

FMEA und Funktionale Sicherheit

Dr. Alexander Schloske

FMEA UND FUNKTIONALE SICHERHEIT

Fehlervermeidung in der Produktentwicklung
FpF-Veranstaltung am 14. und 26. Oktober 2010



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
fmea@ipa.fraunhofer.de
Internet: www.ipa.fraunhofer.de



© Fraunhofer

Fraunhofer
IPA

Vortragsinhalte

- Grundlagen Funktionaler Sicherheit
- Software in mechatronischen Systemen
- Methoden zur Analyse mechatronischer Systeme
- Auslegung und Absicherung von mechatronischen Systemen
- Auszugsweise Erläuterung anhand eines Beispielsystems
- Fazit

© Fraunhofer

Fraunhofer

GRUNDLAGEN DER FUNKTIONALEN SICHERHEIT

© Fraunhofer



Ursprung der Funktionalen Sicherheit



Chemieunfall in Seveso, Italien 1976:
Hochgiftiges Dioxin mit katastrophalen Folgen
für Menschen, Tierwelt und Natur ausgetreten

- Unkontrollierte Reaktion führte zur Überhitzung
- Automatische Kühlsysteme und Warnanlagen waren nicht vorhanden

Unglück löste Normungsbestrebungen für funktionale Sicherheit aus:

- IEC 61508 (allgemein) – 1998/2000
- ISO 26262 (automotive) – 2011

© Fraunhofer



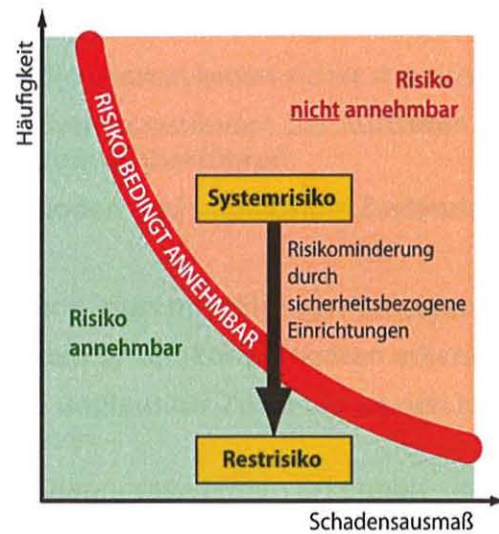
Definition der funktionalen Sicherheit

- Funktionale Sicherheit ist die Fähigkeit eines elektrischen, elektronischen bzw. programmierbarer elektronischen Systems (E/E/PE-System) bei Auftreten
 - zufälliger und/oder systematischer Ausfälle mit gefahrbringender Wirkung
 - im sicheren Zustand zu bleiben bzw. einen sicheren Zustand einzunehmen

Begriffe der funktionalen Sicherheit

- Sicherheitsfunktion
Funktion eines sicherheitsbezogenen Systems, um im Gefahrfall einen Zustand mit tolerierbarem Restrisiko einzunehmen oder aufrecht zu erhalten
- Sicherheitsintegrität
„Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraums anforderungsgemäß ausführt“
[DIN EN 61508-4]
- Sicherheits-Integritätslevel (A)SIL
vier diskrete Stufen zur Festlegung von Anforderungen für die Sicherheitsintegrität der Sicherheitsfunktionen (SIL1 bis SIL4 bei IEC 61508 bzw. ASIL A bis ASIL D bei ISO DIS 26262)

Grundprinzip der Funktionalen Sicherheit: „Risikominderung“



© Fraunhofer

Fraunhofer

SOFTWARE IN MECHATRONISCHEN SYSTEMEN

© Fraunhofer

Fraunhofer

Charakteristika von Software in mechatronischen Systemen

Die Software / Steuerung muss

- das System in allen Systemzuständen sicher steuern
- das System in allen Systemzuständen bei Auftreten von Fehlfunktionen in einen sicheren Zustand überführen
- relevante Fehlfunktionen und unplausible Zustände dem Benutzer melden

Die Software / Steuerung muss mit Hilfe von Sensoren und Algorithmen

- Fehlfunktionen an den Systemkomponenten erkennen
- Fehlfunktionen und unplausible Zustände an den Informationsschnittstellen erkennen
- Fehlfunktionen im Diagnosesystemen erkennen
(kann ich meinem Diagnosesystem noch trauen?)

© Fraunhofer

 **Fraunhofer**

METHODEN ZUR ANALYSE MECHATRONISCHER SYSTEME

© Fraunhofer

 **Fraunhofer**

Methoden zur Analyse mechatronischer Systeme

Methoden zur SIL-Klassifizierung und Vorgabewerte für SIL-Klassen

- Gefahren- und Risikoanalyse
- Risikograph
- Vorgabewerte

Methoden zur Analyse systematischer Fehler

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

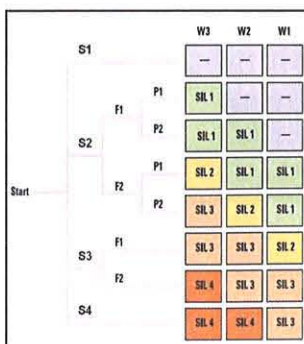
Methoden zur Analyse zufälliger Fehler

- Reliability Block Diagramm und Berechnungsverfahren
- Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse (FMEDA)

© Fraunhofer



Gefahren- und Risikoanalyse und Risikograph



Zielsetzung:

- Systematische Ermittlung potentieller Risiken des Systems sowie des erforderlichen SIL-Levels

Methodisches Vorgehen:

- Definition der Hauptfunktionen des Systems
- Ermittlung der potentiellen Fehlfunktionen
- Ermittlung der Gefahren und Risiken
- Ermittlung des SIL-Levels anhand Risikograph

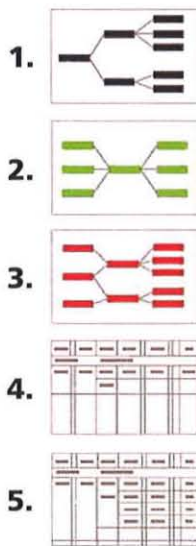
Nutzen/Anmerkung:

- Frühzeitige Durchführung
- Betrachtung unabhängig vom Sicherheitskonzept (Grundlage für Sicherheitskonzept)

© Fraunhofer



Fehlermöglichkeits- und Einflussanalyse (FMEA)



Zielsetzung:

- Systematische Ermittlung potentieller Fehlfunktionen für die Komponenten des 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:

- Detaillierte Übersicht über Fehlfunktionen
- Verwendung von Funktionsnetzen
- Präzise Benennung der Fehlfunktionen

