
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

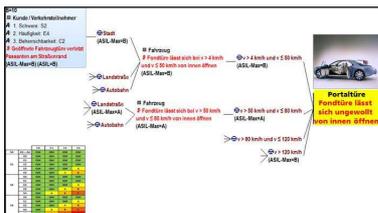
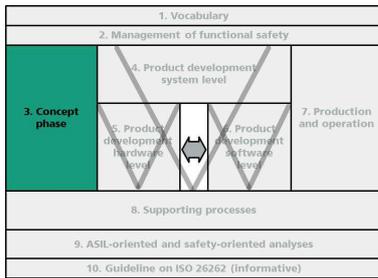
www.stuttgarter-produktionsakademie.de

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

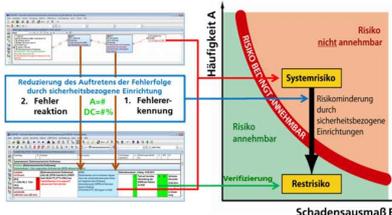
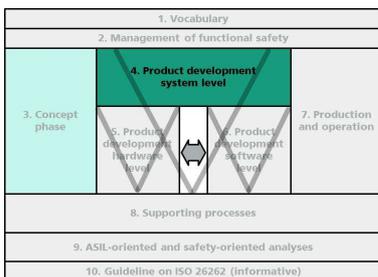


- Analyse der Betriebsbedingungen und Identifikation der Gefahren
 - Vollständige Auflistung der Betriebsbedingungen
 - Systematische Ableitung der Gefahren (Auswirkungen) anhand von Systemfehlfunktion für alle Betriebsbedingungen
- Bewertung der Gefahren
 - S0-S3: Schwere der potentiellen Gefahr
 - E0-E4: Dauer des Ausgesetztseins 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

ISO 26262

Anforderungen (komprimiert) der ISO 26262-4

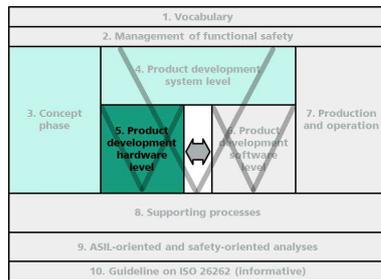


- Entwicklung des technischen Sicherheitskonzepts (TeSiKo)
 - Systemspezifikation und Systemarchitektur
 - Maßnahmen zur Vermeidung systematischer Fehler
 - Maßnahmen zur Beherrschung zufälliger HW-Fehler im Betrieb (inkl. Hardware Software Interface = HSI)
 - Definition der Sicherheitsmechanismen (Fehlererkennung 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

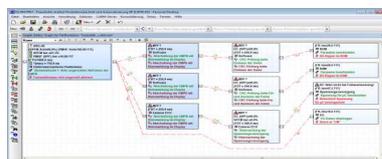
Quelle: ISO 26262

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

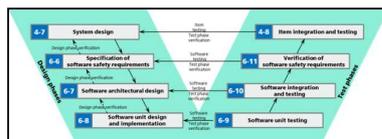
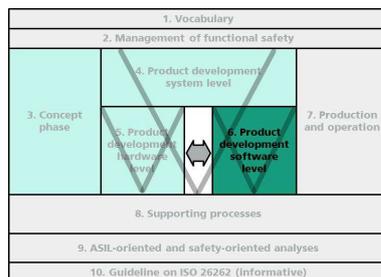


- Bewertung der Hardwarearchitektur in Bezug auf Behandlung zufälliger Hardwarefehler
- ASIL (B, C, D): Anwendung Hardwaremetriken
 - Single Point Faults Metric (bewertet die Robustheit gegenüber Single Point Faults und Residual Faults)
 - Latent Faults Metric (bewertet die Robustheit gegenüber Latent 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

