IQ-FMEA-RM-PRO 6.5 - GRAPH-EDITOR NUTZUNG BEI SICHERHEITSANALYSEN

Vertiefungsseminar der Stuttgarter Produktionsakademie,
28. Januar 2015, Stuttgart

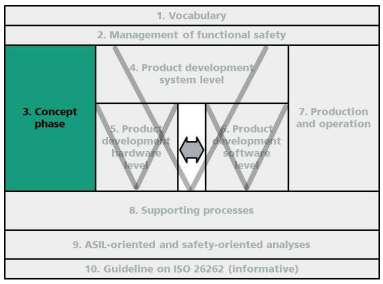
Dr.-Ing. Alexander Schloske
Senior Expert Quality Management
Functional Safety Engineer ISO 26262 und IEC 61508 (TÜV-Rheinland)
Leiter Stuttgarter Produktionsakademie
Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA

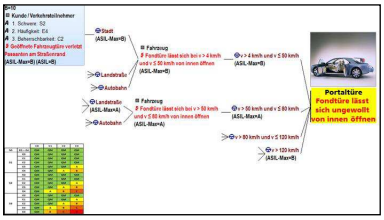
Telefon: +49(0)711 / 970-1890
E-Mail: alexander.schloske@ipa.fraunhofer.de
Internet: www.ipa.fraunhofer.de
www.stuttgarter-produktionsakademie.de

IQ-FMEA-RM-Pro 6.5 - Graph-Editor
Vortragsinhalte

- Welche Inhalte der ISO 26262 betreffen das Risikomanagement?
- Wo kann ich die IQ-RM-Pro 6.5 bei FuSi-Projekten nutzen?
- Was brauche ich bei Safety-Analysen in FuSi-Projekten?
- Welche Inhalte und Funktionalitäten bietet mir der Graph-Editor?
- Wie modelliere ich FuSi-Systeme in der IQ-RM-Pro 6.5 ?
- Was bringt mir der Graph-Editor bei FuSi-Projekten?

ISO 26262
Anforderungen (komprimiert) der ISO 26262-3



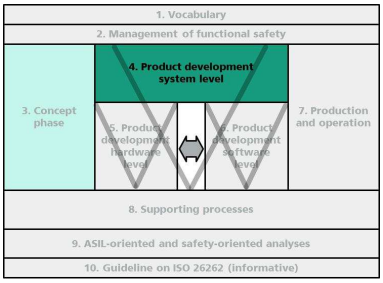


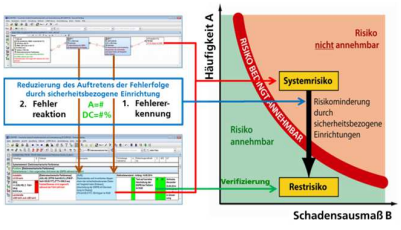
- Analyse der Betriebsbedingungen und Identifikation der Gefahren
  - Vollständige Auflistung der Betriebsbedingungen
  - Systematische Ableitung der Gefahren (Auswirkungen) anhand von Systemfehlfunktion für alle Betriebsbedingungen
- Bewertung der Gefahren
  - S0-S3: Schwere der potentiellen Gefahr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

Quelle: ISO 26262

Fraunhofer IPA

ISO 26262
Anforderungen (komprimiert) der ISO 26262-4



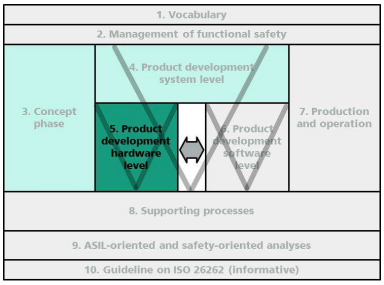


- Entwicklung des technischen Sicherheitskonzepts (TeSiKo)
  - Systemspezifikation und Systemarchitektur
  - Maßnahmen zur Vermeidung systematischer Fehler
  - Maßnahmen zur Beherrschung zufälliger HW-Fehler im Betrieb (inkl. Hardware Software Interface = HSI)
  - Definition der Sicherheitsmechanismen (Fehlererkennung und Fehlerreaktion)
  - Definition des Fehlertoleranzintervalls (FTT) und des Notfallbetriebsintervalls
  - Vermeidung schlafender (latenter) Abweichungen (empfohlen bei A und B / gefordert bei C und D)
- Verifizierung des TeSiKos