© Fraunhofer

 Fraunhofer

Fehlerbasierte System-Reaktionsanalyse (FSR)

Fehlerbasierte System-Reaktionsanalyse (FSR)	Strukturallogisch Strikta/ide content				
Diagnose Diagnosefunktion Regel: 1. Elemente können nur analysiert, wenn die bekannt sind 2. Elemente, die in einer vorgegebenen Phase nicht analysiert werden, werden in der nächsten Phase weiter betrachtet Funktion Schleife: Diagnose Schleife: Diagnose Schleife: Diagnose Schleife: Diagnose	Phasenplan 1 Phasenplan 2 Phasenplan 3 Phasenplan 4 Phasenplan 5	Phasenplan 1 Phasenplan 2 Phasenplan 3 Phasenplan 4 Phasenplan 5	Phasenplan 1 Phasenplan 2 Phasenplan 3 Phasenplan 4 Phasenplan 5	Phasenplan 1 Phasenplan 2 Phasenplan 3 Phasenplan 4 Phasenplan 5	Phasenplan 1 Phasenplan 2 Phasenplan 3 Phasenplan 4 Phasenplan 5

Zielsetzung:

- Analyse der Diagnose- und Absicherungsmaßnahmen auf systematische Fehler

Methode:

- Übernahme der Fehlfunktionen aus der System-FMEA für alle beteiligten Komponenten
- Bewertung der Entdeckbarkeit unter Berücksichtigung von nutzerbedingten Interaktionen und Systemzuständen

Nutzen/Anmerkung:

- Hinweise auf „schlafende Fehler“ im System
- Kompakte Darstellung komplexer FMEAs

© Fraunhofer

 Fraunhofer

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

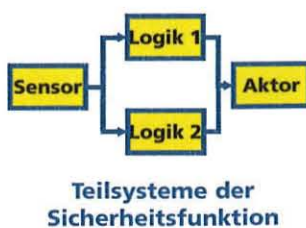
Methode:

- 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)

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

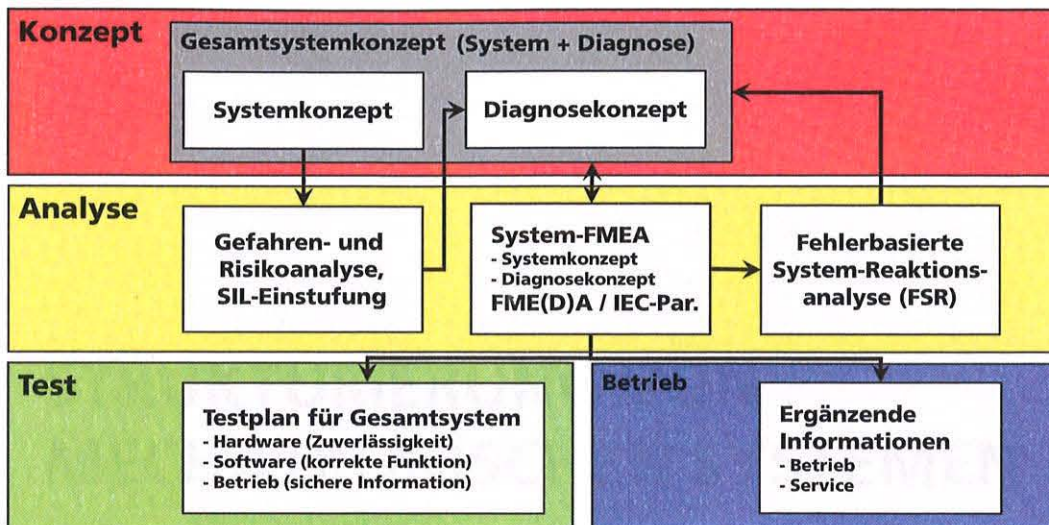
Nutzen/Anmerkung:

- Voraussetzung zur Berechnung der Parameter PFH, PFD und SFF in der FMEDA

Failure Modes, Effects and Diagnostic Analysis (FMEDA)



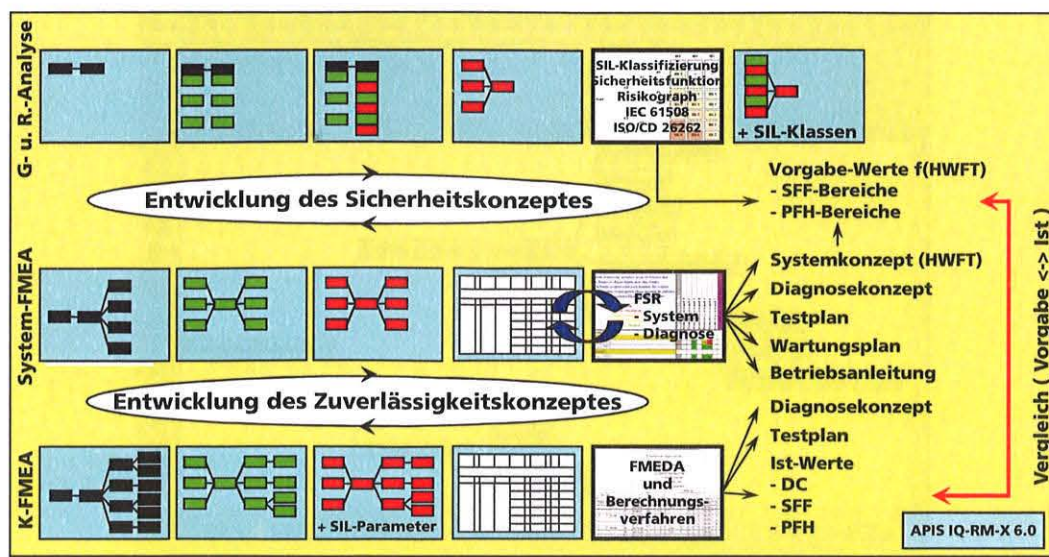
Auslegung und Absicherung von mechatronischen Systemen



