Beitrag zur Betrachtung von $MTTF_{Spurious}$-Modellierung im Zusammenhang mit dem internationalen Sicherheitsstandard IEC 61508

P.N. Thao Dang

kassel university press

Pham Nhu Thao Dang

Beitrag zur Betrachtung von $MTTF_{Spurious}$-Modellierung im Zusammenhang mit dem internationalen Sicherheitsstandard IEC 61508

kassel university press

Die vorliegende Arbeit wurde vom Fachbereich Elektrotechnik / Informatik der Universität Kassel als Dissertation zur Erlangung des akademischen Grades eines Doktors der Ingenieurwissenschaften (Dr.-Ing.) angenommen.

Gutachter: Prof. Dr. Michael H. Schwarz
Prof. Dr. Ilker Üstoglu

Weitere Mitglieder des Promotionsausschusses: Prof. Dr.-Ing. habil. Peter Lehmann
Prof. Dr. rer. nat. Hartmut Hillmer

Tag der mündlichen Prüfung: 04. August 2016

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Zugl.: Kassel, Univ., Diss. 2016
ISBN 978-3-7376-0204-4 (print)
ISBN 978-3-7376-0205-1 (e-book)
DOI: http://dx.medra.org/10.19211/KUP9783737602051
URN: http://nbn-resolving.de/urn:nbn:de:0002-402057

Printed in Germany

Für meine Familie

Danksagung

Die vorliegende Arbeit entstand im Rahmen meiner wissenschaftlichen Tätigkeit als Doktorand an der Universität Kassel am Lehrstuhl für Rechnerarchitektur und Systemprogrammierung.

Mein besonderer Dank gilt meinem Doktorvater Herrn Prof. Dr. Michael H. Schwarz für die hervorragende Betreuung und Unterstützung, die weit über den Rahmen dieser Arbeit hinausging. Daneben möchte ich Herrn Prof. Dr. Ilker Üstoglu, Herrn Prof. Dr.-Ing. habil. Peter Lehmann und Herrn Prof. Dr. rer. nat. Hartmut Hillmer für die Mitwirkung in der Prüfungskommission danken.

Ebenso möchte ich meinen Arbeitskollegen für die stets gute Arbeitsatmosphäre und die jederzeit vorhandene Bereitschaft zur Unterstützung und Zusammenarbeit bedanken. Herr Prof. Dr.-Ing. habil. Josef Börcsök, Herr Dr.-Ing. Peter Holub, Herr Dr.-Ing. Daod Machmur und Herr Dipl.-Ing. Jürgen Hölzel möchte ich für die vielen fachlichen Diskussionen und Anregungen meinen Dank aussprechen. Allen weiteren Kolleginnen und Kollegen, besonders Herr Dr.-Ing Tarif Amro, Herr Dipl.-Ing. Mike Wagner und Herr Karl Lukas, die durch fachliche sowie persönliche Unterstützung zum Gelingen dieser Doktorarbeit beigetragen haben, sei hier gedankt.

Danken möchte ich auch allen Mitarbeiter des Fachgebietes Rechnerarchitektur und Systenprogrammierung der Universität Kassel.

Des Weiteren möchte ich mich bei all denjenigen Personen bedanken, die mir während der Arbeit ihre volle Unterstützung zukommen ließen.

Schließlich gebührt ein besonderer Dank meinen Eltern sowie meinem Bruder, meinem Mann und meinen Freunden, besonders Frau Dr.-Ing. Hong Hanh Mai, die mich auf meinem bisherigen Weg stets unterstützt und begleitet haben und widme ich diese Arbeit unserem kleinen Sohn Ben.

Zusammenfassung

Um das Risiko von Fehlern einer Anlage zu minimieren, werden sicherheitsrelevante Systeme entwickelt, damit die Anlage überwacht werden kann und, im Falle eines Fehlverhaltens, das Gesamtsystem rechtzeitig sicher reagieren kann. Je nach dem Anwendungsbereich wird der sichere Zustand bzw. die Sicherheitsfunktion anders definiert. Der sichere Zustand kann ein stromloser Zustand oder ein stromführender Zustand sein. Ob das sicherheitsrelevante System in der Betriebsart mit niedriger Anforderungsrate oder in der Betriebsart mit hoher Anforderungsrate eingesetzt werden soll, wird durch ein Konzept für die Implementierung des sicherheitsrelevanten Systems bestimmt. In der Norm IEC 61508 [48] werden zum Beispiel die Anforderungen für sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme definiert. Tritt ein Fehler innerhalb des Bereichs der Hardwarefehlertoleranz auf, wird die Sicherheitsfunktion ausgeführt. Allerdings sind die sicherheitsrelevanten Systeme nicht immer für die Verfügbarkeitsbetrachtung besonders geeignet, da der stromlose Zustand durch einen Spurious-Trip Fehler[1] erreicht werden kann. Somit ist der Prozess der zu überwachenden Anlage nicht mehr verfügbar. Durch solche Zwischenfälle kann es nicht nur zu wirtschaftlichen Schäden, sondern auch zu großen Schäden für Menschen kommen. Daher ist es wichtig, solche Ausfälle aufgrund von Spurious-Trip zu betrachten und dessen Parameter zu bewerten.

Diese Dissertation legt den Fokus auf die Fehler, die aufgrund von Spurious-Trip im Zusammenhang mit der Norm IEC 61508 [48] entstehen. Die Unterschiede zwischen den unterschiedlichen Betriebsarten werden in der Arbeit noch mal kurz beschrieben und diskutiert. Aus diesen Unterschieden werden die neuen Gleichungen für die Bestimmung der Parameter des Spurious-Trip Ausfalls bestimmt. Die Ergebnisse werden durch ein Beispiel evaluiert und dann mit den herkömmlichen Formeln verglichen und diskutiert. Die Analyse des Spurious-Trip Ausfalls und die Berechnung dessen Parameter werden mittels Blockdiagramm und Markov-Modell durchgeführt.

Schlüsselwörter: Spurious-Trip Rate, PFS[2], PFS_{avg}[3], $MTTF_{Spurious}$[4], niedrige Anforderungsrate, hohe Anforderungsrate

[1] Spurious-Trip Fehler ist ein unerwarteter Fehler, weswegen das System in den sicheren Zustand geht.
[2] PFS: Probability of Failure Spurious-Trip
[3] PFS_{avg}: Average Probability of Failure Spurious-Trip
[4] $MTTF_{Spurious}$: Mean Time To Failure Spurious-Trip

Abstract

To minimize the risk of errors of a plant, safety systems are developed to respond to hazardous events and unwanted events. So the plant can reach the safe state in time. Depending on the application sectors the safe state or the safety function is defined differently. The safe state may be an energized state or a de-energized state. Whether the safety system is to be used in the mode with low demand rate or in the mode with high demand rate, is determined by a concept for the implementation of the safety system. In the standard IEC 61508 [48] the requirements are defined for a safety-related systems comprised of electrical and/or electronic and/or programmable electronic. If an error occurs within the range of hardware fault tolerance, the safety function is executed. However, the safety systems are not always for the point of view of availability perspective particularly suitable, since the de-energized state can lead to a spurious trip error[5]. Therefore, spurious activation normally leads to lost production or low availability of the plant. Some of the spurious activations can lead to a hazardous state and a great damage for humans. So the plant cost can be extremely increased. Therefore, it is important to consider such failures due to spurious trip and evaluate its parameters.

This dissertation focuses on the errors that arise due to spurious trip in connection with the IEC 61508 [48]. The differences between the different modes are briefly described in the work and discussed with what is described in IEC 61508. From these differences, the new equations are determined that leads to the spurious trip failure. The results will be evaluated through example, and then compared with the predetermined formulas and discussed. The spurious trip failure and the calculation of its parameters are analysed by using of block diagram and Markov model.

Key-Words: Spurious-Trip Rate, PFS[6], PFS_{avg}[7], $MTTF_{Spurious}$[8], low demand rate, high demand rate

[5] Spurious trip error is an unwanted failure and leads the plant in to the safe state.
[6] PFS: Probability of Failure Spurious-Trip
[7] PFS_{avg}: Average Probability of Failure Spurious-Trip
[8] $MTTF_{Spurious}$: Mean Time To Failure Spurious-Trip

Inhaltsverzeichnis

Abkürzungsverzeichnis

CCF	Common Cause Failure
DIN	Deutsches Institut für Normung
E/E/PE System	Electrical/Electronic/Programmable Electronic System
EUC	Equipment Under Control
FTA	Fault Tree Analysis
MA	Markov Analysis
IEC	International Electrotechnical Commission
IEV	International Electrotechnical Vocabulary
ISA	The Instrumentation, Systems, and Automation Society Seit 2008: The International Society of Automation
PDS	Pålitelighet av Databaserte Sikkerhetssystemer (Reliability of Computer-based Safety Systems)
RBD	Reliability Block Diagram
SIS	Safety Instrumented System
FD	False Demand

Abbildungsverzeichnis

Tabellenverzeichnis

Symbolverzeichnis

β_S	Wichtung für CCF aufgrund der sicheren Fehler
β_D	Wichtung für CCF aufgrund der gefährlich erkannten Fehler
$\lambda(t)$	Failure rate, deut. Ausfallrate
f(t)	Density function of failure
MDT	Mean Down Time
MTBF	Mean Time Between Failure
$MTTF_{Spurious}$	Mean Time To Failure Spurious-Trip
MTTR	Mean Time To Repair
$MTTR_S$	Mean Time To Repair Safe Failure
$MTTR_D$	Mean Time To Failure Dangerous Detected Failure
MUT	Mean Up Time
P(t)	Probability of Failure
PA	Point Availability
PFD	Probability of Failure on Demand
PFD_{avg}	Average Probability of Failure on Demand
PFH	Probability of Failure per Hour
PFS	Probability of Failure Spurious-Trip
PFS_{avg}	Average Probability of Failure Spurious-Trip
R(t)	Reliability
SIL	Safety Integrity Level
STR	Spurious-Trip Rate
HFT	Hardware Fault Tolerance, deut. Hardware-Fehlertoleranz
HFT_D	Hardware-Fehlertoleranz in Bezug auf Sicherheitsfunktion
$HFT_{Spurious}$	Hardware-Fehlertoleranz in Bezug auf Spurious-Trip
T	Characteristic lifetime, deut. Charakteristische Lebensdauer oder Lageparameter
t_0	zeitliche Abzugsgröße oder Korrekturparameter
λ_{DE}	Demand rate, deut. Anforderungsrate
τ_{DE}	Demand duration, deut. Anforderungsdauer
λ_D	Dangerous failure rate, deut. Rate der gefährlichen Fehler

λ_{DD}	Dangerous detected failure rate, deut. Rate der gefährlich erkannten Fehler
λ_{DU}	Dangerous undetected failure rate, deut. Rate der gefährlich unerkannten Fehler
λ_{S}	Safe failure rate, deut. Rate der sicheren Fehler
λ_{SD}	Safe detected failure rate, deut. Rate der sicheren erkannten Fehler
λ_{SU}	Safe undetected failure rate, deut. Rate der sicheren erkannten Fehler
STR_{koon_FD}	Spurious-Trip Rate due to False Demand of a koon-Architecture
STR_{koon_S}	Spurious-Trip Rate due to Safe Failure of a koon-Architecture
STR_{koon_DD}	Spurious-Trip Rate due to Dangerous Detected Failure of a koon-Architecture
STR_{koon_CCF}	Spurious-Trip Rate due to Common Cause Failure of a koon-Architecture

1 Einleitung

Seit einigen Jahren steigt das Gefahrenrisiko für Mensch und Umwelt, da Automatisierungssysteme immer komplexer werden [16]. Um diese Gefahren und Risiken für Mensch und Umwelt zu minimieren, ist es notwendig, Sicherheitssysteme mit hoher Zuverlässigkeit und Sicherheit zu entwickeln. Da jedoch auch bei diesen Sicherheitssystemen Fehlfunktionen oder Ausfälle auftreten können, werden sicherheitstechnische Schutz- und Kontrollsysteme entwickelt und integriert. Dabei wird zwischen den zu überwachenden Anlagen (engl. Equipment Under Control EUC) und dem Sicherheitssystem unterschieden (siehe Abbildung 1.1).

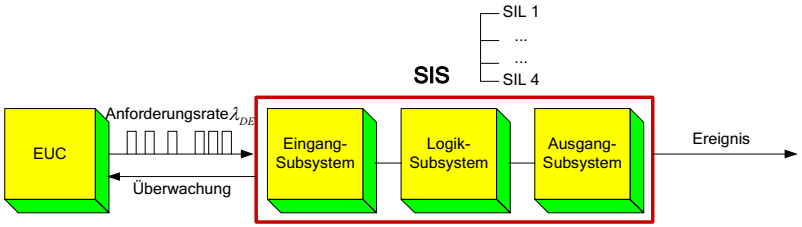

Abbildung 1.1: EUC und SIS [45], [68]

Das EUC umfasst alle Einrichtungen, Maschinen, Geräte oder Anlagen, die Gefährdungen verursachen können und wird von einem oder mehreren sicherheitsbezogenen Systemen[9] (SIS) überwacht [48]. Falls ein unerwartetes Ereignis durch das EUC verursacht wird, sind Sicherheitsfunktionen notwendig, um das EUC in den sicheren Zustand zu bringen, damit größere Schäden vermieden werden können. Die Häufigkeit der Anforderung des EUC an das SIS in einem Zeitintervall wird als Anforderungsrate[10] λ_{DE} bezeichnet und wird als homogener Poisson-Prozess modelliert [77]. Die Anforderungsrate lässt sich nach folgender Gleichung bestimmen:

$$\lambda_{DE} = \frac{N_{DE}(t)}{t} \qquad \textbf{(1.1)}$$

wobei: $N_{DE}(t)$ ist die Anzahl der Anforderungen in einem Zeitintervall t.

Die Zeit, wie lange eine Anforderung dauert, wird als Anforderungsdauer[11] τ_{DE} bezeichnet. In dieser Zeit muss das SIS unbedingt die Sicherheitsfunktion richtig ausführen, um das Gesamtsystem in den sicheren Zustand zu bringen. Falls das SIS in dieser Zeit die Sicherheitsfunktion nicht richtig ausführt, ist das Gesamtsystem in einem sehr gefährlichen Zustand. Eine Ka-

[9] SIS: Safety Instrumented System, wird in Punkt 3.2.72 im Teil 1 des Standards IEC 61511 [49] definiert.
[10] Demand rate
[11] Demand duration

tastrophe kann danach folgen. Die Anforderungsdauer ist bei jedem System unterschiedlich [77].

Die Sicherheitsfunktionen werden durch ein oder mehrere sicherheitsbezogene Systeme ausgeführt. In der Norm IEC[12] 61511 [49], die von der Norm IEC 61508 [48] abgeleitet ist, wird ein sicherheitsbezogenes System auch als „sicherheitstechnisches System" für die Prozessindustrie definiert. Ein SIS besteht aus einer beliebigen Kombination von Sensoren (Eingang-Subsystem), Logik (Logik-Subsystem) und Aktuatoren (Ausgang-Subsystem) und wird verwendet, um gefährliche Fehler im System zu erkennen und die Sicherheitsfunktionen auszuführen. Um ein SIS auf seine funktionale Sicherheit bewerten zu können, muss deshalb die gesamte Verarbeitungskette vom Sensor bis zum Aktuator betrachtet werden. Der Ausfall einer Sicherheitsfunktion kann fatale Folgen für Mensch und Umwelt bedeuten. Je nach Anwendung ergeben sich für ein SIS nach einem angestrebten Sicherheits-Intergritätslevel (SIL[13]) die sicherheitsgerichteten Konstruktionsprinzipien, die eingehalten werden müssen, um das Gefahrrisiko zu minimieren. Die Normen IEC 61508 [48] und IEC 61511 [49] definieren vier unterschiedliche Sicherheitsstufen, die qualitativ auf dem PFD_{avg} [14]- oder PFH [15]-Wert basieren. Je höher der Zahlenwert des SIL ist, desto größer ist die Risikoreduzierung.

In der Prozessindustrie wird Sicherheit allgemein definiert als: „*relativer Zustand, der als Gefahrenfreiheit angesehen wird, der stets nur für einen bestimmten Zeitraum, eine bestimmte Umgebung oder unter bestimmten Bedingungen gegeben ist*", [89], [I02], [I03].

In diesem Bereich haben sich SISs in der Regel als Emergency Shutdown Systeme (ESD) durchgesetzt. Jede Funktion, die in einem SIS implementiert ist, wird als Sicherheitsfunktion bezeichnet. Die Sicherheitsfunktion wird normalerweise in Betriebsart mit niedriger Anforderungsrate (Low-Demand-Mode) implementiert.

Das SIS kann aus einer von zwei unterschiedlichen Sichten betrachtet werden: eine aus Sicht der Sicherheit und eine andere aus Sicht der Verfügbarkeit, [46]. In Houtermans [46] und Buddy Creef [I01] wird Sicherheit als Sicherheitsverfügbarkeit und Verfügbarkeit als Prozessverfügbarkeit (oder Betriebsverfügbarkeit) bezeichnet. Eine zusätzliche Bedeutung der Verfügbarkeit wird in der Prozessindustrie aus der Sicht der Sicherheitsfunktion definiert: Verfügbarkeit einer Sicherheitsfunktion [64].

Um die Sicherheit oder die Verfügbarkeit eines SIS zu erhöhen, werden fehlertolerante Systeme eingesetzt. Hier ist anzumerken, dass zwischen der Sicherheits- und der Verfügbarkeits-Redundanz ein großer Unterschied besteht. Dieser Unterschied soll hier verdeutlicht werden. Ein unerwünschtes Ereignis in einem redundanten Verfügbarkeitssystem kann fatale Folgen für die Verfügbarkeit haben, muss aber nicht zwangsläufig die Sicherheit beeinträchtigen und

---

12 Norm der International Electrotechnical Commission IEC
13 SIL: Safety Integrity Level [48]
14 PFD_{avg}: Average Probability of Failure on Demand (durchschnittliche Ausfallwahrscheinlichkeit bei Anforderung)
15 PFH: Probability of Failure per Hour (Ausfallwahrscheinlichkeit pro Stunde)

umgekehrt, d. h. die Erhöhung der Sicherheit verringert in vielen Fällen die Betriebsverfügbarkeit und umgekehrt. Zum Beispiel: wird beim ersten Auftreten eines HW[16]-Fehlers immer sofort abgeschaltet (sicherer Zustand), so ist zwar die Systemsicherheit gewährleistet, aber die Betriebsverfügbarkeit ist gering. Gerade deshalb müssen „Sicherheit" und „Verfügbarkeit" getrennt behandelt werden [02] oder das Verhältnis Verfügbarkeit und Sicherheit muss durch zielführende Anwendung der IEC 61508 optimiert werden [I06]. Bei einem SIPS[17] haben Panteli und Crossley [75] die Sicherheit und Verfügbarkeit mit verschiedenen Strategien bewertet, wobei die Bewertungen auf die Bestimmung des SIL und des STL[18] basieren. Als Ergebnis haben die beiden Autoren gezeigt, dass die Verfügbarkeit immer größer wird, wenn die Sicherheit immer kleiner wird. Beer und Rau [I06] haben gezeigt, dass die Einhaltung der Sicherheit bei gleichzeitiger Erhöhung der Verfügbarkeit eines Fahrzeugs nicht im Widerspruch stehen muss. Wang und Bai [99] haben eine Optimierung vorgeschlagen, die auf Genetischen Algorithmen (GA) basieren, um Sicherheit und Zuverlässigkeit im Designprozess eines SIS zu realisieren. Um Sicherheit und Verfügbarkeit sicher zu beurteilen und sicherheitsrelevante Sicherheitssysteme zu entwickeln, wurden für die Umsetzung dieser Sicherheitssysteme internationale Standards entworfen. In Europa ist die Norm IEC 61508 [48] eine allgemeine Norm für mehrere Branchen und wird häufig von Herstellern bei der Entwicklung neuer Produkte verwendet. Die Norm ermöglicht die Bereitstellung einer allgemeingültigen Grundlage für die Implementierung anwendungsorientierter Standards. Zentrales Element ist die Bestimmung eines Sicherheitsintegritätslevels[19]. Aus der IEC 61508 [48] wurden weitere Normen abgeleitet, die für das jeweilige Anwendungsgebiet angepasst wurden. Dazu zählen z. B. die IEC 62061 [50] für den Maschinenbau, die IEC 61511 [49] für die Prozessindustrie sowie die ISO 26262 [51] für die Automobilindustrie. Ähnlich wie die Norm IEC 61508 [48] definiert die Norm IEC 61511 [49] auch vier Sicherheitsstufen, SIL 1 bis SIL 4, die die Maßnahmen zur Risikoreduzierung auf ein vertretbares Niveau beschreiben. In den USA wurden die Standards ANSI/ISA-TR84.00.xx[20] [05], [06], [07], [08] entwickelt und werden in der Prozess-Industrie angewendet. Besonders wird in der Norm ANSI/ISA TR84.00.02-2002 [06] die Spurious-Trip Rate (STR) bzw. die mittlere Zeit bis zum Spurious-Trip Ausfall ($MTTF_{Spurious}$ [21]) eines SIS durch verschiedene Methoden wie die Methode der einfachen Gleichungen (abgeleitet von der Blockdiagramm-Methode, Fehlerbaum und Markov-Modell bestimmt).

16 Hardware
17 SIPS: System Integrity Protection Schemes
18 STL: Spurious-Trip Level
19 SIL: Safety Integrity Level
20 The Instrumentation, Systems, and Automation Society
21 $MTTF_{Spurious}$: Mean Time To Failure Spurious-Trip

1.1 Stand der internationalen Normen

Die im vorherigen Abschnitt definierten unterschiedlichen Betrachtungsweisen von SIS-Sicherheit und Verfügbarkeit werden in diesem Abschnitt konkretisiert. Ein SIS wird aus zwei unterschiedlichen Sichten betrachtet: einmal aus der Sicht der Sicherheit und einmal aus der Sicht der Verfügbarkeit. Nach der Sicherheitsbetrachtung werden die Parameter wie PFD_{avg}, PFH, $MTTF$ [22] berechnet, um den SIL zu beurteilen. Die Norm IEC 61508 [48] unterscheidet zwischen der Betriebsart mit niedriger Anforderungsrate[23] und der Betriebsart mit hoher Anforderungsrate[24] oder Betriebsart mit kontinuierlicher Anforderung[25]. Grundlage dieser unterschiedlichen Betriebsarten bildet den Parameter „Anforderungsrate", d. h. wie häufig die Anforderung an die Sicherheitsfunktion im System gestellt wird. Eine Anforderung ist ein Ereignis oder eine Bedingung, die die Sicherheitsfunktion zu aktivieren erfordert, um ein unerwünschtes Ereignis zu verhindern oder um die Auswirkung eines unerwünschten Ereignisses zu mildern [77]. Die Anforderung kann die Änderung von Eingangssignalen des Prozesses oder das Auftreten eines internen Fehlers sein. Die Häufigkeit der Anforderung wird oft als ein homogener Poisson-Prozess dargestellt [77].

Eine Sicherheitsfunktion, die in niedriger Anforderungsrate arbeitet, wird auf Anforderung ausgeführt und bringt das zu überwachende System in einen definierten sicheren Zustand. Die Anforderungsrate beträgt in diesem Fall nicht mehr als einmal pro Jahr T_1 [48]. Das sicherheitsbezogene E/E/PE-System[26], das diese Sicherheitsfunktion ausführt, hat keinen Einfluss auf das EUC, bevor eine Anforderung kommt, zum Beispiel: Notabschaltsystem oder Schutzsysteme in chemischen Anlagen. Da die Anforderung normalerweise immer seltener als einmal im Jahr auftritt, ist für die Prozessindustrie die Betriebsart mit hoher Anforderungsrate in den meisten Fällen bedeutungslos [I08].

Bei der Betriebsart mit kontinuierlicher Anforderung hält die Sicherheitsfunktion die EUC immer in seinem normalen sicheren Zustand als Teil des normalen Betrieb [48].

Eine Sicherheitsfunktion, die in hoher Anforderungsrate arbeitet, wird auf Anforderung ausgeführt, um das zu überwachende System in einen definierten sicheren Zustand zu bringen, und die Anforderungsrate in diesem Fall beträgt mehr als einmal pro Jahr [48]. Ein gefährlicher Ausfall des SIS führt unmittelbar zu einer Gefährdung, falls es keine weiteren Maßnahmen im System zur Risikominderung gibt. Beispiele hierfür sind die Drehzahlüberwachungen an Maschinen oder Eisenbahn-Signal-System. Daher wird diese Betriebsart meist in der Fertigungstechnik angewandt [I08].

---

22 MTTF: Mean Time To Failure
23 „Low Demand Mode", wird im Standard IEC 61508 [48], Teil 4, Punkt 3.5.16 definiert.
24 „High Demand Mode", wird im Standard IEC 61508 [48], Teil 4, Punkt 3.5.16 definiert.
25 „Continuous Mode", wird im Standard IEC 61508 [48], Teil 4, Punkt 3.5.16 definiert.
26 E/E/PE-System: elektrischer/elektronischer/programmierbarer elektronischer System

Ein weiterer unterschiedlicher Punkt zwischen Betriebsart mit niedriger Anforderungsrate und Betriebsart mit hoher Anforderungsrate ist der Anteil von systematischen Fehlern. Der Anteil systematischer Fehler ist bei der Betriebsart mit niedriger Anforderungsrate höher als bei der Betriebsart mit hoher Anforderungsrate. W. Krämer et. al. [I07] stellt diesen Zusammenhang in folgender Abbildung dar:

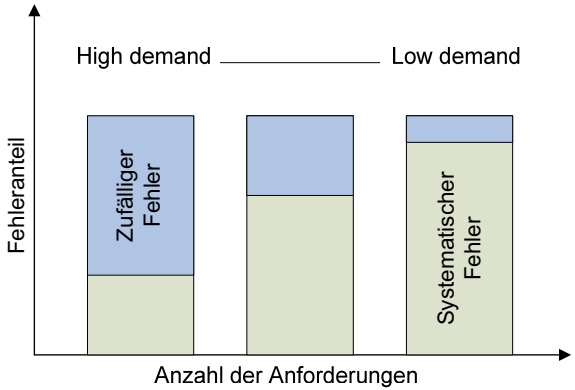

Abbildung 1.2: Fehlerverteilung für elektromechanische Komponente [I07]

Da die zufälligen Fehler im System bei der Betriebsart mit hoher Anforderungsrate im Vergleich zu der Betriebsart mit niedriger Anforderungsrate relativ oft auftreten, werden deshalb mehr Maßnahmen zur Fehlererkennung im System implementiert. Daher ist der Diagnosedeckungsgrad bei der Betriebsart mit hoher Anforderungsrate größer als bei der Betriebsart mit niedriger Anforderungsrate.

Je nach Betriebsart werden die Ausfallgrenzwerte für sicherheitsbezogene Systeme unterschiedlich festgelegt. Und zwar:

- PFD_{avg} : mittlere Ausfallwahrscheinlichkeit der Funktion im Anforderungsfall (Average Probability of Failure on Demand) oder
- PFH : Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (Probability of Failure per Hour).

Detaillierte Informationen befinden sich in Abschnitt 3.5.13 in Teil 4 der IEC 61508 [48]. Je kleiner der PFD_{avg} bzw. der PFH -Wert ist, desto sicherer ist das System. Der ideale Wert wäre Null, der aber nie erreicht werden kann, da immer ein Restrisiko verbleibt. Je nach Randbedingung wird entweder die Versagenswahrscheinlichkeit im Fall einer Anforderung (PFD) oder die Ausfallwahrscheinlichkeit pro Stunde (PFH) bestimmt. Aus diesen Werten kann dann der SIL-Wert bestimmt werden.

Die Unterschiede zwischen Betriebsart mit hoher Anforderungsrate und Betriebsart mit niedriger Anforderungsrate haben Einfluss auf die Berechnung des PFD_{avg} und PFH -Werts [59]. Liu Y. und Raussand M. [59] haben gezeigt, wie abhängig der PFD_{avg} und PFH -Wert von der Anforderungsrate und Anforderungsdauer sind. Weiter haben Liu Y. und Raussand M. [60] die Beziehung zwischen Anforderungsrate und Verfügbarkeit eines SISs mit verschiedenen Test-Strategien (simultaneous, sequential und staggered testing) untersucht. Für diese Untersuchung haben die beiden Autoren ein 1oo2-System mittels Petri-Netz analysiert. Allerdings wurden die Unterschiede zwischen Betriebsart mit hoher Anforderungsrate und Betriebsart mit niedriger Anforderungsrate für verschiedene SIS-Konfigurationen in der Studie nicht betrachtet.

Um ein SIS nach der Verfügbarkeit zu bewerten, ist die Spurious-Trip Rate (STR) bzw. Mean Time To Failure Spurious-Trip ($MTTF_{Spurious}$) zu berechnen. Diese Variable gibt an, wie oft ein SIS einen Spurious-Trip Ausfall erwartet und die Anlage heruntergefahren werden muss. In den Arbeiten von Alejandro Esparza, Monica Levy Hochleitner [32] als auch Miller et. al. [73] wurden die Zeitdauer eines Herunterfahrens von unterschiedlichen Prozessen und die Kosten eines solchen Vorfalls, der aufgrund eines Spurious-Trips erfolgt, ermittelt. Die folgende Tabelle zeigt die Schätzung der Schadenskosten eines Spurious-Trip Ausfalls in der Prozessindustrie [32], [73].

Tabelle 1.1: Spurious-Trip Kosten in der Prozessindustrie [32], [73]

Prozess Applikation	**Spurious-Trip Kosten (in US Dollars)**
Oil & Gas Platforms	bis zu $2 Million pro Tag
Polystyrene	20 Tage zu prüfen mit $20k pro Tag = $400k
Refinery Coker Heater	$35k pro Tag
Refinery Catalytic Cracker	$500k
Complete Refinery	$1 Million pro Tag
Ammonia & Urea Plants	$1 Million pro Tag
Power Generation	$100k/MW Stunden bis $Million pro Seite
Ethylene	$1 Million gehört immer Produkt nach Spezifikation

Besonders in der Öl- und Gas-Industrie ist es sehr wichtig, die Anzahl von Spurious-Trip Ausfällen zu reduzieren. Dadurch können nicht nur unnötige Produktionsausfälle, sondern auch die Risiken, die im Zusammenhang mit Belastungen durch falsche Aktivierung (spurious activation) verursacht werden, vermieden werden. Außerdem werden dadurch auch die Gefahren bei der außerplanmäßigen Systemwiederherstellung und beim Neustart vermieden [65].

In der Norm IEC 61511 (Teil 1) [49] wird „Spurious-Trip“ als „ungefährlicher Ausfall“ [27] definiert. Das ist der *„Ausfall ohne das Potential, das sicherheitstechnische System in einen gefahrbringenden oder funktionsunfähigen Zustand zu setzen“* (Abschnitt 3.2.65 in [49]). Hier wird auch der maximale Wert für die Spurious-Trip Rate *STR* in der Spezifikation der Sicherheitsanforderungen an das SIS angegeben (Abschnitt 10.3 in [49]) aber es gibt keine Herleitung wie dieser Wert bestimmt wird. Die Berechnung der *STR* bzw. $MTTF_{Spurious}$ eines SIS wird in der Norm ANSI/ISA TR84.00.02-2002 [06] durch verschiedene Methoden wie Blockdiagramm, Fehlerbaum und Markov-Modell bestimmt.

In der Öl-Industrie in Norwegen wird die Methode PDS [86], [87], [88] verwendet, um die Spurious-Trip Rate *STR* bzw. $MTTF_{Spurious\_Trip}$ eines SISs zu berechnen. PDS ist eine norwegische Abkürzung für „**P**ålitelighet av **D**atabaserte **S**ikkerhetssystemer“ und bedeutet im Englischen „Reliability of computer based safety system“ [38]. Diese Methode wird verwendet, um die Zuverlässigkeit, Sicherheit und den Lebenszyklus (Life Cycle Cost = LCC) eines computerbasierten Sicherheitssystems zu quantifizieren. Die PDS-Methode ist in der Öl-Industrie in Norwegen verbreitet und wird auch in vielen anderen Fachbereichen, wie Eisenbahn, Prozessindustrie usw... angewendet [86], [87], [88]. Die PDS-Methode basiert auf den Grundsätzen der Normen IEC 61508 [48] und IEC 61511 [49]. Um einige Unklarheiten in den IEC Normen zu vermeiden, verwendet die PDS-Methode eine andere Interpretation der Ausfallklassifikation und schlägt einen alternativen Ansatz zur Modellierung des Ausfalls infolge gemeinsamer Ursachen[28] (CCF) vor und beschreibt wie der systematische Fehler berücksichtigt werden soll. Die Abbildung 1.3 stellt den Unterschied der Klassifikation von Ausfällen zwischen der Norm IEC 61508 [48] und dem PDS-Handbuch dar [86], [87], [88].

[27] safe failure

[28] CCF: „Common Cause Failures: “Systemausfall, bei dem zwei oder mehreren getrennten Kanälen in einem mehrkanaligen System wegen einer Ursache gleichzeitig ausfällen (Teil 4 der Norm IEC 61508 [48])

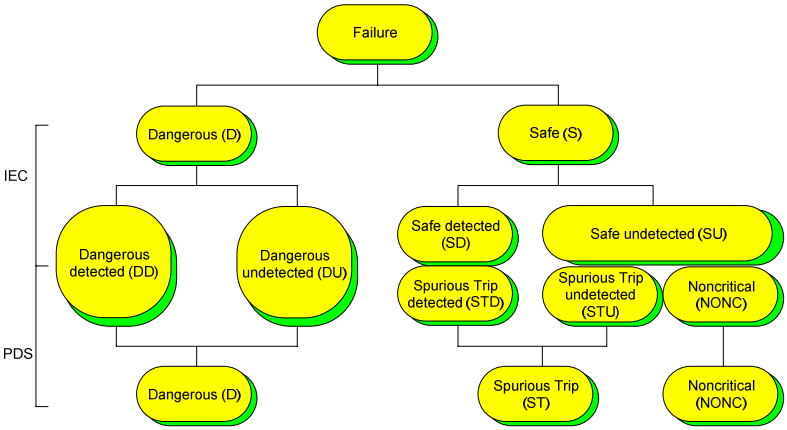

Abbildung 1.3: Klassifikation der Ausfälle [86], [87], [88]

Während der *PFD*-Wert in der Norm IEC 61508 als die Wahrscheinlichkeit, dass das SIS unfähig ist, die Sicherheitsfunktion auf Anforderung auszuführen, definiert wird, wird der *PFD*-Wert in der PDS[29]-Methode durch den gefährlich unerkannten Fehler, Konfigurationsfaktor und dem *CCF* [30]-Faktor bestimmt.

Die PDS Methode führt auch einen neuen sicherheitsrelevanten Parameter *CSU* ein. *CSU* steht für *„Critical Safety Unavailability“* und gibt die Wahrscheinlichkeit an, dass eine Komponente oder ein System wegen eines zufälligen gefährlichen Ereignisses ausgefallen ist.

Außerdem behandelt die PDS-Methode den *STR* [31]-Wert. Der *STR*-Wert ist vom sicheren unerkannten Fehler abhängig. Je nach Architektur der System-Komponente wird der Common Cause Faktor β für die Bestimmung des *STR*-Werts mitberücksichtigt.

1.2 Stand der Technik

Die Berechnung des *STR*-Werts und dessen Einflüsse auf die Verfügbarkeit bzw. auf die Kosten eines Systems werden in zahlreichen Beiträgen beschrieben. Allerdings ist es beim Vergleich dieser Formeln offensichtlich, dass es keine eindeutige Auslegung des Begriffs des Spurious-Trips gibt. Während die PDS-Methode [86], [87], [88] Spurious-Trip als Spurious-Aktivierung eines SIS-Element oder einer SIF definiert, wird Spurious-Trip in der ANSI/ISA 84 [05], [06], [07], [08] als „non-intended process shutdown“ betrachtet. Deswegen ist es schwierig die *STR* in verschiedenen Applikationen zu vergleichen, denn die Konzepte des Spurious-Trips sind unterschiedlich. Mary Ann Lundteigen und Marvin Rausand [65] haben

[29] PDS: Pålitelighet av Databaserte Sikkerhetssystemer
[30] CCF: Common Cause Failure
[31] STR: Spurious-Trip Rate

die Ursachen und Wirkungen von Spurious-Trip entsprechend den Konzepten in den Normen IEC 61508, IEC 61511 und OREDA (**O**ffshore **RE**liabiliy **DA**ta) diskutiert. Dazu sind die neuen Begriffe von „Spurious-Operation", „Spurious-Trip" und „Spurious-Shutdown" definiert und erklärt. Die neuen Formeln wurden für die Berechnung der STR präsentiert. Diese Formeln erfassen alle wichtigen Parameter von Ursachen des Spurious-Trips, entsprechend verschiedenen Arten von gefährlichen und Spurious Operation-Ausfällen zu Spurious-Trip und sind für alle Architekturen geeignet. Im Gegensatz zur PDS-Methode [86] und ANSI/ISA 84 [06] wurden die Faktoren von CCF aufgrund der Spurious Operation (β^{SO}) und gefährlichen Ausfällen (β^{D}) in dem Beitrag unterschieden. Anschließend wurden die beschriebenen Formeln mit den Formeln, die in der Öl- und Gas-Industrie oft verwendet werden, verglichen. Allerdings sind die Formeln von Mary Ann Lundteigen und Marvin Rausand [65] durch Verwendung eines einfachen Ansatzes (Simplified equations) aus dem Blockdiagramm gebildet und die Ergebnisse der Berechnungen sind deshalb ungenauer als durch Verwendung von Markov-Modellen. Bukowski [21], [20] hat sichere Fehler auch als Spurious-Trip genannt und die Berechnung des $MTTF_S$ [32]-, $MTTF_D$ [33]- und $MTTF$ -Wertes für einen Safety Shutdown Controller mit dem Markov-Modell durchgeführt.

Der Ansatz von Lu und Jiang in [63] ist ähnlich wie der von Mary Ann Lundteigen und Marvin Rausand [65]. Lu und Jiang betrachten die Anzahl der Spurious-Operation als binomiale Zufallsvariablen. Allerdings ist ihr Fokus auf Spurious-Aktivierung unter verschiedenen Instandhaltungsstrategien zu beurteilen und sie enthalten keine anderen Fehler als unabhängige Spurious-Operation Ausfälle. Andrews und Bartlett [03] haben einen Suchalgorithmus verwendet, um den Beitrag von Spurious-Aktivierung, die $koon$ [34]-Konfigurationen verwenden können, zu modellieren. Deren Algorithmus konzentriert sich auf die optimale Auswahl von k und n, die zu minimalen Kosten und einem System innerhalb vorgegebener Einschränkungen führt.

Je kleiner der STR-Wert ist, desto größer ist die Verfügbarkeit des Systems und somit werden die Kosten für das unnötige Herunterfahren des Systems verringert. So hat Buddy Creef [I01] einige Kriterien (wie z. B. $MTTF_{Spurious}$ [35], Redundanz und die Möglichkeit ohne Prozessabbruch bei Online-Reparatur oder die Möglichkeit ein SIS online zu modifizieren ohne Prozessabbruch oder anderen Beeinträchtigungen des Prozesses) für die Auswahl eines SISs mit hoher Prozess-Verfügbarkeit vorgeschlagen. Das bedeutet, Spurious-Trip hat einen großen Einfluss auf die Wirtschaftlichkeit und muss deshalb in der Lebenszykluskostenrechnung (LCC[36]) in Betracht gezogen werden [65]. Um die LCC-Kosten bei gleichbleibender funktio-

---

32 $MTTF_S$: Mean Time To Safe Failure

33 $MTTF_D$: Mean Time To Dangerous Failure

34 k out of n, wobei n die Anzahl der unabhängigen Kanäle ist und k die Anzahl der Kanäle, die das System benötigt um die Sicherheitsfunktionen auszuführen.

35 $MTTF_{Spurious}$: Mean Time To Failure Spurious-Trip

36 LCC: Life Cycle Cost

naler Sicherheit zu minimieren, wurden einige Optimierungen für SIS-Designs dargestellt [69], [92], [94]. Der Einfluss von Spurious-Trip auf SIS wird von Hildebrand A. [43] behandelt. Dazu hat der Autor die Formel zur Berechnung des STR-Werts für homogene SISs definiert. Machleidt K. und Lothar Litz [69] haben die von Hildebrand A. [43] beschriebenen Formeln für heterogene SIS-Architektur verallgemeinert: es wird davon ausgegangen, dass die gefährlichen erkannten Fehler nicht zu einem Spurious-Trip verursacht wurden. Dazu werden die Formeln zur Berechnung des STR-Werts für 1oo1-, 1oo2- und 2oo3-System präsentiert. Thomas Gabriel, Lothar Litz, Bernd Schrörs [34] haben einen formalen Ansatz zur Berechnung des PFD-Werts bzw. der Wahrscheinlichkeit des Spurious-Trips (engl. Probability of Tripping Spuriously PTS) mittels Markov-Modellen für beliebige strukturierte Sicherheitsfunktionen beschrieben. Eine innovative Berechnungsmethode des Spurious-Trips, die auch auf Markov-Modellen basiert, wurde von Xie et al. [101] vorgeschlagen, um die Wirkung von Reparaturen auf die Zuverlässigkeit des Systems zu bewerten. Durch Analyse der Verfügbarkeit des klassischen 1oo2 reparierbaren Systems haben L.Y. Xie, M.N. James, Y.X. Zhao and W.X. Qian [101] eine Definition von Spurious-Trip vorgeschlagen, in der eine Online-Reparatur in Betracht gezogen wurde. Im Vergleich mit den Vorteilen der Online-Reparatur wurde die von Spurious-Trip verursachte Reparatur in dieser Veröffentlichung analysiert. Die numerische Berechnung ergab, dass die Online-Reparatur hilfreich ist, um Spurious-Trip in 1oo2 redundanten Systemen zu verkleinern. Gefährliche Fehler, wenn diese nicht repariert oder online behoben werden können, haben komplexe Einflüsse auf die Zuverlässigkeit des Systems. Der gefährliche Ausfall ist manchmal ein Vorteil für den Anti-Spurious-Trip, wenn dieser nicht repariert wird, da kein Prozess abgebrochen wird. Aber Mean Time To Failure Spurious-Trip ($MTTF_{Spurious}$) reduziert sich mit der Zunahme des gefährlichen Ausfalls, sofern die gefährliche Ausfallrate größer als die sichere Ausfallrate ist.

Obwohl die Ausfallwahrscheinlichkeit aufgrund des CCF zu klein ist und oft vernachlässigt wird, wird der CCF trotzdem von Kang H. G. und Kim H. E. [53] in der Berechnung der Nichtverfügbarkeit und Ausfallwahrscheinlichkeit aufgrund des Spurious-Trips besonders betrachtet, da der CCF die Auftrittswahrscheinlichkeit des Spurious-Trips reduzieren kann. Die Autoren haben die Berechnung der Nichtverfügbarkeit und Ausfallwahrscheinlichkeit aufgrund des Spurious-Trips für 2oo3-, 2oo4- und 2oo4-Voting-Systeme als Beispiele durchgeführt. Als Ergebnisse wurde gezeigt, dass CCF die Nichtverfügbarkeit und Ausfallwahrscheinlichkeit aufgrund des Spurious-Trips dominieren.

Lu und Lewis [60], [62] präsentierten die analytischen Modelle basierend auf der Binomial-Verteilung für die Ausfallwahrscheinlichkeit aufgrund von Spurious-Trip und Nichtverfügbarkeit. Der Beitrag dieser Arbeit ist wichtig, weil sie die Bewertung der relativen Zeit des Systems präsentiert, in der das System im normalen Betrieb, Test und Wartung verbringt, in denen die Ausfallwahrscheinlichkeit aufgrund Spurious-Trips verändert.

Torres-Echevarría et al. [95], [93], [94] haben Modelle für die Quantifizierung des $PFD(t)$- und STR-Werts eines Systems mit parallelen Architekturen entwickelt. Die Modelle sind

ausreichend für die Anforderungen in der Norm IEC 61508 (einschließlich CCF, Diagnosedeckungsgrad, Redundanz, Prooftest-Intervall und Strategien) und geeignet für die Optimierung von Design und Teststrategien mit der Metaheuristik-Methode. Die Modelle wurden für die Optimierungen der Sicherheitssysteme mittels genetischer Algorithmen angewendet: Optimierung von Design des Sicherheitssystems mit Parallelredundanz [95], Optimierung von Design mit diversitärer Parallelredundanz [93] und Optimierung von Teststrategien des Sicherheitssystems [94]. Weiteres haben Torres- Echevarría et al. [92] diese Modelle angewendet, um Design und Teststrategien eines SISs zu optimieren. Die Modelle wurden in Lebenszykluskosten-Modellen integriert. Als Ergebnis wurde gezeigt, dass für den gleichen PFD_{avg}-Wert kleinere STR- und LCC-Werte erreichbar sind. Bei Optimierung des Designs eines SISs wurde gezeigt, dass bei Erhöhung der Komponentenanzahl der PFD_{avg}-Wert vergrößert und STR-Wert verkleinert wird.

