Beitrag zur dynamischen Fehlerbaumanalyse ohne Modulbildung und zustandsbasierte Erweiterungen

---

Vom Fachbereich D der Abteilung Sicherheitstechnik der
Bergischen Universität Wuppertal
zur Erlangung des akademischen Grades
Doktor-Ingenieur (Dr.-Ing.)
genehmigte Dissertation

von
Diplom-Ingenieur Simon J. Schilling
aus München, Deutschland

Gutachter:
Univ.-Prof. Dr.-Ing. A. Meyna
Univ.-Prof. Dr. rer. nat. P. C. Müller

Tag der mündlichen Prüfung:
21. Dezember 2009

D468

Fuer
Albert und Alexandra und Lieselotte

Vorwort

Die vorliegende Arbeit entstand großteils im Rahmen meiner Tätigkeit als wissenschaftlicher Mitarbeiter des Zentralteams Funktionssicherheit der BMW Group in München.

Mein ganz besonderer Dank gilt in gleichem Maße Herrn Univ.-Prof. Dr.-Ing. Arno Meyna und Herrn Dipl.-Ing. Christoph Jung.

Meinem Doktorvater Professor Meyna danke ich für die hervorragende Förderung und Betreuung dieser Arbeit im Rahmen meiner externen Promotion im Fachgebiet Sicherheitstheorie und Verkehrstechnik an der Bergischen Universität Wuppertal.

Herrn Jung, dem ehemaligen Leiter des Zentralteams Funktionssicherheit der BMW Group sowie Convenor der ISO TC 22 SC 3 WG 16 und als Solcher maßgeblicher Kopf hinter und verantwortlich für die neue ISO 26262, danke ich nicht nur für die Ermöglichung dieser Arbeit sondern auch für das wiederholt in mich gesetzte Vertrauen und die fachliche und die menschliche Unterstützung während der vergangenen Jahre.

Herrn Univ.-Prof. Dr. rer. nat. P. C. Müller danke ich für die Erstellung des zweiten Gutachtens und die Mitwirkung im Promotionsausschuss. Herrn Univ.-Prof. Dr.-Ing. Dipl.-Wirtsch.-Ing. B. H. Müller danke ich für seinen Vorsitz im Promotionsausschuss. Herrn Univ.-Prof. Dr.-Ing. U. Barth danke ich für seine Mitwirkung im Promotionsausschuss.

Meinen Kollegen bei BMW danke ich für die sehr gute und angenehme Zusammenarbeit, ihr Interesse und ihre Unterstützung.

Ein besonderer Dank gilt Herrn Dr.-Ing. Martin Woltereck, der mich zur Funktionssicherheit und mit der Fehlerbaumanalyse in Berührung brachte.

München im Dezember 2009 Simon Schilling

Kurzfassung

Hintergrund

Die *Fehlerbaumanalyse* (engl. *Fault Tree Analysis*, FTA) ist eine etablierte Methode zur qualitativen und quantitativen Modellierung und Analyse des Ausfallverhaltens von Systemen unter Gesichtspunkten der Zuverlässigkeit und funktionalen Sicherheit. Die FTA vermag als eine Boolesche, statische Modellierungsmethode ohne Zeitkonzept dynamische Effekte im Ausfallverhalten nicht oder nur mit statischen Näherungen zu modellieren.

Existierende Erweiterungen der FTA um dynamische Effekte, insbesondere Reihenfolgen, überführen die in der FTA modellierte Systemstruktur ganz oder teilweise in zustandsbasierte Modelle, lösen diese und führen die Ergebnisse in die FTA zurück. Eine solche *dynamische FTA* besitzt Einschränkungen, insbesondere die exponentielle Zunahme der zu berücksichtigenden Zustände und den Verzicht auf Vereinfachungspotentiale der (Booleschen) Fehlerbaum-Logik. Der Wechsel in den Zustandsraum erschwert zudem die Durchführung bzw. Aussagekraft qualitativer Analysen, wie sie aus der statischen FTA bekannt sind.

Insbesondere mit Blick auf den jeweils notwendigen Aufwand als limitierende Anforderung an eine praxisgerechte Modellierungs-Methode besteht daher Bedarf nach einem Vorgehen, welches dynamische Effekte wie Reihenfolgen von Ausfallereignissen berücksichtigt, ohne auf den Zustandsraum auszuweichen.

Die vorliegende Arbeit liefert einen Beitrag zur Lösung dieser Problematik.

Konzept

Der hier beschriebene neue Ansatz erweitert die statische FTA um die Abbildung von Ereignissequenzen zur *Temporale Fehlerbaumanalyse* (TFTA).

Die TFTA beruht auf einer *temporalen Logik*, welche die Boolesche Logik und Algebra der herkömmlichen FTA um ein Zeitkonzept erweitert. Diese temporale Logik beschreibt qualitativ *temporal-logische Ereignis-Beziehungen* zwischen Ereignissen und berücksichtigt dabei deren Zusammenspiel und Eintretens-Zeitpunkte. Temporal-logische Ereignis-Beziehungen werden mit den *Booleschen Operatoren* AND „$\wedge$“, OR „$\vee$“, NOT „$\neg$“ sowie den neuen *temporalen Operatoren* PAND „$\vec{\wedge}$“ und SAND „$\bar{\wedge}$“ ausgedrückt.

Ein *temporaler Term* mit diesen Operatoren lässt sich mit Hilfe der Booleschen Algebra sowie eines Satzes an *temporalen Logik-Regeln* in eine der Booleschen DNF ähnliche Form überführen, die sogenannte *Temporale Disjunktive Normalform* (TDNF).

Der das TOP repräsentierende temporale Term heißt *temporale Systemfunktion* ϖ. Analog zu den *Minimalschnitten* (*Minimal Cutsets*, MCS) der herkömmlichen FTA mit *Boolescher Systemfunktion* φ heißen die Ereignissequenzen der temporalen Systemfunktion ϖ in TDNF *Minimalsequenzen* (*Minimal Cutsets Sequences*, MCSS), wenn sie keine weiteren Ereignissequenzen enthalten.

Neben der qualitativen Analyse der MCSS ermöglicht die TFTA eine Quantifizierung des temporalen Fehlerbaums ohne Transformation und Berechnung im Zustandsraum. Analog zur herkömmlichen FTA ergibt sich die Eintretenswahrscheinlichkeit bzw. -rate des TOP aus den jeweiligen Größen der einzelnen MCSS. Diese berücksichtigen die Reihenfolge ihrer Basisereig-

nisse. Ihre Eintretenswahrscheinlichkeit bzw. -rate ergibt sich durch Faltung der Ausfalldichten ihrer Basisereignisse.

Realisierung

Ausgehend von der statischen FTA beschreibt diese Arbeit Regeln für die TFTA, mit denen sich a) temporallogische Terme in eine TDNF überführen lassen und b) in dieser TDNF auch disjunkte Terme erzeugen lassen. Die vorliegende Arbeit beschreibt weiterhin die Quantifizierung temporaler Ausfallfunktionen ausgehend von der TDNF mit disjunkten Termen. Zudem werden zwei Näherungsverfahren vorgestellt, mit denen sich die exakten probabilistischen Ergebnisse mit deutlich verringertem Aufwand annähern lassen. Die Vorgehensweisen werden an verschiedenen Beispielen unterschiedlicher Komplexität demonstriert.

Ergebnisse

Die wesentliche Neuerung des hier beschriebenen, neuen Ansatzes einer temporalen FTA gegenüber anderen Ansätzen einer Dynamisierung der herkömmlichen FTA ist die qualitative und quantitative Modellierung und Analyse von Reihenfolgen zwischen den (Basis-)Ereignissen eines Fehlerbaums ohne Modularisierung und Transformation in den Zustandsraum.

Zu den besonderen Vorteilen der TFTA zählen die Modellierung dynamischer Effekte auf allen Ereignisebenen des Fehlerbaums, die vollständige qualitative Analyse sowie eine quantitative Modellierung und Analyse ohne Methodenwechsel.

Abstract

Background

Fault tree analysis (FTA) is a well established method for qualitative as well as probabilistic reliability and safety analysis. Fault trees are Boolean models and thus do not support modelling of dynamic effects like sequence dependencies between fault events. In order to overcome this limitations, *dynamic fault tree* methods were defined previously. Most of these are based on complete or partial transformation of the fault tree model into state-space-models like Markov chains or Petri nets. These state-space-models generally suffer from exponential state explosion which imposes the necessity to define small "dynamic" modules which need to be independet from the rest of the model. Moreover, these state-space-models lack some of the FTA's benefits like logical simplification of complex system functions or a real cutset analysis. Because of these deficiencies, a method is needed that allows consideration of sequence dependencies without transformations into state-space. This work describes such a new approach.

Concept

The new *temporal fault tree analysis* (TFTA) described in this work extends the Boolean FTA in order to take sequence dependencies into account. The TFTA is based on a new *temporal logic* which adds a *concept of time* to the Boolean logic and algebra. This allows modelling of temporal relationships between events using Boolean operators (AND „$\wedge$“, OR „$\vee$“, NOT „$\neg$“) and two new temporal operators (PAND „$\vec{\wedge}$“ and SAND „$\bar{\wedge}$“). With a set of *temporal logic rules*, a given *temporal term* may be simplified to its *temporal disjunctive normal form* (TDNF) which is similar to the Boolean DNF but includes event sequencies. In TDNF the top event's temporal system function may be reduced to a list of *minimal cutset sequences* (MCSS). These allow qualitative analyses similar to Boolean cutset analysis in normal FTA. Furthermore the TFTA may also be used for probabilistic analyses. Probabilities and rates of MCSS may be calculated without using state-space models. Again the procedure is similar to the normal FTA: top event failure probabilities and rates are derived from the failure probabilities and rates of the basic events including sequence dependencies.

Realisation

Starting with the Boolean FTA this work describes a new notation and new rules for a temporal logic. This temporal logic aims at transforming temporal terms into a TDNF, which then may be transformed further into a form where all terms are mutually exclusive. This form is well suited for quantification, too. Several examples are provided which explain each step in detail. Furthermore, there are two probabilistic approximation methods described, which allow a significant reduction of the calculatory effort.

Results

One significant aspect of the new TFTA described in this work is the possibility to take sequence dependencies into account for qualitative and probabilistic analyses without state-space transformations. Among others, this allows for modelling of event sequencies at all levels within a fault tree, a real qualitative analysis similar to the FTA's cutset analysis, and quantification of sequence dependencies within the same model.

Allgemeiner Hinweis

Die in dieser Arbeit vorgestellten Sicherheits- und Zuverlässigkeitsuntersuchungen dienen der Darstellung neuer Analysemethoden an Hand von Beispielen. Dazu werden u. a. technische Funktionen und Daten in Anlehnung an reale Systeme verwendet. Diese lassen jedoch keine Aussagen über die Sicherheit und Zuverlässigkeit spezieller, real existierender Systeme zu.

Inhaltsverzeichnis

1 Einleitung

System safety is organized common sense.

(Mueller)

1.1 Motivation

Die FTA ist eine der wichtigsten Methoden zur qualitativen und quantitativen Modellierung und Analyse von Systemen unter Gesichtspunkten von Zuverlässigkeit und funktionaler Sicherheit. In der Automobiltechnik nimmt der Anteil sicherheitsrelevanter Elektronik zu [1], wodurch das Thema der funktionalen Sicherheit zunehmend größere Bedeutung erlangt [2]. Diese Entwicklung schlägt sich aktuell auch in der Ableitung eines neuen branchenspezifischen Sicherheits-Standards ISO 26262 [3] aus der generischen Grundnorm IEC 61508 [4] nieder.

In der Automobilindustrie kommt die FTA in verschiedenen Phasen der Entwicklung zur Allokation von Sicherheitsanforderungen ebenso wie für Nachweise gegenüber normativen Anforderungen oder dem Architektur-Vergleich zum Einsatz.

Die FTA ist in ihren Grundzügen heute Stand der Technik, vgl. z. B. [5–9]. Gleichwohl existieren verschiedene bislang unvollständig behandel te und noch nicht zufriedenstellend gelöste Problemfelder rund um die Methode FTA. Zu diesen findet auch heute noch rege Forschungstätigkeit statt.

Die vorliegende Arbeit resultiert aus der Praxiserfahrung in der Zentralabteilung für funktionale Sicherheit eines großen deutschen Fahrzeugherstellers. Die herkömmliche, d. h. statische FTA kann die an sie gestellten Anforderungen nicht immer erfüllen, insbesondere in Bezug auf eine realistische aber nicht zu konservative Modellierung moderner elektrischer / elektronischer (E / E) Systeme.

Betriebs- und Ausfallverhalten dieser Systeme ist u. a. gekennzeichnet durch einen hohen Grad an Dynamik. Diese äußert sich in strukturellen wie zeitlichen Abhängigkeiten zwischen einzelnen Teilsystemen, Funktionen oder Komponenten bzw. deren Ausfällen [10].

Die Fehlerbaum-Methode ist jedoch auf binäre und diskrete Prozessgrößen beschränkt und basiert auf der Booleschen (Ausfall-)Logik. Dies hat u. a. zur Folge, dass keine zeitlichen Abhängigkeiten oder Abhängigkeiten zwischen Ausfallraten der Basisereignisse bestehen dürfen. Beide Einschränkungen lassen sich im Einzelfall und unter Einbeziehung bestimmter Annahmen und Modellierungs-Kniffe teilweise umgehen, sie lassen sich aber nicht vollständig aufheben.

Darüber hinaus existiert bei der Verwendung der FTA ein Konflikt zwischen konservativen Näherungen und dem Ziel, unnötigen Aufwand beim System-Design zu vermeiden. Es ist darauf zu achten, dass nicht die Ungenauigkeit der Modellierung der Auslöser für eine komplexere und aufwändigere Lösung, also letztlich ein teureres System, ist.

Die Problematik einer realistischen Abbildung von dynamischen Effekten und Abhängigkeitseffekten in der FTA ist nicht neu [11–13]. Grundsätzlich besteht die Möglichkeit, die Modellierung mit anderen – dynamischen – Modellierungs-Methoden anstelle der FTA durchzuführen. Allerdings besticht die FTA im Vergleich zu den meisten anderen Methoden durch einfache Benutzbarkeit sowie gute Lesbarkeit, Verständlichkeit und Skalierbarkeit. Letztendlich resultieren diese Eigenschaften aus der Nähe der Fehlerbaumstruktur zur realen Systemstuktur, wie sie insbesondere für zustandsbasierte Modellierungen nicht gegeben ist. Aus diesen praktischen Gründen entwickelte sich die FTA nicht nur in der Automobiltechnik zur Standard-Methode für Zuverlässigkeits- und Sicherheitsanalysen [14, Kapitel 14.4.2].

Seit einigen Jahren existieren Ansätze, zustandsbasierte Modellierungen und die FTA so zu kombinieren, dass die Vorteile beider Verfahren genutzt und die Nachteile umgangen werden. Konkret soll der Nutzer innerhalb seiner gewohnten und intuitiven Fehlerbaum-Methode arbeiten, während Dynamik- und Abhängigkeitseffekte automatisiert und im Hintergrund durch zustandsbasierte Methoden berechnet werden.

Auch diese hybriden Ansätze einer dynamischen FTA besitzen jedoch spezifische Nachteile. Insbesondere nutzen sie den Fehlerbaum primär als Werkzeug zur Visualisierung bzw. Modellerstellung und nicht auch für die tatsächliche Analyse und Berechnung und verzichten daher auf einige der Vorteile der FTA.

Aus diesen Problemen, aber auch aus rein wissenschaftlicher Neugierde, motivierte sich die intensive Beschäftigung mit der Frage, ob und wie sich zumindest Teilaspekte der dynamischen und abhängigkeitstechnischen Probleme effizienter innerhalb des Fehlerbaums lösen lassen.

Die vorliegende Arbeit beschreibt die Ergebnisse dieser Überlegungen.

1.2 Aufbau der Arbeit

Diese Dissertation befasst sich mit der Erfassung dynamischer Effekte in Sicherheits- und Zuverlässigkeits-Analysen, insbesondere dem Teilgebiet der Modellierung von Reihenfolgen mehrerer Ausfall-Ereignisse mittels der Fehlerbaum-Methode. Die Arbeit ist wie folgt aufgebaut.

Kapitel 2 beschreibt den für diese Arbeit relevanten Stand der Technik, insbesondere die statische, Boolesche FTA (Kapitel 2.2) sowie dynamische Erweiterungen derselben (Kapitel 2.3) durch einerseits Transformationen des Fehlerbaum-Modells in den Zustandsraum und andererseits die Verwendung erweiterter, temporaler Logiken.

Diese Übersicht zeigt Defizite im heutigen Stand der Technik auf, welche in direktem Zusammenhang mit dem Wechsel der Betrachtungsweise und dem Bruch zwischen den Berechnungsmethoden stehen. Kapitel 3 erfasst die daraus resultierende Problemstellung und leitet daraus Kriterien und Eigenschaften ab, die an einen neuen Ansatz zu stellen sind.

Kapitel 4 beschreibt diesen neuen Ansatz, die Reihenfolge von Ereignissen innerhalb der Fehlerbaum-Methode abzubilden, ohne in den Zustandsraum zu wechseln. Die neue *Temporale Fehlerbaumanalyse* (TFTA) benötigt eine über die Boolesche Algebra und Logik hinausgehende *Temporale Logik* mit eigener Notation (Kapitel 4.1) und eigenen Logik-Regeln (Kapitel 4.2). Kapitel 4.3 beschreibt den Übergang zu disjunkten minimalen Ausfallsequenzen. Eine Verringerung des Aufwandes zur Beschreibung komplexerer temporaler Ausfallfunktionen liefert die erweiterte Form der TFTA in Kapitel 4.4.

Als Erweiterung zur rein qualitativen TFTA diskutiert Kapitel 5 die Quantifizierung temporaler Terme als Grundlage einer quantitativen Auswertung temporaler Fehlerbäume.

Kapitel 6 vergleicht die neue TFTA anhand typischer Systemstrukturen mit a) der herkömmlichen Booleschen FTA, b) dem Dynamic Faulttree Ansatz (DFT) als typischem Vertreter

herkömmlicher dynamischer Erweiterungen der Booleschen FTA und c) einer reinen Markov-Modellierung.

Die praktische Anwendbarkeit der TFTA wird in Kapitel 7 gezeigt. Anhand einer typischen KFZ-Steuergeräte-Architektur ist die gesamte Kette von der Systemanalyse über die Erstellung des temporalen Fehlerbaums bis zur qualitativen und quantitativen Berechnung und Auswertung skizziert.

Die Arbeit schließt mit einer Zusammenfassung und einem Ausblick (Kapitel 8).

2 Stand der Technik: Statische und dynamische Fehlerbaumanalyse

Of course it is safe, we certified it.

(Ein Sprecher der FAA)

Dieses Kapitel enthält eine Übersicht zum Stand der Technik, der für die TFTA relevant ist.

- Kapitel 2.1 beschreibt das Umfeld sicherheitstechnisch angelegter Fehlerbaumanalysen.
- In ihrer klassischen und rein statischen Form, vgl. Kapitel 2.2, ist die FTA heute eine der gängigsten Modellierungsmethoden für systematische, deduktive, qualitative und quantitative Analysen des Ausfallverhaltens komplexer Systeme.
- Auf Grund der teilweise schwerwiegenden Einschränkungen einer rein statischen Modellierung existieren heute mehrere Ansätze, die FTA um dynamische Ausfalleffekte zu erweitern, vgl. Kapitel 2.3. Diese beruhen entweder auf zustandsbasierten Methoden (Kapitel 2.3.3) oder nutzen temporale Ausfalllogiken (Kapitel 2.3.4).
- Die Zusammenfassung des Standes der Technik in Kapitel 2.4 leitet die dieser Arbeit zugrundeliegende Problemstellung in Kapitel 3 ein.

2.1 Hintergrund und Umfeld

2.1.1 Zuverlässigkeits- und Sicherheitsanalysen

Die *Zuverlässigkeit* eines Systems oder einer Komponente (allgemein: einer Einheit) ist deren „Fähigkeit [...], innerhalb der vorgegebenen Grenzen denjenigen durch den Verwendungszweck bedingten Anforderungen zu genügen, die an das Verhalten ihrer Eigenschaften während der gegebenen Zeitdauer gestellt sind“ [15]. Eine ausgefallene Einheit kann ihre Funktionalität nicht mehr erbringen, weswegen die klassische *Zuverlässigkeitsanalyse* das Ausfallverhalten von Einheiten betrachtet.

Diese Analyse umfasst im wesentlichen die folgenden Aufgaben [16]: Sie unterstützt die Entwicklung neuer Systeme, indem sie – auch zukunftsgerichtet – verschiedene Systemkonzepte untereinander und gegenüber objektiven Anforderungen vergleicht (*Zuverlässigkeits-Voraussage*, *Zuverlässigkeits-Vergleich*, *Zuverlässigkeits-Verfolgung*, *Schwachstellen-Identifikation*). Zudem ermöglicht sie den *Zuverlässigkeits-Nachweis* für bestehende Systeme und Konzepte. Zur Erfüllung dieser Aufgaben kommen oftmals dieselben Methoden und Analyseverfahren zum Einsatz.

Im Gegensatz zur Zuverlässigkeitsanalyse konzentriert sich die *Sicherheitsanalyse* auf die Untermenge solcher System- und Komponentenausfälle, die zu einem Verlust der „Sicherheit“ führen, wobei Sicherheit definiert ist als „Freiheit von unvertretbaren Risiken“ [4]. Die sicherheitstechnisch relevante Zuverlässigkeit einer Einheit ist somit deren Eigenschaft – oder bei quantitativer Betrachtung: deren Wahrscheinlichkeit –, innerhalb eines definierten Zeitraums und unter definierten Randbedingungen keine *gefährlichen Auswirkungen* (Schäden) zu verursachen. Damit berücksichtigt die sicherheitstechnisch relevante Zuverlässigkeit auch die Auswirkungen von Ausfällen.

Sicherheitsanalysen bedürfen somit einer weitergehenden Festlegung hinsichtlich der Frage, welches Risiko bzw. welche Schäden betrachtet werden. Im Umfeld der klassichen Sicherheit – im Sinne von *safety* – technischer Systeme sind dies das Risiko für Leib und Leben bzw. das Verletzen / Töten von Personen [4]. Prinzipiell finden dieselben Analysen und Methoden auch Anwendung in anderen Betrachtungen, z. B. im Umfeld der Sicherheit – im Sinne von *security* – technischer Systeme [17, 18]. Im Rahmen dieser Arbeit wird *Sicherheit* in der Bedeutung von *safety* verwendet. Ausnahme ist der Begriff der *Kenntnisstandsicherheit*, welcher sich auf die Verlässlichkeit (Konfidenz) von Daten und Modellen bezieht.

2.1.2 Statische und dynamische Analysen

2.1.2.1 Dynamisches Systemverhalten

Ein dynamisches Verhalten eines Systems ist nach [19] gegeben, falls die Systemantwort auf eine initiale Störung sich über die Zeit entwickelt, während die System-Komponenten miteinander und mit ihrem Umfeld interagieren. Im Gegensatz dazu behandelt die klassische Fehlerbaumanalyse unerwünschte Ereignisse (Systemausfälle) als statische, festgelegte und zeitlich invariante Folge einer bestimmten Kombination von Komponenten-Ausfällen [ebd.].

In einer Welt voller dynamischer Einflüsse und Wechselwirkungen verhalten sich grundsätzlich alle technischen Systeme ebenfalls dynamisch. Statische Methoden und Modelle zur Zuverlässigkeits- und Sicherheitsanalyse von Systemen approximieren daher notwendigerweise immer nur deren eigentlich dynamisches Verhalten.

Auf Grund dieser Vereinfachung sind statische Analysen wie die FTA oder *Zuverlässigkeits-Blockschaltbild (Reliability Block Diagram)* (RBD) vergleichsweise einfach zu handhaben. Tatsächlich ermöglicht in vielen Fällen erst die Annahme statischen Verhaltens überhaupt eine Analyse. Die in der praktischen Anwendung relevante Frage lautet daher, welche statischen Näherungen es vermögen, das eigentlich dynamische Ausfallverhalten „gut genug“ abzubilden.

Hierbei hat sich gezeigt, dass die herkömmliche FTA sehr gut geeignet ist für die logische und probabilistische Analyse von Systemen, deren Ausfallverhalten zumindest in erster Näherung als frei von zeitlichen Abhängigkeiten oder dynamischen Interaktionen zwischen den einzelnen Komponenten bezeichnet werden kann.

Allerdings beklagen Forscher und Anwender schon seit den Anfängen der systematischen Untersuchung des Ausfallverhaltens technischer Systeme ab der Mitte des 20. Jahrhunderts die vergleichsweise grobe Betrachtungsweise der statischen Analysen [20]. Wissenschaft und Forschung suchen daher nach Möglichkeiten, statische Ausfallmodellierungen wie die FTA um die wichtigsten dynamischen Effekte zu erweitern, ohne den Modellierungs- und Berechnungsaufwand über Gebühr zu erhöhen.

2.1.2.2 Modellierungs-Arten

Mit Blick auf [21] und [22] lassen sich nach den verwendeten Modellierungsmethoden drei Kategorien *dynamischer Zuverlässigkeits- und Sicherheitsanalysen* (ZSA) unterscheiden. Dies sind im jeweils weitesten Sinne

- Zustandsübergangs-Modelle, insbesondere Markov-Modelle, z. B. [23], und
- direkte Simulationen des Systems, insbesondere mittels Monte-Carlo-Simulation (MoCaS), z. B. [13, 24], sowie
- Erweiterungen der eigentlich statischen Ereignisablaufanalysen / der FTA um die Möglichkeit, auch dynamische Effekte abzubilden. Auf diese gehen die folgenden Kapitel näher ein.

2.2 Statische, klassische FTA

Historisch lässt sich die FTA bis in die Mitte des 20. Jahrhunderts zurückverfolgen, als die Zuverlässigkeit der Minuteman Rakete analysiert wurde [25, 26].

Der klassische Fehlerbaum [6–8] ist ein Boolesches Modell, welches auf systematische und methodische Weise das Zusammenspiel von Teil-Ausfällen innerhalb eines Systems zu einem System-Ausfall beschreibt. Es handelt sich um eine *top-down* oder *deduktive* Methode. Ausgehend von einem unerwünschten Ereignis oder Zustand – dem sogenannten *TOP* – werden schrittweise detaillierter alle Ursachen gesucht, die zum TOP führen. Die graphische Darstellung erfolgt in Form eines Schaltnetzes, dem *Fehlerbaum*. Die im Fehlerbaum modellierten Ausfälle von Komponenten werden durch Ereignisse repräsentiert, die gemäß Boolescher Logik zwei Zustände einnehmen: „intakt / Ausfall nicht eingetreten“ wird repräsentiert durch ein logisches False oder 0, „defekt / Ausfall eingetreten“ wird repräsentiert durch ein logisches True oder 1.

Die Auswertung des Fehlerbaums erfolgt auf qualitative und quantitative Weise. Das Gesamt-System besteht aus klar voneinander abgegrenzten Elementen (Komponenten), die jeweils eigene Zuverlässigkeits- bzw. Sicherheits-Eigenschaften besitzen und über die logische Verknüpfung die Systemzuverlässigkeit bzw. -sicherheit beeinflussen. Das Fehlerbaum-Modell leitet mit dieser Verknüpfung die System-Kenngrößen aus den Komponenten-Kenngrößen ab.

Die Vereinfachungsregeln der Booleschen Algebra überführen die *Systemfunktion* / *Ausfallfunktion*, d. h. die Logikfunktion des TOP, in eine minimale disjunktive Normalform. Die so ermittelten *Minimalschnitte* des Fehlerbaums lassen sich gemäß der Regeln der Wahrscheinlichkeitsrechnung in eine probabilistische Form überführen und nummerisch auswerten. Die Wahrscheinlichkeit bzw. Häufigkeit des Eintretens des unerwünschten Ereignisses oder Zustands ist – bei nicht reparierbaren Systemen – die Ausfallwahrscheinlichkeit bzw. Ausfalldichte oder Ausfallrate des TOP oder – bei reparierbaren Systemen – die Unverfügbarkeit bzw. Ausfallfrequenz des TOP [27]. Weiterhin erlaubt die Nähe des Modells zur realen Systemstruktur auch eine qualitative Analyse der System-Architektur und insbesondere der Redundanz-Strukturen sowie Sensitivitäts- [28], Importanz- [29] und Konfidenz-Analysen [30].

Die qualitative und quantitative statische FTA ist Stand der Technik in vielen Anwendungsbereichen wie der Nukleartechnik und Anlagenindustrie [5], der Luft- und Raumfahrt [31] oder der Automobiltechnik [9, 32]. Großer Forschungsbedarf existiert hingegen bei Verwendung der FTA zur Untersuchung von Software-„Ausfällen“ [33], insbesondere auch wegen der unten genannten Schwierigkeiten, dynamische Effekte abzubilden.

Die FTA ist – im Vergleich zu anderen Modellierungsmethoden wie z. B. den zustandsbasierten Markov-Diagrammen – intuitiv in der Anwendung, d. h. sie ist einfach erlernbar und Fehlerbäume lassen sich einfach erstellen, lesen, verstehen, ändern und anpassen, iterativ detaillieren und modular wiederverwenden.

Als wesentliche Einschränkungen fordert die FTA die Zweiwertigkeit der Ereignisse, die Erfüllung der *Monotonie-* oder *Kohärenz-Bedingung* [34, 35] und die Unabhängigkeit zwischen ihren Basis-Ereignissen. Des Weiteren kann die FTA dynamisches Ausfall- und Reparatur-Verhalten nur sehr eingeschränkt abbilden [12]. Dies ergibt sich aus der Booleschen Logik [36], welche kein Zeitkonzept kennt und daher ausschließlich die strukturellen Aspekte der Ausfallkombinatorik erfasst [34]. Sie macht damit keine Aussagen über die Reihenfolge des Eintretens von Ereignissen oder anderen zeitlichen Abhängigkeiten, vgl. Kapitel 2.3.1.

2.3 Dynamische FTA

Der Begriff der *dynamischen FTA* wird heute oftmals gleichgesetzt mit dem DFT-Ansatz nach Dugan [37]. Dieser nutzt Markov-Ketten, um die statische FTA um eine Möglichkeit zu erweitern, auch *sequence dependiencies* (Sequenz-Abhängigkeiten) modellieren und analytisch lösen zu können.

Der DFT-Ansatz definiert somit den Begriff der Dynamik über Ereignissequenzen. Dieses Verständnis von Dynamik als Möglichkeit der Abbildung von Ereignissequenzen wird auch in der vorliegenden Arbeit und dem in Kapitel 4 beschriebenen TFTA-Ansatz zugrunde gelegt.

2.3.1 Dynamik-Definition über die Reihenfolge

Die Boolesche Logik ist mit ihren UND-, ODER- und NICHT-Operationen nicht in der Lage, zeitliche Beziehungen zwischen Ereignissen auszudrücken. Seien z. B. die Ausfälle zweier Komponenten A und B eines Systems betrachtet. Das Ereignis „A UND B“ steht für „beide Komponenten ausgefallen“. Es enthält jedoch keine Informationen über die tatsächlichen Zeitpunkte des Eintretens von A und B bzw. daraus abgeleitet die Reihenfolge des Eintretens beider Ereignisse. Diese Boolesche Betrachtungsweise erfasst ausschließlich den statischen Zustand, dass zwei Komponenten ausgefallen sind bzw. nicht ausgefallen sind.

Im Gegensatz dazu unterscheidet eine dynamische Betrachtungsweise zwischen verschiedenen Wegen, zu einem Ereignis oder Zustand zu gelangen. Damit geht sie über die rein statische Analyse nur der möglichen Kombinationen von Ereignissen hinaus [38].

Für „A UND B“ existieren drei mögliche solche Wege. Erstens kann zunächst A und später B ausfallen. Zweitens kann zunächst B und später A ausfallen. Drittens können A und B genau gleichzeitig ausfallen.

Jeder dieser Wege führt zum – aus Boolescher Sicht selben – Zustand, in dem beide Komponenten ausgefallen sind. Diese Unterscheidung der möglichen Wege zu einem Ereignis / Zustand lässt sich in Zustandsübergangs-Diagrammen darstellen. Abbildung 2.1 zeigt das zu obigem Beispiel passende Zustandsübergangs-Diagramm.

Dynamik als Form der Unterscheidung verschiedener Wege zu einem Ereignis / Zustand erfolgt also mittels zeitlicher Angaben wie „vor“, „nach“, „erst“, „dann“, „gleichzeitig“ usw. Die Modellierung von Dynamik erfordert daher die Fähigkeit, Eintretenszeitpunkte von Ereignissen zu unterscheiden. Diese Fähigkeit setzt die Existenz eines *Zeitkonzeptes* innerhalb des Modells vorraus [39]. Umgekehrt erlaubt die Unterscheidung der Eintretenszeitpunkte die Differenzierung verschiedener Ereignissequenzen. Mit diesen lassen sich eine Vielzahl dynamischer Effekte beschreiben [12, 40].

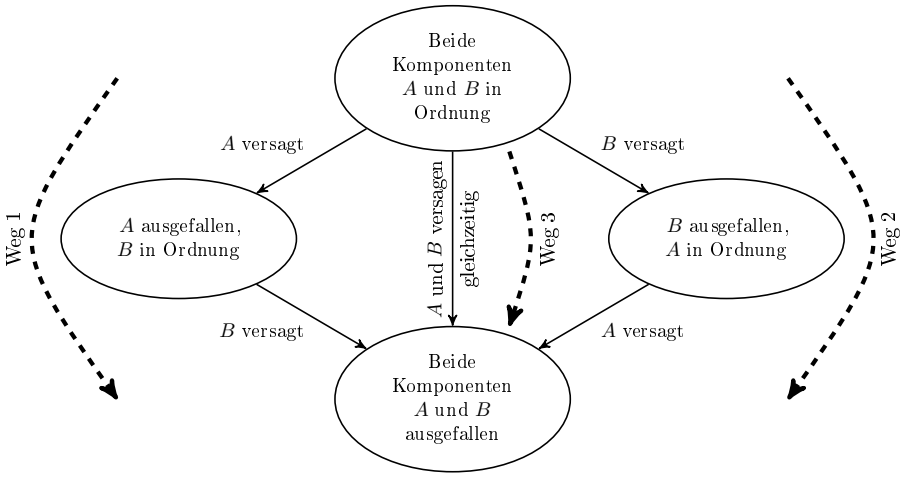


Abbildung 2.1: Zustandsübergangs-Diagramm eines einfachen redundanten, nicht reparierbaren Systems, bestehend aus zwei Komponenten A und B mit den dabei möglichen vier Zuständen und fünf Zustandsübergängen.

Weiteres Vorgehen

Der in dieser Arbeit vorgestellte Beitrag zur dynamischen FTA basiert ebenfalls auf einem Verständnis von Dynamik als Möglichkeit der Abbildung von Ereignissequenzen. Der folgende Abschnitt 2.3.2 grenzt dieses Verständnis von anderen Interpretationen des Begriffs „Dynamik“ im Umfeld allgemeiner ZSA und insbesondere im Umfeld der FTA ab. Abschnitt 2.3.3 diskutiert typische Umsetzungen dieses Dynamik-Verständnisses, insbesondere solche auf Basis von Markov-Ketten und Petri-Netzen. Abschnitt 2.3.4 skizziert anschließend einen grundsätzlich anderen Weg zur Erweiterung der FTA um Reihenfolgen und stellt dazu verschiedene Ansätze einer erweiterten (temporalen) Ausfalllogik vor. Kapitel 2.4 fasst den so aufgezeigten Stand der Technik zur dynamischen FTA zusammen.

2.3.2 Weitere Dynamik-Definitionen

Neben der Berücksichtigung von Reihenfolgen existieren weitere zeitliche Abhängigkeiten zwischen (Ausfall-)Ereignissen und weitere Definitionen von Dynamik im Umfeld von ZSA, von denen einige im Folgenden aufgeführt sind. Eine zwar nicht mehr ganz aktuelle aber weiterhin gültige Übersicht liefert [41].

Grundsätzlich unterscheidet [42] zwischen Dynamikeffekten in Analysen durch zeitabhängige Ausfallraten, zeitabhängige Unverfügbarkeiten, die Abnahme der Kenntnisstandunsicherheit bezüglich der verwendeten Daten sowie durch Ausfall-Sequenzen (Reihenfolgen).

Abstrahiert man diese Kategorien, so ist einerseits zu unterscheiden zwischen Dynamik im Sinne veränderlicher Daten und andererseits Dynamik im Sinne des Ereignis-Ablaufs. Vielfach werden als dritte Kategorie die *Phased Mission* Methoden genannt, vgl. z. B. [39, 43] oder [44]. Prinzipiell lassen sich diese den beiden erstgenannten Kategorien zuordnen oder auch als abschnittsweise statische Analysen bezeichnen.

Eine weitere Unterscheidung in „schnelle“ und „langsame“ dynamische Zeitabhängigkeiten findet sich in [22]. Langsame Dynamik-Effekte treten während des Normalbetriebs auf, z. B. in Form von Alterung, Lerneffekten oder Systemveränderungen. Demgegenüber bezeichnen schnelle Effekte den Störfall und stehen als solche im Fokus der dynamischen ZSA. In [22] erfolgt die Berechnung der dynamischen ZSA mittels MoCaS.

Die genannten Quellen stammen vor allem aus dem Umfeld der (nuklearen) Anlagentechnik. Sie betonen daher neben der expliziten Berücksichtigung von zeitlichen Abhängigkeiten auch die Betrachtung der *Human Reliability Analysis* (HRA) [45] als weiteren wichtigen Teil einer dynamischen ZSA. Die HRA spielt jedoch in der Automobilindustrie heute keine vergleichbare Rolle. Gründe hierfür sind

1. die bevorzugte Auslegung sicherheitskritischer Systeme als *Fail Safe Systeme* bzw. das Fehlen echter *Fail Operational Systeme* [46],

2. das Fehlen menschlicher Operatoren, die das Systemverhalten – auch im Störfall – direkt beeinflussen, und

3. das Fehlen von Inspektions-, Wartungs- und Reparatur-Teams, wie sie aus der Anlagen- oder Luftfahrtindustrie bekannt sind.

Es wird erwartet, dass die HRA für die Bewertung der funktionalen Sicherheit automotiver Systeme zukünftig wichtiger wird, insbesondere auf Grund der zunehmenden Integration hochspannungstechnischer Anlagenelemente in Elektro- und Hybrid-Fahrzeugen sowie der Zusammenführung von aktiver Sicherheit und Fahrerassistenzsystemen.

Zweitens existieren spezielle Ansätze zur dynamischen ZSA mittels MoCaS auch in der Automobiltechnik. So berücksichtigt z. B. [24] über zeitabhängige Ausfalldaten den Einfluss dynamischer Systemänderungen auf das Ausfallverhalten. Auf Grund des vergleichsweise hohen Aufwandes sind diese Ansätze jedoch Nischen-Lösungen und eignen sich (noch) nicht für den flächendeckenden Einsatz.

2.3.3 Dynamische FTA – Verschiedene Umsetzungen

Im Folgenden konzentriert sich diese Arbeit zur dynamischen FTA auf das Verständnis von Dynamik als Möglichkeit der Abbildung von Ereignissequenzen.

Typischerweise handelt es sich bei den bisherigen Ansätzen zu Erweiterungen der FTA um Dynamik-Effekte entweder um eine (automatische) Überführung des Fehlerbaum-Modells in ein Markov-Modell mit anschließender Lösung des resultierenden Differentialgleichungssystems oder um eine Simulation.

Der weithin bekannte DFT-Ansatz [37] basiert auf einer Modularisierung des Fehlerbaums in statische und dynamische Module, die anschließend mittels *Binary Decision Diagrams* (BDD) [47, 48] und Markov-Ketten berechnet werden. Statische Module bestehen ausschließlich aus Booleschen Gattern und Ereignissen, während dynamische Module zusätzlich auch dynamische Gatter enthalten. Mit diesen lassen sich Effekte wie Reihenfolgen, kalte, warme, heiße Redundanzen oder Trigger-Ereignisse erfassen. Abbildung 2.2 zeigt die wesentlichen Schritte dieser Vorgehensweisen im Vergleich zur herkömmlichen, statischen FTA.

DFT sind in einer Vielzahl von Fehlerbaum-Programmen in unterschiedlicher Vollständigkeit umgesetzt, z. B. in DIFTree [49] oder Galileo [38] sowie in einer Reihe kommerzieller FTA-Tools wie Isograph Faulttree+ [50], ITEM Toolkit [51] oder RELAX Reliability Studio [52]. DFT werden zudem in der neueren Version des *Faulttree Handbook* erwähnt [31].

Einen ähnlichen Ansatz verfolgt [53], wobei anstelle der Erstellung und Berechnung der Markov-Ketten *Dynamic Bayesian Networks* zur Anwendung kommen, welche den Berechnungsaufwand reduzieren.

Eine andere Alternative in [54] verwendet zur Lösung der DFT Module modifizierte BDD, die sogenannten *zero-suppressed binary decision diagrams* und bringt anstelle von Markov-Ketten

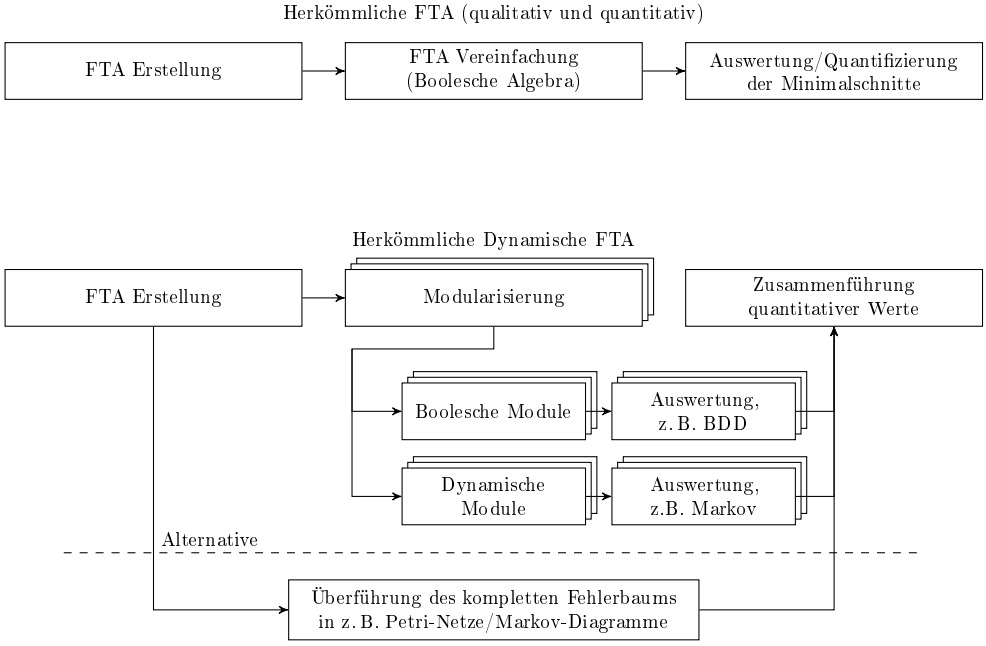


Abbildung 2.2: Die grundlegenden Schritte einer herkömmlichen FTA (oben) und im Vergleich dazu die wesentlichen Schritte bei Verwendung der herkömmlichen dynamischen Erweiterungen der Booleschen FTA mit Transformation in eine zustandsbasierte Modellierung.

die zeitlichen Abhängigkeiten in Form von Reihenfolgenbeschränkungen manuell in die relevanten Minimalschnitte ein. Dies beschränkt die Verwendung dynamischer Gatter jedoch auf vergleichsweise einfache Strukturen. Ein ähnliches Vorgehen ist auch in [55] diskutiert.

Der in [56, 57] vorgestellte Ansatz auf Basis von *Boolean Logic Driven Markov Processes* (BDMP) verbessert gegenüber den genannten Ansätzen die qualitative System-Auswertung und ermöglicht – unter Einschränkungen – auch die Berücksichtigung reparierbarer Komponenten.

Einen anderen Weg zur dynamischen FTA auf Basis von Petri-Netzen und ohne Markov-Modelle beschreiten [58] und [59, 60] sowie die *State-Event-Fault-Trees* in [61].

Diskussion

Diese Ansätze einer dynamischen FTA basieren auf der Transformation des ursprünglichen Fehlerbaum-Modells in eine zustandsbasierte Modellierungsmethode. In dieser lassen sich die zeitlichen Abhängigkeiten und damit auch Reihenfolgen berücksichtigen. Die Varianten unterscheiden sich zwar hinsichtlich der gewählten Transformation (kompletter Fehlerbaum wird transformiert einerseits und Modularisierung und Transformation nur der für die Dynamik relevanten Teilbäume andererseits) sowie der gewählten zustandsbasierten Methode.

Ihnen ist jedoch gemein, dass erstens der Berechnungsaufwand exponentiell mit der Größe der dynamischen Module ansteigt. Neuere Verfahren in [62, 63] reduzieren zwar den für die eigentliche Modularisierung notwendigen Zeitaufwand und erlauben diese mit lediglich linear zur Anzahl der Elemente steigendem Berechnungsaufwand. Die Komplexität der zur Lösung der Markov-Ketten verwendeten Methoden beträgt jedoch $O\{K \cdot N^3\}$ [64], wobei K von der Anzahl der Berechnungsschritte, und damit von der Missionzeit und der Genauigkeit, abhängt und N die Anzahl der Zustände im Markov-Modell ist, welche für n Einheiten in der Größenordnung

von $N = n^n$ liegt. Diese *Zustandsexplosion* (*state explosion*) [65] erzwingt eine Modularisierung mit möglichst kleinen dynamischen Modulen. Allerdings ist die Lösung der aus solchen Markov-Modellen resultierenden Differentialgleichungssysteme trotz Modularisierung oftmals nur näherungsweise möglich, vgl. z. B. [64].

Zweitens basiert die Modularisierung auf der Unabhängigkeit der einzelnen Teil-Probleme voneinander. Dies führt zu einer Beschränkung der berücksichtigten dynamischen Abhängigkeiten zwischen verschiedenen Einheiten des Systems oder zu einer Vergrößerung der einzelnen dynamischen Module – mit oben geschilderter Auswirkung auf den Berechnungsaufwand.

Drittens sind qualitative Analysen nicht bzw. nur für einfache Strukturen möglich. Dies ist durch den Wechsel in die Zustandsebene bedingt, die nicht dieselbe Nähe zur realen Systemstruktur besitzt wie ein Boolesches Systemmodell. Einer der wesentlichen Vorteile der FTA, die „automatische“ Reduzierung der modellierten Struktur auf eine minimale Form, fehlt daher in zustandsbasierten Modellierungen. So liefert z. B. die DFT (je nach Umsetzung) entweder die „normalen“ Booleschen Minimalschnitte, die dann keine Sequenzinformationen enthalten, oder sie liefert Minimalschnitte mit „Meta–Ereignissen“, hinter denen die kompletten Markov-Modelle stehen, die nicht weiter aufgelöst werden.

Viertens fehlt zustandsbasierten Modellierungen die „Benutzerfreundlichkeit“ Boolescher Methoden, welche ebenfalls aus der Nähe der Booleschen Modellstruktur zur realen Systemstruktur resultiert. Stattdessen werden Komponenten und deren Abhängigkeiten z. B. ausgedrückt durch Zustände und Zustandsübergänge (Markov-Methode) bzw. Stellen, engl. „places“, und Transitionen und Marken (Petri-Netze), vgl. Abbildung 2.3. Ein aus diesen Eigenschaften resultierender Effekt ist die im Vergleich zur FTA schlechtere Lesbarkeit, Verständlichkeit, Wartbarkeit und Skalierbarkeit zustandsbasierter Methoden und Modelle [67].

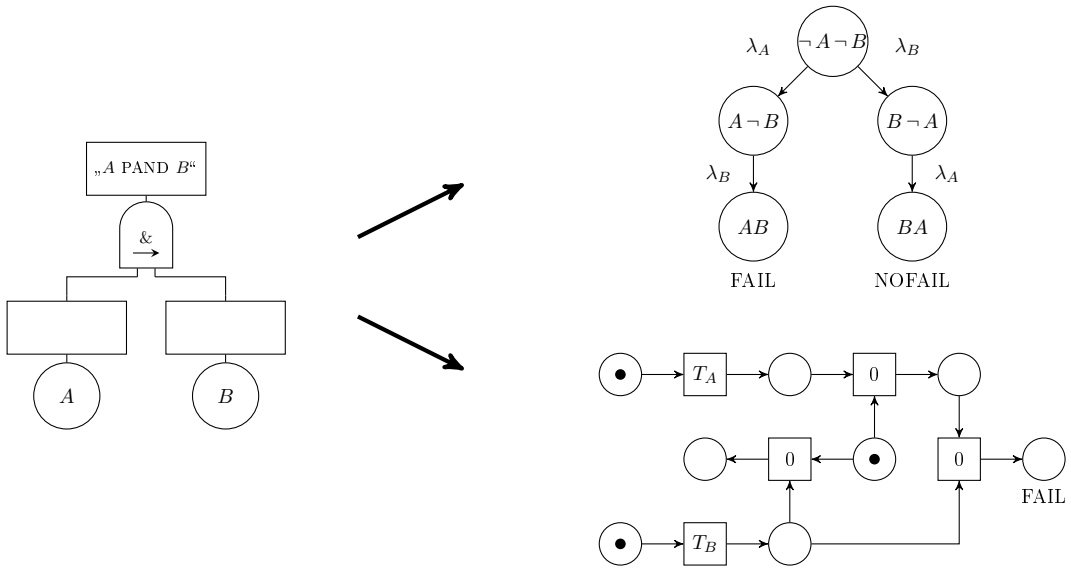


Abbildung 2.3: Links ein PAND-Gatter, dessen Eingänge A und B in der Reihenfolge A vor B eintreten müssen, damit das Gatter-Ereignis eintritt. Das verwendete Symbol entspricht nicht dem in [5] verwendeten, sondern stammt aus dem TFTA-Ansatz aus Kapitel 4. Rechts oben ist ein zu diesem PAND Gatter äquivalentes Markov-Modell nach [66] gezeigt, rechts unten ein äquivalentes Petri-Netz nach [59]. In Letzterem stehen T_A und T_B für die Lebensdauern von A und B.

2.3.4 Dynamische FTA mit temporaler Ausfalllogik

Eine andere Möglichkeit zur Abbildung zeitlicher Abhängigkeitseffekte bietet die Verwendung einer über die Boolesche Logik hinausgehenden, *zeitlichen* oder *temporalen Logik*. Eine solche Logik beschreibt nicht nur die strukturelle Kombination verschiedener Ereignisse – das wäre der Boolesche Ansatz –, sondern verfügt zusätzlich über ein Zeitkonzept. Mit diesem lassen sich Aussagen zu den Eintretens-Zeitpunkten der Ereignisse tätigen und innerhalb der Logikfunktion ausdrücken.

Im Kontext der Zuverlässigkeits- oder Sicherheits-Modellierung existieren mehrere Ansätze zeitlicher Logik für Fehlerbäume. Ein früher Ansatz zur Beschreibung von Reihenfolgen findet sich in [68]. Dieser konzentriert sich auf die quantitativen Aspekte der Modellierung einzelner Ereignissequenzen, ein Ansatz, der auch später aufgegriffen und präzisiert wurde, z. B. in [59] und [69]. Diese Arbeiten gehen jedoch nicht auf eine allgemeine zeitliche Logik ein, welche über die Betrachtung der einzelnen Reihenfolge hinausgeht. Sie setzen somit voraus, dass die relevanten minimalen Ausfallsequenzen, die zum TOP führen, auf anderem Wege gefunden werden. Dies schränkt ihre Anwendung für komplexere Projekte stark ein.

Der lange Zeit de-facto Standard der Fehlerbaum-Anleitungen, die erste Version des *Fault Tree Handbook* [5], enthält ebenfalls ein sogenanntes *Priority AND* (PAND) Gatter. Dieses dient ausschließlich der qualitativen Modellierung von Ereignissequenzen, quantitativ wird es wie ein normales AND Gatter behandelt. Auch dieser Ansatz beschränkt sich auf die einzelne Reihenfolge und liefert keine darüber hinausgehende allgemeine zeitliche Logik. So ist z. B. nicht beschrieben, ob und wie die in Abbildung 2.4 links gezeigte Fehlerbaum-Struktur zu vereinfachen ist und / oder ob sie der rechts in Abbildung 2.4 dargestellten Struktur entspricht. Im Booleschen Falle mit AND anstelle der PAND Gatter sind beide Strukturen äquivalent, da wegen des Distributivgesetzes der Booleschen Algebra, vgl. (4.32) auf Seite 35, gilt, dass $(A \wedge B) \vee (A \wedge C) = A \wedge (B \vee C)$.

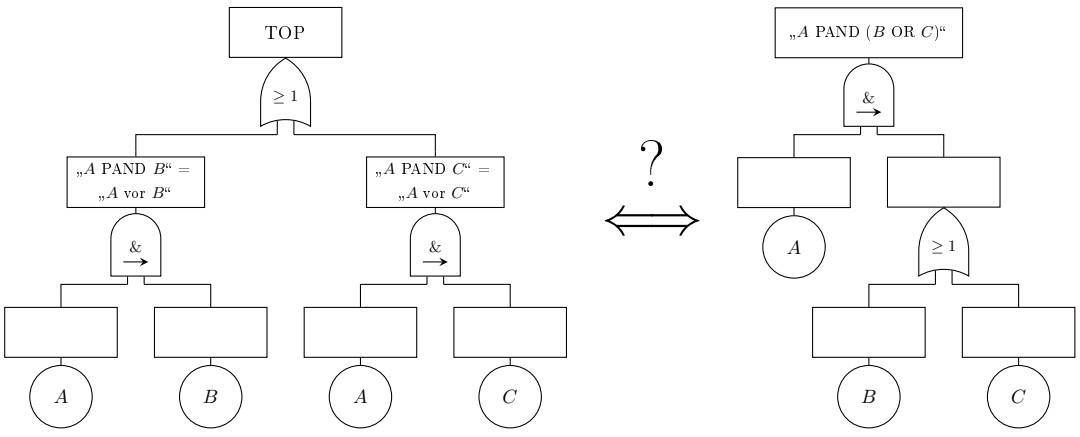


Abbildung 2.4: Fragen zum Stand der Technik dynamischer FTA mittels temporaler Logiken. Da den in [5] eingeführten PAND Gattern eine universelle zeitliche Logik fehlt, ist ungeklärt, ob die beiden dargestellen Fehlerbäume äquivalent sind, oder nicht. Die Symbolik des PAND entspricht hier nicht der aus [5] sondern der des TFTA-Ansatzes aus Kapitel 4.

Einen umfassenderen Ansatz verfolgen die intervallbasierte temporale Logik der sogenannten *AND Then Gatter* in [70], die Arbeiten in [71, 72] sowie die sogenannten *Temporal Faulttrees* in [73]. Diese stammen aus dem Umfeld der formalen Fehlerbaumanalyse, die sich insbesondere aus dem Wunsch motiviert, die Methodik der herkömmlichen FTA auch für die Modellierung von Software-Systemen und deren „Ausfällen“ zu verwenden. Ausfallbetrachtungen von Software-Systemen unterscheiden sich grundsätzlich von den klassischen hardware-orientierten ZSA, insbesondere wegen der andersartigen Ausfall-Mechanismen. Eine Übersicht über den Stand der Technik der FTA in der Softwaretechnik findet sich in [74]. Entsprechend der hohen Dynamik von Software-Systemen gestalten sich auch die in oben genannten Arbeiten diskutierten zeitlichen Logiken aufwändig und kompliziert, deren Anwendung zudem wegen der sehr strikten Definitionen nur bedingt mit der klassischen FTA vergleichbar ist.

Bereits früher übertrug Heidtmann in [11] und [34] die ursprünglich aus der theoretischen Philosophie stammende *modale Logik* [75] auf die Zuverlässigkeits-Modellierung. Seine temporale Logik beschreibt Reihenfolgen von Ereignissen nicht direkt, sondern stellt sogenannte *Irgendwann-* und *Immer-Beziehungen* zwischen den Ereignissen auf. Mit diesen lassen sich vielfältige zeitliche Abhängigkeiten und Zusammenhänge abbilden, u. a. auch Reihenfolgen. Heidtmann diskutiert sowohl die qualitative als auch die quantitative Anwendung seiner temporalen Logik und beschränkt diese nicht ausschließlich auf die Fehlerbaum-Methode. Allerdings erfordert diese Logik gerade wegen ihrer Mächtigkeit auch vergleichsweise komplexe Modelle und Berechnungen.

Ein der herkömmlichen FTA ähnliches, „anwendbares“ Vorgehen zu entwickeln, ist das erklärte Ziel des *Pandora*-Ansatzes in [76, 77]. Der Name „Pandora“ ist ein Wortspiel, einerseits ein Bezug auf die griechische Sagenfigur und andererseits zusammengesetzt aus „Priority AND“ und dem griechischen Wort ὥρα (*ora*) für Zeit [76]. Die Erstellung und Analyse von Pandora-Fehlerbäumen ähnelt der Vorgehensweise der herkömmlichen Booleschen FTA. Unter Verwendung zusätzlicher temporaler Gatter (genannt PAND, SAND und POR) ergibt sich für das TOP eine temporale Ausfallfunktion. Diese wird anhand von in [77] skizzierten temporalen Logik-Regeln zur qualitativen Vereinfachung in eine minimale Form überführt. Kern dieser temporalen Logik sind sogenannte *Doublets*. Ein Doublet beschreibt den zeitlichen Zusammenhang zwischen genau zwei Ereignissen und wird wie ein eigenes Basisereignis behandelt. Es werden ausschließlich relative Zeitangaben verwendet, d. h. die absoluten Eintretenszeitpunkte von Ereignissen werden nicht betrachtet. Diese Minimalform ist die Entsprechung der Minimalschnitte in der herkömmlichen FTA und erlaubt die qualitative Analyse des Ausfallverhaltens unter Berücksichtigung von Ereignissequenzen. Das Konzept der Doublets vereinfacht die Analyse erheblich, limitiert andererseits jedoch den Pandora-Ansatz hinsichtlich einer quantitativen Analyse, insbesondere wegen der nicht aufgelösten (zeitlichen) Abhängigkeiten zwischen den Doublets. Beispielsweise ergibt der Ausdruck „A tritt vor B und C ein“ nach Pandora [77] den Term (es wird die Notation aus Kapitel 4 verwendet, nicht die originale Pandora-Notation, um die Vergleichbarkeit der folgenden Ergebnisse zu vergrößern)

$$A \vec{\wedge} (B \wedge C) = \Big[(A \vec{\wedge} C) \wedge (B \vec{\wedge} C)\Big] \vee \Big[(A \vec{\wedge} B) \wedge (B \bar{\vec{\wedge}} C)\Big] \vee \Big[(A \vec{\wedge} B) \wedge (C \vec{\wedge} B)\Big] \; . \quad (2.1)$$

Die mit runden Klammern umfassten Ausdrücke der rechten Seite bezeichnen je ein Doublet.

Diese Doublets erlauben zwar die qualitative Analyse, lassen sich jedoch nicht einfach quantifizieren, wie die folgenden Überlegungen zeigen.

Ein Boolescher Konjunktions-Term – z. B. $(A \wedge C) \wedge (B \wedge C)$ – kann im Allgemeinen nicht direkt durch Multiplikation der Einzelwahrscheinlichkeiten quantifiziert werden, also

$$F_{(A \wedge C) \wedge (B \wedge C)} \neq (F_A \cdot F_C) \cdot (F_B \cdot F_C) \; , \quad (2.2)$$

wenn er nicht in minimaler Form vorliegt und die einzelnen Ereignisse voneinander unabhängig sind. Sind diese Bedingungen erfüllt, wie z. B. nach folgender Umformung

$$(A \wedge C) \wedge (B \wedge C) \;=\; A \wedge B \wedge C \;, \tag{2.3}$$

so ist eine direkte Quantifizierung möglich.

$$F_{(A \wedge C) \wedge (B \wedge C)} \;=\; F_{A \wedge B \wedge C} \;=\; F_A \cdot F_B \cdot F_C \;. \tag{2.4}$$

Analog dazu lassen sich auch Pandora-Ausdrücke, wie der oben gezeigte, nicht direkt quantifizieren. So gilt z. B. wegen des „gemeinsamen“ Ereignisses C in den beiden Doublets, d. h. einer nicht aufgelösten Abhängigkeit zwischen den Doublets,

$$F_{(A \,\vec{\wedge}\, C) \wedge (B \,\vec{\wedge}\, C)} \neq F_{(A \,\vec{\wedge}\, C)} \cdot F_{(B \,\vec{\wedge}\, C)} \;. \tag{2.5}$$

Der in dieser Arbeit vorgestellte TFTA-Ansatz übernimmt einige Aspekte des Pandora-Ansatzes. Die TFTA geht jedoch über Pandora hinaus, indem sie u. a.

- die in [77] lediglich skizzierten temporalen Logik-Regeln in ein geschlossenes und systematisches Regelwerk von allgemeiner Gültigkeit und Anwendbarkeit überführt und
- anders als der ausschließlich qualitative Pandora-Ansatz auch quantitative Modellierungen und Analysen ermöglicht und
- sich von dem für quantitative Analysen weniger geeigneten Konzept der Doublets löst
- und keinen POR Operator verwendet.