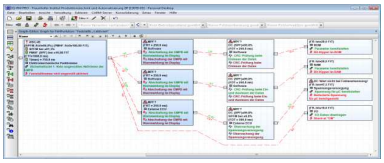
Quelle: ISO 26262

Fraunhofer IPA

ISO 26262
Anforderungen (komprimiert) der ISO 26262-5



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

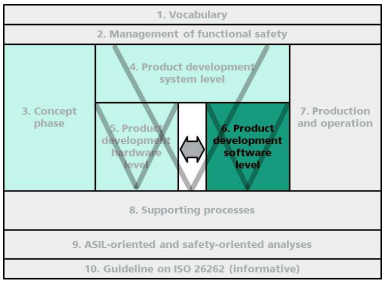


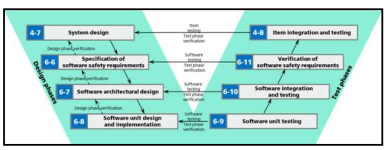
- Bewertung der Hardwarearchitektur in Bezug auf Behandlung zufälliger Hardwarefehler
- ASIL (B), C, D: Anwendung Hardwaremetriken
  - Single Point Faults Metric (bewertet die Robustheit gegenüber Single Point Faults und Residual Faults)
  - Latent Faults Metric (bewertet die Robustheit gegenüber Latent Multiple Point Faults)
- ASIL (B), C, D: Einhaltung von Zielwerten
  - Probabilistic Metric Random Hardware Faults (PMHF)
  - Single point faults metric (SPFM)
  - Latent faults metric (LFM)
- ASIL (B), C, D: Review der Bewertung

Quelle: ISO 26262

Fraunhofer IPA

ISO 26262
Anforderungen (komprimiert) der ISO 26262-6



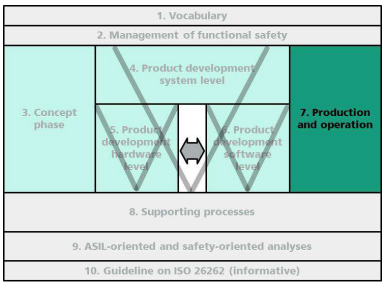


- Entwicklung der Software
  - Definition der Sicherheitsanforderungen
  - Definition der Hardware Software Interfaces
  - Entwicklung der Softwarearchitektur
  - Entwicklung des Softwaredesigns
  - Verifizierung des Softwaredesigns
- Verifizierung der Software
  - Modul-Tests
  - Integration-Tests
  - Item-Integration-Tests

Quelle: ISO 26262

Fraunhofer IPA

ISO 26262
Anforderungen (komprimiert) der ISO 26262-7

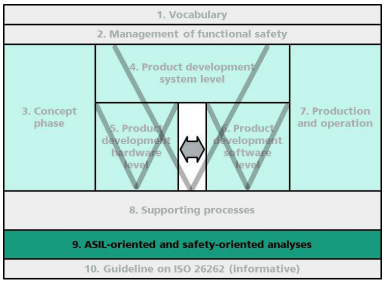


- Planung und Sicherstellung der Produktion
  - Produktionsplanung
  - Prozess-Ablauf-Plan
  - Arbeits-, Transport-, Lagerungsanweisungen
  - Fähigkeitsuntersuchungen
  - Prüfplanung
  - Control Plan (Lenkung, Prüfung, Reaktion)
  - Softwarekonfiguration
  - Kalibrierung von Produktions- u. Prüfmitteln
  - Rückverfolgbarkeit
  - Risikoanalysen

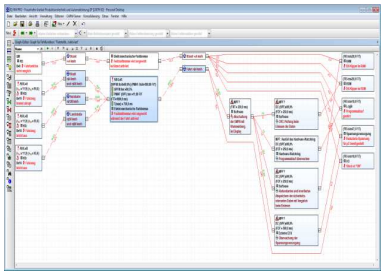
Quelle: ISO 26262

Fraunhofer IPA

ISO 26262
Anforderungen (komprimiert) der ISO 26262-9



- Analyse abhängiger Fehler
- Safety-Analysen
  - Qualitative Analysen (z.B. FMEA)
  - Quantitative Analysen (z.B. FTA)
  - Deduktive Analysen (Top-Down)
  - Induktive Analysen (Bottom-Up)



- Anmerkung:
  Die Analyse nach VDA mit der IQ-FMEA stellt (nach Ansicht des Autors) einen qualitativen und quantitativen Ansatz dar und erlaubt sowohl eine deduktive als auch induktive Herangehensweise. Der Graph-Editor stellt hierbei ein zentrales Element dar.

Quelle: ISO 26262

Fraunhofer IPA

ISO 26262

Zusammenfassung: Was brauche ich bei der Analyse von Funktional sicheren Systemen?

- **ISO 26262-3**
  - Betriebssystemzustände, G&R, Risikograph, Sicherheitsziele
- **ISO 26262-4**
  - System-FMEA, Fehlererkennung/-reaktion, Diagnostic-Coverage, Timing (Fehlertoleranz-, Fehlererkennungs-, Fehlerreaktionszeit), Verifizierung
- **ISO 26262-5**
  - FIT-Werte, Diagnostic-Coverage, Berechnungsalgorithmen, Metriken
- **ISO 26262-6**
  - „Software-FMEA“?
- **ISO 26262-7**
  - Prozess-FMEA und Prozess-Lenkungs-Plan (PLP)
- **ISO 26262-9**
  - Analyse abhängiger Fehler und Safety-Analysen (in ISO 26262 3-5)

Unterstützung bei Erstellung und Analyse durch den Graph-Editor

Fraunhofer IPA

ISO 26262

Welche Unterstützung brauche ich bei der Analyse von funktional sicheren Systemen?

