RISIKOABSICHERUNG VON MECHATRONISCHEN SYSTEMEN

Dr. Alexander Schloske

RISIKOABSICHERUNG VON MECHATRONISCHEN SYSTEMEN

Mit neuen Produkten schneller am Markt
FpF-Veranstaltung, 15. November 2012, Stuttgart

Dr.-Ing. Alexander Schloske

Senior Expert Quality Management

Leiter Stuttgarter Produktionsakademie

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

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

Funktionale Sicherheit
Beispiele aus der Realität zur „Funktionalen Sicherheit“

- „Volvo-City-Safety“ versagt 2010 bei Pressevorführung
  - Das City-Safety-System soll Hindernisse auf der Straße erkennen und das Auto automatisch abbremsen, um einen Zusammenstoß zu verhindern. Wie der Autohersteller später angab, war eine nicht funktionierende Batterie schuld am Ausfall des Systems.
    Quelle: www.auto.de

- Renault ruft 2010 weltweit 695.000 Scénic zurück
  - Bei diesem Modell kann es laut Renault zu einem unbeabsichtigten Anziehen der automatischen Parkbremse während der Fahrt kommen.
    Quelle: www.welt.de

- Toyota ruft 2010 gezielt 373.000 Autos zurück
  - Rückrufaktion auf Grund der Möglichkeit, dass während der Fahrt das Lenkradschloss selbsttätig einrastet. Damit ist das Lenken des Fahrzeugs nicht mehr möglich.
    Quelle: http://www.auto-motor-und-sport.de/

Fraunhofer IPA

Funktionale Sicherheit
Vortragsinhalte

- Grundlagen der Funktionalen Sicherheit
- Aufbau und Inhalte der ISO 26262
- Methoden und Werkzeuge zur Sicherstellung der Funktionalen Sicherheit
- Beispiele

GRUNDLAGEN DER FUNKTIONALEN SICHERHEIT

Funktionale Sicherheit
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)
- ISO 26262 (automotive)

Funktionale Sicherheit
Normenlandschaft

derzeitig:

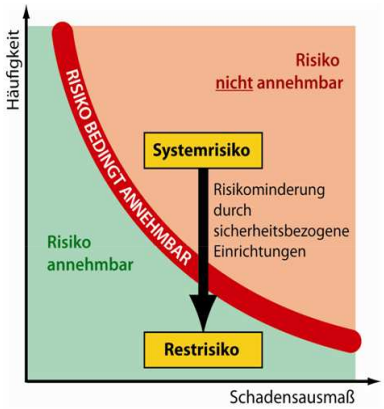
IEC 61508
elektrische, elektronische und programmierbare elektronische Geräte

DIN IEC 61513	DIN IEC 60601	DIN IEC 61511	DIN EN 501xx	DIN EC 62061	(weitere)
Kernkraftwerke	Medizingeräte	Prozessindustrie	Bahnsektor	Maschinen	...

künftig:

ISO 26262 (Erscheinung 14.11.2011)
Automotive
(in Serie produzierte PKW bis 3,5t)

Funktionale Sicherheit
Definition und Zielsetzung Funktionaler Sicherheit nach ISO 26262 (11/2011)



Zielsetzung:
„Risikominderung“
auf das technisch
unvermeidbare
Restrisiko

Funktionale Sicherheit ist die Fähigkeit eines elektrischen, elektronischen od. programmierbar elektronischen Systems (E/E-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.

Primärer Fokus: E/E-Systeme

Funktionale Sicherheit
Begriffe

- Sicherheitsfunktion bzw. funktionale Sicherheitsanforderung

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

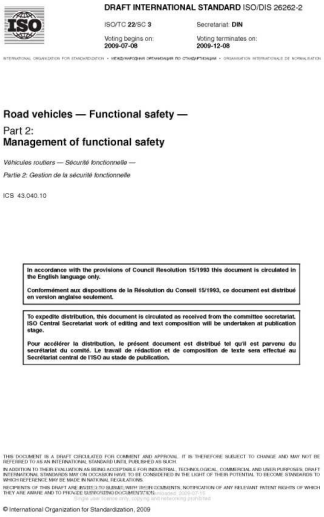
  Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen anforderungsgemäß ausführt
- Automotive Sicherheits-Integritätslevel (A)SIL

  Vier diskrete Stufen zur Festlegung von Anforderungen für die Sicherheitsintegrität der Sicherheitsfunktionen
  - SIL 1 bis SIL 4 (IEC 61508)
  - ASIL A bis ASIL D (ISO 26262)

AUFBAU UND INHALTE DER ISO 26262

Fraunhofer IPA

ISO 26262
Aufbau der ISO 26262



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

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.

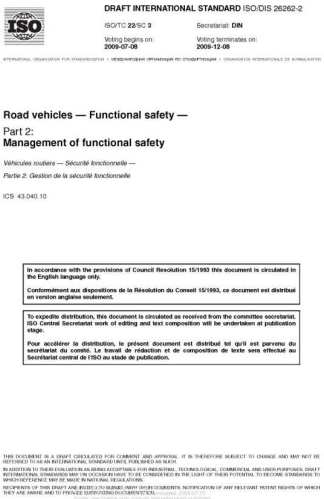
(insgesamt 381 Seiten)

1. Glossar
2. Management der Funktionalen Sicherheit
3. Konzeptphase
4. Produktentwicklung: Systemebene
5. Produktentwicklung: Hardwareebene
6. Produktentwicklung: Softwareebene
7. Produktion und Betrieb
8. Unterstützende Prozesse
9. ASIL- und sicherheitsorientierte Analysen
10. Orientierungshilfen

Quelle: ISO/DIS 26262

Fraunhofer IPA

ISO 26262
Aufbau der Einzelnormen der ISO 26262-#



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

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.

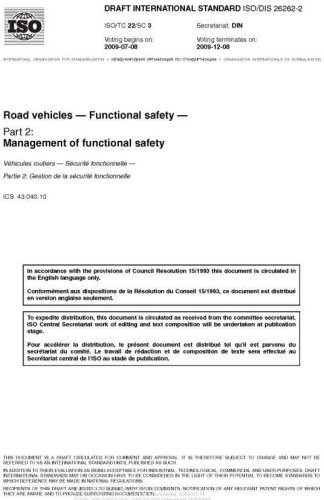
© International Organization for Standardization, 2009

1. Scope
2. Normative reference
3. Terms, definitions, abbreviated terms
4. Requirements for compliance
5. Content
   - Objectivess
   - General
   - Inputs for this clause
   - Requirements and recommendations
   - Work products
6. Annex (informative)
7. Bibliography

Quelle: ISO/DIS 26262

Fraunhofer IPA

ISO 26262
Anforderungen an compliance (Kapitel 4 in ISO 26262-#)



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

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.

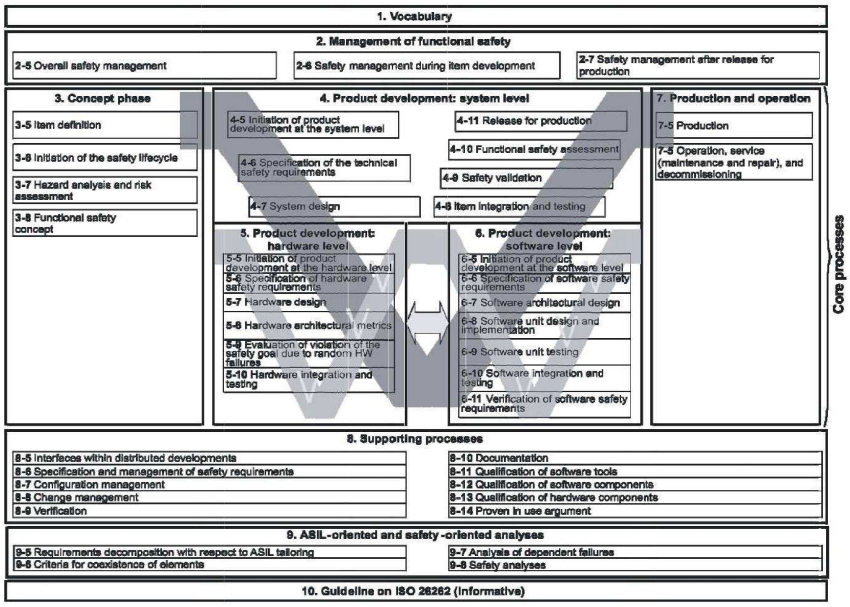
© International Organization for Standardization, 2009

- 4.1 Allgemeine Anforderungen
  - Geplante Anpassungen
  - Begründungen bei Abweichungen
- 4.2 Interpretation der Tabellen
  - ++ Methode für ASIL stark empfohlen
  - \+ Methode für ASIL empfohlen
  - 0 Keine Aussage (für / wider) zur Methode
- 4.3 ASIL-abhängige Anforderungen und Empfehlungen
  - ASIL Anwendung
  - (ASIL) Empfehlung

