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

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

TÜV Functional Safety Engineer
Safety Instrumented Systems
ID: 1427/08
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
Internet: www.ipa.fraunhofer.de

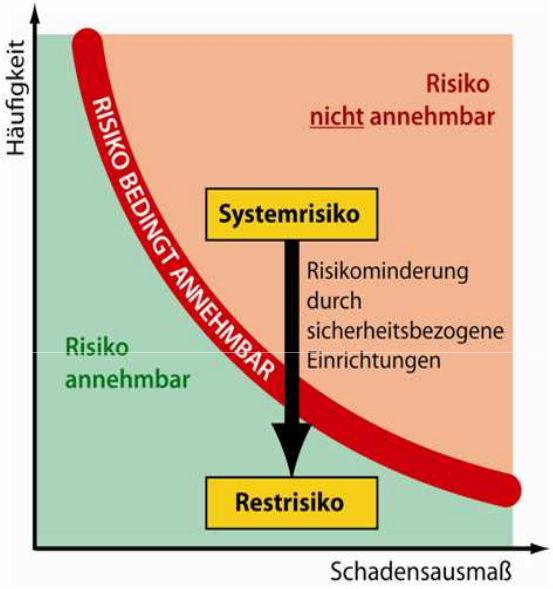
Fraunhofer IPA

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



Zielsetzung
„Risikominderung“

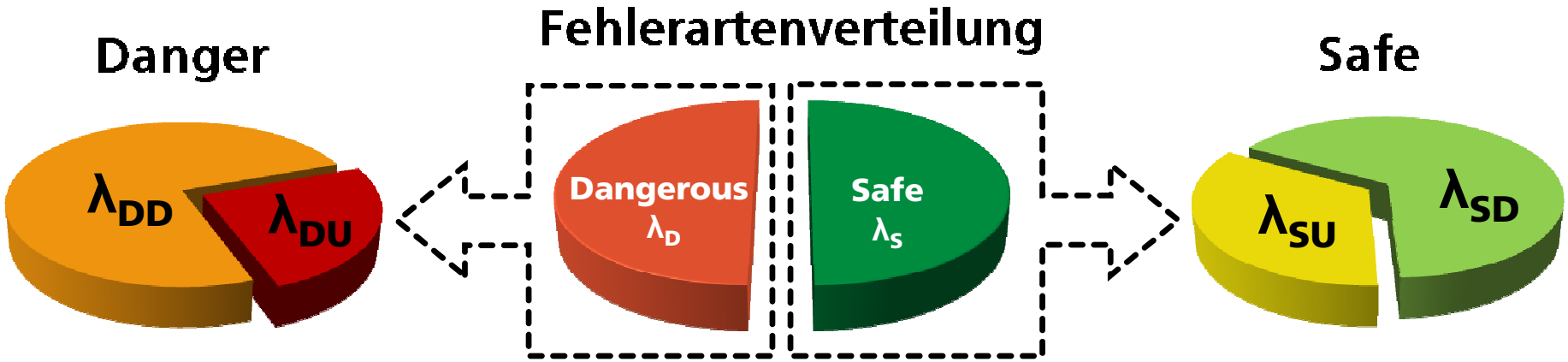
Funktionale Sicherheit ist die Fähigkeit eines elektrischen, elektronischen od. programmierbar elektronischen Systems (E/E/PE-System), beim Auftreten

- 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 – 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 IPA

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)

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

Anteil ungefährlicher Ausfälle (safe failure fraction)

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

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 (PFH / PFD: Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$> 10^{-6}$ 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	HFT = 1	HFT = 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

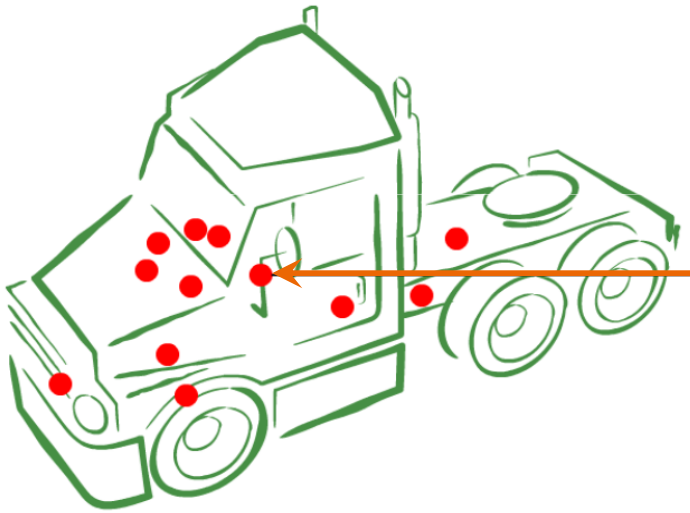
- SFF = Safe Failure Fraction
- HFT = Hardware Failure Tolerance

Quelle: DIN EN 61508

Fraunhofer IPA

PRODUKT UND PROJEKTUMFELD

Produkt- und Projektumfeld
Drehschalter



Schalttechnologie mit Hall-Sensoren

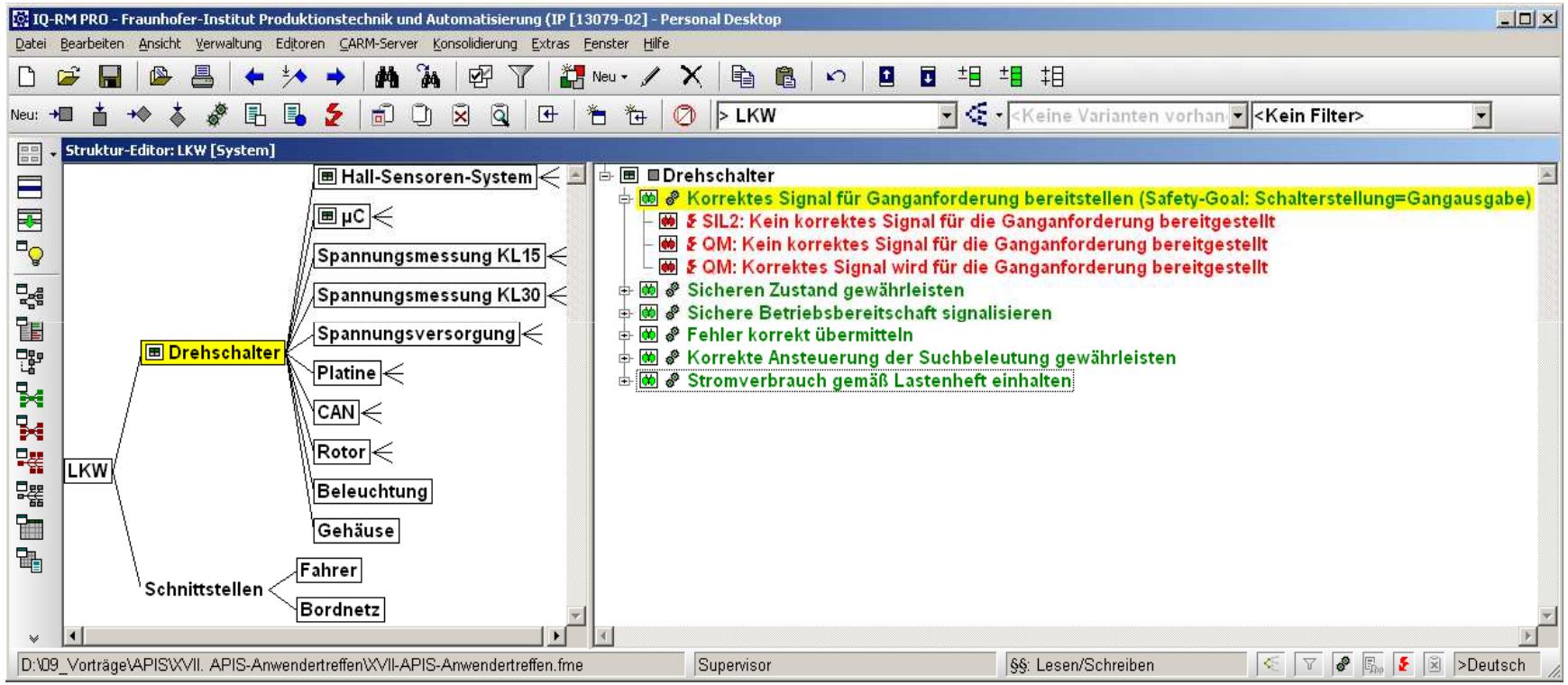
Projekt Drehschalter SIL 2
PFH = 2% von PFH (SIL2) = 20 FIT
SFF = 90%

