FMEA und Funktionale Sicherheit

Dr. Alexander Schloske

FMEA UND FUNKTIONALE SICHERHEIT

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

TÜV Functional Safety Engineer
Safety Instrumented Systems
ID: 1427/08
TÜV FS Engineer
TÜV Rheinland Group

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 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

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. programmierbar 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

Fraunhofer

Begriffe der funktionalen Sicherheit

- Sicherheitsfunktion

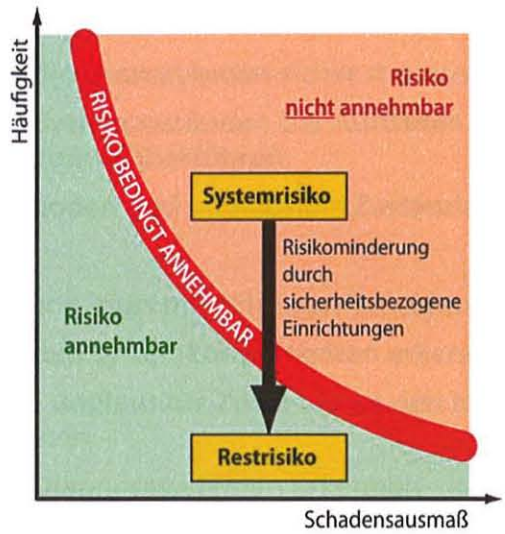
  Funktion eines sicherheitsbezogenen Systems, um im Gefahrfall einen Zustand mit tolerierbarem Restrisiko einzunehmen oder aufrecht zu erhalten
- Sicherheitsintegrität

  „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 Sicher.-heitsintegrität der Sicherheitsfunktionen (SIL1 bis SIL4 bei IEC 61508 bzw. ASIL A bis ASIL D bei ISO DIS 26262)

Fraunhofer

Grundprinzip der Funktionalen Sicherheit: „Risikominderung"



Fraunhofer

SOFTWARE IN MECHATRONISCHEN SYSTEMEN

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 Informations-schnittstellen erkennen
- Fehlfunktionen im Diagnosesystemen erkennen (kann ich meinem Diagnosesystem noch trauen?)

Fraunhofer

METHODEN ZUR ANALYSE MECHATRONISCHER SYSTEME

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

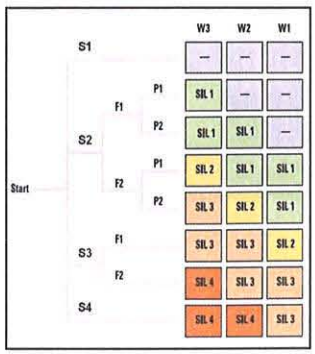
- Fehlermöglichkeits- und Einflussanalyse (FMEA)
- Fehlerbasierte System-Reaktionsanalyse (FSR) und Paarvergleichsmatrix
- Fehlerbaumanalyse (FBA)

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:

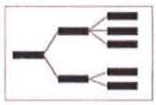
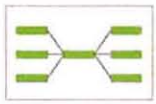
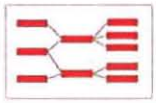
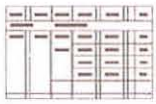
- Definition der Hauptfunktionen des Systems
- Ermittlung der potentiellen Fehlfunktionen
- Ermittlung der Gefahren und Risiken
- Ermittlung des SIL-Levels anhand Risikograph

Nutzen/Anmerkung:

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

Fraunhofer

Fehlermöglichkeits- und Einflussanalyse (FMEA)

1. 
2. 
3. 
4. 
5. 

Zielsetzung:

- Systematische Ermittlung potentieller Fehlfunktionen für die Komponenten des Systems

Methode nach VDA 4 Kapitel 3 (2006):

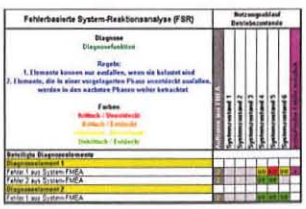
1: Strukturanalyse (Strukturbaum)
2: Funktionsanalyse (Funktionsnetze)
3: Fehleranalyse (Fehlernetze)
4: Maßnahmenanalyse und Bewertung
5: Optimierung (falls notwendig)

Nutzen/Anmerkung:

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

Fraunhofer

Fehlerbasierte System-Reaktionsanalyse (FSR)



Zielsetzung:

- Analyse der Diagnose- und Absicherungsmaßnahmen auf systematische Fehler

Methode:

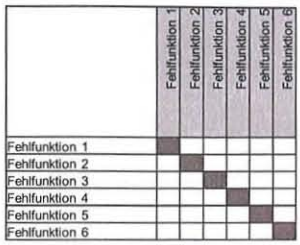
- Übernahme der Fehlfunktionen aus der System-FMEA für alle beteiligten Komponenten
- Bewertung der Entdeckbarkeit unter Berücksichtigung von nutzerbedingten Interaktionen und Systemzuständen

Nutzen/Anmerkung:

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

Fraunhofer

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:

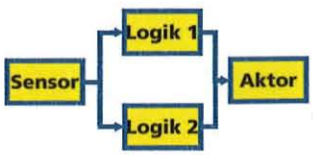
- Gegenüberstellung schlafender Fehler in der Paarvergleichsmatrix
- Bewertung der Auswirkungen und Entdeckbarkeit in Abhängigkeit des zeitlichen Auftretens

Nutzen/Anmerkung:

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

Fraunhofer

Reliability Block Diagramm



Teilsysteme der Sicherheitsfunktion

Zielsetzung:

- Hilfsmittel zur Zerlegung der an der Sicherheitsfunktion beteiligten Teilsysteme

Methode:

