
ERFAHRUNGSBERICHT AUS EINEM FUSI-PROJEKT NACH DIN EN 61508 IM AUTOMOTIVE UMFELD

EUROFORUM-Jahrestagung ISO 26262, 26.-27. September 2011, 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



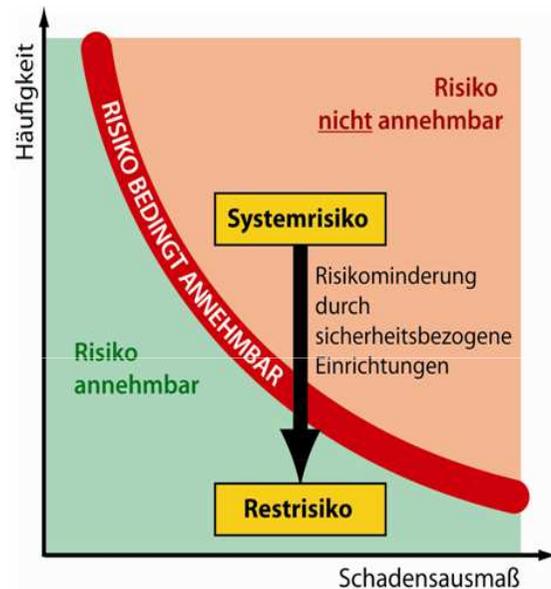
Erfahrungsbericht aus einem FuSi-Projekt nach DIN EN 61508

Vortragsinhalte

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

Funktionale Sicherheit

Definition und Zielsetzung



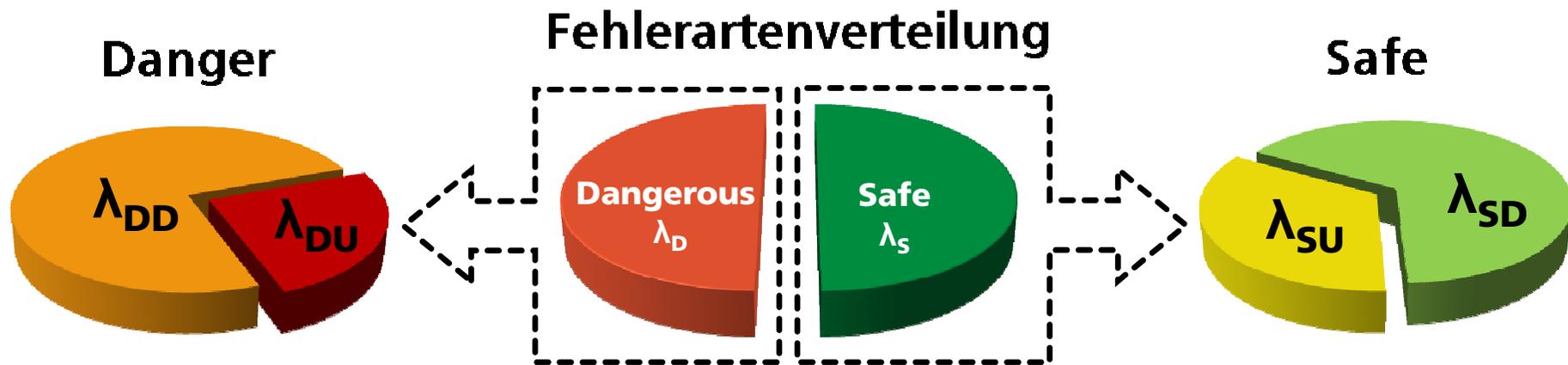
Funktionale Sicherheit ist die Fähigkeit eines elektrischen, elektronischen od. programmierbar elektronischen Systems (E/E/PE-System), beim Auftreten

- systematischer Ausfälle (z.B. fehlerhafte Systemauslegung)
- zufälliger Hardwareausfälle (z.B. Alterung von Bauteilen)

mit gefahrbringender Wirkung, einen sicheren Zustand einzunehmen bzw. in einem sicheren Zustand zu bleiben.