© Fraunhofer

Fraunhofer

Unterstützung der Analysen zur Funktionalen Sicherheit



© Fraunhofer

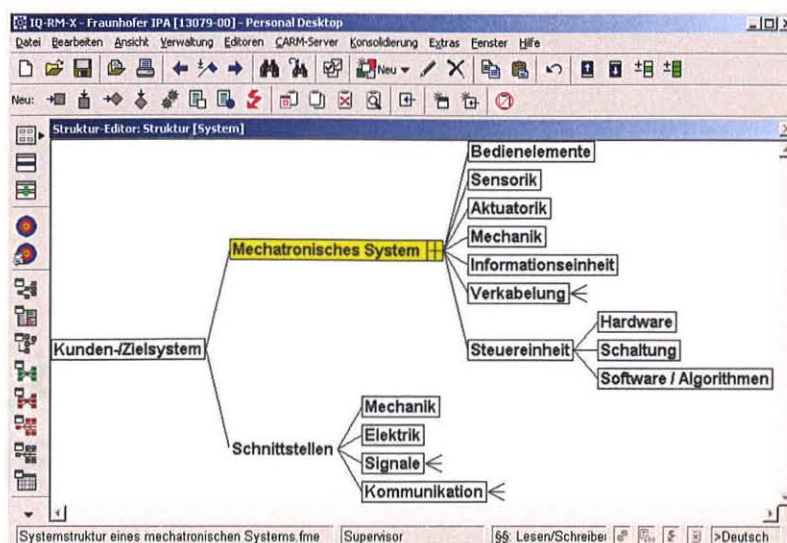
Fraunhofer

STRUKTURIERUNG VON MECHATRONISCHEN SYSTEMEN

© Fraunhofer



Mögliche Systemstruktur eines mechatronischen Systems



© Fraunhofer



Mögliche Maßnahmenstruktur eines mechatronischen Systems

ID-4M.3 - Fraunhofer IPA [13079-00] - Personal Desktop									
Formblatt (Datei VDA 96-Mechatronisches System (Struktur (System)))									
Fehlerfolge	B	K	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Erdeckungsmaßnahme	E	RPZ VIT
Funktion: Mechatronische Funktion									
[Handlen-Zielsystem] Fehlerfolge im Zielsystem	10	YC	[Mechatronisches System] Fehlerursache eines mechatronischen Systems	[Mechatronische Komponente] Fehlerursache einer mechatronischen Komponente	Maßnahmenstand: Anfang Entwicklung				
					Konzeptionelle Maßnahmen zur Vermeidung der Fehlerursache				
					2		10	200	Entwicklung
					Maßnahmenstand: Hardwaretest				
					Bestätigung der Auftretenswahrscheinlichkeit des Hardwarefehlers				
					4	Maßnahmen zum Test der korrekten Funktion der Hardware	2	80	Versuch
					Maßnahmenstand: Software-Regelwerk				
					Anforderungen an die Software bzw. Steuerung zur Überführung des Systems trotz des Hardwarefehlers in einen sicheren Zustand				
					4		10	(400)	Entwicklung
					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
					Maßnahmenstand: Gesamttest				
					Tests im Gesamtsystem				
					4		2	(80)	Entwicklung
					Maßnahmenstand: Service				
					Maßnahmen zur präventiven Instandhaltung im Service				
					4	Maßnahmen zur Erkennung der Fehlfunktion im Service	3	(120)	Service
					Maßnahmenstand: Betrieb				
					Maßnahmen zur Information des Benutzers über Fehlfunktionen im System				
					4		1	(40)	Kunde

- 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

© Fraunhofer

Fraunhofer

ERLÄUTERUNG ANHAND EINES BEISPIELSYSTEMS

© Fraunhofer

Fraunhofer

Beispielsystem (Fahrzeug zufällig gewählt)



1965

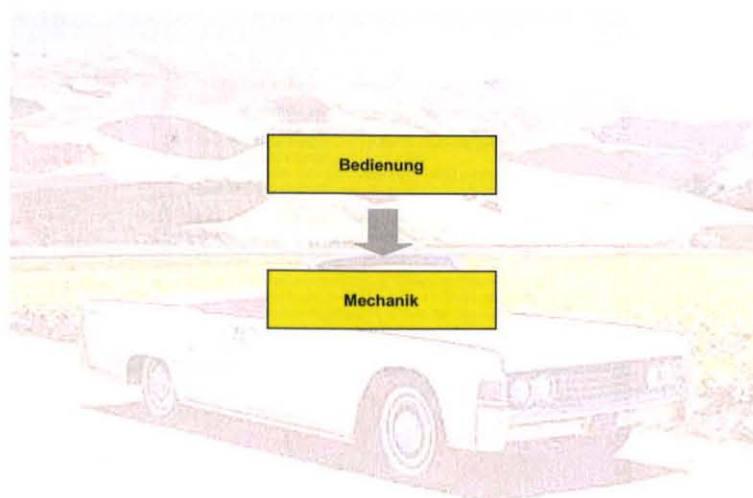


20xx ?

© Fraunhofer

 **Fraunhofer**

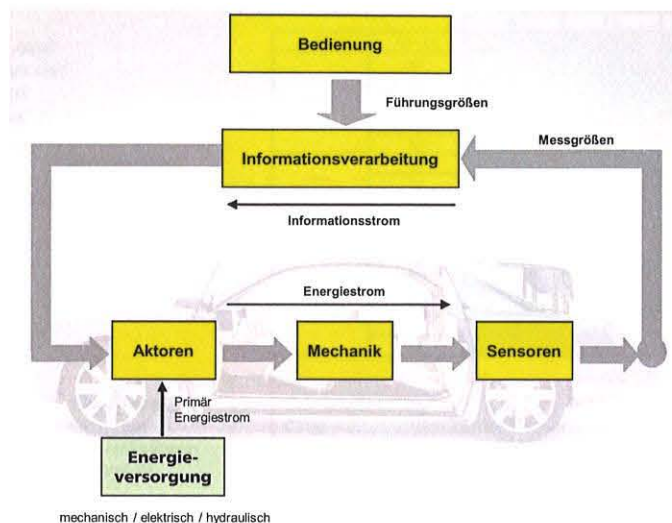
Von der Mechanik ...



© Fraunhofer

 **Fraunhofer**

... zur Mechatronik

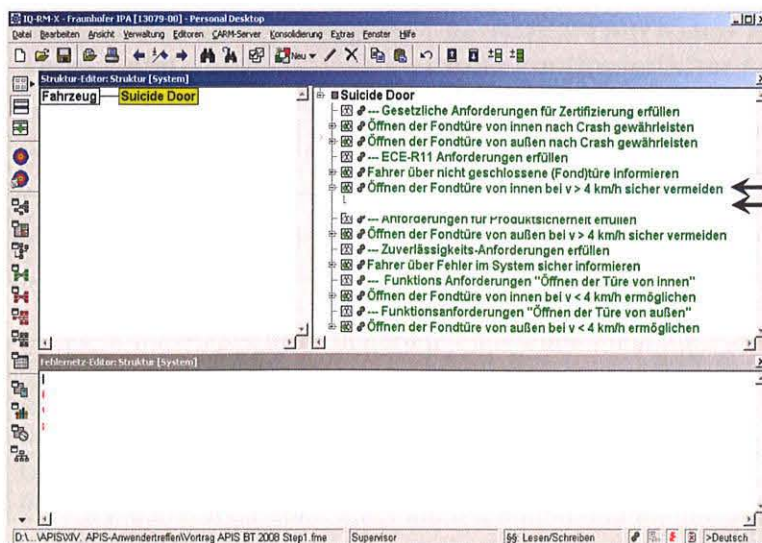


Quelle: in Anlehnung an Isermann (1999)

