UNI STUTTGART

Berichte aus dem
Institut für Maschinenelemente
Antriebs-, Dichtungs-, Schienenfahrzeug- u. Zuverlässigkeitstechnik

Patrick van Bergen

Methode zum simulationsbasierten Nachweis der funktionalen Sicherheit fehlertoleranter Systeme

Bericht Nr. 211

D 93
ISBN 978-3-948308-11-7

Institut für Maschinenelemente
Antriebs-, Dichtungs-, Schienenfahrzeug- u. Zuverlässigkeitstechnik

Universität Stuttgart
Pfaffenwaldring 9
70569 Stuttgart
Tel. (0711) 685 – 66170

Prof. Dr.-Ing. A. Nicola

Methode zum simulationsbasierten Nachweis der funktionalen Sicherheit fehlertoleranter Systeme

Method for a simulation-based safety verification of fault tolerant systems

Von der Fakultät Konstruktions-, Produktions- und Fahrzeugtechnik
der Universität Stuttgart
zur Erlangung der Würde eines Doktor-Ingenieurs (Dr.-Ing.)
genehmigte Abhandlung

Vorgelegt von

Patrick van Bergen
aus Waiblingen

Hauptberichter:	Prof. Dr.-Ing. Bernd Bertsche
Mitberichter:	Prof. Dr.-Ing. Hans-Christian Reuss
Tag der mündlichen Prüfung:	04.05.2023

Institut für Maschinenelemente der Universität Stuttgart
2023

Meiner Familie gewidmet

Vorwort

Die vorliegende Arbeit entstand im Rahmen einer Promotion am Institut für Maschinenelemente (IMA) der Universität Stuttgart.

Mein besonderer Dank gilt meinem Doktorvater Herr Prof. Dr.-Ing. Bernd Bertsche, ehemaliger Leiter des IMA, für die Ermöglichung dieser Arbeit, seinem fachlichen Beistand und dem entgegengebrachten Vertrauen.

Herrn Prof. Dr.-Ing. Reuss danke ich für die Übernahme des Mitberichts, die interessierte Durchsicht meiner Arbeit, sowie die hilfreichen fachlichen Hinweise.

Besonderer Dank gilt Herrn Dr.-Ing. Oliver Koller, ehemaliger Gruppenleiter Engineering Vehicle Systems - Product Area Integrating Devices – Robert Bosch GmbH, für den regen fachlichen Austausch, die motivierende und zielorientierte Art, sowie den positiven zwischenmenschlichen Umgang sowie Herrn Richard Schöttle, Abtelungsleiter der Fachabteilung Engineering Coordination of Electronic Architectures – Robert Bosch GmbH, für die Ermöglichung der Arbeit. Weiterhin gilt mein Dank meinen Doktorandenkollegen Frederic Heidinger, Armin Köhler und Philipp Kilian sowohl für die fachlich und fachfremde Unterstützung. Des Weiteren danke ich den Kollegen der Systementwicklung Energiebordnetze und Experten der Funktionalen Sicherheit Carsten Gebauer und Klaus Kutzias für die gute Zusammenarbeit und den regen fachlichen Austausch.

Ich danke den Kolleginnen und Kollegen am IMA für die gute Zusammenarbeit und das gute Institutsklima. Insbesondere meiner Bürokollegin Nika Nowiziki und meinem Bürokollegen Andreas Ostertag, für die fachlichen Diskussionen, die positive Bürostimmung und das gute Miteinander.

Ich danke den Studenten, die zu dieser Arbeit beigetragen haben, namentlich Herrn Michael Eckstein, Herrn Moritz Kapahnke und vor allem Herrn Manuel Eder.

Mein Dank gilt als letztes meiner Familie und meinen Freunden für die Rücksichtnahme und tatkräftige Unterstützung während meiner Promotionszeit.

Inhaltsverzeichnis

1 Einleitung 1

1.1 Problemstellung und Ziel der Arbeit 2

1.2 Gliederung und Aufbau der Arbeit 5

2 Grundlagen und Stand der Technik und Forschung 7

2.1 Grundlagen automatisiertes Fahren 7

2.2 Energiebordnetz 10

2.2.1 Grundlagen 10

2.2.2 Auslegung von Energiebordnetzen für automatisiertes Fahren 12

2.3 Methodische Grundlagen 13

2.3.1 Grundlagen der ISO 26262 13

2.3.2 Grundlagen der Methoden der Zuverlässigkeitstechnik und der funktionalen Sicherheit nach ISO 26262 23

2.3.3 Abgrenzung Zuverlässigkeit und funktionale Sicherheit nach ISO 26262 35

3 Methodenauswahl zur Sicherheitsbewertung fehlertoleranter Systeme 38

3.1 Anforderungen an das Energiebordnetz für automatisiertes Fahren 38

3.2 Methode zum Nachweis der funktionalen Sicherheit fehlertoleranter Systeme .42

3.2.1 Ziele des Nachweises der funktionalen Sicherheit fehlertoleranter Systeme 42

3.2.2 Eigenschaften zur Bewertung fehlertoleranter Systeme als Basis der Methodenauswahl 44

3.3 Forschungsfragen 47

3.3.1 Ableitung der Sicherheitsanforderungen an fehlertolerante Systeme 47

3.3.2 Nachweis der funktionalen Sicherheit fehlertoleranter Systeme 49

3.4 Bewertung der Methoden zur Analyse der funktionalen Sicherheit fehlertoleranter Systeme 49

4 Anforderungsableitung und Sicherheitsnachweis bei fehlertoleranten Systemen 53

4.1 Ableitung der Anforderungen von der Itemebene an die Komponentenebene ...53

4.1.1 Mathematische Beschreibung der ASIL Dekomposition 54

4.1.2 Algorithmische Realisierung der ASIL Zuweisung 58

4.1.3 Nachweis der Funktionsfähigkeit und Vergleich des Algorithmus 60

4.2 Nachweis der Einhaltung der Anforderungen des fehlertoleranten Systems 64

4.2.1 Überblick über die Methode 64

4.2.2 Erreichung Ziel Z1: Vermeidung systematischer Fehler 68

4.2.3 Erreichung Ziel Z2: Automatisierte Modellbildung und Analyse basierend auf Fehlerauswirkungen 70

4.2.4 Erreichung Ziel Z3: Berechnung der ISO 26262 Metriken 86

4.2.5 Erreichung Ziel Z4: Ermittlung der einflussreichsten Parameter 96

5 Validierung der Methode am Beispiel eines fehlertoleranten Energiebordnetzes 98

5.1 Vorgehensweise – Entwicklung Energiebordnetz für automatisiertes Fahren 98

5.2 Definitionen und Analysen auf Fahrzeugebene 99

5.3 Konzept zur Realisierung der Bremsfunktion 100

5.3.1 Definition der zulässigen Metriken der Teilfunktionen 101

5.3.2 ASIL Dekomposition der Bremsfunktion 102

5.3.3 Fehlertoleranzzeit der Bremsfunktion 102

5.4 Design des Energiebordnetzes 103

5.4.1 Definition der zulässigen PMHF auf Energiebordnetzebene 104

5.4.2 ASIL Anforderungen an das Energiebordnetz 106
5.4.3 Definition der Fehlertoleranzzeiten im Energiebordnetz 106
5.4.4 Definition der sicheren Zustände 110
5.5 Erstellung der Fehlerdatenbank 111
5.6 Erstellung des Sicherheitskonzeptes 113
5.7 Ableitung der ASIL der Komponentenebene 113
5.8 Komponentendesign 117
5.9 Aufbau der Fehlerkombinatorik 118
5.10 Quantifizierung der Komponentenfehler 119
5.11 Aufbau und Durchführung der Fehler-Simulation 123
5.12 Energiebordnetzbewertung und -optimierung mittels ISO 26262-Metriken 126
5.12.1 Analyseergebnisse 127
5.12.2 Beispielhafte Optimierung 129
6 Zusammenfassung und Ausblick 133
7 Literaturverzeichnis 136
A) Anhang 149
A1) Differentialgleichungssystem des Markov-Modells 149
A2) Bewertung der Methoden zur Modellierung fehlertoleranter Systeme 150
A21) FMEDA 150
A22) Fehlerbaumanalyse 153
A23) Markov Analyse 155
A24) Petri Netze 157
A3) Figurierte Zahlen im ASIL C und ASIL D System 159

Formelverzeichnis

$[\lambda] = \frac{1}{h}$	Einheit der Ausfallraten
$[\lambda] = FIT$	Einheit der Ausfallrate (Fehler in $10^9 h$)
DC_{FKL_i}	Diagnosedeckungsgrad mit dem ein Fehler aus Fehlerklasse i erkannt werden kann
DC_K	Diagnosedeckungsgrad der Komponentenebene
DC_n	Diagnosedeckungsgrad zu Fehler n
DC_t	Gesamtdiagnosedeckungsgrad
$E_{nied}, E_{mitt}, E_{hoch}$	Faktoren zur Abbildung des Systemparameters $SysP_{erk}$
F	Kanten des Petri-Netzes
$F(t)$	Ausfallwahrscheinlichkeit zum Zeitpunkt t
$F_{FKL-SA_1}(t_{life})$	Zustandswahrscheinlichkeit des zur Fehlerklasse gehörenden Zustandes
$F_{FKL-SA}(t_{life})$	Gesamtheit der Wahrscheinlichkeit der Zustände, die zur Verletzung des Sicherheitsziels führen
$F_{k-w/o-DC}(t)$	Summe der Ausfallwahrscheinlichkeiten der Komponentenfehler, die ohne Berücksichtigung von Diagnosen ermittelt wurden
$F_{k-w-DC}(t)$	Summe der Ausfallwahrscheinlichkeiten der Komponentenfehler, die unter Berücksichtigung von Diagnosen ermittelt wurden
$F_{MPF_{latent}}(t_{life})$	Gesamtheit der Wahrscheinlichkeit der Zustände, die als MPF_{latent} zur Verletzung des Sicherheitsziels führen
F_n	Fehler n
$F_{RF}(t_{life})$	Gesamtheit der Wahrscheinlichkeit der Zustände, die als RF zur Verletzung des Sicherheitsziels führen
$F_{SPF}(t_{life})$	Gesamtheit der Wahrscheinlichkeit der Zustände, die als SPF zur Verletzung des Sicherheitsziels führen
FTZ, FTZ_{SA_n}	Fehlertoleranzzeit, Fehlertoleranzzeit der Sicherheitsanforderung n

$F_{w/o-DC}(t)$	Ausfallwahrscheinlichkeit einer Komponente unter Vernachlässigung der komponenteneigenen Diagnosen
$F_{w-DC}(t)$	Ausfallwahrscheinlichkeit einer Komponente unter Berücksichtigung von komponenteneigenen Diagnosen
$I_{FKL-SA_1-LFM_{abs}}$	Absoluter Anteil, den die betrachtete Fehlerklasse im Vergleich zu der Gesamtheit der MPF_{latent} an der SPFM hat
$I_{FKL-SA_1-LFM_{rel}}$	Prozentualer Anteil, den die betrachtete Fehlerklasse im Vergleich zu der Gesamtheit der MPF_{latent} an der SPFM hat
I_{FKL-SA_1-PMHF}	Bedeutung einer Fehlerklasse für die PMHF des Systems
$I_{FKL-SA_1-SPFM_{abs}}$	Absoluter Anteil, den die betrachtete Fehlerklasse im Vergleich zu der Gesamtheit der SPF und RF an der SPFM hat
$I_{FKL-SA_1-SPFM_{rel}}$	Prozentualer Anteil, den die betrachtete Fehlerklasse im Vergleich zu der Gesamtheit der SPF und RF an der SPFM hat
$k_{1D} \dots k_{3D}$	Anzahl unbestimmter Minimalschnittelemente eines Minimalschnittes
k_D	Gesamtzahl der Möglichkeiten über alle Minimalschnitte bei ASIL D Bewertung des ME1
λ	Ausfallrate
λ_{FKL_i}	Fehlerrate der Fehlerklasse i
$\lambda_{m,DPF}$	Fehlerrate des Bauteils m das in Kombination mit $\lambda_{sm,DPF,latent}$ zur Verletzung des Sicherheitsziels führt
$\lambda_{m,RF}$	Fehlerrate eines residual faults eines Bauteils m
λ_{MPF}	Ausfallrate der multiple point faults
$\lambda_{MPF_{latent}}$	Ausfallrate der latenten multiple point faults
λ_n	Basisfehlerrate je Bauteil n, dass einen Beitrag zur Verletzung des Sicherheitsziels leistet
λ_{RF}	Ausfallrate der residual faults
$\lambda_{sm,DPF,detected}$	Fehlerrate eines erkannten Fehlers des Sicherheitsmechanismus, der in Verbindung mit $\lambda_{m,DPF}$ zur Verletzung des Sicherheitsziels führt

$\lambda_{sm,DPF,latent}$	Latenter Fehler des Sicherheitsmechanismus, der in Verbindung mit $\lambda_{m,DPF}$ zur Verletzung des Sicherheitsziels führt
λ_{SPF}	Ausfallrate der single point faults
λ_{SR-EBN}	Summe der Basisfehlerrate aller sicherheitsrelevanten Hardware-Bauteile im Energiebordnetz
$\lambda_{SR-gesamt}$	Gesamtfehlerrate der sicherheitsrelevanten Hardwareelemente
λ_{SR-m}	Summe der komponentenzugehörigen Basisfehlerraten aller Bauteile, die einen Beitrag zur Verletzung des Sicherheitsziels leisten
LFM	Latent fault metric
M	Zustandsraum
M_0	Verteilung der Marken zum Zeitpunkt $t = 0$
$ME1 \dots ME7$	Minimalschnittelemente 1 bis 7
n	Anzahl Elemente eines Minimalschnittes
$n_{1D} \dots n_{3D}$	Anzahl Möglichkeiten des jeweiligen Minimalschnittes bei ASIL D Bewertung des ME1
P	Stellen des Petri-Netzes
$p(0)$	Startvektor des Differnetialgleichungssystems
p_A	Gesamtzahl der Möglichkeiten bei ASIL A Bewertung des ME1
$P_{Ausfall}$	Summe der Wahrscheinlichkeiten der Markov-Ausfallzustände
p_B	Gesamtzahl der Möglichkeiten bei ASIL B Bewertung des ME1
p_C	Gesamtzahl der Möglichkeiten bei ASIL C Bewertung des ME1
p_D	Gesamtzahl der Möglichkeiten bei ASIL D Bewertung des ME1
$PMHF$	Probabilistic metric for random hardware failures
P_{MPF}	Summe der Wahrscheinlichkeiten der Markov-Ausfallzustände bedingt durch Multiple Point Faults
p_{QM}	Gesamtzahl der Möglichkeiten bei ASIL QM Bewertung des ME1
$P_{SPF} + P_{RF}$	Summe der Wahrscheinlichkeiten der Markov-Ausfallzustände bedingt durch Single Point und Residual Faults
p_{sum}	Gesamtzahl der Möglichkeiten über alle Minimalschnitte

$SPFM$	Single Point Fault Metric
$SysP_{erk}$	Systemparamter
t	Zeit, Parameter
T	Parameterraum / Transitionen des Petri-Netzes
τ_{SM}	Zeitintervall zur Erkennung von Mehrfachfehlern bevor es zur Verletzung des Sicherheitsziels kommt
t_{FF}	Zeitdauer bis zur Fehlfunktion
$t_{HW-R-4V}$	Zeitdauer bis zur Hardware-Unterspannungsabschaltung
t_{life}	Betriebsdauer
$t_{SW-R-6V}$	Zeitdauer bis zur Software-Unterspannungsabschaltung
$TTSS$	Dauer des Übergangs in den sicheren Zustand
t_{VdF-8V}	Zeitdauer bis zum Verlust der Funktion bei Unterspannung
$t_{Wiedereinschalt}$	Zeitdauer zwischen Überschreitung einer Spannungsschwelle $U_{Wiedereinschalt}$ und der Wieder-Verfügbarkeit einer Funktion
$t_{zul}(U)$	Zeitdauer, die eine gewisse Spannungsschwelle U unterschritten werden darf
$U_{Wiedereinschalt}$	Spannungschwelle nach deren Überschreitung bei SW Abschaltung eine Funktion wieder eingeschaltet wird
W	Pfeil des Petri-Netzes
$X_{min}, X_1, X_2,$ X_{max}	Stützstellen zur Ermittlung der Faktoren des Systemparameters $SysP_{erk}$
$Z(t)$	Zufallsvariablen
Z_i, Z_j	Markov Zustände

Abkürzungsverzeichnis

ASIL	Automotive Safety Integrity Level
B	Batterie
B1	Batterie 1
B2	Batterie B2
B_{HV}	Hochvolt-Batterie
ca.	circa
d.h.	das heißt
DC	Diagnosedeckungsgrad
E/E	Elektrik/Elektronik
E1…E9	Eigenschaften zur Analyse der funktionalen Sicherheit fehlertoleranter Systeme
ECE	Regelungen der Wirtschaftskommission für Europa der Vereinten Nationen
EM	Elektrische Maschine
FMEDA	Gefährdungs- und Risikoanalyse (Failure Modes Effects and Diagnostics Analysis)
FTA	Fehlerbaumanalyse
G	Generator
HV	Hochvolt
ISO	International Organization for Standardization
Kl.	Klemme
MPF	Multiple Point Fault
$MPF_{detected}$	Erkannter Multiple Point Fault
MPF_{latent}	Latenter Multiple Point Fault
QM	Qualitätsmaßnahmen
R	Verbraucher
R_B	Nicht-sicherheitsrelevante Verbraucher

RF	Residual Fault
R_{HV}	Hochvolt-Verbraucher
R_{SR1}	Sicherheitsrelevante Verbraucher 1
R_{SR2}	Sicherheitsrelevante Verbraucher 2
S	Starter
SA	Systemausfall
SAE	Society of Automotive Engineers
SM	Sicherheitsmechanismus
SP	Systemparameter
SPF	Single Point Fault
SR	Sicherheitsrelevant
TTSS	Zeit zum Übergang in den sicheren Zustand
z.B.	zum Beispiel
Z1…Z4	Ziele einer effizienten Analyse der funktionalen Sicherheit fehlertoleranter Systeme
Z1e…Z3e	Abkürzung für die erkannten Zweitfehlerebenen
Z1u…Z2u	Abkürzung für die unerkannten Zweitfehlerebenen
Zul.	Zulässig

Kurzfassung

Zur Realisierung automatisierter Fahrfunktionen ist der Einsatz fehlertoleranter Systeme im Fahrzeug unvermeidbar. Mit steigender Automatisierungsstufe entfällt der Fahrer als Rückfallebene. Aufgrund dessen muss das Fahrzeug im Fehlerfall selbsttätig den sicheren Zustand erreichen. An der Realisierung der automatisierten Fahrfunktionen sind E/E-Systeme beteiligt, weswegen die ISO 26262 bei der Entwicklung berücksichtigt werden muss. Die ISO 26262 umfasst den gesamten Sicherheitslebenszyklus eines Fahrzeuges. Ein Teil der ISO 26262 befasst sich ausgehend von den Sicherheitszielen mit der Ableitung von Sicherheitsanforderungen an die Komponentenebene. Dabei werden unter anderem die ASIL der Sicherheitsziele mittels ASIL Allokation und Dekomposition an untergeordnete Systeme und Komponenten abgeleitet. Aufgrund der hohen Systemkomplexität durch die Fehlertoleranz des Fahrzeugs ist dies händisch nicht effizient durchführbar. Aufgrund dessen werden die mathematischen Grundlagen der ASIL Dekomposition sowie ein Algorithmus zur automatisierten ASIL Allokation und Dekomposition auf Basis einer Fehlerbaumanalyse vorgestellt. Ein weiterer Bestandteil der ISO 26262, der durch die Analyse fehlertoleranter Systeme beeinflusst wird, ist der Nachweis, dass das Fahrzeug ausreichend sicher ist. Aufgrund der hohen Systemkomplexität sind die ISO 26262 Standardmethoden, Fehlerbaumanalyse und FMEDA, zur Modellierung der fehlertoleranten Systeme nur bedingt geeignet. Aufgrund dessen wird ein Ansatz basierend auf einer Markov-Analyse zur Modellierung der Fehlertoleranz vorgestellt. Das Markov-Modell wird automatisiert auf Basis von Fehlerinjektionssimulationen aufgebaut, welche das Systemverhalten im Fehlerfall bei Einfach- und Mehrfachfehlern beschreiben. Die Zustandsübergänge des Markov-Modells werden mittels Fehlerbaumanalysen der fail-safe Komponentenebene quantifiziert. Durch die vorgestellte Methode

- werden die zum Sicherheitsnachweis benötigten ISO 26262-Metriken berechnet,
- eine effiziente Systemoptimierung durch Identifikation der einflussreichsten Fehler / Fehlerkombinationen durchgeführt,
- der Einfluss von Parametervariationen mittels Sensitivitätsanalysen bewertet,
- der Nachweis der Funktionsfähigkeit von Sicherheitsmechanismen durchgeführt,
- die Erkennung und Behebung systematischer Fehler des Systemdesigns, der Komponentendimensionierungen und Fehlerreaktionen umgesetzt.

Abstract

Method for a simulation-based safety verification of fault tolerant systems

For enabling automated driving the use of fault tolerant systems within vehicles is inevitable. With the rising automation level the driver is omitted as fallback solution. In the event of a fault, the vehicle needs to be able to reach the safe state on its own. Examples for the safe state are the standstill on the emergency lane or the standstill in the next parking area. Because E/E-systems are part of realizing the automated driving functions ISO 26262 needs to be considered during the development of automated driving functions in the automotive industry. ISO 26262 encloses the entire safety lifecycle of a vehicle. One part of the ISO 26262 deals with the derivation of the safety requirements at the component level from the safety goals which are defined using the hazard analysis and risk assessment. At this, the ASIL of the safety goals are derived to subordinated systems and components using ASIL allocation and decomposition. Due to the high system complexity of the automated driving vehicle caused by the fault tolerance, the derivation cannot be realized efficiently by hand. Therefore the mathematical basics of the ASIL decomposition and an algorithm for the automated ASIL allocation and ASIL decomposition based on decision trees are introduced. For the derivation of the safety requirements the algorithm uses minimal cut sets which are extracted from a fault tree analysis. The algorithm is compared to a randomized algorithm. The advantages of the decision tree based algorithm over the randomized algorithms are higher speed and the certainty to find every possible solution after the termination of the algorithm. Constraints for ASIL can be considered to get the optimum of all possible solutions. Another part of the ISO 26262 that is affected by fault tolerant automated driving systems is the verification that the vehicle is sufficiently safe and the identified safety goals are only violated below an acceptable degree. Due to the complexity of the fault tolerant system ISO 26262 standard methods fault tree analysis and FMEDA are only suitable in a limited extend. Markov-Analyses described in literature are used for the modeling of fault-tolerant systems, although they are not capable of realizing safety verification compliant with ISO 26262. Thus an approach for modeling the fault tolerant system using Markov-Analysis is introduced. The Markov-Model thereby is automatically built based on the

results of fault injection simulations that describe the system behavior for single and multiple point faults. The transition between the states of the Markov-Model are quantified using fault tree analyses of the fail-safe component level. By the introduced method

- the calculation of the ISO 26262 metrics that are necessary for the safety verification,
- an efficient system optimization by identification of the most influencing faults and fault combinations,
- the evaluation of the influence of parameter variations using sensitivity analysis,
- the verification of the functioning of safety mechanisms and
- the detection and remedy of systematic faults such as the system design, component dimensioning and fault reactions

are possible. The application of the introduced method is shown using the example of a vehicle electrical system which is used for the realization of automated driving functions.

1 Einleitung

Die Entwicklung automatisierter Fahrzeuge birgt das Potential zum größten Umbruch bei der Entwicklung des Automobils seit dessen Erfindung [BER13]. Dies ist ein Trend, an dem neben konventionellen Automobilherstellern auch große Technologiefirmen teilhaben wollen [HAR15]. Die Motivation zur Entwicklung von Fahrzeugen mit automatisierten Fahrfunktionen ist in Abbildung 1.1 dargestellt und umfasst unter anderem die Erhöhung der Verkehrssicherheit [GAS12] und die Optimierung des Verkehrsflusses [GAS12] zur Vermeidung von Staus und zur Minderung der Belastung der Verkehrsinfrastruktur [HAR15, BMVI15]. Durch Automatisierung wird individuelle Mobilität, z.B. bei Krankheit, Müdigkeit oder Medikamenteneinnahme, sowie eine Erhöhung des Fahrkomforts gewährleistet [MAU15, VDA15]. Außerdem kann bei Nutzfahrzeugen die Produktivität, Zuverlässigkeit und Flexibilität durch Fahrzeugautomatisierung erhöht werden [FLÄ12].

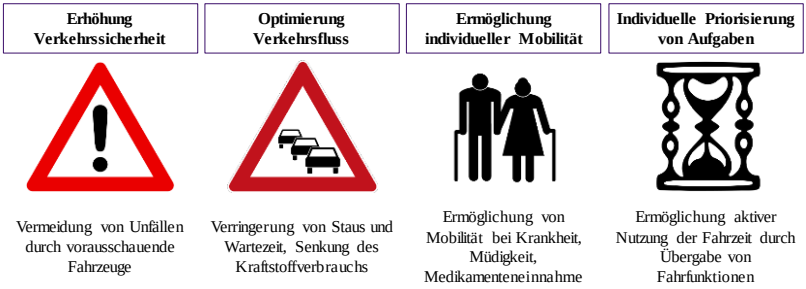


Abbildung 1.1: Motivation zur Entwicklung des automatisierten Fahrens

Heutige Fahrzeugsysteme sind fail-safe ausgelegt. Ein fail-safe System zeichnet sich dadurch aus, dass dieses im Falle eines Fehlers augenblicklich den aktuellen Betriebszustand verlassen muss und durch Abschalten seiner Funktion das System in den sicheren Zustand bringt [KEL18].

Beispielsweise verstärkt das heutige Bremssystem die vom Fahrer über das Bremspedal aufgebrachte Bremskraft [PIS16]. Ein Fehler im Bremssystem führt z.B. zum Entfall der

Bremskraftverstärkung. Die Auswirkungen des Fehlers werden entkoppelt, sodass der Fahrer das Fahrzeug als Rückfallebene durch die aufgebrachte Pedalkraft (Muskelkraft) in den sicheren Zustand bringen kann [BRE17].

Übersteigt ein Fahrzeug die Teilautomatisierung, bei welcher das Fahrzeug in spezifischen Anwendungsfällen Längs- und Querführung übernimmt, der Fahrer jedoch weiterhin als sofortige Rückfallebene zur Verfügung steht, übernimmt das Fahrzeug Funktionen des Fahrers. Im Normalbetrieb erkennt das Fahrzeug sein Umfeld, plant zu fahrende Trajektorien und setzt diese u.a. mittels Brems- und Lenksystem um. Im Fehlerbetrieb steht der Fahrer erst nach einer definierten Übergabezeit oder überhaupt nicht mehr als Rückfallebene zur Verfügung. Dementsprechend muss das Fahrzeug im Fehlerfall seine Fahraufgabe zumindest für eine begrenzte Dauer bis zur Fahrerübernahme oder bis zur Erreichung des sicheren Zustandes weiterführen.

Das Verhalten, bei dem eine aktive Funktion trotz Fehler nach einem im Voraus definierten „sicheren Funktionsverhalten“ weiter ausgeführt wird, bis der sichere Zustand erreicht ist, wird als fail-operational Verhalten bezeichnet. Im Normalfall wird in diesem Modus die Funktionalität im Vergleich zum Normalbetrieb eingeschränkt [KEL18]. Zur sicheren Realisierung des automatisierten Fahrens werden deswegen Verfügbarkeitsanforderungen an die sicherheitsrelevanten Funktionen definiert.

1.1 Problemstellung und Ziel der Arbeit

Wie in Kapitel 1 beschrieben ergeben sich aus automatisierten Fahrfunktionen, welche eine Teilautomatisierung übersteigen, Verfügbarkeitsanforderungen an sicherheitsrelevante Fahrzeugfunktionen, da das Fahrzeug jede Situation im automatisierten Betrieb beherrschen muss. Aus diesem Grund wird der funktionalen Sicherheit durch die Automatisierung eine größere Bedeutung zugeschrieben [GAS12].

Zur Realisierung von Verfügbarkeitsanforderungen können nach [MOT99, AVI04] folgende Strategien eingesetzt werden:

- Fehlervermeidung (fault prevention)

  Bei der Fehlervermeidung wird das Auftreten von Fehlern durch geeignete Maßnahmen, wie z.B. den Einsatz einer geeigneten Entwicklungsmethodik, verhindert [AVI04].
- Fehlerbehebung (fault removal)

  Die Fehlerbehebung befasst sich mit der Erkennung, Lokalisierung und Behebung von Fehlern [MOT99]. Dabei werden die „Fehlerbehebung in der Entwicklungsphase“ und die „Fehlerbehebung im Betrieb“ unterschieden. Die Fehlerbehebung in der Entwicklungsphase umfasst die Verifikation, d.h. die Überprüfung, ob die Spezifikation eingehalten wird. Bei der Verifikation werden mittels Fehlererkennung, z.B. durch Testverfahren, Fehler erkannt und anschließend behoben. Die Verifikation wird durchgeführt, bevor ein System produziert wird. Bei der Fehlerbehebung im Betrieb werden Fehler im Normalbetrieb erkannt und behoben. Ebenso können Fehler, die z.B. in anderen Systemen bereits aufgetreten sind, behoben werden [AVI04].
- Fehlervorhersage (fault forecasting):

  Die Fehlervorhersage dient dazu, Fehler zu einem Zeitpunkt vorherzusagen, bei dem diese noch keine Auswirkung haben, sodass rechtzeitig Maßnahmen zur Vermeidung der Auswirkungen eingeleitet werden können [NIU17].
- Fehlertoleranz (fault tolerance)

  Unter fehlertoleranten Systemen werden Systeme verstanden, die „auch dann noch korrekt arbeiten, wenn während ihrer Ausführung eine bestimmte Anzahl von Fehlern auftreten“ [GÄR01]. Fehlertoleranz lässt sich z.B. durch redundante Strukturen realisieren.

Die Strategien zur Fehlervermeidung und Fehlerbehebung in der Entwicklungsphase sind bereits heute Teil des Entwicklungsvorgehens, das in der für Fahrzeuge gültigen Sicherheitsnorm (ISO 26262) beschrieben ist und muss daher keiner weiteren Betrachtung unterzogen werden. Die Fehlerbehebung im Betrieb wird erst dann relevant, wenn sich bereits Fahrzeuge im Betrieb befinden und Fehler nicht durch den Entwicklungsprozess

erkannt und behoben werden konnten. Automatisierte Fahrzeuge befinden sich zum aktuellen Zeitpunkt noch nicht im Feld, weswegen diese Strategie nicht weiter vertieft wird.

Werden Fehler durch Fehlervorhersage erkannt, bevor diese eintreten bzw. Auswirkungen haben, können diese rechtzeitig behoben werden. Dadurch treten seltener sicherheitsrelevante Fehler auf, wodurch die Kundenakzeptanz für automatisierte Fahrfunktionen steigt.

Zur Ermöglichung der sicheren Weiterfahrt im Fehlerfall (fail-operational) ist die Fehlertoleranz die relevante Strategie. Diese ist für die sicherheitsrelevanten Funktionen wie Lenk- und Bremsfunktion unvermeidbar, um im Fehlerfall ein unkontrollierbares Fahrzeug und damit ein enormes Sicherheitsrisiko zu vermeiden. Daher liegt der Fokus der Arbeit auf Fehlertoleranz. Um Fehlertoleranz zu realisieren, werden z.B. im Energiebordnetz, das im Anwendungsbeispiel aus Kapitel 5 weiter vertieft wird, redundante Strukturen eingeführt. Redundante Strukturen werden für die Lenkfunktion ebenso aus der Gesetzgebung [ECE R 79] gefordert. Da das Energiebordnetz an der Lenkfunktion beteiligt ist, ergeben sich Redundanzanforderung aus der Gesetzgebung an das Energiebordnetz. Durch die Fehlertoleranz ergeben sich neue Anforderungen für die Analysen der Systeme:

- Steigende Anzahl an Komponenten aufgrund der redundanten Funktionsausführung und folglich höherer Modellierungsaufwand
- Wechselwirkungen durch die Umsetzung der redundanten sicherheitsrelevanten Funktionen
- Weiterbetrieb des Systems trotz erkanntem Fehler bis zum Erreichen des sicheren Zustandes inkl. Manöver und Dauer des Übergangs in den sicheren Zustand
- Steigende Komplexität bei der Identifikation von Fehlerauswirkungen von Ein- und Mehrfachfehlern aufgrund der Redundanzstruktur und der Vielzahl an zu berücksichtigenden Einflüssen (Betriebsparameter, Betriebsstrategien, Dimensionierungen, Manöver und Dauer möglicher Übergänge in den sicheren Zustand, spezifizierte Funktionsverlustgrenzen).

Aufgrund der neuen Anforderungen ist eine händische Ableitung der Anforderungen an die Elemente des fehlertoleranten Systems v.a. aufgrund der gestiegenen Anzahl an Komponenten und der Vielzahl an Möglichkeiten zur Partitionierung der Anforderungen händisch nicht mehr möglich. Des Weiteren sind die Modellierungsmethoden zur Analyse der Sicherheit heutiger fail-safe Systeme, wie z.B. FMEDA oder FTA, zur Analyse der Fehlertoleranz nicht vollumfänglich geeignet.
Ziel der Arbeit ist es, durch eine gesamtheitliche Methode die steigende Komplexität durch fehlertolerante Systeme zu behandeln. Dabei liegt der Fokus v.a. auf der

- Effizienten und vollständigen Ableitung der Anforderungen an Komponenten fehlertoleranter Systeme
- Effizienten, reproduzierbaren und vollständigen Bewertung von Fehlern und deren Auswirkungen in fehlertoleranten Systemen.

Dazu wird ermittelt, welche zusätzlichen Effekte durch die Betrachtung fehlertoleranter Systeme bei der quantitativen Bewertung berücksichtigt werden müssen, um einen ISO 26262 konformen Sicherheitsnachweis durchführen zu können.

1.2 Gliederung und Aufbau der Arbeit

In *Kapitel 2* werden die Grundlagen zum automatisierten Fahren und Energiebordnetzen gelegt. Die Zuverlässigkeitstechnik und die funktionale Sicherheit werden gegenübergestellt und die funktionale Sicherheit detailliert vorgestellt. Zusätzlich werden die Grundlagen zu den Methoden, die sowohl bei Zuverlässigkeitsanalysen als auch bei Sicherheitsnachweisen eingesetzt werden können, vorgestellt.
Die Forschungsfrage sowie die Ziele, die für einen effizienten Sicherheitsnachweis erreicht werden müssen, sowie die Eigenschaften, welche die Methode beim Sicherheitsnachweis bei fehlertoleranten Systemen abbilden muss, werden in *Kapitel 3* definiert. Die in Kapitel 2 vorgestellten Methoden werden hinsichtlich der Ziele und Eigenschaften gegenübergestellt und eine geeignete Methode ausgewählt.
Im ersten Teil von *Kapitel 4* wird die Vorgehensweise zur Ableitung der Sicherheitsanforderungen von der Fahrzeugebene bis zur Komponentenebene vorgestellt. Der Prozess wird mathematisch beschrieben und ein Algorithmus zur Umsetzung

vorgestellt. Im zweiten Teil des vierten Kapitels wird die Methode zum Sicherheitsnachweis fehlertoleranter Systeme vorgestellt und aufgezeigt, wie die in Kapitel 3 definierten Ziele und Eigenschaften durch die Methode erreicht werden können.
Anhand eines Energiebordnetzes für automatisiertes Fahren wird die Eignung der in Kapitel 4 vorgestellten Methode zum Sicherheitsnachweis fehlertoleranter Systeme in *Kapitel 5* gezeigt.
In *Kapitel 6* wird das Erarbeitete zusammengefasst, sowie ein Ausblick über die potentielle Weiterarbeit gegeben.

2 Grundlagen und Stand der Technik und Forschung

Im ersten Teil des Kapitels werden Grundlagen zum automatisierten Fahren und der Leistungs- und Energieversorgung automatisierter Fahrzeuge durch Energiebordnetze aufgezeigt. Im Anschluss daran werden die funktionale Sicherheit im Kraftfahrzeug nach [ISO26262] sowie typische Methoden der Zuverlässigkeitstechnik vorgestellt, die ebenso bei der Analyse der funktionalen Sicherheit eingesetzt werden. Zum Schluss des Kapitels werden die Zuverlässigkeitstechnik und die funktionale Sicherheit nach [ISO26262] gegenübergestellt.

2.1 Grundlagen automatisiertes Fahren

Nachfolgend werden die unterschiedlichen Automatisierungsstufen erläutert. Die Stufen, nach welchen die automatisierten Fahrzeugfunktionen eingeteilt werden, sind von der Bundesanstalt für Straßenwesen [GAS12] und der National Highway Traffic Safety Administration [NHTSA13] definiert. Die SAE International J3016 [SAE-J3016] definiert ebenfalls Automatisierungsstufen und stellt die Definitionen der Automatisierungsstufen nach [GAS12] und [NHTSA13] gegenüber. Diese Dissertation verwendet die durch die [VDA15] erweiterten Definitionen der [GAS12]. Die Automatisierungsstufen sind in Abbildung 2.1 dargestellt.

Die niedrigste Automatisierungsstufe ist Stufe null, bei welcher der Fahrer die Fahraufgabe vollumfänglich übernimmt. Beginnend ab Stufe eins steigt der Automatisierungsanteil kontinuierlich mit jeder weiteren Stufe. Die Automatisierungsstufen zwei bis vier werden dabei auf einen Anwendungsfall bezogen, die verbleibenden Anwendungsfälle werden vom Fahrer abgedeckt. Anwendungsfälle werden allgemein durch „Straßentypen, Geschwindigkeitsbereiche und Umfeldbedingungen“ definiert [VDA15], beispielsweise die Fahrt auf der Autobahn bis 140 km/h bei guten Sichtverhältnissen. Bei Automatisierungsstufe fünf übernimmt das Fahrzeug die Fahraufgabe vollumfänglich und in jedem Anwendungsfall.

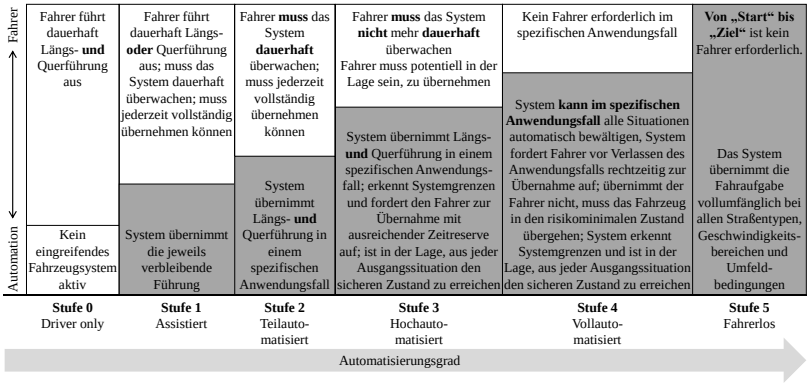


Abbildung 2.1: Automatisierungsstufe nach [GAS12] erweitert mit [VDA15]

Der heutige Stand der Technik erreicht nach [VDA15] die Automatisierungsstufe zwei, vereinzelt wird Stufe drei erreicht. Zum Aufzeigen der Neuerungen bei zukünftigen Fahrfunktionen wird nachfolgend der Stand der Technik (Automatisierungsstufen kleiner gleich zwei) den Automatisierungsstufen größer gleich drei gegenübergestellt. Die Neuerungen sind in Tabelle 2.1 graphisch dargestellt.

Ab Automatisierungsstufe zwei übernimmt das Fahrzeug die Längs- und die Querführung, d.h. das Fahrzeug muss sein Umfeld erkennen, Trajektorien planen und diese mittels Aktuatorik umsetzen. Bei Stufe zwei muss der Fahrer das Fahrzeug dabei dauerhaft überwachen und dieses im Fehlerfall übernehmen. Der Fahrer hat somit die Verantwortung für das Fahrzeug. Ab Automatisierungsstufe drei muss der Fahrer das Fahrzeug im automatisierten Betrieb nicht mehr dauerhaft überwachen („eyes-off System"). Das Fahrzeug muss das Erreichen von Systemgrenzen bzw. Fehler im System rechtzeitig erkennen, den Fahrer zur Übernahme des Fahrzeugs auffordern und bis zur zeitlich begrenzten Fahrerübernahme die Fahrfunktion weiter ausführen. Die Verantwortung im automatisierten Betrieb liegt ab Stufe drei beim Fahrzeug. Ab Automatisierungsstufe vier steht der Fahrer nicht mehr als Rückfallebene zur Verfügung ("mind-off" System) und das Fahrzeug muss im Fehlerfall selbstständig einen risikominimalen Zustand (sicherer Zustand, siehe Kapitel 2.3.1), wie z.B. den

Fahrzeugstillstand erreichen. Um dies zu realisieren ist ein fehlertolerantes System notwendig [BEC15].

Bei den Strategien zum Übergang in den sicheren Zustand werden gesteuerte und geregelte Strategien unterschieden. Bei geregeltem Übergang wird die Rückfallebene mit Umfelderkennung und Trajektorienplanung ausgestattet. Auf diese Weise herrscht auch in der Rückfallebene dauerhaft Sicht, wodurch Ausweichmanöver und Spurwechsel durchgeführt werden können. Dabei sind Reaktionen auf Veränderungen im Umfeld, wie z.B. Hindernisse, bei der geregelten Strategie möglich. Bei der gesteuerten Rückfallstrategie hingegen wird im Normalbetrieb zyklisch eine Rückfalltrajektorie abgespeichert. Im Fehlerfall wird diese Rückfalltrajektorie abgefahren. Dadurch sind bei gesteuerten Rückfallstrategien keine Reaktionen auf sich verändernde Umfeldbedingungen möglich [KUR17].

Tabelle 2.1: Vergleich der Funktionserfüllung beim automatisierten Fahren kleiner gleich Automatisierungsstufe zwei und Automatisierungsstufe größer gleich drei erweitert nach [BER15]

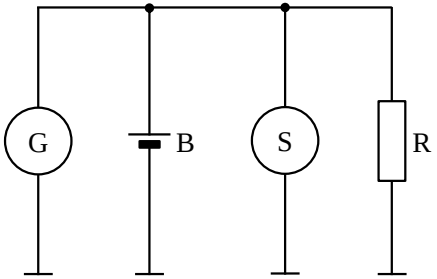
Automatisierungsstufe ≤ zwei		**Automatisierungsstufe ≥ drei**
Verantwortung beim Fahrer		Verantwortung (im Fahrszenario) beim Fahrzeug
Entscheidungsfähigkeiten des Fahrers		Maschinelle Lernverfahren
Gedächtnis des Fahrers		Karte, Umfeldmodell
Augen des Fahrers		Sensoren
Bewegungskoordination und Reflexe des Fahrers		Aktuatorik und zugehörige Regelungssysteme
Ohren des Fahrers		Vehicle-to-X-Kommunikation
Muskelkraft des Fahrers verstärkt durch Fahrzeugenergie		Reine Energieversorgung aus dem Energiebordnetz

2.2 Energiebordnetz

Zur Realisierung der in Kapitel 2.1 beschriebenen Fahrzeugfunktionen mit Automatisierungsstufen größer gleich drei wird die Leistungs- und Energieversorgung durch das Energiebordnetz benötigt, da die Umfelderkennung, Trajektorienplanung, sowie deren Umsetzung durch Brems- und Lenksystem im automatisierten Betrieb rein elektrisch erfolgen. Da das Energiebordnetz im Anwendungsbeispiel aus Kapitel 5 wieder aufgenommen wird, werden in Kapitel 2.2.1 dessen Grundlagen erläutert und in Kapitel 2.2.2 die Auslegung von Energiebordnetzen für automatisiertes Fahren fokussiert.

2.2.1 Grundlagen

Im Fahrzeug-Bordnetz werden sowohl elektrische Energie als auch Informationen übertragen [BAB13][TEI12], wobei der Fokus dieser Arbeit auf dem Energiebordnetz liegt. Zweck des Energiebordnetzes ist die Bereit- und Sicherstellung der Energieversorgung im Fahrzeug [BOR10]. Dabei besteht das Energiebordnetz aus mindestens einer Energiequelle, einem Energiespeicher, mehreren Verbrauchern und dem Kabelbaum [HES11]. Schmelzsicherungen sind ebenfalls Teil des Energiebordnetzes und dienen dazu, einen Fahrzeugbrand durch thermische Überlastung von Kabeln durch permanent anliegende Kurzschlüsse zu verhindern [BOR10]. Die Mindestausführung eines Energiebordnetzes ist in Abbildung 2.2 dargestellt.



Legende:
B Batterie G Generator R Verbraucher S Starter

Abbildung 2.2: Mindestausführung eines Energiebordnetzes [SCH10]

Der Starter (S), ein Elektromotor, dient dazu, den Verbrennungsmotor vom Stillstand auf eine bestimmte Drehzahl zu bringen. Ab dieser Drehzahl kann sich der Verbrennungsmotor selbstständig in Betrieb halten [BOR10]. Dieser leistungsintensive Vorgang wird durch die Batterie (B) ermöglicht. Im Fahrbetrieb wird der Generator (G) durch den Verbrennungsmotor angetrieben [BOR10] und liefert die elektrische Energie zum Laden der Batterie sowie die Energie für den Betrieb der Verbraucher (R) wie z.B. die Zünd- und Einspritzanlage, der Steuergeräte, der Sicherheitselektronik und der Komfortelektronik, für die Beleuchtung und für weitere Geräte und Einrichtungen, die während der Fahrt benötigt werden [REI10]. Verbraucher können in sicherheitsrelevante und nicht sicherheitsrelevante Verbraucher eingeteilt werden [EEHE15]. Zu den nicht sicherheitsrelevanten Verbrauchern gehören z.B. Komfortsysteme wie die Sitzheizung, die Klimaanlage und das Radio. Sicherheitsrelevante Verbraucher sind z.B. das Lenk- und das Bremssystem. Die Wandlung und Speicherung der Energie im Energiebordnetz werden während der Fahrt über ein elektrisches Energiemanagementsystem (EEM) geregelt. Beispielsweise überwacht das EEM bei abgestelltem Motor die Batterie und schaltet alle Stillstands- und Ruhestromverbraucher ab, sobald die Batterieladung einen kritischen Ladezustand erreicht hat. Das EEM regelt den gesamten Energiehaushalt des Fahrzeugs und vergleicht hierfür kontinuierlich die Leistungsanforderungen der Verbraucher mit dem Leistungsangebot des Energiebordnetzes. Auf diese Weise sichert es ein Gleichgewicht zwischen der Leistungserzeugung und der Leistungsabgabe [REI11] [PIS16].

Trotz der erheblich gestiegenen Anforderungen an Energiebordnetzte haben in den letzten zehn Jahren kaum grundlegende Veränderungen an der Struktur des Energiebordnetzes stattgefunden. Die Integration der neuen zusätzlichen Komponenten erfolgte dabei stets durch größere Dimensionierung des Generators, der Batterie, des Kabelbaums und des Stromverteilers im 12-V-Teilnetz [SCH10]. Steigende Komplexitäten ergaben sich durch die steigende Elektrifizierung und Realisierung neuer Funktionen, wie z.B. Start-Stopp-Funktionen, Bremsenergierückgewinnung oder elektrische Lenkunterstützung [BAB13].

2.2.2 Auslegung von Energiebordnetzen für automatisiertes Fahren

Bordnetze für Automatisierungsstufen kleiner gleich zwei werden v.a. hinsichtlich Ladebilanz und Spannungsstabilität ausgelegt. Das Ziel von Ladebilanzuntersuchungen ist es „Aussagen über die Restkapazität einer Bordnetzanlage nach einem bestimmten Fahrzyklus bei vorgegebener Verbraucherleistung zu gewinnen“ [HEN90]. Bei Spannungsstabilitätsuntersuchungen wird überprüft, ob es während des Betriebs im Energiebordnetz zu Spannungseinbrüchen unter einen zulässigen Spannungswert kommt. Dies führt dazu, dass Komponenten des Energiebordnetzes ihre Funktion nicht mehr oder nur noch degradiert ausführen können [RUF15].

Diese Auslegungskriterien sind für Energiebordnetze für Fahrfunktionen größer gleich Automatisierungsstufe drei weiterhin notwendig, jedoch nicht ausreichend, da das Fahrzeug im Fehlerfall noch eine gewisse Zeit funktionsfähig bleiben muss (siehe Kapitel 1). Dadurch muss die Energieversorgung als Basis der automatisierten Fahrzeugfunktionen ebenfalls zur Verfügung stehen, siehe Kapitel 2.1. Nach Abbildung 2.3 muss aus Produkthaftungssicht neben der Ladebilanz und der Spannungsstabilität die Gesetzgebung wie z.B. die [ECE R13-H] und die [ECE R79], sowie technische Standards wie z.B. die ISO 26262 als Norm der funktionalen Sicherheit im Kraftfahrzeug berücksichtigt werden. Zur Entwicklung qualitativ hochwertiger Energiebordnetze und zur Vermeidung von Liegenbleibern muss zusätzlich die Zuverlässigkeitstechnik berücksichtigt werden [KUR17].