1.3 Ziele der Arbeit

Anhand der Abbildung 1.1 kann die Tabelle 1.2 gebildet werden. Diese Wahrheitstabelle stellt den Zustand der Gesamtanlage in Abhängigkeit vom Verhalten der EUC und des SIS dar. Schickt das EUC ein Signal (eine Anforderung) an das SIS und reagiert das SIS aber nicht, wird das Gesamtsystem im gefährlichen Zustand sein. Dieser Zustand kann durch eine der folgenden Möglichkeiten erreicht werden:

- Eine Anforderung wird geschickt, wenn ein gefährlicher Fehler bereits schon existiert, ist aber noch nicht erkannt oder
- Während der Anforderungsdauer ist ein gefährlicher Fehler aufgetreten.

Im Fall, dass das SIS auf Anforderung des EUC richtig reagiert, wird das Gesamtsystem in den sicheren Zustand gebracht. Ein weiterer Fall ist der in dieser Arbeit zu betrachtende Fall: das Gesamtsystem wird abgeschaltet, obwohl der EUC keine echte Anforderung an das SIS geschickt hat. Das bedeutet, dass:

- Eine nicht echte Anforderung entsteht, wenn das SIS ein verfälschtes Signal ausgibt und die Gesamtanlage somit in den stromlosen Zustand geht oder
- Die Gesamtanlage geht in den stromlosen Zustand, sobald ein Fehler im SIS erkannt wird, trotz keiner Anforderung auf Auslösung der Sicherheitsfunktion.

Seien:

- 0 (FALSE-Signal): SIS bzw. Gesamtanlage ist im sicheren Zustand bzw. stromlosen Zustand
- 1 (TRUE-Signal): SIS bzw. Gesamtanlage ist nicht im stromlosen Zustand

dann ergibt sich folgende Tabelle (Tabelle 1.2) für die Kombination zwischen EUC und SIS.

Tabelle 1.2: Zustand der Gesamtanlage in Abhängigkeit von EUC- und SIS-Zustand

EUC	SIS	
	0	1
ohne Anforderung	Spurious-Trip	-
Anforderung mit λ_{DE}	Sicherer Zustand	Gefährlicher Zustand

Die Ziele dieser Dissertation mit dem Thema *„Beitrag zur Betrachtung von $MTTF_{Spurious}$-Modellierung im Zusammenhang mit dem internationalen Sicherheitsstandard IEC 61508“* sind folgende:

- Bestimmung des PFS_{avg}-, STR- bzw. des $MTTF_{Spurious}$-Wertes von sicherheitsgerichteten Rechnerarchitekturen auf der Basis der Normen IEC 61508 durch zwei Methoden: Blockdiagramm und Markov-Modell.
- Untersuchung und Vergleich der Auswirkung von Betriebsarten auf die Berechnung des PFS_{avg}, STR- bzw. des $MTTF_{Spurious}$-Wertes von verschiedenen sicherheitsgerichteten Rechnerarchitekturen zwischen Betriebsart mit niedriger Anforderungsrate und zwischen Betriebsart mit hoher Anforderungsrate im Ruhestromprinzip.
- Untersuchung und Vergleich der Gleichungen zwischen den herkömmlichen Verfahren und dem neuen Modell zur Bestimmung des PFS_{avg}-, STR- bzw. $MTTF_{Spurious}$-Wertes.

1.4 Aufbau der Arbeit

Im zweiten Kapitel dieser Arbeit werden die Grundlagen der Sicherheitstechnik zusammengefasst. Hier wird eine kurze Einführung in die Hardware-Fehler-Toleranz und die Zuverlässigkeitstheorie gegeben. Das Kapitel beschreibt die wichtigsten Anforderungen der Norm IEC 61508. Die wichtigsten Modelle für Zuverlässigkeit und Life Cycle Costing werden beschrieben und analysiert. Dabei liegen die Schwerpunkte auf den notwendigen Begriffen, Methoden und Prinzipien, die später in dieser Arbeit verwendet werden.

Kapitel 3 beschreibt das Spurious-Trip Konzept in einem System. Dabei werden die Kenngrößen des Spurious-Trips (wie STR, $R_{Spurious}(t)$, PFS_{avg} und $MTTF_{Spurious}$) definiert und es wird die Methode dargestellt, um diese Kenngrößen zu bestimmen. Neuer Ansatz wird in diesem Kapitel beschrieben.

Kapitel 4 und 5 sind die Hauptkapitel. In diesen Kapiteln wird der aktuelle Stand der Forschung analysiert. Ein Vorschlag wird für die Analyse des Ausfalls aufgrund von Spurious-Trip gegeben. Dabei werden die am meisten verwendeten Methoden der Zuverlässigkeitsanalyse und Zuverlässigkeitsberechnung von technischen Systemen beschrieben. Die Berechnungen des PFS_{avg}-, STR- bzw. $MTTF_{Spurious}$-Werts werden für unterschiedliche Architekturen, die mit dem Ruhestromprinzip konzipiert sind, durchgeführt.

Zur Veranschaulichung werden die Parameter des Spurious-Trips durch ein Anwendungsbeispiel für unterschiedliche Systemarchitekturen in Kapitel 6 berechnet. Dabei werden die Ergebnisse analysiert und bewertet, um die verwendeten Systeme zu klassifizieren. Die Vor- und Nachteile, bezogen auf die praktische Anwendung, werden in diesem Kapitel beschrieben. Durch diese Beispiele wird ein Vergleich zwischen Gleichungen des neuen Ansatzes und den Gleichungen der bestehenden Standards gegeben.

Kapitel 7 schließt diese Arbeit mit einer Zusammenfassung der wissenschaftlichen Erkenntnisse und einem Ausblick.

2 Sicherheitstechnische Systeme und RAMS+C[37] Modellierung

Ein SIS[38] (Sicherheitstechnisches Systems) arbeitet entweder nach dem Ruhestrom- (de-energized to trip) oder nach dem Arbeitstromprinzip (energized to trip). Die Automatisierungsgeräte sind für das Ruhestromprinzip konzipiert, d. h. die Peripherie und die Funktion der Steuerung betrachten den energielosen Zustand als sicheren Zustand. Als sicherer Zustand im Fehlerfall wird damit bei den Ein- und Ausgangssignalen der spannungs- oder stromlose Zustand eingenommen. Das Gegenteil des Ruhestromprinzips ist das Arbeitsstromprinzip, bei dem der Strom fließen soll, um den sicheren Zustand zu erreichen. Das Design des SISs ist entscheidend, um nach IEC 61508 den entsprechenden SIL zu erreichen. Die Sicherheitsintegrität umfasst die Beschränkung der Ausfallwahrscheinlichkeit PFD_{avg} eines Systems bei Anforderung und die Erfüllung einiger Mindestanforderungen an die Fehlertoleranz. Fehlertoleranz beschreibt die Eigenschaft eines Systems die Funktionsweise aufrecht zu erhalten, wenn ein einfacher Fehler im System auftritt. Die Fehlertoleranz wird durch Redundanz erreicht. Werden identische Komponenten für die Redundanz benutzt, kann das System jedoch zu einem Ausfall gemeinsamer Ursache (Common Cause Failure CCF) führen. Allerdings kann CCF durch Realisierung von Redundanzen mit technologisch unterschiedlichen Komponenten entgegengewirkt werden. Je nach Anwendung werden unterschiedliche Architekturen für Sicherheitssysteme implementiert. Diese Architekturen unterscheiden sich von Design und Sicherheitsparameter, die in diesem Kapitel kurz beschrieben werden.

2.1 Sicherheitstechnische Systeme

Die einfachste Schaltung für SIS ist der einkanalige Aufbau. Wird Hardware-Redundanz benötigt, sind ein SIS parallel aufgebaut und im einfachsten aber nicht immer zuverlässigsten Fall mit einem $koon$ -System versehen, wobei die Anzahl der Komponenten im System oft aus wirtschaftlichen Gründen auf bis zu vier begrenzt wird.

Die IEC 61511 [49] definiert $koon$ als SIS oder als Teil davon, wobei n die Anzahl der unabhängigen Kanäle ist und k die Anzahl der Kanäle, die das System benötigt, um die Sicherheitsfunktionen auszuführen. Dieser Begriff wird auch durch die PDS Methode [87] verwendet. Nach CCPS[39] [23] bezeichnet n die Gesamtzahl der Geräte (oder Kanäle) und k bezeichnet die minimale Anzahl von Geräten (oder Kanälen) von n, die erforderlich sind, um das System zu initiieren oder in den sicheren Zustand zu bringen. Je nach Anwendung wird die entsprechende $koon$-Architektur für das System eingesetzt. Zum Beispiel in Bezug auf Feldgeräte, identifizierten Gruhn und Cheddie [40], [39] die Strukturen 1oo1D, 1oo2D und 2oo3 für Sensoren, während für Aktuatoren die System-Architekturen 1oo1, 1oo2 und 2oo2

[37] RAMS+C: Reliability Availability Maintenance Safety + Cost
[38] SIS: Safety Instrumented System
[39] CCPS: Center for Chemical Process Safety

erwähnt werden. Goble und Cheddie [36] präsentieren praktische Beispiele für die gleichen Sensor-Architekturen. Bodsberg und Hokstad [12] zeigten Sensor-Redundanzen mit bis zu 8 Einheiten, obwohl es nicht klar ist, ob das Beispiel aus der wirklichen Praxis genommen wurde. CCPS [23] identifiziert die folgenden *koon*-Architekturen als die häufigsten: Sensoren: 1oo1, 1oo2, 2oo2 und 2oo3; Logic Solver: 1oo1, 1oo2, 2oo2 und 2oo3; Aktuatoren: 1oo1, 1oo2 und 2oo2.

Goble et. al. [36] zeigen, dass bei den *koon*-Architekturen mit Diagnose (*koonD*) die Diagnose das fehlerhafte Gerät aus der Schaltung trennen kann, um einen gefährlichen Ausfall in einen sicheren Ausfall zu ändern. Diese Idee wurde von Goble in seiner Analyse von Architekturen integriert. Es ist deutlich zu erkennen, dass die Diagnose die Ergebnisse des Entscheiders beeinflusst. Allerdings gilt diese Behauptung nicht für die Geräte, welche eine automatische integrierte Diagnose haben, nur zum Zweck den Fehler anzukündigen. Als Beispiel haben Gruhn und Cheddie [40] sowie Goble und Cheddie [36] *koonD*-Architekturen für intelligente Sensoren (Sensoren mit eingebetteten Mikroprozessoren für zusätzliche Funktionalität und Diagnose) gewählt.

2.2 RAMS+C Modellierung

Alle sicherheitsbezogenen Systeme begrenzen für den Anwender bestimmte Gefährdungspotenziale und damit Risiken, da Systemfehler immer auftreten können. Solche Systemfehler sind meistens zufällig und können deshalb nicht notwendigerweise vorhergesehen werden. Prinzipiell werden sicherheitsbezogene Systeme nur gegen erwartete Fehler geschützt. Deshalb wird die Sicherheit eines Systems akzeptiert, wenn das Risiko, das durch den Umgang mit diesem System entsteht, von der Gesellschaft und den Gesetzgeber akzeptiert wird [27]. Die Zuverlässigkeit hat nicht nur auf die Sicherheit einen großen Einfluss, sondern auch auf die Verfügbarkeit und damit auf die Kosten eines Systems. So soll die Zuverlässigkeit nicht zuletzt vor allem ein wirtschaftlich bestimmender Faktor sein. Um eine hohe Sicherheit zu erreichen, ist eine hohe Zuverlässigkeit hilfreich und auch notwendig. Um Gefahrenpotenziale zu minimieren, sind neben einer hohen Zuverlässigkeit vor allem auch geeignete Sicherheitskonzepte notwendig.

Der Begriff „Verlässlichkeit“ wird für das globale Konzept von Zuverlässigkeit benutzt. Stapelberg [90] verwendet dafür den Sammelbegriff RAMS (Reliability, Availability, Maintainability and Safety). Martorell et al. [71] und Cheng [25] fügten den wichtigen Kostenfaktor C bei der Analyse von Systemen als RAMS + C hinzu. Anzumerken ist, dass RAMS daher eine Teilmenge der Verlässlichkeit ist.

Die Zuverlässigkeit und Sicherheit eines sicherheitsbezogenen Systems werden durch probabilitische Modelle analysiert. Modelle der Zuverlässigkeit und Sicherheit haben das Ziel, zuverlässige- und sicherheitsrelevante Systemeigenschaften, Einflussgrößen und Beziehungen der Systemelemente zu formalisieren und in geeigneter mathematischer Weise abzubilden. Zur Bewertung von PFD_{avg} und STR werden folgende Modellierungsmethoden benutzt:

- Einfache Gleichungen (Simplified equations SE)
- Zuverlässigkeitsblockdiagramm (Reliability Block Diagram RBD)
- Fehlerbaum (Fault Tree Analysis FTA)
- Markov Analyse (MA)
- Petri Netze
- Hybrid Methode

Die kombinatorischen Methoden sind die am häufigsten verwendeten Methode, vor allem Zuverlässigkeitsblockdiagramme (Reliability Block Diagram RBD) und Fehlerbaum (Fault Tree Analysis FTA). RBD ist eine einfache Methode und wird in der Regel für nicht-online-reparierbare Systeme verwendet. Während RBD für die Analyse des Erfolges eines Systems verwendet wird, wird FTA für die Ausfallanalyse eines Systems und für online-reparierbare Systeme verwendet [36]. Aber für Systeme, die eine komplexe Reparatur haben oder die ein zeitabhängiges Verhalten aufweisen, werden andere komplexe Methoden wie Markov-Analyse (MA), Petri-Netze oder Bayes-Netze verwendet.

Die Fehlerbaum-Analyse wird häufig im Vergleich zum Zuverlässigkeits-Blockdiagramm bevorzugt, weil es ein grafisches Verständnis für die Ausfallprozesse bietet, und es konzentriert sich auf die Fehler anstatt auf die Erfolgswahrscheinlichkeit [04]. Dagegen haben vereinfachte Gleichungen und Hybrid-Methoden (basierend auf einfachen Gleichungen) den Nachteil einer zu starken Vereinfachung (IEC 61508-6) und einer Inflexibilität bei sich verändernden Bedingungen des Designs.

Goble [35], Andrew und Ericson [04] haben Fehlerbaum- und Markov-Analyse für mehrere Design-Komplexitäten verglichen. Sie haben herausgefunden, dass eine Fehlerbaum-Analyse entweder gleiche Ergebnisse oder eine sehr gute Annährung zur Markov-Analyse liefert. Obwohl eine Markov-Analyse genauer als eine Fehlerbaum-Analyse und vorteilhaft für die Aufnahme der Zeitabhängigkeit und der Fehlerarten ist, ist sie komplizierter. Deshalb werden meistens numerische Methoden für komplexe Systemlösungen benutzt. Eine Fehlerbaum-Analyse ist dagegen vorteilhafter und leichter für die Modellierung von großen und komplexen Systemen. Bukowski [22] ist der Meinung, dass der Ansatz der einfachen Gleichungen zu erheblichen Fehlern führen kann und eine Markov-Analyse Expertenwissen für ihre Anwendung erfordert. Rouvroye und Brombacher [79] zeigten, dass das Zuverlässigkeits-Blockdiagramm sehr pessimistische Ergebnisse liefert.

Im Allgemeinen hat die Markov-Analyse mehr Vorteile als der Fehlerbaum, denn Markov-Prozesse beschreiben die zeitliche Evolution der Zustände eines Systems und sind somit verhaltensorientiert. Die Grundlagen des Markov-Prozesses befinden sich im Anhang A. Mit Markov-Modellen sind verschiedene fehlerfreie und fehlerbehaftete Zustände mit verschiedenen Übergangsraten unterscheidbar, oder verschiedene Betriebsphasen mit verschiedenen Systemstrukturen. Deshalb wurde das Markov-Modell meist von vielen Autoren [19], [45], [100] verwendet, um die Zuverlässigkeit eines Sicherheitssystems zu analysieren. Allerdings ist nicht jede Kombination von fehlerhaften Zuständen physikalisch sinnvoll. Marcus Abele

[01] vertritt die Ansicht, dass die Anzahl der möglichen Systemzustände nicht von der reinen Kombinatorik der Betriebsmittelfehler abhängt, sondern vor allem von der kausalen Folge der Fehler. Daher meint der Autor auch, dass die weitere Betrachtung von Fehlern in einem Teilsystem nicht unbedingt sinnvoll sein muss und die Berücksichtigung dementsprechend bei der Modellierung hinterfragt werden sollte, wenn dieses Teilsystem bereits durch einen Fehler ausgefallen ist. Eine Haupteinschränkung der Markov-Modellierung ist das schnelle Anwachsen des Zustandsraumes bei größeren Systemen oder komplexen Verhaltensweisen, besonders bei deterministischen Zeiten, beispielsweise müssen fixe Reparaturzeiten über Verteilungsfunktionen nachgebildet werden. Ein weiterer Nachteil ist, dass das Zustandsmodell praktisch von Hand entworfen werden muss. Dadurch ist die Erstellung fehleranfällig und es können Fehlerszenarios übersehen werden. Besonders bei komplexen Systemen, bei denen sich das System auf unterschiedliche Betriebsbedingungen einstellen kann, wächst die Komplexität schnell an. Auch die Modellierung mit mehr als zwei Komponenten kann unüberschaubar werden, wenn mehrere Ausfallarten enthalten sind. Darüber hinaus ist die Fehlerbaum-Analyse im Vergleich zur Markov-Analyse einfacher zu analysieren, da eine grafische Darstellung der Ausfallmechanismen dargestellt werden kann. Andere Methoden, wie Petri-Netze [81], können Zeitabhängigkeiten verarbeiten, aber sie sind auch komplexer zu konstruieren und zu analysieren. Sequentielle Ausfälle können von dynamischen Fehlerbäumen bearbeitet werden [29].

Aus diesen Gründen werden in dieser Arbeit RBD und Markov-Modell für die Analyse des Themas angewendet. Die Vorteile von RBD werden hier genutzt, um die Formeln für einfache und auch komplexe Systeme zu berechnen und zu verallgemeinern. Das Markov-Modell wird dann angewendet, wenn die Berechnungsdurchführung einer Systemarchitektur detaillierter beschrieben werden muss.

2.2.1 Modellierung der Ausfallwahrscheinlichkeit

Die Norm IEC 61508 [48] legt die Verwendung der durchschnittlichen Ausfallwahrscheinlichkeit (PFD_{avg}) als metrischen Standard für den Verlust von Sicherheit fest. Die Methode zur Quantifizierung von PFD_{avg} in der Norm IEC 61508 [48] basiert auf vereinfachten Gleichungen (abgeleitet von RBD). Obwohl die Norm IEC 61508 [48] einen effektiven organisatorischen Rahmen für die Umsetzung und den Betrieb von Sicherheitssystemen bietet und in vielen Bereichen sowie in vielen Ländern benutzt wird, haben allerdings einige Autoren mehrere Einschränkungen und Uneinheitlichkeiten, vor allem mit der Methode zur Quantifizierung von PFD_{avg} und die Auswertung der SIL-Ebenen, identifiziert ([103], [44], [84], [41], [28], [66]). Während T. Zhang et al. [103] und H. Guo et al. [41] die Meinung vertreten, dass die Norm IEC 61508 [48] nicht ausführlich genug die Umsetzung erklärt, sind Signoret et al. [84] der Meinung, dass das Verfahren und die zugrunde liegende Hypothese zur Herleitung der angegebenen Formeln nicht detailliert sind. Daher ist es schwierig zu wissen, unter welchen Bedingungen sie wirklich gültig sind. Zhang et al. [103] fanden einige Unstimmigkeiten

in der Berechnung der Ausfallzeitenbegriffe t_{CE} und t_{GE}, die nicht eindeutig in der Norm definiert sind, und auf denen alle PFD_{avg} Berechnungen basieren. Außerdem sind Signoret et al. [84] und Hokstad et al. [44] der Meinung, dass die Klassifizierung und Definitionen für Ausfälle unzureichend sind sowie die Umsetzung, Test und Wartung von der Norm sehr begrenzt sind. Bei der Redundanz größer als zwei und Mehrheitentscheider-Systemen ist das Faktor-Modell für die Bewertung in der Norm laut Hokstad et al. [44] noch eingeschränkt.

Die in der IEC 61508 [48] vorgestellten Formeln sind nur auf ein paar Architekturen beschränkt und die vorgestellten Tabellen beschränken sich auf bestimmte Kombinationen von Komponenten, Ausfallraten, Diagnosedeckungsgrad und β Faktor. Es wäre notwendig, neue Formeln für andere Architekturen abzuleiten. Grundsätzlich gibt es keine Flexibilität für die verändernden Bedingungen.

Goble [35] stellt eine Alternative zur Modellierung des PFD_{avg} vor. Der Autor verwendet sowohl Fehlerbaum- als auch Markov-Analyse und bietet die detaillierte Modellierung von mehreren Architekturen mit sicheren und gefährlichen Ausfällen sowie *CCF* [40] und Diagnosedeckungsgrad. Goble löst den Fehlerbaum durch Ableitung der vereinfachten Gleichungen und das durchschnittliche Resultat durch Integration. Die in ISA TR84.0.02 [06] präsentierten Methoden (einfache Gleichung, Fehlerbaum- und Markov-Analyse) verwenden die gleiche Ausfallarten-Taxonomie. Der Standard versucht, systematische Fehler zu berücksichtigen, aber es ist sehr kompliziert statistische Daten zu erhalten. Einige andere Autoren wie Knegtering & Brombacher [55], Rouvroye & Brombacher [79], Rouvroye & van den Bliek [78] haben andere komplexere Hybrid-Methoden vorgeschlagen.

SINTEF [86], [87], [88] schlug eine neue analytische Methode vor, die so genannte PDS[41] Methode, für die Quantifizierung der Zuverlässigkeit für Prozess-Sicherheitssysteme [13], [14]. Die PDS-Methode schlägt die Schaffung einer alternativen Ausfallarten-Taxonomie vor, die in direktem Zusammenhang mit Fehlerursache, Konsequenz und ihrer Mittel zur Verbesserung steht. Diese Methode wird auch in den Zuverlässigkeitsberechnungen für LCC[42] Quantifizierung verwendet, um kostengünstige Designs und Bedienphilosophien zu finden. Im Jahr 2004 haben Hokstad und Corneliussen [44] begonnen, die Schwächen der in der IEC 61508 [48] beschriebenen Methoden zu identifizieren sowie ihre neue Ausfall-Klassifizierung und ein genaueres β Faktor-Modell zur Quantifizierung der CCF verschiedener *koon*-Architekturen vorzustellen. Die PDS-Methode ist umfassender als die in der IEC 61508 [48] beschriebenen Methode. Es gibt jedoch die Schwierigkeit, eine explizite Eingabe von Daten für alle verwendeten Parameter zu erhalten. Die PDS-Methode ist ein Hybrid-Verfahren, denn das einfache Zuverlässigkeits-Blockdiagramm wird in diesem Verfahren genutzt.

---

40 CCF: Common Cause Fehler
41 PDS: Pålitelighet av Databaserte Sikkerhetssystemer
42 LCC: Life Cycle Cost

Signoret et al. [84] und Duduit et al. [28] haben die Verwendung von Fehlerbäumen für die vorgeschlagene Quantifizierung von PFD_{avg} mit Hybrid-Verfahren, basierend auf Fehlerbäumen, ergänzt. Somit können Zeit-Abhängigkeiten behandelt werden und Prüf- und Wartungsarbeiten richtig modelliert werden. Die Idee ist, Mehrphasen-Markov-Modelle oder Petri-Netze, die Substitution, Sub-Module der Fehlerbaumanalyse einzuführen.

Mittels Markov-Modell haben Üstoğlu et al. [96] die Auswirkungen des Prooftest-Intervalls und des Diagnoseaufdeckungsgrades auf die PFD_{avg}-Werte der 1oo2- und 1oo2D-Architektur analysiert. Dabei haben die Autoren gezeigt, dass je größer der Prooftest-Intervall oder je kleiner der Diagnoseaufdeckungsgrad ist, desto größer ist der PFD_{avg}-Wert.

2.2.2 Modellierung der Spurious-Trip Rate

Es gibt keine Einigkeit über die Metrik zur Quantifizierung der Auswirkungen des Spurious-Trip Fehlers. Während SINTEF [87] die Spurious-Trip Rate (STR) als die Häufigkeit der Spurious-Aktivierung des Sicherheitssystems pro Zeiteinheit definiert, wird sie von Goble [35] als Rate von sicheren Fehlern betrachtet. Goble [35] hat die Quantifizierung der Ausfallswahrscheinlichkeit aufgrund sicherer Fehler in der Modellierung mit FTA[43] und MA[44] beschrieben. Er hat dabei die Analyse sicherer Ausfälle ähnlich wie bei gefährlichen Ausfällen analysiert. Die Norm IEC 61508 [48] enthält keine Quantifizierung der sicheren Ausfallsfolge und bietet deshalb nicht alle Quantifizierungsmethoden. Allerdings ist eine Anforderung an den maximalen STR-Wert in der Norm IEC 61511 [49] für Sicherheitssysteme in der Prozessindustrie anzugeben und die PDS-Methode verwendet diesen als eine sichere Ausfall-Metrik [87]. STR wirkt sich auf die Vertrauenswürdigkeit aus, die der Benutzer an das System legt, und auf die gesamten Lebenszykluskosten des Systems, da sie zu Produktionsverlusten führt.

Um STR zu quantifizieren, wird in der Norm ISA TR84.0.02 [06] die Methode der einfachen Gleichungen (hergeleitet aus der Methode des Blockdiagramms) verwendet. Die Gleichungen zur Berechnung der Spurious-Trip Rate werden als eine Funktion in Abhängigkeit von der Rate der sicheren Fehler, erkannten Fehler und systematischen Fehler dargestellt.

Die PDS-Methode [86], [87], [88] stellt die grundlegende Bedeutung der Quantifizierung der sicheren Ausfälle für SIS und die Konzeption der STR als Maß für die Fähigkeit des Systems zur sicheren Produktion dar. Daher ist STR ein Maß für die Verluste der Produktion. Die Methode stellt die Notwendigkeit der Quantifizierung von STR fest, um ein Gleichgewicht zwischen dem Verlust der Sicherheit und dem Verlust der Produktion zu erhalten, und zwar nicht nur als eine sekundäre Leistungsmetrik. Eine Reihe von generischen Gleichungen zur Auswertung von STR für verschiedene Architekturen wird gegeben. Die Methode orientiert sich

[43] FTA: Fault Tree Analysis
[44] MA: Markov Analysis

an den unterschiedlichen Auswirkungen der spezifischen *koon* Architektur, eingebettet in das modifizierte β Faktor-Modell.

Lu & Lewis [61], [62] präsentierten analytische Modelle für die Wahrscheinlichkeit von Spurious-Operationen, basierend auf der Binomialverteilung. Die Autoren haben die Bewertung der relativen Zeit, in der das System im normalen Betrieb verbringt, vorgestellt; sowie Test und Wartung, in denen die Ausfallswahrscheinlichkeit von Spurious-Operationen sich verändert.

Die Studie über Spurious-Aktivierung des SIS wurde von Lundteigen & Rausand [65] präsentiert. Dieser Artikel definiert und erläutert Konzepte im Zusammenhang mit der Spurious-Aktivierung von SIS. Außerdem stellt die Arbeit noch verschiedene analytische Ausdrücke für die Quantifizierung von *STR* einschließlich mehrerer Beiträge dar. Sie entwickeln eine Reihe von vereinfachten Gleichungen für eine Reihe von Architekturen und vergleichen die Ergebnisse anhand der Gleichungen der PDS-Methode und ISA TR84.

Zusätzlich zu der Modellierung der Spurious-Trip Rate werden weitere Eigenschaften der Spurious-Trip Rate mitbetrachtet, die in den Kapiteln 3, 4 und 5 in dieser Arbeit vorgestellt werden.

2.2.3 Modellierung der Lebenszykluskosten

Lebenszykluskosten (LCC[45]) sind eine Basis für die erfolgreiche Umsetzung eines Sicherheitssystems. Die Sicherheit der Anlage ist ein hohes Ziel an sich. Allerdings können die Kosten dafür sehr hoch sein. Deswegen wird in der Regel eine Kosten-Nutzen-Analyse vorgenommen. Es gibt eine Reihe von Lebenszykluskosten-Modellen, die speziell für sicherheitstechnische Systeme entwickelt sind. Davon sind einige spezifisch für die Prozessindustrie. Ein umfassender Leitfaden für LCC im Zusammenhang mit Zuverlässigkeitsanwendung ist in [26] zu finden. Das erste Modell wurde speziell für die Prozess-Sicherheit von SINTEF [67] zur Verfügung gestellt. Dieses Modell wurde als Teil der Arbeit für die PDS-Methode entwickelt. Sie definieren die LCC eines Systems als die Gesamtkosten für den Benutzer in Bezug auf Kaufen und Installation sowie die Nutzung und Wartung des Systems. Deshalb müssen nicht nur die anfänglichen Anschaffungskosten, sondern auch die Betriebskosten mitbetrachtet werden. Das allgemeine Modell lautet:

$$LCC = LAC + LSC + LUC \tag{2.1}$$

mit:

- LAC: Life Acquisition Cost. Diese Kosten beinhalten die Kosten von: Hardware-Ausrüstung, Entwurf, Installation und Inbetriebnahme.

[45] LCC: Life Cycle Cost

- *LSC* : Life Support Cost. Diese Kosten umfassen Ressourcen für Betrieb und Wartung, einschließlich ihrer jährlichen Kosten während der gesamten Lebensdauer.
- *LUC* : Life Unavailability Cost. Der Verlust der Produktion (*STR*) ist hier enthalten. Jedoch sind die zu erwartenden Kosten durch mögliche Unfälle, die durch gefährliche Situationen entstehen, d. h. Kosten für Nichtverfügbarkeit der Sicherheit (d. h. failure to prevent accidents) hier nicht enthalten.

Die Berücksichtigung der Unfallkosten in der Quantifizierung der LUC ist ein umstrittenes und schwieriges Thema. Dies ist der Grund, warum die Unfallkosten nicht in dem Modell von Lyndersen et al.[67] aufgenommen werden. Jedoch haben die Autoren auch erwähnt, dass es eine wichtige Unterlassung ist, weil die wirklichen Vorteile der Risikoreduzierung nicht quantifiziert werden und in die LCC aufgenommen werden können.

Eine alternative Methode, die für ein SIS spezifiziert ist, wird von Goble [37] präsentiert. Er spaltet die primären Kostenkategorien in zwei Teile: Anschaffungs- und Betriebskosten (Gl. (2.2)). Das Verhältnis dieser beiden Kostenfaktoren und die Zuverlässigkeit der Anlagen werden in Abbildung 2.1 gegeben.

$$LCC = C_{PRO} + C_{OP} \tag{2.2}$$

Die Beschaffungskosten umfassen Design, Abnahme, Installation und Inbetriebnahme. Die Betriebskosten enthalten grundsätzlich Kosten für technische Änderungen, Verbrauchsmaterialien, feste Wartungskosten und die Kosten des Ausfalls (Risikokosten).

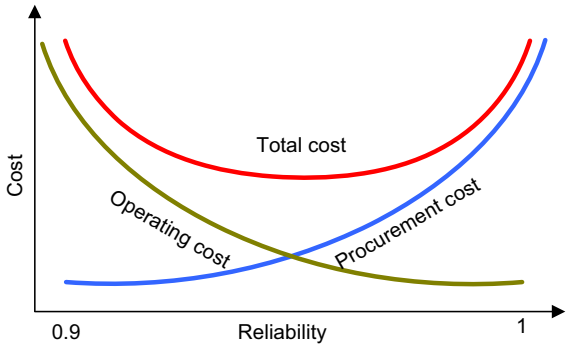

Abbildung 2.1: Kostensverhältnis und Zuverlässigkeit [37]

Goble [37] bestätigt, dass ein SIS einen Sonderfall als Ausfallkosten stellt, die hauptsächlich aus Risikokosten bestehen, und dass dies in der Lebenszykluskosten-Analyse berücksichtigt werden soll. Er schlägt vor, die Berechnung der Risikokosten als Multiplikation der Wahrscheinlichkeit des Ereignisses ohne SIS mit dem PFD des SIS zu berechnen:

$$P_{EVENT\_with\_SIS} = P_{EVENT\_without\_SIS} \times PFD_{SIS} \quad \textbf{(2.3)}$$

Dieses Ereignis enthält Risikokosten von gefährlichen Ausfällen. Ähnlich wie bei SINTEF zählt Goble auch die Kosten aufgrund des Spurious-Trips dazu.

Kawauchi und Rausand [54] legten einen Bericht mit einer Bestandsaufnahme und umfassender Analyse der LCC für die Öl- und chemischen Industrie vor. Sie haben hier keine spezifischen mathematischen Modelle, sondern eine Darstellung der Theorie hinter dem LCC dargestellt.

Martorell et al. [70], [71] haben einen wichtigen Beitrag für die Modelle von Systembetriebskosten unter Berücksichtigung der Prüf- und Instandhaltungsstrategie und die technischen Spezifikationen in kerntechnischen Kraftwerken vorgestellt. Martorell et al. [70] entwickelten einen Funktionstest für die Optimierung des Sicherheitssystems, der auch die jährlichen Kosten, vorbeugende Wartung- und Instandsetzungskosten betrachtet. Dazu gehören auch Ausfalls- sowie Überprüfungskosten. Die Ausfallkostenzeit c_u (ein Konzept ähnlich dem Shutdown) ist ebenfalls enthalten, die von dem Verlust der Produktion abhängig ist:

$$c_u = T_s \times c_{hs} \quad \textbf{(2.4)}$$

mit:

- T_s : Time of start-up
- c_{hs} : cost of production per hour

Martorell et al. [71] haben den Kostenfaktor als zusätzliches Ziel für die Optimierung von Sicherheitssystemen als RAMS + C aufgestellt. Sie haben die möglichen Unfallkosten c_a zum Betriebskosten-Modell hinzugefügt:

$$c_a(x) = R(x) \times c_a \quad \textbf{(2.5)}$$

mit:

- $R(x)$: Funktion des jährlichen Risikos
- c_a : cost per accident

Die Gleichungen (2.4) und (2.5) beschreiben die Äquivalenz der Kosten auf Grund des Spurious-Trips und der gefährlichen Fehler.

Torres- Echevarría et al. [92] haben eine andere Darstellung für die Kosten des Risikos in Abhängigkeit von STR:

$$C_{RISK} = C_{STR} + C_{HAZARD} \quad \textbf{(2.6)}$$

wobei die Kosten aufgrund eines Spurious-Trips wie folgt berechnet werden:

$$C_{STR} = STR \cdot C_{SD} \tag{2.7}$$

und :

$$C_{SD} = SD_{Time} \cdot SD_{LOSS} \tag{2.8}$$

mit:

- SD_{Time} : Restart time after shutdown
- SD_{LOSS} : Cost of production per hour

Die Kosten C_{HAZARD} wird nach folgender Gleichung beschrieben:

$$C_{HAZARD} = C_{ACC} \cdot F(ACC \mid PFD_{avg}) \cdot PFD_{avg} \tag{2.9}$$

mit:

- C_{ACC} : Cost of accident
- $F(ACC \mid PFD_{avg})$: Accident frequency without SIS per year.

Weiter haben Faghih-Roohi et al. [33] die Verfügbarkeit eines *koon*-Systems mittels Markov-Modells analysiert. Dabei wurde eine Optimierung zwischen erwarteten Gesamtkosten eines Systems und den Zuverlässigkeitsanforderungen gegeben. Die Optimierung wurde mit der GA[46]-Methode modelliert. Eine andere Optimierung zwischen DC [47]-Faktor und den Kosten wurde von Wacker et al. [97] für 1oo1- und 2oo2-Systemarchitektur präsentiert. Mit der linearen Programmierung wurde die Optimierung mit zwei Problemen analysiert. Eine ist die Minimierung der Kosten-Funktion unter der Bedingung der DC -Funktion und die andere ist die Maximierung des DC -Faktor unter der Bedingung der Kosten-Funktion.

2.3 Zusammenfassung

Sicherheitstechnische Systeme werden häufig als SIS bezeichnet und werden verwendet, um gefährliche Fehler zu erkennen und die sicherheitstechnischen Funktionen auszuführen. Ziel ist es, das Gefahrenrisiko für Mensch und Umwelt zu minimieren. Daher ist es wichtig, solche Systeme mit hoher Zuverlässigkeit und Sicherheit zu entwickeln und deren Sicherheitsparameter zu modellieren und zu bewerten. Je nach der Anwendung wird ein SIS mit entsprechender *koon*-Architektur verwendet. Wird ein SIS aus der Sicht der Sicherheit betrachtet, wird der SIL [48] anhand des Sicherheitsparameters PFD_{avg} ermittelt. Wird ein SIS aus der

[46] GA: genetic algorithm
[47] DC: Diagnostic Coverage
[48] SIL: Safety Integrity Level

Sicht der Verfügbarkeit betrachtet, ist der STL [49] anhand des Sicherheitsparameters PFS_{avg} [50] bzw. STR [51] zu bewerten. Die Methode, die meist zur Modellierung und Quantifizierung der Sicherheitsparametern PFD_{avg} und STR verwendet werden, wurden bereits mit den Vorteilen und Nachteilen in den Abschnitte 2.2.1 und 2.2.2 dieses Kapitels beschrieben. Zusätzlich wurde auch die Modellierung der Lebenszykluskosten eines SIS im Abschnitt 2.2.3 kurz beschrieben. Zwei dieser Methoden werden in dieser Arbeit für die Analyse des Spurious-Trip Ausfalls und zur Quantifizierung der benötigten Parameter verwendet: Blockdiagramm-Methode und Markov-Modell. Der Spurious-Trip Ausfall sowie dessen Parameter werden in Kapitel 3 beschrieben.

[49] STL: Spurious Trip Level, mehr in Kapitel 3.2.6
[50] PFS: Probability of Failure Spurious, mehr im Kapitel 3.2.4
[51] STR: Spurious Trip Rate, mehr im Kapitel 3.2.1

3 Spurious-Trip Ausfall und dessen Kenngröße

Der Spurious–Trip Ausfall wird als ein unerwarteter Ausfall des Systems definiert, d. h. das System geht in den sicheren Zustand ohne Anforderung (nicht echte Anforderung) der Auslösung der Sicherheitsfunktion. Diese Fehler können durch Anforderung des EUC an das SIS aufgrund eines internen Fehlers im EUC oder durch Fehler vom Bedienpersonal oder durch nicht gefährliche Fehler im SIS verursacht werden. Wird die Sicherheitsfunktion bei einer nicht echten Anforderung ausgelöst, kann die Ausführung der Sicherheitsfunktion des SISs zwar sicher für das Gesamtsystem, aber nicht notwendig für das EUC sein. Durch einen Spurious-Trip Ausfall hat das EUC einen Produktionsverlust. In manchen Fällen kann nur die Verfügbarkeit verloren gehen, wenn das System aufgrund des Spurious-Trips ausfällt, z. B. die Abschaltung des ESD[52] [85]. Wird ein verfälschtes Signal zur Auslösung der Sicherheitsfunktion gesendet, wird das gesamte System abgeschaltet, obwohl es keine notwendige Anforderung gibt. So hat das System einen Produktionsverlust. Als anderes Beispiel ist der Feueralarm zu nennen. Erkennt der Feueralarm ein Feuer, wird die Sicherheitsfunktion ausgeführt. Gibt es kein Feuer und wird die Sicherheitsfunktion trotzdem ausgelöst, ist dies eine verfälschte Auslösung der Sicherheitsfunktion. Der sichere Zustand wird ohne Anforderung in diesem Fall zwar erreicht, aber für das wirtschaftliche Ziel ist es nicht relevant. Allerdings kann auch in manchen Fällen eine Katastrophe dadurch verursacht werden, wenn das System aufgrund des Spurious-Trips ausfällt [102], [74], z. B. die Auslösung des Auto-Airbags. Das Airbag-System ist im Auto vorhanden, um das Verletzungsrisiko des Fahrers beim Zusammenstoß zu verringern. Das heißt, der sichere Zustand ist der Zustand, bei dem das Airbag-System ausgelöst ist. Allerdings ist dieser Zustand nicht immer sicher. Wird das Airbag-System während der Fahrt auf der Autobahn ausgelöst, kann es zu einer Katastrophe kommen. Daher ist es sehr wichtig, den Ausfall aufgrund des Spurious-Trips zu betrachten. Wie in Kapitel 1 schon erwähnt, gibt es bisher noch keine Einigung für die Berechnung der Parameter eines Ausfalls aufgrund des Spurious-Trips. In der Norm ANSI/ISA TR84.00.02-2002 [06] werden die sicheren Fehler und gefährlich erkannten Fehler in der Berechnung der *STR* mitberücksichtigt. In der PDS-Methode ([86], [87], [88]) werden nur die sicheren unerkannten Fehler in der *STR*-Berechnung betrachtet. In der Norm IEC 61511 [49] wird die *STR* als die Rate des sicheren Fehlers definiert. Im folgenden Kapitel werden das Konzept des Spurious-Trips und deren Parameter kurz beschrieben.

3.1 Definition des Spurious-Trips aus herkömmlichen Verfahren

Um die Definition des Spurious-Trips besser darzustellen, wird zuerst die Bedeutung des sicheren Zustands erläutert. Der sichere Zustand wird als *„Zustand des Prozesses, in dem Sicherheit erreicht ist“* [49] (IEC 61511, Abschnitt 3.2.66, Teil 1) oder als *„Zustand der EUC-*

[52] ESD: Emergency Shutdown System

Einrichtung, in dem die Sicherheit erreicht ist" [48] (IEC 61508, Abschnitt 3.1.13, Teil 4) bezeichnet. Bei dem Ruhestromprinzip wird der sicherer Zustand erreicht, wenn kein Strom in das Gesamtssystem hineinfließt. Dagegen ist der sichere Zustand bei dem Arbeitsstromprinzip kein stromloser Zustand.

Der sichere Zustand wird hierbei erreicht, wenn:

- eine Anforderung von der EUC an das SIS zur Auslösung der Sicherheitsfunktion gefordert wird oder
- ein sicherer Fehler im SIS aufgetreten ist oder
- ein gefährlich erkannter Fehler im SIS aufgetreten ist oder
- ein Fehler infolge gemeinsamer Ursache (*CCF* [53]) im SIS aufgetreten ist. Dieser Fehler tritt nur bei einer *koon*-Architektur auf.

Die Sicherheitsanforderung an das SIS definiert *"die Festlegung aller notwendigen Maßnahmen, um im Fall eines erkannten Fehlers im SIS den sicheren Zustand zu erreichen oder beizubehalten. Bei der Festlegung solcher Maßnahmen muss menschliches Verhalten angemessen berücksichtigt werden"* [49] (IEC 61511, Teil 1, Abschnitt 10.3.1).

Bei manchen Fällen muß der Prozess durch eine Reihe von Zuständen gehen, bevor der sichere Zustand erreicht ist [39]. Für einige Situationen existiert ein sicherer Zustand nur so lange, wie die EUC-Einrichtung einer ununterbrochenen Steuerung unterliegt, z. B. ein Flugzeug wird durch ein fly-by-wire-control gesteuert. Solch eine kontinuierliche Steuerung kann für einen kurzen oder einen unbestimmten Zeitraum erfolgen [48] (IEC 61508, Abschnitt 3.1.13, Teil 4).

Spurious-Trip wird beispielsweise als Spurious-Aktivierung, nuisance trip, false trip, usw…. bezeichnet [49], [06], [I01]. In [65] wird Spurious-Aktivierung als Sammelbegriff verwendet: *"Spurious weist darauf hin, dass die Ursache der Aktivierung unsachgemäß, falsch oder nicht echt ist, während die Aktivierung darauf hinweist, dass irgendeine Art des Übergangs von einem Zustand zum anderen führt"*.

M. A. Lundteigen und M. Rausand [65] haben auch beschrieben, wie der Unterschied zwischen "Spurious-Activation" (Spurious-Aktivierung), "Spurious-Trip", "Spurious-Shutdown" und deren Ursachen zu definieren ist:

- Spurious-Activation: ist eine Aktivierung eines SIS-Elements ohne die Anwesenheit einer bestimmten Prozessanfrage [65].
- Spurious-Trip: ist eine Aktivierung eines oder mehrerer SIS-Elemente, sodass das SIS eine SIF[54] ausführt ohne die Anwesenheit einer bestimmten Prozessanfrage [65].