Quelle: ISO/DIS 26262-2

Fraunhofer IPA

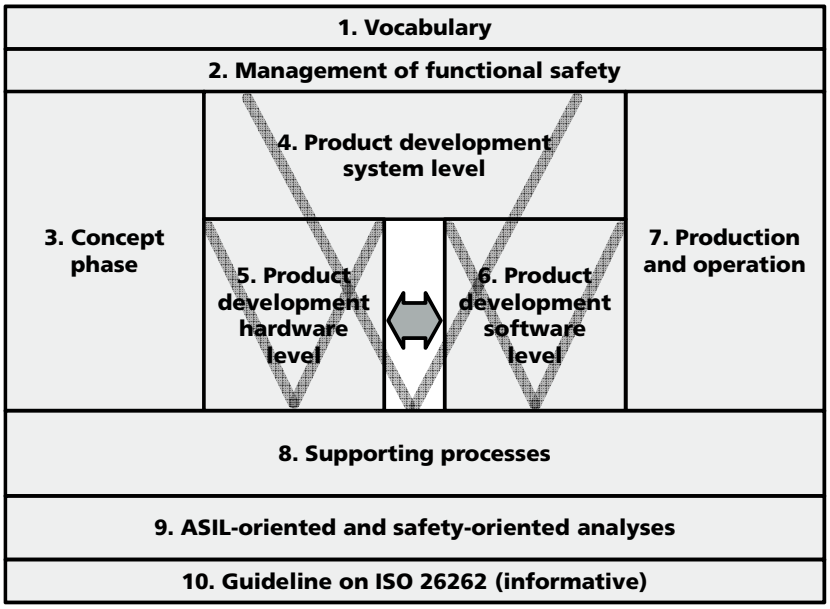
ISO 26262
Lebenszyklusmodell der ISO 26262



Quelle: ISO/DIS 26262

Fraunhofer IPA

ISO 26262
Lebenszyklusmodell der ISO 26262 (vereinfacht)



Quelle: ISO/DIS 26262

Fraunhofer IPA

ANFORDERUNGEN DER ISO 26262 (KAPITEL 2)

Fraunhofer IPA

ISO 26262
Anforderungen der ISO 26262-2

Definition der Anforderungen der für den Sicherheitslebenszyklus verantwortlichen Organisationen

- Sicherheitskultur
- Kompetenzen
- Qualitätsmanagement

Definition der Rollen, Verantwortlichkeiten und Tätigkeiten für das Sicherheitsmanagement während der Entwicklung der Einheit

- Sicherheitsmanager
- Projektmanager
- Audit, Review, Assessment der Sicherheitsaktivitäten

Quelle: ISO/DIS 26262-2

Fraunhofer IPA

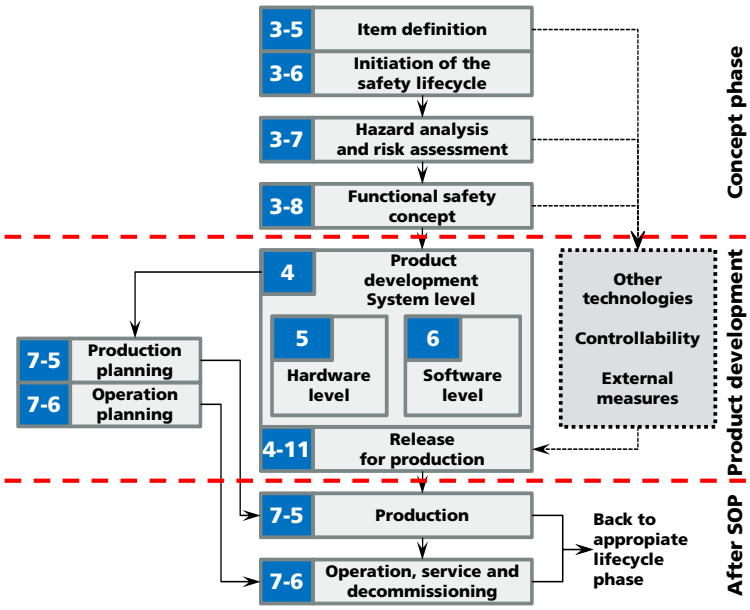
ISO 26262
Management der Funktionalen Sicherheit (Safety plan)

Der Safety-Plan enthält die zur Sicherstellung der Funktionalen Sicherheit erforderliche Aufbau- und Ablaufplanung (Phasen, Meilensteine, Verantwortlichkeiten, Dokumente) hinsichtlich:

- Strategien und Aktivitäten
- Schnittstellenabstimmung mit Lieferanten
- Unterstützende Prozesse
- Gefahren- und Risikoanalyse
- Entwicklung und Umsetzung der Sicherheitsanforderungen
- Verifikation und Validation
- Dokumente

ANFORDERUNGEN DER ISO 26262 (KAPITEL 3)

ISO 26262
Sicherheits-Lebenszyklus (safety lifecycle)



Quelle: ISO/DIS 26262-2

Fraunhofer IPA

ISO 26262
Anforderungen der ISO 26262-3
Hazard analysis and risk assessment

Identifizierung und Kategorisierung der Gefahren durch den Betrachtungsgegenstand

- Analyse der Betriebsbedingungen und Identifikation der Gefahren
  - Vollständige Auflistung der Betriebsbedingungen
  - Systematische Ableitung und Definition der Gefahren sowie Auswirkungen für alle Betriebsbedingungen
- Bewertung der Gefahren
  - S0-S3: Schwere der potentiellen Gefahr
  - E0-E4: Dauer des Ausgesetzseins in der Betriebssituation
  - C0-C3: Beherrschbarkeit durch Fahrer und/oder Beteiligte
- Kategorisierung der Gefahren (ASIL)
  - ASIL A - D
  - QM

Quelle: ISO/DIS 26262-3

Fraunhofer IPA

ISO 26262
Anforderungen der ISO 26262-3
Functional safety concept

Sicherheitsziele zur Vermeidung oder Abschwächung der Gefahren

- Definition der Sicherheitsziele

Spezifikation der funktionalen Sicherheitsanforderungen

- Zustandsbeschreibung
- Warn- und Degradationskonzept
- Notbetriebskonzept
- Reaktionskonzept durch Fahrer

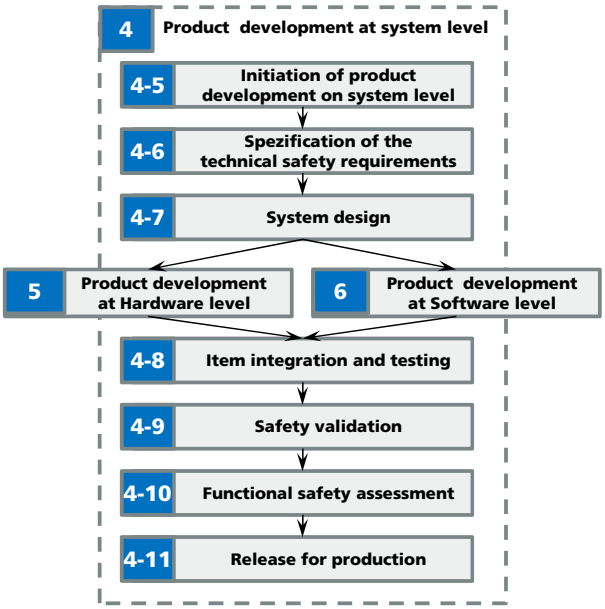
Verifizierung, Bewertung, Validierung und Review des Sicherheitskonzepts

- Verifizierung, Bewertung, Validierung und Review des funktionalen Sicherheitskonzepts auf Übereinstimmung mit den Sicherheitszielen

Quelle: ISO/DIS 26262-3

ANFORDERUNGEN DER ISO 26262 (KAPITEL 4)

ISO 26262
Anforderungen der ISO 26262-4
Produktentwicklung auf Systemebene



Quelle: ISO/DIS 26262-4

Fraunhofer IPA

ISO 26262
Anforderungen der ISO 26262-4

Entwicklung und Verifizierung der technischen Sicherheitsanforderungen

- Sicherheitsmechanismen und Systemreaktionen (safe state)
- Maßnahmen zur Vermeidung von systematischen Fehlern
- Vermeidung schlafender (latent) Abweichungen
  [Empfohlen bei A und B / Gefordert bei C und D]
- Entwicklung von Sicherheitsmechanismen zur Vermeidung / Diagnose schlafender Doppelfehler
- Maßnahmen zur Beherrschung zufälliger HW-Fehler im Betrieb
- Zuordnung der Sicherheitsanforderungen auf Hardware und Software
- Spezifikation der Hardware- und Software-Schnittstellen (HSI)
- Verifizierung des System Designs

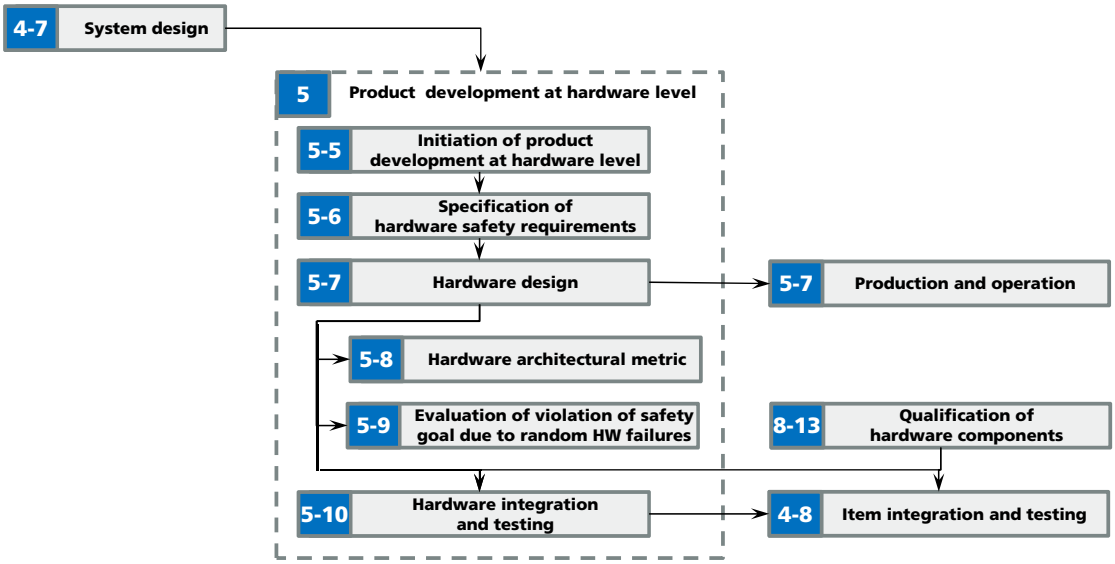
Quelle: ISO/DIS 26262-4

Fraunhofer IPA

ANFORDERUNGEN DER ISO 26262 (KAPITEL 5)

