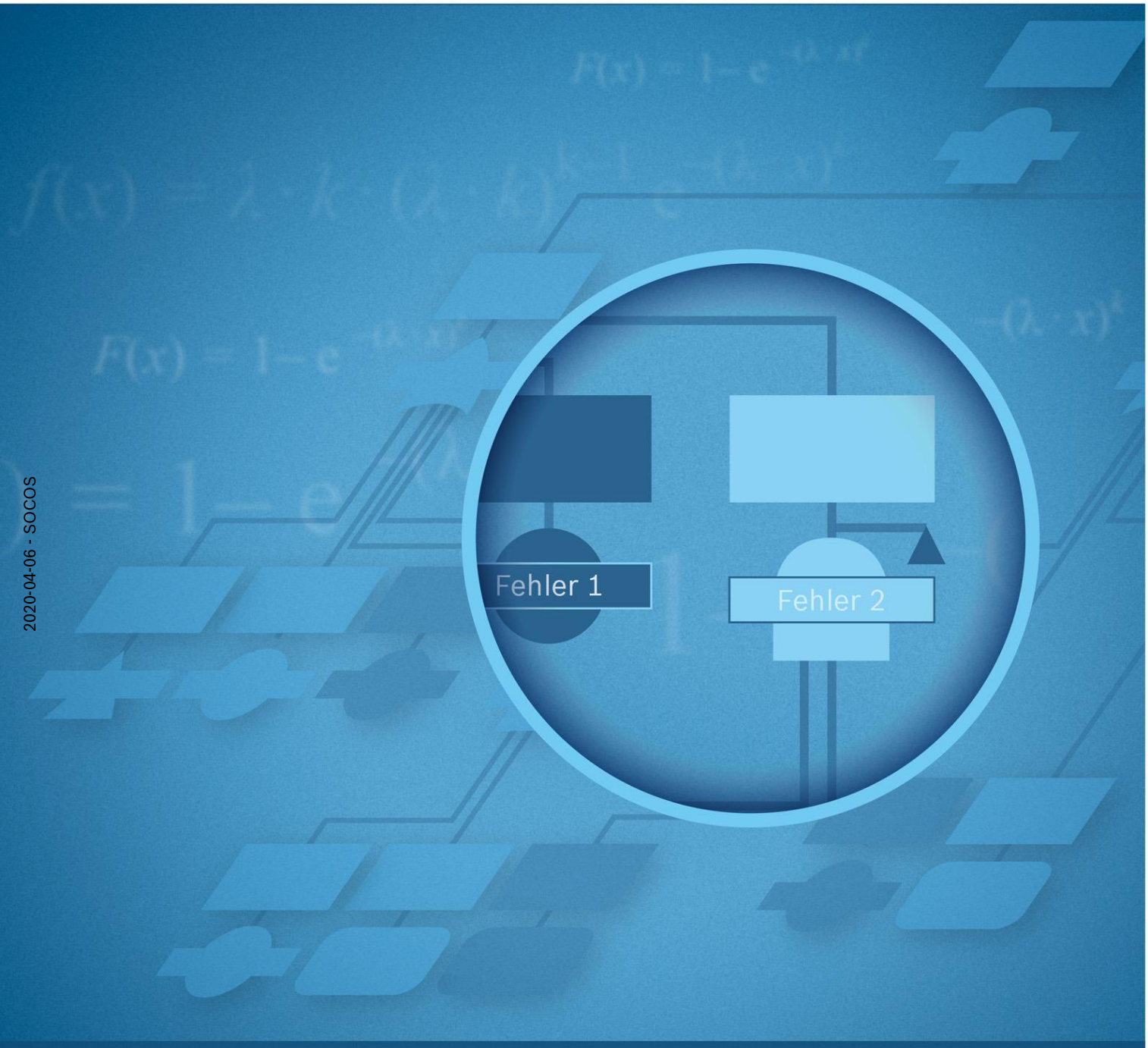


2020-04-06 - SOCOS

Qualitätsmanagement in der Bosch-Gruppe

15. Fehlzustandsbaumanalyse **FTA**

BOSCH
Technik fürs Leben

Inhalt

Abbildungsverzeichnis

1. Vorwort

In dieser Unterlage wird die Fehlzustandsbaumanalyse (englisch: Fault Tree Analysis = FTA, deutsch: gemäß VDA Fehlerbaumanalyse) als Methode der technischen Risikoanalyse beschrieben. Sie kann in allen Unternehmensbereichen angewendet werden. Als deduktive Methode ist sie eine Möglichkeit, den Forderungen der ISO26262 zur funktionalen Sicherheit in der Automobilindustrie nachzukommen und gilt hier als ein anerkannter Standard.

Die FTA kann präventiv oder korrektiv eingesetzt werden. Systematische Betrachtung potentieller Fehler und deren Dokumentation mit Mitteln der FTA helfen, Fehlermechanismen zu beschreiben und relevante Maßnahmen abzuleiten und deren Wirkung zu dokumentieren. Dies trägt zur Entwicklung robuster Produkte und Prozesse bei und sichert somit auch den Unternehmenserfolg.

Die Wirksamkeit der FTA hängt von ihrer rechtzeitigen Durchführung, der Beteiligung kompetenter Mitarbeiter und der Konzentration auf relevante Aspekte ab.

Die FTA Dokumentation und deren Inhalte stellen zusammen mit anderen Dokumenten - wie zum Beispiel FMEA, Zeichnungen, Fertigungs- und Prüfhinweisen - schützenswertes Know-how dar und dürfen nur unter definierten Randbedingungen weitergegeben werden.

Die FTA ist als Methode der qualitativen und quantitativen Risikoanalyse organisatorisch in bestehende Entwicklungs- bzw. Fertigungsplanungsabläufe eingebunden.

2. Einleitung

2.1. Ziele der FTA

Die FTA dient in erster Linie zur Erkennung und Beseitigung von Schwachstellen sowie zur Durchführung von Vergleichsstudien.

Mit Hilfe dieses Verfahrens soll die Wahrscheinlichkeit für das Auftreten eines vorher definierten Ereignisses (Top Event) sowie die entsprechenden Ursachen ermittelt werden. Die FTA geht dabei deduktiv vor – von der Wirkung zur Ursache (Top-Down Ansatz).

Die durch die FTA gewonnenen Daten ermöglichen unter anderem eine...

- Identifikation von Ursachen und Ursachenkombinationen, die zu einem unerwünschten Ereignis (Top Event) führen.
- Berechnung der Eintrittswahrscheinlichkeit des unerwünschten Ereignisses bzw. der Systemverfügbarkeit (Boolesche Algebra).
- Identifikation besonders Kritisches Ereignisse und Ereigniskombinationen (Fehlerpfade).
- Identifikation besonders effektiver Verbesserungsmöglichkeiten.
- Darstellung und Dokumentation der Ausfallmechanismen und deren funktionale Zusammenhänge.
- Ermittlung der Kennwerte zum Sicherheitsnachweis nach ISO26262.

2.2. Geschichte der FTA

Die ersten Sicherheits-/Risikoanalysen (USA 1950) beschränkten sich auf die Untersuchung der verschiedenen Ausfallarten (Failure Modes) von Bauelementen/ -gruppen eines Systems und der Auswirkungen (Failure Effects) der jeweiligen Ausfallart.

Es zeigte sich aber schon nach kurzer Zeit, dass eine ausschließliche Ausfallarten- und Ausfallfolgenanalyse aufgrund zunehmender Komplexität der Geräte und Systeme schwer durchführbar und für eine quantitative Zuverlässigkeitsanalyse ungeeignet war.

Ausgehend von den Erkenntnissen der Zuverlässigkeitstheorie und der Schaltalgebra gelang es den Ingenieuren der Bell Telephone Laboratories (H. Watson, 1961) das Fehlverhalten von Steuerungen in einem Booleschen Modell mit logischen Symbolen darzustellen. Die FTA war geboren!

Ihre erste Bewährungsprobe bestand die FTA bei Boeing in den 60er Jahren. Sie erfuhr in den folgenden Jahren durch ihren Einsatz in Luftfahrt-, Raumfahrt- und Kerntechnik Anpassungen. Später begann dann auch die Chemie-, Roboter- und Softwareindustrie, die FTA für ihre Sicherheitsanalysen zu nutzen.

In den letzten Jahren ist die FTA weiter verfeinert worden und ist eine weit verbreitete Analyse-Methode zur sicherheits- und zuverlässigkeitstechnischen Bewertung großer komplexer Systeme geworden.

Die Einführung der ISO26262 in der Kraftfahrzeugtechnik im November 2011 schreibt den Einsatz deduktiver Methoden wie z. B. der FTA vor.

2.3. Vor- und Nachteile der FTA

Der Erfolg der FTA bzw. der Wert der von ihr ermittelten Analyseergebnisse hängt in hohem Maße von äußeren Rahmenbedingungen ab.

Die Analyse mittels eines Fehlzustandsbaums…

- benötigt einen qualifizierten Moderator, der das Team methodisch führt.
- erfordert eine hohe Disziplin bei der Erstellung des Fehlzustandsbaums, um Fehler zu vermeiden.

- erfordert für jedes unerwünschte Ereignis einen eigenen Teilbaum / Ast.

2.3.1. Vorteile des Verfahrens

Die Analyse mittels eines Fehlzustandsbaums...

- ergibt systematisch den logischen Weg beginnend beim unerwünschten Ereignis, also von einer bestimmten Auswirkung, zurück bis zur eigentlichen Ursache und dokumentiert diesen Weg in graphischer, leicht verständlicher Form.
- berechnet Wahrscheinlichkeiten auf Grundlage der booleschen Algebra.
- erlaubt die Identifikation bislang unerkannter Wirkzusammenhänge.

Das Ergebnis der Analyse ermöglicht…

- quantitative und qualitative Aussagen über Systemkenngrößen wie z.B. Verfügbarkeit, Zuverlässigkeit, Ausfallwahrscheinlichkeit usw. zu machen. Dies ist insbesondere bei großen und komplexen Systemen wertvoll.
- ermöglicht die Betrachtung von Mehrfachereignissen als Ursachen.

Die Analyse kann…

- parallele, redundante oder alternative Fehler- oder Ereignispfade behandeln.
- technische und nichttechnische Systeme jeglicher Art behandeln.
- die Bedeutung von Fehlerursachen für das unerwünschte Ereignis aufzeigen.

2.3.2. Nachteile des Verfahrens

Die Analyse mittels eines Fehlzustandsbaums…

- stellt lediglich die Beziehung zwischen den festgestellten Ursachen zum analysierten Hauptereignis (Top Event) her. Diese Ursachen können aber noch zu anderen nicht dargestellten Auswirkungen führen.
- kann das Zeitverhalten von Systemen bzw. dynamische Prozesse nur schwer modellieren.
- ist nicht immer exakt quantifizierbar, da die Datenbasis für die Basisursachen nicht immer vollständig gegeben ist.
- ist eine aufwändige Methode, wenn ein komplexes System quantitativ analysiert werden soll. Daher wird sie in der Regel auf eine Auswahl von relevanten unerwünschten Ereignissen angewendet.

2.4. Einsatzgebiete der FTA

Die Einsatzgebiete der FTA lassen sich kurz unter dem Begriff „RAMS“ zusammenfassen.

Darunter versteht man:

- die Zuverlässigkeit (**R**eliability),
- die Verfügbarkeit (**A**vailability),
- die Wartbarkeit (**M**aintainability) und
- die Sicherheit (**S**afety).

Prinzipiell gibt es zwei Hauptschwerpunkte der Anwendung der FTA:

- den präventiven Ansatz
- den korrektiven Ansatz

Bei der präventiven Anwendung der FTA liegt der Fokus in der Gefährdungs- bzw. Risikoanalyse.

Ziele einer präventiv eingesetzten FTA:

- die Minimierung von Designfehlern (Fehlfunktion, Nicht-Funktion),
- die Absicherung und der Nachweis der Systemsicherheit,
- die Erhöhung der Systemzuverlässigkeit und
- die Bewertung von potentiellen Risiken im Rahmen des Risikomanagements.

Der korrektive Ansatz der FTA findet seine Anwendung in der Schadensanalyse bzw. Risikoanalyse.

In der Schadensanalyse dient die FTA als Entscheidungshilfe für rechtliche Fragestellungen (z.B. Produkthaftung) und zur Risikoermittlung für den Risikomanagementprozess.

Ergebnisse aus der Analyse werden für die Bewertung eines Schadens- bzw. eines Unfallablaufes herangezogen.

3. Grundlagen der FTA

3.1. Rollen

Aktive Rollen bei der FTA Erstellung

FTA-Koordinator

Der *FTA-Koordinator* ist Vertreter der Methode für einen Bereich (z.B. Geschäftsbereich, Produktbereich,…). Er gestaltet den Anwendungsprozess der Methode in seinem Bereich und ist für die Befähigung der *FTA-Experten* und der Mitglieder der *FTA-Teams* verantwortlich. Hierbei nimmt er folgende Aufgaben war: Wissensmultiplikator, Coach, fachlicher Ansprechpartner, methodischer Entscheider. Ein *FTA-Koordinator* sollte immer auch ein FTA-Experte sein.

FTA-Experte

Der *FTA-Experte* ist für die Moderation eines *FTA-Teams* verantwortlich. Er erstellt Fehlerbäume in Zusammenarbeit mit den Teammitgliedern. Hierbei ist er verantwortlich für die korrekte Anwendung der Methode und die Nutzung der relevanten Darstellungsmedien. Der FTA-Experte hat idealerweise auch Produktkenntnisse, um aktiv an der Diskussion teilnehmen zu können.

Der *FTA-Experte* hat neben den Aufgaben bei der Erstellung der FTA weiterführende Aufgaben: z.B. Coaching der Mitglieder des *FTA-Teams* bezüglich Methode und Tool, Erstellung von Auswertungen und Berichten, Unterstützung bei der Bewertung der Ergebnisse, Präsentation der Ergebnisse.

FTA-Team

Das *FTA-Team* besteht aus dem *FTA-Experten* und den relevanten Fachleuten. Wenn eine FTA im Rahmen eines Projektes erfolgt, ist die Mitarbeit eines technischen Projektmitarbeiters (z.B. Project Safety Managers) erforderlich. Das *FTA-Team* ist verantwortlich, die FTA Inhalte zu erarbeiten, das heißt, das Design abzubilden. Im Falle einer quantitativen FTA sind hierbei zusätzlich Ausfallraten bestimmt worden.

Passive Rollen bei der FTA Erstellung

FTA-Auftraggeber

Der *FTA-Auftraggeber* definiert die Ziele und den Betrachtungsumfang für die durchzuführende FTA. Er ist „Sponsor“ der FTA und stellt Budget und Ressource für die Erstellung sicher. Basierend auf den Analyse Ergebnissen entscheidet er über das weitere Vorgehen z.B. Einführung technischer Anpassungen, Verhandlung mit dem Kunden (Übernahme von Risiken).

FTA-Reviewer

Der *FTA-Reviewer* ist für die inhaltliche Überprüfung einer FTA vor Freigabe zuständig.

FTA-Assessor

Der *FTA-Assessor* ist für die Durchführung von Assessments verantwortlich, um die Reife der Implementierung der Methode festzustellen und die Organisationsweiterentwicklung zu unterstützen.

Weitere Rollen

- Kunde (OEM/ Linie/ ...)
- Qualitätsmanagement
- Zulieferer
- etc.

3.2. "Die 8 Schritte der FTA" – Ein Überblick

Eine Fehlerbaumanalyse lässt sich in folgende Arbeitsschritte gliedern:

0 Vorbereitung inklusive Systemanalyse

1 Definition des unerwünschten Ereignisses (Top Event)

2 Festlegen der Analyse-Zielgrößen

3 Erstellen des Fehlerbaums (qualitative Beschreibung)

4 Qualitative Auswertung

5 Ermittlung der Eintrittswahrscheinlichkeit der Basisereignisse (quantitative Beschreibung)

6 Quantitative Auswertung

7 Festlegung Handlungsbedarf, Maßnahmen, Erfolgskontrolle

8 Dokumentation

3.3. FTA Software bei BOSCH

Bei Bosch ist die Vorzugslösung für die Bearbeitung und Dokumentation von FTA das Programm FT+ der Firma Isograph.

Aktuell: FT+, Floating licence mit zentraler Verwaltung.

4. Das Bosch Vorgehen zur Erstellung einer FTA

Hinweise und Beispiele zur Umsetzung der Methode FTA

4.1. Schritt 0: Vorbereitung inklusive Systemanalyse

4.1.1. Allgemein

Zur Vorbereitung einer FTA sind sowohl inhaltliche als auch formale bzw. organisatorische Festlegungen zu treffen.

Zu den inhaltlichen Festlegungen gehören:

- Beschreibung der Aufgabe (wenn möglich: Formulierung der Top Events)
- Betrachtungsumfang (System mit seinen Grenzen, Schnittstellen und Randbedingungen)

  Zu den Randbedingungen gehören z.B.
  - Eintrittswahrscheinlichkeiten (z.B. aus anderen FTAs/FMEDAs) von Eingangssignalen (wichtig bei Funktionen, die über mehrere Systeme verteilt sind)
  - Betrachtung von Störgrößen aus der Umgebung
  - Abstimmung über die Zuordnung von Sicherheitsmechanismen an den Schnittstellen (keine Mehrfachverwendung, die zu einer Verfälschung führen könnte)
  - Informationen über das übergeordnete System (z.B. Fahrzeug Steuergerät), die für die Erstellung der FTA nötig sind
- Festlegung der zu betrachtenden Fehlerarten: systematische Fehler und/oder zufällige (Hardware-) Fehler
- Art und Umfang der Analyse:
  - Qualitativ: Analyse der Ursache-Auswirkungs-Zusammenhänge
  - Quantitativ: Berechnung der Eintrittswahrscheinlichkeit von Ereignissen und weiterer quantitativer Kenngrößen. Für eine quantitative Analyse ist die Festlegung der Datenbasis und der Einsatz-/Betriebsbedingungen notwendig.
- Wenn für die Erstellung der FTA Informationen des Auftraggebers nötig sind, muss die Bereitstellung dieser Informationen sichergestellt werden. Die Konsequenzen aus Nichtvorliegen dieser Informationen sollen aufgezeigt werden.
- Vorgaben zur FTA-Methode:
  Als Normgrundlage für FTAs bei Bosch dient die DIN EN 61025. Sofern der Auftraggeber (z.B. OEM) eine FTA nach einer anderen Norm oder nach einem Methodenleitfaden fordert, muss dies projektspezifisch vereinbart werden. Es ist schriftlich festzuhalten, dass der Auftraggeber die Verantwortung für Konsequenzen aus dieser Forderung übernimmt.

Die o.g. Festlegungen und andere Annahmen/Randbedingungen sind zu dokumentieren und vom Auftraggeber schriftlich zu bestätigen.

Zu den formalen Festlegungen gehören z.B.:

- Auftraggeber, FTA-Team, Bezahlung, Abnahmekriterien, Zeitrahmen
- Arbeitsprodukte: Bericht , Fehlerbaum-Datei, spezielle Analysen
- Dokumentation, Freigabe/Übergabe an Auftraggeber, Archivierung
- Bei FTA für Kundenprojekte:
  - Klärung von Art und Zeitpunkt der Präsentation
  - Klärung, welche Dokumente an externe Kunden übergeben werden können/sollen (Beachte: „Regelungen der Kundenkommunikation zu Ergebnissen von Qualitätsmanagement-Methoden“ (Zentralanweisung Vertrieb & Marketing „R05“))

4.1.2. Präventive / Korrektive FTA

Präventive FTA

Voraussetzung für den Beginn einer FTA ist die zumindest vorläufige Beschreibung des Betrachtungsgegenstands („System“), das zunächst bezüglich seiner fehlerfreien Funktion dokumentiert vorliegen muss („Systemanalyse“). Diese Beschreibung kann abhängig vom Analyseziel und Betrachtungsumfang mehr detailliert oder eher abstrakt vorliegen.

Typische Datenquellen sind: Lasten- und Pflichtenhefte, Funktionsdiagramme, Wirkketten, Systemarchitekturmodelle, Verhaltens-/Datenmodelle, Blockdiagramme, Konstruktionszeichnungen, Flussdiagramme, Prozessbeschreibungen, …

Idealerweise liegen zum Start einer FTA auch schon Beschreibungen von anderen Risikoanalysen bzw. Fehlerbeschreibungen vor, z.B.: PHA, FHA, FMEA, FMEDA, DRBFM, QFD, 8D-Reports.

Für Analysen der funktionalen Sicherheit sollten zu Beginn der FTA weitere Datenquellen verfügbar sein: Gefährdungs- und Risikoanalyse, Sicherheitsziele, Sicherheitskonzept incl. Übersicht der Sicherheitsmechanismen, Systemdesign, Definition der sicheren Zustände.

Korrektive FTA

Die korrektive FTA analysiert tatsächlich eingetretene Ereignisse. Zu Beginn müssen alle relevanten Informationen zu dem Ereignis zusammengetragen werden, z.B.:

- Fehlerbeschreibung
- 8D-Report
- Auswertungen von Fehlerspeichern
- Designbeschreibungen des Objekts, z.B. TKU
- Protokolle der Aussagen des Anwenders/Entdeckers des Ereignisses
- fehlerbehaftete Objekte

4.2. Schritt 1: Definition des unerwünschten Ereignisses (Top Event)

Das unerwünschte Ereignis (oft auch „Top Event“ genannt) ist der zu betrachtende Ausfall bzw. die zu betrachtende Fehlfunktion des zu untersuchenden Systems. Hierbei ist es unbedeutend, auf welcher Abstraktionsebene das Ereignis definiert wird. Es kann eine Fehlfunktion auf der Fahrzeugebene, eine fehlerhafte Steuergerätefunktion, ein falsches Sensorsignal oder der Ausfall einer Schaltungsgruppe betrachtet werden.

Bei der Beschreibung des unerwünschten Ereignisses ist darauf zu achten, dass sowohl das Ereignis selbst als auch die dafür gültigen Randbedingungen eindeutig definiert sind. Die Aussagekraft der gesamten FTA steht und fällt mit dieser Beschreibung.

Im *präventiven* Anwendungsfall der FTA basiert die Definition des unerwünschten Ereignisses entweder auf

- der Nicht-Erfüllung von Funktionen oder Anforderungen (z.B. Lastenheft, Pflichtenheft).

oder

Fehlerbildern aus zeitlich vorgeschalteten Untersuchungen (z.B. FMEA, FHA, PHA, G&R

G&R	Gefahren- & Risikoanalyse (im engl. unter H&R nach ISO 26262 bekannt)

- bzw. H&R).

Im *korrektiven* Ansatz wird ein real aufgetretener Ausfall bzw. eine Fehlfunktion des Systems als unerwünschtes Ereignis definiert.

4.3. Schritt 2: Festlegen der Analyse-Zielgrößen

4.3.1. Allgemein

Nachdem die Definition des unerwünschten Ereignisses (Top Event) erfolgt ist, wird in diesem Schritt festlegt, welche Ziele mittels Durchführung der FTA verfolgt werden sollen. Dabei liefert die FTA Informationen darüber, ob die definierten Ziele bereits erreicht sind. Ist dies nicht der Fall, kann dann aufgezeigt werden welche Möglichkeiten es gibt, durch Änderungen am Produkt die definierten Vorgaben zu erfüllen.

Bei der Zieldefinition unterscheidet man in der Regel zwischen qualitativen und quantitativen Zielen.

Beispiele für *qualitative* Ziele sind:
- Keine Einzelfehler, d.h. kein Einzelereignis darf zum Top Event führen
- Aufzeigen aller Minimalschnitte
- Aufzeigen aller „Kritischer Pfade“ (mit Diagnose)

Beispiele für *quantitative* Zielgrößen sind:
- Auftretenswahrscheinlichkeit Q für das Top Event
- Auftretenswahrscheinlichkeiten und Rangfolge der Minimalschnitte
- Aufzeigen des „kritischsten Pfades“ (Einzelereignis oder Auftretenswahrscheinlichkeit)
- Einhaltung des Sicherheitsziels (z.B. Ausfallwahrscheinlichkeit < 10^{-8})
- Aufzeigen der Importanzen (z.B. Birnbaum-Importanz)

Gültige Normen, Richtlinien von Industrieverbänden (z.B. VDA), Kundenanforderungen und betriebsinterne Anforderungen sind maßgebend für die Zielsetzung der FTA.

Beispiele für Ziele, die ihren Ursprung in entsprechenden Dokumenten haben, sind:
- Ausfallrate für „Zufällige HW-Fehler“ laut ISO 26262 („Funktionale Sicherheit von Straßenfahrzeugen“)
- Erfüllung des „Stands der Technik“ und „höchste Priorität zur Vermeidung von Fehlern“ laut CDQ0214 („Anforderungen an die Produktsicherheit“)
- Sicherheit gegen Einzelfehler laut „E-Gas-Überwachungskonzept“ oder „3-Ebenen-Konzept“ des Arbeitskreises E-Gas

4.3.2. Präventiv / Korrektiv

In beiden Anwendungsformen der FTA werden prinzipiell ähnliche Ziele angestrebt. Es ist der strukturelle Aufbau eines Designs aufzuzeigen und mögliche kritische Ursachen, die zu dem unerwünschten Ereignis führen können bzw. geführt haben, aufzudecken.

Ziel ist es in beiden Anwendungen, konkrete Möglichkeiten zur Verbesserung des Designs aufzuzeigen und gegebenenfalls deren Einfluss auf die Auftretenswahrscheinlichkeit darzustellen.

Bei der *korrektiven* FTA steht im Unterschied zur *präventiven* FTA dabei schon ein tatsächliches Fehlerbild (unerwünschtes Ereignis) zur Verfügung.

4.4. Schritt 3: Erstellen des Fehlzustandsbaums (qualitative Beschreibung)

4.4.1. Allgemein

Die Struktur einer FTA und deren Aufbau sind stark abhängig von dem zu analysierenden unerwünschten Ereignis (Top Event) und der Architektur des zu analysierenden Objekts.

Allgemein gültig ist der deduktive Ansatz (top-down): Der Start erfolgt beim unerwünschten Ereignis. Es folgt der Aufbau des Baums über mehrere Ebenen bis hinunter zu der kleinsten Betrachtungseinheit (Basisereignis).

Die Struktur des Baums richtet sich nach der Ausfallstruktur bzw. dem Fehlernetz des zu betrachtenden Objekts. Eine während der Vorbereitungsphase bereits durchgeführte Funktionsanalyse ist für die Erstellung des Fehlerbaums sehr hilfreich. Eingangsinformationen für die Erstellung eines Fehlerbaums können z.B. die FMEA und die DRBFM sein.

4.4.2. Symbole und Modellierungsempfehlungen

Die Symbolarten zur FTA-Erstellung sind im „Anhang 1 Symbole und Modellierungsempfehlungen“ definiert:

- Event- und Gattersymbole
- Empfehlungen für Namenskonventionen
- Fehlermodelle
- Varianten-Handling
- Modellierung von Applikationsrandbedingungen
- Modellierung von Überwachungen
- Modellierung von „Common Causes“

4.4.3. Gliederungsprinzipien

Die Gliederung erfolgt z.B. nach

1. Wirkketten (z.B. Aktuator – Ansteuereinheit – Sensor)
2. Gliederung nach physikalischen Domänen (z.B. Teilbäume für mechanisches Subsystem, elektronisches Subsystem, hydraulisches Subsystem,…), die dann unter einem Top Ereignis mit einem Gatter verknüpft sind
3. Gliederung nach Integrationsebenen (z.B. Gesamtsystem – Funktionsschicht – Komponentenschicht)

Bei sehr großen bzw. komplexen Analyse-Objekten empfiehlt sich eine Modularisierung der FTA. Der Vorteil liegt darin, dass die Gesamtzahl der Gates und Events in der System-FTA möglichst klein gehalten und die Rechenzeit verkürzt werden kann.

Dabei sind die Top Events der untergeordneten FTAs (z.B. die FTA eines Sensors) die Basisereignisse (Basic Events) der übergeordneten FTA (z.B. FTA eines Systems, das diesen Sensor enthält). Diese Events werden im folgenden Schnittstellenelemente genannt. Die Elemente bilden zusammen eine Art FTA-Ersatzmodell.

Wenn das Schnittstellenelement in einer UND-Beziehung zu anderen Komponenten steht, sind mögliche gemeinsame Fehlerursachen (Common Cause Fehler) besonders zu betrachten. So kann z.B. bei der Definition der Schnittstellenelemente der Nachweis eventueller Common Causes zu anderen Komponenten von den Komponentenverantwortlichen eingefordert werden.

Beispiel 1 : Sensorersatzmodell

Nachfolgend wird die Bestimmung der Schnittstellenelemente am Beispiel eines Sensors gezeigt, der in einer UND-Beziehung zu einem anderen Sensor (Plausibilitäts-Sensor) stehen soll.

Grundlegende Idee dieser Modellierung ist es, auf der Ebene der System-FTA für Analysezwecke die Unterscheidung nach Einzelfehlern (überwacht und schlafend), Mehrfachfehlern und Common Cause

Einflüssen zu ermöglichen. Damit wird eine Modellierung der **exakten** Beiträge aller Sensoren zur Verletzung des Sicherheitsziels auf Systemebene möglich, inklusive des Beitrags von Common Causes aus der Systemebene auf die Sensoren.

Die methodische Einschränkung besteht darin, dass alle möglichen Common Causes vorab in einer qualitativen Analyse der Common Cause failures ermittelt werden müssen.

Im Beispiel wird angenommen, dass es zwei Arten von Common Cause Fehlern gibt: Erstens die Versorgungsspannung (SUPP) aus dem übergeordneten System und zweitens elektromagnetische Interferenzen von externen Störquellen, die innerhalb oder außerhalb des spezifizierten Bereichs liegen (EXT EMI IN bzw. EXT EMI OUT).

Das Fehlermodell des Sensors wird dabei wie folgt gegliedert:

- Unüberwachte Einfach-Fehler (Single Point Faults („SENS SPF“) die keinerlei Überwachung haben)
- Einfach-Fehler mit einer Überwachung außerhalb der Fehlertoleranzzeit („SENS_SPF DORM“)
- Mehrfachfehler („SENS CIRC THR“), wobei darunter beide Arten von Doppelfehlern fallen (Fehler der Funktion & Ausfall der zugehörigen Überwachung sowie Fehler von Funktion 1 & Fehler von Funktion 2), sowie Fehler höherer Ordnung.