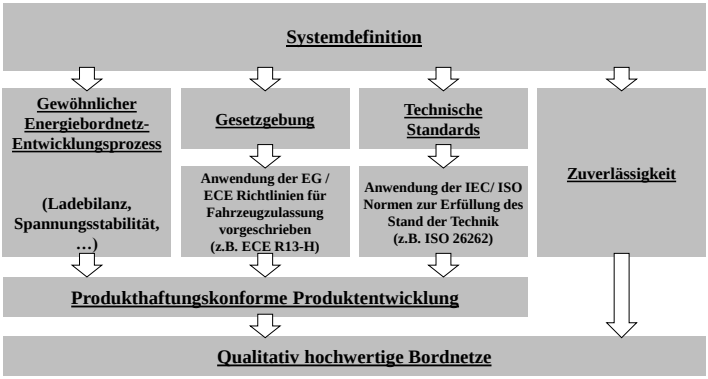


Abbildung 2.3: Auslegung qualitativ hochwertiger Energiebordnetze [KUR17]

2.3 Methodische Grundlagen

2.3.1 Grundlagen der ISO 26262

Die ISO 26262 dient dazu Gefährdungen aufgrund von ungewolltem Verhalten von sicherheitsrelevanten E/E Systemen und deren Interaktionen bei Serien PKW bis zu einem zulässigen Gesamtgewicht von 3,5 Tonnen zu vermeiden [ISO26262-1, Scope]. Dabei werden sicherheitsrelevante elektrische, elektronische und Software-Komponenten bei der Analyse berücksichtigt. Die ISO 26262 stellt einen Leitfaden zur Vermeidung inakzeptabler Risiken mittels geeigneter Anforderungen und Prozesse dar [ISO26262-1, Introduction]. Die ISO 26262 schreibt das Entwicklungsvorgehen nach dem V-Modell vor. Das V-Modell ist in Abbildung 2.4 dargestellt.

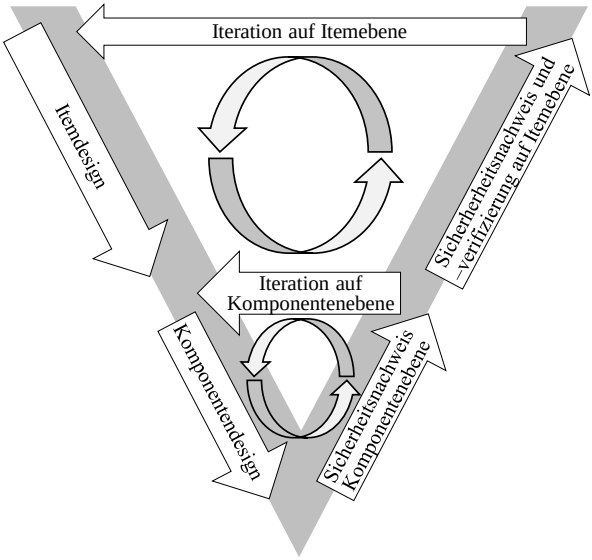


Abbildung 2.4: V-Modell: Entwicklungsprozess der funktionalen Sicherheit nach [ISO 26262-1, Figure 1]

Auf der linken Seite des V-Modells werden im ersten Schritt die Systemgrenzen (Item) definiert. Mittels Gefährdungsanalyse und Risikobewertung werden die Sicherheitsziele des Systems identifiziert. Ein Beispiel für ein Sicherheitsziel ist „Vermeide unterbremstes Fahrzeug“. Im nächsten Schritt wird die funktionale Architektur entwickelt. Im Anschluss daran wird das vorläufige Architekturdesign festgelegt und die Sicherheitsanforderungen den Elementen des vorläufigen Architekturdesigns zugewiesen. Die Bremsfunktion im automatisierten Fahrbetrieb benötigt z.B. die Umfelderkennung, Trajektorienplanung, Bremsaktuation und Energieversorgung.

Um die Komponenten, die zu einem dieser Teilsysteme gehören, entwickeln zu können, werden die Sicherheitsanforderungen an die Komponenten abgeleitet. Eine funktionale Sicherheitsanforderung wird dabei als „Spezifikation von applikationsunabhängigem Sicherheitsverhalten oder einer applikationsunabhängigen Sicherheitsmaßnahme inklusive ihrer zugehörigen sicherheitsbezogenen Attribute“ verstanden [ISO 26262]. Die sicherheitsbezogenen Attribute umfassen den zugehörigen sicheren Zustand, die Fehlertoleranzzeit, das Automotive Safety Integrity Level sowie die zulässigen ISO 26262-Metriken (PMHF, SPFM, LFM).

Der sichere Zustand wird nach [ISO 26262-1, 3.131] als Betriebszustand eines Items definiert, der im Fehlerfall eingenommen wird und kein unzumutbares Risiko aufweist. Dabei werden nach [ISO 26262-1, Figure 5] unterschiedliche Möglichkeiten zum Erreichen des sicheren Zustandes definiert. In dieser Arbeit wird die Definition nach Abbildung 2.5 zugrunde gelegt. Dabei wird nach der Erkennung eines Fehlers die Emergency Operation eingeleitet, welche das Fahrzeug letztendlich in den sicheren Zustand überführt. Ein beispielhafter sicherer Zustand ist in diesem Fall das am Fahrbahnrand abgestellte Fahrzeug. Die Emergency Operation stellt eine Fehlerreaktion zur Umsetzung von Verfügbarkeitsanforderungen dar. Bei Verfügbarkeitsanforderungen muss die geforderte Funktion zumindest in degradiertem Umfang trotz Fehler weiter zu Verfügung stehen. I.d.R. lässt sich die Verfügbarkeitsanforderung und damit die Emergency Operation nur durch fehlertolerante Systeme darstellen [ISO 26262-1, 3.43]. Folglich beinhaltet der Übergang in den sicheren Zustand in dieser Arbeit immer auch die Emergency Operation.

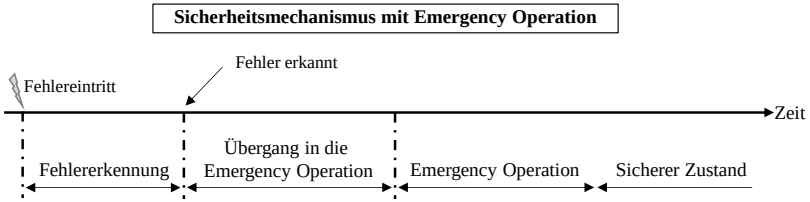


Abbildung 2.5: Definition des sicheren Zustandes nach [ISO 26262-1, Figure 5]

Unter der Fehlertoleranzzeit (FTZ) wird nach [ISO 26262-1, 3.61] die Zeit verstanden, nach deren Überschreitung es zur Verletzung eines Sicherheitsziels kommt, wenn eine sicherheitsrelevante Funktion in diesem Zeitraum nicht zur Verfügung steht. Beispielsweise wird für ein Fahrzeug festgestellt, dass der Verlust einer Bremsfunktion erst dann kritisch ist, wenn der Verlust länger als 400ms anhält. Daher wird die Fehlertoleranzzeit des zugehörigen Sicherheitsziels auf 400ms festgelegt.

Das Automotive Safety Integrity Level (ASIL) steht für „eines von 4 Level, welches die nötigen Anforderungen der ISO 26262 an ein Item oder Element sowie zugehörige Sicherheitsmaßnahmen zur Vermeidung inakzeptabler Risiken, definiert. Dabei ist ASIL D die strengste Anforderung und ASIL A die mildeste.“ [ISO26262-1, 3.6] Komponenten, denen keine zusätzlichen Maßnahmen zugewiesen werden, werden unter Berücksichtigung von Standard-Qualitätssicherungsprozessen entwickelt und als QM eingestuft.

Für die jeweiligen Teilsysteme werden vorläufige Architekturdesigns festgelegt und den vorläufigen Architekturelementen die Funktionen des funktionalen Sicherheitskonzepts zugewiesen. Unter den Metriken der ISO 26262 versteht man probabilistische Zielgrößen, welche eine Aussage über die Güte eines Systems bzgl. zufälliger Hardware-Fehler erlauben, siehe Kapitel 2.3.1.3. Die Metriken der vorläufigen Architekturelemente werden durch Budgetierung der Item Metrik ermittelt. Auf Basis der analysierten Kenngrößen werden die Komponenten, die zur Erreichung der Sicherheitsziele nötig sind, entwickelt.

Der rechte Ast des V-Modells dient zum Nachweis, dass das Risiko der Verletzung des Sicherheitsziels unterhalb des akzeptablen Restrisikos liegt. Der Nachweis wird zunächst auf der Komponenten-, im Anschluss auf der Systemebene durchgeführt.

Nach ISO 26262 müssen in den unterschiedlichen Analysen sowohl systematische als auch zufällige Hardwarefehler berücksichtigt werden. Fehler, die Unabhängigkeitsanforderungen aushebeln und zur Verletzung des Sicherheitsziels führen, müssen ebenso erkannt und behoben werden, siehe Abbildung 2.6.

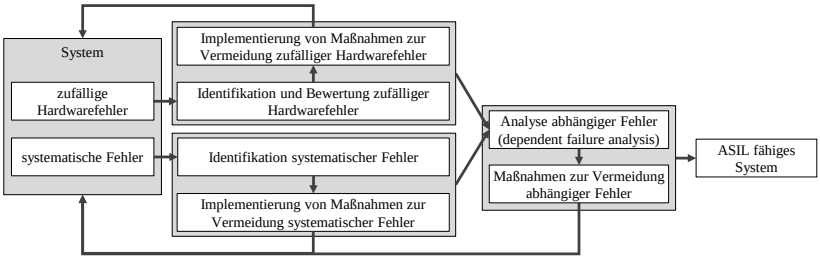


Abbildung 2.6: Iterativer Sicherheitsnachweis zur Entwicklung eines ASIL-fähigen Systems

2.3.1.1 ASIL Dekomposition – Stand der Technik

Ziel der ASIL Dekomposition ist die „redundante Aufteilung von Sicherheitsanforderungen an ausreichend unabhängige Elemente mit dem Ziel das ASIL der redundanten Sicherheitsanforderungen zu reduzieren und an die zugehörigen Elemente zuzuweisen (Allokation)“ [ISO26262-1, 3.3]. Wird keine ausreichende Unabhängigkeit der an der ASIL Dekomposition beteiligten Elemente erreicht, so “erben die redundanten Anforderungen und deren zugehörige Architekturelemente das ursprüngliche ASIL“ [ISO26262-9, 5.2]. Die nötige Unabhängigkeit wird beispielsweise mittels diversitärer Redundanz realisiert [ISO26262-9, 5.2] und mittels „Analyse abhängiger Fehler“ (dependent failure analysis) nachgewiesen [ISO26262-9, 5.4.3]. Die Regeln zur Durchführung der ASIL Dekomposition sind in Abbildung 2.7 dargestellt. Folgt ein geklammertes ASIL auf ein ASIL, so indiziert das geklammerte ASIL die ASIL Einstufung des zugehörigen Sicherheitsziels.

Werden einem Element unterschiedliche ASIL bzw. ASIL und nicht-ASIL zugewiesen, gilt, dass das Element nach dem höchsten zugewiesenen ASIL entwickelt werden muss. Kann mittels „Analyse der Koexistenz von Elementen“ (analysis of the coexistence of

elements) nachgewiesen werden, dass die Funktionen mit niedrigerem ASIL/ nicht-ASIL keine Auswirkungen auf eine Funktion mit höherem ASIL haben (freedom from interference), kann jede Funktion des Elements nach dem zugewiesenen ASIL / nicht-ASIL entwickelt werden. Eine Entwicklung nach dem höchsten zugewiesenen ASIL entfällt in diesem Fall. Die Freiheit von Rückwirkungen (freedom from interference) ist hierbei dadurch sichergestellt, dass nachgewiesen wird, dass keine kaskadierten Fehler auftreten können [ISO26262-9, 6.2].

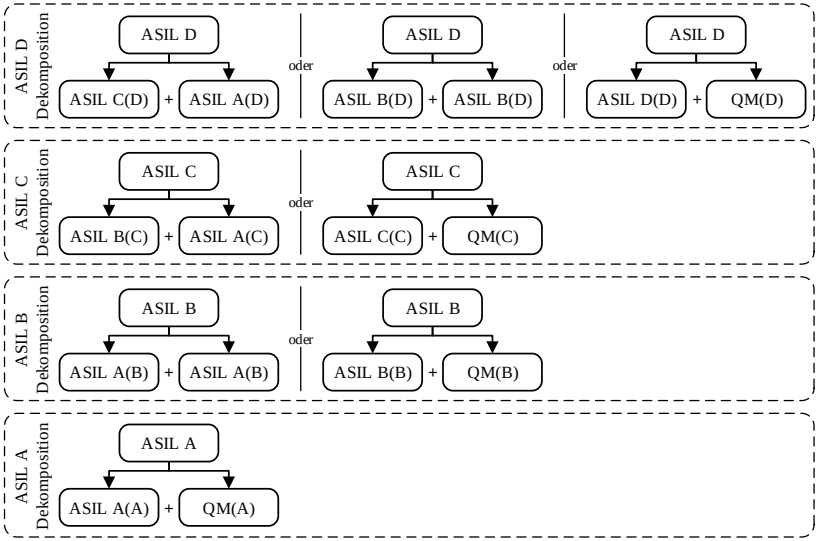


Abbildung 2.7:ASIL Dekompositionsregeln nach [ISO 26262-9, Figure 2]

2.3.1.2 ASIL Dekomposition – Stand der Forschung

Bei komplexen Systemen ist eine händische Ermittlung geeigneter Lösungsvektoren nicht effizient möglich. In der Literatur existieren Methoden zur automatisierten ASIL Dekomposition basierend auf Minimalschnitten, siehe [DHO14], [MAD12], [PAR13], [AZE14], [MUR15], [MIT05] und [GHE15]. [DHO14] nutzt lineare Gleichungssysteme zur automatisierten ASIL Dekomposition. Dieser Ansatz funktioniert bei einfachen Systemen, bei denen keine Abhängigkeiten zwischen den Elementen der Minimalschnitte

berücksichtigt werden. Abhängigkeiten zeigen sich in den Minimalschnitten dadurch, dass mindestens ein Element in mehreren disjunkten Teilen eines Minimalschnitts vorkommt. Bei komplexen Systemen ist das Vorkommen mehrerer Elemente in unterschiedlichen disjunkten Teilen eines Minimalschnitts unausweichlich. [MAD12], [PAR13], [AZE14], [MUR15], [GHE15] nutzen Algorithmen basierend auf Kostenfunktionen. Diese Informationen liegen in frühen Entwicklungsphasen im Normalfall nicht vor. Ungenaue Kenntnisse von Kosten führen zu Einschränkungen bei der Ableitung der ASIL an die Komponentenfunktionen und führen ggfs. zu fehlleitenden Optimierungsanreizen.
In [MIT05] wird ein zufallsbasierter Las Vegas Algorithmus eingesetzt. Dieser ist ebenfalls in der Lage alle existierenden Lösungen zu identifizieren [MIT05]. Unter einem Las Vegas Algorithmus wird dabei ein Monte Carlo basierter Algorithmus verstanden, dessen Ergebnis überprüft werden kann [BAB79].

2.3.1.3 Sicherheitsnachweis (verification)

Ziel des Sicherheitsnachweises ist die Vermeidung systematischer und zufälliger Hardware-Fehler [ISO26262-4, 6.4.4]. Zum Nachweis der Einhaltung der Sicherheitsziele hinsichtlich zufälliger Hardware-Fehler werden Metriken nach ISO 26262 berechnet. Die Berechnung der Metriken ist dabei für ASIL C und D obligatorisch, für ASIL B empfohlen [ISO26262-5, 9.4.2.1] [ISO26262-5, 8.4.1]. Nach [ISO26262] werden die in Abbildung 2.8 beschriebenen Fehler unterschieden.
Für die Berechnung der Metriken sind folgende Fehler relevant:

- Single point faults - SPF: Ein SPF ist ein „Fehler eines Elementes, der nicht durch einen Sicherheitsmechanismus abgedeckt ist und alleine zur Verletzung des Sicherheitsziels führt“ [ISO26262-1, 3.156]
- Residual fault - RF: Ein RF ist “der Anteil eines Fehlers, der nicht durch einen Sicherheitsmechanismus abgedeckt ist und zur Verletzung des Sicherheitsziels führt” [ISO26262-1, 3.125]
- Multiple point faults: - MPF: Ein MPF ist ein “einzelner Fehler, der in Kombination mit einem anderen, unabhängigen Fehler zur Verletzung des Sicherheitsziels führt” [ISO26262-1:1.77, 3.97] Es werden latente (MPF_{latent}) und erkannte ($MPF_{detected}$) MPF unterschieden. MPF_{latent} liegen unerkannt vor und führen bei Eintritt eines

bestimmten, weiteren, unabhängigen Fehlers zur Verletzung des Sicherheitsziels. Beim erkannten $MPF_{detected}$ führt der Eintritt eines bestimmten, weiteren, unabhängigen Fehlers, z.B. während der Fehlerreaktion, zur Verletzung des Sicherheitsziels. Dual point faults (DPFs) stellen eine Untermenge der MPFs dar.

- Gesamtfehlerrate der sicherheitsrelevanten Hardwareelemente $SR - gesamt$: Als Bezug für die Berechnung der Metriken wird die Gesamtheit der sicherheitsrelevanten Hardware-Fehler des Items berücksichtigt [ISO26262-5, C.2.2]. Dazu werden alle Basisfehlerraten von Hardware-Bauteilen, die in Komponenten verbaut sind, die zur Verletzung des betrachteten Sicherheitsziels beitragen können, addiert. Unter Basisfehlerraten versteht man dabei die vollständige Fehlerrate, die einem Hardware-Bauteil zugewiesen werden kann, d.h. vor der Anwendung einer Fehlerverteilung.

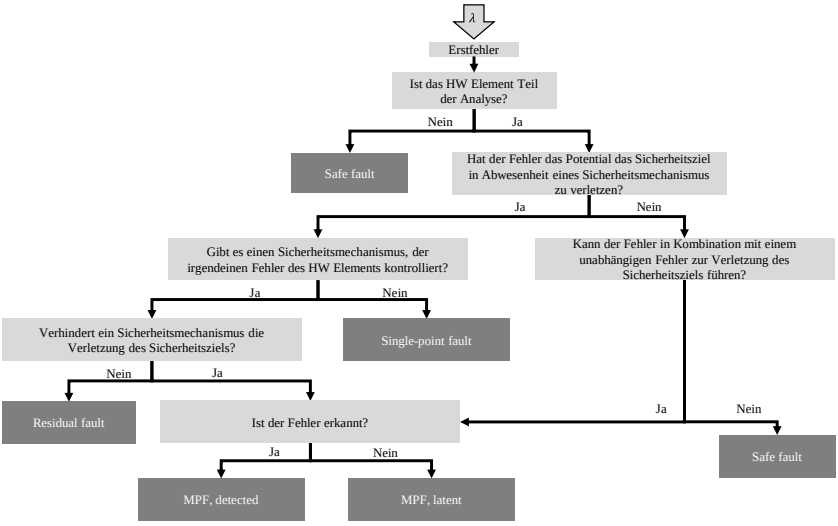


Abbildung 2.8: Fehlereinteilung nach [ISO26262-5, Annex B]

Die „probabilistic metric for random hardware failures“ (PMHF) bewertet, ob das verbleibende Risiko der Verletzung des Sicherheitsziels aufgrund von single point faults, residual faults und multiple point faults ausreichend gering ist [ISO26262-5, 9.2]. In der

Analyse werden zufällige Hardwarefehler sowie Sicherheitsmechanismen berücksichtigt [ISO26262-5, 9.2]. Definiert ist die PMHF als „Mittlere Wahrscheinlichkeit pro Stunde über der betrieblichen Nutzungsdauer des Items“ [ISO26262-5, 9.4.2.1]. Die Berechnung der PMHF ist abhängig vom zu analysierenden System. Für eine Sollfunktion, die von einem Sicherheitsmechanismus überwacht wird, wird die PMHF nach Formel (2.1) berechnet. Dabei wird die Expositionsdauer der Fehler berücksichtigt [ISO26262-10, 8.3.2.2].

$$PMHF = \lambda_{m,RF} + \lambda_{m,DPF} \cdot 0{,}5 \cdot (\lambda_{sm,DPF,latent} \cdot t_{life} + \lambda_{sm,DPF,detected} \cdot \tau_{sm}) \quad (2.1)$$

$\lambda_{m,RF}$	Fehlerrate der Residual Faults der Sollfunktion
$\lambda_{m,DPF}$	Fehlerrate der Dual Point Faults der Sollfunktion
t_{life}	Fahrzeug-Lebensdauer
$\lambda_{sm,DPF,latent}$	Fehlerrate der Latenten Dual Point Faults des Sicherheitsmechanismus
$\lambda_{sm,DPF,detected}$	Fehlerrate der Erkannten Dual Point Faults des Sicherheitsmechanismus
τ_{sm}	Multiple point fault detection intervall des Sicherheitsmechanismus

Um die Einhaltung der Sicherheitsziele zu gewährleisten wird der so errechnete Wert der PMHF mit dem Zielwert des Sicherheitsziels verglichen.

Der Zielwert kann nach ISO 26262 auf unterschiedliche Weisen ermittelt werden.

- Nach Tabelle 2.2
- Aus Felddaten ähnlicher, bewährter Design Richtlinien
- Mittels quantitativer Analysetechniken, die auf ähnliche, bewährte Design Richtlinien angewendet und nach anerkannten Industrienormen bedatet werden [ISO26262-5, 9.4.2.2] (z.B. [SN29500], [IECTR62380], [MIL-HDBK217F]) [ISO26262-5, 8.4.3])

Tabelle 2.2: Zielwerte der PMHF

ASIL	Zielwerte der zufälligen Hardwarefehler
D	$< 10^{-8} \frac{1}{h}$
C	$< 10^{-7} \frac{1}{h}$
B	$< 10^{-7} \frac{1}{h}$

Die „single point fault metric“ (SPFM) und die „latent fault metric“ (LFM) dienen der Bewertung der Wirksamkeit der Architektur des Items im Umgang mit zufälligen Hardwarefehlern [ISO26262-5, 8.2].

Die SPFM macht Aussagen über die “Widerstandsfähigkeit des Items gegen single point faults und residual faults entweder durch Behandlung mittels Sicherheitsmechanismus oder per Design” [ISO26262-5, C.2.1]. Zur Berechnung der SPFM wird die Summe der Fehlerraten der single point faults λ_{SPF} und der residual faults λ_{RF} durch die Summe der Fehlerrate aller sicherheitsrelevanten Hardwareelemente $\lambda_{SR-gesamt}$ geteilt und von eins abgezogen, wie in Gleichung (2.2) beschrieben.

$$SPFM = 1 - \frac{\sum \lambda_{SPF} + \lambda_{RF}}{\sum \lambda_{SR-gesamt}} \tag{2.2}$$

Um die Einhaltung der Sicherheitsziele zu gewährleisten wird der so errechnete Wert der SPFM mit dem Zielwert des Sicherheitsziels verglichen, siehe Tabelle 2.3.

Tabelle 2.3: Zielwerte der SPFM nach [ISO26262-5, Table 4]

	ASIL B	ASIL C	ASIL D
SPFM	≥ 90 %	≥ 97 %	≥ 99 %

Die LFM macht Aussagen über die "Widerstandsfähigkeit des Item gegen Latentfehler entweder durch Behandlung mittels Sicherheitsmechanismus oder durch Erkennung von Fehlern durch den Fahrer bevor diese das Sicherheitsziel verletzen können oder per Design" [ISO26262-5, C.3.1].
Zur Berechnung der LFM wird die Summe der Fehlerraten der Latentfehler $\lambda_{MPF-latent}$ durch die Summe der Fehlerrate aller sicherheitsrelevanten Hardwareelemente $\lambda_{SR-gesamt}$ abzüglich der Summe der Fehlerraten der single point faults λ_{SPF} und der residual faults λ_{RF} geteilt und von eins abgezogen, wie in Gleichung (2.3) beschrieben.

$$LFM = 1 - \frac{\sum \lambda_{MPF_{latent}}}{\sum(\lambda_{SR-gesamt} - \lambda_{SPF} - \lambda_{RF})} \tag{2.3}$$

Um die Einhaltung der Sicherheitsziele zu gewährleisten wird der so errechnete Wert der LFM mit dem Zielwert des Sicherheitsziels verglichen, siehe Tabelle 2.4.

Tabelle 2.4: Zielwerte der LFM nach [ISO26262-5, Table 5]

	ASIL B	ASIL C	ASIL D
LFM	≥ 60 %	≥ 80 %	≥ 90 %

2.3.2 Grundlagen der Methoden der Zuverlässigkeitstechnik und der funktionalen Sicherheit nach ISO 26262

Die Methoden zur probabilistischen Bewertung von Systemen, die in der Zuverlässigkeitstechnik und in der ISO 26262 eingesetzt werden, sind nahezu dieselben. Die FMEDA der ISO 26262 stellt eine Weiterentwicklung der FMEA, die auch in der Zuverlässigkeitstechnik zum Einsatz kommt, dar. Die Fehlerbaumanalyse, Markov-Analyse und Petri-Netze können in beiden Disziplinen eingesetzt werden. Die FMEDA sowie die Fehlerbaumanalyse, die auf der Booleschen Algebra basiert, sind in der ISO 26262 beschriebene Standardmethoden. Dabei werden induktive und deduktive Methoden unterschieden. Induktive Methoden, wie z.B. die FMEDA, betrachten die Fehlerursachen und deren Auswirkung auf das System („bottom-up“). Deduktive Methoden, wie z.B. die Fehlerbaumanalyse betrachten die Fehlerfolge auf das System und untersuchen, welche Fehlerursache dazu führt („top-down“) [BER04].

Anhand der in Kapitel 2.3.1.3 eingeführten Fehlerklassifizierungen der ISO 26262 (SPF, RF, DPF) werden die Grundlagen der Methoden erläutert, siehe Tabelle 2.5 und Abbildung 2.9 bis Abbildung 2.11. Dabei werden drei Komponenten K1, K2 und K3 betrachtet. Die Komponente K1 besitzt zwei Fehlermodi F1 und F2. F1 stellt einen single point fault (SPF) dar. Auf F2 wirkt ein Sicherheitsmechanismus SM2 mit dem Diagnosedeckungsgrad DC2. Der unerkannte Anteil des F2 ist damit ein residual fault (RF). Komponente K2 besitzt Fehlermodus F3 und Komponente K3 Fehlermodus F4. F3 und F4 führen lediglich in Kombination zur Verletzung des Sicherheitsziels und können damit den dual point faults (DPFs) zugewiesen werden.

Die eingeführten Methoden werden in Kapitel 3.3 hinsichtlich deren Eignung zur Modellierung fehlertoleranter Systeme bewertet.

2.3.2.1 FMEDA

Grundlage der FMEDA stellt die FMEA dar. Bei der FMEA werden Fehler durch Expertenschätzungen bewertet, wodurch eine Reproduzierbarkeit und Vergleichbarkeit nicht gegeben ist [BER04]. Die FMEA beschränkt sich dabei auf die Analyse von Einfachfehlern [DINEN16602-30-02]. Die FMEDA wird zur Bewertung der Funktionalen Sicherheit eingesetzt. Im Gegensatz zur FMEA wird bei der FMEDA die Ermittlung der Risikoprioritätszahl durch die Quantifizierung aller Fehler eines Systems ersetzt. Zusätzlich werden Sicherheitsmechanismen und deren zugehörigen Diagnosedeckungsgrade, sowie Mehrfachfehler berücksichtigt.

Bei der FMEDA handelt es sich um eine induktive Methode. Für die Analyse einer Hardware-Komponente werden im ersten Schritt deren Hardwarebauteile in die FMEDA übertragen. Die zugehörigen Fehlerraten der Hardwarebauteile werden bestimmt. Es wird analysiert, ob die Bauteile für die Sicherheitsanalyse relevant sind, und die Fehlermodi inklusive der zugehörigen Verteilung je Bauteil bestimmt. Im nächsten Schritt wird definiert, ob es sich bei den Fehlern um SPF oder RF bzw. MPF_{latent} handelt. Für die jeweiligen Fehler wird der zugehörige Diagnosedeckungsgrad bestimmt und eingetragen. Im letzten Schritt werden die Fehlerraten der residaul faults (λ_{RF}), der single point faults (λ_{SPF}) und der multiple point faults latent ($\lambda_{MPF-latent}$) berechnet [GOL12]. Auf Basis der Fehlerraten können die ISO 26262 Metriken nach Gleichung (2.1) berechnet werden, siehe Kapitel 2.3.1.3. Die FMEDA des in Kapitel 2.3.2 eingeführten Beispiels ist in Tabelle 2.5 dargestellt.

Tabelle 2.5: FMEDA des in Kapitel 2.3.2 eingeführten Beispiels

K3	K2	K1		Komponentenname
λ_3	λ_2	λ_1		Fehlerrate [FIT]
ja	ja	ja		Sicherheitsrelevanter Fehler?
F4	F3	F2	F1	Fehlermodi
100	100	40	60	Verteilung der Fehlerraten [%]
nein	nein	ja	ja	Hat der Fehlermode das Potential das Sicherheitsziel bei nicht vorhandenem Sicherheitsmechanismus zu verletzen?
-	-	SM2	-	Sicherheitsmechanismus
-	-	DC2	-	Erkennungswahrscheinlichkeit des Fehlermode
-	-	$\lambda_1 \cdot 0{,}4 \cdot (1 - DC2)$	$\lambda_1 \cdot 0{,}6$	Fehlerrate [FIT] des Residual λ_{RF} oder Single-Point Fault λ_{SPF}
ja	ja	-	-	Verletzung des Sicherheitsziels in Kombination mit einem Fehler einer unabhängigen Komponente?
-	-	-	-	Sicherheitsmechanismen zur Vermeidung des Fehlers
-	-	-	-	Erkennungswahrscheinlichkeit des Fehlermode
λ_3	λ_2	-	-	Fehlerrate des latenten Mehrfachfehlers $\lambda_{MPF-latent}$ [FIT]

2.3.2.2 Fehlerbaumanalyse

Die Fehlerbaumanalyse (FTA, engl.: Fault Tree Analysis) hat das Ziel alle Einflüsse und Ereignisse in einem System oder einer Komponente, die allein oder in Kombination zu einem definierten Top-Ereignis führen, zu ermitteln [DIN61025].

Sie eignet sich neben Zuverlässigkeits- auch für Sicherheitsanalysen und verfolgt dabei einen deduktiven Ansatz, der vom Top-Ereignis ausgeht und anschließend dessen Ursachen ermittelt [MEY03]. Durch logische Verknüpfung von Ereignissen und Einflüssen mittels sogenannten „Gates“, wird das betrachtete System realitätsnah abgebildet. Die Verkettung der Fehlerbaumelemente wird dabei in der klassischen FTA hauptsächlich durch logische UND- und ODER-Verknüpfungen realisiert. Die nicht weiter unterteilten Elemente der untersten Ebene werden als Events bezeichnet. Weitere Verknüpfungselemente und Beispiele für Fehlerbaummodellierungen sind unter anderem zu finden in [BER04] [DIN25424-1].

Fehlerbäume können sowohl für qualitative als auch für quantitative Analysen eingesetzt werden. Bei einer qualitativen Analyse ist ein Ziel die Darstellung von kritischen Ereignissen und Ereigniskombinationen [BER04]. Dabei werden die Minimalschnitte eines Fehlerbaums analysiert, um auf diese Weise Ursachen unerwünschter Ereignisse, wie z.B. Schwächen im Design, beispielsweise durch Common Cause Effekte aufzudecken. Ein Minimalschnitt ist so definiert, dass es zum Systemausfall kommt, wenn alle Elemente eines Minimalschnittes ausfallen, während alle sonstigen Komponenten intakt sind. Ein Schnitt ist nur dann minimal, wenn kein weiterer Schnitt in ihm enthalten ist [DIN 25424-2]. Ein Common Cause Effekt ergibt sich z.B., wenn in redundanten Pfaden dasselbe Event vorkommt und alleine zum Ausfall beider Pfade führt. Common Cause Effekte sind bei komplexen Systemen aufgrund dessen Umfang nicht einfach zu erkennen. Die Events, die aufgrund Common Cause zum Top-Event führen, treten in den Minimalschnitten erster Ordnung auf und können auf diese Weise identifiziert werden.

Die Basis zur Analyse von Minimalschnitten wurde in [FUS72] gelegt. Eine mögliche Umsetzung der Minimalschnitt-Aufstellung kann nach [RAU03] oder [VER10] erfolgen. In Abbildung 2.9 ist dazu der Fehlerbaum des in Kapitel 2.3.2 eingeführten Beispiels dargestellt. Die Minimalschnitte werden nach Gleichungen (2.4)…(2.7) ermittelt.

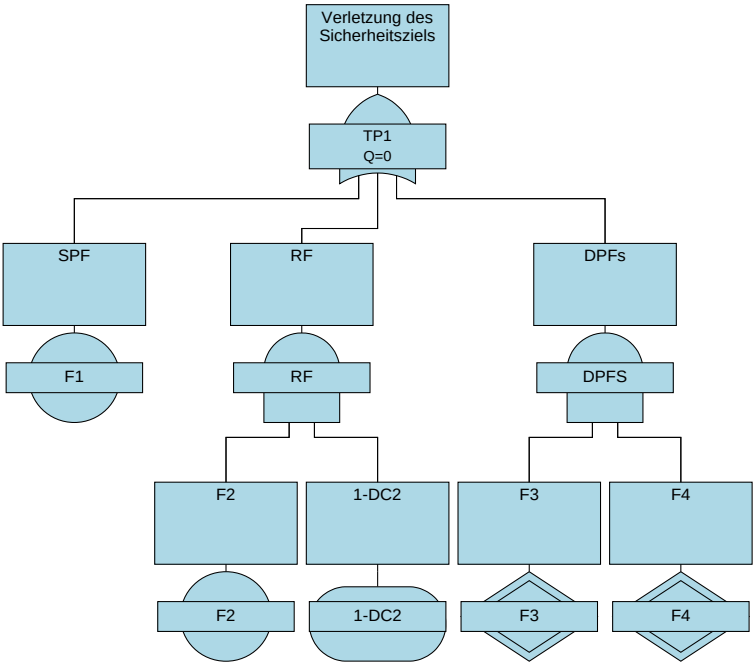


Abbildung 2.9: Fehlerbaum des in Kapitel 2.3.2 eingeführten Beispiels

1. Aufstellen der logischen Verknüpfungen der Elemente

$$TP1 = F1 \vee RF \vee DPFs \quad (2.4)$$

$$RF = F2 \wedge (1 - DC2) \quad (2.5)$$

$$DPFs = F3 \wedge F4 \quad (2.6)$$

2. Bottom-up Kombination der logischen Verknüpfungen

$$TP1 = F1 \vee (F2 \wedge (1 - DC2)) \vee (F3 \wedge F4) \quad (2.7)$$

3. Anwendung Boolescher Vereinfachungen und Umformungen (falls notwendig)

   In diesem Fall keine Vereinfachungen / Umformungen sinnvoll

Bei der quantitativen Analyse wird jedem Fehlerbaumevent die zugehörige Ausfallwahrscheinlichkeit zugeordnet. Durch die Übersetzung der Booleschen Algebra in Wahrscheinlichkeiten lassen sich die Eintrittswahrscheinlichkeiten der Fehlerbaum-Gates ermitteln [DIN61025]. Diese Art der Systemanalyse lässt Einschätzungen bezüglich der Systemzuverlässigkeit und Systemsicherheit zu [DIN25424-1].

Die boolesche Algebra dient dazu, ein System und dessen Verhalten zu beschreiben. Dies wird durch Aussagen über den Zustand von Systemkomponenten und deren logische Verknüpfungen realisiert. Auf diese Weise erhält man ein vereinfachtes System. Die Modellbildung mittels boolescher Algebra bringt die Einschränkungen mit, dass nur die Zustände „funktioniert“ und „ausgefallen“ betrachtet werden können. Außerdem dürfen sich die Zustände nicht beeinflussen und die Modellierung von Zeit- oder Reihenfolgenabhängigkeiten ist nicht möglich. Die Anwendung ist primär für Systeme, die nicht reparierbar sind, geeignet [DIN61078] [BER04]. Die Regeln, auf welchen die boolesche Algebra basiert, sind in Tabelle 2.6 dargestellt.

Tabelle 2.6: Regeln der Booleschen Algebra nach [WIT13] und [MEI11]

Kommutativgesetz	$x \wedge y = y \wedge x$	Absorption	$x \wedge (y \vee x) = x$
	$x \vee y = y \vee x$		$x \vee (y \wedge x) = x$
Idempotenz	$x \wedge x = x$	Doppelte Komplementbildung	$\overline{\overline{x}} = x$
	$x \vee x = x$		
Assoziativgesetz	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$	Beziehungen mit 0 und 1	$x \wedge 1 = x$
	$x \vee (y \vee z) = (x \vee y) \vee z$		$x \vee 0 = 0$
Distributivgesetz	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$		$x \vee 1 = 1$
	$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$		$x \wedge 0 = 0$
De Morgansche Regeln	$\overline{x \vee y} = \overline{x} \wedge \overline{y}$	Komplementen	$x \wedge \overline{x} = 0$
	$\overline{x \wedge y} = \overline{x} \vee \overline{y}$		$x \vee \overline{x} = 1$

Die Transformation der Booleschen Algebra in Wahrscheinlichkeiten kann bei einfachen Systemen, bei denen jedes Fehlerbaum-Element nur einmal vorkommt (kein Common Cause / Common Mode Effekte) nach den Regeln aus Tabelle 2.7 durchgeführt werden.

Tabelle 2.7: Berechnung der Ausfallwahrscheinlichkeit einfacher Systeme [BER04]

	Oder-Verknüpfung	Und-Verknüpfung
Boolesche Funktion	$y = \bigvee_{i=1}^{n} x_i$	$y = \bigwedge_{i=1}^{n} x_i$
System-Ausfall-wahrscheinlichkeit	$F_S(t) = 1 - \prod_{i=1}^{n}(1 - F_i(t))$	$F_S(t) = \prod_{i=1}^{n} F_i(t)$

Um fehlertolerante Systeme realitätsnah mittels Fehlerbaumanalysen abbilden zu können, müssen u.a. Reihenfolgeeffekte abgebildet werden. Dazu werden dynamische Fehlerbäume eingesetzt, bei denen die klassische Fehlerbaumanalyse durch Einsatz von Temporallogik oder Markov-Modelle erweitert wird [EDL15].

2.3.2.3 Markov-Analyse

Bei der Markov-Analyse handelt es sich um eine induktive Methode. Zeitkontinuierliche Markov-Ketten sind dadurch definiert, dass Übergänge zwischen den Markov-Zuständen durch konstante Übergangsraten definiert sind [CHI13]. Für die Analyse der funktionalen Sicherheit sind die zeitkontinuierlichen Markov-Ketten von Bedeutung, da zufällige Hardware-Fehler durch Fehlerraten quantifiziert werden (siehe Kapitel 2.3.1).

Stochastische Prozesse bieten die Möglichkeit, auch solche Vorgänge zu betrachten, die nicht streng determinierbar sind, also eine oder mehrere Zufallsvariablen besitzen. Der Prozess besteht dabei aus einer Menge an Zufallsvariablen $Z(t)$. Diese Menge wird auch als Zustandsraum ($M = Z_1, Z_2, \dots Z_m$) bezeichnet. Die Variablen sind vom Parameter t abhängig, dieser durchläuft den Parameterraum T. Bei den im Rahmen dieser Arbeit betrachteten Modellen ist t ein Parameter für die Zeit. Damit stellt der Verlauf der Zufallsvariablen den Verlauf der Zustände des stochastischen Prozesses dar $\{Z(t), t \in T\}$.

Markov-Prozesse sind durch folgende Bedingungen definiert:

- Markovsche Zustandsbedingung

  Der Übergang von einem Zustand Z_i in einen anderen Zustand Z_j hängt nur vom ausgehenden Zustand Z_i ab und nicht von weiter davorliegenden Zuständen. Aufgrund dieser Bedingungen werden Markov-Prozesse auch als gedächtnislose Prozesse bezeichnet.
- Markovsche Zeitbedingung

  Der Zustandsübergang ist für Markov Ketten erster Ordnung im Zeitintervall $(t, t + dt)$ ausschließlich von t und nicht von weiter davorliegenden Zeitpunkten abhängig [MEY03].

Sind die Übergangsraten zwischen den Markov-Zuständen konstant über der Zeit, handelt es sich um homogene Markov-Ketten [MEY03]. Homogene Markov-Ketten können zur Analyse der funktionalen Sicherheit nach ISO 26262 eingesetzt werden, da bei der Sicherheitsanalyse, wie in Kapitel 2.3.1 beschrieben, nur konstante Fehlerraten berücksichtigt werden.

Durch Verwendung der homogenen Markov Analyse können folgende Effekte zusätzlich zu den Methoden basierend auf Boolescher Algebra abgebildet werden:

- Reihenfolgeneffekte
- Abbildung unterschiedlicher Zustände neben „funktionsfähig“ und „ausgefallen“
- Abhängigkeiten zwischen Zuständen [DIN61165]
- Unterschiedliche Verweildauern in Zuständen [ABE08]

Zur Berechnung der Zustandswahrscheinlichkeiten wird ein homogenes lineares Differentialgleichungssystem aufgestellt, dessen Lösung die Zustandswahrscheinlichkeit nach vorgegebener Zeitdauer ist. Das Differentialgleichungssystem lässt sich mit den gängigen mathematischen Methoden berechnen [MEY03].

Bei zunehmender Systemgröße kommt das Markov-Verfahren an seine Grenzen, da mit steigender Elementzahl die Anzahl an Kombinationen und damit abzubildender Zustände überproportional ansteigt. Es kommt zu der sogenannten Zustandsraumexplosion und das System ist mittels Markov-Analyse nicht mehr lösbar [DIN EN 61165].

Abbildung 2.10 zeigt das Zustandsübergangsdiagramm eines redundanten Systems bestehend aus zwei Elementen. Das Zustandsübergangsdiagramm lässt sich nach [DIN61165] und [BER04] mittels Differentialgleichungssystem und dem zu betrachtenden Zeitintervall t beschreiben, siehe Anhang A1). Die Lösung des Differentialgleichungssystems ergibt die Wahrscheinlichkeit der Zustände zum Ende des Betrachtungszeitraums.

In der Literatur gibt es unterschiedliche Ansätze, bei welchen Markov-Analysen eingesetzt werden, siehe [ABE08], [MAH00], [ZUO05], [DOM06], [BAZ12] und [SON16].

In [MAH00] wird die Kopplung von Fehlerbaumanalyen und Markov-Analysen vorgeschlagen. In unterschiedlichen Anwendungsfällen wird die Markov Analyse zur Modellierung fehlertoleranter Systeme, z.B. by-wire Systeme [MAH00], [ZUO05], [DOM06] und [ABE08] oder Motorantrieben [BAZ12] eingesetzt.

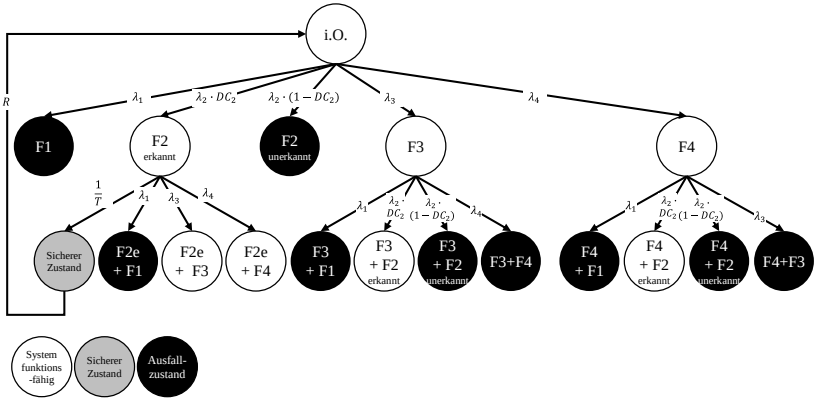


Abbildung 2.10: Markov Graph des in Kapitel 2.3.2 eingeführten Beispiels modelliert bis Zweitfehlerebene

2.3.2.4 Petri-Netze

Petri-Netze sind eine induktive Methode und dienen zur allgemeinen mathematischen Beschreibung der Beziehungen zwischen Bedingungen und Ereignissen [PET62]. Bei Petri-Netzen handelt es sich um eine zustandsorientierte Modellierungsmethode. Petri-Netze zählen zu den gerichteten Graphen und können mathematisch als 5-Tupel $PN = \{P, T, F, W, M_0\}$ beschrieben werden, bestehend aus:

- der Menge der Stellen $P = \{p_1, \dots p_n\}$ (oder Plätze, dargestellt durch Kreise), die Bedingungen, Voraussetzungen oder Zustände beschreiben
- der Transitionen $T = \{t_1, \dots t_n\}$ (dargestellt durch Rechtecke), die Ereignisse, Aktivitäten oder Regeln symbolisieren. Transitionen nach [PET62] sind deterministische Transitionen, die bei einer Aktivierung aller hinführenden Stellen nach einem bestimmten Zeitparameter schalten.
- Kanten $F \subseteq P \times T \cup T \times P$ (dargestellt durch Pfeile), die Stellen und Transitionen verbinden
- der Anzahl der Marken für jeden Pfeil $W: F \to \mathbb{N}$ und der Anzahl der Marken, die zu Beginn auf jeder Stelle liegen $M_0: P \to \mathbb{N}$ (dargestellt durch schwarze

Punkte), die die Modellierung dynamischer Effekte ermöglichen [HAA02], [AJM95], [COR04], [BAU97].

Marken werden von Transitionen aufgebraucht und erstellt, können aber nur auf Stellen verweilen. Der momentane Stand der Marken in den Plätzen innerhalb des Systems gibt den momentanen Systemzustand an. Die Dynamik entsteht durch das Feuern von Transitionen bei Erfüllung der Bedingungen. Durch das Feuern kommt es zu einem Platzwechsel der Marken nach den vorgegebenen Regeln [DIN EN 62551]. Aus dem Aufbau der Petri-Netz Struktur ergeben sich Restriktionen, die den Fluss der Marken bestimmen. Dieser Fluss stellt das dynamische Verhalten des Systems dar und folgt Schaltregeln, die im Voraus für das Netz festgelegt sind [VDI4008-4].

Für die Analyse der funktionalen Sicherheit und Zuverlässigkeit können stochastische Petri-Netze eingesetzt werden. Dabei werden die deterministischen Transitionen durch stochastische Transitionen ersetzt. Stochastische Transitionen ermitteln den Zeitparameter aus einer Schaltwahrscheinlichkeit beziehungsweise Wahrscheinlichkeitsverteilung [DIN EN 62551]. Generalisierte stochastische Petri-Netze werden durch Nulltransitionen ergänzt [AJM95]. Bei Nulltransitionen kommt es bei Aktivierung sofort zum Schalten der Transition [BAU02]. Erweiterte stochastische Petri-Netze ermöglichen die Berücksichtigung unterschiedlicher Verteilungen der Transitionen [SUG92].

Bei generalisierten stochastischen Petri-Netzen werden nur Exponentialverteilungen eingesetzt. Aufgrund dessen können diese mittels Markov-Analyse ausgewertet werden. Kommen beliebige Verteilungen zum Einsatz (Erweiterte stochastische Petri-Netze), werden Monte Carlo Simulationen zur Auswertung der Petri-Netze eingesetzt [DIN EN 62551]. Durch Monte Carlo Methoden werden Größen, deren Berechnung üblicherweise zu kompliziert für analytische Lösungsansätze ist, durch Nutzung von Zufallszahlen berechnet [BON13]. Beispielsweise werden numerische Probleme näherungsweise gelöst [WEI00]. Ein Beispiel eines stochastischen Petri-Netzes ist in Abbildung 2.11 dargestellt.

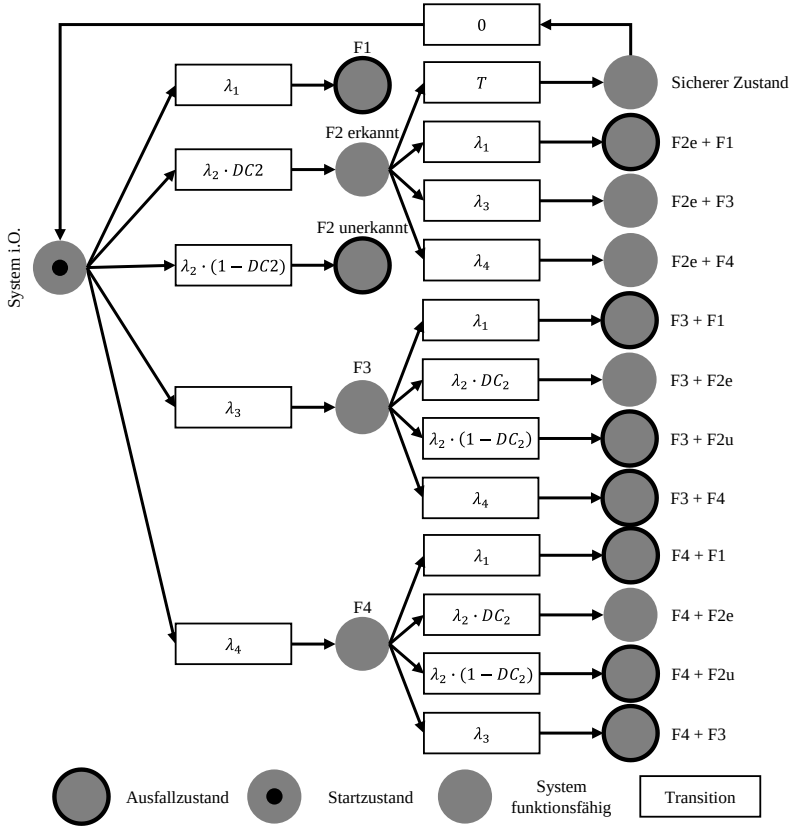


Abbildung 2.11: Petri-Netz des in Kapitel 2.3.2 eingeführten Beispiels modelliert bis Zweitfehlerebene

2.3.2.5 Vergleich der eingeführten Methoden

Anhand des in Kapitel 2.3.2 eingeführten Beispiels ergibt sich der Vergleich der Methoden nach Tabelle 2.8.