Fraunhofer IPA

ISO 26262
Anforderungen der ISO 26262-5
Produktentwicklung auf Hardwareebene



Quelle: ISO/DIS 26262-5

Fraunhofer IPA

ISO 26262
Anforderungen der ISO 26262-5
Hardware architectural metrics

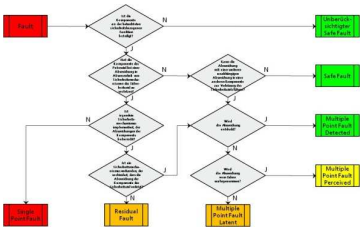
Bewertung der Hardwarearchitektur in Bezug auf Behandlung zufälliger Hardwarefehler

- ASIL (B), C, D: Anwendung Hardwaremetriken und Einhaltung von Zielwerten
  - Robustheit gegenüber Einfachfehlern
  - Robustheit gegenüber Mehrfachfehlern
  - Zufällige Hardwarefehler mit gefahrbringender Wirkung
- ASIL (B), C, D: Review der Bewertung

Quelle: ISO/DIS 26262-5

Fraunhofer IPA

ISO 26262
ISO 26262-5, Annex C
Zufällige Hardwarefehler

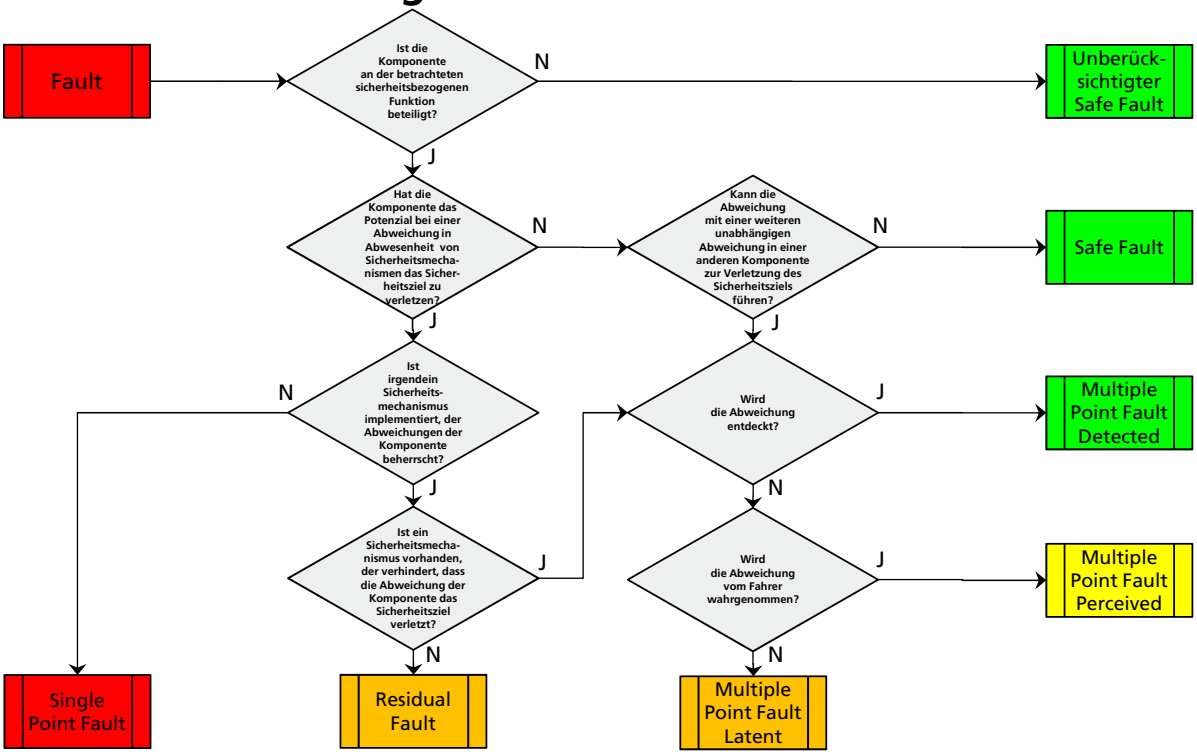


- Single point fault (SPF)
  Abweichung, die durch keinen Sicherheitsmechanismus abgedeckt ist und sofort zur Verletzung eines Sicherheitsziels führt
- Residual fault (RF)
  Teil einer Abweichung, der nicht durch einen Sicherheitsmechanismus abgedeckt wird und welcher zur Verletzung eines Sicherheitsziels führt
- Multiple point fault (MPF)
  Abweichung unter mehreren unabhängigen Abweichungen, welche in Kombination zu einem Mehrfachfehler führt
  - Perceived (MPF P)
    bemerkt
  - Detected (MPF D)
    entdeckt
  - Latent (MPF L)
    schlafend

Quelle: ISO/DIS 26262-5

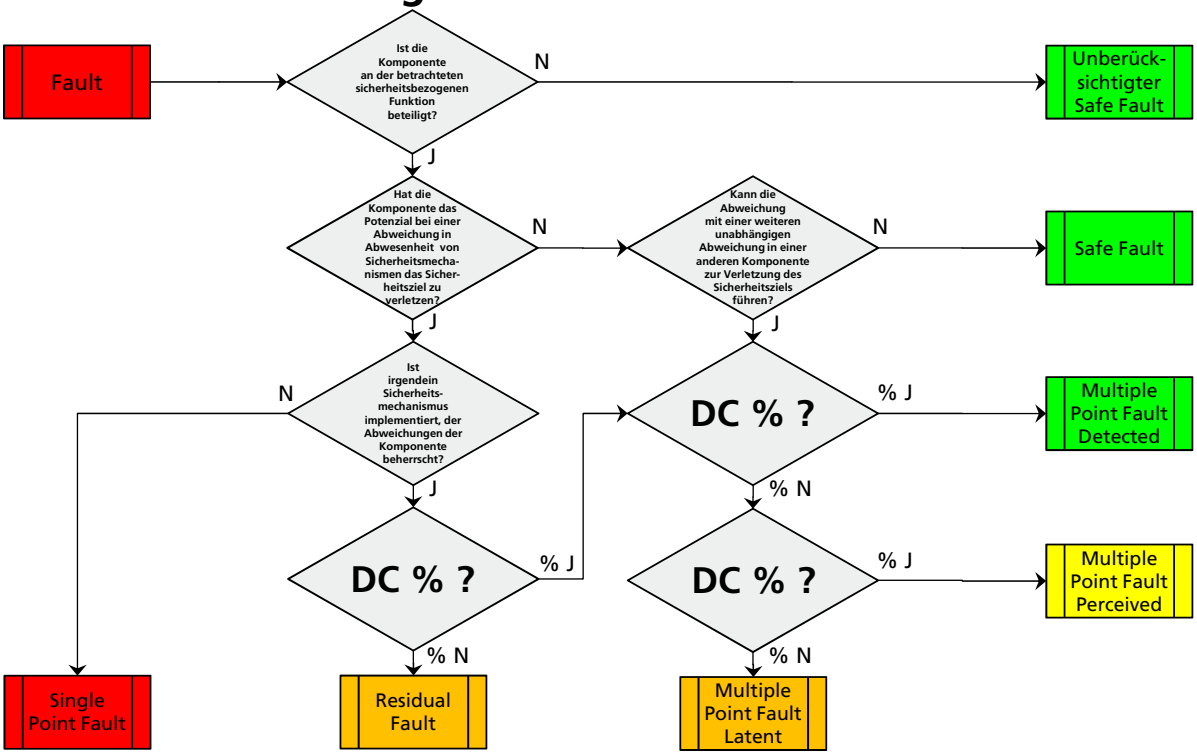
Fraunhofer IPA

Fault-Klassifizierung nach ISO 26262



Fraunhofer IPA

Fault-Klassifizierung nach ISO 26262



Fraunhofer IPA

ISO 26262

Berechnungsalgorithmen für Fault-Metriken und gefahrbringende Ausfälle nach ISO 26262-5, Annex E und G

$$\text{Single Point Fault metric} = 1 - \frac{\sum(\lambda_{SPF} + \lambda_{RF})}{\sum \lambda}_{\text{Safety related HW elements}} = \frac{\sum(\lambda_{MPF} + \lambda_{S})}{\sum \lambda}_{\text{Safety related HW elements}}$$

$$\text{Latent Fault metric} = 1 - \frac{\sum(\lambda_{MPF\ Latent})}{\sum(\lambda - \lambda_{SPF} - \lambda_{RF})}_{\text{safety related HW elements}} = \frac{\sum(\lambda_{MPF\ perceived\ or\ detected} + \lambda_{S})}{\sum(\lambda - \lambda_{SPF} - \lambda_{RF})}_{\text{safety related HW elements}}$$

where $\sum \lambda_x$ (safety related HW elements) is the sum of λ_x of the safety-related hardware elements of the item.