Quelle: www.seuffer.de

Fraunhofer IPA

Produkt

Systemstruktur Drehschalter und Safety Goal



Fraunhofer IPA

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)

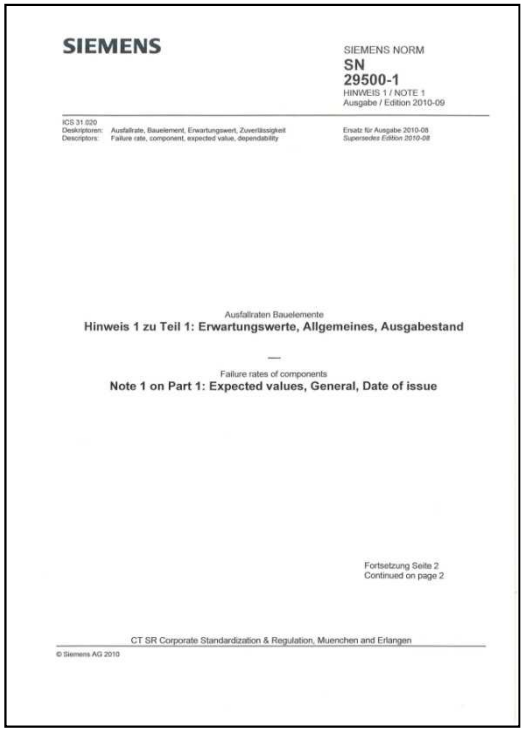
Methoden zur Analyse zufälliger Fehler

- 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



SIEMENS

SIEMENS NORM
SN
29500-1
HINWEIS 1 / NOTE 1
Ausgabe / Edition 2010-09

ICS 31.020
Deskriptoren: Ausfallrate, Bauelement, Erwartungswert, Zuverlässigkeit
Descriptors: Failure rate, component, expected value, dependability

Ersatz für Ausgabe 2010-08
Supersedes Edition 2010-08

Ausfallraten Bauelemente
Hinweis 1 zu Teil 1: Erwartungswerte, Allgemeines, Ausgabestand

—

Failure rates of components
Note 1 on Part 1: Expected values, General, Date of issue

Fortsetzung Seite 2
Continued on page 2

CT SR Corporate Standardization & Regulation, Muenchen and Erlangen

© Siemens AG 2010

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

Fraunhofer IPA

Funktionale Sicherheit

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

Tabelle 2 Ausfallraten für Widerstände
Table 2 Failure rates for resistors

Widerstand / *Resistor*		λ_{ref} in FIT	θ_1 [1] in °C
Kohleschicht / *Carbon film*	≤100 kOhm	0,3	55
	>100 kOhm	1	
Metallschicht / *Metal film*		0,2	55
Netzwerke (Schichtschaltung) je Widerstandselement *Networks (film circuits) per resistor element*			
	Standard	0,1	55
	kundenspezifische / *Custom design*	0,5	
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 FIT equals one failure per 10^9 component hours
[1] Oberflächentemperatur — [1] Resistor element temperature

Fehlermodi für Widerstände:
Open = 40% **0,4 FIT (open)**
Drift = 60% **0,6 FIT (drift)**

Quellen:
SN 29500-4 (2004)
Birolini (2007)

Fraunhofer IPA

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):

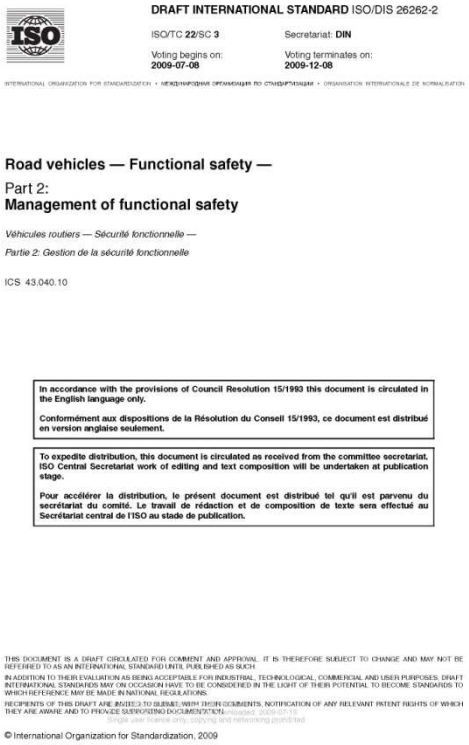
- 50/50-Aufteilung
- Aufteilung auf Funktionsgruppen
- Aufteilung nach Chipflächen
- Aufteilung nach Empfehlungen (z.B. Birolini, SN 29500)

Bildquelle: www.kurz-elektronik.de

Fraunhofer IPA

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 • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • 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.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Ermittlung und Realisierung der Diagnosedeckungsgrade:

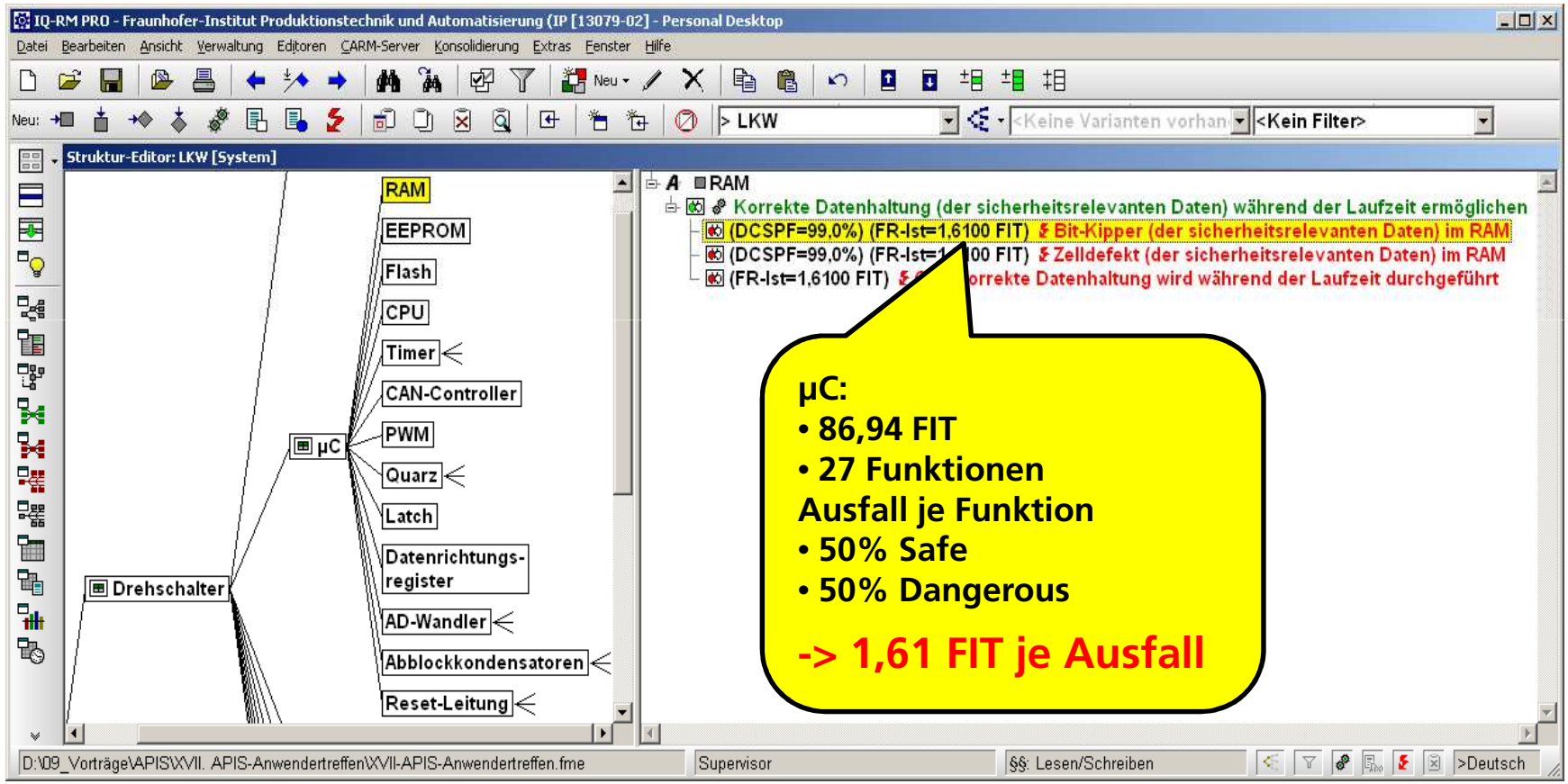
- Einfache Systeme und Fehlerfälle
  - Empfehlungen der IEC 61508
  - Empfehlungen der ISO 26262-5
- Komplexe Systeme und Fehlerfälle
  - Fehlerbasierte-Systemreaktionsanalyse (FSR)

BEISPIEL FIT-/DC-ERMITTLUNG FÜR EINEN EINFACHEN FEHLERFALL


Bit-Kipper ☺

FIT-/DC-Ermittlung

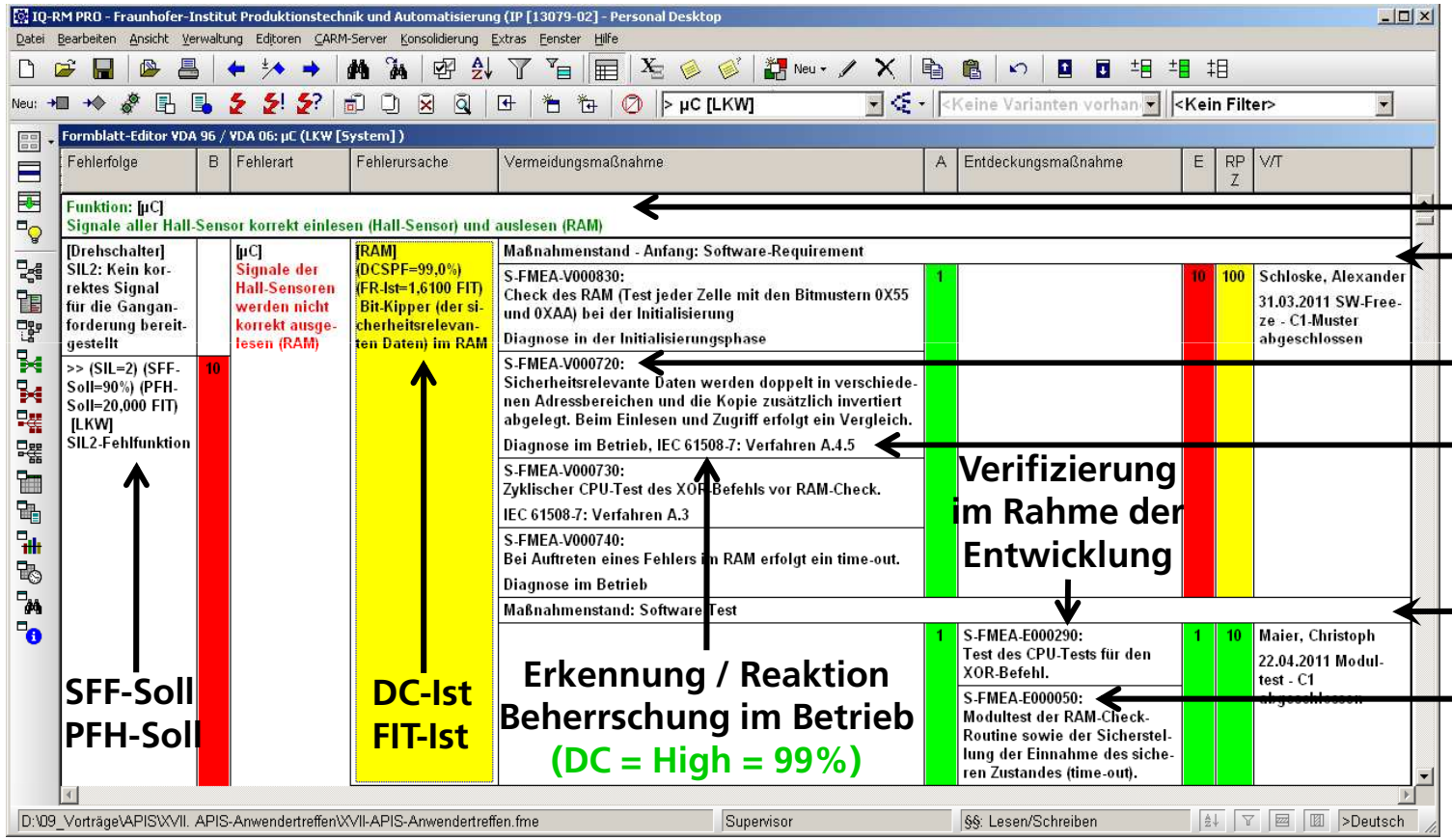
Einfacher Fehlerfall „Bit-Kipper im RAM“