[53] CCF: Common Cause Failure
[54] SIF: Safety Instrumented Function

- Spurious-Shutdown: ist ein teilweises oder vollständiges Herunterfahren eines Prozesses ohne die Anwesenheit einer bestimmten Prozessanfrage [65].

In der Norm IEC 61511 [49] (Abschnitt 3.2.65, Teil 1, 2003) und ISA-TR84.00.02-2002 [06] (Anschnitt 3.1.68, Teil 1) wird der sichere Ausfall auch „Spurious-Trip Ausfall" genannt. Allerdings wird der „Spurious-Trip" in dem Abschnitt 3.1.87 in der ISA-TR84.00.02-2002 [06] wie folgt definiert: *„spurious trip refers to the shutdown of the process for reasons not associated with a problem in the process that the SIF is designed to protect (e.g., the trip resulted due to a hardware fault, transient, ground plane interference, etc.). Other terms used include nuisance trip and false shutdown."*

Anforderungen an Betreiber und Geräte bei der Erkennung eines Fehlers werden in [06], Abschnitt 11.3 angegeben. Die Erkennung eines gefährlichen Fehlers (durch Diagnose, Prooftest oder ähnliche Tests) in einem Subsystem, das ein Hardware-Fehler tolerieren kann, kann die folgenden Auswirkungen haben:

- Eine definierte Aktion zu erreichen oder den sicheren Zustand aufrechtzuerhalten [06] oder
- Die sichere Operation des Prozesses fortzusetzen, während das defekte Teil benötigt wird. Wenn die Reparatur des defekten Teils nicht innerhalb der Reparaturzeit ($MTTR$) vollständig ist, dann muss eine definierte Aktion erreicht werden oder den sicheren Zustand aufrechterhalten [06].

Das heißt, wird ein Fehler im toleranten SIS erkannt, kann der Prozess noch während der Reparaturzeit ($MTTR$) weiterlaufen. Daher folgt: ist das fehlertolerierbare System während der Reparaturzeit online reparierbar, wird der Prozess nicht abgebrochen. Wenn nicht, muss der Prozess innerhalb der Reparaturzeit planmäßig unterbrochen werden [I01]. Der Reparatur-Mechanimus bei einem sicheren Fehler ist im Allgemein anders und meistens auch einfacher als bei einem gefährlichen Fehler. Daher ist die Reparaturzeit bei einem sicheren Fehler ($MTTR_S$) kleiner als die Reparaturzeit bei einem gefährlichen Fehler ($MTTR_D$) [77].

3.2 Spurious-Trip Kenngröße

Spurious-Trip Ausfall ist homogen poissonverteilt[55] mit den Parameter $STR \cdot t$, unter der Bedingung, dass die Reparaturdauer viel kleiner als $MTTF_{Spurious}$ und vernachlässigbar ist [77].

Im folgenden Unterkapitel werden die Kenngröße und deren Berechnungen eines Spurious-Trip Ausfalls beschrieben:

- Spurious-Trip Rate STR [56]
- Ausfallwahrscheinlichkeit aufgrund des Spurious-Trips PFS [57]

[55] Ein homogener Poisson-Prozess ist ein Markov-Prozess in stetiger Zeit mit diskretem Zustandraum.
[56] STR: Spurious-Trip Rate

- Mittlere Zeit bis zum Ausfall aufgrund des Spurious-Trips $MTTF_{Spurious}$ [58]

3.2.1 Hardware-Fehlertoleranz

Fehlertoleranz wird im Punkt 3.6.3 der Norm IEC 61508 [48] definiert als: „*Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen*". Die Hardware-Fehlertoleranz HFT [59] ist die Fähigkeit einer Komponente oder eines Teilsystems bei Bestehen von Fehlern die geforderte Sicherheitsfunktion auszuführen. Eine $koon$-Architektur hat eine HFT von $n-k$ in Bezug auf Sicherheitsfunktion bzw. Sicht der Sicherheit. Die Hardware-Fehlertoleranz ist in Bezug auf Spurious-Trip bzw. die Sicht der Verfügbarkeit nicht gleich dieser HFT-Wert, sondern gleich $k-1$ [77]. Daher werden in dieser Arbeit die Bezeichnungen HFT_D für die Hardware-Fehlertoleranz in Bezug auf Sicherheitsfunktion bzw. Sicht der Sicherheit und $HFT_{Spurious}$ für die Hardware-Fehlertoleranz in Bezug auf Spurious-Trip bzw. Sicht der Verfügbarkeit verwendet. Die folgende Tabelle stellt die HFT_D-Wert und $HFT_{Spurious}$-Wert für $koon$-Architekturen dar:

Tabelle 3.1: HFT_D-Wert und $HFT_{Spurious}$-Wert für $koon$-Architektur [77]

	1oo1	**1oo2**	**2oo2**	**2oo3**	**2oo4**	**1oon**	**koon**
HFT_D	0	1	0	1	2	n-1	n-k
$HFT_{Spurious}$	0	0	1	1	1	0	k-1

3.2.2 Spurious-Trip Rate

Die Spurious-Trip Rate gibt die Häufigkeit an, mit welcher das Sicherheitssystem in den sicheren Zustand ohne echte Anforderung überführt wird. Im Abschnitt 3.1.88, Teil 1 in der ANSI/ISA-TR84.00.02-2002 [06] wird STR-Wert definiert als: *„die erwartete Ausfallrate (Anzahl der Ausfälle pro Zeiteinheit) einer SIF aus Gründen nicht mit einem Problem im Prozess entstehen, den SIF schützen soll (z. B. Hardware-Fehler, Software-Fehler, elektrische Störung, usw…)" (the expected rate (number of trips per unit time) at which a trip of the SIF can occur for reasons not associated with a problem in the process that the SIF is designed to protect (e.g., the trip resulted due to a hardware fault, software fault, electrical fault, transient, ground plane interference, etc.))*. Die Spurious-Trip Rate wird auch als nuisance trip rate bezeichnet.

[57] PFS: Probability of Failure Spurious-Trip
[58] $MTTF_{Spurious}$: Mean Time To Failure Spurious-Trip
[59] HFT: Hardware fault tolerance

Seien $N_{Spurious}(t)$ die Anzahl der Spurious-Trip Ausfälle im Zeitintervall $(0,t)$ und STR konstant. So ist der Spurious-Trip Ausfall homogen poissonverteilt. Dann wird die Wahrscheinlichkeit von $n = 0,1,2,...$ Ausfälle aufgrund des Spurious-Trips wie folgt definiert [77]:

$$p(N_{Spurious}(t) = n) = \frac{(STR \cdot t)^n}{n!} \cdot e^{-STR \cdot t} \tag{3.1}$$

Der Erwartungswert von Spurious-Trip Ausfall ist deshalb:

$$E[N_{Spurious}(t)] = STR \cdot t \tag{3.2}$$

Daraus folgt die Formel der STR-Berechnung:

$$STR = \frac{E[N_{Spurious}(t)]}{t} \tag{3.3}$$

Die Ursachen zu einem Spurious-Trip Ausfall wurde bereits in Kapitel 3.1 beschrieben. Daher wird die Spurious-Trip Rate einer $koon$-Architektur wie folgt berechnet:

$$STR_{koon} = STR_{koon\_S} + STR_{koon\_DD} + STR_{koon\_CCF} + STR_{koon\_FD} \tag{3.4}$$

mit:

- STR_{koon_S} : Spurious-Trip Rate aufgrund eines sicheren Fehler
- STR_{koon_DD} : Spurious-Trip Rate aufgrund eines gefährlich erkannten Fehler
- STR_{koon_CCF} : Spurious-Trip Rate aufgrund eines Fehler infolge gemeinsamer Ursache
- STR_{koon_FD} : Spurious-Trip Rate aufgrund einer nicht echten Anforderung

Der STR-Wert eines Sicherheitssystems (SIS) ist die Summe der STR-Werte der einzelnen Komponenten:

$$STR = \sum STR_i \tag{3.5}$$

In nachfolgender Tabelle werden die Spurious-Trip Formeln für verschiedene Systeme mit niedriger Anforderungsrate aus der Norm ANSI/ISA-TR84.00.02-2002 [06], PDS-Methode [86], [87], [88] und von Machleidt & Litz [69] verglichen, wobei der C_{koon}-Faktor aus der PDS-Methode nach der Formel in Tabelle 3.3 berechnet wird:

Tabelle 3.2: STR -Formel im Überblick aus verschiedenen herkömmlichen Verfahren

Architektur	ANSI/ISA TR84.00.02-2002 [06]	PDS-Methode [86], [87], [88]	Machleidt & Litz [69]
1oo1	$STR = \lambda_S + \lambda_{DD} + \lambda_F^S$	$STR = \lambda_{STU}$	$STR = \lambda_{sp} = \lambda_S$
1oo2	$STR = 2 \cdot (\lambda_S + \lambda_{DD}) + \beta \cdot (\lambda_S + \lambda_{DD}) + \lambda_F^S$	$STR = 2 \cdot \lambda_{STU}$	$STR = (2 - \beta_{sp}) \lambda_{sp}^{1oo2}$ $\lambda_{sp}^{1oo2} = \sqrt{\lambda_{sp1} \lambda_{sp2}}$
2oo2	$STR = 2 \cdot \lambda_S \cdot (\lambda_S + \lambda_{DD}) \cdot MTTR + \beta \cdot (\lambda_S + \lambda_{DD}) + \lambda_F^S$	$STR = \beta \cdot \lambda_{STU}$	
2oo3	$STR = 6 \cdot \lambda_S \cdot (\lambda_S + \lambda_{DD}) \cdot MTTR + \beta \cdot (\lambda_S + \lambda_{DD}) + \lambda_F^S$	$STR = C_{2oo3} \cdot \beta \cdot \lambda_{STU}$	$STR = \beta_{sp} \lambda_{sp}^{2oo3}$ $\lambda_{sp}^{2oo3} = \sqrt{(\lambda_{sp1} \lambda_{sp2}} \sqrt{+ \lambda_{sp1} \lambda_{sp3}} \sqrt{+ \lambda_{sp2} \lambda_{sp3})} / \sqrt{3}$
2oo4	$STR = 12 \cdot (\lambda_S + \lambda_{DD})^3 \cdot MTTR^2 + \beta \cdot (\lambda_S + \lambda_{DD}) + \lambda_F^S$	$STR = C_{2oo4} \cdot \beta \cdot \lambda_{STU}$	

Tabelle 3.3: C_{koon} -Faktor aus der PDS-Methode [86], [87], [88]

k\n	n=2	n=3	n=4	n=5	n=6
k=1	$C_{1oo2} = 1$	$C_{1oo3} = 0{,}5$	$C_{1oo4} = 0{,}3$	$C_{1oo5} = 0{,}21$	$C_{1oo6} = 0{,}17$
k=2		$C_{2oo3} = 2$	$C_{2oo4} = 1{,}1$	$C_{2oo5} = 0{,}7$	$C_{2oo6} = 0{,}4$
k=3			$C_{3oo4} = 2{,}9$	$C_{3oo5} = 1{,}8$	$C_{3oo6} = 1{,}1$
k=4				$C_{4oo5} = 3{,}7$	$C_{4oo6} = 2{,}4$
k=5					$C_{5oo6} = 4{,}3$

Wie bei dem gefährlichen Fehler werden die Definitionen von Zuverlässigkeit, Ausfallwahrscheinlichkeit und mittlere Zeit bis zum Ausfall aufgrund des Spurious-Trip-Fehlers in den folgenden Abschnitten beschrieben.

3.2.3 Zuverlässigkeitsfunktion des Spurious-Trips

Die Zuverlässigkeit eines Spurious-Trips ($R_{Spurious}(t)$) gibt die Wahrscheinlichkeit an, dass das System im Zeitintervall t verfügbar ist, ohne Ausfall aufgrund des Spurious-Trips. Die $R_{Spurious}(t)$-Funktion ist in der Form einer Exponential-Verteilung in Abhängigkeit von der Spurious-Trip Rate STR darzustellen.

$$R_{Spurious}(t) = e^{-\int_0^{\tau} STR(\tau)\cdot d\tau} \tag{3.6}$$

Sind die Ausfallraten bzw. STR konstant, wird die Zuverlässigkeitsfunktion des STR bestimmt durch:

$$R_{Spurious}(t) = e^{-STR\cdot t} \tag{3.7}$$

Für eine $koon$-Architektur wird $R_{Spurious\_koon}(t)$ als eine Funktion y in Abhängigkeit von STR dargestellt:

$$\begin{aligned} R_{Spurious\_koon}(t) &= \sum_{i=k}^{n} \binom{n}{i} \cdot R_{Spurious}^{i} \cdot (1 - R_{Spurious})^{n-i} \\ &= \sum_{i=0}^{n-k} \binom{n}{i} \cdot R_{Spurious}^{n-i} \cdot (1 - R_{Spurious})^{i} \\ &= y(STR) \end{aligned} \tag{3.8}$$

3.2.4 Probability of Failure Spurious-Trip

Probability of Failure Spurious-Trip (PFS) ist die Ausfallwahrscheinlichkeit aufgrund des Spurious-Trips. Je kleiner dieser Wert, desto verfügbarer ist das System. Für die Berechnung des Systems wird meist der PFS-Mittelwert PFS_{avg} angegeben. Die Formel für die PFS_{avg} sieht wie folgt aus:

$$PFS_{avg}(T) = \frac{1}{T}\int_0^T PFS(t)\cdot dt \tag{3.9}$$

$PFS(t)$ ist das Komplement der Zuverlässigkeitsfunktion $R_{Spurious}(t)$ des Spurious-Trips. Wenn die Ausfallrate bzw. Spurious-Trip Rate als nicht zeitabhängig angenommen wird, wird der $PFS(t)$-Wert anhand folgender Gleichung gerechnet:

$$\begin{aligned} PFS(t) &= 1 - R_{Spurious}(t) \\ &= 1 - e^{-STR\cdot t} \\ &\approx 1 - STR\cdot t \end{aligned} \tag{3.10}$$

Wird die (3.10) in die (3.9) eingesetzt, ergibt sich der PFS_{avg}-Wert wie folgt:

$$
\begin{aligned}
PFS_{avg}(T) &= \frac{1}{T}\int_0^T PFS(t)\cdot dt \\
&= \frac{1}{T}\int_0^T (1 - R_{Spurious}(t))\cdot dt \\
&= \frac{1}{T}\int_0^T (1 - e^{-STR\cdot t})\cdot dt \\
&= \frac{1}{T}\cdot [t]_0^T - \frac{1}{T}\cdot \left[\frac{e^{-STR\cdot t}}{-STR}\right]_0^T \\
&= 1 + \frac{e^{-STR\cdot T} - 1}{STR\cdot T}
\end{aligned}
\tag{3.11}
$$

3.2.5 Mean Time To Failure Spurious-Trip

Nach der ISA-TR84.00.02-2002 Norm [06] wird der Wert „Mean Time To Failure Spurious-Trip" ($MTTF_{Spurious}$) als die mittlere Zeit bis zum Ausfall aufgrund des Spurious-Trips des Prozesses oder EUC definiert. Der $MTTF_{Spurious}$ - Wert wird auch als die mittlere Zeit bis zum Auftreten eines sicheren Systemfehlers bezeichnet (S. 35, Teil 1, [06]).

Um den $MTTF_{Spurious}$ -Wert zu bestimmen, können einige Methoden angewendet werden wie z. B.: Blockdiagramm, Markov-Modell oder Monte-Carlo Simulation.

Mit der Blockdiagramm-Methode wird die Berechnung des $MTTF_{Spurious}$ -Werts über das Integral der Funktion $R_{Spurious}(t)$ mit:

$$
\begin{aligned}
MTTF_{Spurious} &= \int_0^\infty R_{Spurious}(t)\cdot dt \\
&= \int_0^\infty e^{-STR\cdot t} = \frac{1}{STR}
\end{aligned}
\tag{3.12}
$$

berechnet, wobei $R_{Spurious}(t)$ von der STR abhängt. Der STR -Wert wird ausgewertet, wenn das System nicht mehr verfügbar ist und durch die Summe der sicheren und gefährlich erkannten Ausfallrate bestimmt.

Die Bestimmung des $MTTF_{Spurious}$ -Werts nach dem Markov-Modell wird wie in [15], [17], [16], [19] beschriebenen Methode zur Bestimmung des $MTTF$ -Werts angewendet, das heißt, das Vorgehen ist wie folgt:

- Bestimmung der Übergangsmatrix P
- Bestimmung der absorbierenden Zustände und daraus folgt die Bildung der Matrix Q.
- Die M -Matrix ist das Berechnungsergebnis von $(I - Q)$
- Bestimmung der N -Matrix, welches die Inverse-Matrix von M ist

- Die Summe aller Elemente der ersten Zeile der N-Matrix ergibt den $MTTF_{Spurious}$-Wert.

Mit dem Markov-Modell wird die Bestimmung des $MTTF_{Spurious}$-Werts für unterschiedliche Systemarchitekturen in Kapitel 5 näher beschrieben.

3.2.6 Spurious-Trip Level

Für den Endanwender ist es wichtig, die Sicherheitsfunktionen, die sowohl ausreichende Sicherheits- als auch Prozess-Verfügbarkeit bieten, zu definieren. Die Prozess-Verfügbarkeit ist nicht im Standard IEC 61508 [48] oder in der IEC 61511 [49] definiert. Diese Standards definieren den SIL aber nicht den Level von Spurious-Trip. Zu diesem Zweck hat *Risknowlogy*© den Spurious-Trip Level™ (STL) definiert [47]. Der Zweck des STL ist es, dem Endanwender die gewünschte Prozess-Verfügbarkeit der Sicherheitsfunktion zu definieren. Auf Basis des STL-Werts wird der PFS-Wert berechnet. Die bessere Sicherheitsfunktion hat einen höheren STL-Level.

Tabelle 3.4: Spurious-Trip Level™ [47]

STL	Probability of Fail Safe Per Year	Kosten aufgrund Spurious-Trip
X	$\geq 10^{-(x+1)}$ to $< 10^{-x}$	...
…	…	…
5	$\geq 10^{-6}$ to $< 10^{-5}$	10M€ - 20M€
4	$\geq 10^{-5}$ to $< 10^{-4}$	5M€ - 10M€
3	$\geq 10^{-4}$ to $< 10^{-3}$	1M€ - 5M€
2	$\geq 10^{-3}$ to $< 10^{-2}$	500k€ - 1M€
1	$\geq 10^{-2}$ to $< 10^{-1}$	100k€ – 500k€

3.3 Neuer Ansatz zur Betrachtung des Spurious-Trips

Die Unterschiede zwischen Betriebsart mit niedriger Anforderungsrate und hoher Anforderungsrate wurden bereits im Kapitel 1 beschrieben. Diese Unterschiede, besonders die Anforderungsrate, haben großen Einfluss auf die PFD-Berechnung eines Systems mit periodischem Prooftest-Intervall [57], [58], und können sich auch auf die Berechnung des PFS_{avg}-, STR- und $MTTF_{Spurious}$-Werts auswirken. Außerdem spielt die Anforderungsdauer jeder Situation auch eine große Rolle, besonders wenn die Ausführung der Sicherheitsfunktion mehr Zeit benötigt [77]. Es gibt zahlreiche Literaturquellen über die Berechnung des STR-Werts, aber dieser Punkt wird bis jetzt nicht klar in diesen Arbeiten dargestellt. Es wird oft behauptet, dass es nicht notwendig ist, die niedrige Betriebsart von der hohen Betriebsart zu trennen. Allerdings sind die folgenden Eigenschaften bei beiden Betriebsarten unterschiedlich [52], [59]:

- Definition des sicheren Zustands
- Sequenz der Schutzschichten (sequence of protective layer)
- Art des Hazardous Event, wenn ein SIS und deren Schutzschicht teilweise bei Anforderung ausfallen
- Teststrategie für SIS: funktionaler Test und Diagnose-Test
- Potentielle Konsequenz von Spurious-Aktivierung auf EUC und SIS-Komponente
- Anforderungsrate und Anforderungsdauer

Daher liegt der Fokus dieser Arbeit auf der Auswirkung der Betriebsart auf die PFS_{avg}-, STR- und $MTTF_{Spurious}$-Berechnungen. Um diese Behauptung zu beweisen, werden die Blockdiagramm-Methode und das Markov-Modell benutzt. Die Formel der PFS_{avg}-Berechnung kann in Form einer Funktion $PFS_{avg} = f(\lambda_{DE}, \mu_{DE})$ in Abhängigkeit von Anforderungsrate λ_{DE} und Anforderungsdauer $\tau_{DE} = \frac{1}{\mu_{DE}}$ dargestellt werden. Mittels der PFS_{avg}-Funktion können die STR- und $MTTF_{Spurious}$-Funktionen auch in Abhängigkeit von der Anforderungsrate und Anforderungsdauer abgeleitet werden.
Durch diesen Ansatz ergeben sich die folgenden Vorteile bzw. Unterschiede zu den bestehenden Methoden:

- Das System wird je nach Betriebsart konkreter betrachtet und bewertet.
- Die Unterschiede der PFS_{avg}-, STR- und $MTTF_{Spurious}$-Berechnung zwischen System mit niedriger und hoher Anforderungsrate wird durch die Grafiken besser angezeigt.
- Alle Berechnungen werden gemäß der Norm IEC 61508 durchgeführt.

3.3.1 Lösungsansatz mit Blockdiagramm

Die Anwendung des Blockdiagramms ist die einfachste Methode um Spurious-Trip Fehler zu analysieren. Die Analyse kann in folgenden Schritten durchgeführt werden:

- Darstellung der System-Architektur als Block.
- Bestimmung der Fehlerart und welcher Zustand der Architektur erreicht wird. (Wie und wann tritt ein Fehler aufgrund eines Spurious-Trips auf? Welchen Zustand hat das Sicherheitssystem in diesem Fehlerfall?)
- Bestimmung der Spurious-Trip Rate, PFS_{avg} und $MTTF_{Spurious}$ in Abhängigkeit von der Anforderungsrate.

Zur Verdeutlichung des Lösungsansatzes mit dem Blockdiagramm wird ein Beispiel gegeben. Die Abbildung 3.1 stellt das Ruhestromsprinzip eines Sicherheitssystems mit einer 1oo2-Architektur dar. Die 1oo2-Architektur besteht aus zwei parallelen Kanälen. Es wird hier angenommen, dass beide Kanäle identisch sind. Die Schalter a und b seien geschlossen, sodass der Strom durchfließen kann, d. h. am Ausgang ergibt sich ein „1-Signal“. Die Schalter a und

b seien geöffnet (entweder gleichzeitig oder nacheinander oder einzeln), sodass kein Strom durchfließen kann, d. h., am Ausgang ergibt sich ein „0-Signal“. Das bedeutet:

- 0-Signal: eine Anforderung wird geschickt und somit muss SIS bzw. Gesamtanlage den sicheren Zustand bzw. stromlosen Zustand erreichen.
- 1-Signal: keine Anforderung wird geschickt und somit ist SIS bzw. Gesamtanlage nicht im stromlosen Zustand.

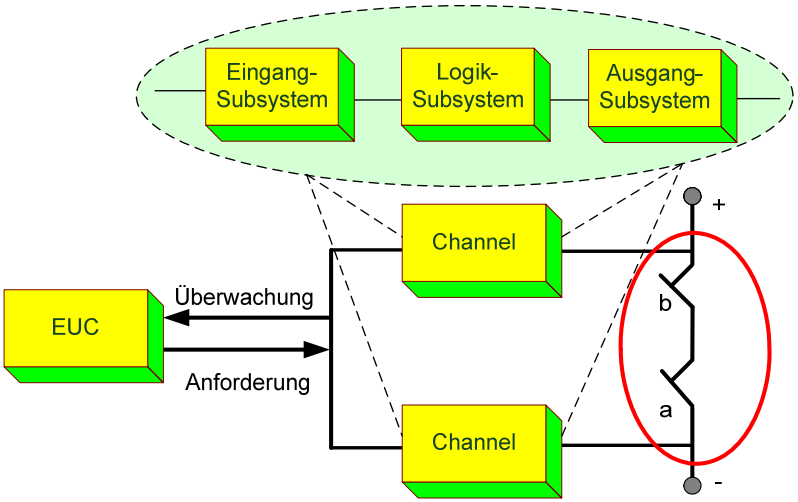

Abbildung 3.1: Arbeitsprinzip einer 1oo2-Architektur [17], [16]

Das Sicherheitssystem überwacht eine EUC-Anlage. Falls das EUC eine Anforderung an das SIS schickt, wird die Sicherheitsfunktion ausgeführt. In diesem Fall wird der stromlose Zustand erreicht, d. h. Schalter a und b öffnen sich. Es kann der Fall auftreten, dass ein „1- Signal“, welches das EUC an das SIS geschickt hat, im Sicherheitssystem verarbeitet und am Ausgang als „0-Signal“ ausgegeben wird. Dieser Fehler kann ein Fehler beim Einlesen des Eingangs-Subsystems oder bei der Verarbeitung des Logik-Subsystems oder bei der Ausgabe des Ausgang-Subsystems sein. Deshalb wird die Sicherheitsfunktion in diesem Fall auch ausgeführt, also Schalter a und b werden geöffnet. Der Fehlerfall, dass die Sicherheitsfunktion aufgrund einer nicht echten Anforderung ausgeführt wird, wird als Spurious-Trip Fehlerfall bezeichnet. Das bedeutet, am Ausgang wird ein 0-Signal ausgegeben, obwohl das 1-Signal eingentlich eingelesen und ausgegeben werden soll. Die 1oo2-Architektur fällt aufgrund eines Spurious-Trips aus, d. h. der bzw. die Schalter wird bzw. werden geöffnet obwohl keine echte Anforderung an SIS geschickt wurde, wenn einer von den folgenden Fällen auftritt:

- Ein CCF in beiden Kanälen:

Tabelle 3.5: Signale bei CCF der 1oo2-Architektur

Beide Eingangs-signale	Beide Logik-signale	Beide Ausgangs-signale	Fehlerart	Schalter a und b
0	0	0	unerkannter Fehler	offen
0	0	1	unerkannter Fehler	geschlossen
0	1	0	erkannter Fehler	offen
0	1	1	unerkannter Fehler	geschlossen
1	0	0	unerkannte Fehler	offen
1	0	1	unerkannte Fehler	geschlossen
1	1	0	erkannte Fehler	offen
1	1	1	kein Fehler	geschlossen

- Ein zufälliger Hardwarefehler bei einem Kanal:

Tabelle 3.6: Signale bei zufälligem Fehler in einem Kanal der 1oo2-Architektur

Eingangssignal	Logiksignal	Ausgangssignal	Fehlerart	Schalter a oder b
0	0	0	erkannter Fehler	offen
0	0	1	unerkannter Fehler	geschlossen
0	1	0	erkannter Fehler	offen
0	1	1	unerkannter Fehler	geschlossen
1	0	0	erkannter Fehler	offen
1	0	1	unerkannter Fehler	geschlossen
1	1	0	erkannter Fehler	offen
1	1	1	kein Fehler	geschlossen

- Die Auslösung der Sicherheitsfunktion wegen einer nicht echten Anforderung.

Die Fehler, die aufgrund eines Spurious-Trip zu dem sicheren Zustand führen, sind deshalb nach der Wahrheitstabelle sowohl der sicher (erkannte oder unerkannte) als auch der gefährliche erkannte Fehler. Daher ist die Rate des Spurious-Trips von diesen drei Fehlerarten und Anforderungsraten abhängig. Die Formel des Spurious-Trips der 1oo2-Architektur kann wie folgt beschrieben werden, welche noch ausführlich im Kapitel 4.2 dargestellt wird:

$$\begin{aligned} STR_{1oo2} &= STR_{1oo2\_S} + STR_{1oo2\_DD} + STR_{1oo2\_CCF} + STR_{1oo2\_FD} \\ &= 2 \cdot (1-\beta_S) \cdot \lambda_S + 2 \cdot (1-\beta_D) \cdot \lambda_{DD} \\ &+ \beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD} + \gamma \cdot \lambda_{DE} \end{aligned} \tag{3.13}$$

3.3.2 Lösungsansatz mit Markov-Modell

Die adäquate Methode zur Realisierung des in Abschnitt 1.3 genannten Ziels ist die Erstellung eines Markov-Modells. Ein Markov-Modell ist ein stochastisches (wahrscheinlichkeitstheoretisches) Modell und beschreibt ein System, welches in zufälliger Weise Zustände einnehmen kann. Dieser spezielle stochastische Prozess ist die Markov-Kette. Markov-Ketten zeichnen sich durch die so genannte Markov-Eigenschaft aus: Die Zukunft des Systems ist nur von der Gegenwart abhängig und nicht von der Vergangenheit [82].

Der $MTTF_{Spurious\_Trip}$-Wert kann in der Terminologie der Markov-Ketten als eine Absorptionszeit oder allgemeiner als eine Zeit des ersten Eintritts in eine Teilmenge des Zustandsraumes angesehen werden. Absorptionszeiten sind Zeiten des ersten Eintritts in einen absorbierenden Zustand. Der Begriff „absorbierender Zustand" ist selbsterklärend: Er ist ein Zustand, in welchen eine Markov-Kette mit positiver Wahrscheinlichkeit eintreten kann, aus welchem sie aber nur mit der Wahrscheinlichkeit 0 wieder austritt. Die Theorie der Markov-Kette stellt eine ganze Reihe von Resultaten und Methoden zur Berechnung derartiger Zeiten bereit. Diese gelten häufig nur unter gewissen zusätzlichen Voraussetzungen an die Markov-Kette. Die Aufgabe der Forschungsarbeiten ist es dann, diese Voraussetzungen in dem vorliegenden Spezialfall der Risikoanalyse entweder zu verifizieren oder ihnen eine praktische Bedeutung beizumessen. Ganz konkret sollen also die bereits über Absorptionszeiten (Eintrittszeiten) bekannten Aussagen aus der Theorie der Markov-Ketten auf die in Abschnitt 1.3 erwähnte Zielsetzung angewandt werden.

Absorptionszeiten sind wahrscheinlichkeitstheoretisch ausgedrückt Erwartungswerte. Dementsprechend unterscheiden sich ihre Berechnungsmethoden, je nachdem ob eine Markov-Kette mit diskreter Zeit oder mit kontinuierlicher Zeit vorliegt. Im Falle diskreter Zeit kommen die Neumannsche[60] Reihe (geometrische Reihe für Matrizen, benannt nach Carl Neuman, der diese auf die Potentialtheorie anwandte) und die Eigenwerttheorie von Matrizen zur Anwendung (siehe [42]). Im Falle kontinuierlicher Zeit hingegen werden dazu Methoden des Dunfordschen Funktionalkalküls eingesetzt (Einsetzen von Matrizen in holomorphe Funktionen oder Potenzreihen, siehe [30]).

Ähnlich wie in der Berechnung des *MTTF*-Wertes [19] lassen sich die Methoden zur Realisierung der in Abschnitt 1.3 genannten Ziele also wie folgt in zwei Gruppen zusammenfassen:

- Methoden der Stochastik oder Wahrscheinlichkeitstheorie:
  - Beschreibung des Systems.
  - Klassifikation der Zustände.
  - Berechnung von Erwartungswerten
- Methoden der Funktionalanalysis oder Operatorentheorie:
  - Neumannsche Reihe.
  - Eigenwerttheorie von Matrizen.
  - Dunfordscher Funktionalkalkül.

Diese beiden Gruppen von Methoden sind nur scheinbar völlig gegensätzlicher Natur, weil sie durch den übergeordneten Begriff der Maßtheorie sehr wohl eng miteinander verknüpft sind.

---

[60] Neumannsche Reihe ist eine Reihe der Form: $\sum_{n=0}^{\infty} T^n$, wobei $T : X \to X$ ein stetiger linearer Operator auf einem normierten Raum X ist und $T^0 := Idx$

Im Folgenden soll angenommen werden, dass die Markov-Kette eines Systems eine Zustandsmenge von S hat. Diese Zustandsmenge S lässt sich in die nicht leere Menge R der rekurrenten Zustände und die nicht leere Menge T der transienten Zustände teilen. Mehr über die rekurrenten Zustände und die transienten Zustände sind im Anhang A zu finden.

Seien der Anfangszustand $i \in T$ und D die Zeit bis der Prozess in einem Zustand von R landet, d. h. die Zeit zur Absorption in der Menge R. Die Bezeichnung μ_{iR} wird hier als der Erwartungswert der Absorptionszeit verwendet und es gilt die folgende Gleichung:

$$\mu_{iR} = E(D \mid X_0 = i) \tag{3.14}$$

Sei D' die Dauer bis zur Absorption vom Zeitpunkt nach dem ersten Übergang aus gerechnet. Es ist:

$$D' = D + 1 \tag{3.15}$$

Mit der Markov-Eigenschaft gilt:

$$E(D' \mid X_1 = j,\ X_0 = i) = E(D \mid X_0 = j) \tag{3.16}$$

Aus der Definition von D folgt:

$$E(D \mid X_1 = j,\ \ X_0 = i) = 1 \qquad \text{für } i \in T,\ j \in R \tag{3.17}$$

Der Stichprobenraum wird im Zeitpunkt 1 zerlegt:

$$\begin{aligned} E(D \mid X_0 = i) &= \sum_{j \in S} E(D \mid X_1 = j,\ X_0 = i) \cdot P\{X_1 = j \mid X_0 = i\} \\ &= \sum_{j \in T} E(D \mid X_1 = j,\ X_0 = i) \cdot p_{ij} + p_{iR} \\ &= \sum_{j \in T} [E(D' \mid X_1 = j,\ X_0 = i) + 1] \cdot p_{ij} + p_{iR} \\ &= \sum_{j \in T} E(D' \mid X_1 = j,\ X_0 = i) \cdot p_{ij} + 1 \\ &= \sum_{j \in T} p_{ij} E(D \mid X_0 = j) + 1 \end{aligned} \tag{3.18}$$

Aus Gleichungen (3.14) und (3.18) gilt für die Absorptionszeit:

$$\mu_{iR} = 1 + \sum_{j \in T} p_{ij} \mu_{jR} \qquad \forall i \in T \tag{3.19}$$

Da $MTTF_{Spurious}$ als die Absorptionszeit definiert ist, gilt für $MTTF_{Spurious}$ auch diese Behauptung.

3.3.3 Voraussetzung und Beschränkung der Analyse des Lösungsansatzes

Um die Analyse des Lösungsansatzes besser zu beschreiben, werden folgende Voraussetzungen angewendet, die gemäß der Norm IEC 61508 [48] sind:

- Alle Berechnungen werden per SIF-Teil durchgeführt und sind daher ausschließlich auf einen Sensorik, Logik oder Aktorik bezogen.
- Die Bauteil-Ausfallraten sind während der Lebensdauer des Systems konstant.
- Nur ein Ausfall darf in einem einzelnen Kanal auftreten bis der nächste Prooftest stattfindet, z. B. kann somit in einem Kanal mit DU[61]-Fehler kein zusätzlich DD[62]-Fehler auftreten.
- Ist keine der untergeordneten Komponenten ausgefallen, hat der Kanal insgesamt den Status OK. Ansonsten wird dem Kanal der Fehlertyp der ausgefallenen Baugruppe zugeordnet.
- Die Kanäle in einem System haben gleiche Ausfallraten und den gleichen Diagnosedeckungsgrad.
- Online-Reparatur ist bei 2oo2 möglich, jedoch nicht bei 1oo1, 1oo2.
- Fehler, die durch Online-Diagnose erkannt werden, werden auch in der Reparaturzeit repariert. Die Reparaturzeit des sicheren Fehler $MTTR_S$ sei gleich die Reparaturzeit des gefährlichen Fehler $MTTR_D$, d. h. $MTTR_S = MTTR_D = MTTR$ Die Fehler, die nicht durch Online-Diagnose erkannt werden, werden als unerkannte Fehler definiert.
- Während der Wiederholungsprüfung werden alle im System enthaltenen Fehler gefunden und repariert. Somit hat das System nach der Wiederholungsprüfung einen „wie neuen“ Zustand.
- Tritt ein Fehler infolge gemeinsamer Ursache auf, sind alle Kanäle in der SIF ausgefallen. Der Faktor dieses Fehlers sei bei allen Architekturen gleich. Der Faktor β_S sei bei sicherem Fehler größer als β_D bei gefährlichem Fehler.
- Bei allen Markov-Modellen kann nur ein Fehler pro diskreten Zeitschritt T auftreten. Tritt ein Common Cause Fehler auf, werden alle Kanäle in der SIF ausfallen.
- Das Diagnose-Testintervall[63] jedes Teilsystems, das eine Fehlertoleranz der Hardware von Null besitzt und die Sicherheitsfunktion(en) in der Betriebsart mit niedriger Anforderungsrate ausführt, muss so gewählt sein, damit das SIS die Anforderung zur Wahrscheinlichkeit eines zufälligen Hardwareausfalls erfüllen kann.
- Das Diagnose-Testintervall jedes Teilsystems, das eine Fehlertoleranz der Hardware von Null besitzt und die Sicherheitsfunktion(en) in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben werden, muss so gewählt sein, dass das erwartete Intervall den Anforderungen mindestens um eine Zehnerpotenz größer als das Diagnosetestintervall oder die Summe der Diagnosetestintervalle ist, und die

[61] DD: Dangerous undetected
[62] DU: Dangerous detected
[63] Diagnose-Testintervall ist die Zeit, in dem der Diagnosetest vollständig durchgeführt und wiederholt wird. Innerhalb dieser Zeit werden zufällige Hardwarefehler erkannt (Abschnitt 3.8.7, Teil 4 [48]).

Zeit, um den sicheren Zustand zu erreichen, ist kleiner als die Prozess-Sicherheitszeit[64] (Abschnitt B.3 des Teil 6 der IEC 61508 [48]) oder das Verhältnis der Diagnose-Testrate zur Anforderungsrate 100 gleicht oder übertrifft (7.4.4.1.4 Teil 2 der IEC 61508 [48]).

- Das Diagnose-Testintervall jedes Teilsystems, das eine Fehlertoleranz der Hardware größer als Null besitzt, muss so gegeben sein, dass das SIS die Anforderung zur Wahrscheinlichkeit eines zufälligen Hardwareausfalls erfüllen kann.

3.4 Zusammenfassung

Der Spurious-Trip Ausfall ist ein unerwarteter Ausfall eines Systems, da die Sicherheitsfunktion auf eine nicht echte Anforderung ausgelöst wird. Dieser Ausfall ist deshalb für wirtschaftliche Gründe nicht gut geeignet, wenn das System besonders aus der Sicht der Verfügbarkeit betrachtet wird. Allerdings gibt es noch keine eindeutige Auslegung des Begriffs des Spurious-Trips. Daher sind die Konzepte des Spurious-Trips in verschiedenen Applikationen auch unterschiedlich. Diese Unterschiede wurden bereits in Abschnitt 3.1 beschrieben. Im Abschnitt 3.2 wurden die Sicherheitsparameter des Spurious-Trips (wie PFS_{avg}, $MTTF_{Spurious}$, STR und STL) definiert, sowie deren Berechnungsgleichungen dargestellt. Aus den herkömmlichen Verfahren haben der STR- bzw. $MTTF_{Spurious}$-Wert bei der Betriebsart mit niedriger Anforderungsrate und hoher Anforderungsrate ein gleiches Ergebnis. Allerdings können die Unterschiede zwischen beiden Betriebsarten die Berechnung des PFS_{avg}-, $MTTF_{Spurious}$- und STR-Wertes beeinflussen. Aus diesem Grund wurde ein neuer Ansatz zur Betrachtung des Spurious-Trips im Abschnitt 3.3 dieses Kapitels beschrieben. Der neue Ansatz wird mittels Blockdiagramm und Markov-Modell bewiesen. Die Vorgehensweise des Beweises wurde anhand des Blockdiagramms im Abschnitt 3.3.1 und anhand des Markov-Modells im Abschnitt 3.3.2 beschrieben. Mit der im Abschnitt 3.3.3 vorgegebenen Voraussetzungen und Beschränkungen werden die Sicherheitsparameter des Spurious-Trips in Kapitel 4 mittels Blockdiagramm und in Kapitel 5 mittels Markov-Modell berechnet. Der neue Ansatz zur Betrachtung des Spurious-Trips Ausfalls wird dadurch detaillierter dargestellt.

[64] Die Prozess-Sicherheitszeit ist die Zeitspanne zwischen dem Auftreten eines Ausfalls der EUC und dem Zeitpunkt, bei dem die Reaktion in der EUC abgeschlossen sein muss, um das Auftreten des gefährlichen Vorfalls zu verhindern (Abschnitt 3.6.20, Teil 4 [48]).

4 Berechnung der Spurious-Trip Parameter mittels Blockdiagramm

In diesem Kapitel werden die Kenngrößen des Spurious-Trips für unterschiedliche Systemarchitekturen nach dem Ruhestromprinzip unter den Voraussetzungen, die bereits in Kapitel 3.3.3 beschrieben wurden, bestimmt. Die Bestimmung dieser Kenngrößen wird mittels Blockdiagramm durchgeführt. Die zu untersuchenden Systemarchitekturen sind: 1oo1, 1oo2, 2oo2 und 2oo3. Zum Schluss dieses Kapitels wird die STR-, PFS_{avg}- und $MTTF_{Spurious}$-Formel für ein allgemeines 1*oon* und *koon*-System dargestellt. Die in diesem Kapitel resultierenden Gleichungen sind Funktionen in Abhängigkeit der Anforderungsrate. Um die Beeinflussung der Anforderungsrate auf Sicherheitsparameter des Spurious-Trips besser darzustellen, werden die Berechnungsbeispiele und die daraus resultierenden Diagramme in Kapitel 6 beschrieben. Die folgenden Annahmen werden für die Herleitung der Gleichungen verwendet:

- β_S: Ausfallsteilheit, Gewichtung für CCF aufgrund des sicheren Fehlers
- β_D: Ausfallsteilheit, Gewichtung für CCF aufgrund des gefährlich erkannten Fehlers
- λ_{SD}: sicher erkannte Ausfallrate
- λ_{SU}: sicher unerkannte Ausfallrate
- λ_{DD}: gefährlich erkannte Ausfallrate
- λ_S: sichere Ausfallrate
- λ_D: gefährliche Ausfallrate
- λ_{DE}: Anforderungsrate
- $0 < \gamma < 1$: Faktor einer nicht echten Anforderung zu den Gesamtanforderungen an SIS in einem betrachteten Zeitintervall.
- $STR_{FD} = \gamma \cdot \lambda_{DE}$: Spurious-Trip Rate aufgrund einer nicht echten Anforderung

4.1 1oo1-Architektur

Diese Architektur besteht aus einem einzelnen Kanal. Daher führt jeder gefährliche Ausfall zu einem Ausfall der Sicherheitsfunktion, wenn eine Anforderung auftritt.