Fehlerarten für zufällige Fehler

Unterteilung der verschiedenen Fehlerarten



Abkürzung und Formel	Bedeutung
DC	Diagnostic coverage – Diagnoseddeckungsgrad (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)

Kennwerte der DIN EN 61508 zur Funktionalen Sicherheit

Anteil sicherer Ausfälle – SFF (Safe Failure Fraction)

Diagnosedeckungsgrad – DC (Diagnostic Coverage)

Bestimmung aller zufälligen Ausfallarten der an einer Sicherheitsfunktion beteiligten E/E-Bauteile und Einstufung in

- gefahrbringend (dangerous)
- ungefährlich (safe)
- entdeckbar (detected)
- nicht entdeckbar (undetected)

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

Anteil ungefährlicher Ausfälle
(safe failure fraction)

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

Diagnosedeckungsgrad
(diagnostic coverage)

Quelle: DIN EN 61508

Vorgabewerte der DIN EN 61508 in Abhängigkeit vom SIL

Beispiel SIL 2

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

Ausfallwahrscheinlichkeit

- PFH = Probability of Failures per Hour
- PFD = Probability of Failures on Demand

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
≥ 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

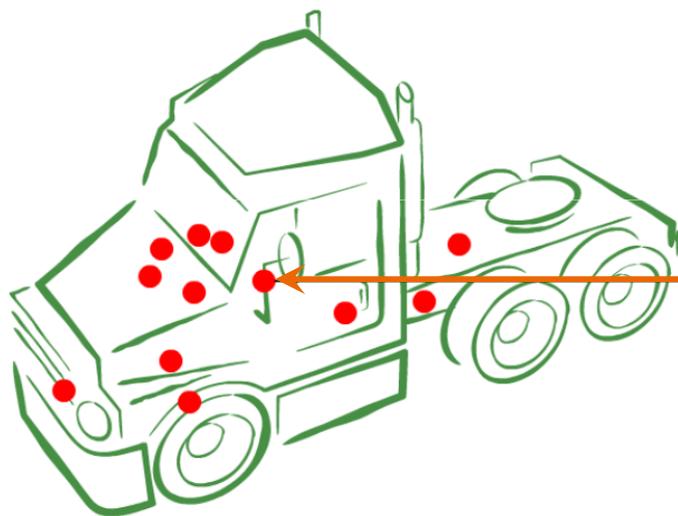
Quelle: DIN EN 61508

6

PRODUKT UND PROJEKTUMFELD

Produkt- und Projektumfeld

Drehschalter



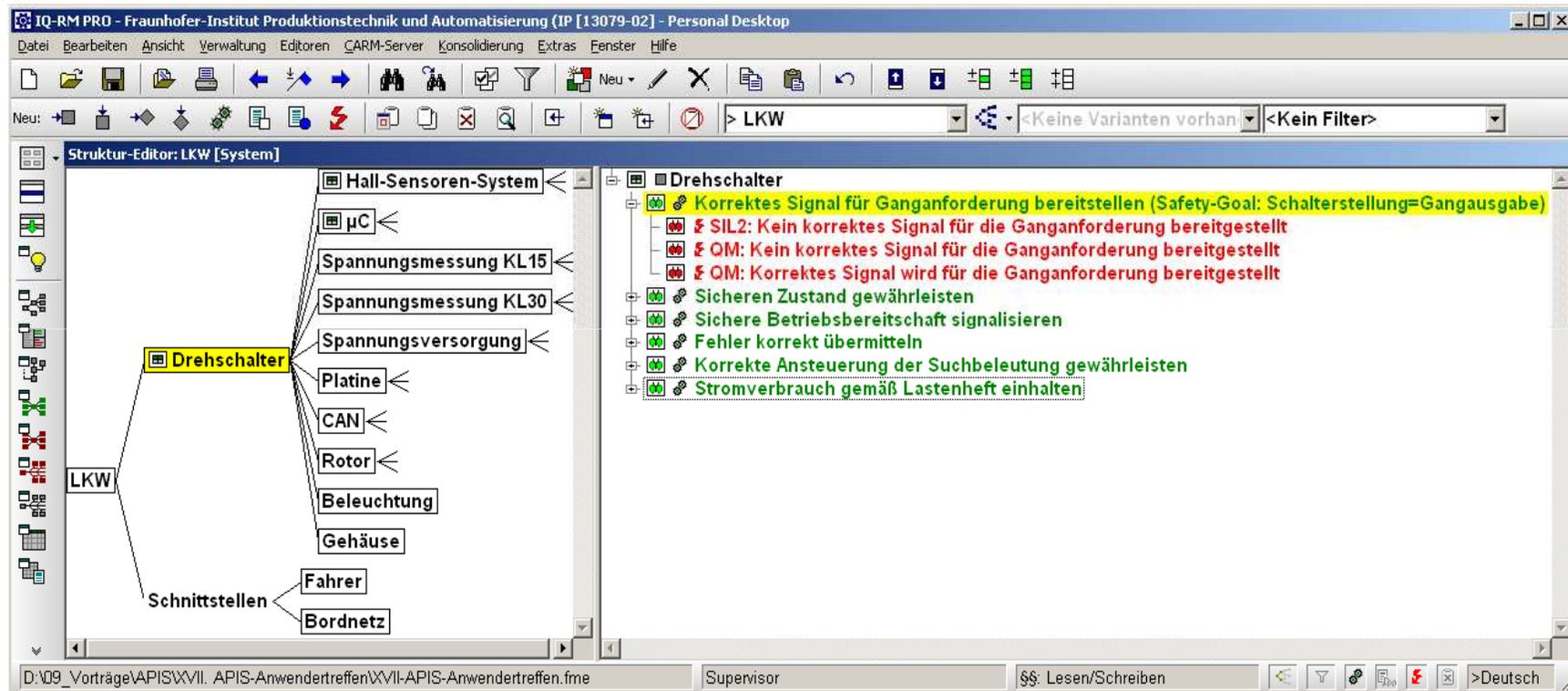
**Schaltechnologie
mit Hall-Sensoren**

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

Quelle: www.seuffer.de

Produkt

Systemstruktur Drehschalter und Safety Goal



Projektumfeld

Teamzusammensetzung



- Systemlieferant
 - Projektleiter
 - Safety Ingenieur / Qualität
 - Hardwareentwicklung
 - Softwareentwicklung