Fraunhofer IPA

Einfacher Fehlerfall „Bit-Kipper im RAM“

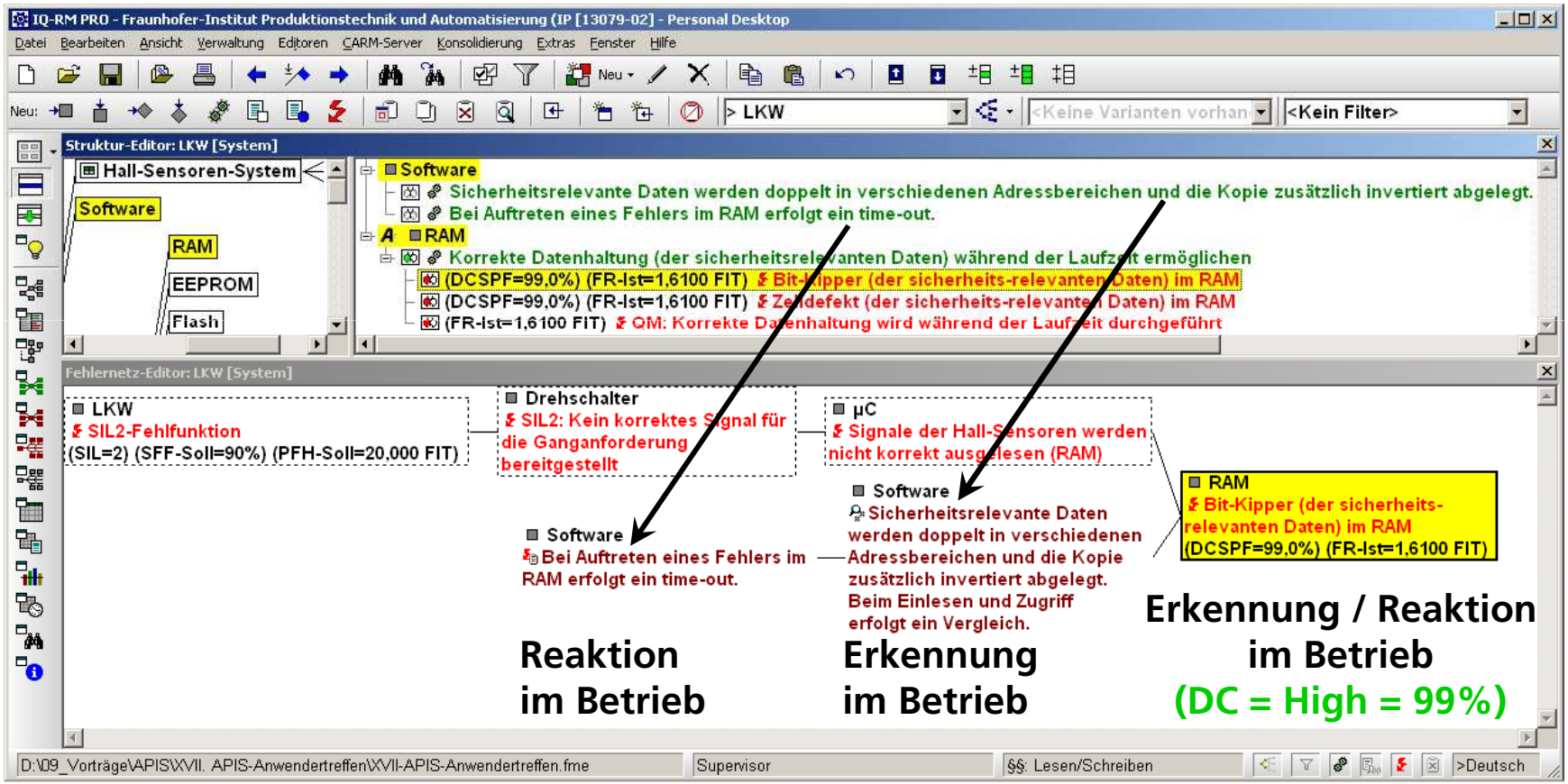
FMEA-Formblattinhalte (Beispiel nach DIN EN 61508)