Tabelle 2.8: Tabellarischer Vergleich der Methoden anhand des in Kapitel 2.3.2 eingeführten Beispiels

	FMEDA	Fehlerbaum-analyse	Markov-Analyse	Petri-Netz
Induktiv / deduktiv	Induktiv	Deduktiv	Induktiv	Induktiv
Modellierungs-aufwand	4 Zeilen	3 Gates 5 Events	18 Zustände	18 Stellen

2.3.3 Abgrenzung Zuverlässigkeit und funktionale Sicherheit nach ISO 26262

In diesem Kapitel werden die funktionale Sicherheit nach ISO 26262 und die Zuverlässigkeit in tabellarischer Form gegenübergestellt, siehe Tabelle 2.9. Ein Vergleich hinsichtlich deren Fokus ist in Abbildung 2.12 dargestellt. Zusammengefasst lässt sich sagen, dass Ausfallraten der Zuverlässigkeit und der funktionalen Sicherheit nach ISO 26262 getrennt betrachtet werden müssen, da diese unterschiedliche Sachverhalte darstellen und nicht miteinander korrelieren. ISO 26262 Kenngrößen dürfen nicht als Feldprognose missverstanden werden.

Tabelle 2.9: Gegenüberstellung funktionaler Sicherheit und Zuverlässigkeit

	Funktionale Sicherheit (nach ISO 26262)	Zuverlässigkeit
Definition	"Abwesenheit unangemessener Risiken aufgrund von Gefährdungen, die durch unbeabsichtigtes Verhalten von E/E-Systemen verursacht werden" [ISO 26262-1, 3.67]	„Wahrscheinlichkeit dafür, dass ein Produkt während einer definierten Zeitdauer und unter gegebenen Funktions- und Umgebungsbedingungen *nicht ausfällt*" [VDI4001-2]

Fokus	Die ISO 26262 berücksichtigt systematische Fehler und zufällige Hardwarefehler von E/E Systemen [ISO26262-1, Introduction]. Bei der Analyse der zufälligen Hardwarefehler werden nur konstante Fehlerraten [ISO26262-1, 3.53] d.h. exponential verteilte Fehler berücksichtigt, siehe Abbildung 2.12.	Zuverlässigkeitsanalysen sind nicht auf E/E-Systeme beschränkt. Mittels Zuverlässigkeitsanalysen können unterschiedliche Verteilungen, wie z.B. Weibull-, Exponential- oder Logarithmische Verteilungen abgebildet werden. Die Art der Verteilung ist abhängig vom Ausfallverhalten des zu analysierenden Produktes. Ziel ist es das Ausfallverhalten mittels Verteilung möglichst realitätsnah abzubilden [BER04]. Frühausfälle, Zufallsausfälle, sowie Verschleißausfälle werden dabei berücksichtigt [HOR15], siehe Abbildung 2.12.
Ziel	Vermeidung eines unangemessenen Restrisikos definiert durch die Erreichung eines ausreichenden und akzeptablen Maßes an Sicherheit [ISO26262-1, Introduction], um dadurch Gefährdung von Mensch und Umwelt auszuschließen	Funktionsfähigkeit des Systems sicherstellen [BER04]
Anspruch	Für die Analyse der zufälligen Hardwarefehler gilt: “Die quantitativen Zielwerte haben keine absolute Bedeutung und sind nur dafür gedacht neue Designs mit existierenden zu vergleichen. Auf diese Weise werden Gestaltungsrichtlinien und der Nachweis, dass das Design die Sicherheitsziele erfüllt, zur Verfügung gestellt“ [ISO26262-5, 9.4.2.2] (relative Größen)	Prognose des Ausfallverhaltens im Feld unter Berücksichtigung von Materialermüdung und Verschleiß [BER09] (absolute Größe)

Zielgrößen	Die Zielgrößen zur Bewertung der zufälligen Hardwarefehler sind die ISO 26262 Metriken: $PMHF = f(\lambda_{RF}, \lambda_{SPF}, \lambda_{MPF})$ $SPFM = f(\lambda_{RF}, \lambda_{SPF}, \lambda_{SR-gesamt})$ $LFM = f(\lambda_{RF}, \lambda_{SPF}, \lambda_{MPF}, \lambda_{SR-gesamt})$ Genauere Beschreibung in Kapitel 2.3.1	Ausfallrate im Feld $\lambda(t)$ $\lambda(t) = f(\text{Belastung}, \text{Belastbarkeit})$

Um Systeme mit hoher Kundenzufriedenheit zu entwickeln, ist neben der Betrachtung der funktionalen Sicherheit die Betrachtung der Zuverlässigkeit notwendig. Systeme, die lediglich nach der funktionalen Sicherheit entwickelt werden, könnten andernfalls häufig den Übergang in den sicheren Zustand anstreben, um bei nichtzuverlässiger Funktion eine Gefährdung für Mensch und Umwelt zu vermeiden. Die Folge sind z.B. „Liegenbleiber“, die es zu vermeiden gilt.

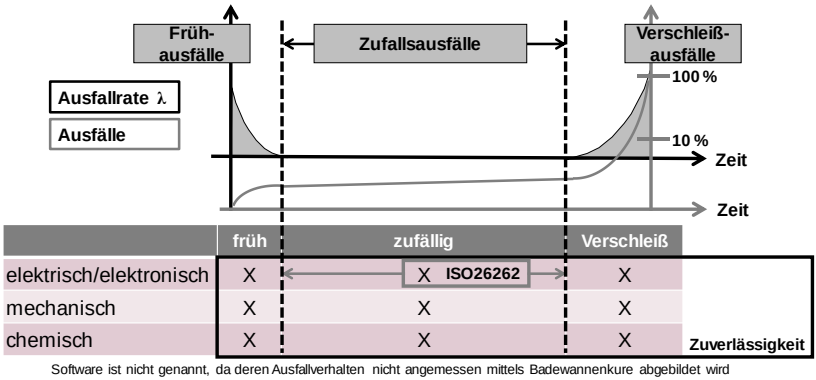


Abbildung 2.12: Funktionale Sicherheit und Zuverlässigkeit [HOR15]

3 Methodenauswahl zur Sicherheitsbewertung fehlertoleranter Systeme

Im ersten Teil des Kapitels werden die Anforderungen an das Energiebordnetz durch das automatisierte Fahren analysiert, um die zusätzlichen Anforderungen zur Bewertung von fehlertoleranten Systemen zu identifizieren. Im zweiten Schritt werden die Ziele der Methode sowie die zu modellierenden Eigenschaften zum Nachweis der funktionalen Sicherheit fehlertoleranter Systeme ermittelt. Auf Basis der ersten beiden Kapitel wird in den Forschungsfragen die Abgrenzung zu bestehender Literatur durchgeführt und bisher ungelöste Fragenstellungen bei der Betrachtung fehlertoleranter Systeme abgeleitet. Im letzten Teil des Kapitels wird eine Bewertung der vorgestellten Methoden zur Analyse der funktionalen Sicherheit fehlertoleranter Systeme durchgeführt.

3.1 Anforderungen an das Energiebordnetz für automatisiertes Fahren

In Tabelle 3.1 sind die Auswirkungen der Automatisierungsstufen auf das Energiebordnetz beschrieben. Dabei wird ein Energiebordnetz zur Realisierung der Energieversorgung bis einschließlich Automatisierungsstufe zwei einem Energiebordnetz zur Realisierung der Energieversorgung von Automatisierungsstufe drei und höher gegenübergestellt.

Tabelle 3.1: Bedeutung des Energiebordnetzes für Automatisierungsstufen kleiner gleich zwei und größer gleich drei

	Bis Automatisierungsstufe 2	Ab Automatisierungsstufe 3
Energie-versorgung sicherheits-relevanter Funktionen	Kraft des Fahrers, verstärkt durch elektrische oder durch den Antriebsmotor betriebene Unter-stützungssysteme (z.B. Servo-lenkung, Bremskraftverstärkung)	Im automatisierten Fahrbetrieb rein elektrisch, da Fahrer nicht im Regelkreis
Rückfall-szenario im Fehlerfall	Fehler wird dem Fahrer gemeldet / durch den Fahrer erkannt; Fahrzeug ist so entwickelt, dass der Fahrer das Fahrzeug durch Muskelkraft kontrollieren und in den sicheren Zustand bringen kann	Fehler wird durch das Fahrzeug erkannt; Fahrzeug muss den sicheren Zustand (z.B. Übergabe des Fahrzeugs an den Fahrer innerhalb einer definierten Zeitspanne) selbstständig erreichen
Verhalten im Fehlerfall	Komponenten müssen so gestaltet sein, dass deren Fehler möglichst keinen Einfluss auf das System haben (fail-safe) [FEL11]	Fehlertoleranz notwendig, da Übergang in den sicheren Zustand unter Verwendung der Energie des Energiebordnetzes gewährleistet werden muss (fail-operational) siehe z.B. [PIE15]
Bordnetz-relevanz	Mittel bis hoch, abhängig vom Fahrzeug, einige Fahrzeuge sind ohne elektrische Unterstützung nicht kontrollierbar (ins-besondere für schwere Fahrzeuge der oberen Fahrzeugklasse)	Sehr hoch, da der Fahrer das Fahrzeug nicht mehr dauerhaft überwacht; ab Level 4 entfällt der Fahrer als Rückfallebene

Im Normalbetrieb von Fahrzeugen mit Automatisierungsstufe drei oder höher werden alle sicherheitsrelevanten Systeme, die zur Realisierung der automatisierten Fahrfunktionen nötig sind, durch das Energiebordnetz mit Energie versorgt. Dieser Zusammenhang ist in Abbildung 3.1 dargestellt. Kommt es im Energiebordnetz zu einem Fehler, so muss dieser erkannt und der Übergang in den sicheren Zustand umgesetzt werden. Für den Übergang in den sicheren Zustand muss eine Mindestanzahl an sicherheitsrelevanten Verbrauchern auch im Fehlerfall mit Energie versorgt werden. Dazu ist eine Fehlertoleranz im Energiebordnetz unerlässlich.

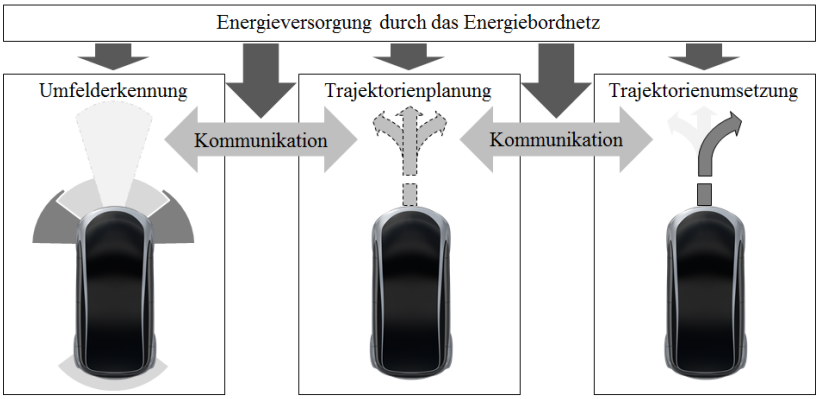
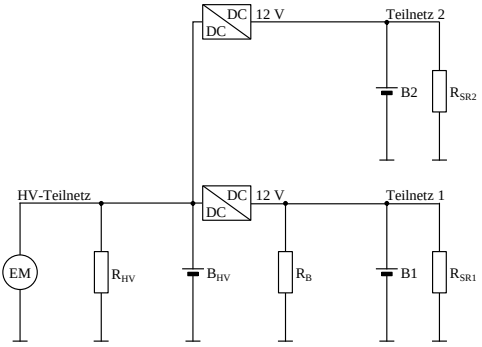


Abbildung 3.1: Bedeutung des Energiebordnetzes für Fahrzeuge mit Automatisierungsstufe drei oder höher

Am Beispiel Bremssystem werden die Auswirkungen unterschiedlicher Automatisierungsstufen auf das Energiebordnetz beschrieben. Bei Fahrzeugen mit Automatisierungsstufe zwei oder niedriger gibt es Fahrerassistenzsysteme wie den Abstandsregelautomat (engl. Adaptive Cruise Control - ACC) [WIN15], die das Fahrzeug bei zu geringem Abstand zum vorausfahrenden Fahrzeug selbsttätig verzögern. Der Fahrer muss das Assistenzsystem dauerhaft überwachen. Fällt das Assistenzsystem beispielsweise aufgrund eines Fehlers in der elektrischen Energieversorgung eines elektrischen aktuierten Bremssystem aus, kann der Fahrer das Fahrzeug notfalls mittels mechanischer Rückfallebene den gesetzlichen Vorgaben entsprechend mit einer

Mindestverzögerung verzögern. Bei Fahrzeugen mit Automatisierungsstufe drei oder höher steht der Fahrer nicht mehr als sofortige Rückfallebene zur Verfügung. Kommt es zum Fehler in der Energieversorgung des Bremssystems, fällt das Bremssystem aus. Im Fehlerfall muss das Fahrzeug jedoch in der Lage sein, den sicheren Zustand einzunehmen. Aufgrund dessen wird die Energieversorgung der Bremsfunktion redundant und ausreichend unabhängig ausgeführt.

Ein Beispielenergiebordnetz, das zur Realisierung von automatisiertem Fahren größer gleich Automatisierungsstufe drei eingesetzt werden kann, ist in Abbildung 3.2 dargestellt. Dieses besteht aus einem Hochvolt-Teilnetz, das eine elektrische Maschine (EM), Hochvolt-Verbraucher (R_{HV}) und eine Hochvolt-Batterie (B_{HV}) enthält. Am Hochvolt-Teilnetz sind mittels Gleichspannungswandlern jeweils 12V-Teilnetz 1 und 12V-Teilnetz 2 angeschlossen. Teilnetz 1 besteht dabei aus einer Batterie B1, den nicht sicherheitsrelevanten Verbrauchern R_B und den Verbrauchern mit sicherheitsrelevanten Funktionen R_{SR1}. Teilnetz 2 umfasst eine Batterie B2 und bei den Verbrauchern, die redundant vorgesehen werden müssen, eine funktionell redundante Ausführung der Verbraucher mit sicherheitsrelevanten Funktionen R_{SR2}.



B1/2	Batterie 1/2	B_{HV}	Hochvolt-Batterie
EM	Elektrische Maschine	R_B	Nicht-sicherheitsrelevante Verbraucher
R_{HV}	Hochvolt-Verbraucher	$R_{SR1/2}$	Sicherheitsrelevante Verbraucher 1 / 2

Abbildung 3.2: Beispiel eines fehlertoleranten HV-12V-Energiebordnetzes für Automatisierungsstufe drei oder höher [AUG16]

3.2 Methode zum Nachweis der funktionalen Sicherheit fehlertoleranter Systeme

Nach dem V-Modell der ISO 26262 muss ein Nachweis zur Einhaltung der funktionalen Sicherheit durchgeführt werden, siehe Abbildung 3.3. Methoden und Vorgehensweisen der ISO26262 bilden die Eigenschaften eines fehlertoleranten Systems nicht vollständig ab. Aus diesem Grund werden in Kapitel 3.2.1 die Ziele definiert, welche zum Nachweis der funktionalen Sicherheit erreicht werden müssen. In Kapitel 3.2.2 werden die Eigenschaften des fehlertoleranten Systems zur Auswahl einer geeigneter Methoden beschrieben.

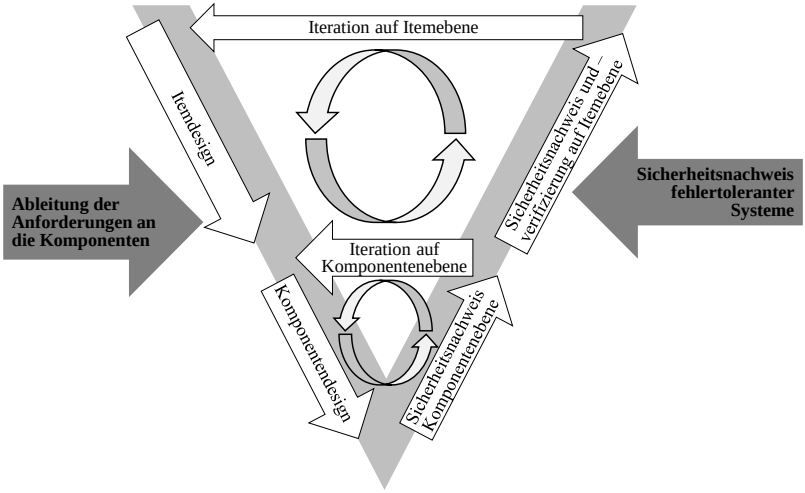


Abbildung 3.3: Einordnung der Ableitung der ASIL an die Elemente eines Systems und des Sicherheitsnachweises eines Systems im V-Modell nach [ISO26262]

3.2.1 Ziele des Nachweises der funktionalen Sicherheit fehlertoleranter Systeme

Um einen effiziente, ISO 26262 konformen Sicherheitsnachweis fehlertoleranter Systeme durchführen zu können, müssen die in Tabelle 3.2 beschriebenen Ziele erreicht werden.

Tabelle 3.2: Ziele einer effizienten Analyse der funktionalen Sicherheit fehlertoleranter Systeme

	Ziel	Nr.	Beschreibung
ISO 26262 Anforderung	Vermeidung systematischer Fehler	Z1	Neben der Berechnung der ISO 26262 Metriken wird die Vermeidung systematischer Fehler von der ISO 26262 gefordert [ISO 26262-4, 6.4.4].
Notwendigkeit aus Effizienzgründen	Automatisierte Modellbildung, Analyse und Ermittlung der Fehler-auswirkungen	Z2	Um die Komplexität des Systems effizient handhaben zu können, muss das Modell automatisiert auf Basis der Fehler-auswirkungen aufgebaut werden können. Die Fehleraus-wirkungen müssen dabei reproduzierbar ermittelt werden.
ISO 26262 Anforderung	Berechnung der ISO 26262 Metriken	Z3	Die ISO 26262 fordert die Berechnung der probabilistic metric for random hardware failures (PMHF), der single point fault metric (SPFM), sowie der latent fault metric (LFM) [ISO 26262-5, 9.2, 8.4.5, 8.4.6]. Für die Berechnung der Metriken müssen die sicherheitsrelevanten Fehler bestimmt und quantifiziert werden. Zusätzlich müssen die Fehlerauswirkungen identifiziert und ein passendes Systemmodell erstellt werden.
Unterstützung bei der Erreichung der Zielwerte	Ermittlung der einflussreichsten Parameter	Z4	Für den Fall, dass das System das ISO 26262 Ziel „das Restrisiko, das aufgrund von zufälligen Hardware Fehlern zur Verletzung des Sicherheitsziels führt, ausreichend gering“ [ISO 26262-5, 9.1] ist, nicht erreicht, müssen Maßnahmen für die Vermeidung oder Kontrollierbarkeit der Fehler getroffen werden. Um die bestmöglichen Maßnahmen im Rahmen einer effizienten Optimierung ableiten zu können, sollen die Parameter, welche die Zielgrößen am meisten beeinflussen, identifiziert werden.

3.2.2 Eigenschaften zur Bewertung fehlertoleranter Systeme als Basis der Methodenauswahl

Die Eigenschaften fehlertoleranter Systeme, die mit der auszuwählenden Methode analysiert werden müssen, sind in Tabelle 3.3 beschrieben. Die Eigenschaften dienen als Grundlage für die Auswahl einer geeigneten Methode zur Analyse der funktionalen Sicherheit fehlertoleranter Systeme. Für jede Eigenschaft ist ein Beispiel im Kontext eines fehlertoleranten Energiebordnetzes zugeordnet.

Tabelle 3.3: Eigenschaften fehlertoleranter Systeme zur Analyse der funktionalen Sicherheit ergänzt um Beispiele im Kontext fehlertolerantes Energiebordnetz

Zusammenfassung	Nr.	Beschreibung	
Berücksichtigung zufällig verteilter Fehler	E1	Die ISO 26262 schreibt die Berücksichtigung zufälliger Hardware Fehler vor [ISO 26262-5, 9.2]. Aus diesem Grund muss die Methode in der Lage sein, zufällig verteilte Fehler mit zeitlich konstanten Fehlerraten (Exponentialverteilung) zu berücksichtigen [ISO 26262-1, 3.53]. Alterungseffekte, die üblicherweise mit einer Weibullverteilung modelliert werden, sind nicht Teil der Betrachtungen nach ISO 26262.	
		Beispiel	Für die Analyse des Komponentenfehlers „Generator liefert dauerhafte maximale Leistung“ werden die Hardware Fehler der Bauteile des Generators analysiert. Für die Quantifizierung der Fehler können z.B. die Siemens Norm [SN29500] oder die [IEC TR 62380] in Kombination mit den Fehlerverteilungen nach [BIR14] genutzt werden. Da Alterungseffekte in der ISO 26262 nicht berücksichtigt werden, wird von zeitinvarianten Ausfallraten während der Betriebsdauer ausgegangen. Die konstante Ausfallrate wird in Abhängigkeiten von Applikationsfaktoren z.B. nach [SN29500] ermittelt.

<table>
<tr><td rowspan="3">Berechnungen mit niedrigen Fehlerraten</td><td rowspan="3">E2</td><td colspan="2">Auf Bauteilebene (z.B. Transistoren, Kondensatoren, …) sind Fehlerraten im Bereich weniger FIT üblich, siehe z.B. [SN29500]. Die logischen Verknüpfungen einer Vielzahl an Bauteilfehlern zu Komponentenfehlern führen zu höheren Fehlerraten auf Komponentenebene. Abhängig vom Systemdesign sind auf Systemebene sehr niedrige Fehlerraten zum Erreichen der Sicherheitsziele notwendig. Zur Verringerung der Fehlerraten auf Komponenten- und Systemebene werden Sicherheitsmechanismen zur Verringerung der sicherheitsrelevanten Fehlerrate eingeführt. Abhängig vom Design sind folglich auch niedrige Fehlerraten auf höheren Systemebenen möglich. Die eingesetzte Methode muss in der Lage sein, das Ausfallverhalten eines Systems mit niedriger sicherheitsrelevanter Fehlerrate mathematisch korrekt zu beschreiben.</td></tr>
<tr><td>Beispiel</td><td>Auf Bauteilebene wird z.B. der Fehler eines Kondensators mit 1 FIT (Fehler in 10^9h) bewertet. Da mehrere Kondensatorfehler zu dem Komponentenfehler “Generator liefert dauerhaft maximale Leistung” beitragen, wird eine Fehlerrate in der Größenordnung von 1000 FIT erreicht. Aufgrund dessen müssen Sicherheitsmaßnahmen eingeführt werden, um eine ASIL D Energieversorgung, deren Grenzwert bei 10 FIT liegt [ISO 26262-5, Table 6], zu erreichen.</td></tr>
<tr><td rowspan="2">Abbildung unterschiedlicher Komponenten-zustände</td><td rowspan="2">E3</td><td colspan="2">Für die Analyse redundanter Systeme müssen unterschiedliche Fehlerbilder der Komponenten analysiert werden.</td></tr>
<tr><td>Beispiel</td><td>Neben den Zuständen “funktioniert” und “ausgefallen” kann der Generator z.B. “degradieren” oder „dauerhaft Maximalleistung liefern“.</td></tr>
</table>

Abbildung von Abhängigkeiten zwischen Fehlern	E4	Fehler von Bauteilen einer Komponente können Teil unterschiedlicher Fehler einer Komponente sein. Diese Abhängigkeiten zwischen den Komponentenfehlern müssen mittels ausgewählter Methode abgebildet werden können.	
		Beispiel	Beim Ausfall und der Degradierung des Generators sind teilweise dieselben Komponenten beteiligt.
Berücksichtigung von Diagnose-deckungsgraden	E5	Diagnosedeckungsgrade zwischen 0% und 100% müssen mittels Methode berücksichtigt werden [ISO 26262-5, 9.4.2.4].	
		Beispiel	Die Degradation des Generators kann beispielsweise mit einem Diagnosedeckungsgrad von 60% erkannt werden.
Berücksichtigung unterschiedlicher Verweildauern in Zuständen	E6	Auf Fahrzeugebene ist die Fehlerreaktion der Übergang in den sicheren Zustand. Der Übergang in den sicheren Zustand kann sich je nach Fehler und Automatisierungsgrad in Manövern und Dauer unterscheiden. Je länger der Übergang in den sicheren Zustand dauert, desto größer wird die Wahrscheinlichkeit für zusätzliche Fehler in diesem Zeitraum, welche durch die Methode analysiert werden müssen.	
		Beispiel	Eine beispielhafte Fehlerreaktion auf einen erkannten Fehler “Generator liefert dauerhaft maximale Leistung”, der zu einer Überspannung führt, ist das Verzögern des Fahrzeugs bis zum Fahrzeugstillstand innerhalb von 30 Sekunden. Für den ausgefallenen Generator ist das Anhalten auf dem Standstreifen als möglicher sicherer Zustand definiert. Die Dauer des Übergangs wird beispielsweise auf 120 Sekunden festgelegt. Die Batterie übernimmt für die festgelegte Dauer die Leistungs-/Energieversorgung der sicherheitsrelevanten Komponenten.

Analyse von Mehrfachfehlern	E7	Mehrfachfehler müssen bei der Analyse berücksichtigt werden. Die ISO 26262 fordert mindestens die Analyse der Zweifachfehlerebene. Mehrfachfehler höherer Ordnung müssen nur dann berücksichtigt werden, wenn sie einen spürbaren Einfluss auf die funktionale Sicherheit des Systems haben.[ISO 26262-5, 8.2]	
		Beispiel	Der Generator kann zuerst dauerhaft maximale Leistung liefern und dann ausfallen.
Abbildung von Reihenfolge-effekten	E8	Reihenfolgeeffekte müssen bei der Analyse berücksichtigt werden.	
		Beispiel	Der Generator kann zuerst dauerhaft maximale Leistung liefern, was zu einer Überspannung führt und dann ausfallen, was zu einer Unterspannung führt, aber nicht umgekehrt.
Analyse komplexer Systeme mit einer Vielzahl an Komponenten	E9	Komplexe Systeme mit einer großen Anzahl an Komponenten, wobei die Komponenten aus einer großen Anzahl an Bauteilen bestehen, müssen mit der Methode analysiert werden.	
		Beispiel	Ein redundantes Energiebordnetz besteht z.B. aus einem Generator, zwei Batterien, einem Koppelelement und einer Vielzahl an Verbrauchern. Der Generator selbst besteht aus einer Menge an Bauteilen, die bei der Sicherheitsanalyse berücksichtigt werden müssen.

3.3 Forschungsfragen

3.3.1 Ableitung der Sicherheitsanforderungen an fehlertolerante Systeme

Ein wichtiger Schritt bei der Entwicklung sicherheitsrelevanter E/E-Systeme ist die Ableitung der Sicherheitsanforderungen an die Elemente des Systems, siehe Abbildung 3.3

Wie in Kapitel 2.3.1 beschrieben umfassen die Sicherheitsanforderungen den zugehörigen sicheren Zustand, die Fehlertoleranzzeit, das Automotive Safety Integrity Level sowie die zulässigen Metriken. Aufgrund der Vielzahl an möglichen Varianten zur Zuordnung der ASIL liegt der Fokus nachfolgend auf der ASIL Ermittlung.
Folgende Nachteile ergeben sich bei den im Stand der Forschung existierenden Algorithmen, siehe Kapitel 2.3.1.2:

- Abhängigkeiten zwischen Minimalschnitten werden nicht berücksichtigt. Daher kann eine Anforderungsableitung für fehlertolerante Systeme nicht durchgeführt werden [DHO14]
- Mehrere Algorithmen basierend auf Kostenfunktionen. Diese Informationen liegen in frühen Entwicklungsphasen im Normalfall nicht vor. Ungenaue Kenntnisse von Kosten führen zu Einschränkungen bei der Ableitung der ASIL an die Komponentenfunktionen und führen ggfs. zu fehlleitenden Optimierungsanreizen [MAD12], [PAR13], [AZE14], [MUR15], [GHE15].
- Zufallsbasierte Algorithmen sind in der Lage alle existierenden Lösungen zu identifizieren [MIT05]. Im aktuellen Stand der Forschung existiert jedoch keine mathematische Herleitung, wie für komplexe Systeme die Anzahl möglicher Lösungen ermittelt werden kann. Dadurch kann die Vollständigkeit der Möglichkeiten bei zufallsbasierten Algorithmen aktuell nicht sichergestellt werden. Des Weiteren kann die Dauer der Ermittlung der Möglichkeiten bei komplexen Systemen und damit mit einer Vielzahl an Minimalschnitten aufgrund der zugrundeliegenden Monte Carlo Simulationen sehr viel Zeit in Anspruch nehmen (siehe Kapitel 4.1.3).

Folgende Aufgabenstellungen zur ASIL Allokation werden im Rahmen dieser Arbeit adressiert:

- Mathematische Ermittlung der Anzahl gültiger Lösungskombinationen der ASIL Allokation (Kapitel 4.1.1)
- Definition eines Algorithmus zur vollständigen und effizienten Ermittlung aller gültigen Lösungskombinationen der ASIL Allokation (Kapitel 4.1.2)
- Nachweise der Funktionsfähigkeit des definierten Algorithmus (Kapitel 4.1.3)

3.3.2 Nachweis der funktionalen Sicherheit fehlertoleranter Systeme

In Kapitel 3.2 werden die Anforderungen an die Methode zur Durchführung des Sicherheitsnachweises für fehlertolerante Systeme identifiziert. Die in Kapitel 2.3.2 beschriebenen Methoden sind dabei nicht in der Lage alle an den Sicherheitsnachweis fehlertoleranter Systeme nach ISO 26262 gestellten Anforderungen zu erfüllen.
Beispielsweise ist nicht beschrieben, wie durch die vorgestellten Methoden systematische Fehler vermieden werden können (Z1). Des Weiteren wird nicht gezeigt, wie eine Vollständigkeit, Reproduzierbarkeit und Automatisierbarkeit der Analysen durchgeführt werden kann (Z2).
Ziel der Arbeit ist es daher, eine gesamtheitlichen Methode zur Erfüllung der Ziele und Eigenschaften aus Kapitel 3.2.1 und 3.2.2 zu erarbeiten. Dabei gilt es die Vor- und Nachteile der Berechnungsmethoden aus Kapitel 2.3.2 zu bewerten (Kapitel 3.4) und die ausgewählte Berechnungsmethode in eine gesamtheitliche Methode zur Bewertung fehlertoleranter Systeme zu integrieren (Kapitel 4.2.1).

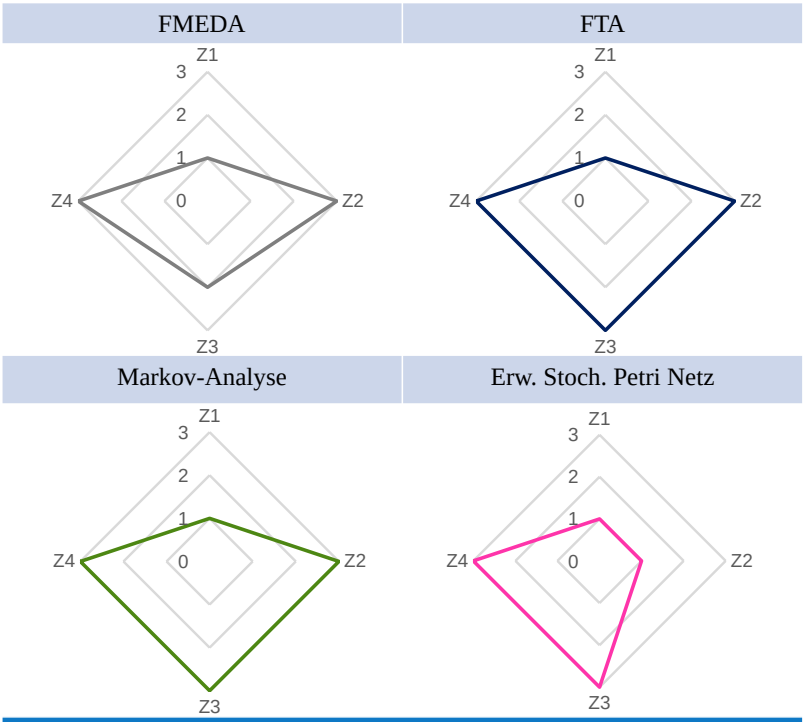
3.4 Bewertung der Methoden zur Analyse der funktionalen Sicherheit fehlertoleranter Systeme

Eine ausführliche Bewertung der Methoden FMEDA, Fehlerbaumanalyse, Markov und erweiterte stochastische Petri-Netz hinsichtlich der genannten Ziele der Analyse der funktionalen Sicherheit (siehe Kapitel 3.2.1) und Eigenschaften der Methoden zur Analyse fehlertoleranter System (siehe Kapitel 3.2.2) ist im Anhang in Kapitel A1) dargestellt.
In Abbildung 3.4 ist die Erreichung der in Tabelle 3.2 beschriebenen Ziele zur Analyse der funktionalen Sicherheit nach ISO 26262 durch die betrachteten Methoden gegenübergestellt. Systematische Fehler (Z1) können während des gesamten Entwicklungs- und Produktionsprozesses auftreten. Systematische Fehler werden durch die ISO26262 vorgegebenen Entwicklungsprozesse und Teststrategien erkannt und behoben. Simulationen können dabei unterstützen und z.B. fehlerhafte Dimensionierungen aufdecken, siehe Kapitel 4.2.2 Die Erfüllung dieses Ziels ist durch die

Methoden allein nicht möglich, ggfs. können diese jedoch einen Beitrag dazu leisten. Die verbleibenden Ziele zur Analyse der funktionalen Sicherheit Z2-Z4 werden sowohl durch die Fehlerbaumanalyse als auch die Markov Analyse erreicht. FMEDA und Petri Netze sind nicht in der Lage die Ziele vollumfänglich zu erreichen.

Die Erfüllung der Eigenschaften, welche die Methoden zur Abbildung fehlertoleranter Systeme erfüllen müssen (siehe Tabelle 3.3), sind für die betrachteten Methoden in Abbildung 3.4 gezeigt. FMEDA und klassische FTA sind nicht in der Lage die geforderten Eigenschaften vollumfänglich zu erfüllen. Petri Netze zeigen eine Schwäche beim Umgang mit kleinen Fehlerraten, welche bei der Berechnung der ISO26262-Metriken jedoch auftreten, da zur Lösung erweiterte stochastischer Petri-Netze simulative Experimente mittels Monte Carlo Simulationen durchgeführt werden. Bei niedrigen Fehlerraten muss eine Vielzahl an Experimenten durchgeführt werden, bis Konvergenz erreicht wird. Dies führt zu einer hohen Rechenzeit zur Lösung der Petri-Netze mit niedrigen Fehlerraten.

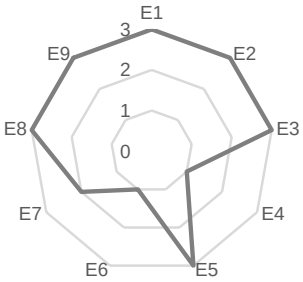
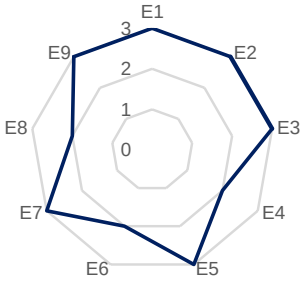
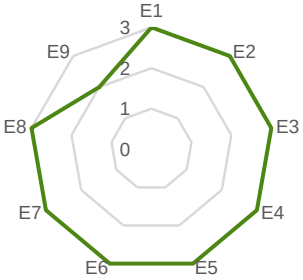
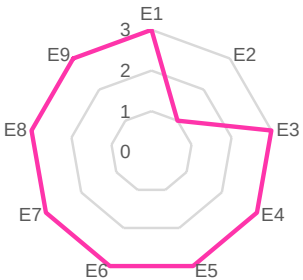
Die Markov Analyse hingegen ist in der Lage fehlertolerante Systeme abzubilden, weswegen sich in dieser Ausarbeitung die Markov-Analyse als geeignete Methode herausgestellt hat. Der Nachteil der Markov-Analyse, dass die Anzahl an Zuständen begrenzt werden muss, da es sonst zur Zustandsraumexplosion kommt, wird in Kapitel 4.2.1 näher betrachtet.



Skala							
0	-	1	Eigenschaft nicht erfüllt	2	Eigenschaft teilweise erfüllt	3	Eigenschaft vollständig erfüllt

Nr.	Ziel	Notwendigkeit
Z1	Vermeidung systematischer Fehler	ISO 26262 Anforderung
Z2	Automatisierte Modellbildung und Analyse basierend auf Fehlerauswirkungen	Effizienz
Z3	Berechnung der ISO 26262 Metriken	ISO 26262 Anforderung
Z4	Ermittlung der einflussreichsten Parameter	Unterstützung bei der Erreichung der Zielwerte

Abbildung 3.4: Gegenüberstellung der Methoden bezüglich ihrer Eignung zum Nachweis der funktionalen Sicherheit

FMEDA	FTA
	
Markov-Analyse	**Erw. Stoch. Petri Netz**
	

Skala							
0	-	1	Eigenschaft nicht erfüllt	2	Eigenschaft teilweise erfüllt	3	Eigenschaft vollständig erfüllt

Nr.	Eigenschaft	Nr.	Eigenschaft
E1	Berücksichtigung zufällig verteilter Fehler	E6	Berücksichtigung unterschiedlicher Verweildauern in Zuständen
E2	Berechnungen mit niedrigen Fehlerraten	E7	Analyse von Mehrfachfehlern
E3	Abbildung unterschiedlicher Komponentenzustände	E8	Abbildung von Reihenfolgeeffekten
E4	Abbildung von Abhängigkeiten zwischen Fehlern	E9	Analyse komplexer Systeme mit einer Vielzahl an Komponenten
E5	Berücksichtigung von Diagnosedeckungsgraden		

Abbildung 3.5: Gegenüberstellung der Methoden bezüglich ihrer Eignung zur Modellierung fehlertoleranter Systeme

4 Anforderungsableitung und Sicherheitsnachweis bei fehlertoleranten Systemen

Anhand des V-Modells der ISO 26262 (Grundlagen siehe Kapitel 2.3.1) wird die Vorgehensweise zur Ableitung der Anforderungen an die Komponenten eines fehlertoleranten Systems (Kapitel 4.1) sowie der Nachweis der funktionalen Sicherheit des fehlertoleranten Systems (Kapitel 4.2) vorgestellt, siehe Abbildung 4.1.

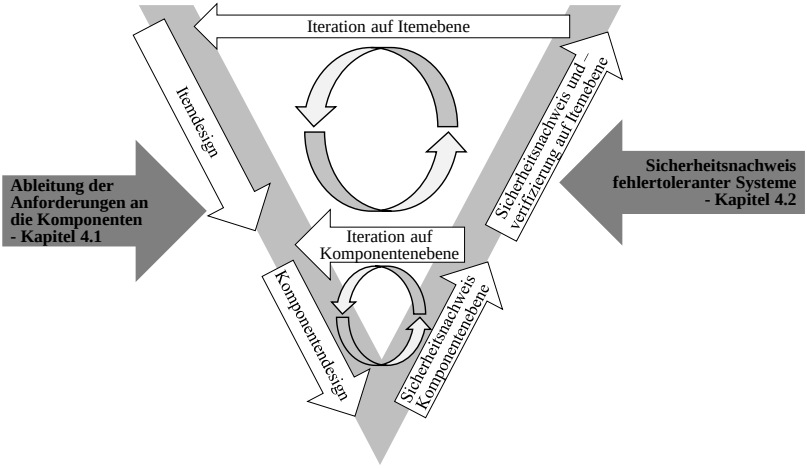


Abbildung 4.1: Einordnung der Arbeit in das V-Modell der [ISO26262]

4.1 Ableitung der Anforderungen von der Itemebene an die Komponentenebene

Im ersten Schritt des V-Modells wird das Item definiert. Unter dem Item versteht man „ein System oder eine Gruppe von Systemen, welche eingesetzt werden, um eine Funktion auf Fahrzeugebene umzusetzen und auf welche die ISO 26262 angewendet wird“ [ISO26262]. Im nächsten Schritt wird die Gefährdungsanalyse und

Risikobewertung durchgeführt. Dabei werden für das betrachtete Item die Sicherheitsziele und die zugehörigen Attribute ASIL, Fehlertoleranzzeiten, sichere Zustände und zulässige Metriken ermittelt. Im funktionalen Sicherheitskonzept wird für jedes Sicherheitsziel die vollständige Wirkkette, die zur Funktionserfüllung relevant ist, abgebildet. Dabei wird eine vorläufige Architekturannahme festgelegt, die zur Erfüllung der Sicherheitsziele geeignet scheint. Im nächsten Schritt werden die Anforderungen an das zu entwickelnde fehlertolerante System abgeleitet. Die Ergebnisse der beschriebenen Analysen werden für die weitere Betrachtung als gegeben vorausgesetzt. Auf Basis der vorherigen Analysen wird die zulässige Fehlerrate jedes Sicherheitsziels bis auf die einzelnen Komponentenfunktionen budgetiert. Die Fehlertoleranzzeiten sowie die sicheren Zustände werden ebenso auf die Komponentenebene heruntergebrochen.

Wie in Kapitel 2.3.1.1 beschrieben kann bei ausreichend unabhängiger, redundanter Ausführung einer Funktion die ASIL Dekomposition zur Reduzierung der ASIL angewendet werden. Die mathematische Beschreibung der ASIL Dekomposition (Kapitel 4.1.1), die Vorstellung eines Algorithmus zur automatisierten ASIL Dekomposition (Kapitel 4.1.2) sowie der Nachweis dessen Wirksamkeit (Kapitel 4.1.3) werden nun beschrieben.

4.1.1 Mathematische Beschreibung der ASIL Dekomposition

Die ASIL Dekomposition darf nur dann durchgeführt werden, wenn eine ausreichende Unabhängigkeit zwischen den Elementen, auf die dekomponiert werden soll, gegeben ist. Die Zuweisung der ASIL auf die Komponentenfunktionen basiert in dieser Analyse auf Minimalschnitten. Um die Minimalschnitte zu erhalten, werden die Systemzusammenhänge mittels Fehlerbaumanalyse abgebildet und die Minimalschnitte ermittelt. Die Minimalschnitte umfassen die Kombinationen der sicherheitsrelevanten Fehlfunktionen, die zur Verletzung des zu analysierenden Sicherheitsziels führen können. Für die ASIL Zuweisung werden die Minimalschnitte als mathematische Gleichung interpretiert. Jeder Minimalschnitt muss das ASIL des zugehörigen Sicherheitsziels erreichen, siehe Gleichung (4.1).

$$\begin{aligned} Minimalschnitt_1 &\geq \text{ASIL D} \\ &\vdots \\ Minimalschnitt_n &\geq \text{ASIL D} \end{aligned} \tag{4.1}$$

Jeder Minimalschnitt besteht dabei aus einer Anzahl n_E an sicherheitsrelevanten Fehlfunktionen der Komponentenebene, bezeichnet als $Event_n$. Alle Elemente eines Minimalschnittes sind dabei miteinander UND-verknüpft (∧). D.h. wenn alle Elemente eines Minimalschnittes eintreten, kommt es zur Verletzung des Sicherheitsziels. Dieser Zusammenhang ist in Gleichung (4.2) beschrieben.

$$Minimalschnitt_1 = Event_1 \wedge Event_2 \wedge \ldots \wedge Event_n \tag{4.2}$$

Die Anzahl an Möglichkeiten n_{ges}, wie die ASIL auf die Komponenten-Funktionen eines Minimalschnitts verteilt werden können, werden nachfolgend beschrieben. Die Anzahl an Möglichkeiten ist abhängig von der Anzahl an Elementen des Minimalschnitts n_E und dem ASIL des zu analysierenden Sicherheitsziels. Bei der Analyse werden nur Minimallösungen berücksichtigt. Eine Minimallösung ist eine Lösung, welche das ASIL des Sicherheitsziels erfüllt, aber durch keine Lösung mit niedrigeren ASIL ersetzt werden kann. Höhere ASIL Anforderungen als durch die Minimallösung gefordert sind immer möglich, führen jedoch zu einer Übererfüllung des ASIL des Sicherheitsziels. Aus diesem Grund werden diese bei der Analyse nicht betrachtet.

Für jeden Minimalschnitt wird ein Entscheidungsbaum nach Abbildung 4.2 aufgebaut. Das ASIL des Sicherheitsziels definiert die Anzahl der Möglichkeiten, die jedem Minimalschnittelement zugewiesen werden kann und demnach der Anzahl an Ästen, die jedem Knoten folgen. Wird ein ASIL B, wie in Abbildung 4.2 als ASIL des Sicherheitsziels angenommen, kann dem ersten Element QM, ASIL A oder ASIL B zugewiesen werden. Die Anzahl der Ebenen entspricht dabei der Anzahl an Elementen eines Minimalschnitts. Für das erste Element ergibt sich somit die erste Ebene mit den genannten Auswahlmöglichkeiten. Sind im Minimalschnitt zwei Elemente enthalten, wird der Entscheidungsbaum um eine Ebene erweitert. Wurde dem ersten Element QM zugewiesen, kann auch dem zweiten Element QM, ASIL A oder ASIL B zugeordnet

werden, wie am linken Knoten dargestellt. Wurde dem ersten Element bereits ein ASIL A zugewiesen, kann dem zweiten Element nur noch QM und ASIL A zugewiesen werden, da es sonst übererfüllt ist. Nach dem ASIL B des ersten Elements wird der Aufbau mit QM fortgeführt, da das ASIL des Sicherheitsziels mit dem ersten Element bereits erreicht ist.

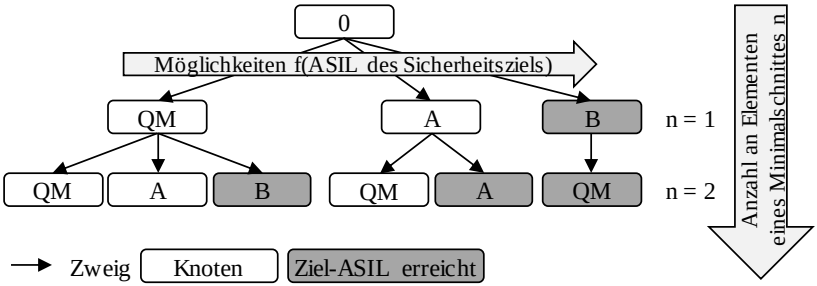


Abbildung 4.2: Beispiel eines Entscheidungsbaums eines Minimalschnittes, der ASIL B erreichen muss [MUE18]

In Abbildung 4.3 und Abbildung 4.4 werden Entscheidungsbäume für die unterschiedlichen ASIL aufgebaut. Die Anzahl neuer Lösungen je Ebene und damit je hinzukommender sicherheitsrelevanter Fehlfunktion werden mit einem schwarzen Punkt symbolisiert.

Wird der Minimalschnitt als QM eingestuft, so wird jedes Element des Minimalschnitts QM eingestuft. Unabhängig von der Anzahl an Elementen im Minimalschnitt n_E gibt es in diesem Fall genau eine Lösung, die die Anforderung erfüllt, siehe Abbildung 4.3, links. Bei ASIL A Anforderungen steigt die Anzahl an Möglichkeiten mit jedem neuen Element linear an, da jede sicherheitsrelevante Fehlfunktion mit ASIL A eingestuft werden kann, während alle anderen QM eingestuft werden, siehe Abbildung 4.3, rechts.

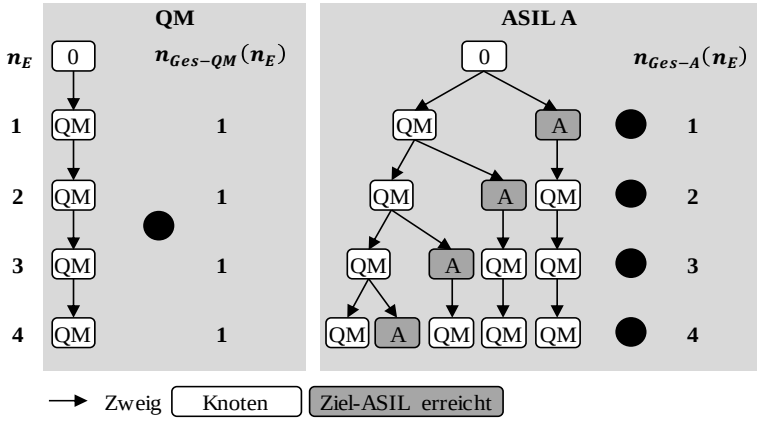


Abbildung 4.3: Anzahl Möglichkeiten n_{ges} zur ASIL Dekomposition in Abhängigkeit der Anzahl sicherheitsrelevanter Fehlfunktionen n_E für QM und ASIL

Für die Systeme, die größer als ASIL A eingestuft werden, ergibt sich die Anzahl an Möglichkeiten nach den figurierten Zahlen. Für ASIL B Systeme lässt sich die Anzahl an Möglichkeiten beispielsweise nach den Dreieckszahlen ermitteln, siehe Abbildung 4.4. Für ASIL C Systeme ist die Ermittlung nach den Tetraederzahlen (Anhang Abbildung A1, links) und für ASIL D Systeme nach den Pentatopzahlen (Anhang Abbildung A1, rechts) möglich.