- Kunde
 - Projektleiter
 - Safety Ingenieur
- Zertifizierer
 - Hardware und Software
- FMEA-/FuSi-Moderation



Projektumfeld

Eingesetzte Methoden zur Analyse des Systems

Methoden zur Analyse systematischer Fehler

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

Methoden zur Analyse zufälliger Fehler

- Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse (FMEDA)

ERMITTLUNG DER FUSI-KENNWERTE FIT-WERTE / DIAGNOSEDECKUNG

Ermittlung der FuSi-Kennwerte

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

Funktionale Sicherheit

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	λ_{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 = 1×10^{-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)
Birolini (2007)

14

Ermittlung der FuSi-Kennwerte

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

15

Ermittlung der FuSi-Kennwerte

Ermittlung und Realisierung der Diagnosedeckungsgrade



DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-2

ISO/TC 22/SC 3

Secretariat: DIN

Voting begins on:
2009-07-08

Voting terminates on:
2009-12-08

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • INTERNACIONAL ORGANIZACION DE ESTANDARIZACION • ORGANISATION INTERNATIONALE DE NORMALISATION

Road vehicles — Functional safety —

Part 2:

Management of functional safety

Véhicules routiers — Sécurité fonctionnelle —

Partie 2: Gestion de la sécurité fonctionnelle

ICS 43.040.10

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 AVAILABLE TO SUBSCRIBERS THROUGH THE INTERNET. NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.
© International Organization for Standardization, 2009

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)