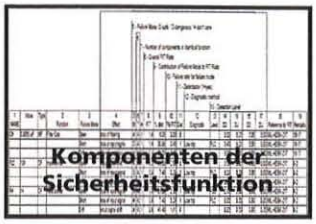
- Abbildung der an der Sicherheitsfunktion beteiligten Teilsysteme entsprechend der Architektur
  - Seriell
  - Parallel
  - Common cause

Nutzen/Anmerkung:

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

Fraunhofer

Failure Modes, Effects and Diagnostic Analysis (FMEDA)



FMEDA

Zielsetzung:

- Analyse der Fehlermodi der an der Sicherheitsfunktion beteiligten Komponenten

Methode:

- Auflistung aller Fehlerarten der an der Sicherheitsfunktion beteiligten Komponenten
- Bewertung der Ausfälle in „Sichere Ausfälle" und „Gefährliche Ausfälle"
- Ermittlung der Kennwerte λ, λ_S, λ_D, λ_{DD}, λ_{DU}

Nutzen/Anmerkung:

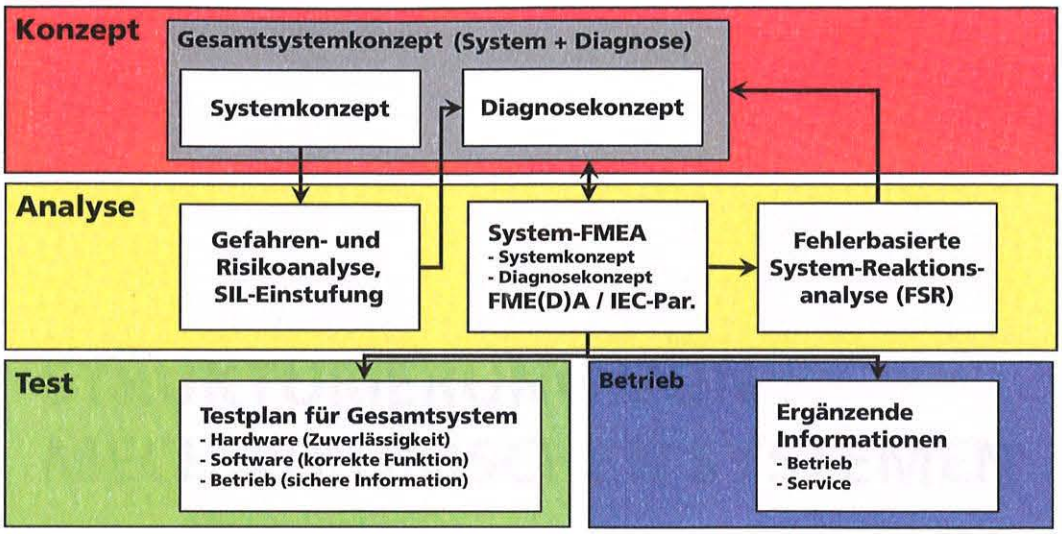
- Tabellarisches Verfahren zur Vorbereitung der Berechnung der FuSi-Parameter PFH, PFD u. SFF