© Fraunhofer

Fraunhofer

Gefahren- und Risikoanalyse

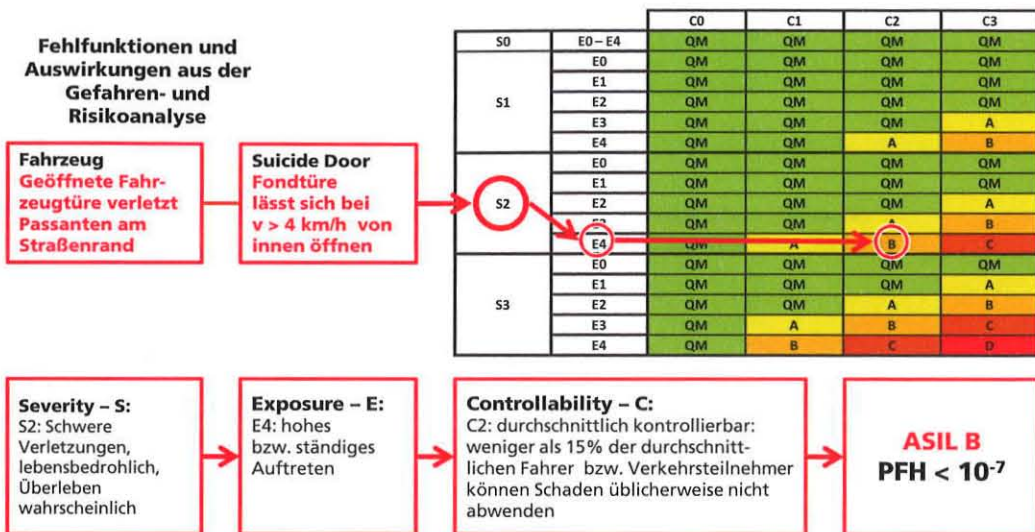


Hauptfunktion
Hauptfehlfunktion

© Fraunhofer

Fraunhofer

Möglicher Risikograph gemäß ISO DIS 26262



© Fraunhofer

Fraunhofer

Vorgabewerte ISO DIS 26262 in Abhängigkeit vom ASIL

Automotive Safety Integrity Level – ASIL	Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (PFH – Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
D	$< 10^{-8}$
C	$< 10^{-7}$
B	$< 10^{-7}$
A	$< 10^{-6}$

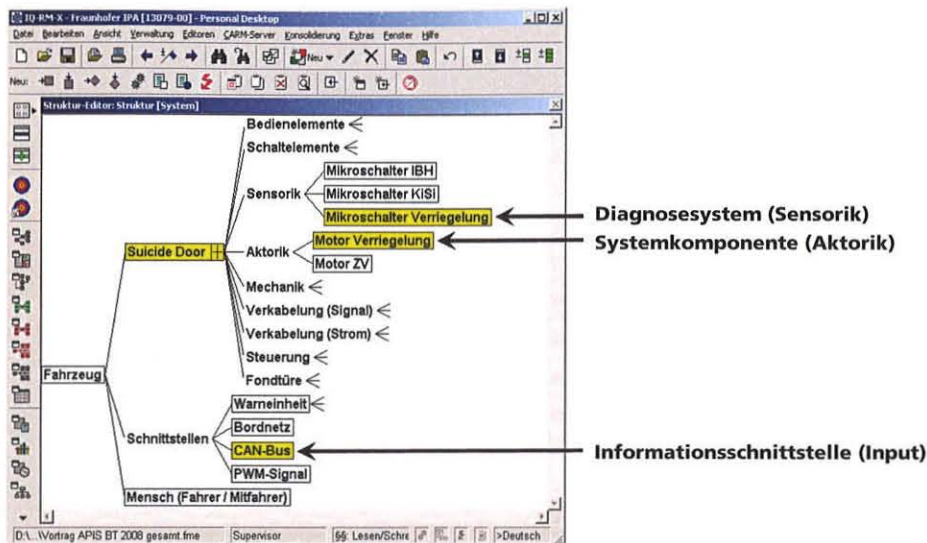
Metrik	ASIL A	ASIL B	ASIL C	ASIL D
Single point faults metric	Nicht relevant	>90%	>97%	>99%
Latent faults metric	Nicht relevant	>60%	>80%	>90%

[Quelle: ISO DIS 26262]

© Fraunhofer

Fraunhofer

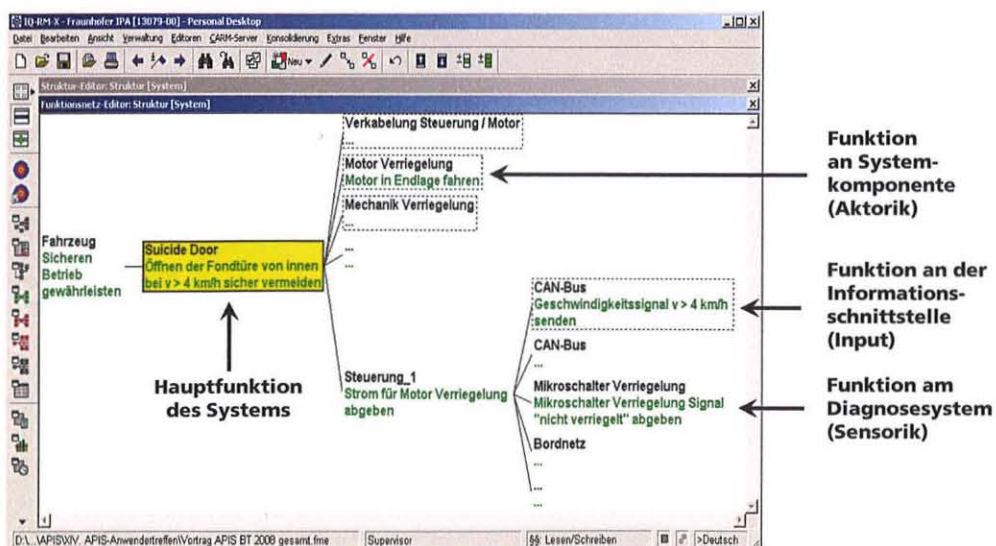
Mögliche Systemstruktur einer „Suicide Door“