(Symbole zu den Basisereignissen und logischen Gattern des Fehlerbaums werden in Anhang 1 erklärt.)

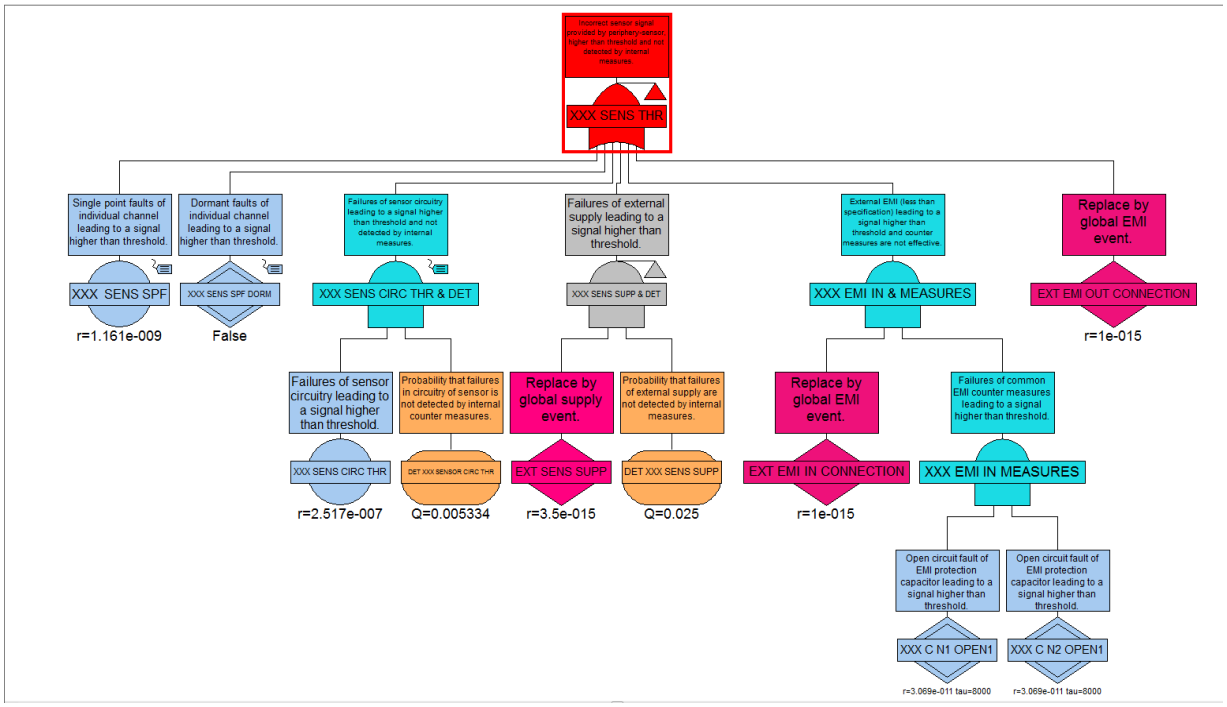


Abbildung 4.1: Sensorersatzmodell für den Sensor XXX

Ermittlung der Schnittstellenelemente (im Folgenden werden die Eingänge des ODER-Gatters als Elemente bezeichnet):

Element 1 = Basisereignis XXX SENS SPF

Ermittlung der single point faults (XXX SENSOR SPF)

In der zugrunde liegenden Sensor-FTA wird für das zu untersuchende Top Event eine Cut- Set Analyse durchgeführt. Die Ausfallrate für die single point faults ergibt sich aus der Summe aller Cut-Sets der Ordnung 1 (echte Einzelfehler). Typischerweise werden die Berechnungen nach Export der Cut-Sets in ein Excel-File vorgenommen.

Element 2 = Basisereignis XXX SENS SPF DORM

Die Ausfallrate ergibt sich hier aus der Summe aller Fehler mit einer Überwachung außerhalb der Fehlertoleranzzeit. In diesem Beispiel gab es keine solchen, daher erscheint im Fehlerbaum ein Basisereignis ohne Zahlenwert.

Element 3 = Gatter XXX SENSOR CIRC THR & DET

Das Gate SENSOR CIRC THR & DET steht für alle Mehrfachfehler und Fehler mit Überwachung innerhalb der Fehlertoleranzzeit. Zur Ermittlung der Ausfallraten wird wieder eine Cut- Set Analyse in Excel durchgeführt. Voraussetzung ist die Einhaltung einer Namenskonvention, die das effektive Filtern in Excel zulässt.

Zunächst werden die Einfachfehler und die Common Cause relevanten Cut-Sets mit EMI und mit Power Supply herausgefiltert. Die Ausfallrate für „XXX SENSOR CIRC THR & DET“ ergibt sich aus der Summe der übrigen Cut-Sets. Die Fehlerrate für „XXX SENSOR CIRC THRES“ ergibt sich aus der Summe der Fehlerraten der zugehörigen Basisereignisse (Funktionsfehler ohne Überwachungen). Der Schlupf der Überwachung „DET SENSOR CIRC THRES“ kann dann berechnet werden als Quotient der Fehlerraten XXX SENSOR CIRC THR & DET / XXX SENSOR CIRC TRHES. Nähere Erklärungen zur quantitativen Auswertung von Fehlerbäumen finden sich im Kapitel 4.5 zu Schritt 4.

Element 4 = Gatter XXX SENSOR SUPP & DET

Das Event EXT SENSOR SUPP wird hier mit einem Event der System-FTA identifiziert. Es ist ein Beispiel für die Modellierung einer für den Sensor externen (daher die Namenskonvention „EXT“), aber für das System internen Power Supply Schaltung. Diese Power Supply Schaltung kann für andere angeschlossene Sensoren und ICs einen C*ommon Cause* darstellen.

Der Schlupf der Überwachung DET XXX SENS SUPP wird ähnlich wie bei Element 3 ermittelt.

Element 5 = Gatter XXX EMI IN & MEASURES

Die Modellierung einer für die Sensoren einen Common Cause darstellenden EMI Störung wird in ähnlicher Weise dargestellt durch die Ver-UND-ung eines Basisereignisses EXT EMI IN CONNECTION mit der Ausfallrate der EMI Schutzbeschaltung (Ver-UND-ung der Ausfalls zweier Schutz-Kapazitäten).

Element 6 = Gatter XXX EMI OUT CONNECTION

Für diese externe Störung wurde angenommen, dass sie jenseits der Spezifikationsgrenze ist (Namenskonvention EMI OUT) und daher die implementierten Schutzmaßnahmen nicht (mehr) greifen. Die Modellierung ist ein Vorhalt für eine Sensitivitätsanalyse bzgl. der Fehlerrate des externen Ereignisses.

Dieses Beispiel stammt von CC-PS/EPH. Detailliertere Informationen zur Modellierungsweise können zur Verfügung gestellt werden.

Beispiel 2 : Übergang von FTA zu FMEDA

Werden Komponenten eines Systems mittels FMEDA (Failure Mode Effect and Diagnosis Analysis) analysiert, ist ein wohldefinierter Übergang zwischen den beiden Methoden erforderlich. Die FTA definiert die Sicherheitsanforderung, deren Erfüllung mittels der Ergebnisse der FMEDA bestätigt werden soll. Zum Einbinden der FMEDA in eine FTA sind auf Seiten der FMEDA folgende Fehlerarten zu ermitteln.

Einzelfehler:

Ein Einzelfehler ist ein Fehler, der durch keinen Sicherheitsmechanismus abgedeckt ist und unmittelbar zur Verletzung des Sicherheitsziels führt.

FMEDA-Ergebnis: Summe der Fehlerraten aller Einzelfehler: λ_{SPF} = Lambda Single Point Faults

Restfehler:

Der Restfehler ist der Anteil eines Fehlers, der nicht durch eine Überwachung erfasst wird und der zur Verletzung des Sicherheitsziels führt.

FMEDA-Ergebnis: Summe der Fehlerraten aller Restfehler der überwachten Fehler: λ_{RF} = Lambda Residual Faults (RF)

Latente Fehler:

Ein latenter Fehler ist eine der Ursachen eines Mehrfachfehlers, der für sich alleine aber nicht zu einer Verletzung des Sicherheitsziels führt und innerhalb seiner Latenzzeit nicht entdeckt wird.

FMEDA-Ergebnis: Summe der Fehlerraten aller latenten (Mehrfach-)Fehler: $\lambda_{MPF,L}$ = Lambda Multiple Point Faults Latent

Dies ist die Summe der Fehlerraten aller Fehler, die erst im Mehrfachfehlerfall das Sicherheitsziel verletzen und für die keine Maßnahme gegen Latenz implementiert ist (bzw. der Schlupf solcher Maßnahmen gegen Latenz).

Gesamtfehlerrate:

Zur korrekten Berücksichtigung der Mehrfachfehlerwahrscheinlichkeit, ist die Summe der Gesamtfehlerrate aller für das Sicherheitsziel relevanten Elemente erforderlich:

FMEDA-Ergebnis: $\lambda_{SR,HW}$ = Lambda Safety Related Hardware Elements bzw. λ_{SRHE} = Lambda Related Hardware Elements

Dies ist die Summe aller Fehlerraten von Komponenten, die auf eine der obengenannten Weisen auf das Sicherheitsziel Einfluss nehmen können. Dabei werden die Fehlerraten vor Berücksichtigung von Redundanzen (=> führt zu Multipoint Faults) bzw. Überwachungen (=> führt zu Residual Faults) aufsummiert.

Die nachfolgende Grafik beschreibt die Zusammenhänge zwischen den Fehlerklassen.

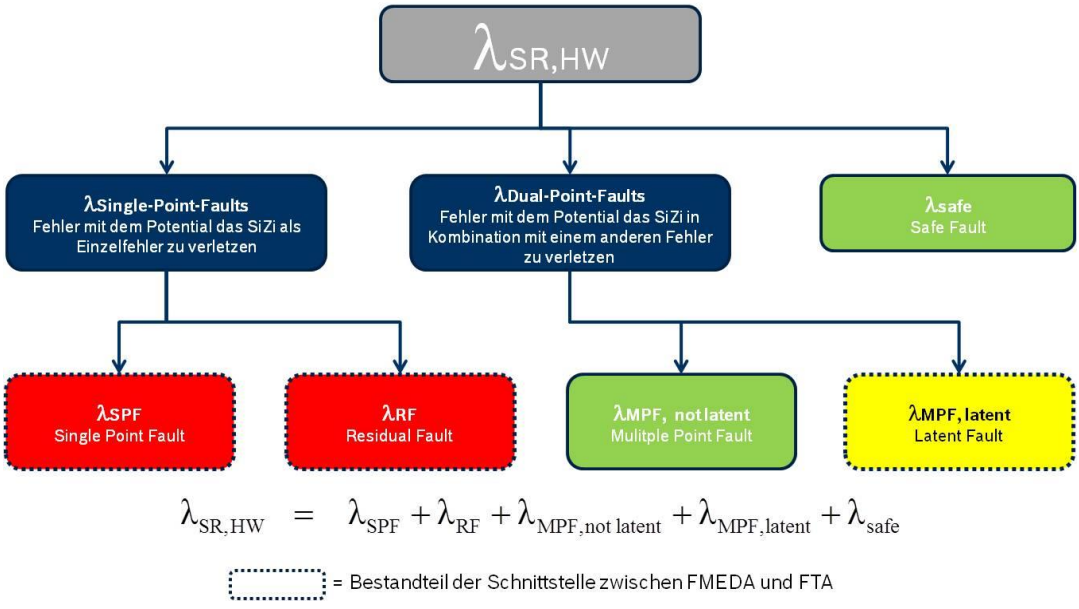


Abbildung 4.2: Fehlertypen

Die zu betrachtende Sicherheitsanforderung wird als Gatter in der FTA geführt. Die entsprechende Fehlerrate ($\lambda_{SR,HW}$) errechnet sich aus den von der FMEDA ermittelten Fehlerraten entsprechend ihrer Bedeutung für das System.

Ermittelte Einzel- und Restfehlerraten gehen direkt in den Fehlerbaum ein. Ein Einzelfehler der FMEDA muss nicht zwangsläufig auch in der FTA ein Einzelfehler bleiben, sondern kann auch durch die in der FTA abgebildete Systemarchitektur Teil eines Mehrfachfehlers werden.

Ein in der FMEDA ermittelter Mehrfachfehler muss auch in der FTA ein Mehrfachfehler bleiben, da sonst in der FTA nicht mehr ersichtlich ist, dass es sich schon auf Komponentenebene um einen Mehrfachfehler handelt. Diesen Umstand muss die FTA/FMEDA-Schnittstelle berücksichtigen. Da die FMEDA durch methodische Grenzen den zu jedem als Mehrfachfehler deklarierten Fehler gehörigen Zweitfehler im Einzelnen nicht ausweisen kann, muss eine konservative Modellierung in Bezug auf die resultierende Mehrfachfehlerwahrscheinlichkeit realisiert werden. Dies ist umgesetzt durch ein UND-Gatter in der Schnittstelle, das die Fehlerrate der unentdeckten Mehrfachfehler mit der Fehlerrate *aller* sicherheitsrelevanten Elemente kombiniert. Es ist davon auszugehen, dass die Wahrscheinlichkeit der „wirklichen“ Zweitfehler der Mehrfachfehler niedriger ist, als die Summe der Fehlerrate aller sicherheitsrelevanten Elemente; also ist die Produktwahrscheinlichkeit konservativ berechnet. Es ist darauf zu achten, dass der unentdeckte Mehrfachfehler als „Dormant“-Fehler mit der entsprechenden Latenzzeit modelliert wird.

Abbildung 3 und 4 zeigen eine Umsetzung der FTA/FMEDA Schnittstelle als Fehlerbaumlogik.

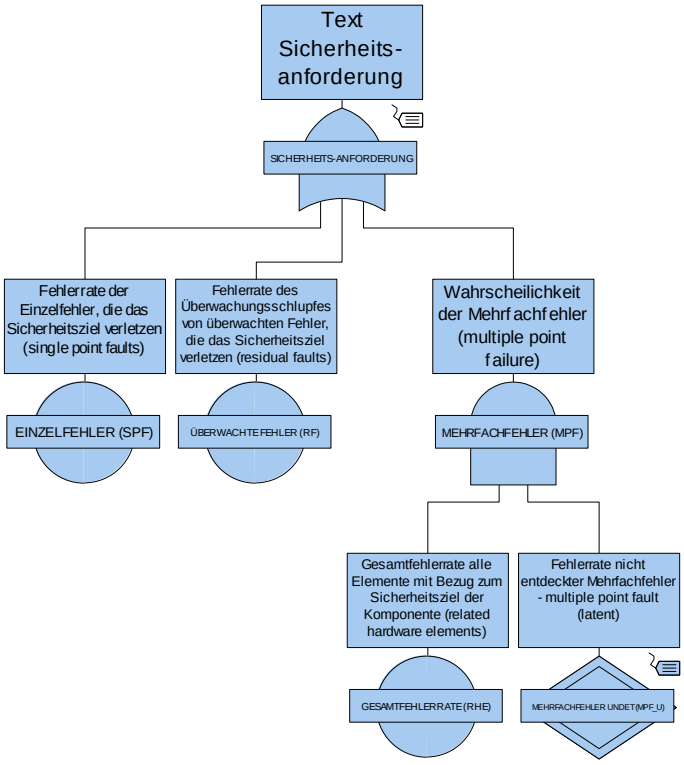


Abbildung 4.3: FTA/FMEDA Schnittstellen generieren

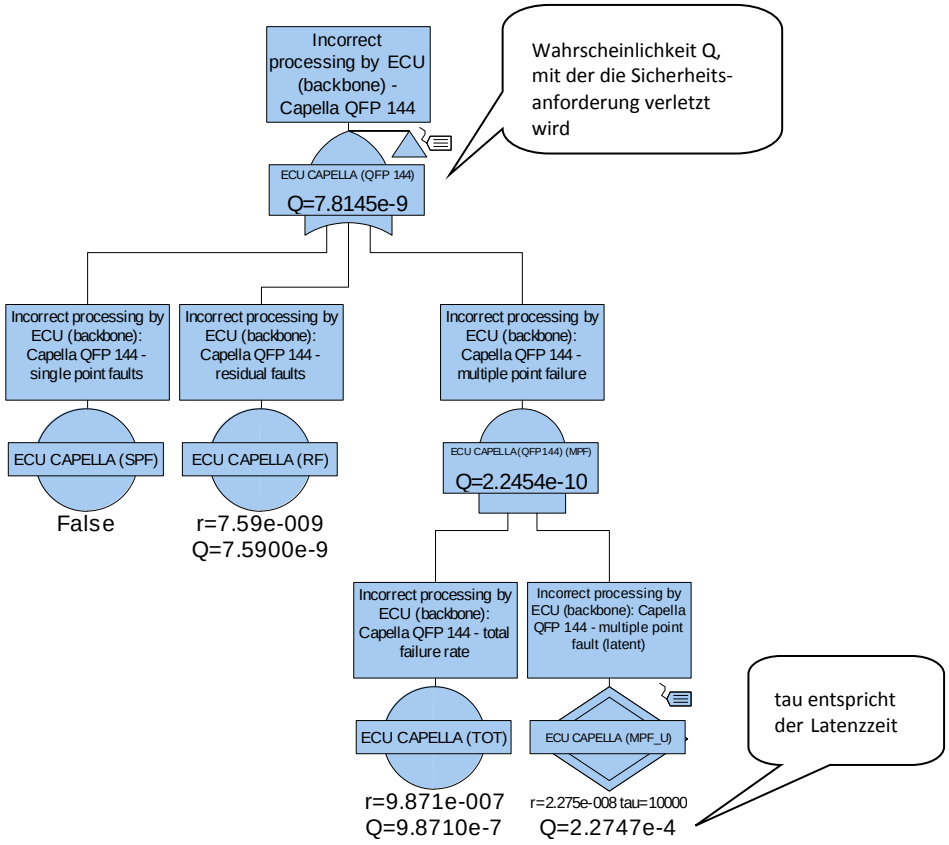


Abbildung 4.4: FTA/FMEDA Schnittstellen - Beispiel

4.5. Schritt 4: Qualitative Auswertung

4.5.1. Allgemein

Die qualitativen Ergebnisse einer FTA umfassen die

- Fehlerbaumdarstellung
- Fehlerkombinationen (Minimalschnitte bzw. Cut-Sets)
- Importanz (Birnbaum) für die in der FTA durch Logik verknüpften Ereignisse (Events)

Die Auswertungen bezüglich Fehlerkombinationen und Importanzen erfolgen stets in Bezug auf ein ausgewähltes unerwünschtes Ereignis (Top Event). Dieses Ereignis ist repräsentiert durch ein logisches Gatter, unterhalb dessen der eigentliche Fehlerbaum beginnt.

Die in den nachfolgenden Kapiteln gezeigten Auswertebeispiele sind mit folgendem Fehlerbaum erzeugt worden.

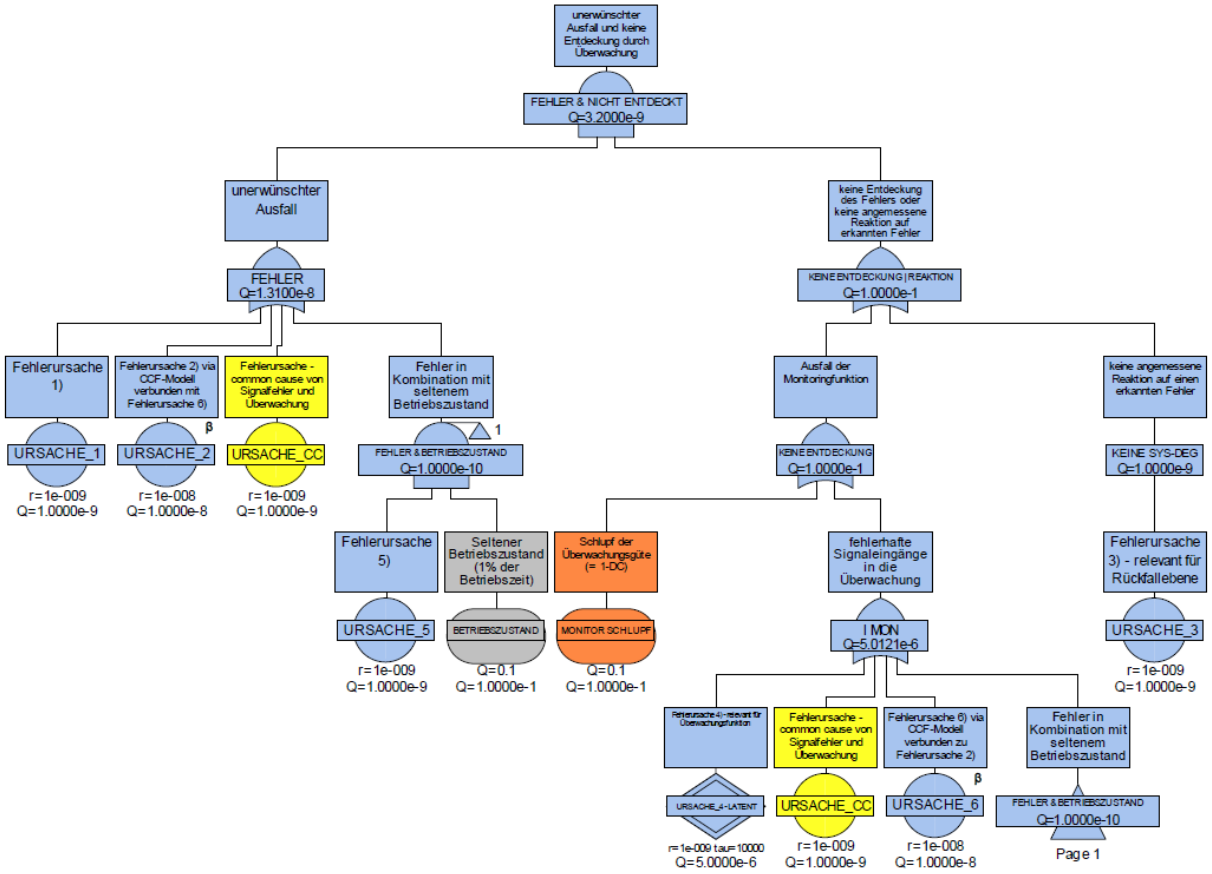


Abbildung 4.5: Beispielfehlerbaum

Das Beispiel stellt eine Überwachung von Fehlerursachen dar.

URSACHE_1, URSACHE_2, URSACHE_5 sowie URSACHE_CC stellen die zu überwachenden Fehler dar, wobei URSACHE_5 nur in Kombination mit seltenen Betriebszuständen wirksam wird. Dabei sind sowohl das Gate „FEHLER & Betriebszustand“ als auch URSACHE_CC auch an den Eingang der Überwachung geknüpft (Gatter „I MON“) – es ist daher zu erwarten, dass für diese Fehler das UND-Gatter „FEHLER & NICHT ENTDECKT“ aufgehoben ist.

URSACHE_4_LATENT und URSACHE_6 stellen nun Fehler dar, bei deren Auftreten der Überwachungsmechanismus versagt. Tritt URSACHE_3 ein, dann wird bei einem erkannten Fehler keine angemessene Reaktion (z.B. Systemdegradierung) ausgelöst (hier dargestellt im Gatter „KEINE SYS-DEG“).

Weiterhin ist als Besonderheit URSACHE_2 mittels eines Common Cause Fehlermodells (CCF Model) mit URSACHE_6 verbunden (Zeichen β). Das CCF Modell beschreibt den Anteil der Gesamtwahrscheinlichkeit, mit der beide Fehler (URSACHE_2 und URSACHE_6) *gleichzeitig* auftreten. Anmerkung: Die Rechenergebnisse des Beta-Modells können in den Projektoptionen „Sets Generation“ von Fault-Tree+ beeinflusst werden (Bereich CCF-Analysis).

Hinweis: Soll eine FTA zur reinen qualitativen Betrachtung erstellt werden, ist es trotzdem sinnvoll, den Basisevents Fehlerraten zuzuweisen. Um Missverständnisse bei eventuellen Präsentationen zu vermeiden, empfiehlt sich die Verwendung eines generisch angelegten Fehlermodells, das dann allen Events zugewiesen wird. Effekt: Die berechneten Fehlerkombinationen werden nach ihrer Wahrscheinlichkeit sortiert vom Tool ausgegeben. Die Anzeige der resultierenden Wahrscheinlichkeiten der Gatter kann in den Tool-Optionen „View“ unterdrückt werden.

4.5.2. Fehlerkombinationen

Bei der Auswertung der Fehlerkombinationen können verschiedene Typen von Fehlerkombinationen identifiziert werden. Es sind dies Einzelfehler, Restfehler (überwachte Fehler), Mehrfachfehler und als Teilmenge der Mehrfachfehler die Gruppe der latenten Mehrfachfehler.

a) Einzelfehler

Ein Ziel der FTA ist es, Einzelfehler zu identifizieren, die zu einem unerwünschten Ereignis führen.

Ein Einzelfehler ist wie folgt gekennzeichnet:

- Es gibt keine Sicherheitsmechanismen (z. B. Überwachungen oder Redundanzen), die verhindern, dass bei Eintritt des Fehlers das zugehörige unerwünschte Ereignis (Top Event) eintritt.

Auswertung im FT-Tool:

Das FT-Tool bietet im Wesentlichen zwei Möglichkeiten zur Auswertung der Fehlerkombinationen an. Diese sind

- die Cut-Set Liste, welche die durch das Tool errechneten Fehlerkombinationen (Minimalschnitte) geordnet nach Wahrscheinlichkeit ihres Eintretens anbietet
- und die Importanz-Liste, welche für jedes im Fehlerbaum vorkommende Basis-Ereignis seine Bedeutung (Importanz) ausweist. Zur qualitativen Auswertung kann die Birnbaum-Importanz herangezogen werden.

Um die vom FT-Tool angebotenen Listen effizient auswerten zu können, ist es unabdingbar, eine Namenskonvention für die Bezeichnungen der Basis-Ereignisse (Event Names) einzuhalten. Sie erlaubt erst die schnelle Identifikation der beteiligten Basis Ereignisse anhand ihrer Bezeichnung. Selbst im Beispiel oben (siehe Abbildung 4.5) ist dies in rudimentärer Form eingehalten (z.B. heißen alle Fehler „URSACHE_#“). Hinweise und Empfehlungen hierzu siehe auch „Anhang 1 Symbole und Modellierungsempfehlungen“.

Anmerkung: Bevor mit der Auswertung begonnen werden kann, muss sichergestellt sein, dass für das interessierende Gate während der Berechnung die Speicherung der Fehlerkombinationen aktiviert ist. Dies erfolgt bei den bei Bosch verwendeten FT-Tools über die Aktivierung der Gate-Option „Retain Results“. Andernfalls erscheint das interessierende Gate gar nicht erst in der Liste der zur Verfügung stehenden Gatter. Abbildung 4.6 zeigt den Auswerte-Dialog, wenn im Beispiel-Fehlerbaum lediglich für das Top Gate die Option „Retain Results“ aktiviert ist. Im oberen Bereich wird nur 1 Gatter angeboten (im Gegensatz zu Abbildung 4.7, wo mehrere Gatter zur Analyse ausgewählt werden können).

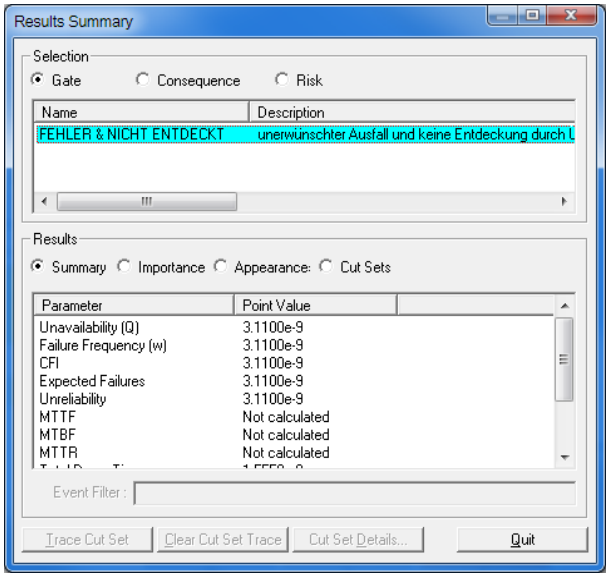


Abbildung 4.6: Retain results ausschließlich für das Top Gate aktiviert

Einzelfehler in der Cut-Set Liste:

In der Cut-Set Liste des jeweiligen Top Events können nun Einzelfehler identifiziert werden:

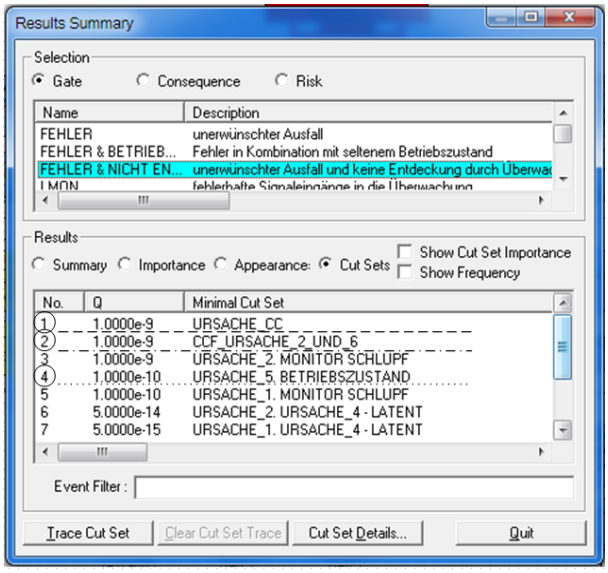


Abbildung 4.7: Cut-Set list in FaultTree+ für das Top Event

- Cut-Sets der Order 1
  → die Anzahl der beteiligten Ereignisse ist 1 (Cut-Set Nummer 1 und 2 in Abbildung 4.7)
  URSACHE_CC ist der modellierte Common Cause Fehler, der sowohl an Fehler, als an Überwachungsseite angehängt ist.
  Im Beispiel: „CCF_URSACHE_2_UND_6“ ist im Fehlerbaum nicht durch ein Basis-Ereignis repräsentiert. Das Tool berechnet vielmehr auf Basis des verwendeten CCF-Modells die Wahrscheinlichkeit des gleichzeitigen Ausfalls von Ursache_2 und Ursache_6 und weist diesen Betrag als Einzelfehlereintrag (mit dem Namen des CCF-Modells) in der Cut-Set Liste aus. Verfolgt man dieses Cut-Set via FT-Tool zu seinen Ursprüngen (mittels Option Trace Cut-Set), endet der „Trace“ bei URSACHE_2 bzw. URSACHE_6.
- Cut-Sets Order > 1
  → höchstens 1 Ereignis stellt den Fehler dar - die restlichen beteiligten Ereignisse repräsentieren wahrscheinlichkeitsreduzierende Bedingungen (z.B. seltene Betriebszustände – modellierbar als „Conditional Events“ mit fixer Auftretenswahrscheinlichkeit) (Cut-Set Nummer 4 in Abbildung 4.7)
  Im Beispiel: „URSACHE_5“ kombiniert mit dem „BETRIEBSZUSTAND“ (dieses Event beschreibt weder einen Fehler noch einen Überwachungsmechanismus)

Einzelfehler in der Importanz Liste:

In der Importanzliste des jeweiligen Top Events kann die Birnbaum Importanz (BI) dazu verwendet werden, Einzelfehler zu identifizieren.