Fraunhofer

AUSLEGUNG / ABSICHERUNG MECHATRONISCHER SYSTEME

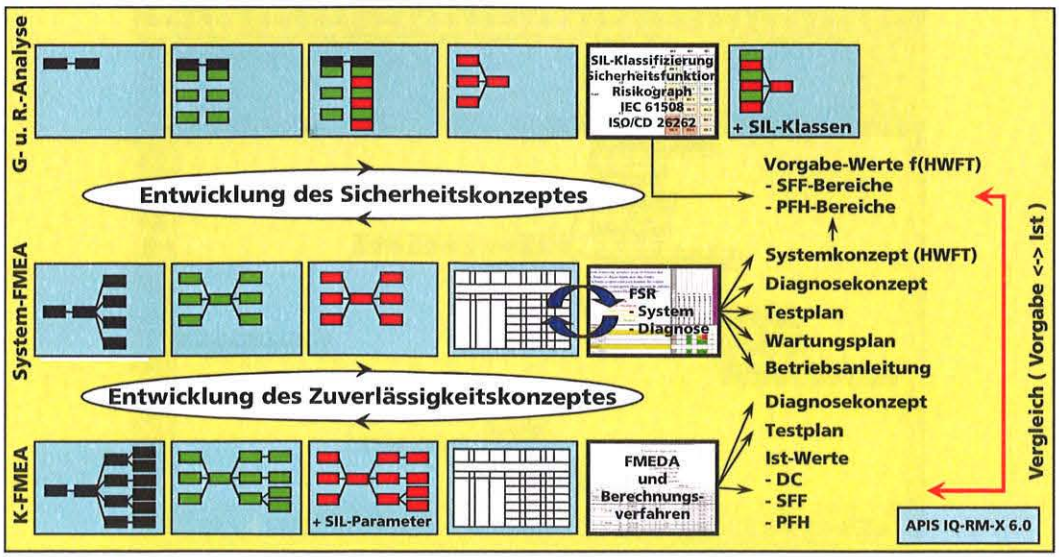
Fraunhofer

Auslegung und Absicherung von mechatronischen Systemen



Fraunhofer

Unterstützung der Analysen zur Funktionalen Sicherheit

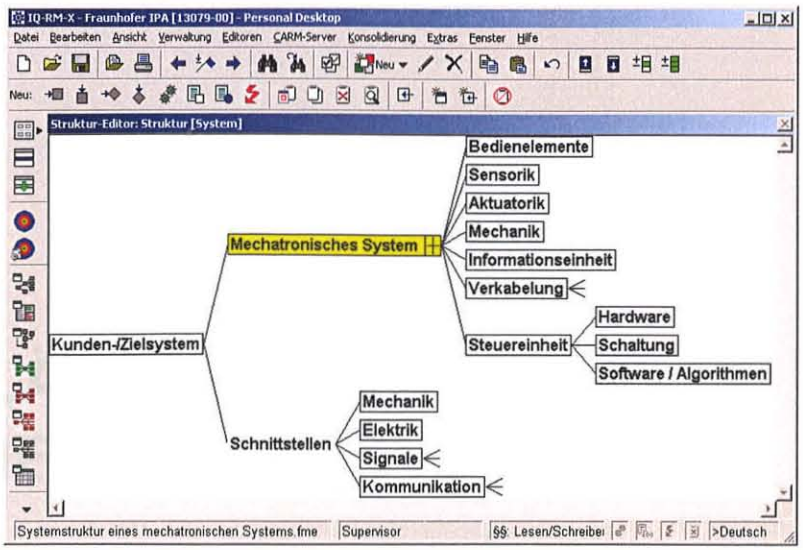


Fraunhofer

STRUKTURIERUNG VON MECHATRONISCHEN SYSTEMEN

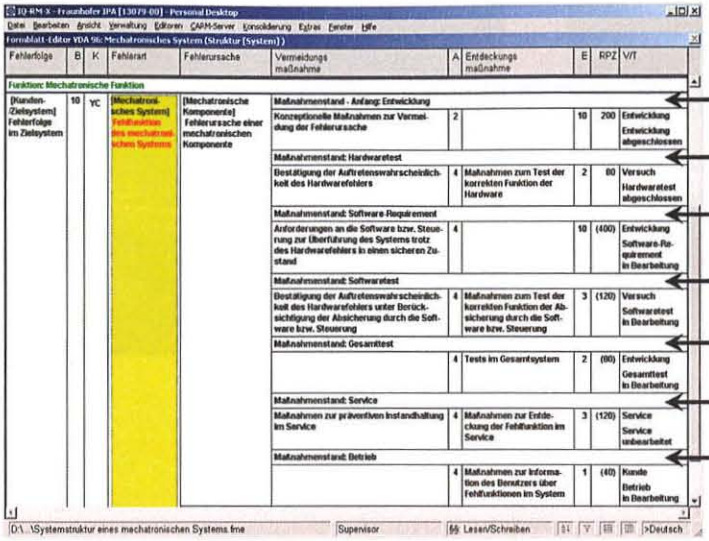
Fraunhofer

Mögliche Systemstruktur eines mechatronischen Systems



Fraunhofer

Mögliche Maßnahmenstruktur eines mechatronischen Systems



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

ERLÄUTERUNG ANHAND EINES BEISPIELSYSTEMS

Fraunhofer

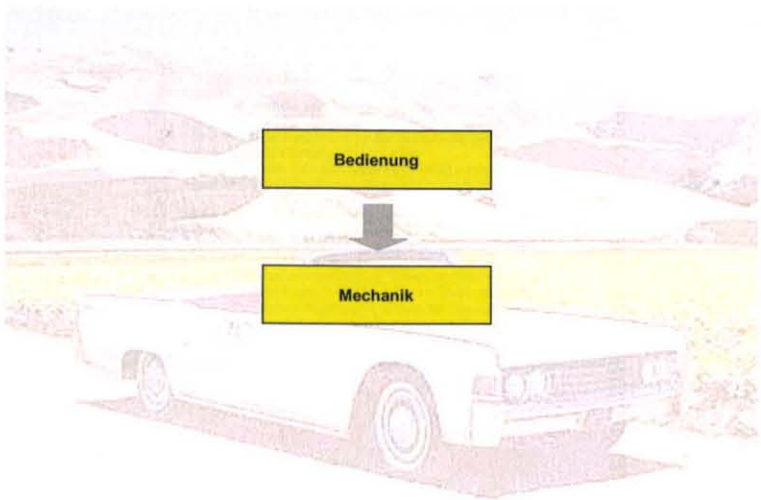
Beispielsystem (Fahrzeug zufällig gewählt)

1965

20xx ?

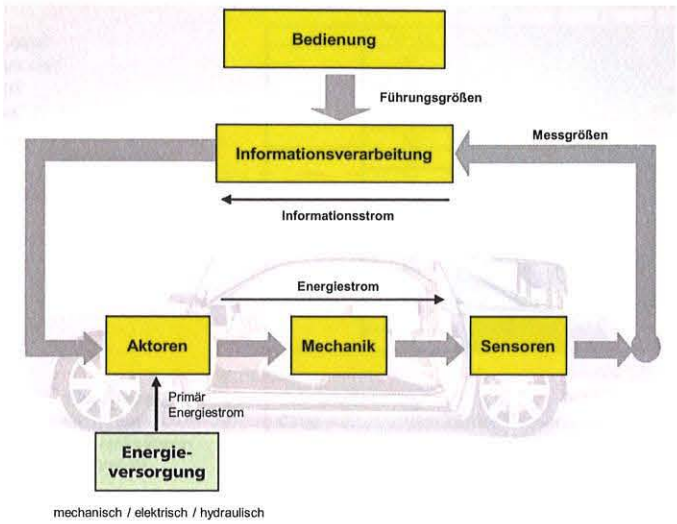
Fraunhofer

Von der Mechanik ...