Check auf Vollständigkeit der Safety-Analyse

- Habe ich für jedes Sicherheitsziel mindestens eine Fehlfunktion definiert?
- Habe ich zu allen Sicherheitszielen das Timing (Fehlertoleranzintervall und Notfallbetriebsintervall) definiert und analysiert?
- Habe ich alle meine verschiedenen Betriebszustände analysiert?
- Habe ich für jede Fehlfunktion der Sicherheitsfunktion die an der Sicherheitsfunktion beteiligten Bauteile analysiert?
- Habe ich zu allen an der Sicherheitsfunktion beteiligten Bauteilen die Fehlermodi und FIT-Werte (Failure in Time, Ausfälle in 10^9 h) definiert?
- Habe ich zu allen Fehlermodi, der an der Sicherheitsfunktion beteiligten Bauteile, die das Potenzial haben, die Sicherheitsfunktion zu verletzen, Sicherheitsmechanismen definiert?

Fraunhofer IPA

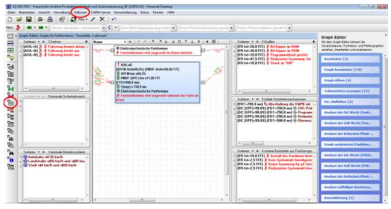
ISO 26262
Welche Unterstützung brauche ich bei der Analyse von funktional sicheren Systemen?

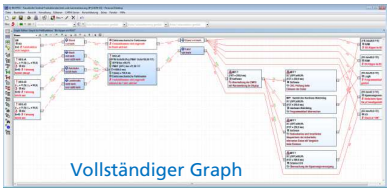
Check auf Vollständigkeit der Safety-Analyse

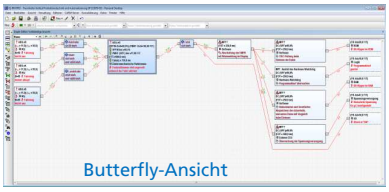
- Habe ich zu allen Sicherheitsmechanismen die
  - Diagnosedeckungsgrade (Diagnostic Coverage = DC)
  - Fehlererkennungszeiten (Fault Detection Time = FDT)
  - Fehlerreaktionszeiten (Fault Reaction Time = FRT)

  definiert?
- Habe ich zu allen Sicherheitszielen die FuSi-Kennwerte analysiert (Forderung in ISO 26262-5 bei ASIL C und D)?
  - Probabilistic Metric of random Hardware Faults (PMHF)
  - Single Point Fault Metric (SPFM)
  - Latent Fault Metric (LFM)