Die daraus resultierenden Unterschiede zeigen sich, wenn man den oben genannten Pandora-Ausdruck mit dem äquivalenten Logik-Ausdruck nach der TFTA vergleicht. Als Vorgriff auf die folgenden Kapitel ergibt sich

$$\begin{aligned} A \,\vec{\wedge}\, (B \wedge C) \;=\; & \Big[A \,\vec{\wedge}\, B \,\vec{\wedge}\, C\Big] \vee \Big[B \,\vec{\wedge}\, A \,\vec{\wedge}\, C\Big] \vee \Big[A \,\vec{\wedge}\, C \,\vec{\wedge}\, B\Big] \vee \Big[C \,\vec{\wedge}\, A \,\vec{\wedge}\, B\Big] \vee \\ & \vee \Big[(A \,\overline{\vec{\wedge}}\, B) \,\vec{\wedge}\, C\Big] \vee \Big[A \,\vec{\wedge}\, (B \,\overline{\vec{\wedge}}\, C)\Big] \vee \Big[(A \,\overline{\vec{\wedge}}\, C) \,\vec{\wedge}\, B\Big] \;. \end{aligned} \tag{2.6}$$

Wie in dieser Arbeit gezeigt wird, lassen sich diese Terme direkt quantifizieren – und auf Wunsch auch in kompakterer Form darstellen, um den Rechenaufwand zu reduzieren:

$$A \,\vec{\wedge}\, (B \wedge C) \;=\; \Big[(A \wedge B) \,\vec{\wedge}\, C\Big] \vee \Big[(A \wedge C) \,\vec{\wedge}\, B\Big] \vee \Big[A \,\vec{\wedge}\, (B \,\overline{\vec{\wedge}}\, C)\Big] \tag{2.7}$$

Da die Terme der rechten Seite sogar disjunkt sind, folgt

$$\begin{aligned} F_{A \,\vec{\wedge}\, (B \wedge C)}(t) \;&= F_{(A \wedge B) \,\vec{\wedge}\, C}(t) + F_{(A \wedge C) \,\vec{\wedge}\, B}(t) + F_{A \,\vec{\wedge}\, (B \,\overline{\vec{\wedge}}\, C)}(t) \;= \\ &= \int_0^t \Big(F_A(\tau) F_B(\tau) f_C(\tau) + F_A(\tau) F_C(\tau) f_B(\tau)\Big) \cdot \mathrm{d}\tau \;. \end{aligned} \tag{2.8}$$

2.4 Zusammenfassung

Die herkömmliche und Boolesche FTA ist Stand der Technik für eine systematische, deduktive, qualitative und quantitative Analyse des Ausfallverhaltens komplexer Systeme in vielen verschiedenen Industrie- und Anwendungsbereichen (Kapitel 2.1 und 2.2).

Die Forderung nach besserer Berücksichtigung zeitlicher Abhängigkeiten führte zur Entwicklung verschiedener Erweiterungen der Booleschen FTA um dynamische Effekte und dabei insbesondere um *sequence dependencies*, also Ereignissequenzen, vgl. Kapitel 2.3.1. Im Wesentlichen lassen sich dabei für die Abbildung von Reihenfolgen zwei Stoßrichtungen unterscheiden: Entweder erfolgt eine Transformation des Booleschen Fehlerbaum-Modells in eine zustandsbasierte Betrachtung, in der sich dynamische Effekte berechnen lassen (Kapitel 2.3.3). Oder es kommt anstelle der Booleschen (Ausfall-)Logik eine erweiterte, temporale Logik zum Einsatz (Kapitel 2.3.4).

In der Vergangenheit wurden Vorschläge für beide Ansätze vorgestellt. Auch werden einige der zustandsbasierten Erweiterungen bereits für die Lösung praxisrelevanter Aufgaben eingesetzt. Durch den Wechsel in den Zustandsraum brechen diese Ansätze jedoch mit einigen zentralen Vorteilen der herkömmlichen FTA, insbesondere hinsichtlich des Aufwandes, der Intuitivität in der praktischen Anwendung und der Möglichkeit aussagekräftiger qualitativer Analysen.

Auf dem Gebiet der Erweiterungen mit temporalen Logiken dominieren die sehr mächtigen aber dadurch auch komplexen Ansätze, die mehrheitlich der Erforschung der Anwendbarkeit von FTA in der Softwaretechnik entspringen. Forschungs- und Handlungsbedarf besteht hier vor allem hinsichtlich der Anwendbarkeit, um die „Benutzerfreundlichkeit“ der herkömmlichen Booleschen FTA auch auf dynamische FTA zu übertragen .

Abbildung 2.5 zeigt die Einordnung des hier vorgestellten TFTA Ansatzes in den Stand der Technik und grenzt die TFTA von anderen Ansätzen ab.

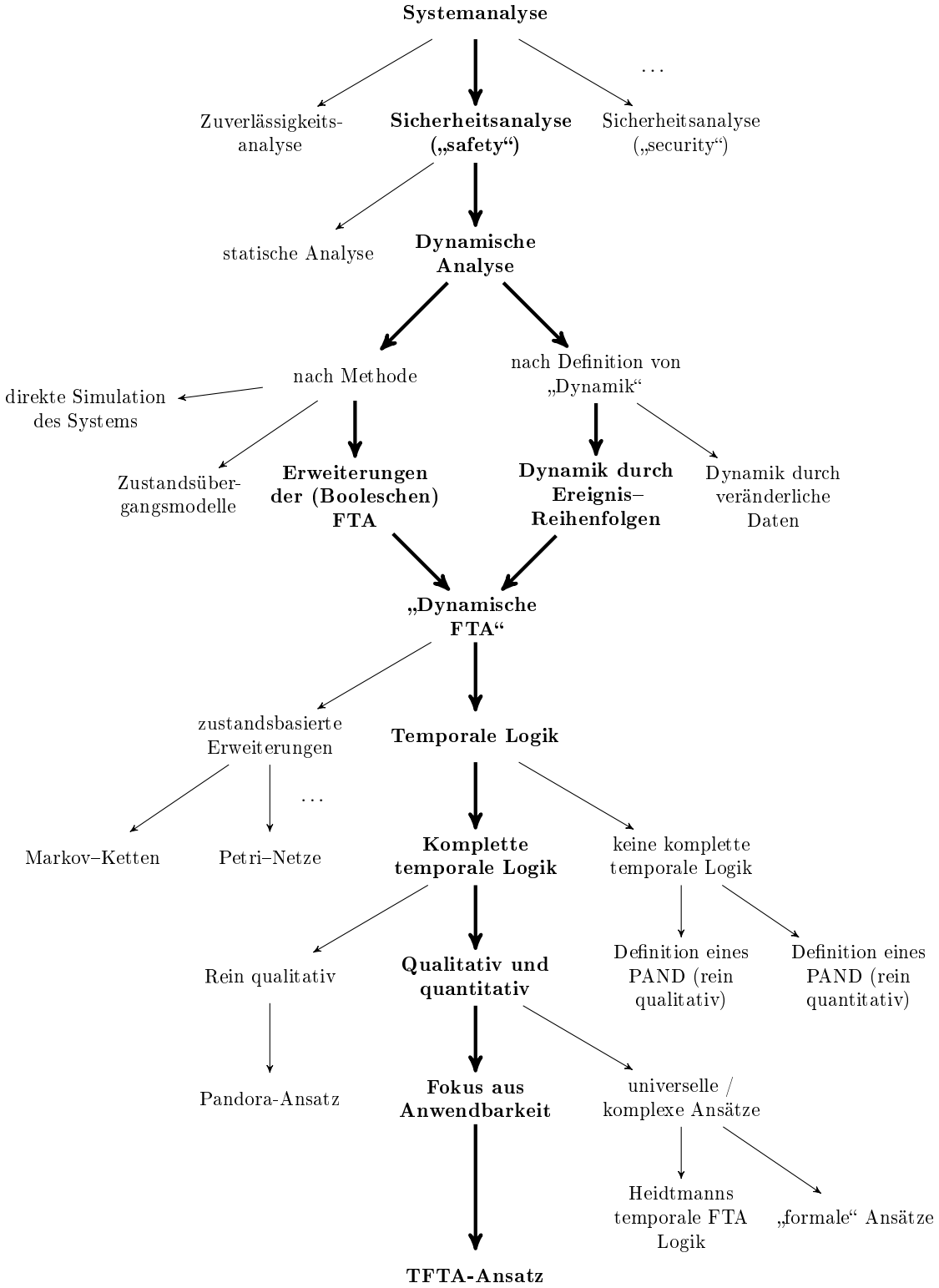


Abbildung 2.5: Einordnung des TFTA Ansatzes in den Stand der Technik und andere Methoden zur Berücksichtigung „dynamischer Effekte“ in ZSA.

3 Problemstellung: Ereignissequenzen in der FTA ohne Modularisierung

Simplicity is the final achievement.

(Frédéric Chopin)

3.1 Bedarf

3.1.1 Grundsätzlicher Bedarf an dynamischen FTA

Eines der wesentlichen Ziele der FTA ist der quantitative Nachweis, dass die Ausfallrate und Ausfallwahrscheinlichkeit eines Systems unterhalb eines Grenzwertes liegt. Die praktische Erfahrung zeigt, dass in vielen Fällen normative Grenzwerte, z.B. aus Normen wie IEC 61508 oder ISO 26262, nur knapp erreicht werden. Eine dynamische FTA liefert im Vergleich zur herkömmlichen FTA weniger konservative Ergebniswerte und erleichtert somit die Einhaltung der quantitativen Ziele. Die Verwendung einer solchen detaillierteren Modellierungsmethode ist dabei wesentlich glaubwürdiger als die – oftmals nur schwerlich begründbare – Reduzierung der verwendeten Eingangs-Ausfalldaten.

Für Systeme mit hohen Sicherheits-Anforderungen ist die klassische qualitative Einzelfehleranalyse mittels FMEA [9, 78] nicht mehr ausreichend. Hier dient die qualitative FTA in den zunehmend sehr komplexen Systemarchitekturen auch als Werkzeug für ein systematisches Verständnis des Zusammenspiels mehrerer Fehler. Sehr effizient lässt sich die Sicherheit gerade von programmierbaren Systemen erhöhen, indem Schaltbedingungen mit bestimmten Sequenzinformationen verknüpft werden. Fehl-Aktivierungen werden reduziert, wenn nur bestimmte Reihenfolgen von Trigger-Ereignissen relevant sind. Oftmals lassen sich solche Sequenzbedingungen ohne zusätzliche Kosten in hochintegrierten Schaltkreisen integrieren. Eine FTA mit qualitativer Berücksichtigung dieser Reihenfolgen liefert ein wesentlich aussagekräftigeres Bild des Systems als die klassische FTA.

An dieser Stelle sei auf Kapitel 6 verwiesen. Dort ist ein Beispielsystem gezeigt, dessen Boolesche Fehlerbaum-Modellierung nur unpräzise Ergebnisse liefert.

3.1.2 Bedarf an besseren dynamischen FTA

Die in Kapitel 2.3 genannten dynamischen Erweiterungen, insbesondere die zustandsbasierten Methoden wie die DFT, zielen primär auf die korrekte quantitative Berechnung von Fehlerbäumen. Kapitel 6.3 zeigt beispielhaft, dass die DFT dieses Ziel erreicht und insofern eine echte Verbesserung gegenüber der Booleschen FTA darstellt.

Die Kritik an den zustandsbasierten Erweiterungen umfasst insbesondere folgende Aspekte:

- Sie eignen sich nur eingeschränkt auch für qualitative Analysen der Reihenfolgen-Effekte. Ursache dafür ist der erzwungene Methodenwechsel zwischen Boolescher Fehlerbaum-Logik und zustandsbasiertem, dynamischen Modell.
- Sie stoßen an ihre Grenzen, wenn Vermaschungen zwischen dynamischen und nichtdynamischen Modulen notwendig sind.
- Ihre quantitative Berechnung ist vergleichsweise aufwändig und Näherungslösungen sind nicht einfach errechenbar.

Die Praxiserfahrung zeigt jedoch, dass eine gewisse Korrelation zwischen der Notwendigkeit einer quantitativen und qualitativen Berücksichtigung von dynamischen Effekten besteht. Aus Aufwandssicht ist es wünschenswert, beide Aspekte durch dieselbe Methode abzudecken. Gesucht sind daher Methoden, die dies – bei vertretbarem Aufwand – zulassen und idealerweise auch abgestufte Berechnungen zulassen, in denen zunächst Näherungen und dann nur für die „wirklich wichtigen“ Teile die exakten Werte berechnet werden.

3.1.3 Überlegungen zum praktischen Nutzen einer dynamischen FTA

Ganz allgemein gilt, dass bei allem verständlichen Bestreben, die (dynamische, vgl. Kapitel 2.1.2.1) Wirklichkeit möglichst exakt und detailliert im Modell zu berücksichtigen, der Aufwand immer im Verhältnis zum Nutzen zu betrachten ist. Obwohl heute eine Vielzahl an Ansätzen existiert, welche die Boolesche FTA um dynamische Effekte / Ereignissequenzen zu erweitern versucht, sind viele dieser Erweiterungen auf einfache und eher akademische Beispiele beschränkt. Dies betrifft insbesondere viele Ansätze mit einer temporalen Logik, da deren hohe Komplexität oftmals im Widerspruch zur praktischen Anwendbarkeit steht.

Praxistauglichkeit, (relative) Einfachheit und Skalierbarkeit sind drei wesentliche Erfolgsfaktoren der herkömmlichen FTA, die maßgeblich dazu beitgetragen haben, dass die FTA heute in vielen Bereichen die Modellierungsmethode der Wahl für ZSA ist.

Will man dieses Erfolgskonzept auf eine dynamische FTA übertragen, so muss diese mindestens den folgenden generischen Ansprüchen genügen:

- leichte Übertragbarkeit der realen Effekte in die Modell-Logik,
- geringer Modellierungsaufwand (Umsetzung im tatsächlichen Fehlerbaum),
- qualitative und quantitative Berechnung / Analyse ohne Methoden-Bruch,
- akzeptable Rechenzeiten,
- hohe Lesbar- und Verständlichkeit sowohl des Fehlerbaums als auch seiner Ergebnisse,
- Skalierbarkeit und Möglichkeit der Detaillierung und Erweiterung.

3.2 Konzept

3.2.1 Anforderungen an die TFTA

Vor dem Hintergrund dieser Gesichtspunkte zur praktischen Anwendbarkeit werden folgende Anforderungen an den TFTA-Ansatz gestellt:

1. Die temporale Logik der TFTA soll Sequenz-Abhängigkeiten zwischen Ereignissen abbilden können.

2. Die temporale Logik der TFTA soll eine Detaillierung der Booleschen Logik sein.

3. Die TFTA soll sich in Notation, Begrifflichkeiten, Arbeitsschritten und Arbeitsprodukten an denen der herkömmlichen FTA orientieren.

4. Für die qualitative Analyse soll die TFTA minimale Ereignissequenzen analog zu den Minimalschnitten der Booleschen Logik liefern. Eine *Minimalschnitt-Sequenz* soll aus „temporalen Konjunktionstermen“ bestehen, die sich von Booleschen AND verknüpften Basisereignissen insbesondere durch die enthaltenen Ereignissequenz-Informationen unterscheiden. Die Ausfallfunktion des Systems / TOP soll sich dann in einer „temporalen disjunktiven Normalform“ mittels dieser Minimalschnitt-Sequenzen darstellen lassen.

5. Für die quantitative Analyse sollen diese Minimalschnitt-Sequenzen disjunkt sein, um die anschließende Quantifizierung über Faltung der Ausfalldichten zu vereinfachen bzw. überhaupt zu ermöglichen.

6. Zur Aufwandsreduzierung sollen abgestufte Modellierungen möglich sein. Dabei kommen im ersten Ansatz Näherungslösungen zum Einsatz. Die exakte Berechnung erfolgt danach nur für die wichtigsten Beiträge. Die aufwändigere Berechnung exakter Lösungen soll weiterhin möglich sein.

Annahmen zur TFTA

Die Diskussionen zur TFTA erfolgen unter zwei Annahmen:

1. Monotonie oder Kohärenz des Fehlerbaums und

2. Nichtreparierbarkeit der modellierten Komponenten(-Ausfälle).

3.2.2 Schematischer Ablauf der TFTA

Abbildung 3.1 zeigt den Ablauf der TFTA mit der zweistufigen qualitativen Umformung des Logik-Terms in zunächst eine minimale und dann eine disjunkte Form und anschließender Quantifizierung. Dieser Ablauf ähnelt dem der herkömmlichen FTA, in der ebenfalls die Minimalschnitte nicht notwendigerweise immer auch disjunkt sind. Ursache der Zweiteilung bei der TFTA ist der Aufwand, der für die Überführung in eine disjunkte Form erforderlich ist.

An diesen Schritten orientiert sich auch der Aufbau des Kapitels 4 mit der temporalen Notation der TFTA in Kapitel 4.1, den temporalen Logikregeln in Kapitel 4.2 und der Umformung zu disjunkten Sequenzen in Kapitel 4.3. Die Quantifizierung temporaler Ausdrücke folgt in Kapitel 5.

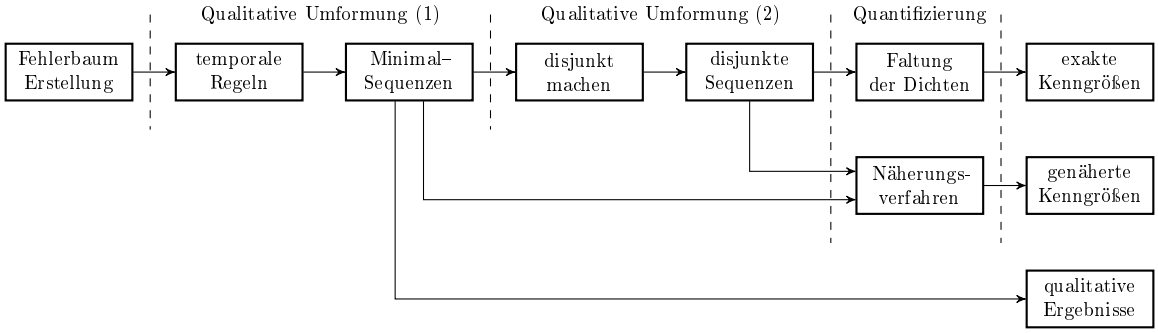


Abbildung 3.1: Schematischer Ablauf der TFTA mit zweistufiger Umformung des Logik-Terms in zunächst eine minimale und dann disjunkte Form und anschließende Quantifizierung. Genäherte Ergebnisse lassen sich entweder auf Basis der disjunkten Ereignissequenzen berechnen oder – mit etwas größerer Ungenauigkeit – auch direkt auf Basis der Minimal-Sequenzen.

4 Temporale Fehlerbaumanalyse (TFTA): Ein neuer Ansatz der dynamischen FTA

> Time is the worst place, so to speak, to get lost in.
>
> *(Douglas Adams)*

Dieses Kapitel beschreibt die *Temporale Fehlerbaumanalyse* (TFTA) als einen neuen Ansatz, die Boolesche FTA um die Abbildung von Ereignissequenzen zu erweitern.

- Kapitel 4.1 beschreibt die Notation der neuen temporalen Logik der TFTA. Diese Notation umfasst insbesondere zwei neue temporale Operatoren mit entsprechenden temporalen Gattern innerhalb der Fehlerbaum-Methode.
- Den Kern der temporalen Logik der TFTA bilden die Regeln für die Umformung temporaler Terme in Kapitel 4.2. Ziel dieser Umformungen ist die „temporale disjunktive Normalform".
- Kapitel 4.3 diskutiert die Minimalität und Disjunktheit temporaler Terme.
- Die in Kapitel 4.4 beschriebene „erweiterte Form" temporaler Terme reduziert den Aufwand zur Beschreibung komplexerer temporaler Ausfallfunktionen, insbesondere wenn diese nur wenige temporale Beziehungen enthalten.

4.1 Notation des TFTA-Ansatzes

Vorab einige Anmerkungen zu Begrifflichkeiten: In der Fehlerbaum-Methode repräsentieren die Basisereignisse atomare Ausfall-Ereignisse realer Einheiten (Systeme, Komponenten, Bauteile, Funktionen). Ebenso repräsentieren die Gatter eines Fehlerbaums nichtatomare, „übergeordnete" Ausfall-Ereignisse realer Einheiten. Begrifflich wird oftmals nicht unterschieden zwischen dem „Eintreten eines realen Ausfall-Ereignisses" und dem „Eintreten eines Fehlerbaum-Ereignisses", welches das reale Ausfall-Ereignis im Modell repräsentiert.

4.1.1 Boolesche Algebra und Ausfalllogik des Fehlerbaums

Im Kontext der FTA handelt es sich bei Ereignissen um Ausfallereignisse. Im Gegensatz zur zuverlässigkeitsorientierten Anwendung der Booleschen Algebra verwendet die FTA daher eine

Negativ-Logik [14, Kapitel 14.4.2]. Auf eine Negierung aller Ereignisse wird im Folgenden aus Gründen der Übersichtlichkeit verzichtet. Für alle Ausfallereignisse gilt

$$X_i = \begin{cases} \textit{True} \text{ oder } 1 & \text{Einheit } i \text{ ist ausgefallen} \\ \textit{False} \text{ oder } 0 & \text{Einheit } i \text{ ist funktionsfähig} \end{cases} . \tag{4.1}$$

Im TFTA-Ansatz bleibt die Boolesche Logik und ihre Anwendung auf den Fehlerbaum größtenteils unverändert:

Die *Konjunktion* mit dem *AND Operator* und

$$X_{\text{AND}} = A \wedge B \tag{4.2}$$

ist *True*, wenn beide Ereignisse A und B *True* sind. Im Fehlerbaum wird die Konjunktion durch das AND Gatter ausgedrückt.

Die *Disjunktion* mit dem *OR Operator* und

$$X_{\text{OR}} = A \vee B \tag{4.3}$$

ist *True*, wenn entweder Ereignis A oder Ereignis B *True* ist oder wenn beide Ereignisse *True* sind. Im Fehlerbaum wird die Disjunktion durch das OR Gatter ausgedrückt.

Die *Negation* mit dem *NOT Gatter* und

$$X_{\text{NOT}} = \neg A \tag{4.4}$$

ist *True*, wenn das Ereignis A *False* ist. Im Folgenden wird anstelle von $A \wedge \neg B$ auch das kürzere $A \neg B$ verwendet. Im Fehlerbaum wird die Negation durch das NOT Gatter ausgedrückt.

4.1.2 Operationen der temporalen Logik

Neben den Booleschen Operatoren bzw. Gattern beschreiben in der TFTA zwei temporale Operatoren bzw. Gatter die temporallogischen Ereignisbeziehungen, vgl. Abbildung 4.1.

PAND: Die Reihenfolge

Die *PAND Operation* (*Priority AND*) mit dem *PAND Operator* und

$$X_{\text{PAND}} = A \vec{\wedge} B \tag{4.5}$$

ist *True*, wenn

- beide Ereignisse A und B *True* sind und
- A zeitlich vor B eingetreten ist.

Sie beschreibt somit das zeitlich aufeinanderfolgende Eintreten von Ereignissen. Im Fehlerbaum wird die PAND Operation durch das PAND Gatter ausgedrückt.

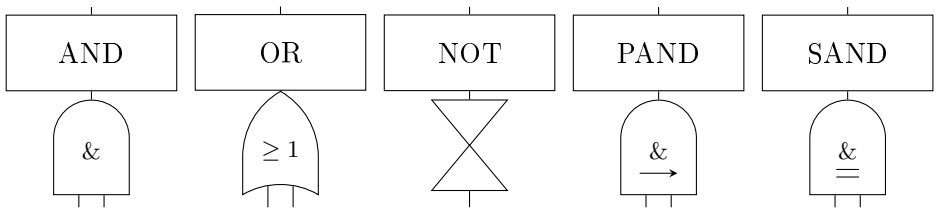


Abbildung 4.1: Die Gatter der TFTA: links die Booleschen und rechts die temporalen Gatter

SAND: Die Gleichzeitigkeit
Die *SAND Operation* (*Simultaneous AND*) mit dem *SAND Operator* und

$$X_{\text{SAND}} = A \barwedge B \tag{4.6}$$

ist *True*, wenn

- beide Ereignisse A und B *True* sind und
- A und B gleichzeitig eintreten.

Sie beschreibt somit das gleichzeitige Eintreten von Ereignissen. Im Fehlerbaum wird die SAND Operation durch das SAND Gatter ausgedrückt.

Anmerkung: Sowohl für PAND als auch für SAND sind Zeitangaben relativ zu verstehen, d. h. sie enthalten keine Aussagen zum absoluten Eintretens-Zeitpunkt eines Ereignisses.

4.1.3 Boolesche und temporale Operationen in Mengendarstellung

Die Mengendarstellung in Abbildung 4.2 verdeutlicht die Zusammenhänge zwischen Booleschen und temporalen Operationen. Sie zeigt (als Mengen) zwei Ereignisse A und B. Sind A und B die Operanden von AND und OR Operatoren bzw. im Fehlerbaum Eingänge zu den Booleschen AND und OR Gattern, so ergeben sich die zwei Ereignisse (Mengen) $A \wedge B = B \wedge A$ (Schnittmenge) und $A \vee B = B \vee A$ (Vereinigungsmenge). Sind A und B die Operanden von PAND und SAND Operatoren bzw. im Fehlerbaum Eingänge zu den PAND und SAND Gattern, so ergeben sich die drei Ereignisse (Mengen) $A \vec{\wedge} B$ und $B \vec{\wedge} A$ und $A \barwedge B = B \barwedge A$. Nicht abgebildet sind die negierten Ereignisse / Mengen.

Diese Darstellung in Abbildung 4.2 eignet sich für eine erste qualitative Aussage zur Bedeutung der temporalen Operatoren / Gatter.

Gemäß der Beschreibungen in (4.5) und (4.6) sind PAND und SAND Ereignisse echte Teilmengen der Konjunktion $A \wedge B = B \wedge A$ („. . . beide Ereignisse A und B *True* sind. . .“). Tatsächlich existieren genau drei Möglichkeiten, dass zwei Ereignisse A und B „zusammen“ eintreten. Entweder A ist vor B eingetreten oder B ist vor A eingetreten oder A und B sind gleichzeitig eingetreten, vgl. das *Vervollständigungsgesetz* in Kapitel 4.2.

In einer Mengendarstellung lässt sich daher schreiben, dass

$$A \vec{\wedge} B \subset A \wedge B\,, \qquad A \barwedge B \subset A \wedge B\,, \qquad B \vec{\wedge} A \subset A \wedge B\,, \tag{4.7}$$

$$A \wedge B \subset A\,, \qquad A \wedge B \subset B\,. \tag{4.8}$$

Die Ereignisse $A \vec{\wedge} B$, $B \vec{\wedge} A$ und $A \barwedge B$ sind paarweise disjunkt, besitzen also keine Schnittmengen, vgl. auch Kapitel 4.3:

$$A \vec{\wedge} B \perp A \barwedge B\,, \qquad A \vec{\wedge} B \perp B \vec{\wedge} A\,, \qquad A \barwedge B \perp B \vec{\wedge} A\,. \tag{4.9}$$

4.1.4 Temporale Operationen: zeitlicher Ablauf

Zeitliche Ablaufdiagramme verdeutlichen (zeitliche) Zusammenhänge zwischen dem Eintreten von Ereignissen. Abbildung 4.3 zeigt den Verlauf der logischen Pegel für die Booleschen und temporalen Operationen der TFTA. Grundsätzlich können Ereignisse nacheinander oder gleichzeitg eintreten, vgl. Teilabbildungen (a) und (c) bzw. (b) und (d).

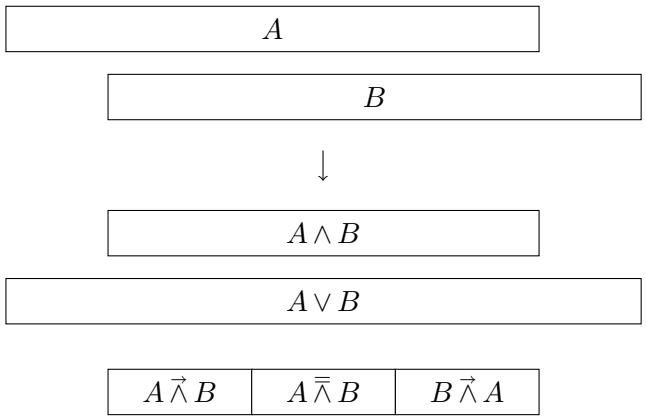


Abbildung 4.2: Temporale Operationen; von oben nach unten: die Ereignisse A und B; deren Schnitt- (AND) und Vereinigungsmengen (OR); die drei durch Unterscheidung der Ereignissequenz definierten Teilmengen der Schnittmenge (PAND und SAND).

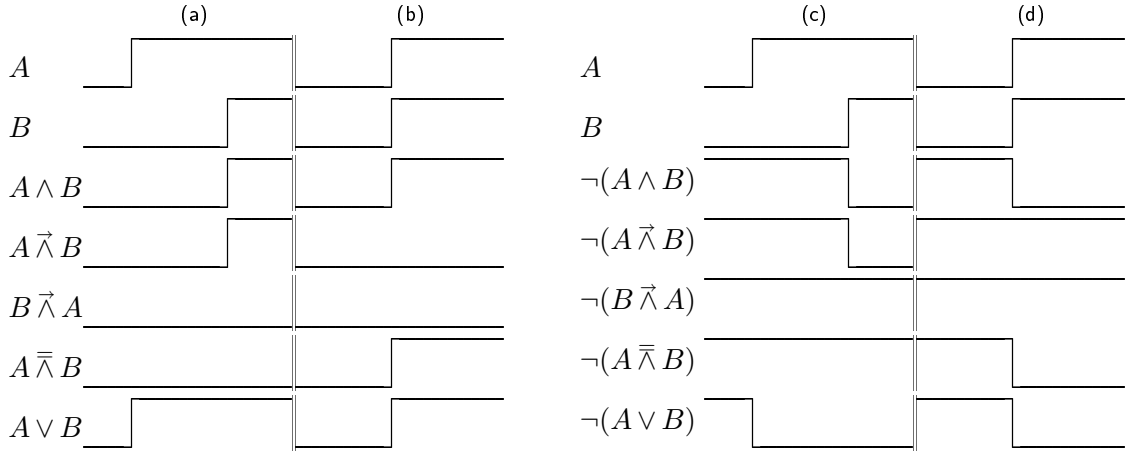


Abbildung 4.3: Zeitlicher Ablauf zweier Ereignisse: In (a) und (c) tritt A vor B ein (obere zwei Zeilen); die folgenden Zeilen zeigen an, welche aus A und B konstituierten Ereignisse wann *True* werden. In (b) und (d) treten A und B gleichzeitig ein.

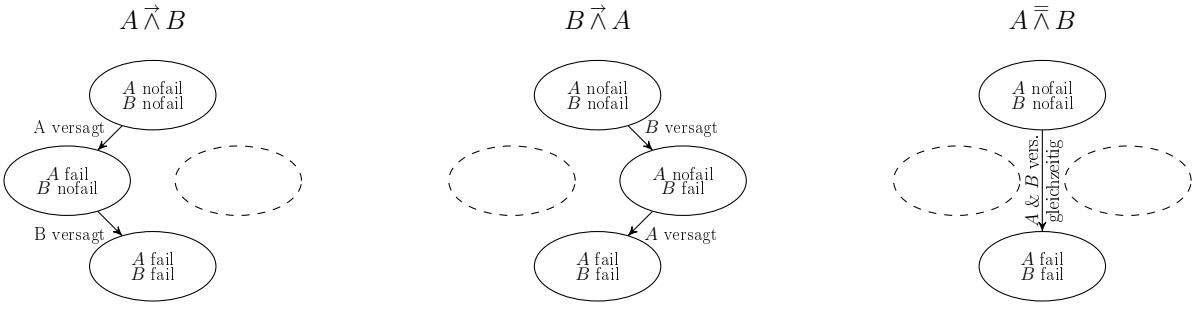


Abbildung 4.4: Separate Betrachtung der drei möglichen (und disjunkten) Zustandsübergänge, welche zum Ausfall beider Komponenten des Beispielsystems aus Abbildung 2.1 führen.

Die aus diesen zeitlichen Abläufen resultierenden Möglichkeiten für verschiedene Ausfall-Abläufe in einem System zeigen sich z. B. in einem Zustandsübergangsdiagramm. Die Möglichkeiten, dass Ausfall-Ereignisse nacheinander oder gleichzeitig eintreten, führen bei einem einfachen Beispielsystem aus zwei redundanten Komponenten (vgl. Zustandsübergangsdiagramm in Abbildung 2.1) zu den drei möglichen und in Abbildung 4.4 verdeutlichten Übergängen. Diese Übergänge entsprechen den beiden PAND Operationen $A \vec{\wedge} B$ und $B \vec{\wedge} A$ sowie der SAND Operation $A \overline{\vec{\wedge}} B$.

Anhand einiger Beispiele werden ab Seite 37 zeitliche Ablaufdiagramme mit weiteren Visualisierungsmethoden verglichen.

4.1.5 Syntax temporaler Terme

Ein logischer Ausdruck mit mindestens einem temporalen Operator heißt *temporallogischer Term* oder kurz *temporaler Term*.

In der herkömmlichen FTA heißt ein Boolescher Term, welcher durch das TOP Ereignis des Fehlerbaums repräsentiert wird, *Boolesche Ausfallfunktion* und wird mit φ symbolisiert. In der TFTA repräsentiert das TOP Ereignis einen temporalen Term, welcher als *temporale Ausfallfunktion* bezeichnet und zur besseren Unterscheidung mit ϖ symbolisiert wird.

Die folgenden Abschnitte erläutern die Elemente einer Grammatik der temporalen Logik der TFTA. Diese ist in Tab. 4.1 zusammengefasst. Dabei werden die Operatoren der temporalen Logik $\{\wedge, \vee, \vec{\wedge}, \overline{\vec{\wedge}}, \neg\}$ als Terminalsymbole verwendet.

Atomare Ereignisse / Basisereignisse

Atomare Ereignisse stellen die kleinste, nicht teilbare Einheit eines temporalen Terms dar. Im temporalen Fehlerbaum sind sie durch Basisereignisse repräsentiert. Diese unterscheiden sich nicht von den Basisereignissen der herkömmlichen FTA. Insbesondere können ihnen probabilistische Daten zugewiesen werden.

In der formalen Grammatik der temporalen Logik besitzen atomare Ereignisse das Token `ae`.

Negierte atomare Ereignisse mit Token `nae` sind die Negation atomarer Ereignisse:

$$\texttt{nae} \quad \rightarrow \quad \neg \ \texttt{ae} \qquad . \tag{4.10}$$

Negierte Ereignisse besitzen in der TFTA eine besondere Bedeutung, vgl. Kapitel 4.2.8.

Allgemeine temporale Terme

Allgemein besteht ein temporaler Term entweder aus einem Basisereignis oder aus zwei temporalen Termen, die mit einem der temporalen Operatoren verbunden sind oder mit einer Negation davon. Formal ist

$$\begin{aligned} \texttt{tt} \quad \rightarrow \quad & \texttt{ae} && \mid \\ & \texttt{tt} \ \wedge \ \texttt{tt} && \mid \\ & \texttt{tt} \ \vee \ \texttt{tt} && \mid \\ & \texttt{tt} \ \vec{\wedge} \ \texttt{tt} && \mid \\ & \texttt{tt} \ \overline{\vec{\wedge}} \ \texttt{tt} && \mid \\ & \neg \ \texttt{tt} && . \end{aligned} \tag{4.11}$$

Bis auf die zusätzlichen temporalen Operatoren entspricht dies der formalen Darstellung eines Booleschen Terms.

Token	Beschreibung	Format	Beispiele
ae	Atomares Ereignis (Basisereignis, Basic Event)	-	X Y Z
nae	Negiertes Atomares Ereignis	$\neg$ ae	$\neg X$
ce	Kernereignis (Core Event)	ae	s. o.
		ce $\overline{\barwedge}$ ae	$X \overline{\barwedge} Y$ $X \overline{\barwedge} Y \overline{\barwedge} Z$
nce	Negiertes Kernereignis	nae	s. o.
		nce $\wedge$ nae	$\neg X \wedge \neg Y = \neg X \neg Y$ $\neg X \wedge \neg Y \wedge \neg Z = \neg X \neg Y \neg Z$
es	Ereignissequenz	ce	s. o.
		es $\vec{\barwedge}$ ce	$X \vec{\barwedge} Y$ $(X \overline{\barwedge} Y) \vec{\barwedge} Z$
nes	Ereignissequenz mit negierten Ereignissen	nce $\wedge$ es	$\neg X \wedge Y$ $\neg X \wedge (Y \vec{\barwedge} Z)$ $(\neg X \neg Y) \wedge Z$ $(\neg X \neg Y) \wedge (A \vec{\barwedge} Z)$
tdnf	Temporaler Term in TDNF	es	s. o.
		nes	s. o.
		tdnf $\vee$ tdnf	$X \vee Y$ $\left[\neg X \wedge (Y \vec{\barwedge} Z)\right] \vee \left[(X \overline{\barwedge} Y) \vec{\barwedge} Z\right]$
ece	erweitertes Kernereignis	ae $\wedge$ ae	$X \wedge Y$
		ece $\wedge$ ae	$X \wedge Y \wedge Z$
ees	erweiterte Ereignissequenz	ece	s. o.
		ees $\vec{\barwedge}$ ece	$(X \wedge Y) \vec{\barwedge} (A \wedge Z)$
		ees $\vec{\barwedge}$ ce	$(X \wedge Y) \vec{\barwedge} (A \overline{\barwedge} Z)$
		es $\vec{\barwedge}$ ece	$X \vec{\barwedge} (Y \overline{\barwedge} Z) \vec{\barwedge} (A \wedge B)$
nees	erweiterte Ereignissequenz mit negierten Ereignissen	nce $\wedge$ ees	$\neg Z \wedge (X \wedge Y)$ $\neg Z \wedge \left[(X \wedge Y) \vec{\barwedge} (A \wedge B)\right]$ $\neg Z \wedge \left[(X \wedge Y) \vec{\barwedge} (A \overline{\barwedge} B)\right]$ $(\neg X \neg Y) \wedge \left[X \vec{\barwedge} Y \vec{\barwedge} (A \wedge B)\right]$
etdnf	Temporaler Term in erweiterter TDNF	ees	s. o.
		nees	s. o.
		etdnf $\vee$ tdnf	$(X \wedge Y) \vee Z$ $\left[\neg X \wedge (Y \wedge Z)\right] \vee \left[(X \overline{\barwedge} Y) \vec{\barwedge} Z\right]$
		etdnf $\vee$ etdnf	$(X \wedge Y) \vee (A \wedge B)$ $\left[\neg A \wedge (X \wedge Y)\right] \vee \left[Z \vec{\barwedge} (A \wedge B)\right]$
tt	Allgemeiner temporaler Term	ae	s. o.
		tt $\wedge$ tt	$(A \vee B) \wedge (C \vec{\barwedge} D)$
		tt $\vee$ tt	$A \vee \neg(C \vec{\barwedge} D)$
		tt $\vec{\barwedge}$ tt	$(A \vee B) \vec{\barwedge} (C \vee D)$
		tt $\overline{\barwedge}$ tt	$(A \vee B) \overline{\barwedge} (C \vee D)$
		$\neg$ tt	$\neg(C \vec{\barwedge} D)$

Tabelle 4.1: Syntax temporaler Terme: Ausgehend vom Token eines atomaren Ereignisses (Basisereignis) als nicht weiter unterteilbarer Einheit bauen sich die komplexeren Token wie Kernereignisse, Ereignissequenzen und temporale Terme in TDNF auf. Komplexe Token lassen sich auf verschiedene Weisen zusammensetzen. Die Beispiele umfassen nicht alle Kombinationsmöglichkeiten. Im unteren Teil: allgemeine Form temporaler Terme, die nicht direkt für weiterführende Analysen geeignet ist.

Diese allgemeine Form eignet sich jedoch weder für qualitative noch für quantitative Untersuchungen. Die ab Kapitel 4.2 erläuterten Regeln der temporalen Logik dienen dazu, beliebige temporale Terme in eine erweiterte TDNF zu überführen, die weitergehende Analysen erlaubt. Die folgenden Abschnitte erläutern den Aufbau dieser Form.

4.1.5.1 Temporale disjunktive Normalform

Kernereignisse

Kernereignisse (Core Events) der temporalen Logik stehen für das Eintreten eines Ereignisses oder mehrerer gleichzeitiger Ereignisse zu einem bestimmten Zeitpunkt. Negierte Kernereignisse zeigen an, dass zu einem bestimmten Zeitpunkt ein Ereignis oder mehrere Ereignisse noch nicht eingetreten sind. In vielen Gleichungen dieser Arbeit werden Kernereignisse mit K bezeichnet.

Ein Kernereignis hat das Token ce und besteht aus einem atomaren Ereignis oder aus einem (geklammerten) temporalen Term, der ausschließlich SAND verknüpfte atomare Ereignisse enthält.

Formal ist

$$\mathsf{ce} \rightarrow \begin{cases} \mathsf{ae} & | \\ \mathsf{ce} \ \overline{\overline{\wedge}} \ \mathsf{ae} & . \end{cases} \tag{4.12}$$

Ein *negiertes Kernereignis* (Token nce) besteht aus einem negierten atomaren Ereignis oder aus einem (geklammerten) temporalen Term, der ausschließlich AND verknüpfte negierte atomare Ereignisse enthält.

Formal ist

$$\mathsf{nce} \rightarrow \begin{cases} \mathsf{nae} & | \\ \mathsf{nce} \ \wedge \ \mathsf{nae} & . \end{cases} \tag{4.13}$$

Ereignissequenzen

Ereignissequenzen sind das temporallogische Äquivalent zu den Booleschen Schnitten. Sie beschreiben die zeitliche Abfolge eines oder mehrerer Kernereignisse. Analog zu den Booleschen Minimalschnitten besitzen auch in der temporalen Logik minimale Ereignissequenzen, die sog. MCSS vgl. Kap. 4.3.2, eine besondere Bedeutung. *Ereignissequenzen mit negierten Ereignissen* spielen insbesondere für die Bildung disjunkter Terme eine große Rolle (wiederum analog zum Booleschen Fall). In vielen Gleichungen dieser Arbeit werden Ereignissequenzen mit ES bezeichnet.

Ereignissequenzen haben das Token es und bestehen aus genau einem Kernereignis oder ausschließlich PAND verknüpften Kernereignissen.

Formal ist

$$\mathsf{es} \rightarrow \begin{cases} \mathsf{ce} & | \\ \mathsf{es} \ \vec{\wedge} \ \mathsf{ce} & . \end{cases} \tag{4.14}$$

Neben diesen existieren Ereignissequenzen mit negierten Ereignissen aus genau einem negierten Kernereignis, AND verknüpft mit genau einer Ereignissequenz. Sie erhalten das Token nes.

Formal ist

$$\mathsf{nes} \rightarrow \mathsf{nce} \ \wedge \ \mathsf{es} \quad . \tag{4.15}$$

Temporaler Term in TDNF
Disjunktiv verbundene Ereignissequenzen liefern die *Temporale Disjunktive Normalform* (TDNF) eines temporalen Terms:

$$\varpi = \bigvee_{j=1}^{\zeta} ES_j = ES_1 \vee ES_2 \vee \ldots \vee ES_\zeta \ . \tag{4.16}$$

Dabei steht ζ für die Anzahl der – nicht zwangsläufig schon minimalen – Ereignissequenzen ES von ϖ.

Formal ist

$$\begin{array}{lll} \mathsf{tdnf} & \rightarrow & \mathsf{es} \quad | \\ & & \mathsf{nes} \quad | \\ & & \mathsf{tdnf} \ \vee \ \mathsf{tdnf} \quad . \end{array} \tag{4.17}$$

4.1.5.2 Erweiterte temporale disjunktive Normalform

Temporaler Term in erweiterter TDNF
Die erweiterte TDNF einer temporalen Ausfallfunktion ϖ lässt sich darstellen als eine Anzahl ζ disjunktiv verbundener *erweiterter Ereignissequenzen* eES_j:

$$\varpi = \bigvee_{j=1}^{\zeta} eES_j = eES_1 \vee eES_2 \vee \ldots \vee eES_\zeta \ . \tag{4.18}$$

Diese erweiterte TDNF vereinfacht die qualitativen und quantitativen Umformungen und Berechnungen erheblich.

Formal ist

$$\begin{array}{lll} \mathsf{etdnf} & \rightarrow & \mathsf{ees} \quad | \\ & & \mathsf{nees} \quad | \\ & & \mathsf{etdnf} \ \vee \ \mathsf{tdnf} \quad | \\ & & \mathsf{etdnf} \ \vee \ \mathsf{etdnf} \quad . \end{array} \tag{4.19}$$

Elemente der erweiterten TDNF sind erweiterte Kernereignisse und erweiterte Ereignissequenzen mit und ohne negierten Ereignissen.

Erweiterte Kernereignisse
Ein *erweitertes Kernereignis* hat das Token ece und besteht aus zwei oder mehr AND verbundenen atomaren Ereignissen. Es ist damit identisch zum einfachen Konjunktionsterm der Booleschen Algebra aus atomaren Ereignissen. Formal ist

$$\begin{array}{lll} \mathsf{ece} & \rightarrow & \mathsf{ae} \ \wedge \ \mathsf{ae} \quad | \\ & & \mathsf{ece} \ \wedge \ \mathsf{ae} \quad . \end{array} \tag{4.20}$$

Erweiterte Ereignissequenzen

Erweiterte Ereignissequenzen mit Token ees bestehen aus genau einem erweiterten Kernereignis oder ausschließlich aus PAND verknüpften erweiterten Kernereignissen oder aus einer Mischung aus PAND verknüpften normalen und erweiterten Kernereignissen.

Formal ist

$$\begin{aligned} \texttt{ees} \quad &\rightarrow \quad \texttt{ece} && | \\ &\quad\ \ \texttt{ees} \ \vec{\wedge} \ \texttt{ece} && | \\ &\quad\ \ \texttt{ees} \ \vec{\wedge} \ \texttt{ce} && | \\ &\quad\ \ \texttt{es} \ \vec{\wedge} \ \texttt{ece} && . \end{aligned} \tag{4.21}$$

Erweiterte Ereignissequenzen mit negierten Ereignissen sind Ereignissequenzen aus genau einem negierten Kernereignis, AND verknüpft mit genau einer erweiterten Ereignissequenz und erhalten das Token nees. Formal ist

$$\texttt{nees} \quad \rightarrow \quad \texttt{nce} \ \wedge \ \texttt{ees} \qquad . \tag{4.22}$$

Die folgenden Kapitel beziehen sich zunächst noch nicht auf die erweiterte Form. Kapitel 4.4 erläutert, wie die qualitative Analyse durch die Verwendung erweiterter Ereignissequenzen vereinfacht wird. Kapitel 5.4.2 diskutiert die Quantifizierung erweiterter Ereignissequenzen.

4.1.6 Ereignisse als „Teil“ eines Terms

Mitunter ist es für die im Weiteren diskutierte temporale Logik notwendig zu wissen, ob ein Ereignis „Teil“ eines Terms ist bzw. ob ein Term ein bestimmtes Ereignis „enthält“. Von besonderem Interesse ist dabei die Frage, ob ein Ereignis X_i Teil eines (erweiterten) Kernereignisses bzw. Teil einer (erweiterten) Ereignissequenz ist.

Sei X_i ein Ereignis und ϖ ein Term mit

$$\varpi = \begin{cases} X_1 \wedge X_2 \wedge \ldots \wedge X_n & , \\ X_1 \,\vec{\wedge}\, X_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, X_n & , \\ X_1 \,\bar{\vec{\wedge}}\, X_2 \,\bar{\vec{\wedge}}\, \ldots \,\bar{\vec{\wedge}}\, X_n & \end{cases} \qquad \text{und} \qquad i \in \{1,2,\ldots,n\} \ , \tag{4.23}$$

dann ist X_i „Teil“ des Terms ϖ bzw. der Term ϖ „enthält“ X_i. Dafür wird ein neuer Operator vorgeschlagen:

$$X_i \Subset \varpi \ . \tag{4.24}$$

Beispielsweise gelten

$$A \Subset A \wedge B \ , \qquad A \Subset A \,\vec{\wedge}\, B \ , \qquad B \Subset A \,\vec{\wedge}\, B \ , \qquad B \Subset A \,\vec{\wedge}\, B \,\vec{\wedge}\, C \ .$$

4.1.7 Visualisierung mittels sequentieller Ausfallbäume

Sequentielle Ausfallbäume visualisieren die möglichen Ausfall-Sequenzen in einem (nicht reparierbaren) System. Sie erleichtern somit das Verständnis der exakten Bedeutung und Logik-Aussage temporaler Terme und dienen zugleich als Werkzeug zur Verifikation. Beispielsweise sind zwei unterschiedliche temporale Terme logisch identisch, wenn sie denselben sequentiellen Ausfallbaum besitzen.

Die folgenden Erläuterungen orientieren sich für „einfache“ sequentielle Ausfallbäume (ohne gleichzeitig eintretende Ereignisse, d. h. ohne SAND verknüpfte Ereignisse) im Wesentlichen an den Ausführungen in [79]. Kapitel 4.1.7.2 erweitert diese Überlegungen auf allgemeine temporale Terme der TFTA, die auch SAND Verknüpfungen enthalten können.

Vorab zwei Beispiele: Abbildung 4.5 zeigt die sequentiellen Ausfallbäume zu den temporalen Termen $A \vec{\wedge} B \vec{\wedge} C$ (links) und $A \vec{\wedge} C$ (rechts), jeweils für ein System mit drei Ausfallereignissen A, B, C.

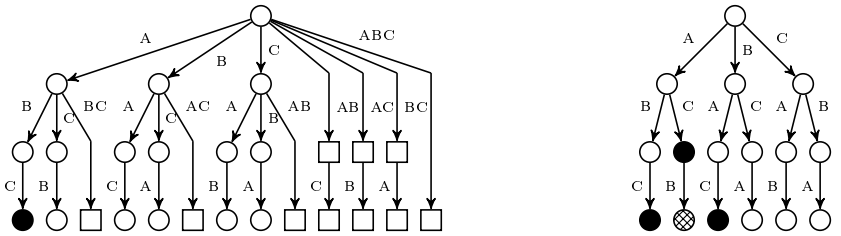


Abbildung 4.5: Sequentielle Ausfallbäume zu den Ausdrücken $A \vec{\wedge} B \vec{\wedge} C$ (links, mit SAND Verknüpfungen) und $A \vec{\wedge} C$ (rechts, ohne SAND Verknüpfungen im vereinfachten Baum). Rechteckige Knoten enthalten eine SAND Verknüpfung, runde Knoten enthalten keine SAND Verknüpfung. Knoten, die keinen Systemausfall repräsentieren, sind weiss ausgefüllt, minimale Ausfallknoten sind schwarz ausgefüllt und nichtminimale Ausfallknoten sind gemustert.

4.1.7.1 Einfache sequentielle Ausfallbäume (ohne SAND)

Für ein System aus n Einheiten besitzt der sequentielle Ausfallbaum $n+1$ Ebenen mit $\binom{n}{i} \cdot i!$ Knoten je Ebene $i \in \{0,1,\ldots,n\}$, vgl. Abbildung 4.5. Jeder Knoten steht für einen bestimmten System-Zustand r und lässt sich mit einem Vektor $\vec{K}_r = (X_1, X_2, \ldots, X_n)$ beschreiben, in dem alle in diesem Zustand nicht ausgefallenen Elemente mit 0 ($False$) und alle ausgefallenen Elemente mit $1, 2, \ldots, i$, entsprechend der zu diesem Zustand führenden Ausfall-Sequenz, bezeichnet sind. Beispielsweise entspricht die Sequenz $A \vec{\wedge} B \vec{\wedge} C$, also „$A$ vor B vor C“, dem Vektor $\vec{K} = (1,2,3)$. Der Knoten auf Ebene Null, der obersten Ebene, besitzt den Nullvektor $\vec{K} = (0,0,\ldots,0)$.

Die temporale Ausfallfunktion ϖ eines Systems lässt sich als Funktion der Vektoren $\vec{K}_r$ darstellen:

$$\varpi(\vec{K}_r) = \begin{cases} 1 & \text{, wenn System in Zustand } r \text{ ausgefallen.} \\ 0 & \text{, wenn System in Zustand } r \text{ nicht ausgefallen.} \end{cases} \tag{4.25}$$

Jeder Knoten $\vec{K}$, mit Ausnahme des einen Knotens auf Ebene Null, besitzt genau einen *Vorgängerknoten* $\vec{K}'$. Jeder Knoten $\vec{K}$, mit Ausnahme der Knoten der letzten Ebene n, besitzt mindestens einen *Nachfolgerknoten* $\vec{K}''$.

Aufgrund der eindeutigen Reihenfolge gilt dabei immer

$$\vec{K} > \vec{K}' \,, \tag{4.26}$$

wobei diese „Vektor-Ungleichung“ besagt, dass kein Element von $\vec{K}$ einen kleineren Wert haben darf als das entsprechende Element in $\vec{K}'$ und mindestens ein Element von $\vec{K}$ einen größeren Wert haben muss, als das entsprechende Element in $\vec{K}'$. Entsprechend gilt

$$\vec{K} < \vec{K}'' \,. \tag{4.27}$$

Unter Annahme der Monotonieeigenschaft bedeutet dies für die Ausfallfunktion, dass

$$\varpi(\vec{K}) \geq \varpi(\vec{K}') \ . \tag{4.28}$$

Aus der Monotonieeigenschaft folgt zweitens, dass für den Vorgängerknoten $\vec{K}'$ eines Knotens $\vec{K}$ die Systemfunktion $\varpi(\vec{K}') = 0$, wenn $\varpi(\vec{K}) = 0$.

Ein Knoten $\vec{K}$ heißt *minimaler Ausfallknoten*, wenn die durch ihn repräsentierte Ausfall-Sequenz zum *erstmaligen* Ausfall des Systems führt, wenn also

$$\varpi(\vec{K}) = 1 \qquad \text{und} \qquad \varpi(\vec{K}') = 0 \ . \tag{4.29}$$

Die Nachfolgerknoten eines minimalen Ausfallknotens heißen *nichtminimale Ausfallknoten*. Die Nachfolgerknoten eines nichtminimalen Ausfallknotens sind wiederum nichtminimale Ausfallknoten. Weiterhin folgt – ebenfalls aus der Monotonieeigenschaft –, dass auch für alle Nachfolgerknoten $\vec{K}''$ eines minimalen oder nichtminimalen Knotens $\vec{K}$ die Systemfunktion $\varpi(\vec{K}'') = 1$, da für diese immer $\varpi(\vec{K}) = 1$.

Die Parallele zur Notation der TFTA ergibt sich aus den folgenden Entsprechungen: Der *Knoten* im sequentiellen Ausfallbaum entspricht einer *Sequenz* in der TFTA; der *minimale Ausfallknoten* entspricht der *MCSS*; der *nichtminimale Ausfallknoten* entspricht der *nichtminimalen Ausfall-Sequenz*.

Für die eindeutige Beschreibung der Ausfallfunktion ϖ und damit auch des TOP des temporalen Fehlerbaums genügt die Angabe aller minimalen Ausfallknoten bzw. aller MCSS.

Abbildung 4.6 (links) zeigt den vereinfachten sequentiellen Ausfallbaum (ohne SANDs) für ein System aus $n = 3$ Einheiten A, B, C und der Ausfallfunktion $\varpi = (C \,\vec{\wedge}\, B \,\vec{\wedge}\, A) \vee (B \,\vec{\wedge}\, C)$. Der Baum besteht aus $n + 1 = 4$ Ebenen. Vier der $\sum_{i=0}^{i=n=3} \binom{n}{i} \cdot i! = 16$ möglichen Knoten (ohne SANDs) sind minimale Ausfallknoten entsprechend der vier MCSS $A \,\vec{\wedge}\, B \,\vec{\wedge}\, C$ und $\neg A \wedge (B \,\vec{\wedge}\, C)$ und $B \,\vec{\wedge}\, A \,\vec{\wedge}\, C$ und $C \,\vec{\wedge}\, B \,\vec{\wedge}\, A$. Hinzu kommt der nichtminimale Ausfallknoten entsprechend der Ausfallsequenz $B \,\vec{\wedge}\, C \,\vec{\wedge}\, A$.

Knoten, die keinen Systemausfall repräsentieren, werden als einfache Kreise dargestellt, minimale Ausfallknoten sind schwarz ausgefüllt und nichtminimale Ausfallknoten sind gemustert.

4.1.7.2 Erweiterung um gleichzeitig eintretende Ereignisse (SAND)

Abbildung 4.6 (rechts) zeigt den sequentiellen Ausfallbaum zu einem System mit Ausfallfunktion $\varpi = (C \,\vec{\wedge}\, B \,\vec{\wedge}\, A) \vee (B \,\vec{\wedge}\, C)$, in dem auch SAND Verknüpfungen berücksichtigt sind.

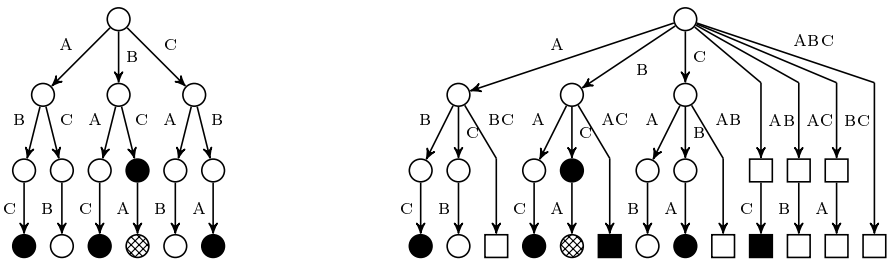


Abbildung 4.6: Sequentieller Ausfallbaum ohne SANDs (links) und mit SANDs (rechts) zu einem System mit Ausfallfunktion $\varpi = (C \,\vec{\wedge}\, B \,\vec{\wedge}\, A) \vee (B \,\vec{\wedge}\, C)$.

Zur besseren Unterscheidung sind Ausfallknoten (Systemzustände) ohne SAND Verknüpfungen als Kreise und Ausfallknoten mit mindestens einer SAND Verknüpfung als Quadrate stilisiert.

Die in Kapitel 4.1.7.1 eingeführte Notation bleibt ansonsten erhalten. Beispielsweise entspricht die Sequenz $(A \,\vec{\overline{\wedge}}\, B) \,\vec{\wedge}\, C$ dem Vektor $\vec{K} = (1,1,2)$ und die Sequenz $A \,\vec{\wedge}\, (B \,\vec{\overline{\wedge}}\, C)$ dem Vektor $\vec{K} = (1,2,2)$. Somit gelten auch (4.25) bis (4.29) für sequentielle Ausfallbäume mit SAND Verknüpfungen.

4.1.7.3 Nutzung sequentieller Ausfallbäume

Sequentielle Ausfallbäume ermöglichen eine intuitive Visualisierung temporaler Terme und erleichtern damit die Analyse temporaler Terme:

- Sie dienen der direkten Darstellbarkeit von temporalen Termen, wie sie analog für Boolesche Terme durch Logik-Tabellen gegeben ist. Insbesondere sind mehrere temporale Terme genau dann logisch äquivalent, wenn sie denselben sequentiellen Ausfallbaum besitzen.

- Sie zeigen direkt an, ob temporale Terme minimal sind oder sich gegenseitig enthalten, vgl. Kapitel 4.3.2. Mehrere temporale Terme sind genau dann minimal, wenn jeder der sequentiellen Ausfallbäume mindestens einen minimalen Ausfallknoten aufweist, der in keinem der anderen sequentiellen Ausfallbäume auch ein Ausfallknoten ist.

- Sie zeigen direkt an, ob temporale Terme disjunkt sind oder Schnittmengen existieren, vgl. Kapitel 4.3.3. Mehrere temporale Terme sind genau dann disjunkt, wenn die sequentiellen Ausfallbäume der Terme keine gemeinsamen Ausfallknoten aufweisen.

Im Folgenden werden sowohl die in Abbildung 4.7 links gezeigte „ausführliche Form“ sequentieller Ausfallbäume verwendet als auch eine „kompakte Form“, vgl. Abbildung 4.7 rechts.

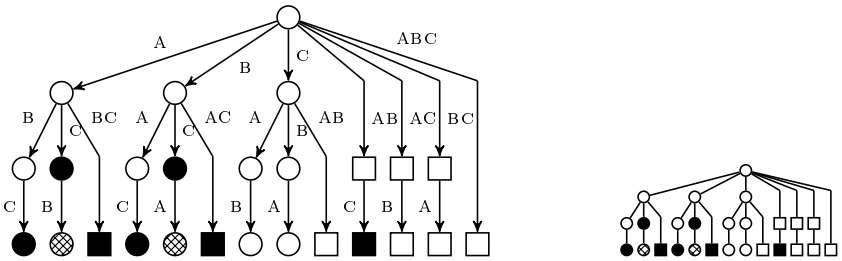


Abbildung 4.7: Ausführliche und kompakte Form eines sequentiellen Ausfallbaums zu einem System mit Ausfallfunktion $\varpi = (A \,\vec{\wedge}\, C) \vee (B \,\vec{\wedge}\, C)$. Beide Formen werden in dieser Arbeit verwendet.

Anhand einiger Beispiele werden ab Seite 37 Aufstellung und Anwendung sequentieller Ausfallbäume demonstriert und sequentielle Ausfallbäume mit weiteren Visualisierungsmethoden verglichen. Der Anhang enthält ab Seite 126 eine weitere Erläuterung des Umgangs mit sequentiellen Ausfallbäumen.

Zusammenfassung Kapitel 4.1:
Die TFTA Notation beruht auf den drei Booleschen Operatoren AND, OR, NOT, sowie zwei neuen temporalen Operatoren PAND, SAND. Temporale Terme lassen sich analog zur Booleschen

disjunktiven Normalform auf eine TDNF aus OR verknüpften Ereignissequenzen reduzieren, welche ihrerseits aus PAND verknüpften Kernereignissen bestehen. Die erweiterte TDNF erlaubt darüber hinaus auch AND verknüpfte Kernereignisse, wodurch der Berechnungsaufwand sinkt. Sequentielle Ausfallbäume ermöglichen eine Visualisierung temporaler Terme sowie Aussagen über Minimalität und Disjunktheit temporaler Terme.

4.2 Temporale Logik-Regeln

Die temporalen Logik-Regeln des TFTA Ansatzes sind eine Erweiterung der herkömmlichen Booleschen Logik und Algebra. Sie beschreiben *temporal-logische Ereignis Beziehungen*, d. h. den kombinatorischen Zusammenhang zwischen dem Eintreten mehrerer Ereignisse unter Berücksichtigung der Reihenfolgen der einzelnen Eintretens-Zeitpunkte dieser Ereignisse. Das enthaltene Zeitkonzept macht dieses Regelwerk im Vergleich zur Booleschen Algebra umfangreicher und komplexer.

Bei der Anwendung der temporalen Logik sind zwei wesentliche Unterschiede zur Booleschen Logik zu beachten:

1. Ereignis-Abfolgen werden durch die Reihenfolge und Anordnung der Operatoren und Ereignisse ausgedrückt, weswegen Kommutativ-, Assoziativ- und Distributivgesetze für temporale Gatter nicht bzw. eingeschränkt gelten.

2. Die temporal-logische Notation kennt *Widersprüche* durch „unmögliche“ temporal-logische Ereignis-Beziehungen. Widersprüche ergeben immer *False*. Beispielsweise kann ein Ereignis nicht nach sich selbst eintreten, sodass $X \vec{\wedge} X = \mathit{False}$.