Fraunhofer

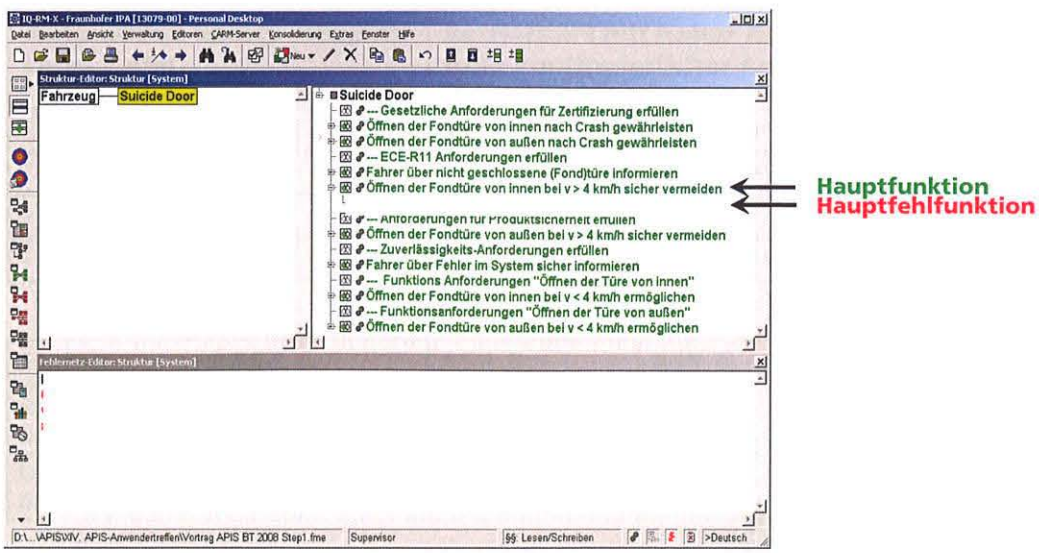
... zur Mechatronik



Quelle: in Anlehnung an Isermann (1999)

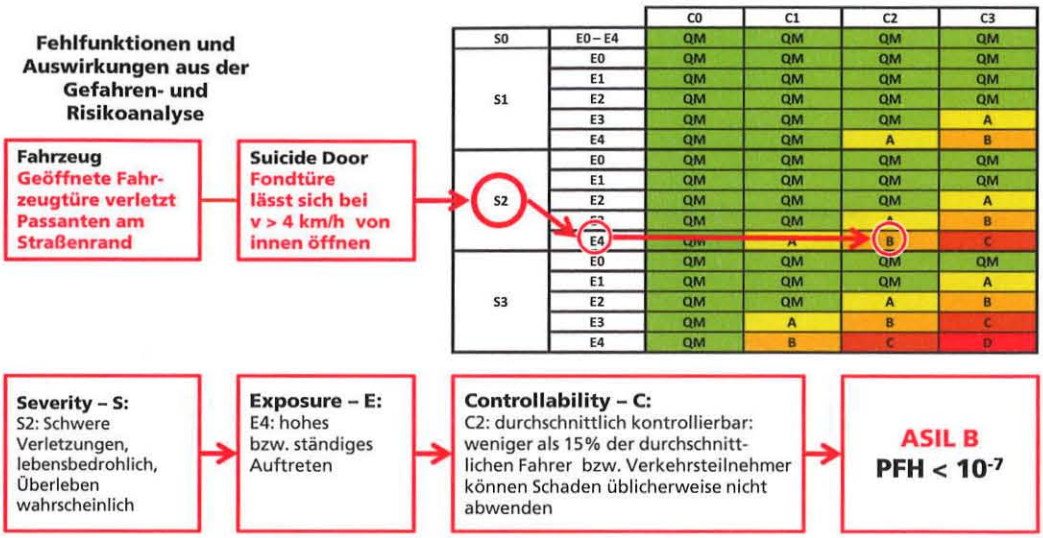
Fraunhofer

Gefahren- und Risikoanalyse



Fraunhofer

Möglicher Risikograph gemäß ISO DIS 26262



		C0	C1	C2	C3
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

Fraunhofer

Vorgabewerte ISO DIS 26262 in Abhängigkeit vom ASIL

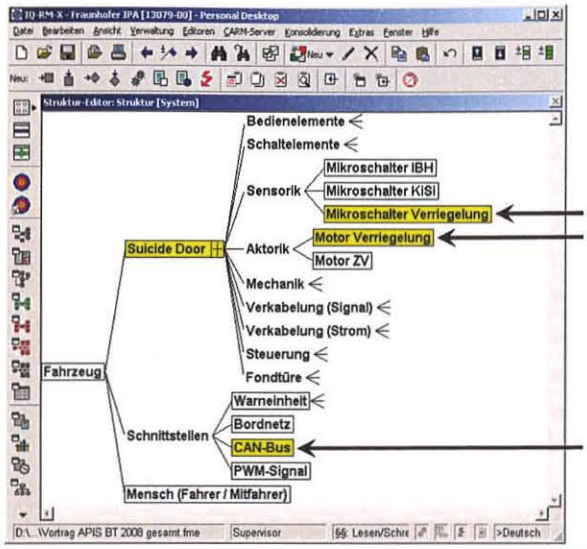
Automotive Safety Integrity Level – ASIL	**Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung** (PFH – Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
D	$< 10^{-8}$
C	$< 10^{-7}$
B	$< 10^{-7}$
A	$< 10^{-6}$

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]

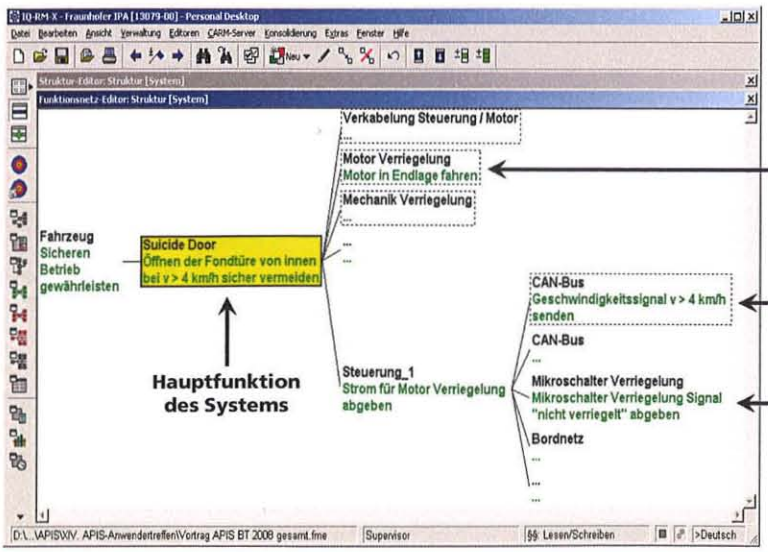
Fraunhofer

Mögliche Systemstruktur einer „Suicide Door"