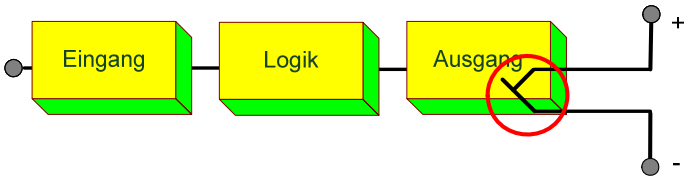

Abbildung 4.1: Blockdiagramm der 1oo1-Architektur

Bei jedem erkannten Ausfall bringt das Sicherheitssystem mit 1oo1-Architektur die EUC in den sicheren Zustand. Außerdem wird das Gesamtsystem ohne Fehler in den sicheren Zustand gebracht, wenn eine Anforderung kommt. Wie ein Sicherheitssystem mit 1oo1-Architektur und EUC bei dem Fehlerfall sich verhalten, wird in der Abbildung 4.2 gezeigt:

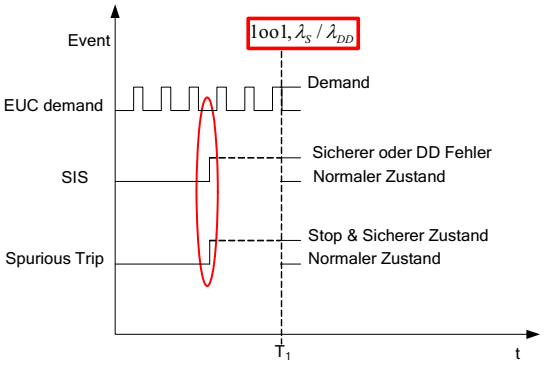

Abbildung 4.2: EUC und SIS mit 1oo1-Architektur

Der Spurious-Trip Zustand wird erreicht, wenn im SIS:

- ein sicherer Fehler aufgetreten ist oder
- ein gefährlich erkannter Fehler aufgetreten ist oder
- eine nicht echte Anforderung auf Auslösung der Sicherheitsfunktion gefordert wird

Daher besteht die Spurious-Trip Rate nicht nur aus der Rate des sicheren Fehlers λ_S und des gefährlich erkannten λ_{DD} Fehlers sondern auch aus der Anforderungsrate λ_{DE}. Daraus folgt die Berechnung der Spurious-Trip Rate für die 1oo1-Architektur:

$$\begin{aligned} STR_{1oo1} &= STR_{1oo1\_S} + STR_{1oo1\_DD} + STR_{FD} \\ &= \lambda_S + \lambda_{DD} + \gamma \cdot \lambda_{DE} \end{aligned} \qquad \textbf{(4.1)}$$

Um den PFS_{avg_1oo1}-Wert zu berechnen, werden erst die $PFS_{avg\_1oo1\_S}$[65]-, $PFS_{avg\_1oo1\_DD}$[66] und PFS_{avg_FD}[67]-Wert bestimmt. Der $PFS_{avg\_1oo1\_S}$- und der $PFS_{avg\_1oo1\_DD}$-Wert wird über Intergral im Prooftest-Intervall $(0...T)$ wie folgt berechnet:

[65] $PFS_{avg\_1oo1\_S}$: Ausfallwahrscheinlichkeit aufgrund Spurious-Trip des sicheren Fehlers.
[66] $PFS_{avg\_1oo1\_DD}$: Ausfallwahrscheinlichkeit aufgrund Spurious-Trip des gefährlich erkannten Fehlers.
[67] $PFS_{avg\_1oo1\_FD}$: Ausfallwahrscheinlichkeit aufgrund Spurious-Trip der nicht echten Anforderung

$$
\begin{aligned}
PFS_{avg\_1oo1\_S} &= \frac{1}{T}\int_0^T PFS_{1oo1\_S}(t)\cdot dt \\
&= \frac{1}{T}\int_0^T (1-e^{-STR_{1oo1\_S}\cdot t})\cdot dt \\
&= 1-\frac{1}{T}\int_0^T e^{-STR_{1oo1\_S}\cdot t}\cdot dt \\
&= 1-\frac{1}{T}\cdot\left[\frac{e^{-STR_{1oo1\_S}\cdot t}}{-STR_{1oo1\_S}}\right]_0^T \\
&= 1-\frac{1}{T}\cdot\left[\frac{e^{-STR_{1oo1\_S}\cdot T}}{-STR_{1oo1\_S}}-\frac{1}{-STR_{1oo1\_S}}\right] \\
&= 1-\frac{1}{T}\cdot\frac{1}{STR_{1oo1\_S}}\cdot\left(1-e^{-STR_{1oo1\_S}\cdot T}\right) \\
&\approx \frac{STR_{1oo1\_S}\cdot T}{2} = \frac{\lambda_S\cdot T}{2}
\end{aligned}
\qquad \textbf{(4.2)}
$$

Der $PFS_{avg\_1oo1\_DD}$-Wert wird analog wie der $PFS_{avg\_1oo1\_S}$-Wert gerechnet. Somit gilt die Gleichung:

$$PFS_{avg\_1oo1\_DD} \approx \frac{STR_{1oo1\_DD}\cdot T}{2} = \frac{\lambda_{DD}\cdot T}{2} \qquad \textbf{(4.3)}$$

Fällt ein System aufgrund der nicht echten Anforderung zum Spurious-Trip Ausfall aus, ist das System innerhalb der Anforderungsdauer τ_{DE} nicht verfügbar. Die PFS_{avg_FD}-Berechnung ist bei allen Architekturen gleich und wird wie folgt bestimmt:

$$PFS_{avg\_FD} = \gamma\cdot\lambda_{DE}\cdot\tau_{DE} \qquad \textbf{(4.4)}$$

Anhand der Gleichungen (3.11), (4.2), (4.3) und (4.4) wird die Formel für PFS_{avg_1oo1}-Wert beschrieben als:

$$
\begin{aligned}
\Rightarrow PFS_{avg\_1oo1} &= PFS_{avg\_1oo1\_S} + PFS_{avg\_1oo1\_DD} + PFS_{avg\_FD} \\
&= \frac{(\lambda_S+\lambda_{DD})\cdot T}{2} + \gamma\cdot\lambda_{DE}\cdot\tau_{DE}
\end{aligned}
\qquad \textbf{(4.5)}
$$

Aus der Gleichung (3.7), (3.12) und (4.1) wird der $MTTF_{Spurious\_1oo1}$-Wert wie folgt bestimmt:

$$MTTF_{Spurious\_1oo1} = \int_0^\infty R_{Spurious\_1oo1}(t) \cdot dt = \int_0^\infty e^{-STR_{1oo1} \cdot t} = \frac{1}{\lambda_S + \lambda_{DD} + \gamma \cdot \lambda_{DE}} \quad (4.6)$$

4.2 1oo2-Architektur

Im Gegensatz zu einem 1oo1-System besitzt das 1oo2-System zwei voneinander unabhängige Kanäle. Bei der 1oo2-Architektur muss ein gefährlicher Ausfall in beiden Kanälen vorliegen, bevor die Sicherheitsfunktion bei Anforderung ausfallen würde.

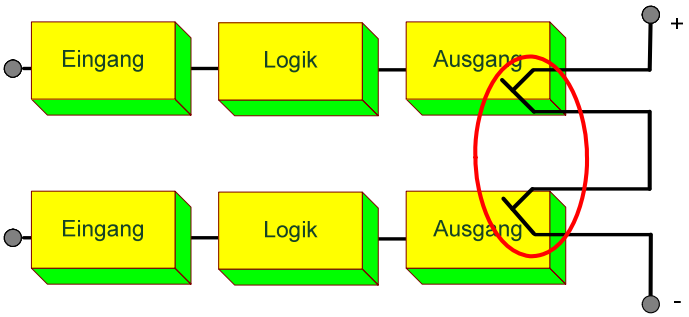

Abbildung 4.3: Blockdiagramm der 1oo2-Architektur

Bei Erkennung eines Ausfalls in einem der beiden Kanäle bringt das Sicherheitssystem mit 1oo2-Architektur das EUC in den sicheren Zustand. Somit fällt das Gesamtsystem aufgrund von Spurious-Trip aus, wenn im Fehlerfall einer dieser Fälle im System auftritt:

- ein sicherer Fehler ist bei einem Kanal im SIS aufgetreten
- ein gefährlich erkannter Fehler ist aufgetreten
- ein CCF ist im SIS aufgetreten
- eine nicht echte Anforderung wird auf Auslösung der Sicherheitsfunktion gefordert.

Das Verhalten zwischen dem Sicherheitssystem mit 1oo2-Architektur und dem EUC im Fehlerfall aufgrund Spurious-Trips wird in der Abbildung 4.4 und Abbildung 4.5 dargestellt:

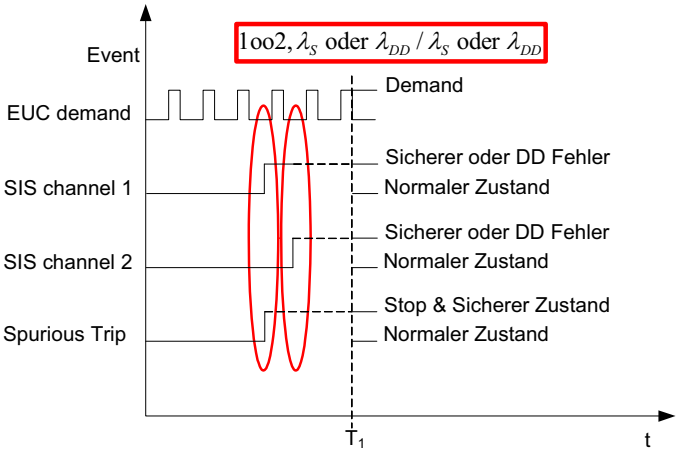

Abbildung 4.4: EUC und SIS mit 1oo2-Architektur (zufällige Fehler)

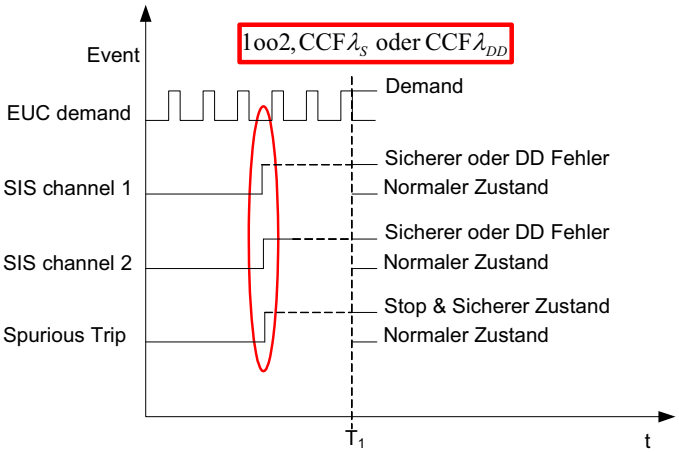

Abbildung 4.5: EUC und SIS mit 1oo2-Architektur (CCF)

Die *STR*-Gleichung einer 1oo2-Architektur wird daher nicht nur aus dem Teil, der sich bezüglich auf zufällige Fehler bezieht, gebildet, sondern auch aus dem Teil, der sich auf Common Cause Fehler (CCF) bezieht, wobei die beiden Fehlerarten sichere erkannte Fehler sind.

- Wird ein Spurious-Trip Ausfall durch CCF verursacht, ist der *STR*-Wert gleich: $\beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD}$.

- Für den sich auf zufällige Fehler beziehender Teil wird der STR_S-Wert aus der Summe $[(1-\beta_S)\cdot\lambda_S]$ gerechnet. Da es bei einer 1oo2-Architektur zwei Möglichkeiten für einen zufälligen Ausfall eines Kanals gibt, wird die Gleichung um den Faktor zwei erweitert: $2\cdot[(1-\beta_S)\cdot\lambda_S]$.
- Analog für gefährlich erkannter Fehler ist $STR_{DD} = 2(1-\beta_D)\cdot\lambda_{DD}$
- Wird ein Spurious-Trip Ausfall durch eine nicht echte Anforderung verursacht, ist der STR_{FD}-Wert gleich: $\gamma\cdot\lambda_{DE}$

Die Formel für die STR_{1oo2}-Berechnung ergibt sich dann:

$$\begin{aligned} STR_{1oo2} &= STR_{1oo2\_S} + STR_{1oo2\_DD} + STR_{1oo2\_CCF} + STR_{1oo2\_FD} \\ &= 2\cdot(1-\beta_S)\cdot\lambda_S + 2\cdot(1-\beta_D)\cdot\lambda_{DD} \\ &+ \beta_S\cdot\lambda_S + \beta_D\cdot\lambda_{DD} + \gamma\cdot\lambda_{DE} \end{aligned} \quad \textbf{(4.7)}$$

Der PFS_{1oo2_S}-Wert lässt sich bestimmen durch:

$$PFS_{1oo2\_S} = 1 - R_{Spurious\_1oo2\_S} \quad \textbf{(4.8)}$$

wobei:

$$\begin{aligned} R_{Spurious\_koon} &= \sum_{i=k}^{n}\binom{n}{i}\cdot R_{Spurious}^{i}\cdot(1-R_{Spurious})^{n-i} \\ &= \sum_{i=0}^{n-k}\binom{n}{i}\cdot R_{Spurious}^{n-i}\cdot(1-R_{Spurious})^{i} \end{aligned} \quad \textbf{(4.9)}$$

Die Zuverlässigkeit $R_{Spurious\_1oo2\_S}$ der 1oo2-Architektur lautet damit:

$$\begin{aligned} R_{Spurious\_1oo2\_S} &= \sum_{i=0}^{1}\binom{2}{i}R_{Spurious\_S}^{2-i}\cdot(1-R_{Spurious\_S})^{i} \\ &= 2\cdot R_{Spurious\_S} - R_{Spurious\_S}^{2} \\ &= 2\cdot e^{-STR_{1oo2\_S}\cdot t} - e^{-2\cdot STR_{1oo2\_S}\cdot t} \end{aligned} \quad \textbf{(4.10)}$$

Daraus folgt die Berechnung für $PFS_{avg\_1oo2\_S}$ anhand der Gleichung (3.9):

$$
\begin{aligned}
PFS_{avg\_1oo2\_S} &= \frac{1}{T}\int_0^T PFS_{1oo2\_S}(t) \\
&= \frac{1}{T}\int_0^T (1 - R_{Spurious\_1oo2\_S}) \cdot dt \\
&= 1 - \frac{1}{T} \cdot \left[\frac{2 \cdot e^{-STR_{1oo2\_S} \cdot t}}{-STR_{1oo2\_S}} - \frac{e^{-2 \cdot STR_{1oo2\_S} \cdot t}}{-2 \cdot STR_{1oo2\_S}} \right]_0^T \\
&= 1 + \frac{2}{T} \cdot \frac{e^{-STR_{1oo2\_S} \cdot T} - 1}{STR_{1oo2\_S}} - \frac{e^{-2 \cdot STR_{1oo2\_S} \cdot T} - 1}{2 \cdot T \cdot STR_{1oo2\_S}}
\end{aligned}
\tag{4.11}
$$

Nach der MacLaurin'sche Reihen-Entwicklung [16]:

$$
e^{-a \cdot T} = 1 - a \cdot T + \frac{a^2 \cdot T^2}{2!} - \frac{a^3 \cdot T^3}{3!} + R_4 \tag{4.12}
$$

und:

$$
e^{-2 \cdot a \cdot T} = 1 - 2 \cdot a \cdot T + \frac{(2 \cdot a)^2 \cdot T^2}{2!} - \frac{(2 \cdot a)^3 \cdot T^3}{3!} + R_4 \tag{4.13}
$$

Das Restglied R_4 konvergiert an der Stelle $T = 0$ gegen den Wert 0 und ist bei der Bildung des Grenzwertes an der Stelle $T = 0$ gegenüber dem vierten Term vernachlässigbar klein [16]:

$$
\lim_{T \to 0} R_4 = 0 \tag{4.14}
$$

Durch Ersetzen der Gleichungen (4.12), (4.13)und (4.14) in die (4.11) ergibt sich dann:

$$
\begin{aligned}
\Rightarrow PFS_{avg\_1oo2\_S} &= 1 + \frac{2}{T} \cdot \frac{e^{-STR_{1oo2\_S} \cdot T} - 1}{STR_{1oo2\_S}} - \frac{e^{-2 \cdot STR_{1oo2\_S} \cdot T} - 1}{2 \cdot T \cdot STR_{1oo2\_S}} \\
&= 1 + \frac{2}{T \cdot STR_{1oo2\_S}} \cdot [1 - STR_{1oo2\_S} \cdot T \\
&\quad + \frac{STR_{1oo2\_S}{}^2 \cdot T^2}{2} - \frac{STR_{1oo2\_S}{}^3 \cdot T^3}{6} - 1] \\
&\quad - \frac{1}{T \cdot STR_{1oo2\_S}} \cdot [1 - 2 \cdot STR_{1oo2\_S} \cdot T \\
&\quad + \frac{(2 \cdot STR_{1oo2\_S})^2 \cdot T^2}{2} - \frac{(2 \cdot STR_{1oo2\_S})^3 \cdot T^3}{6} - 1] \\
&= \frac{STR_{1oo2\_S}{}^2 \cdot T^2}{3}
\end{aligned}
\tag{4.15}
$$

Analog wie der $PFS_{avg\_1oo2\_S}$-Wert lässt sich der $PFS_{avg\_1oo2\_DD}$-Wert wie folgt berechnen:

$$PFS_{avg\_1oo2\_DD} = \frac{STR_{1oo2\_DD}{}^2 \cdot T^2}{3} \tag{4.16}$$

Der PFS_{avg_1oo2}-Wert ist die Summe von Ausfallwahrscheinlichkeit aufgrund Spurious-Trip der sicheren Fehler $PFS_{avg\_1oo2\_S}$, Ausfallwahrscheinlichkeit aufgrund Spurious-Trip der gefährlich erkannten Fehler $PFS_{avg\_1oo2\_DD}$, Ausfall Ausfallwahrscheinlichkeit aufgrund Spurious-Trip der Fehler infolge gemeinsamen Ursache PFS_{avg_CCF} und Ausfallwahrscheinlichkeit aufgrund Spurious-Trip der nicht echten Anforderung PFS_{avg_FD}. Weil der Faktor der Fehler infolge gemeinsamer Ursache gemäß der Voraussetzung in Kapitel 3.3.3 bei allen Architekturen gleich ist, ist der PFS_{avg_CCF}-Wert bei allen Architekturen auch gleich und wird wie folgt bestimmt:

$$PFS_{avg\_CCF} = (\beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD}) \cdot MTTR \tag{4.17}$$

Aus der Gleichung (4.4), (4.15), (4.16) und (4.17) wird der PFS_{avg_1oo2}-Wert nach folgender Gleichung gerechnet:

$$\begin{aligned} PFS_{avg\_1oo2} &= PFS_{avg\_1oo2\_S} + PFS_{avg\_1oo2\_DD} + PFS_{avg\_CCF} + PFS_{avg\_1oo2\_FD} \\ &= \frac{STR_{1oo2\_S}{}^2 \cdot T^2}{3} + \frac{STR_{1oo2\_DD}{}^2 \cdot T^2}{3} \\ &+ (\beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD}) \cdot MTTR + \gamma \cdot \lambda_{DE} \cdot \tau_{DE} \end{aligned} \tag{4.18}$$

Anhand der Gleichung (4.9) wird die Zuverlässigkeit $R_{Spurious\_1oo2}$ für eine 1oo2-Architektur wie folgt bestimmt:

$$\begin{aligned} R_{Spurious\_1oo2} &= \sum_{i=0}^{1} \binom{2}{i} R_{Spurious}^{2-i} \cdot (1 - R_{Spurious})^i \\ &= 2 \cdot R_{Spurious} - R_{Spurious}^2 \\ &= 2 \cdot e^{-STR_{1oo2} \cdot t} - e^{-2 \cdot STR_{1oo2} \cdot t} \end{aligned} \tag{4.19}$$

Der $MTTF_{Spurious\_1oo2}$-Wert kann berechnet werden, indem die Gleichungen (4.7) und (4.19) in die Gleichung (3.12) eingesetzt werden.

$$\begin{aligned} MTTF_{Spurious\_1oo2} &= \int_0^\infty R_{Spurious\_1oo2}(t) \cdot dt \\ &= \int_0^\infty \left[2 \cdot e^{-STR_{1oo2} \cdot t} - e^{-2 \cdot STR_{1oo2} \cdot t} \right] \cdot dt \\ &= \left[\frac{2 \cdot e^{-STR_{1oo2} \cdot t}}{-STR_{1oo2}} - \frac{e^{-2 \cdot STR_{1oo2} \cdot t}}{-2 \cdot STR_{1oo2}} \right]_0^\infty = \frac{3}{2 \cdot STR_{1oo2}} \end{aligned} \tag{4.20}$$

4.3 2oo2-Architektur

Die 2oo2-Architekur besteht, wie das 1oo2-System, aus zwei voneinander unabhängigen parallelen Kanälen. Jeder dieser Kanäle muss die Sicherheitsfunktion anfordern, bevor die Sicherheitsfunktion für das Gesamtsystem ausgeführt werden kann.

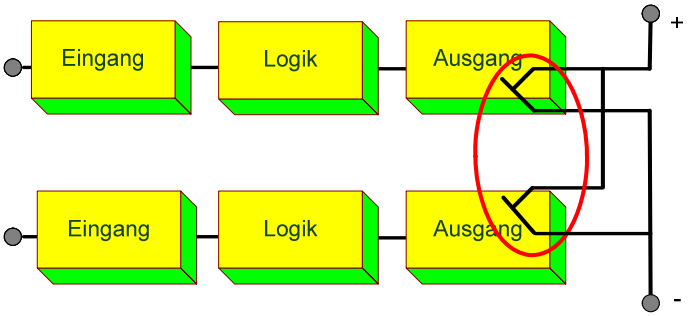

Abbildung 4.6: Blockdiagramm der 2oo2-Architektur

Bei dieser Architektur wird jeder Kanal bei Erkennung irgendeines Fehlers in den sicheren Zustand gesetzt. Das System mit einer 2oo2-Architektur ist aufgrund des Spurious-Trips ausgefallen, wenn einer der folgenden Fälle auftritt:

- ein sicherer Fehler oder ein gefährlich erkannter Fehler ist bei beiden Kanälen (CCF) im SIS aufgetreten
- bei einem Kanal ist ein sicherer Fehler aufgetreten und befindet sich in der Reparaturzeit. Bei diesem Fall reagiert das System wie ein System mit 1oo1-Architektur in der Betriebsart mit niedriger Anforderungsrate.
- eine nicht echte Anforderung wird auf Auslösung der Sicherheitsfunktion gefordert.

Die Abbildung 4.7 und Abbildung 4.8 stellen den Fall eines Spurious-Trip Ausfalls für zufällige Fehler und CCF dar.

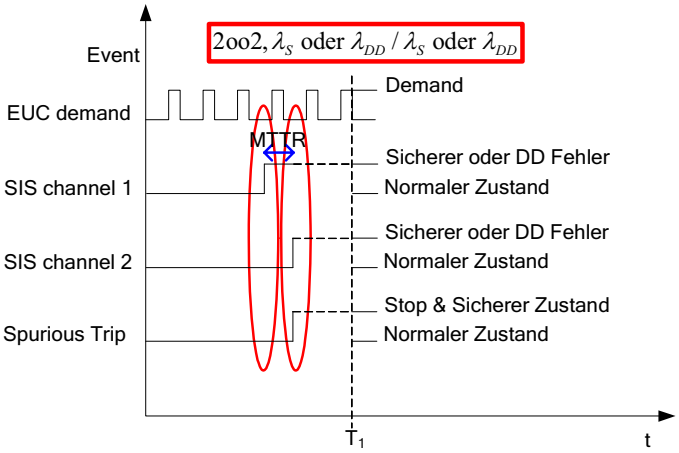

Abbildung 4.7: EUC und SIS mit 2oo2-Architektur (zufällige Fehler)

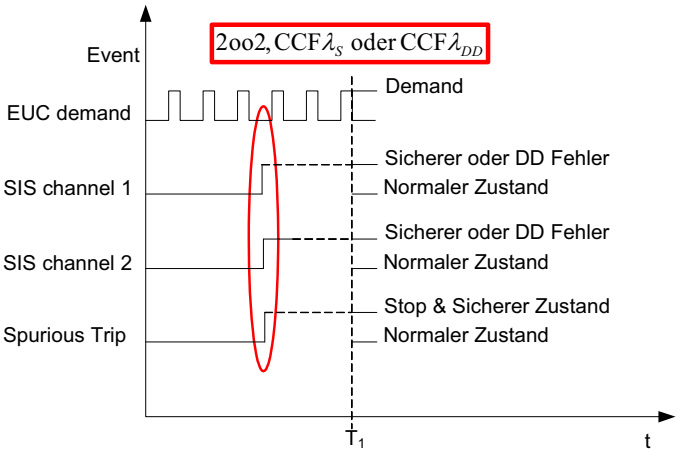

Abbildung 4.8: EUC und SIS mit 2oo2-Architektur (CCF)

Daher unterscheiden sich die *STR*-Gleichungen zwischen 1oo2- und 2oo2-Architektur in dem Produkt, bestehend aus der Ausfallrate für zufällige Fehler (sichere und gefährlich erkannter Fehler) und der Reparaturzeit (*MTTR*). Das ist damit zu erklären, dass bei einem Ausfall eines Kanals in diesem 2oo2-System, im Gegensatz zu einem 1oo2-System, der andere Kanal noch verfügbar ist und während der ausgefallene Kanal repariert wird, kann der zweite verfügbare Kanal ausfallen. Das System ist nicht mehr verfügbar, wenn beide Kanäle gefährlich

erkannt oder sicher ausfallen. Die Berechnung des STR-Werts der 2oo2-Architektur wird durch die folgenden Schritte ausgeführt:

- Spurious-Trip aufgrund von sicheren Fehler: jeder unabhängige sichere Fehler kann zu einem Spurious-Trip Fehler mit der Rate $(1-\beta_S)\cdot\lambda_S$ führen. Da 2oo2-Architektur 2 unabhängige Kanäle hat, hat der erste Spurious-Trip Fehler eine Rate von $2\cdot(1-\beta_S)\cdot\lambda_S$. Der fehlerhafte Kanal wird in den Reparatur-Zustand gebracht. Die Wahrscheinlichkeit, dass einer Kanal aufgrund Spurious-Trip ausfällt und in der Reparatur ist, beträgt

$$p_S = 1 - e^{-(1-\beta_S)\cdot\lambda_S\cdot MTTR} \approx (1-\beta_S)\cdot\lambda_S\cdot MTTR \tag{4.21}$$

  Während der Reparatur des ersten ausgefallenen Kanals kann der andere Kanal aufgrund einen sicheren Fehlers mit einer Wahrscheinlichkeit $p(N_S \geq 1)$ zu einem Spurious-Trip Ausfall führen, wobei N_S die Anzahl des Spurious-Trip Fehlers ist aufgrund des sicheren Fehlers in der Reparaturzeit des ersten Kanals. Daher ist dieser Fehler binomial verteilt. Die Spurious-Trip Rate wird aufgrund eines sicheren Fehlers nach der folgenden Gleichung bestimmt:

$$\begin{aligned} STR_{2oo2\_S} &= 2\cdot(1-\beta_S)\cdot\lambda_S\cdot p(N_S\geq 1) \\ &= 2\cdot(1-\beta_S)\cdot\lambda_S\cdot\sum_{m=1}^{1}\binom{1}{m}\cdot(p_S)^m\cdot(1-p_S)^{1-m} \\ &\approx 2\cdot(1-\beta_S)\cdot\lambda_S\cdot p_S \\ &= 2\cdot(1-\beta_S)\cdot\lambda_S\cdot(1-\beta_S)\cdot\lambda_S\cdot MTTR \\ &= 2\cdot[(1-\beta_S)\cdot\lambda_S]^2\cdot MTTR \end{aligned} \tag{4.22}$$

- Spurious-Trip aufgrund von gefährlich erkannten Fehler: der erste Fehler einer 2oo2-Architektur fällt mit einer Rate von $2\cdot(1-\beta_D)\cdot\lambda_{DD}$ aus und wird in den Reparatur-Zustand gebracht. Die Wahrscheinlichkeit, dass einer Kanal aufgrund Spurious-Trip ausfällt und in der Reparatur ist, beträgt

$$p_{DD} = 1 - e^{-(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR} \approx (1-\beta_D)\cdot\lambda_{DD}\cdot MTTR \tag{4.23}$$

  Während der Reparatur des ersten ausgefallenen Kanals kann der andere Kanal aufgrund eines gefährlich erkannten Fehlers mit einer Wahrscheinlichkeit $p(N_{DD}\geq 0)$ zu einem Spurious-Trip Ausfall führen, wobei N_{DD} die Anzahl des Spurious-Trip Fehlers ist aufgrund des gefährlich erkannten Fehlers in der Reparaturzeit des ersten Kanals. Dieser Fehler ist binomial verteilt. Die Spurious-Trip Rate wird aufgrund des gefährlich erkannten Fehlers nach der folgenden Gleichung bestimmt:

$$
\begin{aligned}
STR_{2oo2\_DD} &= 2 \cdot (1-\beta_D) \cdot \lambda_{DD} \cdot p(N_{DD} \geq 0) \\
&= 2 \cdot (1-\beta_D) \cdot \lambda_{DD} \cdot \sum_{m=0}^{1} \binom{1}{0} \cdot (p_{DD})^m \cdot (1-p_{DD})^{1-m} \\
&= 2 \cdot (1-\beta_D) \cdot \lambda_{DD} \cdot \binom{1}{1} \cdot (p_{DD})^1 \cdot (1-p_{DD})^{1-m} \\
&\approx 2 \cdot (1-\beta_D) \cdot \lambda_{DD} \cdot p_{DD} \\
&= 2 \cdot [(1-\beta_D) \cdot \lambda_{DD}]^2 \cdot MTTR
\end{aligned}
\tag{4.24}
$$

- Spurious-Trip Fehler infolge gemeinsamer Ursache mit der Rate:

$$
STR_{2oo2\_CCF} = \beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD} \tag{4.25}
$$

- Spurious-Trip aufgrund nicht echter Anforderung mit der Rate:

$$
STR_{2oo2\_FD} = \gamma \cdot \lambda_{DE} \tag{4.26}
$$

Durch Ersetzen von (4.22), (4.24), (4.25) und (4.26) in die Gleichung (3.4) ergibt sich die Gleichung (4.27) für die Bestimmung des STR_{2oo2}-Werts der 2oo2-Architektur:

$$
\begin{aligned}
STR_{2oo2} &= STR_{2oo2\_S} + STR_{2oo2\_DD} + STR_{2oo2\_CCF} + STR_{2oo2\_FD} \\
&= 2 \cdot [(1-\beta_S) \cdot \lambda_S]^2 \cdot MTTR + \beta_S \cdot \lambda_S \\
&\quad 2 \cdot [(1-\beta_D) \cdot \lambda_{DD}]^2 \cdot MTTR + \beta_D \cdot \lambda_{DD} + \gamma \cdot \lambda_{DE}
\end{aligned}
\tag{4.27}
$$

Der $PFS_{avg\_2oo2\_S}$-Wert wird dann durch folgende Gleichung berechnet:

$$
\begin{aligned}
PFS_{avg\_2oo2\_S} &= \frac{1}{T} \cdot \int_0^T PFS_{2oo2\_S}(t) \cdot dt \\
&= \frac{1}{T} \cdot \int_0^T \left(1 - R_{Spurious\_2oo2\_S}\right) \cdot dt
\end{aligned}
\tag{4.28}
$$

mit:

$$
\begin{aligned}
R_{Spurious\_2oo2\_S} &= \sum_{i=0}^{0} \binom{2}{i} R_{Spurious\_S}^{2-i} \cdot (1-R_{Spurious\_S})^i \\
&= R_{Spurious\_S}^2 \\
&= e^{-2 \cdot STR_{2oo2\_S} \cdot t}
\end{aligned}
\tag{4.29}
$$

Nach der MacLaurin'sche Reihe-Entwicklung:

$$
e^{-2 \cdot a \cdot T} = 1 - 2 \cdot a \cdot T + \frac{[2 \cdot a]^2 \cdot T^2}{2!} - \frac{[2 \cdot a]^3 \cdot T^3}{3!} + R_4 \tag{4.30}
$$

mit:

$$R_4 \approx 0 \tag{4.31}$$

Durch Ersetzen von (4.29), (4.30) und (4.31) in die (4.28) ergibt sich:

$$\begin{aligned} \Rightarrow PFS_{avg\_2oo2\_S} &= 1 - \frac{1}{T} \cdot \left[\frac{e^{-2 \cdot STR_{2oo2\_S} \cdot t} - 1}{-2 \cdot STR_{2oo2\_S}} \right]_0^T \\ &= STR_{2oo2\_S} \cdot T - \frac{4 \cdot (STR_{2oo2\_S} \cdot T)^2}{3} \end{aligned} \tag{4.32}$$

Die $PFS_{avg\_2oo2\_DD}$-Berechnung wird analog wie bei der $PFS_{avg\_2oo2\_S}$-Berechnung durchgeführt. Daraus folgt die Formel für $PFS_{avg\_2oo2\_DD}$-Berechnung:

$$PFS_{avg\_2oo2\_DD} = STR_{2oo2\_DD} \cdot T - \frac{4 \cdot (STR_{2oo2\_DD} \cdot T)^2}{3} \tag{4.33}$$

Aus der Gleichung (4.3), (4.17), (4.32) und (4.33) ergibt sich die Formel für die PFS_{avg_2oo2}-Berechnung wie folgt:

$$\begin{aligned} PFS_{avg\_2oo2} &= PFS_{avg\_2oo2\_S} + PFS_{avg\_2oo2\_DD} + PFS_{avg\_CCF} + PFS_{avg\_FD} \\ &= STR_{2oo2\_S} \cdot T - \frac{4 \cdot (STR_{2oo2\_S} \cdot T)^2}{3} \\ &+ STR_{2oo2\_DD} \cdot T - \frac{4 \cdot (STR_{2oo2\_DD} \cdot T)^2}{3} \\ &+ (\beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD}) \cdot MTTR + \gamma \cdot \lambda_{DE} \cdot \tau_{DE} \end{aligned} \tag{4.34}$$

Anhand der Gleichung (4.9) wird die Zuverlässigkeit $R_{Spurious\_2oo2}$ für eine 2oo2-Architektur wie folgt bestimmt:

$$\begin{aligned} R_{Spurious\_2oo2} &= \sum_{i=0}^{0} \binom{2}{i} R_{Spurious}^{2-i} \cdot (1 - R_{Spurious})^i \\ &= R_{Spurious}^2 \\ &= e^{-2 \cdot STR_{2oo2} \cdot t} \end{aligned} \tag{4.35}$$

Gemäß der Gleichung (3.12) lässt sich der $MTTF_{Spurious\_2oo2}$-Wert der 2oo2-Architekur wie folgt bestimmen:

$$MTTF_{Spurious\_2oo2} = \int_0^\infty R_{Spurious\_2oo2}(t) \cdot dt$$
$$= \int_0^\infty \left[e^{-2 \cdot STR_{2oo2} \cdot t} \right] \cdot dt \qquad (4.36)$$
$$= \left[\frac{e^{-2 \cdot STR_{2oo2} \cdot t}}{-2 \cdot STR_{2oo2}} \right]_0^\infty = \frac{1}{2 \cdot STR_{2oo2}}$$

4.4 2oo3-Architektur

Die 2oo3-Architektur besteht aus drei redundanten Kanälen. Wird dieses 2oo3-System als Sicherheitssystem eingesetzt, bedeutet dies, dass 2 von den 3 Kanälen korrekt, d. h. fehlerfrei, arbeiten müssen, damit das System im Anforderungsfall sicher abschaltet. Somit wird gewährleistet, dass – auch wenn ein Kanal mit einem gefährlich erkannten Fehler behaftet ist – das Sicherheitssystem korrekt (im Sinne einer 2oo3-Architektur) funktioniert. Das heißt, das 2oo3-System ist 1-fehlertolerant, oder auch, das 2oo3-System besitzt eine Hardwarefehlertoleranz von 1. Ist das 2oo3-System in einem Kanal mit einem gefährlichen nicht erkannten Fehler behaftet, so erkennt der 2oo3-Mehrheitsentscheider den gefährlichen fehlerhaften Kanal natürlich nicht. Trotzdem ist im Anforderungsfall der sichere Zustand auf Grund der 2oo3-Architektur gewährleistet. In der Abbildung 4.9 wäre beispielhaft der rot gezeichnete Kanal gefährlich nicht erkannt ausgefallen. Trotzdem ist der sichere Zustand gewährleistet: mindestens einer der beiden angesteuerten Schalter in jedem der drei Schaltkreise muss öffnen, damit der Ausgangszustand energielos ist. Liegt ein sicherer erkannter oder nicht erkannter Fehler vor, so hat dieser Fehler keinen Einfluss auf die Sicherheitsfunktion. Die Sicherheitsfunktion – energieloser Ausgangszustand – ist immer gewährleistet. Gleiches gilt, wenn 2 sichere oder gar 3 sichere Fehler (d. h. in jedem Kanal einer) vorliegen: die Sicherheitsfunktion ist immer gewährleistet.

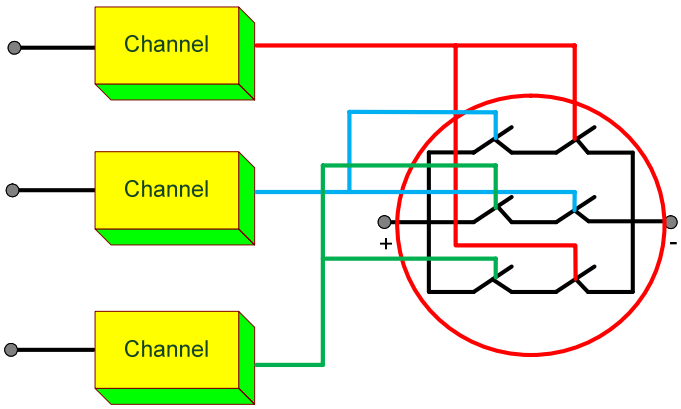

Abbildung 4.9: Blockdiagramm der 2oo3-Architektur

Wenn 2 Kanäle mit jeweils einem gefährlichen Fehler ausfallen, ist das 2oo3-System im Anforderungsfall nicht mehr sicher. Die einzige Möglichkeit einen sicheren Zustand zu erzwingen, besteht darin, dass, bevor ein Anforderungsfall eintritt, eine externe Diagnose erkennt, dass 2 gefährlich erkannte Fehler innerhalb des 2oo3-Systems aufgetreten sind, und eine übergeordnete Logik – beispielsweise ein Watch-Dog – eine Abschaltung, d. h. einen energielosen Zustand für das 2oo3-System erzwingt.

Eine Verbesserung der Situation – 2 gefährliche erkannte Fehler treten kurz hintereinander auf und ein Anforderungsfall ist nicht gegeben – ergibt sich, wenn ein Degradierungsmechanismus für das 2oo3-System vorliegt. Dann kann das 2oo3-System in ein 1oo2-System degradiert werden. Für das Beispiel, das in der Abbildung 4.9 dargestellt ist, bedeutet dies, unter der Annahme, dass ein gefährlich erkannter Fehler im rot gezeichneten Kanal aufgetreten ist, dass die beiden Schaltkreise, in denen der rot eingezeichnete Kanal einen Schalter ansteuert, stillgelegt werden. Der grüne und der blaue Kanal steuern nur noch den mittleren Kanal, der alleine die Sicherheitsfunktion darstellt. Liegt ein gefährlicher nicht erkannter oder liegen zwei gefährliche nicht erkannte Fehler vor, so ist eine Degradierung nicht möglich!

Der Vorteil der Degradierung liegt in einer höheren Sicherheit eines degradierbaren 2oo3-Sicherheitssystems begründet. Wie oben erläutert tritt bei Auftreten von zwei gefährlich erkannten Fehlern und einem anschließenden Anforderungsfall ein gefährlicher Zustand ein. Das 2oo3-System ohne Degradierungsmechanismus kann nicht mehr entscheiden, ob die zwei fehlerbehafteten Kanäle (die trotz Fehler ein gleichartiges Signal aufweisen) korrekt arbeiten oder der eigentlich korrekt arbeitende Kanal scheinbar fehlerhaft ist. Eine Degradierung bedeutet hingegen, dass nach einem Auftreten eines ersten gefährlich erkannten Fehlers, das 2oo3-System in ein 1oo2-System degradiert wird. Dieses 1oo2-System hat auf Grund seiner impliziten Sicherheitsarchitektur die Eigenschaft bei Auftreten eines jetzt auftretenden gefährlich erkannten Fehlers einen sicheren Zustand einnehmen zu können. In der dargestellten Abbildung 4.9 bedeutet dies, egal welcher der beiden Kanäle fehlerhaft ist, der andere Kanal öffnet den Schalter und erzwingt einen sicheren Zustand.

Wie sieht das Ganze bei Auftreten von sicheren Fehlern aus? Auch hier gilt wieder: Sichere Fehler haben – per Definition – keinen Einfluss auf die Sicherheitsfunktion.

Ein wichtiges Kriterium eines Sicherheitssystems für einen Anlagenbetreiber ist die Verfügbarkeit eines Systems. Aus Anlagenbetreibersicht gilt es hier sowohl die Verfügbarkeit der Sicherheitsfunktion auf der Grundlage der gefährlichen nicht erkannten Fehler als auch die Verfügbarkeit auf der Grundlage sowohl der sicheren als auch der gefährlichen erkannten Fehler zu betrachten. Ein Anlagenbetreiber achtet in der Regel darauf, dass auch die sicheren Fehler zu gegebener Zeit repariert werden, um nicht beispielsweise Gefahr zu laufen, dass aus zwei oder mehreren sicheren Fehlern ein gefährlicher Fehler entsteht. Die letztgenannte Verfügbarkeit wird mit Hilfe der Spurious-Trip Rate berechnet. Diese Rate ist eine Funktion der sicheren und der gefährlich erkannten Fehlerrate. Folgende Fälle können definiert werden, bei denen ein System auf Grund eines Spurious-Trips ausfällt:

- ein sicherer Fehler bei einem Kanal ist schon aufgetreten und der Kanal ist in der Reparatur. Nun wird die Architektur auf eine 1oo2-Architektur degradiert und verhält sich weiter wie eine 1oo2-Architektur in Betriebsart mit niedriger Anforderungsrate.
- ein sicherer Fehler oder erkannter gefährlicher Fehler bei allen Kanälen (CCF) im SIS ist aufgetreten
- eine nicht echte Anforderung wird auf Auslösung der Sicherheitsfunktion gefordert.