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

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

Quelle: ISO/DIS 26262-5

Fraunhofer IPA

ISO 26262

ISO 26262-5, Annex D (informative) Ermittlung von Diagnosedeckungsgraden (DC)

Ermittlung und Realisierung der Diagnosedeckungsgrade kann auf Basis von Empfehlungen der ISO/DIS 26262-5, Annex D (Tabelle 1-12 und Erläuterung D 2.1-D 2.11) erfolgen (z.B. ROM und Block replication)

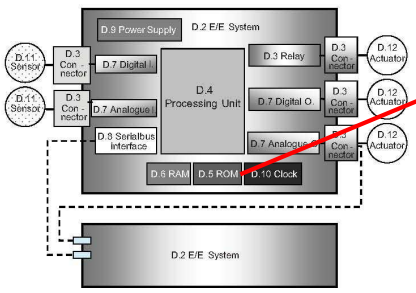


Table D.5 — Invariable memory ranges

Diagnostic technique/measure	See overview of techniques	Maximum diagnostic coverage considered achievable	Notes
Parity bit	-	Low	
Detection of memory data failures with error-detection-correction codes (EDC)	D.2.4.1	High	The effectiveness depends on the number of redundant bits.
Modified checksum	D.2.4.2	Low	-
Signature of one byte (8-bit) (CRC)	D.2.4.3	Medium	The effectiveness of the signature depends on the polynomial in relation to the block length of the information to be protected.
Signature of a double byte (16-bit) (CRC)	D.2.4.4	High	The effectiveness of the signature depends on the polynomial in relation to the block length of the information to be protected.
Block replication	D.2.4.5	High	-

D.2.4.5 Block replication (for example double memory with hardware or software comparison)

NOTE This technique/measure is referenced in Table D.5 and D.6.

Aim: To detect each bit failure.

Description: The address space is duplicated in two memories. The first memory is operated in the normal manner. The second memory contains the same information and is accessed in parallel to the first. The outputs are compared and a failure message is produced if a difference is detected. In order to detect certain kinds of bit errors, the data is to be stored inversely in one of the two memories and inverted once again when read.

Quelle: ISO/DIS 26262-5

Fraunhofer IPA

Funktionale Sicherheit
Ermittlung der Fehlermodi und Fehlerraten von Systemelementen


SIEMENS

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

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

Ermittlung der Fehlermodi und FIT-Werte von Systemelementen:

- Literatur zur Zuverlässigkeit (z.B. Birolini)
- 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 von Systemelementen

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 >100 kOhm	0,3 1	55
Metallschicht / *Metal film*		0,2	55
Netzwerke (Schichtschaltung) je Widerstandselement ***Networks (film circuits) per resistor element***	Standard kundenspezifische / *Custom design*	0,1 0,5	55
Metalloxidschicht / *Metal-oxide*		5	85
Draht / *Wire-wound*		5	85
Veränderbare / *Variable*		30	55

1 FIT = $1x10^{-9}$ 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 aus Birolini:
Open = 40% 0,4 FIT (open)
Drift = 60% 0,6 FIT (drift)

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

Ermittlung der Fehlerraten komplexer Systemelemente

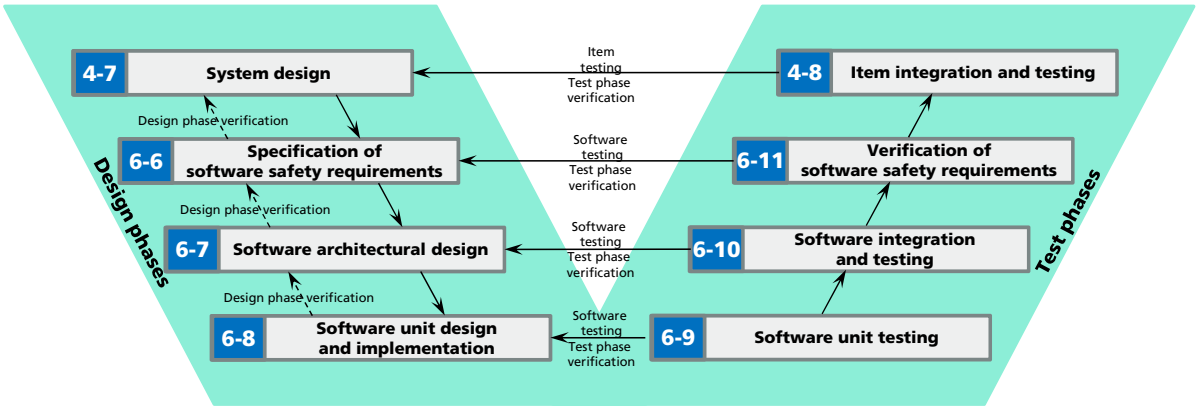
Verfahren zur Aufteilung von FIT-Werten bei komplexen Bauteilen:

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

Bildquelle: www.kurz-elektronik.de

ANFORDERUNGEN DER ISO 26262 (KAPITEL 6)

ISO 26262
Anforderungen der ISO 26262-6
Produktentwicklung auf Softwareebene



Quelle: ISO/DIS 26262-6

Fraunhofer IPA

Software in mechatronischen System
Charakteristika von Software

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 IPA

Testplan

- Auf Basis von systematischen Risikoanalysen lassen sich detaillierte Testpläne ableiten mit deren Hilfe das korrekte Funktionieren der Diagnose- und Absicherungsmaßnahmen (im Allgemeinen durch die Software realisiert) unter allen nutzerbedingten Interaktionen und Systemzuständen analysiert werden kann.

Anmerkung:

- Detaillierte und für den Testingenieur verständliche Beschreibung der Testfälle
- Durchführung der Testfälle auf der Test-Bench mit der Zielsoftware
- Verwendung von speziellen Fehlermustern und Break-Out-Boxen zur Simulation der Fehlerfälle (neue Testverfahren)

ANFORDERUNGEN DER ISO 26262 (KAPITEL 7)

ISO 26262
Anforderungen der ISO 26262-7

Planung und Sicherstellung der Produktion sicherheitsbezogener Produkte

- Planung und Beschreibung der Produktion
- Software und Kalibrierung
- Prüfmaßnahmen
- Risikoanalysen
- Abweichungsmanagement
- Planung der Prozesse für Benutzer, Service, Reparatur und Außerbetriebnahme
- Erstellung der Benutzerdokumentation
- Feldbeobachtung

Quelle: ISO/DIS 26262-7

Fraunhofer IPA

ANFORDERUNGEN DER ISO 26262 (KAPITEL 8)

Fraunhofer IPA

ISO 26262
Anforderungen der ISO 26262-8
Supporting processes

- Schnittstellenmanagement bei verteilter Entwicklung
- Management von Sicherheitsanforderungen
- Konfigurationsmanagement
- Änderungsmanagement
- Dokumentation
- Qualifizierung von Softwarekomponenten
- Qualifizierung von Hardwarekomponenten
- Argumentation „Proven in use“

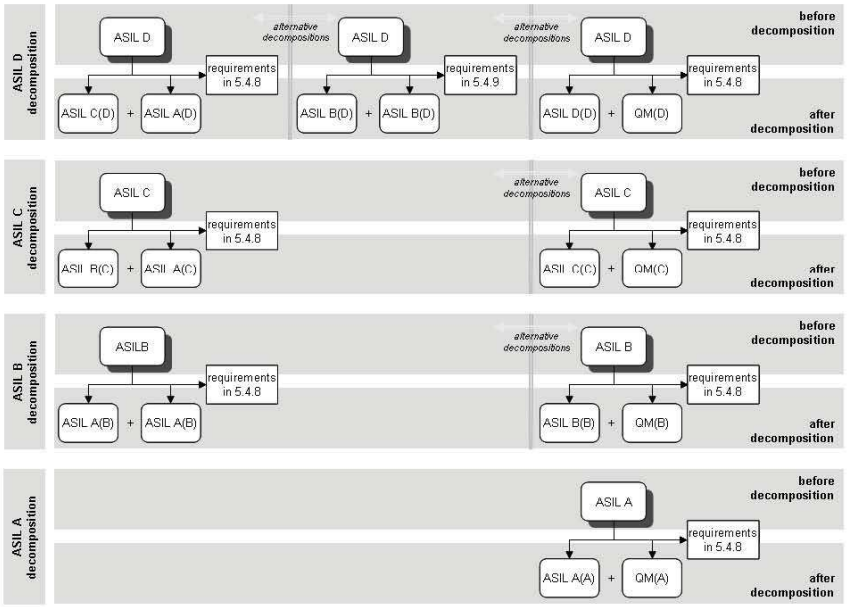
Quelle: ISO/DIS 26262-8

Fraunhofer IPA

ANFORDERUNGEN DER ISO 26262 (KAPITEL 9)

Fraunhofer IPA

ISO 26262
Anforderungen der ISO 26262-9
Dekomposition



Quelle: ISO/DIS 26262-9

Fraunhofer IPA

METHODEN ZUR ANALYSE MECHATRONISCHER SYSTEME

Fraunhofer IPA

Methoden zur SIL-Klassifizierung

- Gefahren- und Risikoanalyse
- Risikograph

Methoden zur Analyse systematischer Fehler

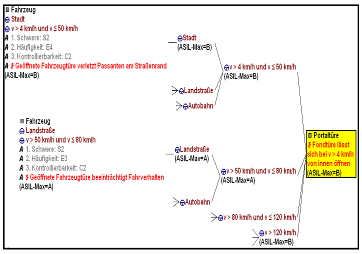
- Fehlermöglichkeits- und Einflussanalyse (FMEA)
- Fehlerbasierte System-Reaktionsanalyse (FSR)

Methoden zur Analyse zufälliger Fehler

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

METHODEN ZUR SIL-KLASSIFIZIERUNG

Methoden zur Analyse mechatronischer Systeme
Gefahren- und Risikoanalyse



Zielsetzung:

- Systematische Ermittlung potentieller Gefahren- und Risiken des Systems

Methodisches Vorgehen:

- Definition der Hauptfunktionen des Systems
- Ermittlung der potentiellen Fehlfunktionen
- Ermittlung der Gefahren und Risiken

Nutzen/Anmerkung:

- Frühzeitige Durchführung
- Betrachtung unabhängig vom Sicherheits-konzept (Grundlage für Sicherheitskonzept)
- Voraussetzung zur (A)SIL-Einstufung