ISO 26262

Anforderungen (komprimiert) der ISO 26262-6

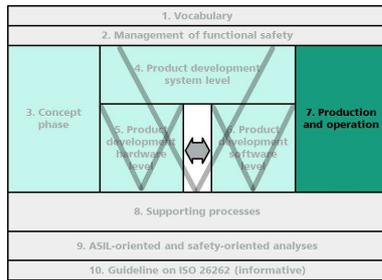


- Entwicklung der Software
 - Definition der Sicherheitsanforderungen
 - Definition der Hardware Software Interfaces
 - Entwicklung der Softwarearchitektur
 - Entwicklung des Softwaredesigns
 - Verifizierung des Softwaredesigns
- Verifizierung der Software
 - Modul-Tests
 - Integration-Tests
 - Item-Integration-Tests

Quelle: ISO 26262

ISO 26262

Anforderungen (komprimiert) der ISO 26262-7

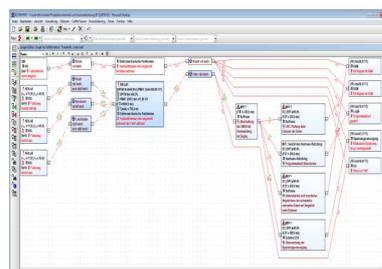
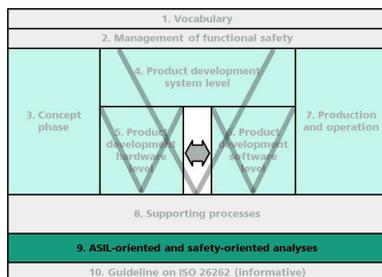


- Planung und Sicherstellung der Produktion
 - Produktionsplanung
 - Prozess-Ablauf-Plan
 - Arbeits-, Transport-, Lagerungsanweisungen
 - Fähigkeitsuntersuchungen
 - Prüfplanung
 - Control Plan (Lenkung, Prüfung, Reaktion)
 - Softwarekonfiguration
 - Kalibrierung von Produktions- u. Prüfmitteln
 - Rückverfolgbarkeit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

Quelle: ISO 26262

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

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
↓

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?

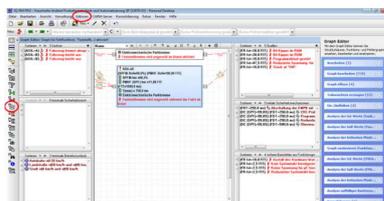
ISO 26262

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

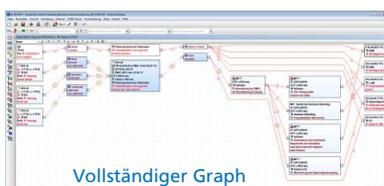
Check auf Vollständigkeit der Safety-Analyse

- 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

The screenshot shows the Graph-Editor interface with several callouts pointing to specific features:

- Top-Fehlerfolgen mit ASIL**: Points to the top-left panel showing error sequences.
- Terminale Liste**: Points to the 'Terminale Sicherheitmech' panel.
- Initiale Liste**: Points to the 'Initiale Sicherheitmech' panel.
- Basisfehler mit Fehlermodi und FIT-Werten**: Points to the '4 sichere Basisfehler aus Funktionsgr...' panel.
- Kontextsensitives Menüfeld**: Points to the right-hand menu with options like 'Bearbeiten (3)', 'Graph bearbeiten (7/9)', etc.
- Sicherheitsmechanismen**: Points to the 'Sicherheitsmechanismen' panel.
- Fehlfunktionsgraph mit FuSi-Kennwerten**: Points to the central graph area.
- Kanten mit FIT-Werten oder Zeiten**: Points to the edges of the graph.
- Sichere Basisfehler**: Points to the bottom-right panel.
- Betriebszustände**: Points to the '3 terminale Betriebszustände' panel.