Graph-Editor
Aufruf des Graph-Editors

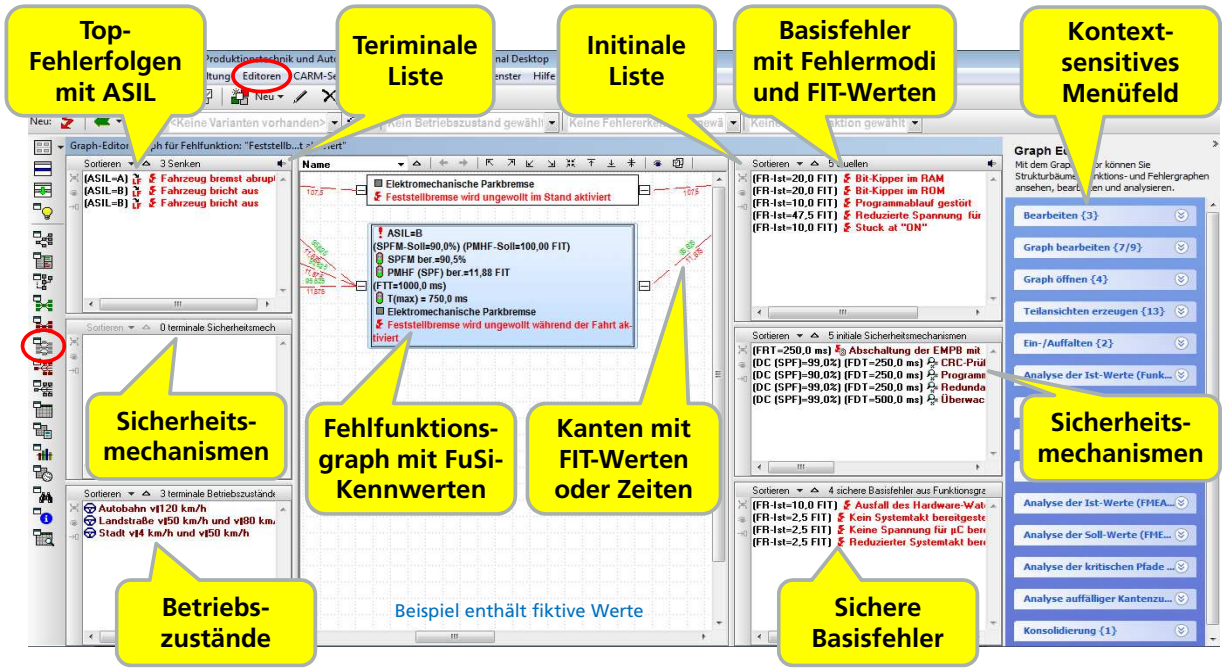






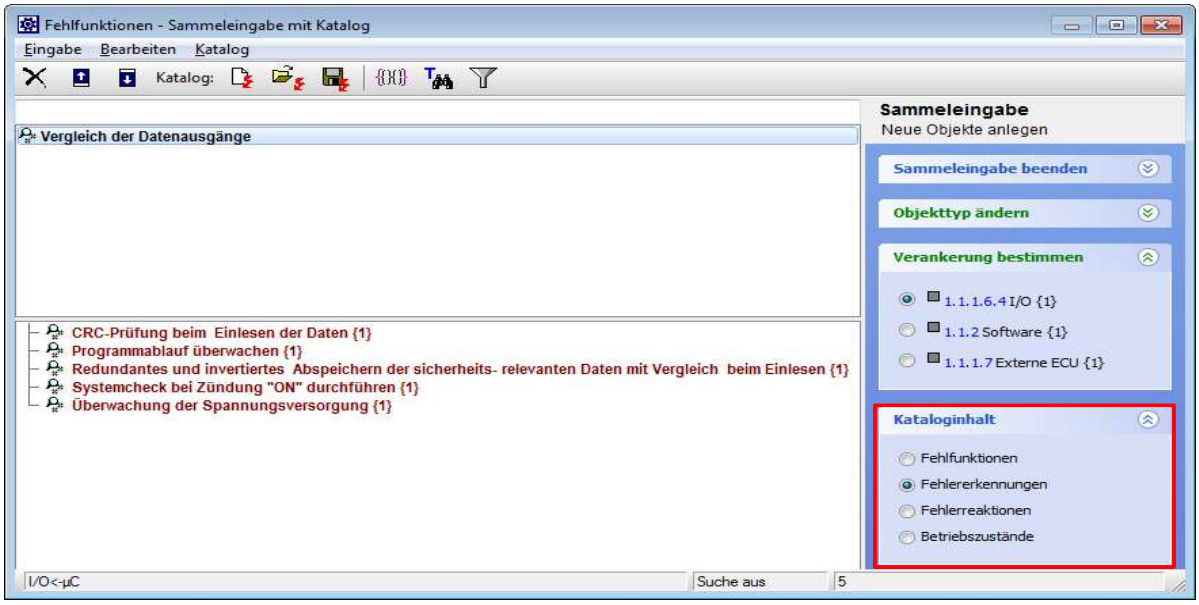
- Aufruf über
  - Menüleiste oder Menüpunkt Editoren
  - Rechte Maustaste im Listenfenster oder im Fehlernetz-Editor (Shortcut: CTRL-SHIFT-G)
- Aufruf als
  - Vollständiger Graph (Darstellung aller an der Sicherheitsfunktion beteiligten Bauteile mit ihren potenziellen Fehlfunktionen in Bezug auf das betrachtete System)
  - Butterfly-Ansicht (Darstellung aller an der Sicherheitsfunktion beteiligten Bauteile mit ihren potenziellen Fehlfunktionen in Bezug auf die Sicherheitsfunktion)

Graph-Editor
Aufruf, Inhalte und Funktionalitäten



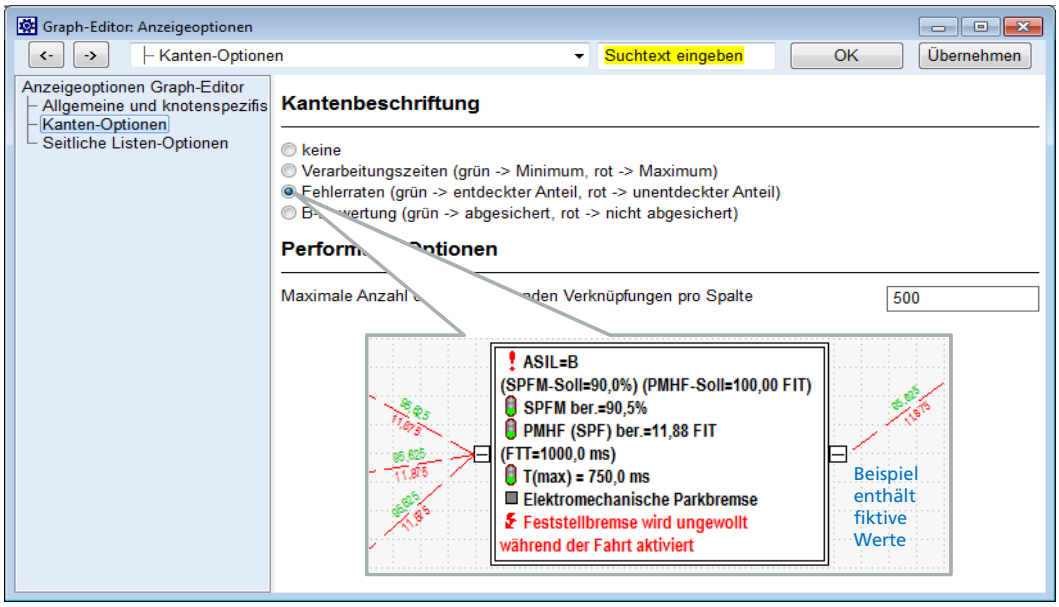
Fraunhofer IPA

Graph-Editor
Eingabemöglichkeit über „zentralen Katalog“ mit Fokussierung des Kataloginhalts und der Verankerung