Fraunhofer IPA

Methoden zur Analyse mechatronischer Systeme
Risikograph zur ASIL-Klassifizierung nach ISO/DIS 26262

Severity S	Exposure E	Controllability C: 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

[nach ISO DIS 26262]

Zielsetzung:

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

Methodisches Vorgehen:

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

Nutzen/Anmerkung:

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

Fraunhofer IPA

Risikograph zur ASIL-Klassifizierung nach ISO/DIS 26262

Exposure E Controllability C

Severity S		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

[nach ISO/DIS 26262]

Schwere (Severity)

S0: **keine** Verletzungsgefahr
S1: **geringe** und **mäßige** Verletzungen
S2: **ernste** und **möglicherweise tödliche** Verletzungen
S3: **schwere** und **wahrscheinlich tödliche** Verletzungen

Häufigkeit des Ausgesetztseins (Exposure)

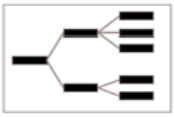
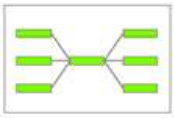
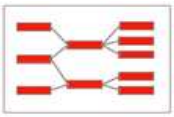
E1: **selten:** Situation tritt für die meisten Fahrer seltener als einmal pro Jahr auf
E2: **gelegentlich:** Situation tritt für die meisten Fahrer wenige Male pro Jahr auf
E3: **ziemlich oft:** Situation tritt für Durchschnittsfahrer einmal im Monat oder öfter auf
E4: **oft:** Situation die bei nahezu jeder Fahrt auftritt

Beherrschbarkeit (Controllability)

C1: **einfach beherrschbar:** mehr als 99% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden
C2: **durchschnittlich beherrschbar**: mehr als 90% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden
C3: **schwierig oder gar nicht beherrschbar**: weniger als 90% der Fahrer oder der anderen Verkehrsteilnehmer können den Schaden üblicherweise abwenden

METHODEN ZUR ANALYSE SYSTEMATISCHER FEHLER

Methoden zur Analyse mechatronischer Systeme
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):

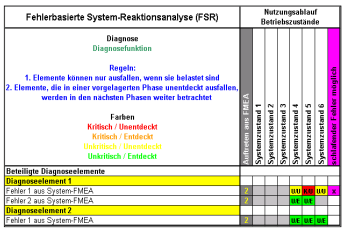
1: Strukturanalyse (Strukturbaum)
2: Funktionsanalyse (Funktionsnetze)
3: Fehleranalyse (Fehlernetze)
4: Maßnahmenanalyse und Bewertung
5: Optimierung (falls notwendig)

Nutzen/Anmerkung:

- Detaillierte Übersicht über Fehlfunktionen
- Maßnahmenplan für sichere Systemauslegung
- Präzise Benennung der Fehlfunktionen

Fraunhofer IPA

Methoden zur Analyse mechatronischer Systeme
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 von Ausfallarten unter Berücksichtigung von nutzerbedingten Interaktionen und Systemzuständen

Nutzen/Anmerkung:

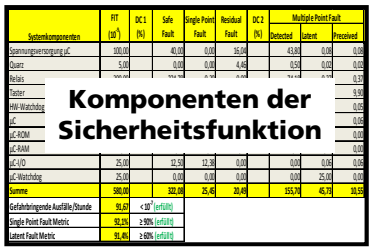
- Hinweise auf „schlafende Fehler“ im System
- Weitere Gegenüberstellung schlafender Fehler in Paarvergleichsmatrizen

Fraunhofer IPA

METHODEN ZUR ANALYSE ZUFÄLLIGER FEHLER

Fraunhofer IPA

Methoden zur Analyse mechatronischer Systeme
Failure Modes, Effects and Diagnostic Analysis (FMEDA)



FMEDA

Zielsetzung:

- Analyse der Fehlermodi der an der Sicherheits-funktion beteiligten Komponenten

Methode:

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

Nutzen/Anmerkung:

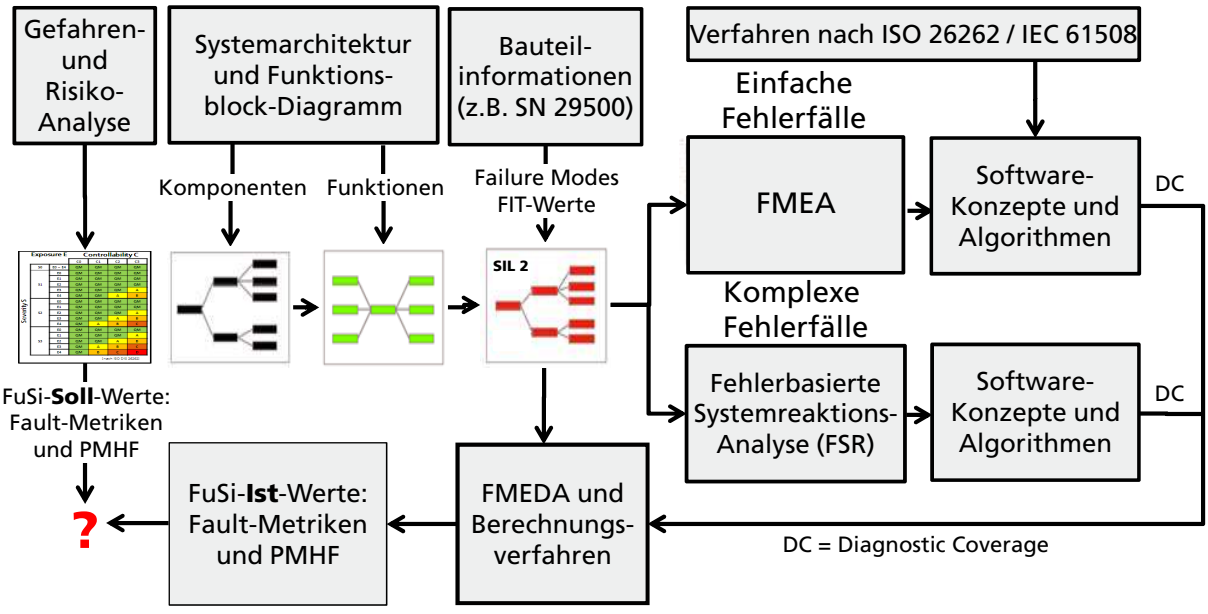
- Tabellarisches Verfahren zur Berechnung der FuSi-Parameter (z.B. PMHF, Fault-Metriken)
- Pro Sicherheitsziel Erstellung einer FMEDA

Fraunhofer IPA

VORGEHENSWEISE ZUR ANALYSE MECHATRONISCHER SYSTEME

Fraunhofer IPA

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



Fraunhofer IPA

ERLÄUTERUNG ANHAND EINES BEISPIELSYSTEMS

Fraunhofer IPA

Erläuterung anhand eines Beispielsystems
Beispielsystem (Fahrzeug und Werte zufällig gewählt)

Quelle: http://www.imcdb.org

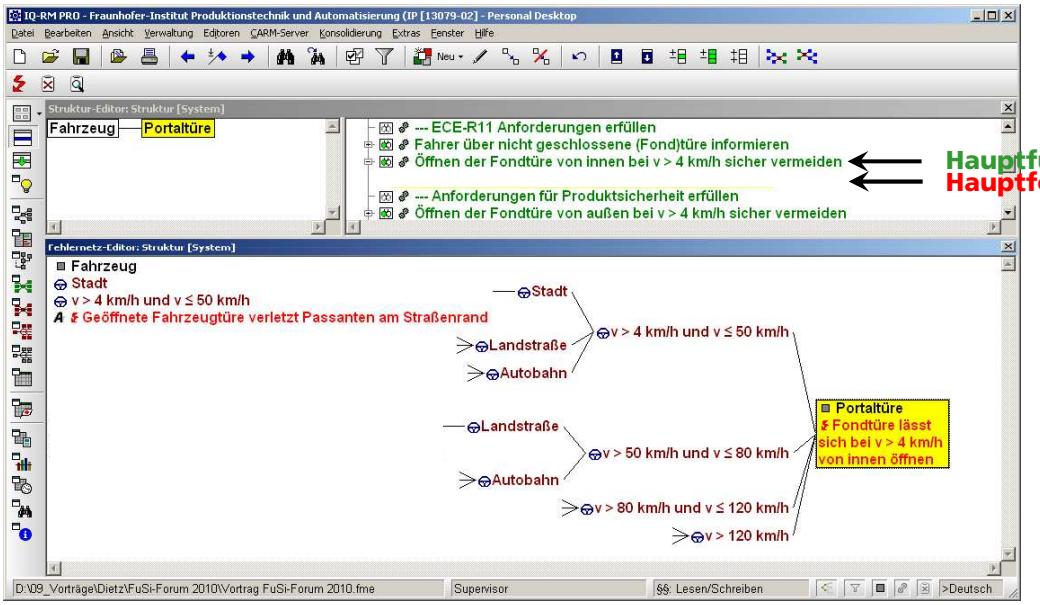
1965

Quelle: http://www.automobilrevue.de/detroit2002.htm

20xx ?