Dabei ist es aufgrund der Berechnung der BI zunächst unerheblich, *welche* Bedatung dem jeweiligen Einzelfehlerevent zugeordnet ist, Hauptsache es sind überhaupt Fehlerraten definiert. Bei einer fehlenden oder unvollständigen Bedatung (r=0) kann die Importanzliste nicht sinnvoll angewendet werden, da dann bei der Berechnung der BI durch Null dividiert werden müsste. Denn die BI ist definiert als Verhältnis zwischen Auftretenswahrscheinlichkeiten und beschreibt die bedingte Wahrscheinlichkeit des Eintretens des Top Events, wenn das zu betrachtende Event bereits eingetreten ist. Da im Falle eines Einzelfehlers – also ohne jegliche Sicherheitsmechanismen – die Wahrscheinlichkeit des Eintretens des Top Events sichergestellt ist (Wahrscheinlichkeit ist 1), muss daher die BI für Einzelfehler gleich 1 sein. Details siehe „Schritt 6: Quantitative Auswertung“.

Umgekehrt stellen alle Events mit einer BI = 1 zwingend Einzelfehler dar. (URSACHE_CC und CCF_URSACHE_2_UND_6 – gestrichelt umrandet in Abbildung 4.8)

N.B.: Die BI für Events, die in einer Kombination mit seltenen Betriebszuständen vorkommen, erlauben keine eindeutige Aussage darüber, ob es sich dabei um Einzelfehler handelt. Denn eine BI < 1 kann auch durch den seltenen Betriebszustand bedingt sein und bedeutet daher nicht zwangsläufig, dass es sich bei dem betrachteten Event um eines in einer Mehrfachfehlerkombination handelt. (URSACHE_5 – gepunktet umrandet in Abbildung 4.8)

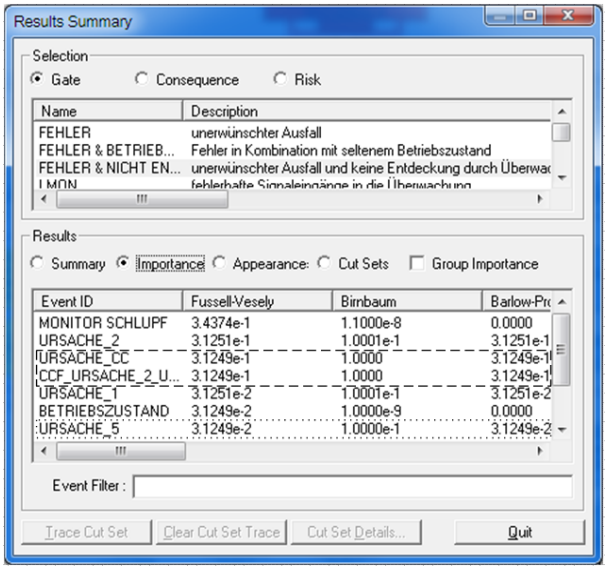


Abbildung 4.8: Importanz Liste in FaultTree+

b) Restfehler (überwachte Fehler)

Die FTA ist in der Lage, überwachte (Einzel-)Fehler (Residual Faults im Sinne der ISO 26262) zu identifizieren.

Ein überwachter Fehler stellt eine Fehlerkombination aus einem Fehler und einem oder mehreren Basiselementen dar, die den Schlupf der Diagnosedeckung der Überwachungsfunktionen ausweisen.

Auswertung im FT-Tool:

Das FT-Tool bietet zwei Möglichkeiten zur Auswertung der Fehlerkombinationen an. Diese sind

- die Cut-Set Liste, welche die errechneten Fehlerkombinationen (Minimalschnitte) geordnet nach Wahrscheinlichkeit ihres Eintretens enthält,
- und die Importanz-Liste, welche für jedes im Fehlerbaum vorkommende Basis-Ereignis seine Bedeutung (Importanz) ausweist. Zur qualitativen Auswertung kann die *Birnbaum*-Importanz herangezogen werden.

Überwachte Fehler in der Cut-Set Liste:

In der Cut-Set Liste des jeweiligen Top Events können überwachte Fehler identifiziert werden:

- Cut-Sets der Order 2 sind überwachte Fehler, wenn
  (1) ein Ereignis den überwachten Fehler darstellt

  UND

  (2) das zweite Ereignis den Schlupf der Diagnosedeckung der Überwachung repräsentiert
- Cut-Sets Order > 2 sind als überwachte Fehler zu werten, wenn

  (1) *höchstens ein einziges* Ereignis einen Fehler darstellt

  UND

  (2) von den restlichen beteiligten Ereignissen *mindestens* eines die Diagnosedeckung der Überwachung repräsentiert

  UND

(3) die restlichen Ereignisse wahrscheinlichkeitsreduzierende Bedingungen (z.B. seltene Betriebszustände) oder weitere Diagnosedeckungen, *NICHT* aber Fehler repräsentieren.

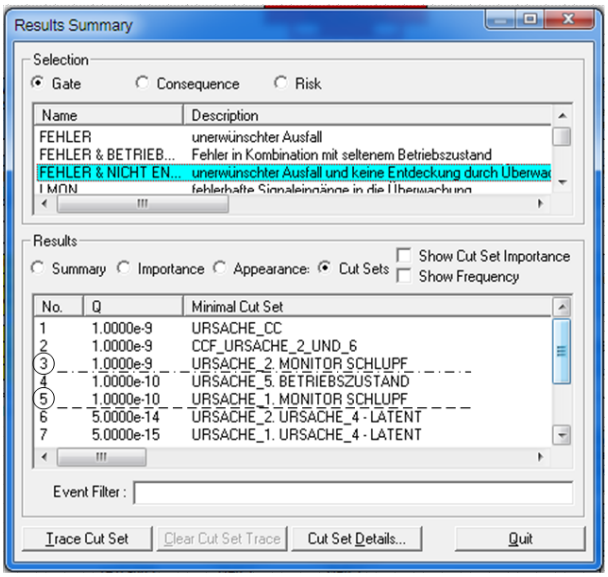


Abbildung 4.9: Überwachte Fehler in FaultTree+ in der Cut-Set Liste

Überwachte Fehler in der Importanz Liste:

Auf Basis der Importanz Liste lassen sich keine eindeutigen Schlüsse auf überwachte Fehler ziehen. Die im betrachteten Beispiel gelisteten Birnbaum-Importanzen mit 0,01 < BI < 1 sind nicht zwangsläufig durch Überwachungen begründet. Events mit einer BI = 0,1 können entweder mit seltenen Betriebszuständen (URSACHE_5 – gepunktet umrandet in Abbildung 4.10:) oder aber mit einer Überwachung (mit einer Diagnosedeckung des Monitors von 90 %: URSACHE_1 und URSACHE_2 gestrichelt umrandet in Abbildung 4.10 kombiniert sein (s. außerdem: c) Mehrfachfehlerkombinationen S. 23)

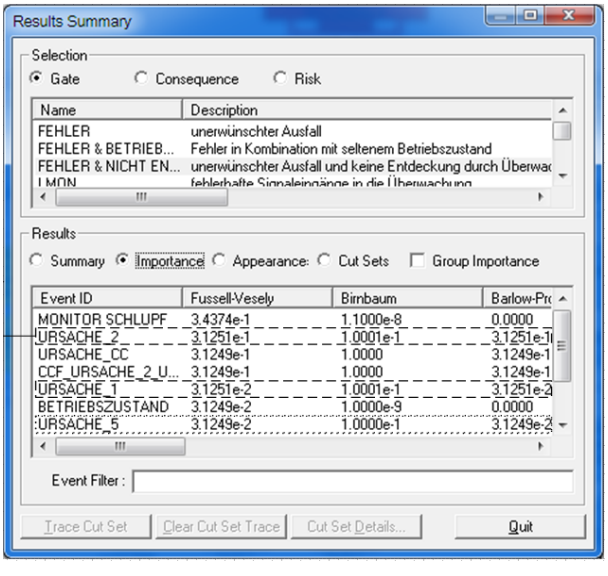


Abbildung 4.10: Uneindeutige Klassifizierung via BI: gepunktet – Einzelfehler mit seltenem Betriebszustand – gestrichelt – überwachte Fehler

c) Mehrfachfehlerkombinationen

Eine Mehrfachfehlerkombination (Multiple Point Failure) besteht aus mehreren Fehlern.

Auswertung im FT-Tool:

Mehrfachfehlerkombinationen in der Cut-Set Liste:

In der Cut-Set Liste des jeweiligen Top Events können Mehrfachfehlerkombinationen identifiziert werden:

- Cut-Sets der Order 2 sind Mehrfachfehlerkombinationen, wenn BEIDE Ereignisse Fehler, nicht aber Diagnoseschlupf oder Betriebszustände, darstellen.
- Cut-Sets höherer Ordnung sind Mehrfachfehlerkombinationen, wenn MINDESTENS ZWEI Ereignisse Fehler darstellen – die restlichen Ereignisse dürfen dann beliebige Inhalte repräsentieren (also Betriebsbedingungen, Überwachungen o.ä.).

N.B: Im Sinne der ISO26262 ist es notwendig, überwachte Mehrfachfehlerkombinationen von überwachten Einzelfehlern (Residual Faults) zu unterscheiden, weil die Norm unterschiedliche Anforderungen an den Umgang mit solchen Fehlerkombinationen stellt.

d) Latente Fehler

Latente Fehler sind Fehler, die eine zweite Fehlerbedingung erfordern, um das unerwünschte Ereignis (Top Event) auslösen zu können. Latente Fehler sollten differenziert werden von „schlafenden" Fehlern, die einen seltenen *Betriebszustand* benötigen, um für das unerwünschte Ereignis wirksam zu werden.

Latente Fehler sind zum Zeitpunkt ihres Auftretens daher

- ohne direkte Auswirkung auf das unerwünschte Ereignis (ein Zweitfehler muss eintreten)
- nicht durch sekundäre Auswirkungen (z.B. Geräusche oder Komforteinbußen) bemerkbar
- während ihrer Latenzzeit nicht durch Überwachungen entdeckbar

Einzelfehler und überwachte Fehler können im Sinne der obigen Definition daher niemals latent sein. Im Gegensatz zu „schlafenden" Fehlern, die mit einem seltenen Betriebszustand kombiniert sind, muss ein als latent identifizierter Fehler also in Mehrfachfehlerkombinationen – überwacht oder nicht überwacht – gesucht werden.

Die Identifikation von latenten Fehlern kann auf mehrfache Weise erfolgen:

a) Der Fehlerbaum wird an den UND-Gattern während der Erstellungsphase untersucht
b) Die berechneten Cut-Sets werden hinsichtlich ihrer Zusammensetzung auf latente Fehler untersucht

Untersuchung des Fehlerbaums zur Bestimmung von latenten Fehlern (Option a)

Latente Fehler können mittels Betrachtung der Fehlerbaumstruktur identifiziert werden. Da latente Fehler nur in Mehrfachfehlerkombinationen auftreten, sind insbesondere solche Gatter von Interesse, die aufgrund ihrer Logik zu solchen Mehrfachfehlerkombinationen führen können (AND, XOR, VOTE).

Beispiel:

Der in Kapitel 4.5.1 vorgestellte Beispielfehlerbaum (s.a. Abbildung 4.5) wird auf potentiell latent vorliegende Fehler untersucht.

Die Betrachtung beginnt bei Gate „FEHLER & NICHT ENTDECKT". Es ist ein AND-Gate, das einen Fehler mit dem Versagen einer Überwachung kombiniert:

Schritt 1) Die Eingänge von „FEHLER & NICHT ENTDECKT" werden zunächst auf *potentielle* Latenz hin untersucht.

Im Beispiel stellt das Gatter eine Kombination aus Fehler und Überwachung dar. Da der Fehler ohne Überwachung ganz sicher zum unerwünschten Ereignis führen würde, wird der Fehlerpfad (Gatter „FEHLER") als nicht-latent gewertet. Ein Ausfall der Überwachung bleibt hingegen ohne Folgen, solange der Fehler nicht eingetreten ist (=> Gatter „KEINE ENTDECKUNG | REAKTION")

N.B. Eine Farbgebung der bereits analysierten Gatter kann bei der Abarbeitung dieser Aufgabe hilfreich sein.

Im Beispiel(siehe Abbildung 11, Abbildung 12, Abbildung 13): GRÜN: keine potentielle Latenz; PINK: potentiell latent; GELB/CREME: Fehler; GRAU: Betriebszustand; ORANGE: Schlupf Diagnosedeckung; HELLBLAU: noch abzuarbeiten

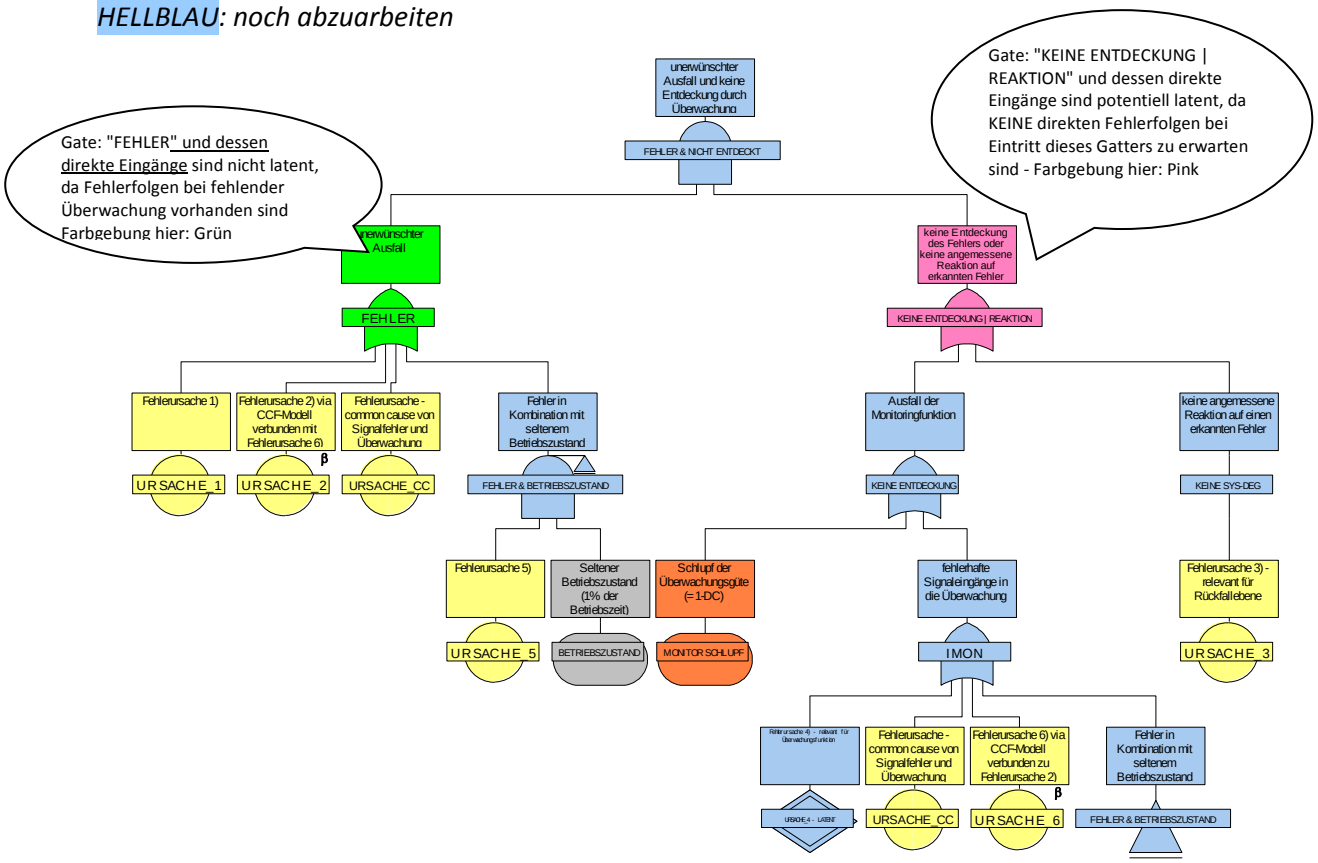


Abbildung 4.11: Schritt 1) – Bestimmung potentiell latenter / nicht latenter Pfade

Im nächsten Schritt werden alle Fehlerbäume und Events, die eine direkte Verbindung zum betrachteten Eingang haben (also nicht via UND-Gatter) entsprechend der Einteilung des betrachteten Gatters gekennzeichnet.

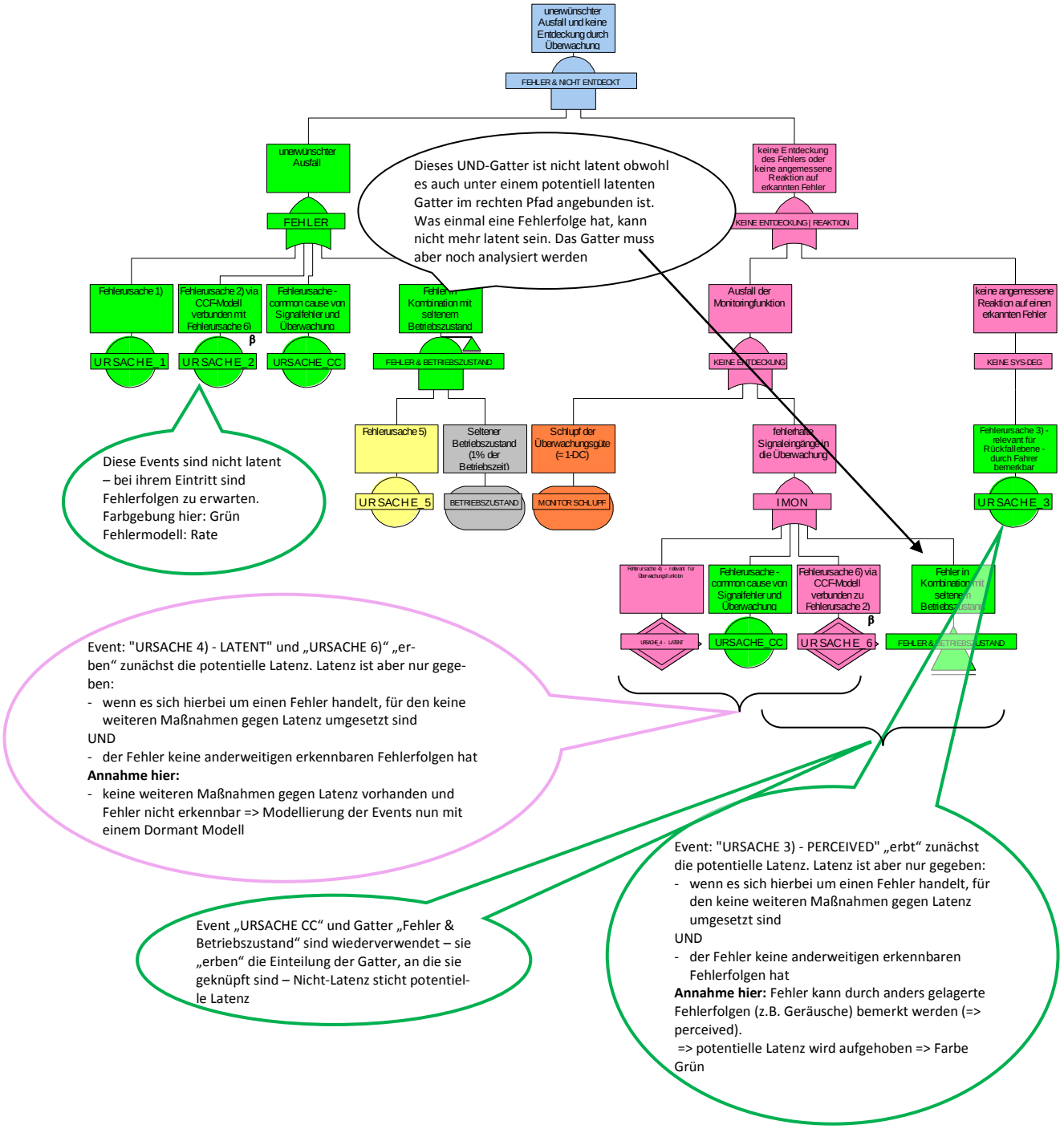


Abbildung 4.12: Schritt 2) – Vererbung der initialen Einteilung auf direkt verbundene FT-Elemente (ODER-Gatter oder Events)

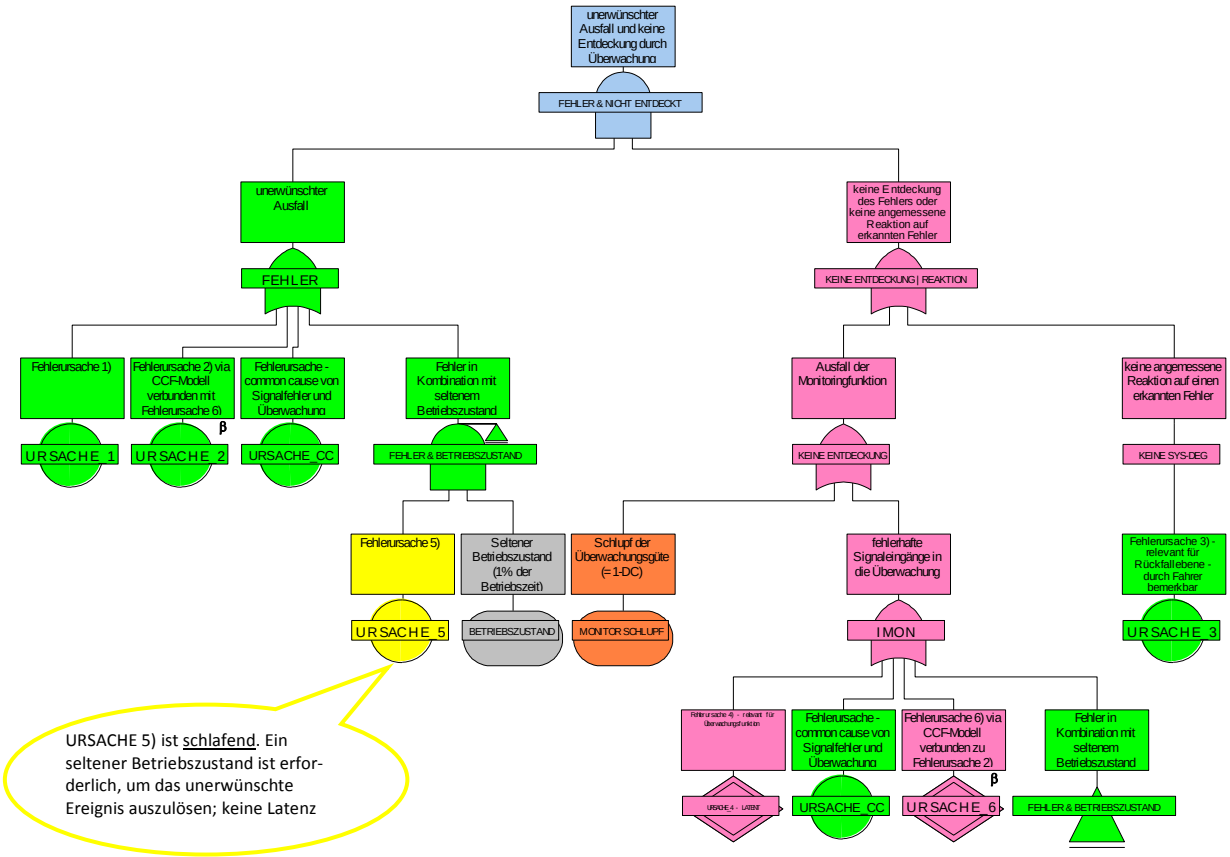


Abbildung 4.13: Schritt 3ff) – Analyse der tiefer liegenden UND-Gatter

Ergebnis:

Im Fehlerbaum wurden folgende Events als potentiell latent identifiziert:

URSACHE_4_LATENT; URSACHE_6

Wenn Fehler als latent eingestuft worden sind, sollte dies durch entsprechende Fehlermodelle (z.B. Dormant-Fehlermodell vergeben) berücksichtigt werden. Die Latenzzeit der einzelnen Fehler (Parameter τ im Dormant-Modell) muss vorhandene Maßnahmen gegen Latenz einbeziehen (z.B. auch nicht im betrachteten Fehlerbaum modellierte Power-On Selftests).

Hinweis: Option a) ist geeignet für kleinere Fehlerbäume mit einer begrenzten Anzahl von UND-Gattern. Sie kann auch begleitend zur Fehlerbaum Erstellung durchgeführt werden. Bei umfangreichen Fehlerbäumen bietet sich aus Aufwandsgründen hingegen Option b) an.

Untersuchung der ermittelten Fehlerkombinationen zur Bestimmung von latenten Fehlern (Option b)

Auch anhand von Minimalschnitten (Cut-Sets) kann eine Untersuchung auf latente Fehler vorgenommen werden. Dabei kommen naturgemäß nur Cut-Sets ab Ordnung 2 in Frage, da eine latente Fehlerursache bei ihrem Eintritt weder direkte Fehlerfolge haben noch entdeckbar sein darf.

N.B: Die Identifikation von latenten Fehlern auf Basis der Cut-Sets kann nicht direkt im FT-Tool vorgenommen werden, sondern erfordert einen Datenexport in eine geeignete Tabellenkalkulation. Die Sortierung der Cut-Sets nach Auftretenswahrscheinlichkeit darf in der Tabellenkalkulation nicht geändert werden.

Bei der Betrachtung der Fehlerkombinationen ist jedes Event des Cut-Sets für sich gesehen zu beleuchten – wenn eine folgenden Aussagen zutrifft, dann handelt es sich NICHT um einen latenten Fehler.

- Es gibt Überwachungsmechanismen, die den Fehler zur Anzeige bringen. (z.B. Initiale Tests oder Online-Monitore)

- Der Fehler hat Folgen, die zwar nicht unmittelbar das unerwünschte Ereignis auslösen (schließlich kommt es in einem Mehrfachfehler vor), aber in anderem Zusammenhang bemerkbar sind (z.B. Komforteinschränkungen, Geräusche oder aber der Fehler ist bzgl. eines anderen unerwünschten Ereignisses im selben System ein Einzelfehler) → der Fehler ist „perceived".
- Ein potentiell latent identifizierter Fehler hat unter keinen Umständen eine Auswirkung auf das betrachtete unerwünschte Ereignis. Dies ist der Fall, wenn es in der zu betrachteten Fehlerkombination der Ordnung n (mit n > 2) mehr als einen einzigen nicht-latenten Fehler gibt. Denn in einer Fehlerkombination mit mehr als 1 nicht-latenten Fehler verhindert der zweite nicht-latente Fehler, dass im Cut-Set vorkommende latente Fehler zum unerwünschten Ereignis durchschlagen.

Zeitlicher Ablauf	Fehler 1 nicht latent	Fehler 2 latent	Fehler 3 latent	Effekt auf System
1	0	0	1	Kein Effekt
2	0	1	1	Kein Effekt
3	1	1	1	Unerwünschtes Ereignis tritt ohne Vorwarnung ein

Zeitlicher Ablauf	Fehler 1 nicht latent	Fehler 2 nicht latent	Fehler 3 latent	Effekt auf System
1	0	0	1	Kein Effekt
2	0	1	1	Fehler 2 entdeckt oder perceived

Zeitlicher Ablauf	Fehler 1 nicht latent	Fehler 2 nicht latent	Fehler 3 latent	Effekt für System
1	0	0	1	Kein Effekt
2	1	0	1	Fehler 1 entdeckt oder perceived

- Das betrachtete Event beschreibt einen der folgenden Inhalte (Betriebszustand, Überwachungsschlupf (Monitor), andere Bedingungen); diese Events werden als nicht latent angesehen

Die einmal getroffene Kategorisierung gilt dann für das Event und seine Rolle generell in diesem betrachteten Fehlerbaum.

Beispieltabelle für den Beispielfehlerbaum aus Abbildung 4.5:

Die Suche nach latenten Fehlern nach der zweiten Methode identifiziert dieselben Events wie die Erste.

Zeilenweise wird nun jedes Cut-Set separat betrachtet. Der 1. beteiligte Fehler (1st fault) wird klassifiziert und diese Klassifikation dann auf alle Zeilen übertragen, in denen der betrachtete Fehler auftritt. Ein Fehler ist dann als latent zu bewerten, wenn die potentielle Latenz dadurch bestätigt wird, dass es keine Maßnahmen gegen die Latenz gibt. In der Tabelle bedeutet das sowohl einen Eintrag „pL" und einen weiteren Eintrag „L". Bestätigt sich die potentielle Latenz später hingegen nicht, kann ein „P" eingetragen werden (im Beispiel gilt dies für URSACHE_3)

N.B.: Features der Tabellenkalkulation wie z.B. Filtermöglichkeiten oder sinnvoll programmierte Makros können beim Ausfüllen der Tabelle effizient unterstützen und die Analyse erheblich beschleunigen!