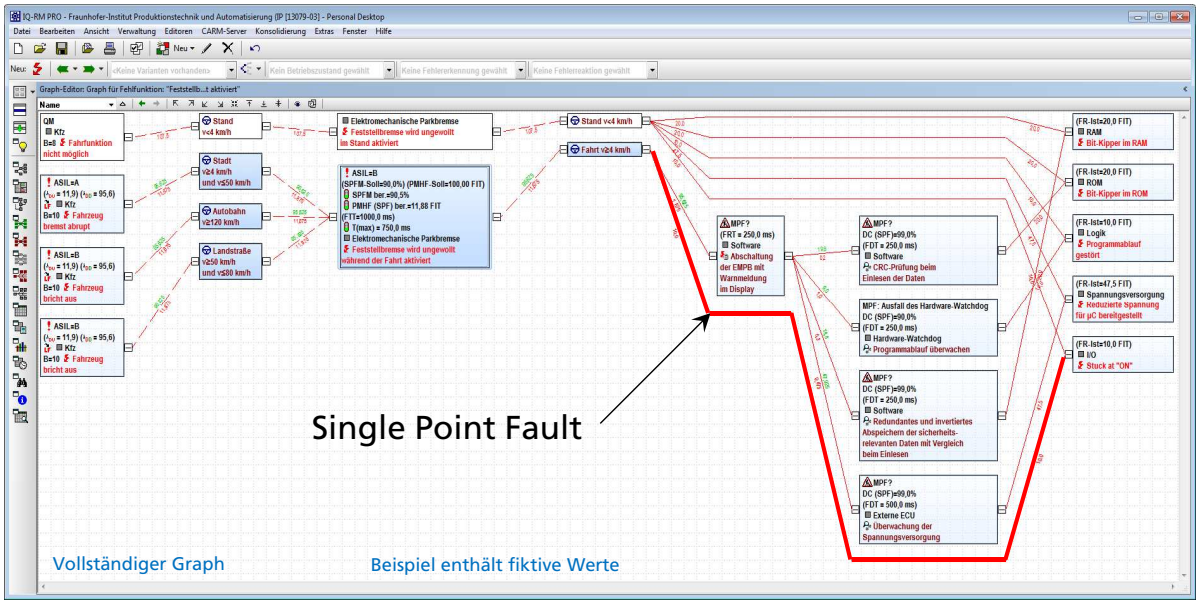
Fraunhofer IPA

Graph-Editor
Anzeigeoptionen Kanten



Fraunhofer IPA

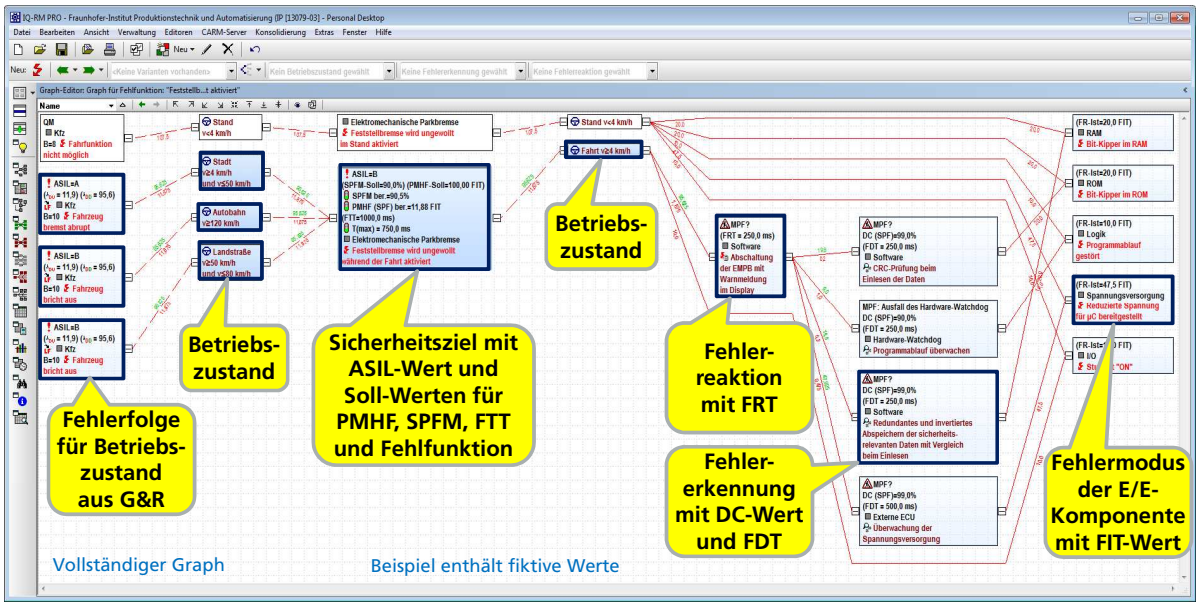
Graph-Editor
Vollständiger Graph mit Hinweis auf Single Point Fault