© Fraunhofer

Fraunhofer

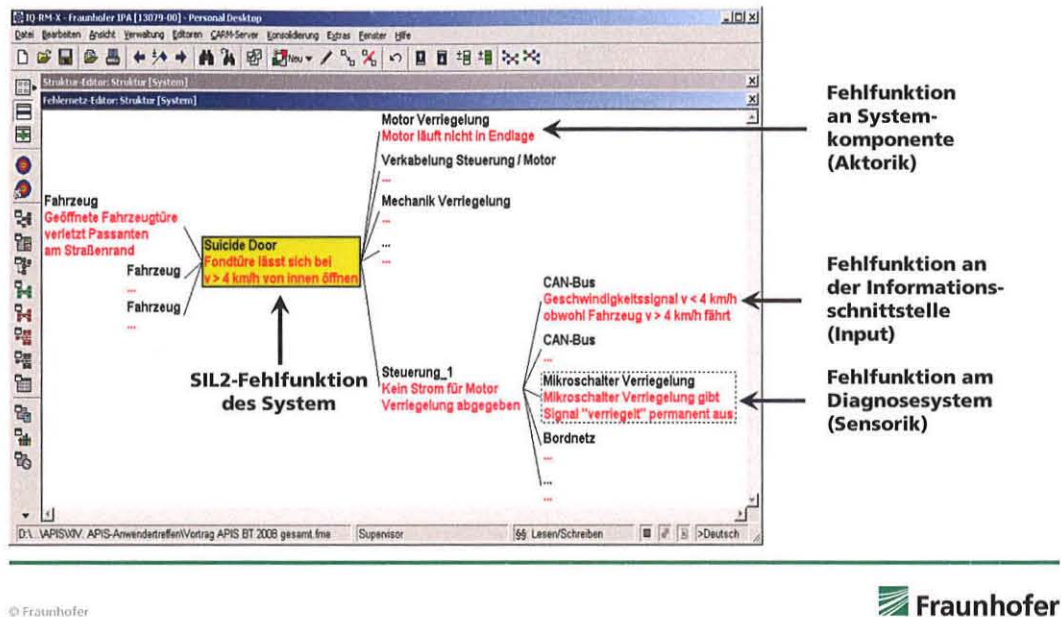
Mögliches Funktionsnetz einer „Suicide Door“



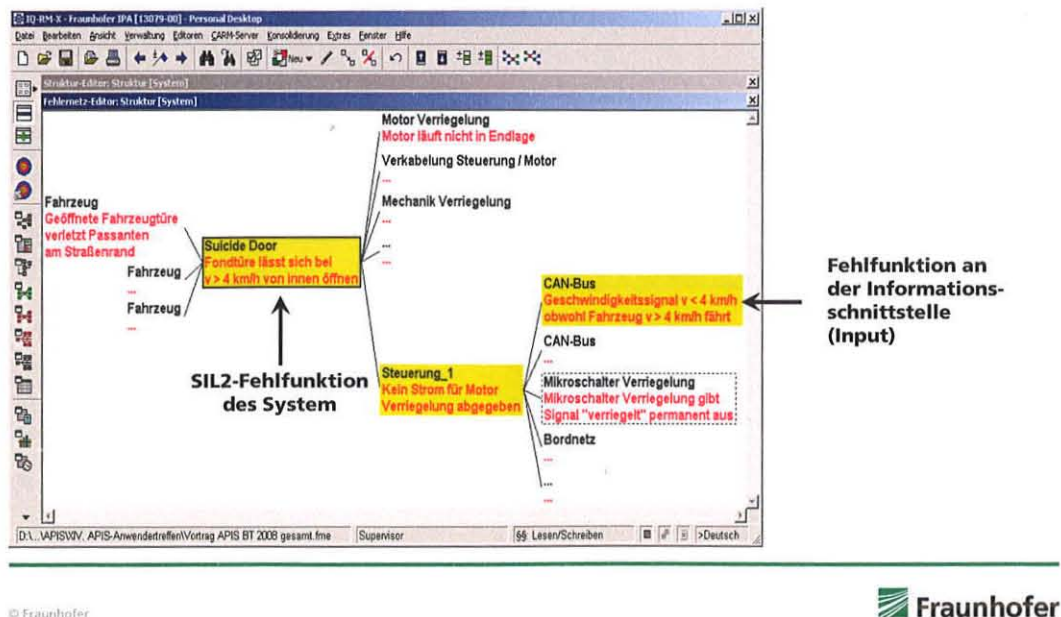
© Fraunhofer

Fraunhofer

Mögliches Fehlernetz einer „Suicide Door“



Mögliches Fehlernetz einer „Suicide Door“



Mögliches Formblatt einer „Suicide Door“

10-HM-X - Fraunhofer IPA [13079-00] - Personal Desktop

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

Struktur Editor Struktur (System)

Formblatt Editor VDA 96 Steuerung_1 (Struktur (System))

Fehlerfolge	B	K	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RPZ	VIT
Funktion: Strom für Motor Verriegelung abgeben										
[Suicide Door] Fundture lässt sich bei v > 4 km/h von innen öffnen				[CAN-Bus] Geschwindigkeitssignal v < 4 km/h obwohl Fahrzeug v > 4 km/h fährt						
>> [SIL-2] [Fahrzeug] Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand	10	CC								
>> [Fahrzeug]	10	CC								
>> [Fahrzeug]	0									
Maßnahmenstand - Anfang: Entwicklung										
Maßnahmenstand: Hardwaretest										
Maßnahmenstand: Software-Requirements										
Software-Requirement: Redundante Geschwindigkeitssignale (ABS/ESP und PWM) die in Steuerung_1 und Steuerung_2 unabhängig voneinander ausgewertet werden und als ODER-Logik die Verriegelung auslösen und die Warneinheit aktivieren										
Maßnahmenstand: Softwaretest										
Maßnahmenstand: Betrieb										

D:_LAPIS\WV_APIS-Anwendertreffen\Vortrag APIS BT 2008_gesamt.fme Supervisor Lesen/Schreiben >Deutsch

Sichere Verriegelung bei Fehlfunktion an der Informationschnittstelle (Input) und sichere Information des Fahrers.