BEISPIEL FIT-/DC-ERMITTLUNG FÜR EINEN EINFACHEN FEHLERFALL

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 list of failure events for RAM is shown on the right, including "Korrekte Datenhaltung (der sicherheitsrelevanten Daten) während der Laufzeit ermöglichen", "Bit-Kipper (der sicherheitsrelevanten Daten) im RAM", and "Zelldefekt (der sicherheitsrelevanten Daten) im RAM". 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 header.
- 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 'Maßnahmenstand: Software Test' row.
- Test-ID**: Points to 'S-FMEA-E000050'.
- Verifizierung im Rahmen der Entwicklung**: A large green box covering the middle rows.
- Erkennung / Reaktion Beherrschung im Betrieb (DC = High = 99%)**: A large green box at the bottom.
- SFF-Soll** and **PFH-Soll**: Labels pointing to the 'B' column.
- DC-Ist** and **FIT-Ist**: Labels pointing to the 'Fehlerart' column.

Einfacher Fehlerfall „Bit-Kipper im RAM“

Fehlererkennung und Fehlerreaktion im Betrieb durch die Software

The screenshot shows the IQ-RM PRO software interface with the following components and annotations:

- 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**
 - EEPROM
 - Flash

- Fehlernetz-Editor: LKW [System]**
- LKW
 - SIL2-Fehlfunktion (SIL=2) (SFF-Soll=90%) (PFH-Soll=20,000 FIT)
 - Drehschalter
 - SIL2: Kein korrektes Signal für die Ganganforderung bereitgestellt
 - µC
 - Signale der Hall-Sensoren werden nicht korrekt ausgelesen (RAM)
 - Software
 - Sicherheitsrelevante Daten werden doppelt in verschiedenen Adressbereichen und die Kopie zusätzlich invertiert abgelegt. Beim Einlesen und Zugriff erfolgt ein Vergleich.

Annotations and Labels:

- Two arrows point from the RAM error messages in the structure editor to the 'Software' entry in the fault network editor.
- Text labels below the fault network editor:
 - Reaktion im Betrieb** (under the Software entry)
 - Erkennung im Betrieb** (under the µC entry)
 - Erkennung / Reaktion im Betrieb (DC = High = 99%)** (under the RAM entry)

BEISPIEL FIT-/DC-ERMITTLUNG FÜR EINEN KOMPLEXEN FEHLERFALL

FIT-/DC-Ermittlung

Komplexer Fehlerfall „Fehler im Hall-Sensoren-System“

The screenshot shows the IQ-RM PRO software interface. The title bar reads "IQ-RM PRO - Fraunhofer-Institut Produktionstechnik und Automatisierung (IP [13079-02] - Personal Desktop)". The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Verwaltung", "Editoren", "CARM-Server", "Konsolidierung", "Extras", "Fenster", and "Hilfe". The toolbar contains various icons for file operations and editing. The main window is titled "Struktur-Editor: LKW [System]".

The left pane shows a hierarchical tree structure of the system components:

- Hall-Sensoren-System
 - µC
 - Spannungsmessung KL15
 - Spannungsmessung KL30
 - Spannungsversorgung
 - Drehschalter
 - Platine
 - CAN
 - Rotor
 - Beleuchtung
 - Gehäuse
 - Schnittstellen
 - Fahrer
 - Bordnetz

The right pane shows a list of detected faults for the "Hall-Sensoren-System":

- Position der Magneten korrekt erkennen
- (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
- (FR-Ist=4,0800 FIT) ⚠ QM: Position der Magnete wird 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 >> (SIL=2) (SFF-Soll=90%) (PFH-Soll=20,000 FIT) [LKW] SIL2-Fehlfunktion	10	[Hall-Sensoren-System] (DCSPF=99,0%) (FR-Ist=2,0400 FIT) Wechsel von einer Fahrstufe (D od. R) zu N wird nicht korrekt erkannt	[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
				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