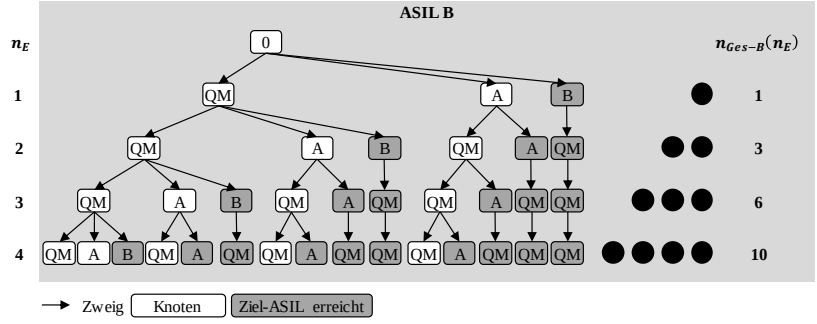


Abbildung 4.4: Anzahl Möglichkeiten n_{ges} zur ASIL Dekomposition in Abhängigkeit der Anzahl sicherheitsrelevanter Fehlfunktionen n_E für ASIL B

Die Anzahl an Möglichkeiten n_{ges} in Abhängigkeit der Anzahl an Elementen im Minimalschnitt n_E und des zu erreichenden ASILs sind in Tabelle 4.1 zusammengefasst.

Tabelle 4.1: Gleichungen für die Berechnung der Anzahl an möglichen Lösungsvektoren der ASIL Zuordnung in Abhängigkeit der Minimalschnitt-Elemente und dem ASIL des Sicherheitsziels; mathematische Beschreibung der Zahlenfolgen nach [CON96]

ASIL	**zugehörige Gleichung**	**#**	$n_E = 1$	$n_E = 2$	$n_E = 3$	$n_E = 4$	...
QM	$\binom{n}{0} = 1$	(4.3)	1	1	1	1	…
A	$\binom{n}{1} = n$	(4.4)	1	2	3	4	…
B	$\binom{n+1}{2} = \frac{n(n+1)}{2}$	(4.5)	1	3	6	10	…
C	$\binom{n+2}{3} = \frac{n(n+1)(n+2)}{6}$	(4.6)	1	4	10	20	…
D	$\binom{n+3}{4} = \frac{n(n+1)(n+2)(n+3)}{24}$	(4.7)	1	5	15	35	…

4.1.2 Algorithmische Realisierung der ASIL Zuweisung

In Kapitel 2.3.1.1 wurde die Notwendigkeit einer neuen Methode zur ASIL Zuweisung bei komplexen Systemen dargelegt. Der Ablauf des entwickelten Algorithmus ist in Abbildung 4.5 dargestellt. Die ASIL der Sicherheitsziele sind Eingangsparameter des Algorithmus. Um den Lösungsraum einzuschränken zu können müssen ASIL bestimmter Funktionen als Randbedingungen definiert werden. Die erste Möglichkeit, weswegen eine Randbedingung gesetzt werden kann, ist, dass eine bestimmte Komponentenfunktion bereits mit einem bestimmten ASIL entwickelt wurde. Folglich ist eine niedrigere ASIL Einstufung nicht sinnvoll. Für diesen Fall müssen alle ASIL, die unter dem bereits entwickelten ASIL liegen, nicht berücksichtigt werden. Ein weiterer Grund, warum Randbedingungen gesetzt werden können, ist das Wissen über Technologiegrenzen bestimmter Funktionen. Kann eine Funktion maximal mit ASIL B entwickelt werden, wohingegen für die Entwicklung der ASIL C oder ASIL D Fähigkeit neue Technologien

entwickelt werden müssen, kann das ASIL der Funktion nach oben begrenzt werden. Eine fixe ASIL Randbedingung ist dann sinnvoll, wenn z.B. eine Komponente nicht mit ASIL entwickelt werden kann.

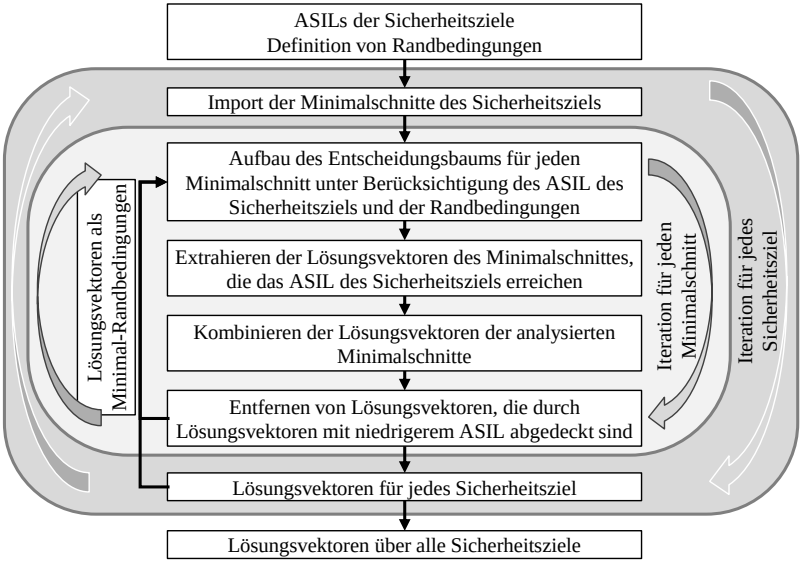


Abbildung 4.5: Entscheidungsbaumbasierter Algorithmus zur ASIL Zuweisung [MUE18]

Im Algorithmus berücksichtigte Effekte:

- Manuell definierte Randbedingungen (fixiert, minimal, maximal)
- Abhängigkeiten zwischen Minimalschnitten eines Sicherheitsziels
- Abhängigkeiten zwischen Minimalschnitten mehrerer Sicherheitsziele
- ASIL jedes Sicherheitsziels

Als Ergebnis erhält man die möglichen Lösungsvektoren über alle Sicherheitsziele, die entsprechend sortiert werden können, um den optimalen Lösungsvektor zu erhalten.

4.1.3 Nachweis der Funktionsfähigkeit und Vergleich des Algorithmus

Minimalschnitte, anhand welchen die Funktionsfähigkeit des Systems und ein Vergleich mit einem anderen Ansatz durchgeführt werden, sind in (4.8)…(4.10) dargestellt. ME steht dabei für Minimalschnittelement. Die Minimalschnittelemente einer Minimalschnittzeile werden dabei UND verknüpft (∧). Die Minimalschnittzeilen sind ODER verknüpft.

ME1∧ME2∧ME3∧ME4 (4.8)

ME1∧ME5∧ME6 (4.9)

ME1∧ME7 (4.10)

Es gibt eine bestimmte Anzahl an Möglichkeiten, wie die ASIL auf die sicherheitsrelevanten Fehlfunktionen verteilt werden können. Die Anzahl an Möglichkeiten kann auf Basis der Minimalschnitte nach den Gleichungen (4.3)…(4.7) durchgeführt werden.

In jeder Zeile der Minimalschnitte kommt das Element (ME1) vor. Alle anderen Elemente sind nur einmalig in den Minimalschnitten vorhanden. Das ASIL des ME1 hat demnach Einfluss auf die ASIL aller anderen Minimalschnittelemente. Wird für die Systemebene ein ASIL D angenommen, kann ME1 von QM(D) bis ASIL D(D) variieren. Die verbleibenden Elemente eines Minimalschnittes müssen ein entsprechendes ASIL besitzen, um in Kombination das ASIL D Sicherheitsziel zu erreichen.

Beispielhaft wird ME1 auf QM(D) gesetzt. Folglich müssen die verbleibenden Elemente jedes Minimalschnittes ASIL D(D) erfüllen. Die sich daraus ergebende Anzahl an Möglichkeiten wird in den Gleichungen (4.11)…(4.14) berechnet. Mittels Gleichung (4.11) wird die Anzahl der Möglichkeiten, die sich aus Minimalschnitt (4.8) (k_{1D}) mit drei unbestimmten Elementen $n_{1D} = 3$ ergeben, berechnet. Analog dazu aus Gleichung (4.12) die Anzahl an Möglichkeiten von Minimalschnitt (4.9) (k_{2D}) mit zwei unbestimmten Elementen $n_{2D} = 2$ und aus Gleichung (4.13) die Anzahl an Möglichkeiten von Minimalschnitt (4.10) (k_{3D}) mit einem unbestimmten Elemente $n_{3D} = 1$. Die Gesamtzahl

an Möglichkeiten (k_D) für die Zuweisung des QM(D) auf ME1 ergibt sich aus der Multiplikation der Möglichkeiten je Minimalschnitt ($k_{1D}…k_{3D}$) nach Gleichung (4.14).

$$k_{1D} = \frac{n_{1D}(n_{1D}+1)(n_{1D}+2)(n_{1D}+3)}{24} = \frac{3(3+1)(3+2)(3+3)}{24} = 15 \quad (4.11)$$

$$k_{2D} = \frac{n_{2D}(n_{2D}+1)(n_{2D}+2)(n_{2D}+3)}{24} = \frac{2(2+1)(2+2)(2+3)}{24} = 5 \quad (4.12)$$

$$k_{3D} = \frac{n_{3D}(n_{3D}+1)(n_{3D}+2)(n_{3D}+3)}{24} = \frac{1(1+1)(1+2)(1+3)}{24} = 1 \quad (4.13)$$

$$k_D = k_{1D} \cdot k_{2D} \cdot k_{3D} = 15 \cdot 5 \cdot 1 = 75 \quad (4.14)$$

Die analoge Berechnung der Anzahl an Möglichkeiten für ME1 mit ASIL A(D), B(D), C(D) und D(D) ist in Tabelle 4.2 mit den Gleichungen (4.15)…(4.18) dargestellt. Die Gesamtzahl der Lösungsmöglichkeiten für die Minimalschnitte aus (4.8)…(4.10) wird nach Gleichung (4.19) berechnet.

Tabelle 4.2: Anzahl an Kombinationsmöglichkeiten zur Erreichung eines ASIL D Sicherheitsziels für die Minimalschnitte (4.8)…(4.10)

ASIL des ME1	**ASIL des verbleibenden Minimalschnittteils**	**Anzahl an Möglichkeiten**	**Gleichung**
QM(D)	D(D)	$p_D = 15 \cdot 5 \cdot 1 = 75$	(4.14)
A(D)	C(D)	$p_C = 10 \cdot 4 \cdot 1 = 40$	(4.15)
B(D)	B(D)	$p_B = 6 \cdot 3 \cdot 1 = 18$	(4.16)
C(D)	A(D)	$p_A = 3 \cdot 2 \cdot 1 = 6$	(4.17)
D(D)	QM(D)	$p_{QM} = 1 \cdot 1 \cdot 1 = 1$	(4.18)
		$p_{sum} = p_D + p_C + p_B + p_A + p_{QM} = 140$	(4.19)

Der beschriebene entscheidungsbaumbasierte Algorithmus ist in der Lage, alle existierenden Lösungen zu finden. Die Anzahl der gefundenen Lösungen ist in Abbildung 4.6 über der Zeit aufgetragen.

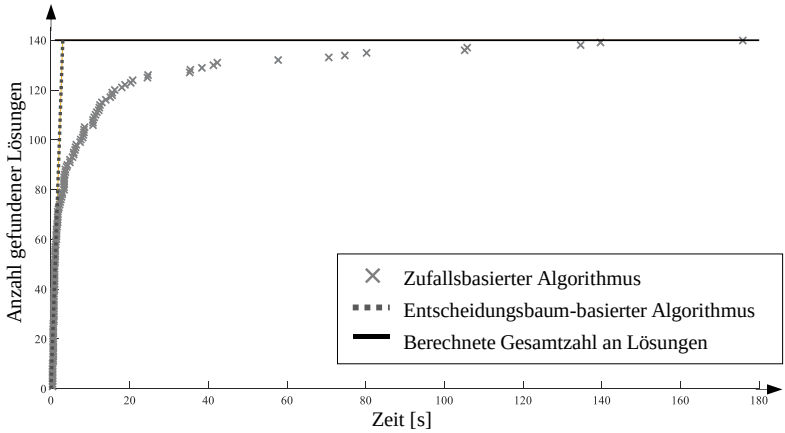


Abbildung 4.6: Anzahl Lösungen über der Zeit [MUE18]

Mit einem zufallsbasierten Las Vegas Algorithmus nach [MIT05] ist es ebenfalls möglich alle existierenden Lösungen zu identifizieren. Mit steigender Zeitdauer sinkt das Auftreten neuer Lösungen, siehe Abbildung 4.6, während die Anzahl durchgeführter Wiederholungen steigt. In diesem Beispiel benötigt der Las Vegas Algorithmus ca. 60-mal so lang für die Identifikation aller Lösungsmöglichkeiten, wie der entscheidungsbaumbasierte Algorithmus. Aufgrund der geringen Anzahl an Minimalschnitten, handelt es sich hierbei um ein sehr einfaches Beispiel. Bei der Anforderungsableitung fehlertoleranter Systeme müssen i.d.R. mehrere hundert Minimalschnitte berücksichtigt werden. Für diesen Fall wird es deutlich, warum die schnellere Ermittlung aller Lösung durch den entscheidungsbaumbasierten Algorithmus einen Vorteil gegenüber dem zufallsbasierten Algorithmus darstellt.

Zur Lösung der komplexen Fehlerbäume von Energiebordnetzsystemen, welche eine Vielzahl an Minimalschnitten umfassen, ist die Zeitdauer, die ein zufallsbasierter Algorithmus zur Identifikation aller Lösungen im Vergleich zum entscheidungsbaum-basierten Algorithmus benötigt, zu hoch. Der entscheidungsbaumbasierte Algorithmus hat den Vorteil, dass er deutlich schneller ist und die Sicherheit besteht, dass nach Beendigung des Algorithmus alle existierenden Lösungen gefunden wurden.

Wie in Kapitel 4.1.2 beschrieben, ist es durch Setzen von Randbedingungen möglich die Anzahl an Lösungsmöglichkeiten einzuschränken. Beispiele für Entscheidungsbäume für die Minimalschnitte aus (4.8)…(4.10) sind in Abbildung 4.7 dargestellt. Die zugehörigen Lösungsvektoren für ein ASIL D Sicherheitsziel sind in Tabelle 4.3 gezeigt.

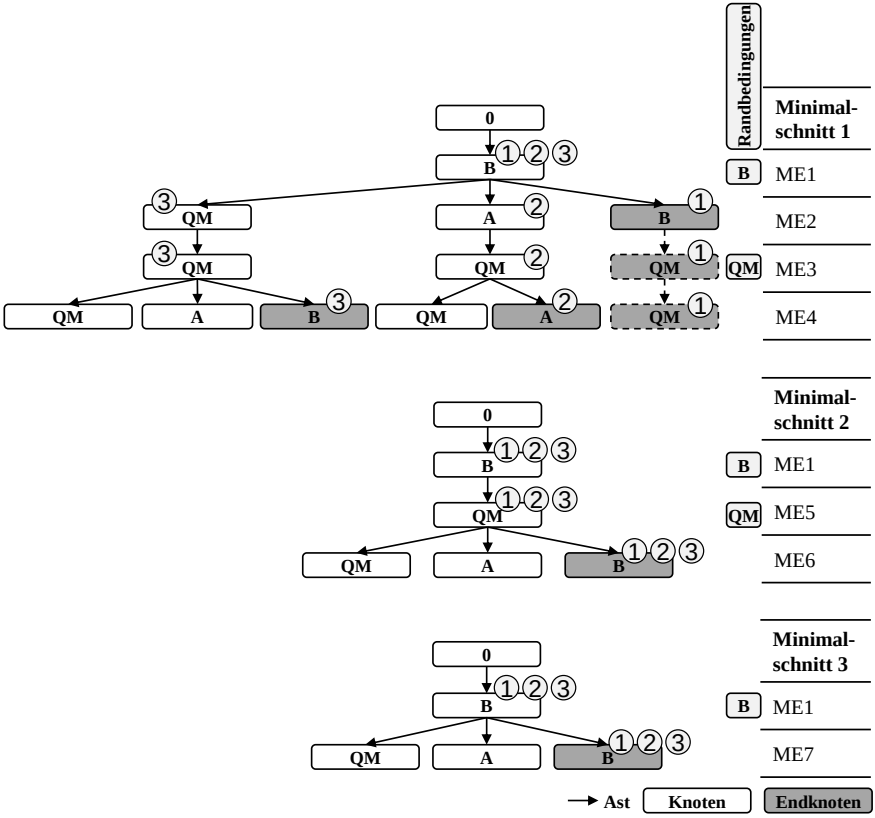


Abbildung 4.7: Entscheidungsbäume für die Minimalschnitte aus (4.8)…(4.10) unter Verwendung von fixen Randbedingungen [MUE18]

Tabelle 4.3: Verbleibende Lösungsvektoren nach Setzen von fixen Randbedingungen referenziert auf Abbildung 4.7

Lösungs-vektor	ME1	ME2	ME3	ME4	ME5	ME6	ME7
1	B(D)	B(D)	QM(D)	QM(D)	QM(D)	B(D)	B(D)
2	B(D)	A(D)	QM(D)	A(D)	QM(D)	B(D)	B(D)
3	B(D)	QM(D)	QM(D)	B(D)	QM(D)	B(D)	B(D)

4.2 Nachweis der Einhaltung der Anforderungen des fehlertoleranten Systems

Sobald das System und die zugehörigen Komponenten entwickelt sind, muss die Erfüllung der an das System gestellten Anforderungen nachgewiesen werden.
Aus Kapitel 3.3 hat sich gezeigt, dass die Markov-Analyse Ziele zur effizienten Sicherheitsanalyse-Analyse (Z2-Z4) sowie die Eigenschaften fehlertoleranter Systeme (E1-E8) abdecken kann. Die Analyse systematischer Fehler (Z1) ist durch keine der gezeigten Methoden vollumfänglich abbildbar. Des Weiteren neigt die Markov-Analyse bei Systemen mit einer Vielzahl an Komponenten (E9) zur Zustandsraumexplosion.
Aufgrund der aufgezeigten Schwächen der reinen Markov-Analyse wird in Kapitel 4.2.1 ein Konzept zur Erweiterung der Markov-Analyse vorgestellt. Die Eignung der beschriebenen Methode zur Sicherheitsanalyse fehlertoleranter Systeme wird in Kapitel 4.2.2 bis 4.2.5 beschreiben.

4.2.1 Überblick über die Methode

Nach [ISO26262] müssen sicherheitsrelevante systematische und zufällige Hardwarefehler des Items erkannt und behoben bzw. deren Auswirkungen gemindert werden, siehe Kapitel 2.3.1.3. Um dies zu erreichen wird das Verfahren nach Abbildung 4.8 eingesetzt. Systematische Fehler werden darin mittels Simulation erkannt. Die simulationsbasierte Vermeidung systematischer Fehler ist in Kapitel 4.2.2 beschrieben.

Zufällige Hardwarefehler werden in der Simulation als Einzel- und Mehrfachfehler eingeprägt und deren Auswirkung für den quantitativen Nachweis eingesetzt. Im letzten Schritt wird die Analyse abhängiger Fehler durchgeführt.

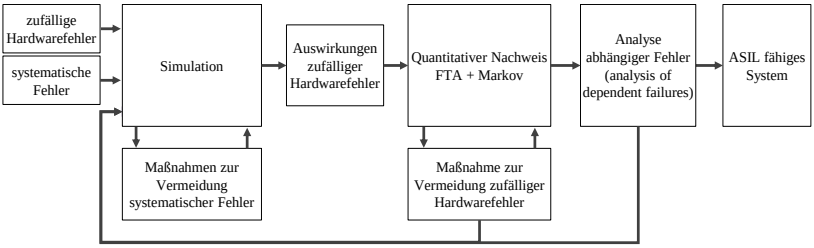


Abbildung 4.8: Vorgehen zum Nachweis eines ASIL-fähigen Systems unter Berücksichtigung systematischer und zufälliger Hardwarefehler

Das Konzept zum quantitativen Nachweis fehlertoleranter Systeme ist in Abbildung 4.9 dargestellt. Zur Modellierung des fehlertoleranten Systems wird die Markov-Analyse eingesetzt. Um eine Zustandsraumexplosion zu vermeiden, wird die Anzahl an zu modellierenden Markov-Zuständen durch folgende Maßnahmen reduziert:

- Lediglich die Systemebene (Energiebordnetzebene) wird mittels Markov-Analyse modelliert. Die darunterliegende Komponentenebene, in welcher die Vielzahl an Hardwarefehlern je Komponente berücksichtigt werden, wird mittels Fehlerbaumanalysen abgebildet. Dabei wird für jeden Komponentenfehler eine eigene Fehlerbaumanalyse durchgeführt. Die auf diese Weise ermittelten Fehlerraten der Fehler der Komponentenebene werden anschließend zur Quantifizierung der Übergangsraten zwischen den Markov-Zuständen eingesetzt.
- Fehler, die nach Experteneinschätzung dieselbe Auswirkung haben, werden zusammengefasst. Die Experteneinschätzung wird im Nachhinein mittels Simulation validiert.

Die Struktur der Markov-Analyse wird automatisiert auf Basis der Ergebnisse der Fehler-Simulationen aufgebaut, siehe Kapitel 4.2.3. Anschließend werden die [ISO26262] Metriken berechnet, wie in Kapitel 4.2.4 dargestellt. Um die Zielwerte zu erreichen,

werden Maßnahmen, wie z.B. die Einführung oder Verbesserung von Diagnosen oder die Implementierung redundanter Strukturen, ergriffen und deren Wirksamkeit durch die Methode nachgewiesen.

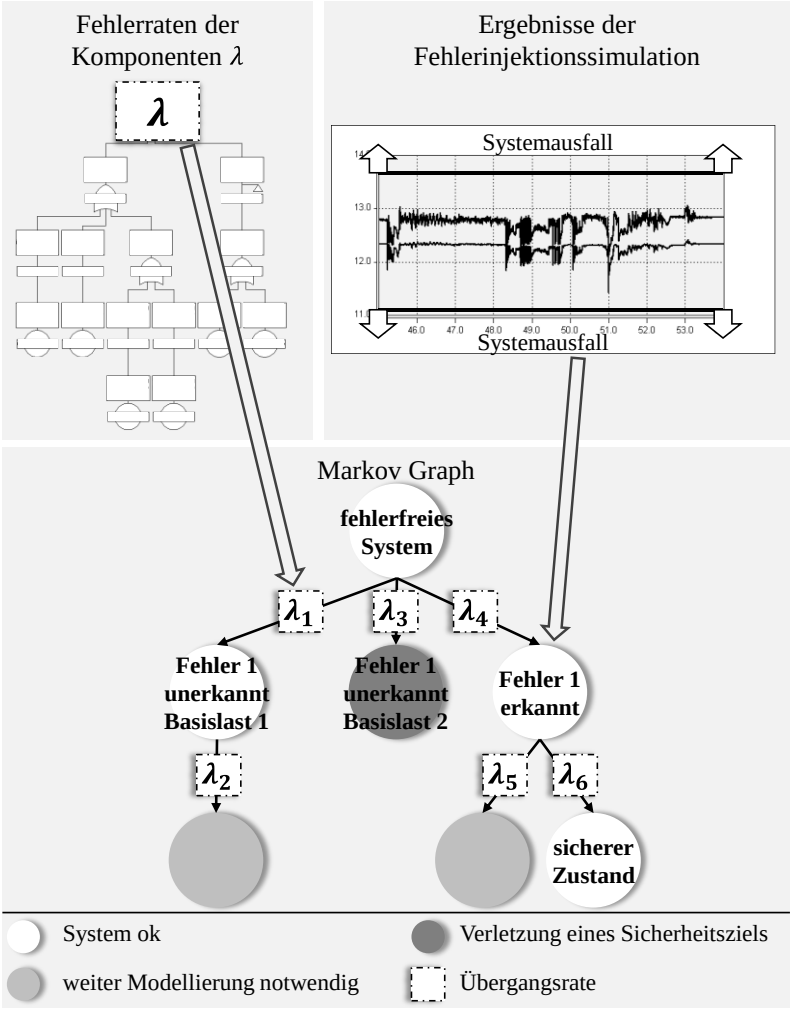


Abbildung 4.9: Kopplung der Markov-Analyse mit Fehlerbaumanalyse und Fehlerinjektionssimulation [MUE17]

Die Kopplung aus Fehlerbaumanalyse, Markov-Analyse und Fehlerinjektionssimulation stellt den Kern der Sicherheitsanalyse dar und wird in die Gesamtvorgehensweise aus Abbildung 4.10 eingebettet. Im ersten Schritt der Sicherheitsanalyse wird die Fehlerdatenbank (1) aufgebaut, in der die Struktur des Systems sowie alle Fehler der zugehörigen Komponente eingetragen werden. Die Komponentenfehler werden nach einem vorgegebenen Muster benannt, sodass eine exakte Zuordnung zu den Fehler-Simulationen und der Quantifizierung mittels Fehlerbaumanalyse möglich ist. Komponentenfehler, die nach Experteneinschätzung dieselbe Auswirkung haben, werden zu Fehlerklassen zusammengefasst. Das Zusammenfassen der Komponentenfehler hat das Ziel den Modellierungsaufwand in der Markov-Analyse gering zu halten. Ob die Bildung der Fehlerklassen zulässig ist, wird im Nachhinein mittels Simulation überprüft. Dazu werden die unterschiedlichen Komponentenfehler simuliert und deren Auswirkungen gegenübergestellt. Weichen diese zu stark ab, müssen neue Fehlerklassen erstellt und die Komponentenfehler unterschiedlichen Fehlerklassen zugeordnet werden. Um Mehrfachfehler abbilden zu können, wird eine Fehlerkombinatorik (2) aufgebaut. Dabei werden alle Fehlerklassen miteinander kombiniert und technisch nicht sinnvolle Fehlerklassenkombinationen ausgeschlossen. Die Fehlerkombinatorik ist die Basis für den automatisierten Aufbau des Markov-Modells. Mittels Fehlerbaumanalyse (3) werden die Fehlerraten der Komponentenfehler ermittelt und zu Fehlerklassen zusammengefasst. Dabei werden Diagnosen auf Komponentenebene mitbetrachtet, sodass Diagnosedeckungsgrade der Komponentenfehler ermittelt werden können. Im funktionalen Sicherheitskonzept werden mögliche Diagnosen auf Systemebene (4) inklusive deren Diagnosedeckungsgrade definiert. Weiterhin umfasst das funktionale Sicherheitskonzept die Fehlerreaktion der Systemebene (5) sowie die Fehlerreaktion der Fahrzeugebene (6). Die Diagnosedeckungsgrade der Komponenten- sowie Systemebene werden zu einem fehlerklassenspezifischen Diagnosedeckungsgrad zusammengerechnet, siehe Kapitel 4.2.4. Die Struktur der Markov-Analyse (8) ergibt sich aus den Ergebnissen der Fehlerinjektionssimulationen (7), die für eine Fehlerklasse als Worst-Case der Simulationsergebnisse aller Komponentenfehler zusammengefasst werden. Die Übergangsraten zwischen den Markov-Zuständen werden aus den Ergebnissen der Fehlerbaumanalysen und den fehlerklassenspezifischen Diagnosedeckungsgraden

definiert. Wurden für das System bereits Sicherheitsmechanismen definiert, gehen diese ebenfalls in die Modellierung der Markov-Analyse ein. Auf Basis der Markov-Analyse werden die Metriken der ISO26262 berechnet (9). Werden die geforderten Zielwerte nicht erreicht, werden Optimierungsmaßnahmen abgeleitet und das System iterativ verbessert. Dabei wird für jede abgeleitete Sicherheitsmaßnahme ein iterativer Durchgang der Methode durchgeführt und auf diese Weise die Wirksamkeit der Sicherheitsmechanismen nachgewiesen. Sensitivitätsanalysen (10) dienen dazu den Einfluss variierter Parameter auf das Gesamtsystem zu identifizieren und bei der Ableitung von Sicherheitsmaßnahmen zu unterstützen.

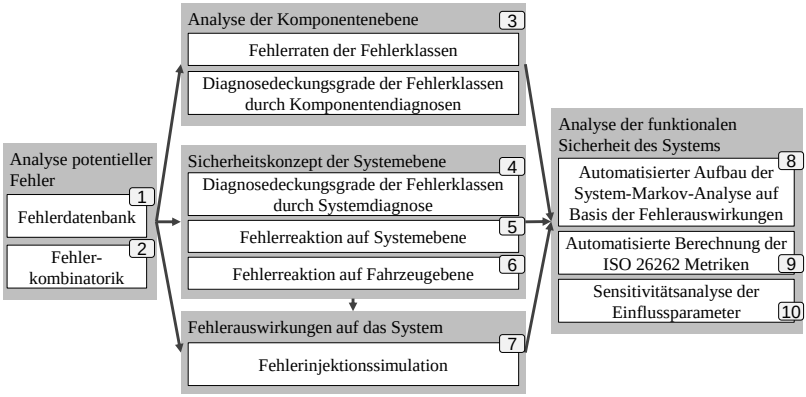


Abbildung 4.10: Gesamtvorgehensweise zum Nachweis der funktionalen Sicherheit

4.2.2 Erreichung Ziel Z1: Vermeidung systematischer Fehler

Systematische Fehler können während des gesamten Entwicklungs- und Produktionsprozesses auftreten. Systematische Fehler werden durch die ISO26262 vorgegebenen Entwicklungsprozesse und Teststrategien erkannt und behoben. Dabei können Simulationen frühzeitig in der Entwicklung systematische Fehler aufdecken. Die Ermittlung der Auswirkungen von Fehlern durch Experteneinschätzungen oder ähnliche Maßnahmen ist aufgrund der Komplexität des Systems, d.h. der vielfachen Wechselwirkungen und Abhängigkeiten der Komponenten und Systeme, nicht

zielführend. Aufgrund dessen ist es notwendig das betrachteten Systems in einem Verhaltensmodell abzubilden und mittels Fehlerinjektion die Auswirkungen von Fehlern auf die Funktion der sicherheitsrelevanten Komponenten bzw. Systeme objektiv zu analysieren. Ein weiterer Vorteil der Fehlerinjektionssimulation ist die Überprüfung der Wirksamkeit der beschriebenen Sicherheitsmechanismen.

Ziel der Fehlerinjektionssimulation ist es die Verletzung der Sicherheitsanforderungen durch Abbildung der Fehlerwirkketten ermitteln zu können. Hierfür werden in ein Verhaltensmodell die Fehler der Fehlerdatenbank durch Fehlermodelle injiziert und deren Auswirkungen bestimmt. Dabei werden die Kriterien, die zur Verletzung der Sicherheitsanforderungen führen, in der Simulation abgefragt. In der Fehlersimulation wird das Zusammenspiel der Komponenten des Systems unter Berücksichtigung der Redundanzstruktur abgebildet. Weiterhin werden unterschiedliche Fälle je Fehler betrachtet. Erkannte und unerkannte Fehler werden unterschieden. Neben den Einfachfehlern können Mehrfachfehler in der Simulation abgebildet und deren Auswirkungen ermittelt werden.

Zusammengefasst sind die Ziele der Simulation:

- Systematische Fehler auszuschließen
- Auswirkungen von zufälligen Hardwarefehlern im System zu identifizieren.

Systematische Fehler, die mittels Simulation erkannt werden können sind z.B.:

- im Systemdesign
- bei Komponentendimensionierungen
- bei Betriebsstrategien
- hinsichtlich Einsatzgrenzen von Verbrauchern
- fehlerhafte Fehlerreaktionen.

Um systematische Fehler vollumfänglich auszuschließen muss nach [ISO26262] eine Analyse abhängiger Fehler (dependent failure analysis – DFA) durchgeführt werden. Die Analyse kann auf die Ergebnisse der Simulation aufgebaut werden.

4.2.3 Erreichung Ziel Z2: Automatisierte Modellbildung und Analyse basierend auf Fehlerauswirkungen

Ein beispielhafter Markov-Graph ist in Abbildung 4.11 dargestellt. Dabei werden die modellierungstypischen Eigenschaften aus Kapitel 3.2.2 mittels Markov-Modell berücksichtigt:

- E3: Unterschiedliche Komponentenzustände werden durch eigene Markov-Zustände mit den zugehörigen Übergangsraten modelliert
- E4: Abhängigkeiten zwischen Fehlern werden durch Anpassung der Übergangsraten zwischen den Markov-Zuständen abgebildet
- E5: Diagnosedeckungsgrade werden durch Anpassung der Übergangsraten und Aufteilung von Fehlern in erkannte und unerkannte Fehler berücksichtigt
- E6: Unterschiedliche Zeitdauern von Zuständen werden durch die Anpassung der Übergangsrate, welche die Dauer zum Übergang in den sicheren Zustand definiert (TTSS), berücksichtigt
- E7: Mehrfachfehler werden durch Aneinanderreihung der Markov-Zustände und durch Berücksichtigung der entsprechenden Übergangsraten modelliert
- E8: Reihenfolgeeffekte werden dadurch abgebildet, dass auf einen Zustand ein anderer Zustand folgt. Die umgekehrte Reihenfolge wird jedoch nicht modelliert. Als Beispiel folgt der Ausfall einer Komponente auf deren Degradierung. Die umgekehrte Fehler-Reihenfolge ist nicht möglich und wird nicht abgebildet.

Ausgehend vom fehlerfreien Zustand (1) werden die Markov-Zustände basierend auf den Simulationsergebnissen nach dem beschriebenen Vorgehen, siehe 4.2.3.2 ff, aufgebaut und die Übergangsraten durch die Ergebnisse der Fehlerbaumanalyse festgelegt. Dabei sind im Markov-Graphen alle Fehler, die zur Berechnung der Metriken (Kapitel 4.2.4) notwendig sind, exemplarisch dargestellt. In Zustand (2) ist der erkannte Fehler 1 aufgetreten. Wird ein Fehler erkannt, wird die im Sicherheitskonzept definierte Fehlerreaktion auf Systemebene eingeleitet. Eine solche Reaktion ist z.B. eine Reduzierung der System-Belastung und damit eine Stabilisierung des Systems. Ebenso wird auf Fahrzeugebene der Übergang in den sicheren Zustand als Fehlerreaktion

eingeleitet, der in Zustand (3) eingenommen wird. Da der Übergang eine bestimmte Dauer benötigt, können in diesem Zeitintervall weitere Fehler auftreten, die ggfs. zum Systemausfall und damit zur Verletzung des Sicherheitsziels führen können, siehe Zustand (4). Zustand (5) stellt den unerkannten Fehler 1 dar (multiple point fault latent - MPF_{latent}). In Zustand (6) folgen auf diesen latenten Fehler weitere Fehler, die in Kombination zur Verletzung des Sicherheitsziels führen (dual point faults - DPFs). Zustand (7) umfasst den Fehler 2, der direkt das Sicherheitsziel verletzt (single point fault – SPF). In Zustand (8) ist Fehler 3 eingetreten und wurde erkannt. Der Übergang in den sicheren Zustand wird in Zustand (9) erreicht. Während des Übergangs können weitere Fehler auftreten, die zu Zustand (10) führen. Zu Zustand (11) führt der unerkannte Fehler 3, der zur Verletzung des Sicherheitsziels führt (residual fault – RF). Weitere Analysen sind zur Analyse der weiteren Einfachfehler (12) notwendig.

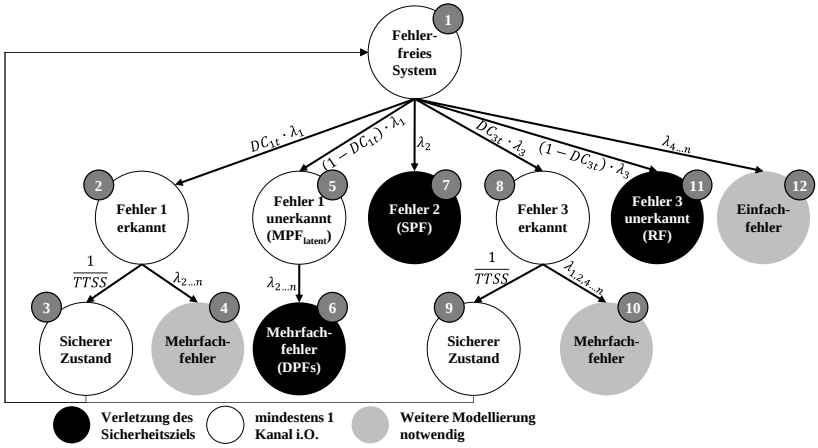


Abbildung 4.11: Ausschnitt eines möglichen Markov-Graphen

Für die Berechnung der ISO 26262 Metriken, siehe Kapitel 4.2.4, müssen die Markov-Zustände in SPF, RF und MPF_{latent} eingeteilt werden. Nach ISO 26262 müssen bei SPF zusätzliche Maßnahmen ergriffen werden, weswegen hier eine Ausgabe zur manuellen Weiterbearbeitung erfolgt [ISO 26262-5, 9.4.1.2/3].

In Abbildung 4.11 sind folgende Übergangsraten definiert, die für die Berechnung der ISO 26262 Metriken benötigt werden:

- $(1 - DC_{1t}) \cdot \lambda_1$: Übergangsrate des unerkannten Fehlers 1, eines Multiple Point Fault latent (MPF_{latent}), der kombiniert mit den Fehlern $2 \dots n$ (Fehlerraten $\lambda_{2\dots n}$) das Sicherheitsziel verletzt und dadurch zum Dual Point Fault (DPF) wird.
- λ_2: Übergangsrate des Fehlers 2, der direkt das Sicherheitsziel verletzt und somit ein Single Point Fault (SPF) ist
- $(1 - DC_{3t}) \cdot \lambda_3$: Übergangsrate des unerkannten Fehlers 3, der direkt das Sicherheitsziel verletzt und somit als Residual Fault (RF) definiert ist

Das Systemverhalten ist abhängig von einem Systemparameter. Der Einfluss des Systemparameters wird in Kapitel 4.2.3.1 beschrieben.

Das zu analysierende redundante System wird in der Simulationsumgebung modelliert und die zu untersuchenden Fehler bzw. Fehlerkombinationen eingeprägt. Dabei werden Simulationen sowohl für den erkannten, als auch für den unerkannten Fall durchgeführt. Im erkannten Fall werden die Fehlerreaktionen abgebildet. Im unerkannten Fall kann keine Fehlerreaktion umgesetzt werden. Beeinflussen weitere Systemparameter das System, wird auch deren Einfluss auf das System in der Simulation abgebildet. Während den Fehler-Simulationen werden die Grenzen überwacht, bei denen es zum Funktionsverlust einer oder beider redundanter Subsysteme kommt. Das Vorgehen zum automatisierten Aufbau der Markov-Struktur wird in 4.2.3.2 ff beschrieben. Dabei werden die genannten Fallunterscheidungen durchgeführt und auf Basis der Simulationsergebnisse der relevante Fall extrahiert. Der Ablauf wird nacheinander für jeden sicherheitsrelevanten Fehler durchgeführt.

4.2.3.1 Berücksichtigung der Systemparameter

Es ist möglich, dass bestimmte Systemparameter SysP Einfluss auf die Einhaltung der definierten Grenzwerte haben. Beispielhafte Systemparameter sind Temperaturen oder Belastungen. Diese Systemparameter können z.B. in Form von Verteilungen definiert werden. In Abbildung 4.12 ist ein beispielhafter zeitlicher Verlauf des Systemparameters SysP dargestellt. Am Beispiel Energiebordnetz ist der Systemparameter z.B. die Last im

Energiebordnetz, die sich aus den aktiven Verbrauchern ergibt. Schwankungen in der Energiebordnetz-Last ergeben sich z.B. jahreszeitenabhängig. Verbraucher, die eine große Last im Energiebordnetz darstellen sind z.B. Heizungen, die hauptsächlich im Winter eingeschaltet sind und damit zu einer hohen Last im Energiebordnetz führen. Für die Analyse wird der Systemparameter für den erkannten ($SysP_{erk}$) und den unerkannten Fall ($SysP_{unerk}$) unterschieden.

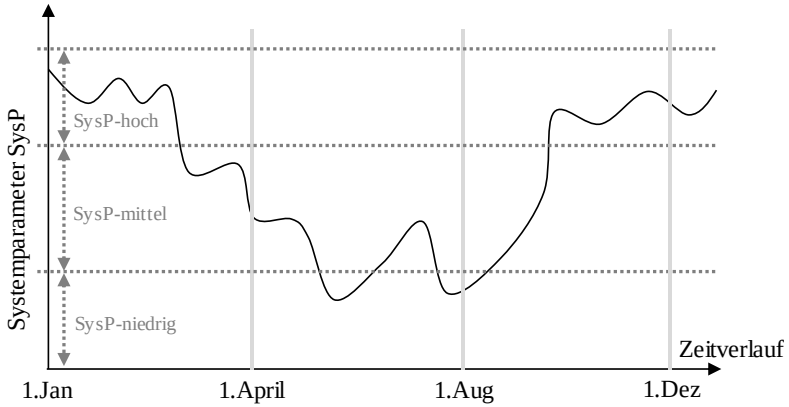


Abbildung 4.12: Exemplarischer zeitlicher Verlauf des Systemparameters SysP

Systemparameter $SysP_{erk}$

Im Fall eines erkannten Fehlers im System kann der Systemparameter $SysP_{erk}$ im Normalbetrieb durch Maßnahmen angepasst werden, die im Sicherheitskonzept definiert sind. Im Energiebordnetz kann im Falle eines Fehlers z.B. die Abschaltung von Komfort-Verbrauchern durchgeführt werden. Auf diese Weise wird die Belastung im Energiebordnetz reduziert und die Fehlerauswirkung kann minimiert werden. Sind im Sicherheitskonzept keine Maßnahmen vorgegeben, muss der Effekt des Parameters berücksichtigt werden. Dasselbe gilt, falls durch den Eintritt eines Fehlers die Einschränkung des Parameters aufgehoben wird. Die Wirkungsdauer des Systemparameters $SysP_{erk}$ ist dabei auf die Dauer des Übergangs in den sicheren Zustand begrenzt. Aufgrund der kurzen Zeitdauer kann davon ausgegangen werden, dass der

Parameter konstant ist. Um die Effekte des Parameters definieren zu können, wird in diesem Fall das Intervall des Parameters in drei Bereiche $SysP_{erk}$ -niedrig, -mittel und -hoch unterteilt. Die Auswirkungen des Parameters auf die zu analysierenden Fehler-bzw. Fehlerkombinationen werden simulativ ermittelt. Die Häufigkeit jedes Intervalls wird nachfolgend durch die Faktoren $E_{nied}, E_{mitt}, E_{hoch}$ quantifiziert.

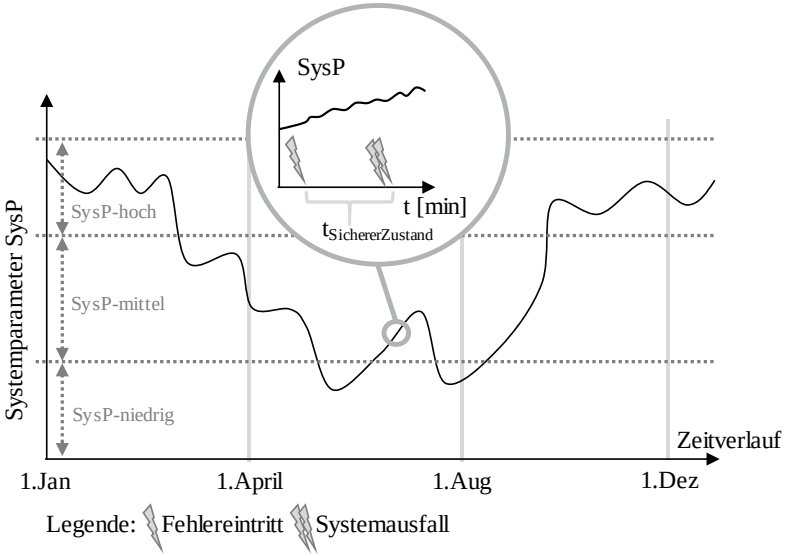


Abbildung 4.13: Einfluss des Systemparameters beim erkannten Fehler

Ein möglicher Aufbau eines Markov-Graphen, bei dem der Effekt des Systemparameters berücksichtigt ist, ist in Abbildung 4.14 dargestellt. Die Struktur des Markov-Graphen ergibt sich dabei aus den Simulationsergebnissen und den Bildungsvorschriften des Markov-Graphen nach Kapitel 4.2.3.2 ff. Durch Faktoren $E_{nied}, E_{mitt}, E_{hoch}$ werden die Übergangsraten der Markov-Zustände zur Unterscheidung der Effekte des Systemparameters angepasst. Da die Summe der Übergangsraten eines Fehlers konstant bleiben muss, muss die Summe der Faktoren $E_{nied}, E_{mitt}, E_{hoch}$ immer eins ergeben, siehe Formel (4.20). Die Quantifizierung der Faktoren ist in Kapitel 4.2.4.3 beschrieben.

$$E_{nied} + E_{mitt} + E_{hoch} = 1 \tag{4.20}$$

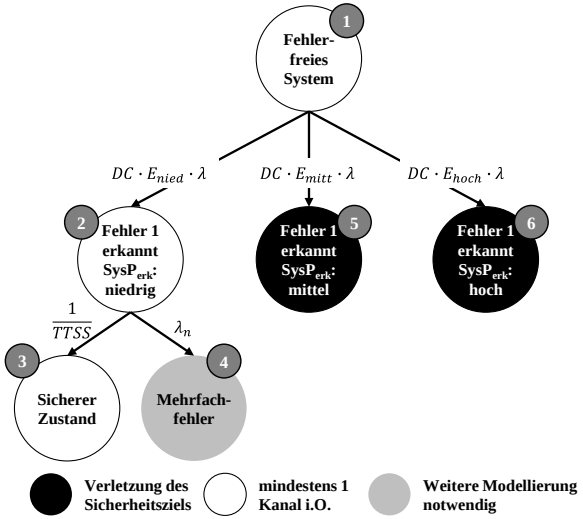


Abbildung 4.14: Ausschnitt eines beispielhaften Markov-Modells unter Berücksichtigung des Systemparameters SysP$_{erk}$

Systemparameter SysP$_{unerk}$

Im Unterschied zum erkannten Fall ist die Fehlerauswirkung im unerkannten Fall aufgrund des langen Zeithorizontes von Schwankungen des Systemparameters abhängig. Wenn ein Fehler bzw. eine Fehlerkombination vom Systemparameter abhängig ist, kann nach Fehlereintritt von einer Energiebordnetzlast ausgegangen werden, die zum Ausfall des Systems führt. Es handelt sich bei dem Fehler um einen schlafenden Fehler. Aufgrund dieses Zusammenhangs kann als worst-case Annahme argumentiert werden, dass solch ein Fehler immer zum Ausfall führt. Dabei ist es unerheblich, dass der Ausfall mit zeitlicher Verzögerung auftritt. Es wird kein Korrekturfaktor zur Unterscheidung unterschiedlicher Systemzustände eingeführt und damit keine Veränderungen am Markov-Graphen des Ausfalls bei unerkanntem Fehler vorgenommen, siehe Abbildung 4.16.

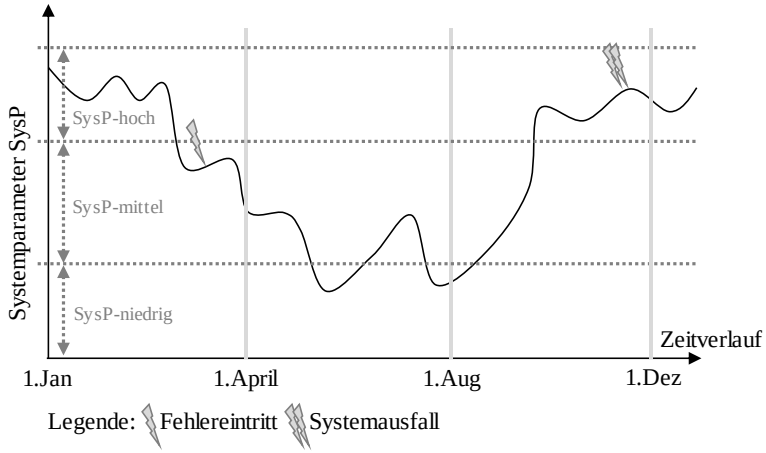


Abbildung 4.15: Einfluss des Systemparameters beim unerkannten Fehler

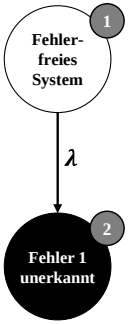


Abbildung 4.16: Einfluss des Systemparameters beim unerkannten Fehler

4.2.3.2 Markov-Modellierung – Normalfall – Erstfehlerebene

Im ersten Schritt wird unterschieden, ob der Erstfehler erkannt oder unerkannt ist. Dazu wird jeweils ein Zustand für den erkannten und den unerkannten Erstfehler erstellt. Die Übergangsraten vom fehlerfreien Zustand (1-Abbildung 4.11) zum erkannten Zustand (z.B. 2 / 8-Abbildung 4.11) werden dabei aus der Multiplikation der Fehlerrate und des Diagnosedeckungsgrades des Erstfehler bestimmt. Der Übergang zum unerkannten Zustand (z.B. 5 / 11-Abbildung 4.11) definiert sich aus der Multiplikation der Fehlerrate sowie des negierten Diagnosedeckungsgrades des Erstfehlers.