Das Verhalten von EUC und SIS werden in der Abbildung 4.10 und Abbildung 4.11 dargestellt:

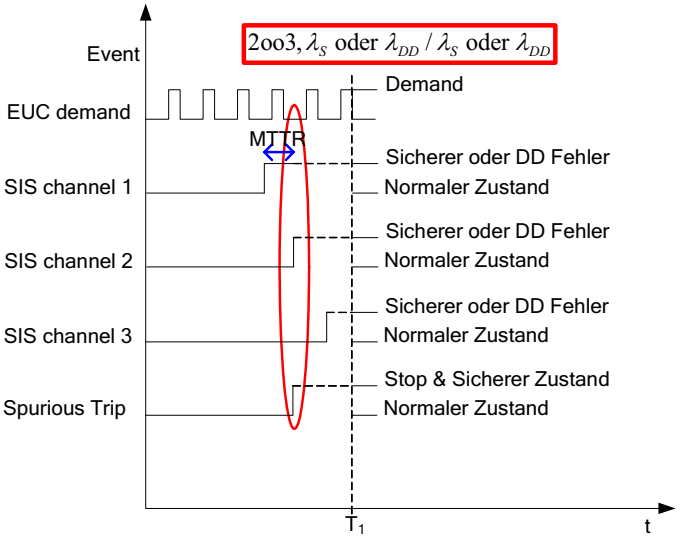

Abbildung 4.10: EUC und SIS mit 2oo3-Architektur (zufällige Fehler)

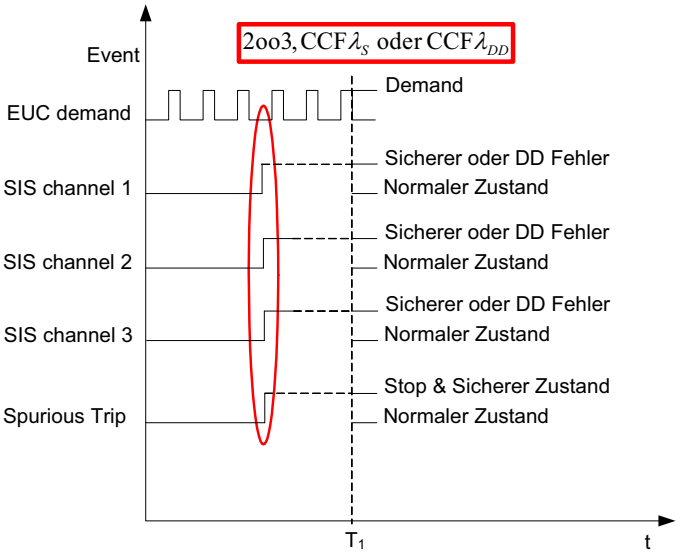

Abbildung 4.11: EUC und SIS mit 2oo3-Architektur (CCF)

Die Berechnung des STR-Werts der 2oo3-Architektur wird durch die folgenden Schritte ausgeführt:

- Spurious-Trip aufgrund von sicheren Fehler: jeder unabhängige sichere Fehler kann zu einem Spurious-Trip Fehler mit der Rate $(1-\beta_S)\cdot\lambda_S$ führen. Da 2oo3-Architektur 3 unabhängige Kanäle hat, hat der erste Spurious-Trip Fehler eine Rate von $3\cdot(1-\beta_S)\cdot\lambda_S$. Der fehlerhafte Kanal wird in den Reparatur-Zustand gebracht. Die Wahrscheinlichkeit, dass ein Kanal aufgrund Spurious-Trip ausfällt und in der Reparatur ist, beträgt

$$p_S = 1 - e^{-(1-\beta_S)\cdot\lambda_S\cdot MTTR} \approx (1-\beta_S)\cdot\lambda_S\cdot MTTR \qquad \textbf{(4.37)}$$

  Während der Reparatur des ersten ausgefallenen Kanals können die anderen Kanäle aufgrund des sicheren Fehlers mit einer Wahrscheinlichkeit $p(N_S \geq 1)$ zu einem Spurious-Trip Ausfall führen, wobei N_S die Anzahl des Spurious-Trip Fehlers ist aufgrund des sicheren Fehlers in der Reparaturzeit des ersten Kanals. Daher ist dieser Fehler binomial verteilt. Die Spurious-Trip Rate wird aufgrund sicheren Fehlern nach der folgenden Gleichung bestimmt:

$$
\begin{aligned}
STR_{2oo3\_S} &= 3\cdot(1-\beta_S)\cdot\lambda_S\cdot p(N_S\geq 1)\\
&= 3\cdot(1-\beta_S)\cdot\lambda_S\cdot\sum_{m=1}^{2}\binom{2}{m}\cdot(p_S)^m\cdot(1-p_S)^{2-m}\\
&= 3\cdot(1-\beta_D)\cdot\lambda_S\cdot\left[\binom{2}{1}(p_S)\cdot(1-p_S)+\binom{2}{2}(p_S)^2\cdot(1-p_S)^0\right]\\
&= 3\cdot(1-\beta_S)\cdot\lambda_S\cdot[2\cdot p_S\cdot(1-p_S)+(p_S)^2]\\
&= 3\cdot(1-\beta_S)\cdot\lambda_S\cdot[2\cdot p_S-{p_S}^2]\\
&\approx 3\cdot(1-\beta_S)\cdot\lambda_S\cdot 2\cdot[(1-\beta_S)\cdot\lambda_S]\cdot MTTR\\
&= 6\cdot[(1-\beta_S)\cdot\lambda_S]^2\cdot MTTR
\end{aligned}
\tag{4.38}
$$

- Spurious-Trip aufgrund von gefährlich erkannten Fehler: der erste Fehler einer 2oo3-Architektur fällt mit einer Rate von $3\cdot(1-\beta_D)\cdot\lambda_{DD}$ aus und wird in den Reparatur-Zustand gebracht. Die Wahrscheinlichkeit, dass ein Kanal aufgrund Spurious-Trip ausfällt und in der Reparatur ist, beträgt

$$
p_{DD} = 1-e^{-(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR}\approx(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR \tag{4.39}
$$

Während der Reparatur des ersten ausgefallenen Kanals können die anderen Kanäle aufgrund eines gefährlich erkannten Fehlers mit einer Wahrscheinlichkeit $p(N_{DD}\geq 1)$ zu einem Spurious-Trip Ausfall führen, wobei N_{DD} die Anzahl des Spurious-Trip Fehlers ist aufgrund des gefährlich erkannten Fehlers in der Reparaturzeit des ersten Kanals. Dieser Fehler ist binomial verteilt. Die Spurious-Trip Rate wird aufgrund gefährlich erkannten Fehlers nach der folgenden Gleichung bestimmt:

$$
\begin{aligned}
STR_{2oo3\_DD} &= 3\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot p(N_{DD}\geq 1)\\
&= 3\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot\sum_{m=1}^{2}\binom{2}{1}\cdot(p_{DD})^m\cdot(1-p_{DD})^{2-m}\\
&= 3\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot\left[\binom{2}{1}\cdot p_{DD}\cdot(1-p_{DD})+\binom{2}{2}\cdot(p_{DD})^2\cdot(1-p_{DD})^0\right]\\
&= 3\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot\left[2\cdot(p_{DD})\cdot(1-p_{DD})+(p_{DD})^2\right]\\
&= 6\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot\left[p_{DD}-(p_{DD})^2\right]\\
&\approx 6\cdot\left[(1-\beta_D)\cdot\lambda_{DD}\right]^2\cdot MTTR
\end{aligned}
\tag{4.40}
$$

- Spurious-Trip aufgrund Fehler infolge gemeinsamer Ursache mit der Rate:

$$
STR_{2oo3\_CCF} = \beta_S\cdot\lambda_S+\beta_D\cdot\lambda_{DD} \tag{4.41}
$$

- Spurious-Trip aufgrund nicht echter Anforderung mit der Rate:

$$STR_{2oo3\_FD} = \gamma \cdot \lambda_{DE} \tag{4.42}$$

Durch Ersetzen von (4.38), (4.40), (4.41) und (4.42) in die Gleichung (3.4) ergibt sich die Gleichung (4.43) für die Bestimmung des STR_{2oo3}-Werts der 2oo3-Architektur:

$$\begin{aligned} STR_{2oo3} &= STR_{2oo3\_S} + STR_{2oo3\_DD} + STR_{2oo3\_CCF} + STR_{2oo3\_FD} \\ &= 6 \cdot [(1-\beta_S) \cdot \lambda_S]^2 \cdot MTTR \\ &+ 6 \cdot [(1-\beta_D) \cdot \lambda_{DD}]^2 \cdot MTTR + \beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD} + \gamma \cdot \lambda_{DE} \end{aligned} \tag{4.43}$$

Anhand der Gleichung (3.11) wird $PFS_{avg\_2oo3\_S}$ berechnet:

$$\begin{aligned} PFS_{avg\_2oo3\_S} &= \frac{1}{T} \cdot \int_0^T P_{Spurious\_2oo3\_S}(t) \cdot dt \\ &= \frac{1}{T} \cdot \int_0^T \left(1 - R_{Spurious\_2oo3\_S}\right) \cdot dt \end{aligned} \tag{4.44}$$

mit:

$$\begin{aligned} R_{Spurious\_2oo3\_S} &= \sum_{i=0}^{1} \binom{3}{i} R_{Spurious\_2oo3\_S}^{3-i} \cdot (1 - R_{Spurious\_2oo3\_S})^i \\ &= 3 \cdot R_{Spurious\_2oo3\_S}^2 - 2 \cdot R_{Spurious\_2oo3\_S}^3 \\ &= 3 \cdot e^{-2 \cdot STR_{2oo3\_S} \cdot t} - 2 \cdot e^{-3 \cdot STR_{2oo3\_S} \cdot t} \end{aligned} \tag{4.45}$$

Nach der MacLaurin'schen Reihen-Entwicklung:

$$e^{-2 \cdot a \cdot T} = 1 - 2 \cdot a \cdot T + \frac{[2 \cdot a]^2 \cdot T^2}{2!} - \frac{[2 \cdot a]^3 \cdot T^3}{3!} + R_4 \tag{4.46}$$

und:

$$e^{-3 \cdot a \cdot T} = 1 - 3 \cdot a \cdot T + \frac{[3 \cdot a]^2 \cdot T^2}{2!} - \frac{[3 \cdot a]^3 \cdot T^3}{3!} + R_4 \tag{4.47}$$

mit:

$$R_4 \approx 0 \tag{4.48}$$

Durch Einsetzen von Gleichung (4.43), (4.45), (4.46), (4.47) und (4.48) in die Gleichung (4.44) ergibt sich dann:

$$
\begin{aligned}
\Rightarrow PFS_{avg\_2oo3\_S} &= \frac{1}{T}\cdot\int_0^T\left(1-R_{Spurious\_2oo3\_S}\right)\cdot dt \\
&1-\frac{1}{T}\cdot\left[\frac{3\cdot e^{-2\cdot STR_{2oo3\_S}\cdot t}}{-2\cdot STR_{2oo3\_S}}+\frac{2\cdot e^{-3\cdot STR_{2oo3\_S}\cdot t}}{-3\cdot STR_{2oo3\_S}}\right]_0^T \\
&=1+\frac{3}{T}\cdot\frac{e^{-2\cdot STR_{2oo3\_S}\cdot t}-1}{2\cdot STR_{2oo3\_S}}-\frac{2}{T}\cdot\frac{e^{-3\cdot STR_{2oo3\_S}\cdot t}-1}{3\cdot STR_{2oo3\_S}} \\
&=1+\frac{3}{T\cdot 2\cdot STR_{2oo3\_S}}\cdot[1-2\cdot STR_{2oo3\_S}\cdot T \\
&+\frac{\left[2\cdot STR_{2oo3\_S}\right]^2\cdot T^2}{2!}-\frac{\left[2\cdot STR_{2oo3\_S}\right]^3\cdot T^3}{3!}-1] \\
&-\frac{2}{T\cdot 3\cdot STR_{2oo3\_S}}\cdot[1-3\cdot STR_{2oo3\_S}\cdot T \\
&+\frac{\left[3\cdot STR_{2oo3\_S}\right]^2\cdot T^2}{2!}-\frac{\left[3\cdot STR_{2oo3\_S}\right]^3\cdot T^3}{3!}-1] \\
&=(STR_{2oo3\_S}\cdot T)^2
\end{aligned}
\qquad \textbf{(4.49)}
$$

Der $PFS_{avg\_2oo3\_DD}$-Wert wird ähnlich wie der $PFS_{avg\_2oo3\_S}$-Wert berechnet und wird nach folgender Gleichung bestimmt:

$$PFS_{avg\_2oo3\_DD} = (STR_{2oo3\_DD}\cdot T)^2 \qquad \textbf{(4.50)}$$

Aus der Gleichung (4.3), (4.17), (4.49) und (4.50) wird der PFS_{avg_2oo3}-Wert gemäß der Gleichung (4.51) bestimmt:

$$
\begin{aligned}
PFS_{avg\_2oo3} &= PFS_{avg\_2oo3\_S}+PFS_{avg\_2oo3\_DD}+PFS_{avg\_CCF}+PFS_{avg\_FD} \\
&=(STR_{2oo3\_S}\cdot T)^2+(STR_{2oo3\_DD}\cdot T)^2 \\
&+(\beta_S\cdot\lambda_S+\beta_D\cdot\lambda_{DD})\cdot MTTR+\gamma\cdot\lambda_{DE}\cdot\tau_{DE}
\end{aligned}
\qquad \textbf{(4.51)}
$$

Anhand der Gleichung (4.9) wird die Zuverlässigkeit $R_{Spurious\_2oo3}$ für eine 2oo3-Architektur wie folgt bestimmt:

$$
\begin{aligned}
R_{Spurious\_2oo3} &= \sum_{i=0}^{1}\binom{3}{i}R_{Spurious\_2oo3}^{3-i}\cdot(1-R_{Spurious\_2oo3})^i \\
&=3\cdot R_{Spurious\_2oo3}^2-2\cdot R_{Spurious\_2oo3}^3 \\
&=3\cdot e^{-2\cdot STR_{2oo3}\cdot t}-2\cdot e^{-3\cdot STR_{2oo3}\cdot t}
\end{aligned}
\qquad \textbf{(4.52)}
$$

Der $MTTF_{Spurious\_2oo3}$-Wert der 2oo3-Architekur wird anhand der Gleichung (3.12) bestimmt:

$$
\begin{aligned}
MTTF_{Spurious\_2oo3} &= \int_0^\infty R_{Spurious\_2oo3}(t) \cdot dt \\
&= \int_0^\infty \left[3 \cdot e^{-2 \cdot STR_{2oo3} \cdot t}\right] \cdot dt - \int_0^\infty \left[2 \cdot e^{-3 \cdot STR_{2oo3} \cdot t}\right] \cdot dt \\
&= \left[\frac{3 \cdot e^{-2 \cdot STR_{2oo3} \cdot t}}{-2 \cdot STR_{2oo3}}\right]_0^\infty - \left[\frac{2 \cdot e^{-3 \cdot STR_{2oo3} \cdot t}}{-3 \cdot STR_{2oo3}}\right]_0^\infty \\
&= \frac{5}{6 \cdot STR_{2oo3}}
\end{aligned}
\tag{4.53}
$$

4.5 1oon-Architektur

In diesem Abschnitt werden die Berechnungen von STR, PFS_{avg} und $MTTF_{Spurious}$ der 1oon-Architektur hergeleitet. Eine 1oon-Architektur besitzt n voneinander unabhängige Kanäle und wird wie in der Abbildung 4.12 geschaltet.

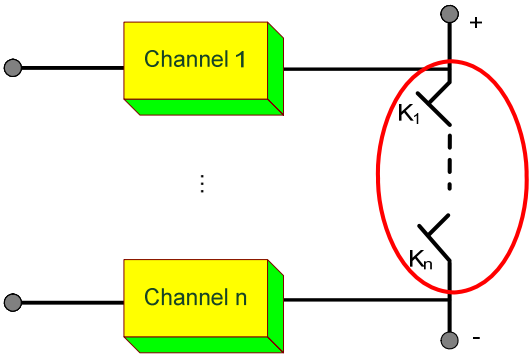

Abbildung 4.12: Blockdiagramm der 1oon-Architektur

Bei dieser 1oon-Architektur muss ein gefährlicher Ausfall in n Kanälen vorliegen, bevor die Sicherheitsfunktion bei Anforderung ausfallen würde. Ein Spurious-Trip Ausfall würde dann im Gesamtsystem entstehen, wenn eine nicht echte Anforderung auf Auslösung der Sicherheitsfunktion gefordert wird oder ein zufälliger sicherer oder gefährlich erkannter Fehler oder ein CCF auftritt. Die Berechnung des STR-Werts der 1oon-Architektur wird durch die folgenden Schritte ausgeführt:

- Spurious-Trip aufgrund von sicheren Fehler: jeder unabhängige sichere Fehler kann zu einem Spurious-Trip Fehler mit der Rate $(1-\beta_S) \cdot \lambda_S$ führen. Da die 1oon-Architektur n unabhängige Kanäle hat, hat der erste Spurious-Trip Fehler eine Rate von $n \cdot (1-\beta_S) \cdot \lambda_S$. Der fehlerhafte Kanal wird bei dieser Architektur nicht in den Repara-

tur-Zustand gebracht. Die Spurious-Trip Rate wird aufgrund eines sicheren Fehlers mittels den Gleichungen (3.1), (3.2) und (3.3) nach der folgenden Gleichung bestimmt:

$$STR_{1oon\_S} = n \cdot (1 - \beta_S) \cdot \lambda_S \tag{4.54}$$

Spurious-Trip aufgrund von gefährlich erkannten Fehler: der erste Fehler einer 1*oon*-Architektur fällt mit einer Rate von $n \cdot (1 - \beta_D) \cdot \lambda_{DD}$ aus und wird in den Reparatur-Zustand gebracht. Die Spurious-Trip Rate wird aufgrund eines gefährlich erkannten Fehlers mittels den Gleichungen (3.1), (3.2) und (3.3) nach der folgenden Gleichung bestimmt:

$$STR_{1oon\_DD} = n \cdot (1 - \beta_D) \cdot \lambda_{DD} \tag{4.55}$$

- Spurious-Trip aufgrund Fehler infolge gemeinsamer Ursache mit der Rate:

$$STR_{1oon\_CCF} = \beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD} \tag{4.56}$$

- Spurious-Trip aufgrund nicht echter Anforderung mit der Rate:

$$STR_{1oon\_FD} = \gamma \cdot \lambda_{DE} \tag{4.57}$$

Durch Ersetzen von (4.54), (4.55), (4.56) und (4.57) in die Gleichung (3.4) ergibt sich die Gleichung (4.58) für die Bestimmung des STR_{1oon}-Werts der 1*oon*-Architektur

$$\begin{aligned} STR_{1oon} &= STR_{1oon\_S} + STR_{1oon\_DD} + STR_{1oon\_CCF} + STR_{1oon\_FD} \\ &= n \cdot (1 - \beta_S) \cdot \lambda_S \\ &+ n \cdot (1 - \beta_D) \cdot \lambda_{DD} + \beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD} + \gamma \cdot \lambda_{DE} \end{aligned} \tag{4.58}$$

Eine allgemeine Formel für die $PFS_{avg\_1oon\_S}$-Bestimmung eines Sicherheitssystems mit 1*oon*-Architektur wird dargestellt als:

$$\begin{aligned} PFS_{avg\_1oon\_S} &= \frac{1}{T}\int_0^T P_{Spurious\_1oon\_S}(t) \cdot dt \\ &= \frac{1}{T}\int_0^T (1 - R_{Spurious\_1oon\_S}(t)) \cdot dt \end{aligned} \tag{4.59}$$

wobei der $R_{Spurious\_1oon\_S}$-Wert anhand der Gleichung (4.9) gegeben wird als:

$$
\begin{aligned}
R_{Spurious\_1oon\_S} &= \sum_{i=1}^{n}\binom{n}{i}\cdot R_{Spurious\_S}^{i}\cdot(1-R_{Spurious\_S})^{n-i} \\
&= \sum_{i=0}^{n-1}\binom{n}{i}\cdot R_{Spurious\_S}^{n-i}\cdot(1-R_{Spurious\_S})^{i} \\
&= R_{Spurious\_S}^{n} \\
&+ n\cdot R_{Spurious\_S}^{n-1}\cdot(1-R_{Spurious\_S}) \\
&+ .... \\
&+ \binom{n}{i}\cdot R_{Spurious\_S}^{n-i}(1-R_{Spurious\_S})^{i} \\
&+ ... \\
&+ n\cdot R_{Spurious\_S}\cdot(1-R_{Spurious\_S})^{n-1}
\end{aligned}
\tag{4.60}
$$

Ähnlich wie die $PFS_{avg\_1oon\_S}$-Bestimmung wird der $PFS_{avg\_1oon\_DD}$-Wert wie folgt bestimmt:

$$
PFS_{avg\_1oon\_DD} = \frac{1}{T}\int_{0}^{T}(1-R_{Spurious\_1oon\_DD}(t))\cdot dt \tag{4.61}
$$

wobei der $R_{Spurious\_1oon\_DD}$-Wert anhand der Gleichung (4.9) gegeben wird als:

$$
\begin{aligned}
R_{Spurious\_1oon\_DD} &= R_{Spurious\_DD}^{n} \\
&+ n\cdot R_{Spurious\_DD}^{n-1}\cdot(1-R_{Spurious\_DD}) \\
&+ .... \\
&+ \binom{n}{i}\cdot R_{Spurious\_DD}^{n-i}(1-R_{Spurious\_DD})^{i} \\
&+ ... \\
&+ n\cdot R_{Spurious\_DD}\cdot(1-R_{Spurious\_DD})^{n-1}
\end{aligned}
\tag{4.62}
$$

Der PFS_{avg_1oon}-Wert wird nach folgender Gleichung gerechnet:

$$
\begin{aligned}
PFS_{avg\_1oon} &= PFS_{avg\_1oon\_S} + PFS_{avg\_1oon\_DD} + PFS_{avg\_CCF} + PFS_{avg\_FD} \\
&= \frac{1}{T}\int_{0}^{T}(1-R_{Spurious\_1oon\_S}(t))\cdot dt \\
&+ \frac{1}{T}\int_{0}^{T}(1-R_{Spurious\_1oon\_DD}(t))\cdot dt \\
&+ (\beta_S\cdot\lambda_S + \beta_D\cdot\lambda_{DD})\cdot MTTR + \gamma\cdot\lambda_{DE}\cdot\tau_{DE}
\end{aligned}
\tag{4.63}
$$

Anhand der Gleichung (4.9) wird die Zuverlässigkeit $R_{Spurious\_1oon}$ für eine 1oon-Architektur wie folgt bestimmt:

$$
\begin{aligned}
R_{Spurious\_1oon} &= \sum_{i=1}^{n} \binom{n}{i} \cdot R_{Spurious}^{i} \cdot (1 - R_{Spurious})^{n-i} \\
&= \sum_{i=0}^{n-1} \binom{n}{i} \cdot R_{Spurious}^{n-i} \cdot (1 - R_{Spurious})^{i} \\
&= R_{Spurious}^{n} \\
&+ n \cdot R_{Spurious}^{n-1} \cdot (1 - R_{Spurious}) \\
&+ .... \\
&+ \binom{n}{i} \cdot R_{Spurious}^{n-i} (1 - R_{Spurious})^{i} \\
&+ ... \\
&+ n \cdot R_{Spurious} \cdot (1 - R_{Spurious})^{n-1}
\end{aligned}
\tag{4.64}
$$

Der $MTTF_{Spurious\_1oon}$-Wert wird wie folgt gerechnet:

$$
\begin{aligned}
MTTF_{Spurious\_1oon} &= \int_0^{\infty} R_{Spurious\_1oon}(t) \cdot dt \\
&= \int_0^{\infty} \left[\sum_{i=0}^{n-1} \binom{n}{i} \cdot R_{Spurious}^{n-i} \cdot (1 - R_{Spurious})^{i} \right] \cdot dt \\
&= \int_0^{\infty} R_{Spurious}^{n} \cdot dt \\
&+ \int_0^{\infty} n \cdot R_{Spurious}^{n-1} \cdot (1 - R_{Spurious}) \cdot dt \\
&+ .... \\
&+ \int_0^{\infty} \binom{n}{i} \cdot R_{Spurious}^{n-i} (1 - R_{Spurious})^{i} \cdot dt \\
&+ ... \\
&+ \int_0^{\infty} n \cdot R_{Spurious} \cdot (1 - R_{Spurious})^{n-1} \cdot dt
\end{aligned}
\tag{4.65}
$$

mit:

$$
R_{Spurious} = e^{-STR_{1oon} \cdot t} \tag{4.66}
$$

daraus folgt:

$$
\begin{aligned}
R_{Spurious\_1oon} &= e^{-n\cdot STR_{1oon}\cdot t} \\
&+ n\cdot e^{-(n-1)\cdot STR_{1oon}\cdot t}\cdot(1-e^{-STR_{1oon}\cdot t}) \\
&+ .... \\
&+ \binom{n}{i}\cdot e^{-(n-i)\cdot STR_{1oon}\cdot t}\cdot(1-e^{-STR_{1oon}\cdot t})^{i} \\
&+ ... \\
&+ n\cdot e^{-STR_{1oon}\cdot t}\cdot(1-e^{-STR_{1oon}\cdot t})^{n-1}
\end{aligned}
\tag{4.67}
$$

$$
\begin{aligned}
\Rightarrow MTTF_{Spurious\_1oon} &= \frac{e^{-n\cdot STR_{1oon}\cdot t}}{-n\cdot STR_{1oon}}\Bigg|_0^{\infty} \\
&+ \frac{n\cdot e^{-(n-1)\cdot STR_{1oon}\cdot t}}{-(n-1)\cdot STR_{1oon}}\Bigg|_0^{\infty} + \frac{n\cdot e^{-STR_{1oon}\cdot t}}{-STR_{1oon}}\Bigg|_0^{\infty} \\
&+ .... \\
&+ \binom{n}{i}\cdot\int_0^{\infty} e^{-(n-i)\cdot STR_{1oon}\cdot t}\cdot(1-e^{-STR_{1oon}\cdot t})^{i}\cdot dt \\
&+ ... \\
&+ n\cdot\int_0^{\infty} e^{-STR_{1oon}\cdot t}\cdot(1-e^{-STR_{1oon}\cdot t})^{n-1}\cdot dt \\
&= \frac{1}{n\cdot STR_{1oon}} \\
&+ \frac{n}{(n-1)\cdot STR_{1oon}} + \frac{n}{STR_{1oon}} \\
&+ ... \\
&+ \binom{n}{i}\cdot\int_0^{\infty} e^{-(n-i)\cdot STR_{1oon}\cdot t}\cdot(1-e^{-STR_{1oon}\cdot t})^{i}\cdot dt \\
&+ ... \\
&+ n\cdot\int_0^{\infty} e^{-STR_{1oon}\cdot t}\cdot(1-e^{-STR_{1oon}\cdot t})^{n-1}\cdot dt
\end{aligned}
\tag{4.68}
$$

4.6 koon-Architektur

In diesem Kapitel werden die Berechnungen von STR, PFS_{avg} und $MTTF_{Spurious}$ der $koon$-Architektur mit $n \geq k \geq 2$ hergeleitet. Die Abbildung 4.13 stellt das Blockdiagramm einer $koon$-Architektur voneinander unabhängige Kanäle dar. Gemäß der Tabelle 3.1 hat die $koon$-Architektur eine HFT_D von $n-k$ in Bezug auf Sicherheitsfunktion bzw. Sicht der Sicherheit und eine Hardware-Fehlertoleranz $HFT_{Spurious}$ von $k-1$ in Bezug auf Spurious-Trip bzw. die Sicht der Verfügbarkeit [77].

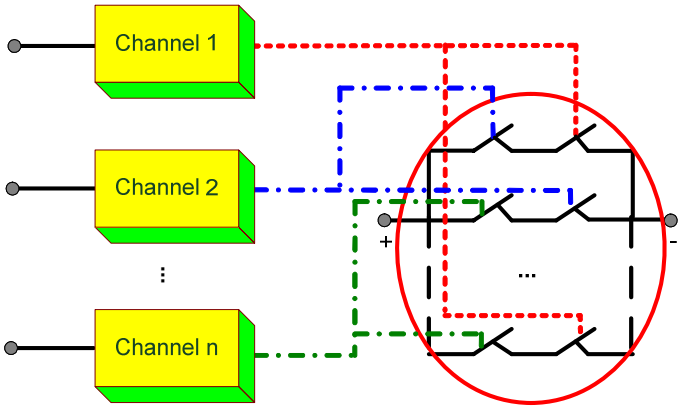

Abbildung 4.13: Blockdiagramm der koon-Architektur

Die Berechnung des STR-Werts der $koon$-Architektur wird durch die folgenden Schritte ausgeführt:

- Spurious-Trip aufgrund von sicheren Fehler: jeder unabhängige sichere Fehler kann zu einem Spurious-Trip Fehler mit der Rate $(1-\beta_S)\cdot\lambda_S$ führen. Da $koon$-Architektur n unabhängige Kanäle hat, hat der erste Spurious-Trip Fehler eine Rate von $n\cdot(1-\beta_S)\cdot\lambda_S$. Der fehlerhafte Kanal wird in den Reparatur-Zustand gebracht. Die Wahrscheinlichkeit, dass ein Kanal aufgrund Spurious-Trip ausfällt und in der Reparatur ist, beträgt:

$$p_S = 1 - e^{-(1-\beta_S)\cdot\lambda_S\cdot MTTR} \approx (1-\beta_S)\cdot\lambda_S\cdot MTTR \tag{4.69}$$

  Während der Reparatur des ersten ausgefallenen Kanals können die anderen $(n-1)$ Kanäle aufgrund eines sicheren Fehlers mit einer Wahrscheinlichkeit $p(N_S \geq k-1)$ zu einem Spurious-Trip Ausfall führen, wobei N_S die Anzahl des Spurious-Trip Fehlers ist aufgrund des sicheren Fehlers in der Reparaturzeit des ersten Kanals [77]. Daher ist dieser Fehler binomial verteilt. Die Spurious-Trip Rate wird aufgrund des sicheren Fehlers nach der folgenden Gleichung bestimmt:

$$\begin{aligned} STR_{koon\_S} &= n\cdot(1-\beta_S)\cdot\lambda_S\cdot p(N_S \geq k-1) \\ &= n\cdot(1-\beta_S)\cdot\lambda_S\cdot\sum_{m=k-1}^{n-1}\binom{n-1}{m}\cdot(p_S)^m\cdot(1-p_S)^{2-m} \end{aligned} \tag{4.70}$$

  mit:

$$\begin{aligned}\sum_{m=k-1}^{n-1}\binom{n-1}{m}\cdot(p_S)^m\cdot(1-p_S)^{n-1-m} &= \binom{n-1}{k-1}(p_S)^{k-1}\cdot(1-p_S)^{n-k} \\ &+\binom{n-1}{k}(p_S)^{k}\cdot(1-p_S)^{n-1-k} \\ &\approx \binom{n-1}{k-1}(p_S)^{k-1}\cdot(1-p_S)^{n-k} \\ &\approx \binom{n-1}{k-1}(p_S)^{k-1}\end{aligned} \tag{4.71}$$

wobei $p << 1$ ist, daher folgt $p^{m+1} << p^m$ für $\forall m \geq 1$ und $(1-p)^m = 1$.
Durch Ersetzen (4.71) und (4.69) in die Gleichung (4.70) lässt sich die Bestimmung des STR_{koon_S}-Werts wie folgt definieren:

$$STR_{koon\_S} = n\cdot\binom{n-1}{k-1}\cdot\left[(1-\beta_S)\cdot\lambda_S\right]^k(MTTR)^{k-1} \tag{4.72}$$

- Spurious-Trip aufgrund eines gefährlich erkannten Fehlers: der erste Fehler einer *koon*-Architektur fällt mit einer Rate von $n\cdot(1-\beta_D)\cdot\lambda_{DD}$ aus und wird in den Reparatur-Zustand gebracht. Die Wahrscheinlichkeit, dass ein Kanal aufgrund Spurious-Trip ausfällt und in der Reparatur ist, beträgt

$$p_{DD} = 1-e^{-(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR} \approx (1-\beta_D)\cdot\lambda_{DD}\cdot MTTR \tag{4.73}$$

Während der Reparatur des ersten ausgefallenen Kanals können die anderen $(n-1)$ Kanäle aufgrund eines gefährlich erkannten Fehlers mit einer Wahrscheinlichkeit $p(N_{DD} \geq n-k)$ zu einem Spurious-Trip Ausfall führen, wobei N_{DD} die Anzahl des Spurious-Trip Fehlers ist aufgrund des gefährlich erkannten Fehlers in der Reparaturzeit des ersten Kanals [77]. Dieser Fehler ist binomial verteilt. Die Spurious-Trip Rate wird aufgrund des gefährlich erkannten Fehlers nach der folgenden Gleichung bestimmt:

$$\begin{aligned}STR_{koon\_DD} &= n\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot p(N_{DD}\geq n-k) \\ &= n\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot\sum_{m=n-k}^{n-1}\binom{n-1}{m}\cdot(p_{DD})^m\cdot(1-p_{DD})^{n-1-m}\end{aligned} \tag{4.74}$$

mit:

$$\begin{aligned}\sum_{m=n-k}^{n-1}\binom{n-1}{m}\cdot(p_S)^m\cdot(1-p_S)^{n-1-m} &= \binom{n-1}{n-k}(p_S)^{n-k}\cdot(1-p_S)^{k-1} \\ &+\binom{n-1}{n-k+1}(p_S)^{n-k+1}\cdot(1-p_S)^{k-2} \\ &+ \ldots\ldots \\ &\approx \binom{n-1}{n-k}(p_S)^{n-k}\end{aligned} \tag{4.75}$$

wobei $p << 1$ ist, daher folgt $p^{m+1} << p^m$ für $\forall m \geq 1$ und $(1-p)^m = 1$. Außerdem gelten die folgenden Gleichungen:

$$\binom{m}{t} = \binom{m}{m-t} \tag{4.76}$$

$$\Rightarrow \binom{n-1}{n-k}(p_S)^{n-k} = \binom{n-1}{n-1-(n-k)}(p_S)^{n-1-(n-k)} = \binom{n-1}{k-1}(p_S)^{k-1} \tag{4.77}$$

Durch Ersetzen (4.73) und (4.75) und (4.77) in die Gleichung (4.74) lässt sich die Bestimmung des STR_{koon_DD}-Werts wie folgt definieren:

$$STR_{koon\_DD} = n\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot\left[\binom{n-1}{k-1}\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR\right]^{k-1} \tag{4.78}$$

- Spurious-Trip aufgrund Fehler infolge gemeinsamer Ursache mit der Rate:

$$STR_{koon\_CCF} = \beta_S\cdot\lambda_S + \beta_D\cdot\lambda_{DD} \tag{4.79}$$

- Spurious-Trip aufgrund nicht echter Anforderung mit der Rate:

$$STR_{koon\_FD} = \gamma\cdot\lambda_{DE} \tag{4.80}$$

Durch Ersetzen von (4.72), (4.78), (4.79) und (4.80) in die Gleichung (3.4) ergibt sich die folgende Gleichung für die Bestimmung des STR_{koon}-Werts der $koon$-Architektur:

$$
\begin{aligned}
STR_{koon} &= STR_{koon\_S} + STR_{koon\_DD} + STR_{koon\_CCF} + STR_{koon\_FD} \\
&= n \cdot \binom{n-1}{k-1} \cdot \left[(1-\beta_S)\cdot\lambda_S\right]^k (MTTR)^{k-1} \\
&+ n \cdot (1-\beta_D)\cdot\lambda_{DD} \cdot \left[\binom{n-1}{n-k}\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR\right]^{n-k} \\
&+ \beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD} + \gamma \cdot \lambda_{DE}
\end{aligned}
\tag{4.81}
$$

Die Formel für PFS_{avg_koon} wird ähnlich wie bei der 1*oon* -Architektur berechnet.

$$
\begin{aligned}
PFS_{avg\_koon} &= PFS_{avg\_koon\_S} + PFS_{avg\_koon\_DD} + PFS_{avg\_CCF} + PFS_{avg\_FD} \\
&= \frac{1}{T}\int_0^T (1 - R_{Spurious\_koon\_S}(t))\cdot dt \\
&+ \frac{1}{T}\int_0^T (1 - R_{Spurious\_koon\_DD}(t))\cdot dt \\
&+ (\beta_S \cdot \lambda_S + \beta_D \cdot \lambda_{DD})\cdot MTTR + \gamma \cdot \lambda_{DE} \cdot \tau_{DE}
\end{aligned}
\tag{4.82}
$$

mit:

$$
\begin{aligned}
R_{Spurious\_koon\_S} &= \sum_{i=k}^{n} \binom{n}{i} \cdot R_{Spurious\_S}^{i} \cdot (1 - R_{Spurious\_S})^{n-i} \\
&= \sum_{i=0}^{n-k} \binom{n}{i} \cdot R_{Spurious\_S}^{n-i} \cdot (1 - R_{Spurious\_S})^{i}
\end{aligned}
\tag{4.83}
$$

und:

$$
\begin{aligned}
R_{Spurious\_koon\_DD} &= \sum_{i=k}^{n} \binom{n}{i} \cdot R_{Spurious\_DD}^{i} \cdot (1 - R_{Spurious\_DD})^{n-i} \\
&= \sum_{i=0}^{n-k} \binom{n}{i} \cdot R_{Spurious\_DD}^{n-i} \cdot (1 - R_{Spurious\_DD})^{i}
\end{aligned}
\tag{4.84}
$$

Anhand der Gleichung (4.9) wird der $MTTF_{Spurious\_koon}$-Wert wird als folgende Gleichung beschrieben:

$$
\begin{aligned}
MTTF_{Spurious\_koon} &= \int_0^\infty R_{Spurious\_koon}(t)\cdot dt \\
&= \int_0^\infty \left[\sum_{i=0}^{n-k}\binom{n}{i}\cdot R_{Spurious}^{n-i}\cdot(1-R_{Spurious})^{i}\right]\cdot dt \\
&= \int_0^\infty R_{Spurious\_koon}^{n}\cdot dt \\
&+ \int_0^\infty n\cdot R_{Spurious}^{n-1}\cdot(1-R_{Spurious})\cdot dt \\
&+ .... \\
&+ \int_0^\infty \binom{n}{i}\cdot R_{Spurious}^{n-i}(1-R_{Spurious})^{i}\cdot dt \\
&+ ... \\
&+ \int_0^\infty [(n-k)\cdot R_{Spurious}\cdot(1-R_{Spurious})^{n-k}]\cdot dt
\end{aligned}
\tag{4.85}
$$

$$
\begin{aligned}
\Rightarrow MTTF_{Spurious\_koon} &= \left.\frac{e^{-n\cdot STR_{koon}\cdot t}}{-n\cdot STR_{koon}}\right|_0^\infty \\
&+ \left.\frac{n\cdot e^{-(n-1)\cdot STR_{koon}\cdot t}}{-(n-1)\cdot STR_{koon}}\right|_0^\infty + \left.\frac{n\cdot e^{-STR_{koon}\cdot t}}{-STR_{koon}}\right|_0^\infty \\
&+ .... \\
&+ \binom{n}{i}\cdot\int_0^\infty e^{-(n-i)\cdot STR_{koon}\cdot t}\cdot(1-e^{-STR_{koon}\cdot t})^{i}\cdot dt \\
&+ ... \\
&+ (n-k)\cdot\int_0^\infty e^{-STR_{koon}\cdot t}\cdot(1-e^{-STR_{koon}\cdot t})^{n-k}\cdot dt \\
&= \frac{1}{n\cdot STR_{koon}} \\
&+ \frac{n}{(n-1)\cdot STR_{koon}} + \frac{n}{STR_{koon}} \\
&+ ... \\
&+ \binom{n}{i}\cdot\int_0^\infty e^{-(n-i)\cdot STR_{koon}\cdot t}\cdot(1-e^{-STR_{koon}\cdot t})^{i}\cdot dt \\
&+ ... \\
&+ (n-k)\cdot\int_0^\infty e^{-STR_{koon}\cdot t}\cdot(1-e^{-STR_{koon}\cdot t})^{n-k}\cdot dt
\end{aligned}
\tag{4.86}
$$

4.7 Zusammenfassung

Unter den Voraussetzungen, die bereits im Abschnitt 3.3.3 beschrieben wurden, wurden die Sicherheitsparameter des Spurious-Trips in diesem Kapitel für unterschiedliche Systemarchitekturen nach dem Ruhestromprinzip bestimmt. Um die Formel für einfache und auch komplexe Systeme zu verallgemeinern, wurde die Blockdiagramm-Methode (RBD[68]) für die Bestimmung dieser Kenngrößen verwendet. Da es Unterschiede zwischen Betriebsart mit niedriger Anforderungsrate und Betriebsart mit hoher Anforderungsrate gibt, die bereits im Abschnitt 3.3 beschrieben wurden, wurden die Berechnungsformeln der Sicherheitsparameter des Spurious-Trips als Funktion in Abhängigkeit der Anforderungsrate angegeben. Die zu bestimmenden Werte sind: PFS, STR- und $MTTF_{Spurious}$-Wert. Die untersuchten Systemarchitekturen sind: 1oo1, 1oo2, 2oo2 und 2oo3. Zum Schluss dieses Kapitels wurden die PFS, STR- und $MTTF_{Spurious}$-Formel für eine allgemeine 1oon- und $koon$-Architektur in den Abschnitten 4.5 und 4.6 angegeben. Die Blockdiagramm-Methode wurde für die Berechnung in diesem Kapitel verwendet. Mit dem Markov-Modell wird die Berechnungsdurchführung einer Systemarchitektur, die im Kapitel 5 beschrieben wird, detaillierter dargestellt. Daraus folgt, dass die Gleichungen anhand des Markov-Modells komplexer als mit dem Blockdiagramm sind. Die in diesem Kapitel resultierenden Gleichungen werden für die Berechnungsbeispiele im Kapitel 6 angewendet, um die Beeinflussung der Anforderungsrate auf die Sicherheitsparameter im Fall eines Spurious-Trips besser darstellen zu können.

[68] RBD: Reliability Block Diagram

5 Berechnung der Spurious-Trip Parameter mittels Markov-Modell

Die Anforderungsrate und Anforderungsdauer können für jede Anforderung unterschiedlich sein. Um diesen Aspekt für das Sicherheitssystem besser zu analysieren, haben einige Autoren das Markov-Modell verwendet. Hui Jin et al. [52] und Yiliu Liu et al. [59] haben gezeigt, dass mit dem Markov-Modell die Grenzlinie zwischen der Betriebsart mit niedriger Anforderungsrate und der Betriebsart mit hoher Anforderungsrate besser dargestellt werden kann. Der Unterschied wurde durch die Berechnung des PFD- und PFH-Wertes in Abhängigkeit von Anforderungsrate und Anforderungsdauer gezeigt. Basierend auf dieser Kenntnis und der Theorie der Verfügbarkeit [11] wird der Einfluss von Anforderungsrate und Anforderungsdauer auf PFS-, $MTTF_{Spurious}$- und STR-Wertes in diesem Kapitel betrachtet. Die Berechnungen sind für das Ruhestromprinzip gedacht. Deshalb ist der sichere Zustand bei solchen Strukturen ein stromloser Zustand.

Wie bereits im Kapitel 3.3.2 erwähnt, kann der $MTTF_{Spurious}$-Wert in der Terminologie der Markov-Ketten als eine Absorptionszeit angesehen werden. Absorptionszeit ist eine zufällige Zeit, die eine Markov-Kette braucht, um in einen absorbierenden[69] Zustand zu gelangen. Für die $MTTF_{Spurious}$-Berechnung wird die Zeit, die der Prozess vom Anfangszustand „OK“ zum stromlosen Zustand braucht, berechnet. Je nach Pfad, wie der Prozess vom Anfangszustand zum Endzustand nimmt, ist diese Zeit unterschiedlich. Daher hat die Anzahl der Übergangszustände einen großen Einfluss auf die Berechnung der Absorptionszeit. Die Übergangszustände werden aus der Anzahl der Komponenten im System und der Kombination der Fehlerart berechnet. Eine Komponente kann bei einem Zeitpunkt einen der folgenden Zustände erreichen:

- OK: bei diesem Zustand tritt kein Fehler auf
- SD: bei dem Zustand ist ein sicherer erkannter Fehler aufgetreten
- SU: bei dem Zustand ist ein sicherer unerkannter Fehler aufgetreten
- DD: bei dem Zustand ist ein gefährlicher erkannter Fehler aufgetreten
- DU: bei dem Zustand ist ein gefährlicher unerkannter Fehler aufgetreten
- Demand Zustand: in diesem Zustand muss die Sicherheitsfunktion ausgelöst werden
- Sicherer Zustand: dieser Zustand ist ein stromloser Zustand

Aus diesen Bedingungen wird eine Markov-Kette mit diskretem Zustandsraum und diskreter Zeit angewendet.

Fällt ein System aufgrund eines Spurious-Trip Fehlers aus, wird das System den stromlosen Zustand (de-energized) erreichen. Das bedeutet, dass das Gesamtsystem nicht verfügbar ist.

[69] Ein Zustand heißt absorbiert, wenn die Markov-Kette in diesem Zustand angekommen ist und von dort nicht mehr entkommen kann.

Diese Nicht-Verfügbarkeit ist die Wahrscheinlichkeit P_S, dass das Gesamtsystem sich im sicheren Zustand befindet. Mittels Markov-Modell kann die PFS_{avg}-Funktion in Abhängigkeit von der Anforderungsrate und Anforderungsdauer dargestellt werden:

$$PFS = P_S = g(\lambda_{DE}, \mu_{DE}) \tag{5.1}$$

So wird die Berechnung der Spurious-Trip Rate auch als eine Funktion h in Abhängigkeit von der Anforderungsdauer und Anforderungsrate dargestellt:

$$STR = h(\lambda_{DE}, \mu_{DE}) \tag{5.2}$$

Daraus folgt die $MTTF_{Spurious}$-Berechnung anhand der Gleichungen (3.12) und (5.2):

$$\begin{aligned} MTTF_{Spurious} &= \int_0^\infty R_{Spurious}(t) \cdot dt \\ &= \int_0^\infty y(h(\lambda_{DE}, \mu_{DE})) \cdot dt \end{aligned} \tag{5.3}$$

Im weiteren Verlauf des Kapitels werden diese Eigenschaften in der Berechnung von PFS_{avg}, $MTTF_{Spurious}$ und STR mitberücksichtigt. Die Berechnungen werden für unterschiedliche System-Architekturen durchgeführt.

5.1 1oo1-Architektur

Die Abbildung 5.1 stellt das Markov-Modell der 1oo1 System-Architektur dar. Das Modell besteht aus vier Zuständen. Zustand Z0 stellt den Zustand dar, in dem das System fehlerfrei funktioniert. Aus diesem Zustand kann das System in die restlichen drei Zustände direkt oder indirekt übergehen:

- Zustand Z1: dieser Zustand repräsentiert den Spurious-Trip Zustand (stromloser Zustand oder sicherer Zustand)
- Zustand Z2: in diesem Zustand weist das System einen gefährlich erkannten Fehler auf.
- Zustand Z3: in diesem Zustand weist das System einen gefährlich unerkannten Fehler auf.

Weist das System einen sicheren Fehler oder eine Anforderung auf, wird es in den Zustand Z1 mit einer Übergangsrate $\lambda_S + \lambda_{FD}$ überführt. Aus dem Spurious-Trip Zustand kann das System über die Übergangsrate μ_R [70] wegen einem sicheren oder gefährlich erkannten Fehler oder

[70] $\mu_R = \frac{1}{MTTR}$, wobei MTTR: Mean Time To Repair

über die Übergangsrate μ_{DE} [71] wegen einer Anforderung den fehlerfreien Zustand Z0 erreichen.

Ist ein gefährlich erkannter Fehler im System aufgetreten, geht das System aus dem Zustand Z0 in den Zustand Z2 mit einer Übergangsrate λ_{DD} über. Der Zustand Z2 kann auch über den direkten Weg μ_0 [72] in den Zustand Z1 gelangen.

Weist das System einen gefährlich unerkannten Fehler auf, wird es in Zustand Z3 mit einer Übergangsrate λ_{DU} überführt. Befindet sich das System im Zustand Z3 und erfolgt eine Anforderung mit der Rate λ_{DE}, um die Sicherheitsfunktion auszulösen, dann ist das System nicht mehr in der Lage die Sicherheitsfunktion auszuführen und es kann deshalb eine Katastrophe folgen. Um das System funktionsfähig zu machen und es in den fast „wie neu" Zustand zu versetzen, benötigt das System eine Zeit τ_{LT} [73], in der alle Tests durchgeführt werden. Mit einer Übergangsrate μ_{LT} [74] geht das System aus dem Zustand Z3 in den Zustand Z0 über.