Verwendete Klassifikationen in der Tabelle:

n.a. = nicht relevant;
M = Monitorschlupf (→ nicht latent);
B = Betriebszustand (→ nicht latent);
P = perceived (bemerkt → nicht latent);
L = Latent;
SPF = Single Point Fault (=> nicht latent);
RF = residual fault (überwachter Fehler => nicht latent);

S = schlafender Fehler (nicht latent);
pL = potentiell latent

Number	Cut-Set	Event Descriptions	Una-vailabil-ity	Order	1st fault	latent fault perceived fault	2nd fault	latent fault perceived fault
1	URSACHE_CC	Fehlerursache - Common Cause von Signalfehler und Überwachung	1E-09	1	SPF	n.a.		
2	CCF_URSACHE_2_UND_6	Common Cause Fehler Modell	1E-09	1	RF	n.a.		
3	URSACHE_2. MONITOR SCHLUPF	Fehlerursache 3) via CCF-Modell verbunden mit Fehlerursache 6) Schlupf der Überwachungsgüte (= 1-DC)	1E-09	2	RF	n.a.	M	n.a.
4	URSACHE_1. MONITOR SCHLUPF	Fehlerursache 1) Schlupf der Überwachungsgüte (= 1-DC)	1E-10	2	RF	n.a.	M	n.a.
5	URSACHE_5. ETRIEBSZUSTAND	Fehlerursache 5) Seltener Betriebszustand (1% der Betriebszeit)	1E-11	2	S	n.a.	B	n.a.
6	URSACHE_2. URSACHE_6	Fehlerursache 3) via CCF-Modell verbunden mit Fehlerursache 6) Fehlerursache 6) via CCF-Modell verbunden zu Fehlerursache 2)	5E-13	2	RF	n.a.	pL	L
7	URSACHE_2. URSACHE_4 - LATENT	Fehlerursache 3) via CCF-Modell verbunden mit Fehlerursache 6) Fehlerursache 4) - relevant für Überwachungsfunktion	5E-14	2	RF	n.a.	pL	L
8	URSACHE_1. URSACHE_6	Fehlerursache 1) Fehlerursache 6) via CCF-Modell verbunden zu Fehlerursache 2)	5E-14	2	RF	n.a.	pL	L
9	URSACHE_1. URSACHE_4 - LATENT	Fehlerursache 1) Fehlerursache 4) - relevant für Überwachungsfunktion	5E-15	2	RF	n.a.	pL	L
10	URSACHE_2. URSACHE_3	Fehlerursache 3) via CCF-Modell verbunden mit Fehlerursache 6) Fehlerursache 3) - relevant für Rückfallebene - durch Fahrer be-merkbar	1E-17	2	RF	n.a.	pL	P
11	URSACHE_1. URSACHE_3	Fehlerursache 1) Fehlerursache 3) - relevant für Rückfallebene - durch Fahrer be-merkbar	1E-18	2	RF	n.a.	pL	P

Ergebnis:

Das Ergebnis deckt sich mit der grafischen Analysemethode. In der Cut-Set Liste wurden folgende Events als potentiell latent identifiziert:

URSACHE_4 – LATENT; URSACHE_6

Die Latenzzeit der latenten Fehler (Parameter τ im Dormant-Modell) muss vorhandene Maßnahmen gegen Latenz einbeziehen (z.B. auch nicht im betrachteten Fehlerbaum modellierte Power-On Self-tests).

Identifizierte latente Fehler – Konsequenzen für die Fehlerbaum-Modellierung.

Latente Fehler müssen mit einem Fehlermodell ausgestattet werden, das ihrer Latenzzeit Rechnung trägt. Dies kann durch die Vergabe eines Dormant-Models im FTA-Tool erfolgen.

Die Latenz wird bestimmt durch das Zeitintervall, das zwischen dem Auftreten des Fehlers und seiner möglichen Entdeckung verstreichen kann.

Bsp.: Wird ein Fehler durch einen regelmäßig (z.B. alle 10 Betriebsstunden) durchgeführten Test entdeckt, so entspricht das längst mögliche Zeitintervall von 10 h seiner Latenz (Fehler tritt unmittelbar nach dem letzten Test ein; danach dauert es wieder 10 h bis zum nächsten Test).

Durch die Anwendung des Dormant Fehlermodells führt die Latenzzeit bei Ermittlung der Ausfallwahrscheinlichkeit des Fehlers – eine sinnvolle Wahl der Fehlerbaum-Rechenparameter vorausgesetzt – zu einer wesentlich erhöhten Ausfallwahrscheinlichkeit latenter Fehler im Vergleich zu nicht latenten Fehlern. Es ist daher sinnvoll, Maßnahmen gegen Latenz von Fehlern in Systemen zu ergreifen.

Details zu den Fehlermodellen siehe *Anhang 1: Symbole und Modellierungsempfehlungen*

4.6. Schritt 5: Ermittlung der Eintrittswahrscheinlichkeiten der Basisereignisse (quantitative Beschreibung)

4.6.1. Allgemein

Um eine quantitative Analyse des Fehlzustandsbaums durchführen zu können, müssen den Basisereignissen die jeweiligen Eintrittswahrscheinlichkeiten zugeordnet werden. Diese Eintrittswahrscheinlichkeiten können anhand von geeigneten Zuverlässigkeitskenngrößen ermittelt werden.

Zuverlässigkeitskenngrößen sind zum Beispiel

- die Ausfallrate λ (zeitabhängige Größe, z.B. r= 1 E-09/h = 1 FIT)
- die Ausfallwahrscheinlichkeit Q_A (zeitunabhängige Wahrscheinlichkeit, z.B. Q = 0,1)
- die Eintrittswahrscheinlichkeit Q_E (zeitunabhängige Wahrscheinlichkeit, z.B.
- Umgebungsbedingungen wie Regen, Schnee, …)

Um die Zuverlässigkeitskenngrößen für die quantitative Analyse des Fehlerbaums zu ermitteln, gibt es unterschiedliche Ansätze. Oftmals ist ein bestimmter Ansatz durch den Auftraggeber vorgegeben. Wenn nicht, muss dies im Team abgestimmt werden.

In der Regel werden die Zuverlässigkeitskenngrößen aus einer der folgenden fünf Informationsquellen ermittelt:

- eigene Feld- bzw. Betriebserfahrung
  Vorteil: reale Einsatzbedingungen
  Nachteil: Produkt muss im Feld sein, Daten sind dann spät verfügbar.

  Alternativ: Verwendung von Daten eines vergleichbaren Vorgängerprodukts (Einschränkung: Übertragbarkeit ist zu prüfen.)
- eigene Tests bzw. Versuchserfahrung
  Vorteil: Information, bevor Produkt im Feld ist (Stichprobe/Zeitraffung)
  Nachteil: nur Testbedingungen; Zusatzaufwand und -kosten
- Literaturdaten / generische Daten aus Datensammlungen (z.B. Handbücher; empfohlen wird die Verwendung von „Siemens SN29500“ oder „IEC62380“)
  Vorteil: breite Datenbasis, anerkannte Datengrundlage
  Nachteile: Übertragbarkeit auf eigene Anwendung nicht immer gegeben;
  Neuartige Bauelemente / Technologien nicht enthalten;
  historische Daten – eher konservativ

  Hinweis: Falls die Einsatz- bzw. Rahmenbedingungen (z.B. Temperaturprofil), die den Handbuchdaten zugrunde liegen, für das zu untersuchende unerwünschte Ereignis bzw. Produkt anders sein sollten, ist eine Anpassung der Daten vor Verwendung im Fehlerbaum notwendig.

  Bei FTA im Kontext von automotiven Anwendungen hat sich bei der Ermittlung der Zuverlässigkeitskenngrößen zur Absicherung von Produkten die Siemensnorm (SN29500) bewährt.
- Erfahrungen von Bosch-externen Quellen z. B. Zulieferern

- Expertenschätzung (mit Begründung), sofern keine der oben genannten Möglichkeiten eine für den Anwendungsfall geeignete ZKG liefert

Die Daten sind meistens als Ausfallraten, in „ppm pro Zeiteinheit“ oder „FIT“ angegeben.

Die Werte beziehen sich in der Regel auf das gesamte Bauelement. In der FTA wird aber die Ausfallrate bezogen auf den Fehlermodus eines Teils des Bauelements benötigt.

Für einfache Bauelemente (z.B. Diode, Widerstand,…) kann die Gesamtrate nach Fehlerkatalogen (z.B. Kurzschluss, offen, Drift) aufgeteilt werden. Dazu wird am häufigsten das Standardwerk von A. Birolini (Reliability Engineering: Theory and Practice, Springer Verlag) verwendet.

Für komplexe Bauteile (z.B. Mikrocontroller) wird die Gesamtausfallrate typischerweise nach Flächenanteilen der Schaltungsblöcke aufgeteilt. Die Feinheit der Untergliederung bestimmt sich nach den Erfordernissen der FTA.

Im Laufe einer Entwicklung eines Projekts kann es nötig sein, die Zuverlässigkeitskenngrößen zu aktualisieren.

4.6.2. Präventiv / Korrektiv

In der präventiven Anwendung der FTA kann man prinzipiell alle Informationsquellen zur Ermittlung von Zuverlässigkeitskenngrößen verwenden (siehe 4.6.1).

Im korrektiven Anwendungsfall der FTA werden vorrangig Zuverlässigkeitskenngrößen aus der eigenen bzw. fremden Feld- bzw. Betriebserfahrung verwendet, da in diesem Fall ein in der Anwendung aufgetretenes Fehlerbild untersucht werden soll.

4.7. Schritt 6: Quantitative Auswertung

4.7.1. Allgemein

Damit die quantitative Auswertung zu aussagekräftigen Ergebnissen führen kann, muss die qualitative Analyse – sprich der Fehlerbaum – belastbar sein. Des Weiteren muss sowohl die Bedatung der Basisereignisse geklärt sein, als auch die Parameter, die zur Berechnung der Fehlerbaumergebnisse gesetzt werden müssen.

4.7.2. Definition der Rechenparameter im FTA-Werkzeug

Mission Time

Schon während der Vorbereitung der FTA ist festzulegen, welche Mission Time (Berechnungszeit) – im Automotive Bereich entspricht das dem Fahrzyklus – für die quantitative Auswertung der FTA gewählt wird. Hiervon hängt entscheidend ab, welche Ergebnisse die FTA liefern wird.

Anmerkung: Die entsprechende Option im FT-Tool FT+ ist die „System life time“ (Options/Calculation).

Abhängig vom Anwendungsfall können hier unterschiedliche Zeiten sinnvoll sein. In der Automobilindustrie hat sich z.B. bei der Anwendung der FTA zur Unterstützung des Sicherheitsnachweises nach ISO26262 eine Mission Time von 1 h durchgesetzt. Sie hat einen gewissen Bezug zur durchschnittlichen Nutzungszeit von Fahrzeugen und ermöglicht eine sinnvolle Berechnung der Ausfallrate von nicht latenten Fehlern (Raten Model) im Vergleich zu latenten Fehlern (Dormant Model).

Dormant Failure Model

Die Berechnung des Dormant Failure Models ist auf verschiedene Weisen möglich. Das konservativste Ergebnis (höchste Ausfallwahrscheinlichkeit) liefert die Einstellung „Max“. Hierbei wird davon ausgegangen, dass der latente Fehler zu Beginn des Fahrzeuglebens auftritt und dann über die gesamte Latenzzeit anliegt. Der Fehler tritt also hier „zufällig“ immer am Anfang des Fahrzeuglebens auf – in der Realität ist das nicht der Fall.

Die Option „Mean“ geht von einer Gleichverteilung des Fehlerauftretens über der Fahrzeuglebensdauer aus. Die Berechnung liefert daher den Mittelwert der Wahrscheinlichkeit ($Q = \lambda * \tau / 2$) eines latenten Fehlers.

Es kann projektabhängig aber auch die verbleibende Rechenmethode (ISO61508) sinnvoll sein. Weitere Informationen hierzu liefert die Toolhilfe von FaultTree+ (bzw. RWB)

4.7.3. Zahlenwert des Top Gates

Das FTA-Tool errechnet automatisch für jedes Gatter

- die Nichtverfügbarkeit Q
- die Eintrittshäufigkeit ω
- Mean Time To Failure (MTTF)
- Mean Time to Repair (MTTR)
- Mean Time between Failure (MTBF)

Das Tool unterstützt die Anzeige des jeweils gewünschten Ergebnistyps im Fehlerbaum.

Abhängig von den Rahmenbedingungen, unter denen eine FTA erstellt wird, muss die jeweilige Kenngröße mit den vorher definierten Zielwerten in Einklang gebracht werden.

Nichtverfügbarkeit Q:

Q ist dimensionslos und beschreibt die Wahrscheinlichkeit des Eintretens des unerwünschten Ereignisses am Ende des berechneten Zeitraums. Sollen Aussagen von Q in Bezug auf eine bestimmte Zeitdauer gemacht werden, muss die Berechnungszeit berücksichtigt werden. Ist die Berechnungszeit (Mission Time, „System life time“ s. o.) ungleich 1 Stunde gewählt, führt dies allerdings zu Fehlern im Endergebnis, weil die Division von Q durch eine Zahl die Wahrscheinlichkeit pro Stunde limitiert.

Beispiel: Ein nach 10.000 Stunden sicher eintretendes Ereignis mit der Wahrscheinlichkeit Q = 1 wird durch Division zu:

$$Q^*/1h = Q / 10.000\ h = 1E\text{-}04\ 1/h$$

D.h. die Wahrscheinlichkeit dieses Ereignisses kann nie oberhalb von Q*/1h = 1E-04 1/h liegen! Dies ist nicht plausibel.

Eintrittshäufigkeit ω

ω hat die Dimension 1/h und entspricht Q differenziert nach der Zeit. D.h. ω beschreibt den zeitlichen Verlauf (math. die Steigung) der Wahrscheinlichkeitskurve Q über t. Solange die Produkte aus Fehlerraten und Berechnungszeit sehr viel kleiner als 1 sind ($\lambda * t << 1$), befindet sich die Wahrscheinlichkeitskurve im linearen Bereich, d.h. die Ableitung der Exponentialkurve liefert denselben Betrag wie die Kurve selbst → $\omega \approx Q$.

Fehlerbäume, die zahlreiche Basisereignisse mit fixen (konstanten) Wahrscheinlichkeiten enthalten (hier ist $\omega = 0$), können zu Abweichungen in den Zahlenwerten zwischen ω und Q führen.

Mean Time To Failure (MTTF), Mean Time to Repair (MTTR), Mean Time between Failure (MTBF)

Diese Begriffe spielen in der Regel in reparierbaren Systemen eine Rolle, wobei MTTF einen Bezug zur Fehlerrate λ hat (unter bestimmten Voraussetzungen gilt: MTTF ≈ $1/\lambda$). In dieser Guideline wird auf diese Begriffe nicht näher eingegangen.

4.7.4. Optimierungspotential identifizieren

Ergibt sich aus der Betrachtung des Zahlenwerts im Top Event Handlungsbedarf, weil z.B. die gesetzten Ziele noch nicht erreicht worden sind, kann mittels Importanzbetrachtungen von Basisereignissen Optimierungspotential identifiziert werden, denn Importanz-betrachtungen lassen Aussagen über die Bedeutung von Basisereignissen in Bezug auf besondere Fragestellungen zu.

Beispiel 1: Reduktion der Gesamtausfallwahrscheinlichkeit

Eine mögliche Aufgabe nach Ermittlung der Auftretenswahrscheinlichkeit des Top Events könnte lauten: *Die Gesamtauftretenswahrscheinlichkeit muss unter einen bestimmten Wert gesenkt werden*. Damit das effizient erfolgt, müssen jetzt die Stellen der FTA, an denen Veränderungen in Bezug auf die gestellte Aufgabe besonders wirksam sind, identifiziert werden. Die dazu passende Fragestellung hierzu lautet:

Welche Beiträge leisten die Basis-Ereignisse zur Gesamtausfallrate des Top Events?

Diese Frage kann mit der Fussel-Vesely Importanz beantwortet werden.

Fussel-Vesely Importanz (FVI):

Die FVI ist ein Quotient aus

- der Summe der Auftretenswahrscheinlichkeiten *aller* Minimalschnitte, in denen das betrachtete Basisereignis A mit der Auftretenswahrscheinlichkeit q_A beteiligt ist, und
- der Auftretenswahrscheinlichkeit des unerwünschten Ereignisses Q_{SYS}.

$$I_A^{FV} = \frac{q_A \cdot q_B + q_A \cdot q_C + \ldots}{Q_{SYS}}$$

Da q_A größer als Null sein muss, nie aber größer als Q_{SYS} sein kann, gilt für die FVI

$0 < \text{FVI} \leq 1$.

Wäre die FVI = 0, dann hätte das Event keinen Beitrag zum Gesamtergebnis – dann dürfte es aber auch in keinem Minimalschnitt vorkommen, der das Top Event auslösen kann, also muss gelten FVI > 0.

Ist hingegen FVI = 1, dann ist das Basisereignis das *einzige* Event, das das unerwünschte Ereignis auslösen kann.

Anmerkung: Die Auswahl der Näherungsmethode „Rare" im Tool FT+ kann dazu führen, dass FVI = 1 ist und trotzdem noch weitere Ursachen das Top Event auslösen können. Hintergrund ist hier eine vereinfachte Berechnung der Gesamtauftretenswahrscheinlichkeit als einfache Summe der Teilwahrscheinlichkeiten der vorhandenen Cut-Sets.

Basisereignisse die eine hohe FVI haben (z.B. FVI = 0,7), tragen also maßgeblich zur Gesamtauftretenswahrscheinlichkeit bei – im Beispiel zu 70%. Es ist außerdem wahrscheinlich, dass Basisereignisse mit hoher FVI Einzelfehler, oder aber überwachte Fehler mit hoher Fehlerrate sind. Diese Events und ihre Position im Fehlerbaum sind daher von Interesse, wenn es darum geht, die Auftretenswahrscheinlichkeit des Unerwünschten Ereignisses zu reduzieren.

Maßnahmen zur Verringerung des Einflusses siehe Schritt 7.

Beispiel 2: Wirksamkeit von Überwachungen und Redundanzen bzgl. Absicherung gegen das Top Event

Mit Vorliegen der quantitativen Analyseergebnisse kann es von Interesse sein zu wissen, wie wahrscheinlich der Eintritt des unerwünschten Ereignisses ist, wenn ein Fehler eingetreten ist.

Die zugehörige Frage könnte dann lauten:

> *Mit welcher Wahrscheinlichkeit tritt das Unerwünschte Ereignis ein, wenn ein zu betrachtendes Basis-Ereignis eingetreten ist?*

Diese Frage kann mit der Birnbaum Importanz beantwortet werden.

Birnbaum Importanz (BI)

Die Birnbaum Importanz (BI) ist definiert als Quotient aus

- der Summe der Auftretenswahrscheinlichkeit *aller* Minimalschnitte, in denen das betrachtete Basisereignis A mit der Auftretenswahrscheinlichkeit q_A beteiligt ist, und
- der Auftretenswahrscheinlichkeit des Basisereignisses q_A selbst

$$I_A^{BI} = \frac{q_A \cdot q_B + q_A \cdot q_C + \ldots}{q_A}$$

Da der Nenner q_A größer als Null sein muss, nie aber größer als q_A sein kann (wenn im Zähler q_A als Einzelfehler steht), ist die BI definiert mit

$0 < BI \leq 1.$

Wäre die BI = 0, dann hätte das Event keinen Beitrag zum Gesamtergebnis – dann dürfte es aber auch in keinem Minimalschnitt vorkommen, der das Top Event auslösen kann, also muss gelten BI > 0. Fehler mit BI = 0 werden in der Importanzliste nicht geführt.

Ist hingegen BI = 1, dann ist das Basisereignis ein Einzelfehler, der das unerwünschte Ereignis auslösen kann. Denn dann muss im Zähler q_A als Minimalschnitt stehen (ohne weiteren Fehler, der dann eine kleinere Produktwahrscheinlichkeit zur Folge hätte) – der Nenner ist ohnehin q_A.

Anmerkung: In einigen Fällen kommt es trotz obiger Definitionen zur Ausgabe von BI > 1. Dies deutet auf Logikprobleme im Fehlerbaum hin und tritt u.a. dann auf, wenn ein und dasselbe Event Cut-Sets mit mehreren weiteren Ereignissen innerhalb eines Fehlerbaums bildet. Die Summe der Wahrscheinlichkeiten dieser Basisereignisse muss 1 überschreiten. Bei solchen Ereignissen mit hohen Wahrscheinlichkeiten handelt es sich oftmals um die Repräsentation von Diagnoseschlupf. Eine Überprüfung der Fehlerbaumlogik ist dann angebracht. Beispiel: q_A = 1E-07; q_B = 0,6; q_C = 0,7 mit den Fehlerkombinationen $q_A.q_B$ ODER $q_A.q_C$ ergäbe BI(q_A)=1,3, da $q_B + q_C = 1,3$

Basisereignisse, die eine hohe BI haben, führen mit hoher Wahrscheinlichkeit oder sogar sicher (im Falle BI = 1) zum unerwünschten Ereignis. Basic Events mit niedriger BI hingegen benötigen mindestens ein zweites oder drittes Ereignis, um das unerwünschte Ereignis auszulösen.

Folgende weitere Fragestellung lässt sich anhand der Birnbaum Importanz untersuchen:

- Welche Bedeutung haben Überwachungen im System?
  - ⇨ Die BI für das Basisereignis, das das Versagen der Überwachung definiert, liefert die Summe der Auftretenswahrscheinlichkeiten aller Fehler, die mit der Überwachung entdeckt werden können – je höher die BI desto wichtiger die Überwachung
- Welche Basisereignisse sind durch Überwachungen abgesichert?
  - ⇨ *überwachte Fehler haben eine BI zwischen 0,001 und 1 je nach Überwachungsschlupf der zugehörigen Überwachung (d.h. eine 99% wirksame Überwachung hat einen Schlupf von 1%=0,01 und diese Zahl wird dann als BI des überwachten Fehlers erscheinen)*

Anmerkung: „schlafende Fehler“ (Fehler die nur in Kombination mit seltenen Betriebszuständen wirksam werden) haben die BI in Höhe der Wahrscheinlichkeit des seltenen Betriebszustandes. Es besteht u.U. die Gefahr der Verwechslung mit überwachten Fehlern.

Beispiel 3: Auswertung eines Beispielfehlerbaums:

Der in Abbildung 4.14 gezeigte Beispielfehlerbaum wird bereits in Schritt 4: Qualitative Auswertung verwendet. Dort finden sich auch Erläuterungen zum technischen Hintergrund des Fehlerbaums.

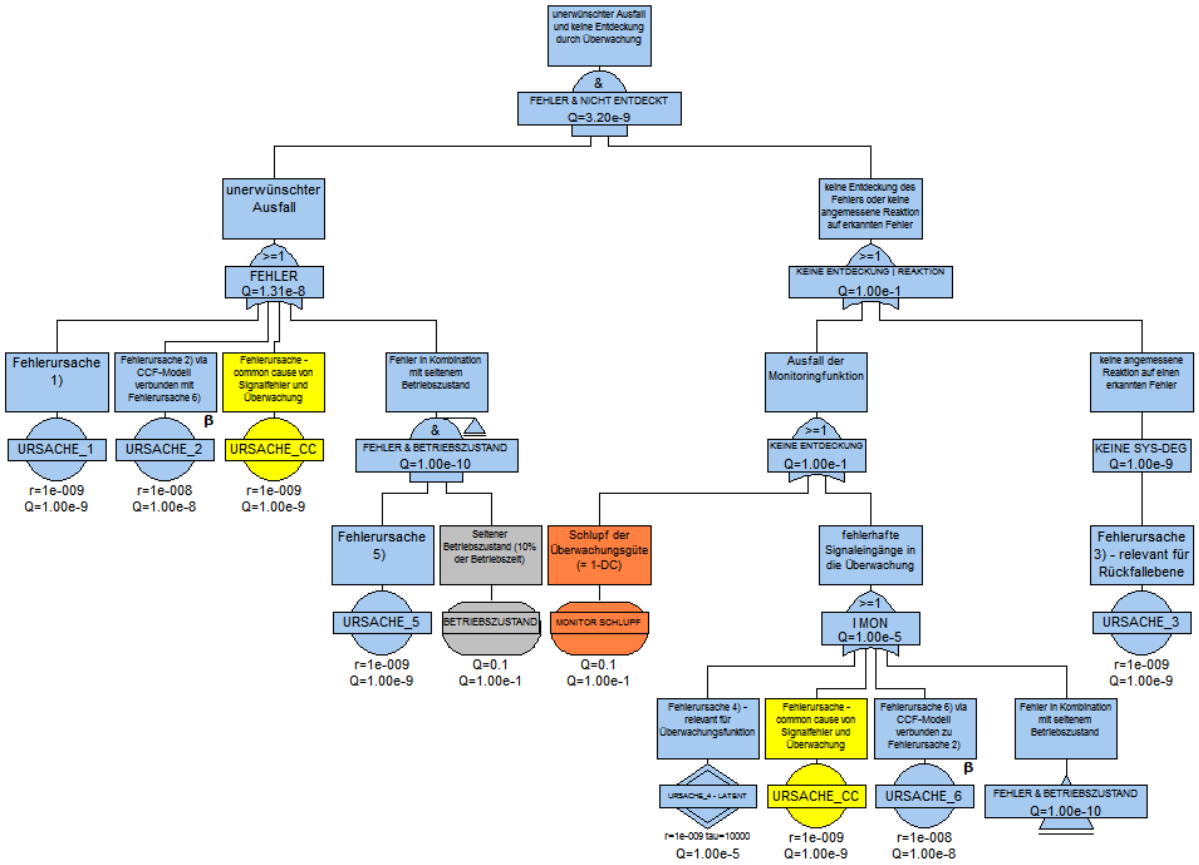


Abbildung 4.14 : Beispielfehlerbaum

Der obige Fehlerbaum liefert folgende Minimal-Schnitte für das Top Gate „FEHLER & NICHT ENTDECKT“:

No.	Cut-Set	Event Descriptions	Unavailability	Order
1	URSACHE_CC	Fehlerursache - Common Cause von Signalfehler und Überwachung	1E-09	1
2	CCF_URSACHE_2_UND_6	Common Cause Fehler Modell	1E-09	1
3	URSACHE_2. MONITOR SCHLUPF	Fehlerursache 2) via CCF-Modell verbunden mit Fehlerursache 6) Schlupf der Überwachungsgüte (= 1-DC)	1E-09	2
4	URSACHE_5. BETRIEBSZUSTAND	Fehlerursache 5) Seltener Betriebszustand (10% der Betriebszeit)	1E-10	2
5	URSACHE_1. MONITOR SCHLUPF	Fehlerursache 1) Schlupf der Überwachungsgüte (= 1-DC)	1E-10	2
6	URSACHE_2. URSACHE_4 - LATENT	Fehlerursache 2) via CCF-Modell verbunden mit Fehlerursache 6) Fehlerursache 4) - relevant für Überwachungsfunktion	5E-14	2
7	URSACHE_1. URSACHE_4 -	Fehlerursache 1)	5E-15	2

No.	Cut-Set	Event Descriptions	Unavailability	Order
	LATENT	Fehlerursache 4) - relevant für Überwachungs-funktion		
8	URSACHE_2. URSACHE_6	Fehlerursache 2) via CCF-Modell verbunden mit Fehlerursache 6) Fehlerursache 6) via CCF-Modell verbunden zu Fehlerursache 2)	1E-16	2
9	URSACHE_1. URSACHE_6	Fehlerursache 1) Fehlerursache 6) via CCF-Modell verbunden zu Fehlerursache 2)	1E-17	2
10	URSACHE_2. URSACHE_3	Fehlerursache 2) via CCF-Modell verbunden mit Fehlerursache 6) Fehlerursache 3) - relevant für Rückfallebene	1E-17	2
11	URSACHE_1. URSACHE_3	Fehlerursache 1) Fehlerursache 3) - relevant für Rückfallebene	1E-18	2

Die dazugehörige Importanzliste für das Top Gate „FEHLER & NICHT ENTDECKT“ lautet:

Name	Fussell-Vesely Importance	Birnbaum Importance
MONITOR SCHLUPF	0,343744	1,1E-08
URSACHE_2	0,31251	0,100005
URSACHE_CC	0,312495	1
CCF_URSACHE_2_UND_6	0,312495	1
URSACHE_1	0,031251	0,100005
BETRIEBSZUSTAND	0,031249	1E-09
URSACHE_5	0,031249	0,1
URSACHE_4 - LATENT	1,72E-05	1,1E-08
URSACHE_6	3,44E-08	1,1E-08
URSACHE_3	3,44E-09	1,1E-08

Bewertung der Basisereignisse anhand der Fussel-Vesely Importance (FVI)

Anhand der Importanz-Liste (sortiert nach FVI) ist erkennbar, dass es vier Basisereignisse gibt (MONITORING_SCHLUPF, URSACHE_2, URSACHE_CC CCF_URSACHE_2_UND_6), deren drei Fehlerkombinationen (siehe Cut-Set Liste) jeweils über 30 % zum Ergebnis beitragen (FVI > 0,3). Wollte man letzteres reduzieren, sollte der Fokus auf diese Fehlerursachen und ihre Fehlerkombinationen gelegt werden. In zwei Fällen handelt es sich um Common Cause Fehler für beide Teilfehlerbäume (CCF_URSACHE_2_UND_6 sowie URSACHE_CC). Diese schlagen als Einzelfehler durch – erkennbar unter anderem auch an ihren Werten für die Birnbaum Importance (BI = 1).

Drei weitere Basisereignisse tragen durch ihre Fehlerkombinationen mit jeweils ca. 3% zum Gesamtergebnis bei (URSACHE_1, BETRIEBSZUSTAND, URSACHE_5 mit FVI = 0,031251).