4.2.1 Boolesche Algebra

Die herkömmliche Boolesche Algebra beschreibt *Boolesche Ereignis-Beziehungen*, d. h. kombinatorische Zusammenhänge zwischen dem Eintreten mehrerer Ereignisse ohne Berücksichtigung der Reihenfolgen der einzelnen Eintretens-Zeitpunkte dieser Ereignisse. Sie besteht im Wesentlichen aus den folgenden Regeln [8, 14], die hier der Vollständigkeit halber nochmals aufgeführt sind:

Kommutativgesetze

$$A \wedge B = B \wedge A \qquad \text{und} \qquad A \vee B = B \vee A \,, \tag{4.30}$$

Assoziativgesetze

$$\begin{aligned} A \wedge (B \wedge C) &= (A \wedge B) \wedge C = A \wedge B \wedge C \qquad \text{und} \\ A \vee (B \vee C) &= (A \vee B) \vee C = A \vee B \vee C \,, \end{aligned} \tag{4.31}$$

Distributivgesetze

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C) \qquad \text{und} \qquad A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C) \,, \tag{4.32}$$

Idempotenzgesetze

$$A \wedge A = A \qquad \text{und} \qquad A \vee A = A \,, \tag{4.33}$$

Absorptionsgesetze

$$A \wedge (A \vee B) = A \qquad \text{und} \qquad A \vee (A \wedge B) = A \,, \tag{4.34}$$

De Morgansche Theoreme

$$\neg(A \wedge B) = \neg A \vee \neg B \qquad \text{und} \qquad \neg(A \vee B) = \neg A \wedge \neg B \;, \tag{4.35}$$

Operationen mit *False* und *True*

$$\begin{aligned} &\neg \mathit{False} = \mathit{True} \;, \\ &A \wedge \mathit{False} = \mathit{False} \qquad \text{und} \qquad A \wedge \mathit{True} = A \;, \\ &A \vee \mathit{False} = A \qquad \text{und} \qquad A \vee \mathit{True} = \mathit{True} \;. \end{aligned} \tag{4.36}$$

4.2.2 Vervollständigungsgesetz

Das *Vervollständigungsgesetz der Konjunktion* in (4.37) beschreibt den Zusammenhang zwischen Booleschen und temporalen Operatoren / Gattern, vgl. Abbildung 4.2. Es gilt

$$A \wedge B = (A \,\vec{\wedge}\, B) \vee (A \,\overline{\vec{\wedge}}\, B) \vee (B \,\vec{\wedge}\, A) \;. \tag{4.37}$$

Die Terme der rechten Seite sind disjunkt.

Die SAND Verbindung zwischen *unterschiedlichen* Ereignissen steht für (strukturell) abhängige Ausfälle, welche sich als Common Cause Failure (CCF) interpretieren lassen. Es lässt sich zeigen, dass unter der Annahme *unabhängiger* Ausfälle der Erwartungswert für Basisereignisse mit SAND Operator immer Null beträgt, also z. B. $\mathrm{E}[A \,\overline{\vec{\wedge}}\, B] = 0$, vgl. Kapitel 5.3.1. Über die Abbildung von CCF hinaus spielt der SAND Operator bei der qualitativen Vereinfachung von temporalen Termen wie auch für qualitative Analysen eine wesentliche Rolle.

4.2.3 Widerspruchsgesetze

Grundsätzlich entsteht ein logischer Widerspruch, falls dasselbe Ereignis zeitlich nach sich selbst eintreten soll. Dies ergibt sich unmittelbar aus der Monotonieannahme in Kombination mit nicht reparierbaren Komponenten, vgl. Annahmen zur TFTA in Kapitel 3.2.1.

Im einfachsten Fall ist

$$A \,\vec{\wedge}\, A = \mathit{False} \;. \tag{4.38}$$

Allgemein ergibt eine Ereignissequenz *False*, wenn mindestens ein Ereignis mehrfach in ihr vorkommt, also

$$X_1 \,\vec{\wedge}\, X_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, X_n = \mathit{False} \;, \tag{4.39}$$

wenn $\exists\; X_i = X_j$ für $i, j \in \{1, 2, \ldots, n\}$ und $i \neq j$. Für den Fehlerbaum bedeutet dies, dass ein PAND Gatter *False* wird, falls dasselbe Ereignis mehrfach als Eingang dient.

Das Widerspruchsgesetz gilt auch für nichtatomare Kernereignisse:

$$(A \,\overline{\vec{\wedge}}\, B) \,\vec{\wedge}\, A = (B \,\overline{\vec{\wedge}}\, A) \,\vec{\wedge}\, A = \mathit{False} \;, \tag{4.40}$$

$$A \,\vec{\wedge}\, (A \,\overline{\vec{\wedge}}\, B) = A \,\vec{\wedge}\, (B \,\overline{\vec{\wedge}}\, A) = \mathit{False} \;, \tag{4.41}$$

bzw. im allgemeinen

$$K_1 \,\vec{\wedge}\, K_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, K_n = \mathit{False} \;, \tag{4.42}$$

wenn mindestens ein Basisereignis X in zwei oder mehr der Kernereignisse K enthalten ist, d. h. wenn $\exists\; (X \in K_i) \wedge (X \notin K_j)$ für $i, j \in \{1, 2, \ldots, n\}$ und $i \neq j$.

Bespielsweise gilt: $(A \,\overline{\vec{\wedge}}\, B) \,\vec{\wedge}\, C \,\vec{\wedge}\, (A \,\overline{\vec{\wedge}}\, D \,\overline{\vec{\wedge}}\, E) = \mathit{False}$, da $(A \,\overline{\vec{\wedge}}\, B)$ und $(A \,\overline{\vec{\wedge}}\, D \,\overline{\vec{\wedge}}\, E)$ beide dasselbe Basisereignis A enthalten.

4.2.4 Temporales Idempotenzgesetz

Aus den bereits bekannten Vervollständigungs- und Widerspruchsgesetzen lässt sich ein *temporales Idempotenzgesetz* ableiten, welches ausschließlich für den SAND Operator gilt. Aus (4.37) und (4.38) sowie dem Booleschen Idempotenzgesetz aus (4.33) folgt dann

$$\begin{aligned} A \wedge A &= (A \,\vec{\barwedge}\, A) \vee (A \,\overline{\barwedge}\, A) \vee (A \,\vec{\barwedge}\, A) = \mathit{False} \vee (A \,\overline{\barwedge}\, A) \vee \mathit{False} \qquad \text{und} \\ A \wedge A &= A \qquad \text{, sodass} \\ A \,\overline{\barwedge}\, A &= A \end{aligned} \tag{4.43}$$

gilt.

4.2.5 Temporales Kommutativgesetz

Ein Kommutativgesetz exsitiert ausschließlich für den SAND Operator

$$A \,\overline{\barwedge}\, B = B \,\overline{\barwedge}\, A \,, \tag{4.44}$$

nicht jedoch für den PAND Operator

$$A \,\vec{\barwedge}\, B \neq B \,\vec{\barwedge}\, A \,. \tag{4.45}$$

4.2.6 Temporale Assoziativgesetze

Der SAND Operator ist als einziger temporaler Operator assoziativ, sodass

$$A \,\overline{\barwedge}\, (B \,\overline{\barwedge}\, C) = A \,\overline{\barwedge}\, B \,\overline{\barwedge}\, C = (A \,\overline{\barwedge}\, B) \,\overline{\barwedge}\, C \,. \tag{4.46}$$

Der PAND Operator ist lediglich links-assoziativ, weswegen

$$(A \,\vec{\barwedge}\, B) \,\vec{\barwedge}\, C = A \,\vec{\barwedge}\, B \,\vec{\barwedge}\, C \neq A \,\vec{\barwedge}\, (B \,\vec{\barwedge}\, C) \,. \tag{4.47}$$

4.2.7 Weitere grundlegende Logik-Regeln

Von besonderer Bedeutung sind auch die beiden folgenden temporalen Logik-Regeln:

$$A \,\vec{\barwedge}\, (B \,\vec{\barwedge}\, C) = (A \wedge B) \,\vec{\barwedge}\, C \qquad \text{und} \tag{4.48}$$

$$A \,\overline{\barwedge}\, (B \,\vec{\barwedge}\, C) = B \,\vec{\barwedge}\, (A \,\overline{\barwedge}\, C) \,. \tag{4.49}$$

Beispiele der Visualisierung temporaler Logik-Regeln

Die Korrektheit dieser beiden Logik-Regeln wird im Folgenden mittels drei verschiedener Methoden gezeigt. Diese sind:

- Tabelle 4.2 zeigt auf Seite 38 die Korrektheit von (4.48) und (4.49) mit Wahrheitstabellen ähnlich den aus der Booleschen Logik bekannten. Es sind jedoch bei Konjunktionstermen in der temporalen Logik alle möglichen Ereignissequenzen zu beachten.
- Abbildung 4.8 zeigt auf Seite 39 die sequentiellen Ausfallbäume zu (4.48) und (4.49), die sich besonders für die manuelle Prüfung und Darstellung temporaler Terme eignen.

- Abbildung 4.9 zeigt auf Seite 40 die Korrektheit von (4.48) und (4.49) anhand von zeitlichen Ablaufdiagrammen.

Die Anzahl der Einträge (Zeilen) in der Wahrheitstabelle gleicht der Anzahl der Knoten im sequentiellen Ausfallbaum. Tatsächlich bietet es sich oftmals an, sequentielle Ausfallbäume zu verwenden, um die Wahrheitstabelle zu befüllen. Zeitliche Ablaufdiagramme eignen sich insbesondere für die (punktuelle) Überprüfung besonders komplexer Terme.

	$A \vec{\wedge} (B \vec{\wedge} C)$	$(A \wedge B) \vec{\wedge} C$		$A \bar{\vec{\wedge}} (B \vec{\wedge} C)$	$B \vec{\wedge} (A \bar{\vec{\wedge}} C)$
$\neg A \neg B \neg C$	*False*	*False*	$\neg A \neg B \neg C$	*False*	*False*
$\neg B \neg C \wedge A$	*False*	*False*	$\neg B \neg C \wedge A$	*False*	*False*
$\neg A \neg C \wedge B$	*False*	*False*	$\neg A \neg C \wedge B$	*False*	*False*
$\neg A \neg B \wedge C$	*False*	*False*	$\neg A \neg B \wedge C$	*False*	*False*
$\neg C \wedge (A \vec{\wedge} B)$	*False*	*False*	$\neg C \wedge (A \vec{\wedge} B)$	*False*	*False*
$\neg C \wedge (B \vec{\wedge} A)$	*False*	*False*	$\neg C \wedge (B \vec{\wedge} A)$	*False*	*False*
$\neg C \wedge (A \bar{\vec{\wedge}} B)$	*False*	*False*	$\neg C \wedge (A \bar{\vec{\wedge}} B)$	*False*	*False*
$\neg B \wedge (A \vec{\wedge} C)$	*False*	*False*	$\neg B \wedge (A \vec{\wedge} C)$	*False*	*False*
$\neg B \wedge (C \vec{\wedge} A)$	*False*	*False*	$\neg B \wedge (C \vec{\wedge} A)$	*False*	*False*
$\neg B \wedge (A \bar{\vec{\wedge}} C)$	*False*	*False*	$\neg B \wedge (A \bar{\vec{\wedge}} C)$	*False*	*False*
$\neg A \wedge (B \vec{\wedge} C)$	*False*	*False*	$\neg A \wedge (B \vec{\wedge} C)$	*False*	*False*
$\neg A \wedge (C \vec{\wedge} B)$	*False*	*False*	$\neg A \wedge (C \vec{\wedge} B)$	*False*	*False*
$\neg A \wedge (B \bar{\vec{\wedge}} C)$	*False*	*False*	$\neg A \wedge (B \bar{\vec{\wedge}} C)$	*False*	*False*
$A \vec{\wedge} B \vec{\wedge} C$	*True*	*True*	$A \vec{\wedge} B \vec{\wedge} C$	*False*	*False*
$B \vec{\wedge} A \vec{\wedge} C$	*True*	*True*	$B \vec{\wedge} A \vec{\wedge} C$	*False*	*False*
$A \vec{\wedge} C \vec{\wedge} B$	*False*	*False*	$A \vec{\wedge} C \vec{\wedge} B$	*False*	*False*
$C \vec{\wedge} A \vec{\wedge} B$	*False*	*False*	$C \vec{\wedge} A \vec{\wedge} B$	*False*	*False*
$B \vec{\wedge} C \vec{\wedge} A$	*False*	*False*	$B \vec{\wedge} C \vec{\wedge} A$	*False*	*False*
$C \vec{\wedge} B \vec{\wedge} A$	*False*	*False*	$C \vec{\wedge} B \vec{\wedge} A$	*False*	*False*
$A \vec{\wedge} (B \bar{\vec{\wedge}} C)$	*False*	*False*	$A \vec{\wedge} (B \bar{\vec{\wedge}} C)$	*False*	*False*
$B \vec{\wedge} (A \bar{\vec{\wedge}} C)$	*False*	*False*	$B \vec{\wedge} (A \bar{\vec{\wedge}} C)$	*True*	*True*
$C \vec{\wedge} (A \bar{\vec{\wedge}} B)$	*False*	*False*	$C \vec{\wedge} (A \bar{\vec{\wedge}} B)$	*False*	*False*
$(A \bar{\vec{\wedge}} B) \vec{\wedge} C$	*True*	*True*	$(A \bar{\vec{\wedge}} B) \vec{\wedge} C$	*False*	*False*
$(A \bar{\vec{\wedge}} C) \vec{\wedge} B$	*False*	*False*	$(A \bar{\vec{\wedge}} C) \vec{\wedge} B$	*False*	*False*
$(B \bar{\vec{\wedge}} C) \vec{\wedge} A$	*False*	*False*	$(B \bar{\vec{\wedge}} C) \vec{\wedge} A$	*False*	*False*
$A \bar{\vec{\wedge}} B \bar{\vec{\wedge}} C$	*False*	*False*	$A \bar{\vec{\wedge}} B \bar{\vec{\wedge}} C$	*False*	*False*

Tabelle 4.2: Wahrheitstabelle, welche die Gültigkeit der Zusammenhänge aus (4.48) (links) und (4.49) (rechts) demonstriert. Inklusive der SAND Verknüpfungen existieren je 26 mögliche Sequenzen. Die (temporal)logische Äquivalenz der beiden Terme zeigt sich in beiden Fällen in der Übereinstimmung der Ergebnisse aller möglichen Sequenzen.

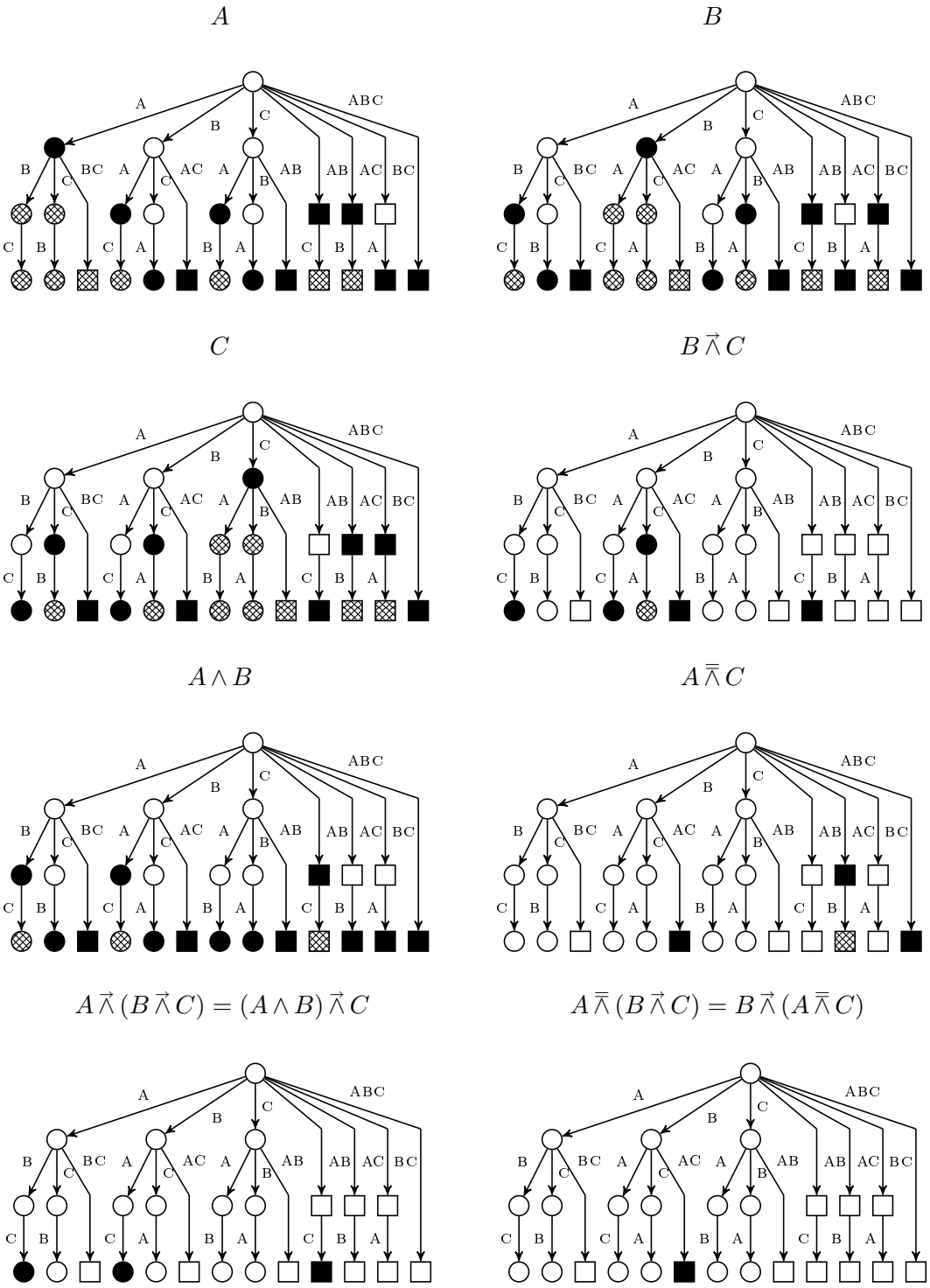


Abbildung 4.8: Sequentielle Ausfallbäume, welche die Gültigkeit der Zusammenhänge aus (4.48) und (4.49) demonstrieren. Von links nach rechts und oben nach unten: A, B, C, $B \vec{\wedge} C$, $A \wedge B$, $A \bar{\vec{\wedge}} C$, $A \vec{\wedge} (B \vec{\wedge} C) = (A \wedge B) \vec{\wedge} C$, $A \bar{\vec{\wedge}} (B \vec{\wedge} C) = B \vec{\wedge} (A \bar{\vec{\wedge}} C)$.

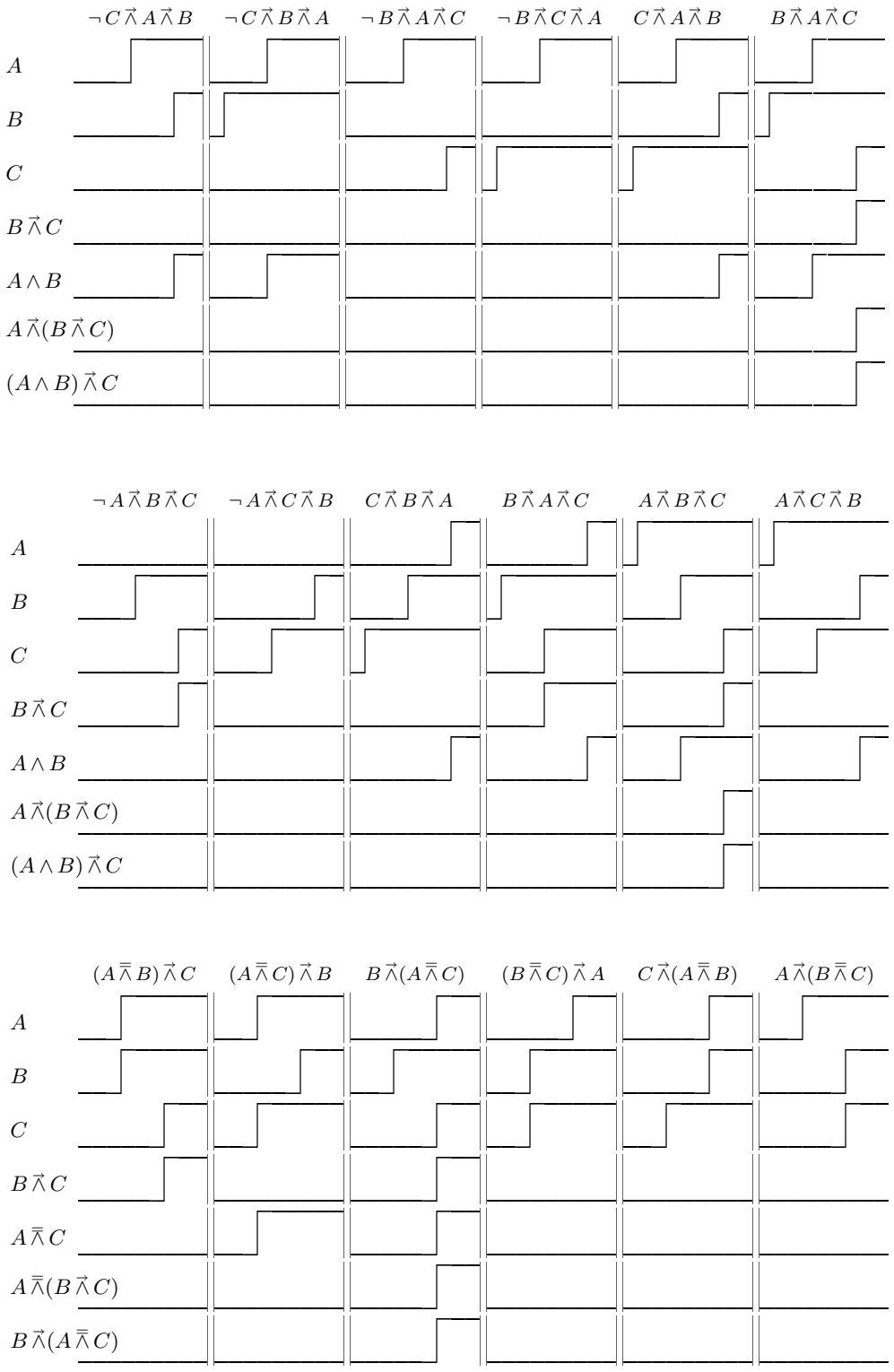


Abbildung 4.9: Zeitliche Ablaufdiagramme für eine Auswahl der möglichen Sequenzen aus Tabelle 4.2, welche die Gültigkeit der Zusammenhänge aus (4.48) (obere zwei Diagramme) bzw. (4.49) (unteres Diagramm) demonstrieren.

4.2.8 Temporale Operationen mit negierten Ereignissen

Anmerkung: Die folgenden Ausführungen beziehen sich zunächst ausschließlich auf atomare negierte Ereignisse. Besonderheiten, wie sie mit nichtatomaren negierten Ereignissen verbunden sind, werden ab Seite 44 behandelt.

4.2.8.1 Interpretation negierter Ereignisse in der TFTA

Ein nichtnegiertes Ereignis repräsentiert in der TFTA ebenso wie in der klassischen FTA das Eintreten eines Ausfalls einer realen Einheit. Entsprechend repräsentiert ein negiertes Ereignis das „Nicht-Ausfallen“ einer realen Einheit.

Prinzipiell sind zwei Interpretationen möglich:

1. Die Reparatur einer vorher ausgefallenen realen Einheit. Dabei ist das „Nicht-Ausfallen“ ein Zustandswechsel oder eine Aktion.

2. Das „Noch-Nicht-Ausgefallen-Sein“ einer noch funktionierenden realen Einheit. Dabei ist das „Nicht-Ausfallen“ ein Zustand.

Für die hier diskutierte temporale Logik in der Anwendung der TFTA sind für die weitere Interpretation die angenommene Monotonie der (temporalen) Ausfallfunktionen und die Nichtreparierbarkeit von Einheiten von großer Bedeutung.

Erstens sind anfangs bei $t = 0$ alle Einheiten funktionstüchtig. Ausfälle treten zu $t > 0$ ein und werden im (temporalen) Fehlerbaum durch (nichtnegierte) Ausfallereignisse X_i repräsentiert. Diese wechseln zu $t_{X_i} > 0$ von *False* nach $True$.

Zweitens sind alle Einheiten nicht reparierbar. Einmal zu t_{X_i} eingetretene Ausfall-Ereignisse bleiben eingetreten. Für negierte Ereignisse bedeutet dies, dass sie zwar zu t_{X_i} von *True* nach *False* wechseln, danach aber nicht wieder von *False* nach $True$ wechseln können. Entsprechend ist ein negiertes Ereignis in der TFTA

$$\neg X_i = \begin{cases} True & \text{von } [0; t_{X_i}[\quad \text{und} \\ False & \text{von } [t_{X_i}; \infty[\ , \end{cases} \tag{4.50}$$

wobei $t_{X_i} > 0$ gilt.

Somit wird klar, dass die erste Interpretation in der TFTA nicht zulässig ist und negierte Ereignisse in der TFTA ausschließlich „noch nicht ausgefallene“ Einheiten repräsentieren.

4.2.8.2 Verwendung negierter Ereignisse in der TFTA

Die Verwendung negierter Ereignisse erfolgt in der TFTA – wie auch in der herkömmlichen FTA – prinzipiell in zwei verschiedenen Ausprägungen:

1. Ohne explizite Modellierung von NOT Gattern im Fehlerbaum-Modell enthält die temporale Ausfallfunktion negierte Ereignisse als Folge einer logischen Umformung. So erfolgt z. B. die Überführung nichtdisjunkter Terme in eine disjunkte Form unter Verwendung negierter Ereignisse.

2. Mit Hilfe von NOT Gattern werden im Fehlerbaum-Modell negierte Ereignisse explizit modelliert. Diese Negationen von Basisereignissen oder nichtatomaren Ereignissen (Teilbäumen) dienen wiederum als Eingang zu weiteren, übergeordneten Fehlerbaum-Gattern. Entsprechend des so erzeugten Fehlerbaums enthält auch die Ausfallfunktion negierte Ereignisse.

Negierte Ereignisse als Resultat logischer Umformungen
Im Booleschen Fall erfordert die Überführung nichtdisjunkter Terme in eine disjunkte Form negierte Ereignisse [34, 80, 81]. Diese treten allerdings ausschließlich in Konjunktionstermen in Kombination mit mindestens einem nichtnegierten Ereignis auf. Die Monotonie-Bedingung ist dabei nicht verletzt, da keine wesentlichen Vermaschungen entstehen, vgl. [7]. Darüber hinaus führt keine der Booleschen Logik-Regeln negierte Ereignisse neu ein (die De Morganschen Theoreme beschreiben lediglich die Umformung existierender negierter Ereignisse).

Auch in der temporalen Logik basiert die Überführung in eine disjunkte Form auf der Verwendung negierter Ereignisse, vgl. Kapitel 4.3. Anders als in der Booleschen Logik existieren mit den temporalen Distributivgesetzen, vgl. Kapitel 4.2.10, allerdings Umformungs-Regeln, die ebenfalls negierte Ereignisse erfordern. Auch dabei treten negierte Ereignisse jedoch ausschließlich in Konjunktionstermen in Kombination mit mindestens einem nichtnegierten Ereignis auf, ohne die Monotonie-Bedingung zu verletzen.

Explizites Modellieren negierter Ereignisse im Fehlerbaum
Diese Verwendung ist ohne Verletzung der Monotonie-Bedingung genau dann erlaubt, wenn wiederum keine wesentlichen Vermaschungen mit negierten Ereignissen entstehen, vgl. [7]. Dies ist insbesondere für solche Spezialfälle gegeben, in denen im Fehlerbaum das Ergebnis einer der oben beschriebenen logischen Umformungen explizit modelliert wird.

Allgemein ist festzustellen, dass in der TFTA Ausdrücke wie

- „A ist noch nicht ausgefallen bevor B noch nicht ausgefallen ist“, also ein $\neg A \,\vec{\wedge}\, \neg B$,
- „A und B sind gleichzeitig noch nicht ausgefallen“, also ein $\neg A \,\overline{\vec{\wedge}}\, \neg B$,
- „A ist ausgefallen, weil B noch nicht ausgefallen ist oder C ausgefallen ist“, also $A = \neg B \vee C$,

nicht zulässig (und auch logisch nicht sinnvoll) sind. Daher besteht keine Notwendigkeit, negierte Ereignisse explizit als Eingang eines PAND oder SAND Gatters oder in Kombination mit nichtnegierten Ereignissen als Eingang eines OR Gatters zu modellieren.

Wie oben erwähnt ist es hingegen zulässig, Ausdrücke wie $\neg A \wedge B$ auch explizit im Fehlerbaum zu modellieren, wenn dabei die Monotonie erhalten bleibt.

4.2.8.3 Regeln der temporalen Logik für negierte Ereignisse

Aus dem oben Diskutierten folgt, dass das Vervollständigungsgesetz nach (4.37) nicht gilt, wenn mindestens einer der beiden Operanden der Konjunktion ein negiertes Ereignis ist.

Dies hat primär zur Folge, dass auch durch die Anwendung der anderen Gesetzmäßigkeiten der temporalen Logik keine Situation entsteht, in der ein negiertes Ereignis als Operand eines PAND oder SAND Operators erscheint (im Falle der temporalen Distributivgesetze sind alle negierten Ereignisse Teil eines Konjunktionsterms, vgl. Kap 4.2.10). Daraus folgt, dass im Wesentlichen die Booleschen Regeln für den Umgang mit negierten Ereignissen greifen, vgl. Kapitel 4.2.1.

Besondere Aufmerksamkeit erfordern „Mischterme“, in denen negierte Ereignisse und temporale Terme gemeinsam Teil eines Konjunktionsterms sind. Es gelten

$$\neg A \wedge (\ldots \vec{\wedge}\, A \vec{\wedge} \ldots) = \mathit{False}\ , \tag{4.51}$$

$$\neg A \wedge (\ldots \vec{\wedge} (A \,\overline{\vec{\wedge}}\, \ldots) \vec{\wedge} \ldots) = \mathit{False}\ , \tag{4.52}$$

sowie

$$(\neg A \wedge B) \wedge C = \big[\neg A \wedge (B \wedge C)\big] \vee \big[(B \,\vec{\wedge}\, A) \wedge C\big] =$$

$$= \left[\neg A \wedge (B \wedge C)\right] \vee \left[B \,\vec{\wedge}\, A \,\vec{\wedge}\, C\right] \vee \left[B \,\vec{\wedge}\, (A \,\bar{\vec{\wedge}}\, C)\right] , \tag{4.53}$$

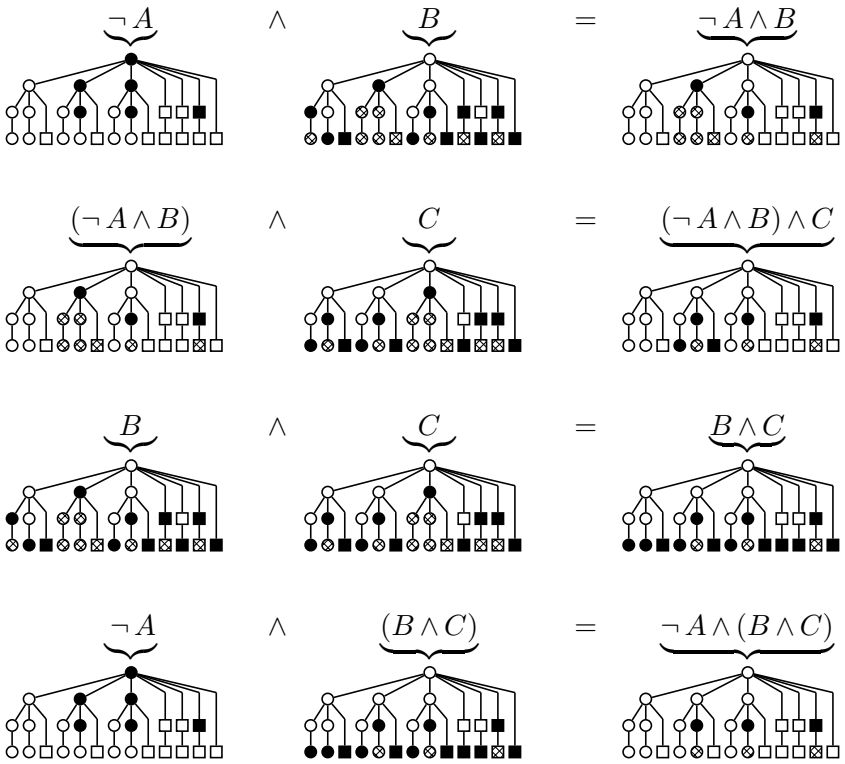
$$(\neg A \wedge B) \,\vec{\wedge}\, C = \left[\neg A \wedge (B \,\vec{\wedge}\, C)\right] \vee \left[B \,\vec{\wedge}\, A \,\vec{\wedge}\, C\right] \vee \left[B \,\vec{\wedge}\, (A \,\bar{\vec{\wedge}}\, C)\right] , \tag{4.54}$$

$$(\neg A \wedge B) \,\bar{\vec{\wedge}}\, C = \neg A \wedge (B \,\bar{\vec{\wedge}}\, C) , \tag{4.55}$$

$$C \,\vec{\wedge}\, (\neg A \wedge B) = \neg A \wedge (C \,\vec{\wedge}\, B) . \tag{4.56}$$

Anhand von (4.53) zeigt sich der eine wesentliche Unterschied bei der Verwendung negierter Ereignisse in der temporalen Logik im Vergleich zur Booleschen Logik.

In Letzterer gilt auch bei negierten Ereignissen das Assoziativgesetz aus (4.31). Im Gegensatz dazu besitzen negierte Ereignisse in der temporalen Logik eine „Gültigkeitsdauer“, ausgedrückt durch die Klammerung. So bedeutet $(\neg A \wedge B) \wedge C$, dass zum Zeitpunkt des Eintretens von B das Ereignis A „noch nicht“ eingetreten ist, und – ohne Aussage einer zeitlichen Beziehung – Ereignis C eingetreten ist. Im Gegensatz dazu beinhaltet $\neg A \wedge (B \wedge C)$ zeitliche Beziehungen zwischen allen drei Ereignissen und bedeutet, dass zum Zeitpunkt des Eintretens von „B und C“ das Ereignis A „noch nicht“ eingetreten ist:



Diese Regelung wirkt sich insbesondere auch aus auf Terme der folgenden Art:

$$(\neg A \wedge B) \,\bar{\vec{\wedge}}\, A = \neg A \wedge (B \,\bar{\vec{\wedge}}\, A) = \mathit{False} , \tag{4.57}$$

$$A \,\vec{\wedge}\, (\neg A \wedge B) = \neg A \wedge (A \,\vec{\wedge}\, B) = \mathit{False} , \tag{4.58}$$

$$\begin{aligned}(\neg A \wedge B) \,\vec{\wedge}\, A &= \left[\neg A \wedge (B \,\vec{\wedge}\, A)\right] \vee \left[B \,\vec{\wedge}\, A \,\vec{\wedge}\, A\right] \vee \left[B \,\vec{\wedge}\, (A \,\bar{\vec{\wedge}}\, A)\right] = \\ &= \mathit{False} \vee \mathit{False} \vee \left[B \,\vec{\wedge}\, A\right] = B \,\vec{\wedge}\, A .\end{aligned} \tag{4.59}$$

Kapitel 4.3.2.2 behandelt die in diesen Termen enthaltene „zeitliche (Nicht-)Minimalität“.

4.2.8.4 Konjunktion aus mehreren negierten Ereignissen

Bislang wurden Konjunktionen aus mehreren negierten Ereignissen, z. B.

$$\neg A \neg B \;=\; \neg A \wedge \neg B \tag{4.60}$$

nicht explizit betrachtet. Für die Anwendung in der TFTA werden solche Konjunktionen als nicht unterteilbare Einheiten betrachtet, sodass die oben aufgeführten Logik-Regeln für negierte Ereignisse sinngemäß gelten.

Aus dieser Annahme folgt auch, dass

$$\neg A \wedge (\neg B \wedge C) \;=\; (\neg A \neg B) \wedge C \;. \tag{4.61}$$

4.2.8.5 Temporale Negationsgesetze / Negation nichtatomarer negierter Ereignisse

Alle Ausführungen zu negierten Ereignissen beziehen sich bisher ausschließlich auf atomare Ereignisse, d. h. Basisereignisse. Im Falle negierter nichtatomarer Ereignisse, z. B. $\neg(A \vec{\wedge} B)$ sind zusätzliche Punkte zu beachten.

Im Falle Boolescher nichtatomarer Terme, also $\neg(A \wedge B)$ und $\neg(A \vee B)$, erfolgt die Negation nach den Vorgaben der De Morganschen Theoreme in (4.35). Die Negationen von SAND oder PAND Termen lassen sich aus der Darstellung in Abbildung 4.2 ableiten und besagen, dass

$$\neg(A \vec{\wedge} B) \;=\; (\neg A \neg B) \vee (\neg B \wedge A) \vee (\neg A \wedge B) \vee (B \vec{\wedge} A) \vee (A \overline{\vec{\wedge}} B) \qquad \text{und} \tag{4.62}$$

$$\neg(A \overline{\vec{\wedge}} B) \;=\; (\neg A \neg B) \vee (\neg B \wedge A) \vee (\neg A \wedge B) \vee (A \vec{\wedge} B) \vee (B \vec{\wedge} A) \;. \tag{4.63}$$

Die Teil-Terme auf den rechten Seiten sind jeweils disjunkt und enthalten jeweils explizite Angaben zu allen beteiligten Ereignissen, vgl. Kapitel 4.3.3.

Auch solche nichtatomaren negierten Terme treten in der TFTA nur als Konjunktion mit weiteren nichtnegierten Ereignissen auf. Sie beschreiben dann einen Systemzustand, in dem zu einem bestimmten Zeitpunkt bestimmte Ereignissequenzen „noch nicht“ eingetreten sind. Die rechten Seiten in (4.35) und (4.62) und (4.63) geben jeweils verschiedene Möglichkeiten an, wie dieser Systemzustand erreicht wurde.

So beschreibt z. B. der temporale Term $\neg(A \vec{\wedge} B) \wedge C$ einen Zustand, in dem zum Zeitpunkt des Eintretens von C nicht die Ereignissequenz $A \vec{\wedge} B$ eingetreten sein darf. Dies ist genau dann der Fall, wenn zum Zeitpunkt des Eintretens von C

- weder A noch B eingetreten sind – also $(\neg A \neg B) \wedge C$ –
- oder zwar A aber nicht B eingetreten ist – also $\neg B \wedge (A \wedge C)$ –
- oder zwar B aber nicht A eingetreten ist – also $\neg A \wedge (B \wedge C)$ –
- oder B vor A eingetreten ist – also $(B \vec{\wedge} A) \wedge C$ –
- oder A und B gleichzeitig eingetreten sind – also $(A \overline{\vec{\wedge}} B) \wedge C$.

Das *erste temporale Negationsgesetz* besagt somit, dass

$$\begin{aligned} \neg(A \overline{\vec{\wedge}} B) \wedge C \;=\; & \big[(\neg A \neg B) \wedge C\big] \vee \big[\neg B \wedge (A \wedge C)\big] \vee \big[\neg A \wedge (B \wedge C)\big] \vee \\ & \vee \big[(A \vec{\wedge} B) \wedge C\big] \vee \big[(B \vec{\wedge} A) \wedge C\big] \;. \end{aligned} \tag{4.64}$$

Analog dazu lautet das *zweite temporale Negationsgesetz*

$$\begin{aligned} \neg(A \vec{\wedge} B) \wedge C \;=\; & \big[(\neg A \neg B) \wedge C\big] \vee \big[\neg B \wedge (A \wedge C)\big] \vee \big[\neg A \wedge (B \wedge C)\big] \vee \\ & \vee \big[(B \vec{\wedge} A) \wedge C\big] \vee \big[(A \overline{\vec{\wedge}} B) \wedge C\big] \;. \end{aligned} \tag{4.65}$$

4.2.9 Temporale Operationen mit *True* und *False*

Operationen mit den „zeitlosen“ Ausdrücken *True* und *False* sollten in der TFTA nur dann vorkommen, wenn ein komplexerer Term zu *True* und *False* vereinfacht werden konnte. Für selbst nicht negierte X und $X \neq True$ gelten

$$X \vec{\wedge} True = False\ , \quad X \bar{\vec{\wedge}} True = False\ , \quad True \vec{\wedge} X = X\ , \tag{4.66}$$
$$X \vec{\wedge} False = False\ , \quad X \bar{\vec{\wedge}} False = False\ , \quad False \vec{\wedge} X = False\ . \tag{4.67}$$

Weiterhin gelten

$$True \vec{\wedge} True = False\ , \quad True \bar{\vec{\wedge}} True = True\ , \quad False \vec{\wedge} True = False\ . \tag{4.68}$$

Somit ist die Durchlässigkeit zu den weiterhin geltenden Booleschen Regeln gegeben, denenzufolge $X \wedge True = X$ und $X \wedge False = False$:

$$X \wedge True = (X \vec{\wedge} True) \vee (X \bar{\vec{\wedge}} True) \vee (True \vec{\wedge} X) = True \vec{\wedge} X = X\ ,$$
$$X \wedge False = (X \vec{\wedge} False) \vee (X \bar{\vec{\wedge}} False) \vee (False \vec{\wedge} X) = False \vec{\wedge} X = False\ .$$

4.2.10 Temporale Distributivgesetze

Die Boolesche Logik kennt das Distributivgesetz aus (4.32). In Kombination mit der Assoziativität der Booleschen Operatoren OR und AND, vgl. (4.31), gilt

$$(A \vee B) \wedge C = C \wedge (B \vee A) = (A \wedge C) \vee (B \wedge C) = (C \wedge B) \vee (C \wedge A)\ . \tag{4.69}$$

Das Distributivgesetz spielt eine große Rolle für die Umformung Boolescher Ausdrücke hin zu einer disjunktiven Normalform (DNF).

Ähnlich den Booleschen Operatoren ist auch der SAND Operator der temporalen Logik assoziativ, d. h. es gelten Assoziativ- und Kommutativgesetze, vgl. (4.44) und (4.46). Hingegen gilt für den PAND Operator der temporalen Logik offenbar kein Kommutativgesetz, vgl. (4.45), da dieser seine Logikinformation gerade in der Sequenz der Ereignisse „speichert“.

Für ein möglicherweise geltendes Distributivgesetz für den PAND Operator ist somit jedenfalls zu unterscheiden zwischen

$$A \vec{\wedge} (B \vee C) \quad \text{, genannt } \textit{Typ I}, \quad \text{und} \tag{4.70}$$
$$(A \vee B) \vec{\wedge} C \quad \text{, genannt } \textit{Typ II}. \tag{4.71}$$

Die folgenden beiden Abschnitte diskutieren zunächst die temporalen Distributivgesetze für den PAND Operator und die beiden Typen I und II und das temporale Distributivgesetz für den SAND Operator, für den eine weitere Unterscheidung nicht notwendig ist.

4.2.10.1 Distributivgesetz für PAND-OR Terme vom Typ I

Die logische Aussage des Terms $A \vec{\wedge} (B \vee C)$ lautet: „A muss eintreten, bevor der geklammerte Ausdruck $(B \vee C)$ eintritt“. Wie Tabelle 4.3 und Abbildung 4.10 zeigen, ist dies *nicht* gleichbedeutend mit der Aussage „A muss vor B eintreten ODER A muss vor C eintreten“. Da somit

$$A \vec{\wedge} (B \vee C) \neq (A \vec{\wedge} B) \vee (A \vec{\wedge} C)\ , \tag{4.72}$$

existiert zumindest für Terme vom Typ I kein „einfaches“ Distributivgesetz.

Tatsächlich enthält der ursprüngliche Term, also die linke Seite in (4.72), keine explizite zeitliche Abhängigkeit zwischen den Ereignissen B und C, wohl aber eine durch den gesamten Term implizit ausgedrückte zeitliche Abhängigkeit zwischen B und C. Diese zeitliche Abhängigkeit betrifft primär nicht das Eintreten (weiterer) Ereignisse, sondern vielmehr das Nicht-Eintreten von $A \vec{\wedge} (B \vee C)$, wenn nur eines der beiden Ereignisse B oder C vor A eintritt. Diese Abhängigkeit ist auf der rechten Seite des Terms in (4.72) verloren gegangen. Dieses Problem lässt sich umgehen, indem die in (4.72) links implizit enthaltenen zeitlichen Abhängigkeiten auch explizit aufgeführt werden.

Der Term $(B \vee C)$ lässt sich allgemein in fünf mögliche Sequenzen aufteilen:

$$(B \vee C) = (\neg C \,\vec{\wedge}\, B) \vee (\neg B \,\vec{\wedge}\, C) \vee (B \,\vec{\wedge}\, C) \vee (C \,\vec{\wedge}\, B) \vee (B \,\overline{\vec{\wedge}}\, C) \ ,$$

von denen jedoch nur drei Sequenzen minimal sind, vgl. Abbildung 4.10 (links):

$$(B \vee C) = (\neg C \wedge B) \vee (\neg B \wedge C) \vee (B \,\overline{\vec{\wedge}}\, C) \ . \tag{4.73}$$

Einsetzen in (4.70) liefert für temporale Terme von Typ I somit

$$A \vec{\wedge} (B \vee C) \ = \ A \vec{\wedge} \left[(\neg C \wedge B) \vee (\neg B \wedge C) \vee (B \,\overline{\vec{\wedge}}\, C) \right] \ . \tag{4.74}$$

Eine Berücksichtigung der nichtminimalen Sequenzen ist an dieser Stelle nicht erforderlich. Da der geklammerte Term mit der OR Verknüpfung rechts vom PAND Operator steht und somit „später“ eintritt, treten die nichtminimalen Terme „noch später“ ein. Sie sind somit von den minimalen Termen abgedeckt oder in ihnen enthalten.

	$A\vec{\wedge}(B\vee C)$	$(A\vec{\wedge}B)\vee(A\vec{\wedge}C)$		$A\vec{\wedge}(B\vee C)$	$(A\vec{\wedge}B)\vee(A\vec{\wedge}C)$
$\neg A \neg B \neg C$	*False*	*False*	$A \,\vec{\wedge}\, B \,\vec{\wedge}\, C$	*True*	*True*
$\neg B \neg C \wedge A$	*False*	*False*	$B \,\vec{\wedge}\, A \,\vec{\wedge}\, C$	***False***	***True***
$\neg A \neg C \wedge B$	*False*	*False*	$A \,\vec{\wedge}\, C \,\vec{\wedge}\, B$	*True*	*True*
$\neg A \neg B \wedge C$	*False*	*False*	$C \,\vec{\wedge}\, A \,\vec{\wedge}\, B$	***False***	***True***
$\neg C \wedge (A \,\vec{\wedge}\, B)$	*True*	*True*	$B \,\vec{\wedge}\, C \,\vec{\wedge}\, A$	*False*	*False*
$\neg C \wedge (B \,\vec{\wedge}\, A)$	*False*	*False*	$C \,\vec{\wedge}\, B \,\vec{\wedge}\, A$	*False*	*False*
$\neg C \wedge (A \,\overline{\vec{\wedge}}\, B)$	*False*	*False*	$A \,\vec{\wedge}\, (B \,\overline{\vec{\wedge}}\, C)$	*True*	*True*
$\neg B \wedge (A \,\vec{\wedge}\, C)$	*True*	*True*	$B \,\vec{\wedge}\, (A \,\overline{\vec{\wedge}}\, C)$	*False*	*False*
$\neg B \wedge (C \,\vec{\wedge}\, A)$	*False*	*False*	$C \,\vec{\wedge}\, (A \,\overline{\vec{\wedge}}\, B)$	*False*	*False*
$\neg B \wedge (A \,\overline{\vec{\wedge}}\, C)$	*False*	*False*	$(A \,\overline{\vec{\wedge}}\, B) \,\vec{\wedge}\, C$	***False***	***True***
$\neg A \wedge (B \,\vec{\wedge}\, C)$	*False*	*False*	$(A \,\overline{\vec{\wedge}}\, C) \,\vec{\wedge}\, B$	***False***	***True***
$\neg A \wedge (C \,\vec{\wedge}\, B)$	*False*	*False*	$(B \,\overline{\vec{\wedge}}\, C) \,\vec{\wedge}\, A$	*False*	*False*
$\neg A \wedge (B \,\overline{\vec{\wedge}}\, C)$	*False*	*False*	$A \,\overline{\vec{\wedge}}\, B \,\overline{\vec{\wedge}}\, C$	*False*	*False*

Tabelle 4.3: Wahrheitstabelle für die Terme $A \vec{\wedge} (B \vee C)$ und $(A \vec{\wedge} B) \vee (A \vec{\wedge} C)$. Inklusive der SAND Verknüpfungen existieren 26 Sequenzen, hier in zweimal 13 Zeilen partitioniert. Da die Ergebnisse der beiden Terme nicht für alle Sequenzen übereinstimmen (Abweichungen fett markiert), sind die beiden Terme nicht logisch äquivalent.

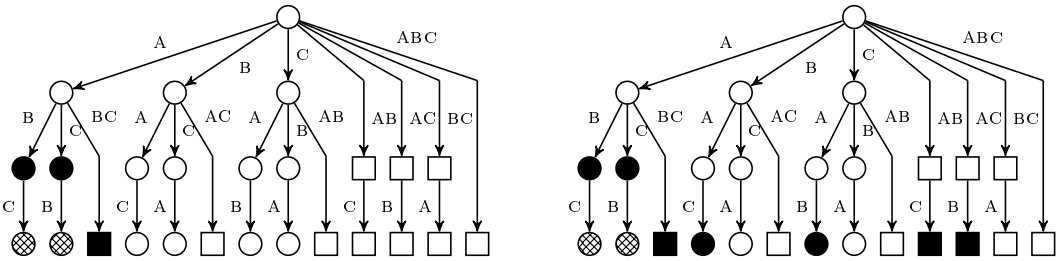


Abbildung 4.10: Links: Sequentieller Ausfallbaum für den Ausdruck $A \vec{\wedge} (B \vee C)$. Rechts: Sequentieller Ausfallbaum für den Ausdruck $(A \vec{\wedge} B) \vee (A \vec{\wedge} C)$. Im Gegensatz zur Abbildung links sind zusätzliche Sequenzen enthalten, da jeder der beiden Teilterme $(A \vec{\wedge} B)$ und $(A \vec{\wedge} C)$ keine Aussage zum Eintreten des jeweils fehlenden dritten Ereignisses macht.

An dieser Stelle sind alle zeitlichen Abhängigkeiten explizit berücksichtigt, sodass eine Distribution nun möglich ist:

$$A \vec{\wedge} (B \vee C) = \left[A \vec{\wedge} (\neg C \wedge B)\right] \vee \left[A \vec{\wedge} (\neg B \wedge C)\right] \vee \left[A \vec{\wedge} (B \bar{\wedge} C)\right]. \tag{4.75}$$

Weitere Umformungen aus Kapitel 4.2.8 führen dann zum temporalen Distributivgesetz für temporale Terme vom Typ I:

$$A \vec{\wedge} (B \vee C) = \left[\neg C \wedge (A \vec{\wedge} B)\right] \vee \left[\neg B \wedge (A \vec{\wedge} C)\right] \vee \left[A \vec{\wedge} (B \bar{\wedge} C)\right] . \tag{4.76}$$

Das temporale Distributivgesetz für Terme vom Typ I erfordert also in jedem disjunktiv verbundenen Teilterm explizite Angaben zum (Nicht-)Eintreten aller beteiligten Ereignisse. Ausdrücke, die diese Eigenschaft erfüllen, werden in Analogie zur Booleschen Algebra mit ihren *Mintermen* (auch: *vollständige Konjunktionsterme*) als *temporale Minterme* bezeichnet.

Unter Anwendung der temporalen Negationsgesetze gilt (4.76) auch für den Fall nichtatomarer Ereignisse A, B, C.

Die Terme der rechten Seite in (4.76) sind disjunkt. Dies vereinfacht später die Quantifizierung erheblich, vgl. Kapitel 5.

Sonderfall disjunkter Terme

Der in (4.76) beschriebene Zusammenhang gilt zwar auch für den Sonderfall disjunkter Ereignisse B und C, also $B \perp C$. Aus $B \perp C$ folgt jedoch, dass jedes Ereignis B oder C nur dann eintritt, wenn das jeweils andere Ereignis nicht eintritt bzw. eingetreten ist, sodass an Stelle von (4.76) auch das wesentlich einfachere

$$A \vec{\wedge} (B \vee C) = \left[A \vec{\wedge} B\right] \vee \left[A \vec{\wedge} C\right] \tag{4.77}$$

gilt, wenn $B \perp C$.

4.2.10.2 Distributivgesetz für PAND-OR Terme vom Typ II

Die logische Aussage des Terms $(A \vee B) \vec{\wedge} C$ lautet: „Der geklammerte Ausdruck $(A \vee B)$ muss eintreten, bevor C eintritt“. Wie die sequentiellen Ausfallbäume in Abbildung 4.11 zu den drei Termen $(A \vee B) \vec{\wedge} C$, $(A \vec{\wedge} C)$ und $(B \vec{\wedge} C)$ zeigen, ist dies *logisch* gleichbedeutend mit der Aussage „A muss vor C eintreten ODER B muss vor C eintreten“. Somit gilt folgendes temporale

Distributivgesetz für temporale Terme vom Typ II:

$$(A \vee B) \vec{\wedge} C = (A \vec{\wedge} C) \vee (B \vec{\wedge} C) \ . \tag{4.78}$$

Abbildung 4.11 zeigt jedoch auch, dass $(A \vec{\wedge} C)$ und $(B \vec{\wedge} C)$ nicht disjunkt sind. Die in den beiden Termen enthaltenen Sequenzen lassen sich durch Bildung der Schnittmenge leicht ermitteln:

$$(A \vec{\wedge} C) \wedge (B \vec{\wedge} C) \ = \ (A \wedge B) \vec{\wedge} C \ = \ \left[A \vec{\wedge} B \vec{\wedge} C\right] \vee \left[B \vec{\wedge} A \vec{\wedge} C\right] \vee \left[(A \bar{\wedge} B) \vec{\wedge} C\right] \ .$$

In Abbildung 4.11 sind sie zur Verdeutlichung mit einem $\star$ markiert.

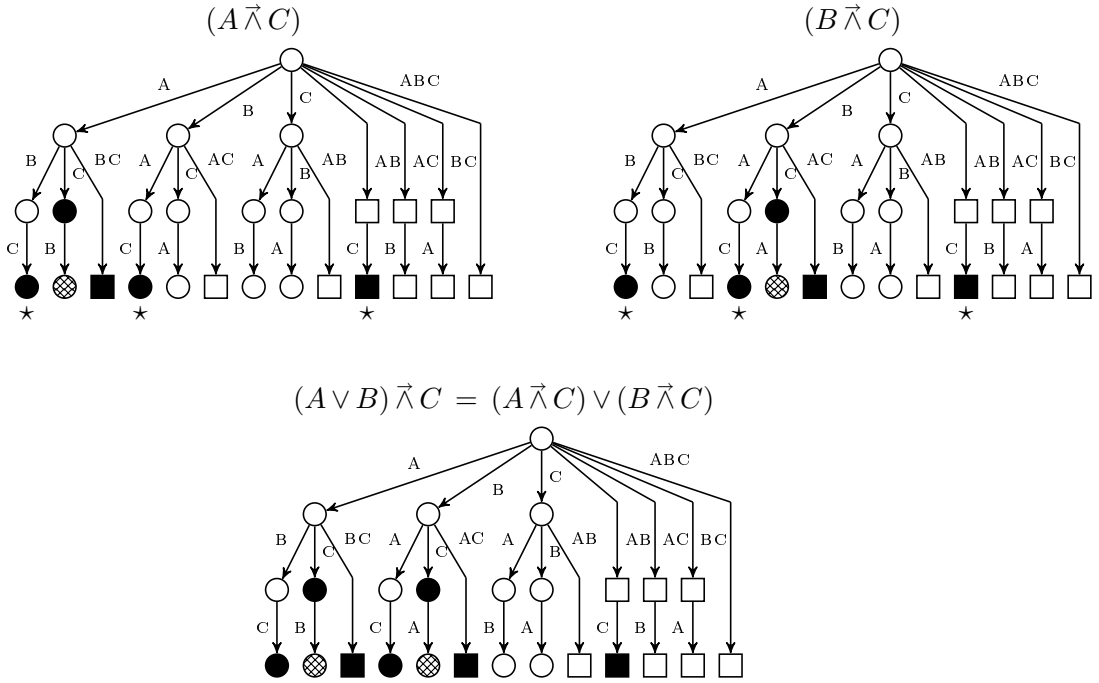


Abbildung 4.11: Distributivgesetz für Terme vom Typ II: Die sequentiellen Ausfallbäume zu den Termen $(A \vee B) \vec{\wedge} C$, $(A \vec{\wedge} C)$, $(B \vec{\wedge} C)$ zeigen, dass $(A \vec{\wedge} C)$ und $(B \vec{\wedge} C)$ minimal sind, wegen der mit $\star$ markierten Sequenzen aber nicht disjunkt sind.

4.2.10.3 Distributivgesetz für SAND-OR Terme

Die logische Aussage des Terms $A \bar{\wedge} (B \vee C)$ lautet: „A muss gleichzeitig mit dem geklammerten Ausdruck $(B \vee C)$ eintreten“. Analog zum Distributivgesetz für Terme vom Typ I lässt sich einfach zeigen, dass dies *nicht* gleichbedeutend ist mit der Aussage „A muss gleichzeitig mit B eintreten ODER A muss gleichzeitig mit C eintreten“, vgl. Abbildung 4.12. Somit existiert auch für solche temporalen Terme mit SAND Verknüpfung kein „einfaches“ Distributiv-Gesetz.

Tatsächlich lautet das Distributivgesetz für SAND Terme daher in Analogie zu (4.76):

$$A \bar{\wedge} (B \vee C) = \left[\neg C \wedge (A \bar{\wedge} B)\right] \vee \left[\neg B \wedge (A \bar{\wedge} C)\right] \vee \left[A \bar{\wedge} B \bar{\wedge} C\right] \ . \tag{4.79}$$

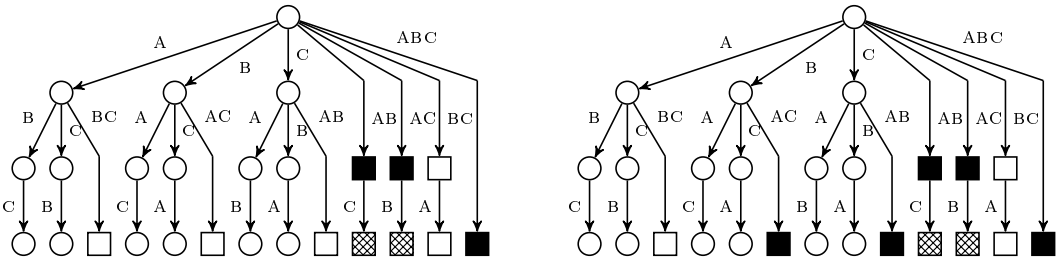


Abbildung 4.12: Links: Sequentieller Ausfallbaum für den Ausdruck $A \,\overline{\overline{\wedge}}\, (B \vee C)$. Rechts: Sequentieller Ausfallbaum für den Ausdruck $(A \,\overline{\overline{\wedge}}\, B) \vee (A \,\overline{\overline{\wedge}}\, C)$. Im Gegensatz zur Abbildung links sind zusätzliche Sequenzen enthalten, da jeder der beiden Teilterme $(A \,\overline{\overline{\wedge}}\, B)$ und $(A \,\overline{\overline{\wedge}}\, C)$ keine Aussage zum Eintreten des jeweils fehlenden dritten Ereignisses macht.

Sonderfall disjunkter Terme

Der in (4.79) beschriebene Zusammenhang gilt zwar auch für den Sonderfall disjunkter Ereignisse B und C, also $B \perp C$. Aus $B \perp C$ folgt jedoch, dass jedes Ereignis B oder C nur dann eintritt, wenn das jeweils andere Ereignis nicht eintritt bzw. eingetreten ist, sodass an Stelle von (4.79) auch das wesentlich einfachere

$$A \,\overline{\overline{\wedge}}\, (B \vee C) \;=\; \big[A \,\overline{\overline{\wedge}}\, B\big] \vee \big[A \,\overline{\overline{\wedge}}\, C\big] \;. \tag{4.80}$$

gilt, wenn $B \perp C$.

4.2.11 Temporale Absorptionsgesetze

Analog zu den Booleschen Absorptionsgesetzen aus (4.34) lassen sich auch *temporale Absorptionsgesetze* beschreiben. Auf Grund der bei der Berücksichtigung von Reihenfolgen möglichen Permutationen hängen die temporalen Absorptionsgesetze zunächst scheinbar von der Anzahl der beteiligten Ereignisse ab. Wie im Folgenden gezeigt, handelt es sich bei den temporalen Absorptionsgesetzen jedoch lediglich um Spezialisierungen der Booleschen Absorptionsgesetze in (4.34).

Im einfachsten Fall mit lediglich zwei Ereignissen ergeben sich die temporalen Absorptionsgesetze mit Hilfe des Vervollständigungsgesetzes in (4.37) direkt aus (4.34) zu

$$A \vee (A \wedge B) \;=\; A \;=\; A \vee \big[(A \,\vec{\wedge}\, B) \vee (A \,\overline{\overline{\wedge}}\, B) \vee (B \,\vec{\wedge}\, A)\big] \;, \tag{4.81}$$

und weiter zu

$$A \vee (A \,\vec{\wedge}\, B) \;=\; A \;, \tag{4.82}$$

$$A \vee (B \,\vec{\wedge}\, A) \;=\; A \;, \tag{4.83}$$

$$A \vee (A \,\overline{\overline{\wedge}}\, B) \;=\; A \;. \tag{4.84}$$

Analog zum Booleschen Fall absorbiert das „allgemeinere“ Ereignis A das „konkretere“ Ereignis, wenn dieses eine Teilmenge von A ist. Ist ES eine (erweiterte) Ereignissequenz, so gilt

$$A \vee ES \;=\; A \qquad\qquad \text{, wenn } A \notin ES, \text{ d\,h. } ES \subseteq A \;. \tag{4.85}$$

Dieser Zusammenhang gilt allgemein, insbesondere auch für nichtatomare Ereignisse A. Im Vergleich zum Booleschen Absorptionsgesetz sind für komplexere Terme jedoch die Teilmengen

nicht immer offensichtlich. Dazu tragen insbesondere bei, dass für den PAND Operator kein Kommutativgesetz existiert, und dass durch das Konzept der Kernereignisse Verschachtelungen möglich sind.