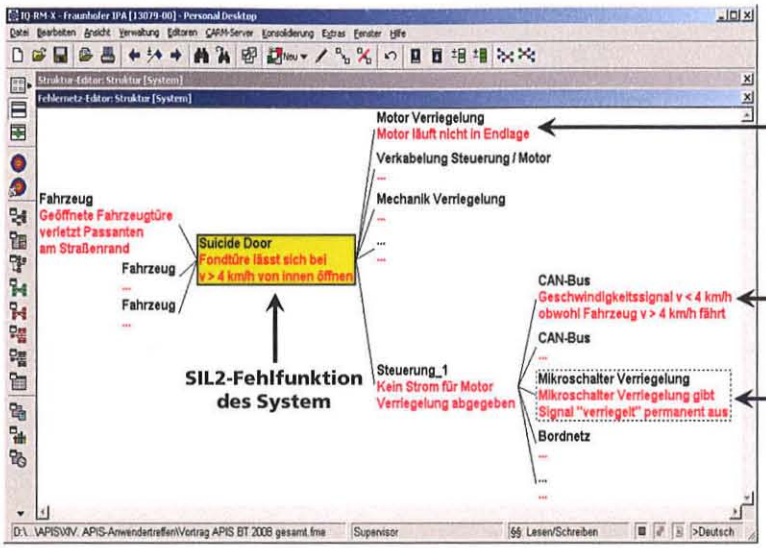
Fraunhofer

Mögliches Funktionsnetz einer „Suicide Door"



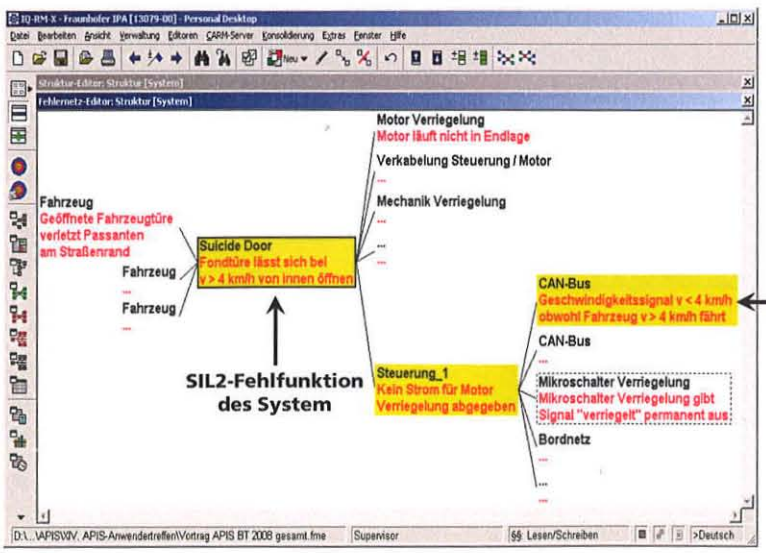
Fraunhofer

Mögliches Fehlernetz einer „Suicide Door“



Fraunhofer

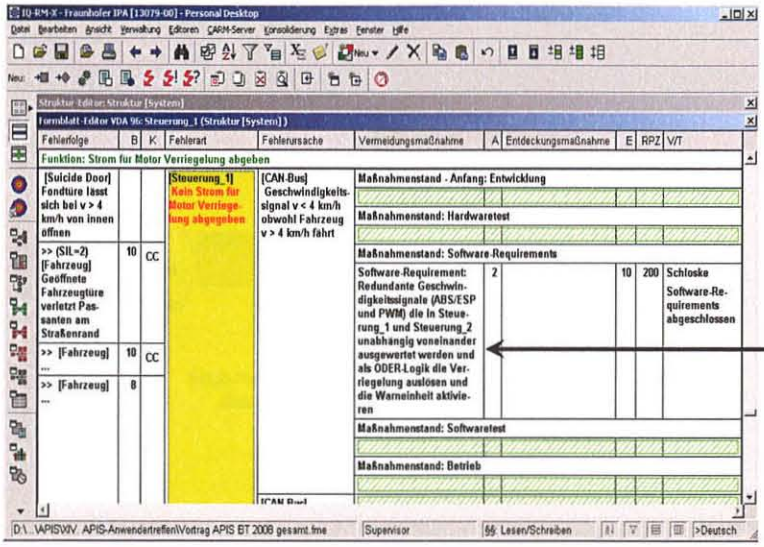
Mögliches Fehlernetz einer „Suicide Door“



© Fraunhofer

Fraunhofer

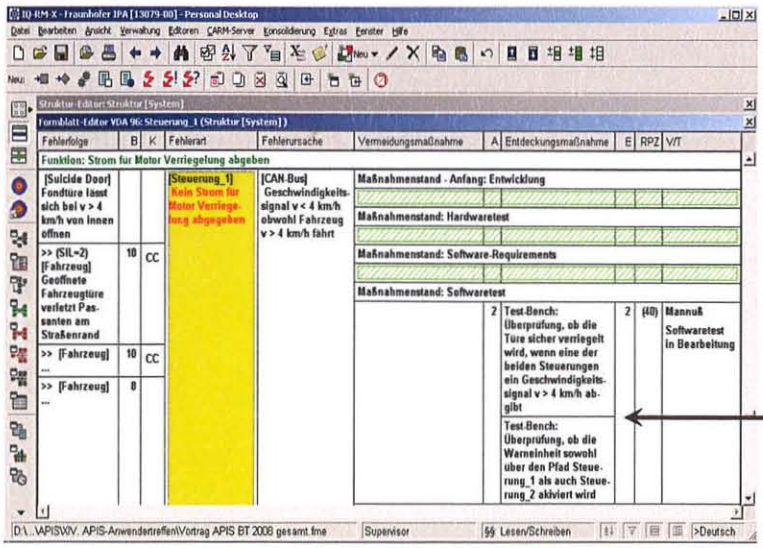
Mögliches Formblatt einer „Suicide Door"