Schließlich gibt es noch drei Basisereignisse, deren Fehlerkombinationen nur geringen Einfluss auf das Gesamtergebnis haben. Ihre FVI ist daher sehr klein (FVI << 1). Die Optimierung dieser Ereignisse bzw. des Fehlerbaums, in dem sie wirken, ist daher keine sinnvolle Option, wenn das Gesamtergebnis gesenkt werden soll.

Bewertung der Basisereignisse anhand der Birnbaum-Importance (BI)

Die Überwachung MONITOR SCHLUPF erkennt Fehler, deren Wahrscheinlichkeit 1,1E-08 beträgt. Wenn man berücksichtigt, dass MONITOR SCHLUPF eine fixe Wahrscheinlichkeit von 0,1 hat (siehe Abbildung 4.14), sind auch die BI von URSACHE 1 und URSACHE 2 mit BI = 0,1 nachvollziehbar – denn dies sind gerade die von MONITOR SCHLUPF überwachten Fehler, von denen URSACHE 1 eine Wahrscheinlichkeit von 1E-09 und URSACHE 2 eine Wahrscheinlichkeit von 1E-08 mitbringt (nachzulesen in der Fehlerbaumdarstellung). Dass die BI für diese Ereignisse nicht exakt 0,1 (BI = 0,100005) beträgt, liegt an den Kombinationen, die diese Fehler noch mit anderen Basisereignissen bilden.

Anhand der BI lassen sich also Aussagen über die „Wichtigkeit“ einer Überwachung treffen und auch Vergleiche zwischen unterschiedlichen Überwachungen lassen sich anstellen. Liegt eine BI einer Überwachung z.B. im Bereich einer Doppelfehlerwahrscheinlichkeit (typ. Für ISO26262-Anwendung Q < 1E-12) so kann hinterfragt werden, ob diese Überwachung zur Absicherung gegen Einzelfehler benötigt wird – allerdings sollte dabei ihre etwaig vorhandene Wirkung gegen latent auftretende Fehler nicht außer Acht gelassen werden.

Der schlafende Fehler ist URSACHE 5, dessen BI von 0,1 genau der fixen Wahrscheinlichkeit von BETRIEBSZUSTAND entspricht.

Tritt der latente Fehler URSACHE 4) – LATENT ein, folgt das unerwünschte Ereignis FEHLER & NICHT ENTDECKT mit einer Wahrscheinlichkeit von 1.1E-08 (URSACHE 1 mit Q=1.0E-09 *oder* noch eintreten).

Weitere Importanzen:

Weitere vom Fault Tree Tool FT+ angebotene Importanzen (Barlow-Proschan, Sequential Importance) spielen nur in Zusammenhang mit sequentiell auftretenden Fehlern eine Rolle und werden hier nicht weiter behandelt.

4.8. Schritt 7: Festlegung Handlungsbedarf, Maßnahmen, Erfolgskontrolle

Nach Durchführung der qualitativen bzw. quantitativen Auswertung des Fehlerbaums kann anhand der Ergebnisse entschieden werden, ob und in welchem Rahmen Handlungsbedarf besteht.

Die vorher bestimmten Zielgrößen der Analyse sollten in diesem Schritt wieder herangezogen werden.

Beispielsweise kann die Auswertung des Fehlerbaums zeigen, dass es Einzelfehler gibt, die direkt zum Top Event führen, oder dass die Auftretenswahrscheinlichkeit des Top Events höher ist als es zur Einhaltung des Sicherheitsziels gefordert ist.

In diesen Fällen kann es notwendig sein, geeignete Maßnahmen zu definieren, um eben diese Ziele der FTA zu erreichen.

Die eigentliche Entscheidung wird dabei vom Auftraggeber getroffen.

Der FTA-Moderator kann bei der Interpretation der Ergebnisse unterstützen, das FTA-Team steht ihm dabei beratend zur Seite und kann bei der Maßnahmendefinition und –umsetzung helfen.

Zur Interpretation der Cut-Set Listen und Importanzlisten siehe auch Schritt 6 (quantitative Auswertung).

Beispiele für mögliche Maßnahmen:

- Nutzung von *Komponenten mit reduzierter Fehlerrate* (=> führt zu einer anderen Bedatung des Basisereignisses)
- *Einführung von Redundanzen*, die das betreffende Basisereignis zum Mehrfachfehler machen (=> nimmt Einfluss auf die Architektur und verlagert das Basisereignis in einen Mehrfachfehler => Wirksamkeit besser als bei Einführung einer Überwachung)
- *Einführung von Überwachungen*, die die Fehlerrate, mit der ein Basisereignis auf das unerwünschte Ereignis durchschlägt, reduzieren (überführt einen Einzelfehler in einen überwachten Fehler => Wirksamkeit abhängig von der Güte der Überwachung)
- *Überprüfung der spezifizierten Einsatzbedingungen (z.B. Temperatur,…)* (=> Einfluss auf Fehlerraten bereits eingesetzter Komponenten und Überwachungen möglich)
- *Detaillierung der Analyse zur Überprüfung des Einzelfehlerstatus* (eine Analyse im Detail kann bislang durch Vereinfachung unberücksichtigte Sicherheitsmaßnahmen zur Geltung bringen, z.B. Überwachungen oder Redundanzen in einer Subkomponente)
- *Feldmaßnahmen*

Erfolgskontrolle

Sollte die Wahrscheinlichkeit des Top Events reduziert werden, kann eine Erfolgskontrolle der angewendeten Maßnahmen bei der präventiven FTA durch eine erneute Berechnung der Auftretenswahrscheinlichkeit des Top Events erfolgen.

Sollte die Anzahl der Einzelfehler reduziert werden kann zur Überprüfung der Maßnahmen die Cut-Set Liste herangezogen werden.

Bei der korrektiven Anwendung der FTA (Implementierung der daraus abgeleiteten Maßnahmen) ergibt sich eine Erfolgskontrolle durch das Ausbleiben des Fehlerzustandes, z.B. keine weiteren Feldausfälle.

4.9. Schritt 8: Freigabe und Dokumentation der FTA

Eine detaillierte Dokumentation der Ergebnisse einer FTA ist unerlässlich, da das FTA-Diagramm alleine in der Regel nicht alle Informationen enthält (oder anzeigt), die für das Verständnis oder die Bewertung notwendig sind. Eine bloße Abspeicherung der FTA-Datei erfüllt diesen Zweck in der Regel nicht. Hinzu kommt, dass durch eine wechselnde Teamzusammensetzung Wissensträger des Projekts zu einem späteren Zeitpunkt nicht mehr zur Verfügung stehen. Zudem bildet der FTA-Bericht die Grundlage für einen möglichen Unterschriftenumlauf, der – vergleichbar einem FMEA-Unterschriftenumlauf – mittels „eSignature“ durchgeführt werden kann.

Aufgrund der Verschiedenartigkeit der einzelnen Fehlerbaumzustandsanalysen in Umfang, Betrachtungstiefe, usw. kann es keine feste Vorgabe für die Gestaltung des FTA-Berichts geben. Aus diesem Grund kann in diesem Dokument nur eine Empfehlung gegeben werden.

Es ist grundsätzlich zu beachten, dass eine FTA und damit auch der zugehörige Bericht schützenswerte Informationen enthalten kann. Bei einer Übergabe an externe Stellen (z.B. Kunde) sind daher die „Regelungen der Kundenkommunikation zu Ergebnissen von Qualitätsmanagement-Methoden“ (Zentralanweisung Vertrieb & Marketing „R05“) in seiner jeweils aktuellen Ausgabe zu beachten.

Eine bewährte Gliederung sieht wie folgt aus:

- Zusammenfassung der Ergebnisse (vergleichbar mit dem Deckblatt einer FMEA):
    - Überblick über die Aufgabe (z.B. Top Events)
    - beteiligte Personen
    - Detaillierte Auflistung der Ergebnisse (Ziel-/Ist-Vergleich) für jedes einzelne Top Event (inkl. der Bewertung durch Experten):
    - Name / Beschreibung
    - Zielwerte / ermittelte Werte
    - Top-Fehlerursachen (z.B. anhand einer Cut-Sets-Analyse)
    - Auflistung der getroffenen Annahmen (z.B. Eingrenzung des Betrachtungsumfangs, Definition der „sicheren Zustände“)
    - Angabe zur verwendeten Datenbasis (z.B. Randbedingungen, Quellen der Ausfallraten, Annahmen zur Güte von Überwachungen)
    - Auflistung der angefügten Anlage

- Liste der empfohlenen Anhänge:
    - Liste der in der FTA definierten Gates
      (inkl. Bemerkungen; kann aus FT+ exportiert werden)
    - Liste der in der FTA definierten Events
      (inkl. Bemerkungen zur Herleitung der Ausfallraten bzw. Datenquelle; kann aus FT+ exportiert werden)

- Ausdruck des Fehlzustandsbaums (FTA-Diagramm)
- Ausdruck einer evtl. geführten „Offene-Punkte-Liste“
- Ausdruck einer Termin- / Anwesenheits- / Teilnehmerliste
- Blockschaltbilder / Diagramme / Grafiken / Foliensätze, die zum Systemverständnis beitragen

Ein Beispiel für einen solchen Bericht auf Basis der Bosch-eForms-Vorlage „Bericht“ befindet sich in der *„Anhang 2 – Beispiel Report“*

5. Literatur zur FTA

Normen, Richtlinien, Handbücher

5.1. Normen

[5.1.1] DIN 25424-1, Fehlerbaumanalyse – Methode und Bildzeichen (Deutsche Norm)

Deutsches Institut für Normung, Sep. 1981, Beuth Verlag GmbH, Berlin

[5.1.2] DIN 25424-2, Fehlerbaumanalyse – Handrechenverfahren zur Auswertung eines Fehlerbaumes (Deutsche Norm)

Deutsches Institut für Normung, April 1990, Beuth Verlag GmbH, Berlin

[5.1.3] DIN EN 61025 Fehlzustandsbaumanalyse (Deutsche Version der europ. Norm EN 61025)

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, August 2007, Beuth Verlag GmbH, 10772 Berlin

[5.1.4] ISO 26262 Straßenfahrzeuge – Funktionale Sicherheit (Teil 1 - 10)

Internationale Organisation für Normung, November 2011, Genf (Schweiz)

[5.1.5] SN 29500, Ausfallraten Bauelemente (Teil 1-16) (Siemens Norm)

Siemens AG, 2004-2014, München und Erlangen

5.2. Standards

[5.2.1] Qualitätsmanagement in der Automobilindustrie, Band 4, Kapitel 4, Fehlerbaumanalyse

VDA, Verband der Automobilindustrie e.V., Oberursel, Deutschland (2003)

5.3. Handbücher

[5.3.1] Fault Tree Handbook, NUREG-0492 (US-Standard)

D. F. Haasl et al., U.S. Nuclear Regulatory Commission, Washington, USA (1981)

[5.3.2] Fault Tree Analysis Application Guide (international standard)

D. J. Mahar et al., Reliability Analysis Center, Rome, USA (1990)

[5.3.3] Fault Tree Handbook with Aerospace Applications (Aerospace industry)

W. Vesely et al., NASA Office of Safety and Mission Assurance, Washington, USA (2002)

[5.3.4] IEC TR 62380, Reliabilty Data Handbook (Internationaler Standard)

(Ermittlung von Zuverlässigkeitsdaten, die für die Berechnung der FTA benötigt werden)

Internat. Electrotechnical Commission, Geneve, Switzerland (2004)

[5.3.5] Reliability Engineering: Theory and Practice

Alessandro Birolini, ISBN: 3-642-39534-1, Springer Verlag, 2014 (7th edition)

5.4. Fachbücher

[5.4.1] Die Fehlerbaum-Methode

W. Schneeweiss, ISBN 3-934447-02-3, LiLoLe Verlag, Hagen, Germany (1999)

[5.4.2] Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik

(Darstellung unterschiedlicher Methoden und Techniken der Zuverlässigkeits- und Sicherheitstechnik)
A. Meyna, B. Pauli et al., ISBN 3-446-21594-8, Carl Hanser Verlag, München – Wien (2003)

6. Glossar

Ausfall	Beendigung der Fähigkeit einer Betrachtungseinheit, eine geforderte Funktion zu erfüllen. Anmerkung: Bei komplexen Systemen wird „Ausfall“ als Synonym für „Versagen“ verwendet. (DIN 40 041-3)
Betriebszustand	Der Arbeitspunkt, auch Betriebspunkt oder -zustand genannt, ist ein bestimmter Punkt im Kennfeld, der Kennlinie eines technischen Gerätes oder Systems, der aufgrund der Systemeigenschaften und einwirkenden äußeren Einflüsse und Parameter eingenommen wird.
CCF	Common Cause Failure
Common Cause	Gemeinsame Fehlerursache innerhalb von Komponenten, die innerhalb eines Systems eigentlich als unabhängig gesehen werden und eine Redundanz bilden. Der Common Cause überwindet diese Redundanz. Bsp.: Fehler einer gemeinsamen Spannungsversorgung zweier unabhängiger Sensoren
Cut-Set-Analyse	Ist eine Auswertung des Fehlerbaums und liefert eine Liste Minimalschnitte des Fehlerbaums.
Diagnosedeckung/ Diagnosedeckungsgrad	Anteil der Gesamtfehlerrate einer Fehlerursache, die entdeckt oder kontrolliert ist. (englisch Diagnostic Coverage)
DRBFM	Design Review Based on Failure Modes
ECU	Electronic Control Unit, Steuergerät
E-Gas	Elektronisches Gaspedal
et al.	**et al.** bedeutet wortwörtlich „und andere“.
Fehlzustand	Nichterfüllung mindestens einer Anforderung an ein erforderliches Merkmal einer Betrachtungseinheit. (VDI/VDE 3542)
FHA	Functional Hazard Analysis
FIT	**Failure In Time** Für technische Systeme wird die Ausfallrate üblicherweise in FIT angegeben. 1 FIT = $1 \cdot 10^{-9}$ Ausfälle pro Stunde
FMEA	Fehler-Möglichkeits- und Einfluss-Analyse
FMEDA	Failure Modes Effects and Diagnostic Analysis

G&R	Gefahren- & Risikoanalyse (im engl. unter H&R nach ISO 26262 bekannt)
H&R	Hazard Analysis & Risk Assessment
Importanz	Einfluss bestimmter Ursachen = Basis-Ereignisse auf die Sicherheit, Zuverlässigkeit, Eintrittswahrscheinlichkeit oder Verfügbarkeit des betrachteten Top Events
Kritisches Ereignis	Kritische Ereignisse können Minimalschnitte sein oder anderweitige im Rahmen der Systemanalyse definierte Ereignisse, die einem besonderen Betrachtungsfokus unterliegen. Die Priorisierung kann z.B. anhand der Eintrittswahrscheinlichkeiten oder durch Festlegung auf singuläre Ereignisse erfolgen.
Kritischer Pfad	Kritische Pfade dienen zur Visualisierung / Ausweisung der Kausalkette vom Top Event hin zu einem Ereignis / Ereigniskombination, welches als kritisch eingestuft wird.
Minimalschnitt	**Minimalschnitt nach EN 61025** Kleinste Ereignismenge, die für den Eintritt des Hauptereignisses erforderlich ist. **Minimal Cut-Set** Die Fehlerbaum-Struktur stellt den funktionalen Zusammenhang des Top Events über die logischen Verknüpfungen hin zu den Basisereignissen dar. Die logischen Verknüpfungen führen zur Bildung von Teilmengen von Ereignissen, bei deren Eintreten das Top Event herbeigeführt wird bzw. die Betrachtungseinheit (z.B. System) ausfällt. Diese nennt man Schnitte. Die kleinste gemeinsame Menge von Basisereignissen bildet einen **Minimalschnitt**, wenn sie keinen anderen Schnitt als echte Teilmenge enthält. Die Summe aller Minimalschnitte beschreibt das Ausfallverhalten der Fehlerbaum-Struktur vollständig. Die kleinste Menge an Elementen des Minimalschnittes kann ein Ereignis darstellen. Die maximale Menge der Elemente des Minimalschnittes und Anzahl der Minimalschnitte wird durch die logischen Verknüpfungen der Fehlerbaum-Struktur bestimmt.
MPF	Multiple-Point Fault (Bezeichnung aus dem Kontext ISO26262): Fehler, der, solange er alleine auftritt, nicht unmittelbar zur Verletzung eines Sicherheitsziels bzw. zum Eintritt des unerwünschten Ereignisses führt. Hierfür ist ein Zweitfehler erforderlich.
OEM	Original Equipment Manufacture; in dieser Schrift ist somit Fahrzeughersteller gemeint

PHA	Preliminary Hazard Analysis
ppm	**parts per million** Verhältnis der Fehler bezogen auf 1 Million Teile. 100 ppm bedeuten 100 Fehler/1 Million Teile. Das entspricht 0,01 % Fehler.
QFD	Quality-Function-Deployment bzw. Qualitätsfunktionendarstellung
RAMS	**R**: Reliability (Zuverlässigkeit) **A**: Availability (Verfügbarkeit) **M**: Maintenance (Wartbarkeit) **S**: Safety (Sicherheit)
Redundanz	Vorhandensein von mehr funktionsfähigen Mittel in einer Einheit, als für die Erfüllung der geforderten Funktion notwendig sind. Anmerkung 1: Wieviele Mittel ohne Redunanz notwendig sind, hängt vom Einzelfall ab. Anmerkung 2: Die Aufrechterhaltung der Redundanz erfordert Instandhaltung, d.h. die Überwachung, die Erhaltung und bei Versagen die Wiederherstellung der Funktionsfähigkeit aller Mittel. (DIN 40 041) **In Fall dieser Schrift:** Redundanz ist das zusätzliche Vorhandensein funktional gleicher oder vergleichbarer Ressourcen eines technischen Systems, wenn diese bei einem störungsfreien Betrieb im Normalfall nicht benötigt werden. (Quelle: Wikipedia)
RF	Residual Fault (Bezeichnung aus dem Kontext ISO26262) = Restfehler eines Single Point Faults, der nach Berücksichtigung von Sicherheitsmechanismen (Überwachungen) zur Verletzung von Sicherheitszielen bzw. zum Eintritt des unerwünschten Ereignisses führt.
RWB	Reliability Work Bench (ISOGRAPH SW); Nachfolger von FT+
Sensitivitätsanalyse	Methodik, mit der bewertet werden kann, wie empfindlich Kennzahlen auf kleine Änderungen von Eingangsparametern reagieren.
SPF	Single Point Fault (Bezeichnung aus dem Kontext ISO26262) = Fehler, der direkt und ohne Sicherheitsmechanismus zur Verletzung von Sicherheitszielen bzw. zum Eintritt des unerwünschten Ereignisses führt
TKU	Technische Kunden-Unterlage(n)
VDA	Verband der Automobilindustrie e.V.
ZKG	Zuverlässigkeitskenngrößen

8D-Report	Ein **8D-Report** ist ein Dokument, das im Rahmen des Qualitätsmanagements bei einer Reklamation zwischen Lieferant und Kunde ausgetauscht wird. **8D** steht dabei für die **acht** obligatorischen **Disziplinen** (Prozessschritte), die bei der Abarbeitung einer Reklamation erforderlich sind, um das zu Grunde liegende Problem zu überwinden. Im 8D-Report werden die Art der Beanstandung, Verantwortlichkeiten und Maßnahmen zum Beheben des Mangels festgeschrieben. Der 8D-Report ist u. a. durch den Verband der Automobilindustrie standardisiert.

7. Anhang 1 Symbole und Modellierungsempfehlungen

7.1. Varianten-Handling

Zur Darstellung von Varianten können Teilbäume über logische Schalter aktiviert oder deaktiviert werden. Das Tool FaultTree+ bietet dazu das Event Symbol „House“ an.

Varianten-Handling für einen ergänzenden Zweig

Abbildung 16 zeigt beispielhaft einen per Schalter „SW ZUSATZFUNKTION“ aktivierbaren Zweig.

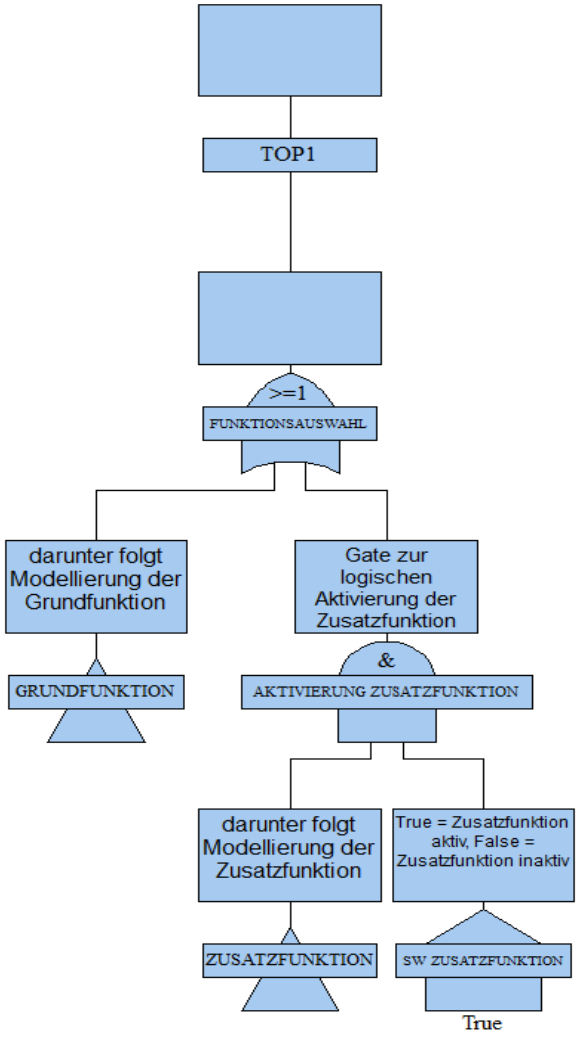


Abbildung 7.1: Varianten-Handling für einen ergänzenden Zweig

Varianten-Handling sich ausschließender Optionen

Abbildung 7.2 zeigt beispielhaft einen logischen „Entweder-Oder-Schalter“ für die Funktionen 1 und 2.

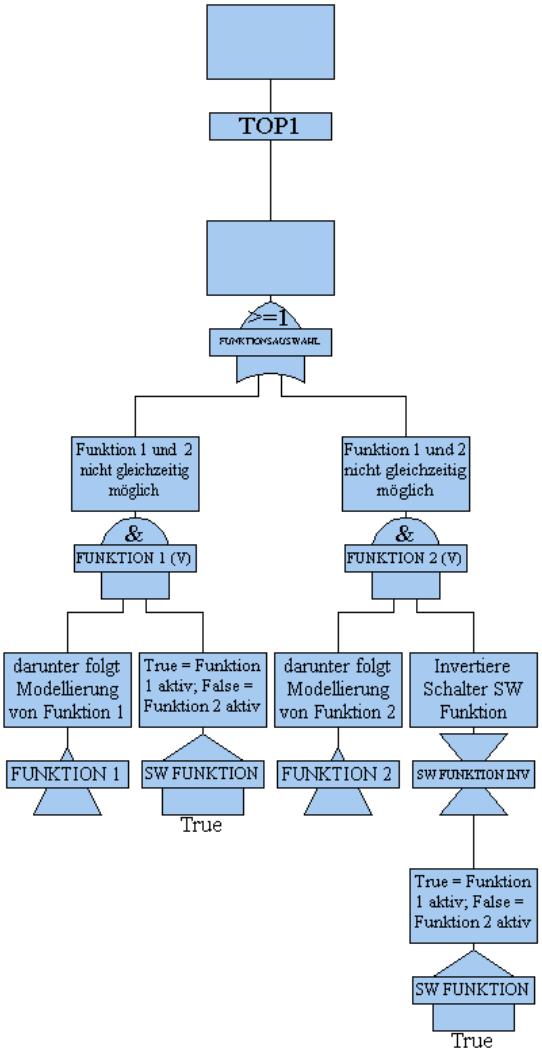


Abbildung 7.2: Varianten-Handling sich ausschließender Optionen

7.2. Modellierung von Applikationsrandbedingungen:

Oftmals sind Funktionen nur unter ganz bestimmten Randbedingungen aktiv (z.B. Warnungen an Fahrer nur, wenn Fahrzeug in Bewegung) oder Störungen treten nur bei speziellen Fahrbedingungen auf (z.B. Schlechtwegstrecke). Diese Spezialfälle werden modelliert durch eine UND-Verknüpfung mit einer Bedingung(= „conditional event“). Ist die Wahrscheinlichkeit des Eintretens des Spezialfalles zeitlich konstant, wird das conditional event mit einer konstanten Wahrscheinlichkeit (Q) modelliert.

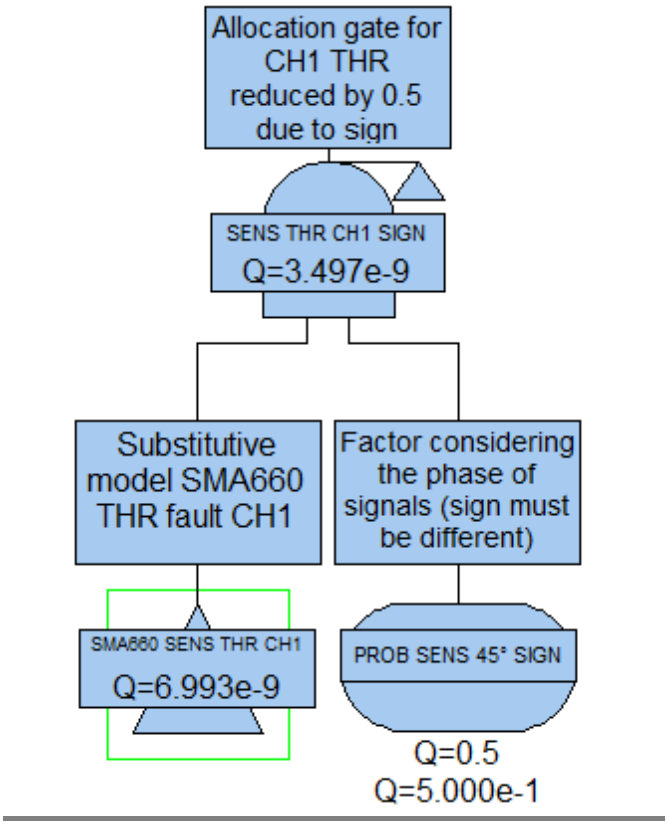


Abbildung 7.3: Modellierung von Applikationsrandbedingungen

Im obigen Beispiel wird die Wahrscheinlichkeit für gleiches bzw. verschiedenes Vorzeichen eines Signals (je 50%) durch das oval abgebildete conditional event mit Q=0,5 modelliert.

7.3. Spezielle Tipps bzgl. Fehlerbaumerstellung zum Nachweis nach ISO26262

Die ISO26262 legt den Einsatz der FTA nahe.

- Eine qualitative FTA zur Identifikation von systematischen Fehlern (ISO26262-4) – hierbei sollten *alle* Fehlertypen (mechanisch, elektrisch, Software) berücksichtigt werden (die ISO26262 macht in Band 4 keine Aussage bezüglich Einschränkung der Analyse auf rein elektrische Fehler)
- Eine quantitative FTA zum Nachweis der Hardware-Metriken (ISO26262-5) – dabei sollen nur die zufällig auftretenden *elektrischen* Hardwarefehler berücksichtigt werden

Beiden, sich im Grunde widersprechenden, Anforderungen kann durch eine angemessene Bedatung der entsprechenden Basis-Ereignisse begegnet werden. Durch eine entsprechende gering gewählte Fehlerrate für mechanische Fehler bzw. Software-Implementierungsfehler lässt sich ihr Einfluss so steuern, dass sie einerseits in den Ergebnislisten (Cut-Sets) ausgewiesen werden können, andererseits aber keinen *signifikanten* Einfluss auf die Höhe der Hardware-Metriken nehmen. Zur besseren Unterscheidung der Zusammensetzung des Rechenergebnisses, können unterschiedliche Fehlerraten für die verschiedenen Fehlertypen eingetragen werden.

Bewährt hat sich folgende Bedatung:

- Mechanische Fehler: Datenmodel „Rate“ mit l = 1E-15 1/h
  (Die resultierende Wahrscheinlichkeit des mechanischen Einzelfehlers ist größer als die eines elektrischen Doppelfehlers → der mechanische Einzelfehler fällt in einer Cut-Set-Liste auf)

- Software Implementierungsfehler: Datenmodell „Fixed“ mit r = 1E-12 1/h (Das Datenmodell „Fixed“ wird gewählt, weil die Wahrscheinlichkeit eines Softwarefehlers über der Zeit konstant bleibt.

Diese Bedatung ist nur im Kontext der ISO26262 sinnvoll. Sie ist bewusst so gewählt und hat keinerlei Bezug zu etwaigen Felddaten!

7.4. Modellierung von Überwachungen (Monitoren)

Bei der quantitativen Modellierung typischer elektrisch-elektronischer Systeme tritt häufig folgende Problemstellung auf: Ein Hardware-Element ist von einem anderen Element überwacht. Die Überwachung (der Monitor) ist aber nicht perfekt (Diagnosedeckungsgrad DC < 100%), außerdem kann die Überwachungsschaltung selbst ausfallen, bzw. die von dem Monitor ausgelöste vorgesehene Systemreaktion fehlschlagen.

Eine mögliche Modellierung im Fehlerbaum muss daher berücksichtigen:

- den zu entdeckenden Fehler
- den Diagnosedeckungsgrad der Überwachung (modelliert mittels eines fixen Werts)
- die eventuell von der Überwachung genutzten Vergleichssignale
- die von der Überwachung ausgelöste Systemreaktion, die in den sicheren Zustand führt

Modellierung einer in Hardware implementierten Überwachung

➔ Modellierungs-Prinzip

Monitorfunktion wird für die HW-Metriken nur ausgewertet, wenn sie innerhalb der Fehlertoleranzzeit wirksam sind.