Fraunhofer IPA

Erläuterung anhand eines Beispielsystems
Gefahren- und Risikoanalyse



Fraunhofer IPA

Erläuterung anhand eines Beispielsystems
Möglicher Risikograph gemäß ISO/DIS 26262

Fehlfunktionen und Auswirkungen aus der Gefahren- und Risikoanalyse

Fahrzeug
Geöffnete Fahrzeugtüre verletzt Passanten am Straßenrand

Portaltüre
Fondtüre lässt sich bei v > 4 km/h von innen öffnen

S	E	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

Severity – S:
S2: Schwere Verletzungen, lebensbedrohlich, Überleben wahrscheinlich

Exposure – E:
E4: hohes bzw. ständiges Auftreten

Controllability – C:
C2: durchschnittlich beherrschbar: mehr als 90% der Fahrer bzw. Verkehrsteilnehmer können den Schaden üblicherweise abwenden

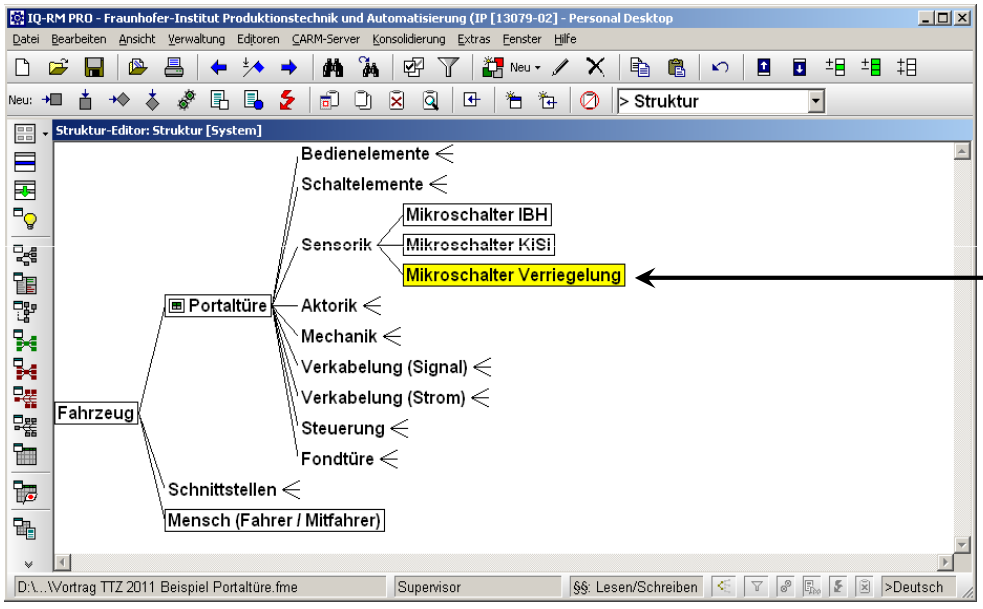
ASIL B
PFH < 10^{-7}
SPFM ≥ 90%
LFM ≥ 60%

Fraunhofer IPA

ANALYSE SYSTEMATISCHER FEHLER

Fraunhofer IPA

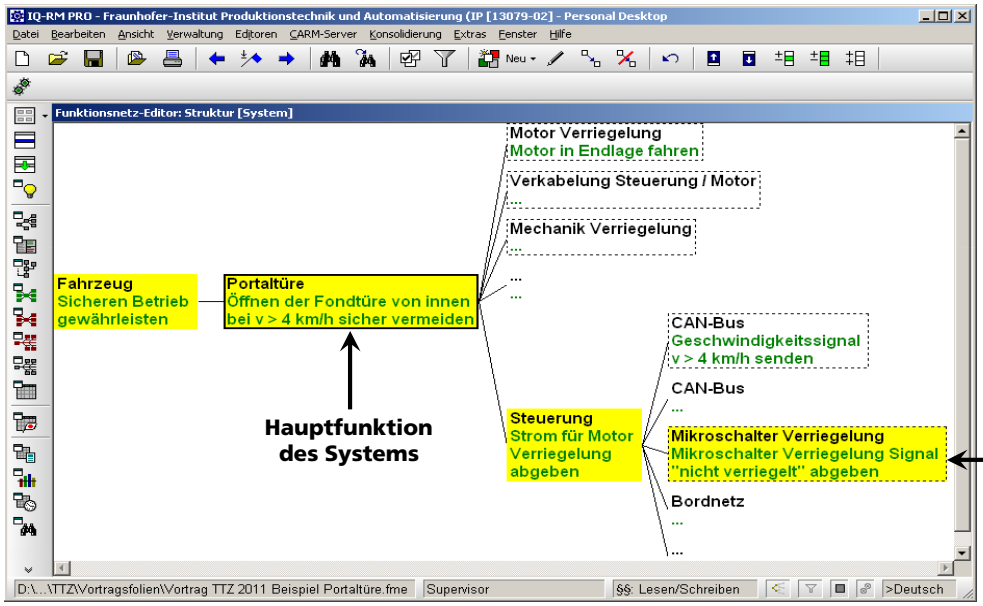
Erläuterung anhand eines Beispielsystems
Mögliche Systemstruktur einer „Portaltüre“



Diagnose-system (Sensorik)

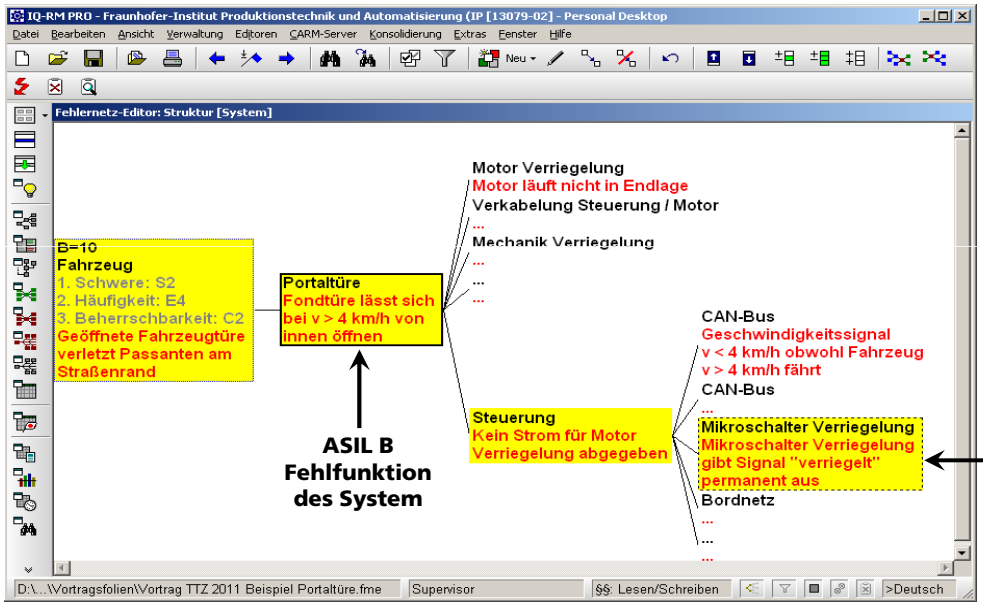
Fraunhofer IPA

Erläuterung anhand eines Beispielsystems
Mögliches Funktionsnetz einer „Portaltüre“



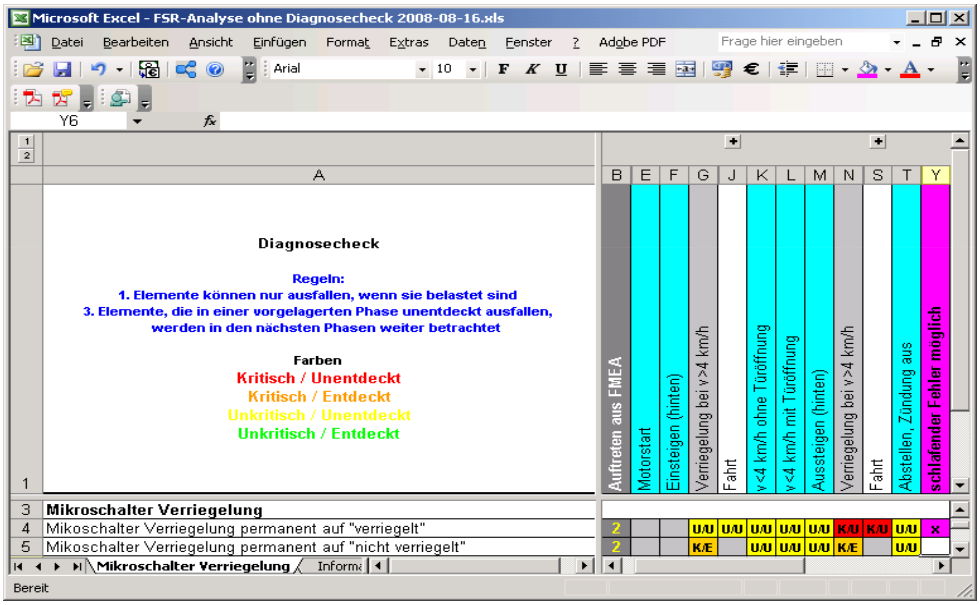
Fraunhofer IPA

Erläuterung anhand eines Beispielsystems
Mögliches Fehlernetz einer „Portaltüre“



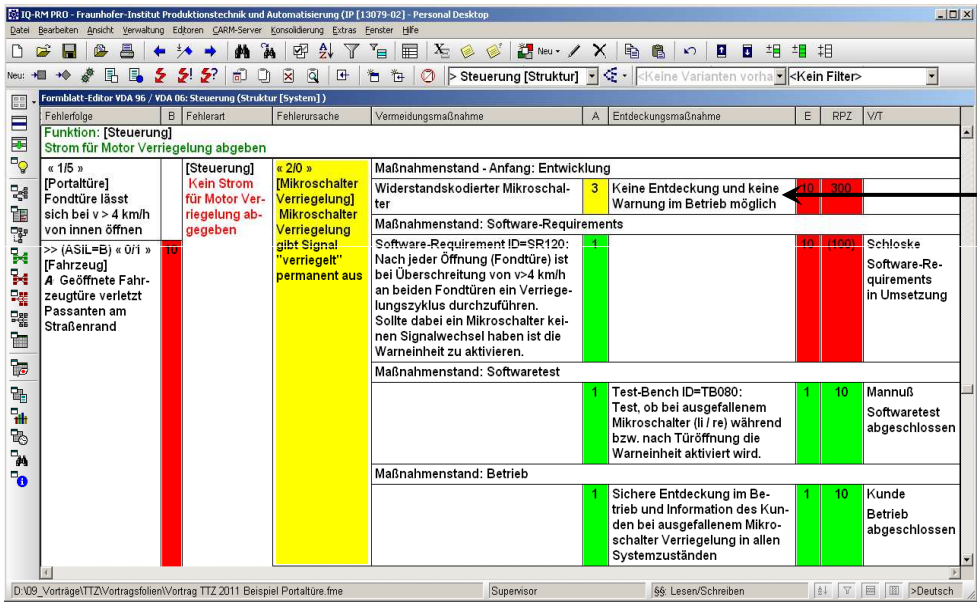
Fraunhofer IPA

Erläuterung anhand eines Beispielsystems
Mögliche FSR eines Diagnosesystems der „Portaltüre“