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

Fraunhofer

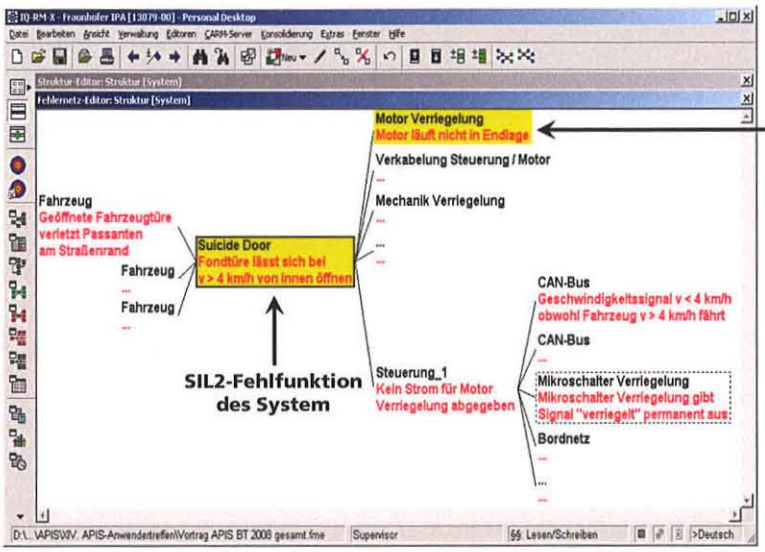
Mögliches Formblatt einer „Suicide Door"



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

Fraunhofer

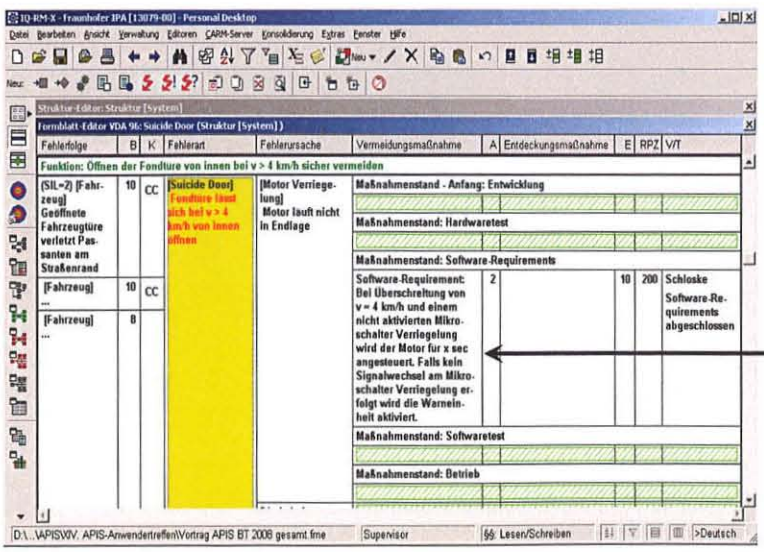
Mögliches Fehlernetz einer „Suicide Door“



Fehlfunktion an System-komponente (Aktorik)

Fraunhofer

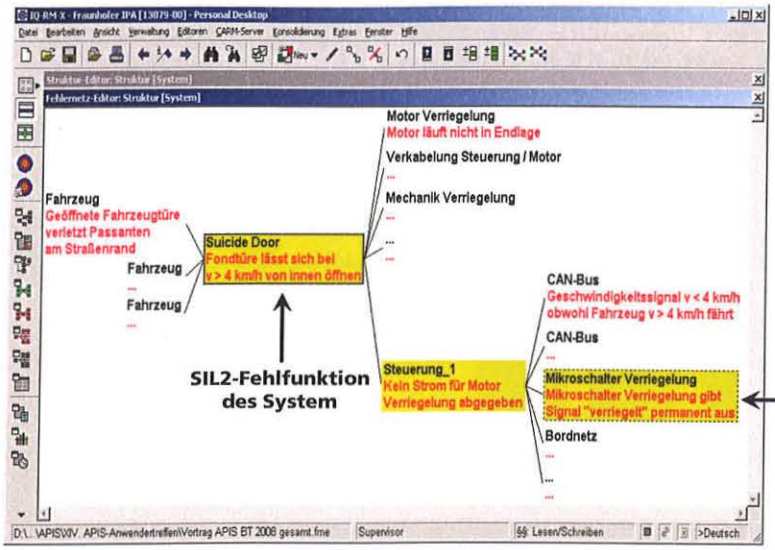
Mögliches Formblatt einer „Suicide Door“



Sichere Erkennung der Fehlfunktion an der Aktuatorik und sichere Information des Fahrers.