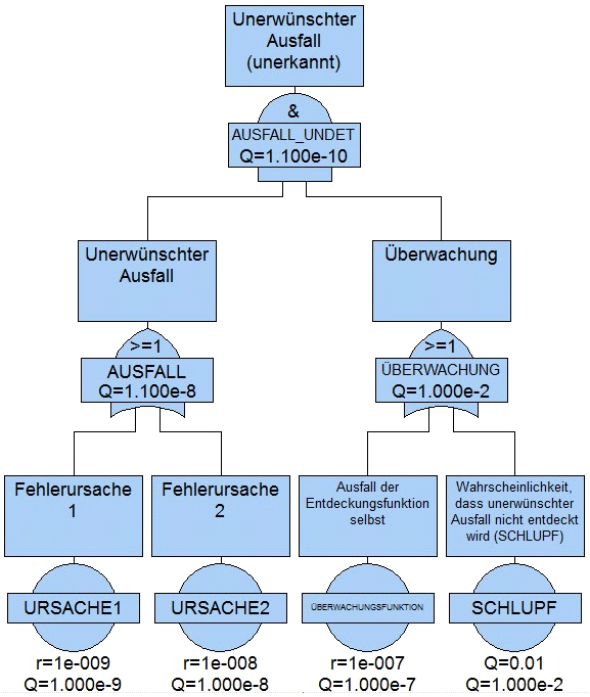


Abbildung 7.4: Modellierung einer in Hardware implementierten Überwachung

Modellierung einer „modellbasierten“ Überwachung, für die Software erforderlich sein kann. Die Aufgabe der Überwachung ist der Vergleich eines zu überwachenden Signals (URSACHE_1 und URSACHE_2) mit einem Referenzsignal (URSACHE_4).

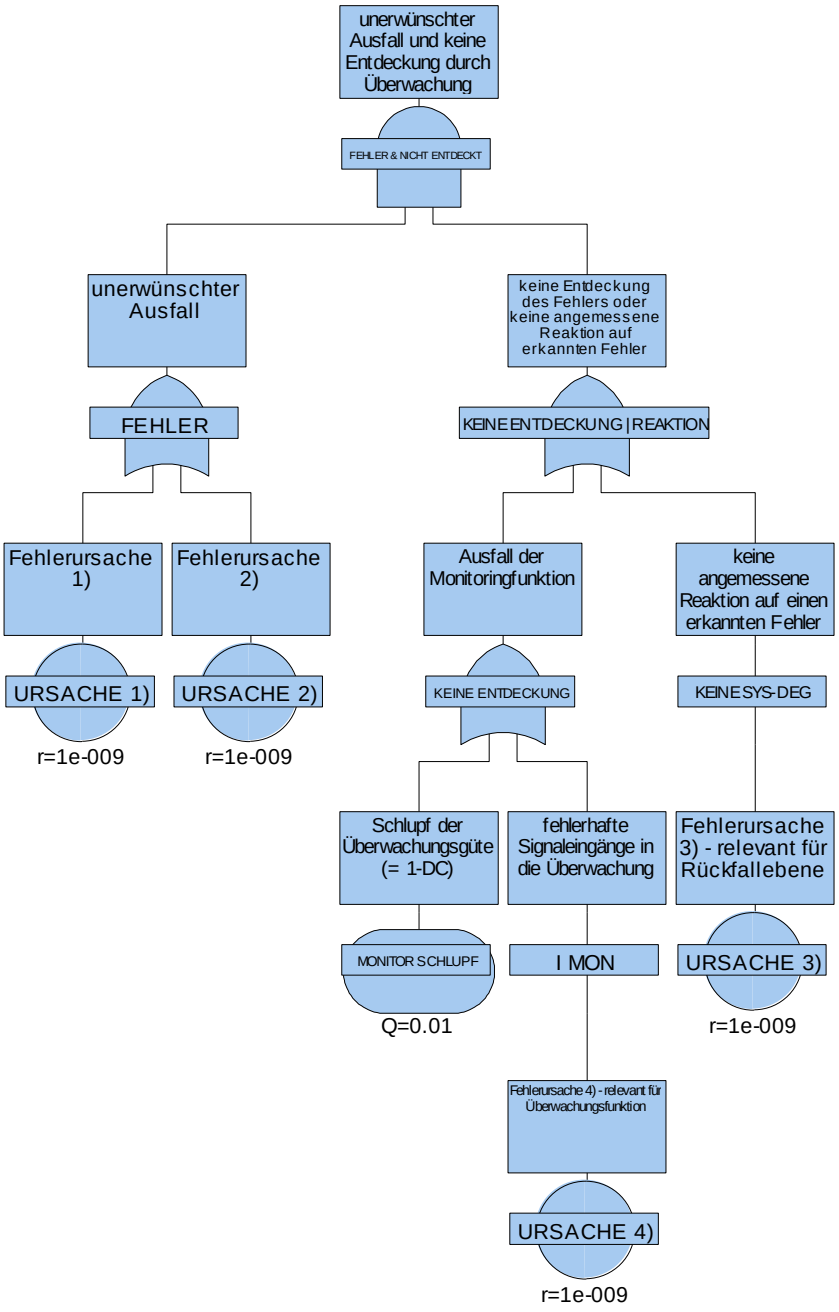
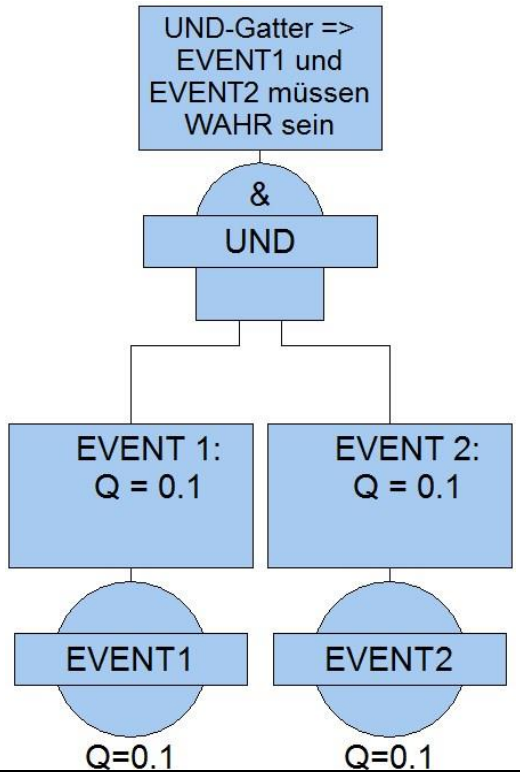
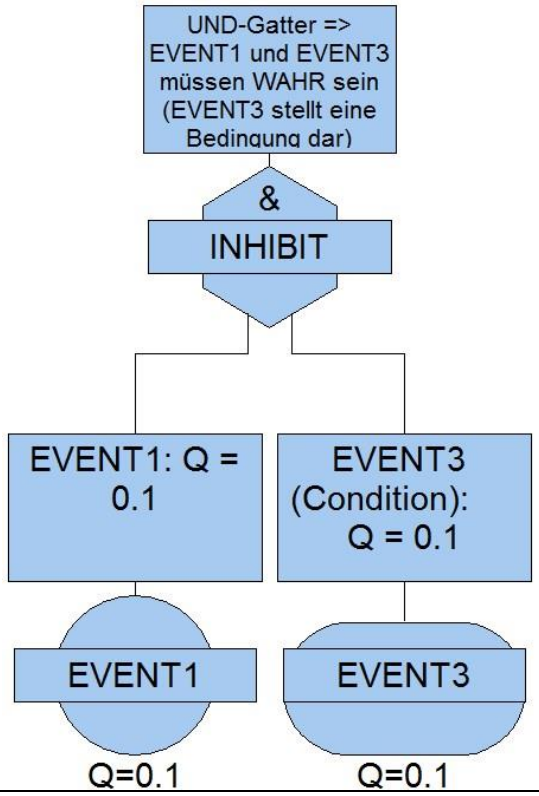
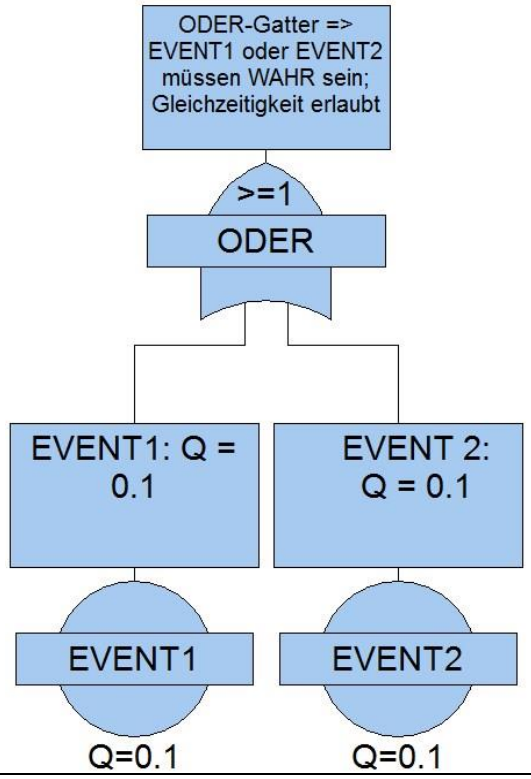
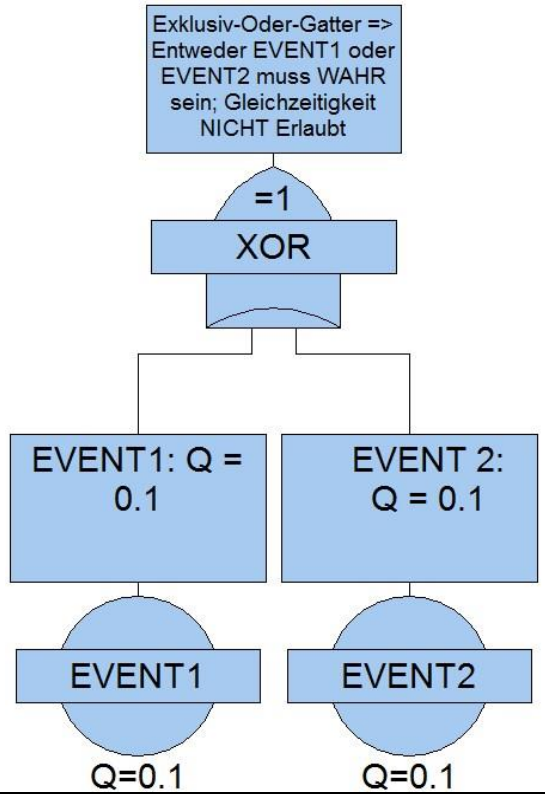


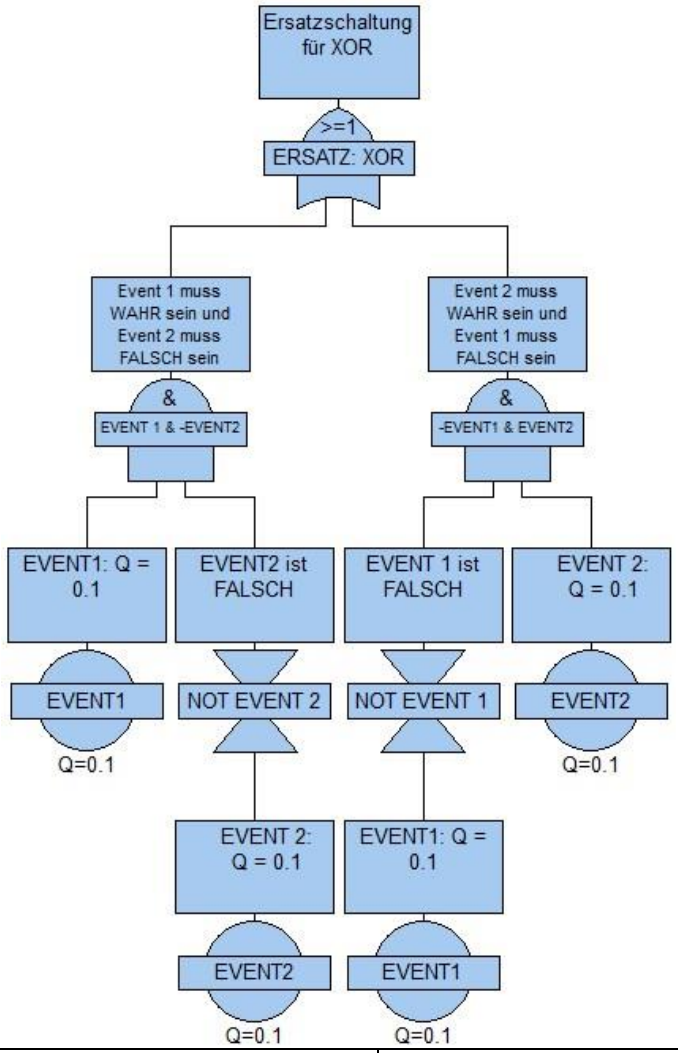
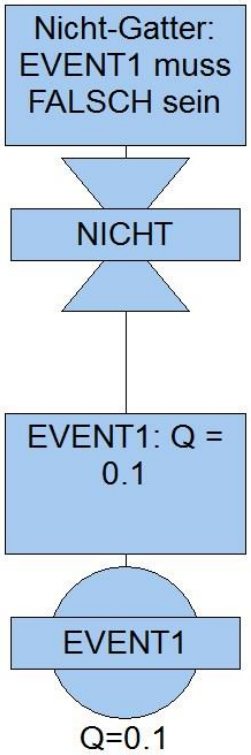
Abbildung 7.5: Modellierung einer in Software implementierten Überwachung

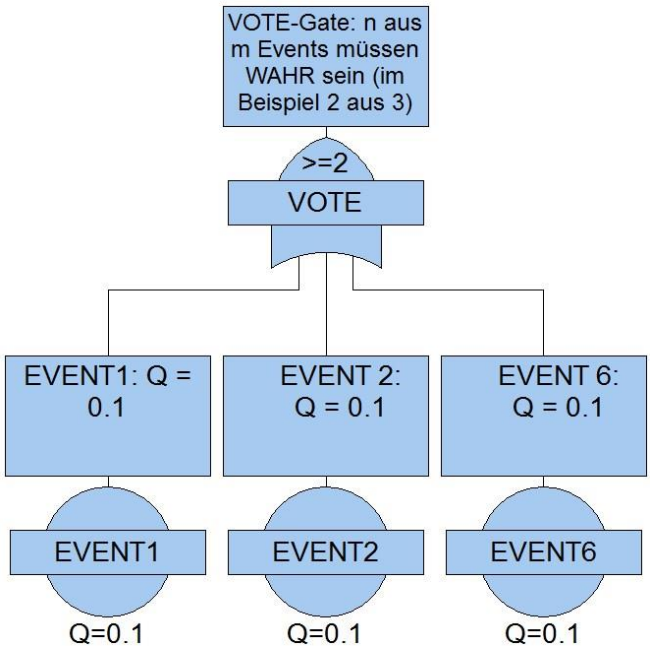
7.5. Übersicht der Event- und Gattertypen im Tool FaultTree +

7.5.1. Verfügbare Gattertypen

Typ	Symbol	Bemerkung
UND-Gatter		• Alle Eingänge müssen WAHR sein. • A ∧ B • Cut-Set List: EVENT1.EVENT2 • Berechnung von Q $Q = q_A * q_B$ • Im Beispiel Q = 0,1 * 0,1 = 0,01 • Anmerkung: FaultTree+ limitiert die maximale Anzahl von Eingängen auf 18
Inhibit		• Alle Eingänge müssen WAHR sein – ein Eingang repräsentiert eine Bedingung • A ∧ B • Cut-Set List: EVENT1.EVENT3 • Berechnung von Q $Q = q_A * q_B$ • Im Beispiel Q = 0,1 * 0,1 = 0,01 • Anmerkung: FaultTree+ limitiert die maximale Anzahl von Eingängen auf 18

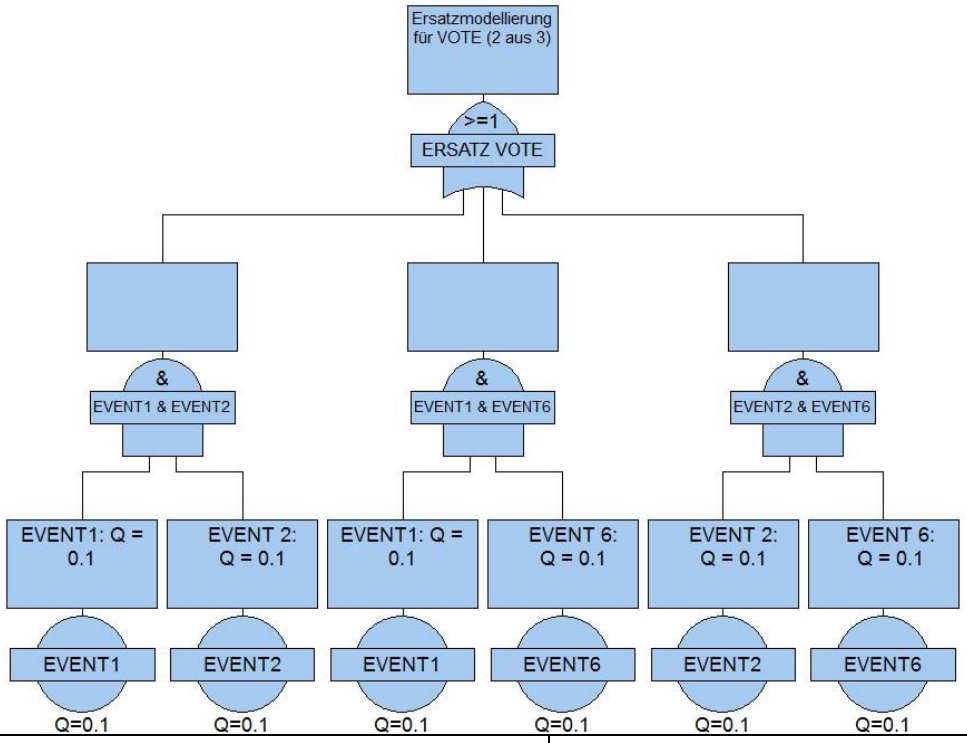
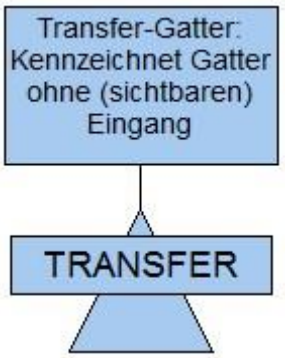
Typ	Symbol	Bemerkung
ODER-Gatter		• Ein Eingang muss WAHR sein • A ∨ B • Cut-Set List: EVENT1 EVENT2 • Berechnung von Q (Summenregel) $Q = q_A+q_B - q_A*q_B$ • Im Beispiel Q = 0,1 + 0,1 – (0,1*0,1) = 0,2 – 0,01 = 0,19 • Anmerkung: FaultTree+ limitiert die maximale Anzahl von Eingängen auf 18
Exklusiv-ODER-Gatter		• Nur ein Eingang darf WAHR sein, der andere muss FALSCH sein • (-A∧B)∨(A∧-B) • Cut-Set List: -EVENT1.EVENT2 EVENT1.-EVENT2 • Berechnung von Q Q = $(1-q_A)*q_B + (1-q_B)*q_A – 0$ *da (-EVENT1.EVENT2) * (EVENT1.-EVENT2) = 0* • Im Beispiel: Q = (1-0,1)*0,1 + (1-0,1)*0,1 = 0,9*0,1 + 0,9*0,1 =0,09 + 0,09 = 0,18

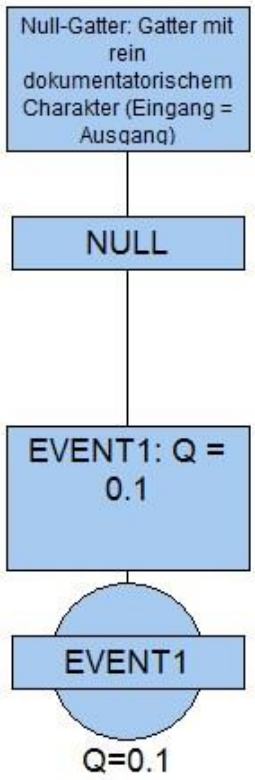
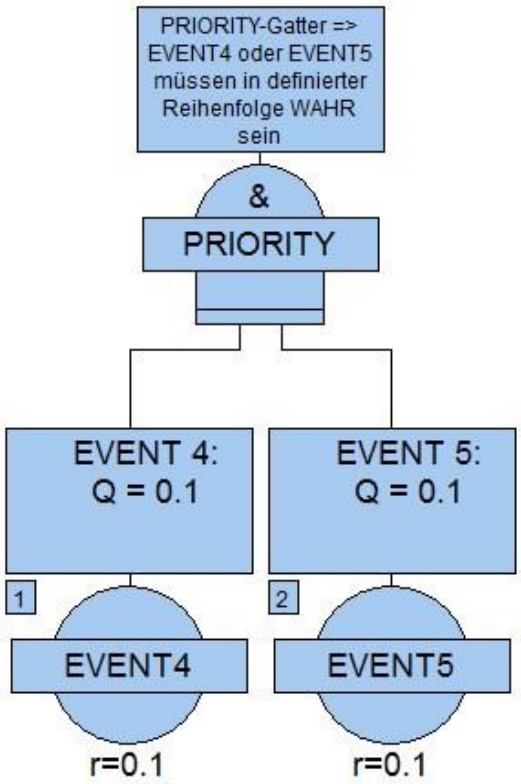
Typ	Symbol	Bemerkung
Ersatz-schaltbild XOR		
Nicht-Gatter		• Der Eingang muss FALSCH sein • -A • Cut-Set List: -EVENT1 • Berechnung von Q $Q = (1-q_A)$ • Im Beispiel: Q = 1 – 0,1 = 0,9

Typ	Symbol	Bemerkung
Vote-Gatter (n aus m)		

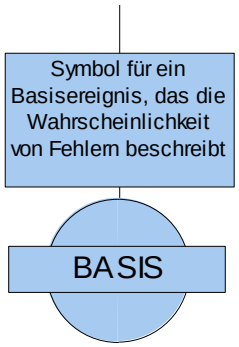
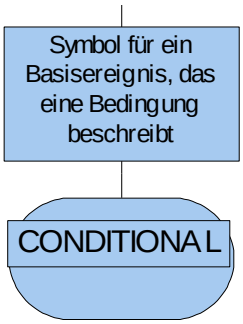
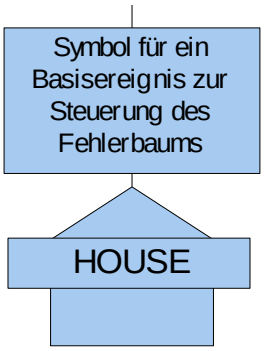
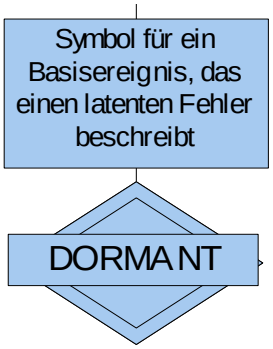
Bemerkung:

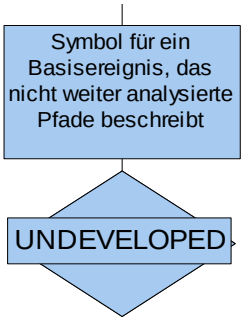
- n von m Eingängen müssen WAHR sein.
  Hier: 2 von 3 Eingängen...
- $(A \wedge B) \vee (A \wedge C) \vee (B \wedge C)$
- Cut-Set List:
  EVENT1.EVENT2
  EVENT1.EVENT6
  EVENT2.EVENT6
- Berechnung von Q (Summenregel)
  $Q = q_A*q_B + q_A*q_C + q_B*q_C$
  $- [(q_A*q_B)*(q_A*q_C) + (q_A*q_B)*(q_B*q_C) + (q_B*q_C)*(q_A*q_C)]$
  $+ (q_A*q_B)*(q_A*q_C)*(q_B*q_C)$
  $= q_A*q_B + q_A*q_C + q_B*q_C - [(q_A*q_B*q_C) + (q_A*q_B*q_C) + (q_B*q_C*q_A)]$
  $+ (q_A*q_B*q_C)$
- Im Beispiel ist...
  $q_x*q_y = 0{,}01$
  $q_x*q_y*q_z = 0{,}001$
- Also:
  $Q = 0{,}01 + 0{,}01 + 0{,}01 - [0{,}001 + 0{,}001 + 0{,}001] + 0{,}001$
  $= 0{,}03 - 0{,}003 + 0{,}001$
  $= 0{,}028$
- Anmerkung: FaultTree+ limitiert die maximale Anzahl von Eingängen auf 18

Typ	Symbol	Bemerkung
Ersatzschaltbild VOTE (2 aus 3)		
Transfer-Gatter		• Gatter hat keine oder keine sichtbaren Eingänge • Kennzeichnet Gatter, bei denen die Eingänge noch nicht definiert sind, oder die als Top Gate einer neuen Seite im Fault-Tree+ definiert sind • Transfer-Gatter ohne definierten Eingang können in FaultTree+ über den Befehl „Verify Data“ angezeigt werden.

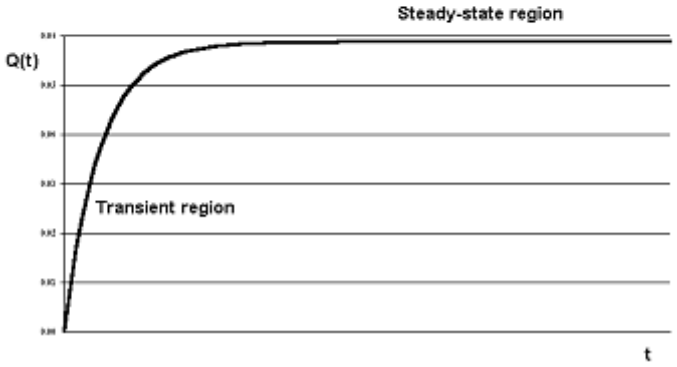
Typ	Symbol	Bemerkung
Null-Gatter		• Gatter hat keine Logikfunktion • A = A • Cut-Set List EVENT1 • Berechnung von Q: • Im Beispiel: $Q = q_A$ • Nullgatter können zu dokumentatorischen Zwecken benutzt werden (z.B. Dokumentation der Änderung eines Signalnamens in einer Wirkkette).
Priority		• Alle Eingänge müssen in definierter Reihenfolge WAHR sein. • $A \wedge B$ • Cut-Set List: EVENT1.EVENT2 • Berechnung von Q Das Ergebnis ist gegenüber dem Ergebnis des reinen UND-Gatters, bei dem die Reihenfolge keine Rolle spielt, reduziert. • Details zum Priority Gate siehe auch FaultTree+ Hilfe • Anmerkung: FaultTree+ limitiert die maximale Anzahl von Eingängen auf 18

7.5.2. Verfügbare Event-Typen/Event-Symbole

Typ	Symbol	Bemerkung
Basis		**Verwendung:** • Alle Arten von Fehlern **Typisch verwendete Fehlermodelle:** • Alle außer Dormant
Conditional		**Verwendung:** • Zur Berücksichtigung von Zuständen in Fehlerbäumen oder Schlupf von Überwachungen **Typisch verwendete Fehlermodelle:** • Fix oder TRUE und FALSE (Rate model ist nur dann zu verwenden, wenn die Wahrscheinlichkeit des Zustands über die Betriebsdauer zunimmt)
House		**Verwendung:** • Zur Steuerung des Einflusses von Teilfehlerbäumen **Typisch verwendete Fehlermodelle:** • Zwingend Logisch TRUE oder FALSE
Dormant		**Verwendung:** • Zur Berücksichtigung latenter Fehler **Typisch verwendete Fehlermodelle:** • Dormant

Undeveloped		**Verwendung:** • Zur Dokumentation nicht weiter verfolgter Pfade bzw. zur Dokumentation von Eingängen mit und ohne Einfluss **Typisch verwendete Fehlermodelle:** • Alle außer Dormant, auch TRUE und FALSE

7.5.3. Verfügbare Fehlermodelle

Typ	Verwendung	Bemerkung
Ratenmodell „Rate“	Zur Beschreibung zufällig auftretender Fehler mit konstanter Fehlerrate, die sofort entdeckt bzw. behoben werden. Frühausfälle und Ausfälle am Lebensdauerende werden nicht berücksichtigt. Verwendung: Elektrische Fehler Verwendbar im Rahmen des Sicherheitsnachweises nach ISO26262-5.	Wichtigste Parameter: r: Fehlerrate lambda (1/h) t: Betrachteter Zeitraum (Rechenzeit oder auch mission time) Berechnung (Quelle: Hilfe von FaultTree+): $Q(t) = \frac{\lambda}{\lambda+\mu}(1-e^{-(\lambda+\mu)t})$ $\omega(t) = \lambda(1-Q(t))$ where $Q(t)$ = component unavailability $\omega(t)$ = component failure frequency λ = component failure rate μ = component repair rate  Anmerkung: µ: Reparaturrate ist gleich Null in nicht-reparierbaren Systemen

Fixe Ausfallrate: „Fix“	Zur Beschreibung zufällig auftretender Fehler, die mit konstanter Wahrscheinlichkeit auftreten. Verwendung: Betriebszustände; prinzipbedingter Diagnoseschlupf Verwendbar im Rahmen des Sicherheitsnachweis nach ISO26262-5.	Wichtigster Parameter: Q(t) = konstante Wahrscheinlichkeit

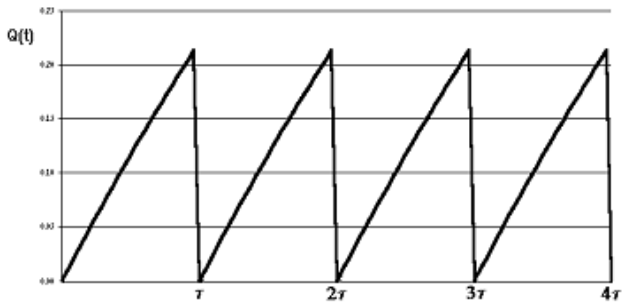
<table>
<tr>
<td>Dormant</td>
<td>Zur Berechnung der Auftretenswahrscheinlichkeit von latent auftretenden Fehlern.