© Fraunhofer

Fraunhofer

Mögliches Formblatt einer „Suicide Door“

10-HM-X - Fraunhofer IPA [13079-00] - Personal Desktop

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

Struktur Editor Struktur (System)

Formblatt Editor VDA 96 Steuerung_1 (Struktur (System))

Fehlerfolge	B	K	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RPZ	VIT
Funktion: Strom für Motor Verriegelung abgeben										
[Suicide Door] Fundture lässt sich bei v > 4 km/h von innen öffnen				[CAN-Bus] Geschwindigkeitssignal v < 4 km/h obwohl Fahrzeug v > 4 km/h fährt						
>> [SIL-2] [Fahrzeug] Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand	10	CC								
>> [Fahrzeug]	10	CC								
>> [Fahrzeug]	0									
Maßnahmenstand - Anfang: Entwicklung										
Maßnahmenstand: Hardwaretest										
Maßnahmenstand: Software-Requirements										
Maßnahmenstand: Softwaretest										
2 Test-Bench: Überprüfung, ob die Türe sicher verriegelt wird, wenn eine der beiden Steuerungen ein Geschwindigkeitssignal v > 4 km/h abgibt										
2 Test-Bench: Überprüfung, ob die Warneinheit sowohl über den Pfad Steuerung_1 als auch Steuerung_2 aktiviert wird										
2 (H) Manuall Softwaretest in Bearbeitung										

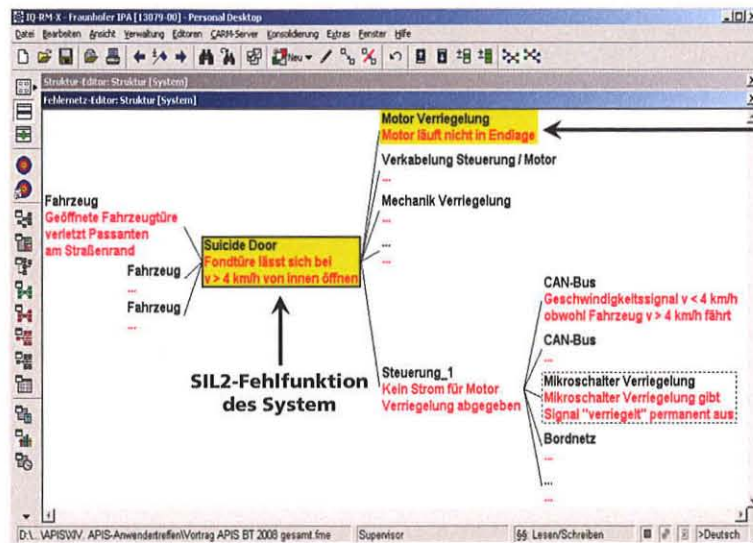
D:_LAPIS\WV_APIS-Anwendertreffen\Vortrag APIS BT 2008_gesamt.fme Supervisor Lesen/Schreiben >Deutsch

Überprüfung auf der Test Bench, ob die Software beim Auftreten der Fehlfunktion korrekt reagiert.

© Fraunhofer

Fraunhofer

Mögliches Fehlernetz einer „Suicide Door“



Fehlfunktion
an System-
komponente
(Aktorik)

© Fraunhofer

Fraunhofer

Mögliches Formblatt einer „Suicide Door“

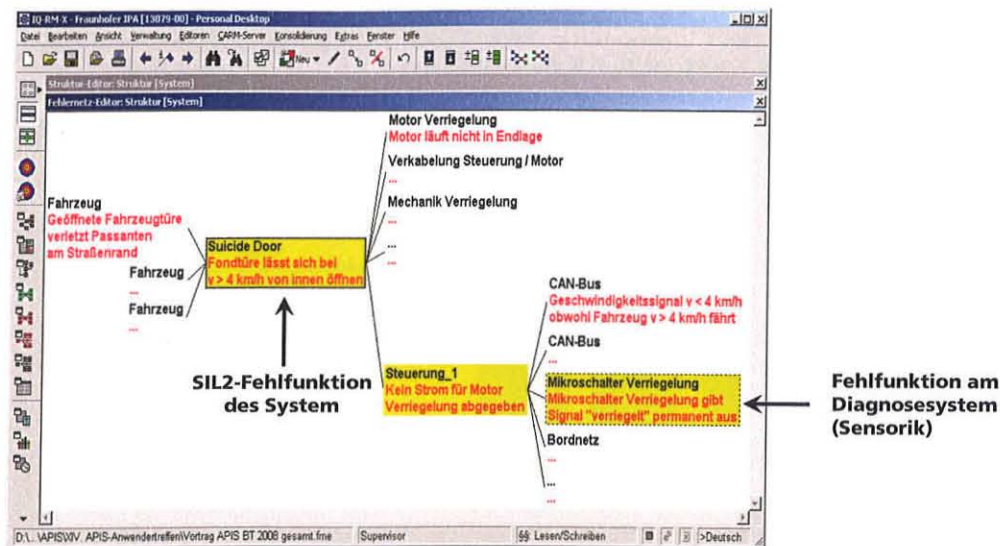
Struktur-Editor: Struktur (System)									
Formblatt-Editor VDA 91: Suicide Door (Struktur (System))									
Fehlerfolge	B	K	Fehlerart	Fehlerursache	Vermeldungsmaßnahme	A	Entdeckungsmaßnahme	E	RPZ VIT
Funktion: Öffnen der Fondtüre von innen bei v > 4 km/h sicher vermeiden									
(SIL-2) (Fahrzeug) Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand	10	CC	[Suicide Door] Fondtüre lässt sich bei v > 4 km/h von innen öffnen	[Motor Verriegelung] Motor läuft nicht in Endlage	Maßnahmenstand - Anfang: Entwicklung				
					Maßnahmenstand: Hardwaretest				
					Maßnahmenstand: Software-Requirements				
					Software-Requirement: Bei Überschreitung von v = 4 km/h und einem nicht aktivierten Mikroschalter Verriegelung wird der Motor für x sec angesteuert. Falls kein Signalwechsel am Mikroschalter Verriegelung erfolgt wird die Warneinheit aktiviert.	2		10	200
									Schlosse Software-Requirements abgeschlossen
					Maßnahmenstand: Softwaretest				
					Maßnahmenstand: Betrieb				

Sichere Erkennung
der Fehlfunktion
an der Aktuatorik
und sichere Informa-
tion des Fahrers.