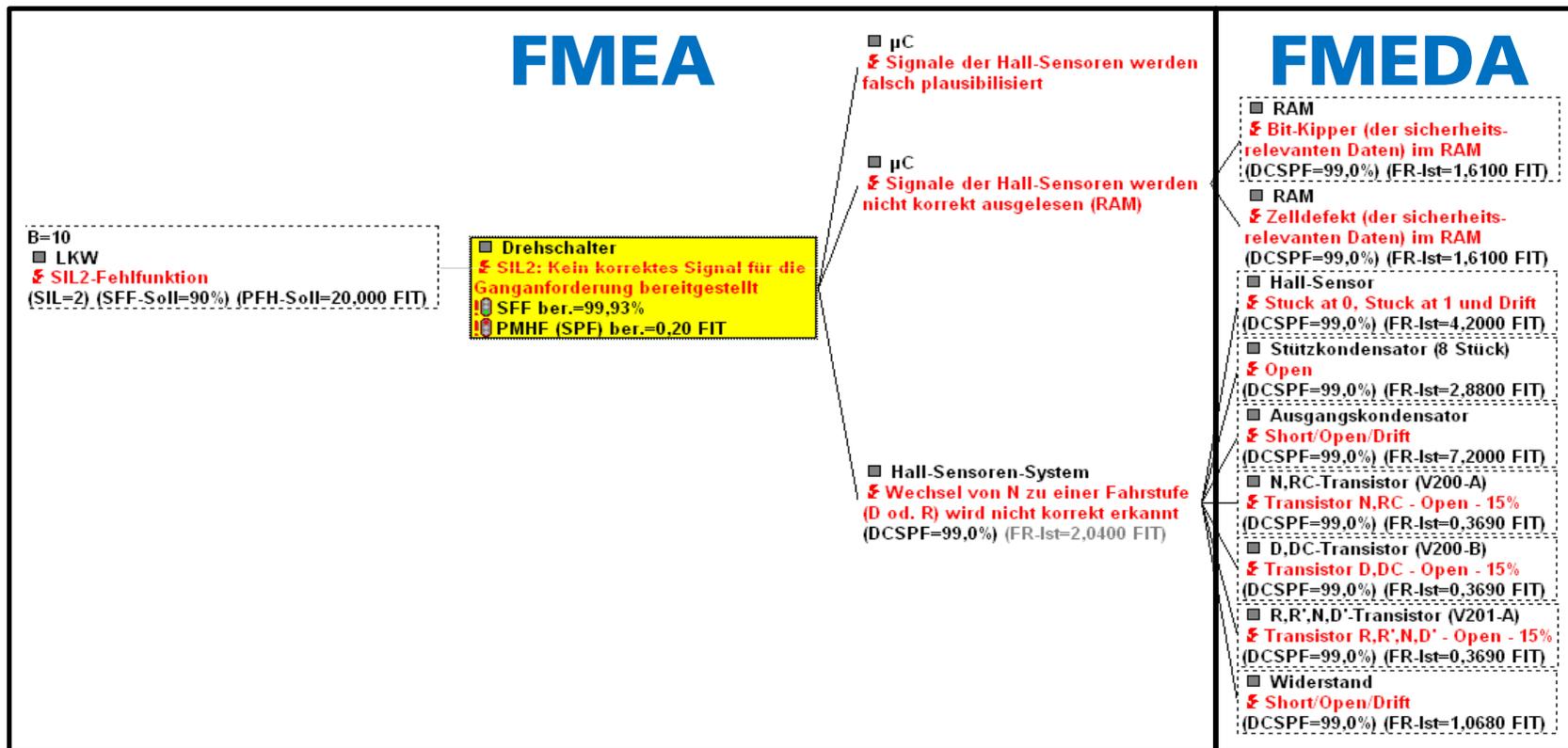
FMEA UND FMEDA

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