Anschließend an den erkannten Erstfehler, wird die zugehörige Fehlerreaktion auf Systemebene überprüft. Ist eine Fehlerreaktion definiert, so ist der Systemparameter $SysP_{erk}$ definiert und der Ablauf für den erkannten Normalfall nach Abbildung 4.17 wird angewandt. Ist der Systemparameter $SysP_{erk}$ nicht definiert, ist der Sonderfall nach Kapitel 4.2.3.3 zu betrachten.

Für den *erkannten Normalfall* wird überprüft, ob während der Simulation in den Teilnetzen die definierten Grenzwerte eingehalten werden.

- Kommt es in beiden Teilnetzen zur Verletzung der Grenzwerte, so ist das Sicherheitsziel verletzt (Systemausfall – SA). Die Modellierung des erkannten Fehlers endet nach einem SA-Zustand, da mit der Verletzung des Sicherheitsziels das System seine Funktionsfähigkeit verliert.
- Werden nur in einem oder keinem Teilnetz die Grenzwerte verletzt, wird der definierte Übergang in den sicheren Zustand und dessen Dauer in der Markov-Struktur angelegt. Aufgrund der zeitlichen Verzögerung beim Erreichen des sicheren Zustands können weitere Fehler auftreten, die mittels Zweitfehleranalyse Z1e, siehe Kapitel 4.2.3.5 und 4.2.3.6 modelliert werden.

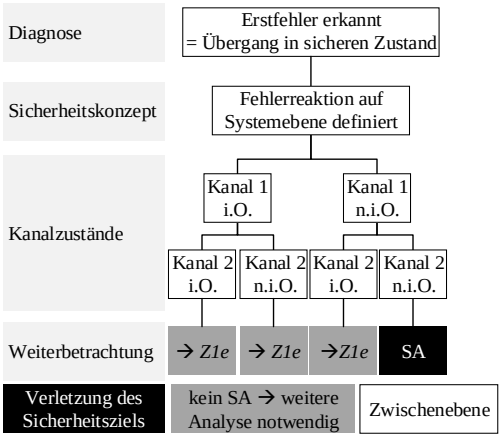


Abbildung 4.17: Fallunterscheidung des erkannten Erstfehlers im Normalfall zum Aufbau des Markov-Graphen

Bei der Analyse des *unerkannten Fehlers*, siehe Abbildung 4.18, kann keine Fehlerreaktion berücksichtigt werden, da die Anwesenheit des Fehlers unbekannt ist.

1. Führt der Systemparameter in einer Ausprägung in der Zukunft in beiden Teilnetzen zur Verletzung der Grenzwerte, so ist das Sicherheitsziel verletzt. Der Markov-Zustand wird als „SA“ markiert Die Modellierung des unerkannten Fehlers endet.
2. Führt der unerkannte Fehler bei keiner Ausprägung des Systemparameters zur Verletzung des Sicherheitsziels, so wird die Zweitfehlerbetrachtung Z1u, siehe Kapitel 4.2.3.7 ff, angestoßen.

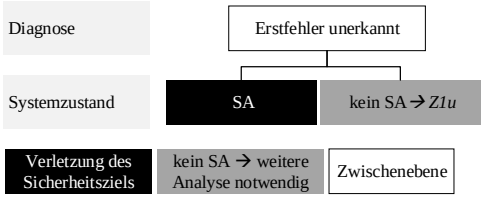


Abbildung 4.18: Fallunterscheidung des unerkannten Erstfehlers zum Aufbau des Markov-Graphen

4.2.3.3 Markov-Modellierung – Sonderfall – Erstfehlerebene

Der *erkannte Sonderfall* ist dadurch definiert, dass für den betrachteten Fehler keine Fehlerreaktion auf Systemebene definiert ist. Dadurch ist der Systemparameter $SysP_{erk}$ des erkannten Falls variabel.

Dadurch ergeben sich folgende Möglichkeiten:

1. Im ersten Schritt wird überprüft, ob es durch den Fehler unabhängig vom Systemparameter $SysP_{erk}$ in beiden Teilnetzen zur Verletzung der Grenzwerte kommt. In diesem Fall ist das Sicherheitsziel verletzt. Die Modellierung des erkannten Fehlers endet mit dem zugehörigen Zustand und der Zuweisung „SA“.
2. Führt der Fehler in Kombination mit dem variablen Systemparameter $SysP_{erk}$ nicht zur Verletzung des Sicherheitsziels, wird die Modellierung des Übergangs in den sicheren Zustand sowie der Zweitfehlerebene Z2e angestoßen, siehe Kapitel 4.2.3.6,.
3. Hat der Systemparameter $SysP_{erk}$ einen Einfluss auf die Fehlerauswirkung, so wird eine detaillierte systemparameterabhängige Betrachtung durchgeführt. Der bisher erstellte Zustand wird aufgeteilt, sodass für jede Ausprägung des Systemparameters $SysP_{erk}$ ein eigener Zustand erstellt wird. Die Übergangsraten zu den neu erstellten Zuständen werden dabei um den Faktor des $SysP_{erk}$ angepasst, siehe Kapitel 4.2.4.3. Die Verletzung der Grenzwerte wird für jeden neuen Zustand überprüft.
    a. Kommt es abhängig vom Systemparameter $SysP_{erk}$ in beiden Teilnetzen zur Verletzung der Grenzwerte, so ist das Sicherheitsziel verletzt. Die Modellierung des erkannten Fehlers mit dem betrachteten Systemparameter endet. Der Zustand wird mit „SA“ markiert.
    b. Wird der SA vermieden, wird der Übergang in den sicheren Zustand sowie die Zweitfehlerbetrachtung Z3e, siehe Kapitel 4.2.3.5, durchgeführt.

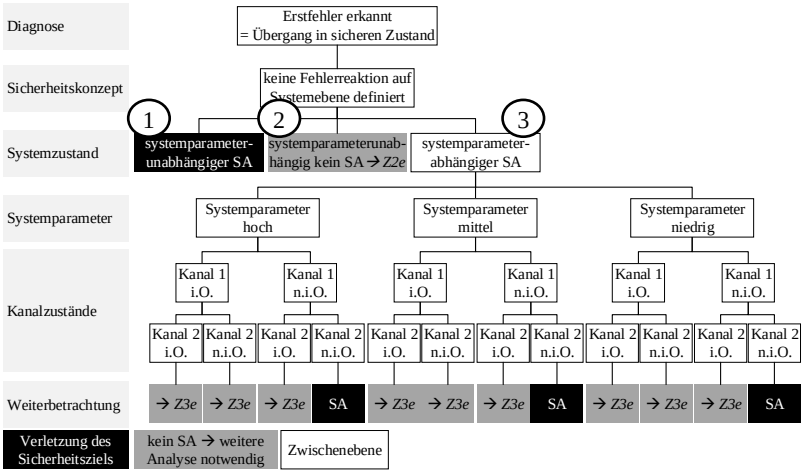


Abbildung 4.19: Fallunterscheidung des erkannten Erstfehlers im Sonderfall zum Aufbau des Markov-Graphen

4.2.3.4 Markov-Modellierung – Zweifachfehler

Die Fehlerkombinatorik gibt an, welche Zweitfehler nach dem aktuell betrachteten Erstfehler analysiert werden müssen. Nach [ISO26262] ist die Betrachtung einschließlich der Zweifachfehlerebene ausreichend, sofern Fehler höherer Ordnung keinen nennenswerten Einfluss auf das System haben. Aufgrund der niedrigen analysierten Fehlerraten wird davon ausgegangen, dass Fehler höherer Ordnung keinen Einfluss haben. Dementsprechend endet die Modellierung mit der Zweifachfehlerebene. Eine Erweiterung der Modellierung auf höhere Ebenen ist bei Erweiterung des beschriebenen Vorgehens möglich.

4.2.3.5 Markov-Modellierung – Normalfall Z1e / Z3e

Die Vorgehensweise nach Abbildung 4.20 ist für den *Normalfall der Zweitfehler Z1e* und *Z3e* aufgrund der Randbedingungen aus dem Erstfehler identisch:

- Z1e: Fehler beim Übergang in den sicheren Zustand; Systemparameter $SysP_{erk}$ ist durch Fehlerreaktion des Erstfehlers definiert

- Z3e: Fehler beim Übergang in den sicheren Zustand; Systemparameter $SysP_{erk}$ ist durch Berücksichtigung des Faktors des Systemparameters $SysP_{erk}$ definiert

Unabhängig von der weiteren Modellierung wird ein Markov-Zustand zur Definition des Systems angelegt. Die Übergangsrate vom Erstfehlerzustand zum neu angelegten Zustand wird mittels Fehlerrate des Zweitfehlers quantifiziert.

- Kommt es in beiden Teilnetzen zur Verletzung der Grenzwerte, so ist das Sicherheitsziel verletzt. Der Markov-Zustand wird als „SA“ markiert.
- Werden nur in einem oder keinem Teilnetz die Grenzwerte verletzt, wird der Zustand als „kein SA“ markiert. Die Betrachtung endet, da die Zweitfehlerebene erreicht ist.

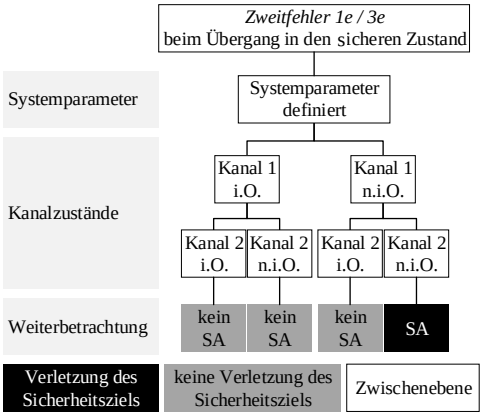


Abbildung 4.20: Zweitfehler Betrachtung Normalfall Z1e / Z3e

4.2.3.6 Markov-Modellierung – Sonderfall Z1e / Normalfall Z2e

Die Vorgehensweise nach Abbildung 4.21 ist für den *Sonderfall des Zweitfehler Z1e* und den *Normalfall des Zweitfehlers Z2e* aufgrund der Randbedingungen aus dem Erstfehler identisch:

- Z1e: Fehler beim Übergang in den sicheren Zustand; Systemparameter $SysP_{erk}$ ist durch Fehlerreaktion des Erstfehlers definiert; Aufhebung der Definition des Systemparameters durch den Zweitfehler

- Z2e: Fehler beim Übergang in den sicheren Zustand; Systemparameter $SysP_{erk}$ ist nicht definiert, da Erstfehler nie zur Verletzung des Sicherheitsziels führt

1. Im ersten Schritt wird überprüft, ob es durch die Fehlerkombination unabhängig vom Systemparameter $SysP_{erk}$ in beiden Teilnetzen zur Verletzung der Grenzwerte kommt. In diesem Fall ist das Sicherheitsziel verletzt. Es wird ein neuer Markov Zustand angelegt und als „SA“ markiert. Die Übergangsrate wird durch die Fehlerrate des Zweitfehlers definiert.
2. Führt die Fehlerkombination unabhängig vom Systemparameter $SysP_{erk}$ nie zur Verletzung des Sicherheitsziels, wird ein neuer Markov Zustand angelegt und als „kein SA“ markiert. Die Übergangsrate wird durch die Fehlerrate des Zweitfehlers definiert.
3. Hat der Systemparameter $SysP_{erk}$ einen Einfluss auf die Fehlerauswirkung, so wird eine detaillierte systemparameterabhängige Betrachtung durchgeführt. Für jede Ausprägung des Systemparameters wird ein eigener Zustand erstellt. Die Übergangsraten ergeben sich dabei aus der Kombination der Fehlerrate des Zweitfehlers und dem Korrekturfaktor zur Berücksichtigung des Systemparameters $SysP_{erk}$, siehe Kapitel 4.2.4.3.
   a. Kommt es abhängig vom Systemparameter $SysP_{erk}$ in beiden Teilnetzen zur Verletzung der Grenzwerte, so ist das Sicherheitsziel verletzt. Der zugehörige Markov-Zustand wird als „SA“ markiert.
   b. Führt die Kombination nicht zum SA, wird der zugehörige Markov-Zustand als „kein SA“ markiert.

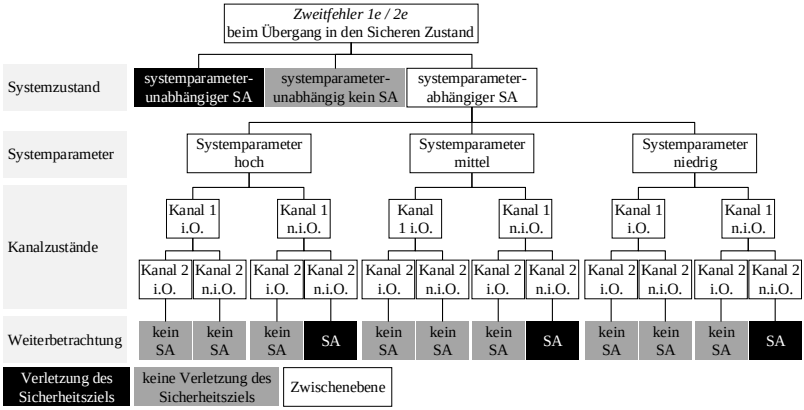


Abbildung 4.21: Zweitfehler Betrachtung Sonderfall Z1e / Normalfall Z2e

4.2.3.7 Markov-Modellierung – Normalfall Z1u erkannt

Nach dem unerkannten Erstfehler wird überprüft, ob der Zweitfehler erkannt oder unerkannt ist. Sowohl für den erkannten als auch für den unerkannten Fall wird ein Zustand an den zugehörigen Erstfehler angehängt. Die Übergangsraten der Zustände ergeben sich aus der Multiplikation der Fehlerrate und dem positiven bzw. negierten Diagnosedeckungsgrad des Zweitfehlers.

Hier wird der erkannte Normalfall für die Zweitfehler Z1u, d.h. für den erkannten Fehler ist eine Fehlerreaktion auf Systemebene definiert, betrachtet. Dabei gilt für die zugehörigen Erstfehler folgende Vorgeschichte:

- Z1u: Erstfehler unerkannt und führt nie zur Verletzung des Sicherheitsziels

Das Vorgehen zur Analyse des erkannten Zweitfehlers ist in Abbildung 4.22 dargestellt.

- Kommt es in beiden Teilnetzen zur Verletzung der Grenzwerte, so ist das Sicherheitsziel verletzt. Die Modellierung des erkannten Fehlers endet nach einem SA-Zustand.
- Werden nur in einem oder keinem Teilnetz die Grenzwerte verletzt, wird der definierte Übergang in den sicheren Zustand und dessen Dauer in der Markov-Struktur angelegt. Aufgrund der zeitlichen Verzögerung beim Erreichen des sicheren Zustands können weitere Fehler auftreten. In diesem Fall werden

Drittfehler angelegt, die als Abschätzung zur sicheren Seite per Definition zum SA führen.

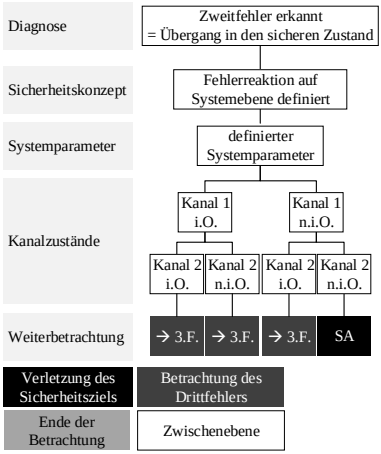


Abbildung 4.22: Zweitfehler Betrachtung Normalfall Z1u erkannt

4.2.3.8 Markov-Modellierung – Sonderfall Z1u erkannt

Beim Sonderfall für den erkannten Zweitfehler Z1u ist keine Fehlerreaktion auf Systemebene $SysP_{erk}$ definiert. Die Vorgeschichte der Fehler ist:

- Z1u: Erstfehler unerkannt und führt nie zur Verletzung des Sicherheitsziels

Das Vorgehen zur Analyse des erkannten Zweitfehlers ist in Abbildung 4.23 dargestellt.

1. Im ersten Schritt wird überprüft, ob es durch den Fehler unabhängig vom Systemparameter $SysP_{erk}$ in beiden Teilnetzen zur Verletzung der Grenzwerte kommt. In diesem Fall ist das Sicherheitsziel verletzt. Die Modellierung des erkannten Fehlers endet mit dem zugehörigen Zustand und der Definition als „SA“.
2. Führt der Fehler in Kombination mit dem variablen Systemparameter $SysP_{erk}$ nie zur Verletzung des Sicherheitsziels, wird die Modellierung des Übergangs in den sicheren Zustand sowie der Drittfehler angestoßen, die als Abschätzung zur sicheren Seite per Definition zum SA führen.

3. Hat der Systemparameter $SysP_{erk}$ einen Einfluss auf die Fehlerauswirkung, so wird eine detaillierte systemparameterabhängige Betrachtung durchgeführt. Dazu wird der bisherige Zustand in mehrere Zustände aufgeteilt, sodass für jede Ausprägung des Systemparameters $SysP_{erk}$ ein eigener Zustand erstellt wird. In den Übergangsraten der neu angelegten Zustände wird der Korrekturfaktor des Systemparameters $SysP_{erk}$ berücksichtigt. Die Modellierung der Systemparameter ist in Kapitel 4.2.4.3 beschrieben.
   a. Kommt es abhängig vom Systemparameter $SysP_{erk}$ in beiden Teilnetzen zur Verletzung der Grenzwerte, so ist das Sicherheitsziel verletzt. Die Modellierung des erkannten Fehlers mit dem betrachteten Systemparameter endet und der zugehörige Zustand wird als „SA“ markiert
   b. Kommt es nicht zum SA, wird der Übergang in den sicheren Zustand sowie die Drittfehlerbetrachtung angestoßen, die als Abschätzung zur sicheren Seite per Definition zum SA führt.

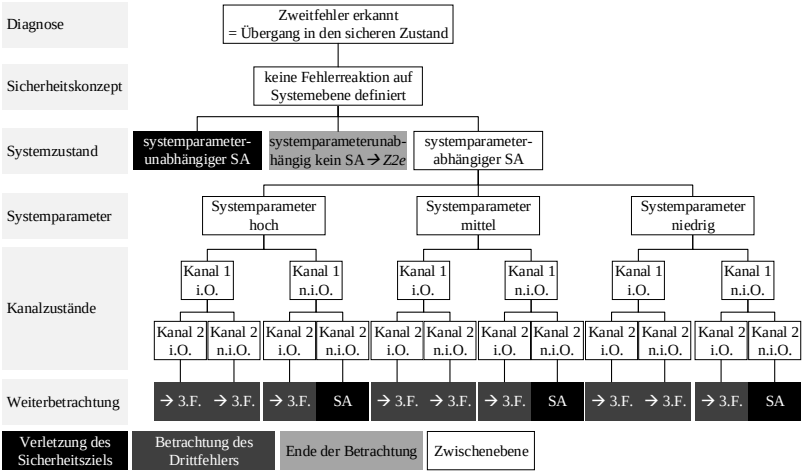


Abbildung 4.23: Zweitfehler Betrachtung Z1u erkannt Sonderfall

4.2.3.9 Markov-Modellierung – Normalfall Z1u unerkannt

Die Vorbedingungen zur Analyse des Zweitfehlers Z1u sind:

- Z1u: Erstfehler unerkannt und führt nie zur Verletzung des Sicherheitsziels

Bei der Analyse des *unerkannten Zweitfehlers Z1u*, siehe Abbildung 4.24, werden folgende Fälle unterschieden:

1. Kommt es bei einer Ausprägung des Systemparameters in beiden Teilnetzen zur Verletzung der Grenzwerte, so ist das Sicherheitsziel verletzt. Der Zustand wird als „SA“ markiert und die Die Modellierung des unerkannten Zweifachfehlers endet.
2. Führt der unerkannte Fehler bei keiner Ausprägung des Systemparameters zur Verletzung des Sicherheitsziels, wird der Zustand als „kein SA“ markiert und die Betrachtung endet mit der Zweifachfehlerebene.

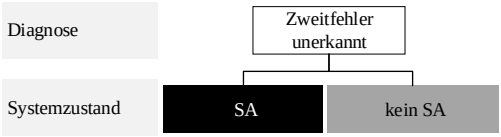


Abbildung 4.24: Zweitfehler Betrachtung Z1u unerkannt

4.2.4 Erreichung Ziel Z3: Berechnung der ISO 26262 Metriken

Die Markov-Struktur wird auf Basis der Simulationsergebnisse nach Kapitel 4.2.3 automatisiert aufgebaut. Zur Berechnung der ISO 26262 Metriken (Kapitel 4.2.4.4) müssen im nächsten Schritt die Zustandswahrscheinlichkeiten des Markov-Graphen berechnet werden. Dazu werden die Übergangsraten des Markov-Graphen quantifiziert. Die Übergangsraten setzen sich aus den Fehlerraten und Diagnosedeckungsgraden der Komponenten nach Kapitel 4.2.4.1, den fehlerspezifischen Diagnosedeckungsgraden nach Kapitel 4.2.4.2 sowie den Systemparametern nach Kapitel 4.2.4.3 zusammen.

4.2.4.1 Quantifizierung der Komponentenebene

Durch die Berechnung der Fehlerraten auf Komponentenebene mittels Fehlerbaumanalyse wird die Komplexität der Modellierung der Komponentenebene in die Fehlerbaumanalyse ausgelagert. Dadurch und durch die Kombination der Komponentenfehler zu

Fehlerklassen, wird eine Zustandsraumexplosion in der Markov-Analyse der Energiebordnetzebene vermieden (E9 – Kapitel A23)). Die Berechnung der Fehlerraten der Fehlerklassen erfolgt durch Addition der Fehlerraten der fehlerklassenzugehörigen Komponentenfehler. Die Fehlerbaumanalyse bildet dabei

- das Design der abgebildeten Komponente
- zufällig verteile (exponentialverteilte) Fehler (E1)
- niedrige Fehlerraten der Bauteilebene (E2)
- den Diagnosedeckungsgrad der Komponentenebene des Fehlers (E5)
- die Fehlerrate des Komponentenfehlers

der Komponente ab.

Ein Ausschnitt eines beispielhaften Fehlerbaums zur Quantifizierung der Komponentenebene ist in Abbildung 4.25 dargestellt.

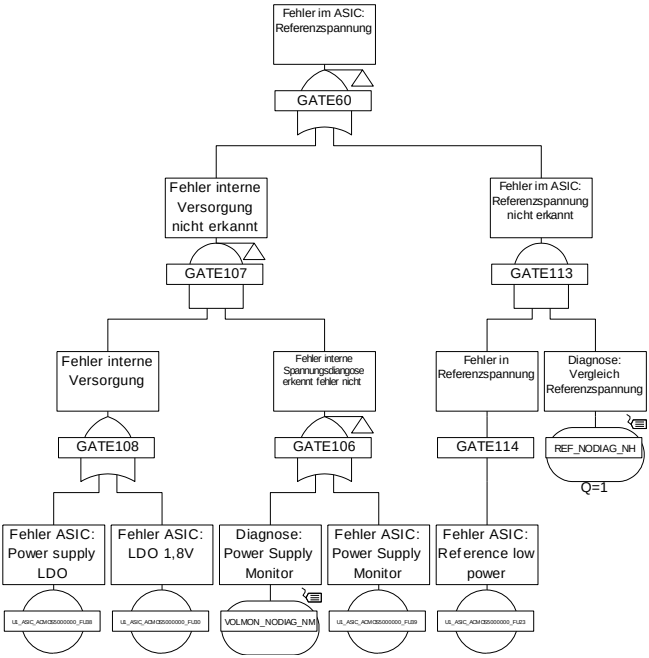


Abbildung 4.25: Ausschnitt eines exemplarischen Fehlerbaums zur Analyse der Komponentenebene

Die Berechnung der komponentenspezifischen Fehlerraten λ_K wird auf Basis der Exponentialverteilung nach Gleichung (4.21) durchgeführt. Diese ist Teil der Übergangsraten der Markov-Systemanalyse (Kapitel 4.2.4.4). Für $\lambda \cdot t \ll 1$ kann näherungsweise die PMHF der Komponentenebene $PMHF_K$ als λ_K eingesetzt werden. Es gilt Gleichung (4.22).

$$\lambda_K = \frac{-\ln(1 - F_{w-DC}(t_{life}))}{t_{life}} \tag{4.21}$$

$$\lambda_K \approx PMHF_K = \frac{F_{w-DC}(t_{life})}{t_{life}}; f\ddot{u}r\ \lambda \cdot t \ll 1 \tag{4.22}$$

$F_{w-DC}(t_{life})$	Fehlerwahrscheinlichkeit des Komponentenfehlers unter Berücksichtigung von Diagnosen
t_{life}	Lebensdauer des Systems

Der Diagnosedeckungsgrad der Komponentenebene DC_{Fx-K} ergibt sich nach Gleichung (4.23).

$$DC_{Fx-K} = 1 - \frac{F_{w-DC}(t_{life})}{F_{w/o-DC}(t_{life})} \tag{4.23}$$

DC_{Fx-K}	Eigen-Diagnosedeckungsgrad der Komponentenebene
$F_{w-DC}(t_{life})$	Fehlerwahrscheinlichkeit des Komponentenfehlers unter Berücksichtigung von Diagnosen
$F_{\mathrm{w/o-}DC}(t_{life})$	Fehlerwahrscheinlichkeit des Komponentenfehlers ohne Berücksichtigung von Diagnosen
t_{life}	Lebensdauer des Systems

Für die Berechnung der SPFM und der LFM der Energiebordnetzebene wird die Gesamtfehlerrate der sicherheitsrelevanten Hardwareelemente $\lambda_{SR-gesamt}$ benötigt, siehe Kapitel 2.3.1.3. Dazu muss jede Komponente ihren Beitrag λ_{SR-m} zur Gesamtfehlerrate

der sicherheitsrelevanten Hardwareelemente $\lambda_{SR-gesamt}$ an die Systemebene übermitteln. λ_{SR-m} ergibt sich für jede Komponente m nach Gleichung (4.24) aus der Summe der komponentenzugehörigen Basisfehlerraten aller Bauteile n, die einen Beitrag zur Verletzung des Sicherheitsziels leisten (λ_n). Dabei muss darauf geachtet werden, dass keine Basisfehlerrate mehrfach berücksichtigt wird, da dies sonst eine unzulässige Verfälschung zur unsicheren Seite zur Folge hat.

$$\lambda_{SR-m} = \sum_{1}^{n} \lambda_n \tag{4.24}$$

4.2.4.2 Ermittlung fehlerspezifischer Diagnosedeckungsgrad

Bestimmte Komponentenfehler können sowohl durch die Eigendiagnose der Komponente DC_{Fx-K}, als auch durch Diagnosen auf Systemebene (Systemdiagnosen) DC_{Fx-S} erkannt werden. Die Diagnosedeckungsgrade der Komponenten- sowie der Systemebene lassen sich in Anlehnung an [ISO26262-5, Annex D] ermitteln. Die Diagnosen der Komponenten- sowie Systemebene ergänzen sich zum Gesamtdiagnosedeckungsgrad des Komponentenfehlers DC_{Fx-t} (E5), der sich nach Abbildung 4.26 ermitteln lässt. Die komponenteninternen Diagnosen wirken auf einzelne Bauteilfehler, die zum Komponentenfehler Fx führen. Dementsprechend wird jedem Bauteilfehler Bx ein Diagnosedeckungsgrad zugewiesen. Der Diagnosedeckungsgrad der Systemdiagnose wirkt dabei auf den Komponentenfehler Fx und unterscheidet die einzelnen Bauteilfehler nicht. Um den Gesamtdiagnosedeckungsgrad DC_{Fx-t} des Komponentenfehlers Fx zu ermitteln wird in diesem Beispiel jedem Bauteilfehler das Maximum des Diagnosedeckungsgrades aus komponenteninterner Diagnose und Systemdiagnose zugewiesen. Anschließend wird der Fehlerbaum des Komponentenfehlers Fx mit den Diagnosedeckungsgraden des Gesamtdiagnosedeckungsgrades erneut berechnet und der Gesamtdiagnosedeckungsgrad DC_{Fx-t} nach Gleichung (4.25) abgeleitet.

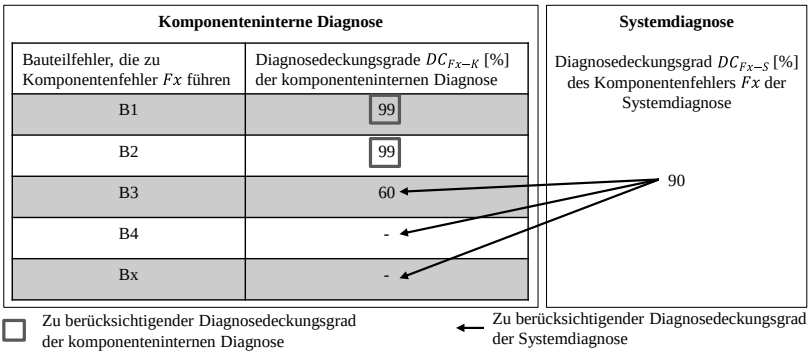


Abbildung 4.26: Beispielhafte Ermittlung des Gesamtdiagnosedeckungsgrades DC_{Fx-t} des Komponentenfehlers Fx aus Komponentendiagnose DC_{Fx-K} und Systemdiagnose DC_{Fx-S}

$$DC_{Fx-t} = 1 - \frac{F_{w-DC_t}(t_{life})}{F_{\frac{w}{o}-DC}(t_{life})} \tag{4.25}$$

DC_{Fx-t}	Gesamtdiagnosedeckungsgrades des Komponentenfehlers Fx
$F_{w-DC_t}(t_{life})$	Fehlerwahrscheinlichkeit des Komponentenfehlers unter Berücksichtigung der komponenteninternen und Systemdiagnose Diagnosedeckungsgrade
$F_{\frac{w}{o}-DC}(t_{life})$	Fehlerwahrscheinlichkeit des Komponentenfehlers ohne Berücksichtigung von Diagnosen
t_{life}	Lebensdauer des Systems

4.2.4.3 Quantifizierung des Systemparameters $SysP_{erk}$

Das Vorgehen zur Quantifizierung der Faktoren $E_{nied}, E_{mitt}, E_{hoch}$ wird anhand Abbildung 4.27 vorgestellt. Für den Systemparameter $SysP_{erk}$ wird angenommen, dass dieser normalverteilt ist. Die zugehörige Dichtefunktion wird als $f(x)$ bezeichnet. Um die Faktoren $E_{nied}, E_{mitt}, E_{hoch}$ quantifizieren zu können, werden die Stützstellen Xmin, X1, X2 und Xmax definiert. Xmin stellt den Wert des Systemparameters dar, welcher das System mindestens einnimmt, um die Nennfunktion zu realisieren. Im Energiebordnetz ist dies die Last, die im Betrieb zur Realisierung der Fahrzeugnennfunktion mindestens vorherrscht. Xmax definiert den Wert des Systemparameters, der im Betrieb maximal vorherrschen kann. Im Energiebordnetz ergibt sich dieser Wert sobald alle Verbraucher aktiv sind. Durch die Stützstellen ergeben sich die Bereiche $SysP_{erk}$ –niedrig, -mittel und -hoch. Die Bereiche entsprechend der Häufigkeit, mit der sich der Systemparameter in dem zugehörigen Intervall aufhält. Werden auf der Ordinate der Dichtefunktion relative Häufigkeiten verwendet, so ergibt deren Fläche immer eins [BER04]. In diesem Fall ist Formel (4.20) gültig. Somit ergeben sich die Faktoren $E_{nied}, E_{mitt}, E_{hoch}$ aus den Bereichen $SysP_{erk}$ –niedrig, -mittel und –hoch näherungsweise nach Formel (4.26).

$$E_{nied} = \int_{-\infty}^{X1} f(x)dx\,;\; E_{mitt} = \int_{X1}^{X2} f(x)dx\,;\; E_{hoch} = \int_{X2}^{+\infty} f(x)dx \qquad (4.26)$$

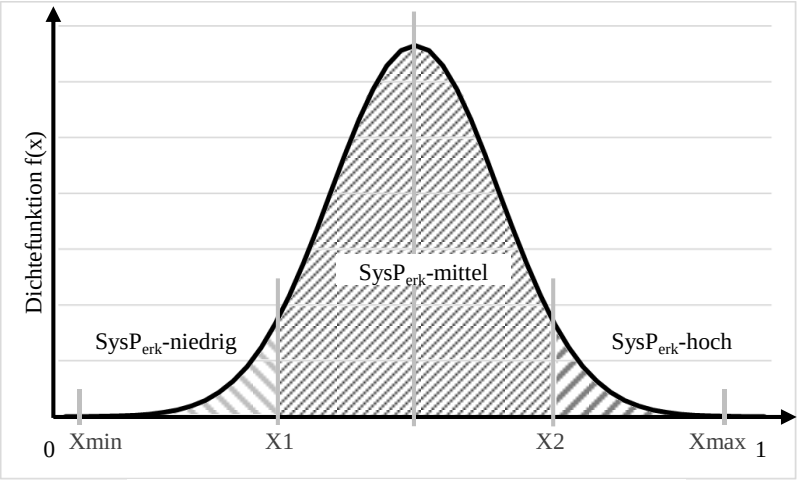


Abbildung 4.27: Mögliche Dichtefunktion der Verteilung des Systemparameters SysP$_{erk}$

4.2.4.4 Berechnung der ISO 26262 Metriken der Systemebene

Die Basis zur Berechnung der ISO 26262 Metriken stellt die Berechnung der Zustandswahrscheinlichkeiten des Markov-Modells durch das Lösen des Differentialgleichungssystems dar. Auf diese Weise sind die Berücksichtigung zufällig verteilter (exponentialverteilte) Fehler (E1) sowie die Berechnungen mit niedrigen Fehlerraten (E2) möglich. Der Aufbau des Markov-Modells ist dabei in Kapitel 4.2.3 beschrieben. Für das Beispiel aus Abbildung 4.11 ergibt sich Gleichung (4.27) mit dem Startvektor $p(0)$ und dem Zeitintervall t. Der Startvektor beschreibt die Wahrscheinlichkeitsverteilung der Markov-Zustände zu Beginn der Analyse für das fehlerfreie System. Die Übergangsraten werden nach Kapitel 4.2.4.1 ff berechnet. Als Ergebnis erhält man die Wahrscheinlichkeiten der Markov-Zustände nach der Zeit $t_{mission}$.

$$\begin{bmatrix} \frac{d}{dt}p_1(t) \\ \frac{d}{dt}p_2(t) \\ \frac{d}{dt}p_3(t) \\ \frac{d}{dt}p_4(t) \\ \frac{d}{dt}p_5(t) \\ \frac{d}{dt}p_6(t) \\ \frac{d}{dt}p_7(t) \\ \frac{d}{dt}p_8(t) \\ \frac{d}{dt}p_9(t) \\ \frac{d}{dt}p_{10}(t) \\ \frac{d}{dt}p_{11}(t) \\ \frac{d}{dt}p_{12}(t) \end{bmatrix} = \begin{bmatrix} -\lambda_{1\dots n} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ DC_{1t}\cdot\lambda_1 & -\frac{1}{TTSS}-\lambda_{2\dots n} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{TTSS} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_{2\_n} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ (1-DC_{1t})\cdot\lambda_1 & 0 & 0 & 0 & -\lambda_{2\dots n} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_{2\dots n} & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ DC_{3t}\cdot\lambda_3 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{TTSS}-\lambda_{1,2,4\dots n} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{TTSS} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{1,2,4\dots n} & 0 & 0 & 0 \\ (1-DC_{3t})\cdot\lambda_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_{4\dots n} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} p_1(t) \\ p_2(t) \\ p_3(t) \\ p_4(t) \\ p_5(t) \\ p_6(t) \\ p_7(t) \\ p_8(t) \\ p_9(t) \\ p_{10}(t) \\ p_{11}(t) \\ p_{12}(t) \end{bmatrix} \tag{4.27}$$

$$\text{mit } p(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \text{ und } t = [0, t_{mission}]$$

Für die Berechnung der PMHF (probabilistic metric for random hardware failures) werden die Wahrscheinlichkeiten der Zustände $F(t_{mission})$ aufsummiert, bei denen es zur Verletzung des Sicherheitsziels kommt. Die PMHF ergibt sich nach Gleichung (4.28) aus der Division der Summe der Wahrscheinlichkeiten $F(t_{mission})$ durch die Betriebsdauer $t_{mission}$.

$$PMHF = \frac{F(t_{mission})}{t_{mission}} \tag{4.28}$$

Zur Berechnung der SPFM (single point fault metric) und der LFM (latent fault metric) werden die Markov-Zustände nach den ISO 26262 Fehlerkategorien SPF, RF und MPF_{latent} klassifiziert. In die jeweiligen Fehlerkategorien der ISO 26262 gehen nun die

- λ_{SPF}: Markov-Zustand 7 (siehe Abbildung 4.11)

- λ_{RF}: Markov-Zustand 11 (siehe Abbildung 4.11)
- $\lambda_{MPF-latent}$: Markov-Zustand 5+6 (siehe Abbildung 4.11)

Die Wahrscheinlichkeiten aller zu einer Fehlerkategorie gehörenden Zustände werden addiert und die zugehörigen Fehlerraten nach der umgeformten Gleichung der Exponentialverteilung (4.29) berechnet. Die Berechnung der SPFM erfolgt nach Gleichung (4.30) und die Berechnung der LFM nach Gleichung (4.31), siehe Kapitel 2.3.1.3.

$$\lambda = \frac{-\ln(1 - F(t_{mission}))}{t_{mission}} \tag{4.29}$$

$$SPFM = 1 - \frac{\sum \lambda_{SPF} + \lambda_{RF}}{\sum \lambda_{SR-gesamt}} \tag{4.30}$$

$$LFM = 1 - \frac{\sum \lambda_{MPF_{latent}}}{\sum(\lambda_{SR-gesamt} - \lambda_{SPF} - \lambda_{RF})} \tag{4.31}$$

Des Weiteren wird die Gesamtfehlerrate der sicherheitsrelevanten Hardwareelemente $\lambda_{SR-gesamt}$ für die Metriken-Berechnung benötigt. Zur Berechnung der Gesamtfehlerrate der sicherheitsrelevanten Hardwareelemente $\lambda_{SR-gesamt}$ werden die Basisfehlerraten der Hardware-Bauteile der Fehlerbaumanalysen verwendet, die zur Quantifizierung der Übergangsraten der Markov-Analyse eingesetzt werden, siehe λ_{SR-m} aus Kapitel 4.2.4.1 Aus den Simulationsergebnissen wird abgeleitet, ob ein Komponentenfehler zur Verletzung des Sicherheitsziels beiträgt oder nicht. $\lambda_{SR-gesamt}$ ergibt sich aus der Summe aller λ_{SR-m}, deren Fehler einen Beitrag zur Verletzung des Sicherheitsziels haben, siehe Gleichung (4.32).

$$\lambda_{SR-gesamt} = \sum_{1}^{m} \lambda_{SR-m} \tag{4.32}$$

Im nächsten Schritt wird die Berechnung der ISO 26262-Metriken anhand des Markov-Graphen aus Abbildung 4.11 mit beispielhaften Werten in Abbildung 4.28 und nach Gleichung (4.33)bis (4.35) durchgeführt.

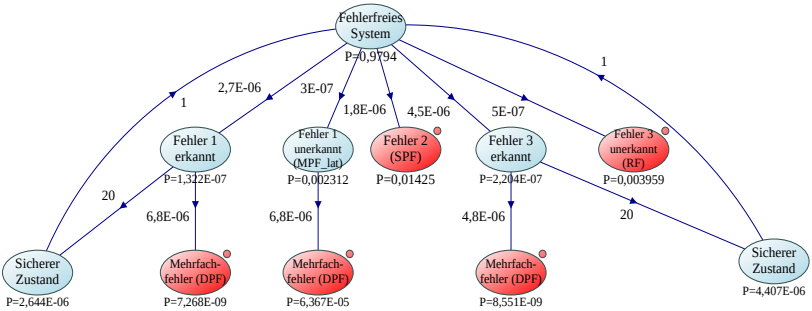


Abbildung 4.28: Ergebnisse des Markov-Graphen aus Abbildung 4.11 mit exemplarischen Übergangsraten

$$PMHF = \frac{P_{Ausfall}}{t_{mission}} \approx 2284\ FIT \tag{4.33}$$

$$SPFM = 1 - \frac{\lambda_{SPF} + \lambda_{RF}}{\lambda_{SR-gesamt}} = 1 - \frac{\left(\frac{P_{SPF} + P_{RF}}{t_{mission}}\right)}{\lambda_1 + \lambda_2 + \lambda_3} \approx 77\% \tag{4.34}$$

$$LFM = 1 - \frac{\lambda_{MPF}}{\lambda_{SR-gesamt} - (\lambda_{SPF} + \lambda_{RF})}$$

$$= 1 - \frac{\left(\frac{P_{MPF}}{t_{mission}}\right)}{\lambda_{SR-gesamt} - \left(\frac{P_{SPF} + P_{RF}}{t_{mission}}\right)} \approx 96\% \tag{4.35}$$

mit

$\lambda_1 = 3000\ FIT; DC_1 = 90\%$
$\lambda_2 = 1800\ FIT$
$\lambda_3 = 5000\ FIT; DC_3 = 90\%$
$TTSS = 3\ min$

$P_{Ausfall} = 7{,}268 \cdot 10^{-9} + 6{,}367 \cdot 10^{-5} + 1{,}425 \cdot 10^{-2}$
$+ 8{,}551 \cdot 10^{-9} + 3{,}959 \cdot 10^{-3}$

$t_{life} = 8000h$

$P_{SPF} + P_{RF} = 1{,}425 \cdot 10^{-2} + 3{,}959 \cdot 10^{-3}$

$P_{MPF} = 1{,}322 \cdot 10^{-7} + 7{,}268 \cdot 10^{-9} + 2{,}312 \cdot 10^{-3}$
$+6{,}367 \cdot 10^{-5} + 2{,}204 \cdot 10^{-7} + 8{,}551 \cdot 10^{-9}$

4.2.5 Erreichung Ziel Z4: Ermittlung der einflussreichsten Parameter

Werden die Zielwerte der ISO 26262-Metriken nicht erreicht, folgt die iterative Optimierung des Systems. Um eine effiziente Optimierung durchführen zu können, werden die Fehlerklassen bzw. Fehlerzustände, die den größten Einfluss auf die Metriken haben, ausgegeben.

Der absolute Anteil I_{FKL-SA_1-PMHF}, den eine Fehlerklasse an der PMHF ausmacht, wird nach Gleichung (4.36) berechnet. Dabei wird die Wahrscheinlichkeit $F_{FKL-SA_1}(t_{mission})$, die der zu analysierenden Fehlerklasse zugeordnet werden kann ermittelt und durch die Gesamtausfallwahrscheinlichkeit $\sum F_{FKL-SA}(t_{mission})$ geteilt. Dieser Quotient wird mit der PMHF multipliziert.

$$I_{FKL-SA_1-PMHF} = \frac{F_{FKL-SA_1}(t_{life})}{\sum F_{FKL-SA}(t_{life})} \cdot PMHF \tag{4.36}$$

Für die Berechnung der SPFM haben nur SPF (single point faults) und RF (residual faults) eine Bedeutung. Dementsprechend kann der Einfluss auf die SPFM nur für Fehlerklassen, die SPF oder RF zugeordnet werden können, ermittelt werden.

Der relative Einfluss einer Fehlerklasse auf die SPFM $I_{FKL-SA_1-SPFM_{rel}}$ kann nach Gleichung (4.37) berechnet werden. Dabei wird die Wahrscheinlichkeit $F_{FKL-SA_1}(t_{mission})$, die die Fehlerklasse an der SPFM hat, durch die Gesamtheit der Wahrscheinlichkeit von RF und SPF $(\sum F_{RF}(t_{mission}) + \sum F_{SPF}(t_{mission}))$ geteilt. Um den Anteil in Prozent zu erhalten, wird das Ergebnis mit 100% multipliziert.

Den absoluten Anteil $I_{FKL-SA_1-SPFM_{abs}}$, den die betrachtete Fehlerklasse in Prozentpunkten an der SPFM ausmacht, wird nach Gleichung (4.38) berechnet. Dabei wird der relative Anteil der Fehlerklasse $I_{FKL-SA_1-SPFM_{rel}}$ nach Gleichung (4.37) mit den zu 1 fehlenden Prozentpunkten der SPFM multipliziert.

$$I_{FKL-SA_1-SPFM_{rel}} = \frac{F_{FKL-SA_1}(t_{life})}{\sum F_{RF}(t_{life}) + \sum F_{SPF}(t_{life})} \cdot 100\% \tag{4.37}$$

$$I_{FKL-SA_1-SPFM_{abs}} = I_{FKL-SA_1-SPFM_{rel}} \cdot (1 - SPFM) \tag{4.38}$$

Die Berechnung des Einflusses einer Fehlerkasse an der LFM ist analog zur SPFM Berechnung durchzuführen. Der relative Anteil einer Fehlerklasse an der LFM ergibt sich nach Gleichung (4.39), der absolute Anteil nach Gleichung (4.40).

$$I_{FKL-SA_1-LFM_{rel}} = \frac{F_{FKL-SA_1}(t_{life})}{\sum F_{MPF_{latent}}(t_{life})} \cdot 100\% \tag{4.39}$$

$$I_{FKL-SA_1-LFM_{abs}} = I_{FKL-SA_1-LFM_{rel}} \cdot (1 - LFM) \tag{4.40}$$

In einem weiteren Schritt kann mittels Sensitivitätsanalyse der Einfluss von Parametervariationen auf die Metriken analysiert werden.

5 Validierung der Methode am Beispiel eines fehlertoleranten Energiebordnetzes

Die Validierung der Methode aus Kapitel 4 wird in diesem Kapitel anhand eines Energiebordnetzes für automatisiertes Fahren durchgeführt. Dazu wird im ersten Unterkapitel die Vorgehensweise vorgestellt. In den darauffolgenden Unterkapiteln werden die einzelnen Schritte der Vorgehensweise näher beleuchtet. Die verwendeten Zahlenwerte sind von den realen Werten abweichend.

5.1 Vorgehensweise – Entwicklung Energiebordnetz für automatisiertes Fahren

Die in Abbildung 5.1 dargestellte Vorgehensweise basiert auf dem V-Modell der ISO 26262, wobei der Fokus auf der Entwicklung des fehlertoleranten Energiebordnetzes zur Befähigung der automatisierten Fahrfunktionen liegt. Im ersten Arbeitsschritt „Definition und Analysen auf Fahrzeugebene“ werden die Rahmendaten des automatisierten Fahrzeugs definiert, sowie die Gefährdungsanalyse und Risikobewertung durchgeführt. Auf Basis des ersten Arbeitsschritts wird im zweiten Arbeitsschritt als Beispiel eine vorläufige Annahme zur Realisierung der Bremsfunktion getroffen und die Attribute der Teilsysteme werden definiert. Im dritten Arbeitsschritt wird eine vorläufige Energiebordnetz-Architekturannahme getroffen und die Attribute an das Energiebordnetz werden abgeleitet. Im vierten Arbeitsschritt, der Erstellung der Fehlerdatenbank, werden die relevanten Energiebordnetzfehler aufgelistet. Mittels Sicherheitskonzept wird im fünften Arbeitsschritt der Umgang mit Fehlern festgelegt. Anschließend werden die Anforderungen des Energiebordnetzes an die Energiebordnetz-Komponenten im sechsten Arbeitsschritt abgeleitet. Komponenten, die nicht bereits auf dem Markt erhältlich sind, werden im siebten Arbeitsschritt neu entwickelt. Anschließend wird in Arbeitsschritt acht eine Fehlerkombinatorik aufgebaut. Im neunten Arbeitsschritt, auf dem rechten Ast des V-Modells, werden die Komponentenfehler mittels Fehlerbaumanalyse quantifiziert. Das

Simulationsmodell wird im zehnten Arbeitsschritt aufgebaut und die Fehler-Simulation durchgeführt. Anschließend wird in Arbeitsschritt elf das Energiebordnetz mittels ISO 26262 Metriken bewertet. Erreicht das Energiebordnetz die vorgegebenen Zielwerte nicht, werden in Arbeitsschritt zwölf iterativ Maßnahmen definiert und implementiert, bis die Zielwerte erreicht werden.

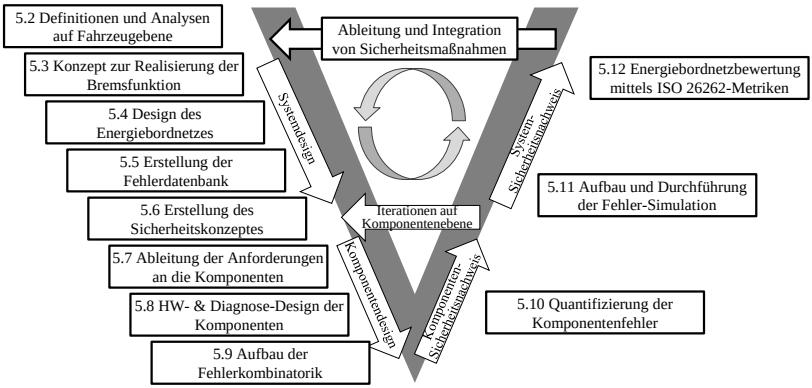


Abbildung 5.1:Vorgehensweise zur Bewertung von Energiebordnetztopologien für automatisiertes Fahren

5.2 Definitionen und Analysen auf Fahrzeugebene

Im Folgenden wird ein Oberklassefahrzeug mit Verbrennungsmotor analysiert. Dieses ist mit einem Autobahnpiloten der Automatisierungsstufe drei ausgestattet. Mittels Gefährdungsanalyse und Risikobewertung werden die Sicherheitsziele und deren Attribute ermittelt. Als Beispiel eines Sicherheitszieles wird die „Vermeidung eines unterbremsten Fahrzeuges“ analysiert. Das Sicherheitsziel „Vermeide Unterbremsung des Fahrzeugs“ wird mit ASIL D bewertet. Da es sich um ein System mit Automatisierungsstufe drei handelt, muss dieses im automatisierten Fahrbetrieb vom Fahrer nicht dauerhaft überwacht werden („eyes-off“ System). Der Fahrer muss in der

Lage sein, das Fahrzeug im Fehlerfall zu übernehmen um dieses mittels mechanischem Durchgriff sicher abzustellen.