© Fraunhofer

Fraunhofer

Mögliches Fehlernetz einer „Suicide Door“



© Fraunhofer

 Fraunhofer

Mögliches Formblatt einer „Suicide Door“

Datei Bearbeiten Ansicht Verwaltung Editoren Gantt-Server Konsolidierung Extras Fenster Hilfe												
Struktur Editor: Struktur [System]												
[Modellart (der VDA 96: Steuerung_1 (Struktur [System]))]												
Fehlerfolge	B	K	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Erdeckungsmaßnahme	E	RPZ_VIT			
Funktion: Strom für Motor Verriegelung abgeben												
[Suicide Door] Fenster lässt sich bei v > 4 km/h von innen öffnen >> [SIL=2] [Fahrzeug] Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand >> [Fahrzeug] 10 CC ... >> [Fahrzeug] 10 CC ... >> [Fahrzeug] 8 ...	10	CC	[Steuerung_1] Kein Strom für Motor Verriegelung abgeben [Mikroschalter Verriegelung] Mikroschalter Verriegelung gibt Signal "verriegelt" permanent aus	Maßnahmenstand - Anfang: Entwicklung	2		10	200				
				Zuverlässiger widerstandsfähiger Mikroschalter								
				Maßnahmenstand: Entwicklung				2		5	100	Henke Hardwaretest abgeschlossen
				Dauerschaltversuch des Mikroschalters unter Temperatureinfluss und Umgebungseiden Schaltversuch unter Extremtemperaturen nach längerer Liegezeit in beiden Schaltstellungen								
Maßnahmenstand: Betrieb				2	Information des Kunden: Keine Information des Kunden bei ausgefallenem Mikroschalter Verriegelung möglich	10	200	Kunde Betrieb in Bearbeitung				
[CAN-Bus] Geschwindigkeitssignal v < 4 km/h obwohl Fahrzeug v > 4 km/h fährt												

**Keine Erkennung
der Fehlfunktionen
an der Sensorik
und keine Infor-
mation des Fahrers**

© Fraunhofer

 Fraunhofer

Mögliche FSR eines Diagnosesystems der „Suicide Door“

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
Risiko/Unentdeckt / Unentdeckt
Unkritisch / Entdeckt

	B	E	F	G	J	K	L	M	N	S	T	Y
1	Antriebs aus FMEA											
2	Motorstart											
3	Einsteigen (hinten)											
4	Verriegelung bei >4 km/h											
5	Fahrt											
6	<4 km/h ohne Türöffnung											
7	<4 km/h mit Türöffnung											
8	Aussteigen (hinten)											
9	Verriegelung bei >4 km/h											
10	Fahrt											
11	Abstellen, Zündung aus											
12	Verbleibendes Fahren möglich											

3 Mikroschalter Verriegelung

4 Mikroschalter Verriegelung permanent auf "verriegelt"

5 Mikroschalter Verriegelung permanent auf "nicht verriegelt"

H < > H Mikroschalter Verriegelung / Inform

Bereit

© Fraunhofer

Fraunhofer

Mögliches Formblatt einer „Suicide Door“

10-HM-X - Fraunhofer IPA [13079-00] - Personal Desktop

Struktur-Editor: Struktur (System)

Formblatt-Editor: YOA 96-Steuerung_1 (Struktur (System))

Fahledolge	B	K	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RPZ	VIT
Funktion: Strom für Motor Verriegelung abgeben										
[Suicide Door]				[Steuerung_1] Kein Strom für Motor Verriegelung abgegeben						
Fondüre lässt sich bei >4 km/h von Innen öffnen										
>> [SIL=2] [Fahrzeug] Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand	10	CC								
>> [Fahrzeug] ...	10	CC								
>> [Fahrzeug] ...	8									
Maßnahmenstand - Anfang: Entwicklung										
Maßnahmenstand: Entwicklung										
Maßnahmenstand: Software Requirements										
Software-Requirement: Check des Mikroschalters Verriegelung bei "Zündung an" durch Ausführung eines Verriegelungszyklus. Falls von der Steuerung ein Mikroschalter Verriegelung kein Signalwechsel erkannt wird ist die Warneinheit einzuschalten.										
Maßnahmenstand: Softwaretest										
2 Test Bench: Überprüfung, ob die Warneinheit bei einem auf "verriegelt" ausgefallenen Mikroschalter aktiviert wird.										
Maßnahmenstand: Betrieb										
1 (20) Manusk. Softwaretest in Bearbeitung										

D:_VAPISWV_APIS-Anwender\ref\ Vortrag APIS BT 2008 gesamt ES.fne Supervisor 99 Lesen/Schreiben 11 11 >Deutsch

Sichere Erkennung von Fehlfunktionen an der Sensorik bei Zündung an und Information des Fahrers.

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

© Fraunhofer

Fraunhofer

Mögliche FSR eines Diagnosesystems der „Suicide Door“

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

Datei Bearbeiten Ansicht Einfügen Format Extras Daten Fenster ? Adgbe PDF Frage hier eingeben

Arial - 8 - F X U

O4 K/U

1		2																		
3		4																		
5		6																		
7		8																		
9		10																		
11		12																		
13		14																		
15		16																		
17		18																		
19		20																		
21		22																		
23		24																		
25		26																		
27		28																		
29		30																		
31		32																		
33		34																		
35		36																		
37		38																		
39		40																		
41		42																		
43		44																		
45		46																		
47		48																		
49		50																		
51		52																		
53		54																		
55		56																		
57		58																		
59		60																		
61		62																		
63		64																		
65		66																		
67		68																		
69		70																		
71		72																		
73		74																		
75		76																		
77		78																		
79		80																		
81		82																		
83		84																		
85		86																		
87		88																		
89		90																		
91		92																		
93		94																		
95		96																		
97		98																		
99		100																		
101		102																		
103		104																		
105		106																		
107		108																		
109		110																		
111		112																		
113		114																		
115		116																		
117		118																		
119		120																		
121		122																		
123		124																		
125		126																		
127		128																		
129		130																		
131		132																		
133		134																		
135		136																		
137		138																		
139		140																		
141		142																		
143		144																		
145		146																		
147		148																		
149		150																		
151		152																		
153		154																		
155		156																		
157		158																		
159		160																		
161		162																		
163		164																		
165		166																		
167		168																		
169		170																		
171		172																		
173		174																		
175		176																		
177		178																		
179		180																		
181		182																		
183		184																		
185		186																		
187		188																		
189		190																		
191		192																		
193		194																		
195		196																		
197		198																		
199		200																		
201		202																		
203		204																		
205		206																		
207		208																		
209		210																		
211		212																		
213		214																		
215		216																		
217		218																		
219		220																		
221		222																		
223		224																		
225		226																		
227		228																		
229		230																		
231		232																		
233		234																		
235		236																		
237		238																		
239		240																		
241		242																		
243		244																		
245		246																		
247		248																		
249		250																		
251		252																		
253		254																		
255		256																		

© Fraunhofer

 Fraunhofer

Mögliches Formblatt einer „Suicide Door“

The screenshot shows the 'Formblatt Editor VIDA 9.0: Steuerung_1 (Struktur [System])' window. The table below is a detailed view of the fault codes and measures listed in the screenshot.