Fraunhofer IPA

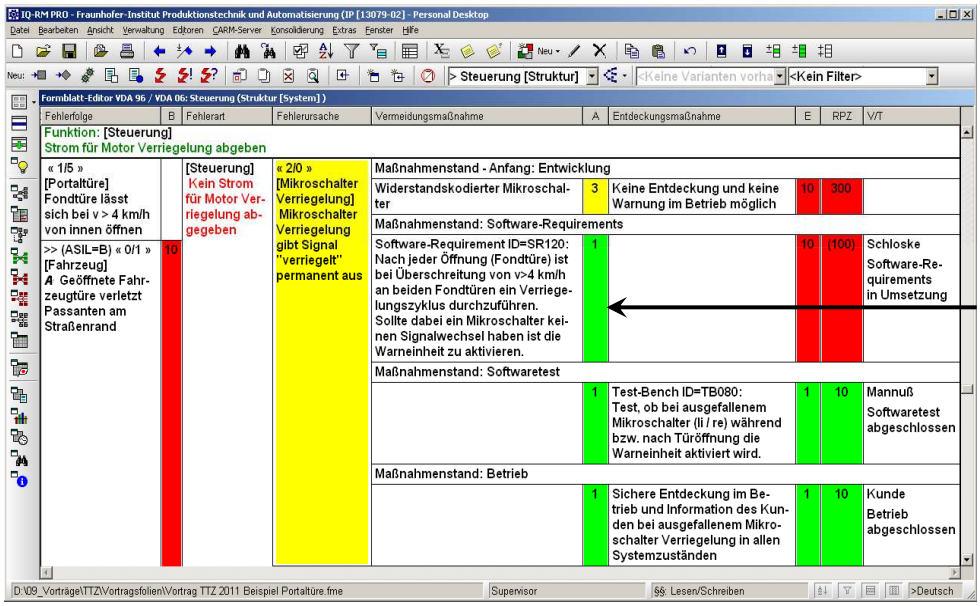
Erläuterung anhand eines Beispielsystems
Mögliches Formblatt einer „Portaltüre“



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

Fraunhofer IPA

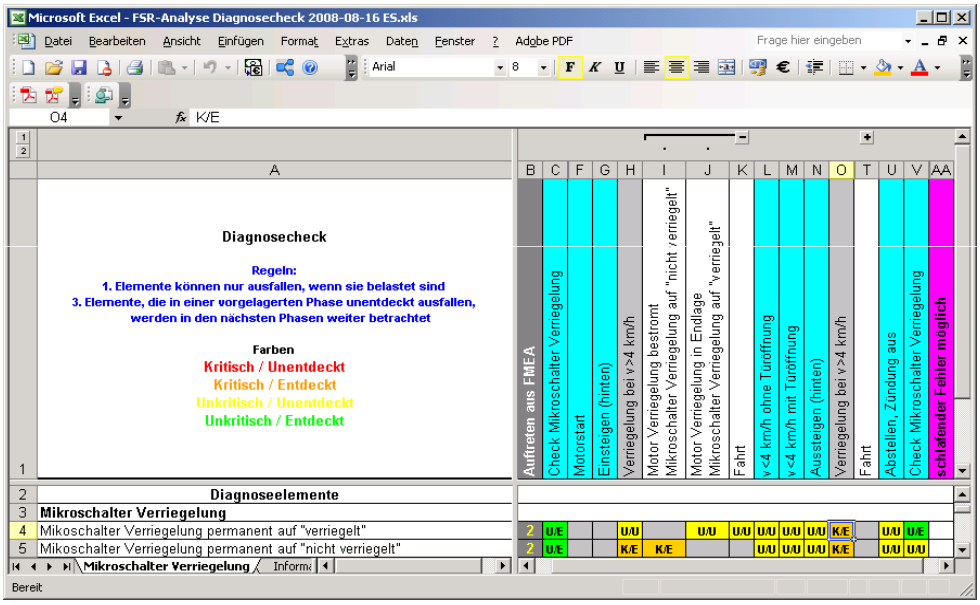
Erläuterung anhand eines Beispielsystems
Mögliches Formblatt einer „Portaltüre“



Sichere Fehlererkennung der Sensorik im Betrieb und Information des Fahrers

Fraunhofer IPA

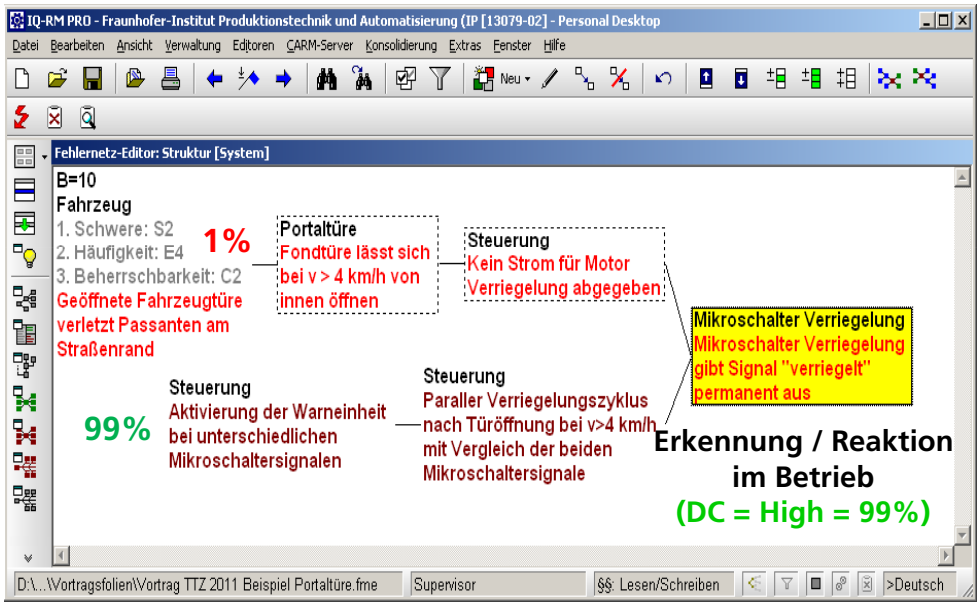
Erläuterung anhand eines Beispielsystems
Mögliche FSR eines Diagnosesystems der „Portaltüre“



Fraunhofer IPA

Erläuterung anhand eines Beispielsystems

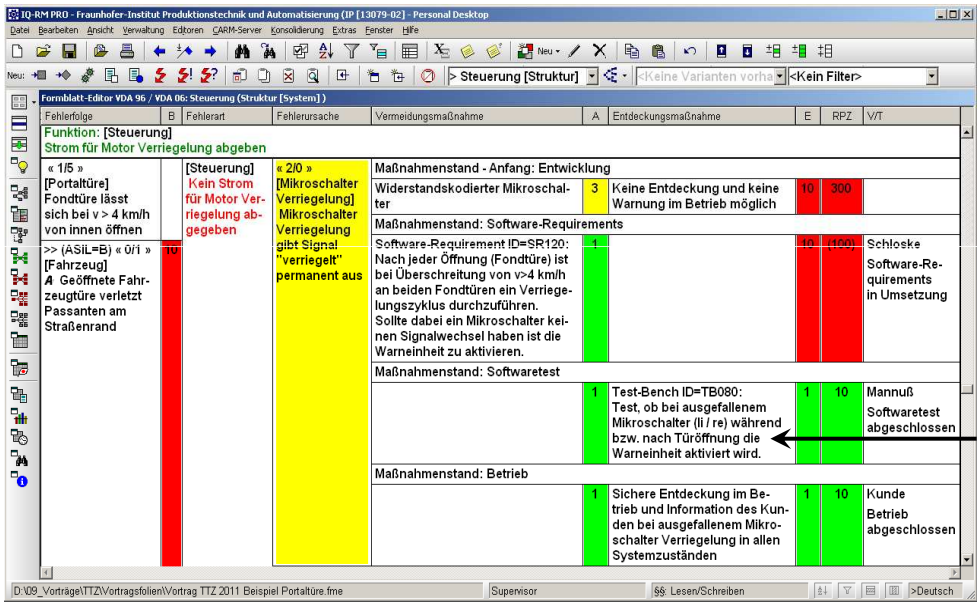
Analyse und Bewertung von Fehlfunktionen, Fehlererkennung und Fehlerreaktion im System „Portaltüre“



