Werkzeuge
- Eine sinnvolle integrierte Anwendung der vorhandenen Methoden und Werkzeuge erleichtert die durchgängige Betrachtung und Aktualisierung der Daten
- Die Methoden und Werkzeuge entwickeln sich in Richtung Unterstützung der Funktionalen Sicherheit
- Eine alleinige Darstellung komplexer Zusammenhänge mechatronischer Systeme mit EXCEL-Werkzeugen wird nicht die gewünschten Ergebnisse liefern



ISO 26262 FUNKTIONALE SICHERHEIT

- NEUE HERAUSFORDERUNGEN
- ERFOLG VERSPRECHENDE LÖSUNGSANSÄTZE