Fehlerfolge	B	K	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	A	Entdeckungsmaßnahme	E	RPZ	VIT
[Suicide Door] Fonditure lässt sich bei v > 4 km/h von innen öffnen			[Steuerung_1] Kein Strom für Motor Verriegelung abgeben	[Mikroschalter Verriegelung] Mikroschalter Verriegelung gibt Signal "verriegelt" permanent aus	Maßnahmenstand - Anfang: Entwicklung					
>> [SIL-2] [Fahrzeug] Geöffnete Fahrzeugtüre verlässt Passanten am Straßenrand	10	CC			Maßnahmenstand: Entwicklung					
>> [Fahrzeug]	10	CC			Maßnahmenstand: Software-Requirements					
>> [Fahrzeug]	8				Maßnahmenstand: Softwaretest					
					Maßnahmenstand: Software-Requirements					
					Software-Requirement Nach jeder Öffnung (Fonditure) ist bei Überschreitung der Geschwindigkeit von v > 4 km/h an beiden Fondituren ein Verriegelungszyklus durchzuführen. Sollte dabei ein Mikroschalter keinen Signalwechsel haben ist die Warneinheit zu aktivieren.	1		10	(100)	Schlosse Software-Requirements in Bearbeitung
					Maßnahmenstand: Softwaretest					
					Maßnahmenstand: Betrieb					

**Sichere Erkennung
der Fehlfunktion
an der Sensorik
im Betrieb und
Information des
Fahrers im Betrieb.**

© Fraunhofer

 Fraunhofer

Mögliche FSR eines Diagnosesystems der „Suicide Door“

Microsoft Excel - FSR-Analyse Diagnosecheck 2008-08-16 ESals

Diagnosecheck

Regel:
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

	A	B	C	F	G	H	I	J	K	L	M	N	O	T	U	V	AA	
1	Diagnosecheck	Austritt aus EMEA	Check Mikroschalter Verriegelung	Motorstart	Einsteigen (hinten)	Verriegelung bei >4 km/h	Motor Verriegelung beibehalten	Mikroschalter Verriegelung auf "nicht verriegelt"	Motor Verriegelung in Endlage	Mikroschalter Verriegelung auf "verriegelt"	Fahrt	<4 km/h ohne Türöffnung	>4 km/h mit Türöffnung	Aussteigen (hinten)	Verriegelung bei >4 km/h	Fahrt	Abstellen, Zündung aus	Check Mikroschalter Verriegelung
2	Diagnoseelemente																	
3	Mikroschalter Verriegelung																	
4	Mikroschalter Verriegelung permanent auf "verriegelt"		UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE
5	Mikroschalter Verriegelung permanent auf "nicht verriegelt"		UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE	UE

H < > > > Mikroschalter Verriegelung / Inform < > <

Bereit

© Fraunhofer

Fraunhofer

Unterteilung der verschiedenen Fehlerarten

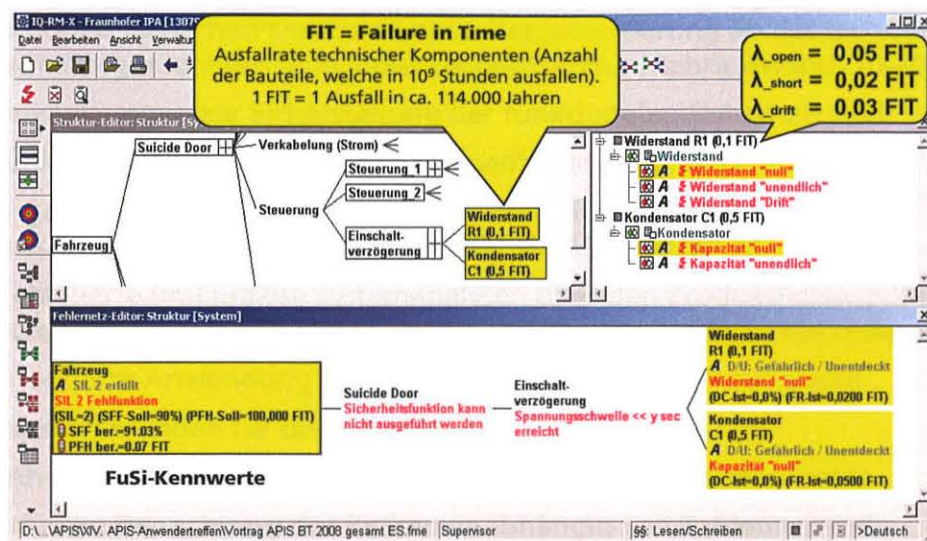


Abkürzung und Formel	Bedeutung
DC	Diagnostic coverage – Diagnosedeckungsgrad (0-100%)
$\lambda_S = \lambda_{SD} + \lambda_{SU}$	Sichere Fehler
$\lambda_{SD} = \lambda_S \cdot DC$	Sicherer Fehler, der entdeckt werden kann (SD = Safe Detected)
λ_{SU}	Sicherer Fehler, der nicht entdeckt werden kann (SU = Safe Undetected)
$\lambda_D = \lambda_{DD} + \lambda_{DU}$	Gefährlicher Fehler
$\lambda_{DD} = \lambda_D \cdot DC$	Gefährlicher Fehler, der entdeckt werden kann (DD = Dangerous Detected)
λ_{DU}	Gefährlicher Fehler, der nicht entdeckt werden kann (DU = Dangerous Undetected)

© Fraunhofer

Fraunhofer

FuSi-Kennwerte anhand von Fehlernetzen und Ausfallraten



© Fraunhofer

Fraunhofer

FAZIT

© Fraunhofer

Fraunhofer

Fazit

Funktionale Sicherheit stellt eine neue Herausforderung an das technische Risikomanagement dar (von Industrie geschätzter Mehraufwand: 10-20%)

Voraussetzungen zur Sicherstellung der funktionalen Sicherheit sind:

- Funktionierende Qualitätsmanagementsysteme (z.B. nach TS 16949)
- Organisatorische Erweiterungen für das Safety Management entsprechend den Anforderungen der IEC 61508 bzw. ISO CD 26262
- Detaillierte und präzise Systemanalysen über den Produktlebenszyklus durch den OEM sowie Weitergabe der Anforderungen an die Lieferanten
- Integrierte Anwendung vorhandener technischer Risikoanalysen

Herausforderungen für die Zukunft:

- Entwicklung integrierter Analysemethoden und Analysesoftware
- Kritische Betrachtung der Risiken unabhängig von Zahlenwerten