So lauten die temporalen Absorptionsgesetze für drei Ereignisse z. B.

$$(A \vec{\wedge} B) \vee (A \vec{\wedge} B \vec{\wedge} C) = A \vec{\wedge} B \ , \tag{4.86}$$
$$(A \vec{\wedge} B) \vee (A \vec{\wedge} C \vec{\wedge} B) = A \vec{\wedge} B \ , \tag{4.87}$$
$$(A \vec{\wedge} B) \vee (C \vec{\wedge} A \vec{\wedge} B) = A \vec{\wedge} B \ , \tag{4.88}$$
$$(A \vec{\wedge} B) \vee ((A \bar{\vec{\wedge}} C) \vec{\wedge} B) = A \vec{\wedge} B, \tag{4.89}$$
$$(A \vec{\wedge} B) \vee ((A \vec{\wedge} B) \bar{\vec{\wedge}} C) = (A \vec{\wedge} B) \vee (A \vec{\wedge} (B \bar{\vec{\wedge}} C)) = A \vec{\wedge} B \ . \tag{4.90}$$

Tatsächlich handelt es sich bei (4.86) bis (4.90) lediglich um die Ausformulierung von

$$(A \vec{\wedge} B) \vee ((A \vec{\wedge} B) \wedge C) = (A \vec{\wedge} B) \ . \tag{4.91}$$

Dies zeigt die folgende Umformung:

$$\begin{aligned} (A \vec{\wedge} B) \wedge C &= \left[(A \vec{\wedge} B) \vec{\wedge} C\right] \vee \left[(A \vec{\wedge} B) \bar{\vec{\wedge}} C\right] \vee \left[C \vec{\wedge} (A \vec{\wedge} B)\right] = \\ &= \left[A \vec{\wedge} B \vec{\wedge} C\right] \vee \left[A \vec{\wedge} (B \bar{\vec{\wedge}} C)\right] \vee \left[A \vec{\wedge} C \vec{\wedge} B\right] \vee \left[C \vec{\wedge} A \vec{\wedge} B\right] \vee \left[(A \bar{\vec{\wedge}} C) \vec{\wedge} B\right] \ . \end{aligned} \tag{4.92}$$

Abstrahiert auf den allgemeinen Fall lautet das temporale Absorptionsgesetz somit in vollständiger Analogie zum Booleschen Absorptionsgesetz:

$$ES_i \vee ES_j = ES_i \qquad \text{für } ES_j \subseteq ES_i \ . \tag{4.93}$$

Auch das zweite Absorptionsgesetz der Booleschen Algebra in (4.34) besitzt in der temporalen Logik eine Entsprechung. So gelten

$$A \vec{\wedge} (A \vee B) = \left[\neg B \wedge (A \vec{\wedge} A)\right] \vee \left[\neg A \wedge (A \vec{\wedge} B)\right] \vee \left[A \vec{\wedge} (A \bar{\vec{\wedge}} B)\right] = \mathit{False} \ , \tag{4.94}$$
$$(A \vee B) \vec{\wedge} A = (A \vec{\wedge} A) \vee (B \vec{\wedge} A) = B \vec{\wedge} A \ , \tag{4.95}$$
$$\begin{aligned} A \bar{\vec{\wedge}} (A \vee B) &= \left[\neg B \wedge (A \bar{\vec{\wedge}} A)\right] \vee \left[\neg A \wedge (A \bar{\vec{\wedge}} B)\right] \vee \left[A \bar{\vec{\wedge}} (A \bar{\vec{\wedge}} B)\right] = \\ &= (\neg B \wedge A) \vee (A \bar{\vec{\wedge}} B) \ . \end{aligned} \tag{4.96}$$

Die Stimmigkeit dieser zunächst wenig intuitiven Ergebnisse zeigt sich durch folgende Umformung: Einerseits ist offensichtlich, dass

$$\left[A \vec{\wedge} (A \vee B)\right] \vee \left[(A \vee B) \vec{\wedge} A\right] \vee \left[A \bar{\vec{\wedge}} (A \vee B)\right] = A \wedge (A \vee B) = A \ .$$

Andererseits zeigen (4.94) bis (4.96), dass

$$\left[A \vec{\wedge} (A \vee B)\right] \vee \left[(A \vee B) \vec{\wedge} A\right] \vee \left[A \bar{\vec{\wedge}} (A \vee B)\right] = (B \vec{\wedge} A) \vee (\neg B \wedge A) \vee (A \bar{\vec{\wedge}} B) \ .$$

Da weiterhin $\neg B \wedge A$ auch die dazu nicht minimale Sequenz $A \vec{\wedge} B$ abdeckt, folgt

$$\begin{aligned} \left[A \vec{\wedge} (A \vee B)\right] \vee \left[(A \vee B) \vec{\wedge} A\right] \vee \left[A \bar{\vec{\wedge}} (A \vee B)\right] &= (B \vec{\wedge} A) \vee (\neg B \wedge A) \vee (A \bar{\vec{\wedge}} B) = \\ = (\neg B \wedge A) \vee (A \vec{\wedge} B) \vee (A \bar{\vec{\wedge}} B) \vee (B \vec{\wedge} A) &= (\neg B \wedge A) \vee (A \wedge B) = A \ . \end{aligned}$$

Diese Umformungen verdeutlichen, dass es sich auch bei (4.94) bis (4.96) lediglich um Ausformulierungen des Booleschen Absorptionsgesetzes handelt.

4.2.12 Temporale Konkretisierungsgesetze

Durch Einführung der PAND und SAND Operatoren in der temporalen Logik der TFTA existieren Terme wie $A \wedge (A \vec{\wedge} B)$, $B \wedge (A \vec{\wedge} B)$ oder $A \wedge (A \bar{\vec{\wedge}} B)$. Solche Terme lassen sich nur schlecht unter dem temporalen Absorptionsgesetz behandeln, da bei ihnen nicht – wie bei den Absorptionsgesetzen der Fall – der „allgemeinere" Term den „konkreteren" Term absorbiert. Daher wird für solche Terme im Folgenden eine neue Klasse von *temporalen Konkretisierungsgesetzen* vorgeschlagen.

Die temporalen Konkretisierungsgesetze beschreiben die Konjunktion zweier Terme, wobei der eine Term eine Schnittmenge oder *Konkretisierung* des anderen Terms ist. Im Booleschen Falle lässt sich dieses direkt mittels Assoziativ- und Idempotenzgesetzen vereinfachen:

$$A \wedge (A \wedge B) = A \wedge A \wedge B = A \wedge B \ . \tag{4.97}$$

Im temporalen Fall sind die folgenden drei Arten solcher Terme zu unterscheiden:

$$A \wedge (A \vec{\wedge} B) = (A \vec{\wedge} B) \wedge A = A \vec{\wedge} B \ , \tag{4.98}$$
$$B \wedge (A \vec{\wedge} B) = (A \vec{\wedge} B) \wedge B = A \vec{\wedge} B \ , \tag{4.99}$$
$$A \wedge (A \bar{\vec{\wedge}} B) = (A \bar{\vec{\wedge}} B) \wedge A = (B \bar{\vec{\wedge}} A) \wedge A = A \wedge (B \bar{\vec{\wedge}} A) = A \bar{\vec{\wedge}} B \ . \tag{4.100}$$

Diese Zusammenhänge lassen sich einfach durch Anwendung der bereits bekannten temporalen Regeln zeigen. So ist z. B.

$$\begin{aligned} A \wedge (A \vec{\wedge} B) &= \left[A \vec{\wedge} (A \vec{\wedge} B)\right] \vee \left[A \bar{\vec{\wedge}} (A \vec{\wedge} B)\right] \vee \left[(A \vec{\wedge} B) \vec{\wedge} A\right] = \\ &= (A \wedge A) \vec{\wedge} B \vee \mathit{False} \vee \mathit{False} = A \vec{\wedge} B \ . \end{aligned}$$

Entsprechendes gilt auch für die allgemeinen Fälle mit komplexeren Termen, also

$$X_i \wedge \ldots \wedge X_j \wedge (\ldots \vec{\wedge} X_i \vec{\wedge} \ldots) = X_j \wedge (\ldots \vec{\wedge} X_i \vec{\wedge} \ldots) \text{ und} \tag{4.101}$$
$$X_i \wedge \ldots \wedge X_j \wedge (\ldots \bar{\vec{\wedge}} X_i \bar{\vec{\wedge}} \ldots) = X_j \wedge (\ldots \bar{\vec{\wedge}} X_i \bar{\vec{\wedge}} \ldots) \ , \tag{4.102}$$

sowie für Terme, in denen die Konkretisierung nichtatomare Kernereignisse enthält, d. h.

$$X_i \wedge \ldots \wedge X_j \wedge (\ldots \vec{\wedge} (X_i \bar{\vec{\wedge}} \ldots) \vec{\wedge} \ldots) = (\ldots \vec{\wedge} X_j \wedge (X_i \bar{\vec{\wedge}} \ldots) \vec{\wedge} \ldots) \ . \tag{4.103}$$

Abstrahiert lautet das temporale Konkretisierungsgesetz somit:

$$ES_i \wedge ES_j = ES_j \qquad \text{für } ES_j \subseteq ES_i \ . \tag{4.104}$$

4.3 Minimalität und Disjunktheit in der temporalen Logik

4.3.1 Minimalität und Disjunktheit Boolescher Ausdrücke

Das folgende Kapitel behandelt zwei Eigenschaften temporaler Terme. Minimalität und Disjunktheit temporaler Terme besitzen in der temporalen Logik der TFTA einen ähnlichen Stellenwert wie in der Booleschen FTA. In beiden Fällen erlauben die Regeln der zugrundegelegten Logik, wie in Kapitel 4.2 aufgeführt, eine Überführung beliebiger Logik-Terme in eine Disjunktive Normalform (DNF) bzw. TDNF, d. h. in OR-verknüpfte Konjunktionsterme.

Im Allgemeinen enthalten diese Schnitte (Boolescher Fall) oder Ereignissequenzen (temporale Logik) jedoch noch redundante Informationen. Erst die Überführung in eine DNF aus minimalen

Konjunktionstermen, d. h. Minimalschnitte bzw. MCSS, liefert eine für die reale Anwendung sinnvolle Darstellung.

Für quantitative Berechnungen bietet es sich darüber hinaus an, diese minimale Form der (temporalen) Ausfallfunktion in eine Minterm-Darstellung umzuformen, in der die einzelnen Minterme zueinander disjunkt sind, vgl. Kapitel 4.3.3.

Disjunktive Normalform

Boolesche Terme φ lassen sich mit Hilfe der Regeln der Booleschen Algebra in eine DNF überführen:

$$\varphi = \bigvee_{j=1}^{\zeta} S_j = \bigvee_{j=1}^{\zeta} \Big(\bigwedge_{i=1}^{n_j} X_{j,i} \Big) \; . \tag{4.105}$$

Dabei steht ζ für die Anzahl der – nicht zwangsläufig schon minimalen – *Schnitte* S von φ und n_j für die Anzahl der Ereignisse X des Schnitts S_j.

Minimale DNF

Die Schnitte S eines Booleschen Terms φ sind minimal, wenn keiner der Schnitte einen der anderen Schnitte „enthält“. Zur Unterscheidung werden diese als *Minimalschnitte* und mit *MS* bezeichnet. Mit Hilfe der Regeln der Booleschen Algebra – vgl. Kapitel 4.2.1 – lassen sich (monotone) Boolesche Ausdrücke nach (4.105) immer in eine minimale Form bringen, in der

$$\varphi = \bigvee_{j=1}^{\xi} MS_j = \bigvee_{j=1}^{\xi} \Big(\bigwedge_{i=1}^{n_j} X_{j,i} \Big) \; . \tag{4.106}$$

Dabei gilt $\xi \leq \zeta$. Für alle der insgesamt ξ Minimalschnitte MS_j und $MS_{j'}$ mit $j, j' \in \{1, 2, \ldots, \xi\}$ und $j' \neq j$ gilt paarweise, dass

$$MS_j \wedge MS_{j'} \neq MS_j \qquad \text{und} \qquad MS_j \wedge MS_{j'} \neq MS_{j'} \; . \tag{4.107}$$

Disjunkte Ausdrücke für einfachere Quantifizierung

Oftmals ist es hilfreich, die Logikfunktion nach den Regeln der zugrundegelegten (Booleschen) Logik in eine für die jeweilige Aufgabenstellung besonders geeignete äquivalente Form zu überführen. Im Falle des herkömmlichen Fehlerbaums ist z. B. die Minimalschnitt-Form der Ausfallfunktion des Systems nach (4.106) besonders anschaulich und eignet sich für qualitative Analysen, während z. B. die logisch äquivalente aber weniger intuitive Form

$$\varphi = \bigvee_{j=1}^{\xi} \Big(MS_j \cdot \bigwedge_{i=1}^{j-1} \neg \left(MS_i \right) \Big) \; , \tag{4.108}$$

in der die einzelnen disjunktiv (OR) verknüpften Terme zueinander disjunkt sind, quantitative Analysen erheblich erleichtert, vgl. Kapitel 5.

Zwei Boolesche Ausdrücke φ_1 und φ_2 sind genau dann disjunkt, wenn ihre Konjunktion (AND Verknüpfung) *False* ergibt:

$$\varphi_1 \wedge \varphi_2 = \mathit{False} \qquad \Longleftrightarrow \qquad \varphi_1 \perp \varphi_2 \; . \tag{4.109}$$

4.3.2 Minimalität temporaler Terme

Die Minimalität temporal-logischer Ausdrücke lässt sich analog zum Booleschen Fall betrachten. Temporal-logische Ausdrücke sind dann minimal, wenn sie sich „nicht gegenseitig enthalten". Auf Grund der im Vergleich zur Booleschen Logik anderen Operatoren, der besonderen Bedeutung negierter Ereignisse und der fehlenden Kommutativität und Assoziativität sind dabei Besonderheiten zu beachten. Insbesondere existieren in temporalen Ausdrücken zwei Ursachen für Nicht-Minimalität: die *strukturelle Nicht-Minimalität*, vgl. Kapitel 4.3.2.1, und die *zeitliche Nicht-Minimalität*, vgl. Kapitel 4.3.2.2. Zunächst jedoch einige allgemeine Punkte.

Notation der minimalen temporalen Ausfallfunktion

Temporale Terme ϖ lassen sich mit Hilfe der Regeln der Temporalen Logik in eine der Booleschen DNF ähnliche TDNF überführen. Der Übersichtlichkeit halber sei (4.16) hier wiederholt:

$$\varpi \;=\; \bigvee_{j=1}^{\zeta} ES_j \;=\; ES_1 \vee ES_2 \vee \ldots \vee ES_\zeta \;. \tag{4.110}$$

Dabei steht ζ für die Anzahl der – nicht zwangsläufig schon minimalen – Ereignissequenzen ES von ϖ.

Die entsprechende minimale Form besteht aus ξ disjunktiv verbundenen *minimalen Ereignissequenzen* (MCSS, minimal Cutset Sequences):

$$\varpi \;=\; \bigvee_{j=1}^{\xi} MCSS_j \;=\; MCSS_1 \vee MCSS_2 \vee \ldots \vee MCSS_\xi \;. \tag{4.111}$$

Wiederum gilt $\xi \leq \zeta$.

Minimalitäts-Bedingung

Auch im temporalen Fall zeichnet sich Minimalität dadurch aus, dass keine der $MCSS_j$ eine der anderen $MCSS_{j'}$ (mit $j, j' \in \{1, 2, \ldots, \xi\}$ und $j' \neq j$) enthält. Die folgenden Abschnitte zeigen, dass im temporalen Fall ein zu (4.107) ähnliches Kriterium für Minimalität existiert.

Ereignissequenzen sind minimal, wenn paarweise für alle $MCSS_j$ und $MCSS_{j'}$ mit $j, j' \in \{1, 2, \ldots, \xi\}$ und $j' \neq j$ gilt, dass

$$MCSS_{j'} \not\subseteq MCSS_j \quad \Longleftrightarrow \quad MCSS_j \wedge MCSS_{j'} \neq MCSS_{j'} \qquad \text{und} \tag{4.112}$$

$$MCSS_j \not\subseteq MCSS_{j'} \quad \Longleftrightarrow \quad MCSS_j \wedge MCSS_{j'} \neq MCSS_j \;. \tag{4.113}$$

Dies wird im Folgenden durch einen eigenen Operator ausgedrückt:

$$MCSS_j \not\supseteq MCSS_{j'} \tag{4.114}$$

bedeutet, dass $MCSS_j$ und $MCSS_{j'}$ minimal sind.

Im Gegensatz zum Booleschen Fall lassen sich auf Grund der temporalen Distributivgesetze aus Kapitel 4.2.10 temporale Terme im Allgemeinen nur unter Inanspruchnahme auch negierter Ereignisse in einer TDNF darstellen. Dies erfordert eine Diskussion zur Minimalität temporaler Terme mit negierten Ereignissen.

4.3.2.1 Strukturelle Nicht-Minimalität temporaler Terme

Strukturelle Nicht-Minimalität zwischen temporalen Termen liegt vor, wenn einer der Terme eine „Konkretisierung" eines der anderen Terme darstellt. Die strukturelle Nicht-Minimalität temporaler Terme wird durch Anwendung der temporalen Absorptionsgesetze aus Kapitel 4.2.11 und der temporalen Konkretisierungsgesetze aus Kapitel 4.2.12 aufgelöst.

4.3.2.2 Zeitliche Nicht-Minimalität temporaler Terme

Über die strukturelle Nicht-Minimalität hinaus stellt sich die Frage der Minimalität insbesondere bei Termen wie

$$(\neg B \wedge A) \vee (A \,\vec{\wedge}\, B) \; . \tag{4.115}$$

Diese beiden Terme sind nicht minimal, wie die folgende Prüfung auf Minimalität nach (4.113) zeigt. Ausgehend von

$$(\neg B \wedge A) \wedge (A \,\vec{\wedge}\, B) \tag{4.116}$$

ergibt sich mit (4.53) zunächst

$$\begin{aligned}(\neg B \wedge A) \wedge (A \,\vec{\wedge}\, B) \; &= \\ &= \left[\neg B \wedge (A \wedge (A \,\vec{\wedge}\, B))\right] \vee \left[(A \,\vec{\wedge}\, B) \,\vec{\wedge}\, (A \,\vec{\wedge}\, B)\right] \vee \left[A \,\vec{\wedge}\, (B \,\overline{\vec{\wedge}}\, (A \,\vec{\wedge}\, B))\right] \; .\end{aligned} \tag{4.117}$$

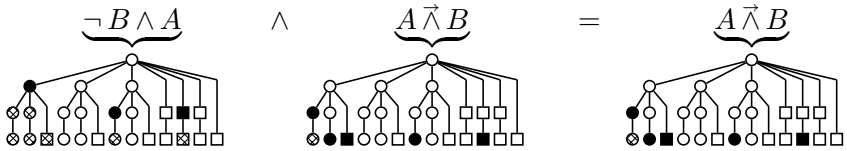
Der erste Teilterm der rechten Seite vereinfacht sich wegen (4.51) zu

$$\neg B \wedge (A \wedge (A \,\vec{\wedge}\, B)) \; = \; \neg B \wedge (A \,\vec{\wedge}\, B) \; = \; \mathit{False} \; . \tag{4.118}$$

Der zweite Teilterm der rechten Seite ergibt wegen des Widerspruchsgesetzes ebenfalls *False*, vgl. (4.38).

Offensichtlich ist mit dem verbleibenden

$$(\neg B \wedge A) \wedge (A \,\vec{\wedge}\, B) \; = \; A \,\vec{\wedge}\, (B \,\overline{\vec{\wedge}}\, (A \,\vec{\wedge}\, B)) \; = \; A \,\vec{\wedge}\, (A \,\vec{\wedge}\, B) \; = \; A \,\vec{\wedge}\, B \tag{4.119}$$



die Minimalitäts-Bedingung aus (4.113) nicht erfüllt, sodass (4.115) nicht minimal ist. Die entsprechenden sequentiellen Ausfallbäume zeigen, dass $A \,\vec{\wedge}\, B$ ausschließlich aus für $\neg B \,\vec{\wedge}\, A$ nicht-minimalen Ausfallknoten besteht. Die minimale Form lautet somit $\neg B \,\vec{\wedge}\, A$ und „enthält" den zweiten Term $A \,\vec{\wedge}\, B$.

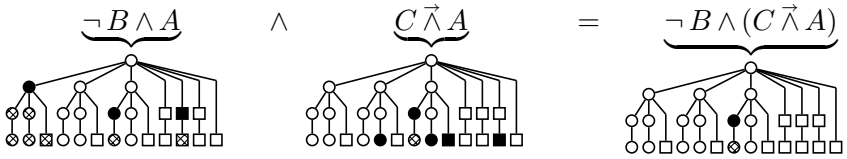
Verallgemeinerung

Dieses Beispiel lässt sich mit Blick auf die in Kapitel 4.2.8.3 aufgeführten Regeln zum Umgang mit negierten Ereignissen verallgemeinern. Insbesondere leitet sich aus (4.59) ab, dass $\neg X \wedge ES$ mit $X \notin ES$ zeitlich minimal ist zu allen temporalen Termen, in denen ES vor X eintritt, also $ES \,\vec{\wedge}\, X$.

Da somit $(\neg X \wedge ES) \vee (ES \,\vec{\wedge}\, X)$ mit $X \notin ES$ auf Grund des zeitlichen Ablaufs nicht minimal ist, wird dieser Effekt als *zeitliche Nicht-Minimalität* bezeichnet.

Zwei weitere Beispiele

$(\neg B \wedge A) \vee (C \vec{\wedge} A)$ ist eine bereits minimale Form, da wiederum mit (4.53) gilt, dass



(4.120)

sodass (4.113) erfüllt ist. In der graphischen Darstellung besitzt jeder der beiden Terme Ausfallknoten, die nicht im anderen Term enthalten sind:

Hingegen ist $\neg B \wedge A$ die Minimalform aller Sequenzen, in denen zwar A aber nicht $B \vec{\wedge} A$ enthalten ist (hier ohne SANDs), d. h. $\neg B \wedge (A \vec{\wedge} C)$, $\neg C \wedge (A \vec{\wedge} B)$, $A \vec{\wedge} B \vec{\wedge} C$, $A \vec{\wedge} C \vec{\wedge} B$ und $C \vec{\wedge} A \vec{\wedge} B$. Exemplarisch sei dies hier nur an einer dieser Kombinationen gezeigt:

$$\begin{aligned}(\neg B \wedge A) \wedge (A \vec{\wedge} C \vec{\wedge} B) = \quad & \big[\neg B(\wedge A \wedge (A \vec{\wedge} C \vec{\wedge} B))\big] \vee \\ & \vee \big[A \vec{\wedge} B \vec{\wedge} ((A \vec{\wedge} C \vec{\wedge} B) \vec{\wedge} A)\big] \vee \\ & \vee \big[A \vec{\wedge} (B \,\overline{\vec{\wedge}}\, (A \vec{\wedge} C \vec{\wedge} B))\big] = \\ = \quad & \mathit{False} \vee \mathit{False} \vee A \vec{\wedge} (A \vec{\wedge} C \vec{\wedge} B) = A \vec{\wedge} C \vec{\wedge} B \,.\end{aligned} \tag{4.121}$$

$(\neg B \vec{\wedge} A) \vee (A \vec{\wedge} C \vec{\wedge} B)$ ist somit nichtminimal, da (4.113) nicht erfüllt ist, vgl. auch obige sequentielle Ausfallbäume zur Veranschaulichung.

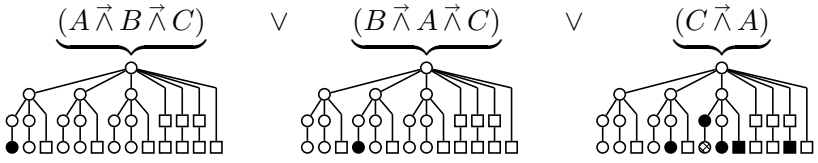
4.3.3 Disjunktheit temporaler Terme

Minimale temporale Terme sind nicht zwangsläufig auch immer disjunkt. Z. B. liegt die Ausfallfunktion $\varpi = (\neg B \wedge A) \vee (C \vec{\wedge} A)$ in minimaler Form vor. Ihre beiden Ereignissequenzen $\neg B \wedge A$ und $C \vec{\wedge} A$ sind jedoch nicht disjunkt, sondern besitzen die Schnittmenge $\neg B \wedge (C \vec{\wedge} A)$, vgl. (4.120).

Die folgenden Kapitel diskutieren Besonderheiten der Disjunktheit temporaler Terme und ein Verfahren der Erzeugung disjunkter temporaler Terme.

4.3.3.1 Disjunktheits-Bedingung

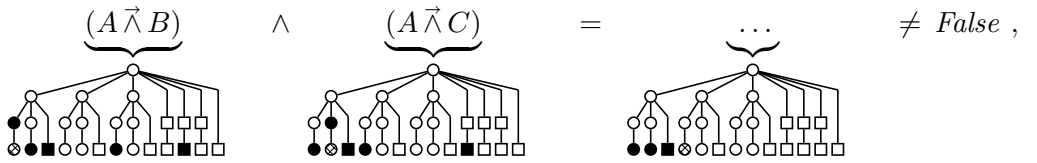
Analog zu den Überlegungen in Kapitel 4.3.1 zeigt sich Disjunktheit zwischen zwei temporalen Termen, wenn deren Konjunktion (AND Verknüpfung) *False* ergibt, wenn also keine Schnittmengen zwischen zwei temporalen Termen bestehen. In der graphischen Darstellung mittels sequentieller Ausfallbäume besitzen disjunkte temporale Terme somit keine gemeinsamen Ausfallknoten. Dies ist z. B. in folgendem Ausdruck der Fall, dessen drei Teilterme disjunkt sind:



Dabei sind

$$\begin{aligned}(A \vec{\wedge} B \vec{\wedge} C) \wedge (B \vec{\wedge} A \vec{\wedge} C) &= \mathit{False}\,, \\ (A \vec{\wedge} B \vec{\wedge} C) \wedge (C \vec{\wedge} A) &= \mathit{False}\,, \\ (B \vec{\wedge} A \vec{\wedge} C) \wedge (C \vec{\wedge} A) &= \mathit{False}\,.\end{aligned}$$

In folgendem Beispiel existieren jedoch Überschneidungen:



da

$$(A \vec{\wedge} B) \wedge (A \vec{\wedge} C) = \left[(A \vec{\wedge} B) \vec{\wedge} (A \vec{\wedge} C)\right] \vee \left[(A \vec{\wedge} B) \bar{\vec{\wedge}} (A \vec{\wedge} C)\right] \vee \left[(A \vec{\wedge} C) \vec{\wedge} (A \vec{\wedge} B)\right] = \\ = \left[A \vec{\wedge} B \vec{\wedge} C\right] \vee \left[A \vec{\wedge} (B \bar{\vec{\wedge}} C)\right] \vee \left[A \vec{\wedge} C \vec{\wedge} B\right] .$$

4.3.3.2 Strukturelle und zeitliche Disjunktheit temporaler Terme

In der temporalen Logik der TFTA existieren zwei Arten von Disjunktheit:

1. Dasselbe Ereignis kann nicht zugleich eingetreten und nicht eingetreten sein. Analog zur Booleschen Logik sind daher zwei temporale Terme dann disjunkt, wenn der eine Term ein nichtnegiertes Ereignis und der andere Term die Negation desselben Ereignisses enthält. So sind z. B. $\neg A \wedge B$ und $A \vec{\wedge} B$ disjunkt. Allgemein drückt sich diese Art von Disjunktheit in (4.51) und (4.52) aus.

2. Anders als in der Booleschen Logik existiert wegen der Möglichkeit temporaler Widersprüche in temporalen Termen eine zweite Art disjunkter Terme. Aus den temporalen Vervollständigungs- und Widerspruchsgesetzen (vgl. Kapitel 4.2.2 und 4.2.3) leitet sich ab, dass zwei Terme dann disjunkt sind, wenn sie dieselben Ereignisse in verschiedenen Reihenfolgen enthalten. So sind z. B. $B \vec{\wedge} A$ und $A \vec{\wedge} B$ auch ohne negierte Ereignisse disjunkt.

In beiden Fällen zeigt sich die Disjunktheit durch das Fehlen von Schnittmengen. Sie lässt sich daher immer mit der in Kapitel 4.3.3.1 genannten Disjunktheits-Bedingung prüfen. Damit unterscheidet sich die Disjunktheit temporaler Terme auch nicht wesentlich von der Disjunktheit Boolescher Terme, für welche dieselbe Disjunktheits-Bedingung existiert, vgl. (4.109).

4.3.3.3 Disjunkte Zerlegung mit temporalen Mintermen

Temporale Minterme sind Ereignissequenzen, in denen alle u Variablen der betrachteten u-stelligen temporalen Logikfunktion genau einmal enthalten sind.

Temporale Minterme werden genutzt, um einen temporalen Ausdruck in disjunkte Ereignissequenzen zu zerlegen. Diese eignen sich besonders für eine anschließende Quantifizierung, analog zu den Überlegungen in Kapitel 4.3.1.

Sie lassen sich durch ein Verfahren ähnlich dem Shannonschen Zerlegungsverfahren für die Boolesche Algebra ermitteln:

1. Die betrachtete Funktion ϖ mit u Variablen muss als TDNF vorliegen. Andernfalls ist ϖ mit Hilfe der Regeln der temporalen Logik zunächst in eine TDNF zu überführen.

2. Es wird der erste der disjunktiv verbundenen Teilterme (die erste Sequenz) $ES = ES_1$ gewählt.

3. Falls ES alle u Variablen enthält: weiter zu Schritt sieben.

4. Wähle die erste in ES fehlende Variable X.

5. ES wird gemäß

$$ES \implies ES \wedge (\neg X \vee X) = (\neg X \wedge ES) \vee (X \wedge ES) \tag{4.122}$$

in eine disjunkte Form überführt.

6. Für alle weiteren in ES fehlenden Variablen X wird Schritt fünf wiederholt.

7. Falls die aktuelle ES nicht die Letzte in ϖ ist, wird die nächste Ereignissequenz ES gewählt; weiter zu Schritt drei.

8. Mit den Regeln der temporalen Logik, insbesondere mit den temporalen Absorptionsgesetzen, lässt sich die Minimalität der resultierenden Teilterme / Sequenzen prüfen.

Dieses Verfahren ist im Anhang A.3 ab Seite 128 beispielhaft an zwei Ausfallfunktionen demonstriert.

4.4 Vereinfachung durch erweiterte Ereignissequenzen, erweiterte TDNF, erweiterte MCSS

Die bisherigen Ausführungen bezogen sich auf „normale“ temporale Terme nach den Definitionen in Kapitel 4.1.5.1. Die in Kapitel 4.2 und 4.3 eingeführte temporale Logik ermöglicht die Überführung temporaler Terme ϖ in eine – ggf. minimale und disjunkte – TDNF. Diese gibt alle zum Eintreten des TOP führenden Ereignissequenzen an und eignet sich daher sowohl für weitergehende qualitative Analysen als auch als Ausgangsbasis für eine Quantifizierung.

4.4.1 Motivation und Anforderungen

Obwohl damit die beiden in Kapitel 3.2 aufgeführten Ziele erreicht werden, ist der praktische Nutzen dieser Logik mitunter durch die hohe Anzahl resultierender Ergebnissequenzen eingeschränkt. So ergeben sich z. B. aus dem vergleichsweise einfachen Term $A \vec{\wedge} (B \wedge C) \vec{\wedge} (D \wedge E)$ auch ohne SANDs bereits 32 temporale Minterme, vgl. Kapitel 5.5.2. Zu dieser Aufblähung der Anzahl der Ereignissequenzen trägt vor allem das Vervollständigungsgesetz aus Kapitel 4.2.2 bei.

Zwar sind die Umformungen gemäß der temporalen Logik grundsätzlich notwendig, um komplexe Terme in überschaubare und handhabbare Teile zu überführen. Jedoch spielt für die Klarheit und Interpretierbarkeit der Ergebnisse auch die Anzahl solcher Teile eine wesentliche Rolle.

In diesem Spannungsfeld ist es sinnvoll, die Vereinfachung eines komplexen temporalen Terms nur so weit voranzutreiben, dass praktisch nutzbare, insbesondere minimale, Informationseinheiten geschaffen werden, und zugleich die Anzahl dieser Einheiten so gering wie möglich ist.

An eine solche vereinfachte Form temporaler Terme stellen sich folgende Anforderungen:

1. Auch in der vereinfachten Form müssen sowohl qualitative als auch quantitative Analysen möglich sein.

2. Auch in der vereinfachten Form muss der temporale Term in einer disjunktiven Normalform vorliegen.

3. Die einzelnen Ereignissequenzen dieser Normalform müssen minimal sein.

4. Die einzelnen Ereignissequenzen dieser Normalform müssen direkt quantifizierbar sein.

5. Für diese Quantifizierung sollten die einzelnen Ereignissequenzen dieser Normalform disjunkt sein.

Die in Kapitel 4.1.5.2 definierte erweiterte TDNF ist eine Möglichkeit, diese Anforderungen zu erfüllen.

In der erweiterten Form enthalten temporale Terme neben normalen atomaren und nichtatomaren Kernereignissen auch *erweiterte Kernereignisse* der Art

$$eK = X_1 \wedge X_2 \wedge \ldots \quad . \tag{4.123}$$

Ereignissequenzen mit erweiterten Kernereignissen heißen *erweiterte Ereignissequenzen*, vgl. die Grammatik der temporalen Logik in Kapitel 4.1.5.

Die Verwendung dieser Form ist immer dann sinnvoll, wenn alle Sequenzen mehrerer Ereignisse gleichermaßen für das TOP relevant sind. Die erweiterte Form fasst mehrere „echte“ Sequenzen zusammen und dient somit der Aufwandsreduzierung und prägnanteren Ergebnisdarstellung.

Ohne die erweiterte Form dienen die Umformungen temporaler Terme dazu, eine TDNF zu erzeugen, in der ausschließlich Ereignissequenzen verbleiben, die ihrerseits aus Kernereignissen bestehen. Jedes Kernereignis gibt an, dass Ereignisse zu bestimmten (relativen) Eintretenszeitpunkten eintreten. Ein Term $A \vec{\wedge} (B \overline{\vec{\wedge}} C)$ zeigt z. B. an, dass ein atomares Kernereignis A zu einem Zeitpunkt eintritt, der vor dem Eintretenszeitpunkt der zu einem späteren Zeitpunkt gleichzeitig eintretenden Ereignisse B und C liegt. Die Eintrittszeitpunkte aller Ereignisse werden somit durch die Ereignissequenz eindeutig beschrieben.

Mit der erweiterten Form dienen die Umformungen temporaler Terme dazu, eine erweiterte TDNF zu erzeugen. Diese enthält normale Ereignissequenzen, die aus normalen Kernereignissen bestehen, und erweiterten Ereignissequenzen, die aus normalen und erweiterten Kernereignissen bestehen.

Die erweiterten Kernereignisse geben an, dass zu einem bestimmten Zeitpunkt bestimmte Ereignisse *eingetreten sind*. Ein Term $A \vec{\wedge} (B \wedge C)$ zeigt z. B. an, dass ein atomares Kernereignis A zu einem Zeitpunkt eintritt, bevor sowohl B als auch C eingetreten sind. Die tatsächlichen Eintretenszeitpunkte der an einem erweiterten Kernereignis beteiligten Ereignisse sind durch die erweiterte Ereignissequenz somit nicht eindeutig definiert, es wird lediglich ein „letztmöglicher“ Eintretenszeitpunkt angegeben.

Erweiterte Ereignissequenzen können mehrere erweiterte Kernereignisse enthalten, z. B. in $(A \wedge B) \vec{\wedge} (C \wedge D)$. Sind Ereignisse in derselben erweiterten Ereignissequenz mehrfach enthalten, so ist diese weiter zu vereinfachen.

Andererseits widerspricht es der erweiterten TDNF, mehrere (erweiterte) Ereignissequenzen mit einem AND zu verbinden. Stattdessen sind weitere Umformungen vorzunehmen. Beispielsweise ergibt erst die Vereinfachung von $(A \vec{\wedge} B) \wedge C$ gemäß der Regeln der temporalen Logik in

$$(A \vec{\wedge} B) \wedge C = \left[C \vec{\wedge} (A \wedge B)\right] \vee \left[A \vec{\wedge} (B \overline{\vec{\wedge}} C)\right] \vee \left[A \vec{\wedge} B \vec{\wedge} C\right] \tag{4.124}$$

eine korrekte erweiterte TDNF.

4.4.2 Verwendung der erweiterten Form temporaler Terme

Die Entscheidung, ob die erweiterte Form verwendet wird, fällt bei der qualitativen Umformung der temporalen Ausfallfunktion während der qualitativen Analysen:

- Zum einen wird das Boolesche Distributivgesetz vorrangig eingesetzt bevor das temporale Vervollständigungsgesetz zur Anwendung kommt.
- Zum anderen werden AND Verknüpfungen nicht aufgelöst, wenn die AND verbundenen Ereignisse
  - selbst Ereignissequenzen ohne negierte Ereignisse sind und
  - sowohl zueinander als auch zum Rest der aktuellen (erweiterten) Ereignissequenz „teilerfremd“ sind, also keine Vermaschungen über selbe Ereignisse bestehen.

Grundsätzlich gelten die temporalen Logikregeln aus Kapitel 4.2 und Kapitel 4.3 auch für erweiterte Kernereignisse und erweiterte Ereignissequenzen. Erweiterte Kernereignisse werden dabei analog zu normalen nichtatomaren Kernereignissen, also $X_1 \,\overline{\vec{\wedge}}\, X_2 \,\overline{\vec{\wedge}}\, \ldots$, als feste Einheiten behandelt.

Zusätzlich existieren weitere Regeln speziell für den Umgang mit der erweiterten Form. Diese Regeln sind in den folgenden Abschnitten beschrieben.

Widerspruchsgesetz für erweiterte Ereignissequenzen

Das Widerspruchsgesetz für normale temporale Terme aus Kapitel 4.2.3 gilt nicht einfach auch für erweiterte Ereignissequenzen. So besteht zwar der Ausdruck $(A \wedge B) \,\vec{\wedge}\, (B \wedge C)$ aus zwei erweiterten Kernereignissen, die dasselbe Basisereignis B enthalten. Allerdings ergibt dieser Ausdruck offensichtlich nicht *False*, sondern ist mit (4.48) weiter zu vereinfachen zu

$$(A \wedge B) \,\vec{\wedge}\, (B \wedge C) \;=\; (A \wedge B \wedge B) \,\vec{\wedge}\, C \;=\; (A \wedge B) \,\vec{\wedge}\, C \;. \tag{4.125}$$

Allerdings können auch erweiterte Ereignissequenzen Widersprüche enthalten. Dabei sind die folgenden drei Fälle zu unterscheiden, die zusammen das *Widerspruchsgesetz für erweiterte Ereignissequenzen* ergeben:

Erstens gilt analog zu (4.39) für erweiterte Ereignissequenzen mit normalen und erweiterten Kernereignissen eK, dass

$$eK_1 \,\vec{\wedge}\, eK_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, eK_n \;=\; \mathit{False} \;, \tag{4.126}$$

wenn $\exists\; eK_i = eK_j$ für $i, j \in \{1, 2, \ldots, n\}$ und $i \neq j$. Dies zeigt sich durch Auflösung der erweiterten Form mittels (4.37) und (4.77). So ergibt z. B.

$$\begin{aligned}(A \wedge B) \,\vec{\wedge}\, (A \wedge B) \;&=\; (A \wedge B) \,\vec{\wedge}\, \left[(A \,\vec{\wedge}\, B) \vee (B \,\vec{\wedge}\, A) \vee (A \,\overline{\vec{\wedge}}\, B)\right] \;= \\ &=\; \left[(A \wedge B \wedge A) \,\vec{\wedge}\, B\right] \vee \left[(A \wedge B \wedge B) \,\vec{\wedge}\, A\right] \vee \left[(A \wedge B) \,\vec{\wedge}\, (A \,\overline{\vec{\wedge}}\, B)\right] \;= \\ &=\; \mathit{False} \;.\end{aligned} \tag{4.127}$$

Zweitens ergibt eine erweiterte Ereignissequenz durch Widerspruch *False*, wenn sie ein erweitertes Kernereignis eK und ein in der Sequenz *später eintretendes* normales Kernereignis K besitzt und es mindestens ein X gibt, welches sowohl in K als auch in eK enthalten ist:

$$eK_1 \,\vec{\wedge}\, eK_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, K_j \,\vec{\wedge}\, \ldots \;=\; \mathit{False} \;, \tag{4.128}$$

wenn $\exists\ (X \Subset eK_i) \wedge (X \Subset K_j)$ für $i < j$. Dabei kann K sowohl ein atomares als auch ein nichtatomares Kernereignis sein. So führt der Term $(A \wedge B) \vec{\wedge} B$ zu einem Widerspruch, da er fordert, dass sowohl A als auch B bereits eingetreten sind, bevor B eintritt. Auch der Term $(A \wedge B) \vec{\wedge} (A \overline{\vec{\wedge}} C)$ liefert einen Widerspruch, da er fordert, dass sowohl A als auch B bereits eingetreten sind, bevor A gleichzeitig mit C eintreten. In beiden Fällen tritt kein Widerspruch auf, wenn das normale Kernereignis in der Sequenz *vor* dem erweiterten Kernereignis steht: So ergeben $A \vec{\wedge} (A \wedge B) = A \vec{\wedge} B$ und $(A \overline{\vec{\wedge}} C) \vec{\wedge} (A \wedge B) = (A \overline{\vec{\wedge}} C) \vec{\wedge} B$.

Drittens ergibt eine erweiterte Ereignissequenz durch Widerspruch *False*, wenn sie mehrere normale Kernereignisse enthält, für die das normale Widerspruchsgesetz in (4.42) greift.

Umgang mit negierten Ereignissen für erweiterte Ereignissequenzen / Kernereignisse

Auch im Umgang mit negierten Ereignissen gelten grundsätzlich die bereits aus Kapitel 4.2.8 bekannten Regeln und Überlegungen. Zusätzlich sind für erweiterte Ereignissequenzen / Kernereignisse einige Besonderheiten zu berücksichtigen.

Die Negation erweiterter Ereignissequenzen erfolgt analog zu (4.65), wobei erweiterte Kernereignisse zunächst als Einheiten behandelt werden.

Die Negation erweiterter Kernereignisse erfolgt mit Hilfe der De Morganschen Theoreme:

$$\neg\, eK = \neg\big(X_1 \wedge X_2 \wedge \ldots\big) = \neg X_1 \vee \neg X_2 \vee \ldots \quad . \tag{4.129}$$

Als negierte Ereignisse sind Negationen erweiterter Kernereignisse eingebunden in (erweiterte) Ereignissequenzen mit negierten Ereignissen, vgl. Diskussion in Kapitel 4.2.8.

In Erweiterung zu (4.51) und (4.52) gilt zudem

$$\neg A \wedge (\ldots \vec{\wedge} (A \wedge \ldots) \vec{\wedge} \ldots) = \mathit{False}\ . \tag{4.130}$$

Sonstige Erweiterungen für erweiterte Ereignissequenzen / Kernereignisse

Das Konkretisierungsgesetz für erweiterte Ereignissequenzen / Kernereignisse lautet

$$A \vec{\wedge} (A \wedge B \wedge \ldots) = A \vec{\wedge} B \wedge \ldots \quad . \tag{4.131}$$

Die Korrektheit lässt sich durch Auflösen des erweiterten Kernereignisses leicht nachweisen.

4.5 Zusammenfassung

Die in diesem Kapitel beschriebene neue temporale Logik der TFTA erweitert die herkömmliche FTA für nicht reparierbare Komponenten(-Ausfälle) um die Möglichkeit, Ereignissequenzen abzubilden.

Die TFTA ist eine Erweiterung der Booleschen Algebra und Logik und verzichtet auf zustandsbasierte Modellierungen. Neben den Booleschen Operationen der Konjunktion, Disjunktion, Negation unterscheidet die TFTA darüber hinaus mit den zwei neuen temporalen Operationen PAND und SAND zwei Arten von „spezialisierten Konjunktionstermen“, die Reihenfolgen bzw. Gleichzeitigkeit von Ereignissen beschreiben.

Mit Hilfe der bekannten Booleschen Algebra und eines Satzes an temporalen Logikregeln ist es möglich, komplexe temporale Terme in eine temporale disjunktive Normalform (TDNF) zu überführen, die aus einzelnen Ereignissequenzen besteht. Analog zu den Booleschen Schnitten eines Fehlerbaums lassen sich diese Ereignissequenzen auf eine minimale Form, die sogenannten MCSS reduzieren. Die TFTA erlaubt somit analog zur herkömmlichen FTA aussagekräftige und effiziente qualitative Analysen.

Als Erweiterung der Booleschen Algebra ist die temporale Logik der TFTA allgemeingültig und nicht nur auf einzelne Verteilungsformen der Ausfallgrößen beschränkt.

In einem weiteren Verfahrensschritt lassen sich die MCSS in eine disjunkte Form überführen. Diese eignet sich besonders für die im folgenden Kapitel 5 diskutierte direkte Quantifizierung und ermöglicht somit auch probabilistische Analysen temporaler Terme.

Die TFTA orientiert sich in Notation, Begriffen und auch in Prozessschritten und Arbeitsprodukten an der herkömmlichen FTA. Im Vergleich zu zustandsbasierten dynamische Modellierungen besitzt die TFTA somit auch ähnliche positive Eigenschaften wie z. B. intuitive Nutzbarkeit, Lesbarkeit und Verständlichkeit der Logik-Ausdrücke und Ergebnisse sowie Skalierbarkeit.

Die Vereinfachung temporaler Terme hin zu einer – ggf. disjunkten – minimalen Form erfordert prinzipbedingt einen relativ großen Aufwand und bedeutet gegenüber der Booleschen FTA einen Mehraufwand. Dies ist jedoch kein spezifisches Problem der TFTA sondern trifft auf alle dynamischen Modellierungen in ähnlicher Form zu. Die TFTA bietet jedoch mit der erweiterten Form eine Möglichkeit zur effektiven Reduzierung des Aufwandes. Wenn sich mehrere Sequenzen zu einer normalen, d. h. Booleschen, Konjunktion zusammenfassen lassen, werden diese in der erweiterten Form nicht explizit aufgeschlüsselt. Dadurch lässt sich der exponentielle Anstieg des Berechnungsaufwandes eindämmen.

5 Quantifizierung des TFTA Ansatzes

Probable impossibilities are to be
preferred to improbable possibilities.

(Aristoteles)

Die quantitative TFTA erweitert die rein qualitative Analyse. Die Zuweisung von Ausfalldaten, z. B. Ausfallraten und -wahrscheinlichkeiten, zu den Basisereignissen erlaubt die Berechnung der Kenngrößen des TOP. Mit diesen erfolgt die Beurteilung der Sicherheitsintegrität bzw. der zu erwartenden Zuverlässigkeit des Systems.

Dem zusätzlichen Aufwand für eine quantitative Berechnung der TOP-Kenngrößen unter Berücksichtigung von Ereignisreihenfolgen stehen die im Vergleich zur rein Booleschen Modellierung kleineren Ergebnisse gegenüber.

Das Kapitel gliedert sich in folgende Abschnitte:

- Einleitend sind in Kapitel 5.1 der Vollständigkeit halber die grundlegenden Aspekte der Booleschen quantitativen FTA aufgeführt.
- Kapitel 5.2 beschreibt das der TFTA-Logik zugrundegelegte Quantifizierungskonzept auf Basis der Ausfalldichten.
- Konkrete Vorgaben zur Quantifizierung der temporalen PAND und SAND Operationen sind in Kapitel 5.3 aufgeführt.
- Diese dienen in Kapitel 5.4 der Quantifizierung ganzer temporaler Ausfallfunktionen, also der Berechnung der TOP Ausfallwahrscheinlichkeiten und Ausfalldichten bzw. Ausfallraten.
- Auf Grund des ggf. exponentiell ansteigenden Berechnungsaufwandes diskutiert Kapitel 5.5 ein weniger aufwändiges Verfahren zur Berechnung genäherter Kenngrößen zu temporalen Logik-Termen.

Anmerkung: Die im vorangegangenen Kapitel 4 diskutierten qualitativen Aspekte der TFTA sind allgemein gültig für nicht reparierbare Komponenten. Dasselbe gilt für das allgemeine Konzept einer Quantifizierung, wie in den folgenden Kapiteln bis 5.3.1 vorgestellt. Die Ausführungen ab Kapitel 5.3.2 konzentrieren sich dann auf den Spezialfall exponentialverteilter Ausfallgrößen.

5.1 Quantifizierung der Booleschen FTA

In der Booleschen wie temporalen FTA erfolgt die quantitative Analyse des TOP auf Basis der in den qualitativen Analyseschritten ermittelten System- oder TOP-Ausfallfunktion. Oftmals ist es hilfreich, diese Logikfunktion nach den Regeln der zugrundegelegten (Booleschen oder temporalen) Logik in eine für die jeweilige Aufgabenstellung besonders geeignete äquivalente Form zu überführen.

Im Falle des Booleschen Fehlerbaums ist z. B. die Minimalschnitt-Form der Ausfallfunktion des Systems aus (4.106)

$$\varphi = \bigvee_{j=1}^{\xi} MS_j = \bigvee_{j=1}^{\xi} \Big(\bigwedge_{i=1}^{n_j} X_{j,i} \Big)$$

besonders anschaulich und eignet sich für qualitative Analysen, während die logisch äquivalente aber weniger intuitive Form aus (4.108)

$$\varphi = \bigvee_{j=1}^{\xi} \Big(MS_j \cdot \bigwedge_{i=1}^{j-1} \neg \left(MS_i \right) \Big) \ ,$$

in der die einzelnen Terme (Minimalschnitte) zueinander disjunkt sind, quantitative Analysen erheblich erleichtert.

Die Quantifizierung der Minimalschnitte der herkömmlichen FTA, welche die Booleschen Operationen AND und OR und NOT enthalten, ist wohlbekannt und sei hier nur der Vollständigkeit halber aufgeführt.

Unter Annahme von jeweils n voneinander unabhängigen Ereignissen gelten

$$F_{\mathrm{AND}}(t) = \prod_{i=1}^{n} F_i(t) \ , \tag{5.1}$$

$$F_{\mathrm{OR}}(t) = 1 - \prod_{i=1}^{n} (1 - F_i(t)) \ , \tag{5.2}$$

$$f_{\mathrm{AND}}(t) = \frac{\mathrm{d}}{\mathrm{d}t} F_{\mathrm{AND}}(t) = \sum_{i=1}^{n} \left(f_i(t) \cdot \prod_{j=1; j \neq i}^{n} F_j(t) \right) \ , \tag{5.3}$$

$$f_{\mathrm{OR}}(t) = \frac{\mathrm{d}}{\mathrm{d}t} F_{\mathrm{OR}}(t) = \sum_{i=1}^{n} \left(f_i(t) \cdot \prod_{j=1; j \neq i}^{n} (1 - F_j(t)) \right) \ . \tag{5.4}$$

Komplexe oder nicht voneinander unabhängige Terme, wie Ausfallfunktionen von Fehlerbäumen, sind zweckmäßigerweise vor der Quantifizierung auf ihre Minimalschnitte zu reduzieren und diese ggf. zueinander disjunkt zu machen [80, 81] (oder für nichtmonotone Funktionen [82, 83]). Letzteres erlaubt eine vereinfachte Berechnung, da sich (5.2) und (5.4) für disjunkte Ereignisse vereinfachen zu

$$F_{\mathrm{OR}}(t) = \sum_{i=1}^{n} F_i(t) \ , \tag{5.5}$$

$$f_{\mathrm{OR}}(t) = \sum_{i=1}^{n} f_i(t) \ . \tag{5.6}$$

Da negierte Ereignisse in monotonen Fehlerbäumen mit nicht reparierbaren Ausfall-Ereignissen ausschließlich als Bedingungen verwendet werden, lässt sich für diese keine Dichtegröße angeben. Dies gilt gleichermaßen für die TFTA, vgl. die Überlegungen in Kapitel 4.2.8, nach denen negierte Ereignisse immer nur vor, nie aber nach anderen (nicht negierten) Ereignissen eintreten.

Die Eintretenswahrscheinlichkeit eines negierten Ereignisses $\neg X_i$ beträgt

$$F_{\neg X_i}(t) = 1 - F_{X_i}(t) = R_{X_i}(t) \; . \tag{5.7}$$

5.2 Quantitative TFTA: Zeitkonzept der Ausfalldichte

Im Gegensatz zur Booleschen FTA erlaubt die temporale Logik der TFTA, in Konjunktionstermen nur bestimmte Ereignisreihenfolgen zuzulassen. Eine quantitative TFTA erfordert daher die Möglichkeit auch quantitativ nur bestimmte Ereignisreihenfolgen zu berücksichtigen. Dieses Vorgehen zu erläutern ist Aufgabe des vorliegenden Kapitels. Die daraus für die konkrete Anwendung abgeleiteten Regeln zur Quantifizierung der beiden temporalen Operationen PAND und SAND werden in Kapitel 5.3 behandelt.

Allgemein bestehen zwischen der Ausfallwahrscheinlichkeit, Ausfalldichte, Ausfallrate und Zuverlässigkeit folgende Zusammenhänge [14]:

$$f_X(t) = \frac{\mathrm{d}}{\mathrm{d}t} F_X(t) \qquad \text{und} \tag{5.8}$$

$$f_X(t) = \lambda_X(t) \cdot (1 - F_X(t)) = \lambda_X(t) \cdot R_X(t) \; . \tag{5.9}$$

Im Falle konstanter Ausfallraten gilt für Ausfallwahrscheinlichkeit und Ausfalldichte, dass

$$F_X(t) = 1 - \mathrm{e}^{-\lambda_X t} \qquad \text{und} \qquad f_X(t) = \lambda_X \cdot \mathrm{e}^{-\lambda_X t} \; . \tag{5.10}$$

5.2.1 Reihenfolgen bei zwei Ereignissen

Für eine Konjunktion mit stochastisch unabhängigen Eingangs-Basisereignissen A und B gilt

$$F_{A \wedge B}(t) = F_A(t) \cdot F_B(t) \; . \tag{5.11}$$

Gleichung (5.11) gibt die Wahrscheinlichkeit an, dass zum Zeitpunkt t beide Fehlerbaum-Ereignisse A und B *True* sind. Dies ist die Wahrscheinlichkeit, dass die durch A und B repräsentierten Ausfallereignisse beide irgendwann innerhalb des Intervalls $]0;t]$ eingetreten sind. Es lassen sich aber keinerlei Aussagen machen zur Reihenfolge der Ausfälle oder dem absoluten Zeitpunkt des jeweiligen Ausfalls.

Anders als die Ausfallwahrscheinlichkeit $F(t)$ berücksichtigt die Ausfalldichte $f(t)$ hingegen die Reihenfolgen von Ereignissen, da

$$f_{A \wedge B}(t) = \frac{\mathrm{d}}{\mathrm{d}t} F_{A \wedge B}(t) = f_B(t) F_A(t) + f_A(t) F_B(t) \tag{5.12}$$

und daraus mit (5.9)

$$f_{A \wedge B}(t) = F_A(t) R_B(t) \lambda_B(t) + F_B(t) R_A(t) \lambda_A(t) \; . \tag{5.13}$$

Gleichung (5.13) lässt sich interpretieren als die Wahrscheinlichkeit pro Zeit, dass [84]

- entweder A irgendwann innerhalb des Intervalls $]0;t]$ eingetreten ist ($F_A(t)$) und B nicht innerhalb des Intervalls $]0;t]$ eingetreten ist ($R_B(t)$) und B im auf t folgenden (infinitesimal) kleinen Zeitabschnitt $]t;t+\Delta t]$ eintreten wird ($\lambda_B(t)$)
- oder B irgendwann innerhalb des Intervalls $]0;t]$ eingetreten ist ($F_B(t)$) und A nicht innerhalb des Intervalls $]0;t]$ eingetreten ist ($R_A(t)$) und A im auf t folgenden (infinitesimal) kleinen Zeitabschnitt $]t;t+\Delta t]$ eintreten wird ($\lambda_A(t)$).

Diese Möglichkeiten beschreiben die beiden Reihenfolgen „erst A, dann B“ und „erst B, dann A“, welche sich gegenseitig ausschließen, sodass sich ihre Wahrscheinlichkeiten ohne die aufwändige Berechnung von Schnittmengen addieren lassen.

Dieses Vorgehen ermöglicht die quantitative Betrachtung einzelner Ereignissequenzen. Ist z.B. nur die Ereignissequenz „erst A, dann B“ von Interesse, so ist

$$f_{\text{„erst } A\text{, dann } B\text{“}}(t) \;=\; F_A(t)\cdot\frac{\mathrm{d}}{\mathrm{d}t}F_B(t) \;=\; f_B(t)F_A(t) \;=\; \lambda_B(t)R_B(t)F_A(t)\;. \tag{5.14}$$

Die entsprechende Ausfallwahrscheinlichkeit ergibt sich durch Integration über die Dichte zu

$$F_{\text{„erst } A\text{, dann } B\text{“}}(t) \;=\; \int_0^t f_{\text{„erst } A\text{, dann } B\text{“}}(\tau)\cdot\mathrm{d}\tau \;=\; \int_0^t f_B(\tau)F_A(\tau)\cdot\mathrm{d}\tau\;. \tag{5.15}$$

5.2.2 Reihenfolgen bei mehr als zwei Ereignissen

Bei mehr als zwei Ereignissen sind auch die Reihenfolgen der nicht zuletzt eintretenden Ereignisse zu berücksichtigen. Im Falle eines AND Gatters mit drei Eingängen A, B, C ist für die Ereignissequenz „erst A, dann B, dann C“ eine einfache Ableitung von $F_{A\wedge B\wedge C}(t)$ nicht ausreichend, da

$$f_{A\wedge B\wedge C}(t) \;=\; f_A(t)F_B(t)F_C(t) + f_B(t)F_A(t)F_C(t) + f_C(t)F_A(t)F_B(t)\;. \tag{5.16}$$

Keiner der Terme der rechten Seite in (5.16) gibt die Ereignissequenz „erst A, dann B, dann C“ an. So steht z. B. $f_C(t)F_A(t)F_B(t)$ für den Dichte-Beitrag von „erst A und B, dann C“ und beschreibt somit die beiden Ereignissequenzen „erst A, dann B, dann C“ und „erst B, dann A, dann C“.

Andererseits lassen sich die Reihenfolgen der nicht zuletzt eintretenden Ereignisse A und B korrekt berücksichtigen, wenn „erst A, dann B“ als eigenes Ereignis behandelt wird. Aus

$$f_{\text{„erst } A\text{, dann } B\text{, dann } C\text{“}}(t) \;=\; f_{\text{„erst (erst } A\text{, dann } B\text{), dann } C\text{“}}(t) \;=\; f_C(t)F_{\text{„erst } A\text{, dann } B\text{“}}(t)$$

folgt mit (5.15) die Ausfalldichte

$$f_{\text{„erst } A\text{, dann } B\text{, dann } C\text{“}}(t) \;=\; f_C(t)\int_0^t f_B(\tau)F_A(\tau)\cdot\mathrm{d}\tau\;. \tag{5.17}$$

und daraus mittels Integration die Ausfallwahrscheinlichkeit

$$F_{\text{„erst } A\text{, dann } B\text{, dann } C\text{“}}(t) \;=\; \int_0^t f_C(\tau)\int_0^\tau f_B(\tau')F_A(\tau')\cdot\mathrm{d}\tau'\cdot\mathrm{d}\tau\;. \tag{5.18}$$

Dieses Vorgehen ermöglicht die Quantifizierung auch komplexerer Sequenzen mit mehr als zwei Ereignissen.

5.2.3 Zielgröße für quantitative Nachweise

Als Zielgröße quantitativer FTA zu Nachweiszwecken z. B. nach IEC 61508 oder ISO 26262 eignet sich insbesondere die Ausfallrate $\lambda(t)$ [85]. Bei bekannter Ausfallwahrscheinlichkeit $F(t)$ und Ausfalldichte $f(t)$ berechnet sich diese gemäß (5.9).

In vielen Fällen ist eine Berechnung der Ausfallrate allerdings nicht erforderlich. Insbesondere bei sichterheitstechnischen Fragestellungen mit ihren kleinen absoluten Eintretenswahrscheinlichkeiten, d. h. $F(t) \ll 1$, folgt aus (5.9)

$$f(t) \approx \lambda(t) \ . \tag{5.19}$$

Die Ausfalldichte stellt dann eine gute Näherung der Ausfallrate dar und kann direkt als Nachweisgröße verwendet werden.

5.3 Quantifizierung der PAND und SAND Operationen

Auf Basis der im vorangegangenen Kapitel 5.2 beschriebenen generischen Methode zur quantitativen Berücksichtigung von Ereignissequenzen lassen sich die temporalen Operationen der TFTA quantifizieren. Zunächst ist es jedoch hilfreich, die temporal-logische Bedeutung der PAND und SAND Operationen auch quantitativ zu erfassen, vgl. Kapitel 5.3.1. Der in Kapitel 5.3.2 anschließende Vergleich mit einer Zustandsübergangsmodellierung als Referenz zeigt die Korrektheit dieser Ergebnisse.

5.3.1 Quantifizierung mittels Logikfunktionen

Die Ausfallwahrscheinlichkeit ist definiert als Erwartungswert des Eintretens eines Ausfalls [14]:

$$F_i(t) \ = \ \mathrm{E}\big[X_i(t) \ = \ \mathit{True}\big] \ = \ \mathrm{E}\big[X_i(t)\big] \ . \tag{5.20}$$

Entsprechend ist die Ausfalldichte definiert als [59]

$$\begin{aligned} f_i(t) \ &= \ \lim_{\Delta t \to 0} \frac{1}{\Delta t} \, \mathrm{E}\big[(X_i(t) \ = \ \mathit{False}) \wedge (X_i(t+\Delta t) \ = \ \mathit{True})\big] \ = \\ &= \ \lim_{\Delta t \to 0} \frac{1}{\Delta t} \, \mathrm{E}\big[\neg \, X_i(t) \wedge X_i(t+\Delta t)\big] \ . \end{aligned} \tag{5.21}$$

Durch einfaches Umformen folgt daraus die für die folgenden Überlegungen hilfreiche Form

$$f_i(t)\Delta t + \mathrm{o}(\Delta t) \ = \ \mathrm{E}\big[\neg \, X_i(t) \wedge X_i(t+\Delta t)\big] \qquad \text{mit} \qquad \lim_{\Delta t \to 0} \frac{\mathrm{o}(\Delta t)}{\Delta t} \ = \ 0 \ . \tag{5.22}$$

PAND Operation

Der PAND Operator in $A \, \vec{\wedge} \, B$ beschreibt das Eintreten von B zu t nachdem A schon eingetreten ist. Dies bedeutet bei nichtinfinitesimaler Betrachtung, dass

- zu Zeitpunkt t Ereignis A bereits eingetreten und B noch nicht eingetreten ist und
- zu $t + \Delta t$ sowohl A als auch B eingetreten sind.