Fraunhofer IPA

Erläuterung anhand eines Beispielsystems

Mögliches Formblatt einer „Portaltüre“



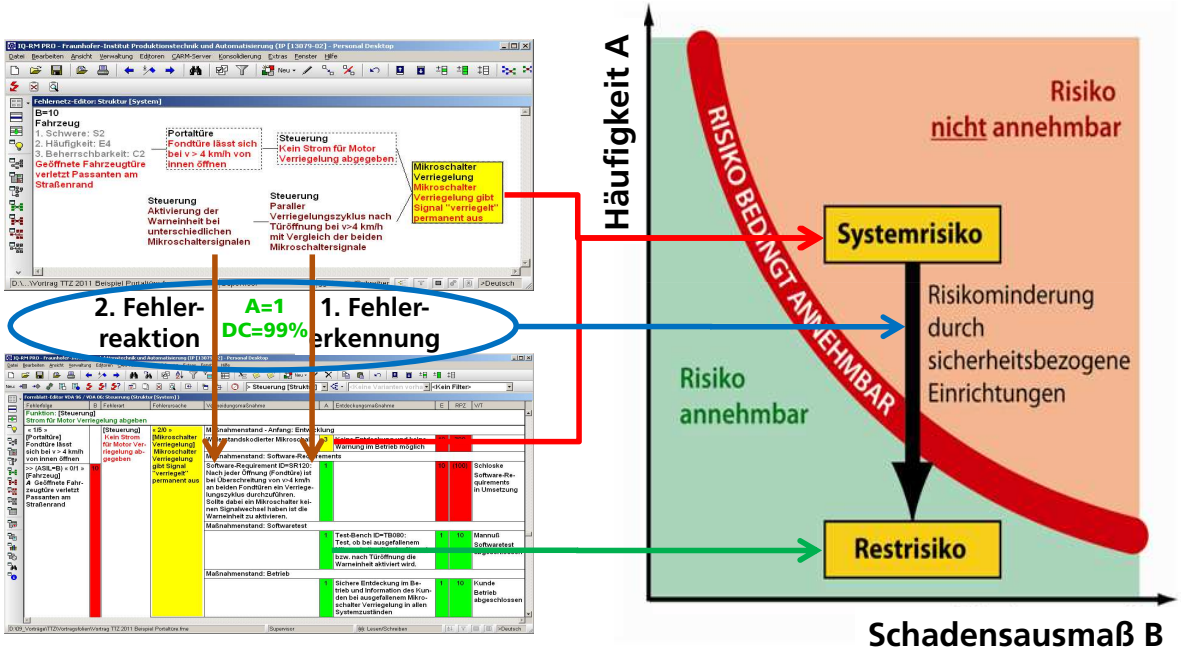
Nachweis erbracht!

Sichere Fehlererkennung an der Sensorik im Betrieb und Information des Fahrers

Fraunhofer IPA

Fehlermöglichkeits- und Einflussanalyse (FMEA)

Analyse und Bewertung von Fehlfunktionen, Fehlererkennungen und Fehlerreaktionen im Betrieb



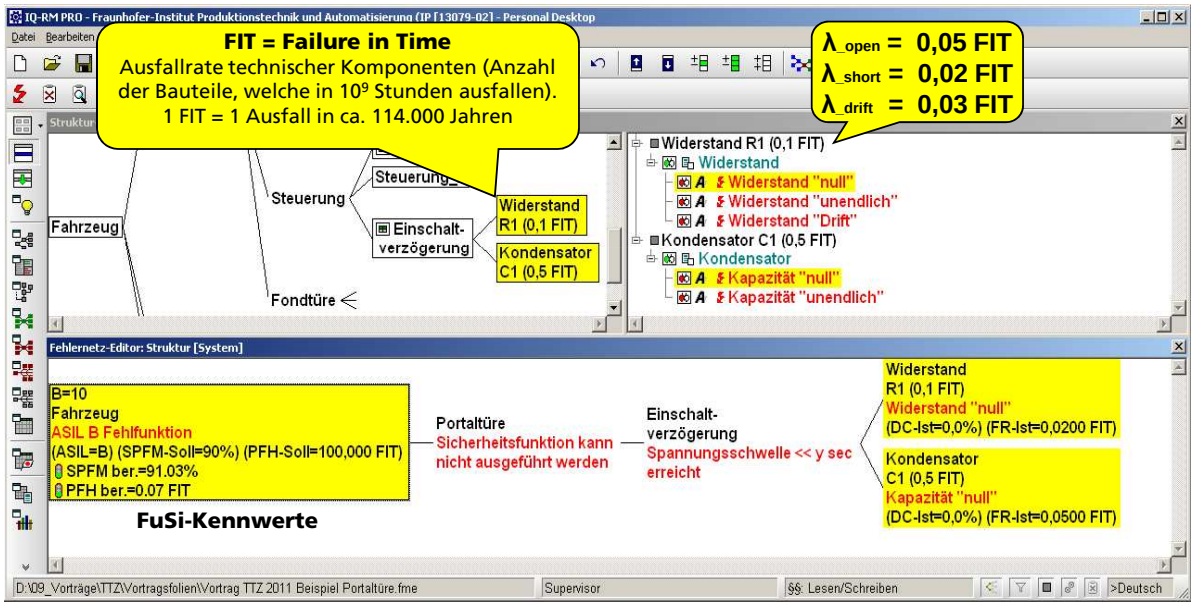
Fraunhofer IPA

ANALYSE ZUFÄLLIGER FEHLER

Fraunhofer IPA

Erläuterung anhand eines Beispielsystems

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



Fraunhofer IPA

Failure Modes, Effects and Diagnostic Analysis (FMEDA)

FMEDA für einen µC (gemäß ISO 26262)

Sicherheitsziel 1: Keine ungewollte Aktivierung der EPB während der Fahrt													
Komponente	FIT-Wert	Sicherheitsrelevant:	Fehlerart / Abweichung	Fehlerratenverteilung (FIT)	Potenzial zur Verletzung des Sicherheitsziels in Abwesenheit eines Sicherheitsmechanismus	Sicherheitsmechanismus zur Vermeidung der Verletzung des Sicherheitsziels	Abdeckung der Fehlerart / Abweichung zur Verletzung des Sicherheitsziels	Residual oder Single Point Fault (Fehlerrate / FIT)	Fehlerart / Abweichung, welche zusammen mit einer anderen unabhängigen Fehlerart / Abweichung zu einer Verletzung des Sicherheitsziels führen kann	Sicherheitsmechanismus zur Vermeidung eines latenten Fehlers / Abweichung	Abdeckung der der latenten Fehlerart / Abweichung	Latent Multiple-Point Fault (Fehlerrate / FIT)	
µC-Logik	20,00	ja	Ausfall zu Stuck at ON während der Fahrt	9,9000	x	keine	0%	9,9000					
			Ausfall zu Stuck at OFF während der Fahrt	9,9000									
			Ausfall zu Stuck at ON im Stand	0,1000									
			Ausfall zu Stuck at OFF im Stand	0,1000									
µC-ROM	20,00	ja	Bitkipper oder Zelldefekt	10,0000	x	Checksummenprüfung beim Einlesen	99%	0,1000					
			Bitkipper oder Zelldefekt	10,0000									
µC-RAM	20,00	ja	Bitkipper oder Zelldefekt während der Fahrt	9,9000	x	Checksummenprüfung beim Ein-/Auslesen	99%	0,0990					
			Bitkipper oder Zelldefekt während der Fahrt	9,9000									
			Bitkipper oder Zelldefekt im Stand	0,1000									
			Bitkipper oder Zelldefekt im Stand	0,1000									
µC-I/O	20,00	ja	Ausfall zu Stuck at ON während der Fahrt	9,9000	x	keine	0%	9,9000					
			Ausfall zu Stuck at OFF während der Fahrt	9,9000									
			Ausfall zu Stuck at ON im Stand	0,1000									
			Ausfall zu Stuck at OFF im Stand	0,1000									
µC-Watchdog	20,00	nein	Ausfall	20,0000					x			20,0000	

Fraunhofer IPA

FAUSTFORMEL

Einfache Abschätzung eines funktional sicheren Systems
Faustformel

Rechenweg

- Summe der FIT-Werte aller beteiligten E/E-Komponenten 250 FIT
- Aufteilung auf 50% Dangerous und 50% Safe 125 FIT / 125 FIT
- Geforderte Safe Failure Fraction 90%
- (100%- SFF) x Dangerous FIT-Werte 12,5 FIT
- Vergleich mit zulässigen PFH-Wert 20,0 FIT

Quelle: Herr Habicht, TÜV Süd (2010)

FAZIT

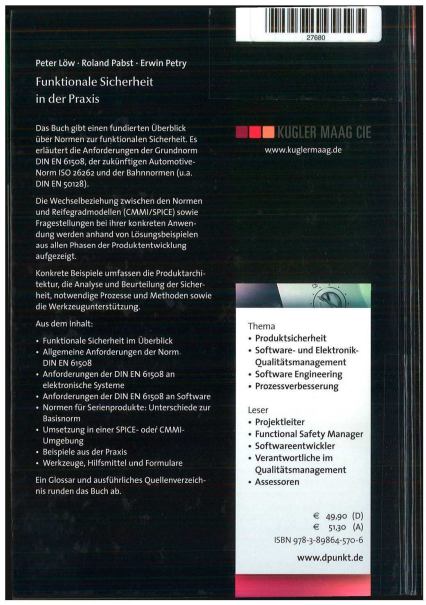
Funktionale Sicherheit
Fazit

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 Managementsysteme und Reifegradmodelle (z.B. TS 16949, SPICE, CMMI)
- Organisatorische Erweiterungen für das Safety Management entsprechend den Anforderungen der ISO 26262
- Integrierte Anwendung der Methoden und Werkzeuge
- Detaillierte und präzise Systemanalysen durch den OEM sowie effektives Schnittstellenmanagement/Kommunikation mit den Lieferanten
- Kritische Betrachtung der Risiken unabhängig von Zahlenwerten

Funktionale Sicherheit
Literaturempfehlung



Fraunhofer IPA

Fraunhofer
IPA

METHODEN DER PRODUKTENTWICKLUNG

MIT NEUEN PRODUKTEN SCHNELLER AM MARKT

Fraunhofer IPA Workshop
15. November 2012
Stuttgart