>

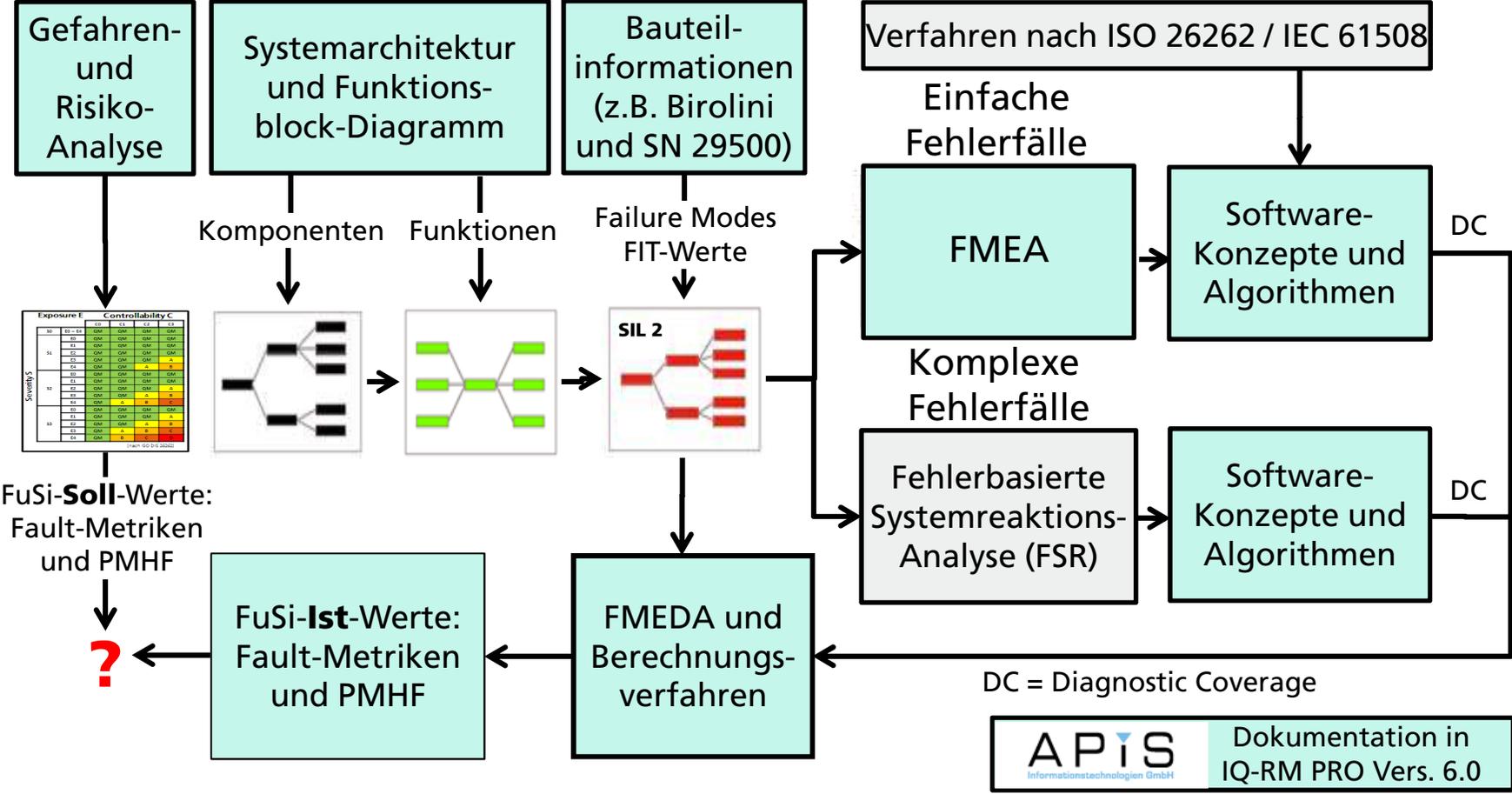
FMEDA-Formblatt: LKW [System]