Somit ist

$$A(t) \ \wedge \ \neg B(t) \ \ \wedge \ \ A(t+\Delta t) \ \wedge \ B(t+\Delta t) \ , \tag{5.23}$$

sodass unter der Annahme unabhängiger Ereignisse A und B aus (5.22) folgt, dass

$$\begin{aligned} f_{A\,\vec{\wedge}\,B}(t)\Delta t + \mathrm{o}(\Delta t) \ &= \ \mathrm{E}\big[A(t) \wedge \neg B(t) \wedge A(t+\Delta t) \wedge B(t+\Delta t)\big] \ = \\ &= \ \mathrm{E}\big[A(t) \wedge A(t+\Delta t)\big] \cdot \mathrm{E}\big[\neg B(t) \wedge B(t+\Delta t)\big] \ . \end{aligned} \tag{5.24}$$

Der rechte Erwartungswert $\mathrm{E}\big[\neg B(t) \wedge B(t+\Delta t)\big]$ lässt sich mit (5.22) direkt ersetzen. Der linke Erwartungswert $\mathrm{E}\big[A(t) \wedge A(t+\Delta t)\big]$ ist nicht durch das einfache Produkt der Erwartungswerte der Ereignisse $A(t)$ und $A(t+\Delta t)$ gegeben, da Letztere nicht unabhängig sind. Stattdessen gilt

$$\mathrm{E}\big[A(t) \wedge A(t+\Delta t)\big] \ = \ \mathrm{E}\big[A(t+\Delta t) \mid A(t)\big] \cdot \mathrm{E}\big[A(t)\big] \ = \ \mathrm{E}\big[A(t)\big] \ , \tag{5.25}$$

da ein Ausfall zu t auch zum (infinitesimal) späteren Zeitpunkt $t+\Delta t$ später anliegt. Damit ist

$$f_{A\,\vec{\wedge}\,B}(t)\Delta t + \mathrm{o}(\Delta t) \ = \ F_A(t) \cdot \big[f_B(t)\Delta t + \mathrm{o}(\Delta t)\big] \ . \tag{5.26}$$

Dividieren durch Δt und $\Delta t \to 0$, also

$$f_{A\,\vec{\wedge}\,B}(t) \ = \ \lim_{\Delta t \to 0} \left(F_A(t) \cdot \left[f_B(t) + \frac{\mathrm{o}(\Delta t)}{\Delta t} \right] - \frac{\mathrm{o}(\Delta t)}{\Delta t} \right) \ , \tag{5.27}$$

führt schließlich zu

$$f_{A\,\vec{\wedge}\,B}(t) \ = \ F_A(t) \cdot f_B(t) \ . \tag{5.28}$$

Damit entspricht das $A\,\vec{\wedge}\,B$ aus (5.28) dem „erst A, dann B“ aus (5.14). Die Ausfallwahrscheinlichkeit des PAND ist damit gegeben durch

$$F_{A\,\vec{\wedge}\,B}(t) \ = \ \int_0^t F_A(\tau) f_B(\tau) \cdot \mathrm{d}\tau \ . \tag{5.29}$$

SAND Operation

Der SAND Operator in $A\,\overline{\vec{\wedge}}\,B$ beschreibt das exakt gleichzeitige Eintreten von A und B zu t. Dies bedeutet bei nichtinfinitesimaler Betrachtung, dass

- zu Zeitpunkt t weder A noch B eingetreten sind und
- zu $t+\Delta t$ sowohl A als auch B eingetreten sind,

also

$$\neg A(t) \ \wedge \ \neg B(t) \ \ \wedge \ \ A(t+\Delta t) \ \wedge \ B(t+\Delta t) \ , \tag{5.30}$$

sodass unter der Annahme unabhängiger Ereignisse für die Ausfalldichte folgt, dass

$$\begin{aligned} f_{A\,\overline{\vec{\wedge}}\,B}(t)\Delta t + \mathrm{o}(\Delta t) \ &= \ \mathrm{E}\big[\neg A(t) \wedge A(t+\Delta t)\big] \cdot \mathrm{E}\big[\neg B(t) \wedge B(t+\Delta t)\big] \ = \\ &= \ \big[f_A(t)\Delta t + \mathrm{o}(\Delta t)\big] \cdot \big[f_B(t)\Delta t + \mathrm{o}(\Delta t)\big] \ = \\ &= \ f_A(t) \cdot \Delta t \cdot f_B(t)\Delta t + \mathrm{o}(\Delta t) \cdot \big[\ldots\big] \ . \end{aligned}$$

Dividieren durch Δt und $\Delta t \to 0$, also

$$f_{A\,\overline{\wedge}\,B}(t) = \lim_{\Delta t \to 0} \left(f_A(t) f_B(t) \Delta t + \frac{o(\Delta t)}{\Delta t} [\ldots] - \frac{o(\Delta t)}{\Delta t} \right) , \tag{5.31}$$

führt schließlich zu

$$f_{A\,\overline{\wedge}\,B}(t) = 0 . \tag{5.32}$$

Dies bedeutet, dass die Wahrscheinlichkeit für das exakt gleichzeitige Eintreten zweier unabhängiger Ereignisse immer 0 beträgt, da jede minimale Abweichung von dieser Gleichzeitigkeit – quantitativ – in den Termen mit PAND Operatoren enthalten ist. Daher sind

$$F_{A\,\overline{\wedge}\,B}(t) = 0 , \tag{5.33}$$

$$\lambda_{A\,\overline{\wedge}\,B}(t) = 0 . \tag{5.34}$$

Obwohl der SAND Operator somit für die quantitative Modellierung überflüssig erscheint, spielt er bei der qualitativen Vereinfachung von temporalen Termen wie auch für qualitative Analysen eine wesentliche Rolle. Hierbei ist insbesondere auch das temporale Idempotenzgesetz aus (4.43) zu nennen, welches eine wichtige Filterfunktion bei der Vereinfachung temporaler Terme übernimmt.

5.3.2 Quantifizierung durch Vergleich mit Zustandsübergangs-Diagrammen

Anmerkung: Die Zusammenhänge bis (5.34) sind allgemeingültig. Die folgenden Überlegungen konzentrieren sich nur auf exponentialverteilte Kenngrößen.

Kapitel 5.2 nähert sich der gesuchten Quantifizierungsregel für die PAND Operation über die Definition der beteiligten Kenngrößen. Kapitel 5.3 zeigt, dass der Weg über die logische Bedeutung der PAND und SAND Operationen zum selben Ergebnis führt. In diesem Kapitel folgt der Vergleich dieses Ergebnisses mit einem Referenzmodell, welches die Korrektheit des Ergebnisses bestätigt.

Dieser Vergleich gliedert sich in zwei Teile. Auf die Quantifizierung der Booleschen AND und OR Operationen folgt die Quantifizierung der temporalen PAND und SAND Operationen unter Verwendung der Vervollständigungsgesetze aus Kapitel 4.2.2.

Boolesche Operationen

Abbildung 5.1 zeigt nochmals das qualitativ schon aus Abbildung 2.1 bekannte Zustandsübergangs-Diagramm eines Beispielsystems aus zwei nicht reparierbaren Einheiten A und B mit (konstanten) Übergangs- / Ausfallraten $\lambda_{i,j}$. Die Zustandswahrscheinlichkeiten $P_i(t)$ sind beschrieben durch das DGL-System

$$\begin{bmatrix} \dot{P}_1(t) \\ \dot{P}_2(t) \\ \dot{P}_3(t) \\ \dot{P}_4(t) \end{bmatrix} = \begin{bmatrix} -(\lambda_{1,2}+\lambda_{1,3}+\lambda_{1,4}) & 0 & 0 & 0 \\ \lambda_{1,2} & -\lambda_{2,4} & 0 & 0 \\ \lambda_{1,3} & 0 & -\lambda_{3,4} & 0 \\ \lambda_{1,4} & \lambda_{2,4} & \lambda_{3,4} & 0 \end{bmatrix} \cdot \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \end{bmatrix} . \tag{5.35}$$

Unter Annahme der Markov-Bedingungen besitzen A und B konstante Ausfallraten, sodass

$$\lambda_A = \lambda_{1,2} = \lambda_{3,4} \qquad \text{und} \qquad \lambda_B = \lambda_{1,3} = \lambda_{2,4} . \tag{5.36}$$

Die Lösung des DGL-Systems in (5.35) liefert die vier Zustandswahrscheinlichkeiten $P_1(t)$ bis $P_4(t)$. Die Interpretation dieser Wahrscheinlichkeiten für die Zuverlässigkeit bzw. Sicherheit des Systems ergibt sich aus der Verschaltung der Komponenten A und B:

- Im Falle einer Parallelschaltung müssen A und B ausfallen, damit das System ausfällt. Die System-(Ausfall-)funktion lautet $\varphi = A \wedge B$, entsprechend bezeichnet Zustand 04 den Systemausfall, weswegen $F_\varphi(t) = P_4(t)$ und $R_\varphi(t) = 1 - P_4(t) = P_1(t) + P_2(t) + P_3(t)$.

- Im Falle einer Serienschaltung müssen A oder B oder beide ausfallen, damit das System ausfällt. Die Ausfallfunktion lautet $\varphi = A \vee B$, entsprechend bezeichnen die Zustände 2 und 3 und 4 den Systemausfall, weswegen $F_\varphi(t) = P_2(t) + P_3(t) + P_4(t)$ und $R_\varphi(t) = 1 - P_4(t) = P_1(t)$.

Vereinfachung

Zunächst wird mit dem Wissen der Ergebnisse aus Kapitel 5.3.1 für den SAND Übergang $\lambda_{1,4} = 0$ angesetzt, also von struktureller Unabhängigkeit zwischen A und B ausgegangen.

Für das Beispielsystem in (5.35) ergeben sich mit (5.36)

$$F_{A \wedge B}(t) = P_4(t) = (1 - \mathrm{e}^{-\lambda_A t})(1 - \mathrm{e}^{-\lambda_B t}) = F_A(t) F_B(t) \tag{5.37}$$

und

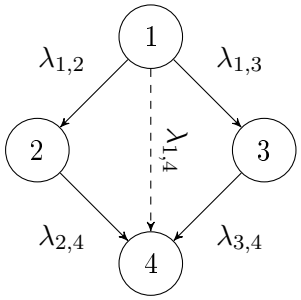
$$F_{A \vee B}(t) = P_2(t) + P_3(t) + P_4(t) = 1 - \mathrm{e}^{-(\lambda_A + \lambda_B)t} = 1 - \big[1 - F_A(t)\big]\big[1 - F_B(t)\big] \,. \tag{5.38}$$

Die Verallgemeinerung dieser Zusammenhänge führt zu den in (5.1) bis (5.6) bereits genannten Quantifizierungsfunktionen der Booleschen Operationen.

PAND und SAND Operationen

Die Quantifizierung temporaler Fehlerbäume erfolgt mittels der MCSS und analog zur Quantifizierung herkömmlicher Fehlerbäume und deren Minimalschnitte. Mit Hilfe von Zustandsübergangs-Diagrammen lassen sich die Gültigkeit der Vervollständigungsgesetze zeigen sowie Vorgaben zur Quantifizierung der temporalen Operationen ableiten.

Abbildung 5.2 zeigt das Beispielsystem aus Kapitel 5.3.2 unter Berücksichtigung von Reihenfolgen. Im Unterschied zu Abbildung 5.1 ist der Zustand 4 („A und B ausgefallen“) jetzt in drei Zustände unterteilt. Zustand 4a beschreibt das System, wenn erst A und dann B ausgefallen ist; Zustand 4b beschreibt das System, wenn erst B und dann A ausgefallen ist; Zustand 4c beschreibt das System, wenn A und B gleichzeitig ausgefallen sind. Damit handelt es sich bei dieser Art von Zustandsdiagrammen um sequentielle Ausfallbäume, vgl. Seite 31.

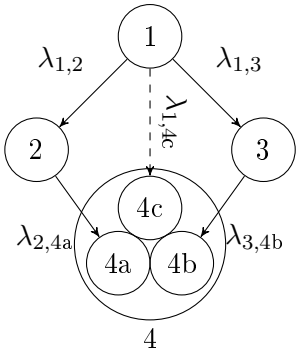


Zustände:
1: $\neg A \neg B$
2: $A \neg B$
3: $B \neg A$
4: $A \wedge B$

Abbildung 5.1: Zustandsübergangs-Diagramm eines Systems aus zwei nicht reparierbaren Einheiten A und B mit Übergangs- / Ausfallraten $\lambda_{i,j}$.

Diese drei Möglichkeiten sind disjunkt und vollständig, d. h. es existieren keine weiteren Möglichkeiten für „A und B ausgefallen“. Für den „Metazustand“ 4 gilt daher

$$P_4(t) \;=\; P_{4\mathrm{a}}(t) + P_{4\mathrm{b}}(t) + P_{4\mathrm{c}}(t)\;. \tag{5.39}$$



Zustände:
1: $\neg A \neg B$
2: $A \neg B$
3: $B \neg A$
4: $A \wedge B$
4a: $A \vec{\wedge} B$
4b: $B \vec{\wedge} A$
4c: $A \overline{\vec{\wedge}} B$

Abbildung 5.2: Markov-Modell des Beispielsystems aus Abbildung 5.1 mit Aufteilung des Zustands 4 (= „A und B ausgefallen“) in drei Zustände (4a, 4b, 4c) .

Das zugehörige DGL-System der Zustandswahrscheinlichkeiten $P_i(t)$ in Matrixschreibweise lautet

$$\begin{bmatrix} \dot{P}_1(t) \\ \dot{P}_2(t) \\ \dot{P}_3(t) \\ \dot{P}_4(t) \\ \dot{P}_{4\mathrm{a}}(t) \\ \dot{P}_{4\mathrm{b}}(t) \\ \dot{P}_{4\mathrm{c}}(t) \end{bmatrix} = \begin{bmatrix} -(\lambda_{1,2}+\lambda_{1,3}+\lambda_{1,4\mathrm{c}}) & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_{1,2} & -\lambda_{2,4\mathrm{a}} & 0 & 0 & 0 & 0 & 0 \\ \lambda_{1,3} & 0 & -\lambda_{3,4\mathrm{b}} & 0 & 0 & 0 & 0 \\ \lambda_{1,4\mathrm{c}} & \lambda_{2,4\mathrm{a}} & \lambda_{3,4\mathrm{b}} & 0 & 0 & 0 & 0 \\ 0 & \lambda_{2,4\mathrm{a}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_{3,4\mathrm{b}} & 0 & 0 & 0 & 0 \\ \lambda_{1,4\mathrm{c}} & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \\ P_{4\mathrm{a}}(t) \\ P_{4\mathrm{b}}(t) \\ P_{4\mathrm{c}}(t) \end{bmatrix}. \tag{5.40}$$

Abbildung 5.3 zeigt die Markov-Modelle des Beispielsystems für $A \wedge B$ und $A \vee B$.

Unter Annahme der Markov-Bedingungen gelten

$$\lambda_A \;=\; \lambda_{1,2} \;=\; \lambda_{3,4\mathrm{b}} \qquad \text{und} \qquad \lambda_B \;=\; \lambda_{1,3} \;=\; \lambda_{2,4\mathrm{a}}\;. \tag{5.41}$$

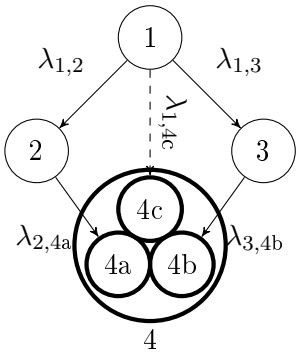
Die Lösung des DGL-Systems in (5.40) ergibt für $\lambda_{1,4\mathrm{c}} = 0$ wieder die bereits aus (5.37) und (5.38) bekannten

$$F_{A\wedge B}(t) \;=\; P_4(t) \;= (1-\mathrm{e}^{-\lambda_A t})(1-\mathrm{e}^{-\lambda_B t}) \;=\; F_A(t)F_B(t) \tag{5.42}$$

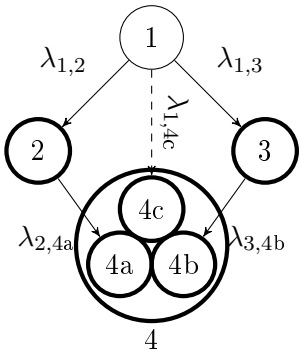
und

$$F_{A\vee B}(t) \;=\; P_2(t)+P_3(t)+P_4(t) \;=\; 1-\mathrm{e}^{-(\lambda_A+\lambda_B)t} \;=\; 1-\big[1-F_A(t)\big]\big[1-F_B(t)\big]\;. \tag{5.43}$$

Gemäß der Vervollständigungsgesetze aus Kapitel 4.2.2 lässt sich eine AND Operation mittels PAND und SAND Operationen darstellen. Abbildung 5.4 zeigt die beteiligten Zustandsübergangs-Diagramme und Ausfallfunktionen.

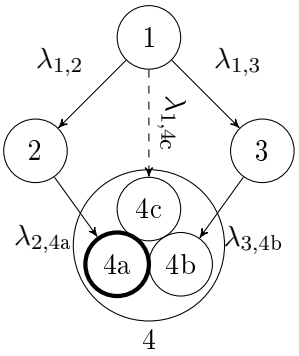


Ausfallfunktion $A \wedge B$:
rel. Zustände sind 4a, 4b, 4c $\rightarrow$
$F_{A \wedge B}(t) = P_4(t)$

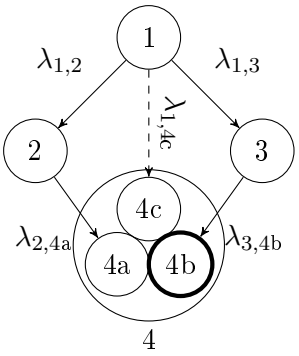


Ausfallfunktion $A \vee B$:
rel. Zustände sind 2, 3, 4 $\rightarrow$
$F_{A \vee B}(t) = P_2(t) + P_3(t) + P_4(t)$

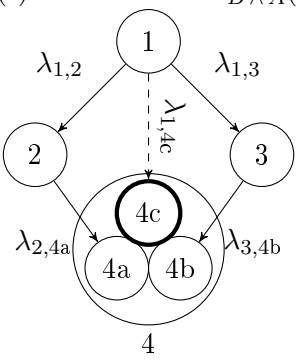
Abbildung 5.3: Markov-Modelle des Beispielsystems für die Ausfallfunktionen $A \wedge B$ und $A \vee B$ für das DGL-Systems aus (5.40). Relevante Ausfallzustände sind fett markiert.



Ausfallfunktion $A \vec{\wedge} B$:
rel. Zustand ist 4a $\rightarrow$
$F_{A \vec{\wedge} B}(t) = P_{4a}(t)$



Ausfallfunktion $B \vec{\wedge} A$:
rel. Zustand ist 4b $\rightarrow$
$F_{B \vec{\wedge} A}(t) = P_{4b}(t)$



Ausfallfunktion $A \vec{\vec{\wedge}} B$:
rel. Zustand ist 4c $\rightarrow$
$F_{A \vec{\vec{\wedge}} B}(t) = P_{4c}(t)$

Abbildung 5.4: Markov-Modelle des Beispielsystems für die Ausfallfunktionen $A \vec{\wedge} B$, $B \vec{\wedge} A$, $A \vec{\vec{\wedge}} B$ für das DGL-Systems aus (5.40). Relevante Ausfallzustände sind fett markiert.

Die Lösung des DGL-Systems in (5.40) liefert

$$F_{A\,\vec{\wedge}\,B}(t) \;=\; P_{4\mathrm{a}}(t) \;=\; \int_0^t f_B(\tau)F_A(\tau)\cdot \mathrm{d}\tau \;, \tag{5.44}$$

$$F_{B\,\vec{\wedge}\,A}(t) \;=\; P_{4\mathrm{b}}(t) \;=\; \int_0^t f_A(\tau)F_B(\tau)\cdot \mathrm{d}\tau \;, \tag{5.45}$$

$$F_{A\,\bar{\vec{\wedge}}\,B}(t) \;=\; P_{4\mathrm{c}}(t) \;=\; 0 \;. \tag{5.46}$$

Einsetzen von (5.44), (5.45), (5.46) in (5.39) führt zu

$$\begin{aligned} F_{A\wedge B}(t) \;&=\; F_{A\,\vec{\wedge}\,B}(t) + F_{B\,\vec{\wedge}\,A}(t) + F_{A\,\bar{\vec{\wedge}}\,B}(t) \;= \\ &=\; \int_0^t \big(f_B(\tau)F_A(\tau) + f_A(\tau)F_B(\tau)\big)\cdot \mathrm{d}\tau + 0 \;=\; F_A(t)\cdot F_B(t) \;. \end{aligned} \tag{5.47}$$

Dies zeigt die Gültigkeit des Vervollständigungsgesetzes auch in der quantitativen Berechnung sowie die Korrektheit der Berechnungen in Kapitel 5.3.

Die entsprechenden Ausfalldichten und -raten berechnen sich nach den allgemeinen Zusammenhängen aus (5.8) bzw. (5.9).

5.4 Quantifizierung der temporalen Ausfallfunktion

Kapitel 5.2 zeigt das grundlegende Konzept einer Quantifizierung von Ereignissequenzen. Die Anwendung dieses Konzepts auf beliebige temporale Terme in TDNF ermöglicht die Quantifizierung temporaler Fehlerbäume, d. h. die Angabe von Wahrscheinlichkeiten bzw. Häufigkeiten zu den Ereignissen und insbesondere zum TOP des Fehlerbaums.

5.4.1 Quantifizierung von Ereignissequenzen und MCSS

Die quantitative Berechnung eines temporalen Fehlerbaums erfordert zunächst die Ermittlung der MCSS als der minimalen logischen Form aller kritischen Ereignisverknüpfungen inklusive der Reihenfolgen-Aussagen. Dies erfolgt durch die in Kapitel 4.2 und 4.3 beschriebenen qualitativen Umformungen. Anschließend werden die quantitativen Kenngrößen der einzelnen MCSS ermittelt und daraus die Kenngrößen des TOP berechnet.

Vereinfachung für unabhängige Ausfallereignisse

Für den Fall unabhängiger Ausfallereignisse ist eine wesentliche Vereinfachung möglich: Vor dem Hintergrund der Überlegungen in Kapitel 5.3 sind nach der Überführung der Ausfallfunktion in ihre MCSS Form und vor deren eigentlicher Quantifizierung alle solchen MCSS zu entfernen, die mindestens einen SAND Operator enthalten. Solche MCSS sind ausschließlich für die qualitative Analyse von Bedeutung und liefern quantitativ keinen Beitrag zur Wahrscheinlichkeit bzw. Rate / Dichte der temporalen Ausfallfunktion. Die Quantifizierung beschränkt sich somit auf solche MCSS, die keine SAND Operatoren enthalten. Somit verbleiben zur Quantifizierung der Ereignissequenzen MCSS Terme der Art

$$X_1\,\vec{\wedge}\,X_2\,\vec{\wedge}\,\ldots\,\vec{\wedge}\,X_n \;, \tag{5.48}$$

ggf. noch in Konjunktion mit negierten Ereignissen

$$(\neg X_I \wedge \neg X_{II} \cdots) \wedge (X_1 \vec{\wedge} X_2 \vec{\wedge} \ldots \vec{\wedge} X_n) \ . \tag{5.49}$$

MCSS nach (5.48) lassen sich direkt mittels Faltungsintegralen über die Ausfalldichten quantifizieren, vgl. (5.28) und (5.29), sodass

$$\begin{aligned} f_{MCSS}(t) &= f_{X_1 \vec{\wedge} X_2 \vec{\wedge} \ldots \vec{\wedge} X_n}(t) = \\ &= f_{X_n}(t) \int_0^t f_{X_{n-1}}(\tau^{\{1\}}) \int_0^{\tau^{\{1\}}} f_{X_{n-2}}(\tau^{\{2\}}) \cdots \int_0^{\tau^{\{n-2\}}} f_{X_2}(\tau^{\{n-1\}}) \int_0^{\tau^{\{n-1\}}} f_{X_1}(\tau^{\{n\}}) \cdot \\ &\qquad \cdot \mathrm{d}\tau^{\{n\}} \cdot \mathrm{d}\tau^{\{n-1\}} \cdots \mathrm{d}\tau^{\{2\}} \cdot \mathrm{d}\tau^{\{1\}} \ . \end{aligned} \tag{5.50}$$

MCSS mit negierten Ereignissen
Die Wahrscheinlichkeiten von ggf. in den MCSS enthaltenen negierten Ereignissen werden zu diesen Ergebnissen multipliziert. Die Quantifizierung von MCSS nach (5.49) erfolgt somit gemäß

$$\begin{aligned} f_{MCSS}(t) &= f_{(\neg X_I \wedge \neg X_{II} \cdots) \wedge (X_1 \vec{\wedge} X_2 \vec{\wedge} \ldots \vec{\wedge} X_n)}(t) = \\ &= f_{X_1 \vec{\wedge} X_2 \vec{\wedge} \ldots \vec{\wedge} X_n}(t) \cdot R_{X_I}(t) \cdot R_{X_{II}}(t) \cdots \ , \end{aligned} \tag{5.51}$$

wobei $f_{X_1 \vec{\wedge} X_2 \vec{\wedge} \ldots \vec{\wedge} X_n}(t)$ aus (5.50) stammt.

Ausfallwahrscheinlichkeit und Ausfallrate
Die Ausfallwahrscheinlichkeiten und -raten zu (5.50) und (5.51) ergeben sich durch Einsetzen in die allgemein gültigen Gleichungen (5.8) und (5.9).

5.4.2 Quantifizierung erweiterter Ereignissequenzen

Erweiterte Ereignissequenzen und erweiterte MCSS besitzen mindestens ein erweitertes Kernereignis. Sie stellen daher eine Mischung aus Booleschem und temporallogischem Term dar. Ihrer logischen Bedeutung nach fassen erweiterte MCSS mehrere echte MCSS zusammen und decken somit mehrere Ereignissequenzen ab, vgl. Kapitel 4.4.

Aus der Liste der zu quantifizierenden MCSS lassen sich alle erweiterten MCSS entfernen, die mindestens eine SAND Verknüpfung enthalten, da diese für unabhängige Ereignisse keinen Beitrag zur Eintretenswahrscheinlichkeit liefern.

Erweiterte MCSS mit einem erweiterten Kernereignis
Sei

$$\begin{aligned} &X_1 \vec{\wedge} \ldots \vec{\wedge} X_{k-1} \vec{\wedge} X_k \vec{\wedge} X_{k+1} \vec{\wedge} \ldots \vec{\wedge} X_{n-1} \vec{\wedge} X_n \qquad \text{mit} \\ &X_k \ = \ X_{k,1} \wedge X_{k,2} \wedge \ldots X_{k,r} \end{aligned} \tag{5.52}$$

eine erweiterte MCSS mit einem erweiterten Kernereignis ($w = 1$), bestehend aus r AND-verbundenen Basisereignissen, an Position k innerhalb der PAND-Kette.

Die Ausfalldichte für $X_k(t)$ ergibt sich nach (5.3) zu

$$f_{X_k}(t) \ = \ \sum_{i=1}^{r} \left(f_{k,i}(t) \cdot \prod_{j=1; j \neq i}^{r} (F_{k,j}(t)) \right) \ . \tag{5.53}$$

Ereignissequenzen und damit auch MCSS dürfen wegen der Widerspruchsgesetze Basisereignisse nicht mehrfach enthalten, vgl. (4.42) für normale und (4.126) für erweiterte temporale Terme.

Da somit alle Ereignisse in einer (erweiterten) MCSS unabhängig voneinander sind, lässt sich die Ausfalldichte eines erweiterten Kernereignisses unabhängig vom Rest-Term gemäß (5.53) berechnen. Anschließend wird sie in die gesamte Ausfalldichte der erweiterten MCSS eingesetzt:

$$\begin{aligned} f_{MCSS}(t) &= f_{X_1 \vec{\wedge} \ldots \vec{\wedge} X_{k-1} \vec{\wedge} X_k \vec{\wedge} X_{k+1} \vec{\wedge} \ldots \vec{\wedge} X_{n-1} \vec{\wedge} X_n}(t) = \\ &= f_{X_n}(t) \int_0^t f_{X_{n-1}}(\tau^{\{1\}}) \cdots \int_0^{\tau^{\{n-(k+1)\}}} f_{X_{k+1}}(\tau^{\{n-k\}}) \cdot \\ &\quad \cdot \int_0^{\tau^{\{n-k\}}} \underbrace{f_{X_k}(\tau^{\{n-(k-1)\}})}_{\text{aus (5.53)}} \int_0^{\tau^{\{n-(k-1)\}}} f_{X(k-1)}(\tau^{\{n-(k-2)\}}) \cdots \int_0^{\tau^{\{n-1\}}} f_{X_1}(\tau^{\{n\}}) \cdot \\ &\qquad \cdot \mathrm{d}\tau^{\{n\}} \cdot \mathrm{d}\tau^{\{n-1\}} \cdots \mathrm{d}\tau^{\{n-(k-1)\}} \cdots \mathrm{d}\tau^{\{n-(k+1)\}} \cdots \mathrm{d}\tau^{\{1\}} \ . \end{aligned} \tag{5.54}$$

Erweiterte MCSS mit mehreren erweiterten Kernereignissen

Im Falle erweiterter MCSS mit $w > 1$ erweiterten Kernereignissen werden

1. die $f_{X_k}(t)$ gemäß (5.53) für alle $k \in \{1,2,\ldots,w\}$ berechnet und
2. analog zum Fall mit $w = 1$ aus (5.54) alle w so errechneten Ausfalldichten in die gesamte Ausfalldichte der erweiterten MCSS eingesetzt.

MCSS mit negierten Ereignissen

Die Wahrscheinlichkeiten von in den erweiterten MCSS enthaltenen negierten Ereignissen lassen sich analog zu (5.51) berücksichtigen.

Ausfallwahrscheinlichkeit und Ausfallrate

Die Ausfallwahrscheinlichkeit einer erweiterten MCSS ergibt sich aus der Integration über (5.54) gemäß (5.8); die entsprechende Ausfallrate folgt dann aus (5.9).

5.4.3 Quantifizierung der temporalen Ausfallfunktion des TOP-Ereignisses

Die mittels des Verfahrens nach Kapitel 4.3 bestimmten MCSS sind disjunkt.

Somit ergibt die einfache Addition der quantitativen Beiträge der einzelnen disjunkten MCSS gemäß (5.5) und (5.6) die Ausfallwahrscheinlichkeit bzw. Ausfalldichte des TOP:

$$F_{TOP}(t) = \sum_{i=1}^{\xi} F_{MCSS_i}(t) \ , \tag{5.55}$$

$$f_{TOP}(t) = \sum_{i=1}^{\xi} f_{MCSS_i}(t) \ . \tag{5.56}$$

Je nach gewählter Vorgehensweise stammen dabei die Kenngrößen der disjunkten MCSS

- im Falle normaler MCSS aus Kapitel 5.4.1 oder
- im Falle erweiterter MCSS aus Kapitel 5.4.2.

5.5 Ansatz mit minimiertem Rechenaufwand

Der Berechnungsaufwand für die Mehrfachintegral-Gleichungen nach (5.50) oder (5.51) oder (5.54) ist vergleichsweise groß, insbesondere im Falle komplexerer temporaler Fehlerbäume bzw. Ausfallfunktionen. Dies steht im Konflikt mit dem erklärten Ziel der TFTA, die Modellierung von Ereignissequenzen explizit auch für umfangreiche und komplexe Systeme zu ermöglichen.

Dieses Kapitel diskutiert daher einen Ansatz zur Approximation der Ausfallwahrscheinlichkeit und Ausfalldichte von Ausfallsequenzen bzw. MCSS, welcher den Berechnungsaufwand signifikant verringert. Wesentliche Vorraussetzungen für die Anwendung dieser Näherung sind

- konstante Ausfallraten aller Basisereignisse, d. h. exponentialverteilte Ausfallwahrscheinlichkeiten, und
- „sehr kleine“ Ausfallwahrscheinlichkeiten bzw. -raten, d. h. die Gültigkeit der im sicherheitstechnischen Umfeld i. d. R. immer zutreffenden Näherung aus (5.19), derzufolge für $\lambda\, t \ll 1$ immer $f(t) \approx \lambda(t)$ gilt.

5.5.1 Temporale Terme in MCSS Form

Zunächst werden temporale Terme in MCSS Form diskutiert, wie sie sich z. B. aus einer qualitativen TFTA nach den Umformungen aus Kapitel 4.3 ergeben.

MCSS ohne negierte Ereignisse

Die Ausfallwahrscheinlichkeit / Ausfalldichte von MCSS ohne negierte Ereignisse, aber mit mindestens einem SAND Operator, beträgt den Überlegungen auf Seite 73 folgend immer Null.

Somit verbleiben für die Quantifizierung wieder MCSS ohne negierte Ereignisse der in (5.48) gezeigten Form. Deren Ausfallwahrscheinlichkeit ergibt sich durch Integration über (5.50) zu

$$\begin{aligned} F_{MCSS}(t) &= F_{X_1 \,\vec{\wedge}\, X_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, X_n}(t) = \int_0^t f_{X_1 \,\vec{\wedge}\, X_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, X_n}(\tau) \cdot \mathrm{d}\tau = \\ &= \int_0^t f_{X_n}(\tau) \cdot \int_0^{\tau} f_{X_{n-1}}(\tau^{\{1\}}) \cdots \int_0^{\tau^{\{n-2\}}} f_{X_2}(\tau^{\{n-1\}}) \cdot \int_0^{\tau^{\{n-1\}}} f_{X_1}(\tau^{\{n\}}) \cdot \\ &\qquad \cdot \mathrm{d}\tau^{\{n\}} \cdot \mathrm{d}\tau^{\{n-1\}} \cdots \mathrm{d}\tau^{\{1\}} \cdot \mathrm{d}\tau \ . \end{aligned} \tag{5.57}$$

Bei insgesamt n an einer MCSS beteiligten Basisereignissen repräsentiert jede MCSS genau eine Ereignissequenz der insgesamt $n!$ möglichen Permutationen. Die Wahrscheinlichkeit, dass alle n an einer MCSS beteiligten Ereignisse zu t eingetreten sind, wobei keine Reihenfolgen unterschieden werden, beträgt nach (5.1)

$$F_{X_1 \wedge X_2 \wedge \ldots \wedge X_n}(t) = F_{X_1}(t) \cdot F_{X_2}(t) \cdots F_{X_n}(t) = \prod_{i=1}^{n} F_{X_i}(t) \ . \tag{5.58}$$

Für exponentialverteilte und sehr kleine Ausfallraten gilt mit (5.19) näherungsweise

$$f(t) \approx \lambda(t) = \lambda \qquad \text{und somit auch} \tag{5.59}$$

$$F(t) \approx \lambda \cdot t \qquad \text{für } \lambda \cdot t \ll 1 \ . \tag{5.60}$$

Somit ist

$$F_{X_1 \wedge X_2 \wedge \ldots \wedge X_n}(t) \approx \lambda_{X_1} t \cdot \lambda_{X_2} t \cdots \lambda_{X_n} t = \prod_{i=1}^{n} (\lambda_{X_i} t) \ . \tag{5.61}$$

Sind zudem alle n Ausfallraten $\lambda_X = \lambda_{X_1} = \ldots = \lambda_{X_n}$ gleich groß, so treten alle $n!$ möglichen Permutationen von Ereignissen mit derselben Wahrscheinlichkeit ein, weswegen für jede MCSS gilt, dass

$$F_{MCSS}(t) = \frac{1}{n!} \prod_{i=1}^{n} F_{X_i}(t) \approx \frac{1}{n!} \prod_{i=1}^{n} (\lambda_{X_i} t) \ . \tag{5.62}$$

Gleichung (5.62) gilt darüber hinaus auch als allgemeine Näherung für den Fall unterschiedlicher Ausfallraten, sofern die Größte der n Ausfallraten der Bedingung

$$\max\left(\lambda_{X_1}; \lambda_{X_2}; \cdots ; \lambda_{X_n}\right) \cdot t \ll 1 \tag{5.63}$$

genügt, sodass

$$F_{MCSS}(t) \approx \frac{1}{n!} \prod_{i=1}^{n} (\lambda_{X_i} t) \ . \tag{5.64}$$

Die Approximation der Ausfalldichte einer MCSS ergibt sich analog zu diesen Überlegungen. Sei ohne Einschränkung der Allgemeinheit X_n das zuletzt eintretende Ereignis einer MCSS mit n beteiligten Ereignissen, dann gilt

$$f_{MCSS}(t) = f_{X_1 \,\vec{\wedge}\, X_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, X_n}(t) = f_{X_n}(t) \cdot F_{X_1 \,\vec{\wedge}\, X_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, X_{n-1}}(t) \ , \tag{5.65}$$

woraus mit (5.59) und (5.60) folgt, dass

$$f_{MCSS}(t) \approx \frac{1}{(n-1)!} \cdot \lambda_{X_n} \cdot \prod_{i=1}^{n-1} (\lambda_{X_i} t) \ . \tag{5.66}$$

MCSS mit negierten Ereignissen

Die Berechnung einer Näherungslösung für MCSS mit negierten Ereignissen kombiniert das Vorgehen in Kapitel 5.4.1 mit der Eintretenswahrscheinlichkeit negierter Ereignisse nach (5.7) und die soeben für MCSS ohne negierte Ereignisse diskutierte Lösung. Unter Verwendung von (5.64) bzw. (5.66) folgt

$$\begin{aligned} F_{MCSS}(t) &= F_{(\neg X_I \wedge \neg X_{II} \cdots) \wedge (X_1 \,\vec{\wedge}\, X_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, X_n)}(t) \cdots \approx \\ &\approx \frac{1}{n!} \cdot \prod_{i=1}^{n} (\lambda_{X_i} t) \cdot R_{X_I}(t) \cdot R_{X_{II}}(t) \cdots \ , \end{aligned} \tag{5.67}$$

$$\begin{aligned} f_{MCSS}(t) &= f_{X_1 \,\vec{\wedge}\, X_2 \,\vec{\wedge}\, \ldots \,\vec{\wedge}\, X_n}(t) \cdot R_{X_I}(t) \cdot R_{X_{II}}(t) \cdots \approx \\ &\approx \frac{1}{(n-1)!} \cdot \lambda_{X_n} \cdot \prod_{i=1}^{n-1} (\lambda_{X_i} t) \cdot R_{X_I}(t) \cdot R_{X_{II}}(t) \cdots \ . \end{aligned} \tag{5.68}$$

5.5.2 Temporale Terme in erweiterter MCSS Form

Es gelten die in Kapitel 5.5.1 vorangestellten Annahmen, insbesondere werden keine SAND-Verknüpfungen betrachtet, da diese keinen Wahrscheinlichkeitsbeitrag liefern.

Die Erweiterung des Ansatzes mit minimiertem Rechenaufwand auch auf erweiterte MCSS erfordert eine Diskussion über die Anzahl der normalen MCSS, die durch eine erweiterte MCSS abgedeckt sind.

Im einfachsten Fall deckt z. B. die erweiterte MCSS $(X_1 \wedge X_2)\,\vec{\wedge}\,X_3$ die beiden echten und zueinander disjunkten MCSS $X_1\,\vec{\wedge}\,X_2\,\vec{\wedge}\,X_3$ und $X_2\,\vec{\wedge}\,X_1\,\vec{\wedge}\,X_3$ ab. Mit (5.62) besitzt jede der beiden echten MCSS die Wahrscheinlichkeit

$$F_{X_1\,\vec{\wedge}\,X_2\,\vec{\wedge}\,X_3}(t) \;=\; F_{X_2\,\vec{\wedge}\,X_1\,\vec{\wedge}\,X_3}(t) \approx \frac{1}{6} F_{X_1} F_{X_2} F_{X_3}\;. \tag{5.69}$$

Entsprechend ist

$$F_{(X_1 \wedge X_2)\,\vec{\wedge}\,X_3}(t) \approx 2 \cdot \frac{1}{6} F_{X_1} F_{X_2} F_{X_3} \;=\; \frac{1}{3} F_{X_1} F_{X_2} F_{X_3}\;. \tag{5.70}$$

Die durch eine erweiterte MCSS abgedeckten echten MCSS sind wegen des Vervollständigungsgesetzes immer zueinander disjunkt. Die Ausfallwahrscheinlichkeit / Ausfalldichte einer erweiterten MCSS ergibt sich daher aus der einfachen Summe über die Ausfallwahrscheinlichkeiten / Ausfalldichten der durch sie abgedeckten echten MCSS.

Allgemein hängt die Anzahl Υ der durch eine erweiterte MCSS abgedeckten echten MCSS (ohne SAND Verknüpfungen) ab

- von w, der Anzahl der erweiterten Kernereignisse innerhalb der erweiterten MCSS,
- sowie für jedes erweiterte Kernereignis $i \in \{1,\ldots,w\}$ von r_i, der Anzahl seiner AND verbundenen Basisereignisse
- und von k_i, der Position dieses erweiterten Kernereignisses innerhalb der MCSS.

Einige Beispiele:

$$\begin{aligned}
&(X_1 \wedge X_2)\,\vec{\wedge}\,X_3 && \rightarrow \quad w = 1\;;\; r = 2\;;\; k = 1\;,\\
&X_1\,\vec{\wedge}\,(X_2 \wedge X_3) && \rightarrow \quad w = 1\;;\; r = 2\;;\; k = 2\;,\\
&(X_1 \wedge X_2)\,\vec{\wedge}\,(X_3 \wedge X_4) && \rightarrow \quad w = 2\;;\; r_1 = r_2 = 2\;;\; k_1 = 1\;;\; k_2 = 3\;,\\
&X_1\,\vec{\wedge}\,(X_2 \wedge X_3 \wedge X_4) && \rightarrow \quad w = 1\;;\; r = 3\;;\; k = 2\;.
\end{aligned}$$

Man beachte im dritten Beispiel das $k_2 = 3$. Für die Position der $i \in \{2,\ldots,w\}$-ten erweiterten Kernereignisse zählen alle Ereignisse inkl. solcher in „früheren“ erweiterten Kernereignissen, also solcher, die in der MCSS links vom i-ten erweiterten Kernereignis stehen. Die folgende Anwendung des Vervollständigungsgesetzes verdeutlicht dies (SAND Verknüpfung wird vernachlässigt):

$$(X_1 \wedge X_2)\,\vec{\wedge}\,(X_3 \wedge X_4) \;=\; \Big[X_1\,\vec{\wedge}\,X_2\,\vec{\wedge}\,(X_3 \wedge X_4)\Big] \vee \Big[X_2\,\vec{\wedge}\,X_1\,\vec{\wedge}\,(X_3 \wedge X_4)\Big]\;. \tag{5.71}$$

Die Position des zweiten erweiterten Kernereignisses ist hierbei $k_2 = 3$.

Allgemein deckt jedes erweiterte Kernereignis i mit r_i Basisereignissen und an Position k_i

$$\Upsilon_i \;=\; \binom{(k_i - 1) + (r_i - 1)}{(k_i - 1)} \cdot r_i! \tag{5.72}$$

echte MCSS ab. Dies ergibt sich erstens aus den $r_i!$ Permutationen innerhalb des erweiterten Kernereignisses. Für jede dieser Permutationen können zweitens die $(k_i - 1)$ Ereignisse vor dem erweiterten Kernereignis auf Grund des Zusammenhangs aus (4.48) an insgesamt $(k_i-1)+(r_i-1)$ Stellen stehen.

Einige Beispiele:

- $(X_1 \wedge X_2) \vec{\wedge} X_3 \quad \rightarrow \quad w = 1 \; ; \; r = 2 \; ; \; k = 1 \quad \rightarrow \quad \Upsilon = 2 \; :$
  $\rightarrow \quad X_1 \vec{\wedge} X_2 \vec{\wedge} X_3 \; , \; X_2 \vec{\wedge} X_1 \vec{\wedge} X_3 \; .$
- $X_1 \vec{\wedge} (X_2 \wedge X_3) \quad \rightarrow \quad w = 1 \; ; \; r = 2 \; ; \; k = 2 \quad \rightarrow \quad \Upsilon = 4 \; :$
  $\rightarrow \quad X_1 \vec{\wedge} X_2 \vec{\wedge} X_3 \; , \; X_1 \vec{\wedge} X_3 \vec{\wedge} X_2 \; , \; X_2 \vec{\wedge} X_1 \vec{\wedge} X_3 \; , \; X_3 \vec{\wedge} X_1 \vec{\wedge} X_2 \; .$
- $X_1 \vec{\wedge} X_2 \vec{\wedge} (X_3 \wedge X_4) \quad \rightarrow \quad w = 1 \; ; \; r = 2 \; ; \; k = 3 \quad \rightarrow \quad \Upsilon = 6 \; :$
  $\rightarrow \quad X_1 \vec{\wedge} X_2 \vec{\wedge} X_3 \vec{\wedge} X_4 \; , \; X_1 \vec{\wedge} X_2 \vec{\wedge} X_4 \vec{\wedge} X_3 \; , \; X_1 \vec{\wedge} X_3 \vec{\wedge} X_2 \vec{\wedge} X_4 \; ,$
  $X_1 \vec{\wedge} X_4 \vec{\wedge} X_2 \vec{\wedge} X_3 \; , \; X_3 \vec{\wedge} X_1 \vec{\wedge} X_2 \vec{\wedge} X_4 \; , \; X_4 \vec{\wedge} X_1 \vec{\wedge} X_2 \vec{\wedge} X_3 \; .$

Bei $w > 1$ erweiterten Kernereignissen ist die Gesamtzahl abgedeckter Permutationen

$$\Upsilon = \prod_{i=1}^{w} \Upsilon_i \; . \tag{5.73}$$

Beispielsweise steht die erweiterte MCSS $(X_1 \wedge X_2) \vec{\wedge} (X_3 \wedge X_4)$ mit $w = 2$, $r_1 = r_2 = 2$, $k_1 = 1$, $k_2 = 3$ für die insgesamt $\Upsilon = \Upsilon_1 \cdot \Upsilon_2 = 2 \cdot 6 = 12$ Permutationen

$$\begin{aligned}
&X_1 \vec{\wedge} X_2 \vec{\wedge} X_3 \vec{\wedge} X_4 \; , \; X_1 \vec{\wedge} X_2 \vec{\wedge} X_4 \vec{\wedge} X_3 \; , \; X_1 \vec{\wedge} X_3 \vec{\wedge} X_2 \vec{\wedge} X_4 \; , \\
&X_1 \vec{\wedge} X_4 \vec{\wedge} X_2 \vec{\wedge} X_3 \; , \; X_3 \vec{\wedge} X_1 \vec{\wedge} X_2 \vec{\wedge} X_4 \; , \; X_4 \vec{\wedge} X_1 \vec{\wedge} X_2 \vec{\wedge} X_3 \; , \\
&X_2 \vec{\wedge} X_1 \vec{\wedge} X_3 \vec{\wedge} X_4 \; , \; X_2 \vec{\wedge} X_1 \vec{\wedge} X_4 \vec{\wedge} X_3 \; , \; X_2 \vec{\wedge} X_3 \vec{\wedge} X_1 \vec{\wedge} X_4 \; , \\
&X_2 \vec{\wedge} X_4 \vec{\wedge} X_1 \vec{\wedge} X_3 \; , \; X_3 \vec{\wedge} X_2 \vec{\wedge} X_1 \vec{\wedge} X_4 \; , \; X_4 \vec{\wedge} X_2 \vec{\wedge} X_1 \vec{\wedge} X_3 \; .
\end{aligned}$$

In Analogie zu (5.67) beträgt somit die Ausfallwahrscheinlichkeit einer erweiterten MCSS im Allgemeinen näherungsweise

$$F_{MCSS}(t) \approx \Upsilon \cdot \frac{1}{n!} \cdot \prod_{i=1}^{n} (\lambda_{X_i} t) \cdot R_{X_I}(t) \cdot R_{X_{II}}(t) \cdots \; . \tag{5.74}$$

Eine entsprechende Approximation der Ausfalldichte ist in Analogie zu (5.68) gegeben durch

$$f_{MCSS}(t) \approx \Upsilon \cdot \frac{1}{(n-1)!} \cdot \lambda_{X_n} \cdot \prod_{i=1}^{n-1} (\lambda_{X_i} t) \cdot R_{X_I}(t) \cdot R_{X_{II}}(t) \cdots \; . \tag{5.75}$$

Zusammenfassung Kapitel 5.5 Ansatz mit minimiertem Rechenaufwand

Für konstante Ausfallraten und „sehr kleine“ Ausfallwahrscheinlichkeiten unterscheiden sich die Eintretenswahrscheinlichkeiten und -häufigkeiten einzelner Permutationen der an einer MCSS beteiligten Ereignisse nicht mehr wesentlich voneinander. Für die Berechnung von $F_{MCSS}(t)$ und $f_{MCSS}(t)$ spielt die Sequenzinformation somit nur noch eine untergeordnete Rolle. Dies ist vorteilhaft, da die quantitative Berechnung der exakten Sequenzinformationen die mehrfach geschachtelten Integrale aus Kapitel 5.3 erfordert und somit sehr aufwändig ist. Die hier vorgestellte Approximation erlaubt hingegen – unter den eingangs genannten Bedingungen – eine Abschätzung der Größen $F_{MCSS}(t)$ und $f_{MCSS}(t)$ ausschließlich auf Basis der Anzahl der an einer MCSS beteiligten Ereignisse und deren Ausfallraten, vgl. (5.67) und (5.68). Eine explizite Berechnung der Sequenzinformationen ist nicht notwendig. Auch erweiterte MCSS lassen sich so quantifizieren, vgl. (5.74) und (5.75).

6 Vergleich der TFTA mit anderen dynamischen Modellierungen

Much may be said on both sides.

(Henry Fielding)

Zur Verdeutlichung des Potentials der TFTA werden im Folgenden an Hand eines in Kapitel 6.1 beschriebenen Beispiels

- die klassische Boolesche FTA, vgl. Kapitel 6.2,
- eine dynamische Fehlerbaum-Modellierung nach dem DFT Ansatz, vgl. Kapitel 2.3, und
- eine reine Markov-Modellierung, vgl. Kapitel 6.4,

mit dem neuen TFTA Ansatz verglichen (Kapitel 6.5). Die Vergleichs-Modellierungen erfolgten mit dem Fehlerbaum-Programm FaultTree+ [50].

6.1 Das Beispielsystem

Die folgenden Vergleiche verwenden ein Beispielsystem aus [79], vgl. Abbildung 6.1 .

Systembeschreibung
Die Systemfunktion des vorliegenden Systems ist die Versorgung des Punktes X mit Energie. Eine Energieversorgung E versorgt dazu über einen Umschalter U zwei redundante Stränge A und B. Zunächst ist U so geschaltet, dass der Energiefluss über A erfolgt. Bei einem Fehler in A schaltet U den Energiefluss auf Strang B um, sodass die Systemfunktion zunächst erhalten bleibt.

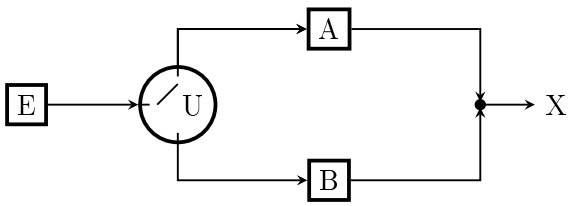


Abbildung 6.1: Beispielsystem für den Vergleich zwischen Boolescher FTA, DFT, Markov-Modellierung und TFTA.

Betrachtet werden die folgenden Fehler der Komponenten:

E: Keine Bereitstellung von Energie. Die Ausfallrate beträgt $\lambda_E = 1 \cdot 10^{-9} \frac{1}{\text{h}}$.

U: Keine Umschaltung von A nach B möglich. Die Ausfallrate beträgt $\lambda_U = 5 \cdot 10^{-6} \frac{1}{\text{h}}$.

A: Interner Fehler, der den Energiefluss unterbricht. Die Ausfallrate beträgt $\lambda_A = 1 \cdot 10^{-6} \frac{1}{\text{h}}$.

B: Interner Fehler, der den Energiefluss unterbricht. Die Ausfallrate beträgt $\lambda_B = 1 \cdot 10^{-6} \frac{1}{\text{h}}$.

Alle Komponenten sind nicht reparierbar, alle Ausfallraten sind konstant, die Missionszeit beträgt $T_M = 400\text{h}$. Die zeitliche Reihenfolge der einzelnen Ausfälle spielt eine Rolle, da zwar der Ausfall von U vor dem Ausfall von A zum Systemausfall führt, gleichwohl aber der Ausfall von U nach erfolgter Umschaltung, also nach dem Ausfall von A, nicht zum Systemausfall führt. Die qualitativen und quantitativen Ergebnisse der verschiedenen Modellierungen sind in den Tabellen 6.1 und 6.2 auf Seite 88) zusammengefasst.

6.2 Vergleichsmodellierung: Boolesche FTA

Ein rein Boolesches Modell kann die für das System-Ausfallverhalten relevante Reihenfolge von Ereignissen nicht berücksichtigen. Näherungsweise ist an Stelle des echten Systemplans aus Abbildung 6.1 eine der in Abbildung 6.2 dargestellten Varianten als Ausgangsbasis eines Booleschen Fehlerbaums zu wählen, vgl. [79]. Abbildung 6.3 zeigt die Booleschen Fehlerbäume zu diesen beiden Varianten „Bool 1“ und „Bool 2“.

Qualitative und quantitative Berechnung

Die Ausfallwahrscheinlichkeiten und Ausfalldichten der Komponenten am Ende der Missionszeit betragen mit (5.10)

$$F_A(T_M) = 3{,}9992 \cdot 10^{-4}\,, \qquad f_A(T_M) = 9{,}9960 \cdot 10^{-7} \tfrac{1}{\text{h}}\,, \tag{6.1}$$

$$F_B(T_M) = 3{,}9992 \cdot 10^{-4}\,, \qquad f_B(T_M) = 9{,}9960 \cdot 10^{-7} \tfrac{1}{\text{h}}\,, \tag{6.2}$$

$$F_U(T_M) = 1{,}9960 \cdot 10^{-3}\,, \qquad f_U(T_M) = 4{,}9900 \cdot 10^{-6} \tfrac{1}{\text{h}}\,, \tag{6.3}$$

$$F_E(T_M) = 4{,}0000 \cdot 10^{-7}\,, \qquad f_E(T_M) = 1{,}0000 \cdot 10^{-9} \tfrac{1}{\text{h}}\,. \tag{6.4}$$

Die Ausfallfunktion φ ergibt sich zu

$$\varphi_{\text{Bool 1}} = (A \vee E) \wedge (B \vee U \vee E) = \big[A \wedge B\big] \vee \big[A \wedge U\big] \vee \big[E\big] \qquad \text{und} \tag{6.5}$$

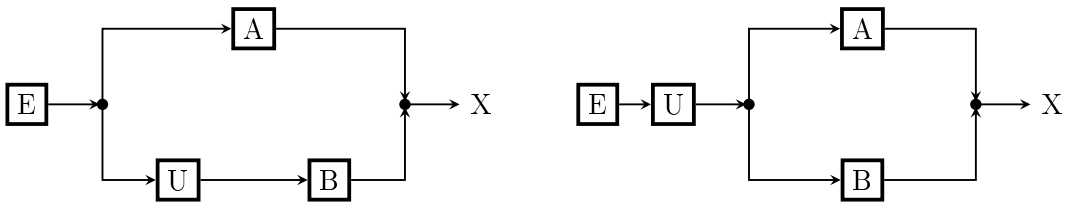


Abbildung 6.2: Zwei mögliche Varianten einer rein Booleschen Näherungsbetrachtung des Beispielsystems aus Abbildung 6.1 als Ausgangsbasis für die herkömmliche Boolesche FTA. Die linke Variante wird im Folgenden als „Bool 1“ und die rechte Variante als „Bool 2“ bezeichnet.

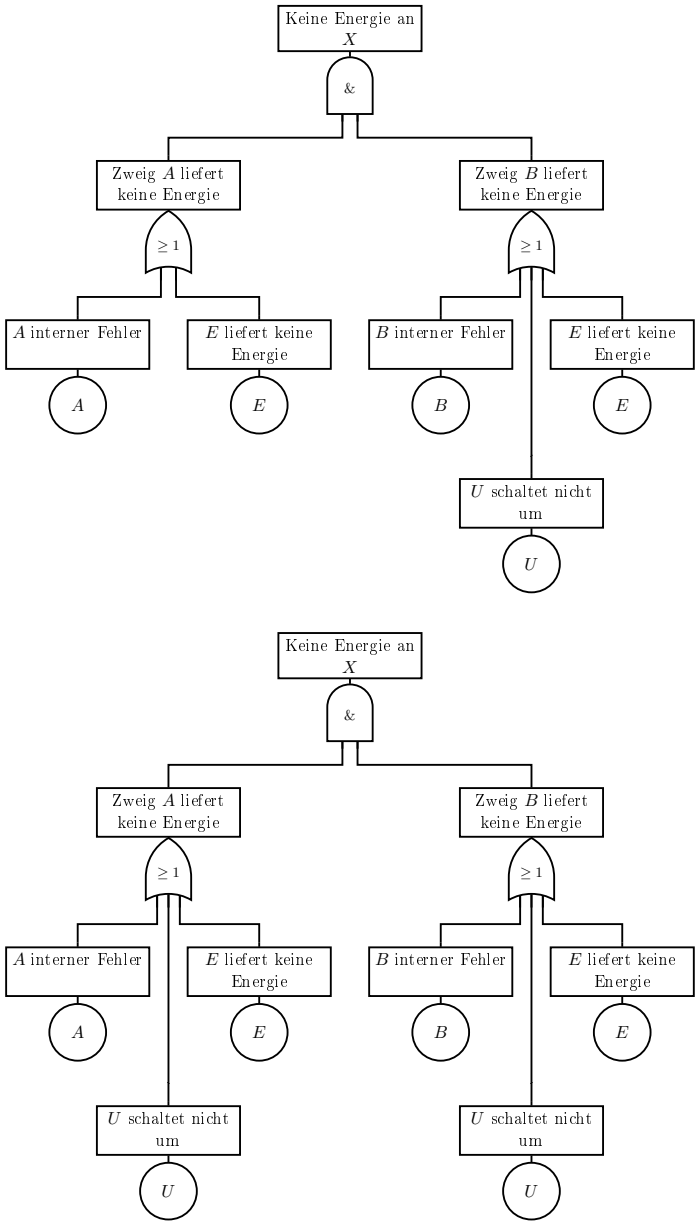


Abbildung 6.3: Boolesche Fehlerbäume der Varianten „Bool 1“ (oben) und „Bool 2“ (unten).

$$\varphi_{\text{Bool 2}} = (A \vee U \vee E) \wedge (B \vee U \vee E) = \big[A \wedge B\big] \vee \big[U\big] \vee \big[E\big] \ . \tag{6.6}$$

Überführt in eine disjunkte Form mit

$$\varphi_{\text{Bool 1}} = \big[A \wedge B \wedge \neg E \wedge \neg U\big] \vee \big[A \wedge U \wedge \neg E\big] \vee \big[E\big] \qquad \text{und} \tag{6.7}$$

$$\varphi_{\text{Bool 2}} = \big[A \wedge B \wedge \neg E \wedge \neg U\big] \vee \big[U \wedge \neg E\big] \vee \big[E\big] \tag{6.8}$$

und quantifiziert, ergeben sich die TOP Ergebnisse mit den oben angegebenen Daten zu

$$F_{\text{Bool 1}}(T_M) = 1{,}3587 \cdot 10^{-6} \ , \qquad f_{\text{Bool 1}}(T_M) = 5{,}7899 \cdot 10^{-9} \tfrac{1}{\text{h}} \qquad \text{und} \tag{6.9}$$

$$F_{\text{Bool 2}}(T_M) = 1{,}9986 \cdot 10^{-3} \ , \qquad f_{\text{Bool 2}}(T_M) = 4{,}9918 \cdot 10^{-6} \tfrac{1}{\text{h}} \ . \tag{6.10}$$

Dies sind auch die Ergebnisse der Berechnung in FaultTree+.

Aspekte der Erstellung der Fehlerbäume

In beiden Fällen lässt sich der Fehlerbaum auf systematische Weise aus dem System-Schaltplan ableiten, indem dieser vom Ausgang zum Eingang durchschritten wird. Dabei muss der Anwender keine Rücksicht auf mögliche Doppelungen nehmen, da diese durch die Boolesche Logik korrekt eliminiert werden.

Ergebnisdiskussion

Die qualitative Analyse der Minimalschnitte zeigt, dass in beiden Fällen Systemausfälle berechnet werden, obwohl tatsächlich kein Systemausfall vorliegt. Bei „Bool 1“ liegt die Ungenauigkeit im Minimalschnitt $\big[A \wedge U\big]$ und bei „Bool 2“ im Minimalschnitt $\big[U\big]$. „Bool 2“ ist somit besonders konservativ: auf der qualitativen Seite enthält der Fehlerbaum einen Einzelfehler mehr als nötig und quantitativ ergeben sich wesentlich höhere Werte für die TOP Ausfallkenngrößen. Im Vergleich der Booleschen Varianten ist sicherlich „Bool 1“ die realistischere Modellierung.

6.3 Vergleichsmodellierung: Dynamische FTA mit DFT Ansatz

Im Gegensatz zum Booleschen Modell berücksichtigt ein DFT Fehlerbaum die für das System-Ausfallverhalten relevante Ereignissequenz mittels eines PAND Gatters.

Abbildung 6.4 zeigt die zwei Varianten „DFT 1“ und „DFT 2“ mit dem dynamischen Modul (Gatter „U fällt vor A aus“), hinter dem sich ein Markov Diagramm verbirgt, vgl. Abbildung 2.3. Es wird hier zur besseren Unterscheidung nicht die TFTA Form des PAND Gatters (ein AND Gatter mit horizontalem Pfeil von links nach rechts) verwendet, sondern die originale Form des DFT Ansatzes aus [37], d. h. ein AND Gatter mit doppeltem Querbalken.