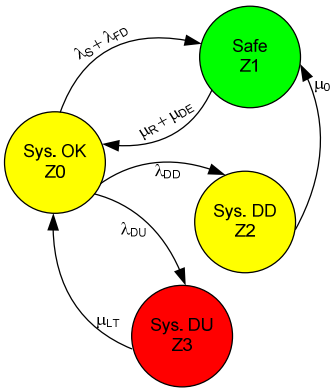

Abbildung 5.1: Markov-Modell der 1oo1-Architektur

Die Übergangsmatrix kann daher wie folgt gebildet werden:

---

71 $\mu_{DE} = \frac{1}{\lambda_{DE}}$

72 $\mu_0 = \frac{1}{\tau_{Test}}$

73 τ_{LT} : Life Time (Lebensdauer)

74 $\mu_{LT} = \frac{1}{\tau_{LT}}$

$$P = \begin{bmatrix} 1-A_0 & \lambda_S + \lambda_{FD} & \lambda_{DD} & \lambda_{DU} \\ \mu_R + \mu_{DE} & 1-(\mu_R + \mu_{DE}) & 0 & 0 \\ 0 & \mu_0 & 1-\mu_0 & 0 \\ \mu_{LT} & 0 & 0 & 1-\mu_{LT} \end{bmatrix} \quad \textbf{(5.4)}$$

mit:

$$\begin{aligned} A_0 &= \lambda_S + \lambda_{FD} + \lambda_{DD} + \lambda_{DU} = \lambda_S + \lambda_{FD} + \lambda_D \\ \lambda_{FD} &= \gamma \cdot \lambda_{DE} \end{aligned} \quad \textbf{(5.5)}$$

PFS_{avg_1oo1}-Wert werden anhand des folgenden Gleichungssystems gelöst:

$$\begin{aligned} &(\lambda_S + \lambda_{FD}) \cdot P_0 - (\mu_R + \mu_{DE}) \cdot P_1 + \mu_0 P_2 = 0 \\ &\lambda_{DD} \cdot P_0 - \mu_0 P_2 = 0 \\ &\lambda_{DU} \cdot P_0 - \mu_{LT} P_3 = 0 \\ &P_0 + P_1 + P_2 + P_3 = 1 \end{aligned} \quad \textbf{(5.6)}$$

Durch Lösen dieses Gleichungssystems ergeben sich die Zustandswahrscheinlichkeiten:

$$\begin{aligned} A &= 1 + \frac{\lambda_S + \lambda_{DD} + \lambda_{FD}}{\mu_R + \mu_{DE}} + \frac{\lambda_{DD}}{\mu_0} + \frac{\lambda_{DU}}{\mu_{LT}} \\ P_0 &= \frac{1}{A} \\ P_1 &= \frac{\lambda_S + \lambda_{DD} + \lambda_{FD}}{\mu_R + \mu_{DE}} \cdot P_0 \\ P_2 &= \frac{\lambda_{DD} \cdot P_0}{\mu_0} \\ P_3 &= \frac{\lambda_{DU} \cdot P_0}{\mu_{LT}} \end{aligned} \quad \textbf{(5.7)}$$

Das System fällt aufgrund Spurious-Trips aus, wenn es sich im Zustand Z1 befindet. Daher werden der STR_{1oo1}- und PFS_{avg_1oo1}-Wert durch folgende Gleichungen bestimmt:

$$STR_{1oo1} = (\lambda_S + \lambda_{FD}) \cdot P_0 + \mu_0 \cdot P_2 \quad \textbf{(5.8)}$$

$$PFS_{avg\_1oo1} = P_1 \quad \textbf{(5.9)}$$

Da die Zustände Z1, Z2 und Z3 absorbierende Zustände sind, wird die M-Matrix wie folgt dargestellt:

$$M = [A_0] \Rightarrow N = M^{-1} = \frac{1}{A_0} = \frac{1}{\lambda_S + \lambda_{FD} + \lambda_D} \quad \textbf{(5.10)}$$

Der $MTTF_{Spurious\_1oo1}$-Wert lässt sich dann berechnen durch:

$$MTTF_{Spurious\_1oo1} = \frac{1}{\lambda_S + \lambda_{FD} + \lambda_D} \tag{5.11}$$

Mit diesen Ergebnissen wurde bewiesen, dass die Anforderungsrate und Anforderungsdauer auf die PFS_{avg_1oo1} und STR_{1oo1}-Werte Einfluss haben. Diese Eigenschaften wurden mit dem Markov-Modell gezeigt.

5.2 1oo2-Architektur

Die Abbildung 5.2 beschreibt das aus sieben Zuständen bestehende Markov-Modell eines 1oo2-Systems. Der Zustand Z0 ist der Zustand, in dem das System fehlerfrei und im Betrieb ist. Hat das System einen sicheren Fehler (zufälligen Fehler oder Fehler infolge gemeinsamer Ursache) oder eine Anforderung, geht das System in den Zustand Z1 mit der Rate $2(1-\beta_S)\lambda_S + \beta_S\lambda_S + \lambda_{FD}$ über. Tritt ein Fehler DD oder DU im System auf, geht das System in den Zustand Z2, oder Z4 über. Vom Zustand Z0 geht das System in den Zustand Z4 mit einer Rate $\beta_D\lambda_{DD}$ oder Z5 mit einer Rate $\beta\lambda_{DU}$, wenn ein Fehler infolge gemeinsamen Ursache DD oder DU im System auftritt. Das System wird von Zustand Z2, Z3 oder Z4 mit der Rate μ_0 in den Zustand Z1 gebracht. Somit ist das System im sicheren Zustand (stromloser Zustand oder Spurious-Trip Zustand). Nach der Reparaturzeit oder Anforderungsdauer kehr das System wider in den Zustand Z0 mit der Rate $\mu_R + \mu_{DE}$ zurück.

Soll eine Anforderung ausgelöst werden, wenn das System sich in einem der Zustände Z3, Z5, und Z6 befindet, hat das System versagt. Keine Sicherheitsfunktion wird in diesen Fällen ausgelöst. Der gefährliche Zustand wird dadurch erreicht. Das System soll dann mit einer Übergangsrate μ_{LT} [75] von Zustand Z3, Z5 oder Z6 in den „fast wie neu“ Zustand Z0 überführt werden.

[75] $\mu_{LT} = \frac{1}{\tau_{LT}}$

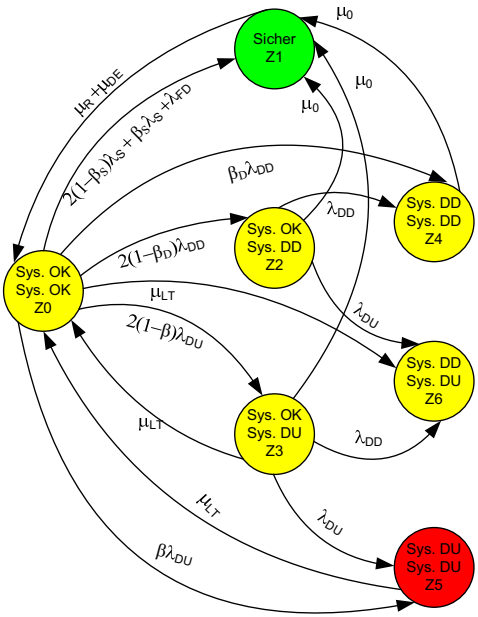

Abbildung 5.2: Markov-Modell für 1oo2-Architektur

Die Übergangsmatrix wird mittels Markov-Modell (Abbildung 5.2) wie folgt gebildet:

$$P = \begin{bmatrix} P_1 & P_2 \end{bmatrix} \qquad \textbf{(5.12)}$$

wobei:

$$P_1 = \begin{bmatrix} 1-A_0 & 2\cdot(1-\beta_S)\cdot\lambda_S + \beta_S\cdot\lambda_S + \lambda_{FD} & 2\cdot(1-\beta_D)\cdot\lambda_{DD} \\ \mu_R + \mu_{DE} & 1-(\mu_R+\mu_{DE}) & 0 \\ 0 & \mu_0 & 1-A_2 \\ \mu_{LT} & \mu_0 & 0 \\ 0 & \mu_0 & 0 \\ \mu_{LT} & 0 & 0 \\ \mu_{LT} & 0 & 0 \end{bmatrix} \quad \textbf{(5.13)}$$

$$P_2 = \begin{bmatrix} 2\cdot(1-\beta)\cdot\lambda_{DU} & \beta_{DD}\cdot\lambda_{DD} & \beta\cdot\lambda_{DU} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \lambda_{DD} & 0 & \lambda_{DU} \\ 1-A_3 & 0 & \lambda_{DU} & \lambda_{DD} \\ 0 & \mu_0 & 0 & 0 \\ 0 & 0 & \mu_{LT} & 0 \\ 0 & 0 & 0 & \mu_{LT} \end{bmatrix} \quad \textbf{(5.14)}$$

mit:

$$\begin{aligned} A_0 &= 2\cdot(1-\beta_S)\cdot\lambda_S + \beta_S\cdot\lambda_S + \lambda_{FD} + 2\cdot(1-\beta_D)\cdot\lambda_{DD} + \beta_D\cdot\lambda_{DD} \\ &\quad + 2\cdot(1-\beta)\cdot\lambda_{DU} + \beta\cdot\lambda_{DU} \\ \lambda_{FD} &= \gamma\cdot\lambda_{DE} \\ A_2 &= \mu_0 + \lambda_{DD} + \lambda_{DU} = \mu_0 + \lambda_D \\ A_3 &= \mu_{LT} + \mu_0 + \lambda_{DD} + \lambda_{DU} = \mu_{LT} + \mu_0 + \lambda_D \end{aligned} \quad \textbf{(5.15)}$$

PFS_{avg_1oo2}-Wert werden anhand des folgenden Gleichungssystems gelöst:

$$\begin{aligned} &[2(1-\beta_S)\lambda_S + \beta_S\lambda_S + \lambda_{FD}]P_0 - (\mu_R+\mu_{DE})P_1 + \mu_0(P_2+P_3+P_4) = 0 \\ &2(1-\beta_D)\lambda_{DD}P_0 - A_2P_2 = 0 \\ &2(1-\beta)\lambda_{DU}P_0 - A_3P_3 = 0 \\ &\beta_D\lambda_{DD}P_0 + \lambda_{DD}P_2 - \mu_0P_4 = 0 \\ &\beta\lambda_{DU}P_0 + \lambda_{DU}P_3 - \mu_{LT}P_5 = 0 \\ &\lambda_{DU}P_2 + \lambda_{DD}P_3 - \mu_{LT}P_6 = 0 \\ &P_0 + P_1 + P_2 + P_3 + P_4 + P_5 + P_6 = 1 \end{aligned} \quad \textbf{(5.16)}$$

Durch Lösen dieses Gleichungssystems ergeben sich die Zustandswahrscheinlichkeiten:

$$
\begin{aligned}
P_0 &= \frac{1}{1+B_1+B_2+B_3+B_4+B_5+B_6} \\
P_1 &= \frac{[2(1-\beta_S)\lambda_S+\beta_S\lambda_S+\lambda_{FD}]P_0+\mu_0(B_2+B_3+B_4)P_0}{\mu_R+\mu_{DE}} = B_1P_0 \\
P_2 &= \frac{2(1-\beta_D)\lambda_{DD}P_0}{A_2} = B_2P_0 \\
P_3 &= \frac{2(1-\beta)\lambda_{DU}P_0}{A_3} = B_3P_0 \\
P_4 &= \frac{(\beta_D\lambda_{DD}+\lambda_{DD}B_2)P_0}{\mu_0} = B_4P_0 \\
P_5 &= \frac{(\beta\lambda_{DU}+\lambda_{DU}B_3)P_0}{\mu_{LT}} = B_5P_0 \\
P_6 &= \frac{(B_2\lambda_{DU}+\lambda_{DD}B_3)P_0}{\mu_{LT}} = B_6P_0
\end{aligned}
\qquad \textbf{(5.17)}
$$

Das System fällt aufgrund von Spurious-Trips aus, wenn es sich im Zustand Z1 befindet. Daher werden der STR_{1oo2}- und PFS_{avg_1oo2}-Wert durch folgende Gleichungen bestimmt:

$$STR_{1oo2} = [2(1-\beta_S)\lambda_S+\beta_S\lambda_S+\lambda_{FD}]P_0+\mu_0(P_2+P_3+P_4) \qquad \textbf{(5.18)}$$

$$PFS_{avg\_1oo2} = P_1 \qquad \textbf{(5.19)}$$

Da die Zustände Z1, Z4, Z5 und Z6 absorbierende Zustände sind, wird die M-Matrix wie folgt dargestellt:

$$M = \begin{bmatrix} A_0 & -2(1-\beta_D)\lambda_{DD} & -2(1-\beta)\lambda_{DU} \\ 0 & A_2 & 0 \\ -\mu_{LT} & 0 & A_3 \end{bmatrix} \qquad \textbf{(5.20)}$$

$$\Rightarrow N = M^{-1} = \begin{bmatrix} \frac{1}{A_0} & \frac{[2(1-\beta_D)\lambda_{DD}]^2\mu_{LT}}{A_0A_2A_0} & \frac{2(1-\beta)\lambda_{DU}}{A_0A_7} \\ 0 & \frac{2(1-\beta_D)\lambda_{DD}\mu_{LT}}{A_0A_2} & 0 \\ 0 & 0 & \frac{1}{A_7} \end{bmatrix} \qquad \textbf{(5.21)}$$

Der $MTTF_{Spurious\_1oo2}$-Wert lässt sich dann berechnet durch:

$$MTTF_{Spurious\_1oo2} = \frac{1}{A_0}+\frac{[2(1-\beta_D)\lambda_{DD}]^2\mu_{LT}}{A_0A_2A_0}+\frac{2(1-\beta)\lambda_{DU}}{A_0A_7} \qquad \textbf{(5.22)}$$

mit:

$$A_7 = A_3 - \frac{2(1-\beta_D)\lambda_{DD}\mu_{LT}}{A_0} \tag{5.23}$$

5.3 2oo2-Architektur

Wie bei der 1oo2-Architektur besteht das Markov-Modell der 2oo2-Architektur auch aus sieben Zuständen und wird in der Abbildung 5.3 dargestellt. Arbeitet das System fehlerfrei, befindet es sich im Zustand Z0. Hat das System einen sicheren Fehler (zufälligen Fehler oder Fehler infolge gemeinsamer Ursache) oder eine Anforderung, geht das System in den Zustand Z1 mit der Rate $2(1-\beta_S)\lambda_S + \beta_S\lambda_S + \lambda_{FD}$ über. Tritt ein zufälliger Fehler DD oder DU im System auf, geht das System in den Zustand Z2, oder Z4 über. Bei einer 2oo2-Architektur ist der übrige Kanal noch verfügbar, während der ausgefallene Kanal in der Reparatur ist. So befindet sich das System im Zustand Z2, wird das System nach der Reparaturzeit wieder in den Zustand Z0 gebracht. Diese Eigenschaft hat eine 1oo2-Architektur nicht. Bei einer 1oo2-Architektur wird das System abgeschaltet, wenn ein von beiden Kanäle fehlerhaft und erkannt ist. Vom Zustand Z0 geht das System in den Zustand Z4 mit einer Rate $\beta_D\lambda_{DD}$ oder Z5 mit einer Rate $\beta\lambda_{DU}$, wenn ein Fehler infolge gemeinsamen Ursache DD oder DU im System auftritt. Das System wird von Zustand Z2 oder Z4 mit der Rate μ_0 in den Zustand Z1 gebracht. Somit ist das System im sicheren Zustand (stromloser Zustand oder Spurious-Trip Zustand). Nach der Reparaturzeit oder Anforderungsdauer kehrt das System wieder in den Zustand Z0 mit der Rate $\mu_R + \mu_{DE}$ zurück.

Soll eine Anforderung ausgelöst werden, wenn das System sich in einem der Zustände Z3, Z5, und Z6 befindet, hat das System versagt. Keine Sicherheitsfunktion wird in diesen Fällen ausgelöst. Der gefährliche Zustand wird dadurch erreicht. Das System soll dann mit einer Übergangsrate μ_{LT} [76] von Zustand Z3, Z5 oder Z6 in den „fast wie neu“ Zustand Z0 überführt werden.

[76] $\mu_{LT} = \frac{1}{\tau_{LT}}$

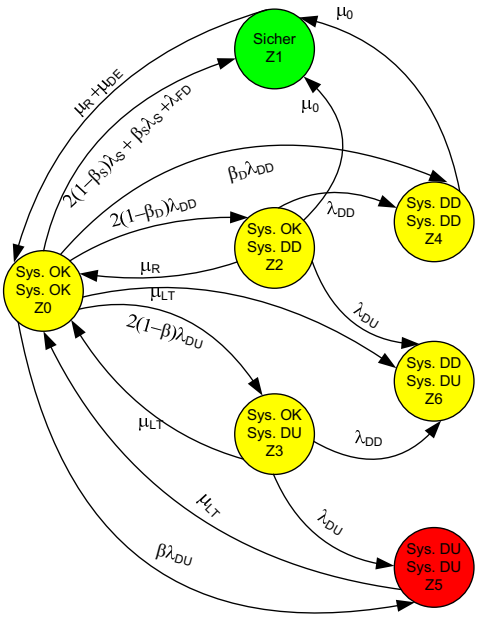

Abbildung 5.3: Markov-Modell der 2oo2-Architektur

Die Übergangsmatrix wird mittels Markov-Modell (Abbildung 5.3) wie folgt gebildet:

$$P = \begin{bmatrix} P_1 & P_2 \end{bmatrix} \qquad \textbf{(5.24)}$$

wobei:

$$P_1 = \begin{bmatrix} 1-A_0 & 2\cdot(1-\beta_S)\cdot\lambda_S + \beta_S\cdot\lambda_S + \lambda_{FD} & 2\cdot(1-\beta_D)\cdot\lambda_{DD} \\ \mu_R + \mu_{DE} & 1-(\mu_R+\mu_{DE}) & 0 \\ \mu_R & \mu_0 & 1-A_2 \\ \mu_{LT} & 0 & 0 \\ 0 & \mu_0 & 0 \\ \mu_{LT} & 0 & 0 \\ \mu_{LT} & 0 & 0 \end{bmatrix} \tag{5.25}$$

$$P_2 = \begin{bmatrix} 2\cdot(1-\beta)\cdot\lambda_{DU} & \beta_{DD}\cdot\lambda_{DD} & \beta\cdot\lambda_{DU} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \lambda_{DD} & 0 & \lambda_{DU} \\ 1-A_3 & 0 & \lambda_{DU} & \lambda_{DD} \\ 0 & \mu_0 & 0 & 0 \\ 0 & 0 & \mu_{LT} & 0 \\ 0 & 0 & 0 & \mu_{LT} \end{bmatrix} \tag{5.26}$$

mit:

$$\begin{aligned} A_0 &= 2\cdot(1-\beta_S)\cdot\lambda_S + \beta_S\cdot\lambda_S + \lambda_{FD} + 2\cdot(1-\beta_D)\cdot\lambda_{DD} + \beta_D\cdot\lambda_{DD} \\ &\quad + 2\cdot(1-\beta)\cdot\lambda_{DU} + \beta\cdot\lambda_{DU} \\ \lambda_{FD} &= \gamma\cdot\lambda_{DE} \\ A_2 &= \mu_R + \mu_0 + \lambda_{DD} + \lambda_{DU} = \mu_R + \mu_0 + \lambda_D \\ A_3 &= \mu_{LT} + \lambda_{DD} + \lambda_{DU} = \mu_{LT} + \lambda_D \end{aligned} \tag{5.27}$$

PFS_{avg_2oo2}-Wert werden anhand des folgenden Gleichungssystems gelöst:

$$\begin{aligned} &[2(1-\beta_S)\lambda_S + \beta_S\lambda_S + \lambda_{FD}]P_0 - (\mu_R+\mu_{DE})P_1 + \mu_0(P_2+P_4) = 0 \\ &2(1-\beta_D)\lambda_{DD}P_0 - A_2P_2 = 0 \\ &2(1-\beta)\lambda_{DU}P_0 - A_3P_3 = 0 \\ &\beta_D\lambda_{DD}P_0 + \lambda_{DD}P_2 - \mu_0P_4 = 0 \\ &\beta\lambda_{DU}P_0 + \lambda_{DU}P_3 - \mu_{LT}P_5 = 0 \\ &\lambda_{DU}P_2 + \lambda_{DD}P_3 - \mu_{LT}P_6 = 0 \\ &P_0 + P_1 + P_2 + P_3 + P_4 + P_5 + P_6 = 1 \end{aligned} \tag{5.28}$$

Durch Lösen dieses Gleichungssystems ergeben sich die Zustandswahrscheinlichkeiten:

$$
\begin{aligned}
P_0 &= \frac{1}{1 + B_1 + B_2 + B_3 + B_4 + B_5 + B_6} \\
P_1 &= \frac{[2(1-\beta_S)\lambda_S + \beta_S\lambda_S + \lambda_{FD}]P_0 + \mu_0(B_2 + B_4)P_0}{\mu_R + \mu_{DE}} = B_1 P_0 \\
P_2 &= \frac{2(1-\beta_D)\lambda_{DD}P_0}{A_2} = B_2 P_0 \\
P_3 &= \frac{2(1-\beta)\lambda_{DU}P_0}{A_3} = B_3 P_0 \\
P_4 &= \frac{(\beta_D\lambda_{DD} + \lambda_{DD}B_2)P_0}{\mu_0} = B_4 P_0 \\
P_5 &= \frac{(\beta\lambda_{DU} + \lambda_{DU}B_3)P_0}{\mu_{LT}} = B_5 P_0 \\
P_6 &= \frac{(B_2\lambda_{DU} + \lambda_{DD}B_3)P_0}{\mu_{LT}} = B_6 P_0
\end{aligned}
\tag{5.29}
$$

Das System fällt aufgrund von Spurious-Trips aus, wenn es sich im Zustand Z1 befindet. Daher werden der STR_{2oo2}- und PFS_{avg_2oo2}-Wert durch folgende Gleichungen bestimmt:

$$STR_{2oo2} = [2(1-\beta_S)\lambda_S + \beta_S\lambda_S + \lambda_{FD}]P_0 + \mu_0(P_2 + P_4) \tag{5.30}$$

$$PFS_{avg\_2oo2} = P_1 \tag{5.31}$$

Da die Zustände Z1, Z4, Z5 und Z6 absorbierende Zustände sind, wird die M-Matrix wie folgt dargestellt:

$$M = \begin{bmatrix} A_0 & -2(1-\beta_D)\lambda_{DD} & -2(1-\beta)\lambda_{DU} \\ -\mu_R & A_2 & 0 \\ -\mu_{LT} & 0 & A_3 \end{bmatrix} \tag{5.32}$$

$$\Rightarrow N = M^{-1} = \begin{bmatrix} \frac{1}{A_0} & A_{12} & A_{13} \\ 0 & A_{11} & \frac{2(1-\beta)\lambda_{DU}\mu_R}{A_0 A_7 A_{10}} \\ 0 & \frac{-A_8}{A_7 A_{10}} & \frac{1}{A_{10}} \end{bmatrix} \tag{5.33}$$

Der $MTTF_{Spurious\_2oo2}$-Wert lässt sich dann berechnet durch:

$$MTTF_{Spurious\_2oo2} = \frac{1}{A_0} + A_{12} + A_{13} \tag{5.34}$$

mit:

$$
\begin{aligned}
A_7 &= A_2 - \frac{2(1-\beta_D)\lambda_{DD}\mu_R}{A_0} \\
A_8 &= -\frac{2(1-\beta_D)\lambda_{DD}\mu_{LT}}{A_0} \\
A_9 &= A_3 - \frac{2(1-\beta)\lambda_{DU}\mu_{LT}}{A_0} \\
A_{10} &= A_9 + \frac{2(1-\beta)\lambda_{DU}\mu_R A_8}{A_0 A_7} \\
A_{11} &= \frac{1}{A_7} - \frac{2(1-\beta)\lambda_{DU}\mu_R}{A_0 A_7} \cdot \frac{A_8}{A_7 A_{10}} \\
A_{12} &= A_{11} \cdot \frac{2(1-\beta_D)\lambda_{DD}}{A_0} + \frac{2(1-\beta)\lambda_{DU}}{A_0} \cdot \frac{A_8}{A_7} \\
A_{13} &= \frac{2(1-\beta)\lambda_{DU}}{A_0 A_{10}} + \frac{2(1-\beta_D)\lambda_{DD}}{A_0} \cdot \frac{2(1-\beta)\lambda_{DU}\mu_R}{A_0 A_7 A_{10}}
\end{aligned}
\tag{5.35}
$$

5.4 koon-Architektur

Es seien $n>1$ Komponenten im System und somit hat die Markov-Kette dieses Systems eine Zustandsmenge S. Die Übergangswahrscheinlichkeit von Zustand i nach j wird als Summe möglicher Wege mit Zwischenzuständen k dargestellt. Dies wird Chapman-Kolmogorow Gleichung[77] genannt:

$$
p(X_n = j \mid X_0 = i) = \sum_{k \in S} p(X_n = j \mid X_l = k)\, p(X_l = k \mid X_0 = i) \tag{5.36}
$$

Die Übergangswahrscheinlichkeiten zwischen den Zuständen bilden dann eine $s \times s$-Matrix. Diese Matrix lässt sich wie folgt darstellen:

$$
\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1s_0} \\ p_{21} & p_{22} & \cdots & p_{2s_0} \\ \vdots & \vdots & \cdots & \vdots \\ p_{s_0 1} & p_{s_0 2} & \cdots & p_{s_0 s_0} \end{bmatrix} = \begin{bmatrix} M & \Lambda \\ 0 & I \end{bmatrix} \tag{5.37}
$$

wobei:

- (r,r)-Matrix M: Übergangsmatrix zwischen transienten[78] Zuständen
- (r,s)-Matrix Λ: Übergangsmatrix zwischen transienten und absorbierenden Zuständen
- Matrix 0: Übergangsmatrix zwischen absorbierenden und transienten Zuständen
- Einheitsmatrix I: Übergangsmatrix zwischen absorbierenden Zuständen

[77] siehe Anhang A.

[78] Ein Zustand heißt transient dann und nur dann, wenn die Wahrscheinlichkeit nicht mehr in den Zustand zu gelangen positiv ist.

Somit wird die Zustandswahrscheinlichkeit $p(X_n = j)$, wobei $n \in \aleph_0$, bei einer homogenen Markov-Kette mit minimalem Zustandsraum $S = \{1,2,.....,k\}$ auf dem Wahrscheinlichkeitsraum (Ω, A, p) mit Anfangsverteilung p_{i_0} und Übergangsmatrix $\mathbf{P}$ wie folgt dargestellt [I05]:

$$p(X_n = j) = \sum_{i=1}^{k} p_i (\mathbf{P}^n)_{ij} \quad \text{für } \forall j \in S \tag{5.38}$$

Die Gleichung des PFS_{avg_koon}-Werts wird in Abhängigkeit von der Zustandswahrscheinlichkeit des sicheren Zustands dargestellt:

$$PFS_{avg\_koon} = p_{\text{sicherer\_Zustand}} = p_1 \tag{5.39}$$

Aus den Gleichungen (5.38) und (5.39) folgt die Berechnung der Spurious-Trip Rate eines $koon$-Systems:

$$STR_{koon} = \sum_{j=0}^{k} p(X_n = j) \cdot p_{j1} \tag{5.40}$$

Anhand der Matrix M kann der $MTTF_{Spurious\_koon}$-Wert bestimmt werden:

$$M^{-1} = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1r} \\ m_{21} & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ m_{r1} & m_{r2} & \cdots & m_{rr} \end{bmatrix} \tag{5.41}$$

$$\Rightarrow MTTF_{Spurious\_koon} = m_{11} + m_{12} + ... + m_{1r} \tag{5.42}$$

Die Abbildung 5.4 stellt das Markov-Modell einer $koon$-Architektur dar:

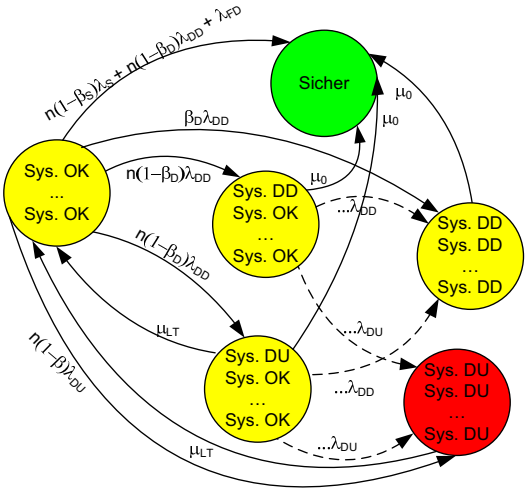

Abbildung 5.4: Markov-Modell einer koon-Architektur

5.5 Zusammenfassung

Mit dem Markov-Modell wurde die Berechnungsdurchführung verschiedener Architekturen, die in diesem Kapitel beschrieben wurden, detailliert dargestellt. Die untersuchten Systemarchitekturen sind: 1oo1, 1oo2, 2oo2 und *koon*. Die resultierenden Gleichungen wurden unter der Voraussetzungen, die bereits im Abschnitt 3.3.3 beschrieben wurden, hergeleitet. Die *STR*-, *PFS*-, $MTTF_{Spurious}$-Formeln werden als Funktion in Abhängigkeit von Anforderungsrate und Anforderungsdauer dargestellt. Da das Markov-Modell verschiedene fehlerfreie und fehlerbehaftete Zustände mit verschiedenen Übergangsraten darstellt, enthalten alle Gleichungen nicht nur die Ausfallraten der sicheren, sondern auch noch der gefährlichen Fehler. Im Vergleich zu den Gleichungen, die in Kapitel 4 mittels Blockdiagramm hergeleitet wurden, sind die in diesem Kapitel hergeleiteten Gleichungen komplexer und detaillierter. Daher haben die Ergebnisse aus beiden Methoden auch kleine Abweichungen. Dieser Unterschied wird durch die Berechnungsbeispiele und die daraus resultierenden Diagrammen in Kapitel 6 ausführlicher gezeigt.

6 Bewertung und Analyse der Ergebnisse

Die Gleichungen für STR-, PFS_{avg}-, $MTTF_{Spurious}$-Berechnung wurden unter den Voraussetzungen mit dem neuen Ansatz, der im Kapitel 3.3 beschrieben wurde, bewiesen. Die Ergebnisse aus dem Blockdiagramm (Kapitel 4) und dem Markov-Modell (Kapitel 5) weichen geringfügig voneinander ab. Um einen besseren Vergleich zu bekommen, werden diese Sicherheitsparameter für unterschiedliche Systemarchitekturen in diesem Kapitel durch unterschiedliche Beispiele berechnet. Die aus dem Beispiel resultierenden Ergebnisse werden in verschiedenen Diagrammen dargestellt und miteinander verglichen. Zum Schluss des Kapitels werden die Ergebnisse, die mit der in dieser Arbeit hergeleiteten Gleichungen berechnet sind, mit den Ergebnissen, die mit den herkömmlichen Verfahren berechnet wurden, miteinander verglichen. Gegeben seien folgende Daten:

$$
\begin{aligned}
&MTTR = 8h \Rightarrow \mu_R = \frac{1}{MTTR} = \frac{1}{8} \\
&S = 0{,}5 \\
&DC = 0{,}9 \\
&\tau_{Test} = 24h \Rightarrow \mu_0 = \frac{1}{\tau_{Test}} = \frac{1}{24} \\
&\beta_D = 0{,}05 \\
&\beta_S = 0{,}07 \\
&\lambda_B = 5 \cdot 10^{-6} \\
&T = 8760h \\
&\lambda_{DE} = \left[10^{-8} \quad 10^{-6} \quad 10^{-4} \quad 10^{-2}\right] \\
&\tau_{DE} = \left[1s \quad 10s \quad 1m \quad 1h\right] \\
&\mu_{DE} = \frac{1}{\tau_{DE}} \\
&\mu_{LT} = 2{,}28 \cdot 10^{-4} \\
&\gamma = 0{,}01
\end{aligned}
\tag{6.1}
$$

Aus den gegebenen Daten werden die weiteren Sicherheitsparameter bestimmt. Die folgende Gleichung (6.2) ergibt sich aus der sicheren Ausfallrate und der gefährlichen Ausfallrate:

$$
\begin{aligned}
&\lambda_S = (1 - S) \cdot \lambda_B = 2{,}5 \cdot 10^{-6} \frac{1}{h} \\
&\lambda_D = S \cdot \lambda_B = 2{,}5 \cdot 10^{-6} \frac{1}{h}
\end{aligned}
\tag{6.2}
$$

Die Berechnungen der sicheren erkannten Ausfallrate und der sicheren unerkannten Ausfallrate sind in den Gleichungen (6.3) und (6.4) erfolgt.

$$\lambda_{SD} = (1-S)\cdot\lambda_B \cdot DC = 2{,}25\cdot 10^{-6}\,\frac{1}{h} \tag{6.3}$$

$$\lambda_{SU} = (1-S)\cdot\lambda_B \cdot (1-DC) = 2{,}5\cdot 10^{-7}\,\frac{1}{h} \tag{6.4}$$

Die Rate für den gefährlichen erkannten Ausfall und den gefährlichen unerkannten Ausfall werden in den Gleichungen (6.5) und (6.6) berechnet:

$$\lambda_{DD} = S\cdot\lambda_B \cdot DC = 2{,}25\cdot 10^{-6}\,\frac{1}{h} \tag{6.5}$$

$$\lambda_{DU} = S\cdot\lambda_B \cdot (1-DC) = 2{,}5\cdot 10^{-7}\,\frac{1}{h} \tag{6.6}$$

6.1 Bewertung und Analyse der Ergebnisse aus dem Blockdiagramm

In Abbildung 6.1 und Abbildung 6.2 werden die *STR*-Funktionen verschiedener Architekturen in Abhängigkeit der Anforderungsrate für eine Anforderungsdauer von $\tau_{DE} = 1s$ gezeichnet. Die Abbildung 6.2 ist die Vergrößerung der Abbildung 6.1, wobei die *STR*-Funktionen der 2oo2- und 2oo3-Architektur besser zu erkennen sind.

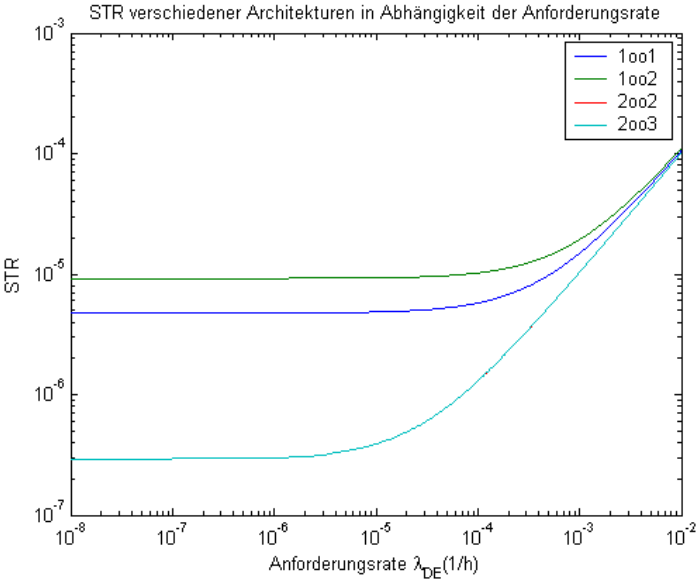

Abbildung 6.1: STR verschiedener Architekturen in Abhängigkeit von λ_{DE} (1)

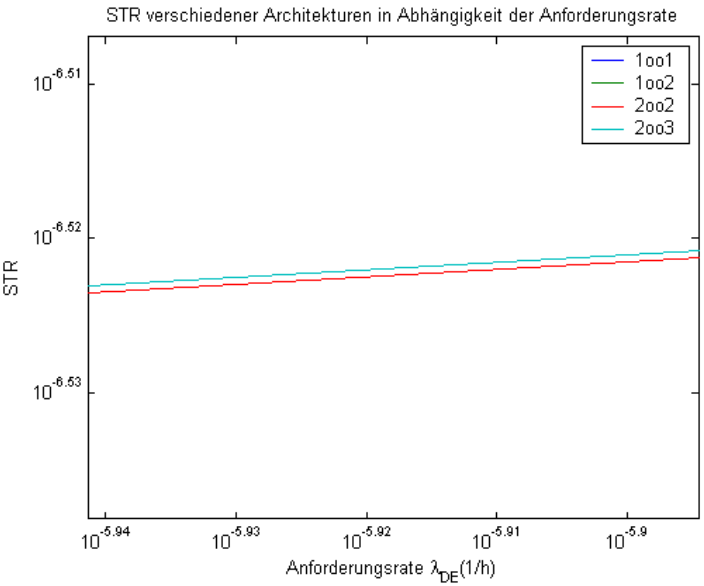

Abbildung 6.2: STR verschiedener Architekturen in Abhängigkeit von λ_{DE} (2)

Der *STR*-Wert ist zur Anforderungsrate proportional. Bei Betriebsart mit hoher Anforderungsrate liegen die *STR*-Kurven sehr nah beieinander. Die Differenz der *STR*-Werte zwischen den Architekturen ist bei Betriebsart mit niedriger Anforderungsrate größer als bei der Betriebsart mit hoher Anforderungsrate. Aus der Abbildung 6.1 und Abbildung 6.2 ist es leicht zu erkennen, dass der *STR*-Wert der 2oo2-Architektur am kleinsten ist. Das bedeutet auch, dass die Verfügbarkeit dieser Architektur größer ist im Vergleich zu anderen Architekturen (1oo1, 1oo2 und 2oo3). Eine Ungleichung wird aus dieser Erkennung für den Zusammenhang der verschiedenen Architekturen dargestellt:

$$STR_{1oo2} > STR_{1oo1} > STR_{2oo3} > STR_{2oo2} \quad \textbf{(6.7)}$$

Die Abbildung 6.3 stellt die PFS_{avg}-Funktionen verschiedener Architekturen in Abhängigkeit der Anforderungsrate dar. Die PFS_{avg}-Werte bleiben nach der Zunahme der Anforderungsrate unverändert. Aus der Abbildung 6.3 kann festgestellt werden, dass der *PFS*-Wert einer 1oo1-Architektur am kleinsten und der *PFS*-Wert einer 2oo3-Architektur am größten ist. Das bedeutet, die 2oo3-Architektur hat eine große Verfügbarkeit im Vergleich zu anderen Architekturen. Eine 1oo2-Architektur ist in der Sicht der Sicherheit besser als die 2oo2-Architektur. Allerdings ist die 1oo2-Architektur schlechter als die 2oo2-Architektur im Hinblick auf die Verfügbarkeit. Es gilt die folgende Ungleichung:

$$PFS_{avg\_1oo1} > PFS_{avg\_1oo2} > PFS_{avg\_2oo2} > PFS_{avg\_2oo3} \quad \textbf{(6.8)}$$

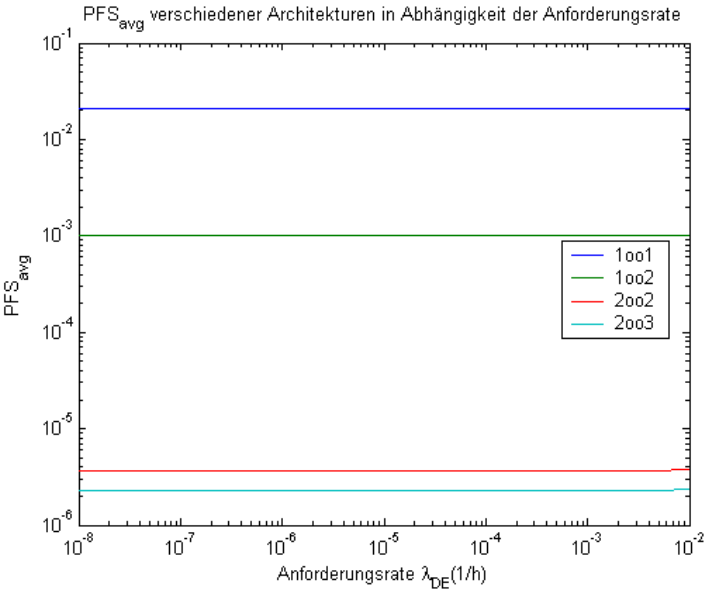

Abbildung 6.3: PFS_{avg} verschiedener Architekturen in Abhängigkeit von λ_{DE}

Die PFS_{avg}-Funktionen werden für verschiedene Architekturen in Abhängigkeit der Anforderungsdauer in der Abbildung 6.4 dargestellt. Die PFS_{avg}-Funktionen haben sehr minimale Abweichungen, wenn die Anforderungsdauer sich ändert, sodass die PFS_{avg}-Funktionen fast konstant dargestellt werden. Aus der Abbildung 6.4 kann die folgende Ungleichung gegeben werden:

$$PFS_{avg\_1oo1} > PFS_{avg\_1oo2} > PFS_{avg\_2oo2} > PFS_{avg\_2oo3} \quad \textbf{(6.9)}$$

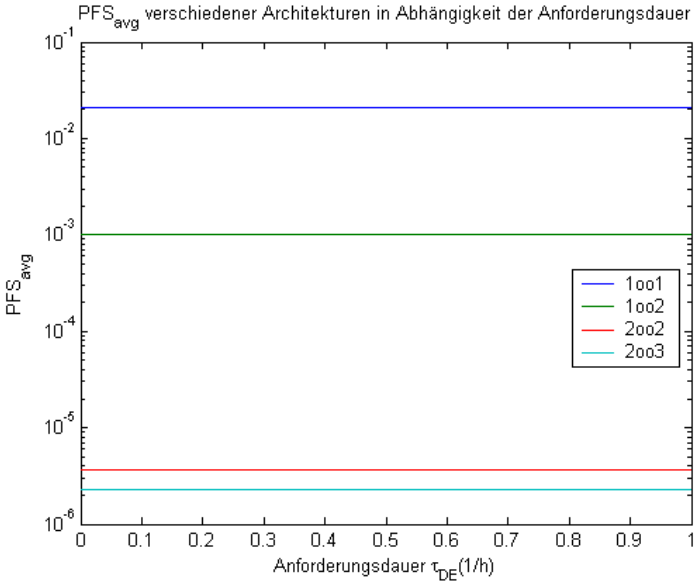

Abbildung 6.4: PFS_{avg} verschiedener Architekturen in Abhängigkeit von τ_{DE}

Die $MTTF_{Spurious}$-Funktionen verschiedener Architekturen in Abhängigkeit der Anforderungsrate werden in der Abbildung 6.5 dargestellt. Der $MTTF_{Spurious}$-Wert nimmt bei allen betrachteten Architekturen ab, wenn die Anforderungsrate zunimmt. Werden die Architekturen miteinander verglichen, so kann festgestellt werden, dass bei der Betriebsart mit niedriger Anforderungsrate die 1oo2-Architektur den kleinsten $MTTF_{Spurious}$-Wert hat und dass diese Architektur bei Betriebsart mit hoher Anforderungsrate den größten $MTTF_{Spurious}$-Wert hat. Daher wird die Ungleichung (6.10) bei der Betriebsart mit niedriger Anforderungsrate gegeben durch:

$$MTTF_{Spurious\_2oo3} > MTTF_{Spurious\_2oo2} > MTTF_{Spurious\_1oo1} > MTTF_{Spurious\_1oo2} \quad \textbf{(6.10)}$$

Bei Betriebsart mit hoher Anforderungsrate gilt die Ungleichung (6.11):

$$MTTF_{Spurious\_1oo2} > MTTF_{Spurious\_1oo1} > MTTF_{Spurious\_2oo3} > MTTF_{Spurious\_2oo2} \quad \textbf{(6.11)}$$

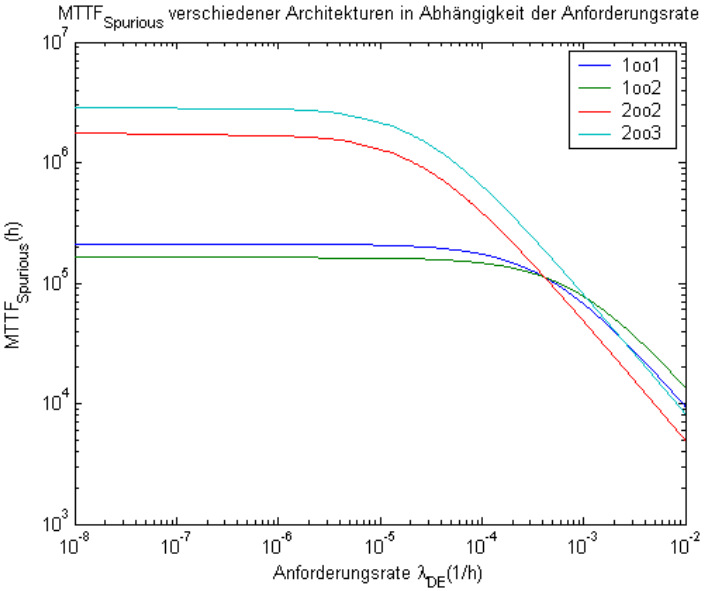

Abbildung 6.5: $MTTF_{Spurious}$ verschiedener Architekturen in Abhängigkeit von λ_{DE}

6.2 Bewertung und Analyse der Ergebnisse aus dem Markov-Modell

Anhand des Markov-Modells wurden im Kapitel 5 die $MTTF_{Spurious}$-Berechnungen für die 1oo1-, 1oo2- und 2oo2-Architektur in Abhängigkeit der Anforderungsrate und Anforderungsdauer durchgeführt. Mit den gegebenen Daten werden die PFS_{avg}-, STR und $MTTF_{Spurious}$-Werte mit der Gleichung (6.1) berechnet und deren Funktionen als Verläufe in den folgenden Abbildungen dargestellt.