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

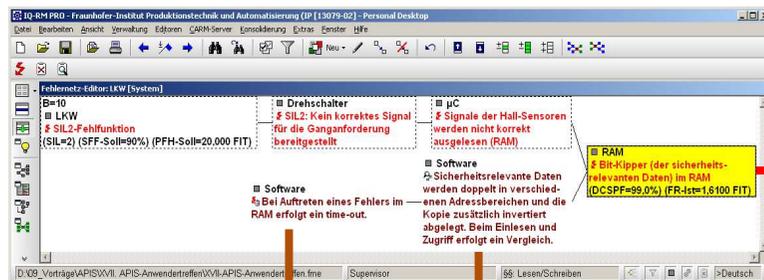
VORGEHENSWEISE ZUR ANALYSE MECHATRONISCHER SYSTEME

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



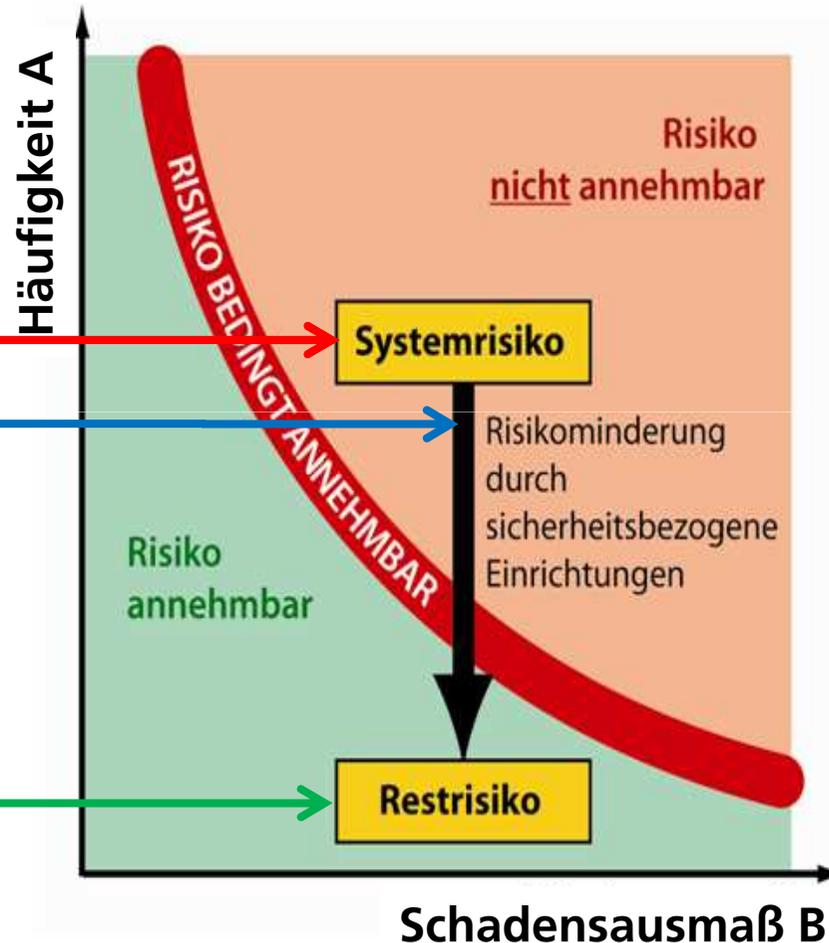
FMEA und FMEDA

Analyse und Bewertung von Fehlfunktionen, Fehlererkennungen und Fehlerreaktionen im Betrieb



2. Fehlerreaktion
 A=1 oder DC=99%
 1. Fehlererkennung

Funktions- [µC]	Fehlerart	Fehlerursache	Vermeidungsmaßnahme	Entdeckungsmaßnahme	E	RP	Z	VT
[Dreheschalter]	SIL2: Kein korrektes Signal für die Ganganforderung bereitgestellt	µC: Signale der Hall-Sensoren werden nicht korrekt ausgelesen (RAM)	Maßnahmenstand - Anfang: Software Requirement	100	11.03.2011	SW	Erz	
[RAM]	SIL2: Fehlreaktion	Software: Sicherheitsrelevante Daten werden doppelt in verschiedenen Adressbereichen und die Kopie zusätzlich invertiert abgelegt. Beim Einlesen und Zugriff erfolgt ein Vergleich.	Maßnahmenstand: Software-Test	100				