In „DFT 1“ besteht über das Basisereignis A eine Vermaschung zwischen dem dynamischen Modul und dem Booleschen Rest des FehlerbaumSeite Dies führt insbesondere dazu, dass das Basiserignis A auch als Eingang zu AND Gatter „Interne Fehler in A und B“ mit gesetztem Sequenz-Flag erscheint. In Bezug auf das Ereignis B ist diese Sequenzinformation jedoch falsch und führt zu quantitativ optimistischen, d. h. zu kleinen, Ergebniswerten.

Die Vermaschung über A ist in „DFT 2“ aufgelöst. Allerdings muss dazu derselbe Ausfall einer realen Komponente A durch zwei verschiedene Basisereignisse A und $A^\star$ abgebildet werden. In komplexen Fehlerbäumen ist dieses Vorgehen unpraktisch, aufwändig und erschwert eine saubere Analyse. Zudem sind die quantitativen Ergebnisse konservativ, da ggf. vorhandene Schnittmengen nicht korrekt berücksichtigt werden können.

Qualitative und quantitative Berechnung

Die Ausfallwahrscheinlichkeiten und Ausfalldichten der Komponenten am Ende der Missionszeit entsprechen denen der Booleschen Modellierung, vgl. Seite 82.

Eine Besonderheit des DFT Ansatzes ist, dass für die qualitative Berechnung der Ausfallfunktion das PAND Gatter als einfaches AND Gatter interpretiert wird. Dies ist sicherlich ein sinnvoller konservativer Ansatz, der allerdings auch dazu führt, dass die Sequenzinformationen nicht in den qualitativen Ergebnissen enthalten sind. Die Ausfallfunktion φ ergibt sich zu

$$\varphi_{\mathrm{DFT\,1}} \;=\; \big[A \wedge B\big] \vee \big[U \wedge A\big] \vee \big[E\big] \qquad \text{und} \tag{6.11}$$

$$\varphi_{\mathrm{DFT\,2}} \;=\; \big[A^\star \wedge B\big] \vee \big[U \wedge A\big] \vee \big[E\big]\ . \tag{6.12}$$

Die Berechnung in Isograph FaultTree+ brachte folgende Ergebnisse:

$$F_{\mathrm{DFT\,1}}(T_M) \;=\; 8{,}7933 \cdot 10^{-7}\ , \qquad f_{\mathrm{DFT\,1}}(T_M) \;=\; 3{,}3946 \cdot 10^{-9}\,\tfrac{1}{\mathrm{h}} \qquad \text{und} \tag{6.13}$$

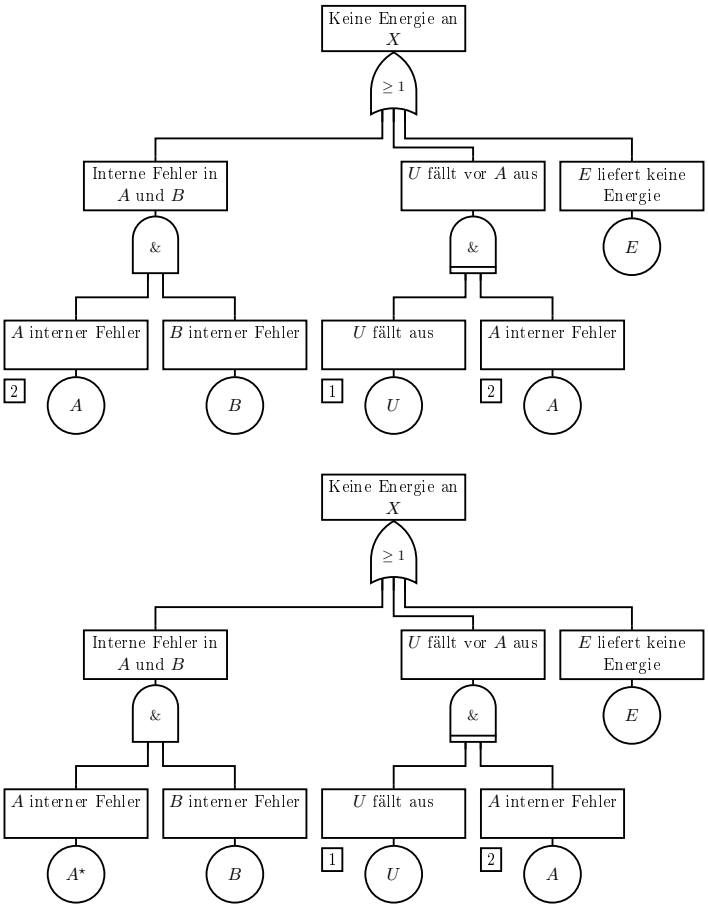


Abbildung 6.4: Fehlerbäume nach dem DFT Ansatz mit den beiden Varianten „DFT 1“ (oben) und „DFT 2“ (unten). Bei „DFT 1“ besteht über das Ereignis A eine (in der DFT unzulässige) Vermaschung zwischen Booleschen und dynamischen Modulen. Bei „DFT 2“ wird dasselbe reale Ausfallereignis der Komponente A durch zwei verschiedene Basisereignisse A und $A^\star$ abgebildet und die Vermaschung somit aufgelöst. Beide Varianten liefern Näherungswerte und bieten keine qualitative Analyse, die Sequenzinformationen enthält.

$$F_{\mathrm{DFT\ 2}}(T_M) \;=\; 9{,}5962 \cdot 10^{-7}\;, \qquad f_{\mathrm{DFT\ 2}}(T_M) \;=\; 3{,}7967 \cdot 10^{-9}\,\tfrac{1}{\mathrm{h}}\;. \tag{6.14}$$

6.4 Vergleichsmodellierung: Markov Diagramm

Die folgende Modellierung des Beispielsystems mittels eines Markov Diagramms dient als Referenz für die quantitativen Berechnungen. Abbildung 6.5 zeigt das entsprechende Diagramm, in dem alle Zustände des Systemausfalls „Keine Energie an X“ fett markiert sind. Dabei wurde die Sequenzinformation zwischen U und A berücksichtigt.

Die Berechnung in FaultTree+ brachte mit $T_M = 400\mathrm{h}$ folgende Ergebnisse:

$$F_{\mathrm{MAR}}(T_M) \;=\; 9{,}5940 \cdot 10^{-7}\;, \qquad f_{\mathrm{MAR}}(T_M) \;=\; 3{,}7955 \cdot 10^{-9}\,\tfrac{1}{\mathrm{h}}\;. \tag{6.15}$$

Eine qualitative Analyse, z. B. Minimalschnittanalyse, ist bei dieser Methode nicht möglich.

Im Vergleich mit der Fehlerbaum Modellierung (in allen Ausprägungen) zeigt sich die Komplexität der Markov Methode, die der praxistauglichen Modellierung vieler realer Systeme im Wege steht.

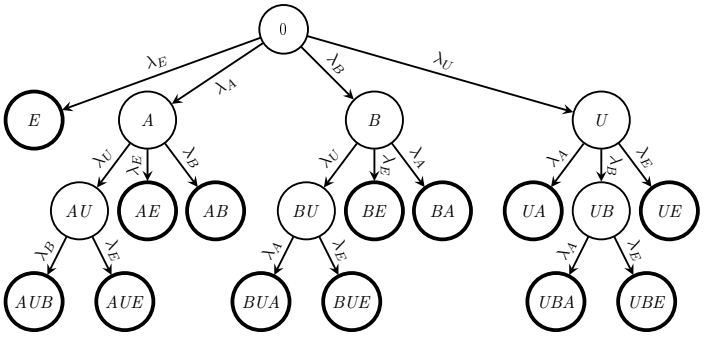


Abbildung 6.5: Markov Diagramm (und zugleich sequentieller Ausfallbaum) zum Beispielsystem. Die Zustände des Systemausfalls „Keine Energie an X“ sind fett markiert.

6.5 Vergleichsmodellierung: Dynamische FTA mit TFTA Ansatz

Die Modellierung des Beispielsystems mit einem temporalen Fehlerbaum der TFTA ergibt den in Abbildung 6.6 gezeigten Fehlerbaum. Einer der wesentlichen Vorteile der TFTA gegenüber der DFT ist die Art und Weise, wie beim Aufbau der Fehlerbaum-Struktur vorgegangen werden kann. Wie bei der herkömmlichen Booleschen FTA ist es möglich, sich „Schaltplan-orientiert“ vom Aktuator ausgehend dem Signalpfad rückwärts folgend bis zu den Eingängen des Systems vorzuarbeiten. Dieses Vorgehen ist einerseits sehr intuitiv und andererseits auch sehr systematisch, wodurch Modellierungsfehler reduziert werden. Auftretende Vermaschungen im Fehlerbaum werden durch die temporale Logik aufgelöst. Dieses Vorgehen ist im Allgemeinen beim DFT Ansatz auf Grund der Modulbildung nicht anwendbar.

Qualitative und quantitative Berechnung

Die temporale Systemfunktion des in Abbildung 6.6 gezeigten temporalen Fehlerbaums ist

$$\begin{aligned}\varpi &= (A \vee E) \wedge \big(B \vee E \vee (U \,\vec{\wedge}\, A)\big) = \\ &= \big[A \wedge B\big] \vee \big[A \wedge E\big] \vee \big[A \wedge (U \,\vec{\wedge}\, A)\big] \vee \big[E \wedge B\big] \vee \big[E\big] \vee \big[E \wedge (U \,\vec{\wedge}\, A)\big] = \\ &= \big[A \wedge B\big] \vee \big[U \,\vec{\wedge}\, A\big] \vee \big[E\big] \ . \end{aligned} \tag{6.16}$$

Diese drei Ereignissequenzen sind bereits minimal, da nach Kapitel 4.3.2 gilt, dass

$$\big[A \wedge B\big] \not\supseteq \big[U \,\vec{\wedge}\, A\big] \qquad \text{und} \qquad \big[A \wedge B\big] \not\supseteq \big[E\big] \qquad \text{und} \qquad \big[E\big] \not\supseteq \big[U \,\vec{\wedge}\, A\big] \ .$$

Die Ereignissequenzen sind also zugleich MCSS und somit Ausgangsbasis für weiterführende qualitative Auswertungen. Die qualitative Analyse der MCSS zeigt, dass die MCSS korrekt berechnet werden und die Sequenzinformation zwischen U und A enthalten.

Für die weitere quantitative Analyse sind die MCSS in eine disjunkte Form zu überführen. Die Umformung gemäß Kapitel 4.3.3 ergibt eine erweiterte TDNF mit disjunkten Termen:

$$\varpi = \big[\neg E \wedge (A \wedge B)\big] \vee \big[\neg B \, \neg E \wedge (U \,\vec{\wedge}\, A)\big] \vee \big[E\big] \qquad . \tag{6.17}$$

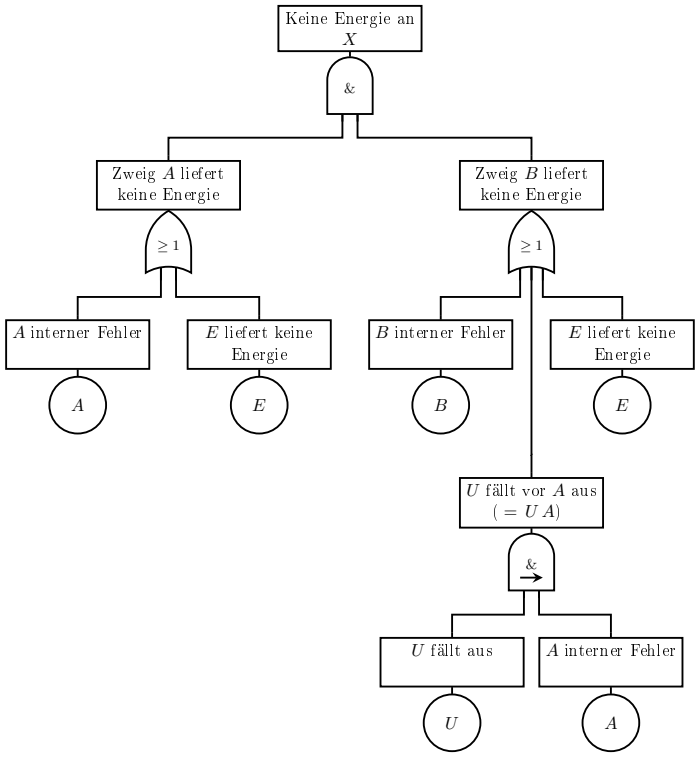


Abbildung 6.6: TFTA Fehlerbaum des Beispielsystems. Dieser berücksichtigt korrekt die Vermaschung des Ereignisses A sowie die Sequenzinformation zwischen U und A und ermöglicht zudem eine „Schaltplan-orientierte“ Fehlerbaum-Erstellung. Quantitativ ergibt sich die korrekte Lösung.

Diese lässt sich mit den Komponenten-Daten von Seite 82 direkt quantifizieren:

$$\begin{aligned} F_{TFTA}(t) &= \big(1 - F_E(t)\big) \cdot F_A(t) \cdot F_B(t) + \\ &\quad + \big(1 - F_E(t)\big)\big(1 - F_B(t)\big) \cdot \int_0^t F_U(\tau) \cdot f_A(\tau) \cdot \mathrm{d}\,\tau + F_E(t) \ , \\ F_{TFTA}(T_M) &= 9{,}5940 \cdot 10^{-7} \ , \qquad (6.18) \\ f_{TFTA}(t) &= \big(1 - F_E(t)\big) \cdot f_A(t) \cdot F_B(t) + \big(1 - F_E(t)\big) \cdot F_A(t) \cdot f_B(t) + \\ &\quad + \big(1 - F_E(t)\big)\big(1 - F_B(t)\big) \cdot F_U(t) \cdot f_A(t) + f_E(t) \\ f_{TFTA}(T_M) &= 3{,}7955 \cdot 10^{-9} \tfrac{1}{\mathrm{h}} \ . \qquad (6.19) \end{aligned}$$

Der Vergleich zu den Referenz-Ergebnissen aus der Markov Modellierung in Kapitel 6.4 zeigt, dass die TFTA auch quantitativ die exakten Ergebnisse berechnet.

Näherungsverfahren

Anstelle der exakten Berechnung lassen sich die TOP Ausfallkenngrößen auch mit dem Ansatz mit minimiertem Rechenaufwand aus Kapitel 5.5 ermitteln.

Im ersten Ansatz wird dieses Verfahren auf die erweiterte TDNF der temporalen Ausfallfunktion mit disjunkten Termen aus (6.17) angewandt. Dies ergibt mit $T_M = 400\mathrm{h}$

$$F_{TFTA}(t) \approx (1 - \lambda_E\, t) \cdot \lambda_A\, t \cdot \lambda_B\, t + \frac{1}{2}(1 - \lambda_E\, t)(1 - \lambda_B\, t) \cdot \lambda_U\, t \cdot \lambda_A\, t + \lambda_E\, t \ ,$$

$$F_{TFTA}(T_M) = 9{,}5984 \cdot 10^{-7} \,, \tag{6.20}$$

$$f_{TFTA}(t) \approx 2(1-\lambda_E\, t)\cdot\lambda_A\cdot\lambda_B\, t + \frac{1}{2}(1-\lambda_E\, t)(1-\lambda_B\, t)\cdot\lambda_U\cdot\lambda_A\, t + \lambda_E \,,$$

$$f_{TFTA}(T_M) = 3{,}7988 \cdot 10^{-7}\, \tfrac{1}{\mathrm{h}} \,. \tag{6.21}$$

Eine weitere deutliche Vereinfachung ergibt sich, wenn anstelle der temporalen Ausfallfunktion aus (6.17) die Form aus (6.16) verwendet wird. So folgt aus (6.16) die Quantifizierung mit

$$F_{TFTA}(t) \approx \lambda_A\, t\cdot\lambda_B\, t + \frac{1}{2}\,\lambda_U\, t\cdot\lambda_A\, t + \lambda_E\, t \,,$$

$$F_{TFTA}(T_M) \approx 9{,}6000 \cdot 10^{-7} \,, \tag{6.22}$$

$$f_{TFTA}(t) \approx 2\,\lambda_A\cdot\lambda_B\, t + \frac{1}{2}\,\lambda_U\cdot\lambda_A\, t + \lambda_E \,,$$

$$f_{TFTA}(T_M) \approx 3{,}8000 \cdot 10^{-7}\, \tfrac{1}{\mathrm{h}} \,. \tag{6.23}$$

Einerseits ist es damit nicht notwendig, die mitunter sehr aufwändige Überführung in eine disjunkte Form vorzunehmen. Andererseits ergeben sich konservative Näherungswerte, die zumindest für eine Erstabschätzung im Rahmen mehrstufiger Analysen oftmals exakt genug sind.

Cutsets/Sequ.	Bool 1	Bool 2	DFT 1	DFT 2	Markov	TFTA
1.	E	E	E	E	–	E
2.	$A \wedge U$	U	$U \wedge A$	$U \wedge A$	–	$U \vec{\wedge} A$
3.	$A \wedge B$	$A \wedge B$	$A \wedge B$	$A^\star \wedge B$	–	$A \wedge B$

Tabelle 6.1: Vergleich der qualitativen Ergebnisse der einzelnen Modellierungen des Beispielsystems aus Kapitel 6.1. Die Minimalschnitte der „Bool ...“ und „DFT ...“ Modellierungen enthalten keine Sequenzinformationen. Es werden daher Systemausfälle für Ausfall-Kombinationen berechnet, die real nicht zum Ausfall des Systems führen. Die Ergebnisse von „Bool 2“ und „DFT 2“ weichen besonders von der korrekten Lösung, dargestellt durch die MCSS der TFTA, ab. Die „Markov“ Methode liefert keine vergleichbaren qualitativen Ergebnisse.

6.6 Zusammenfassung der Ergebnisse

Der direkte Vergleich zwischen Boolescher FTA, dem DFT Ansatz, einer Markov Modellierung und dem neuen TFTA Ansatz zeigt, dass die TFTA die Vorteile der verschiedenen herkömmlichen Methoden verbindet und sogar über diese hinausgeht.

So übernimmt sie die grundsätzlichen Vorgehensweisen zur Erstellung von Fehlerbäumen von der Booleschen FTA. Insbesondere ist es auch bei der TFTA möglich, „Schaltplan-orientiert“ vorzugehen, wodurch ein hoher Grad an Systematik und wenige Modellierungsfehler sichergestellt sind. Die grundsätzlichen Vorgehensweisen zur qualitativen wie quantitativen Auswertung des Fehlerbaums sind ebenfalls sehr ähnlich. Auf die qualitative Vereinfachung der Ausfallfunktion hin zu einer minimalen DNF folgt einerseits die weitere qualitative Auswertung und andererseits die Überführung in disjunkte Teilterme, die anschließend direkt quantifizierbar sind. Anders als die Boolesche FTA berücksichtigt die TFTA jedoch qualitativ und quantitativ die Sequenzinformationen zwischen den einzelnen Ereignissen.

Methode	$F(T_M)$ [.] = 1	$f(T_M)$ [.] = $\frac{1}{\text{h}}$	$\lambda(T_M)$ [.] = $\frac{1}{\text{h}}$
Bool 1	$1{,}3587 \cdot 10^{-6}$	$5{,}7899 \cdot 10^{-9}$	$5{,}7899 \cdot 10^{-9}$
Bool 2	$1{,}9986 \cdot 10^{-3}$	$4{,}9918 \cdot 10^{-6}$	$5{,}0019 \cdot 10^{-6}$
DFT 1	$8{,}7933 \cdot 10^{-7}$	$3{,}3946 \cdot 10^{-9}$	$3{,}3946 \cdot 10^{-9}$
DFT 2	$9{,}5962 \cdot 10^{-7}$	$3{,}7967 \cdot 10^{-9}$	$3{,}7967 \cdot 10^{-9}$
Markov	$9{,}5940 \cdot 10^{-7}$	$3{,}7955 \cdot 10^{-9}$	$3{,}7955 \cdot 10^{-9}$
TFTA	$9{,}5940 \cdot 10^{-7}$	$3{,}7955 \cdot 10^{-9}$	$3{,}7955 \cdot 10^{-9}$
TFTA (Approx. 1)	$9{,}5984 \cdot 10^{-7}$	$3{,}7988 \cdot 10^{-9}$	$3{,}7988 \cdot 10^{-9}$
TFTA (Approx. 2)	$9{,}6000 \cdot 10^{-7}$	$3{,}8000 \cdot 10^{-9}$	$3{,}8000 \cdot 10^{-9}$

Tabelle 6.2: Übersicht der quantitativen Ergebnisse der Vergleichsmodellierungen aus Kapitel 6.2 bis 6.5 für eine Missionszeit von $T_M = 400$h. Deutlich zu erkennen sind die vergleichsweise konservativen Ergebnisse der Booleschen Modellierungen. Die Markov Modellierung dient als Referenz. Die TFTA liefert dieselben, d. h. die korrekten Werte. Die letzten zwei Zeilen zeigen die Ergebnisse für das Näherungsverfahren der quantitativen TFTA. „Approx 1“ quantifiziert die in disjunkte temporale Minterme überführte temporale Ausfallfunktion, „Approx 2“ quantifiziert die temporale Ausfallfunktion in TDNF vor der Umformung in disjunkte Minterme, vgl. (6.20) bis (6.23).

Hinsichtlich der qualitativen Ergebnisse liefert die TFTA als einzige Methode die für den Systemausfall minimal notwendigen Komponentenausfälle unter Berücksichtigung der Sequenzinformationen, vgl. Tabelle 6.1. Die DFT und die herkömmliche FTA liefern stattdessen Minimalschnitte ohne Sequenzinformation. Im Fall der DFT ist zudem die Modulbildung zu beachten: Vermaschungen zwischen Booleschen und dynamischen Modulen können zu schwer entdeckbaren Modellierungsfehlern führen und dabei insbesondere die quantitativen Ergebnisse verfälschen. Die Auflösung existierender Vermaschungen durch Verwendung mehrerer „gleicher“ Ereignisse für dasselbe reale Ausfallereignis liefert zwar quantitativ gute Näherungswerte, reduziert aber andererseits die Aussagekraft der qualitativen Ergebnisse durch unsinnige oder gar unmögliche Ausfallkombinationen.

Die quantitative Berechnung der TFTA liefert die korrekten Ausfallkenngrößen auf TOP Ebene, wie der direkte Vergleich mit der Markov Referenz-Modellierung zeigt, vgl. Tabelle 6.2. Im Gegensatz dazu sind die rein Booleschen Modellierungen teilweise sehr konservativ. Die DFT liefert korrekte Ergebnisse nur für solche Fehlerbäume, in denen es keine Vermaschungen zwischen Booleschen und dynamischen Modulen gibt. Sind Vermaschungen unvermeidlich, so führt dies i. d. R. sogar zu optimistischen Werten.

Durch den Ansatz mit minimiertem Rechenaufwand eignet sich die TFTA auch für eine mehrstufige Modellierung, in der sowohl der Aufwand als auch die Ergebnisgenauigkeit sukzessive erhöht werden. Sie liefert damit bei deutlich reduziertem Aufwand für die quantitative Berechnung weiterhin die minimalen Ausfallsequenzen.

7 TFTA Modellierung einer typischen KFZ Steuergeräte-Architektur

Insight separated from practice
remains ineffective.

(Erich Fromm)

Dieses Kapitel wendet die TFTA-Methode auf ein praxisnahes System an und zeigt, dass sich die TFTA auch für deutlich komplexere Fälle als die bisher diskutierten Minimalbeispiele eignet.

7.1 Das Beispiel

Das Beispielsystem in Abbildung 7.1 stellt die Abstraktion einer Systemarchitektur dar, wie sie im automotiven Umfeld typischerweise für sicherheitsrelevante Systeme mit Anforderungen bis SIL 3 gemäß IEC 61508 bzw. ASIL D gemäß ISO 26262 zum Einsatz kommen könnte.

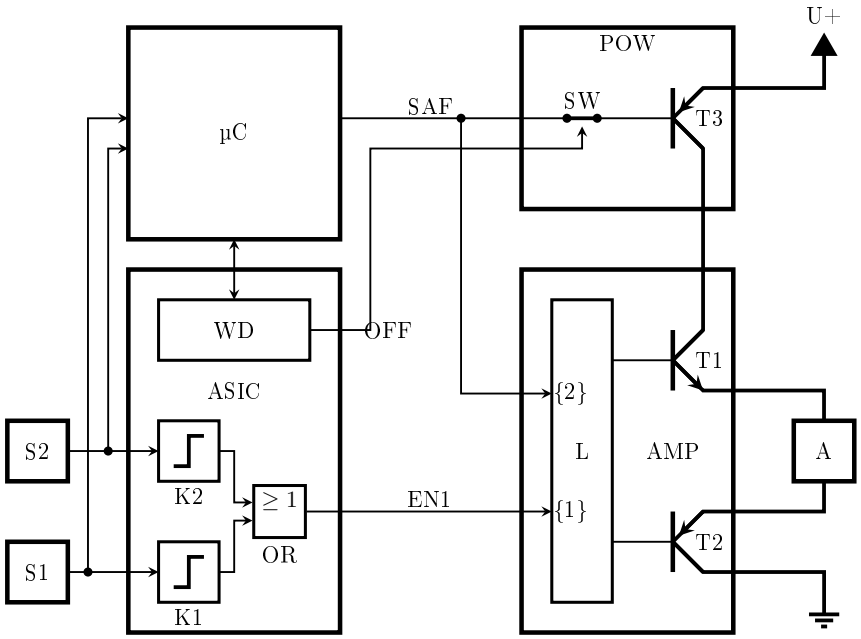


Abbildung 7.1: Ein praxisnahes System, das mittels TFTA analysiert wird.

Zum weiteren Aufbau dieses Kapitels: Kapitel 7.2 zeigt den temporalen Fehlerbaum zu diesem System. Es folgt die qualitative Analyse in Kapitel 7.3 sowie die quantitative Auswertung in Kapitel 7.4. Kapitel 7.5 diskutiert die Ergebnisse.

7.1.1 Systembeschreibung, Sicherheitsziel und sicherer Zustand

Betrachtungsrahmen

Das Beispielsystem besteht aus den in Tabelle 7.1 aufgeführten Komponenten und Signalen.

Komponente	Subkomponente	Beschreibung
S1		Sensor 1
S2		Sensor 2
µC		Microcontroller
ASIC		System-ASIC
	WD	Watchdog für µC
	K1	Komparator 1
	K2	Komparator 2
	OR	ODER Gatter
POW		Power-Schalter
	SW	Notaus-Schalter
	T3	Power-Transistor
AMP		Treiber-IC
	L	Logikbaustein
	T1	High-Side Endstufe
	T2	Low-Side Endstufe
A		Aktuator
Signale		**Beschreibung**
EN		Enable für Logik im Treiber-IC
SAF		Enable für Power-Transistor und Schaltbefehl für Treiber-IC
OFF		Disable (Notaus) via Watchdog

Tabelle 7.1: Komponenten und Signale des Beispielsystems aus Abbildung 7.1

Funktionale Beschreibung / Sicherheitskonzept

Das Beispielsystem dient dazu, einen Aktuator A auf Basis von Sensorinformationen sicher anzusteuern. Der Aktuator ist genau dann zu aktivieren, wenn die Sensorinformationen einen bestimmten Schwellwert überschreiten. Unterschreiten die Sensorinformationen den Schwellwert, so ist der Aktuator zu deaktivieren. Zur Erhöhung der funktionalen Sicherheit besitzt das System mehrere Redundanz-Maßnahmen.

Die beiden Sensoren S1 und S2 nehmen physikalische Umgebungsgrößen auf. Jeder Sensor sendet seine Messwerte über eine eigene serielle Schnittstelle an den Microcontroller µC und den System-ASIC. Diese Übertragung ist mittels CRC und Alive-Zählern abgesichert.

Der Microcontroller µC wertet die Sensorinformationen der zwei getrennten Sensoren S1 und S2 aus. Unterschreitet mindestens einer der aufgenommenen Sensorwerte den Schwellwert, so wird der µC Ausgang SAF deaktiviert. Überschreiten beide aufgenommenen Sensor-Werte den Schwellwert, so aktiviert µC den Power-Transistor T3 über das SAF Signal. Zugleich aktiviert µC damit über den Enable-Eingang {2} im Treiber-IC AMP die Endstufen T1 und T2 im Treiber-

IC AMP. Der Microcontroller bedient über einen weiteren bidirektionalen Port den intelligenten Watchdog WD im System-ASIC.

Der System-ASIC wertet dieselben Sensor-Signale aus wie der Microcontroller. Er besitzt zwei Hardware-Komparatoren K1 und K2. Komparator K1 verarbeitet die Signale von Sensor S1. Komparator K2 verarbeitet die Signale von Sensor S2. Erkennt mindestens einer der beiden Hardware-Komparatoren eine Überschreitung des jeweiligen Schwellwertes, so wird der Ausgang EN aktiviert. Weiterhin enthält der System-ASIC einen intelligenten Watchdog WD. Dieser überwacht durch mehrere Mechanismen sowohl die Funktionsfähigkeit der µC Hardware als auch die korrekte Abarbeitung der Betriebs- und Applikationssoftware im µC. Dazu dient zunächst ein aufziehbarer Fenster-Watchdog mit Programmablauf-spezifischen Setzpunkten; zudem stellt WD dem µC Rechenaufgaben und überwacht die zurückgegebenen Antworten. Antwortet der µC zu früh oder zu spät oder mit einem falschen Ergebnis, so aktiviert (öffnet) WD den Notaus-Schalter SW über das OFF Signal. Ist SW offen, so ist T3 unabhängig von SAF deaktiviert und eine Stromversorgung der Endstufen und damit auch des Aktuators unterbunden.

Das Treiber-IC AMP besteht aus den beiden Endstufen T1 und T2 und einer Schaltlogik L. Die Logik L aktiviert die Endstufen genau dann, wenn zuerst der Enable-Eingang {1} und dann der Enable-Eingang {2} aktiviert werden. Jede andere Reihenfolge führt nicht zum Aktivieren der Endstufen.

Im Normalfall wird die Reihenfolge {1}, {2} eingehalten: Einerseits laufen die durch S1 und S2 aufgenommenen Messwerte nicht genau zeitgleich (z. B. wegen einer räumlichen Trennung zwischen S1 und S2). Somit wird immer zuerst Signal EN aktiviert werden, wenn der erste Sensor eine Schwellwert-Überschreitung meldet. Andererseits bringt auch der Software-Algorithmus im µC eine gewisse Latenz zu EN und sorgt intern für eine verzögerte Ansteuerung von SAF.

Sicherheitsziel, sicherer Zustand und Fehlertoleranzzeit

Die Gefahrenanalyse und Risikobewertung des Systems ergab als Sicherheitsziel das „Verhindern des fälschlichen Bestromens des Aktuators“. Der sichere Zustand zu diesem Sicherheitsziel lautet „Aktuator nicht bestromt“. Die Fehlertoleranzzeit beträgt 0 Sekunden, d. h. eine Bestromen des Aktuators ist „sofort“ gefährlich und daher auch nicht „nur kurz“ erlaubt.

7.1.2 Fehlfunktionen

Unter der vereinfachenden Annahme, dass alle Verbindungen zwischen den einzelnen Komponenten S1, S2, µC, K1, K2, WD, SW, T1, T2, T3, L, A ideal und fehlerfrei sind, verbleiben die in Tabelle 7.2 aufgeführten Fehler der einzelnen Komponenten. Deren Gefährlichkeit bezieht sich auf das Potential des Fehlers, zur Verletzung des Sicherheitsziels beizutragen. Die unter Absicherung genannten Maßnahmen verhindern eine direkte Verletzung des Sicherheitsziels durch den Fehler. Aus Sicht einer dynamischen Ausfallanalyse sind besonders zwei Bereiche des Systems interessant. Dies sind erstens die Sequenzlogik in L und zweitens die gefährlichen Ausfälle von WD (Nr. 18 in der Tabelle) und SW (Nr. 27) in Kombination mit einem Ausfall des Mikrokontrollers. Die genannten Ausfälle des Watchdogs oder des Schalters SW sind genau dann relevant, wenn mindestens einer von ihnen vor dem µC Ausfall eintritt. Fällt jedoch zuerst der µC aus und sind sowohl WD als auch SW funktionstüchtig (oder bereits „sicher“ ausgefallen), so wird davon ausgegangen, dass die Erkennung und Abschaltung stattgefunden hat. Eine weitere Gefährdung ist dann ausgeschlossen. Weiterhin werden abhängige Ausfälle, insbesondere Common Cause Failure (CCF), in diesem Beispiel nicht berücksichtigt.

Komp.	Nr.	Fehler	Fehlerfolge	gefährlich	Absicherung gegen eine direkte Verletzung des Sicherheitsziel
S1	1	liefert fälschlich Wert oberhalb Schwellwert	µC und ASIC erkennen Einschaltkriterium	ja	Einschalten des A nur wenn Zweitfehler in S2
	2	liefert fälschlich Wert unterhalb Schwellwert	µC / ASIC erkennen kein Einschaltkriterium	nein	
	3	keine Kommunikation mit µC	µC erkennt kein Einschaltkriterium	nein	
	4	keine Kommunikation mit ASIC	ASIC kann EN nur noch mit S2 aktivieren	nein	
S2	5	liefert fälschlich Wert oberhalb Schwellwert	µC und ASIC erkennen Einschaltkriterium	ja	Einschalten des A nur wenn Zweitfehler in S1
	6	liefert fälschlich Wert unterhalb Schwellwert	µC / ASIC erkennen kein Einschaltkriterium	nein	
	7	keine Kommunikation mit µC	µC erkennt kein Einschaltkriterium	nein	
	8	keine Kommunikation mit ASIC	ASIC kann EN nur noch mit S1 aktivieren	nein	
µC	9	µC bleibt stehen, Stuck-At	µC kann SAF Ausgang nicht ändern noch ASIC-WD bedienen	nein	WD erkennt µC-Fehler und öffnet Notaus
	10	Adress-, Software-Ablauf-Fehler, IO-Fehler	µC ändert SAF Ausgang beliebig; WD wird nicht korrekt bedient	ja	WD erkennt µC-Fehler und öffnet Notaus; Sequenzlogik in AMP-L verhindert Einschalten von A
	11	Eingang zu S1 Stuck-At	keine Auswertung S1	nein	
	12	Eingang zu S2 Stuck-At	keine Auswertung S2	nein	
	13	Wert von S1 wird fälschlich als oberhalb Schwellwert interpretiert	µC erkennt fälschlich Einschaltkriterium	ja	Einschalten des A nur wenn Zweitfehler in S2
	14	Wert von S1 wird fälschlich als unterhalb Schwellwert interpretiert	µC erkennt fälschlich kein Einschaltkriterium,	nein	
	15	Wert von S2 wird fälschlich als oberhalb Schwellwert interpretiert	µC erkennt fälschlich Einschaltkriterium	ja	Einschalten des A nur wenn Zweitfehler in S1
	16	Wert von S2 wird fälschlich als unterhalb Schwellwert interpretiert	µC erkennt fälschlich kein Einschaltkriterium,	nein	
	17	keine Kommunikation mit Sensoren möglich	µC erkennt kein Einschaltkriterium,	nein	
WD	18	erkennt fälschlich µC-Fehler nicht	Watchdog aktiviert Signal OFF nicht, deaktiviert nicht POW-SW	ja	Einschalten des A nur wenn Zweitfehler in AMP oder EN vor SAF aktiviert
	19	erkennt fälschlich µC-Fehler	Watchdog aktiviert Signal OFF öffnet Notaus, keine Versorgung von AMP (= sicherer Zustand)	nein	
K1	20	erkennt fälschlich einen Wert von S1 unterhalb Schwellwert als oberhalb Schwellwert	ASIC aktiviert EN	ja	Einschalten nur mit Zweitfehler in µC oder AMP
	21	erkennt fälschlich einen Wert von S1 oberhalb Schwellwert als unterhalb Schwellwert	ASIC aktiviert EN nicht,	nein	
K2	22	erkennt fälschlich einen Wert von S2 unterhalb Schwellwert als oberhalb Schwellwert	ASIC aktiviert EN	ja	Einschalten nur mit Zweitfehler in µC oder AMP
	23	erkennt fälschlich einen Wert von S2 oberhalb Schwellwert als unterhalb Schwellwert	ASIC aktiviert EN nicht,	nein	
OR	24	Erkennt fälschlich eine Schaltaufforderung ohne Aufforderung durch ASIC-K1 oder K2	ASIC aktiviert EN	ja	Einschalten nur mit Zweitfehler in µC oder AMP
	25	Erkennt fälschlich keine Schaltaufforderung trotz Aufforderung durch ASIC-K1 oder K2	ASIC aktiviert EN nicht,	nein	
SW	26	öffnet Notaus fälschlich ohne Aktivierung	kein Schalten von T3, wenn SAF aktivert,	nein	
	27	öffnet Notaus fälschlich nicht trotz Signal OFF	Schalten von T3	ja	Einschalten des Aktuators nur mit fälschlich aktiviertem E2 und sonstigem Mehrfachfehler in ASIC oder AMP
T3	28	schaltet fälschlich ohne Anf. von SAF	Energieversorgung liegt an High-Side-Treiber T1	ja	Einschalten des Aktuators nur mit fälschlich aktiviertem SAF und sonstigem Mehrfachfehler in ASIC oder AMP
	29	schaltet fälschlich nicht trotz Anf. von SAF	Keine Energieversorgung an T1,	nein	
T1	30	schaltet fälschlich ohne Anf. von AMP-L	Ausgang T3 zu Aktuator durchgeschaltet	ja	Einschalten des Aktuators nur wenn fälschliches Schalten von T2 und sonstiger Mehrfachfehler in µC oder POW
	31	schaltet fälschlich nicht trotz Anf. von AMP-L	Aktuator wird nicht mit Energie versorgt,	nein	
T2	32	schaltet fälschlich ohne Anf. von AMP-L	Masse zu Aktuator durchgeschaltet	ja	Einschalten des Aktuators nur wenn fälschliches Schalten von T1 und sonstiger Mehrfachfehler in µC oder POW
	33	schaltet fälschlich nicht trotz Anf. von AMP-L	Aktuator hat keine Masseverbindung,	nein	
L	34	aktiviert fälschlich AMP-T1 ohne Anf.	s. 30	ja	s. 30
	35	aktiviert fälschlich AMP-T1 nicht trotz Anf.	s. 31	nein	
	36	aktiviert fälschlich AMP-T2 ohne Anf.	s. 32	ja	s. 32
	37	aktiviert fälschlich AMP-T2 nicht trotz Anf.	s. 33	nein	
	38	aktiviert fälschlich AMP-T1 und T2 ohne Anf.	Ausgang T3 zu Aktuator durchgeschaltet und Aktuator zu Masse durchgeschaltet	ja	Einschalten des Aktuators nur in Kombination mit Zweitfehler in µC oder POW
A	39	keine Aktion trotz geschalteter Versorgung	sicherer Zustand	nein	

Tabelle 7.2: Übersicht der möglichen Fehler des Beispielsystems aus Abbildung 7.1.

Die Fehler des µC lassen sich nicht eindeutig bestimmten Hardware-Fehlern zuordnen, da die Funktionalität des µC wesentlich in Software realisiert ist. Es wird angenommen, dass die einzelnen Fehler des µC (Nr. 9 bis 17 in Tabelle 7.2) unabhängig voneinander eintreten.

7.2 Temporaler Fehlerbaum

Für das Beispielsystem ist ein temporaler Fehlerbaum zu erstellen. Dieser soll dem Nachweis dienen, dass keine gefährlichen Einzelfehler zu einer Verletzung des Sicherheitsziels führen („Einfehler-Festigkeit“). Weiterhin sollen mit einer MCSS-Analyse die wichtigsten Kombinationen gefährlicher Fehler erfasst werden. Darüber hinaus ist durch eine Quantifizierung der Nachweis zu erbringen, dass das Systems die für ASIL D in ISO 26262 definierte Gefährdungsrate unterschreitet.

Das TOP-Ereignis des Fehlerbaums ist die „Verletzung des Sicherheitsziels“, also das „Fälschliche Bestromen des Aktuators“. Die im System vorhandenen Zeitabhängigkeiten zwischen den Komponentenausfällen erfordern es, im Fehlerbaum temporale Gatter zu verwenden. Die Abbildungen 7.2 bis 7.4 zeigen den temporalen Fehlerbaum zum Beispielsystem in drei Teilen. Die Nummern der Basisereignisse beziehen sich auf Tabelle 7.2.

Insgesamt besteht der temporale Fehlerbaum aus 32 Gattern und 34 Basisereignissen. Es gibt 16 vermaschte Gatter und 18 vermaschte Basisereignisse. Zwei der Gatter sind PAND Gatter, die über Vermaschungen insgesamt dreimal vorkommen. Unter diesen temporalen Gattern befinden sich Teil-Fehlerbäume mit 10 unterschiedlichen Basisereignissen und zehn unterschiedlichen Gattern.

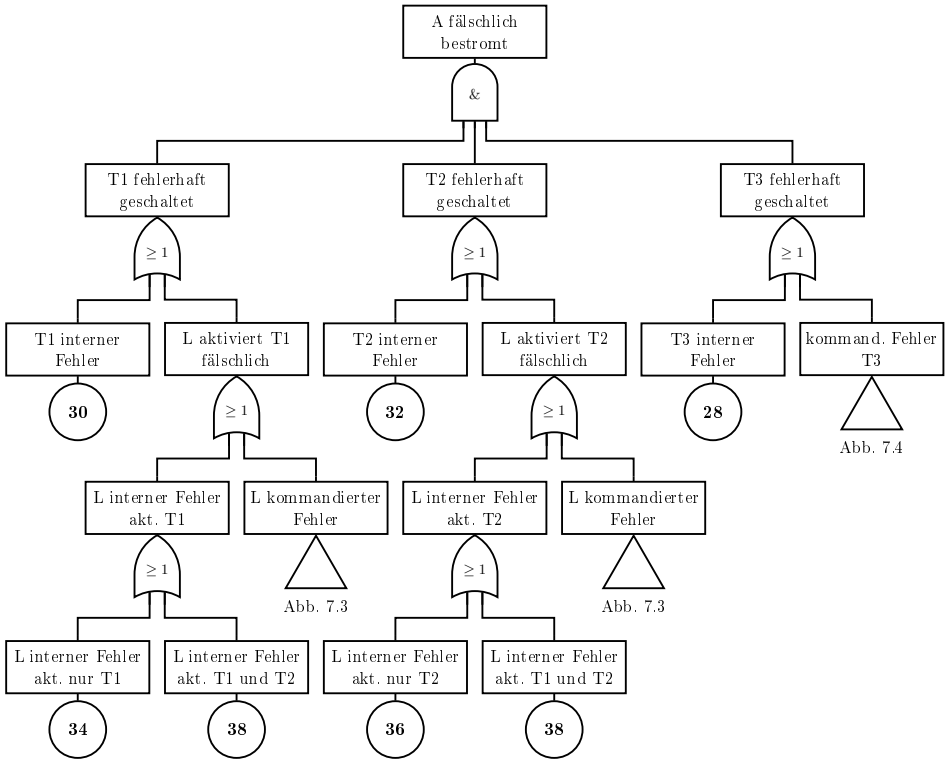


Abbildung 7.2: Fehlerbaum zum Beispielsystem aus aus Abbildung 7.1, Teil 1. Die Fehler-Nummern der Basisereignisse beziehen sich auf Tabelle 7.2.

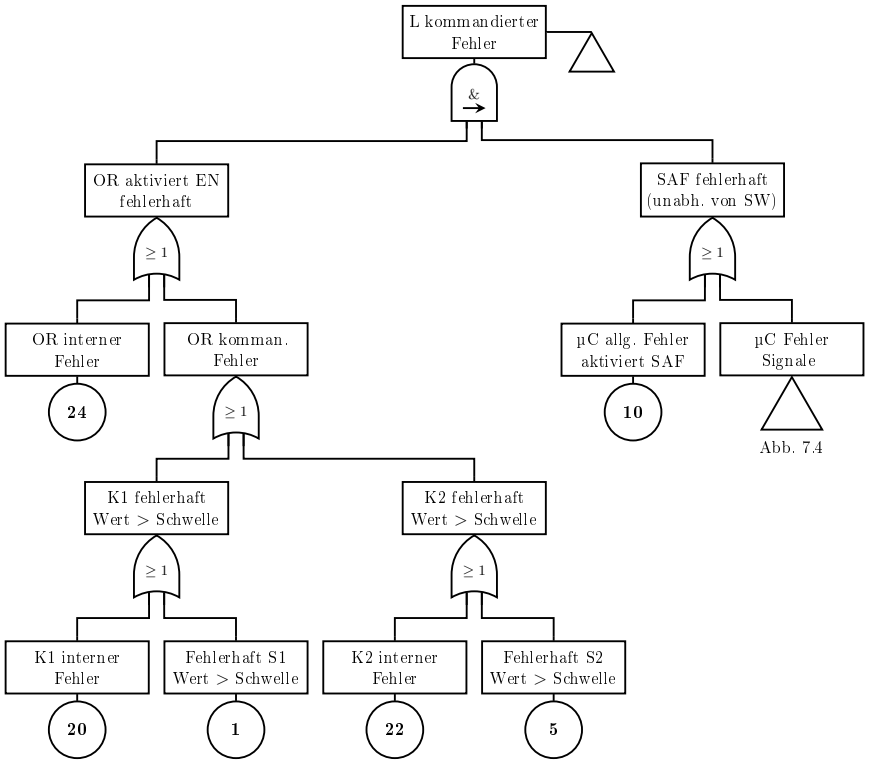


Abbildung 7.3: Fehlerbaum zum Beispielsystem aus aus Abbildung 7.1, Teil 2.

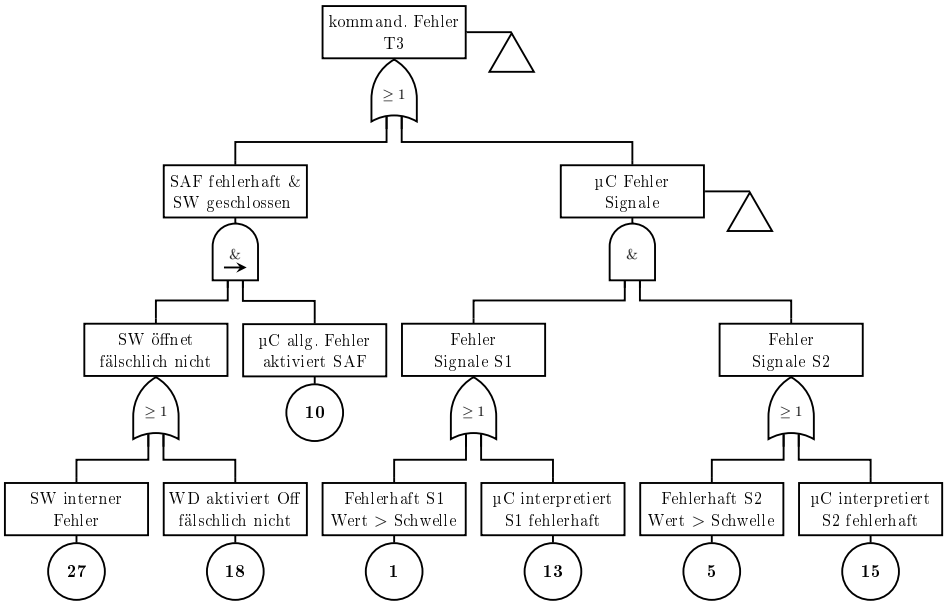


Abbildung 7.4: Fehlerbaum zum Beispielsystem aus aus Abbildung 7.1, Teil 3.

7.3 Qualitative Auswertung des temporalen Fehlerbaums

7.3.1 Temporale Ausfallfunktion

Aus den Fehlerbäumen in Abbildung 7.2 bis 7.4 lässt sich die temporale Ausfallfunktion des TOP direkt ablesen. Sie lautet

$$\begin{aligned}\varpi \;=\; & \Bigg(X_{30} \vee X_{34} \vee X_{38} \vee \Big[\Big(\underbrace{X_{24} \vee X_{20} \vee X_1 \vee X_{22} \vee X_5}_{A} \Big) \vec{\wedge} \\ & \qquad \vec{\wedge} \Big(\underbrace{X_{10} \vee [(X_1 \vee X_{13}) \wedge (X_5 \vee X_{15})]}_{B} \Big) \Big] \Bigg) \wedge \\ & \wedge \Bigg(X_{32} \vee X_{36} \vee X_{38} \vee \Big[A \vec{\wedge} B \Big] \Bigg) \wedge \\ & \wedge \Bigg(\underbrace{X_{28} \vee [(X_1 \vee X_{13}) \wedge (X_5 \vee X_{15})] \vee \Big[(X_{27} \vee X_{18}) \vec{\wedge} X_{10} \Big]}_{C} \Bigg) \; . \end{aligned} \tag{7.1}$$

Die Substitutionen A, B, C erleichtern die Vereinfachung:

$$\begin{aligned}\varpi \;=\; & \Big(X_{30} \vee X_{34} \vee X_{38} \vee \big[A \vec{\wedge} B \big] \Big) \wedge \Big(X_{32} \vee X_{36} \vee X_{38} \vee \big[A \vec{\wedge} B \big] \Big) \wedge \Big(C \Big) \; = \\ =\; & \big[X_{30} \wedge X_{32} \wedge C \big] \vee \big[X_{30} \wedge X_{36} \wedge C \big] \vee \big[X_{30} \wedge X_{38} \wedge C \big] \vee \big[X_{30} \wedge (A \vec{\wedge} B) \wedge C \big] \vee \\ & \vee \big[X_{34} \wedge X_{32} \wedge C \big] \vee \big[X_{34} \wedge X_{36} \wedge C \big] \vee \big[X_{34} \wedge X_{38} \wedge C \big] \vee \big[X_{34} \wedge (A \vec{\wedge} B) \wedge C \big] \vee \\ & \vee \big[X_{38} \wedge X_{32} \wedge C \big] \vee \big[X_{38} \wedge X_{36} \wedge C \big] \vee \big[X_{38} \wedge X_{38} \wedge C \big] \vee \big[X_{38} \wedge (A \vec{\wedge} B) \wedge C \big] \vee \\ & \vee \big[(A \vec{\wedge} B) \wedge X_{32} \wedge C \big] \vee \big[(A \vec{\wedge} B) \wedge X_{36} \wedge C \big] \vee \big[(A \vec{\wedge} B) \wedge X_{38} \wedge C \big] \vee \\ & \vee \big[(A \vec{\wedge} B) \wedge (A \vec{\wedge} B) \wedge C \big] \; . \end{aligned} \tag{7.2}$$

Mit Hilfe der Absorptions- und Idempotenzgesetze vereinfacht sich dies zu

$$\begin{aligned}\varpi \;=\; & \big[X_{30} \wedge X_{32} \wedge C \big] \vee \big[X_{30} \wedge X_{36} \wedge C \big] \vee \big[X_{34} \wedge X_{32} \wedge C \big] \vee \\ & \vee \big[X_{34} \wedge X_{36} \wedge C \big] \vee \big[X_{38} \wedge C \big] \vee \big[(A \vec{\wedge} B) \wedge C \big] \; . \end{aligned} \tag{7.3}$$

Das folgende Kapitel formt die temporale Ausfallfunktion aus (7.3) gemäß der Regeln der temporalen Logik um. Die so bestimmten MCSS zu ϖ werden in Kapitel 7.3.3 analysiert.

7.3.2 Umformung gemäß der Regeln der temporalen Logik

MCSS der ersten fünf Teilterme in (7.3):
Die temporale Ausfallfunktion in (7.3) enthält fünf Teilterme

$$\big[X_{30} \wedge X_{32} \wedge C \big], \big[X_{30} \wedge X_{36} \wedge C \big], \big[X_{34} \wedge X_{32} \wedge C \big], \big[X_{34} \wedge X_{36} \wedge C \big], \big[X_{38} \wedge C \big] \tag{7.4}$$

ohne Bezug zu A. Die Basisereignisse $X_{30}, X_{32}, X_{34}, X_{36}, X_{38}$ sind nicht auch in C enthalten. Jeder der fünf Teilterme ergibt in Kombination mit der TDNF von C, also

$$C \;=\; X_{28} \vee (X_1 X_5) \vee (X_1 X_{15}) \vee (X_5 X_{13}) \vee (X_{13} X_{15}) \vee (X_{27} \vec{\wedge} X_{10}) \vee (X_{18} \vec{\wedge} X_{10}) \; , \tag{7.5}$$

neun verschiedene Ereignissequenzen, wie hier am Beispiel von $X_{38} \wedge C$ gezeigt:

$$X_{38} \wedge C = X_{38} \wedge \big[X_{28} \vee (X_1 X_5) \vee (X_1 X_{15}) \vee (X_5 X_{13}) \vee (X_{13} X_{15}) \vee \vee (X_{27} \vec{\wedge} X_{10}) \vee (X_{18} \vec{\wedge} X_{10})\big] \; . \tag{7.6}$$

Daraus resultieren zunächst folgende fünf Ereignissequenzen:

$$\big[X_{38} X_1 X_5\big], \big[X_{38} X_1 X_{15}\big], \big[X_{38} X_5 X_{13}\big], \big[X_{38} X_{13} X_{15}\big], \big[X_{28} X_{38}\big] \; . \tag{7.7}$$

Hinzu kommen vier Ereignissequenzen (ohne SAND Verknüpfungen) aus $X_{38} \wedge (X_{18} \vec{\wedge} X_{10})$ und $X_{38} \wedge (X_{27} \vec{\wedge} X_{10})$:

$$\big[(X_{18} X_{38}) \vec{\wedge} X_{10}\big], \big[X_{18} \vec{\wedge} X_{10} \vec{\wedge} X_{38}\big], \big[(X_{27} X_{38}) \vec{\wedge} X_{10}\big], \big[X_{27} \vec{\wedge} X_{10} \vec{\wedge} X_{38}\big] \; . \tag{7.8}$$

Insgesamt ergeben sich somit 45 Ereignissequenzen, vgl. Tabelle 7.3.

(erweiterte) MCSS von Rang zwei:	
1: $X_{28} X_{38}$	
(erweiterte) MCSS von Rang drei:	
1: $X_{28} X_{30} X_{32}$	7: $X_{28} X_{30} X_{36}$
2: $X_{28} X_{32} X_{34}$	8: $X_{28} X_{34} X_{36}$
3: $X_{18} \vec{\wedge} X_{10} \vec{\wedge} X_{38}$	9: $X_{27} \vec{\wedge} X_{10} \vec{\wedge} X_{38}$
4: $(X_{18} X_{38}) \vec{\wedge} X_{10}$	10: $(X_{27} X_{38}) \vec{\wedge} X_{10}$
5: $X_{38} X_1 X_5$	11: $X_{38} X_1 X_{15}$
6: $X_{38} X_5 X_{13}$	12: $X_{38} X_{13} X_{15}$
(erweiterte) MCSS von Rang vier:	
1: $X_1 X_5 X_{30} X_{32}$	17: $X_1 X_5 X_{30} X_{36}$
2: $X_1 X_{15} X_{30} X_{32}$	18: $X_1 X_{15} X_{30} X_{36}$
3: $X_{13} X_5 X_{30} X_{32}$	19: $X_{13} X_5 X_{30} X_{36}$
4: $X_{13} X_{15} X_{30} X_{32}$	20: $X_{13} X_{15} X_{30} X_{36}$
5: $X_1 X_5 X_{32} X_{34}$	21: $X_1 X_5 X_{34} X_{36}$
6: $X_1 X_{15} X_{32} X_{34}$	22: $X_1 X_{15} X_{34} X_{36}$
7: $X_{13} X_5 X_{32} X_{34}$	23: $X_{13} X_5 X_{34} X_{36}$
8: $X_{13} X_{15} X_{32} X_{34}$	24: $X_{13} X_{15} X_{34} X_{36}$
9: $X_{18} \vec{\wedge} X_{10} \vec{\wedge} (X_{30} X_{32})$	25: $X_{27} \vec{\wedge} X_{10} \vec{\wedge} (X_{30} X_{32})$
10: $X_{18} \vec{\wedge} X_{10} \vec{\wedge} (X_{30} X_{36})$	26: $X_{27} \vec{\wedge} X_{10} \vec{\wedge} (X_{30} X_{36})$
11: $X_{18} \vec{\wedge} X_{10} \vec{\wedge} (X_{32} X_{34})$	27: $X_{27} \vec{\wedge} X_{10} \vec{\wedge} (X_{32} X_{34})$
12: $X_{18} \vec{\wedge} X_{10} \vec{\wedge} (X_{34} X_{36})$	28: $X_{27} \vec{\wedge} X_{10} \vec{\wedge} (X_{34} X_{36})$
13: $(X_{18} X_{30} X_{32}) \vec{\wedge} X_{10}$	29: $(X_{27} X_{30} X_{32}) \vec{\wedge} X_{10}$
14: $(X_{18} X_{30} X_{32}) \vec{\wedge} X_{10}$	30: $(X_{27} X_{30} X_{32}) \vec{\wedge} X_{10}$
15: $(X_{18} X_{32} X_{34}) \vec{\wedge} X_{10}$	31: $(X_{27} X_{32} X_{34}) \vec{\wedge} X_{10}$
16: $(X_{18} X_{34} X_{36}) \vec{\wedge} X_{10}$	32: $(X_{27} X_{34} X_{36}) \vec{\wedge} X_{10}$

Tabelle 7.3: MCSS mit Rang zwei, drei und vier, die sich aus den ersten fünf Teiltermen in (7.3) ergeben.