Das Fahrzeug darf dem Fahrer dabei nicht in gefährlichen bzw. unüberschaubaren Situationen übergeben werden, da in diesem Fall die Unfallgefahr steigt. Es wird in diesem Fall davon ausgegangen, dass der Fahrer nicht als Rückfallebene zur Verfügung steht und das Fahrzeug den sicheren Zustand am Fahrbahnrand selbsttätig im Rahmen einer Emergency Operation erreicht, Definition siehe Kapitel 2.3.1. Das Energiebordnetz muss für diesen Fall so ausgelegt werden, dass der sichere Zustand am Fahrbahnrand im Fehlerfall immer erreicht werden kann. Um dies gewährleisten zu können, müssen Hindernisse in der Rückfallebene erkannt und umfahren werden. Die Dauer des Übergangs in den sicheren Zustand wird auf maximal vier Minuten festgelegt. Die Fehlertoleranzzeit, welche ein unterbremstes Fahrzeug toleriert werden kann, wird auf 400 ms festgelegt. Die Fehlerrate, welche das Sicherheitsziel nicht überschreiten darf, wird auf 10 FIT definiert. Die nachfolgend genannten Analyseschritte werden für alle Sicherheitsziele durchgeführt.

Sicherheitsziel:
Vermeide unterbremstes Fahrzeug

Attribute	
ASIL	D
Fehlertoleranzzeit	400 ms
Sicherer Zustand inkl. Emergency Operation	Fahrzeugstillstand am Fahrbahnrand
Zul. Fehlerrate	10 FIT

Abbildung 5.2: Attribute des Sicherheitsziels „Vermeide unterbremstes Fahrzeug“

5.3 Konzept zur Realisierung der Bremsfunktion

Die Wirkkette, die zur Vermeidung eines unterbremsten Fahrzeugs beim automatisierten Fahren führt, ist in Abbildung 5.3 dargestellt. Um eine ausreichende Bremsfunktion sicherstellen zu können, müssen der Bedarf und die Intensität der Bremsung korrekt erkannt (SR1), korrekt berechnet (SR2) und kommuniziert (SR3) werden, bevor die

Bremsfunktion mittels Bremsaktuatorik umgesetzt wird (SR4). Zur Umsetzung der Bremsfunktion wird die Energieversorgung aus dem Energiebordnetz benötigt (SR5).
Die Ableitung der Anforderungen an die Funktionen bzw. Systeme, die an der Bremsfunktion beteiligt sind, wird in Kapitel 5.3.1 bis 5.3.3 durchgeführt.

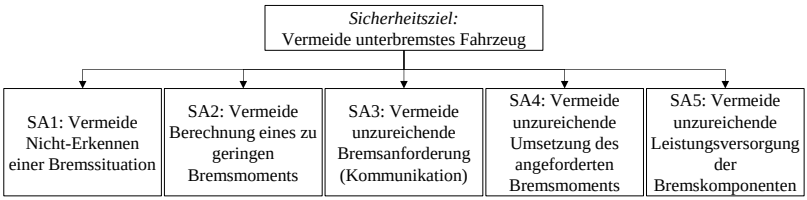


Abbildung 5.3: Wirkkette zur Vermeidung eines unterbremsten Fahrzeugs

5.3.1 Definition der zulässigen Metriken der Teilfunktionen

Nach [ISO26262-5, 9.4.2.3] darf der **PMHF** Zielwert des Sicherheitsziels direkt allen Systemen zugewiesen werden, welches das Potential haben, das Sicherheitsziel zu verletzen. Dies ist dann zulässig, wenn dadurch der Zielwert auf Itemebene um nicht mehr als eine Größenordnung (Faktor zehn) erhöht wird. Folglich wird der PMHF-Zielwert des ASIL D Sicherheitsziels in Höhe von 10 FIT auf die zum Sicherheitsziel beitragende Funktion allokiert, siehe Kapitel 2.3.1.3.
Die relativen Metriken SPFM und LFM sind für das Sicherheitsziel nach Tabelle 5.1 definiert, siehe Kapitel 2.3.1.3. Die Zielwerte der relativen Metriken werden direkt an das Energiebordnetz allokiert.

Tabelle 5.1: SPFM und LFM Zielwerte [ISO26262]

	SPFM	LFM
ASIL D	≥ 99 %	≥ 90 %

5.3.2 ASIL Dekomposition der Bremsfunktion

Aus Gesetzgebungssicht, nach [ECE R13-H], und zur Minderung der Sicherheitsanforderungen an die Komponenten, die an der Bremsfunktion des automatisierten Fahrzeugs beteiligt sind, wird die Bremsfunktion redundant ausgeführt. Dies hat zur Folge, dass die Bremsfunktion durch zwei unabhängige Bremssysteme realisiert wird.

Das ASIL D des Sicherheitsziels wird dementsprechend auf zwei ASIL B(D) Energieversorgungen der Bremssysteme allokiert und dekomponiert. Die sicherheitsrelevante Verfügbarkeitsanforderung „Stelle Energie und Leistungsversorgung innerhalb spezifizierter Spannungsgrenzen sicher“ wird dabei an beide Teilnetze allokiert. Die Spannungsgrenzen in jedem Teilnetz ergeben sich dabei aus den Spannungsgrenzen der zu versorgenden sicherheitsrelevanten Verbraucher, in diesem Fall den Bremssystemen. Zusätzliche Anforderungen können sich aus weiteren Normen oder Fahrzeughersteller-spezifischen Standards ergeben, z.B. [ISO 16750-2], [VW 80000], [MBN LV 124-2] oder [BMW GS 95024-3-1].

Voraussetzung für die ASIL-Dekompositionen ist dabei die ausreichende Unabhängigkeit der Teilbordnetze, um Common-Cause-Fehler zu vermeiden, welche die Redundanz aushebeln Die Unabhängigkeit muss im weiteren Verlauf der Sicherheitsanalyse mittels Analyse abhängiger Fehler („analysis of dependent failures“ [ISO26262-9, 7]) nachgewiesen werden.

5.3.3 Fehlertoleranzzeit der Bremsfunktion

Die Fehlertoleranzzeit der Fahrzeugebene von 400 ms wird direkt an die beteiligten Anforderungen aus Abbildung 5.3 vererbt und zwischen diesen aufgeteilt, sodass Gleichung (5.1) gilt. Für das Energiebordnetz ergibt sich eine Sonderrolle, die in Kapitel 5.4.3 beschrieben ist.

$$FTZ_{Sicherheitsziel} = FTZ_{SA1} + FTZ_{SA2} + FTZ_{SA3} + FTZ_{SA4} \qquad (5.1)$$

In den nachfolgenden Kapiteln wird das Vorgehen zur Bewertung fehlertoleranter Systeme am Beispiel Energiebordnetz näher betrachtet.

5.4 Design des Energiebordnetzes

Wie in Kapitel 5.3 beschrieben wird die Fehlertoleranz des Fahrzeuges bezüglich der Energieversorgung mittels zwei redundanter ASIL B(D) Energiebordnetze sichergestellt. Eine erste Architekturannahme eines Energiebordnetzes (preliminary architectural assumption) zur Realisierung der automatisierten Fahrfunktionen, die auf Basis von Expertenbewertung ausgewählt wurde, ist in Abbildung 5.4 dargestellt.

Dabei handelt es sich um ein 48V/12V Energiebordnetz. Auf der 48V-Seite befindet sich eine elektrische Maschine, eine LiIon-Batterie sowie nicht-sicherheitsrelevante 48V-Verbraucher. Das 12V Energiebordnetz besteht aus Teilnetz Kl.30-1 und Teilnetz Kl.30-2. Teilnetz Kl.30-1 ist mittels DC/DC-Wandler an das 48V-Teilnetz angekoppelt und enthält die nicht-sicherheitsrelevanten 12V-Verbraucher, eine Batterie, die von einem Batteriesensor überwacht wird, und eine Gruppe sicherheitsrelevanter Verbraucher. Die sicherheitsrelevanten Verbraucher werden zur Realisierung der Wirkkette des Sicherheitsziels „Vermeide unterbremstes Fahrzeug“ benötigt (siehe Abbildung 5.3). Teilnetz Kl.30-2 ist über einen 12V/12V DC/DC-Wandler an Kl.30-1 angeschlossen und enthält eine 12V Batterie, die von einem Batteriesensor überwacht wird, sowie die redundante Gruppe sicherheitsrelevanter Verbraucher. Die sicherheitsrelevanten Verbraucher, die zur Realisierung anderer Sicherheitsziele benötigt werden, werden analog integriert. Es wird eine erste Annahme zur Dimensionierung der Energiequellen-, -übertrager und –speicher getroffen, die u.a. durch Spannungsstabilitäts- und Ladebilanzsimulation validiert wird.

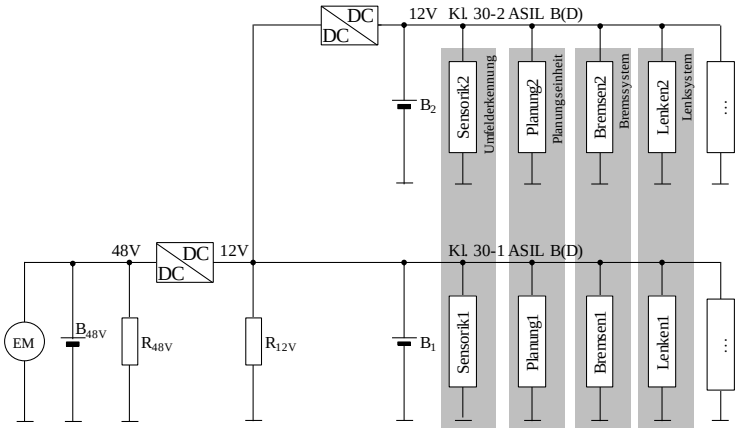


Abbildung 5.4: Beispiel-Energiebordnetz zur Realisierung der automatisierten Fahrfunktion

5.4.1 Definition der zulässigen PMHF auf Energiebordnetzebene

Das PMHF-Budget des Energiebordnetzes ergibt sich aus dem Minimalwert der PMHF-Budgets der Sicherheitsziele, zu deren Verletzung das Energiebordnetz beitragen kann. Es wird davon ausgegangen, dass das in Kapitel 5.3.1 zugewiesene PMHF-Budget von 10 FIT hinsichtlich der Sicherheitsanforderung „Stelle Energie und Leistung innerhalb spezifizierter Spannungsgrenzen sicher“, der schärfsten Anforderung entspricht. Das PMHF-Budget wird nun auf die Teilnetze des Energiebordnetzes heruntergebrochen, siehe Abbildung 5.5. Es wird beispielhaft ein zulässiges Budget von sechs FIT für Common-Cause-Fehler sowie 700 FIT je Teilnetz Kl.30-1 und Kl.30-2 abgeleitet.

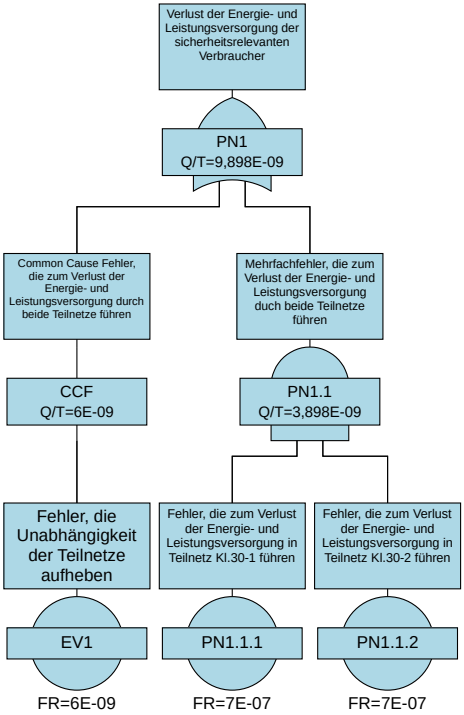


Abbildung 5.5: Mögliche FIT-Budgetierung im Energiebordnetz

Die einzuhaltenden Zielwerte der relativen Metriken ergeben sich aus dem Maximum der an das Energiebordnetz allokierten Werte. In diesem Fall werden die Zielgrößen des Bremssystems festgelegt, siehe Kapitel 5.3.1 und Tabelle 5.2.

Tabelle 5.2: SPFM und LFM Zielwerte [ISO26262]

	SPFM	LFM
ASIL D	≥ 99 %	≥ 90 %

Beim Sicherheitsnachweis in Kapitel 5.12 muss nachgewiesen werden, dass die zulässigen Metriken der Energiebordnetzebene erreicht werden.

5.4.2 ASIL Anforderungen an das Energiebordnetz

Die ASIL Anforderungen an die Teilnetze des Energiebordnetzes ergeben sich aus dem maximalen ASIL der an den Teilnetzen angeschlossenen Komponenten. Teilnetz Kl.30-1 und Teilnetz Kl.30-2 sind ASIL B(D) Teilnetze, während das 48V-Teilnetz QM eingestuft ist.

5.4.3 Definition der Fehlertoleranzzeiten im Energiebordnetz

Wie in Kapitel 5.3 beschrieben hat das Energiebordnetz eine Sonderrolle hinsichtlich der Fehlertoleranzzeit. In Abbildung 5.6 wird anhand der sicherheitsrelevanten Beispielkomponente beschrieben, wie es zur Verletzung der Sicherheitsanforderungen durch das Energiebordnetz kommt. Die betrachtete Komponente erfüllt die volle Funktionalität zwischen 8 V und 16 V. Werden die definierten, komponentenspezifischen Spannungs-Zeit-Grenzen verlassen, führt dies zum Verlust der sicherheitsrelevanten Funktion der Komponente. Steht dabei die Funktion der Komponente länger, als es die Fehlertoleranzzeit des zugehörigen Sicherheitsziels erlaubt, nicht zur Verfügung, führt dies zur Verletzung der an die Komponente gestellten Sicherheitsanforderung.
Für die Unterspannung kann es in folgenden Fällen zur Verletzung der Sicherheitsanforderung kommen:

- Fall 1: Fällt die Spannung für eine Dauer von größer 100µs unter 4 V, tritt ein Hardware-Reset auf. Unter der Annahme, dass die Dauer zur Wiederherstellung der Funktionsfähigkeit der Komponente nach einem Neustart (power-on-reset) deutlich länger ist, als es die Fehlertoleranzzeit des Sicherheitsziels zulässt, müssen die Hardware-Resets der sicherheitsrelevanten Komponenten verhindert werden. Die Fehlertoleranzzeit für die Hardware-Reset-Spannungsschwelle ergibt sich daher nach Gleichung (5.2)
- Fall 2: Fällt die Spannung in das Intervall zwischen 4V und 6V, steht die Funktion der Komponente bereits nicht mehr im geforderten Maße zur Verfügung, siehe Fall 3. Um einen weiteren Spannungseinbruch im Energiebordnetz zu vermeiden, schaltet die Komponente ihre Funktion nach der Zeit $t_{SW-R-6V}$ in diesem Spannungsintervall ab. Die Logik der Komponente

bleibt weiterhin aktiv, sodass die Komponente ihre Funktion nach Überschreiten einer bestimmten Spannung $U_{Wiedereinschalt} = 9V$ innerhalb der Zeit $t_{Wiedereinschalt} = 10\,ms$ wieder einschaltet. Die Fehlertoleranzzeit für die SW-Abschaltung ergibt sich dabei nach Gleichung (5.3)

- Fall 3: Fällt die Spannung an der Komponente in das Spannungsintervall von 6 V bis 8 V für eine Zeit größer t_{VdF-8V}, wird die Funktion aufgrund der unzureichenden Leistungsabgabe des Energiebordnetzes degradiert. Die Funktion wird dementsprechend nicht mehr im geforderten Umfang ausgeführt. Es kann davon ausgegangen werden, dass die Funktion der Komponente beim Wiedereintritt in den Normalspannungsbereich (8 V bis 16 V) sofort wieder zur Verfügung steht. Folglich gilt für die Fehlertoleranzzeit in diesem Spannungsbereich Gleichung (5.4)

Ebenso kann eine Überspannung zur Verletzung der Anforderungen führen. Da Überspannungen analog zu den Unterspannungsgrenzen zu sehen sind, werden diese bis auf folgenden Sonderfall nicht näher betrachtet:

- Fall 4: Steigt die Spannung für länger als t_{FF}über 27 V, kann es bei manchen sicherheitsrelevanten Komponenten nicht nur zum Verlust der sicherheitsrelevanten Funktion, sondern auch zur Fehlfunktion kommen, da die Überspannung zu Überlastung und Beschädigungen in der Komponente führen kann. Diese Fehlfunktion führt ggfs. auch dazu, dass die Funktion potentieller Redundanzen nicht mehr gewährleistet werden kann, wodurch Sicherheitsziele direkt verletzt werden können.

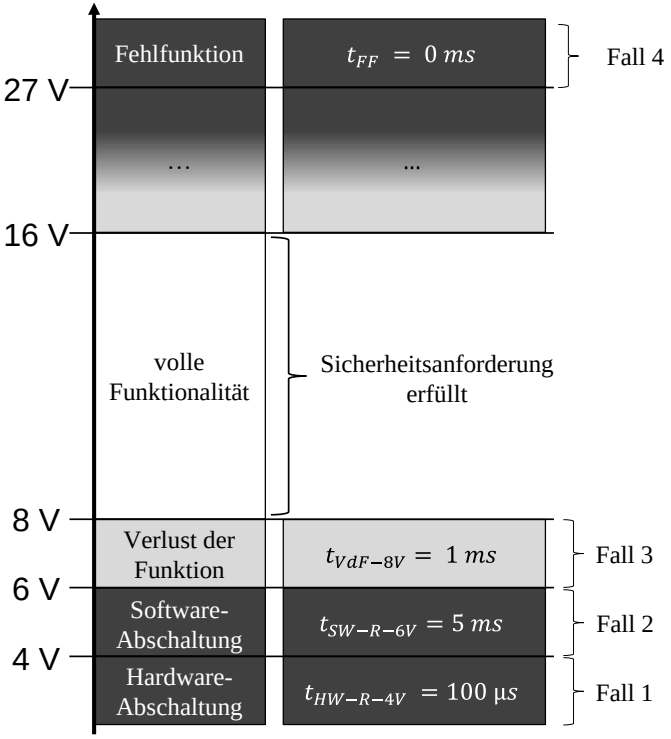


Abbildung 5.6: Funktionsfähigkeit einer Beispielkomponente über der Versorgungsspannung

$$t_{zul}(< 4V) = t_{HW-R-4V} \tag{5.2}$$

$$t_{zul}(4V \ldots 6V) = FTZ_{Sicherheitsziel} - t_{Wiedereinschalt} \tag{5.3}$$

$$t_{zul}(6V \ldots 8V) = FTZ_{Sicherheitsziel} \tag{5.4}$$

Die Spannungs-Zeit-Kombinationen, die im jeweiligen Teilnetz vermieden werden müssen, ergeben sich aus den Überlagerungen der Spannungs-Zeit-Kombinationen aller sicherheitsrelevanten Komponenten, sowie der beschriebenen Normen (siehe Kapitel 5.3.2). Werden die minimalen Spannungs-Zeit-Kombinationen der Komponente mit den zugehörigen ASIL der Komponentenfunktionen kombiniert, ergibt sich Abbildung 5.7 für Teilnetz Kl.30-1 und Abbildung 5.8 für Teilnetz Kl.30-2.

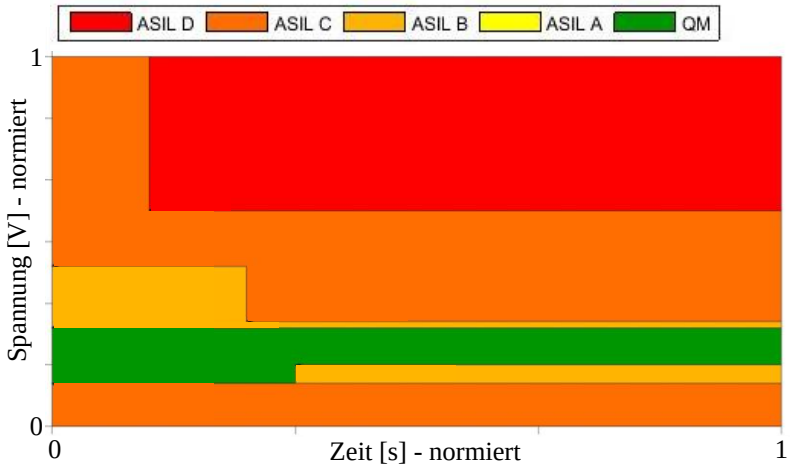


Abbildung 5.7: Normiertes ASIL-Spannung-Zeit Diagramm für Teilnetz Kl.30-1

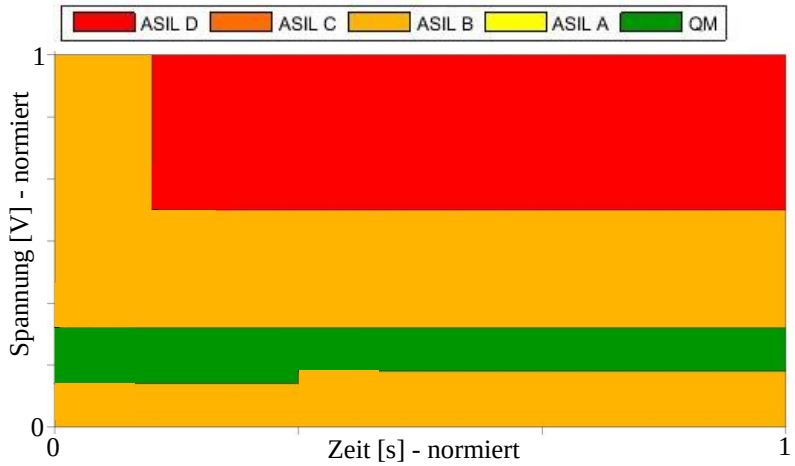


Abbildung 5.8: Normiertes ASIL-Spannung-Zeit Diagramm für Teilnetz Kl.30-2

5.4.4 Definition der sicheren Zustände

Die zugehörigen sicheren Zustände sind in Kapitel 5.3 definiert. Kommt es zu einem Fehler im Energiebordnetz, wird der Fahrer zur Übernahme des Fahrzeuges aufgefordert. Übernimmt er das Fahrzeug nicht innerhalb von zehn Sekunden, wird der Übergang in den sichern Zustand aus dem anderen Teilnetz angestoßen. Das Fahrzeug wird daraufhin auf dem Standstreifen abgestellt. Die Dauer des Übergangs wird auf vier Minuten festgelegt, wie in Kapitel 5.2 beschrieben.

5.5 Erstellung der Fehlerdatenbank

Grundlage zur Analyse der funktionalen Sicherheit ist die Fehlerdatenbank. Die Fehlerdatenbank wird auf Basis von FMEAs bestehender Komponenten und Funktionsanalysen aufgebaut, um systematisch die Vollständigkeit der Fehler zu gewährleisten. Neu entwickelte Komponenten werden iterativ ergänzt. Die Struktur der Fehlerdatenbank und ein Ausschnitt der Fehlerklassen des Teilnetzes Kl.30-2 der Topologie aus Abbildung 5.4 sind in Abbildung 5.9 dargestellt. Die zu einer Fehlerklasse gehörenden Fehler und Sicherheitsmechanismen sind in Abbildung 5.10 dargestellt.

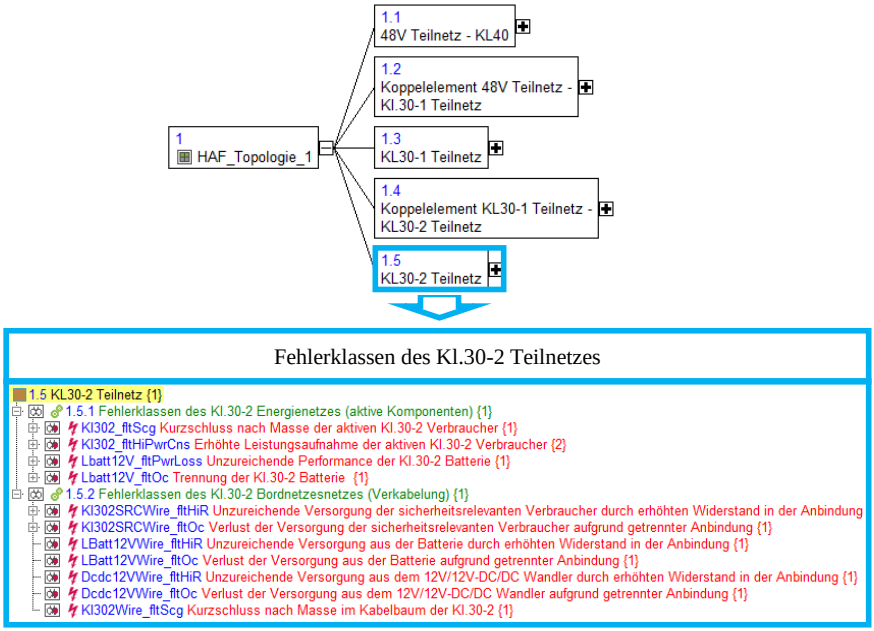


Abbildung 5.9: Struktur der Fehlerdatenbank und Ausschnitt von Fehlerklassen

Der Nutzen der Fehlerdatenbank umfasst:

- Die exakte Fehlerdefinition und Gewährleistung einer durchgängigen Benennung für die ASIL Dekomposition, die quantitative Bewertung der Komponentenebene, die Fehlerkombinatorik, die Markov-Analyse und die Fehlerinjektionssimulation.

- Die systematische, vollständige Ermittlung der relevanten Fehler
- Die Zusammenfassung von Fehlern zu Fehlerklassen, um die Anzahl an Zuständen in der Markov-Analyse zu begrenzen
- Die Zuordnung von Fehlern zu Fehlerklassen, um die Simulationsergebnisse sowie die Quantifizierung mittels Fehlerbaumanalyse einer Fehlerklasse zuordnen zu können
- Die Definition und Dokumentation der zu den Fehlerklassen gehörenden Sicherheitsmechanismen

Die Fehlerklassen sind Voraussetzung für die Erstellung der Fehlerkombinatorik und die automatisierte Markov-Analyse. Außerdem werden die Fehlerklassen zum Aufbau der ASIL Dekomposition verwendet.

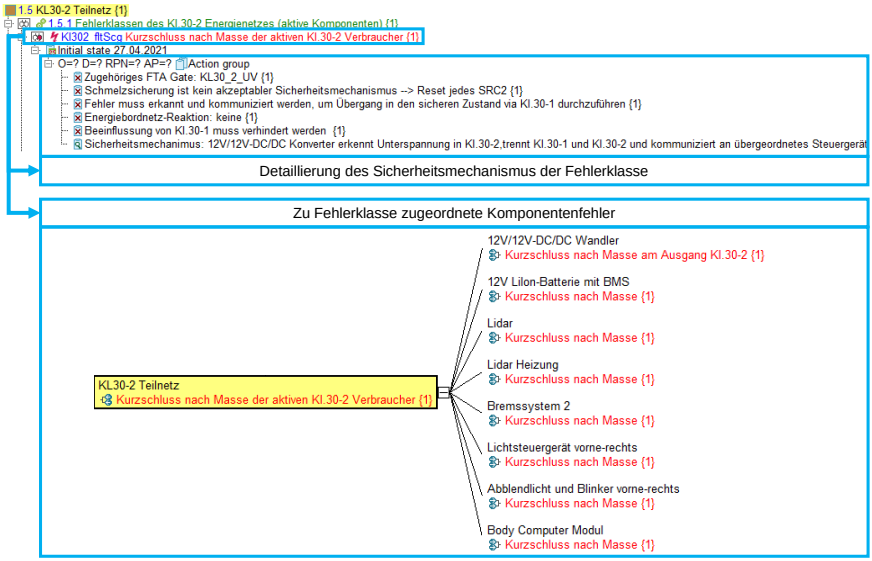


Abbildung 5.10: Zuordnung von Fehlern zur Fehlerklasse und Definition von Sicherheitsmechanismen

5.6 Erstellung des Sicherheitskonzeptes

Im Sicherheitskonzept werden die Fehlerreaktionen, die im Falle eines erkannten Fehlers durchgeführt werden, identifiziert und dokumentiert. Dabei werden die Fehlerreaktionen auf Fahrzeugebene (z.B. Stillstand auf dem Standstreifen, Fahrt bis zum nächsten Rastplatz, usw.) sowie auf Energiebordnetzebene (z.B. Lastzu- oder Lastabschaltungen, usw.) festgelegt.

5.7 Ableitung der ASIL der Komponentenebene

Auf Basis der Liste der Fehlerklassen und Sicherheitsmechanismen (Kapitel 5.5) wird für das Sicherheitsziel ein Fehlerbaum zur ASIL Dekomposition erstellt. Die Metastruktur des Fehlerbaums zur ASIL Dekomposition zur Beispieltopologie aus Abbildung 5.4 ist in Abbildung 5.11 dargestellt. Dazu werden die Spannungsgrenzen der Teilnetze Kl.30-1 und Kl.30-2 aus Abbildung 5.7 und Abbildung 5.8 berücksichtigt. Werden Spannungsgrenzen unter- bzw. überschritten, die zu Fehlfunktionen sicherheitsrelevanter Funktionen führen (z.B. Fehllenker oder fehlerhafte Auslösung des Airbags) müssen die zugehörigen Fehler mit dem höchsten ASIL des betreffenden Sicherheitsziels vermieden werden. Führt ein Fehler zum Verlust der Unabhängigkeit zwischen Teilnetz Kl.30-1 und Teilnetz Kl.30-2, zwischen denen dekomponiert werden soll, wird auch in diesem Fall das ASIL des höchsten betreffenden Sicherheitsziels direkt an die zugehörigen Fehler allokiert. Die Dekomposition des ASIL D der sicheren Energieversorgung der sicherheitsrelevanten Verbraucher auf die Teilnetze Kl.30-1 und Kl.30-2 führt zur Allokation von ASIL B(D) an jede der beiden Teilnetze.

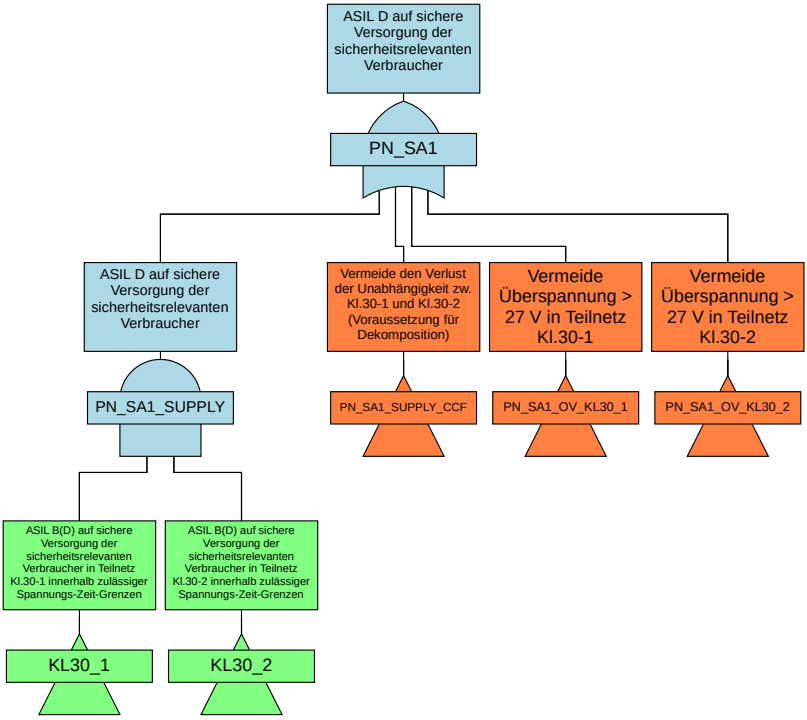


Abbildung 5.11: Metastruktur des Fehlerbaums zur ASIL Dekomposition der vorgestellten Topologie (Abbildung 5.4)

Abbildung 5.12 zeigt einen Ausschnitt des Fehlerbaums zur ASIL Dekomposition der vorgestellten Topologie aus Abbildung 5.4. Dabei wird die Energieversorgung der sicherheitsrelevanten Verbraucher in den redundanten Teilnetzen Kl.30-1 und Kl.30-2 betrachtet. Die Versorgung des Teilnetzes Kl.30-1 kann dabei entweder aus der 48V Seite über den 48V/12V DC/DC und/oder der 12V Batterie des Teilnetzes Kl.30-1 umgesetzt werden. Die Versorgung des Teilnetzes Kl.30-2 wird über die 12V Batterie des Teilnetzes Kl.30-2 umgesetzt.

Um die ASIL der Komponentenfunktionen ableiten zu können, werden die Minimalschnitte des ASIL-Dekompositionsfehlerbaums exportiert. Auf Basis der Minimalschnitte kann die ASIL Dekomposition unter Nutzung des in Kapitel 4.1.2 beschriebenen Algorithmus durchgeführt werden. Auf Basis des dargestellten ASIL-Dekompositionsfehlerbaums (Abbildung 5.12) ergeben sich die in Tabelle 5.3 gezeigten Dekompositionsmöglichkeiten. Aus den Vorgaben, dass die Energieversorgung in Teilnetz Kl.30-1 und Teilnetz Kl.30-2 aufgrund der ASIL Einstufung der sicherheitsrelevanten Verbraucher mit ASIL B(D) abgesichert werden muss und der Annahme, dass das 48V Teilnetz nicht ASIL qualifiziert werden soll, ergibt sich die grau hinterlegte Zeile als Ergebniszeile für den modellierten Ausschnitt.

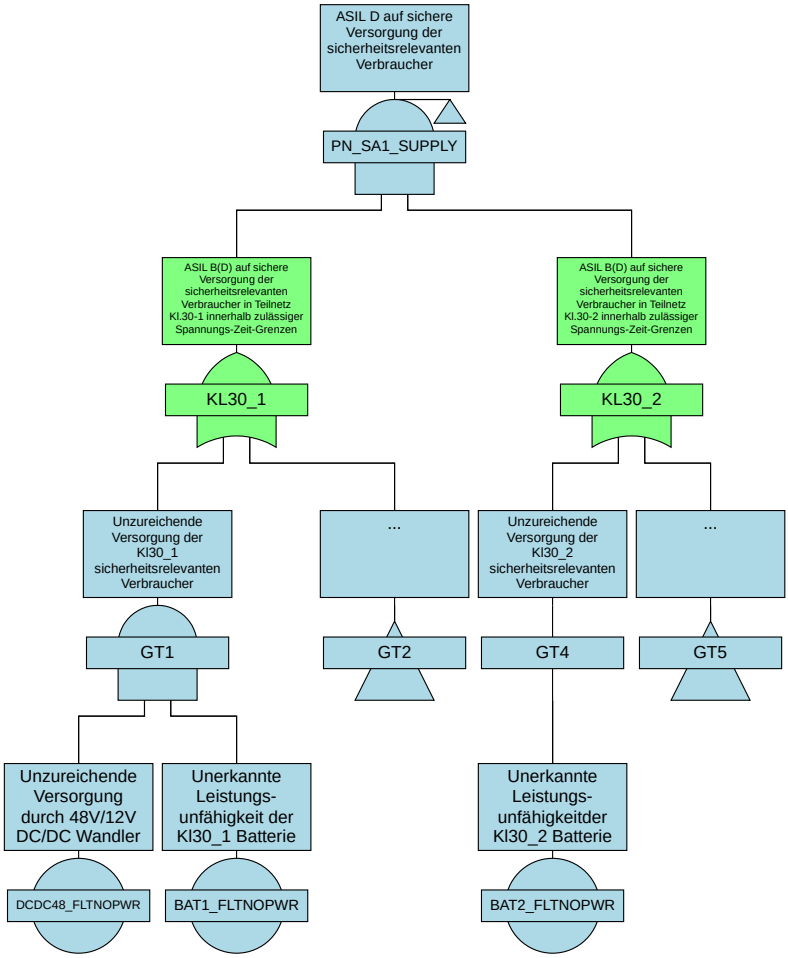


Abbildung 5.12: Ausschnitt des Fehlerbaums zur ASIL Dekomposition der vorgestellten Topologie (Abbildung 5.4)

Tabelle 5.3: Möglichkeiten zur ASIL Dekomposition für den Fehlerbaum aus Abbildung 5.12

Unzureichende Versorgung durch 48V/12V DC/DC Wandler incl. 48 V Teilnetz	**Unerkannte Leistungs-unfähigkeit der Kl30-1 Batterie**	**Unerkannte Leistungs-unfähigkeit der Kl30-2 Batterie**
QM(D)	QM(D)	D(D)
QM(D)	A(D)	C(D)
QM(D)	B(D)	B(D)
QM(D)	C(D)	A(D)
QM(D)	D(D)	QM(D)
A(D)	QM(D)	C(D)
A(D)	A(D)	B(D)
A(D)	B(D)	A(D)
A(D)	C(D)	QM(D)
B(D)	QM(D)	B(D)
B(D)	A(D)	A(D)
B(D)	B(D)	QM(D)
C(D)	QM(D)	A(D)
C(D)	A(D)	QM(D)
D(D)	QM(D)	QM(D)

5.8 Komponentendesign

Im Schritt Komponentendesign werden die Komponenten hinsichtlich Hardware, Software und Diagnose nach den definierten Anforderungen entwickelt, um das fehlertolerante Energiebordnetz zu ermöglichen. Die definierten Anforderungen wurden in Kapitel 5.4 abgleitet und umfassen die zu erfüllenden Funktionen, das zur Verfügung stehende FIT-Budget, die einzuhaltenden relativen Metriken, den ASIL und die Fehlertoleranzzeiten.

5.9 Aufbau der Fehlerkombinatorik

In der Fehlerkombinatorik werden alle technisch sinnvollen Fehlerkombinationen ermittelt. In Abbildung 5.13 ist ein Ausschnitt aus der Fehlerkombinatorik dargestellt. Dabei wird jede Fehlerklasse mit allen anderen Fehlerklassen kombiniert. In der ersten Zeile und der ersten Spalte werden dazu alle identifizierten Fehlerklassen aufgetragen. Die erste Zeile beinhaltet den Erstfehler, während die erste Spalte den Zweitfehler darstellt. Kombiniert werden die Fehler, indem an den Erstfehler (Zeile) der Zweitfehler (Spalte) angehängt wird. Die Erstfehler werden in erkannte (braune Felder) und unerkannte (blaue Felder) Fehler unterschieden. Kommt es zu einem erkannten Fehler, der nicht zur Verletzung des Sicherheitsziels führt, wird in der Markov-Simulation der Übergang in den sicheren Zustand modelliert. Zweitfehler, welche während des Übergangs in den sicheren Zustand auftreten, sind durch grüne Felder markiert. Die Unterscheidung in erkannten oder unerkannten Zweitfehler ist beim Zweitfehler während des Übergangs in den sicheren Zustand irrelevant, da mit dem erkannten Erstfehler der Übergang in den sicheren Zustand bereits eingeleitet wurde. Zum unerkannten Erstfehler wird sowohl der erkannte Zweitfehler (Kombination braun) als auch der unerkannte Zweitfehler (Kombination blau) kombiniert. Führt der unerkannte Erstfehler nicht zur Verletzung des Sicherheitsziels, wird mit dem erkannten Zweitfehler der Übergang in den sicheren Zustand getriggert. Bleibt auch der Zweitfehler unerkannt, wird die unerkannte Fehlerkombination abgebildet.

Händisch wird überprüft, ob es zu technisch nicht sinnvollen Kombinationen kommt. Ein Beispiel für eine technisch nicht sinnvolle Kombination ist die Fehlerkombination aus Batterieverbindung unterbrochen (PBatt2_fltOc) und Energieverlust (PBatt2_fltEgyLoss) bzw. Leistungsverlust (PBatt2_fltPwrLoss) derselben Batterie. Die entsprechenden Einträge werden gelöscht (hellgraue Felder). Die Fehlerkombinatorik ist die Basis dafür, dass systematisch alle möglichen Fehlerklassenkombinationen berücksichtigt werden. Die Fehlerkombinatorik ist die Basis für die Simulation und den automatisierten Aufbau der Markov-Analyse.

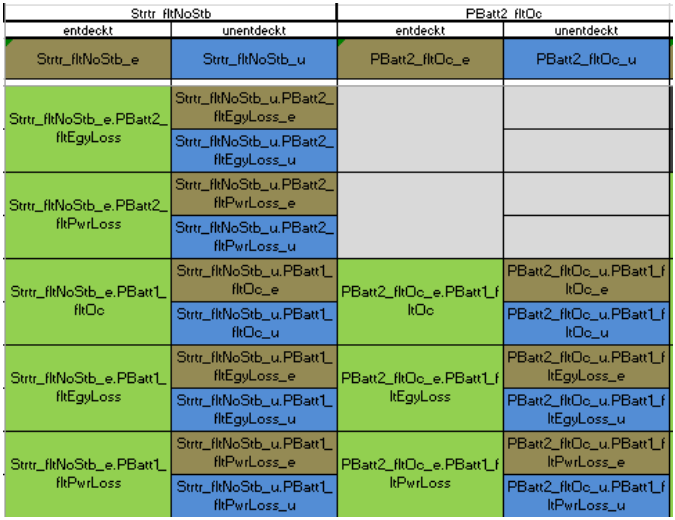


Abbildung 5.13:Fehlerkombinatorik

5.10 Quantifizierung der Komponentenfehler

Auf Basis der Ersatzschaltbilder der Komponenten wird für jeden Komponentenfehler ein Fehlerbaum zur Bestimmung der Fehlerrate aufgebaut. In Abbildung 5.14 ist der Ausschnitt des Fehlerbaums zum Komponentenfehler „elektrische Maschine liefert keine Leistung“ abgebildet. Darin wird die logische Struktur der Bauteilfehler, die zum Komponentenfehler führen, abgebildet. Die Bauteilfehler stellen die unterste Ebene des Fehlerbaums dar und werden nach vorgegebener Namenskonvention benannt. Bei der Modellierung des Fehlerbaums werden Diagnosen der Komponenten mitmodelliert, sodass die Diagnosedeckungsgrade der Komponentenfehler ermittelt werden können. Die Quantifizierung der Bauteilfehler erfolgt automatisiert nach [SN29500] und der Fehlerverteilung nach [BIR14] auf Basis der vorgegebenen Namenskonventionen mittels Excel-Tool, siehe Abbildung 5.15. Die Einsatzbedingungen werden in den Fehlerraten über die Belastungsprofile der Bauteile in Form von Temperaturprofilen, mittleren und maximalen elektrischen Spannungen an den Bauteilen und deren Eigenerwärmung

berücksichtigt. Bei der Analyse wird sowohl die Fehlerwahrscheinlichkeit der Komponentenfehler unter Berücksichtigung der Diagnosen als auch ohne Berücksichtigung der Diagnosen berechnet, um die Diagnosedeckungsgrade auf Komponentenebene abzuleiten, siehe Kapitel 4.2.4.1.

Für die Berechnung der Energiebordnetz-Metriken mittels Markov-Analyse, siehe Kapitel 5.12, werden die Fehlerraten der Fehlerklassen λ_{FKL_i}, Diagnosedeckungsgrade der Fehlerklassen DC_{FKL_i} und die Summe der Fehlerraten aller sicherheitsrelevanten Hardware-Bauteile im Energiebordnetz λ_{SR-EBN} als Eingangsgrößen benötigt. Unter Basisfehlerrate wird die Fehlerrate des Bauteils vor Anwendung einer Fehlerverteilung verstanden.

Die Ermittlung der λ_{FKL_i} wird dabei nach Gleichung (5.5) aus dem Quotienten der Summe der Ausfallwahrscheinlichkeiten der Komponentenfehler, die ohne Berücksichtigung von Diagnosen ermittelt wurden und der betrachteten Fehlerklasse zugeordnet werden können $F_{k-w/o-DC}(t)$ und der betrachteten Betriebsdauer t ermittelt.

Der zugehörige Diagnosedeckungsgrad DC_{FKL_i} wird nach Gleichung (5.6) ermittelt. Dabei wird von eins der Quotient aus der Summe der Ausfallwahrscheinlichkeiten der Komponentenfehler, die unter Berücksichtigung von Diagnosen ermittelt wurden $\sum_1^k F_{k-w-DC}(t)$ und der Summe der Ausfallwahrscheinlichkeiten der Komponentenfehler, die ohne Berücksichtigung von Diagnosen ermittelt wurden, $F_{k-w/o-DC}(t)$ abgezogen.

$$\lambda_{FKL_i} = \frac{\sum_1^k F_{k-\frac{w}{o}-DC}(t_{life})}{t_{life}} \tag{5.5}$$

$$DC_{FKL_i} = 1 - \frac{\sum_1^k F_{k-w-DC}(t_{life})}{\sum_1^k F_{k-\frac{w}{o}-DC}(t_{life})} \tag{5.6}$$

Zur Berechnung der Basisfehlerrate aller sicherheitsrelevanten Hardware-Bauteile im Energiebordnetz λ_{SR-EBN} muss für jede Komponente m, die einen Beitrag zur Verletzung des Sicherheitsziel hat, die zugehörige Fehlerrate (λ_{SR-m}) ermittelt werden. λ_{SR-m} ergibt sich für jede Komponente m nach Gleichung (5.7) aus der Summe der

komponentenzugehörigen Basisfehlerraten aller Bauteile n, die einen Beitrag zur Verletzung des Sicherheitsziels leisten (λ_n). Dabei muss darauf geachtet werden, dass keine Basisfehlerrate mehrfach berücksichtigt wird, da dies sonst eine unzulässige Verfälschung zur unsicheren Seite zur Folge hat.

$$\lambda_{SR-m} = \sum_{1}^{n} \lambda_n \tag{5.7}$$

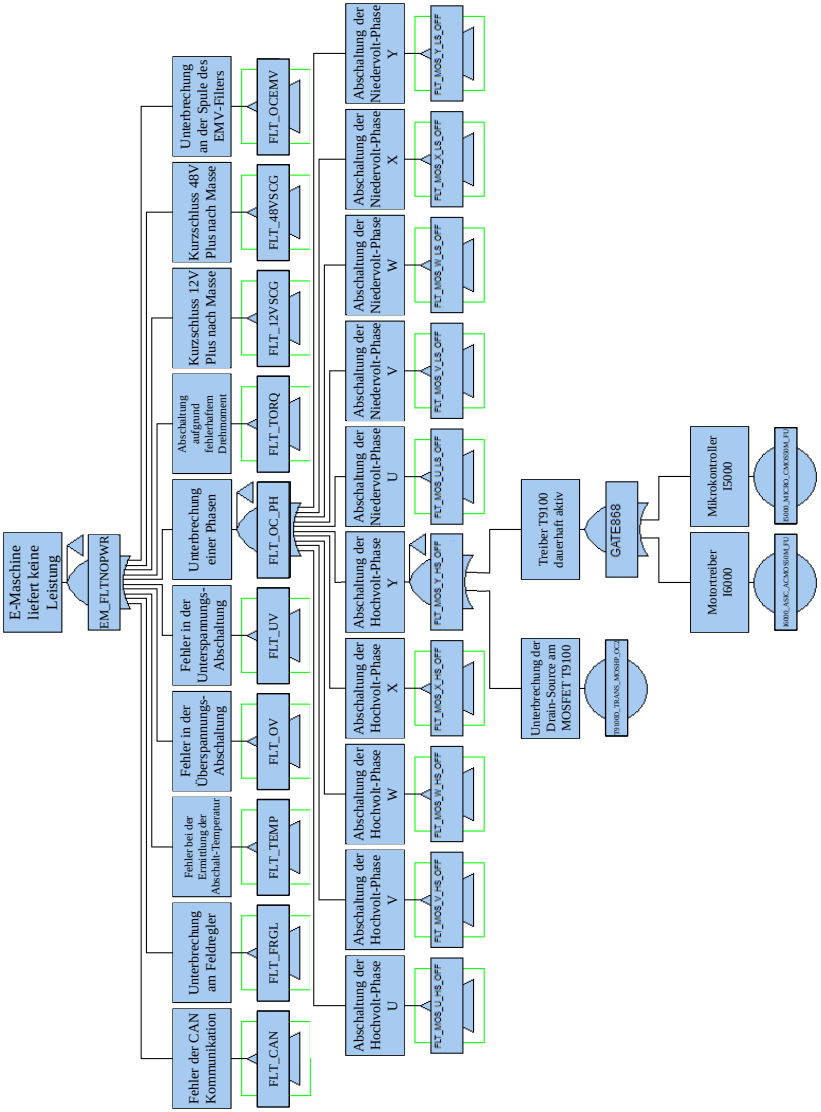


Abbildung 5.14:Ausschnitt der Fehlerbaumanalyse E-Maschine liefert keine Leistung

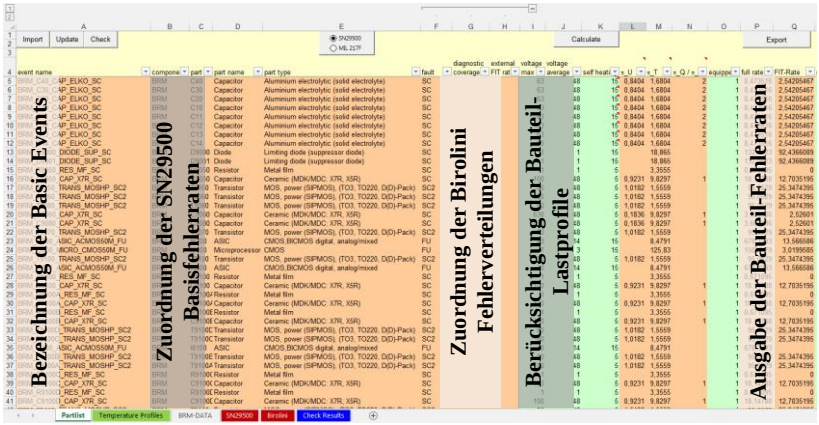


Abbildung 5.15: Excel-File zur automatisierten Berechnung der Bauteil-Fehlerraten

5.11 Aufbau und Durchführung der Fehler-Simulation

Die Simulation der Fehler und Fehlerkombinationen dient dazu, die Auswirkungen der Fehler und Fehlerkombinationen im Energiebordnetz zu identifizieren, und wird aufgrund der Vielzahl an Fehlern automatisiert durchgeführt, siehe z.B. [BEC16]. Mittels Fehler-Simulation können folgende Einflüsse bewertet und systematische Fehler behoben werden:

- Unterschiedliche Energiebordnetz-Designs inklusive Kabelbaum
- Spannungsgrenzen der sicherheitsrelevanten Verbraucher
- Auswirkungen erkannter und unerkannter Fehler
- Sicherheitsmechanismen mit Fehlerreaktion auf Energiebordnetz- und Fahrzeugebene
- Betriebsstrategien
- Dimensionierung der Energiebereitstellungskomponenten

Ein beispielhaftes Ergebnis einer Energiebordnetzsimulation ist in Abbildung 5.16 dargestellt. Im unteren Diagramm ist dabei der Spannungsverlauf an einem

sicherheitsrelevanten Verbraucher in Teilnetz Kl.30-1 und im oberen Diagramm der Spannungsverlauf an einem sicherheitsrelevanten Verbraucher in Teilnetz Kl.30-2 abgebildet. Bei erkannten Fehlern bzw. Fehlerkombinationen wird die Fehlerreaktion auf Fahrzeug- und auf Energiebordnetzebene mitberücksichtigt. Auf diese Weise kann die Wirksamkeit der Sicherheitsmechanismen überprüft werden. Die Fehlerreaktion auf Fahrzeugebene ist der Übergang in den sicheren Zustand, z.B. als doppelter Spurwechsel kombiniert mit einem Bremsmanöver, ein einfacher Spurwechsel gepaart mit dem Ausrollen des Fahrzeugs oder der Nothalt durch ein Bremsmanöver in der aktuellen Spur. Es können unterschiedliche Übergänge in den sicheren Zustand definiert werden, die in der Simulation abgebildet werden (FR1 bis FR3). Aus den unterschiedlichen Übergängen ergeben sich unterschiedliche Belastungen an das Energiebordnetz, da die manöverrealisierenden Komponenten abhängig vom Übergangsszenario unterschiedliche Leistungsprofile aufweisen und damit das Energiebordnetz unterschiedlich belasten. Abhängig von der Grundlast im Energiebordnetz kann ein Fehler bzw. eine Fehlerkombination zur Verletzung der Sicherheitsanforderung führen oder nicht. Zur Verletzung der Sicherheitsanforderung in einem Teilnetz kommt es, wenn der Spannungsverlauf im Teilnetz die zulässigen Spannungs-Zeit-Grenzen aus Kapitel 5.4.3 verlässt. Das Verlassen der Grenzen wird simulativ überprüft. Kommt es zur Verletzung in beiden Teilnetzen, führt dies zur Verletzung von mindestens einem Sicherheitsziel und damit zum unsicheren Fahrzeugzustand. Daher werden als Fehlerreaktionen der Energiebordnetzebene u.a. Lastzu- oder Lastabschaltungen definiert und in der Simulation modelliert. Für den unerkannten Fehler bzw. die unerkannte Fehlerkombination wird der Verlauf der Batteriespannungen je Teilnetz überwacht. Dieser dient zur Prognose, ob die Batterien in Zukunft in der Lage sein werden, den Übergang in den sicheren Zustand aus dem zugehörigen Teilnetz durchzuführen. Dementsprechend wird die Verletzung der Sicherheitsanforderungen eines Teilnetzes bewertet. Ebenso haben Betriebsstrategien einen Einfluss auf das Fehlerverhalten des Energiebordnetzes. Betriebsstrategien können z.B. einen Einfluss auf den Batterieladezustand haben. Der Batterieladezustand muss auf einem Mindestniveau gehalten werden, damit der Übergang in den sicheren Zustand in jeder Situation aus dem zugehörigen Teilnetz möglich ist. Werden Energiebereitstellungskomponenten, wie z.B. eine Batterie, unzureichend dimensioniert,

kann dies dazu führen, dass der Übergang in den sicheren Zustand fehlschlägt. Dieser systematische Fehler kann mittels Simulation erkannt und vermeiden werden.