Fraunhofer IPA

Einfacher Fehlerfall „Bit-Kipper im RAM“

Fehlererkennung und Fehlerreaktion im Betrieb durch die Software

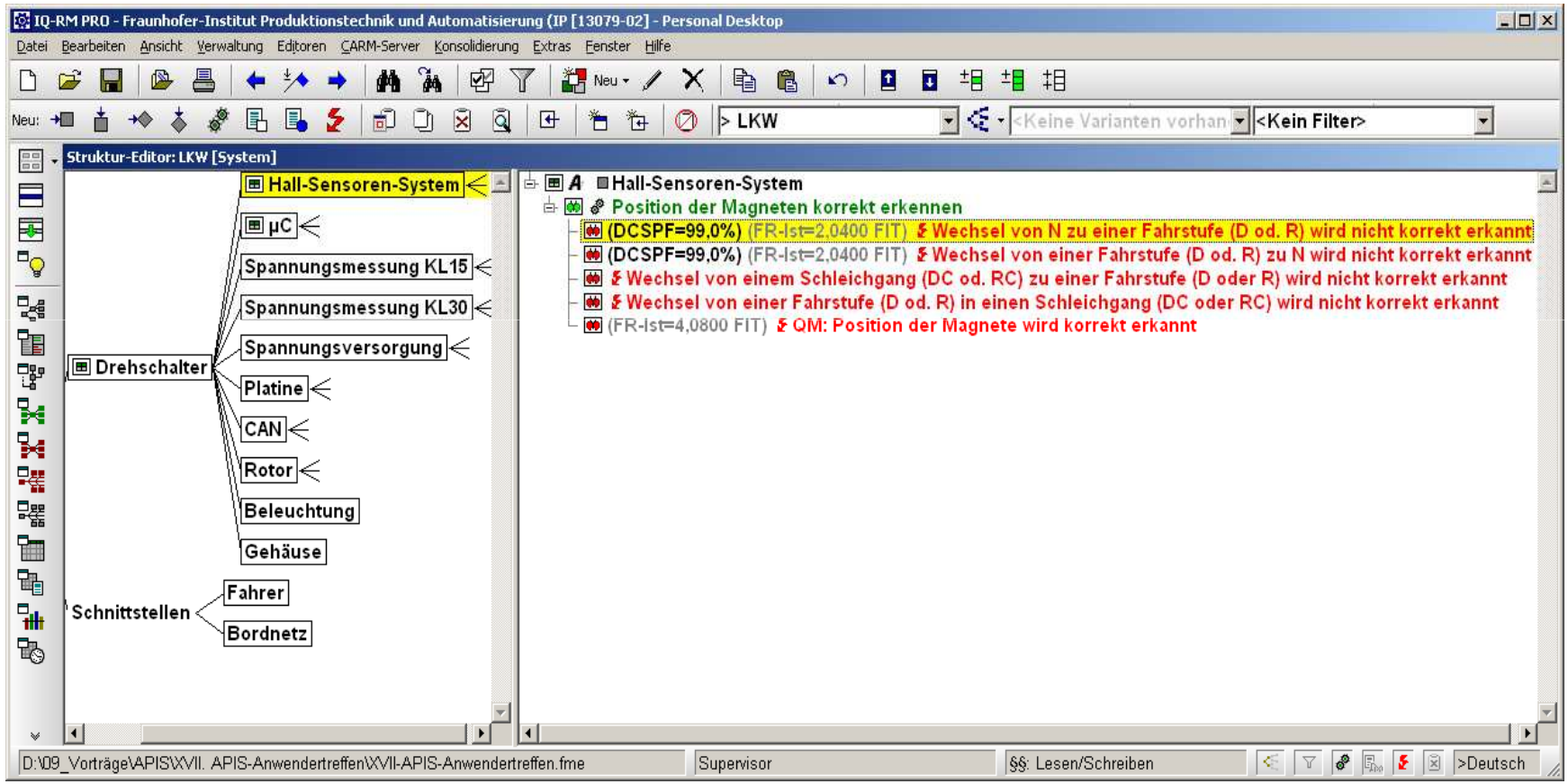


Fraunhofer IPA

BEISPIEL FIT-/DC-ERMITTLUNG FÜR EINEN KOMPLEXEN FEHLERFALL

FIT-/DC-Ermittlung

Komplexer Fehlerfall „Fehler im Hall-Sensoren-System“



Fraunhofer IPA

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-kritsch	Regel	nein	sofort	nächstes N	nächstes D/R	nächstes DC/RC
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			

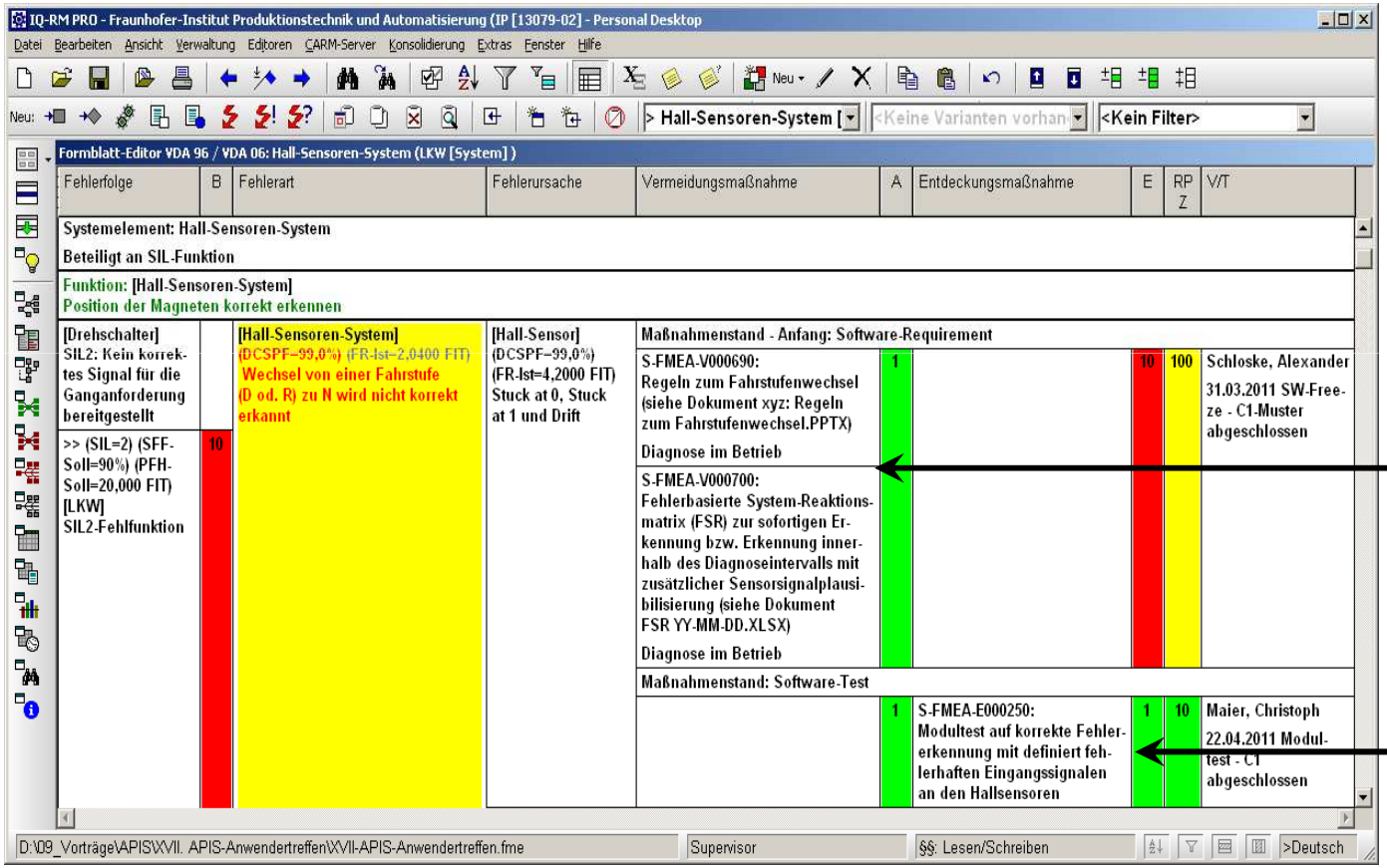
Legende:

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

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

Fraunhofer IPA

Komplexer Fehlerfall „Fehler im Hall-Sensoren-System“
FMEA-Formblattinhalte



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

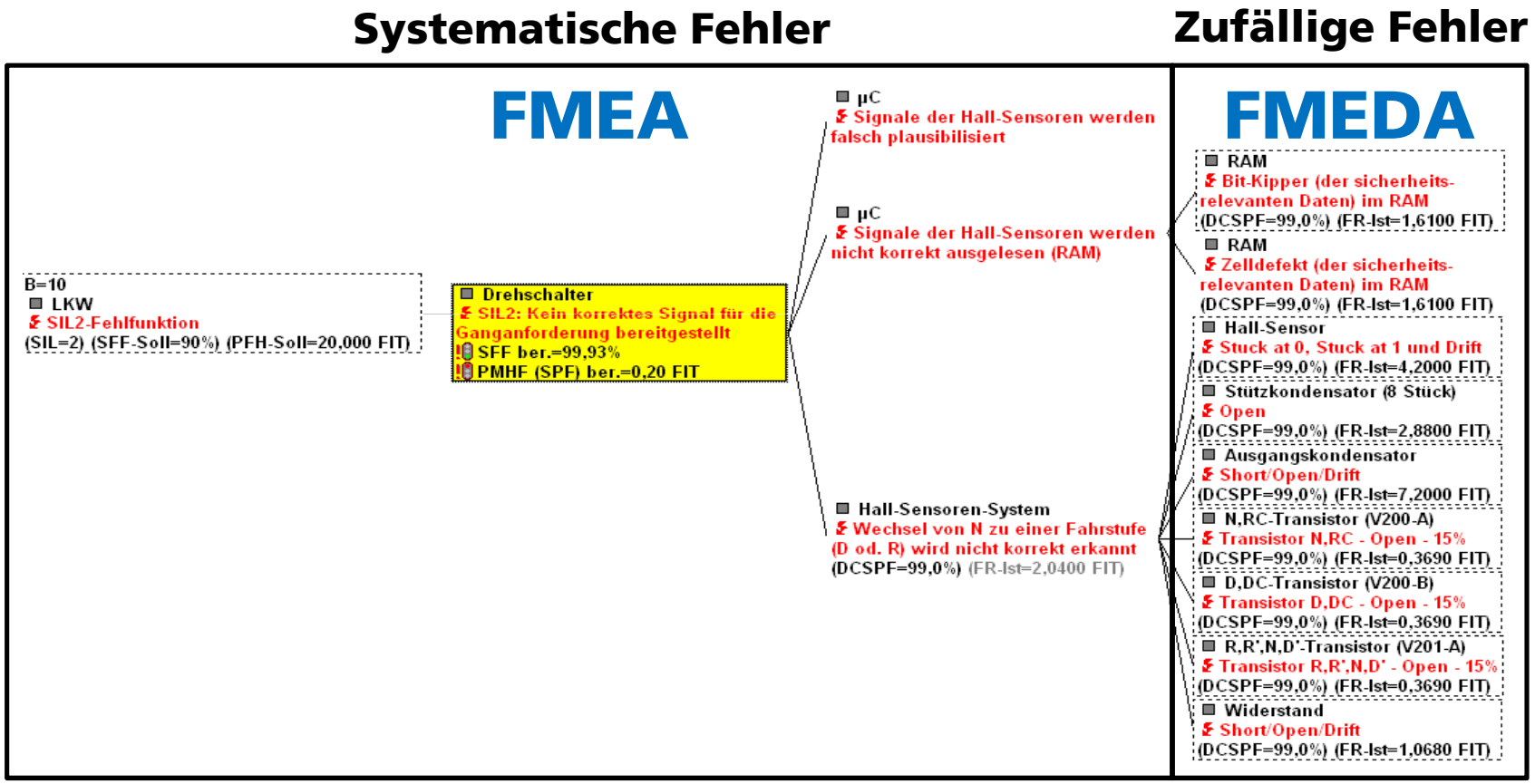
Nachweis erbracht!
Sichere Fehlererkennung der Hallsensoren im Betrieb

Fraunhofer IPA

FMEA UND FMEDA

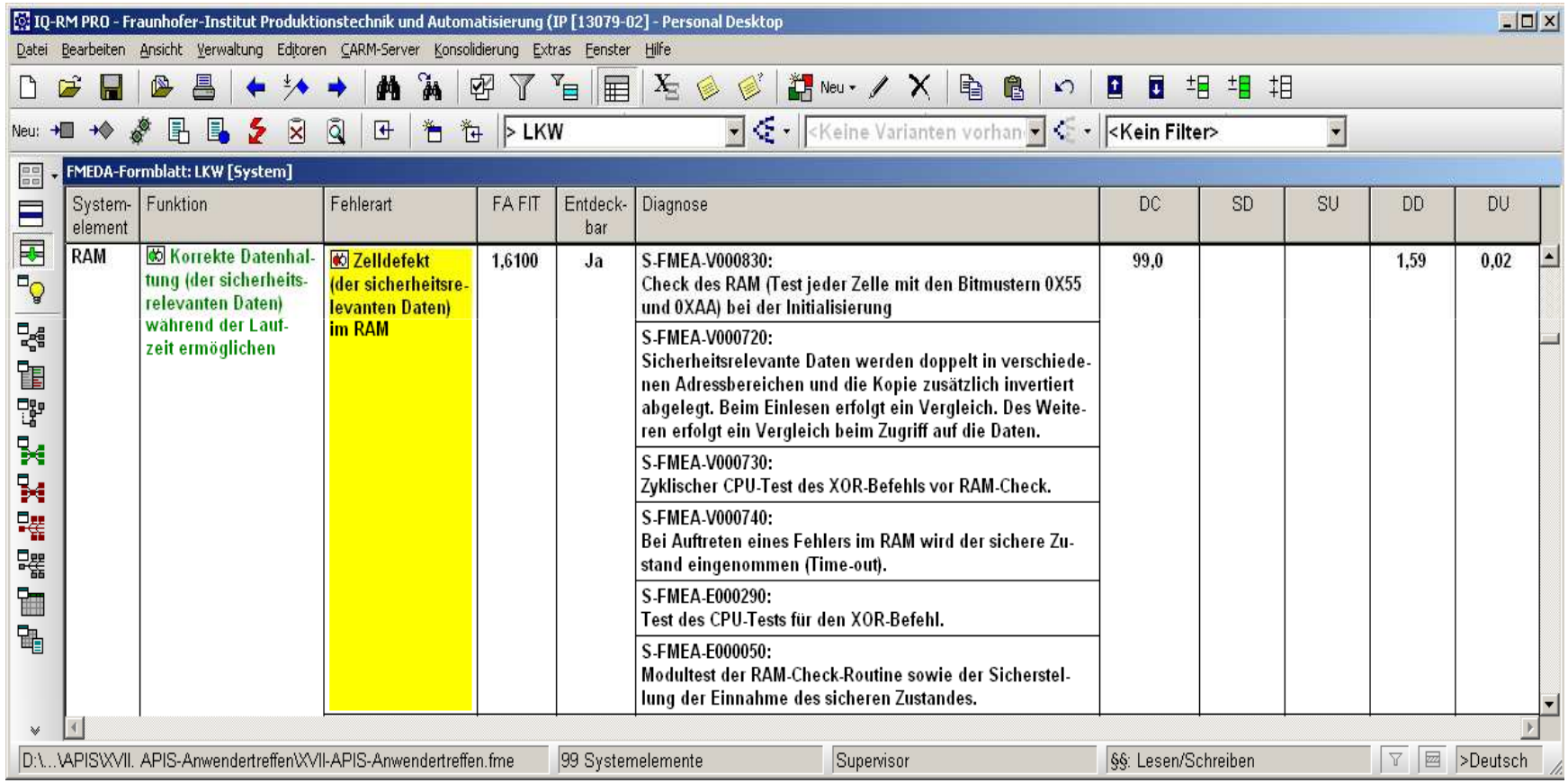
Analyse systematischer und zufälliger Fehler