Rechenergebnis hängt von Projekteinstellungen im Bereich „Sets Generation“ ab:

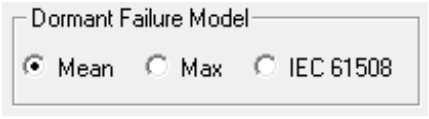
<u>Verwendung:</u>
Zufällig auftretende Fehler im Sinne des Raten-Modells, die aber über einen definierten Zeitraum unentdeckt bleiben, also latent vorliegen

Verwendbar im Rahmen des Sicherheitsnachweis nach ISO26262-5.</td>
<td><u>Wichtigste Parameter für nicht reparierbare Systeme:</u>
r = Fehlerrate lambda (1/h)
Inspection interval = Latenzzeit in h

<u>Verlauf von Q(t) bei Latenz τ:</u>
Der Verlauf von Q(t) ist auch in der Hilfe von FaultTree+ wie unten dargestellt. Der zeitliche Verlauf ist im Tool allerdings so nicht darstellbar und dient lediglich der prinzipiellen Erläuterung, wie der berechnete Endwert zu verstehen ist. Dieser berechnete Endwert wird im Tool als konstante Unvailability verwendet.

Q versus t plot for the dormant failure model with t << MTTF

Einstellungsmöglichkeiten bei FaultTree+ im Bereich „Sets Generation“:
 

<u>Mean:</u>
Kann verwendet werden, wenn davon ausgegangen wird, dass das Auftreten des latenten Fehlers während der Systemlebensdauer gleichverteilt ist.
<u>Anmerkung:</u>
MTTR: „Mean Time To Repair“ ist gleich Null bei nicht-reparierbaren Systemen

Rechenvorschrift <u>(Quelle: Hilfe von FaultTree+):</u>

Bei $\lambda\tau << 1$ and $\lambda . MTTR << 1$ gilt vereinfacht

$$Q_{mean} = \frac{\lambda . \tau}{2} + \lambda . MTTR$$

<u>Max:</u>
Kann verwendet werden, wenn davon ausgegangen wird, dass das Auftreten des latenten Fehlers stets in der ersten Stunde der Systemlebensdauer erfolgt (=> konservativer Ansatz).

Rechenvorschrift:
$$Q_{\max} = 1 - e^{-\lambda\tau}$$</td>
</tr>
</table>

Weibull	Zur Beschreibung zufällig auftretender Fehler mit variabler Fehlerrate. Berücksichtigt Frühausfälle und Ausfälle am Lebensdauerende. Verwendung: z.B. Mechanische Fehler bei ausgeprägtem Verschleißverhalten ! NICHT verwenden für Sicherheitsnachweis nach ISO26262-5!	Fehlerrate: $r(t) = \frac{\beta(t-\gamma)^{\beta-1}}{\eta^{\beta}}$ where $r(t)$ is the failure rate η = characteristic life parameter β = shape parameter γ = location parameter Nichtverfügbarkeit: $Q(t) = F(t)$ mit der „Unreliability“ $F(t) = 1 - \exp\left[-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right]$

Die weiteren in FaultTree+ angebotenen Fehlermodelle werden hier nicht weiter behandelt, da sie bislang in Praxis nur untergeordnete Bedeutung haben.

7.5.4. ISO26262: Zusammenhang Fehlertoleranzzeit-Fehlermodell-Betrachtungszeitraum (mission time) für kontinuierliche bzw. initiale Überwachungen

Im Rahmen der ISO26262 für den Automotive Bereich ist wichtig, dass für den Sicherheitsnachweis nur Überwachungen herangezogen werden, die „schnell genug“ ablaufen, um den Eintritt des Top Events durch Fehlerentdeckung und Systemreaktion zu verhindern. D.h. die Summe aus Ausführungszeit und Fehlerreaktionszeit muss kleiner als die Fehlertoleranzzeit FTTI (Fault Tolerance Time Interval) des zu vermeidenden Top Events sein.

Bezüglich der Modellierung ist für die quantitative Auswertung zu unterscheiden, ob diese immer nur für eine Betrachtungszeit (= Rechenzeit = Mission time) von 1h erfolgen soll (1 h wird von vielen OEMs als power-on-cycle angesehen, Fall A) oder ob andere, längere Mission times betrachtet werden sollen (Fall B), z.B. 8000 h als durchschnittliche Fahrzeugnutzungsdauer oder 15000 h als max. Fahrzeugnutzungsdauer.

Fall A (Mission time = 1 h):

In diesem Fall kann ein nicht latentes Basisereignis, das nur eine initiale Überwachung erfährt (also einmal nach dem Hochfahren des Systems) auf 2 unterschiedliche Arten modelliert werden. Diese sind mathematisch gleichwertig, d.h. Q nach 1h ist genau gleich groß. Dabei darf die initiale Überwachung allerdings nicht zur Reduktion von Q herangezogen werden, weil der zu erkennende Fehler in der Zeit zwischen den Ausführungen wirksam werden kann (Wiederholperiode der Überwachung von 1h >>FTTI des zu vermeidenden Top Events). Es stehen folgende Modellierungsmöglichkeiten zur Verfügung:

1. Symbol „Basic“ und Fehlermodell „rate“
2. Symbol „Basic“ und Fehlermodell „dormant“ mit „inspection interval“ = Mission time. Nachteil ist, dass bei einer Rechenzeit > 1h (im Fall A nicht relevant) der Wert für Q nicht steigt, also von einer Inspektion ohne Schlupf ausgegangen wird. Zudem muss die globale Projekt-Einstellung des „dormant failure models“ = MAX gewählt werden, damit das dormant Fehlermodell in für diesen Verwendungszweck keine zu kleinen Wahrscheinlichkeiten ausgibt. Alle anderen „echten“ latenten Fehler werden dann ebenfalls nach diesem dormant Fehlermodell berechnet (mit entsprechender Anpassung des Inspection interval an die Latenzzeit).

Das MAX-Modell bedeutet dann, dass angenommen wird, dass alle latenten Fehler stets in der ersten Betriebsstunde des Systems auftreten.

Latente Fehler, die *keinerlei* Überwachung während der Fahrzeuglebensdauer haben, müssen mit Fehlermodell „dormant“ und „inspection interval“ = zugesicherte Lebensdauer der ECU (h) modelliert werden.

Fall B (Mission time > 1 h):

Grundsätzlich ist bei Betrachtungen im Zusammenhang mit der ISO26262 von einer Berechnung von Mission Times > 1 h abzuraten, da bei der finalen Ermittlung der Unavailability nach einer Stunde fundamentale Rechenfehler gemacht werden, die zu einer Limitierung der maximal erreichbaren Unavailability nach einer Stunde von 1/(Mission Time) führen, weil eben das Ergebnis auf 1 h bezogen werden muss und nicht auf Mission Times > 1 h. So ist z.B. bei einer Mission Time von 10.000 h die maximal erreichbare Unavailability nach einer Stunde für ein sicher eintretendes Ereignis (also Q = 1 für 10.000 h) begrenzt auf Q = 1E-04, weil bei der Rückrechnung auf 1 h über die Mission Time gemittelt werden muss. Dass dieses Ergebnis nicht korrekt sein kann, liegt auf der Hand. Je höher die Unavailability am Ende der Mission Time, desto wirksamer wird dieser Rechenfehler.

Muss trotz obiger Sachlage eine derartige Berechnung gemacht werden, dann gibt es mehrere Möglichkeiten der Modellierung:

1. Option: Die Wirksamkeit von Initialen Tests soll berücksichtigt werden:
   Nicht latente Fehler: Ein nicht-latentes Basisereignis, das nur initial am Beginn einer Fahrt (mit Fahrtdauer 1 h) überwacht wird, wird mit dem Symbol „Basic“ gekennzeichnet und dem Fehlermodell „dormant“ und „inspection intervall“ = 1 h modelliert (Projekt-option „dormant failure model“ = Max muss gewählt werden). Andernfalls würde davon ausgegangen, dass keinerlei initiale Überwachungen im System installiert sind, bzw. das System während der gesamten Lebensdauer niemals ausgeschaltet wird.
   Nachteile: Man erhält eine Modellierung, die von einer 100%-Wirksamkeit des Initialtests ausgeht. Ein eventueller Schlupf der Überwachung ist nicht abgebildet. Durch die abschließende Division wird Q für diese Fehler auf zu kleine Werte reduziert.
   Latente Fehler: Fehler, die während der Fahrzeuglebensdauer latent bleiben (also unentdeckt und ohne Folgen für das Top Event), sollten mit dem Symbol „Dormant“ gekennzeichnet werden und mit dem Fehlermodell „dormant“ mit „inspection interval“ = Systemlebensdauer modelliert werden. Die wegen den nicht-latenten Fehlern zu wählende Option „dormant failure model“ = Max hat zur Folge, dass Q so berechnet wird, als ob das Auftreten der latenten Fehler stets in der ersten Stunde der Systemlebensdauer erfolgt.

2. Option: Keine Berücksichtigung der Wirksamkeit von initialen Tests:
   Nicht-latente Fehler:
   In diesem Fall wird ein nicht-latentes Basisereignis, das nur initial am Beginn einer Fahrt (mit Fahrtdauer 1 h) überwacht wird, mit dem Fehlermodell „rate“ modelliert.
   Effekt: Man erhält eine sehr konservative Modellierung, die die abschwächende Wirkung des Initialtests und das Ausschalten des Systems nach einer Stunde Betriebszeit nicht berücksichtigt.

   Echte latente Fehler: Latente Fehler, die keinerlei Überwachung während der Fahrzeuglebensdauer haben, könnten mit dem Fehlermodell „dormant“, „inspection interval“ = Mission Time modelliert werden - zudem muss die Einstellung des „dormant failure models“ = MAX gewählt werden, damit das dormant Fehlermodell für diesen Verwendungszweck keine zu kleinen Wahrscheinlichkeiten ausgibt.
   Effekt: Die so berechnete Unavailability entspricht exakt dem Ergebnis einer Modellierung mit dem „rate“ Modell. Latente Fehler können somit anhand ihrer Unavailability nicht von nicht-latenten Fehlern unterschieden werden. Es ist demnach gleichgültig, welche Modellierung gewählt wird. Eine einfache pauschale Modellierung mit „rate“ für alle Fehler liefert

das gleiche Ergebnis. Dies ist ein weiteres Indiz dafür, dass Berechnungen von Mission Times > 1 h nur bei Systemen sinnvoll sind, die auch tatsächlich solch lange ununterbrochene Betriebszeiten aufweisen (z.B. Kraftwerke o.ä.). Bei Systemen mit kürzeren Mission Times treten hingegen Probleme bei der (angemessenen) Berücksichtigung des Einflusses von latenten Fehlern auf.

7.6. Empfehlungen zur Namenskonvention

Die Festlegung von Namenskonventionen in der FTA ist hilfreich unter anderem für die Kombinierbarkeit von FTA´s, sorgt für bessere Lesbarkeit, vereinfacht die Auswertung und die Orientierung innerhalb der FTA.

7.6.1. Benennung von Events/Gates

Benennung vom Allgemeinen zum Besonderen

Dabei ist zu berücksichtigen, dass die Tool-Umgebung in FaultTree+ bestimmte Umsetzungen einer Namenskonvention bevorzugt unterstützt, denn einige Dialoge (Event Table, Gate Table) des Tools sortieren die angebotenen Listen stets in alphabetischer Reihenfolge. Will man bei der Auswahl von Gattern stets ähnliche Gatter nebeneinander angeboten bekommen, so empfiehlt sich eine Namensgebung vom Allgemeinen zum Speziellen hin (Beispiel: Signalfehler_Abweichungsrichtung: PS_HIGH, PS_LOW, Bauteil_Fehlermodus: R19_OPEN, R19_SHORT).

Die im Beispiel-Fehlerbaum aus Schritt 4 gewählte Namenskonvention folgt einer Ordnung. So heißen alle Fehler „URSACHE_*“.

Besondere Zeichen vermeiden

Der Dezimalpunkt „.“ sollte im Gate-Name / Event-Name vermieden werden:

Hintergrund: Der Punkt trennt in der Default-Einstellung bei FaultTree+ bei der Auswertung der Cut-Sets die beteiligten Events innerhalb von Mehrfach-Cut-Sets. Ein Dezimalpunkt könnte hier für Verwirrung sorgen.

Das Leerzeichen im Gate-Name / Event-Name kann durch einen Unterstrich oder Bindestrich ersetzt werden (bessere Lesbarkeit im FaultTree+).

Letztes Zeichen von Event- und Gate-Bezeichnungen

Das letzte Zeichen eines Event-/Gate-Name sollte keine Zahl und auch kein Leerzeichen sein.

Hintergrund: Bei der Wiederverwendung von Bäumen oder Events im Modus „paste special“ fügt Fault-Tree+ eine Zahl ans Ende des Namens. Steht dort bereits eine Zahl, wird diese beim Einfügen via „paste special“ durch FaultTree+ einfach um „1“ erhöht

→ Schlechte Erkennbarkeit von unbeabsichtigten Änderungen („Fehler Drucksensor 1“ wird unbeabsichtigt zu „Fehler Drucksensor 2“).

Ein Leerzeichen am Ende eines Event- oder Gate-Namens kann zu Problemen bei der eindeutigen Identifzierbarkeit von Gattern führen.

Beispiel aus Fehlerbaum in Schritt 4:

URSACHE_1)1 ist erkennbar als noch nicht bearbeitetes Event, das im „paste special“ Modus eingefügt wurde.

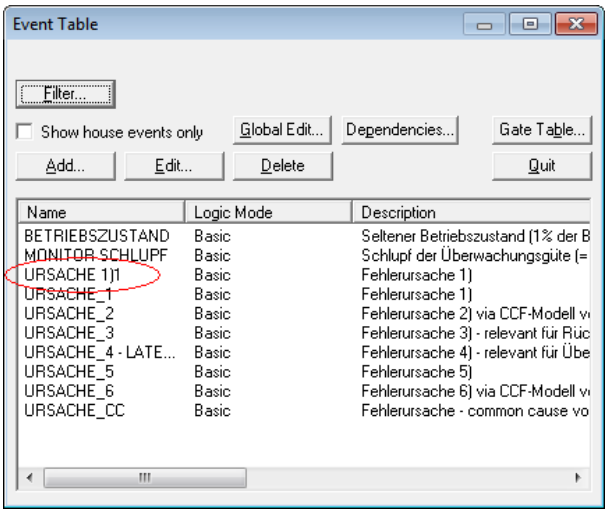


Abbildung 7.6: Namenskonvention in Eventliste

Bezeichnungen von Events entsprechend des Fehlertyps vergeben

Der Event Name kann sich zusammensetzen aus: Eventklasse; Namen/Bezeichnungen; Fehlerbildklasse; Signalabweichung

Beispiele aus einer FTA für das Produkt ESP (Elektronisches Stabilitätsprogramm):

Softwarefehler:

SW_HAL (Software, Hydraulic Actuation Layer)

SW_VDC (Software, Vehicle, Dynamics Controler)

Mechanische Fehler:

M_EV_U_CL (Mechanischer Fehler, Einlassventil, Unintended, Closed)

M_USV_U_O (Mechanischer Fehler, Umschaltventil, Unitended, Open)

Steuergerätefehler:

ECU_EV_U_O (Steuergerätefehler, Einlassventil, Unitended, Open)

ECU_HSV_C2H (Steuergerätefehler, Hochdruckschaltventil, Current, 2(too),High)

ECU_PHZ_2H(>+30) (Steuergerätefehler, HZ-Drucksignal, too high , Abweichung > 30 bar)

ECU_PHZ_2L(>20%) (Steuergerätefehler, HZ-Drucksignal, too low, Abweichung > 20%)

Signalfehler:

P-WHEEL_2L(<-15) (Raddrucksignal, too low, Abweichung > 15 bar)

Überwachungsschlupf

UNDET_BLS_PERM_H (Überwachungsschlupf, BLS-permanent high)

UNDET_MOM_LOW (Überwachungsschlupf, Modulator Monitoring, MomLowPressure)

7.6.2. Event-Gruppen nutzen

Steigt die Anzahl der vergebenen Events, kann eine Sortierung der Events in Gruppen helfen, den Überblick zu behalten. Eventgruppen werden in FaultTree+ im Projekt-Explorer angelegt. Eine Zuordnung eines Events in mehrere Eventgruppen ist möglich.

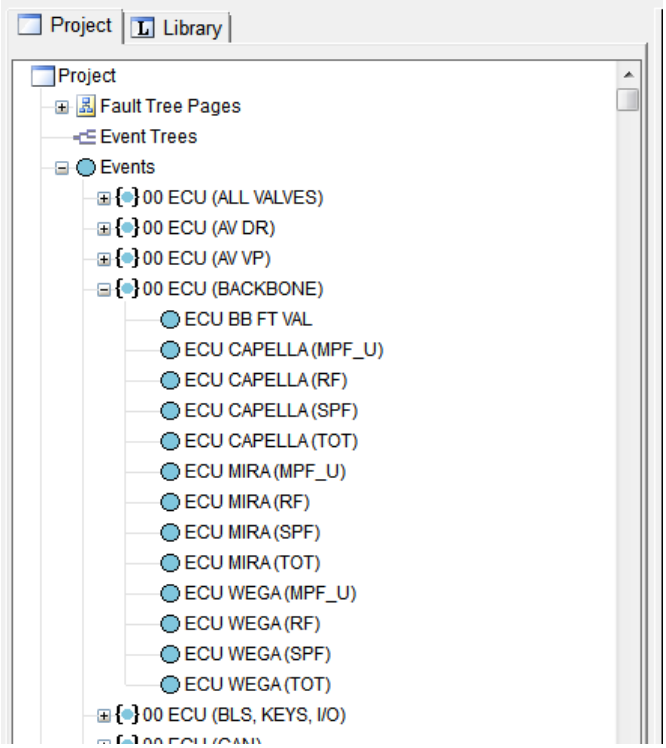


Abbildung 7.7: Eventgruppen

7.6.3. Besonderheiten bei der Benennung von Gattern

Enthält eine Datei mehrere Teilfehlerbäume, die unterschiedliche Top Events analysieren, kann es sinnvoll sein, wenn die Bezeichnungen von Gattern Hinweise auf die Einbindung in den jeweiligen Teilfehlerbaum enthalten. Wird der Hinweis an das Ende der Bezeichnung gesetzt, ergibt sich der Vorteil, dass ähnliche Gatter in unterschiedlichen Hazards alphabetisch sortiert, von FaultTree+ nebeneinander aufgelistet werden.

Vorteil: Die Zusammenhänge gerade zwischen den Gates sind leichter verständlich. Widersprüche zwischen (wiederverwendeten) Signal-Fehlerbäumen und dem Top Event (dem Hazard) des Fehlerbaums sind leicht(er) identifizierbar.

Beispiel für Kennzeichnung von Gates innerhalb von Fehlerbäumen (letzte Buchstaben):

AV(FL) OP E|C * → [Auslassventil] [(Rad vorne links)] [Offen] [Elektrischer oder Ansteuerungsfehler] [Kennzeichnung für den jeweiligen Fehlerbaum (L/ND, L/NP, R,...)]

AV(FL) OP M|E * → [Auslassventil] [(Rad vorne links)] [Offen] [Mechanischer oder Elektrischer Fehler] [Kennzeichnung für den jeweiligen Fehlerbaum (L/ND, L/NP, R, ...)]

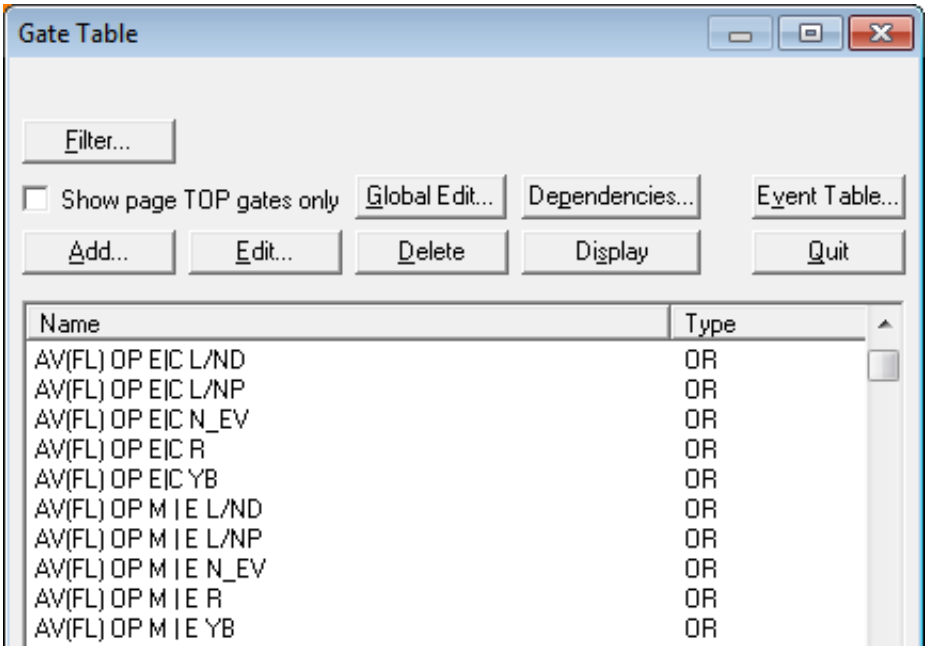
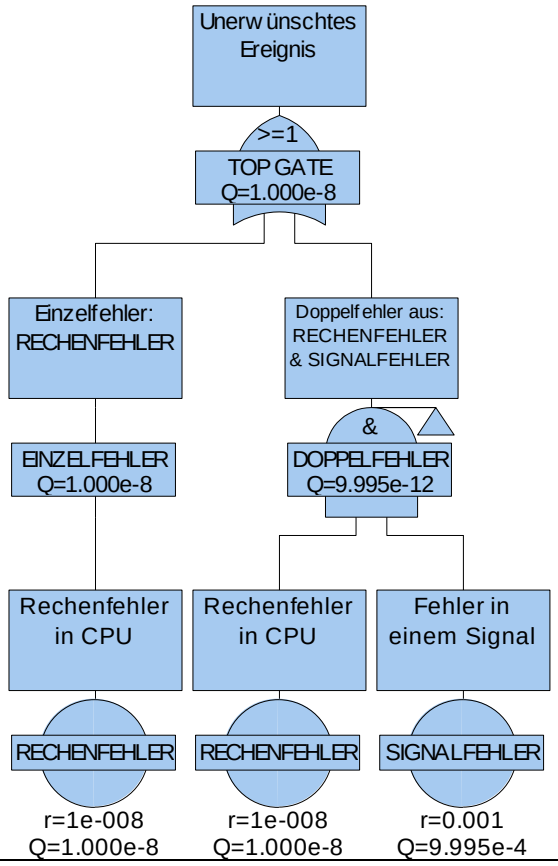


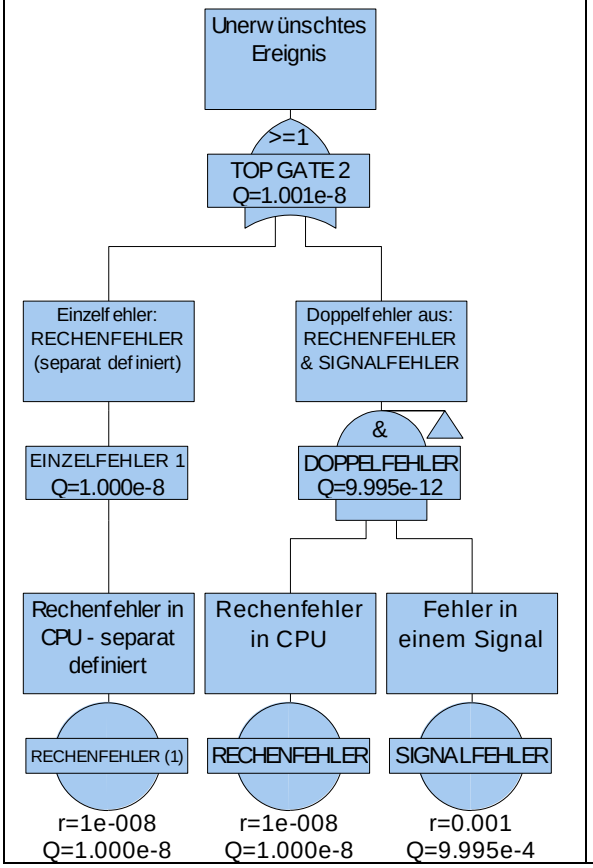
Abbildung 7.8: Namenskonvention Gate Table

7.7. Tipps und Tricks bei Erstellung, Berechnung und Handling von Fehlerbäumen

7.7.1. Mehrfachdefinition eines einzigen Basisereignisses

Kann *ein und derselbe* Fehler an verschiedenen Stellen eines Fehlerbaums relevant sein, so muss darauf geachtet werden, dass im Fehlerbaum stets dasselbe Event benutzt wird. Dies stellt sicher, dass die Fehlerbaumlogik den Einfluss des betreffenden Events korrekt berechnet.

Fehlerbaumlogik	Ergebnis
	Cut-Set list: RECHENFEHLER mit Q=1,0E-08 Der Doppelfehler aus RECHENFEHLER und SIGNALFEHLER wird bei Nutzung des identischen Events RECHENFEHLER absorbiert wegen: $Q = q_A \vee (q_A \wedge q_B) = q_A$ Gesamtwahrscheinlichkeit: Q = 1e-08



Cut-Set list:

RECHENFEHLER (1)=> Q = 1E-08
RECHENFEHLER.SIGNALFEHLER => Q = 9.995E-12

Gesamtwahrscheinlichkeit:

$Q = q_A + q_B * q_C - q_A * q_B * q_C$

Mit $q_B . q_C$ = 9,995E-12

Q = 1E-08 + 9,995E-12 – 1E-08*9,995E-12

Q = 1,001E-08

7.8. Verwendung von NOT- oder XOR-Gattern bei aktivierter „Full Not Logic“

Die Erstellung eines Fehlerbaums unter Verwendung von NOT-Gattern oder XOR-Gattern bei aktivierter „Full Not Logic“ will wohlüberlegt sein. Mögliche Anwendungsfälle wären, dass z.B. bestimmte Fehlerkombinationen durch Sicherheitslogik ausgeschlossen werden sollen. Durch eine UND-Kombination mit einem NOT-Gatter oder XOR sollen sich dann ungültige Fehlerkombinationen auslöschen.

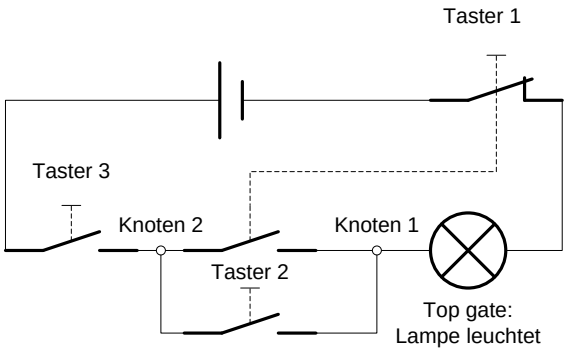
Probleme entstehen aus der Art des Ergebnisses, das NOT-Gatter oder XOR-Gatter liefern. Werden unterhalb dieser Gattertypen Fehler angebunden, deren Logic mode weder TRUE noch FALSE ist, dann liefern NOT und XOR als Ergebnis die Wahrscheinlichkeit des NICHT-Fehlers (also die Wahrscheinlichkeit, dass der Fehler gerade *nicht* auftritt).

Das führt bei großen Fehlerbäumen dazu, dass zusätzlich zu den eigentlich relevanten Fehlerkombinationen die NICHT-Fehler kombiniert werden. In der Regel steigt die Order der daraus entstehenden Cut-Sets dann dramatisch an – obwohl sich an der Höhe des Gesamtergebnisses kaum etwas ändert. Bei entsprechender Logik lassen sich dann weder im Tool FaultTree+ noch durch einen Export nach MS-EXCEL die Cut-Sets vollständig anzeigen, da die Länge des anzuzeigenden Cut-Set Strings die Möglichkeiten beider Tools übersteigt.

Alternativen zur Verwendung von NOT-Gattern oder XOR-Gattern sind:

- Verzicht auf NOT- bzw. XOR-Gatter unterhalb eines UND-Gatters bei bewusster Inkaufnahme von Fehlerkombinationen, deren Eintreten eigentlich ausgeschlossen ist. Wenn dies die wahrscheinlichsten Fehlerkombinationen im Gesamtergebnis sind, dann ist dies eine gute Nachricht, weil sinnvolle Fehlerkombinationen sogar unwahrscheinlicher sind als solche, die sich ausschließen.

- Verzicht auf NOT- bzw. XOR-Gatter durch Freischneiden von Fehlerbäumen unter Berücksichtigung des nicht korrekt darstellbaren Zusammenhangs (der Auslöscheffekt durch die NICHT-Gatter wird im Fehlerbaum explizit berücksichtigt).



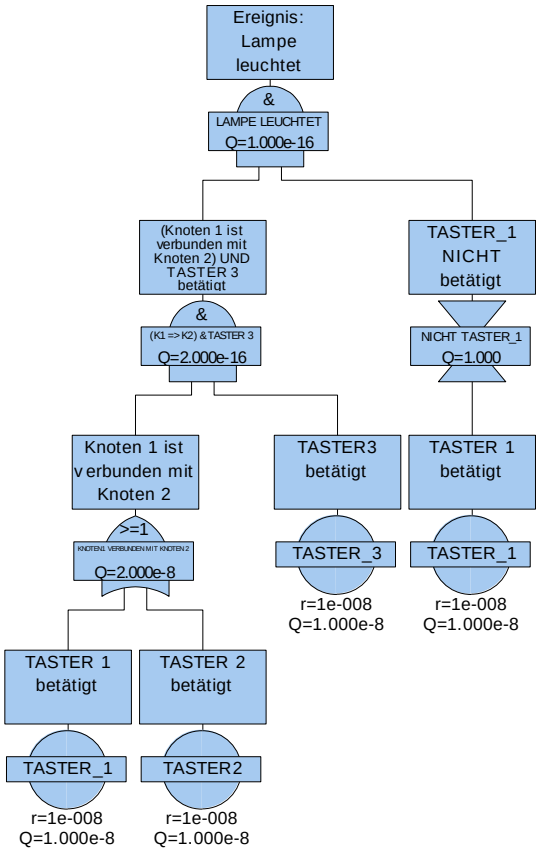
Beispielschaltplan Lampensteuerung.