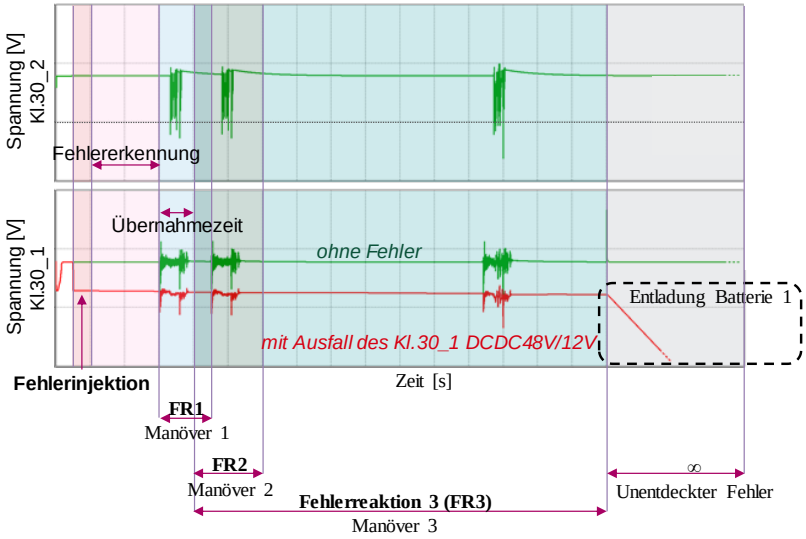


Abbildung 5.16: Fehlerinjektion 48V/12V-DC/DC liefert keine Leistung

Die Ergebnisse der Fehlerinjektionssimulation werden, wie in Abbildung 5.17 dargestellt, zusammengefasst, um diese für den automatisierten Aufbau der Markov-Analyse verwenden zu können. Dabei werden die Informationen über die Verletzung der Sicherheitsanforderungen abhängig davon, ob der Fehler bzw. die Fehlerkombination erkannt oder unerkannt vorliegt, ausgegeben. Für den erkannten Fehler wird die Information zusätzlich in Abhängigkeit von den Fehlerreaktionen der Fahrzeug- sowie der Energiebordnetzebene und der Basislast im Energiebordnetz dargestellt. Für den unerkannten Fall wird das Simulationsergebnis nur abhängig von der aktuell vorliegenden Energiebordnetzlast aufgetragen.

Auf Basis der zusammengefassten Ergebnisse der Fehlerinjektionssimulation kann eine automatisierte Optimierung der Fehlerreaktionen durchgeführt werden. Dabei wird

automatisiert die Fehlerreaktion ausgewählt, die für den Fahrer die angenehmste ist, jedoch nicht zur Verletzung des Sicherheitsziels führt.

		Niedrige Basislast		Mittlere Basislast		Hohe Basislast	
		Zustand Kl.30-1	Zustand Kl.30-2	Zustand Kl.30-1	Zustand Kl.30-2	Zustand Kl.30-1	Zustand Kl.30-2
Erkannt	FR1	✓	✓	✓	✓	✓	✓
	FR2	✓	✓	✓	✓	✓	✓
	FR3	✓	✓	✓	✓	✓	✓
Unerkannt		X	✓	X	✓	X	✓

Abbildung 5.17: Zusammenfassung der Ergebnisse der Fehler-Simulation des Fehlers 48V/12V-DC/DC liefert keine Leistung

5.12 Energiebordnetzbewertung und -optimierung mittels ISO 26262-Metriken

Auf Basis der Ergebnisse der Fehlerinjektionssimulation, ein Beispiel ist in Abbildung 5.17 dargestellt, wird die Struktur des Markov-Modells automatisiert aufgebaut. Die Quantifizierung der Übergangsraten erfolgt dabei auf Basis der Ergebnisse der Fehlerbaumanalysen, siehe Kapitel 5.10. Die Unterscheidung in erkannte und unerkannte Fehler / Fehlerkombinationen wird über die Berücksichtigung der Diagnosedeckungsgrade in den Übergangsraten realisiert. Im erkannten Fall erfolgt die Modellierung des Übergangs in den sicheren Zustand. Während des Übergangs in den sicheren Zustand können weitere Fehler auftreten. Zur Berechnung der ISO 26262-Metriken werden die Zustände wie in 4.2.4 beschrieben in SPF (single point faults), RF (residual faults), MPF_{latent} (latent multiple point faults) eingeteilt. Kommen SPF im Energiebordnetz vor, wird zusätzlich eine Meldung ausgegeben, da in diesem Fall weitere Sicherheitsmaßnahmen getroffen werden müssen [ISO26262-5, 9.4.1.2/3]. Zur Berechnung der Metriken wird nun das dem Markov-Modell zugrundeliegende

Differentialgleichungssystem gelöst. Somit werden den Markov-Zuständen Wahrscheinlichkeiten zugewiesen.

Zur Berechnung der PMHF (probabilistic metric for random hardware failures) werden alle Wahrscheinlichkeiten der Markov-Zustände addiert, die zur Verletzung des Sicherheitsziels führen. Die Berechnung der PMHF erfolgt nach Gleichung (4.28).

Zur Berechnung der SPFM (single point fault metric) nach Gleichung (2.2) muss neben den für die PMHF bereits berechneten Fehlerraten der SPF λ_{SPF} und den Fehlerraten der RF λ_{RF} die Gesamtheit der sicherheitsrelevanten Hardwarefehler λ_{SR-EBN} berücksichtigt werden. Zu deren Berechnung werden die Basisfehlerraten der Hardware-Bauteile der Fehlerbaumanalysen, die zur Quantifizierung der Übergangsraten der Markov-Analyse eingesetzt werden, verwendet, siehe λ_{SR-m} aus Kapitel 5.10. Aus den Simulationsergebnissen geht hervor, ob ein Komponentenfehler zur Verletzung des Sicherheitsziels beiträgt oder nicht. λ_{SR-EBN} ergibt sich aus der Summe aller λ_{SR-m}, deren Fehler einen Beitrag zur Verletzung des Sicherheitsziels haben, siehe Gleichung (5.8).

$$\lambda_{SR-EBN} = \sum_{1}^{m} \lambda_{SR-m} \tag{5.8}$$

Anschließend wird die SPFM-Berechnung durchgeführt. Die Berechnung der LFM (latent fault metric) wird nach Gleichung (2.3) durchgeführt. Dazu sind aus der PMHF Berechnung sowie der SPFM Berechnung alle Größen bekannt.

5.12.1 Analyseergebnisse

Eine Gegenüberstellung der Ziel- und Istwerte und Optimierungspotentiale für zwei identifizierte Fehlerbilder, die hier näher erläutert werden sollen, sind in Abbildung 5.18 für die PMHF, in Abbildung 5.19 für die SPFM und in Abbildung 5.20 für die LFM dargestellt.

- Der Zielwert der PMHF kann mit dem vorgestellten Energiebordnetz ohne zusätzliche Maßnahmen nicht erreicht werden.

- Die SPFM ist bereits im vorgestellten Energiebordnetz erreicht: Aufgrund der redundanten Versorgung der sicherheitsrelevanten Verbraucher durch zwei unabhängige Teilnetze Kl.30-1 und Kl.30-2 sind nur wenige Komponenten in der Lage hinsichtlich zufälliger Hardwarefehler als single point faults, d.h. in diesem Anwendungsfall als abhängige Fehler, zu Unter- oder Überspannungsevents in beiden sicherheitsrelevanten Teilnetzen gleichzeitig zu führen. Eine potentielle Komponente ist der 12V/12V DC/DC Wandler, welcher die Unabhängigkeit der Teilnetze Kl.30-1 und Kl.30-2 sicherstellt. Im DC/DC-Wandler sind Maßnahmen umgesetzt, sodass lediglich Fehler größer zweiter Ordnung zu einer gleichzeitigen Verletzung der Sicherheitsanforderungen in beiden Teilnetzen führen, wodurch dieses Szenario ausreichend unwahrscheinlich ist. Die analoge Argumentation gilt für die Lenkung, die als „Onebox“-Lösung ausgeführt ist.
- Der Zielwert der LFM kann mit dem vorgestellten Energiebordnetz nicht ohne zusätzliche Maßnahmen erreicht werden.

Die Fehlerbilder, die den größten Einfluss auf die Metriken haben, werden durch die Toolkette ausgegeben und dementsprechend eine zielgerichtete Optimierung ermöglicht.

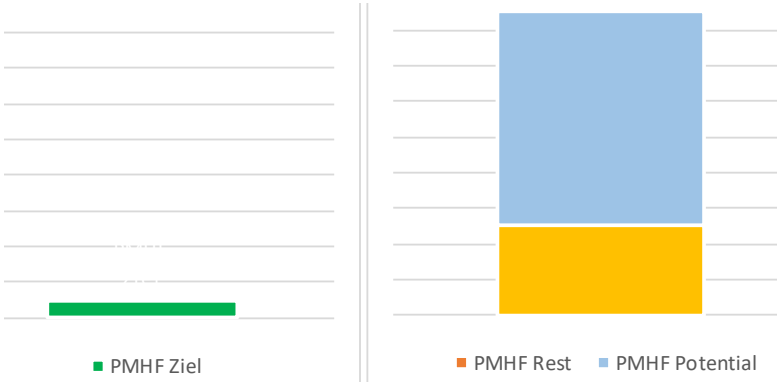


Abbildung 5.18: Ergebnisplot der Energiebordnetzbewertung ohne Sicherheitsmaßnahmen – PMHF inklusive Potential der identifizierten Fehlerbilder

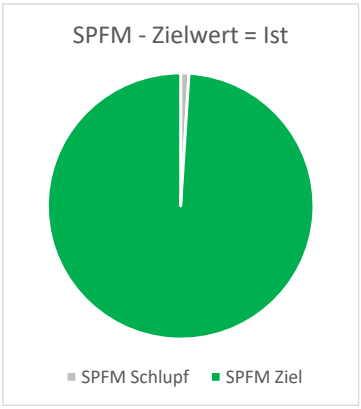


Abbildung 5.19: Ergebnisplot der Energiebordnetzbewertung ohne Sicherheitsmaßnahmen – SPFM

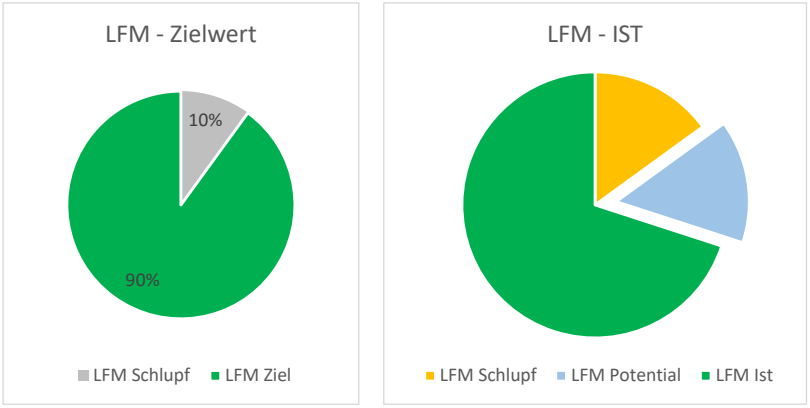


Abbildung 5.20: Ergebnisplot der Energiebordnetzbewertung ohne Sicherheitsmaßnahmen – LFM inklusive Potential der identifizierten Fehlerbilder

5.12.2 Beispielhafte Optimierung

Nachfolgend wird anhand der zwei beispielhaften identifizierten Fehler, deren Potentiale in Abbildung 5.18 und Abbildung 5.20 bereits dargestellt sind, das Vorgehen zur Optimierung des Energiebordnetzes durch die Definition von Maßnahmen definiert.

Die identifizierten Fehlerbilder sind:

- Rückwirkungen von nicht sicherheitsrelevanten Verbrauchern
- Batteriealterung.

5.12.2.1 Fehlerbild 1: Rückwirkungen von nicht sicherheitsrelevanten Verbrauchern

Kommt es zu einem Kurzschluss nach Masse an einem nicht sicherheitsrelevanten Verbraucher, führt dies zu einem Spannungseinbruch im Energiebordnetz. Dieser Unterspannungszustand hält solange an, bis die Schmelzsicherung, welche die Anbindung des betreffenden Verbrauchers vor thermischer Überlastung schützen soll, auslöst. Der betroffene Zweig wird abgetrennt und die Spannung stabilisiert sich. Abhängig von der Anbindung der sicherheitsrelevanten Verbraucher inklusive dem Auslöseverhalten der Schmelzsicherung kommt es zu einem Spannungseinbruch, der zu einem Ausfall der sicherheitsrelevanten Verbraucher führt.
In Abbildung 5.21 wird dies am Beispiel eines Motorlüfters gezeigt. Der Kurzschluss nach Masse des Motorlüfters führt im linken Bild zum Ausfall der Lenkung, da es aufgrund des Kurzschlusses im Motorlüfter zu einer Unterspannung an der Lenkung kommt. Diese Unterspannung führt dazu, dass die Lenkung ausfällt.
Als mögliche Maßnahme, um diese Rückwirkungen der nicht sicherheitsrelevanten Verbraucher verhindern zu können, kann z.B. ein Schalter eingesetzt werden, siehe Abbildung 5.22. Durch den Schalter wird sichergestellt, dass die negativen Rückwirkungen der nicht sicherheitsrelevanten Verbraucher Auswirkungen auf die sicherheitsrelevanten Verbraucher des Teilnetzes Kl.30-1 haben. Dieser Schalter muss so gestaltet sein, dass er schnell genug reagiert, die negativen Rückwirkungen des Teilnetzes Kl.30-0 Seite zu trennen und damit den Ausfall der sicherheitsrelevanten Verbraucher verhindert, siehe Abbildung 5.21 – rechtes Bild. Gleichzeitig muss der Schalter nach ASIL B(D) entwickelt werden, um die ASIL B(D) Integrität des Teilnetzes Kl.30-1 sicherstellen zu können.

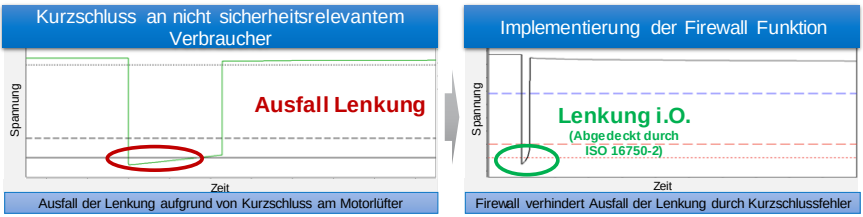


Abbildung 5.21: Simulationsergebnisse zum Kurzschluss an nicht sicherheitsrelevanten Verbrauchern vor und nach Implementierung von Maßnahmen

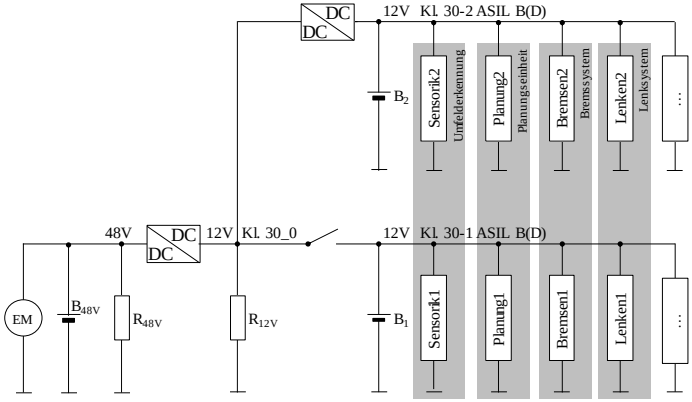


Abbildung 5.22: Beispiel-Energiebordnetz zur Realisierung der automatisierten Fahrfunktion

Durch das iterative Vorgehen zur Optimierung des Energiebordnetzes, in diesem Fall die Integration des Trennschalters, muss überprüft werden, ob vorherige Arbeitsprodukte. angepasst werden müssen. In diesem Fall muss z.B. die Fehlerdatenbank aus Kapitel 5.5 angepasst werden.

5.12.2.2 Fehlerbild 2: Batteriealterung

Im Normalbetrieb werden die sicherheitsrelevanten Verbraucher, zu denen z.B. die Lenkung gehört, redundant versorgt. Die Leistung, die zum Lenken erforderlich ist, wird dabei aus beiden Teilnetzen Kl.30-1 und Kl.30-2 bezogen.

Kommt es durch einen Fehler in einem Teilnetz zum Ausfall der sicherheitsrelevanten Verbraucher dieses Teilnetzes, muss die gesamte Leistung aus dem verbleibenden Teilnetz bereitgestellt werden. Ist die Batterie in der Rückfallebene jedoch bereits soweit gealtert, dass eine Versorgung der Lenkmanöver nicht mehr gewährleistet werden kann, kommt es zum Verlust der Lenkfunktion des Fahrzeugs. Aufgrund dessen muss der latent vorliegende Fehler „Batteriealterung“ erkannt werden, bevor es aufgrund der Batteriealterung zum Verlust der Rückfallebene in den Teilnetzen kommt.

In Abbildung 5.23 ist der Spannungsverlauf an der Lenkung bei wenig gealterter Batterie (blau) und bei gealterter Batterie (grün) dargestellt. Bei gealterter Batterie kommt es zum Ausfall der Lenkung aufgrund von Unterspannung. Folglich wird als Maßnahme ein Algorithmus eingesetzt, der die Alterung der Batterie überwacht und rechtzeitig bevor es zur Leistungsunfähigkeit kommt, den Austausch der Batterie anstößt.

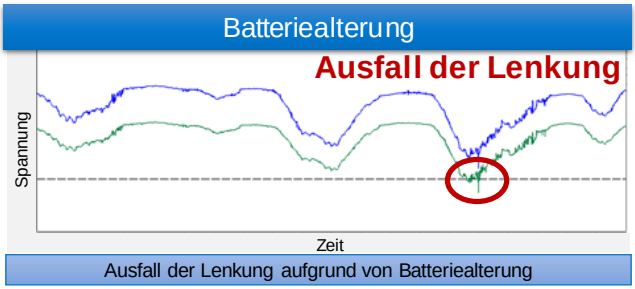


Abbildung 5.23: Simulationsergebnisse mit und ohne Batteriealterung

Die zwölf gezeigten Schritte begleiten die Entwicklung eines sicheren Energiebordnetzes in der praktischen Anwendung. Kritische Wirkpfade, z.B. Rückwirkungen von nicht-sicherheitsrelevanten Verbrauchern und Batteriefehler, die zu einer Verfehlung der ISO26262 Metriken führen, werden identifiziert und iterativ beseitigt.

6 Zusammenfassung und Ausblick

Im ersten Teil werden die mathematischen Grundlagen zur ASIL Dekomposition gelegt sowie ein Algorithmus zur automatisierten ASIL Allokation und Dekomposition vorgestellt, sodass effizient die Sicherheitsanforderungen vom Sicherheitsziel auf die Komponentenebene des komplexen, fehlertoleranten Systems heruntergebrochen werden können.

Der zweite Teil befasst sich mit dem Sicherheitsnachweis fehlertoleranter Systeme. Es werden sowohl die Ziele, die zum effizienten Sicherheitsnachweis fehlertoleranter Systeme nach ISO 26262 führen, erreicht als auch die Eigenschaften, welche die Modellierungsmethode abbilden muss, am Beispiel Energiebordnetz für automatisiertes Fahren vorgestellt. ISO 26262-Standard Methoden wie Fehlerbaumanalyse und FMEDA werden für den ISO 26262-konformen Sicherheitsnachweis von fail-safe Systemen eingesetzt, wobei die Methoden für die Modellierung fehlertoleranter Systeme nur bedingt einsetzbar sind. Die im Stand der Technik beschriebene Markov-Analyse ist zur Modellierung fehlertoleranter Systeme geeignet. Ein ISO 26262-konformer Sicherheitsnachweis ist dabei in der Praxis nicht etabliert.

Aus diesem Grund wird eine Methode zum ISO 26262-konformen Sicherheitsnachweis für fehlertolerante Systeme basierend auf einer Markov-Analyse vorgestellt und am Beispiel eines Energiebordnetzes für automatisiertes Fahren erläutert. Eine Fehlerinjektionssimulation dient zur Bewertung der Auswirkungen von erkannten und unerkannten Fehlern und Fehlerkombinationen unter verschiedenen Randbedingungen. Auf Basis der Ergebnisse der Fehlerinjektionssimulation wird ein Markov-Modell zur Modellierung des fehlertoleranten Systemverhaltens automatisiert aufgebaut. Zur Quantifizierung der Zustandsübergänge wird das Markov-Modell mit Fehlerbaumanalysen zur Modellierung der fail-safe Komponentenebene gekoppelt.

Ergänzend zu den Markov-Analysen des Standes der Technik wird mit der vorgestellten Methode

- zur Handhabbarkeit der Systemkomplexität eine automatisierte Modellbildung des Markov-Graphen basierend auf Fehlerinjektionssimulationen vorgestellt
- die Berechnung der absoluten und der relativen ISO 26262-Metriken mittels Markov-Analyse durchgeführt
- eine effiziente Systemoptimierung durch Identifikation der einflussreichsten Fehler / Fehlerkombinationen ermöglicht
- mittels Sensitivitätsanalysen der Einfluss von Parametervariationen bei einzelnen Fehlern identifiziert
- der Nachweis der Funktionsfähigkeit von Sicherheitsmechanismen umgesetzt
- die Erkennung und Behebung systematischer Fehlern des Systemdesigns, der Komponentendimensionierungen und Fehlerreaktionen realisiert

Der Fokus der Arbeit liegt auf der Berücksichtigung von zufälligen Hardwarefehlern und systematischen Fehlern, die mittels Simulation entdeckt werden können. Zusätzlich dazu müssen systematische Fehler im Energiebordnetz, umfangreicher als in der Arbeit beschrieben, identifiziert und Maßnahmen zur Vermeidung oder Beherrschung definiert werden. Dazu ist die Einhaltung entsprechender Entwicklungsprozesse z.B. inklusive der Durchführung einer Analyse abhängiger Fehler sowie Validierung durch Testung notwendig.

Ein Potential der Toolkette, das aktuell nicht genutzt wird, ist die Berechnung der maximal zulässigen Dauer einer Emergency Operation bis zum Erreichen des sicheren Fahrzeugstillstandes.

Weiterhin wird es v.a. für zukünftige Systeme, deren Nutzung nicht exakt vorhergesagt werden kann, ein wichtiges Kriterium sein zu überprüfen, ob die zur Erfüllung von Sicherheitszielen beitragenden Komponenten innerhalb ihrer Spezifikation betrieben werden. Ist dies nicht der Fall, sind Teile der Sicherheitsanalyse nicht mehr gültig, da z.B. der konstante Bereich der Fehlerraten verlassen wird und es zum Anstieg der Fehlerraten z.B. durch Alterungseffekte kommt. Ebenso wird der dominante Schädigungsmechanismus häufig durch die Alterung bestimmt. Durch geeignete

Maßnahmen, wie z.B. Stress-Strength-Analysen müssen solche Szenarien rechtzeitig erkannt werden, bevor es zu einer negativen Auswirkung kommt.

Außerdem kann eine Übertragbarkeit der beschriebenen Methode auf redundante sicherheitsrelevante Systeme, die entweder anderen Normen unterliegen, wie z.B. der DIN EN 61508 oder der DIN EN 62061, sowie in andere Bereiche, wie z.B. die Luft- und Raumfahrttechnik oder den Schienenverkehr, überprüft werden.

7 Literaturverzeichnis

[ABE08]	Abele, Marcus: Modellierung und Bewertung hochzuverlässiger Energiebordnetz-Architekturen für sicherheitsrelevante Verbraucher in Kraftfahrzeugen, Dissertation, kassel university press GmbH, Kassel, 2008
[AJM95]	Ajmone-Marsan, M.; Balbo, G.; Conte, G.; Donatelli, S.; Franceschinis, G.: Modelling with Generalized Stochastic Petri Nets. Wiley Series in Parallel Computing, John Wiley and Sons, 1995
[AUG16]	Augier, J.-L; Huck, T.; Kilic, A.; Müller, W.; Pieraccini, G.: Efficient, Safe and Reliable Powernet for AD; EEHE Elektrik/Elektronik in Hybrid- und Elektrofahrzeugen und elektrisches Energiemanagement, 2016
[AVI04]	Avizienis, A. et al.: Basic Concepts and Taxonomy of Dependable and Secure Computing, In: IEEE Transactions on dependable and secure computing, Vol.1, No.1, January-March 2004
[AZE14]	Azevedo, L. et al.: Assisted Assignment of Automotive Safety Requirements, IEEE Software, Volume: 31, Issue: 1, Jan.-Feb. 2014
[BAB13]	G. Babiel, Bordnetze und Powermanagement, 1. Auflage. Wiesbaden: Springer Vieweg, ISBN: 978-3-658-01559-6, 2013.
[BAB79]	Babai, L.: Monte-Carlo algorithms in graph isomorphism testing, Université de Montreal technical report, D.M.S. No. 79-10, 1979
[BAR75]	Barlow, R. E.; Proschan, F.; Importance of System Components and Fault Tree Events, Stochastic Processes and their Applications 3 153-173, North-Holland Publishing Company, 1975
[BAU02]	Bause, F.; Kritzinger, P. S.: Stochastic Petri Nets – An Introduction to the Theory, Dortmund und Cape Town, 2002

[BAU97]	Baumgarten, B.: Petri-Netze - Grundlagen und Anwendungen, Spektrum Akademischer Verlag GmbH, Heidelberg Berlin Oxford, 1997.
[BAZ12]	Bazzi, A. M.; Dominguez-Garcia, A. D.; Krein, P. T.: Markov Reliability Modeling for Induction Motor Drives Under Field-Oriented Control, IEEE Transaction on Power Electronics, Vol. 27, No. 2, p. 534-546, 2012
[BEC15]	Becker, Jan; Helmle, Michael: Architecture and System Safety Requirements for Automated Driving, erschienen in Meyer, Gereon; Beiker, Sven: Road Vehicle Automation 2; Springer International Publishing Switzerland, 2015, ISBN 978-3-319-19078-5
[BEC16]	Beckmann, M., Barthlott, J.: Simulation of Fault Tolerant Power Supply Networks for ADAS Vehicles with SaberRD, Saber Seminar, Detroit, 2016
[BEC17]	Becker, Jan; Helmle, Michael; Pink, Oliver: System Architecture and Safety Requirements for Automated Driving, erschienen in Watzenig, Daniel; Horn, Martin: Automated Driving – Safer and More Efficient Future Driving, Springer International Publishing Switzerland, 2017, ISBN 978-3-319-31895-0
[BER04]	Bertsche, B.; Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau: Ermittlung von Bauteil- und System-Zuverlässigkeiten. 3. Aufl. Berlin u.a.: Springer, 2004
[BER09]	Bertsche, B.; Göhner, P.; Jensen, U.; Schinköthe, W.; Wunderlich, H.-J.: Zuverlässigkeit mechatronischer Systeme – Grundalgen und Bewertung in frühen Entwicklungsphasen, Springer-Verlag Berlin Heidelberg, 2009

[BER13]	Bereszewski, M.: Automatisiertes Fahren kommt – mit Sicherheit, ATZ extra, Springer, 2013, S. 4-7
[BER15]	Bernhart, Wolfgang: Automatisiertes Fahren – Evolution statt Revolution, in: ATZextra: Fahrerassistenzsysteme. Auf dem Weg zum autonomen Fahren?, Seite 12 - 14, 2015
[BIR14]	Birolini, A.: Reliability Engineering – Theory and Practice, Springer-Verlag, Berlin Heidelberg, 2014
[BIR68]	Birnbaum, Z. W.: On the Importance of Different Components and Multicomponent System, Technical Report No. 54, 1968
[BMVI15]	Bundesministerium für Verkehr und digitale Infrastruktur: Strategie automatisiertes und vernetztes Fahren, September 2015, Berlin
[BMW GS 95024-3-1]	BMW Norm; Elektrische und elektronische Komponenten in Kraftfahrzeugen bis 3,5t - Allgemeine Anforderungen, Prüfbedingungen und Prüfungen; 2013-07
[BON13]	Bonamente, M.: Statistics and Analysis of Scientific Data, Springer Science+Business, New York, 2013, ISBN: 978-1-4614-7984-0
[BOR10]	Borgeest, Kai: Elektronik in der Fahrzeugtechnik. Hardware, Software, Systeme und Projektmanagement ; mit 28 Tabellen/ von Kai Borgeest. 2., überarbeitete und erweiterte Auflage, Wiesbaden: Vieweg + Teubner, 2010. ISBN 978-3-8348-0548-5
[BRE17]	Breuer, B.; Kill, K. H. (Herausgeber): Bremsenhandbuch – Grundlagen – Komponenten – Systeme – Fahrdynamik, 5. Auflage, Springer Vieweg, Wiesbaden, 2017, ISBN: 978-3-658-15489-9

[CHI13]	Ching, W.-K.; Huang, X.; Ng, M. K.; Siu, T.-K.: Markov Chains – Models, Algorithms and Applications, Springer Science+Business Media, New York, 2013
[CON96]	Conway, J. H., Guy, R. K.: The Book of Numbers. Copernicus, New York, 1996
[COR04]	Cortadella, J.; Reisig, W.: Application and Theory of Petri Nets 2004, 25th International Conference, ICATPN 2004, Bologna, Italy, Proceedings, Springer-Verlag Berlin Heidelberg, 2004
[DHO14]	Dhouibi, M. et al.: Automatic Decomposition and Allocation of Safety Integrity Level Using System of Linear Equations, PESARO 2014: The 4th International Conference on Performance, Safety and Robustness in Complex Systems and Applications
[DIN EN 62551]	Norm. DIN EN 62551 (VDE 0050-4) Analysemethoden für Zuverlässigkeit – Petrinetze, Beuth Verlag GmbH, Berlin, 2013
[DIN25424-1]	Norm. DIN 25424-1: Fehlerbaumanalyse – Methode und Bildzeichen, Berlin: Beuth Verlag GmbH, 1981
[DIN25424-2]	Norm. DIN 25424-2: Fehlerbaumanalyse - Handrechenverfahren zur Auswertung eines Fehlerbaumes, Berlin: Beuth Verlag GmbH, 1990
[DIN61025]	Norm. DIN EN 61025: Fehlzustandsbaumanalyse (IEC 61025:2006); Berlin: Beuth Verlag GmbH, 2007
[DIN61078]	Norm. DIN EN 61078: Techniken für die Analyse der Zuverlässigkeit - Zuverlässigkeitsblockdiagramm und Boole'sche Verfahren (IEC 61078:2006);, Berlin: Beuth Verlag GmbH, 2006

[DIN61165]	Norm. DIN EN 61165: Anwendung des Markoff-Verfahrens (IEC 61165:2006), Berlin: Beuth Verlag GmbH, 2007
[DINEN16602-30-02]	Norm. DIN EN 16602-30-02: Raumfahrtproduktsicherung – Fehlermöglichkeits-, Einfluss- (und Kritikalitäts-)Analyse (FMEA/FMECA); Berlin: Beuth Verlag GmbH, 2014
[DOM06]	Dominguez-Garcia, A. D.; Kassakian, J. G.; Schindall, J. E.: Reliability evaluation of the power supply of an electrical power net for safety-relevant applications, Reliability Engineering and System Safety 91, p. 505–514, Elsevier, 2006
[ECE R13-H]	Regulation No 13-H of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of passenger cars with regard to braking [2015/2364]
[ECE R79]	Regulation No 79 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of vehicles with regard to steering equipment
[EDL15]	Edler, F.; Soden, M.; Hankammer, R.: Fehlerbaumanalyse in Theorie und Praxis – Grundlagen und Anwendungen der Methode, Springer Vieweg, 2015
[FEL11]	Feldhusen, J.; Orloff, M.: Grundlagen technischer Systeme und des methodischen Vorgehens; In: Grote, K.-H.; Feldhusen, J. (Herausgeber): Dubbel – Taschenbuch für den Maschinenbau; Springer-Verlag, Berlin, Heidelberg, 2011, ISBN: 978-3-642-177306-6

[FLÄ12]	Fläming, H.: Autonome Fahrzeuge und autonomes Fahren im Bereich des Gütertransportes, In: Maurer, M.; Gerdes, J. C.; Lenz, B.; Winner, H. (Hrsg.): Autonomes Fahren – Technische, rechtliche und gesellschaftliche Aspekte, Springer-Verlag GmbH Berlin Heidelberg, 2015
[FUS72]	Fussell, J. B.; Vesely, W. E.: A new methodology for obtaining cut sets for fault trees, Trans. Amer. Nucl. Soc., vol. 15, pp. 262–263, Jun. 1972.
[FUS75]	Fussell, J. B.: How to Hand-Calculate System Reliability Characteristics, IEEE TRANSACTIONS ON RELIABILITY, VOL. R-24, NO. 3, AUGUST 1975
[GÄR01]	Gärtner, F. C.: Formale Grundlagen der Fehlertoleranz in verteilten Systemen, Dissertation, Darmstadt, 2001
[GAS12]	Gasser et. al: Rechtsfolgen zunehmender Fahrzeugautomatisierung, Bergisch Gladbach, Bundesanstalt für Straßenwesen, 2012 (Berichte der Bundesanstalt für Straßenwesen, Unterreihe „Fahrzeugsicherheit“, Heft F 83, Januar 2012)
[GHE15]	Gheraibia. Y. et al.: Can Aquatic Flightless Birds Allocate Automotive Safety Requirements?, IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15), 2015
[GOL12]	Goldbach, D.: Zuverlässigkeitsanalyse zur Verifikation der Einhaltung von quantitativen Sicherheitsanforderungen, In: Bäker, B.; Unger, A. (Hrsg.): Diagnose in mechatronischen Fahrzeugsystemen V: Neue Verfahren für Test, Prüfung und Diagnose von E/E-Systemen im Kfz, Renningen, expert-Verlag, 2012, S. 116–132
[HAA02]	Haas, P. J.: Stochastic Petri Nets – Modelling, Stability, Simulation, Springer Science+Business Media, New York, 2002

[HÄG02]	Häggström, O.: Finite markov chains and algorithmic applications. (London mathematical society Student Texts, Band 52) Cambridge University Press, Cambridge, 2010
[HAR15]	Hars, A.: Flotten selbstfahrender Elektrotaxis – Eine Szenarioanalyse, In: Proff, H.: Entscheidungen beim Übergang in die Elektromobilität, Springer Fachmedien Wiesbaden, 2015
[HEN90]	Henneberger G.: Bordnetz-Auslegung. In: Elektrische Motorausrüstung, Vieweg+Teubner Verlag, Braunschweig, 1990, ISBN: 978-3-322-84365-4
[HES11]	B. Hesse, Wechselwirkung von Fahrzeugdynamik und Kfz-Bordnetz unter Berücksichtigung der Fahrzeugbeherrschbarkeit, Bochum: Universität Duisburg-Essen, 2011.
[HOR15]	Horn, Matthias; Koller, Oliver; Kriso, Stefan: Development of safe and reliable Powernets for new vehicle functions – using the example Start-Stop-Coasting, EEHE Elektrik/Elektronik in Hybrid- und Elektrofahrzeugen und elektrisches Energiemanagement, 2015, Bad-Boll
[IECTR62380]	Technical Report. IEC TR 62380, Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment, 2004
[ISO 16750-2]	International standard: Road vehicles — Environmental conditions and testing for electrical and electronic equipment — Part 2: Electrical loads; 4th Edition; 2012-11-01
[ISO26262]	International Standard. ISO 26262：Road vehicles – Functional safety – Part 1-12, 2018-12

[KEL18]	Keller, H. B. et al.: Technical Safety – An Attribute of Quality, Springer International Publishing AG, 2018, ISBN: 978-3-319-68625-7
[KUR17]	Kurita, Yasuaki; Münzing, Patrick; Koller, Oliver: Future powernet topology for automated driving, JSAE Annual Congress 2017, Yokohama
[LEE85]	Lee, W. S.; Grosh, D. L.; Tillman, F. A.; Lie, C. H.: Fault Tree Analysis, Methods, and Applications - A Review; IEEE TRANSACTIONS ON RELIABILITY, VOL. R-34, NO. 3,1985 AUGUST
[MAD12]	Mader, R. et al.: Automatic and Optimal Allocation of Safety Integrity Levels, Reliability and Maintainability Symposium (RAMS), 2012 Proceedings - Annual, 2012
[MAH00]	Mahmoud, R.: Sicherheits- und Verfügbarkeitsanalyse komplexer Kfz-Systeme, Dissertation, Universität-Gesamthochschule Siegen, 2000
[MAU15]	Maurer, M.; Gerdes, J. C.; Lenz, B.; Winner, H. (Hrsg.): Autonomes Fahren – Technische, rechtliche und gesellschaftliche Aspekte, Springer-Verlag GmbH Berlin Heidelberg, 2015
[MBN LV 124-2]	Mercedes Benz Norm; Elektrische und elektronische Komponenten in Kraftfahrzeugen bis 3,5t - Allgemeine Anforderungen, Prüfbedingungen und Prüfungen; 2013-08
[MEI11]	Meinel, Christoph; Mundhenk, Martin: Mathematische Grundlagen der Informatik, Vieweg+Teubner 2011, 5., überarbeitete Auflage, ISBN 978-3-8348-1520-0

[MEY03]	Meyna, A.; Pauli, B.: Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik: Quantitative Bewertungsverfahren. München: Hanser, 2003 (Praxisreihe Qualitätswissen)
[MEY94]	Meyna, A.: Zuverlässigkeitsbewertung zukunftsorientierter Technologien. Vieweg, Wiesbaden, 1994
[MIL-HDBK217F]	Department of Defense; Military Handbook 217 F – Reliability Prediction of Electronic Equipment, 1990
[MIT05]	Mitzenmacher, M.; Upfal, E.: Probability and Computing – Randomized Algorithms and Probabilistic Analysis. Cambridge University Press, 2005; ISBN 0-521-83540-2
[MOT99]	Motet, G.; Powell, D.: Fault Avoidance and Fault Removal in Real-Time Systems & Fault-Tolerant Computing, In: Amestoy P. et al. (eds) Euro-Par'99 Parallel Processing. Euro-Par 1999, Lecture Notes in Computer Science, vol 1685, Springer, Berlin, Heidelberg
[MUE17]	Münzing, P.; Koller, O.; Kapahnke, M.; Bertsche, B.: Sichere Energieversorgung für autonome Fahrzeuge, QZ - Qualität und Zuverlässigkeit; 12/2017; S. 28 ff
[MUE18]	Münzing, P., Ostertag, A., Bertsche, B., and Koller, O.: Automated ASIL Allocation and Decomposition according to ISO 26262, Using the Example of Vehicle Electrical Systems for Automated Driving, SAE Int. J. Passeng. Cars –Electron. Electr. Syst. 11(2):2018, doi: 10.4271/07-11-02-0011.
[MUR15]	Murashkin, A. et al.: Automated Decomposition and Allocation of Automotive Safety Integrity Levels Using Exakt Solvers, SAE International Journal Passeng. Cars – Electronic and Electrical Systems / Volume 8, Issue 1, May 2015
[NHTSA13]	National Highway Traffic Safety Administration, U.S. Department of Transportation

[NIU17]	Niu, G.: Data-Driven Technology for Engineering Systems Health Management, Springer Science+Business Media Singapore and Science Press, Beijing, China 2017
[PAR13]	Parker, D. et al.: Automatic Decomposition and Allocation of Safety Integrity Levels Using a Penality-Based Genetic Algorithm, published in: Ali, M. et al.: Recent Trends in Applied Artificial Intelligence, 26th International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, IEA/AIE 2013 Amsterdam, The Netherlands, June 17-21, 2013, Springer-Verlag Berlin Heidelberg, 2013
[PET62]	Petri, C. A.: Kommunikation mit Automaten, Dissertation, Technische Hochschule Darmstadt, Bonn, 1962
[PIE15]	Pieraccini, Gabriele; Pflüger, Jochen; Horn, Matthias; Augier, Jean-Luc; Powering der Zukunft (Powering the future), Electronics in vehicles (ELIV) 2015
[PIS16]	Pischinger, Stefan; Seiffert, Ulrich (Hrsg.): Vieweg Handbuch Kraftfahrzeugtechnik, 8. Auflage, Springer Vieweg, Wiesbaden, 2016, ISBN 978-3-658-09528-4
[RAU01]	Rauzy, A.: Mathematical Foundations of Minimal Cutsets, IEEE TRANSACTIONS ON RELIABILITY, VOL. 50, NO. 4, DECEMBER 2001
[RAU03]	Rauzy, A.: Toward an Efficient Implementation of the MOCUS Algorithm, IEEE TRANSACTIONS ON RELIABILITY, VOL. 52, NO. 2, JUNE 2003
[RAU93]	Rauzy, A.: New algorithms for fault trees analysis, Reliability Eng. And System Safety, vol. 5, no. 59, pp. 203–211, 1993.

[REI10]	K. Reif, Batterien, Bordnetze und Vernetzung, 1. Auflage. Wiesbaden: Vieweg+Teubner Verlag, ISBN: 978-3-8348-1310-7, 2010.
[REI11]	K. Reif, Bosch Autoelektrik und Autoelektronik - Bordnetze, Sensoren und elektronische Systeme, 6., überar. Wiesbaden: Vieweg+Teubner Verlag, ISBN: 978-3-8348-1274-2, 2011.
[ROS00]	Ross, S. M.: Introduction to probability models, Tenth Edition,. Academic Press, Burlington, 2000
[RUF15]	Ruf, F.: Auslegung und Topologieoptimierung von spannungsstabilen Energiebordnetzen, Dissertation, TU München, 2015
[SAE-J3016]	Surface Vehicle Information Report Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, SAE International, 2014-01
[SCH10]	M. Schöllmann, C. Hoff, und J. Schriek, Energiemanagment und Bordnetze III. Renningen: expert Verlag, ISBN: 978-3-8169-2957-4, 2010.
[SN29500]	Siemens Norm. SN29500-1...5,7,9,10,11,12,15,16, CT SR Corporate Standardization & Regulation Siemens AG, München Erlangen, 2004…2016
[SON16]	Son, K. S.; et al.: Study on the systematic approach of Markov modeling for dependability analysis of complex fault tolerant features with voting logics, Reliability Engineering and System Safety 150, p. 44-57, Elsevier, 2016

[SUG92]	Sugasawa, Y.; Jin, Q.; Seya, K.: Extended stochastic petri net models for systems with parallel and cooperative motions, Computers Math. Applic., Vol. 24, No. 1/2, Seiten 119-126, Pergamon Press Ltd, 1992
[TEI12]	C. Teichert, Untersuchung einer Hilfsstromversorgung auf Brennstoffzellen-Basis für Kfz-Bordnetze, Magdeburg: Otto–von–Guericke–Universität Magdeburg, 2012.
[VAN01]	van der Borst, M., Schoonakker, H.: An overview of PSA importance measures, Reliability Engineering & System Safety 72 p.241-245, Elsevier Science Ltd, 2001
[VDA15]	Verband der Automobilindustrie e.V.: Automatisierung – Von Fahrerassistenzsystemen zum automatisierten Fahren, September 2015, Brandenburgische Universitätsdruckerei und Verlagsgesellschaft Potsdam mbh
[VDI4001-2]	Norm. Terminologie der Zuverlässigkeit, VDI-Handbuch Zuverlässigkeit, VDI-Gesellschaft Systementwicklung und Projektgestaltung, Düsseldorf, 2016
[VER10]	Verma, A. K.; Srividya, A.; Karanki, Durga Rao: Reliability and safety engineering, London: Springer (Springer series in reliability engineering), 2010. ISBN 978-1-84996-231-5
[VW 80000]	VW Norm; Elektrische und elektronische Komponenten in Kraftfahrzeugen bis 3,5t - Allgemeine Anforderungen, Prüfbedingungen und Prüfungen; 2013-06
[WEI00]	Weik M.H.: Monte Carlo method. In: Computer Science and Communications Dictionary. Springer, Boston, MA, 2000

[WIN15]	Winner, H.; Schopper, M.: Adaptve Cruise Constrol, In: Winner, H. et al.: Handbuch Fahrerassistenzsysteme – Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort, Springer Vieweg, 2015 ISBN: 978-3-658-05734-3
[WIT13]	Witt, Kurt-Ulrich: Mathematische Grundlagen für die Informatik, Springer Vieweg, Wiesbaden 2013, ISBN 978-3-658-03079-7
[ZUO05]	Zuo, G. et al.: Quantitative reliability analysis of different design alternatives for steer-by-wire system, Reliability Engineering and System Safety 89, p. 241–247, Elsevier, 2005

A) Anhang

A1) Differentialgleichungssystem des Markov-Modells

In Gleichung (A1.1) ist das Differentialgleichungssystem, in Gleichung (A1.2) der Startvektor des Markov-Modells aus Kapitel 4.2.3 dargestellt.

$$\begin{bmatrix} \frac{d}{dt}p_0(t) \\ \frac{d}{dt}p_1(t) \\ \frac{d}{dt}p_2(t) \\ \frac{d}{dt}p_3(t) \\ \frac{d}{dt}p_4(t) \\ \frac{d}{dt}p_5(t) \\ \frac{d}{dt}p_6(t) \\ \frac{d}{dt}p_7(t) \\ \frac{d}{dt}p8(t) \\ \frac{d}{dt}p_9(t) \\ \frac{d}{dt}p_{10}(t) \\ \frac{d}{dt}p_{11}(t) \\ \frac{d}{dt}p_{12}(t) \\ \frac{d}{dt}p_{13}(t) \\ \frac{d}{dt}p_{14}(t) \\ \frac{d}{dt}p_{15}(t) \\ \frac{d}{dt}p_{16}(t) \\ \vdots \end{bmatrix} = \begin{bmatrix} -\lambda_1-\lambda_2-\lambda_3-\lambda_4 & 0 & 0 & R & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_2 \cdot DC_2 & 0 & -\frac{1}{T}-\lambda_1-\lambda_3-\lambda_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{T} & -R & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_2 \cdot (1-DC_2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda_1-\lambda_2-\lambda_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 \cdot DC_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 \cdot (1-DC_2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda_1-\lambda_2-\lambda_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 \cdot DC_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 \cdot (1-DC_2) & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} p_0(t) \\ p_1(t) \\ p_2(t) \\ p_3(t) \\ p_4(t) \\ p_5(t) \\ p_6(t) \\ p_7(t) \\ p_8(t) \\ p_9(t) \\ p_{10}(t) \\ p_{11}(t) \\ p_{12}(t) \\ p_{13}(t) \\ p_{14}(t) \\ p_{15}(t) \\ p_{16}(t) \\ p_{17}(t) \end{bmatrix} \tag{A1.1}$$

$$\text{mit } p(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}; \; t = [0, t_{end}] \tag{A1.2}$$

A2) Bewertung der Methoden zur Modellierung fehlertoleranter Systeme

A21) FMEDA

Die Bewertung der FMEDA bezüglich der Ziele zur Analyse der funktionalen Sicherheit (Tabelle 3.2) sind in Tabelle A1 dargestellt. Die Bewertung der FMEDA bezüglich der Eigenschaften fehlertoleranter Systeme (Tabelle 3.3) sind in Tabelle A2 durchgeführt.