Fraunhofer IPA

Graph-Editor

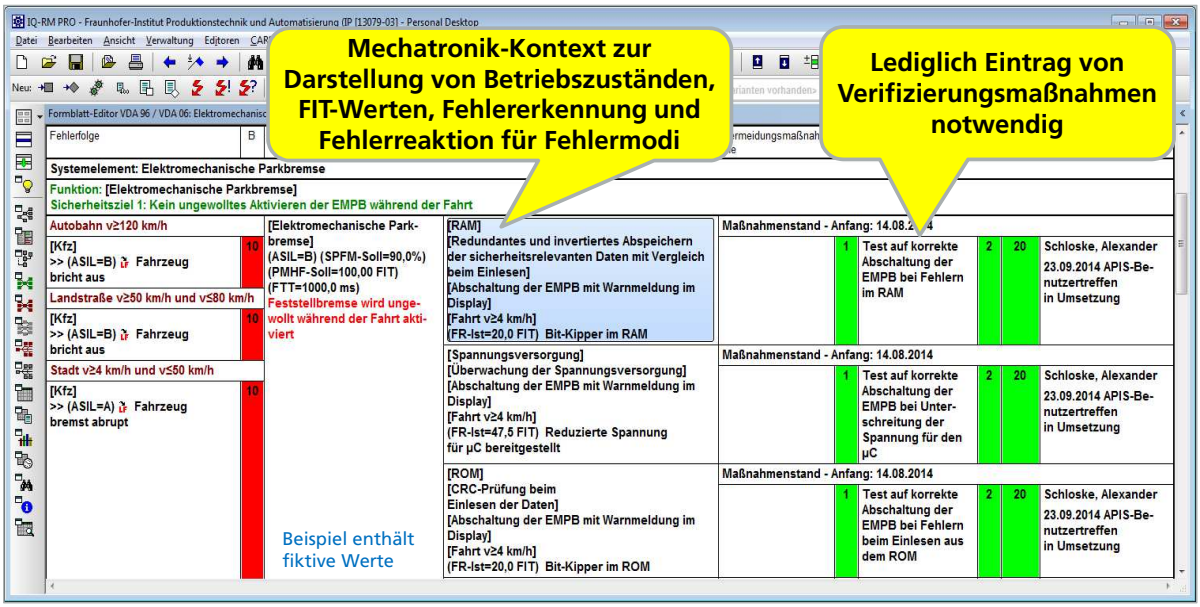
Wie muss ich FuSi-Systeme im Graph-Editor modellieren?



Fraunhofer IPA

Graph-Editor

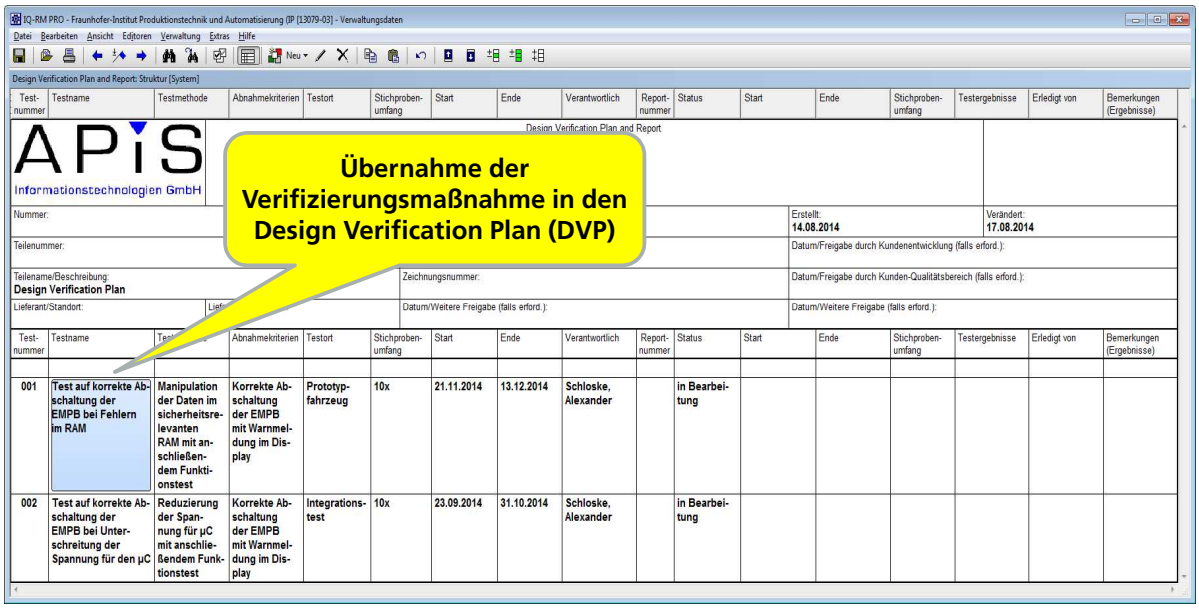
Darstellung des Mechatronik-Kontextes (Anzeigeoption) im FMEA-Formblatt