Text in the center: *Beispiel enthält fiktive Werte*

Graph-Editor

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

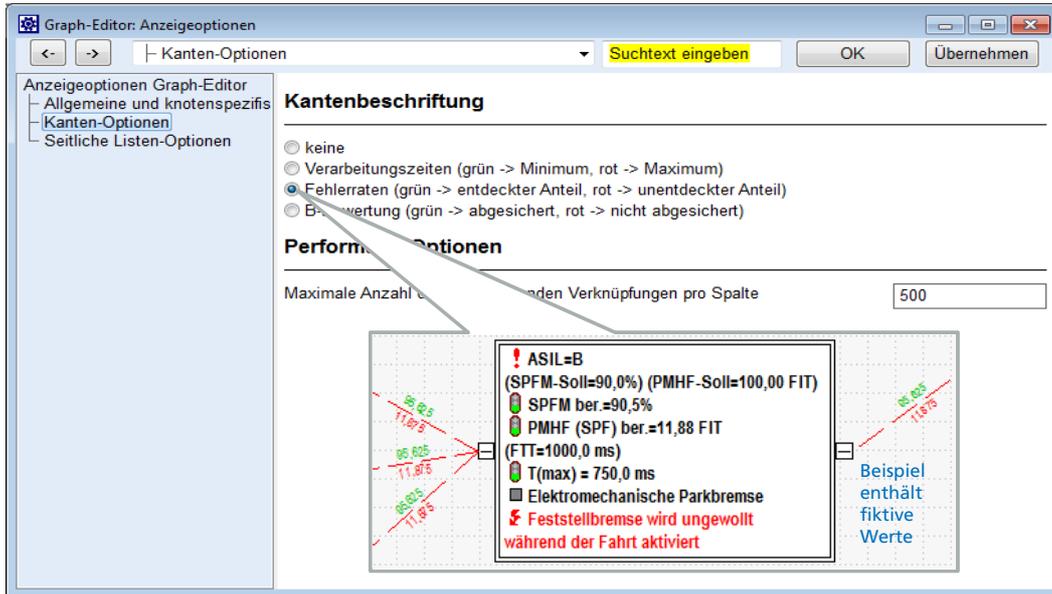
The screenshot shows the 'Fehlfunktionen - Sammeleingabe mit Katalog' dialog box. It has a menu with 'Eingabe', 'Bearbeiten', and 'Katalog'. The main area is divided into two panes:

- Vergleich der Datenausgänge**: A list of functions such as 'CRC-Prüfung beim Einlesen der Daten {1}', 'Programmablauf überwachen {1}', etc.
- Sammeleingabe**: A section for creating new objects, including options like 'Sammeleingabe beenden', 'Objekttyp ändern', and 'Verankerung bestimmen'. Below this is the 'Kataloginhalt' section, which is highlighted with a red box and contains radio buttons for 'Fehlfunktionen', 'Fehlererkennungen', 'Fehlerreaktionen', and 'Betriebszustände'.

At the bottom, there is a search bar labeled 'Suche aus' and a page number '5'.