6.2.1 1oo1-Architektur

Die PFS_{avg}-Funktionen werden in Abhängigkeit der Anforderungsrate in der Abbildung 6.6 für 1oo1-Architektur dargestellt. In der Abbildung 6.6 werden vier PFS_{avg}-Funktionen in Abhängigkeit der Anforderungsrate mit unterschiedlich konstanter Anforderungsdauer $\tau_{DE} = [1s \quad 10s \quad 10m \quad 10h]$ dargestellt. Je öfter die Sicherheitsfunktion angefordert wird, desto größer ist der PFS_{avg}-Wert. Je länger die Anforderungsdauer ist, desto größer ist der PFS_{avg}-Wert. In der Abbildung 6.6 ist zu erkennen, dass die Funktionen streng monoton steigend bei Betriebsart mit hoher Anforderungsrate sind und die PFS_{avg}-Funktionen bei der niedrigen Anforderungsrate fast konstant bleiben.

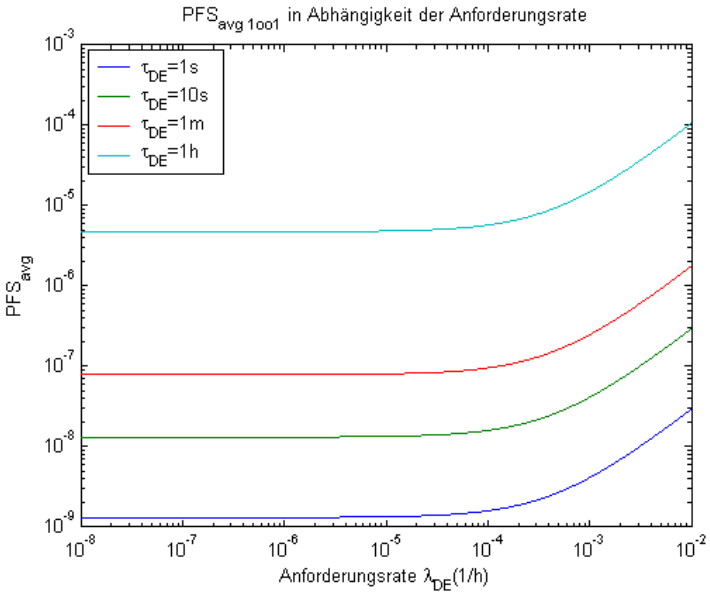

Abbildung 6.6: PFS_{avg} für 1oo1-Architekturen in Abhängigkeit von λ_{DE}

Ähnlich der PFS_{avg}-Funktionen sind die STR-Funktionen der 1oo1-Architektur in Abhängigkeit von der Anforderungsrate in Abbildung 6.7 zu sehen. Wird die Anforderung öfter angefordert, nimmt der STR-Wert zu (Abbildung 6.7). Das bedeutet, die Rate ist aufgrund des Spurious-Trips der 1oo1-Architektur proportional zur Anforderungsrate. Daraus folgt, dass die Prozessverfügbarkeit der 1oo1-Architektur immer kleiner wird, wenn das System aufgrund von Spurious-Trips ausfällt. Um die in der Abbildung 6.7 gezeichneten STR-Funktionen genauer darzustellen, wird eine Vergrößerung in der Abbildung 6.8 und Abbildung 6.9 gegeben. Obwohl es nur eine minimale Differenz zwischen den STR-Funktionen gibt, ist es trotzdem gut zu erkennen, dass STR-Wert proportional zur Anforderungsdauer ist. Das heißt, der STR-Wert wird kleiner, wenn die Anforderungsdauer kleiner ist. Daraus folgt, dass die Prozessverfügbarkeit des Systems immer zunimmt, wenn die Anforderungsdauer abnimmt.

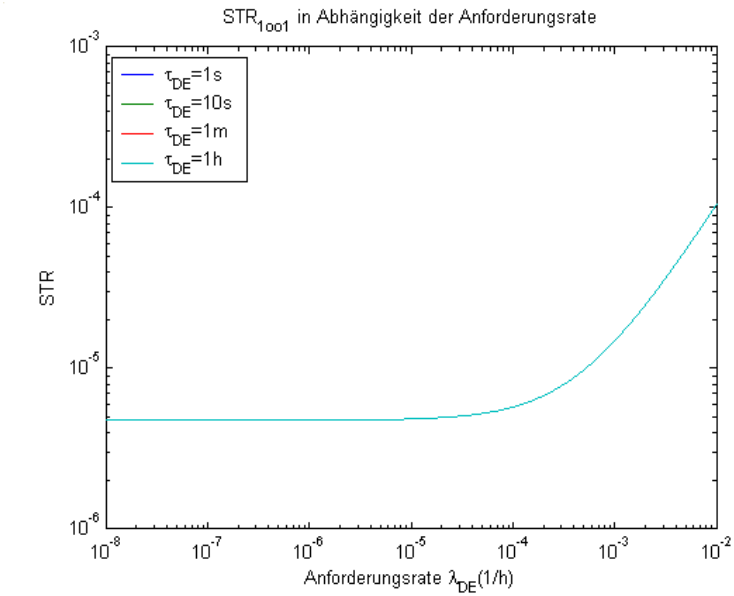

Abbildung 6.7: STR für 1oo1-Architekturen in Abhängigkeit von λ_{DE} (1)

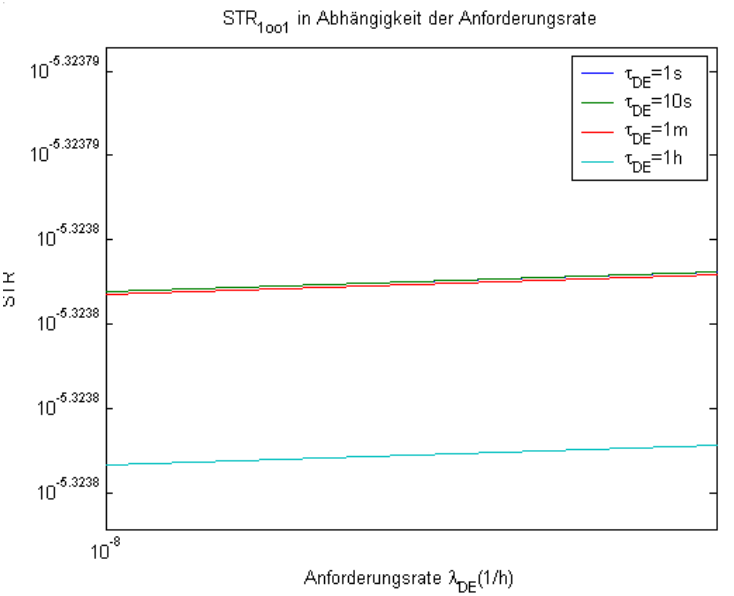

Abbildung 6.8: STR für 1oo1-Architekturen in Abhängigkeit von λ_{DE} (2)

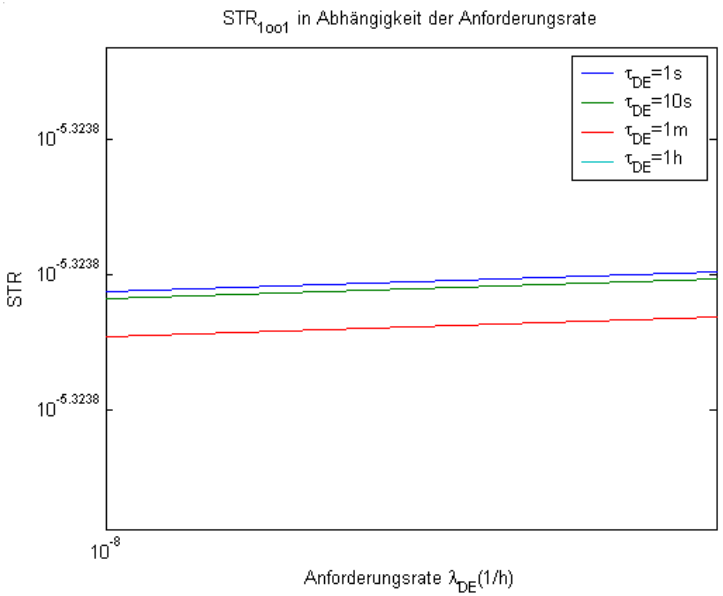

Abbildung 6.9: STR für 1oo1-Architekturen in Abhängigkeit von λ_{DE} (3)

Die Abbildung 6.10 beschreibt die Auswirkung von Anforderungsrate und Anforderungsdauer auf die mittlere Zeit bis zum Ausfall aufgrund des Spurious-Trips einer 1oo1-Architektur. In der Abbildung 6.10 werden die $MTTF_{Spurious}$ -Funktionen in Abhängigkeit zur Anforderungsrate dargestellt. Je größer die Anforderungsrate ist, desto kleiner ist der $MTTF_{Spurious}$ -Wert. Die $MTTF_{Spurious}$ -Funktion ist schneller absteigend bei der Betriebsart mit hoher Anforderungsrate als bei der Betriebsart mit niedriger Anforderungsrate. Die Änderung der Anforderungsdauer hat einen sehr kleinen Einfluss auf die $MTTF_{Spurious}$ -Berechnungen, die auf dem Markov-Modell basieren. Aus diesem Grund sind die $MTTF_{Spurious}$ -Funktionen bei unterschiedlicher Anforderungsdauer fast gleich dargestellt (Abbildung 6.10).

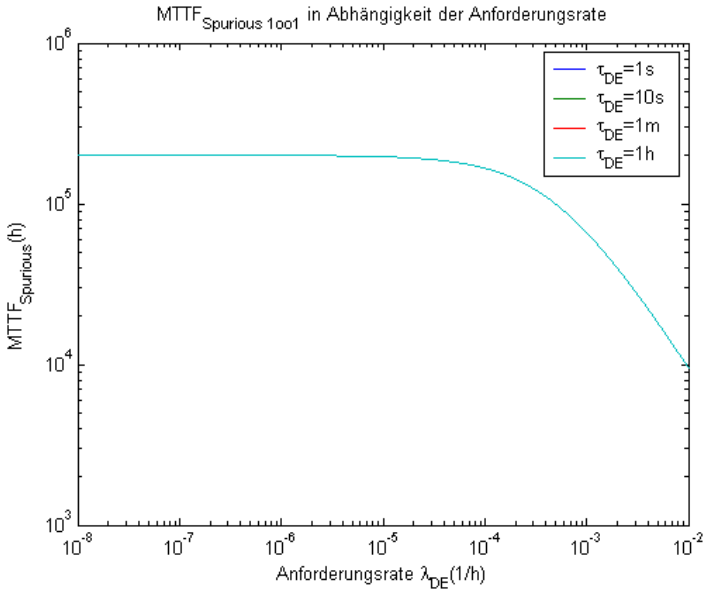

Abbildung 6.10: $MTTF_{Spurious}$ für 1oo1-Architekturen in Abhängigkeit von λ_{DE}

6.2.2 1oo2-Architektur

Die PFS_{avg}-Werte der 1oo2-Architektur werden als Funktion in Abhängigkeit von der Anforderungsrate und Anforderungsdauer in Abbildung 6.11 dargestellt. In der Abbildung ist zu erkennen, dass die PFS_{avg}-Funktionen in den Bereichen von $STL3$ bis $STL9$ liegen. Die PFS_{avg}-Funktionen sind schnell ansteigend, wenn die Anforderungsrate oder Anforderungsdauer zunimmt, d. h. die Ausfallwahrscheinlichkeit ist aufgrund des Spurious-Trips bei dieser Architektur in Betriebsart mit hoher Anforderungsrate größer als Ausfallwahrscheinlichkeit aufgrund des Spurious-Trips in Betriebsart mit niedriger Anforderungsrate. Mit dieser Erkenntnis wird bewiesen, dass auch bei der 1oo2-Architektur die Ausfallwahrscheinlichkeit aufgrund des Spurious-Trips bei Betriebsart mit niedriger Anforderungsrate anders ist als bei Betriebsart mit hoher Anforderungsrate. Mit dieser Erkenntnis kann festgestellt werden, dass der PFS_{avg}-Wert einer Architektur bei allen Betriebsarten nicht gleich ist.

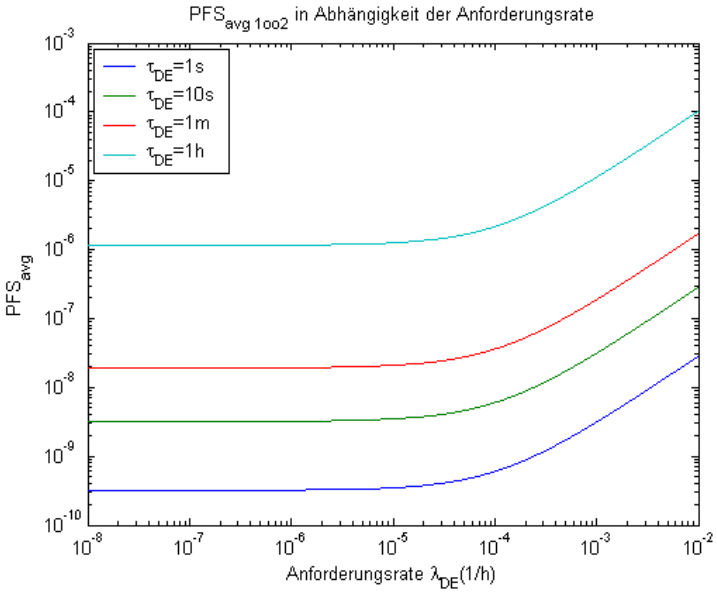

Abbildung 6.11: PFS_{avg} für 1oo2-Architekturen in Abhängigkeit von λ_{DE}

In der Abbildung 6.12 ist die STR-Funktion der 1oo2-Architektur in Abhängigkeit der Anforderungsrate dargestellt. Ähnlich wie bei der PFS_{avg}-Funktion, nimmt der STR-Wert ab, wenn die Anforderungsrate oder Anforderungsdauer abnimmt. Die Abbildung 6.13 und Abbildung 6.14 sind die Vergrößerungen von der Abbildung 6.12. Die Differenzen zwischen den STR-Funktionen sind minimal, während sie bei den PFS_{avg}-Funktionen relativ groß und sehr gut erkennbar sind.

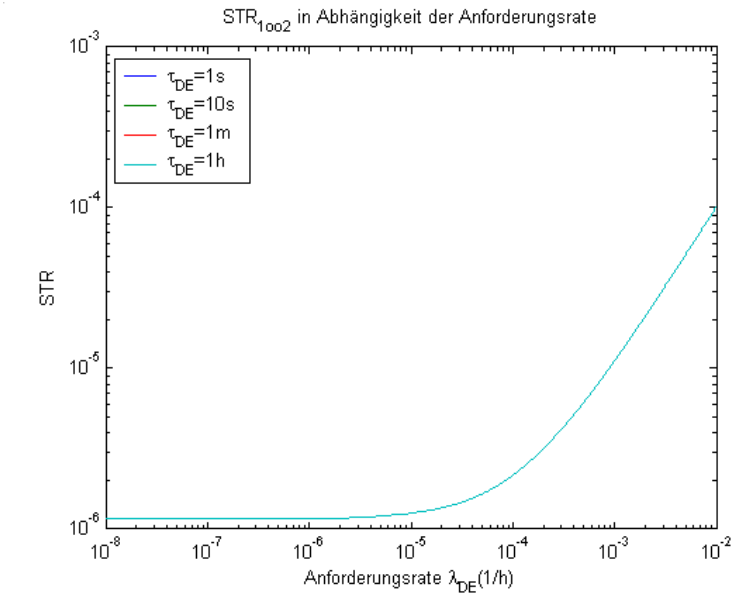

Abbildung 6.12: STR für 1oo2-Architekturen in Abhängigkeit von λ_{DE}

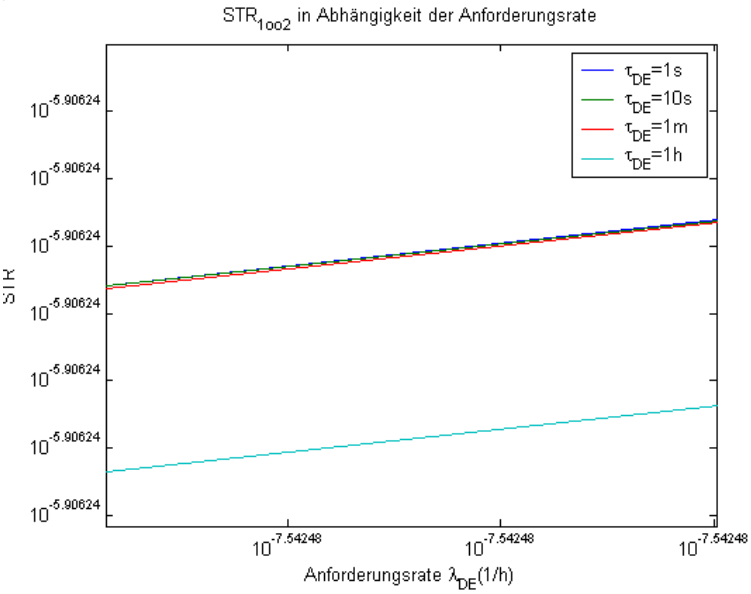

Abbildung 6.13: STR für 1oo2-Architekturen in Abhängigkeit von λ_{DE} (2)

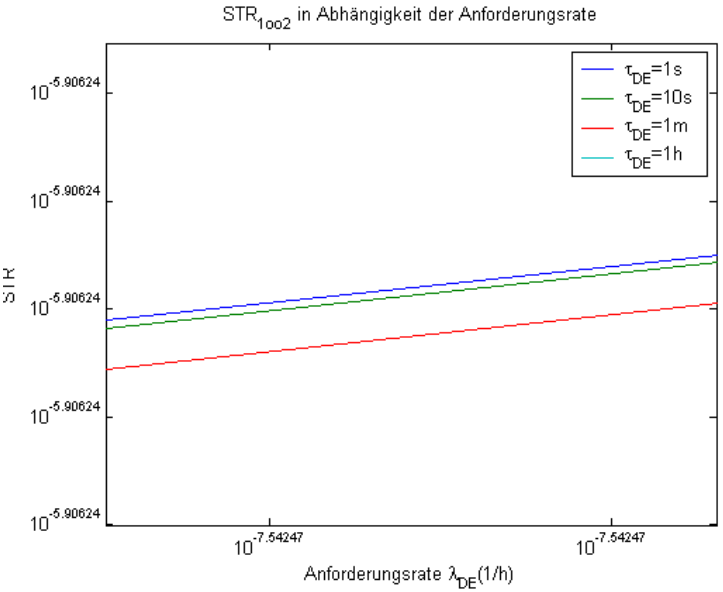

Abbildung 6.14: STR für 1oo2-Architekturen in Abhängigkeit von λ_{DE} (3)

Die Abbildung 6.15 stellt die $MTTF_{Spurious}$-Funktion in Abhängigkeit von der Anforderungsrate dar, wobei die Anforderungsdauer ($\tau_{DE} = [1s \quad 10s \quad 10m \quad 10h]$) konstant bleibt. Der $MTTF_{Spurious}$-Wert ist antiproportional zu Anforderungsrate und zur Anforderungsdauer. Je kleiner die Anforderungsrate ist, desto größer ist der $MTTF_{Spurious}$-Wert. Wie bei der 1oo1-Architektur, hat die Änderung der Anforderungsdauer einen sehr kleinen Einfluss auf die $MTTF_{Spurious}$-Berechnung, sodass die $MTTF_{Spurious}$-Kurven in Abhängigkeit der Anforderungsdauer fast gleich aussehen.

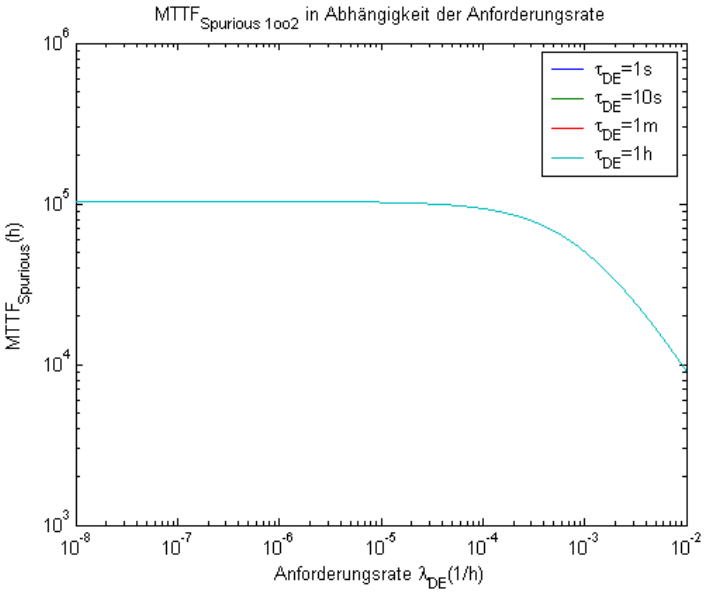

Abbildung 6.15: $MTTF_{Spurious}$ für 1oo2-Architekturen in Abhängigkeit von λ_{DE}

6.2.3 2oo2-Architektur

Die Abbildung 6.16 stellt die PFS_{avg}-Funktionen in Abhängigkeit von Anforderungsrate und Anforderungsdauer der 2oo2-Architektur dar. Wie bei der 1oo1- und 1oo2-Architektur ist die PFS_{avg}-Funktion proportional zur Anforderungsrate und zur Anforderungsdauer. Allerdings ist die Funktionssteigerung bei der 2oo2-Architektur hoch. Das bedeutet, dass bei diesem Beispiel mit der Betriebsart mit niedriger Anforderungsrate die 2oo2-Architektur eine höhere Verfügbarkeit als die 1oo1- und 1oo2-Architektur hat. Ein System mit einer 1oo2-Architektur ist aus der Sicht der Sicherheit sicherer als die 1oo1- und 2oo2-Architektur. Aber aus der Sicht der Verfügbarkeitsbetrachtung ist die 1oo2-Architektur schlechter als die 2oo2-Architektur.

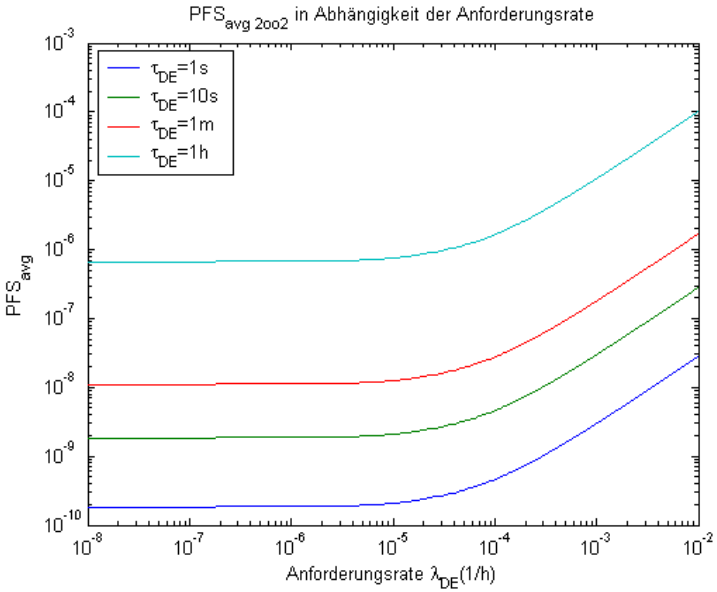

Abbildung 6.16: PFS_{avg} für 2oo2-Architekturen in Abhängigkeit von λ_{DE}

Die *STR*-Funktionen einer 2oo2-Architektur in Abhängigkeit von der Anforderungsrate und Anforderungsdauer werden in der Abbildung 6.17, Abbildung 6.18 und Abbildung 6.19 dargestellt. Der *STR*-Wert nimmt mit der Häufigkeit oder Dauer der Anforderung zu. Daher können die herkömmlichen *STR*-Formeln für unterschiedliche Betriebsarten nicht klar dargestellt werden, weil die *STR*-Werte bei Betriebsart mit hoher Anforderungsrate und Betriebsart mit niedriger Anforderungsrate nicht gleich sind. Diese Werte hängen stark von Anforderungsrate und Anforderungsdauer ab.

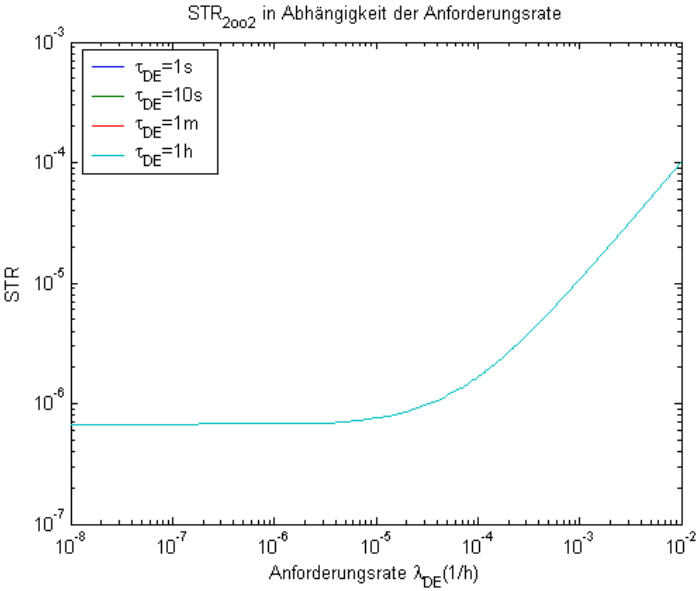

Abbildung 6.17: STR für 2oo2-Architekturen in Abhängigkeit von λ_{DE} (1)

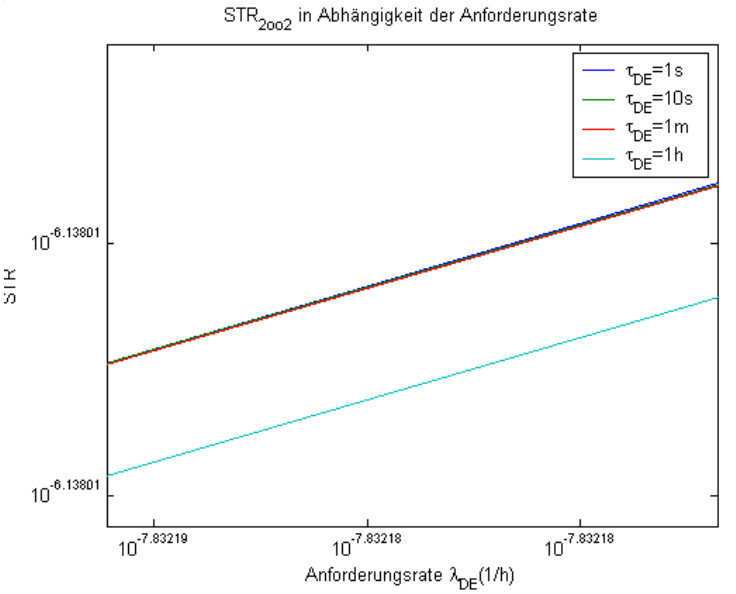

Abbildung 6.18: STR für 2oo2-Architekturen in Abhängigkeit von λ_{DE} (2)

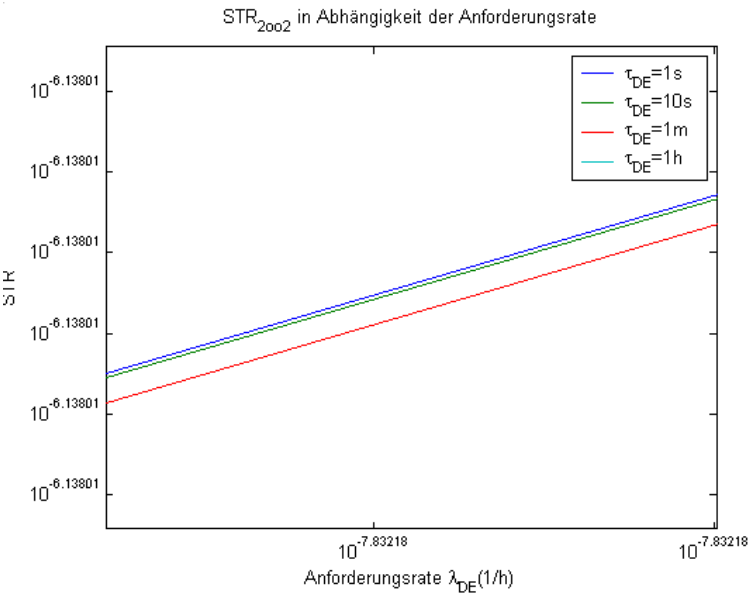

Abbildung 6.19: STR für 2oo2-Architekturen in Abhängigkeit von λ_{DE} (3)

Die $MTTF_{Spurious}$-Funktionen der 2oo2-Architektur werden in der Abbildung 6.20 dargestellt. Während die PFS-Funktionen zu Anforderungsrate und Anforderungsdauer proportional sind, sind die $MTTF_{Spurious}$-Funktionen zu den beiden Größen antiproportional. Daraus folgt: nimmt die Anforderungsrate (Abbildung 6.20) zu, nimmt der $MTTF_{Spurious}$-Wert ab. In Abhängigkeit zur Anforderungsrate sind die $MTTF_{Spurious}$-Funktionen streng monoton fallend, wenn das System in Betriebsart mit niedriger Anforderungsrate ist. Bei der Betriebsart mit niedriger Anforderungsrate sind die $MTTF_{Spurious}$-Funktionen fast konstant. Die $MTTF_{Spurious}$-Funktionen bleiben fast unverändert, wenn die Anforderungsdauer sich ändert.

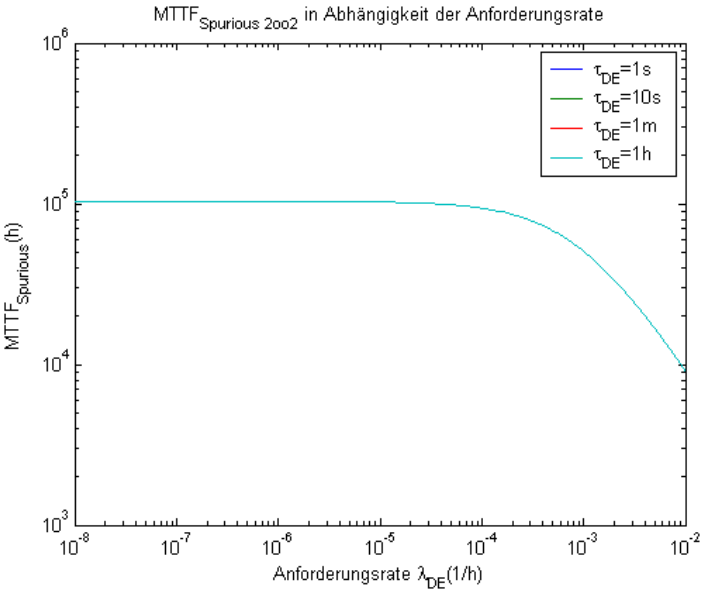

Abbildung 6.20: $MTTF_{Spurious}$ für 2oo2-Architekturen in Abhängigkeit von λ_{DE}

6.2.4 Resultierende Ergebnisse im Vergleich

Die PFS_{avg}-Funktionen der verschiedenen Architekturen (1oo1, 1oo2 und 2oo2) werden in der Abbildung 6.21 miteinander verglichen. Die PFS_{avg}-Funktionen werden in Abhängigkeit von der Anforderungsrate dargestellt. Die PFS_{avg}-Werte verschiedener Architekturen nehmen bei der höheren Anforderungsrate zu. Es ist gezeigt, dass der Verlauf der 1oo1-Architektur über den Verläufen der 1oo2- und 2oo2-Architektur liegt. Das bedeutet auch, dass die Verfügbarkeit einer 1oo1-Architektur kleiner ist als die Verfügbarkeit der 1oo2- oder 2oo2-Architektur. Dagegen hat die 2oo2-Architektur eine niedrigere Ausfallwahrscheinlichkeit aufgrund des Spurious-Trips bzw. höhere Verfügbarkeit im Vergleich zur 1oo1- und 1oo2-Architektur.

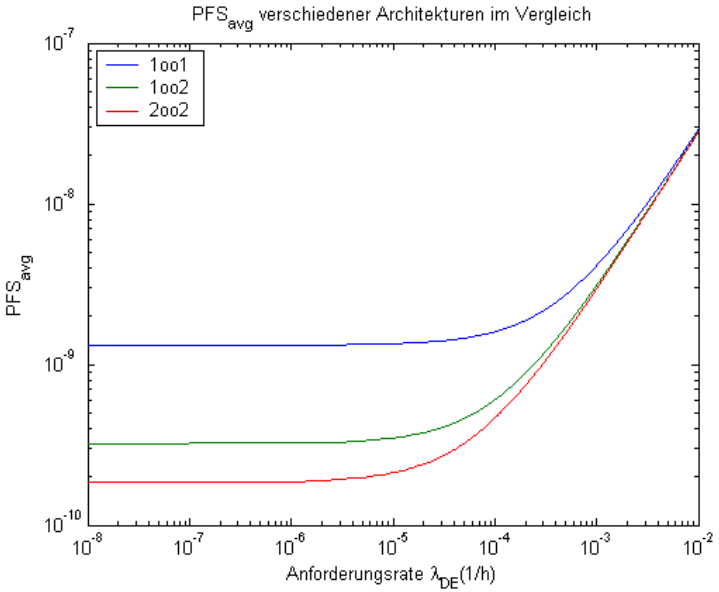

Abbildung 6.21: PFS_{avg} verschiedener Architekturen in Abhängigkeit von λ_{DE}

In der Abbildung 6.22 ist der Vergleich der PFS_{avg}-Funktionen in Abhängigkeit der Anforderungsdauer verschiedener Architekturen für die Betriebsart mit hoher Anforderungsrate von $\lambda_{DE} = 10^{-3}$ gezeigt. Für die Betriebsart mit niedriger Anforderungsrate $\lambda_{DE} = 10^{-8}$ wird der Vergleich der PFS_{avg}-Funktionen in Abhängigkeit der Anforderungsdauer verschiedener Architekturen in Abbildung 6.23 dargestellt. Im Allgemeinen, sowohl bei Betriebsart mit hoher Anforderungsrate als auch bei der Betriebsart mit niedriger Anforderungsrate, liegen die PFS_{avg}-Werte der 1oo1-Architektur über den PFS_{avg}-Werten der 1oo2- und 2oo2-Architektur. Das bedeutet, dass die 2oo2-Architektur im Vergleich zur 1oo1- und 1oo2-Architektur eine größere Verfügbarkeit hat. Bei der Betriebsart mit hoher Anforderungsrate sind die Differenzen zwischen den PFS_{avg}-Funktionen kleiner als bei der Betriebsart mit niedriger Anforderungsrate.

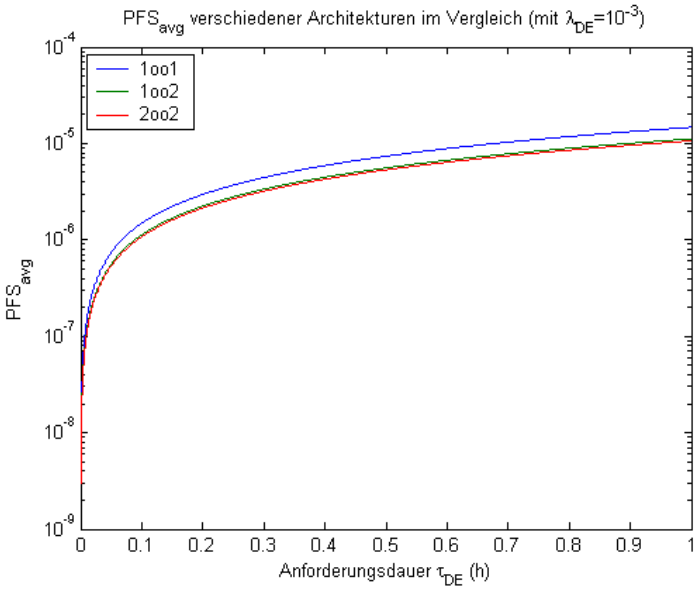

Abbildung 6.22: PFS_{avg} verschiedener Architekturen mit $\lambda_{DE} = 10^{-3}$

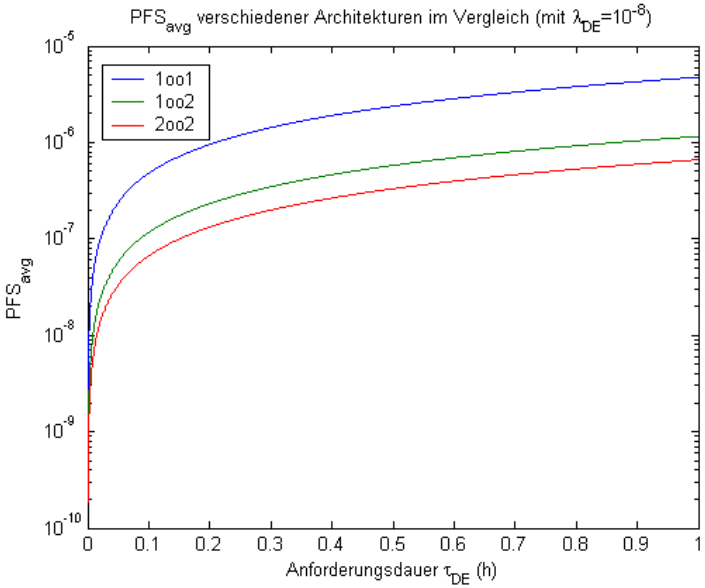

Abbildung 6.23: PFS_{avg} verschiedener Architekturen mit $\lambda_{DE} = 10^{-8}$

In Abbildung 6.24 werden die *STR*-Funktionen verschiedener Architekturen im Vergleich dargestellt. Die *STR*-Funktionen sind in Abhängigkeit der Anforderungsrate. Bei Betriebsart mit hoher Anforderungsrate (Abbildung 6.24), liegen die *STR*-Werte von drei Architekturen nah beieinander. Die Differenz zwischen *STR*-Werte wird bei der Betriebsart mit niedriger Anforderungsrate vergrößert, wenn die Anforderungsrate verkleinert wird. Der *STR*-Wert einer 2oo2-Architektur ist am kleinsten im Vergleich zu 1oo1- und 1oo2-Architektur. Das heißt, ein System mit 2oo2-Architektur fällt selten aufgrund des Spurious-Trips aus, da die Verfügbarkeit dieser Architektur größer als bei der 1oo1- und 1oo2-Architektur ist.

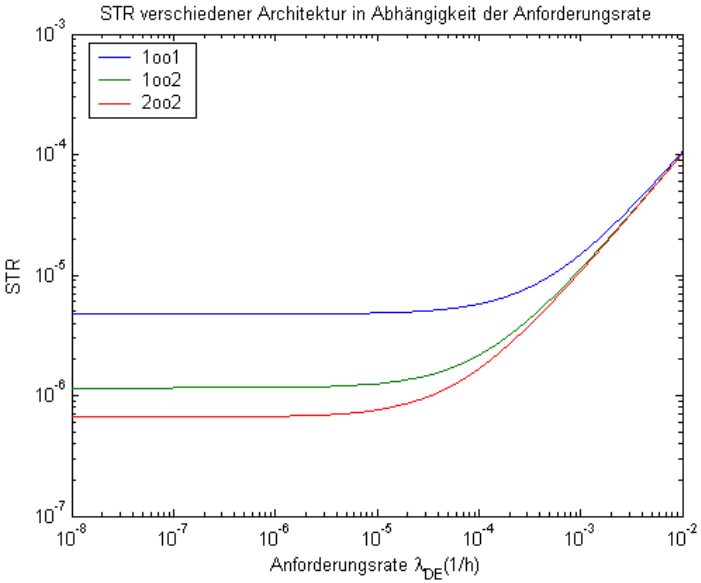

Abbildung 6.24: STR verschiedener Architekturen in Abhängigkeit von λ_{DE}

Die Abbildung 6.25 und Abbildung 6.26 (Vergrößerung von der Abbildung 6.25) zeigen die $MTTF_{Spurious}$-Funktionen der verschiedenen Architekturen in Abhängigkeit von Anforderungsrate. Die $MTTF_{Spurious}$-Funktionen bei allen Architekturen sind abfallend bei der Betriebsart mit hoher Anforderungsrate. Aber bei der Betriebsart mit niedriger Anforderungsrate bleiben die $MTTF_{Spurious}$-Funktionen fast unverändert.