Analyse funktional sicherer mechatronischer Systeme

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

Fehlfunktion: SIL2-Fehlfunktion

SOLL-Werte (Anforderungen):

- SIL/ASIL: **SIL: 2**
- SFF/SPFM/LFM (0-100%): 90
- EFH (FIT): 20,0 (1 FIT = 1*10e-9 pro Stunde)

IST-Werte:

- DCSPF (0-100%):
- DCLF (0-100%):
- FB = Fehlerrate (FIT):
- Fehlertoleranzzeit (FTT) in ms:

Lambda-Werte:

- Anteil entdeckbarer Ausfälle:
- Anteil nicht entdeckter Ausfälle:

Werte zurücksetzen

Links (Tree View):

- LKW
 - SIL2-Fehlfunktion (SIL=2) (SFF-Soll=90%) (PFH-Soll=20.000 FIT)
 - SFF ber.=95,66%
 - PMHF (SPF) ber.=12,05 FIT

Rechts (Component List):

- µC
 - Signale der Hall-Sensoren werden falsch miteinander plausibilisiert
 - Signale der Hall-Sensoren werden nicht korrekt ausgelesen (RAM)
- Hall-Sensoren-System
 - Wechsel von N zu einer Fahrstufe (D od. R) wird nicht korrekt erkannt (DCSPF=99,0%) (FR-Ist=2,0400 FIT)
- RAM
 - Bit-Kipper (der sicherheitsrelevanten Daten) im RAM (DCSPF=99,0%) (FR-Ist=1,6100 FIT)
 - Zelldefekt (der sicherheitsrelevanten Daten) im RAM (DCSPF=99,0%) (FR-Ist=1,6100 FIT)
- Stützkondensator (8 Stück)
 - Open (DCSPF=99,0%) (FR-Ist=2,8800 FIT)
- Ausgangskondensator
 - Short/Open/Drift (DCSPF=99,0%) (FR-Ist=7,2000 FIT)
- Widerstand
 - Short/Open/Drift (DCSPF=99,0%) (FR-Ist=1,0680 FIT)
- R,R',N,D'-Transistor (V201-A)
 - Transistor R,R',N,D' - Open - 15% (DCSPF=99,0%) (FR-Ist=0,3690 FIT)
- N,RC-Transistor (V200-A)
 - Transistor N,RC - Open - 15% (DCSPF=99,0%) (FR-Ist=0,3690 FIT)
- D,DC-Transistor (V200-B)
 - Transistor D,DC - Open - 15% (DCSPF=99,0%) (FR-Ist=0,3690 FIT)
- Hall-Sensor
 - Stuck at 0, Stuck at 1 und Drift (DCSPF=99,0%) (FR-Ist=4,2000 FIT)

FAZIT

Erfahrungen aus einem Projekt zur Funktionalen Sicherheit

Fazit

- Frühzeitige Einbindung des Zertifizierers
- Regelmäßige Reviewmeetings mit Bewertung des Entwicklungsfortschritts
- Frühzeitige Analyse der Funktionen und Erstellung der Funktionsnetze
- Detaillierte Risikoanalyse mit präziser Bezeichnung der Fehlfunktionen
- Ermittlung von FIT-Werten anhand von Zuverlässigkeitsnormen (SN 29500)
- Ermittlung der Diagnosedeckungsgrade anhand von Vorgaben aus den FuSi-Normen (einfache Fehlerfälle) und der FSR (komplexe Fehlerfälle)
- Abbildung der Fehlerzusammenhänge (Fehlernetze) inkl. FIT-/DC-Werte in der IQ-RM PRO der APIS Informationstechnologien GmbH
- Integrierte Anwendung erleichtert die durchgängige Betrachtung und Aktualisierung der Informationen und Daten

No risk – no fun



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

35