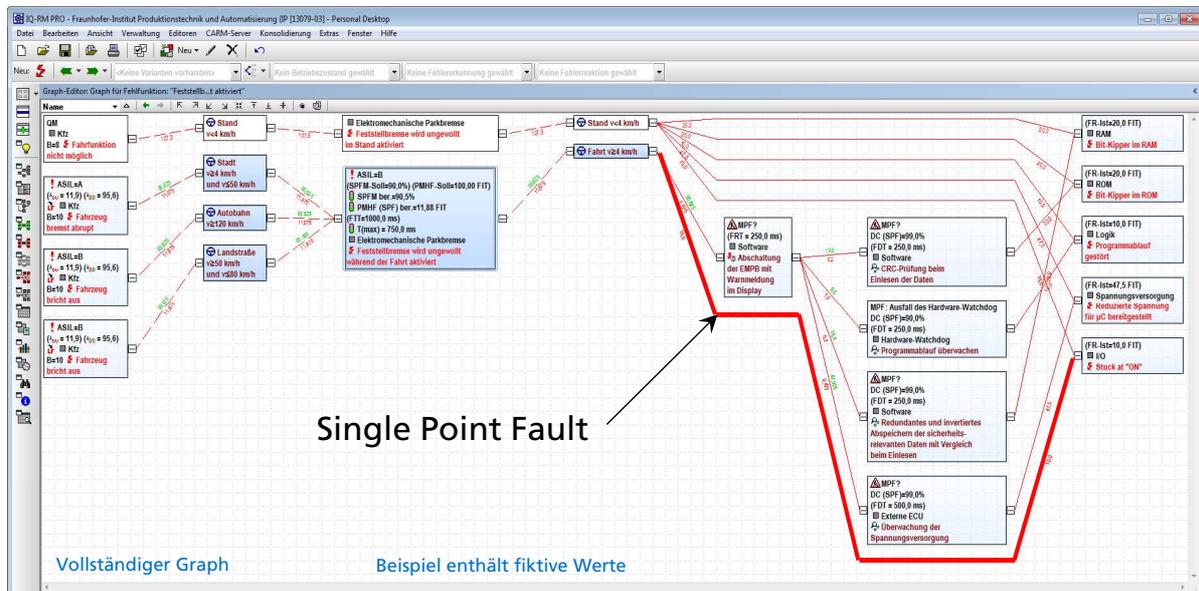
Graph-Editor

Anzeigeoptionen Kanten



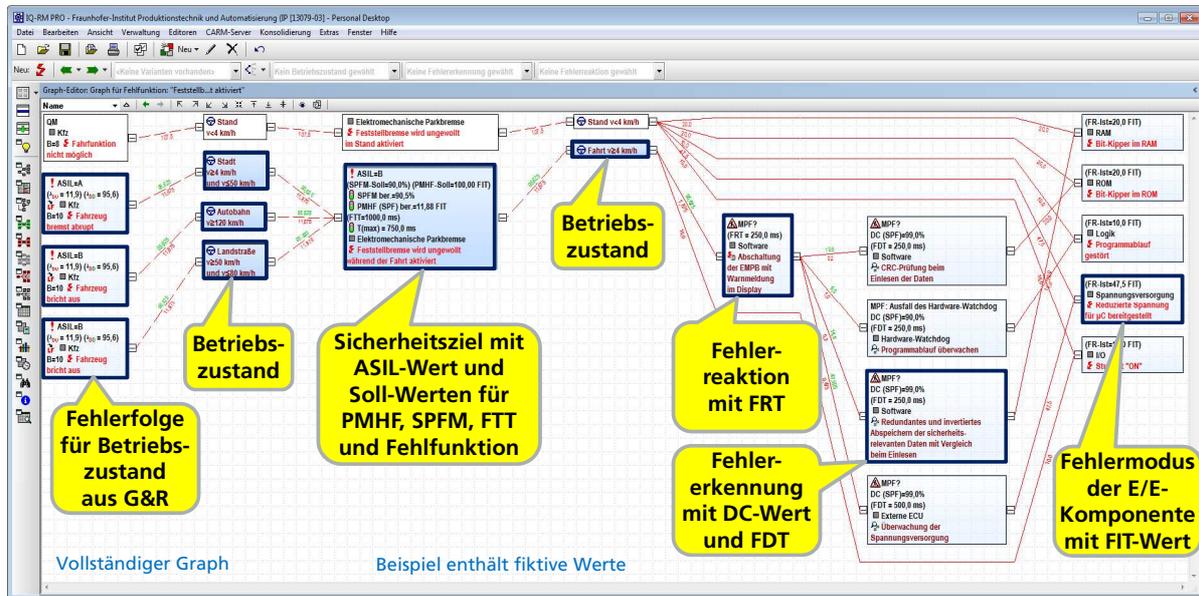
Graph-Editor

Vollständiger Graph mit Hinweis auf Single Point Fault



Graph-Editor

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



Graph-Editor

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

Mechatronik-Kontext zur Darstellung von Betriebszuständen, FIT-Werten, Fehlererkennung und Fehlerreaktion für Fehlermodi