Vereinfachung von $\mathbf{A} \vec{\wedge} \mathbf{B}$:
Zunächst ist $A \vec{\wedge} B$ zu lösen. Aus Platzgründen werden hier nur die ersten Umformungsschritte gezeigt, die für das Verständnis notwendig sind. B lässt sich in folgende DNF überführen:

$$B = X_{10} \vee (X_1 X_5) \vee (X_1 X_{15}) \vee (X_5 X_{13}) \vee (X_{13} X_{15}) = X_{10} \vee \eta \; . \tag{7.9}$$

Nach dem temporalen Distributivgesetz für temporale Terme vom Typ I aus (4.76) gilt

$$\begin{aligned} A \,\vec{\wedge}\, B \;=\; & \big[\neg\,\eta \wedge (A \,\vec{\wedge}\, X_{10})\big] \vee \big[\neg\, X_{10} \wedge (A \,\vec{\wedge}\, \eta)\big] \vee \big[A \,\vec{\wedge}\, \big(X_{10} \,\bar{\vec{\wedge}}\, \eta\big)\big] \;= \\ =\;\; & \big[\neg(X_1X_5 \vee X_1X_{15} \vee X_5X_{13} \vee X_{13}X_{15}) \wedge (A \,\vec{\wedge}\, X_{10})\big] \vee \\ & \vee \big[\neg\, X_{10} \wedge (A \,\vec{\wedge}\, (X_1X_5 \vee X_1X_{15} \vee X_5X_{13} \vee X_{13}X_{15}))\big] \vee \\ & \vee \big[A \,\vec{\wedge}\, \big(X_{10} \,\bar{\vec{\wedge}}\, (X_1X_5 \vee X_1X_{15} \vee X_5X_{13} \vee X_{13}X_{15})\big)\big] \;= \\ =\;\; & \eta_1 \vee \eta_2 \vee \eta_3 \;. \end{aligned} \tag{7.10}$$

Der Term η_1 lässt sich vergleichsweise einfach in eine TDNF überführen:

$$\begin{aligned} \eta_1 \;=\;\; & \neg(X_1X_5 \vee X_1X_{15} \vee X_5X_{13} \vee X_{13}X_{15}) \wedge (A \,\vec{\wedge}\, X_{10}) \;= \\ =\;\; & \big[(\neg\, X_1 \neg\, X_{13}) \wedge (A \,\vec{\wedge}\, X_{10})\big] \vee \big[(\neg\, X_5 \neg\, X_{15}) \wedge (A \,\vec{\wedge}\, X_{10})\big] \;. \end{aligned} \tag{7.11}$$

Deutlich komplexer ist der Term η_2, der iterativ vereinfacht werden muss.

$$\begin{aligned} \eta_2 \;=\;\; & \neg\, X_{10} \wedge \Big(\neg(X_1X_{15} \vee X_5X_{13} \vee X_{13}X_{15}) \wedge (A \,\vec{\wedge}\, (X_1X_5))\Big) \vee \\ & \vee \neg\, X_{10} \wedge \Big(\neg(X_1X_5) \wedge (A \,\vec{\wedge}\, (X_1X_{15} \vee X_5X_{13} \vee X_{13}X_{15}))\Big) \vee \\ & \vee \neg\, X_{10} \wedge \Big(A \,\vec{\wedge}\, \big((X_1X_5) \,\bar{\vec{\wedge}}\, (X_1X_{15} \vee X_5X_{13} \vee X_{13}X_{15})\big)\Big) \;= \\ =\;\; & \eta_{2a} \vee \eta_{2b} \vee \eta_{2c} \;. \end{aligned} \tag{7.12}$$

Der erste Teilterm aus (7.12) ergibt die drei Ereignissequenzen

$$\begin{aligned} \eta_{2a} \;=\;\; & \neg\, X_{10} \wedge \big[([\neg\, X_1 \neg\, X_{13}] \vee [\neg\, X_5 \neg\, X_{15}] \vee [\neg\, X_{13} \neg\, X_{15}]) \wedge (A \,\vec{\wedge}\, (X_1X_5))\big] \;= \\ =\;\; & \big[(\neg\, X_1 \neg\, X_{10} \neg\, X_{13}) \wedge (A \,\vec{\wedge}\, (X_1X_5))\big] \vee \\ & \vee \big[(\neg\, X_5 \neg\, X_{10} \neg\, X_{15}) \wedge (A \,\vec{\wedge}\, (X_1X_5))\big] \vee \\ & \vee \big[(\neg\, X_{10} \neg\, X_{13} \neg\, X_{15}) \wedge (A \,\vec{\wedge}\, (X_1X_5))\big] \;, \end{aligned} \tag{7.13}$$

von denen nur die Dritte gemäß der Regeln in (4.51) und (4.52) nicht *False* ergibt, so dass

$$\eta_{2a} \;=\; \big[(\neg\, X_{10} \neg\, X_{13} \neg\, X_{15}) \wedge (A \,\vec{\wedge}\, (X_1X_5))\big] \;. \tag{7.14}$$

Der zweite Teilterm aus (7.12) unterteilt sich seinerseits in drei Teilterme:

$$\begin{aligned} \eta_{2b} \;=\;\; & (\neg\, X_{10}\, \neg(X_1X_5)) \wedge \Big(\neg(X_5X_{13} \vee X_{13}X_{15}) \wedge (A \,\vec{\wedge}\, (X_1X_{15}))\Big) \vee \\ & \vee (\neg\, X_{10}\, \neg(X_1X_5)) \wedge \Big(\neg(X_1X_{15}) \wedge (A \,\vec{\wedge}\, (X_5X_{13} \vee X_{13}X_{15}))\Big) \vee \\ & \vee (\neg\, X_{10}\, \neg(X_1X_5)) \wedge \Big(A \,\vec{\wedge}\, ((X_1X_{15}) \,\bar{\vec{\wedge}}\, (X_5X_{13} \vee X_{13}X_{15}))\Big) \;= \\ =\;\; & \eta_{2b1} \vee \eta_{2b2} \vee \eta_{2b3} \;. \end{aligned} \tag{7.15}$$

Von

$$\begin{aligned} \eta_{2b1} \;=\;\; & (\neg\, X_{10}\, \neg(X_1X_5)) \wedge \big[(\neg\, X_{13} \vee [\neg\, X_5 \neg\, X_{15}]) \wedge (A \,\vec{\wedge}\, (X_1X_{15}))\big] \;= \\ =\;\; & \big[(\neg\, X_1 \neg\, X_{10} \neg\, X_{13}) \wedge (A \,\vec{\wedge}\, (X_1X_{15}))\big] \vee \\ & \vee \big[(\neg\, X_5 \neg\, X_{10} \neg\, X_{13}) \wedge (A \,\vec{\wedge}\, (X_1X_{15}))\big] \vee \\ & \vee \big[(\neg\, X_1 \neg\, X_5 \neg\, X_{10} \neg\, X_{15}) \wedge (A \,\vec{\wedge}\, (X_1X_{15}))\big] \vee \end{aligned}$$

$$\vee \left[(\neg X_5 \neg X_{10} \neg X_{15}) \wedge (A \vec{\wedge} (X_1 X_{15}))\right] \tag{7.16}$$

verbleibt wegen der Regeln in (4.51) und (4.52) lediglich

$$\eta_{2b1} = \left[(\neg X_5 \neg X_{10} \neg X_{13}) \wedge (A \vec{\wedge} (X_1 X_{15}))\right] . \tag{7.17}$$

Wiederum drei Teilterme folgen aus dem zweiten Teil aus (7.15):

$$\begin{aligned}
\eta_{2b2} = \quad & (\neg X_{10} \wedge (\neg X_1 \vee [\neg X_5 \neg X_{15}])) \wedge \Big(\neg(X_{13} X_{15}) \wedge (A \vec{\wedge} (X_5 X_{13}))\Big) \vee \\
& \vee (\neg X_{10} \wedge (\neg X_1 \vee [\neg X_5 \neg X_{15}])) \wedge \Big(\neg(X_5 X_{13}) \wedge (A \vec{\wedge} (X_{13} X_{15}))\Big) \vee \\
& \vee (\neg X_{10} \wedge (\neg X_1 \vee [\neg X_5 \neg X_{15}])) \wedge \Big(A \vec{\wedge} ((X_5 X_{13}) \,\overline{\vec{\wedge}}\, (X_{13} X_{15}))\Big) = \\
= \; & \eta_{2b2a} \vee \eta_{2b2b} \vee \eta_{2b2c} .
\end{aligned} \tag{7.18}$$

Wegen der Regeln in (4.51) und (4.52) vereinfacht sich der erste dieser Teilterme zu

$$\begin{aligned}
\eta_{2b2a} = \quad & \left[\neg X_{10} \wedge (\neg X_1 \vee [\neg X_5 \neg X_{15}]) \wedge \neg(X_{13} X_{15})\right] \wedge (A \vec{\wedge} (X_5 X_{13})) = \\
= \quad & (\neg X_1 \neg X_{10} \neg X_{13}) \wedge (A \vec{\wedge} (X_5 X_{13})) \vee \\
& \vee (\neg X_1 \neg X_{10} \neg X_{15}) \wedge (A \vec{\wedge} (X_5 X_{13})) \vee \\
& \vee (\neg X_5 \neg X_{10} \neg X_{15}) \wedge (A \vec{\wedge} (X_5 X_{13})) \vee \; = \\
= \; & \left[(\neg X_1 \neg X_{10} \neg X_{15}) \wedge (A \vec{\wedge} (X_5 X_{13}))\right] .
\end{aligned} \tag{7.19}$$

Analog dazu gilt für den zweiten Teilterm, dass

$$\begin{aligned}
\eta_{2b2b} = \; & \left[\neg X_{10} \wedge (\neg X_1 \vee [\neg X_5 \neg X_{15}]) \wedge \neg(X_5 X_{13})\right] \wedge (A \vec{\wedge} (X_{13} X_{15})) = \\
= \; & \left[(\neg X_1 \neg X_5 \neg X_{10}) \wedge (A \vec{\wedge} (X_{13} X_{15}))\right] .
\end{aligned} \tag{7.20}$$

Wegen

$$\begin{aligned}
(X_5 X_{13}) \,\overline{\vec{\wedge}}\, (X_{13} X_{15}) = \quad & \left[(X_5 X_{15}) \vec{\wedge} X_{13}\right] \vee \left[X_{13} \vec{\wedge} (X_5 \,\overline{\vec{\wedge}}\, X_{15})\right] \vee \left[X_{15} \vec{\wedge} (X_5 \,\overline{\vec{\wedge}}\, X_{13})\right] \vee \\
& \vee \left[X_5 \vec{\wedge} (X_{13} \,\overline{\vec{\wedge}}\, X_{15})\right] \vee \left[X_5 \,\overline{\vec{\wedge}}\, X_{13} \,\overline{\vec{\wedge}}\, X_{15}\right]
\end{aligned} \tag{7.21}$$

ergibt der dritte Teilterm in (7.18)

$$\begin{aligned}
\eta_{2b2c} = \quad & (\neg X_1 \neg X_{10}) \wedge \Big(A \vec{\wedge} \left[(X_5 X_{15}) \vec{\wedge} X_{13}\right] \vee A \vec{\wedge} \left[X_{13} \vec{\wedge} (X_5 \,\overline{\vec{\wedge}}\, X_{15})\right] \vee \\
& \vee A \vec{\wedge} \left[X_{15} \vec{\wedge} (X_5 \,\overline{\vec{\wedge}}\, X_{13})\right] \vee A \vec{\wedge} \left[X_5 \vec{\wedge} (X_{13} \,\overline{\vec{\wedge}}\, X_{15})\right] \vee A \vec{\wedge} \left[X_5 \,\overline{\vec{\wedge}}\, X_{13} \,\overline{\vec{\wedge}}\, X_{15}\right]\Big) ,
\end{aligned} \tag{7.22}$$

wobei nur die Ereignissequenz $(\neg X_1 \neg X_{10}) \wedge \left[(A \wedge X_5 \wedge X_{15}) \vec{\wedge} X_{13}\right]$ keine SAND Verbindungen enthält. Nur diese wird im Weiteren betrachtet, da in diesem Beispiel keine abhängigen Ausfälle berücksichtigt werden, vgl. Kapitel 7.1.2.

Einsetzen von (7.22) und (7.20) und (7.19) in (7.18) ergibt die drei Ereignissequenzen

$$\begin{aligned}
\eta_{2b2} = \quad & \left[(\neg X_1 \neg X_{10} \neg X_{15}) \wedge (A \vec{\wedge} (X_5 X_{13}))\right] \vee \\
& \vee \left[(\neg X_1 \neg X_5 \neg X_{10}) \wedge (A \vec{\wedge} (X_{13} X_{15}))\right] \vee \\
& \vee \left[(\neg X_1 \neg X_{10}) \wedge ((A \wedge X_5 \wedge X_{15}) \vec{\wedge} X_{13})\right] .
\end{aligned} \tag{7.23}$$

Der noch ausstehende dritte Teilterm aus (7.15) lässt sich auf diese Weise ebenfalls vereinfachen, sodass

$$\begin{aligned}
\eta_{2b3} &= (\neg X_{10}\,\neg(X_1X_5)) \wedge \Big(A \,\vec{\barwedge}\, ((X_1X_{15}) \,\bar{\vec{\wedge}}\, (X_5X_{13} \vee X_{13}X_{15}))\Big) = \\
&= (\neg X_{10}\,\neg(X_1X_5)) \wedge \Big(\neg(X_{13}X_{15}) \wedge (A \,\vec{\barwedge}\, ((X_1X_{15}) \,\bar{\vec{\wedge}}\, (X_5X_{13})))\Big) \vee \\
&\quad \vee (\neg X_{10}\,\neg(X_1X_5)) \wedge \Big(\neg(X_5X_{13}) \wedge (A \,\vec{\barwedge}\, ((X_1X_{15}) \,\bar{\vec{\wedge}}\, (X_{13}X_{15})))\Big) \vee \\
&\quad \vee (\neg X_{10}\,\neg(X_1X_5)) \wedge \Big(A \,\vec{\barwedge}\, ((X_1X_{15}) \,\bar{\vec{\wedge}}\, (X_5X_{13}) \,\bar{\vec{\wedge}}\, (X_{13}X_{15}))\Big).
\end{aligned}$$

Durch Anwenden der Regeln in (4.51) und (4.52) vereinfacht sich η_{2b3} zu

$$\begin{aligned}
\eta_{2b3} &= \mathit{False} \vee \big[(\neg X_{10}\,\neg(X_1X_5)\,\neg(X_5X_{13})) \wedge ((A \wedge X_1 \wedge X_{13}) \,\vec{\barwedge}\, X_{15})\big] \vee \mathit{False} = \\
&= \big[(\neg X_5\,\neg X_{10}) \wedge ((A \wedge X_1 \wedge X_{13}) \,\vec{\barwedge}\, X_{15})\big]\ . \qquad (7.24)
\end{aligned}$$

Die Ergebnisse aus (7.24) und (7.23) und (7.17) werden in (7.15) eingesetzt und ergeben die fünf Ereignissequenzen (ohne SAND Verknüpfungen) von η_{2b} .

Die Berechnung der noch ausstehenden Terme η_{2c} und η_2 und η_3 erfolgt vollkommen analog zu obigen ausführlichen Beispielen. Sie ist hier nicht explizit aufgeführt.

Der Term η_{2c} aus (7.12) liefert folgende Terme (ohne SAND Verknüpfungen):

$$\begin{aligned}
\eta_{2c} &= \big[(\neg X_{10}\,\neg X_{15}) \wedge ((A \wedge X_1 \wedge X_{13}) \,\vec{\barwedge}\, X_5)\big] \vee \\
&\quad \vee \big[(\neg X_{10}\,\neg X_{13}) \wedge ((A \wedge X_5 \wedge X_{15}) \,\vec{\barwedge}\, X_1)\big]\ . \qquad (7.25)
\end{aligned}$$

Zusammen mit (7.14) und (7.15) ergibt dies die acht Ereignissequenzen (ohne SAND Verknüpfungen) von η_2.

Der Term η_3 liefert ausschließlich Ereignissequenzen, die mindestens eine SAND Verknüpfung enthalten, und wird daher hier nicht weiter berücksichtigt.

Insgesamt besteht $A \,\vec{\barwedge}\, B$ somit aus den zwei Ereignissequenzen (ohne SAND Verknüpfungen) von η_1 aus (7.11) und den acht Ereignissequenzen aus von η_2:

$$\begin{aligned}
A \,\vec{\barwedge}\, B = {} & \big[(\neg X_1\,\neg X_{13}) \wedge (A \,\vec{\barwedge}\, X_{10})\big] \vee && \langle \mathrm{ES1} \rangle \\
& \vee \big[(\neg X_5\,\neg X_{15}) \wedge (A \,\vec{\barwedge}\, X_{10})\big] \vee && \langle \mathrm{ES2} \rangle \\
& \vee \big[(\neg X_{10}\,\neg X_{13}\,\neg X_{15}) \wedge (A \,\vec{\barwedge}\, (X_1X_5))\big] \vee && \langle \mathrm{ES3} \rangle \\
& \vee \big[(\neg X_5\,\neg X_{10}\,\neg X_{13}) \wedge (A \,\vec{\barwedge}\, (X_1X_{15}))\big] \vee && \langle \mathrm{ES4} \rangle \\
& \vee \big[(\neg X_1\,\neg X_{10}\,\neg X_{15}) \wedge (A \,\vec{\barwedge}\, (X_5X_{13}))\big] \vee && \langle \mathrm{ES5} \rangle \\
& \vee \big[(\neg X_1\,\neg X_5\,\neg X_{10}) \wedge (A \,\vec{\barwedge}\, (X_{13}X_{15}))\big] \vee && \langle \mathrm{ES6} \rangle \\
& \vee \big[(\neg X_1\,\neg X_{10}) \wedge ((A \wedge X_5 \wedge X_{15}) \,\vec{\barwedge}\, X_{13})\big] \vee && \langle \mathrm{ES7} \rangle \\
& \vee \big[(\neg X_5\,\neg X_{10}) \wedge ((A \wedge X_1 \wedge X_{13}) \,\vec{\barwedge}\, X_{15})\big] \vee && \langle \mathrm{ES8} \rangle \\
& \vee \big[(\neg X_{10}\,\neg X_{15}) \wedge ((A \wedge X_1 \wedge X_{13}) \,\vec{\barwedge}\, X_5)\big] \vee && \langle \mathrm{ES9} \rangle \\
& \vee \big[(\neg X_{10}\,\neg X_{13}) \wedge ((A \wedge X_5 \wedge X_{15}) \,\vec{\barwedge}\, X_1)\big]\ . && \langle \mathrm{ES10} \rangle \qquad (7.26)
\end{aligned}$$

Die Bezeichner $\langle$ES1$\rangle$ bis $\langle$ES10$\rangle$ dienen im Folgenden als Referenz auf die jeweilige Sequenz. Die Auflösung von A erfolgt mit Hilfe des temporalen Distributivgesetzes für temporale Terme vom Typ II nach (4.78). Einsetzen in (7.26) und weitere Vereinfachung liefert 28 verschiedene Ereignissequenzen für $A \,\vec{\barwedge}\, B$ (aus Platzgründen hier zusammengefasst dargestellt):

$$
\begin{aligned}
&(X_1 \vee X_5 \vee X_{20} \vee X_{22} \vee X_{24}) \,\vec{\wedge}\, B \;=\; \ldots \;= \\
&\quad= \quad \big[(\neg X_1 \neg X_{13}) \wedge ((X_5 \vee X_{20} \vee X_{22} \vee X_{24}) \,\vec{\wedge}\, X_{10})\big] \vee && \langle \text{aus ES1} \rangle \\
&\qquad \vee \big[(\neg X_5 \neg X_{15}) \wedge ((X_1 \vee X_{20} \vee X_{22} \vee X_{24}) \,\vec{\wedge}\, X_{10})\big] \vee && \langle \text{aus ES2} \rangle \\
&\qquad \vee \big[(\neg X_{10} \neg X_{13} \neg X_{15}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \,\vec{\wedge}\, (X_1 X_5))\big] \vee && \langle \text{aus ES3} \rangle \\
&\qquad \vee \big[(\neg X_{10} \neg X_{13} \neg X_{15}) \wedge (X_1 \,\vec{\wedge}\, X_5)\big] \vee && \langle \text{aus ES3} \rangle \\
&\qquad \vee \big[(\neg X_{10} \neg X_{13} \neg X_{15}) \wedge (X_5 \,\vec{\wedge}\, X_1)\big] \vee && \langle \text{aus ES3} \rangle \\
&\qquad \vee \big[(\neg X_5 \neg X_{10} \neg X_{13}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \,\vec{\wedge}\, (X_1 X_{15}))\big] \vee && \langle \text{aus ES4} \rangle \\
&\qquad \vee \big[(\neg X_5 \neg X_{10} \neg X_{13}) \wedge (X_1 \,\vec{\wedge}\, X_{15})\big] \vee && \langle \text{aus ES4} \rangle \\
&\qquad \vee \big[(\neg X_1 \neg X_{10} \neg X_{15}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \,\vec{\wedge}\, (X_5 X_{13}))\big] \vee && \langle \text{aus ES5} \rangle \\
&\qquad \vee \big[(\neg X_1 \neg X_{10} \neg X_{15}) \wedge (X_5 \,\vec{\wedge}\, X_{13})\big] \vee && \langle \text{aus ES5} \rangle \\
&\qquad \vee \big[(\neg X_1 \neg X_5 \neg X_{10}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \,\vec{\wedge}\, (X_{13} X_{15}))\big] \vee && \langle \text{aus ES6} \rangle \\
&\qquad \vee \big[(\neg X_1 \neg X_{10}) \wedge ((X_5 \wedge X_{15}) \,\vec{\wedge}\, X_{13})\big] \vee && \langle \text{aus ES7} \rangle \\
&\qquad \vee \big[(\neg X_5 \neg X_{10}) \wedge ((X_1 \wedge X_{13}) \,\vec{\wedge}\, X_{15})\big] \vee && \langle \text{aus ES8} \rangle \\
&\qquad \vee \big[(\neg X_{10} \neg X_{15}) \wedge ((X_1 \wedge X_{13}) \,\vec{\wedge}\, X_5)\big] \vee && \langle \text{aus ES9} \rangle \\
&\qquad \vee \big[(\neg X_{10} \neg X_{13}) \wedge ((X_5 \wedge X_{15}) \,\vec{\wedge}\, X_1)\big] \;. && \langle \text{aus ES10} \rangle \qquad (7.27)
\end{aligned}
$$

Der Term $A \,\vec{\wedge}\, B$ alleine führt somit zu 12 Ereignissequenzen von Rang zwei und 16 Ereignissequenzen von Rang drei.

Vereinfachung von $(\mathbf{A} \,\vec{\wedge}\, \mathbf{B}) \wedge \mathbf{C}$:
Mit Hilfe der TFTA Logik lässt sich auch die Vermaschung zwischen B und C im sechsten und letzten Teilterm aus (7.3) auflösen.

Gemäß (7.1) sind B und C gegeben als

$$B \;=\; X_{10} \vee [(X_1 \vee X_{13}) \wedge (X_5 \vee X_{15})] \quad \text{und} \tag{7.28}$$

$$C \;=\; X_{28} \vee [(X_1 \vee X_{13}) \wedge (X_5 \vee X_{15})] \vee [(X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}] \,. \tag{7.29}$$

Durch eine weitere Substitution mit

$$D \;=\; (X_1 \vee X_{13}) \wedge (X_5 \vee X_{15}) \;=\; X_1 X_5 \vee X_1 X_{15} \vee X_5 X_{13} \vee X_{13} X_{15} \tag{7.30}$$

wird die Beziehung zwischen B und C deutlich, derzufolge

$$B \;=\; X_{10} \vee D \quad \text{und} \tag{7.31}$$

$$C \;=\; X_{28} \vee D \vee ((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}) \;. \tag{7.32}$$

Einsetzen von (7.31) und (7.32) liefert

$$
\begin{aligned}
&(A \,\vec{\wedge}\, B) \wedge C \;=\; (A \,\vec{\wedge}\, B) \wedge \big(X_{28} \vee D \vee ((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10})\big) \;= \\
&\qquad= \big[(A \,\vec{\wedge}\, B) \wedge X_{28}\big] \vee \big[(A \,\vec{\wedge}\, B) \wedge D\big] \vee \big[(A \,\vec{\wedge}\, B) \wedge \big((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}\big)\big] \;. \qquad (7.33)
\end{aligned}
$$

Der erste Teilterm ergibt (ohne SAND Verknüpfungen)

$$(A \,\vec{\wedge}\, B) \wedge X_{28} \;=\; \big[A \,\vec{\wedge}\, B \,\vec{\wedge}\, X_{28}\big] \vee \big[(A \wedge X_{28}) \,\vec{\wedge}\, B\big] \;. \tag{7.34}$$

Die TDNF von $(A \vec{\wedge} B) \wedge X_{28}$ besteht aus insgesamt 56 MCSS. $\left[A \vec{\wedge} B \vec{\wedge} X_{28}\right]$ liefert 28 MCSS ähnlich denen in (7.27) allerdings jeweils erweitert um das Ereignis X_{28}. $\left[(A \wedge X_{28}) \vec{\wedge} B\right]$ liefert ebenfalls 28 MCSS ähnlich denen in (7.27). Hierbei wird anstelle von A der Term $A \wedge X_{28}$ eingesetzt. 24 der MCSS sind von Rang drei und 32 der MCSS sind von Rang vier.

Der zweite Teilterm in (7.33) ergibt (ohne SAND Verknüpfungen)

$$\begin{aligned}(A \vec{\wedge} B) \wedge D \;&=\; (A \vec{\wedge} (X_{10} \vee D)) \wedge D \;=\; \ldots \;= \\ &=\; \left[\neg X_{10} \wedge (A \vec{\wedge} D)\right] \vee \left[A \vec{\wedge} X_{10} \vec{\wedge} D\right] \;. \end{aligned} \tag{7.35}$$

$\left[\neg X_{10} \wedge (A \vec{\wedge} D)\right]$ liefert 20 MCSS ähnlich denen in (7.27). Da D anders als B das Ereignis X_{10} nicht enthält, entfallen dabei die ersten acht Ereignissequenzen (die ersten zwei Zeilen in (7.27)). Ebenso entfallen die $\neg X_{10}$ in den restlichen Zeilen. Es ist also

$$A \vec{\wedge} D \;=\; A \vec{\wedge} B\big|_{X_{10} = \mathit{False}} \;. \tag{7.36}$$

Für den Term $\left[\neg X_{10} \wedge (A \vec{\wedge} D)\right]$ verbleiben somit vier MCSS von Rang zwei und 16 MCSS von Rang drei, vgl. (7.37).

$$\begin{aligned}\neg X_{10} \wedge (A \vec{\wedge} D) \;=\;& \left[(\neg X_{10}\, \neg X_{13}\, \neg X_{15}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \vec{\wedge} (X_1 X_5))\right] \vee \\ &\vee \left[(\neg X_{10}\, \neg X_{13}\, \neg X_{15}) \wedge (X_1 \vec{\wedge} X_5)\right] \vee \\ &\vee \left[(\neg X_{10}\, \neg X_{13}\, \neg X_{15}) \wedge (X_5 \vec{\wedge} X_1)\right] \vee \\ &\vee \left[(\neg X_5\, \neg X_{10}\, \neg X_{13}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \vec{\wedge} (X_1 X_{15}))\right] \vee \\ &\vee \left[(\neg X_5\, \neg X_{10}\, \neg X_{13}) \wedge (X_1 \vec{\wedge} X_{15})\right] \vee \\ &\vee \left[(\neg X_1\, \neg X_{10}\, \neg X_{15}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \vec{\wedge} (X_5 X_{13}))\right] \vee \\ &\vee \left[(\neg X_1\, \neg X_{10}\, \neg X_{15}) \wedge (X_5 \vec{\wedge} X_{13})\right] \vee \\ &\vee \left[(\neg X_1\, \neg X_5\, \neg X_{10}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \vec{\wedge} (X_{13} X_{15}))\right] \vee \\ &\vee \left[(\neg X_1\, \neg X_{10}) \wedge ((X_5 \wedge X_{15}) \vec{\wedge} X_{13})\right] \vee \\ &\vee \left[(\neg X_5\, \neg X_{10}) \wedge ((X_1 \wedge X_{13}) \vec{\wedge} X_{15})\right] \vee \\ &\vee \left[(\neg X_{10}\, \neg X_{15}) \wedge ((X_1 \wedge X_{13}) \vec{\wedge} X_5)\right] \vee \\ &\vee \left[(\neg X_{10}\, \neg X_{13}) \wedge ((X_5 \wedge X_{15}) \vec{\wedge} X_1)\right] \;. \end{aligned} \tag{7.37}$$

Analog dazu liefert auch der Term $\left[A \vec{\wedge} X_{10} \vec{\wedge} D\right]$ 20 MCSS. Aufgrund des zusätzlichen Ereignisses X_{10} sind davon vier MCSS von Rang drei und 16 MCSS von Rang vier, vgl. (7.38).

$$\begin{aligned}\neg X_{10} \wedge (A \vec{\wedge} D) \;=\;& \left[(\neg X_{13}\, \neg X_{15}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \vec{\wedge} X_{10} \vec{\wedge} (X_1 X_5))\right] \vee \\ &\vee \left[(\neg X_{13}\, \neg X_{15}) \wedge (X_1 \vec{\wedge} X_{10} \vec{\wedge} X_5)\right] \vee \\ &\vee \left[(\neg X_{10}\, \neg X_{13}\, \neg X_{15}) \wedge (X_5 \vec{\wedge} X_{10} \vec{\wedge} X_1)\right] \vee \\ &\vee \left[(\neg X_5\, \neg X_{13}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \vec{\wedge} X_{10} \vec{\wedge} (X_1 X_{15}))\right] \vee \\ &\vee \left[(\neg X_5\, \neg X_{10}\, \neg X_{13}) \wedge (X_1 \vec{\wedge} X_{10} \vec{\wedge} X_{15})\right] \vee \\ &\vee \left[(\neg X_1\, \neg X_{15}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \vec{\wedge} X_{10} \vec{\wedge} (X_5 X_{13}))\right] \vee \\ &\vee \left[(\neg X_1\, \neg X_{10}\, \neg X_{15}) \wedge (X_5 \vec{\wedge} X_{10} \vec{\wedge} X_{13})\right] \vee \\ &\vee \left[(\neg X_1\, \neg X_5) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \vec{\wedge} X_{10} \vec{\wedge} (X_{13} X_{15}))\right] \vee \\ &\vee \left[\neg X_1 \wedge ((X_5 \wedge X_{15}) \vec{\wedge} X_{10} \vec{\wedge} X_{13})\right] \vee \\ &\vee \left[\neg X_5 \wedge ((X_1 \wedge X_{13}) \vec{\wedge} X_{10} \vec{\wedge} X_{15})\right] \vee \end{aligned} \tag{7.38}$$

$$\vee \left[\neg X_{15} \wedge ((X_1 \wedge X_{13}) \,\vec{\wedge}\, X_{10} \,\vec{\wedge}\, X_5)\right] \vee$$
$$\vee \left[\neg X_{13} \wedge ((X_5 \wedge X_{15}) \,\vec{\wedge}\, X_{10} \,\vec{\wedge}\, X_1)\right] \; . \tag{7.38}$$

Die Umformung des dritten Teilterms $\left[(A \,\vec{\wedge}\, B) \wedge \left((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}\right)\right]$, vgl. (7.33), lässt sich am einfachsten für jede der Sequenzen ⟨ES1⟩ bis ⟨ES10⟩ aus (7.26) separat zeigen.

⟨ES1⟩ und ⟨ES2⟩ unterscheiden sich nur durch die betroffenen Ereignisse, so dass

$$\begin{aligned}
\langle \text{ES1} \rangle : \quad & \left[(\neg X_1 \, \neg X_{13}) \wedge ((X_5 \vee X_{20} \vee X_{22} \vee X_{24}) \,\vec{\wedge}\, X_{10})\right] \wedge \left((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}\right) = \\
& = (\neg X_1 \, \neg X_{13}) \wedge \big((X_5 X_{18}) \vee (X_{20} X_{18}) \vee (X_{22} X_{18}) \vee (X_{24} X_{18}) \vee \\
& \qquad \vee (X_5 X_{27}) \vee (X_{20} X_{27}) \vee (X_{22} X_{27}) \vee (X_{24} X_{27})\big) \,\vec{\wedge}\, X_{10} \qquad \text{und} \\
\langle \text{ES2} \rangle : \quad & (\neg X_5 \, \neg X_{15}) \wedge \big((X_1 X_{18}) \vee (X_{20} X_{18}) \vee (X_{22} X_{18}) \vee (X_{24} X_{18}) \vee \\
& \qquad \vee (X_1 X_{27}) \vee (X_{20} X_{27}) \vee (X_{22} X_{27}) \vee (X_{24} X_{27})\big) \,\vec{\wedge}\, X_{10} \; .
\end{aligned} \tag{7.39}$$

Der erste Teil von ⟨ES3⟩ ergibt

$$\langle \text{ES3} \rangle : \quad \left[(\neg X_{10} \, \neg X_{13} \, \neg X_{15}) \wedge ((X_{20} \vee X_{22} \vee X_{24}) \,\vec{\wedge}\, (X_1 X_5))\right] \wedge \left((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}\right) \; . \tag{7.40}$$

Die weitere Vereinfachung liefert ausschließlich Ereignissequenzen von Rang fünf oder größer. Diese werden hier nicht weiter betrachtet, da sie im Vergleich zu den hauptsächlich beitragenden MCSS um Größenordnungen unwahrscheinlicher sind. Eine solche Aufwandsminimierung ist auch in der herkömmlichen FTA möglich und sinnvoll. Dasselbe gilt für die Vereinfachungen des ersten Teils von ⟨ES4⟩ und von ⟨ES5⟩ sowie komplett für ⟨ES6⟩ bis ⟨ES10⟩.

Der zweite Teil von ⟨ES3⟩ ergibt folgende vier MCSS von Rang vier.

$$\begin{aligned}
\langle \text{ES3} \rangle : \left[(\neg X_{10} \, \neg X_{13} \, \neg X_{15}) \wedge (X_1 \,\vec{\wedge}\, X_5)\right] \wedge \left((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}\right) & = \\
= \quad \left[(\neg X_{13} \, \neg X_{15} \, \neg X_{27}) \wedge (X_1 \,\vec{\wedge}\, X_5 \,\vec{\wedge}\, X_{18} \,\vec{\wedge}\, X_{10})\right] & \vee \\
\vee \left[(\neg X_{13} \, \neg X_{15} \, \neg X_{18}) \wedge (X_1 \,\vec{\wedge}\, X_5 \,\vec{\wedge}\, X_{27} \,\vec{\wedge}\, X_{10})\right] & \vee \\
\vee \left[(\neg X_{13} \, \neg X_{15} \, \neg X_{27}) \wedge ((X_1 X_{18}) \,\vec{\wedge}\, X_5 \,\vec{\wedge}\, X_{10})\right] & \vee \\
\vee \left[(\neg X_{13} \, \neg X_{15} \, \neg X_{18}) \wedge ((X_1 X_{27}) \,\vec{\wedge}\, X_5 \,\vec{\wedge}\, X_{10})\right] & \; .
\end{aligned} \tag{7.41}$$

Analog dazu ergeben der dritte Teil von ⟨ES3⟩ sowie die zweiten Teile von ⟨ES4⟩ und ⟨ES5⟩ ebenfalls je vier MCSS von Rang vier:

$$\begin{aligned}
\langle \text{ES3} \rangle : \left[(\neg X_{10} \, \neg X_{13} \, \neg X_{15}) \wedge (X_5 \,\vec{\wedge}\, X_1)\right] \wedge \left((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}\right) & = \\
= \quad \left[(\neg X_{13} \, \neg X_{15} \, \neg X_{27}) \wedge (X_5 \,\vec{\wedge}\, X_1 \,\vec{\wedge}\, X_{18} \,\vec{\wedge}\, X_{10})\right] & \vee \\
\vee \left[(\neg X_{13} \, \neg X_{15} \, \neg X_{18}) \wedge (X_5 \,\vec{\wedge}\, X_1 \,\vec{\wedge}\, X_{27} \,\vec{\wedge}\, X_{10})\right] & \vee \\
\vee \left[(\neg X_{13} \, \neg X_{15} \, \neg X_{27}) \wedge ((X_5 X_{18}) \,\vec{\wedge}\, X_1 \,\vec{\wedge}\, X_{10})\right] & \vee \\
\vee \left[(\neg X_{13} \, \neg X_{15} \, \neg X_{18}) \wedge ((X_5 X_{27}) \,\vec{\wedge}\, X_1 \,\vec{\wedge}\, X_{10})\right] & \; .
\end{aligned} \tag{7.42}$$

$$\begin{aligned}
\langle \text{ES4} \rangle : \left[(\neg X_5 \, \neg X_{10} \, \neg X_{13}) \wedge (X_1 \,\vec{\wedge}\, X_{15})\right] \wedge \left((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}\right) & = \\
= \quad \left[(\neg X_5 \, \neg X_{13} \, \neg X_{27}) \wedge (X_1 \,\vec{\wedge}\, X_{15} \,\vec{\wedge}\, X_{18} \,\vec{\wedge}\, X_{10})\right] & \vee \\
\vee \left[(\neg X_5 \, \neg X_{13} \, \neg X_{18}) \wedge (X_1 \,\vec{\wedge}\, X_{15} \,\vec{\wedge}\, X_{27} \,\vec{\wedge}\, X_{10})\right] & \vee \\
\vee \left[(\neg X_5 \, \neg X_{13} \, \neg X_{27}) \wedge ((X_1 X_{18}) \,\vec{\wedge}\, X_{15} \,\vec{\wedge}\, X_{10})\right] & \vee \\
\vee \left[(\neg X_5 \, \neg X_{13} \, \neg X_{18}) \wedge ((X_1 X_{27}) \,\vec{\wedge}\, X_{15} \,\vec{\wedge}\, X_{10})\right] & \; .
\end{aligned} \tag{7.43}$$

$$\langle \text{ES5} \rangle : \left[(\neg X_1 \, \neg X_{10} \, \neg X_{15}) \wedge (X_5 \,\vec{\wedge}\, X_{13})\right] \wedge \left((X_{27} \vee X_{18}) \,\vec{\wedge}\, X_{10}\right) =$$

$$
\begin{aligned}
= \quad & \left[(\neg X_1 \neg X_{15} \neg X_{27}) \wedge (X_5 \vec{\wedge} X_{13} \vec{\wedge} X_{18} \vec{\wedge} X_{10})\right] \vee \\
\vee \; & \left[(\neg X_1 \neg X_{15} \neg X_{18}) \wedge (X_5 \vec{\wedge} X_{13} \vec{\wedge} X_{27} \vec{\wedge} X_{10})\right] \vee \\
\vee \; & \left[(\neg X_1 \neg X_{15} \neg X_{27}) \wedge ((X_5 X_{18}) \vec{\wedge} X_{13} \vec{\wedge} X_{10})\right] \vee \\
\vee \; & \left[(\neg X_1 \neg X_{15} \neg X_{18}) \wedge ((X_5 X_{27}) \vec{\wedge} X_{13} \vec{\wedge} X_{10})\right] . \qquad (7.44)
\end{aligned}
$$

7.3.3 Analyse der MCSS

Die MCSS der temporalen Ausfallfunktion ϖ ergeben sich aus den Ereignissequenzen der Teilterme aus (7.3), die nicht zwangsläufig bereits MCSS sein müssen (es können Schnittmengen und Überdeckungen zwischen den einzelnen Teiltermen bestehen). Allgemein gilt: die MCSS mit dem kleinsten Rang besitzen die größte Bedeutung. Die folgenden Ausführungen konzentrieren sich daher auf MCSS mit Rang zwei und drei.

Ereignissequenzen der Teilterme

Die Ereignissequenzen der Teilterme mit Rang zwei und drei sind in Tabelle 7.4 aufgeführt. Sie stammen aus Tabelle 7.3 auf Seite 98 und den Gleichungen in (7.34), (7.37), (7.38) und (7.39).

		(erweiterte) Ereignissequenzen von Rang zwei:			
1:	$X_1 \vec{\wedge} X_5$	3:	$X_1 \vec{\wedge} X_{15}$	5:	$X_{28} \wedge X_{38}$
2:	$X_5 \vec{\wedge} X_1$	4:	$X_5 \vec{\wedge} X_{13}$		
		(erweiterte) Ereignissequenzen von Rang drei:			
1:	$X_{28} \wedge X_{30} \wedge X_{32}$	25:	$(X_5 \wedge X_{28}) \vec{\wedge} X_{10}$	49:	~~$X_1 \vec{\wedge} X_{10} \vec{\wedge} X_5$~~
2:	$X_{28} \wedge X_{30} \wedge X_{36}$	26:	$(X_{20} \wedge X_{28}) \vec{\wedge} X_{10}$	50:	~~$X_5 \vec{\wedge} X_{10} \vec{\wedge} X_1$~~
3:	$X_{28} \wedge X_{32} \wedge X_{34}$	27:	$(X_{22} \wedge X_{28}) \vec{\wedge} X_{10}$	51:	~~$X_1 \vec{\wedge} X_{10} \vec{\wedge} X_{15}$~~
4:	$X_{28} \wedge X_{34} \wedge X_{36}$	28:	$(X_{24} \wedge X_{28}) \vec{\wedge} X_{10}$	52:	~~$X_5 \vec{\wedge} X_{10} \vec{\wedge} X_{13}$~~
5:	$X_{18} \vec{\wedge} X_{10} \vec{\wedge} X_{38}$	29:	$(X_1 \wedge X_{28}) \vec{\wedge} X_{10}$	53:	$(X_5 \wedge X_{18}) \vec{\wedge} X_{10}$
6:	$(X_{18} \wedge X_{38}) \vec{\wedge} X_{10}$	30:	$(X_{20} \wedge X_{28}) \vec{\wedge} X_{10}$	54:	$(X_{18} \wedge X_{20}) \vec{\wedge} X_{10}$
7:	~~$X_1 \wedge X_5 \wedge X_{38}$~~	31:	$(X_{22} \wedge X_{28}) \vec{\wedge} X_{10}$	55:	$(X_{18} \wedge X_{22}) \vec{\wedge} X_{10}$
8:	$X_1 \wedge X_{15} \wedge X_{38}$ ◊	32:	$(X_{24} \wedge X_{28}) \vec{\wedge} X_{10}$	56:	$(X_{18} \wedge X_{24}) \vec{\wedge} X_{10}$
9:	$X_5 \wedge X_{13} \wedge X_{38}$ ◊	33:	~~$(X_1 \wedge X_{28}) \vec{\wedge} X_5$~~	57:	$(X_1 \wedge X_{18}) \vec{\wedge} X_{10}$
10:	$X_{13} \wedge X_{15} \wedge X_{38}$	34:	~~$(X_5 \wedge X_{28}) \vec{\wedge} X_1$~~	58:	$(X_{18} \wedge X_{20}) \vec{\wedge} X_{10}$
11:	$X_{27} \vec{\wedge} X_{10} \vec{\wedge} X_{38}$	35:	~~$(X_1 \wedge X_{28}) \vec{\wedge} X_{15}$~~	59:	$(X_{18} \wedge X_{22}) \vec{\wedge} X_{10}$
12:	$(X_{27} \wedge X_{38}) \vec{\wedge} X_{10}$	36:	~~$(X_5 \wedge X_{28}) \vec{\wedge} X_{13}$~~	60:	$(X_{18} \wedge X_{24}) \vec{\wedge} X_{10}$
13:	$X_5 \vec{\wedge} X_{10} \vec{\wedge} X_{28}$	37:	~~$X_{20} \vec{\wedge} (X_1 \wedge X_5)$~~	61:	$(X_5 \wedge X_{27}) \vec{\wedge} X_{10}$
14:	$X_{20} \vec{\wedge} X_{10} \vec{\wedge} X_{28}$	38:	~~$X_{22} \vec{\wedge} (X_1 \wedge X_5)$~~	62:	$(X_{20} \wedge X_{27}) \vec{\wedge} X_{10}$
15:	$X_{22} \vec{\wedge} X_{10} \vec{\wedge} X_{28}$	39:	~~$X_{24} \vec{\wedge} (X_1 \wedge X_5)$~~	63:	$(X_{22} \wedge X_{27}) \vec{\wedge} X_{10}$
16:	$X_{24} \vec{\wedge} X_{10} \vec{\wedge} X_{28}$	40:	$X_{20} \vec{\wedge} (X_1 \wedge X_{15})$ ◊	64:	$(X_{24} \wedge X_{27}) \vec{\wedge} X_{10}$
17:	$X_1 \vec{\wedge} X_{10} \vec{\wedge} X_{28}$	41:	$X_{22} \vec{\wedge} (X_1 \wedge X_{15})$ ◊	65:	$(X_1 \wedge X_{27}) \vec{\wedge} X_{10}$
18:	$X_{20} \vec{\wedge} X_{10} \vec{\wedge} X_{28}$	42:	$X_{24} \vec{\wedge} (X_1 \wedge X_{15})$ ◊	66:	$(X_{20} \wedge X_{27}) \vec{\wedge} X_{10}$
19:	$X_{22} \vec{\wedge} X_{10} \vec{\wedge} X_{28}$	43:	$X_{20} \vec{\wedge} (X_5 \wedge X_{13})$ ◊	67:	$(X_{22} \wedge X_{27}) \vec{\wedge} X_{10}$
20:	$X_{24} \vec{\wedge} X_{10} \vec{\wedge} X_{28}$	44:	$X_{22} \vec{\wedge} (X_5 \wedge X_{13})$ ◊	68:	$(X_{24} \wedge X_{27}) \vec{\wedge} X_{10}$
21:	~~$X_1 \vec{\wedge} X_5 \vec{\wedge} X_{28}$~~	45:	$X_{24} \vec{\wedge} (X_5 \wedge X_{13})$ ◊	69:	~~$(X_5 \wedge X_{15}) \vec{\wedge} X_{13}$~~
22:	~~$X_5 \vec{\wedge} X_1 \vec{\wedge} X_{28}$~~	46:	$X_{20} \vec{\wedge} (X_{13} \wedge X_{15})$	70:	~~$(X_1 \wedge X_{13}) \vec{\wedge} X_{15}$~~
23:	~~$X_1 \vec{\wedge} X_{15} \vec{\wedge} X_{28}$~~	47:	$X_{22} \vec{\wedge} (X_{13} \wedge X_{15})$	71:	~~$(X_1 \wedge X_{13}) \vec{\wedge} X_5$~~
24:	~~$X_5 \vec{\wedge} X_{13} \vec{\wedge} X_{28}$~~	48:	$X_{24} \vec{\wedge} (X_{13} \wedge X_{15})$	72:	~~$(X_5 \wedge X_{15}) \vec{\wedge} X_1$~~

Tabelle 7.4: Ereignissequenzen mit Rang zwei und drei. Mehrfach enthaltene Ereignissequenzen sind unterringelt, nichtminimale Ereignissequenzen sind ~~durchgestrichen~~, „teilweise“ nichtminimale Ereignissequenzen sind mit einem ◊ markiert.

Minimale Form und MCSS der Ausfallfunktion

Insgesamt 12 der 77 Ereignissequenzen in Tabelle 7.4 sind doppelt vorhanden und entfallen daher wegen des Idempotenzgesetzes. Weitere 20 Ereignissequenzen sind nicht minimal und entfallen ebenfalls. Die erweiterten Ereignissequenzen Nummer 8 und 9 sowie 40 bis 45

$$\begin{aligned}&\big[X_1 \wedge X_{15} \wedge X_{38}\big], \big[X_5 \wedge X_{13} \wedge X_{38}\big],\\ &\big[X_{20} \vec{\wedge} (X_1 \wedge X_{15})\big], \big[X_{22} \vec{\wedge} (X_1 \wedge X_{15})\big], \big[X_{24} \vec{\wedge} (X_1 \wedge X_{15})\big],\\ &\big[X_{20} \vec{\wedge} (X_5 \wedge X_{13})\big], \big[X_{22} \vec{\wedge} (X_5 \wedge X_{13})\big], \big[X_{24} \vec{\wedge} (X_5 \wedge X_{13})\big]\end{aligned} \tag{7.45}$$

sind gegenüber den MCSS von Rang zwei

$$\big[X_1 \vec{\wedge} X_{15}\big] \qquad \text{und} \qquad \big[X_5 \vec{\wedge} X_{13}\big] \tag{7.46}$$

„teilweise“ nichtminimal. Es ist daher erforderlich, die erweiterten Ereignissequenzen aufzulösen, um die minimalen von den nichtminimalen Anteilen zu trennen.

Beispielsweise an der Ereignissequenz $X_{20} \vec{\wedge} (X_1 \wedge X_{15})$ durchgeführt, ergeben sich (ohne SAND Verknüpfungen) mit

$$X_{20} \vec{\wedge} (X_1 \wedge X_{15}) \;=\; \big[(X_1 X_{20}) \vec{\wedge} X_{15}\big] \vee \big[(X_{15} X_{20}) \vec{\wedge} X_1\big] \tag{7.47}$$

zwei nichterweiterte Ereignissequenzen, von denen die Erste gegenüber $X_1 \vec{\wedge} X_{15}$ nichtminimal ist. Analog dazu ist auch bei

$$X_1 \wedge X_{15} \wedge X_{38} \;=\; \big[(X_1 \vec{\wedge} X_{15}) \wedge X_{38}\big] \vee \big[(X_{15} \vec{\wedge} X_1) \wedge X_{38}\big] \tag{7.48}$$

nur der zweite Teilterm minimal. Dieser ist zunächst in eine TDNF zu überführen, sodass

$$(X_{15} \vec{\wedge} X_1) \wedge X_{38} \;=\; \big[X_{15} \vec{\wedge} X_1 \vec{\wedge} X_{38}\big] \vee \big[(X_{15} \wedge X_{38}) \vec{\wedge} X_1\big] \;. \tag{7.49}$$

Aus den zwei teilweise nichtminimalen Ereignissequenzen Nummer 8 und 9 werden somit vier minimale MCSS.

Tabelle 7.5 zeigt die bereinigte Form, in der nur noch die MCSS der Ausfallfunktion ϖ von Rang zwei und drei aufgeführt sind.

		(erweiterte) MCSS von Rang zwei:			
1:	$X_1 \vec{\wedge} X_5$	3:	$X_1 \vec{\wedge} X_{15}$	5:	$X_{28} \wedge X_{38}$
2:	$X_5 \vec{\wedge} X_1$	4:	$X_5 \vec{\wedge} X_{13}$		
		(erweiterte) MCSS von Rang drei:			
1:	$X_{28} \wedge X_{30} \wedge X_{32}$	15:	$(X_5 \wedge X_{28}) \vec{\wedge} X_{10}$	29:	$X_{20} \vec{\wedge} X_{10} \vec{\wedge} X_{28}$
2:	$X_{28} \wedge X_{30} \wedge X_{36}$	16:	$(X_{20} \wedge X_{28}) \vec{\wedge} X_{10}$	30:	$X_{22} \vec{\wedge} X_{10} \vec{\wedge} X_{28}$
3:	$X_{28} \wedge X_{32} \wedge X_{34}$	17:	$(X_{22} \wedge X_{28}) \vec{\wedge} X_{10}$	31:	$X_{24} \vec{\wedge} X_{10} \vec{\wedge} X_{28}$
4:	$X_{28} \wedge X_{34} \wedge X_{36}$	18:	$(X_{24} \wedge X_{28}) \vec{\wedge} X_{10}$	32:	$X_1 \vec{\wedge} X_{10} \vec{\wedge} X_{28}$
5:	$X_{18} \vec{\wedge} X_{10} \vec{\wedge} X_{38}$	19:	$(X_1 \wedge X_{28}) \vec{\wedge} X_{10}$	33:	$(X_5 \wedge X_{18}) \vec{\wedge} X_{10}$
6:	$(X_{18} \wedge X_{38}) \vec{\wedge} X_{10}$	20:	$(X_{15} \wedge X_{20}) \vec{\wedge} X_1$	34:	$(X_{18} \wedge X_{20}) \vec{\wedge} X_{10}$
7:	$X_{15} \vec{\wedge} X_1 \vec{\wedge} X_{38}$	21:	$(X_{15} \wedge X_{22}) \vec{\wedge} X_1$	35:	$(X_{18} \wedge X_{22}) \vec{\wedge} X_{10}$
8:	$(X_{15} \wedge X_{38}) \vec{\wedge} X_1$	22:	$(X_{15} \wedge X_{24}) \vec{\wedge} X_1$	36:	$(X_{18} \wedge X_{24}) \vec{\wedge} X_{10}$
9:	$X_{13} \vec{\wedge} X_5 \vec{\wedge} X_{38}$	23:	$(X_{13} \wedge X_{20}) \vec{\wedge} X_5$	37:	$(X_1 \wedge X_{18}) \vec{\wedge} X_{10}$
10:	$(X_{13} \wedge X_{38}) \vec{\wedge} X_5$	24:	$(X_{13} \wedge X_{22}) \vec{\wedge} X_5$	38:	$(X_5 \wedge X_{27}) \vec{\wedge} X_{10}$
11:	$X_{13} \wedge X_{15} \wedge X_{38}$	25:	$(X_{13} \wedge X_{24}) \vec{\wedge} X_5$	39:	$(X_{20} \wedge X_{27}) \vec{\wedge} X_{10}$
12:	$X_{27} \vec{\wedge} X_{10} \vec{\wedge} X_{38}$	26:	$X_{20} \vec{\wedge} (X_{13} \wedge X_{15})$	40:	$(X_{22} \wedge X_{27}) \vec{\wedge} X_{10}$
13:	$(X_{27} \wedge X_{38}) \vec{\wedge} X_{10}$	27:	$X_{22} \vec{\wedge} (X_{13} \wedge X_{15})$	41:	$(X_{24} \wedge X_{27}) \vec{\wedge} X_{10}$
14:	$X_5 \vec{\wedge} X_{10} \vec{\wedge} X_{28}$	28:	$X_{24} \vec{\wedge} (X_{13} \wedge X_{15})$	42:	$(X_1 \wedge X_{27}) \vec{\wedge} X_{10}$

Tabelle 7.5: MCSS mit Rang zwei und drei. Diese Tabelle ist eine um Nichtminimalitäten und Doppelungen bereinigte Variante von Tabelle 7.4.

Ergebnisse

Die MCSS der Ausfallfunktion sind alle von Rang zwei oder höher. Das zeigt, dass im modellierten System keine Einzelfehler zu einer Verletzung des Sicherheitsziels führen können. Die geforderte „Einfehler-Festigkeit“ wird daher vom Beispielsystem erbracht, vgl. die eingangs in Kapitel 7.2 genannten Ziele der TFTA.

Die wichtigsten Kombinationen gefährlicher Fehler, die zu einer Verletzung des Sicherheitsziels führen, sind die MCSS von Rang zwei und drei. Die fünf MCSS von Rang zwei umfassen

1. aufeinander folgende Doppelfehler der Sensoren. In diesem Fall würde EN1 mit dem ersten Sensorfehler aktiviert und SAF mit dem zweiten Sensorfehler aktiviert. Beide Fehler können in beliebiger Reihenfolge eintreten.

2. einen Sensorfehler in Kombination mit einem µC Fehler. Hierbei muss der Sensorfehler vor dem µC Fehler eintreten, da sonst die Schaltlogik in L nicht befriedigt wird.

3. einem Fehler von T3 in Kombination mit einem Fehler in L, der beide Endstufen aktiviert. Beide Fehler können in beliebiger Reihenfolge eintreten.

Als MCSS von Rang drei erscheinen u. a.

1. Doppelfehler in High- und Low-Side des Treiber-IC in Kombination mit einem internen Fehler in T3. Hierbei ist keine Sequenzlogik zu berücksichtigen. Dies sind insbesondere die Nummern 1 bis 4 in Tabelle 7.5.

2. Fehler im System-ASIC in Kombination mit µC und / oder Sensorfehlern. Dies sind insbesondere die Nummern 20 bis 28 in Tabelle 7.5.

3. Fehler im Watchdog oder Notaus-Schalter in Kombination mit ASIC Fehlern, wobei beide vor µC Fehlern eintreten müssen, vgl. z. B. die Nummern 34 bis 36 und 39 bis 41 in Tabelle 7.5.

4. Fehler in einem Sensor in Kombination mit einem Fehler im Watchdog oder Notaus-Schalter, wobei beide vor µC Fehlern eintreten müssen, vgl. z. B. die Nummern 33, 37, 38, 42 in Tabelle 7.5.

7.4 Quantifizierung und Berechnung der TOP Ausfallkenngrößen

Die quantitative Analyse des temporalen Fehlerbaums dient dem Nachweis, dass das System die in ISO 26262 für ASIL D geforderte Gefährdungsrate unterschreitet. Der Grenzwert hierfür liegt bei höchstens $1 \cdot 10^{-8} \frac{1}{\mathrm{h}}$ in jeder Betriebsstunde während der gesamten Lebensdauer.

Dazu ist zu zeigen, dass die Ausfallrate des TOP Ereignisses λ_{TOP} diesen Grenzwert unterschreitet.

Wegen $f_{TOP}(T_M) \approx \lambda_{TOP}$, vgl. (5.59), genügt im ersten Ansatz die Berechnung der Ausfalldichte des TOP.

Weiterhin wird ein iteratives Vorgehen gewählt, welches den Aufwand reduziert und in ähnlicher Form oftmals in realen FTA Berechnungen zum Einsatz kommt. Zunächst ist mit einem Näherungsverfahren und konservativ abgeschätzten Ausfallraten eine erste „Zielorientierung“ durchzuführen.

Der Nachweis gilt als erbracht, wenn auf diese Weise die normativ geforderten Werte unterschritten werden. Ist dies nicht möglich, so können im nächsten Schritt – ggf. beschränkt

auf die wichtigsten Beiträger – die verwendeten Ausfallraten exakter bestimmt werden und / oder statt dem Näherungsverfahren die exakten Werte berechnet werden. Das Ergebnis lässt sich so sukzessive mit vergleichsweise geringem Aufwand verbessern. Abbruchbedingung ist die Unterschreitung der normativen Grenzwerte.

Im Folgenden wird daher auf eine Überführung der MCSS in eine disjunkte Form verzichtet. Stattdessen kommt das Näherungsverfahren aus Kapitel 5.5 zum Einsatz. Dies entspricht dem untersten Pfad in Abbildung 3.1 auf Seite 22.

Die Quantifizierung der Ausfallfunktion ϖ erfolgt auf Basis ihrer MCSS aus Tabelle 7.5. Die Basisereignisse erhalten einheitlich eine Ausfallrate von $\lambda = 10^{-6}\,\frac{1}{\mathrm{h}}$.

Tabelle 7.6 zeigt die Ausfallwahrscheinlichkeit und Ausfalldichte nach (5.74) und (5.75) für jede MCSS aus Tabelle 7.5. Die Missionszeit ist auf $T_M = 1000\mathrm{h}$ angesetzt.

	MCSS von Rang zwei:				
1:	$F{=}5{\cdot}10^{-7}; f{=}1{\cdot}10^{-9}\,\frac{1}{\mathrm{h}}$	3:	$F{=}5{\cdot}10^{-7}; f{=}1{\cdot}10^{-9}\,\frac{1}{\mathrm{h}}$	5:	$F{=}1{\cdot}10^{-6}; f{=}2{\cdot}10^{-9}\,\frac{1}{\mathrm{h}}$
2:	$F{=}5{\cdot}10^{-7}; f{=}1{\cdot}10^{-9}\,\frac{1}{\mathrm{h}}$	4:	$F{=}5{\cdot}10^{-7}; f{=}1{\cdot}10^{-9}\,\frac{1}{\mathrm{h}}$		
	MCSS von Rang drei:				
1:	$F{=}1{\cdot}10^{-9}; f{=}3{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	15:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	29:	$F{=}\frac{1}{6}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
2:	$F{=}1{\cdot}10^{-9}; f{=}3{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	16:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	30:	$F{=}\frac{1}{6}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
3:	$F{=}1{\cdot}10^{-9}; f{=}3{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	17:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	31:	$F{=}\frac{1}{6}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
4:	$F{=}1{\cdot}10^{-9}; f{=}3{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	18:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	32:	$F{=}\frac{1}{6}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
5:	$F{=}\frac{1}{6}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	19:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	33:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
6:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	20:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	34:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
7:	$F{=}\frac{1}{6}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	21:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	35:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
8:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	22:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	36:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
9:	$F{=}\frac{1}{6}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	23:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	37:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
10:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	24:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	38:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
11:	$F{=}1{\cdot}10^{-9}; f{=}3{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	25:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	39:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
12:	$F{=}\frac{1}{6}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	26:	$F{=}\frac{2}{3}{\cdot}10^{-9}; f{=}2{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	40:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
13:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	27:	$F{=}\frac{2}{3}{\cdot}10^{-9}; f{=}2{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	41:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$
14:	$F{=}\frac{1}{6}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	28:	$F{=}\frac{2}{3}{\cdot}10^{-9}; f{=}2{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$	42:	$F{=}\frac{1}{3}{\cdot}10^{-9}; f{=}1{\cdot}10^{-12}\,\frac{1}{\mathrm{h}}$

Tabelle 7.6: Ausfallwahrscheinlichkeit und Ausfalldichte nach (5.74) und (5.75) für jede MCSS aus Tabelle 7.5.

Die Kenngrößen auf TOP Ebene berechnen sich nach (5.55) bzw. (5.56) als die Summe der Beiträge der MCSS. Mit den Werten aus Tabelle 7.6 ergeben sich

$$F_{TOP}(T_M) \approx 3{,}017 \cdot 10^{-6} \qquad \text{und} \tag{7.50}$$

$$f_{TOP}(T_M) \approx 6{,}055 \cdot 10^{-9}\,\frac{1}{\mathrm{h}}\ . \tag{7.51}$$

Bereits mit dieser ersten Näherungslösung kann der nach ISO 26262 normkonforme Nachweis für bis zu ASIL D geführt werden, da die Ausfalldichte des TOP in (7.51) den normativen Grenzwert von $1 \cdot 10^{-8}\,\frac{1}{\mathrm{h}}$ unterschreitet.

Anmerkung: Eine herkömmliche FTA müsste anstelle der PAND Gatter normale AND Gatter einsetzen. Dies würde sich insbesondere auf die Ausfalldichte der Minimalschnitte von Rang zwei auswirken. Diese Minimalschnitte wären dieselben wie die MCSS von Rang zwei, allerdings mit einer AND Verbindung. Entsprechend würde sich bei einer Booleschen FTA die Ausfalldichte des TOP gegenüber dem TFTA Ergebnis auf $> 1 \cdot 10^{-8}\,\frac{1}{\mathrm{h}}$ nahezu verdoppeln und den normativen Grenzwert überschreiten.

7.5 Diskussion

Die Analyse des praxisnahen Systems aus Kapitel 7.1 zeigt, dass sich die TFTA-Methode nicht auf die Modellierung sehr kleiner Beispiele beschränken muss. Damit ergänzt Kapitel 7 die theoretische Beschreibung des TFTA-Ansatzes in den Kapiteln 4 und 5 sowie die Ausführungen zur grundsätzlichen Anwendung der TFTA in Kapitel 6.

Die Nähe zur herkömmlichen FTA zeigt sich in der Erstellung des temporalen Fehlerbaums in den Abbildungen 7.2 bis 7.4. Dabei entsteht bis auf die Wahl der temporalen Gatter gegenüber der Booleschen FTA kein größerer Aufwand.

In diesem temporalen Fehlerbaum existieren mehrfache Vermaschungen von Basisereignissen und ganzen Teilbäumen. So finden sich z. B. die Ereignisse unter „µC Fehler Signale“ unterhalb eines temporalen Gatters („L kommandierter Fehler“). Dieselben Ereignisse sind zugleich Teil des rein Booleschen Rest-Fehlerbaums („kommand. Fehler T3“). Weiterhin ist z. B. das Basisereignis „10 – µC allg. Fehler aktiviert SAF“ in verschiedenen, ansonsten getrennten Teilbäumen unterhalb unterschiedlicher PAND Gatter zu finden.

Solche Vermaschungen würden z. B. in der DFT Methode den Aufwand stark ansteigen lassen, da wegen der erforderlichen Modulbildung mit Unterscheidung zwischen dynamischen und nichtdynamischen Modulen nahezu der komplette Fehlerbaum als dynamisches Modul, d. h. im Falle der DFT als Markov-Kette, zu modellieren wäre.

Die ausführliche qualitative Auswertung des temporalen Fehlerbaums in Kapitel 7.3 zeigt hingegen, dass die TFTA mit ihren temporalen Vereinfachungsregeln solche Vermaschungen aufzulösen vermag.

Zwar steigt auch hierfür der Berechnungsaufwand schnell an, insbesondere durch die temporalen Distributivgesetze. Allerdings handelt es sich bei den notwendigen Berechnungen primär um Manipulationen von Zeichenketten. Diese sind jedoch i. d. R. weniger aufwändig als die in anderen Methoden notwendige Lösung exponentiell wachsender Markov-Modelle oder Simulation entsprechend großer Petri-Netze.

Die Analyse der MCSS in Kapitel 7.3.3 orientiert sich wiederum stark an der Booleschen FTA. Unter anderem bestätigt sich die Eignung der TFTA für echte qualitative Analysen. Wie schon in Kapitel 6 dargelegt, ist dies einer der wesentlichen Vorteile der TFTA.

Auch die in Kapitel 7.4 gezeigte Quantifizierung orientiert sich an dem in der Praxis häufig anzutreffenden stufenweisen Vorgehen. Dieses erlaubt einerseits eine der Fragestellung angepasste Modellierungsgenauigkeit – und damit zusammenhängend: mehr oder weniger Aufwand – und andererseits die Konzentration der verfügbaren Ressourcen auf „die wichtigsten“ Beiträger. Beides ist so mit z. B. der DFT nicht in gleichem Maße möglich.

8 Zusammenfassung und Ausblick

> I want electricity to become so cheap
> that only the rich can afford candles.
>
> *(Thomas Alva Edison)*

Der in dieser Dissertation beschriebene neue Ansatz einer temporalen Fehlerbaumanalyse, kurz TFTA, erweitert die Boolesche FTA um die Möglichkeit, Ereignissequenzen abzubilden. Dies ermöglicht eine im Vergleich zur herkömmlichen FTA realistischere Modellierung des Ausfallverhaltens komplexer, dynamischer Systeme.

Die neue TFTA nutzt eine hier neu beschriebene temporale Logik. Sie unterscheidet sich darin wesentlich von der Mehrzahl existierender Ansätze mit ähnlichen Zielsetzungen, welche das FTA-Modell ganz oder teilweise in ein Zustandsmodell überführen, dort die zeitlichen Effekte berücksichtigen und die so berechneten Ergebnisse wieder in den Fehlerbaum zurückführen. Die TFTA hebt sich von solchen zustandsbasierten Modellierungen insbesondere dadurch ab, dass

- sie eine Erweiterung der Booleschen Algebra und Logik nutzt,
- ihre Notation, Begriffe und insbesondere auch Prozessschritte und Arbeitsprodukte aus der herkömmlichen FTA übernommen werden,
- sie sowohl qualitative als auch quantitative Analysen und Berechnungen mit Berücksichtigung von Sequenzinformationen ermöglicht.

Im Gegensatz zu weiteren bekannten Ansätzen, zeitliche Informationen ebenfalls durch „zeitliche Logiken“ im Fehlerbaum zu erfassen, ist die TFTA zudem deutlich einfacher gehalten. Die TFTA ist insbesondere kein weiterer Versuch, eine formalisierte FTA-Logik zu schaffen, die sich an die Modellierung von Software-Systemen richtet. Stattdessen betont die TFTA stärker praxisbezogene Eigenschaften wie intuitive Nutzbarkeit, Lesbarkeit und Verständlichkeit der Logik-Ausdrücke und Ergebnisse, Übertragbarkeit realer Ausfall-Effekte in die Modell-Logik sowie Skalierbarkeit.