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



Fraunhofer IPA

Analyse zufälliger Fehler
FMEDA



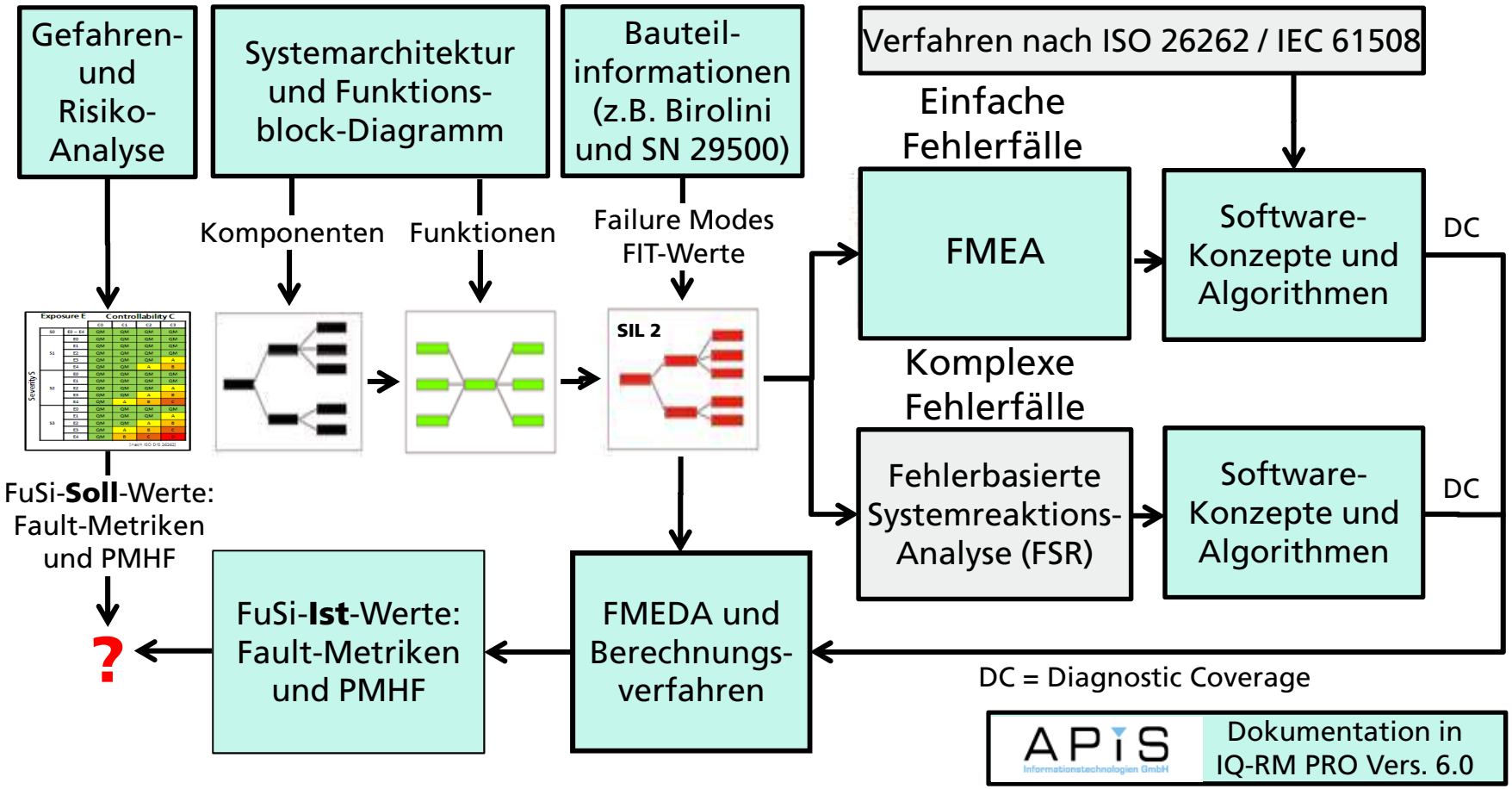
System-element	Funktion	Fehlerart	FA FIT	Entdeck-bar	Diagnose	DC	SD	SU	DD	DU
RAM	Korrekte Datenhal-tung (der sicherheits-relevanten Daten) während der Lauf-zeit ermöglichen	Zelldefekt (der sicherheitsre-levanten Daten) im RAM	1,6100	Ja	S-FMEA-V000830: Check des RAM (Test jeder Zelle mit den Bitmustern 0X55 und 0XAA) bei der Initialisierung	99,0			1,59	0,02
					S-FMEA-V000720: Sicherheitsrelevante Daten werden doppelt in verschiede-nen Adressbereichen und die Kopie zusätzlich invertiert abgelegt. Beim Einlesen erfolgt ein Vergleich. Des Weite-ren erfolgt ein Vergleich beim Zugriff auf die Daten.					
					S-FMEA-V000730: Zyklischer CPU-Test des XOR-Befehls vor RAM-Check.					
					S-FMEA-V000740: Bei Auftreten eines Fehlers im RAM wird der sichere Zu-stand eingenommen (Time-out).					
					S-FMEA-E000290: Test des CPU-Tests für den XOR-Befehl.					
					S-FMEA-E000050: Modultest der RAM-Check-Routine sowie der Sicherstel-lung der Einnahme des sicheren Zustandes.					