Lediglich Eintrag von Verifizierungsmaßnahmen notwendig

Systemelement: Elektromechanische Parkbremse	Funktion: [Elektromechanische Parkbremse]	Sicherheitsziel 1: Kein ungewolltes Aktivieren der EMPB während der Fahrt	Maßnahmenstand - Anfang: 14.08.2014
Autobahn v<120 km/h [Kfz] >> (ASIL=B) Fahrzeug bricht aus Landstraße v<250 km/h und v<50 km/h [Kfz] >> (ASIL=B) Fahrzeug bricht aus Stadt v<24 km/h und v<50 km/h [Kfz] >> (ASIL=A) Fahrzeug bremsst abrupt	[Elektromechanische Parkbremse] (ASIL=B) (SPFM-Soll=90,0%) (PMHF-Soll=100,00 FIT) (FTT=1000,0 ms) Feststellbremse wird ungewollt während der Fahrt aktiviert	[RAM] [Redundantes und invertiertes Abspeichern der sicherheitsrelevanten Daten mit Vergleich beim Einlesen] [Abschaltung der EMPB mit Warnmeldung im Display] [Fahrt v<24 km/h] (FR-ist=20,0 FIT) Bit-Kipper im RAM	1 2 20 Schloske, Alexander 23.09.2014 APIS-Benutzertreffen in Umsetzung
		[Spannungsversorgung] [Überwachung der Spannungsversorgung] [Abschaltung der EMPB mit Warnmeldung im Display] [Fahrt v<24 km/h] (FR-ist=47,5 FIT) Reduzierte Spannung für µC bereitgestellt	1 2 20 Schloske, Alexander 23.09.2014 APIS-Benutzertreffen in Umsetzung
		[ROM] [CRC-Prüfung beim Einlesen der Daten] [Abschaltung der EMPB mit Warnmeldung im Display] [Fahrt v<24 km/h] (FR-ist=20,0 FIT) Bit-Kipper im ROM	1 2 20 Schloske, Alexander 23.09.2014 APIS-Benutzertreffen in Umsetzung

Beispiel enthält fiktive Werte

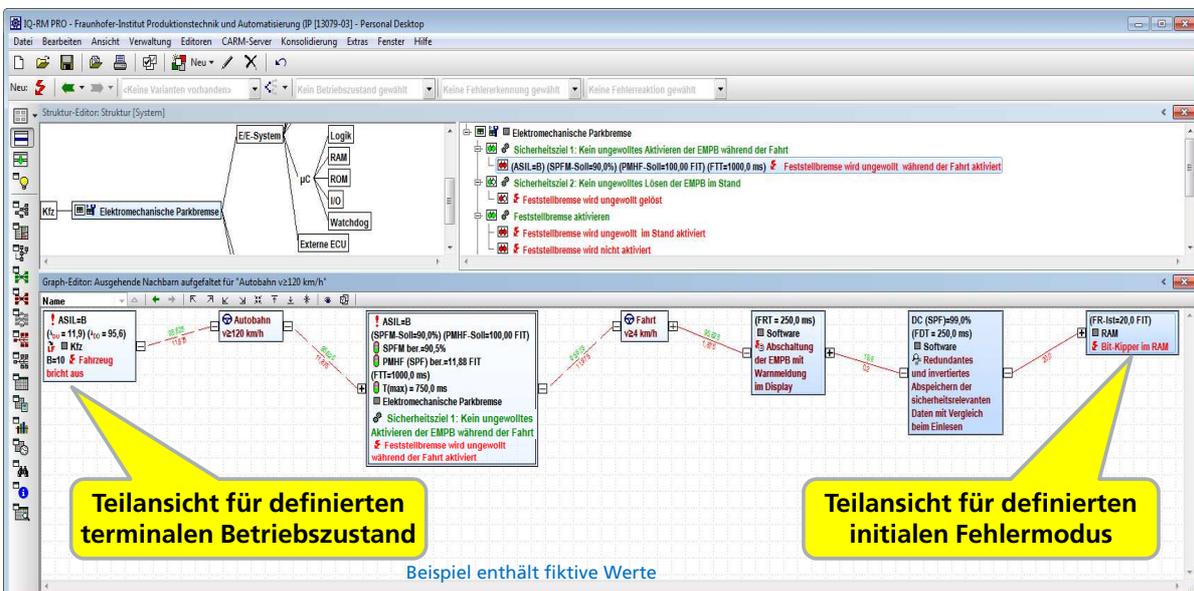
Graph-Editor

Übertragung der Verifizierungsmaßnahmen in den Design Verification Plan (DVP)