Die temporale Logik der TFTA verwendet die Booleschen Operationen der Konjunktion, Disjunktion und Negation. Sie unterscheidet darüber hinaus mit den zwei neuen temporalen Operationen PAND und SAND zwei Arten von „spezialisierten Konjunktionstermen“, die Reihenfolgen bzw. Gleichzeitigkeit von Ereignissen beschreiben.

Mit Hilfe der bekannten Booleschen Algebra und eines Satzes an temporalen Logikregeln ist es dann möglich, komplexe temporale Terme in eine temporale disjunktive Normalform (TDNF) zu überführen, die aus einzelnen Ereignissequenzen besteht. Analog zu den Booleschen Schnitten

eines Fehlerbaums lassen sich diese Ereignissequenzen auf eine minimale Form, die sogenannten MCSS reduzieren.

In einem weiteren Verfahrensschritt werden die MCSS in eine disjunkte Form überführt. Diese disjunkte Form der TDNF eignet sich für eine direkte Quantifizierung und ermöglicht damit eine probabilistische Analyse.

Anders als die herkömmliche FTA erlaubt die quantitative TFTA somit die Berechnung der Zuverlässigkeitskenngrößen Ausfallwahrscheinlichkeit, Ausfalldichte und Ausfallrate für das TOP eines Fehlerbaums unter Berücksichtigung von Sequenzinformationen, ohne auf zustandsbasierte Modelle auszuweichen.

Einschätzung der Arbeit

Ursprünglich sollte die Ableitung einer eigenen temporalen Logik zuvorderst die Probleme lösen, die mit den bekannten dynamischen Erweiterungen der FTA auf Basis von Markov-Ketten einhergehen. Auf Grund der großen Verbreitung des DFT Ansatzes [37] – als Vertreter solcher dynamischen Erweiterungen – liegt es nahe, das in dieser Arbeit Erreichte mit dem DFT Ansatz zu vergleichen.

In Bezug auf den Berechnungsaufwand ist allgemein zu bedenken, dass eine Berücksichtigung der Ereignissequenzen einen Mehraufwand gegenüber der Booleschen FTA bedeutet. Dies trifft auf die zustandsbasierten Erweiterungen ebenso zu wie auf um temporale Effekte erweiterte Logiken. Der Mehraufwand ist problematisch, insbesondere da bereits die Ermittlung disjunkter Minimalschnitte der Booleschen FTA zu exponentiell wachsender Komplexität führt. Es ist jedoch nicht das Ziel der TFTA Methode, hierfür eine Lösung zu erreichen.

Einige Probleme der TFTA begründen sich grundsätzlich aus der Art der verwendeten temporalen Logik. Da Reihenfolgen-Aussagen ausschließlich für die Eintretenszeitpunkte von Ereignissen getätigt werden, lassen sich „andauernde“ Ausfallereignisse nicht mit PAND und SAND Gattern abbilden. Stattdessen sind solche Ereignisse mit klassischen AND Gattern zu erfassen. Im Vergleich zum DFT Ansatz stellt dies keine Verschlechterung dar. Auch die dort verwedeten Markov-Ketten lassen Zustandswechsel nur durch „triggernde“ Ausfallereignisse zu und erfassen daher keine „andauernden“ Ausfallereignisse. Im DFT Ansatz lässt sich dieses Manko wegen der erforderlichen Modularisierung und der fehlenden Möglichkeit von Vermaschung lediglich nicht so einfach erkennen.

Eine wesentliche Einschränkung des DFT Ansatzes ist die Modulbildung. Diese verhindert unter Umständen eine logisch korrekte Vermaschung über die Grenzen dynamischer Fehlerbaum-Gatter hinweg. Im Vergleich dazu erlaubt die TFTA eine solche Vermaschung. Somit ist es möglich, eine größere Zahl von Sequenz-Effekten zu berücksichtigen.

Eine weitere wesentliche Einschränkung betrifft die qualitative Auswertung von Minimalschnitten im DFT Ansatz. Der Wechsel in die Zustandsebene erzwingt entweder in Minimalschnitten neben den Basisereignissen auch „Meta-Ereignisse“, hinter denen sich ganze Markov-Modelle verbergen. Alternativ erfolgt die qualitative Auswertung ohne Berücksichtigung der Sequenzen. Im Vergleich dazu zeigen die (erweiterten) Ereignissequenzen der TFTA die exakten Sequenzinformationen der an Ausfällen des TOP beteiligten Basisereignisse. Die TFTA erlaubt somit analog zur herkömmlichen FTA aussagekräftige und effiziente qualitative Analysen.

Die TFTA ermöglich zudem ebenso wie der DFT Ansatz probabilistische Berechnungen der TOP Ausfallrate / Ausfallwahrscheinlichkeit. Diese Quantifizierung kann einerseits mit vergleichsweise hohem Aufwand durchgeführt werden mit dem Ziel die exakten Ausfallkenngrößen des TOP zu berechnen. Andererseits steht ein Näherungsverfahren zur Verfügung, welches den Berechnungsaufwand deutlich reduziert.

Drei weitere Argumente sprechen in Bezug auf den Berechnungsaufwand für die TFTA: Erstens steigt die Größe der für die DFT zu lösenden Differentialgleichungssysteme exponentiell mit der Anzahl der in einem dynamischen Modul berücksichtigten Komponentenausfälle. Der Mehraufwand für eine TFTA (gegenüber der Booleschen FTA) ist somit zumindest vergleichbar zum Mehraufwand für eine DFT – bei, wie oben festgestellt, aussagekräftigeren Ergebnissen. Großteils handelt es sich zweitens bei den Berechnungen der TFTA jedoch um Umformungen von Zeichenketten. Diese erscheinen i. d. R. weniger aufwändig als die Lösung exponential anwachsender Zustandsmodelle. Drittens besteht mit dem TFTA Näherungsverfahren tatsächlich eine Möglichkeit zur effektiven Reduzierung des Aufwandes unter Inkaufnahme von Ungenauigkeiten, z. B. als Basis für eine mehrstufige Analyse.

Somit lässt sich festhalten, dass die TFTA einen vollwertigen Ersatz für die PAND Gatter des DFT Ansatzes darstellt und darüber hinaus auch methodische und anwendungstechnische Vorteile bietet.

Mögliche weiterführende Untersuchungen

Im Rahmen dieser Arbeit konnten nicht alle entdeckten Themenfelder vollständig untersucht und bearbeitet werden. So werden zwar SAND Verknüpfungen als (strukturelle) Abhängigkeiten zwischen Ausfallereignissen qualitativ definiert und berücksichtigt, für die Quantifizierung aber ausgeblendet. Angesichts der großen Bedeutung abhängiger Ausfälle, oftmals auch vereinfachend CCF genannt, erscheint die Erweiterung des hier beschriebenen TFTA Ansatzes um solche Abhängigkeiten vielversprechend. Die vorliegenden Arbeit beschränkt sich zudem auf nicht reparierbare Ausfälle. Möglicherweise lassen sich die temporale Logik der TFTA und auch die quantitative TFTA auf reparierbare Ausfälle erweitern. Ebenfalls interessant könnte es sein, vereinfachte Verfahren zur Ermittlung disjunkter temporaler Terme aus einer TDNF zu entwickeln. Dabei könnte man sich ggf. an aus der Booleschen Algebra bekannten Verfahren, wie den Zerlegungsverfahren nach Abraham [80] oder Heidtmann [81], orientieren. Auch eine Untersuchung möglicher Synergien zwischen der TFTA Logik und der BDD Methode [86] scheint angeraten. Generell besteht sicherlich ein großer Bedarf an verbesserten Algorithmen für eine praktischen Nutzung der TFTA. Mögliche erscheint insbesondere auch eine Beteilung an der Weiterentwicklung von Open-Source Fehlerbaum-Programmen, wie z. B. OpenFTA [87].

9 Literaturverzeichnis

[1] Flörecke, K. D.: Milliarden für mehr Sicherheit. In: *Automobilwoche 24* (2004), S. 14

[2] Meyer, M.: *Methoden zur Analyse von Garantiedaten für Sicherheits- und Zuverlässigkeitsprognosen von Komponenten und Baugruppen im Kraftfahrzeug.* Wuppertal, Bergische Universität Wuppertal, Diss., 2003

[3] *ISO DIS 26262 Strassenfahrzeuge – Funktionssicherheit. Technical Committee ISO/TC 22, Road vehicles, Subcommittee SC 3, Electric and Electronic Equipment (in 10 Teilen).* 2009

[4] *IEC 61508 Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbar elektrischer Systeme (in 7 Teilen).* 2002

[5] Veseley, W. E. u. a.: *NUREG-0492 Fault tree handbook.* Washington, D.C.: U.S. Nuclear Regulatory Commission, 1981

[6] *IEC 61025 Edition 2.0 Fault tree analysis (FTA).* 2006

[7] *DIN 25424 Fehlerbaumanalyse (in 2 Teilen).* Berlin, 1981 & 1990

[8] Schneeweiss, Winfrid G.: *Die Fehlerbaum-Methode.* Hagen: LiLoLe-Verlag, 1999

[9] Verband der Automobilindustrie: *Sicherung der Qualität vor Serieneinsatz.* Bd. 4: *Fehlerbaumanalyse (Fault Tree Analysis FTA).* 2003

[10] Schilling, Simon J.: Bedeutung und Modellierung abhängiger Ausfälle in automotiven E / E-Systemen. In: *safetronic.2006.* Munich, 2006

[11] Heidtmann, K.D.: Deterministic reliability-modeling of dynamic redundancy. In: *IEEE Transactions on Reliability* 41 (1992), Sep, Nr. 3, S. 378–385. `http://dx.doi.org/10.1109/24.159802`. – DOI 10.1109/24.159802. – ISSN 0018–9529

[12] Manian, R. ; Bechta Dugan, J. ; Coppit, D. ; Sullivan, K.J.: Combining various solution techniques for dynamic fault tree analysis of computer systems. In: *High-Assurance Systems Engineering Symposium, 1998. Proceedings. Third IEEE International*, 1998, S. 21–28

[13] Hauschild, Jan ; Meyna, Arno: Monte Carlo techniques for modelling and analysing the reliability and safety of modern automotive applications. In: Guedes (Hrsg.) ; Soares (Hrsg.) ; Zio (Hrsg.): *Safety and Reliability for Managing Risk, ESREL 06.* London: Taylor and Francis Group, 2006

[14] Meyna, Arno ; Pauli, Bernhard: *Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik: quantitative Bewertungsverfahren.* München: Hanser, 2003

[15] *DIN 40041: 1990-12: Zuverlässigkeit - Begriffe.* Berlin, 1990

[16] Bitter, Peter u. a.: *Technische Zuverlässigkeit - Problematik, math. Grundlagen, Untersuchungsmethoden, Anwendungen.* 3., neubearb. u. erw. Auflage. Berlin: Springer, 1986

[17] Isograph Ltd.: *AttackTree+ V1.0 Technical Specification.* Warrington, UK, 2005

[18] Sulfredge, C. D. ; Sanders, Robert L. ; Peplow, Douglas E. ; Morris, Robert H.: Graphical Expert System for Analyzing Nuclear Facility Vulnerability. In: *Transactions of Interservice/Industry Training, Simulation and Education Conference (I/ITSEC).* Orlando, Florida, 2002

[19] Siu, Nathan O.: Dynamic Approaches – Issues and Methods: An Overview. In: [41], S. 3–7

[20] NRC: *Reactor safety study. An Assessment of accident risks in U. S. commercial nuclear power plants. WASH-1400. NUREG-75/014.* Washington: NRC, 1975

[21] Aldemir, Tunc: Dynamic Approaches – Applications: An Overview. In: [41], S. 81–84

[22] Woltereck, Martin: *Dynamische Zuverlässigkeitsanalyse mit anlagenspezifischen Störfallsimulatoren*, Technische Universität München, Diss., 2000

[23] Fahrmeir, L. ; Kaufmann, H. ; Ost, F.: *Stochastische Prozesse.* München: Hanser Verlag, 1982

[24] Hauschild, Jan: *Beitrag zur Modellierung stochastischer Prozesse in der Sicherheits- und Zuverlässigkeitstechnik mittels Monte-Carlo-Simulation unter Berücksichtigung dynamischer Systemänderungen*, Bergische Universität Wuppertal, Diss., 2007

[25] Leveson, N. G.: *White Paper on Approaches to Safety Engineering.* Massachusetts, 2003

[26] Watson, H. A.: *Launch Control Safety Study.* Murray Hill, NJ: Bell Telephone Laboratories, 1961

[27] Amari, S.V. ; Akers, J.B.: Reliability analysis of large fault trees using the Vesely failure rate. In: *Reliability and Maintainability, 2004 Annual Symposium - RAMS*, 2004, S. 391–396

[28] Skorek, T.: Determination of Input Uncertainties of Uncertainty and Sensitivity Analyses. In: *Probabilistic Safety Assessment and Management, PSAM 07 - ESREL 04.* Berlin: Springer, 2004

[29] Dutuit, Y. ; Rauzy, A.: Efficient algorithms to assess component and gate importance in fault tree analysis. In: *Reliability Engineering and System Safety* 72 (2001), Nr. 2, S. 213 – 222. http://dx.doi.org/10.1016/S0951-8320(01)00004-7. – DOI 10.1016/S0951–8320(01)00004–7. – ISSN 0951–8320

[30] Woltereck, Martin ; Vollmar, Ralph: Reliability Analysis of Automotive Systems: Quantification of Data Uncertainty. In: *Probabilistic Safety Assessment and Management, PSAM 07 - ESREL 04.* Berlin: Springer, 2004

[31] Veseley, W. E. u. a.: *Fault Tree Handbook with Aerospace Applications.* Washington, D.C.: NASA Office of Safety and Mission Assurance, 2002

[32] Limbourg, P. u. a.: Fault tree analysis in an early design stage using the Dempster-Shafer theory of evidence. In: Aven (Hrsg.) ; Vinnem (Hrsg.): *Risk, Reliability and Societal Safety, ESREL 07*. London: Taylor and Francis Group, 2007

[33] Weber, Wolfgang ; Tondok, Heidemarie ; Bachmayer, Michael: Enhancing Software Safety by Fault Trees: Experiences from Application to Flight Critical Software. In: *SAFECOMP 2003*, 2003, S. 289–302

[34] Heidtmann, Klaus: *Teubner-Texte zur Informatik*. Bd. 21: *Zuverlässigkeitsbewertung technischer Systeme*. B. G. Teubner Verlagsgesellschaft, 1997

[35] Andrews, J. D.: To Not or Not to Not! In: *18th International System Safety Conference*, 2000, S. 267–275

[36] Gumm, Heinz-Peter ; Poguntke, Werner: *Boolesche Algebra*. Mannheim: Bibliogr. Inst., 1981 (BI-Hochschultaschenbücher)

[37] Dugan, J.B. ; Bavuso, S.J. ; Boyd, M.A.: Dynamic fault-tree models for fault-tolerant computer systems. In: *IEEE Transactions on Reliability* 41 (1992), Sep, Nr. 3, S. 363–377. http://dx.doi.org/10.1109/24.159800. – DOI 10.1109/24.159800. – ISSN 0018–9529

[38] Sullivan, Kevin J. ; Dugan, Joanne B. ; Coppit, David: The Galileo Fault Tree Analysis Tool. In: *Proceedings of the 29th Annual International Symposium on Fault-Tolerant Computing*. Madison, Wisconsin: IEEE, 1999, S. 232–235

[39] Distefano, Salvatore ; Puliafito, Antonio: Dynamic reliability block diagrams: Overview of a methodology. In: Aven (Hrsg.) ; Vinnem (Hrsg.): *Risk, Reliability and Societal Safety, ESREL 07*. London: Taylor and Francis Group, 2007

[40] Dugan, Joanne B. ; Kevin, Dugan ; Coppit, David ; Sullivan, Kevin J.: Developing a High-Quality Software Tool for Fault Tree Analysis. In: *In Proceedings of the International Symposium on Software Reliability Engineering*, IEEE, 1999, S. 49–59

[41] Aldemir, Tunc (Hrsg.) ; Siu, Nathan O. (Hrsg.) ; Mosleh, Ali (Hrsg.) ; Cacciabue, P. C. (Hrsg.) ; Göktepe, B. G. (Hrsg.): *NATO ASI Series F: Computer and System Sciences*. Bd. 120: *Reliability and Safety Assessment of Dynamic Process Systems*. Springer Verlag, 1994

[42] Hirschberg, Stefan ; Knochenhauer, Michael: Time Dependencies in Probabilistic Safety Assessment. In: [41], S. 196–212

[43] Xing, Liudong ; Dugan, J.B.: Analysis of generalized phased-mission system reliability, performance, and sensitivity. In: *IEEE Transactions on Reliability* 51 (2002), Jun, Nr. 2, S. 199–211. http://dx.doi.org/10.1109/TR.2002.1011526. – DOI 10.1109/TR.2002.1011526. – ISSN 0018–9529

[44] Garrett, C.J. ; Guarro, S.B. ; Apostolakis, G.E.: The dynamic flowgraph methodology for assessing the dependability of embedded software systems. In: *IEEE Transactions on Systems, Man and Cybernetics* 25 (1995), May, Nr. 5, S. 824–840. http://dx.doi.org/10.1109/21.376495. – DOI 10.1109/21.376495. – ISSN 0018–9472

[45] Kolaczkowski, A. u.a.: Human Reliability Analysis (HRA) Good Practices. In: *Probabilistic Safety Assessment and Management, PSAM 07 - ESREL 04*. Berlin: Springer, 2004

[46] Thane, Henrik: Safe and Reliable Computer Control Systems: Concepts and Methods. 1996. – Forschungsbericht

[47] Coudert, O. ; Madre, J.C.: MetaPrime: an interactive fault-tree analyzer. In: *IEEE Transactions on Reliability* 43 (1994), Mar, Nr. 1, S. 121–127. http://dx.doi.org/10.1109/24.285125. – DOI 10.1109/24.285125. – ISSN 0018–9529

[48] Jung, W.S. ; Han, S.H. ; Ha, J.: Development of an Efficient BDD Algorithm to Solve Large Fault Trees. In: *Probabilistic Safety Assessment and Management, PSAM 07 - ESREL 04*. Berlin: Springer, 2004

[49] Dugan, Joanne B. ; Venkataraman, Bharath ; Gulati, Rohit: DIFtree: A software package for the analysis of dynamic fault tree models. In: *Reliability and Maintainability Symposium* (1997), S. 64–70

[50] Isograph Ltd.: *FaultTree+ V11.0*. http://www.isograph-software.com/ftpover.htm, Abruf: 2009.01.26

[51] ITEM Software Inc.: *ITEM ToolKit*. http://www.itemsoft.com/faulttree.shtml, Abruf: 2009.01.26

[52] Relex Software Corporation: *Relex Reliability Studio 2007*. 2007

[53] Montani, S. ; Portinale, L. ; Bobbio, A. ; Codetta-Raiteri, D.: Automatically Translating Dynamic Fault Trees into Dynamic Bayesian Networks by Means of a Software Tool. In: *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security*. Washington, DC, USA: IEEE Computer Society, 2006. – ISBN 0–7695–2567–9, S. 804–809

[54] Tang, Zhihua ; Dugan, J.B.: Minimal cut set/sequence generation for dynamic fault trees. In: *Reliability and Maintainability, 2004 Annual Symposium - RAMS*, 2004, S. 207–213

[55] Bozzano, Marco ; Villafiorita, Adolfo: Integrating Fault Tree Analysis with Event Ordering Information. In: *Safety and Reliability for Managing Risk, ESREL 03*, 2003, S. 247–254

[56] Bouissou, Marc ; Bon, Jean-Louis: A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes. In: *Reliability Engineering and System Safety* 82 (2003), Nr. 2, S. 149–163. http://dx.doi.org/10.1016/S0951-8320(03)00143-1. – DOI 10.1016/S0951–8320(03)00143–1. – ISSN 0951–8320

[57] Bousissou, M.: A Generalization of Dynamic Fault Trees through Boolean logic Driven Markov Processes (BDMP). In: *ESREL 2007*. Stavanger (Norway), 2007

[58] Bobbio, A. ; Franceschinis, G. ; Gaeta, R. ; Portinale, L.: Parametric fault tree for the dependability analysis of redundant systems and its high-level Petri net semantics. In: *IEEE Transactions on Software Engineering* 29 (2003), Nr. 3, S. 270–287. http://dx.doi.org/10.1109/TSE.2003.1183940. – DOI 10.1109/TSE.2003.1183940. – ISSN 0098–5589

[59] Schneeweiss, W. G.: Advanced Fault Tree Modeling. In: *Journal of Universal Computer Science* 5 (1999), Nr. 10, S. 633–643

[60] Schneeweiss, Winfried G.: *Petri Nets for Reliability Modeling.* LiLoLe-Verlag, 1999

[61] Kaiser, Bernhard ; Gramlich, Catharina ; Förster, Marc: State/event fault trees–A safety analysis model for software-controlled systems. In: *Reliability Engineering and System Safety* 92 (2007), Nr. 11, S. 1521–1537. http://dx.doi.org/10.1016/j.ress.2006.10.010. – DOI 10.1016/j.ress.2006.10.010. – ISSN 0951–8320. – SAFECOMP 2004, the 23rd International Conference on Computer Safety, Reliability and Security

[62] Gulati, R. ; Dugan, J.B.: A modular approach for analyzing static and dynamic fault trees. In: *Reliability and Maintainability Symposium. 1997 Proceedings, Annual*, 1997, S. 57–63

[63] Dutuit, Y. ; Rauzy, A.: A linear-time algorithm to find modules of fault trees. In: *IEEE Transactions on Reliability* 45 (1996), Nr. 3, S. 422–425. http://dx.doi.org/10.1109/24.537011. – DOI 10.1109/24.537011. – ISSN 0018–9529

[64] Amari, S. ; Dill, G. ; Howald, E.: A new approach to solve dynamic fault trees. In: *Reliability and Maintainability Symposium, 2003. Annual*, 2003. – ISSN 0149–144X, S. 374–379

[65] Malhotra, M. ; Trivedi, K.S.: Dependability modeling using Petri-nets. In: *IEEE Transactions on Reliability* 44 (1995), Sep, Nr. 3, S. 428–440. http://dx.doi.org/10.1109/24.406578. – DOI 10.1109/24.406578. – ISSN 0018–9529

[66] Manian, R. ; Coppit, D.W. ; Sullivan, K.J. ; Bechta Dugan, J.: Bridging the gap between systems and dynamic fault tree models. In: *Reliability and Maintainability Symposium, 1999. Proceedings. Annual*, 1999, S. 105–111

[67] Walter, Max: OpenSESAME: A Tool's Concept. In: Scientific, Carleton (Hrsg.): *Proceedings of the Satellite Workshops of the 27th International Colloquium on Automata Languages, and Programming* Bd. 8, Proceedings in Informatics, 2000

[68] Fussel, J. B. ; Aber, E. F. ; Rahl, R. G.: On quantitative analysis of PAND failure logic. In: *IEEE Transactions on Reliability* R-25 (1976), Nr. 5, S. 324–326

[69] Long, W. ; Sato, Y. ; Horigome, M.: Quantification of sequential failure logic for fault tree analysis. In: *Reliability Engineering and System Safety* 67 (2000), Nr. 3, S. 269 – 274. http://dx.doi.org/10.1016/S0951-8320(99)00075-7. – DOI 10.1016/S0951–8320(99)00075–7. – ISSN 0951–8320

[70] Wijayarathna, P.G. ; Maekawa, M.: Extending fault trees with an AND-THEN gate. In: *Software Reliability Engineering, 2000. ISSRE 2000. Proceedings. 11th International Symposium on*, 2000. – ISBN 0–7695–0807–3, S. 283–292

[71] Gorski, J.: Extending safety analysis techniques with formal semantics. In: Redmill, F. J. (Hrsg.) ; Anderson, T. (Hrsg.): *Technology and Assessment of Safety Critical Systems.* Springer-Verlag, 1994, S. 147–163

[72] Gorski, J. ; Wardzinski, A.: Timing aspects of fault tree analysis of safety critical systems. In: Redmill, F. J. (Hrsg.) ; Anderson, T. (Hrsg.): *Safer Systems*. Springer-Verlag, 1997

[73] Palshikar, Girish K.: Temporal fault trees. In: *Information and Software Technology* 44 (2002), Nr. 3, S. 137–150. http://dx.doi.org/10.1016/S0950-5849(01)00223-3. – DOI 10.1016/S0950–5849(01)00223–3. – ISSN 0950–5849

[74] Thums, Andreas: *Formale Fehlerbaumanalyse*, Universität Augsburg, Fakultät für Angewandte Informatik, Lehrstuhl für Softwaretechnik und Programmiersprachen, Diss., 2004

[75] Galton, Antony (Hrsg.): *Temporal Logics and their applications*. Academic Press, 1987

[76] Walker, Martin ; Papadopoulos, Yiannis: PANDORA: The time of priority-and gates. Version: 2006. http://dx.doi.org/10.1016/B978-008044654-7/50173-4. In: Dolgui, Alexandre (Hrsg.) ; Morel, Gerard (Hrsg.) ; Pereira, Carlos E. (Hrsg.): *Information Control Problems in Manufacturing 2006*. Oxford: Elsevier Science Ltd, 2006. – DOI 10.1016/B978–008044654–7/50173–4. – ISBN 978–0–08–044654–7, S. 235–240

[77] Walker, Martin ; Papadopoulos, Yiannis: PANDORA 2 : The Time of Priority-OR Gates. In: *IFAC Workshop on Dependable Control of Discrete Event Systems* (2007)

[78] Tietjen, Thorsten ; Müller, Dieter H.: *FMEA- Praxis. Das Komplettpaket für Training und Anwendung*. 2. überarb. Auflage. München: Hanser Fachbuch, 2003

[79] Reinschke, Kurt ; Ušakov, Igoŕ A.: *Zuverlässigkeitsstrukturen*. München, Wien: R. Oldenbourg Verlag, 1988

[80] Abraham, J.A.: An Improved Algorithm for Network Reliability. In: *IEEE Transactions on Reliability* R-28 (1979), Nr. 1, S. 58–61. http://dx.doi.org/10.1109/TR.1979.5220476. – DOI 10.1109/TR.1979.5220476. – ISSN 0018–9529

[81] Heidtmann, K.D.: Smaller sums of disjoint products by subproduct inversion. In: *IEEE Transactions on Reliability* 38 (1989), Nr. 3, S. 305–311. http://dx.doi.org/10.1109/24.44172. – DOI 10.1109/24.44172. – ISSN 0018–9529

[82] Bertschy, R. ; Monney, P. A.: A generalization of the algorithm of Heidtmann to non-monotone formulas. In: *Journal of Computational and Applied Mathematics* 76 (1996), Nr. 1–2, S. 55–76. http://dx.doi.org/10.1016/S0377-0427(96)00089-1. – DOI 10.1016/S0377–0427(96)00089–1. – ISSN 0377–0427

[83] Kohlas, J. ; Monney, P. A.: *Lecture Notes in Economics and Mathematical Systems*. Bd. 425: *A Mathematical Theory of Hints. An Approach to the Dempster-Shafer Theory of Evidence*. Springer, 1995

[84] Alleman, Glen B.: *Fault-Tolerant System Reliability In The Presence Of Imperfect Diagnostic Coverage*. 1989, 2000

[85] Schilling, Simon J.: On the use of "Probabilities" in IEC 61508. In: *BMW Group report, (contact the author for more information or if you would like to obtain a copy of the preprint)* (2007)

[86] Sinnamon, R.M. ; Andrews, J.D.: Fault tree analysis and binary decision diagrams. In: *Reliability and Maintainability Symposium, 1996 Proceedings. 'International Symposium on Product Quality and Integrity'., Annual*, 1996, S. 215–222

[87] Formal Software Construction Ltd: *OpenFTA*. `http://www.openfta.com`, Abruf: 2009.01.26

Anhang

A Vertiefende Erläuterungen

A.1 Kenngrößen

Die probabilistische Beschreibung des Ausfallverhaltens von Systemen erfolgt mittels sogenannter *Kenngrößen*, vgl. Tabelle A.1. Diese sind stochastische bzw. probabilistische Größen, da das deterministische Ausfallverhalten der einzelnen Komponente und des einzelnen Systems in der Regel nicht im Vorraus bekannt ist. Eine Berücksichtigung der aus diesen Größen resultierenden Verteilungsfunktionen bereitet in der realen Anwendungen oft Schwierigkeiten, insbesondere wegen des mit Ihrer Gewinnung verbundenen großen Aufwands. Näherungsweise werden daher oftmals statt verteilter Größen Punktwerte oder gemittelte konstante Größen verwendet.

In dieser Arbeit wird trotz deren sicherheitstechnischer Ausrichtung von Ausfallwahrscheinlichkeiten, -dichten und -raten gesprochen, weil

- die wesentlichen Aussagen analog auch für allgemeine Zuverlässigkeitsfragen gelten und
- die Verwendung dieser eigentlich allgemein auf Zuverlässigkeitsbetrachtungen ausgerichteten Begriffe im Kontext sicherheitstechnischer Anwendungen üblich ist, vgl. z. B. die relevanten Sicherheits-Standards ISO 26262 [3] und IEC 61508 [4].

Nicht reparierbare Systeme			
Zuverlässigkeit		**Sicherheit**	
Kenngröße	*Formelzeichen*	*Kenngröße*	*Formelzeichen*
Ausfallwahrscheinlichkeit	$F(t)$	Gefährdungswahrsch.	$G(t)$
Überlebenswahrsch.	$R(t)$	Sicherheitswahrsch.	$S(t)$
Ausfalldichte	$f(t)$	Gefährdungsdichte	$g(t)$
Ausfallrate	$h(t)$	Gefährdungsrate	$\delta(t)$
falls konstant	λ		
Reparierbare Systeme			
Zuverlässigkeit		**Sicherheit**	
Kenngröße	*Formelzeichen*	*Kenngröße*	*Formelzeichen*
Reparaturrate	$\mu(t)$	Sicherheitsrestitutionsrate	$\nu(t)$
Instandsetzungswahrsch.	$M(t)$	Sicherheitswieder-herstellungswahrsch.	$W(t)$
Instandsetzungsdichte	$m(t)$	Sicherheitswieder-herstellungsdichte	$w(t)$
Verfügbarkeit	$V(t)$	Sicherheitsverfügbarkeit	$V_S(t)$
Unverfügbarkeit	$U(t)$	„Sicherheitsunverfügbarkeit“	$U_S(t)$

Tabelle A.1: Kenngrößen quantitativer Zuverlässigkeits- bzw. Sicherheitsanalysen [14]

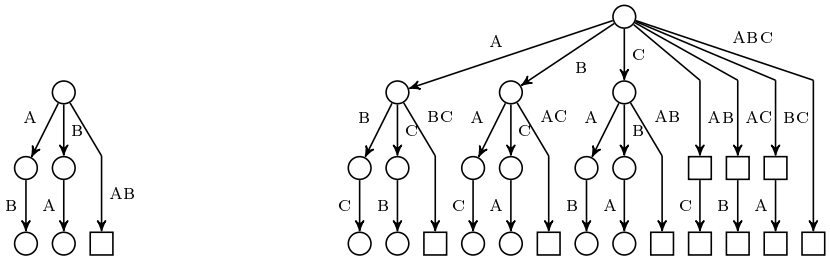
A.2 Umgang mit sequentiellen Ausfallbäumen in der TFTA

Sequentielle Ausfallbäume erlauben die Visualisierung temporallogischer Terme sowie die manuelle Überprüfung von Umformungen nach der temporalen Logik der TFTA. Die Erstellung eines sequentiellen Ausfallbaumes zu einem komplexen temporalen Term ist aufwändig, beruht aber auf nur wenigen grundsätzlichen Schritten.

Wahl des Ausfallbaumes

Entsprechend der Anzahl der an einem Term beteiligten Basisereignisse ist der entsprechende sequentielle Ausfallbaum zu wählen. Dieser muss mindestens für die Anzahl der Basisereignisse ausgelegt sein, er kann aber auch größer sein. Zudem ist je nach Anwendung ggf. die vereinfachte Version ohne SAND Verknüpfungen ausreichend.

Beispiel: Die folgende Abbildung zeigt zwei noch nicht ausgefüllte sequentielle Ausfallbäume, die für den Term $\varpi = A \wedge B$ geeignet sind.



Zerlegung

Ist der temporale Term zu komplex, so sind im ersten Schritt einfache Teilterme zu identifizieren, für die sequentielle Ausfallbäume erstellt werden. Im Extremfall sind die Basisereignisse des temporalen Terms zu wählen. Die folgenden Schritte sind dann für alle gewählten Terme durchzuführen.

Beispiel: Zum Term $\varpi = A \wedge B$ werden die beiden Teilterme A und B gewählt.

Minimale Ausfallknoten

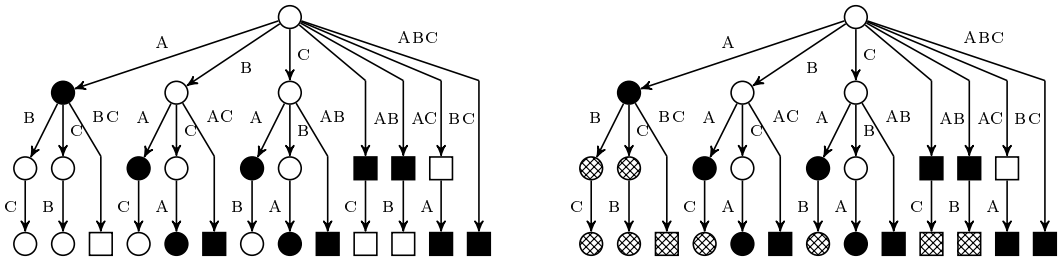
Ausgehend vom Ursprungsknoten werden alle Zweige des sequentiellen Ausfallbaums durchlaufen, jeweils bis der aktuell gewählte Term eingetreten ist, und die minimalen Ausfallknoten markiert.

Beispiel: siehe nächster Schritt.

Folge-Ausfallknoten / nichtminimale Ausfallknoten

Alle unterhalb eines minimalen Ausfallknotens liegenden Knoten sind als Folge-Ausfallknoten zu kennzeichnen.

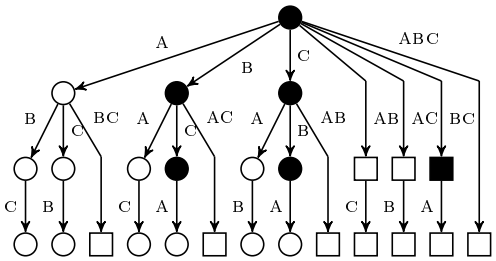
Beispiel: Die folgenden Abbildungen zeigen die minimalen Ausfallknoten (links) sowie die minimalen und Folge-Ausfallknoten (rechts) für $\varpi = A$.



Negierte Ereignisse

Ausgehend vom sequentiellen Ausfallbaum eines Ereignisses werden alle ursprünglichen Nicht-Ausfallknoten als minimale Ausfallknoten und alle ursprünglichen Ausfallknoten als Nicht-Ausfallknoten gekennzeichnet. Es werden *keine* nichtminimalen Ausfallknoten neu hinzugefügt.

Beispiel: Die folgende Abbildung zeigt den sequentiellen Ausfallbaum für $\neg A$.



Konjunktion / AND-Verknüpfung

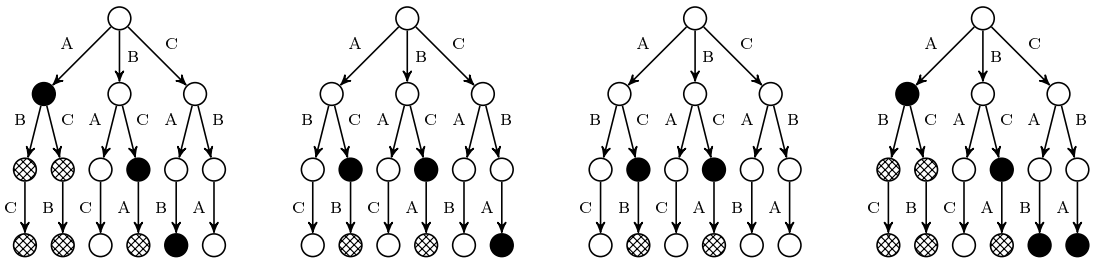
Der sequentielle Ausfallbaum einer Konjunktion aus zwei temporalen Termen ergibt sich durch Bilden einer „Schnittmenge“ aus den sequentiellen Ausfallbäumen der einzelnen Terme. Dabei absorbieren minimale Ausfallknoten die nichtminimalen Ausfallknoten. Anschließend werden ggf. noch fehlende nichtminimale Ausfallknoten neu hinzugefügt. Dieser Fall ist insbesondere in Zusammenhang mit negierten Ereignissen anzutreffen.

Beispiel: siehe nächster Schritt.

Disjunktion / OR-Verknüpfung

Der sequentielle Ausfallbaum einer Disjunktion aus zwei temporalen Termen ergibt sich durch Bilden einer „Vereinigungsmenge“ aus den sequentiellen Ausfallbäumen der einzelnen Terme. Dabei absorbieren nichtminimale Ausfallknoten die minimalen Ausfallknoten. Anschließend werden ggf. noch fehlende nichtminimale Ausfallknoten neu hinzugefügt. Dieser Fall ist insbesondere in Zusammenhang mit negierten Ereignissen anzutreffen.

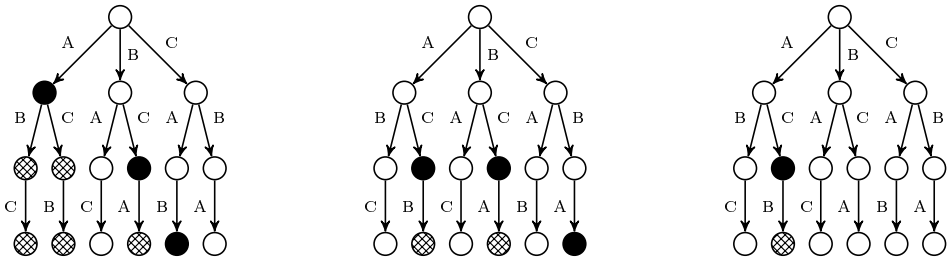
Beispiel: Die folgende Abbildung zeigt zwei vereinfachte sequentielle Ausfallbäume (links und Mitte links) und deren „Schnittmenge“ (Mitte rechts) und „Vereinigungsmenge“ (rechts).



PAND-Verknüpfung

Der sequentielle Ausfallbaum einer PAND-Verknüpfung aus zwei temporalen Termen $\varpi_1 \vec{\wedge} \varpi_2$ ergibt sich folgendermaßen: Als minimale Ausfallknoten werden alle diejenigen Knoten gekennzeichnet, die zugleich minimale Ausfallknoten von ϖ_2 und nichtminimale Ausfallknoten von ϖ_1 sind. Anschließend werden die nichtminimalen Ausfallknoten neu hinzugefügt.

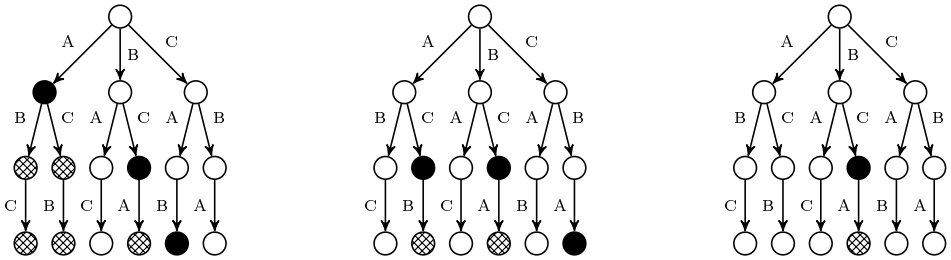
Beispiel: Die folgende Abbildung zeigt zwei vereinfachte sequentielle Ausfallbäume (links und Mitte) und deren „PAND-Verknüpfung“ (rechts).



SAND-Verknüpfung

Der sequentielle Ausfallbaum einer SAND-Verknüpfung aus zwei temporalen Termen $\varpi_1 \bar{\wedge} \varpi_2$ ergibt sich folgendermaßen: Als minimale Ausfallknoten werden alle diejenigen Knoten gekennzeichnet, die zugleich minimale Ausfallknoten von ϖ_2 und minimale Ausfallknoten von ϖ_1 sind. Anschließend werden die nichtminimalen Ausfallknoten neu hinzugefügt.

Beispiel: Die folgende Abbildung zeigt zwei vereinfachte sequentielle Ausfallbäume (links und Mitte) und deren „SAND-Verknüpfung“ (rechts).



A.3 Beispiele zur Disjunktheit temporaler Terme

Es gilt $n = 3$ mit den Ausfallereignissen A, B, C.

1. Beispiel

Die Ausfallfunktion $\varpi = B$ liegt bereits in einer TDNF mit einem Teilterm vor, der jedoch noch kein Minterm ist, da er nicht alle vorhandenen Variablen enthält. Das auf Seite 56 genannte Verfahren erzeugt daraus eine TDNF aus disjunkten, minimalen Ereignissequenzen, die zugleich temporale Minterme sind:

$$\begin{aligned} B &= B \wedge (\neg A \vee A) \wedge (\neg C \vee C) = \\ &= \big[A \wedge B \wedge C\big] \vee \big[\neg C \wedge (A \wedge B)\big] \vee \big[\neg A \wedge (B \wedge C)\big] \vee \big[(\neg A\, \neg C) \wedge B\big] \ . \end{aligned}$$

Der Übersichtlichkeit halber werden die vier resultierenden Teilterme nun einzeln betrachtet.

$$\eta_1 = A \wedge B \wedge C \ .$$

Zweimaliges Anwenden des Vervollständigungsgesetzes liefert

$$\begin{aligned}\eta_1 &= \big[(A \wedge B)\,\vec{\wedge}\,C\big] \vee \big[(A \wedge B)\,\overline{\vec{\wedge}}\,C\big] \vee \big[C\,\vec{\wedge}\,(A \wedge B)\big] = \\ &= \big[(A\,\vec{\wedge}\,B \vee A\,\overline{\vec{\wedge}}\,B \vee B\,\vec{\wedge}\,A)\,\vec{\wedge}\,C\big] \vee \big[(A\,\vec{\wedge}\,B \vee A\,\overline{\vec{\wedge}}\,B \vee B\,\vec{\wedge}\,A)\,\overline{\vec{\wedge}}\,C\big] \vee \\ &\quad \vee \big[C\,\vec{\wedge}\,(A\,\vec{\wedge}\,B \vee A\,\overline{\vec{\wedge}}\,B \vee B\,\vec{\wedge}\,A)\big]\ .\end{aligned}$$

Da die Terme in den runden Klammern disjunkt sind, folgt

$$\begin{aligned}\eta_1 &= \big[A\,\vec{\wedge}\,B\,\vec{\wedge}\,C\big] \vee \big[(A\,\overline{\vec{\wedge}}\,B)\,\vec{\wedge}\,C\big] \vee \big[B\,\vec{\wedge}\,A\,\vec{\wedge}\,C\big] \vee \big[(A\,\vec{\wedge}\,B)\,\overline{\vec{\wedge}}\,C\big] \vee \big[(A\,\overline{\vec{\wedge}}\,B)\,\overline{\vec{\wedge}}\,C\big] \vee \\ &\quad \vee \big[(B\,\vec{\wedge}\,A)\,\overline{\vec{\wedge}}\,C\big] \vee \big[C\,\vec{\wedge}\,(A\,\vec{\wedge}\,B)\big] \vee \big[C\,\vec{\wedge}\,(A\,\overline{\vec{\wedge}}\,B)\big] \vee \big[C\,\vec{\wedge}\,(B\,\vec{\wedge}\,A)\big]\ .\end{aligned}$$

Durch Anwenden der Regeln der temporalen Logik ergibt sich

$$\begin{aligned}\eta_1 &= \big[A\,\vec{\wedge}\,B\,\vec{\wedge}\,C\big] \vee \big[(A\,\overline{\vec{\wedge}}\,B)\,\vec{\wedge}\,C\big] \vee \big[B\,\vec{\wedge}\,A\,\vec{\wedge}\,C\big] \vee \big[A\,\vec{\wedge}\,(B\,\overline{\vec{\wedge}}\,C)\big] \vee \big[A\,\overline{\vec{\wedge}}\,B\,\overline{\vec{\wedge}}\,C\big] \vee \\ &\quad \vee \big[B\,\vec{\wedge}\,(A\,\overline{\vec{\wedge}}\,C)\big] \vee \big[A\,\vec{\wedge}\,C\,\vec{\wedge}\,B\big] \vee \big[(A\,\overline{\vec{\wedge}}\,C)\,\vec{\wedge}\,B\big] \vee \big[C\,\vec{\wedge}\,A\,\vec{\wedge}\,B\big] \vee \\ &\quad \vee \big[B\,\vec{\wedge}\,C\,\vec{\wedge}\,A\big] \vee \big[(B\,\overline{\vec{\wedge}}\,C)\,\vec{\wedge}\,A\big] \vee \big[C\,\vec{\wedge}\,B\,\vec{\wedge}\,A\big] \vee \big[C\,\vec{\wedge}\,(A\,\overline{\vec{\wedge}}\,B)\big]\ .\end{aligned}$$

Damit ist die Umformung des ersten Teilterms beendet. Anwenden des Vervollständigungsgesetzes auf den zweiten Teilterm

$$\eta_2 = \neg C \wedge (A \wedge B)$$

liefert disjunkte Terme, sodass

$$\begin{aligned}\eta_2 &= \neg C \wedge \big((A\,\vec{\wedge}\,B \vee (A\,\overline{\vec{\wedge}}\,B) \vee (B\,\vec{\wedge}\,A)\big) = \\ &= \big[\neg C \wedge (A\,\vec{\wedge}\,B)\big] \vee \big[\neg C \wedge (A\,\overline{\vec{\wedge}}\,B)\big] \vee \big[\neg C \wedge (B\,\vec{\wedge}\,A)\big]\ .\end{aligned}$$

Der dritte Teilterm ergibt sich analog zum Zweiten zu

$$\eta_3 = \neg A \wedge (B \wedge C) = \big[\neg A \wedge (B\,\vec{\wedge}\,C)\big] \vee \big[\neg A \wedge (B\,\overline{\vec{\wedge}}\,C)\big] \vee \big[\neg A \wedge (C\,\vec{\wedge}\,B)\big]\ .$$

Der vierte Teilterm besteht aus einer Sequenz, die sich nicht weiter vereinfachen lässt:

$$\eta_4 = (\neg A \neg C) \wedge B\ .$$

Zusammensetzen liefert die Minterm-Form des Ausdrucks $\varpi = B$ für drei Variablen (Bedeutung der Unterstreichungen s. u.):

$$\begin{aligned}\varpi = B &= \eta_1 \vee \eta_2 \vee \eta_3 \vee \eta_4 = \\ &= \big[\underline{A\,\vec{\wedge}\,B\,\vec{\wedge}\,C}\big] \vee \big[\underline{(A\,\overline{\vec{\wedge}}\,B)\,\vec{\wedge}\,C}\big] \vee \big[\underline{B\,\vec{\wedge}\,A\,\vec{\wedge}\,C}\big] \vee \big[A\,\vec{\wedge}\,(B\,\overline{\vec{\wedge}}\,C)\big] \vee \big[A\,\overline{\vec{\wedge}}\,B\,\overline{\vec{\wedge}}\,C\big] \vee \\ &\quad \vee \big[\underline{B\,\vec{\wedge}\,(A\,\overline{\vec{\wedge}}\,C)}\big] \vee \big[A\,\vec{\wedge}\,C\,\vec{\wedge}\,B\big] \vee \big[(A\,\overline{\vec{\wedge}}\,C)\,\vec{\wedge}\,B\big] \vee \big[C\,\vec{\wedge}\,A\,\vec{\wedge}\,B\big] \vee \big[\underline{B\,\vec{\wedge}\,C\,\vec{\wedge}\,A}\big] \vee \\ &\quad \vee \big[\underline{(B\,\overline{\vec{\wedge}}\,C)\,\vec{\wedge}\,A}\big] \vee \big[\underline{C\,\vec{\wedge}\,B\,\vec{\wedge}\,A}\big] \vee \big[\neg C \wedge (A\,\vec{\wedge}\,B)\big] \vee \big[\neg C \wedge (A\,\overline{\vec{\wedge}}\,B)\big] \vee \\ &\quad \vee \big[\underline{\neg C \wedge (B\,\vec{\wedge}\,A)}\big] \vee \big[\underline{\neg A \wedge (B\,\vec{\wedge}\,C)}\big] \vee \big[\neg A \wedge (B\,\overline{\vec{\wedge}}\,C)\big] \vee \big[\neg A \wedge (C\,\vec{\wedge}\,B)\big] \vee \\ &\quad \vee \big[C\,\vec{\wedge}\,(A\,\overline{\vec{\wedge}}\,B)\big] \vee \big[(\neg A \neg C) \wedge B\big]\ .\end{aligned}$$

In dieser Form ist ϖ jedoch noch nicht minimal. Wie Abbildung A.1 zeigt, sind nur elf der 20 Knoten, in denen $B = \mathit{True}$ ist, auch minimal. Die Minterme zu den nichtminimalen Knoten

sind in obiger Darstellung unterstrichen. Die Anwendung der temporalen Absorptionsgesetze führt zur minimalen Form, in der

$$\begin{aligned}\varpi = B &= \eta_1 \vee \eta_2 \vee \eta_3 \vee \eta_4 = \\ &= \big[A \,\vec{\wedge}\, (B \,\bar{\vec{\wedge}}\, C)\big] \vee \big[A \,\bar{\vec{\wedge}}\, B \,\bar{\vec{\wedge}}\, C\big] \vee \big[A \,\vec{\wedge}\, C \,\vec{\wedge}\, B\big] \vee \big[(A \,\bar{\vec{\wedge}}\, C) \,\vec{\wedge}\, B\big] \vee \big[C \,\vec{\wedge}\, A \,\vec{\wedge}\, B\big] \vee \\ &\quad \vee \big[\neg C \wedge (A \,\vec{\wedge}\, B)\big] \vee \big[\neg C \wedge (A \,\bar{\vec{\wedge}}\, B)\big] \vee \big[\neg A \wedge (B \,\bar{\vec{\wedge}}\, C)\big] \vee \\ &\quad \vee \big[\neg A \wedge (C \,\vec{\wedge}\, B)\big] \vee \big[C \,\vec{\wedge}\, (A \,\bar{\vec{\wedge}}\, B)\big] \vee \big[(\neg A \neg C) \wedge B\big] \;.\end{aligned}$$

Insbesondere gilt auf Grund der strukturellen und zeitlichen Nichtminimalität temporaler Terme (vgl. Kapitel 4.3.2), dass

$(\neg A \neg C) \wedge B$	deckt $\big[B \,\vec{\wedge}\, (A \,\bar{\vec{\wedge}}\, C)\big]$, $\big[\neg A \wedge (B \,\vec{\wedge}\, C)\big]$, $\big[\neg C \wedge (B \,\vec{\wedge}\, A)\big]$ ab,
$\neg A \wedge (B \,\vec{\wedge}\, C)$	deckt $B \,\vec{\wedge}\, C \,\vec{\wedge}\, A$ ab,
$\neg C \wedge (B \,\vec{\wedge}\, A)$	deckt $B \,\vec{\wedge}\, A \,\vec{\wedge}\, C$ ab,
$\neg C \wedge (A \,\vec{\wedge}\, B)$	deckt $A \,\vec{\wedge}\, B \,\vec{\wedge}\, C$ ab,
$\neg A \wedge (C \,\vec{\wedge}\, B)$	deckt $C \,\vec{\wedge}\, B \,\vec{\wedge}\, A$ ab,
$\neg C \wedge (A \,\bar{\vec{\wedge}}\, B)$	deckt $(A \,\bar{\vec{\wedge}}\, B) \,\vec{\wedge}\, C$ ab,
$\neg A \wedge (B \,\bar{\vec{\wedge}}\, C)$	deckt $(B \,\bar{\vec{\wedge}}\, C) \,\vec{\wedge}\, A$ ab.

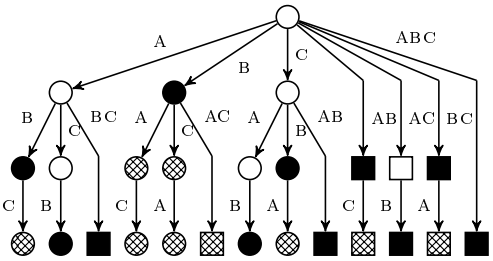


Abbildung A.1: Sequentieller Ausfallbaum zu $\varpi = B$ mit elf minimalen Ausfallknoten und neun nichtminimalen Ausfallknoten. Neun Ausfallknoten enthalten mindestens eine SAND Verknüpfung.

2. Beispiel

Die Ausfallfunktion $\varpi = (A \vee B) \,\vec{\wedge}\, C$ liegt noch nicht in einer TDNF vor. Zunächst werden die Regeln der temporalen Logik verwendet, um eine TDNF herzustellen:

$$\varpi = (A \vee B) \,\vec{\wedge}\, C = (A \,\vec{\wedge}\, C) \vee (B \,\vec{\wedge}\, C) \;.$$

Die beiden Teiltermen rechts enthalten nicht alle drei vorhandenen Variablen. Jeder Teilterm wird mit den Variablen, die nicht in ihm enthalten sind, gemäß (4.122) umgeformt.

$$\begin{aligned}\varpi &= \big[\neg B \wedge (A \,\vec{\wedge}\, C)\big] \vee \big[B \wedge (A \,\vec{\wedge}\, C)\big] \vee \big[\neg A \wedge (B \,\vec{\wedge}\, C)\big] \vee \big[A \wedge (B \,\vec{\wedge}\, C)\big] = \\ &= \big[\neg B \wedge (A \,\vec{\wedge}\, C)\big] \vee \big[B \,\vec{\wedge}\, A \,\vec{\wedge}\, C\big] \vee \big[A \,\vec{\wedge}\, B \,\vec{\wedge}\, C\big] \vee \big[(A \,\bar{\vec{\wedge}}\, B) \,\vec{\wedge}\, C\big] \vee \\ &\quad \vee \big[A \,\vec{\wedge}\, (B \,\bar{\vec{\wedge}}\, C)\big] \vee \big[A \,\vec{\wedge}\, C \,\vec{\wedge}\, B\big] \vee \big[\neg A \wedge (B \,\vec{\wedge}\, C)\big] \vee \big[A \,\vec{\wedge}\, B \,\vec{\wedge}\, C\big] \vee \\ &\quad \vee \big[B \,\vec{\wedge}\, A \,\vec{\wedge}\, C\big] \vee \big[(A \,\bar{\vec{\wedge}}\, B) \,\vec{\wedge}\, C\big] \vee \big[B \,\vec{\wedge}\, (A \,\bar{\vec{\wedge}}\, C)\big] \vee \big[B \,\vec{\wedge}\, C \,\vec{\wedge}\, A\big] \;.\end{aligned}$$

Dabei sind die Terme $A \vec{\wedge} B \vec{\wedge} C$ und $B \vec{\wedge} A \vec{\wedge} C$ und $(A \bar{\vec{\wedge}} B) \vec{\wedge} C$ doppelt enthalten. Zudem decken $\neg A \wedge (B \vec{\wedge} C)$ und $\neg B \wedge (A \vec{\wedge} C)$ die nichtminimalen Terme $B \vec{\wedge} C \vec{\wedge} A$ und $A \vec{\wedge} C \vec{\wedge} B$ ab. Die Minterm-Form der Ausfallfunktion lautet somit

$$\begin{aligned} \varpi = \quad & \left[\neg B \wedge (A \vec{\wedge} C)\right] \vee \left[B \vec{\wedge} A \vec{\wedge} C\right] \vee \left[A \vec{\wedge} B \vec{\wedge} C\right] \vee \left[(A \bar{\vec{\wedge}} B) \vec{\wedge} C\right] \vee \\ & \vee \left[A \vec{\wedge} (B \bar{\vec{\wedge}} C)\right] \vee \left[\neg A \wedge (B \vec{\wedge} C)\right] \vee \left[B \vec{\wedge} (A \bar{\vec{\wedge}} C)\right] \ . \end{aligned}$$

Abbildung A.2 zeigt den sequentiellen Ausfallbaum zum zweiten Beispiel mit sieben minimalen und zwei nichtminimalen Ausfallknoten.

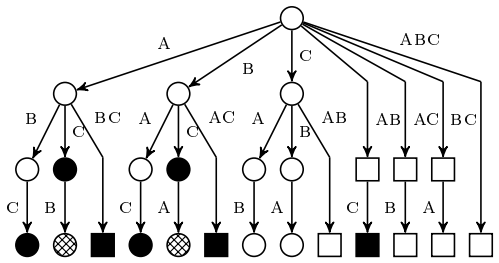


Abbildung A.2: Sequentieller Ausfallbaum zu $\varpi = (A \vee B) \vec{\wedge} C$ mit sieben minimalen Ausfallknoten und zwei nichtminimalen Ausfallknoten. Drei Ausfallknoten enthalten mindestens eine SAND Verknüpfung.

B Abkürzungen

Anmerkung: Für viele Fachbegriffe ist es üblich, auch im Deutschen englische Akronyme zu verwenden, z. B. „FTA“ für „Fehlerbaumanalyse“ vom Englischen „Fault Tree Analysis“.

BDD Binary Decision Diagram

BDMP Boolean Logic Driven Markov Processes

CCF Common Cause Failure

DFT Dynamic Fault Tree

DGL Differential Gleichung

DNF Disjunktive Normalform

DRBD Dynamic Reliability Block Diagram

E / E Elektrisch / Elektronisch

FAA Federal Aviation Administration

FMEA Failure Modes and Effects Analysis

FT Fehlerbaum

FTA Fehlerbaumanalyse (Fault Tree Analysis)

HRA Human Reliability Analysis

MoCaS Monte-Carlo-Simulation

MCSS Minimalsequenzen (Minimal Cutset Sequences)

PAND Priority AND

POR Priority OR

RBD Zuverlässigkeits-Blockschaltbild (Reliability Block Diagram)

SAND Simultaneous AND

TDNF Temporale Disjunktive Normalform

TFTA Temporale Fehlerbaumanalyse

ZSA Zuverlässigkeits- und Sicherheitsanalyse

C Notation

Symbol	Bedeutung
$.(t)$	Zeitabhängige Größe .
$._i$	Größe . bezieht sich auf Element i
$\mathrm{o}(\Delta t)$	Funktion mit $\lim_{\Delta t \to 0} \frac{\mathrm{o}(\Delta t)}{\Delta t} = 0$
$\wedge$	Boolesches AND
$\vee$	Boolesches OR
$\neg$	Boolesches NOT
$\vec{\wedge}$	temporales PAND
$\overline{\vec{\wedge}}$	temporales SAND
$\subset; \subseteq$	echte Teilmenge; unechte Teilmenge
$\perp$	sind disjunkt (für Ereignisse, z.B. $A \vec{\wedge} B \ \perp \ B \vec{\wedge} A$)
$\in$	ist Element von (für Mengen, z.B. $1 \in \{1, 2, \ldots, n\}$)
$\Subset$	ist Teil von (für Ereignisse, z.B. $A \Subset A \vec{\wedge} B$)
$\exists$	es gibt ein
$\not\supseteq$	sind minimal
A,B,C,D	Ausfallereignisse (in konkreten Beispielen), siehe X
ae	Token für atomare Ereignisse
ce	Token für Kernereignisse
E	Erwartungswert
eK	erweitertes Kernereignis
ece	Token für erweiterte Kernereignisse
ES	Ereignissequenz
es	Token für Ereignissequenzen
eES	erweiterte Ereignissequenz
ees	Token für erweiterte Ereignissequenzen
etdnf	Token für erweiterte temporale Terme in TDNF
η	temporaler Teilterm (in Kapitel 7 und Anhang A)
f	Ausfalldichte (Dichtefunktion zur Ausfallwahrscheinlichkeit, failure density)
F	Ausfallwahrscheinlichkeit / Unzuverlässigkeit (failure probability)
i	Zählvariable
j	Zählvariable
k	Zählvariable
k	Position eines erweiterten Kernereignisses in einer erweiterten MCSS
K	Kernereignis
$\vec{K}$	Systemzustandsvektor / -knoten (sequentieller Ausfallbaum)
$\vec{K}'$	Vorgängerknoten (sequentieller Ausfallbaum)
$\vec{K}''$	Nachfolgerknoten (sequentieller Ausfallbaum)

Fortsetzung nächste Seite

Fortsetzung

Symbol	Bedeutung
l	Zählvariable
λ	Ausfallrate (failure rate)
$\lambda_{i,j}$	Übergangsrate von Zustand i nach j
max(.)	Maximum-Funktion
MS	Minimalschnitt (minimal cutset)
MCSS	Minimalsequenz (minimal cutset sequence)
n	Zählvariable
nae	Token für negierte atomare Ereignisse
nce	Token für negierte Kernereignisse
nes	Token für Ereignissequenzen mit negierten Ereignissen
nees	Token für erweiterte Ereignissequenzen mit negierten Ereignissen
O{x}	Komplexität x
P	Zustandswahrscheinlichkeit
$\dot{P}$	zeitliche Änderung der Zustandswahrscheinlichkeit
φ	Boolesche Ausfallfunktion
ϖ	temporale Ausfallfunktion
r	Systemzustand (sequentieller Ausfallbaum)
r	Anzahl AND-verbundener Basisereignisse in einem erweiterten Kernereignis
R	Überlebenswahrscheinlichkeit / Zuverlässigkeit
S	Schnitt (wie in Minimal*schnitt*)
t	Zeit
t_X	Eintretenszeitpunkt von Ereignis X (Zeitpunkt des Eintretens des durch X repräsentierten Ausfalls)
T	Lebensdauer
T_M	Missionzeit
τ	Zeit (Integrationsvariable)
$\tau^{\{i\}}$	i-te Integrationsvariable in Mehrfachintegral
Δt	(infinitesimal) kleiner Zeitabschnitt
tdnf	Token für temporale Terme in TDNF
u	Zählvariable
U	Unverfügbarkeit
w	Anzahl erweiterter Kernereignisse in einer erweiterten MCSS
X	Boolesches Ereignis (Ausfalllogik: $X = 1 \rightarrow$ Ausfall, $X = 0 \rightarrow$ kein Ausfall)
Υ	Anzahl der von einer erweiterten MCSS abgedeckten MCSS
ζ	Anzahl Schnitte eines Booleschen oder temporalen Terms
ξ	Anzahl Minimalschnitte eines Booleschen oder temporalen Terms