Tabelle A1: Erreichung der Ziele zur Analyse der funktionalen Sicherheit fehlertoleranter Systeme mittels FMEDA

	Ziel	Nr.	Beschreibung
ISO 26262 Anforderung	Vermeidung systematischer Fehler	Z1	Systematische Fehler können während des gesamten Entwicklungs- und Produktionsprozesses auftreten. Systematische Fehler werden durch die ISO26262 vorgegebenen Entwicklungsprozesse und Teststrategien erkannt und behoben. Simulationen können dabei unterstützen und z.B. fehlerhafte Dimensionierungen aufdecken, siehe Kapitel 4.2.2. Der Beitrag der FMEDA ist dabei beschränkt.
Notwendigkeit aus Effizienzgründen	Automatisierte Modellbildung und Analyse basierend auf Fehler-auswirkungen	Z2	Die FMEDA kann automatisiert auf Basis der Fehlerauswirkungen zufälliger Hardwarefehler erstellt werden. Einfachfehler, die zur Verletzung des Sicherheitsziels führen, werden den SPF / RF zugeordnet. Mehrfachfehler werden zu MPF_{latent} zugeordnet.
ISO 26262 Anforderung	Berechnung der ISO 26262 Metriken	Z3	Die Berechnung der SPFM und der LFM sind mittels FMEDA möglich. Die Berechnung der PMHF ist nur näherungsweise mittels FMEDA möglich, siehe Kapitel 2.3.2.1.
Unterstützung bei der Erreichung der Zielwerte	Ermittlung der einfluss-reichsten Parameter	Z4	Die einflussreichsten Parameter können durch Sortierung der Fehlerraten nach deren Größe identifiziert werden.

Tabelle A2: Bewertung der FMEDA zur Analyse fehlertoleranter Systeme

Eigenschaft			Beschreibung
Berücksichtigung zufällig verteilter Fehler	E1	+	Die FMEDA beschränkt sich auf die Berücksichtigung zufällig verteilter Fehler (Exponentialverteilung).
Berechnungen mit niedrigen Fehlerraten	E2	+	Aufgrund der arithmetischen Berechnung spielt die Größe der Fehlerrate keine Rolle.
Abbildung unterschiedlicher Komponentenzustände	E3	+	Unterschiedliche Komponentenzustände können in der FMEDA berücksichtigt werden.
Abbildung von Abhängigkeiten zwischen Fehlern	E4	-	Abhängigkeiten zwischen Fehlern können mittels FMEDA nicht berücksichtigt werden
Berücksichtigung von Diagnosedeckungsgraden	E5	+	Diagnosedeckungsgrade sind Teil der FMEDA Analyse.
Berücksichtigung unterschiedlicher Verweildauernd in Zuständen	E6	-	Zeitdauern von Zuständen können mittels FMEDA nicht berücksichtigt werden, da in der FMEDA keine unterschiedlichen Systemzustände unterschieden werden.
Analyse von Mehrfachfehlern	E7	/	Die FMEDA bietet die Möglichkeit Zweifachfehler näherungsweise, konservativ abzubilden, wie in Kapitel 2.3.2.1 beschrieben. Fehler höherer Ordnung und deren Einfluss können nicht berücksichtigt werden.
Abbildung von Reihenfolgeeffekten	E8	+	Durch die Einteilung der Fehler in SPF, RF und MPF_{latent} wird die Reihenfolge von Fehlern berücksichtigt. Bei der Berechnung der LFM führt dies zu einer konservativen Schätzung, da der MPF_{latent} in der Berechnung als Einfachfehler in die Metrik eingeht und nicht deren Multiplikation mit den zugehörigen Zweitfehlern.
Analyse komplexer Systeme mit einer Vielzahl an Komponenten	E9	+	Die FMEDA ist aufgrund der geringen Komplexität in der Lage komplexe Systeme mit einer Vielzahl an Komponenten abzubilden.

\+ Eigenschaft erfüllt / Eigenschaft teilweise erfüllt - Eigenschaft nicht erfüllt

Fazit: Die FMEDA wird zur Bewertung der funktionalen Sicherheit eingesetzt. Diese Methode ist jedoch nicht in der Lage, alle Eigenschaften fehlertoleranter Systeme vollumfänglich zu berücksichtigen.

A22) Fehlerbaumanalyse

Die Bewertung der Fehlerbaumanalyse bezüglich der Ziele zur Analyse der funktionalen Sicherheit (Tabelle 3.2) sind in Tabelle A3 dargestellt. Die Bewertung der Fehlerbaumanalyse bezüglich der Eigenschaften fehlertoleranter Systeme (Tabelle 3.3) ist in Tabelle A4 durchgeführt.

Tabelle A3: Erreichung der Ziele zur Analyse der funktionalen Sicherheit fehlertoleranter Systeme mittels Fehlerbaumanalyse

	Ziel	Nr.	Beschreibung
ISO 26262 Anforderung	Vermeidung systematischer Fehler	Z1	Systematische Fehler können während des gesamten Entwicklungs- und Produktionsprozesses auftreten. Systematische Fehler werden durch die ISO26262 vorgegebenen Entwicklungsprozesse und Teststrategien erkannt und behoben. Fehlerbaumanalysen können dabei z.B. durch Minimalschnittanalysen unterstützen, während Simulationen z.B. fehlerhafte Dimensionierungen aufdecken können, siehe Kapitel 4.2.2
Notwendigkeit aus Effizienzgründen	Automatisierte Modellbildung und Analyse basierend auf Fehler-auswirkungen	Z2	Minimalschnitte können auf Basis von Informationen über Fehlerauswirkungen erstellt werden. Die Minimalschnitte repräsentieren die logischen Verknüpfungen im Fehlerbaum. Auf Basis der Minimalschnitte können daher Fehlerbäume aufgebaut bzw. berechnet werden.
ISO 26262 Anforderung	Berechnung der ISO 26262 Metriken	Z3	Die Berechnung der PMHF ist mittels Fehlerbaumanalyse möglich. Die SPFM und die LFM können entweder durch spezielle Modellierung mittels Fehlerbaumanalyse oder auf Basis der Minimalschnitte berechnet werden.
Unterstützung bei der Erreichung der Zielwerte	Ermittlung der einflussreichsten Parameter	Z4	Einflussreiche Parameter der PMHF lassen sich mittels Importanzanalysen ermitteln. Einflussreiche Parameter der SPFM und LFM lassen sich z.B. über Sortierung der Fehlerraten nach deren Größe identifizieren.

Tabelle A4: Bewertung der Fehlerbaumanalyse zur Analyse fehlertoleranter Systeme

Eigenschaft			Beschreibung
Berücksichtigung zufällig verteilter Fehler	E1	+	Die Fehlerbaumanalyse ist in der Lage zufällig verteilte Fehler (Exponentialverteilung) abzubilden.
Berechnungen mit niedrigen Fehlerraten	E2	+	Die boolesche Algebra wird bei der Quantifizierung in arithmetische Formeln umgewandelt [BER04],
Abbildung unterschiedlicher Komponentenzustände	E3	+	Die Modellierung unterschiedlicher Bauteilzustände mittels Fehlerbaumanalyse ist üblich [EDL15].
Abbildung von Abhängig-keiten zwischen Fehlern	E4	/	Abhängigkeiten zwischen Fehlern können mittels Fehlerbaumanalyse nur näherungsweise z.B. mittels Beta-Faktor-Modell abgebildet werden. Die Annahme bei diesem Modell ist, dass die Fehlerraten der Fehler eine ähnliche Größe
Berücksichtigung von Diagnosedeckungsgraden	E5	+	Diagnosedeckungsgrade können als konstante Multiplikationsfaktoren berücksichtigt werden.
Berücksichtigung unterschiedlicher Verweil-dauernd in Zuständen	E6	/	Unterschiedliche Verweildauern in Komponenten-zuständen können mittels klassischer FTA nur bedingt abgebildet werden, da auf jedes Event maximal zwei Zeitdauern wirken können (Zeitbasis des Fehlerbaums sowie eine eventspezifische Zeitdauer). Zur Berücksichtigung unterschiedlicher Verweildauern muss eine vereinfachte, konservative Modellierung gewählt werden.
Analyse von Mehrfachfehlern	E7	+	Mehrfachfehler können durch logische UND-Verknüpfungen realisiert werden. Dabei gibt es keine Einschränkung hinsichtlich deren Ordnung.
Abbildung von Reihenfolgeeffekten	E8	/	Die klassische FTA kann Reihenfolgeeffekte nicht abbilden. Dynamische Fehlerbäume ermöglichen die Berücksichtigung von Reihenfolgeeffekten durch Erweiterung klassischer FTAs um Temporallogik oder Markov-Modelle [EDL15].
Analyse komplexer Systeme mit einer Vielzahl an Komponenten	E9	+	Die Fehlerbaumanalyse kann komplexe Systeme mit großer Anzahl an Elemente abbilden

\+ Eigenschaft erfüllt / Eigenschaft teilweise erfüllt - Eigenschaft nicht erfüllt

Fazit: Die Fehlerbaumanalyse wird zur Bewertung der funktionalen Sicherheit eingesetzt, ist jedoch nicht in der Lage alle Eigenschaften fehlertoleranter Systeme vollumfänglich zu berücksichtigen.

A23) Markov Analyse

Die Bewertung der Markov-Analyse bezüglich der Ziele zur Analyse der funktionalen Sicherheit (Tabelle 3.2) sind in Tabelle A5 dargestellt. Die Bewertung der Markov Analyse bezüglich der Eigenschaften fehlertoleranter Systeme (Tabelle 3.3) ist in Tabelle A6 durchgeführt.

Tabelle A5: Erreichung der Ziele zur Analyse der funktionalen Sicherheit fehlertoleranter Systeme mittels Markov-Analyse

	Ziel	**Nr.**	**Beschreibung**
ISO 26262 Anforderung	Vermeidung systematischer Fehler	Z1	Systematische Fehler können während des gesamten Entwicklungs- und Produktionsprozesses auftreten. Systematische Fehler werden durch die ISO26262 vorgegebenen Entwicklungsprozesse und Teststrategien erkannt und behoben. Simulationen können dabei unterstützen und z.B. fehlerhafte Dimensionierungen aufdecken, siehe Kapitel 4.2.2 Der Beitrag der Markov-Analyse ist dabei beschränkt.
Notwendigkeit aus Effizienzgründen	Automatisierte Modellbildung und Analyse basierend auf Fehler-auswirkungen	Z2	Der automatisierte Aufbau der Markov-Matrix und des zugrundeliegenden Differentialgleichungssystems ist auf Basis der Fehlerauswirkungen möglich.
ISO 26262 Anforderung	Berechnung der ISO 26262 Metriken	Z3	Die Berechnung der Metriken ist durch Aufsummieren der Zustandswahrscheinlichkeiten, die zu den jeweiligen Fehlern RF, SPF, MPF_{latent} zugeordnet werden können, möglich. Die Umrechnung der Fehlerwahrscheinlichkeit in eine Fehlerrate und die Berechnung der Metriken nach Kapitel 2.3.1 können durchgeführt werden, siehe Kapitel 4.2.4.
Unterstützung bei der Erreichung der Zielwerte	Ermittlung der einfluss-reichsten Parameter	Z4	Ein Ranking des Einflusses der Fehler auf die Metriken basierend auf deren Anteil an den entsprechenden Gesamtfehlerraten, die in den Metriken berücksichtigt werden, kann umgesetzt werden.

Tabelle A6: Bewertung der Markov-Analyse zur Analyse fehlertoleranter Systeme

Eigenschaft			Beschreibung
Berücksichtigung zufällig verteilter Fehler	E1	+	Die Markov-Analyse beschränkt sich auf die Analyse zufällig verteilter Fehler (Exponentialverteilung)
Berechnungen mit niedrigen Fehlerraten	E2	+	Niedrige Fehlerraten können analysiert werden, da bei der Lösung der Markov-Analyse Differentialgleichungssysteme numerisch gelöst werden.
Abbildung unterschiedlicher Komponentenzustände	E3	+	Es können unterschiedliche Komponentenzustände abgebildet werden
Abbildung von Abhängigkeiten zwischen Fehlern	E4	+	Abhängigkeiten zwischen den Fehlern können durch Anpassung der Übergangsraten der Markov-Analyse abgebildet werden
Berücksichtigung von Diagnosedeckungsgraden	E5	+	Diagnosedeckungsgrade werden durch Anpassung der Übergangsraten und Aufteilen von Fehlerzuständen in erkannte und unerkannte Fehlerzustände berücksichtigt
Berücksichtigung unterschiedlicher Verweildauernd in Zuständen	E6	+	Unterschiedliche Verweildauern von Zuständen werden durch die Übergangsraten berücksichtigt
Analyse von Mehrfachfehlern	E7	+	Mehrfachfehler können durch Aneinanderreihung der Zustände modelliert werden
Abbildung von Reihenfolgeeffekten	E8	+	Reihenfolgeeffekte werden durch Aneinanderreihung von Zuständen abgebildet. Im Gegensatz zu anderen Methoden können unidirektionale Fehlerfolgen modelliert werden. (Zustand A folgt auf Zustand B wird modelliert, während Zustand B folgt auf Zustand A ausgelassen wird.)
Analyse komplexer Systeme mit einer Vielzahl an Komponenten	E9	/	Die Anzahl an Zuständen muss begrenzt werden, da dies sonst zur Zustandsraumexplosion und zur Unlösbarkeit führt.

\+ Eigenschaft erfüllt / Eigenschaft teilweise erfüllt - Eigenschaft nicht erfüllt

Fazit: Die Markov-Analyse wird in der Praxis bisher selten zur Bewertung der funktionalen Sicherheit eingesetzt, ist jedoch in der Lage die Eigenschaften fehlertoleranter Systeme zu modellieren. Bei der Markov-Analyse besteht die Gefahr der Zustandsraumexplosion.

A24) Petri Netze

Generalisierte stochastische Petri Netze werden mittels Markov-Analyse nach Kapitel A23) ausgewertet und werden hier daher nicht weiter betrachtet. Die Bewertung der erweiterten stochastischen Petri Netze bezüglich der Ziele zur Analyse der funktionalen Sicherheit (Tabelle 3.2) sind in Tabelle A7 und deren Bewertung bezüglich der Eigenschaften fehlertoleranter Systeme (Tabelle 3.3) in Tabelle A8 dargestellt.

Tabelle A7: Erreichung der Ziele zur Analyse der funktionalen Sicherheit fehlertoleranter Systeme mittels erweiterten stochastischen Petri Netze

	Ziel	Nr	Beschreibung
ISO 26262 Anforderung	Vermeidung systematischer Fehler	Z1	Systematische Fehler können während des gesamten Entwicklungs- und Produktionsprozesses auftreten. Systematische Fehler werden durch die ISO26262 vorgegebenen Entwicklungsprozesse und Teststrategien erkannt und behoben. Simulationen können dabei unterstützen und z.B. fehlerhafte Dimensionierungen aufdecken, siehe Kapitel 4.2.2. Der Beitrag der Petri Netze ist dabei beschränkt.
Notwendigkeit aus Effizienz-gründen	Automatisierte Modellbildung und Analyse basierend auf Fehler-auswirkungen	Z2	Ein automatischer Aufbau von Petri-Netzen auf Basis der Fehlerauswirkungen ist mit heutigen Tools nicht möglich. Aufgrund der Vielzahl an Freiheitsgraden ist die automatisierte Modellbildung komplex, jedoch nicht ausgeschlossen.
ISO 26262 Anforderung	Berechnung der ISO 26262 Metriken	Z3	Die Berechnung der Metriken durch Aufsummieren der Zustandswahrscheinlichkeiten, die zu den jeweiligen Fehlern RF, SPF, MPF_{latent} zugeordnet werden können, ist möglich. Die Umrechnung der Fehlerwahrscheinlichkeiten in Fehlerraten und die Berechnung der Metriken nach Kapitel 2.3.1 kann durchgeführt werden.
Unterstützung bei der Erreichung der Zielwerte	Ermittlung der einflussreichsten Parameter	Z4	Ein Ranking des Einflusses der Fehler auf die Metriken basierend auf deren Anteil an den entsprechenden Gesamtfehlerraten, die in den Metriken berücksichtigt werden, ist möglich.

Tabelle A8: Bewertung erweiterter stochastischer Petri Netze zur Analyse fehlertoleranter Systeme

Eigenschaft			Beschreibung
Berücksichtigung zufällig verteilter Fehler	E1	+	Erweiterte stochastische Petri-Netze können sämtliche Fehlerverteilungen berücksichtigen.
Berechnungen mit niedrigen Fehlerraten	E2	-	Zur Lösung erweiterte stochastischer Petri-Netze werden simulativen Experimente mittels Monte Carlo Simulationen durchgeführt. Bei niedrigen Fehlerraten muss eine Vielzahl an Experimenten durchgeführt werden, bis Konvergenz erreicht wird. Dies führt zu einer hohen Rechenzeit zur Lösung der Petri-Netze mit niedrigen Fehlerraten.
Abbildung unterschiedlicher Komponentenzustände	E3	+	Unterschiedliche Komponentenzustände können abgebildet werden
Abbildung von Abhängig-keiten zwischen Fehlern	E4	+	Abhängigkeiten zwischen Fehlern können durch Anpassung der Übergangsraten abgebildet werden.
Berücksichtigung von Diagnosedeckungsgraden	E5	+	Diagnosedeckungsgrade werden durch Anpassung der Transitionen und Aufteilen von Fehlerzuständen in erkannte und unerkannte Fehlerzustände berücksichtigt
Berücksichtigung unterschiedlicher Verweil-dauernd in Zuständen	E6	+	Unterschiedliche Verweildauern können als Transitionen definiert werden
Analyse von Mehrfachfehlern	E7	+	Mehrfachfehler können durch Aneinanderreihung der Stellen abgebildet werden.
Abbildung von Reihenfolgeeffekten	E8	+	Reihenfolgeeffekte werden durch entsprechende Aneinanderreihung der Stellen modelliert.
Analyse komplexer Systeme mit einer Vielzahl an Komponenten	E9	+	Die Vielzahl an Komponenten können mittels erweiterten stochastischen Petri Netzen abgebildet werden.

\+ Eigenschaft erfüllt / Eigenschaft teilweise erfüllt - Eigenschaft nicht erfüllt

Fazit: Erweiterte stochastische Petri-Netze werden aktuell nicht zur Bewertung der funktionalen Sicherheit eingesetzt und sind nur teilweise in der Lage die Eigenschaften fehlertoleranter Systeme zu berücksichtigen. Ein automatisierter Aufbau der erweiterten stochastischen Petri Netze ist nicht möglich.

A3) Figurierte Zahlen im ASIL C und ASIL D System

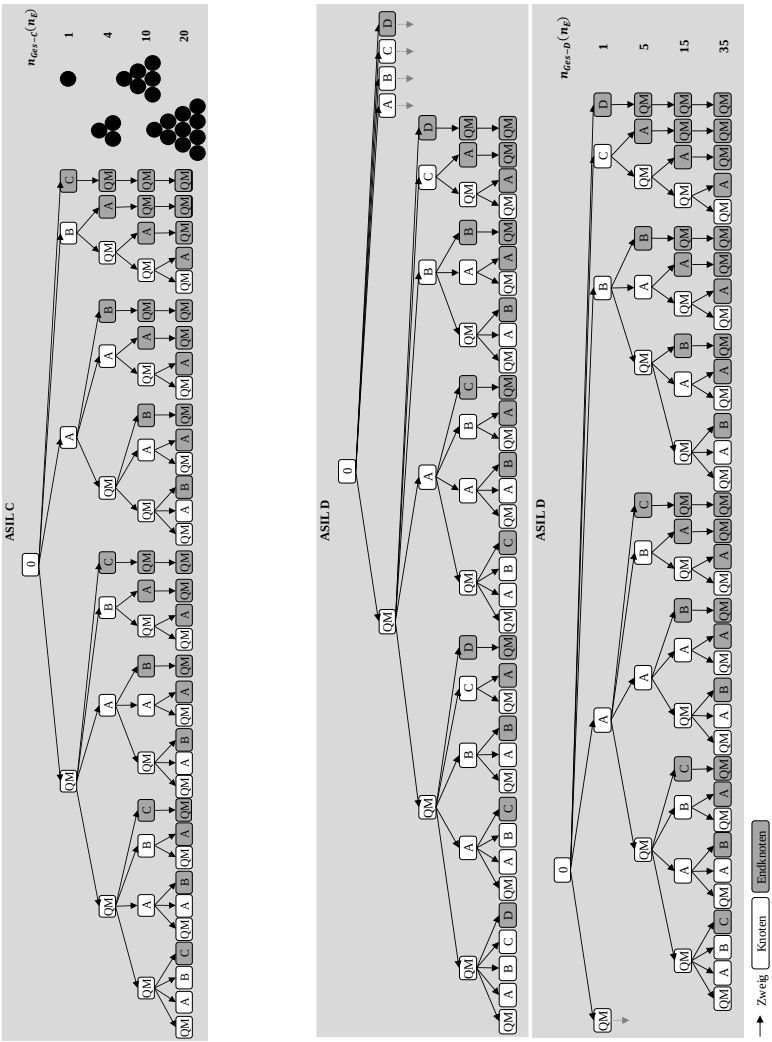


Abbildung A1: Anzahl Möglichkeiten n_{ges} zur ASIL Dekomposition in Abhängigkeit der Anzahl sicherheitsrelevanter Fehlfunktionen n_E für ASIL C und D Einstufungen

Liste der bisher erschienenen Berichte aus dem IMA:

Nr.	Verfasser	Titel
1	H.K. Müller	Beitrag zur Berechnung und Konstruktion von Hochdruckdichtungen an schnellaufenden Wellen
2	W. Passera	Konzentrisch laufende Gewinde-Wellen-Dichtung im laminaren Bereich
	K. Karow	Konzentrische Doppelgewindewellendichtung im laminaren Bereich
3	F.E. Breit	Die Kreiszylinderschalendichtung: Eine Axialspaltdichtung mit druckabhängiger Spaltweite
	W. Sommer	Dichtungen an Mehrphasensystemen: Berührungsfreie Wellendichtungen mit hochviskosen Sperrflüssigkeiten
4	K. Heitel	Beitrag zur Berechnung und Konstruktion konzentrisch und exzentrisch betriebener Gewindewellendichtungen im laminaren Bereich
5	K.-H. Hirschmann	Beitrag zur Berechnung der Geometrie von Evolventenverzahnungen
6	H. Däuble	Durchfluß und Druckverlauf im radial durchströmten Dichtspalt bei pulsierendem Druck
7	J. Rybak	Einheitliche Berechnung von Schneidrädern für Außen- und Innenverzahnungen. Beitrag zu Eingriffsstörungen beim Hohlrad-Verzahnen mittels Schneidräder
8	D. Franz	Rechnergestütztes Entwerfen von Varianten auf der Grundlage gesammelter Erfahrungswerte
9	E. Lauster	Untersuchungen und Berechnungen zum Wärmehaushalt mechanischer Schaltgetriebe
10		Festschrift zum 70. Geburtstag von Prof. Dr.-Ing. K. Talke
11	G. Ott	Untersuchungen zum dynamischen Leckage- und Reibverhalten von Radialwellendichtringen
12	E. Fuchs	Untersuchung des elastohydrodynamischen Verhaltens von berührungsfreien Hochdruckdichtungen
13	G. Sedlak	Rechnerunterstütztes Aufnehmen und Auswerten spannungsoptischer Bilder
14	W. Wolf	Programmsystem zur Analyse und Optimierung von Fahrzeuggetrieben
15	H. v. Eiff	Einfluß der Verzahnungsgeometrie auf die Zahnfußbeanspruchung innen- und außenverzahnter Geradstirnräder
16	N. Messner	Untersuchung von Hydraulikstangendichtungen aus Polytetrafluoräthylen
17	V. Schade	Entwicklung eines Verfahrens zur Einflanken-Wälzprüfung und einer rechnergestützten Auswertemethode für Stirnräder
18	A. Gührer	Beitrag zur Optimierung von Antriebssträngen bei Fahrzeugen
19	R. Nill	Das Schwingungsverhalten loser Bauteile in Fahrzeuggetrieben
20	M. Kammüller	Zum Abdichtverhalten von Radial-Wellendichtringen
21	H. Truong	Strukturorientiertes Modellieren, Optimieren und Identifizieren von Mehrkörpersystemen
22	H. Liu	Rechnergestützte Bilderfassung, -verarbeitung und -auswertung in der Spannungsoptik
23	W. Haas	Berührungsfreie Wellendichtungen für flüssigkeitsbespritzte Dichtstellen
24	M. Plank	Das Betriebsverhalten von Wälzlagern im Drehzahlbereich bis 100.000/min bei Kleinstmengenschmierung
25	A. Wolf	Untersuchungen zum Abdichtverhalten von druckbelastbaren Elastomer- und PTFE-Wellendichtungen
26	P. Waidner	Vorgänge im Dichtspalt wasserabdichtender Gleitringdichtungen
27	Hirschmann u.a.	Veröffentlichungen aus Anlaß des 75. Geburtstags von Prof. Dr.-Ing. Kurt Talke
28	B. Bertsche	Zur Berechnung der Systemzuverlässigkeit von Maschinenbau-Produkten
29	G. Lechner; K.-H. Hirschmann; B. Bertsche	Forschungsarbeiten zur Zuverlässigkeit im Maschinenbau
30	H.-J. Prokop	Zum Abdicht- und Reibungsverhalten von Hydraulikstangendichtungen aus Polytetrafluoräthylen
31	K. Kleinbach	Qualitätsbeurteilung von Kegelradsätzen durch integrierte Prüfung von Tragbild, Einflankenwälzabweichung und Spielverlauf
32	E. Zürn	Beitrag zur Erhöhung der Meßgenauigkeit und -geschwindigkeit eines Mehrkoordinatentasters
33	F. Jauch	Optimierung des Antriebsstranges von Kraftfahrzeugen durch Fahrsimulation
34	J. Grabscheid	Entwicklung einer Kegelrad-Laufprüfmaschine mit thermografischer Tragbilderfassung
35	A. Hölderlin	Verknüpfung von rechnerunterstützter Konstruktion und Koordinatenmeßtechnik
36	J. Kurfess	Abdichten von Flüssigkeiten mit Magnetflüssigkeitsdichtungen
37	G. Borenius	Zur rechnerischen Schädigungsakkumulation in der Erprobung von Kraftfahrzeugteilen bei stochastischer Belastung mit variabler Mittellast
38	E. Fritz	Abdichtung von Maschinenspindeln
39	E. Fritz; W. Haas; H.K. Müller	Berührungsfreie Spindelabdichtungen im Werkzeugmaschinenbau. Konstruktionskatalog

Nr.	Verfasser	Titel
40	B. Jenisch	Abdichten mit Radial-Wellendichtringen aus Elastomer und Polytetrafluorethylen
41	G. Weidner	Klappern und Rasseln von Fahrzeuggetrieben
42	A. Herzog	Erweiterung des Datenmodells eines 2D CAD-Systems zur Programmierung von Mehrkoordinatenmeßgeräten
43	T. Roser	Wissensbasiertes Konstruieren am Beispiel von Getrieben
44	P. Wäschle	Entlastete Wellendichtringe
45	Z. Wu	Vergleich und Entwicklung von Methoden zur Zuverlässigkeitsanalyse von Systemen
46	W. Richter	Nichtwiederholbarer Schlag von Wälzlagereinheiten für Festplattenlaufwerke
47	R. Durst	Rechnerunterstützte Nutprofilentwicklung und clusteranalytische Methoden zur Optimierung von Gewindewerkzeugen
48	G.S. Müller	Das Abdichtverhalten von Gleitringdichtungen aus Siliziumkarbid
49	W.-E. Krieg	Untersuchungen an Gehäuseabdichtungen von hochbelasteten Getrieben
50	J. Grill	Zur Krümmungstheorie von Hüllflächen und ihrer Anwendung bei Werkzeugen und Verzahnungen
51	M. Jäckle	Entlüftung von Getrieben
52	M. Köchling	Beitrag zur Auslegung von geradverzahnten Stirnrädern mit beliebiger Flankenform
53	M. Hildebrandt	Schadensfrüherkennung an Wälzkontakten mit Körperschall-Referenzsignalen
54	H. Kaiser	Konstruieren im Verbund von Expertensystem, CAD-System, Datenbank und Wiederholteilsuchsystem
55	N. Stanger	Berührungsfrei abdichten bei kleinem Bauraum
56	R. Lenk	Zuverlässigkeitsanalyse von komplexen Systemen am Beispiel PKW-Automatikgetriebe
57	H. Naunheimer	Beitrag zur Entwicklung von Stufenlosgetrieben mittels Fahrsimulation
58	G. Neumann	Thermografische Tragbilderfassung an rotierenden Zahnrädern
59	G. Wüstenhagen	Beitrag zur Optimierung des Entlasteten Wellendichtrings
60	P. Brodbeck	Experimentelle und theoretische Untersuchungen zur Bauteilzuverlässigkeit und zur Systemberechnung nach dem Booleschen Modell
61	Ch. Hoffmann	Untersuchungen an PTFE-Wellendichtungen
62	V. Hettich	Identifikation und Modellierung des Materialverhaltens dynamisch beanspruchter Flächendichtungen
63	K. Riedl	Pulsationsoptimierte Außenzahnradpumpen mit ungleichförmig übersetzenden Radpaaren
64	D. Schwuchow	Sonderverzahnungen für Zahnradpumpen mit minimaler Volumenstrompulsation
65	T. Spörl	Modulares Fahrsimulationsprogramm für beliebig aufgebaute Fahrzeugtriebstränge und Anwendung auf Hybridantriebe
66	K. Zhao	Entwicklung eines räumlichen Toleranzmodells zur Optimierung der Produktqualität
67	K. Heusel	Qualitätssteigerung von Planetengetrieben durch Selektive Montage
68	T. Wagner	Entwicklung eines Qualitätsinformationssystems für die Konstruktion
69	H. Zelßmann	Optimierung des Betriebsverhaltens von Getriebeentlüftungen
70	E. Bock	Schwimmende Wellendichtringe
71	S. Ring	Anwendung der Verzahnungstheorie auf die Modellierung und Simulation des Werkzeugschleifens
72	M. Klöpfer	Dynamisch beanspruchte Dichtverbindungen von Getriebegehäusen
73	C.-H. Lang	Losteilgeräusche von Fahrzeuggetrieben
74	W. Haas	Berührungsfreies Abdichten im Maschinenbau unter besonderer Berücksichtigung der Fanglabyrinthe
75	P. Schiberna	Geschwindigkeitsvorgabe für Fahrsimulationen mittels Verkehrssimulation
76	W. Elser	Beitrag zur Optimierung von Wälzgetrieben
77	P. Marx	Durchgängige, bauteilübergreifende Auslegung von Maschinenelementen mit unscharfen Vorgaben
78	J. Kopsch	Unterstützung der Konstruktionstätigkeiten mit einem Aktiven Semantischen Netz
79	J. Rach	Beitrag zur Minimierung von Klapper- und Rasselgeräuschen von Fahrzeuggetrieben
80	U. Häussler	Generalisierte Berechnung räumlicher Verzahnungen und ihre Anwendung auf Wälzfräserherstellung und Wälzfräsen
81	M. Hüsges	Steigerung der Tolerierungsfähigkeit unter fertigungstechnischen Gesichtspunkten
82	X. Nastos	Ein räumliches Toleranzbewertungssystem für die Konstruktion
83	A. Seifried	Eine neue Methode zur Berechnung von Rollenlagern über lagerinterne Kontakt-Beanspruchungen
84	Ch. Dörr	Ermittlung von Getriebelastkollektiven mittels Winkelbeschleunigungen
85	A. Veil	Integration der Berechnung von Systemzuverlässigkeiten in den CAD-Konstruktionsprozeß
86	U. Frenzel	Rückenstrukturierte Hydraulikstangendichtungen aus Polyurethan
87	U. Braun	Optimierung von Außenzahnradpumpen mit pulsationsarmer Sonderverzahnung
88	M. Lambert	Abdichtung von Werkzeugmaschinen-Flachführungen
89	R. Kubalczyk	Gehäusegestaltung von Fahrzeuggetrieben im Abdichtbereich

Nr.	Verfasser	Titel
90	M. Oberle	Spielbeeinflussende Toleranzparameter bei Planetengetrieben
91	S. N. Dogan	Zur Minimierung der Losteilgeräusche von Fahrzeuggetrieben
92	M. Bast	Beitrag zur werkstückorientierten Konstruktion von Zerspanwerkzeugen
93	M. Ebenhoch	Eignung von additiv generierten Prototypen zur frühzeitigen Spannungsanalyse im Produktentwicklungsprozeß
94	A. Fritz	Berechnung und Monte-Carlo Simulation der Zuverlässigkeit und Verfügbarkeit technischer Systeme
95	O. Schrems	Die Fertigung als Versuchsfeld für die qualitätsgerechte Produktoptimierung
96	M. Jäckle	Untersuchungen zur elastischen Verformung von Fahrzeuggetrieben
97	H. Haiser	PTFE-Compounds im dynamischen Dichtkontakt bei druckbelastbaren Radial-Wellendichtungen
98	M. Rettenmaier	Entwicklung eines Modellierungs-Hilfssystems für Rapid Prototyping gerechte Bauteile
99	M. Przybilla	Methodisches Konstruieren von Leichtbauelementen für hochdynamische Werkzeugmaschinen
100	M. Olbrich	Werkstoffmodelle zur Finiten-Elemente-Analyse von PTFE-Wellendichtungen
101	M. Kunz	Ermittlung des Einflusses fahrzeug-, fahrer- und verkehrsspezifischer Parameter auf die Getriebelastkollektive mittels Fahrsimulation
102	H. Ruppert	CAD-integrierte Zuverlässigkeitsanalyse und -optimierung
103	S. Kilian	Entwicklung hochdynamisch beanspruchter Flächendichtverbindungen
104	A. Flaig	Untersuchung von umweltschonenden Antriebskonzepten für Kraftfahrzeuge mittels Simulation
105	B. Luo	Überprüfung und Weiterentwicklung der Zuverlässigkeitsmodelle im Maschinenbau mittels Mono-Bauteil-Systemen
106	L. Schüppenhauer	Erhöhung der Verfügbarkeit von Daten für die Gestaltung und Berechnung der Zuverlässigkeit von Systemen
107	J. Ryborz	Klapper- und Rasselgeräuschverhalten von Pkw- und Nkw-Getrieben
108	M. Würthner	Rotierende Wellen gegen Kühlschmierstoff und Partikel berührungsfrei abdichten
109	C. Gitt	Analyse und Synthese leistungsverzweigter Stufenlosgetriebe
110	A. Krolo	Planung von Zuverlässigkeitstests mit weitreichender Berücksichtigung von Vorkenntnissen
111	G. Schöllhammer	Entwicklung und Untersuchung inverser Wellendichtsysteme
112	K. Fronius	Gehäusegestaltung im Abdichtbereich unter pulsierendem Innendruck
113	A. Weidler	Ermittlung von Raffungsfaktoren für die Getriebeerprobung
114	B. Stiegler	Berührungsfreie Dichtsysteme für Anwendungen im Fahrzeug- und Maschinenbau
115	T. Kunstfeld	Einfluss der Wellenoberfläche auf das Dichtverhalten von Radial-Wellendichtungen
116	M. Janssen	Abstreifer für Werkzeugmaschinenführungen
117	S. Buhl	Wechselbeziehungen im Dichtsystem von Radial-Wellendichtring, Gegenlauffläche und Fluid
118	P. Pozsgai	Realitätsnahe Modellierung und Analyse der operativen Zuverlässigkeitskennwerte technischer Systeme
119	H. Li	Untersuchungen zum realen Bewegungsverhalten von Losteilen in Fahrzeuggetrieben
120	B. Otte	Strukturierung und Bewertung von Eingangsdaten für Zuverlässigkeitsanalysen
121	P. Jäger	Zuverlässigkeitsbewertung mechatronischer Systeme in frühen Entwicklungsphasen
122	T. Hitziger	Übertragbarkeit von Vorkenntnissen bei der Zuverlässigkeitstestplanung
123	M. Delonga	Zuverlässigkeitsmanagementsystem auf Basis von Felddaten
124	M. Maisch	Zuverlässigkeitsorientiertes Erprobungskonzept für Nutzfahrzeuggetriebe unter Berücksichtigung von Betriebsdaten
125	J. Orso	Berührungsfreies Abdichten schnelllaufender Spindeln gegen feine Stäube
126	F. Bauer	PTFE-Manschettendichtungen mit Spiralrille - Analyse, Funktionsweise und Erweiterung der Einsatzgrenzen
127	M. Stockmeier	Entwicklung von Klapper- und rasselgeräuschfreien Fahrzeuggetrieben
128	M. Trost	Gesamtheitliche Anlagenmodellierung und -analyse auf Basis stochastischer Netzverfahren
129	P. Lambeck	Unterstützung der Kreativität von verteilten Konstrukteuren mit einem Aktiven Semantischen Netz
130	K. Pickard	Erweiterte qualitative Zuverlässigkeitsanalyse mit Ausfallprognose von Systemen
131	W. Novak	Geräusch- und Wirkungsgradoptimierung bei Fahrzeuggetrieben durch Festradentkopplung
132	M. Henzler	Radialdichtungen unter hoher Druckbelastung in Drehübertragern von Werkzeugmaschinen
133	B. Rzepka	Konzeption eines aktiven semantischen Zuverlässigkeitsinformationssystems
134	C.G. Pflüger	Abdichtung schnelllaufender Hochdruck-Drehübertrager mittels Rechteckring und hocheffizient strukturierter Gleitfläche
135	G. Baitinger	Multiskalenansatz mit Mikrostrukturanalyse zur Drallbeurteilung von Dichtungsgegenlaufflächen

Nr.	Verfasser	Titel
136	J. Gäng	Berücksichtigung von Wechselwirkungen bei Zuverlässigkeitsanalysen
137	C. Maisch	Berücksichtigung der Ölalterung bei der Lebensdauer- und Zuverlässigkeitsprognose von Getrieben
138	D. Kirschmann	Ermittlung erweiterter Zuverlässigkeitsziele in der Produktentwicklung
139	D. Weber	Numerische Verschleißsimulation auf Basis tribologischer Untersuchungen am Beispiel von PTFE-Manschettendichtungen
140	T. Leopold	Ganzheitliche Datenerfassung für verbesserte Zuverlässigkeitsanalysen
141	St. Jung	Beitrag zum Einfluss der Oberflächencharakteristik von Gegenlaufflächen auf das tribologische System Radial-Wellendichtung
142	T. Prill	Beitrag zur Gestaltung von Leichtbau-Getriebegehäusen und deren Abdichtung
143	D. Hofmann	Verknüpfungsmodell zuverlässigkeitsrelevanter Informationen in der Produktentwicklung mechatronischer Systeme
144	M. Wacker	Einfluss von Drehungleichförmigkeiten auf die Zahnradlebensdauer in Fahrzeuggetrieben
145	B. Jakobi	Dichtungsgeräusche am Beispiel von Pkw-Lenkungen – Analyse und Abhilfemaßnahmen
146	S. Kiefer	Bewegungsverhalten von singulären Zahnradstufen mit schaltbaren Koppelungseinrichtungen
147	P. Fietkau	Transiente Kontaktberechnung bei Fahrzeuggetrieben
148	B. Klein	Numerische Analyse von gemischten Ausfallverteilungen in der Zuverlässigkeitstechnik
149	M. Klaiber	Betriebs- und Benetzungseigenschaften im Dichtsystem Radial-Wellendichtung am Beispiel von additivierten synthetischen Schmierölen
150	A. Baumann	Rasselgeräuschminimierung von Fahrzeuggetrieben durch Getriebeöle
151	M. Kopp	Modularisierung und Synthese von Zuverlässigkeitsmethoden
152	M. Narten	Abdichten von fließfettgeschmierten Getrieben mit Radialwellendichtungen – Reibungsminderung durch Makrostrukturierung der Dichtungsgegenlauffläche
153	P. Schuler	Einfluss von Grenzflächeneffekten auf den Dichtmechanismus der Radial-Wellendichtung
154	A. Romer	Anwendungsspezifischer Zuverlässigkeitsnachweis auf Basis von Lastkollektiven und Vorwissen
155	A. Daubner	Analyse, Modellierung und Simulation von Verschleiß auf mehreren Skalen zur Betriebsdauervorhersage von Wellendichtringen aus PTFE-Compound
156	J. Rowas	Ökologischer Einsatz der Traktionsarten im System Bahn
157	D. J. Maier	Sensorlose online Zustandserfassung von Vorschubantriebskomponenten in Werkzeugmaschinen
158	J.-P. Reibert	Statisches Abdichten auf nicht idealen Dichtflächen in der Antriebstechnik
159	M. Sommer	Einfluss des Schmierfetts auf das tribologische System Radial-Wellendichtung – Betriebsverhalten und Funktionsmodell
160	W. Haas	Basics der Dichtungstechnik
161	U. Nißler	Dichtheit von Hydraulikstangendichtringen aus Polyurethan
162	S. M. Neuberger	Entwicklung einer gasgeschmierten Gleitringdichtung für den Einsatz im Verbrennungsmotor
163	W. Goujavin	Strömungsmechanische Untersuchungen zur Funktionsweise von Manschettendichtungen aus PTFE-Compounds mit Rückförderstrukturen
164	K. Mutter	Simulation der Zuverlässigkeit von Gesamtfahrzeugfunktionen am Beispiel Fahrkomfort
165	S. Sanzenbacher	Reduzierung von Getriebegeräuschen durch Körperschallminderungsmaßnahmen
166	O. Koller	Zuverlässigkeit von Leistungsmodulen im elektrischen Antriebsstrang
167	M. Remppis	Untersuchungen zum Förderverhalten von Dichtsystemen mit Radial-Wellendichtringen aus Elastomer
168	M. Baumann	Abdichtung drallbehafteter Dichtungsgegenlaufflächen – Messung, Analyse, Bewertung und Grenzen
169	M. Schenk	Adaptives Prüfstandsverhalten in der PKW-Antriebstrangerprobung
170	J. Gölz	Manschettendichtringe aus PTFE-Compounds, Funktionsmechanismus von PTFE-Manschettendichtungen und Entwicklung von Rückförderstrukturen für beidseitig drehende Wellen
171	J. Kümmel	Schmutzabdichtung mittels Fettgefüllter Berührungsfreier Wellendichtungen
172	S. Bader	Gehäusedichtungen unter korrosiver Last
173	J. Juskowiak	Beanspruchungsgerechte Bestimmung des Weibull-Formparameters für Zuverlässigkeitsprognosen
174	F. Jakob	Nutzung von Vorkenntnissen und Raffungsmodellen für die Zuverlässigkeitsbestimmung
175	N. P. Tonius	Klauenschaltelemente in Stufenautomatgetrieben
176	V. Schweizer	Berücksichtigung und Bewertung streuender Einflussgrößen in der Zuverlässigkeitssimulation
177	F. Bosch	Abdichtung trockener Stäube mit fettgefüllten berührungsfreien Wellendichtungen
178	M. Botzler	Präventive Diagnose abnutzungsabhängiger Komponentenausfälle
179	C. Fehrenbacher	Förderverhalten im Dichtsystem Radial-Wellendichtung

Nr.	Verfasser	Titel
180	B. Heumesser	Optimierung des Klapper- und Rasselgeräuschverhaltens bei Doppelkupplungsgetrieben
181	A. Eipper	Einfluss transienter Betriebsbedingungen auf den RWDR im System Radial-Wellendichtung
182	Alexander Buck	Einfluss der Oberflächenrauheit auf den Verschleiß an Hydraulikstangendichtungen
183	Andrea Buck	Simulation und Optimierung der Instandhaltung unter Berücksichtigung sich ändernder Belastungen mittels Petrinetzen
184	St. Kemmler	Integrale Methodik zur Entwicklung von robusten, zuverlässigen Produkten
185	T. Rieker	Modellierung der Zuverlässigkeit technischer Systeme mit stochastischen Netzverfahren
186	M. Bartholdt	Kunden- und kostenorientierte Zuverlässigkeitszielermittlung
187	V. Warth	Systematische Synthese und Bewertung von Stufenlosgetrieben
188	N. Nowizki	Funktionale Sicherheit und Zuverlässigkeit in frühen Phasen der Produktentwicklung
189	F. Schiefer	Additive Fertigung von Radial-Wellendichtringen
190	M. Dazer	Zuverlässigkeitstestplanung mit Berücksichtigung von Vorwissen aus stochastischen Lebensdauerberechnungen
191	J. Totz	Funktionsuntersuchungen an Dichtsystemen mit weichgeschliffenen Dichtungsgegenlaufflächen und Radial-Wellendichtringen aus NBR
192	M. Stoll	Entwicklung und Funktionsanalyse rückenstrukturierter Manschettendichtringe aus PTFE-Compound
193	N. Dakov	Elastohydrodynamische Simulation von Wellendichtungen am Beispiel der PTFE-Manschettendichtung mit Rückförderstrukturen
194	Z. Beslic	Modellierung der Schadensdegradation Zahnradgrübchen bei Fahrzeuggetrieben
195	St. Jetter	Zuverlässigkeitsprognose mechanischer Komponenten auf Basis simulierter Betriebsfestigkeit
196	O. R. Orozco	Availability of Particle Accelerators: requirements, prediction methods and optimization
197	V. Schramm	Dependable System Development Methodology and Case Study for the LHC Beam Loss Monitoring System at CERN
198	J. Gröber	Zuverlässigkeitsanalyse neuartiger mechatronischer Systeme
199	K. Lucan	Methodische Ermittlung von repräsentativen Lastkollektiven am Beispiel der Nutzfahrzeugbremse
200	F. Müller	Realitätsnahe Modellierung, Simulation und Analyse der operativen Zuverlässigkeits- und Verfügbarkeitskennwerte technischer Systeme mit Vertrauensbereich
201	A. Ostertag	Zuverlässigkeit, Sicherheit und Nachhaltigkeit adaptiver Tragwerke
202	A. Kremer	Statistische Versuchsplanung in der Lebensdauererprobung mit Vertrauensintervallen
203	T. Herzig	Anforderungsgerechte Produktauslegung durch Planung effizienter beschleunigter Zuverlässigkeitstests
204	M. Henss	Methodik zur Konzeption, Analyse und Modellierung von Lösungen im Prognostic and Health Management (PHM)
205	Y. Gretzinger	Steigerung der nutzbaren Restlebensdauer von Zahnrädern durch eine adaptive Betriebsstrategie
206	A.J. Köhler	Nachweis der Wirksamkeit zeitdiskreter technischer Sicherheitsmechanismen am Beispiel des automatisierten Fahrens
207	S. Skorsetz	Methode zur Übertragbarkeit von Kraftschlussmessungen an Rollenprüfständen unterschiedlicher Skalierung
208	H. Tavakolinik	Beurteilung der Realisierbarkeit der virtuellen Kupplung in Bezug auf Abstandsregelung
209	F. Long	Realitätsnahe Modellierung und Analyse der Verfügbarkeit von Produktionssystemen in Industrie 4.0
210	S. Imle	Modeling and optimization of safety and availability for subsea all-electric Xmas Trees