Fraunhofer IPA

Graph-Editor

Übertragung der Verifizierungsmaßnahmen in den Design Verification Plan (DVP)

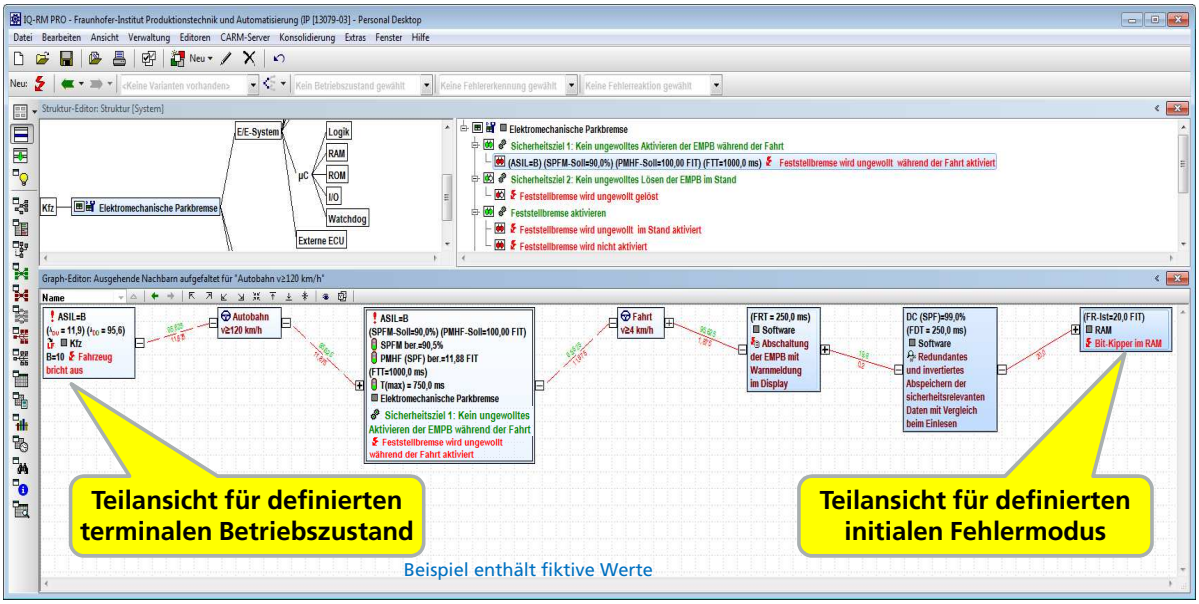


Test-nummer	Testname	Testmethode	Abnahmekriterien	Testort	Stichproben-umfang	Start	Ende	Verantwortlich	Report-nummer	Status	Start	Ende	Stichproben-umfang	Testergebnisse	Erledigt von	Bemerkungen (Ergebnisse)
001	Test auf korrekte Abschaltung der EMPB bei Fehlern im RAM	Manipulation der Daten im sicherheitsrelevanten RAM mit anschließendem Funktionstest	Korrekte Abschaltung der EMPB mit Warnmeldung im Display	Prototyp-fahrzeug	10x	21.11.2014	13.12.2014	Schloske, Alexander		in Bearbeitung						
002	Test auf korrekte Abschaltung der EMPB bei Unterschreitung der Spannung für den µC	Reduzierung der Spannung für µC mit anschließendem Funktionstest	Korrekte Abschaltung der EMPB mit Warnmeldung im Display	Integrations-test	10x	23.09.2014	31.10.2014	Schloske, Alexander		in Bearbeitung						