Zu untersuchendes Ereignis: „LAMPE LEUCHTET“

Taster 1 betätigt synchron zwei Schaltelemente. Eines davon ist als „Öffner“ in Reihe zu allen anderen Elementen geschaltet und eines als „Schließer“ parallel zum Schaltelement, das Taster 2 betätigt.

Taster 3 betätigt einen „Schließer“ und ist in Reihe zu allen Schaltern geschaltet.

Knoten 1 und Knoten 2 sind Stellen, an denen der Stromfluss analysiert werden kann.



Fehlerbaum-Erstellung unter Verwendung „NICHT-Gatter“:

Die Analyse ergibt:

Die Lampe leuchtet, wenn TASTER_1 NICHT betätigt ist („Öffner“ nicht betätigt). Außerdem liefert die Analyse der anderen Schaltungsteile, dass Knoten 1 mit Knoten 2 verbunden sein muss (TASTER_1 oder). Gleichzeitig muss TASTER_3 betätigt sein.

Cut-Set:

TASTER_2.TASTER_3.-TASTER_1

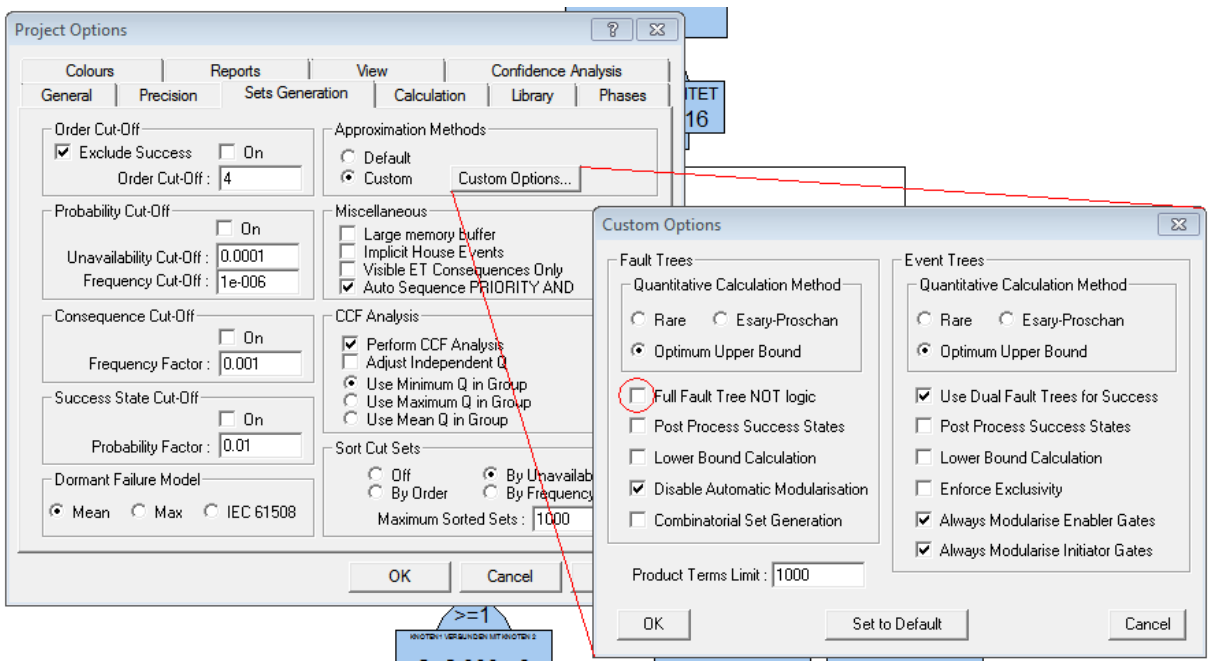
Ausgelöschtes Cut-Set:

TASTER_1.TASTER_2.-TASTER_1

Alternativen:

<u>Deaktiviere: „Full Not Logic“ in den Fault-Tree Optionen (→ Inkaufnahme von Fehlerkombinationen)</u>

Eine Neuberechnung des Fehlerbaums von oben bei deaktivierter „Full Fault Tree NOT logic“ führt zum Ignorieren der Nicht-Gatter bzw. XOR.

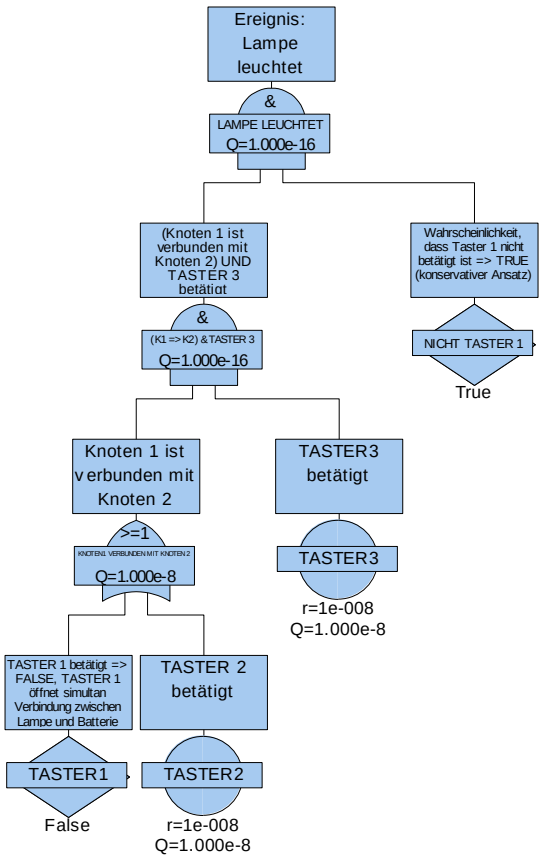


Das Rechenergebnis des Fehlerbaums ändert sich wie folgt: Cut-Set Liste:

TASTER2.TASTER3
TASTER1.TASTER3

Das zweite Cut-Set muss dabei in Kauf genommen werden, obwohl es erwiesenermaßen ungültig ist.

Alternative Erstellung des Fehlerbaums durch Freischneiden:



Die alternative Fehlerbaumlogik berücksichtigt die technischen Zusammenhänge und liefert ein konservatives (also leicht zu hohes) Gesamtergebnis.

Das Nicht-Gatter wurde gewandelt in ein Undeveloped Event „NICHT TASTER 1“ und auf logisch TRUE gesetzt. Dies führt gegenüber der Wahrscheinlichkeit der Nichtbetätigung (Q=1 - 1E-08) zu einem leicht erhöhten Ergebnis im TopEvent (→ konservativ)

Die Bedatung von TASTER1 wird unter Berücksichtigung der widersprüchlichen Fehlereffekte (Schließen und gleichzeitiges Öffnen des Stromkreises) auf Logisch FALSCH gesetzt. D.h. TASTER1 kann nicht via Verbindung von Knoten1 mit Knoten2 zum Leuchten der Lampe beitragen.

Cut-Set Liste:

TASTER2.TASTER3

Die Wahrscheinlichkeit der Nichtbetätigung von Taster1 bleibt wegen NICHT TASTER 1 = TRUE unberücksichtigt. Dieses Vorgehen ist sinnvoll bei Basisereignissen, deren Wahrscheinlichkeit <<1 ist.

Liegt die Wahrscheinlichkeit höher, kann versucht werden, die reziproke Wahrscheinlichkeit in einem Basisereignis, das den Nichteintritt des Fehlers beschreibt (hier „NICHT TASTER 1“) zu berücksichtigen.

7.9. Unbeabsichtigte / beabsichtigte Absorption von Mehrfachfehlern

Bei der Kombination von UND- und ODER-Gattern kann es zu Absorptionseffekten aufgrund der Regeln der Booleschen Algebra kommen. Diese Effekte können gewinnbringend eingesetzt werden, um bei voller Analysetiefe trotzdem die Irrelevanz von Eingängen zeigen zu können.

Beispiel aus der System-FTA des ESP (Elektronisches Stabilitätsprogramm):

Im Produkt ESP gibt es einen Radschlupfregler, der lediglich bei vorliegender Anforderung durch den Fahrdynamikregler aktiv werden kann. Liegt die Anforderung vor, vergleicht der Radschlupfregler dann gemessene Radgeschwindigkeiten mit einer berechneten Fahrzeuggeschwindigkeit.

Unter der Annahme, der Radschlupfregler sollte unbeabsichtigt (also ohne vorliegende Anforderung) aktiv werden, ergibt sich folgender Fehlerbaum...

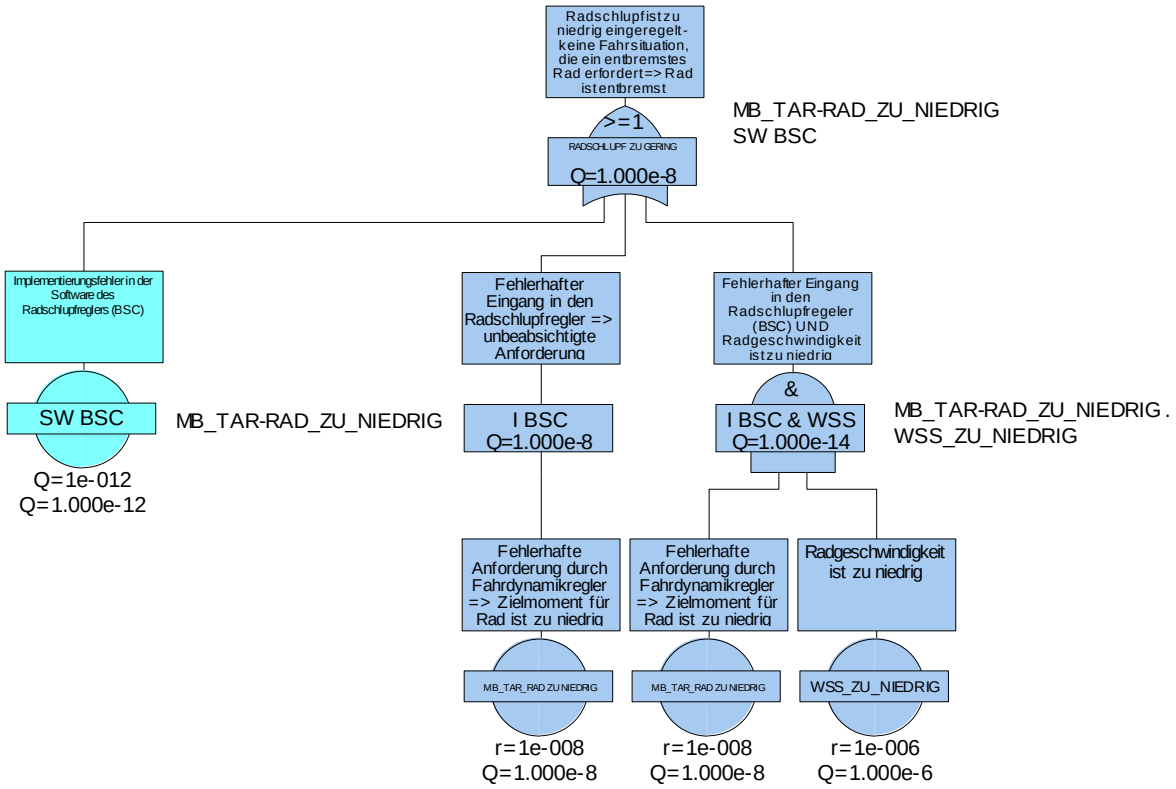


Abbildung 7.9: Absorption Radgeschwindigkeitsfehler

MB_TAR_RAD_ZU_NIEDRIG ist vernachlässigbar, aufgrund der um den Faktor 100 größeren Wahrscheinlichkeit für WSS NIEDRIG. D.h. das Radgeschwindigkeitssignal trägt nicht zur Gesamtwahrscheinlichkeit bei, obwohl es durch Analyse voll berücksichtigt wurde (nützlich bei Diskussionen mit Auftraggebern in Bezug auf vollständige Analyse).

Dieser Absorptionseffekt kann allerdings auch unbeabsichtigt erfolgen. Daher ist Fehlerbäumen, bei denen ODER-Gatter Einzelfehler und UND-Gatter kombinieren, stets besondere Aufmerksamkeit zu widmen.

7.10. Einsatz von Cut- Off Regeln bei der Berechnung

Zuweilen werden Fehlerbäume so groß, dass die Rechenzeiten für die sich ergebenden Fehlerkombination sehr groß werden. Abhilfe kann durch die Aktivierung sogenannter Cut-Offs gefunden werden. Hierdurch wird die Berechnung in FaultTree+ vorzeitig abgebrochen – ein entsprechender Genauigkeitsverlust des Ergebnisses muss dann berücksichtigt werden.

FaultTree+ bietet zwei Cut-Off Bedingungen (Order Cut-Off und Probability Cut-Off) an, die sich für bestimmte Aufgabenstellungen anbieten. Beide Bedingungen können miteinander kombiniert werden.

Order Cut-Off:

FaultTree+ berechnet nur Fehlerkombinationen bis zur genannten Höhe der Order. Die Wahrscheinlichkeit der Fehlerkombination spielt hier keine Rolle.

Probability Cut-Off:

FaultTree+ berechnet nur Fehlerkombinationen bis zur genannten Unavailability / Frequency. Die Order der Fehlerkombinationen spielt dabei keine Rolle.

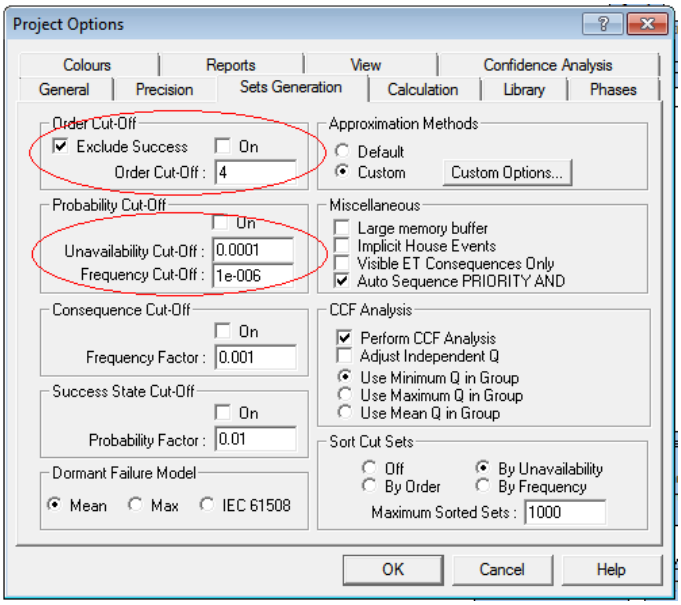


Abbildung 7.10: Projekt Optionen – Cut-Offs

Eine unangemessene Auswahl der Cut-Offs kann unerwartete Auswirkungen auf das berechnete Ergebnis haben. Daher soll die Wirksamkeit der Cut-Off Bedingungen an einem Beispielfehlerbaum demonstriert werden. Die Logik in Abbildung 7.11 hat keinen technischen Hintergrund, liefert aber vom Einzel- bis zum 4-fach-Fehler entsprechende Fehlerkombinationen. Eine Besonderheit ist, das es einige Events gibt, deren Ausfallwahrscheinlichkeit im Bereich von 0,1 liegt.

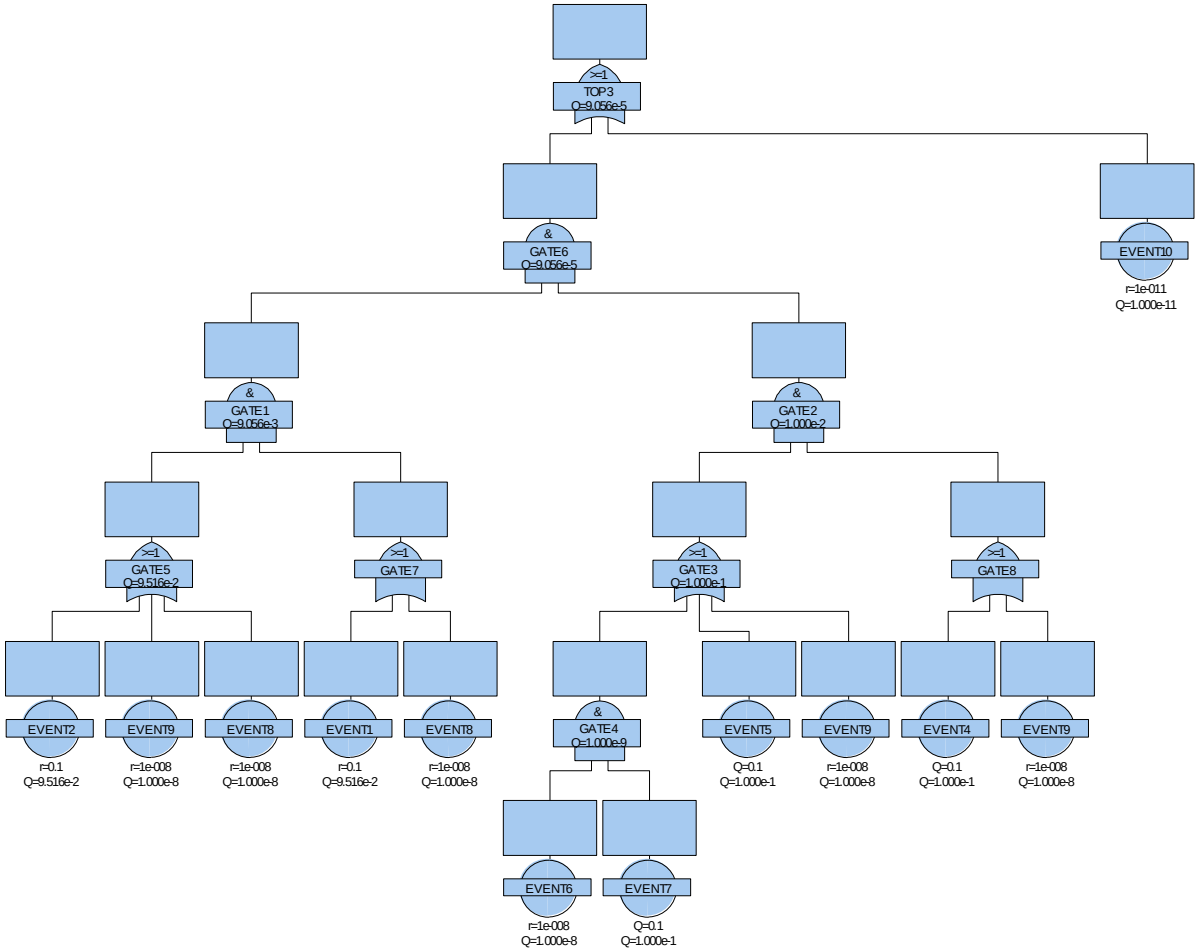


Abbildung 7.11: Beispielfehlerbaum zur Demonstration von Cut-Offs

Der Beispielfehlerbaum liefert bei 1h Mission time („System life time“) folgende Ergebnisse.

ohne aktivierten Cut-Off:

Unverfügbarkeit TOP3: Q = 9.056 E-05

Cut-Set Liste:

Number	Cut-Set	Unavailability	Order
1	EVENT2. EVENT1. EVENT5. EVENT4	9,05592E-05	4
2	EVENT9. EVENT1	9,51626E-10	2
3	EVENT8. EVENT5. EVENT4	1E-10	3
4	EVENT10	1E-11	1
5	EVENT2. EVENT1. EVENT4. EVENT6. EVENT7	9,05592E-13	5
6	EVENT8. EVENT9	1E-16	2
7	EVENT8. EVENT4. EVENT6. EVENT7	1E-18	4

Die wahrscheinlichste Fehlerkombination hat eine Order von 4! In der Praxis können Einzelfehler, die mit mehreren Bedingungen (Q im Prozentbereich) verbunden sind, solche Cut-Sets bilden.

Die Aktivierung eines Order Cut-Off mit dem Wert 3 hat entsprechende Konsequenzen:

Das Ergebnis verbessert sich um Faktor 10.000, weil das abgeschnittene vermeintlich unbedeutende Cut-Set mit Order 4 den entscheidenden Beitrag zum Gesamtergebnis lieferte.

Unverfügbarkeit TOP3: Q = 1.062 E-09

Cut-Set Liste:

Number	Cut-Set	Unavailability	Order
1	EVENT9. EVENT1	9,51626E-10	2
2	EVENT8. EVENT5. EVENT4	1E-10	3
3	EVENT10	1E-11	1
4	EVENT8. EVENT9	1E-16	2

Probability Cut-Off mit Wert 1E-12:

Bei Aktivierung eines Probability Cut-Off mit dem Unavailability-Wert 1E-12 bleibt das Gesamtergebnis nahezu unverändert, weil der Abstand zwischen Cut-Off und dem erwarteten Gesamtergebnis entsprechend hoch ist.

Unverfügbarkeit TOP3: Q = Q = 9.056 E-05

Cut-Set Liste:

Number	Cut-Set	Unavailability	Order
1	EVENT2. EVENT1. EVENT5. EVENT4	9,05592E-05	4
2	EVENT9. EVENT1	9,51626E-10	2
3	EVENT8. EVENT5. EVENT4	1E-10	3
4	EVENT10	1E-11	1

Der hier sinnvoll gewählte Probability Cut-Off berücksichtigt die Größenordnung in der das erwartete Ergebnis liegen wird – er ist um Faktor 1E-07 (!) kleiner als das Gesamtergebnis. (Bsp. aus der Praxis (ESP-FTA): Zielwert liegt im Bereich 1E-08 bis 1E-07 => Probability Cut-Off bei 1E-30).

Fazit:

Ein *Order Cut-Off* sollte nur verwendet werden, wenn

- sicher ist, dass das Ergebnis durch den Order Cut-Off nicht entscheidend verfälscht wird
- der Fokus tatsächlich auf der Ausgabe von Fehlerkombinationen mit begrenzter Order liegt.

Ein *Probability Cut-Off* kann bei Berücksichtigung des erwartenden Ergebnisses so gewählt werden, dass das Gesamtergebnis nicht signifikant beeinflusst wird.

7.11. Berücksichtigung von Eingängen, die keinen Einfluss auf ein Gatter haben

Es kann sinnvoll sein, auch Eingänge in einen Fehlerbaum zu modellieren, von denen bekannt ist, dass sie keinen Einfluss haben. Dies kann durch Anhängen von Basisereignissen mit dem Symbol „Undeveloped“ und dem Logic mode = FALSE erfolgen.

Vorteile:

- Die Vollständigkeit der Analyse kann demonstriert werden und Begründungen für die Nichtrelevanz von Eingängen können geeignet dokumentiert werden.
- Wenn Information im Fehlerbaum fehlt, ist dies eindeutig interpretierbar.
- Die Vergleichbarkeit von Fehlerbäumen steigt.
- Die Vollständigkeit der Analyse kann einfacher geprüft werden.

Nachteil: Die Anzahl der anzulegenden Events steigt.

7.12. Offene Punkte in der FTA (=> Transfer Gates, Labels usw.)

Offene Punkte in der FTA lassen sich durch Labels auf FaultTree Seiten aber auch durch das Einfügen von Gattern ohne Eingang (Transfer-Gates) im Fehlerbaum vermerken.

Nachteil der Verwendung von Labels: Labels sind stets einer Seite im Fehlerbaum zugeordnet. Ändert sich die Zuordnung der Seiten im Fehlerbaum (Seiten werden durch die Option „page“ in Gattern definiert), so geht die Zuordnung des Labels (der offenen Punkte) zum Fehlerbaum verloren.

Vorteil der Verwendung von Transfer-Gates: Die Option „Verify Data“ im Menü „Analysis“ erlaubt eine einfache Identifikation solcher Transfer Gates. Liefert diese Abfrage keine offenen Gatter mehr, sind alle offenen Punkte geschlossen.

7.13. Modellierung von Common-Cause-Failures

Es gibt prinzipiell 2 Möglichkeiten der Modellierung:

1. Modellierung über einen Koppelfaktor zwischen Basisereignissen, die einen gemeinsamen Root Cause-Fehler haben können (β-Faktor-Modell)
2. Modellierung durch Einsetzen des Root-Cause-Ereignisses an allen relevanten Stellen im Fehlerbaum

7.13.1. Modellierung mit β-Faktor Modell

Das ß-Faktor ist das einfachste Modell zur Beschreibung der Abhängigkeit zweier Ereignisse A und B, die zunächst als unabhängig angenommen werden.

Mithilfe eines Faktors (des ß-Faktors, der zwischen 0% und 100% variieren kann) wird ausgedrückt, welcher Anteil der Fehlerrate von A zu einem gleichartigen Fehler bei B führt. Im einfachsten Fall der homogenen Redundanz mit $Q_A = Q_B$ gilt dann:

$Q_{CCF} = \beta \times Q_A$

$Q_{TOP} = Q_{CCF} + (1- \beta)Q_A * (1- \beta)Q_B$

Beispiel: $Q_A = Q_B = 1E\text{-}03$, $\beta = 10\%$

$Q_{TOP} = 0{,}1 * 1E\text{-}03 + 0{,}9 * 1E\text{-}03 * 0{,}9 * 1E\text{-}03 \approx 1{,}0081E\text{-}04$

Andere Fälle siehe FT+ User Manual.

Das β -Faktormodell ist nicht unumstritten, da es kein allgemein erkanntes Verfahren zur Bestimmung des β -Faktors gibt. Die Norm IEC61508 enthält eine Checkliste zur Bestimmung des β -Faktors, die oft verwendet wird.

7.13.2. Modellierung durch Einsetzen des Root-Cause-Ereignisses

Bei der Modellierung von Common Causes durch Einsetzen des Root-Cause-Ereignisses ist lediglich darauf zu achten, dass stets dasselbe Ereignis angebunden wird.

Beispiel: In Abbildung 7.11 (siehe Kapitel: 7.10 Einsatz von Cut- Off Regeln bei der Berechnung) sind die EVENTS 1 und EVENT 9 als Root-Cause-Ereignisse bzgl. der höher liegenden UND-Gatter angebunden.

8. Anhang 2 – Beispiel Report

BOSCH

Von	Bearbeiter	Telefon	Standort Datum

Bericht

Ausgabe *X.X*
Thema ***PROJECT***
Beschreibung FTA-Bericht

1. Aufgabe:

Erstellung einer Fehlzustandsbaumanalyse (FTA) für das Projekt „*XXX*" für die folgenden FTA-TopEvents:

TopEvent-Name	Beschreibung	Kommentar / Hinweise
TopEvent1	*XXX*	*XXX*
TopEvent2	*XXX*	*XXX*
TopEvent3	*XXX*	*XXX*
TopEvent4	*XXX*	*XXX*

2. Arbeitsgruppe:

Name	Abteilung	Aufgabe im FTA-Team	Kommentar / Hinweise
XXX	*XXX*	*XXX*	*XXX*
XXX	*XXX*	*XXX*	*XXX*
XXX	*XXX*	*XXX*	*XXX*
XXX	*XXX*	*XXX*	*XXX*

3. Ergebnisse:

Die Analyse lieferte für die einzelnen TopEvents die folgenden Ergebnisse:

TopEvent-Name	(ggf) ASIL	Zielwert	Ergebniswert	Kommentar / Hinweise / Bewertung
TopEvent1	*XXX*	*XXX*	*XXX*	*XXX*
TopEvent2	*XXX*	*XXX*	*XXX*	*XXX*
TopEvent3	*XXX*	*XXX*	*XXX*	*XXX*
TopEvent4	*XXX*	*XXX*	*XXX*	*XXX*

VERTRAULICH

Seite 1 von 3

BOSCH

Von	Bearbeiter	Telefon	Standort Datum

Bericht
Ausgabe X.X
Thema PROJECT

Für die einzelnen TopEvents haben die folgenden Basisereignisse / Minimalschnitte einen relevanten Einfluss:

TopEvent1	*Beschreibung*	*Ergebniswert*
Basisereignis / Minimalschnitt1	*Beschreibung*	*Ergebnis*
Basisereignis / Minimalschnitt2	*Beschreibung*	*Ergebnis*
Basisereignis / Minimalschnitt3	*Beschreibung*	*Ergebnis*

4. Getroffene Annahmen

Bei der Erstellung der FTA wurden folgende Annahmen getroffen:

Annahme	*Ausführung*
Betrachtungsumfang	*z.B. Variante / Bestückung / ...*
Grenzen des Systems	...
...	...

5. Datengrundlage

Die Ergebnisse beruhen auf den wie folgt hergeleiteten Ausfallraten ...

- *Beispiel-Quelle: „Siemens-Norm" SN29500*
- *Flächenansatz zur Herleitung*
- ...

- *Tabelle der Events und ihrer Ausfallraten an dieser Stelle bzw. Hinweis auf eine im Anhang befindliche Tabelle (Export der Events)*

6. Anlagen *(Beispiele)*

- Block-Diagramm

VERTRAULICH

Seite 2 von 3

BOSCH

Von	Bearbeiter	Telefon	Standort Datum

Bericht
Ausgabe X.X
Thema PROJECT

- FTA-Diagramm
- Liste der definierten FTA-Gatter („Gates")
- Liste der definierten FTA-Basisereignisse („Events")
- Ausdruck „Offene-Punkte-Liste"
- Ausdruck Termin- / Anwesenheits- / Teilnehmerliste

7. Freigabe

Sofern eine Freigabe dieses Berichts (und der zugehörigen FTA) im jeweiligen Projekt gewünscht wird kann an dieser Stelle eine Liste der Personen eingefügt werden die unterschreiben sollen. Der Umlauf selbst kann – vergleichbar einem FMEA-Unterschriftenumlauf – mittels „eSignature" durchgeführt werden.

VERTRAULICH

Seite 3 von 3

Leere Seite

Leere Seite

Leere Seite

Leere Seite

Fehlzustandsbaumanalyse

Robert Bosch GmbH
C/QMM
Postfach 30 02 20
D-70442 Stuttgart
Germany
Phone +49 711 811-71 39
Fax +49 711 811-4 51 55
www.bosch.com