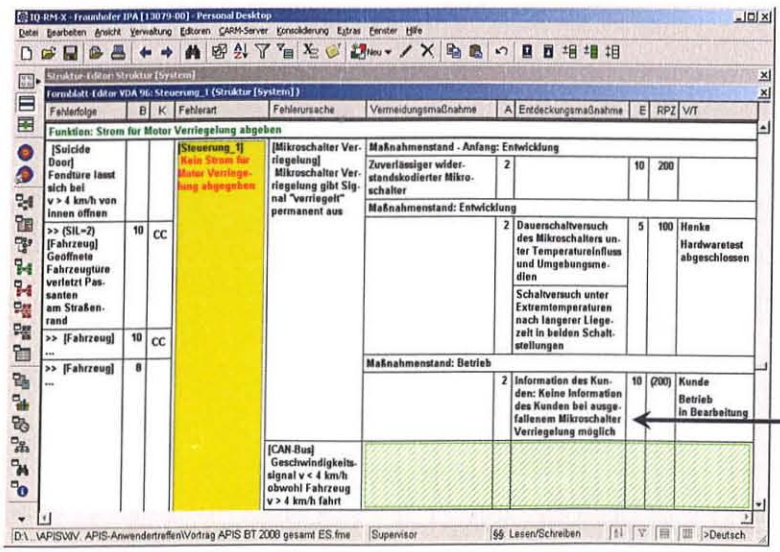
Fraunhofer

Mögliches Fehlernetz einer „Suicide Door“



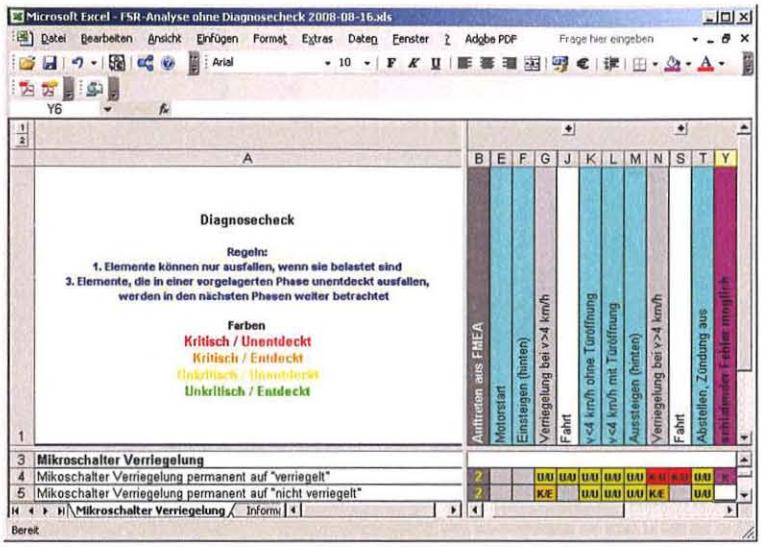
Fraunhofer

Mögliches Formblatt einer „Suicide Door“



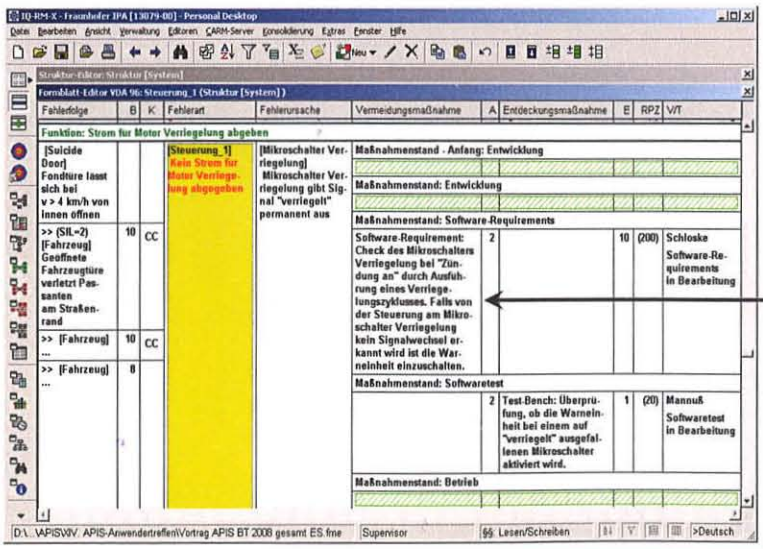
Fraunhofer

Mögliche FSR eines Diagnosesystems der „Suicide Door"



Fraunhofer

Mögliches Formblatt einer „Suicide Door"

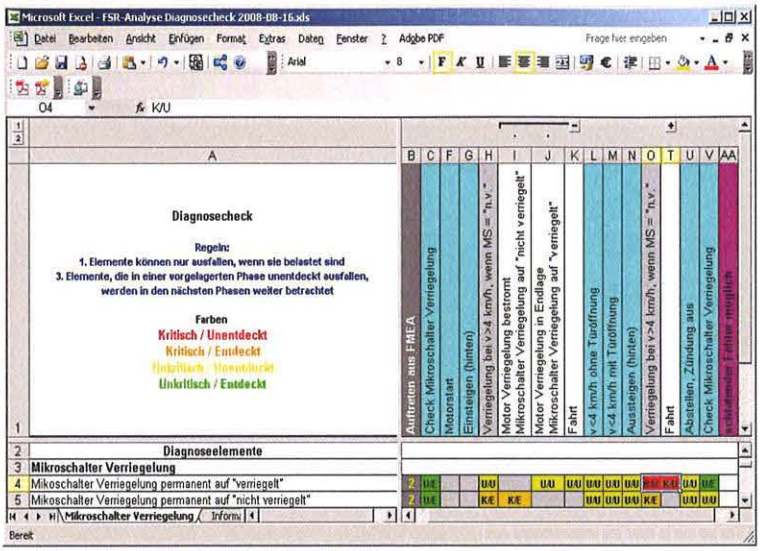


Sichere Erkennung von Fehlfunktionen an der Sensorik bei Zündung an und Information des Fahrers.