Fraunhofer IPA

Graph-Editor

Analyse ausgewählter Zusammenhänge über „Teilansichten erzeugen“

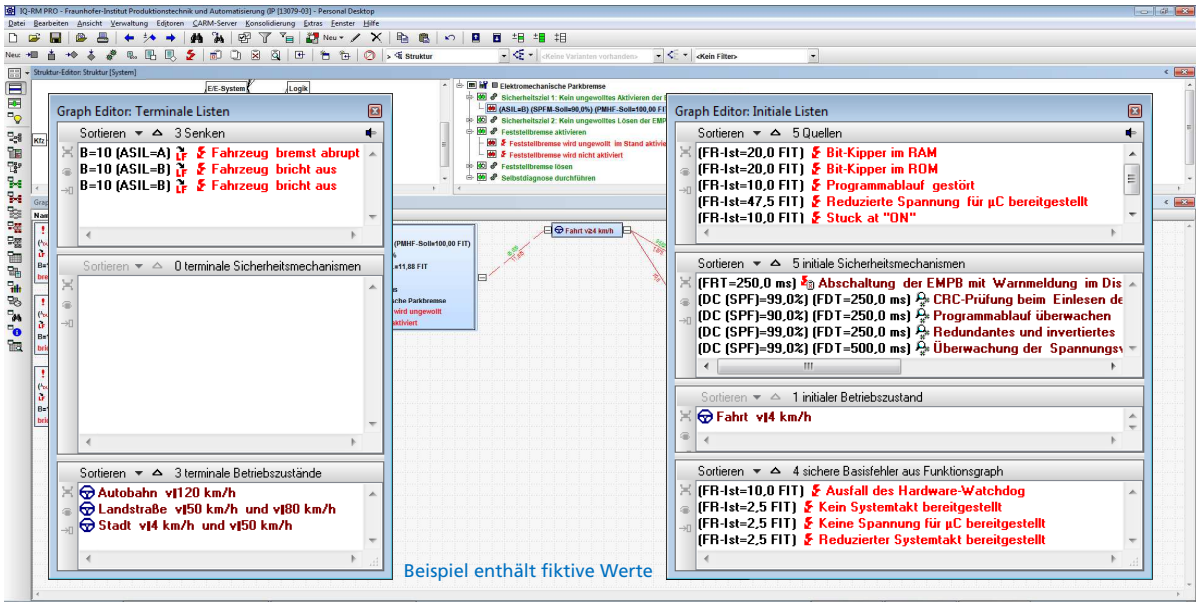


Beispiel enthält fiktive Werte

Fraunhofer IPA

Graph-Editor

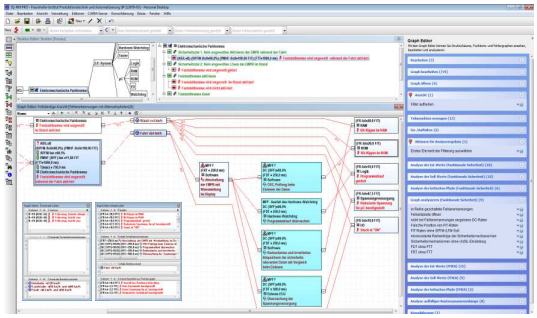
Analyse der Sicherheitsfunktion über „abpinnbare und konfigurierbare seitliche terminale und initiale Listen“

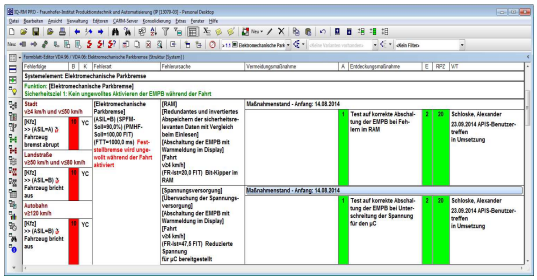


Fraunhofer IPA

Graph-Editor

Was sind sinnvolle Einstellmöglichkeiten?





- Graph-Editor
  - Fehlertoleranzzeit
  - FIT-Werte
  - Seitliche Listen (Darstellung auf separatem Bildschirm)
  - Seitliches Menüfeld
- Formblatt
  - Mechatronik-Kontext
  - Betriebszustände

Fraunhofer IPA

Graph-Editor
Was sind sinnvolle Ansichten und Analysen?

- Graph-Editor
  - Vollständiger Graph
  - Butterfly-Teilansicht
- Teilansichten erzeugen zu
  - Betriebszuständen
  - Sicherheitsmechanismen
- Analyse der Ist-Werte (vorhanden / fehlend)
- Analyse der Soll-Werte (vorhanden / fehlend)
- Analyse kritische Pfade (PMHF, SPFM, FTT)
- Analyse des Graphs (Funktionale Sicherheit)
- Analyse auffälliger Kantenzusammenhänge

Graph-Editor
Woran muss man sich beim Graph-Editor gewöhnen?

- Arbeiten, wie im Fehlernetz ist an manchen Stellen nicht mehr in der gewohnten Form möglich, wie z.B.:
  - Umhängen von Fehlfunktionen bzw. Löschen von Verknüpfungen
    - Markierung der Fehlfunktionen
    - Menüpunkt „Graph bearbeiten“
    - „Neue Verknüpfung“ bzw. „Verknüpfung löschen“
  - Arbeiten in der gewohnten Form (z.B. Umhängen von Fehlfunktionen) erzeugt statt dessen im Graph-Editor eine neue Verbindung
- Fehlererkennung, Fehlerreaktion und Betriebszustände können nicht mehr direkt aus dem Menü heraus aufgerufen werden
  - Statt dessen erfolgt die Eingabe einer Fehlfunktion in einem „zentralen Katalog“ mit anschließender Klassifizierung als Fehlfunktion, Fehlererkennung, Fehlerreaktion oder Betriebszustand