Fraunhofer IPA

VORGEHENSWEISE ZUR ANALYSE MECHATRONISCHER SYSTEME

Zusammenhang zwischen den eingesetzten Methoden

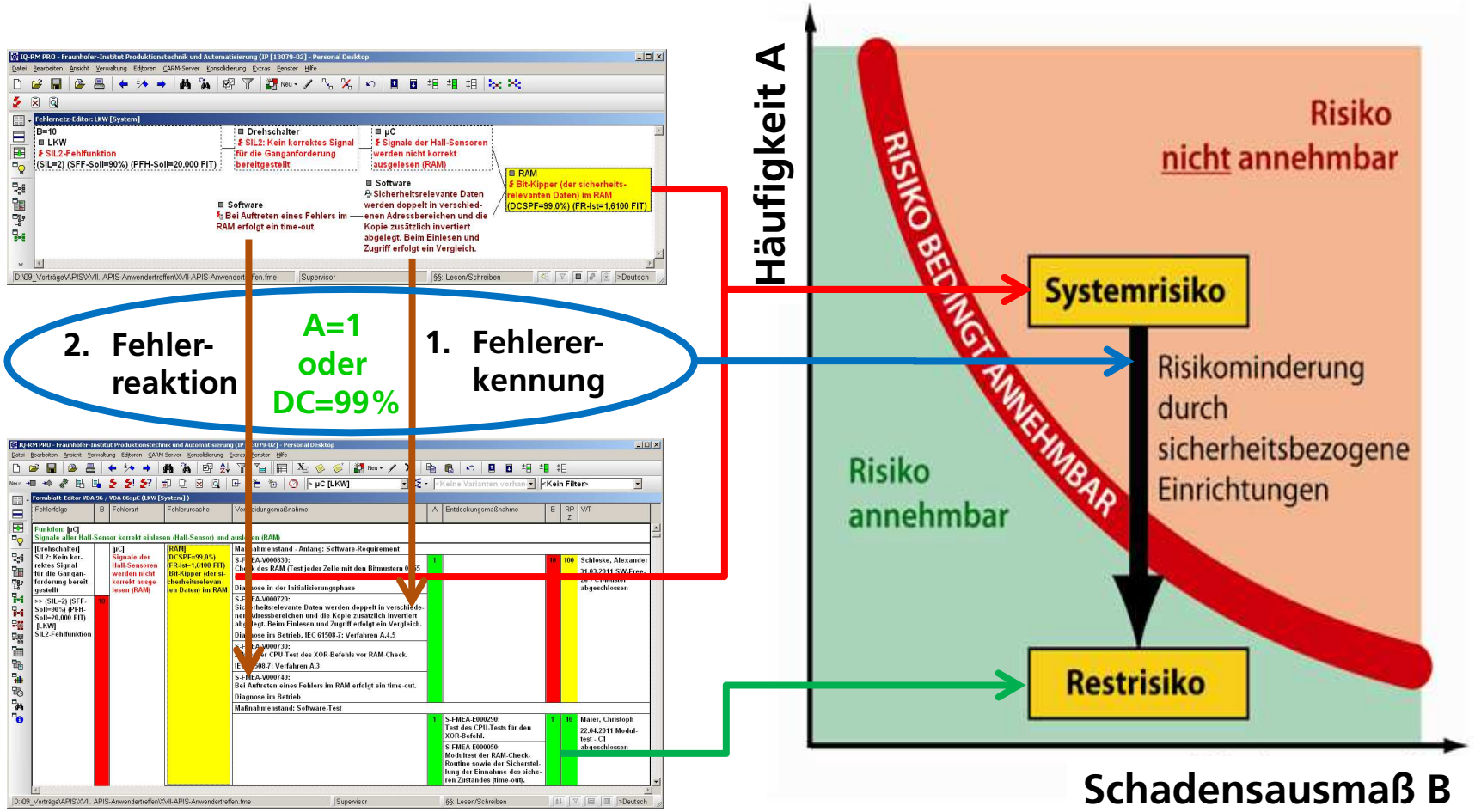
Vorgehensweise zur Analyse und Absicherung funktional sicherer mechatronischer Systeme



Fraunhofer IPA

FMEA und FMEDA

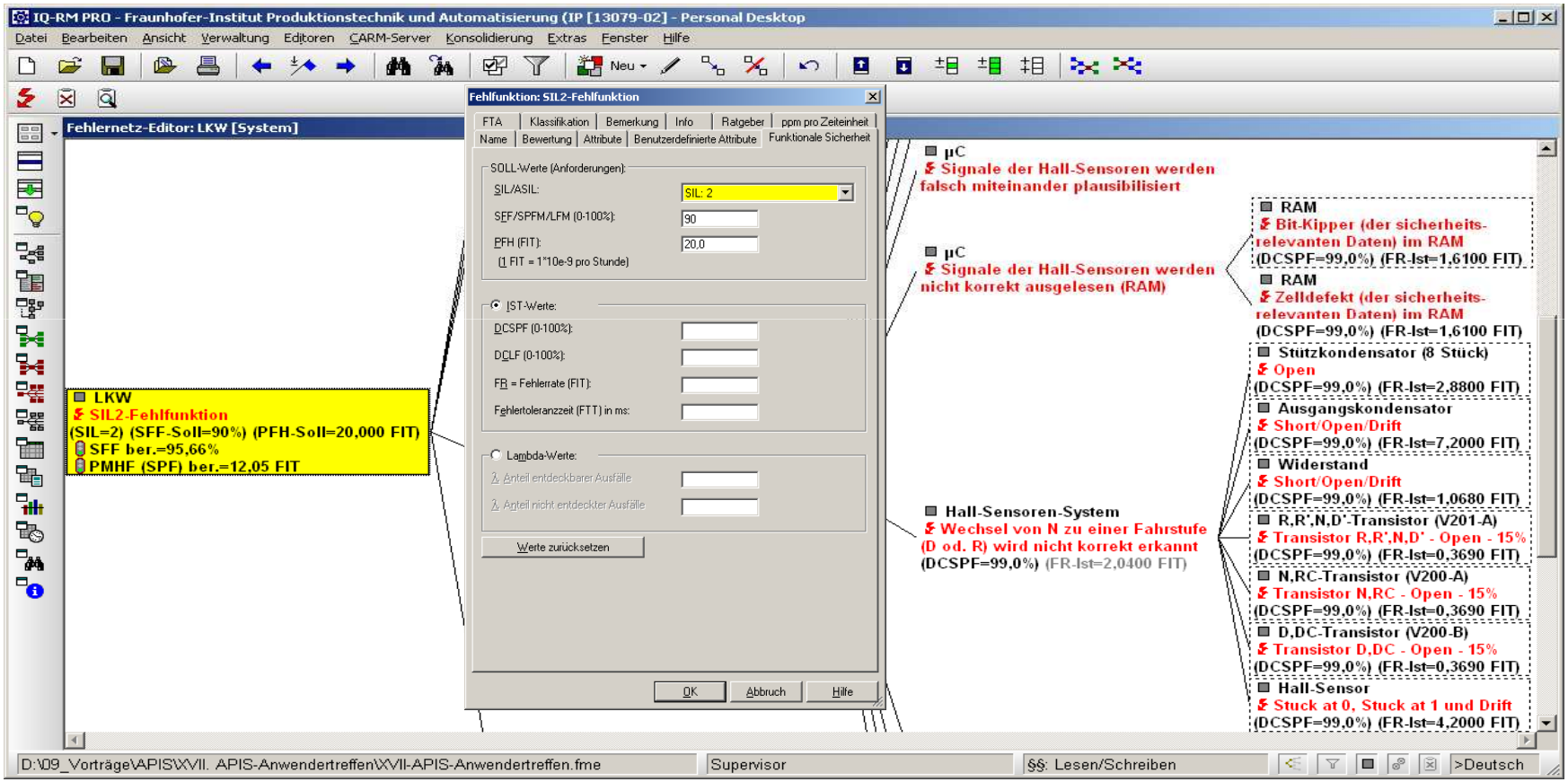
Analyse und Bewertung von Fehlfunktionen, Fehlererkennungen und Fehlerreaktionen im Betrieb



Fraunhofer IPA

Analyse funktional sicherer mechatronischer Systeme

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



Fraunhofer IPA

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/

Fraunhofer IPA