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

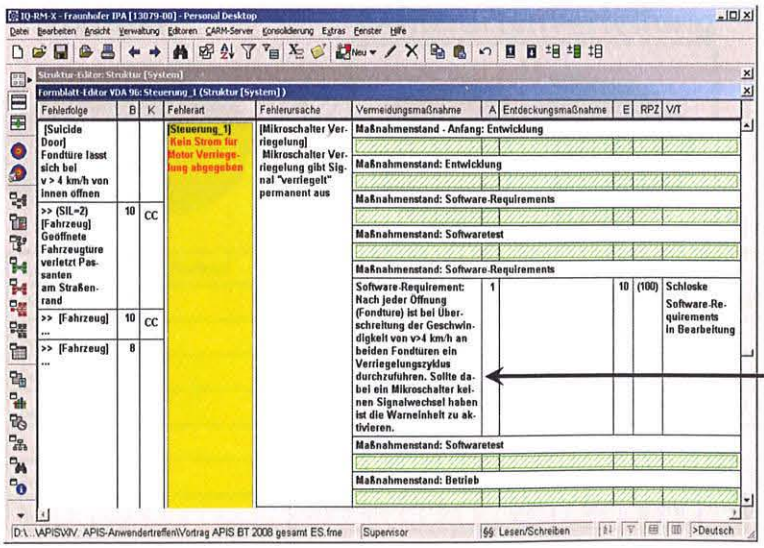
Fraunhofer

Mögliche FSR eines Diagnosesystems der „Suicide Door“



Fraunhofer

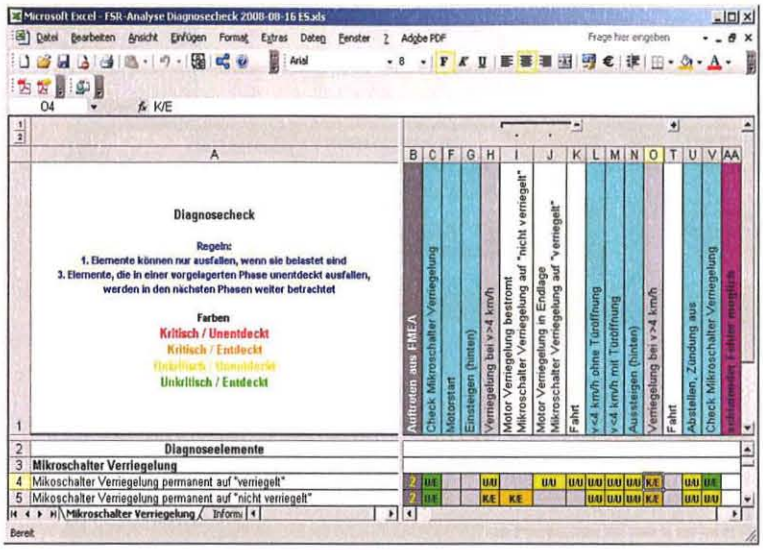
Mögliches Formblatt einer „Suicide Door“



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

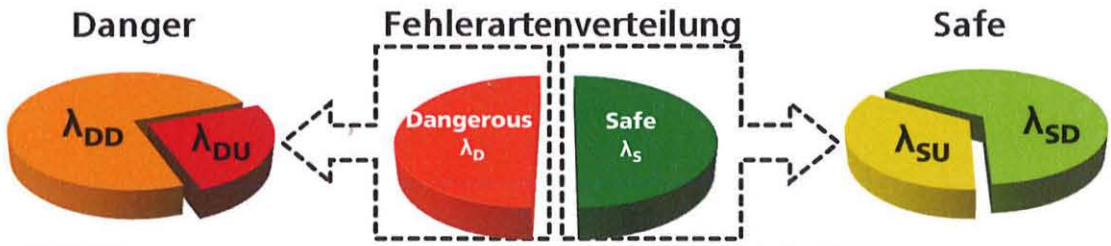
Fraunhofer

Mögliche FSR eines Diagnosesystems der „Suicide Door"



Fraunhofer

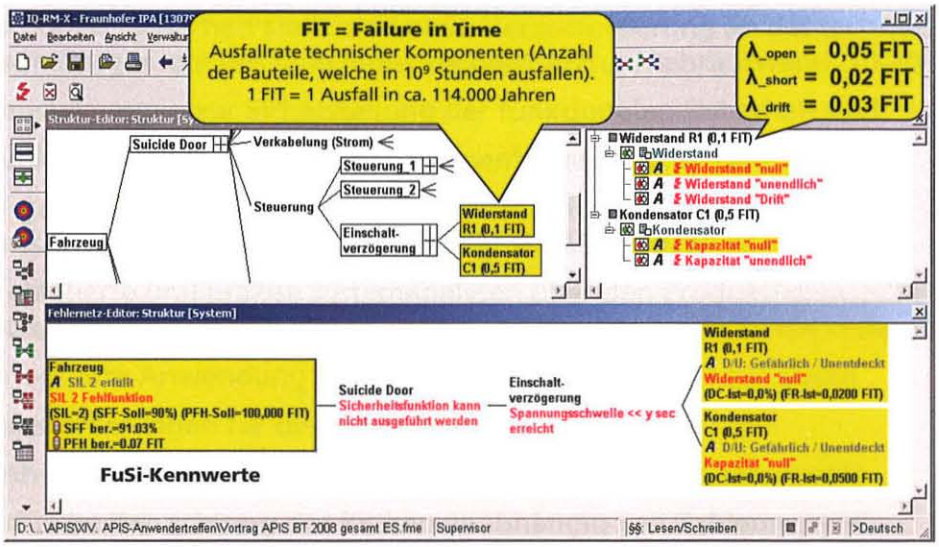
Unterteilung der verschiedenen Fehlerarten



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

Fraunhofer

FuSi-Kennwerte anhand von Fehlernetzen und Ausfallraten



Fraunhofer

FAZIT

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

Fraunhofer