Test-nummer	Testname	Testmethode	Abnahmekriterien	Testort	Stichprobenumfang	Start	Ende	Verantwortlich	Report-nummer	Status	Start	Ende	Stichprobenumfang	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						

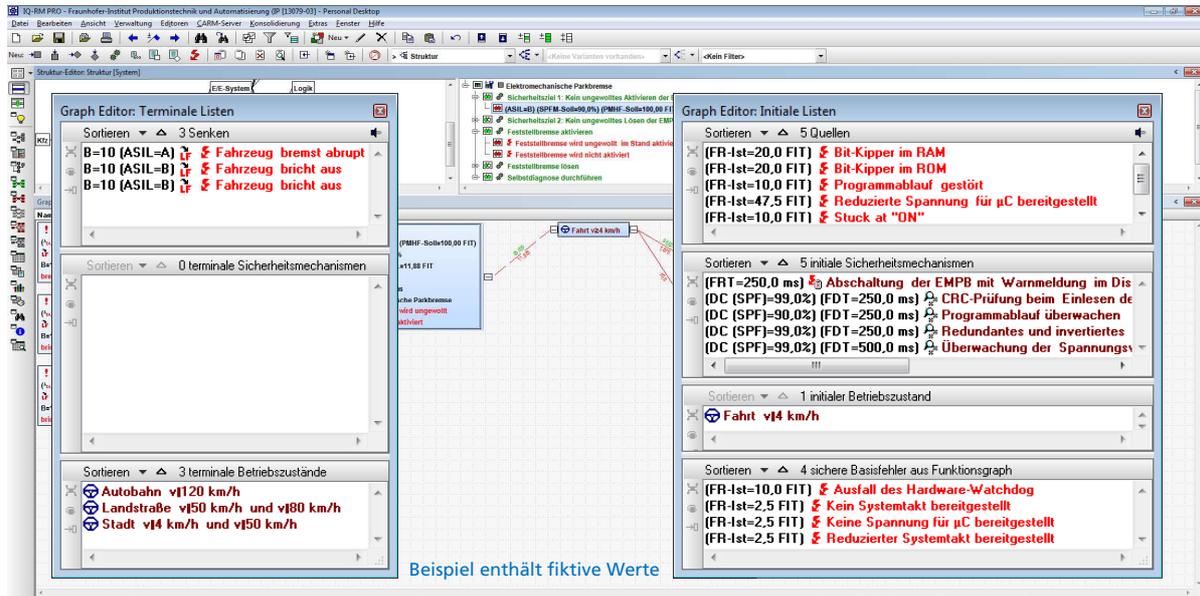
Graph-Editor

Analyse ausgewählter Zusammenhänge über „Teilansichten erzeugen“



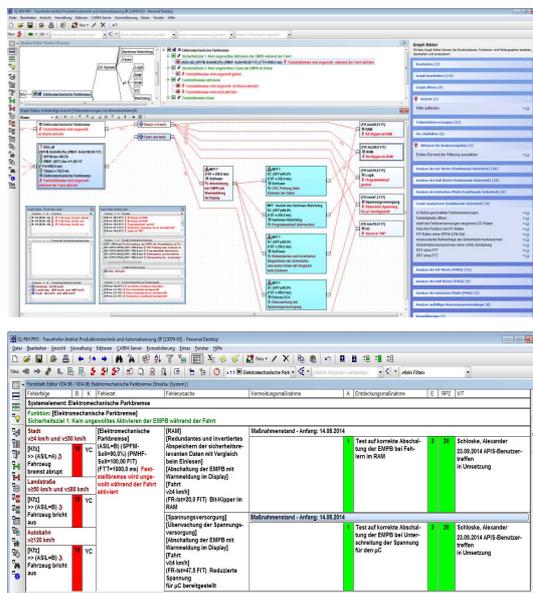
Graph-Editor

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



Graph-Editor

Was sind sinnvolle Einstellmöglichkeiten?



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

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