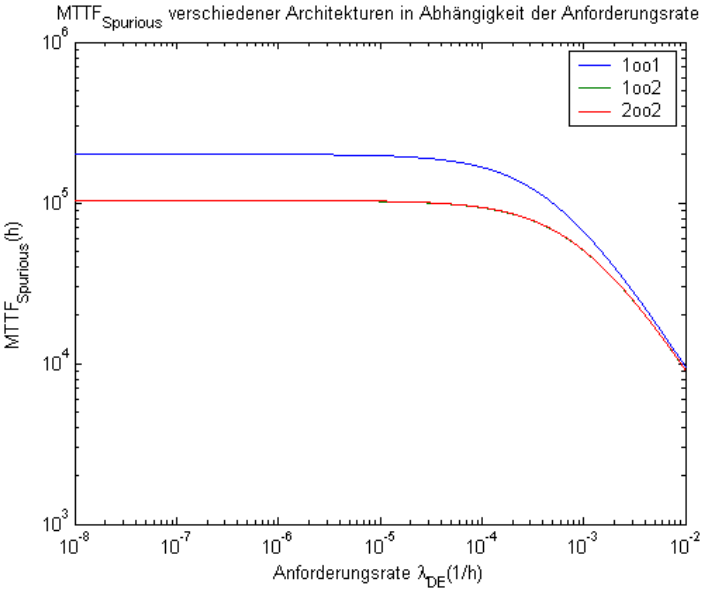

Abbildung 6.25: Funktion $MTTF_{Spurious}(\lambda_{DE})$ verschiedener Architekturen (1)

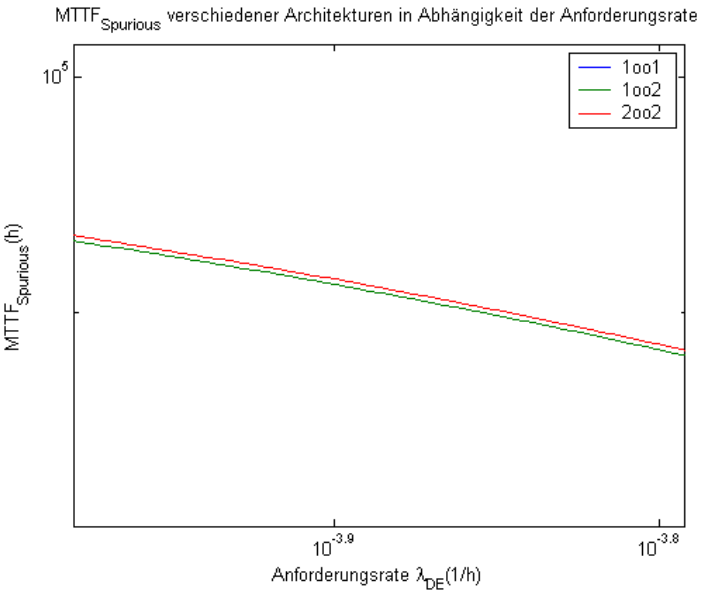

Abbildung 6.26: Funktion $MTTF_{Spurious}(\lambda_{DE})$ verschiedener Architekturen (2)

6.3 Resultierende Ergebnisse und herkömmliche Verfahren im Vergleich

Die Ergebnisse der STR-Funktionen, die sich aus den Berechnungen dieser Arbeit ergeben, werden mit den Werten aus herkömmlichen Verfahren in diesem Kapitel verglichen. Da die STR-Formeln in den herkömmlichen Verfahren nicht von der Anforderungsrate und Anforderungsdauer abhängig sind, werden diese als Funktionen in Abhängigkeit vom DC-Faktor[79] dargestellt. Die Abbildung 6.27 und Abbildung 6.28 stellen zuerst die STR-Funktionen verschiedener Architekturen in Abhängigkeit vom DC-Faktor nach der Norm ANSI/ISA-TR84.00.02-2002 [06] dar. Die STR-Werte bei allen Systemen nehmen zu, wenn der DC-Faktor größer wird. Die Rate des Spurious-Trips STR der 1oo2-Architektur ist am größten und von der 2oo4-Architektur am kleinsten, wenn alle Architekturen miteinander verglichen werden. Das bedeutet auch, dass die Verfügbarkeit bei der 1oo2-Architekur am kleinsten und bei 2oo4-Architektur am größten ist. Aus den Abbildungen wird die folgende Ungleichung gegeben:

$$STR_{1oo2} > STR_{1oo1} > STR_{2oo3} > STR_{2oo2} > STR_{2oo4} \qquad \textbf{(6.12)}$$

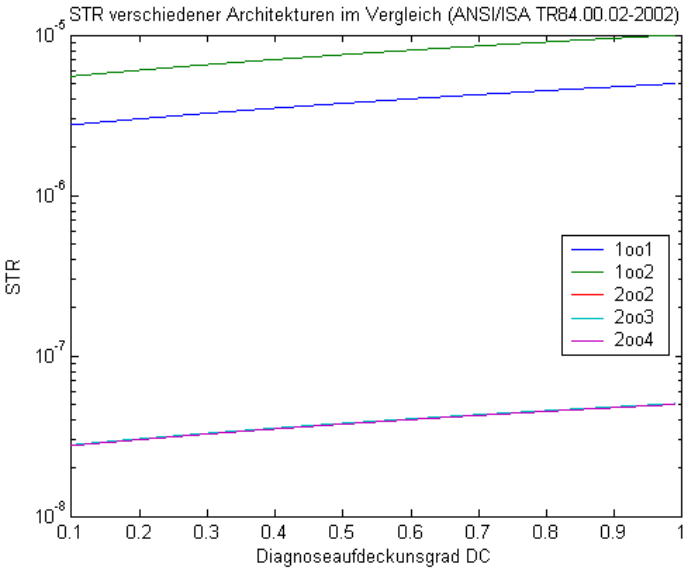

Abbildung 6.27: STR verschiedener Architekturen nach ANSI/ISA-TR84 [06]

[79] DC-Faktor: engl. Diagnose coverage factor (Diagnoseaufdeckungsgrad)

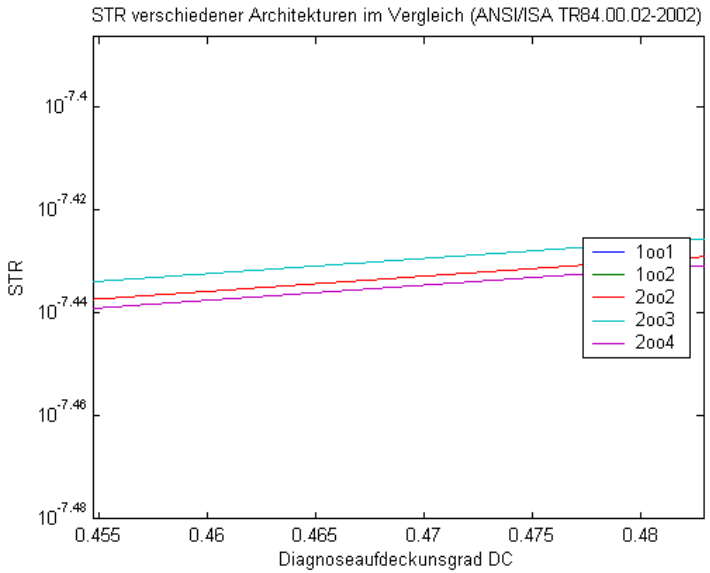

Abbildung 6.28: STR verschiedener Architekturen nach ANSI/ISA-TR84 [06]

Während die *STR*-Werte in der Norm ANSI/ISA-TR84.00.02-2002 [06] nach der Zunahme des *DC*-Faktors zunehmen, nehmen die *STR*-Werte in der PDS-Methode [86], [87], [88] dagegen wieder ab (Abbildung 6.29). Bei der PDS-Methode weist die *STR*-Funktion der 1oo2-Architektur die schlechtesten Werte auf und liegt im Graph in einem Wertebereich von 10^{-7} bis 10^{-5}. Die *STR*-Kurve der 2oo2-Architektur hat die kleinsten Werte. Das heißt, mit der PDS-Methode ist die Verfügbarkeit der 1oo2-Architektur am schlechtesten und die Verfügbarkeit der 2oo2-Architektur am besten im Vergleich zu anderen Architekturen. Nicht wie bei der Berechnung, die aus der Norm ANSI/ISA-TR84.00.02-2002 [06] abgeleitet wird, ist der *STR*-Wert der 2oo4-Architektur bei der PDS-Methode größer als der *STR*-Wert der 2oo2-Architektur. Die Ungleichung (6.13) ergibt sich dann:

$$STR_{1oo2} > STR_{1oo1} > STR_{2oo3} > STR_{2oo4} > STR_{2oo2} \qquad \textbf{(6.13)}$$

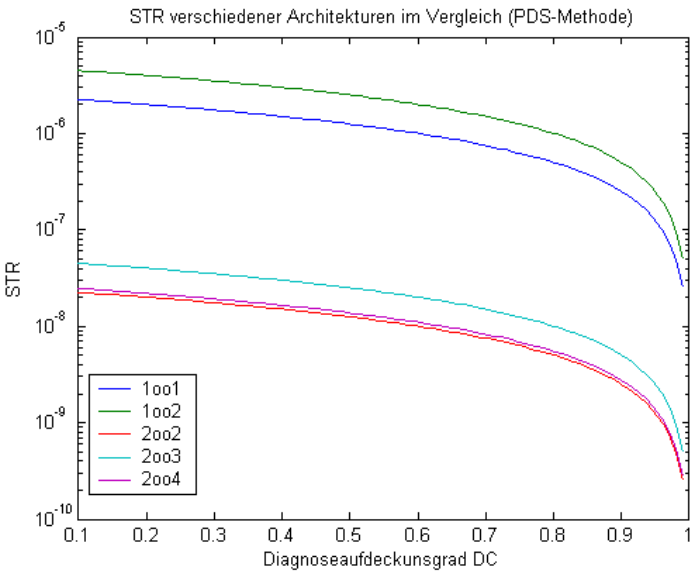

Abbildung 6.29: STR verschiedener Architekturen nach PDS [86], [87], [88]

Die Abbildung 6.30 stellt die *STR* verschiedener Architekturen im Vergleich nach Machleidt & Litz [69] dar. Bei dieser Methode bleiben die *STR*-Funktionen konstant nach der Veränderung des *DC*-Faktors. Bei diesem Verfahren hat die 1oo2-Architektur einen größeren *STR*-Wert als die 1oo1- und 2oo3-Architektur. Eine Ungleichung wird aus der Berechnung gemäß dem Verfahren von Machleidt & Litz [69] wie folgt ausgegeben:

$$STR_{1oo2} > STR_{1oo1} > STR_{2oo3} \tag{6.14}$$

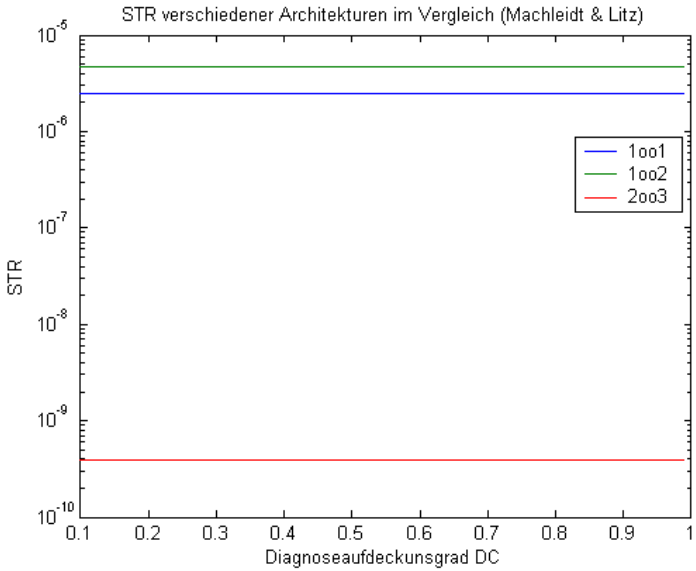

Abbildung 6.30: STR verschiedener Architekturen nach Machleidt & Litz [69]

In der Abbildung 6.31, Abbildung 6.32, Abbildung 6.34, und Abbildung 6.35 werden die *STR*-Funktionen der 1oo1-, 1oo2- und 2oo2-Architekturen nach der Norm ANSI/ISA-TR84.00.02-2002 [06], PDS-Methode [86], [87], [88] und Berechnungsformeln aus dieser Arbeit miteinander verglichen. Alle Funktionen werden auch in Abhängigkeit vom Diagnose-aufdeckungsgrad (*DC*-Faktor) dargestellt. Der Vergleich zwischen den *STR*-Werten für eine 1oo1-Architektur zeigt kleinen signifikanten Unterschied, bei der Berechnung des Wertes nach RBD-Methode oder Markov-Modell sowie aus der Norm ANSI/ISA-TR84.00.02-2002 [06]. Die *STR*-Funktionen sind bei diesen drei Methoden ansteigend. Der *STR*-Wert einer 1oo1-Architektur nach RBD-Methode ist größer bzw. schlechter als bei anderen Methoden. Die *STR*-Funktion aus dem Verfahren von Machleidt & Litz [69] bleibt konstant. Aus der PDS-Methode [86], [87], [88] ist die *STR*-Funktion absteigend, wenn der *DC*-Faktor größer wird. Dieser Unterschied liegt daran, dass bei der PDS-Methode nur der sichere unerkannte Fehler in Betracht von Spurious-Trip gezogen wird. Ist der *DC*-Faktor größer, ist der Anteil von sicherem unerkanntem Fehler kleiner.

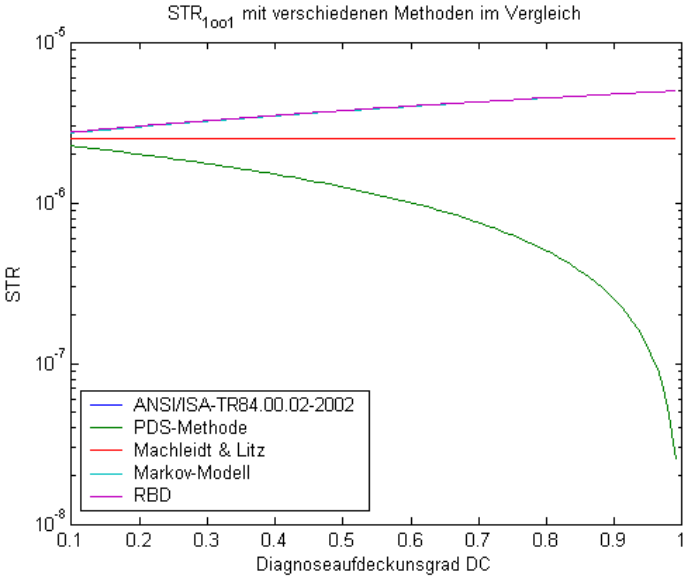

Abbildung 6.31: STR 1oo1-Architektur mit verschiedenen Methoden (1)

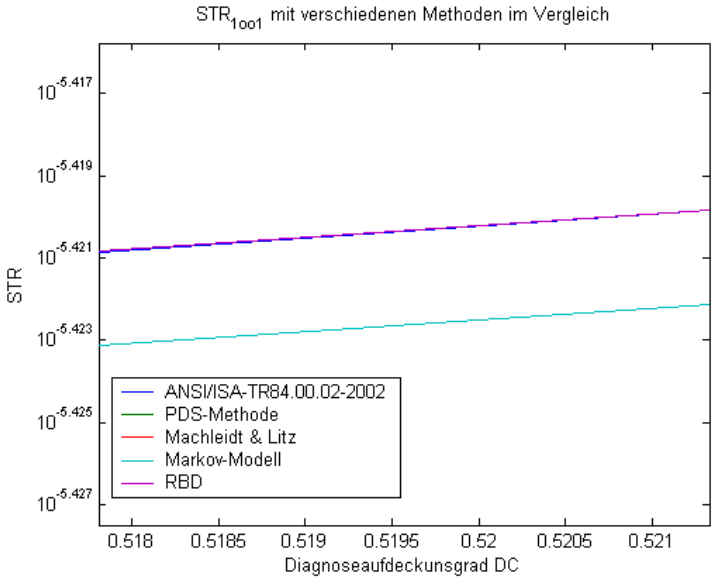

Abbildung 6.32: STR 1oo1-Architektur mit verschiedenen Methoden (2)

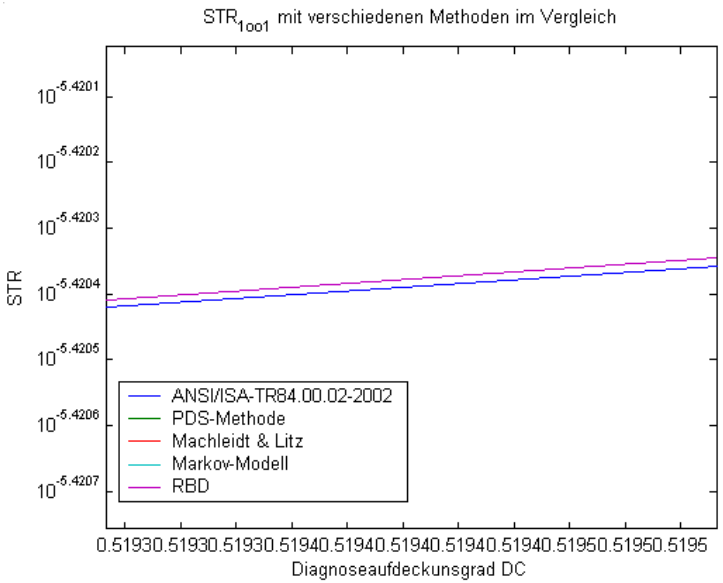

Abbildung 6.33: STR 1oo1-Architektur mit verschiedenen Methoden (3)

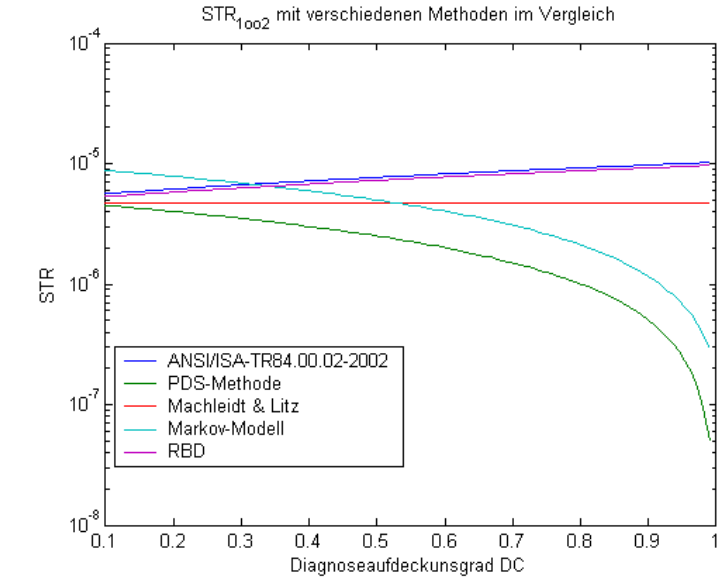

Abbildung 6.34: STR 1oo2-Architektur mit verschiedenen Methoden

Der Vergleich zwischen den *STR*-Werten nach dem Markov-Modell und anderen Methoden (Markov-Modell und herkömmlichen Verfahren (Tabelle 3.2)) zeigt, dass der *STR* einer 1oo2-Architektur nach dem Markov-Modell (Abbildung 6.34) größer bzw. schlechter ist als bei anderen Methoden, wenn der *DC*-Faktor klein ist. Ähnlich wie bei der PDS-Methode [86], [87], [88] ist die *STR*-Funktion bei dem Markov-Modell absteigend, wenn der *DC*-Faktor größer wird. Dagegen sind die *STR*-Funktionen aus dem RBD und aus der Norm ANSI/ISA-TR84.00.02-2002 [06] ansteigend, wenn der *DC*-Faktor größer wird.

Die *STR*-Funktionen werden für die 2oo2-Architektur (Abbildung 6.35) dargestellt. Aus der Abbildung 6.35 wird es gezeigt, dass der *STR*-Wert nach dem Markov-Modell, der aus dieser Arbeit hergeleitet wurde, größer als bei anderen Methoden ist. Ähnlich wie bei der 1oo2-Architektur sind die *STR*-Funktionen bei dem Markov-Modell und bei der PDS-Methode [86], [87], [88] absteigend, wenn der *DC*-Faktor größer wird. Dagegen sind die *STR*-Funktionen aus dem RBD und aus der Norm ANSI/ISA-TR84.00.02-2002 [06] ansteigend, wenn der *DC*-Faktor größer wird. Die Differenzen zwischen den *STR*-Funktionen sind größer als bei der 1oo2-Architektur.

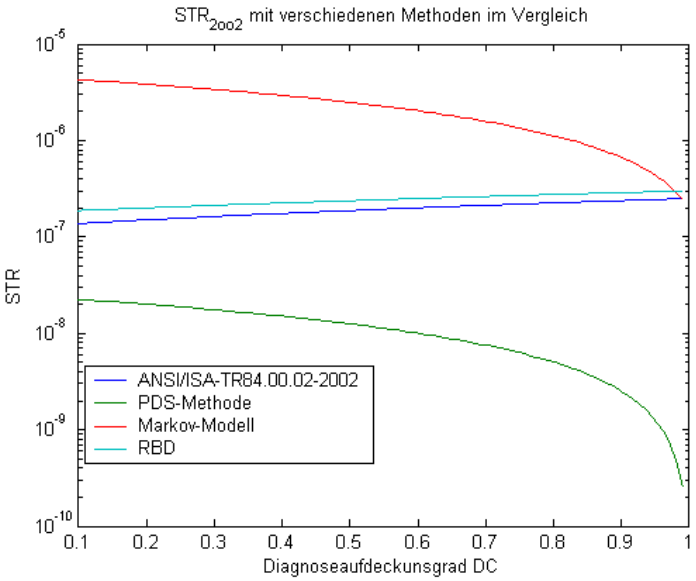

Abbildung 6.35: STR 2oo2-Architektur mit verschiedenen Methoden

6.4 Zusammenfassung

In diesem Kapitel wurden die STR-, PFS_{avg}- und $MTTF_{Spurious}$-Werte unter den Voraussetzungen des neuen Ansatzes, der in Kapitel 3.3 beschrieben wurde, durch vorgegebene Beispiele berechnet. Die Berechnungen wurden für verschiedene Architekturen anhand der Blockdiagramm-Methode im Abschnitt 6.1 und anhand des Markov-Modells im Abschnitt 6.2 durchgeführt. Die aus den Beispielen resultierenden Ergebnisse wurden in verschiedenen Diagrammen dargestellt und miteinander verglichen. Die Ergebnisse aus dem Blockdiagramm (Abschnitt 6.1) haben gezeigt, dass bei allen Architekturen die STR-Funktionen ansteigend und die $MTTF_{Spurious}$-Funktionen abfallend nach der Zunahme der Anforderungsrate sind. Die STR-Werte einer 2oo2-Architektur sind am kleinsten im Vergleich zu anderen Architekturen. Dagegen sind die $MTTF_{Spurious}$-Werte einer 2oo2-Architektur am größten im Vergleich zu anderen Architekturen. Das bedeutet, aus der Sicht der Verfügbarkeit ist die 2oo2-Architektur besser als andere Architekturen. Die PFS_{avg}-Werte haben sich geringfügig verändert, sodass sich die PFS_{avg}-Funktionen fast konstant aussehen, wenn die Anforderungsrate oder Anforderungsdauer sich ändert. Dies ist bei dem Markov-Modell anders.

Wie die Ergebnisse aus dem Blockdiagramm (Abschnitt 6.1) haben die Ergebnisse aus dem Markov-Modell (Abschnitt 6.2) auch gezeigt, dass bei allen Architekturen die STR-, PFS_{avg}-Funktionen ansteigend und die $MTTF_{Spurious}$-Funktionen abfallend bei Zunahme der Anforderungsrate sind. Allerdings haben die Ergebnisse aus dem Markov-Modell (Abschnitt 6.2) kleine Abweichungen zu den Ergebnissen aus dem Blockdiagramm (Abschnitt 6.1), da in der STR-, PFS_{avg}-, $MTTF_{Spurious}$-Funktionen der Anteil des gefährlich unerkannten Fehlers enthalten ist. Mit dem Markov-Modell wurde auch gezeigt, dass die STR-Werte einer 2oo2-Architektur immer kleiner als die STR-Werte einer 1oo2-Architektur sind. Die PFS-Werte sind bei der 2oo2-Architektur auch kleiner als bei der 1oo2-Architektur (Abbildung 6.21). Das bedeutet, dass die 2oo2-Architektur eine größere Verfügbarkeit als die 1oo2-Architektur hat. Die $MTTF_{Spurious}$-Werte haben bei allen betrachteten Architekturen einen minimalen Unterschied, sodass die $MTTF_{Spurious}$-Funktionen bei diesen Architekturen fast gleich dargestellt wurden.

Außerdem wurden die Ergebnisse, die mit der in dieser Arbeit hergeleiteten Gleichungen berechnet wurden, mit den Ergebnissen, die mit den herkömmlichen Verfahren berechnet wurden, miteinander verglichen. Allerdings wurden die Funktionen in Abhängigkeit des Diagnoseaufdeckungsgrads miteinander verglichen, da die STR-Formeln aus den herkömmlichen Verfahren nicht von der Anforderungsrate oder Anforderungsdauer abhängig sind. Mit den Diagrammen aus Kapitel 6 wurde gezeigt, dass die STR-Werte einer 1oo1- und 2oo2-Architektur nach dem Markov-Modell am kleinsten und die STR-Werte einer 1oo2-Architektur im Vergleich zu anderen Methoden am größten sind. Aus der Analyse der Ergebnisse lässt sich schlussfolgern, dass mit dem Markov-Modell die Bewertung der Sicherheits-

parameter des Spurious-Trips detaillierter und die PFS_{avg}-, STR-, $MTTF_{Spurious}$-Funktionen auch in Abhängigkeit der Anforderungsrate und Anforderungsdauer besser dargestellt werden. Wegen des schnellen Zuwachs der Anzahl der Zustände bei einer $koon$-Architektur, besonders wenn $n \geq 3$ ist, ist die Analyse mit der Blockdiagramm-Methode besser geeignet.

7 Abschließende Betrachtung und Ausblick

Die sicherheitsbezogenen Systeme führen die Sicherheitsfunktion(en) aus, um das Gesamtsystem auf Anforderung in den sicheren Zustand zu bringen [18]. Allerdings ist die Ausführung der Sicherheitsfunktion nicht immer der beste Fall für das Gesamtsystem, besonders bei einem Ausfall aufgrund des Spurious-Trips. Bei manchen Systemen kann dieser Ausfall auch gefährlich sein, besonders bei Systemen, die hoch verfügbar sein müssen. Daher ist es wichtig die Fehler aufgrund des Spurious-Trips zu betrachten. Aus diesem Grund ist die Arbeit mit dem Thema „*Beitrag zur Betrachtung von* $MTTF_{Spurious}$ *-Modellierung im Zusammenhang mit dem internationalen Sicherheitsstandard IEC 61508*“ entstanden.

Die Betriebsart mit niedriger Anforderungsrate und die Betriebsart mit hoher Anforderungsrate werden in der Norm IEC 61508 definiert. Für jede Betriebsart wird die Ausfallwahrscheinlichkeit aufgrund von gefährlichen Fehlern anders berechnet. Bei der Betriebsart mit niedriger Anforderungsrate ist der PFD - und bei der Betriebsart mit hoher Anforderungsrate ist der PFH -Wert zu berechnen. Aus diesen Werten wird der Sicherheits-Integritätslevel eines Sicherheitssystems bewertet. Wird bei einem SIS eine hohe Sicherheitswahrscheinlichkeit gefordert, sind diese Kenngrößen (PFD , PFH und SIL) notwendigerweise zu berechnen. Wird bei einem SIS eine hohe Verfügbarkeitswahrscheinlichkeit gefordert, werden die Parameter wie PFS_{avg} , STR und $MTTF_{Spurious}$ berechnet. Mit dem PFS -Wert wird der STL [80] gebildet, um die Ausfallkosten aufgrund des Spurious-Trips eines Systems zu ermitteln. Bei den herkömmlichen Verfahren wird die Berechnung für sowohl Betriebsart mit niedriger Anforderungsrate als auch Betriebsart mit hoher Anforderungsrate mit den gleichen Verfahren durchgeführt und die Unterschiede der beiden Betriebsarten werden außer Betracht gelassen. Die Unterschiede bei der Betrachtung, für die Betriebsart mit niedriger Anforderungsrate und der Betrachtung der Betriebsart mit hoher Anforderungsrate, benötigen folgenden Eigenschaften:

- Definition des sicheren Zustands
- Sequenz von Schutzschicht
- Art des Hazardous Event, wenn SIS und Subsequenz von Schutzschicht bei Anforderung ausfallen
- Teststrategie für SIS: funktionaler Test und Diagnose-Test
- Potentielle Konsequenz von Spurious-Aktivierung auf EUC und SIS-Komponente
- Anforderungsrate und Anforderungsdauer

Aus den genannten Gründen kann es nicht stimmen, dass die Formeln zur Berechnung des PFS_{avg} -, STR - und $MTTF_{Spurious}$ -Werts nur in von den Raten der sicheren Fehler [86], [87], [88], [69] oder auch von den Raten der gefährlichen erkannten Fehlern [06] abhängig sind. Da

[80] STL: Spurious-Trip Level [47]

die Einflussfaktoren zur Ermittlung der Parameter für die beiden Betriebsarten unterschiedlich streng sind, können die STR-Werte bei beiden Betriebsarten nicht gleich sein.

Aufgrund der obigen gegebenen Unterschiede zwischen Betriebsart mit niedriger Anforderungsrate und Betriebsart mit hoher Anforderungsrate wurde in dieser Arbeit ein neuer Ansatz gewählt und bewiesen. Der neue Ansatz fokussiert auf die Auswirkung von Anforderungsrate und Anforderungsdauer sowie die Berechnung der Sicherheitsparameter von Fehlern aufgrund des Spurious-Trips wie STR, PFS_{avg} und $MTTF_{Spurious}$. Die Aussage wurde bereits in dieser Arbeit durch die Analyse des Blockdiagramms und des Markov-Modells bewiesen. Die daraus gebildeten Funktionen werden als Funktionen in Abhängigkeit von Anforderungsrate und Anforderungsdauer dargestellt. Daraus folgen die unterschiedlichen Ergebnisse für die Betriebsart mit niedriger Anforderungsrate und Betriebsart mit hoher Anforderungsrate. Die Ergebnisse aus dem Blockdiagramm zeigen kleine Abweichungen zu den Ergebnissen aus dem Markov-Modell. Durch die Beispiele, die in Kapitel 6 gegeben wurden, wurden die hergeleiteten Formeln angewendet und dessen Ergebnisse miteinander verglichen. Als Beispiele wurden die Sicherheitsparameter von Fehlern aufgrund des Spurious-Trips wie STR, PFS_{avg} und $MTTF_{Spurious}$ für 1oo1-, 1oo2- und 2oo2-Architektur berechnet. Die Verläufe in den Diagrammen aus Kapitel 6 zeigen, dass mit steigender Anforderungsrate oder Anforderungsdauer die STR- und PFS_{avg}-Werte proportional ansteigen. Je größer STR- und PFS_{avg}-Werte umso geringer ist die Prozessverfügbarkeit eines Sicherheitssystems. Daraus folgt, dass je geringer die Prozessverfügbarkeit ist, umso höher sind die Ausfallkosten eines Sicherheitssystems aufgrund des Spurious-Trips. Die PFS- und STR-Funktionen in Abhängigkeit der Anforderungsrate sind bei der Betriebsart mit niedriger Anforderungsrate streng monoton steigend und die $MTTF_{Spurious}$-Funktion streng monoton fallend. Bei der Betriebsart mit hoher Anforderungsrate sind die Funktionen steigend oder fallend aber nicht streng monoton. Diese Betrachtung ist nicht in den herkömmlichen Verfahren miteinbezogen worden. Danach wurden die STR-Funktionen, die aus dieser Arbeit geliefert wurden, mit den Ergebnissen, die aus den herkömmlichen Verfahren hergeleiteten Formeln berechnet werden, verglichen. Die STR-Funktionen wurden in Abhängigkeit des DC-Faktors dargestellt. Aus den dargestellten Diagrammen wurde gezeigt, dass die aus dieser Arbeit gelieferten Ergebnisse kleine Abweichungen zu den aus der Norm ANSI/ISA TR84.00.02-2002 [06] berechneten Ergebnisse aufweisen. Der Grund ist, dass die Anforderungsrate und Anforderungsdauer nicht in den Gleichungen aus der Norm ANSI/ISA TR84.00.02-2002 [06] in Betracht gezogen werden. Anschließend wurde der neue Ansatz, der zunächst für die Hardwarearchitekturen 1oo1, 1oo2 und 2oo2 hergeleitet wurde, verallgemeinert und ist somit für die Berechnung der $koon$-Architektur in beiden Betriebsarten anwendbar.

Allerdings wurde der neue Ansatz in dieser Arbeit nur für Sicherheitssysteme mit dem Ruhestromprinzip betrachtet. Weiterhin könnten noch interessante Punkte und Aspekte für die zukünftige Forschung gegeben werden:

- Betrachtung der Fehler aufgrund des Spurious-Trips für komplexere Sicherheitssystem-Architekturen, beispielsweise wie 2oo3, 2oo4 usw... mit dem Ruhestromprinzip, wobei das Markov-Modell verwendet wird, um diese Architekturen zu analysieren.
- Betrachtung der Fehler aufgrund des Spurious-Trips für Sicherheitssysteme mit dem Arbeitsstromprinzip.
- Betrachtung der Fehler aufgrund des Spurious-Trips für Sicherheitssysteme, wobei die Ausfallrate nicht konstant ist.
- Die Einflüsse von Anforderungsrate und Anforderungsdauer auf die Kosten aufgrund des Spurious-Trips und Lebenszykluskosten.
- Die Einflüsse von Diagnoseaufdeckungsgrad und Teststrategie auf die Sicherheitsparameter des Spurious-Trips.
- Zusammenhang zwischen Spurious-Trip Rate und Hardzard Rate. Daraus könnte ein Zusammenhang zwischen Spurious-Trip Rate und *PFD* oder *PFH* folgen.

Anhang

A Markov-Kette

Eine Familie $(X_t(\omega) \in S : t \in T)$ von reellen Zufallsvariablen über den Wahrscheinlichkeitsraum (Ω, A, p) heißt stochastischer Prozess oder zufällige Funktion. T wird meist als diskrete oder stetige (oder kontinuierliche) Zeit interpretiert und wird als Parameterraum bezeichnet. S ist der Zustandsraum und $X_t(\omega)$ ist der Zustand des Prozesses bei der Zeit t [98].

Ein stochastischer Prozess lässt sich als Funktion (siehe Gleichung (A.1)) der beiden Variablen t und ω auffassen:

$$\begin{aligned} X_t(\omega): \quad & T \times \Omega \to S \\ & (t, \omega) \mapsto X_t(\omega) \end{aligned} \tag{A.1}$$

- Bei einem festen $t_0 \in T$ und variablen ω ist $X_{t_0}(\omega)$ eine Zufallsvariable.
- Bei einem festen $\omega_0 \in \Omega$ und variablen t ist $X_t(\omega_0)$ eine deterministische Funktion von T mit Werten in $\Re$ oder Pfad (Trajektorie) eines stochastischen Prozesses.

Der stochastische Prozess heißt diskret, wenn der Zustandsraum S (Wertebereich der Zufallsvariablen) eine endliche oder eine abzählbar unendliche Menge ist, ansonsten ist der Prozess stetig. Ein diskreter Prozess lässt sich in einen diskreten stochastischen Prozess mit diskreter Zeit (T abzählbar, also T enthält nur ganzzahlige Elemente) und diskreten stochastischen Prozess mit stetiger Zeit (T enthält reelle Elemente) unterteilen. Ein stetiger stochastischer Prozess mit diskreter Zeit unterscheidet sich dagegen mit stetigem stochastischem Prozess mit stetiger Zeit.

Ein stochastischer Prozess heißt stetig[81], rechtsseitig stetig bzw. linksseitig stetig, wenn alle Pfade des Prozesses die entsprechenden Eigenschaften haben.

Ein stochastischer Prozess heißt Markov-Prozess, genau dann, wenn:

$\forall t_1 < t_2 < .... < t_n < t_{n+1} \subset T$ und $\forall s_1, s_2, ..., s_n, s_{n+1} \subset S$ gilt:

$$p(X_{t_{n+1}} = s_{n+1} \mid X_{t_1} = s_1, X_{t_2} = s_2, ..., X_{t_n} = s_n) = p(X_{t_{n+1}} = s_{n+1} \mid X_{t_n} = s_n) \tag{A.2}$$

Für alle Borel[82] messbare Menge B gilt:

---

81 Eine Funktion f heißt in einem Punkt a stetig, wenn: $\lim_{x \to a} f(x) = f(a)$

82 Borelmenge ist eine Menge, die aus Elementen der kleinsten σ-Algebra B besteht, wobei die σ-Algebra alle offenen Menge enthält [09], [72].

$$p(X_t \in B \mid X_{t_1} = s_1, ..., X_{t_n} = s_n) = p(X_t \in B \mid X_{t_n} = s_n) \quad \textbf{(A.3)}$$

Der Markov-Kern ist für jedes x ein Wahrscheinlichkeitsmaß auf der σ-Algebra der Borel messbaren Mengen und wird durch folgende Gleichung dargestellt:

$$p_{t_1, t_2}(B \mid x) = p(X_{t_1} \in B \mid X_{t_2} = x) \quad \textbf{(A.4)}$$

Der Markov-Kern übernimmt die Rolle der Übergangsmatrix.

Im Allgemeinen kann der Markov-Prozess nach Parameterraum und Zustandsraum nach folgender Tabelle klassifiziert werden:

Tabelle 7.1: Klassifizierung der Markov-Prozesse [80]

Parametermenge	**Zustandsraum**	
	diskret	stetig
diskret	(Zeit-) diskrete Markov-Kette	(Zeit-) diskreter Markov-Prozess
stetig	(Zeit-) stetige Markov-Kette	(Zeit-) stetiger Markov-Prozess

In dieser Arbeit wird nur auf den Markov-Prozess mit diskretem Raum, der oft auch Markov-Kette genannt wird, eingegangen.

A.1 Markov-Kette mit diskreter Zeit

Definition 1: Die Markov-Kette ist ein Markov-Prozess mit diskreten Zeitparametern und meistens auch endlichem oder abzählbarem Zustandsraum[83] S [80], [98], [I05].

Die wichtigste Eigenschaft von Markov-Ketten ist, dass das Verhalten des Systems nur vom aktuellen Zustand und nicht von den vorigen Zuständen abhängig ist. Das heißt:

$\forall t_1 < t_2 < .... < t_n < t_{n+1} \subset T$ und $\forall i, j, ..., s_k \subset S$, $k \in \aleph$ gilt:

$$\begin{aligned} &p(X_{t_{n+1}} = j \mid X_{t_n} = i, X_{t_{n-1}} = i_{n-1}, ...X_{t_0} = i_0, \forall k \in \aleph : X_k = s_k) \\ &= p(X_{t_{n+1}} = j \mid X_{t_n} = i) \end{aligned} \quad \textbf{(A.5)}$$

Die Gleichung (A.5) heißt Markov-Eigenschaft oder Markov-Bedingung.

Eine Markov-Kette ist über die Anfangsverteilung, die Übergangswahrscheinlichkeiten und durch ihren Zustandsraum [I05] bestimmt.

Satz 1: (Verallgemeinerte Markov-Eigenschaft)

Für $n, m \in \aleph_0$, $k_1, ..., k_m, i_1, ..., i_{n-1}, i \in S$ und $p(X_0 = i_0, ..., X_n = i_n) > 0$ gilt:

[83] Der Zustandsraum ist die Menge aller Zustände, die das System annehmen kann. Diese Zustände sind voneinander unabhängig, weil sich das System nur in genau einem Zustand befindet. Ist das System diskret in Zeit und Raum, wird es als stochastische Kette bezeichnet[I05].

$$p(X_{n+1} = k_1,...,X_{n+m} = k_m \mid X_0 = i_0, ..., X_{n-1} = i_{n-1}, X_n = i)$$
$$= p(X_{n+1} = k_1,...,X_{n+m} = k_m \mid X_n = i) \qquad \textbf{(A.6)}$$
$$= p(X_1 = k_1,...,X_m = k_m \mid X_0 = i)$$

A.1.1 Übergangswahrscheinlichkeit und Übergangsmatrix

Definition 2: Die Wahrscheinlichkeit, dass eine Markov-Kette zur Zeit $t \in T$ in einem Zustand $i \in S$ ist, heißt (transiente) Zustandswahrscheinlichkeit von i zur Zeit t:

$$p_i^{(t)} = p(X_t = i), \qquad i \in S \qquad \textbf{(A.7)}$$

Definition 3: Der Vektor $\mathbf{p}^{(t)} = (p_i^{(t)}, \quad i \in S)$ der Zustandswahrscheinlichkeiten heißt Wahrscheinlichkeitsverteilung oder Verteilung der Markov-Kette zur Zeit t.

Der Zeilenvektor $\mathbf{p}^{(0)} := (p_i^{(0)})$ wird als die Anfangsverteilung der Markov-Kette bezeichnet. Diese Anfangsverteilung ist ein stochastischer Verktor[84]. Die Summe der Elemente des Vektors $\mathbf{p}^{(0)}$ ist genau eins, d.h. $\sum_{i=1}^{n} p_i = 1$.

Bemerkung:

- Die zeitliche Entwicklung einer diskreten Markov-Kette verläuft in Schritten.
- Der Zustand zur Zeit $t \in \aleph$ ist der Zustand nach t Übergängen, d.h. nach t Schritten.

Definition 4: Die Übergangswahrscheinlichkeit zur Zeit t_n vom Zustand i in den Zustand j zur Zeit t_{n+1} wird als:

$$p_{ij}(t_n, t_{n+1}) = p(X_{t_{n+1}} = j \mid X_{t_n} = i) \qquad \textbf{(A.8)}$$

bezeichnet [I05].

Sind die Übergangswahrscheinlichkeiten nicht von t_n abhängig (d.h., die Übergangswahrscheinlichkeiten sind stationär), ist die Markov-Kette homogen, d.h. $p_{ij}(t_n, t_{n+1}) = p_{ij}$ (z.B.: die Brown'sche Bewegung[85] ist homogen.). Bei einer solchen Markov-Kette wird das Systemverhalten nur durch den aktuellen Zustand bestimmt und nicht durch eine absolute Zeit.

---

[84] Ein Zeilenvektor $z = (z_1, z_2, ..., z_k)$ heißt stochastischer Vektor, wenn $z_i \geq 0$ für $1 \leq i \leq k$ und $\sum_{i=1}^{k} z_i = 1$

[85] Die Brownsche Bewegung ist die Wärmebewegung von Teilchen (Atom oder Molekül) in Flüssigkeiten und Gasen, wobei deren Ausmaß temperaturabhängig ist [09], [56], [105].

$\forall t_0 < t_1 < .... < t_k$

$$p(X_{t_k} = i_k \mid X_{t_{k-1}} = i_{k-1} \mid,..., X_{t_0} = i_0) = p(X_{t_k} = i_k \mid X_{t_{k-1}} = i_{k-1}) \quad \textbf{(A.9)}$$

Die Übergangswahrscheinlichkeit ist eine bedingte Wahrscheinlichkeit, weil das System sich erst im Zustand i befinden muss. Ist ein Übergang von i nach j nicht möglich, dann ist $p_{ij} = 0$. Die Summe der Übergangswahrscheinlichkeit von einem Zustand aus, muss genau eins ergeben, weil irgendein Zustand eintreten muss, d.h., für jedes i gilt: $\sum_{j=1}^{n} p_{ij} = 1$. Die Übergangswahrscheinlichkeit nach n-Schritten wird wie folgt dargestellt:

$$p_{ij}^{(n)} = p(X_n = j \mid X_0 = i) = p(X_{k+n} = j \mid X_k = i) \quad \textbf{(A.10)}$$

$$p_{ij}^{(1)} = p_{ij} \quad \textbf{(A.11)}$$

$$p_{ij}^{(0)} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \quad \textbf{(A.12)}$$

Die Wahrscheinlichkeit p_{ii} ist die Wahrscheinlichkeit, dass der Prozess im Zustand i verbleibt und lässt sich nach folgender Gleichung im Zusammenhang mit der Übergangswahrscheinlichkeit von Zustand i zu Zustand j beschreiben:

$$p_{ii} = 1 - \sum_{i \neq j} p_{ij} \quad \textbf{(A.13)}$$

Definition 5: Da die Markov-Kette homogen ist, ist p_{ij} nicht von t_n abhängig. Die Matrix: $\mathbf{P} := (p_{ij})_{i,j=1}^{k}$ wird Übergangsmatrix oder Übergangskern der Markov-Kette genannt. Die Übergangsmatrix $\mathbf{P}$ ist eine stochastische Matrix[86]. Der 1-Schritt der Übergangsmatrix wird nach der Gleichung (A.14) definiert:

$$\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1s_0} \\ p_{21} & p_{22} & \cdots & p_{2s_0} \\ \vdots & \vdots & \cdots & \vdots \\ p_{s_0 1} & p_{s_0 2} & \cdots & p_{s_0 s_0} \end{bmatrix} \quad \textbf{(A.14)}$$

Definition 6: Für $\forall n \geq 0$ und $i, j \in S$ wird der n-Schritt der Übergangsmatrix wie folgt dargestellt:

---

[86] Eine reelle Matrix $m \times n$-Matrix $A = (a_{ij})_{i=1,...,m;\, j=1,...,n}$ heißt stochastische Matrix, wenn alle Zeilenvektoren $(a_{ij})_{j=1}^{n}, 1 \leq i \leq m$ von der Matrix stochastische Vektoren sind.

$$\mathbf{P}^{(n)} = (p(X_n = j \mid X_0 = i))_{ij} = (p_{ij}^{(n)}) \tag{A.15}$$

Die Wahrscheinlichkeitsverteilung nach n-Schritten ist:

$$(p(X_n = 1,..., p(X_n = s_0)) = (p(X_0 = 1,..., p(X_0 = s_0)) \cdot \begin{bmatrix} p_{11} & \cdots & p_{1s_0} \\ \vdots & \cdots & \vdots \\ p_{n1} & \cdots & p_{s_0 s_0} \end{bmatrix}^n \tag{A.16}$$

$$\Leftrightarrow \mathbf{p}^{(n)} = \mathbf{p}^{(0)} \cdot \mathbf{P}^n \tag{A.17}$$

Bemerkung:

- Ist der Zustandsraum unendlich, dann ist die Übergangsmatrix unendlich.
- Ist der Zustandsraum S endlich, dann ist die Übergangsmatrix $|S| \times |S|$ endlich.

A.1.2 Chapman-Kolmogorow Gleichung

Definition 7: Die Chapman-Kolmogorow Gleichung stellt die Übergangswahrscheinlichkeit von i nach j als Summe möglicher Wege mit Zwischenzuständen k dar und wie folgt definiert:

$$p(X_n = j \mid X_0 = i) = \sum_{k \in S} p(X_n = j \mid X_l = k) p(X_l = k \mid X_0 = i) \tag{A.18}$$

Definition 8: Im Allgemeinen wird die Chapman-Kolmogorov Gleichung für $\forall n, m = 0, 1, 2,....$ wie folgt definiert:

$$p_{ij}^{(n+m)} = \sum_{k \in S} p_{ik}^{(n)} p_{kj}^{(m)} \tag{A.19}$$

Beweis:

$$\begin{aligned} p_{ij}^{(n+m)} &= p(X_{n+m} = j \mid X_0 = i) \\ &= \sum_{k \in S} p(X_{n+m} = j \mid X_0 = i, X_k = k) \cdot p(X_k = k \mid X_0 = i) \\ &= \sum_{k \in S} p(X_{n+m} = j \mid X_k = k) \cdot p(X_k = k \mid X_0 = i) \\ &= \sum_{k \in S} p_{ik}^{(n)} p_{kj}^{(m)} \end{aligned}$$

Aus dem obigen Beweis gelten die folgenden Gleichungen:

$$\mathbf{P}^{(n+m)} = \mathbf{P}^{(n)} \cdot \mathbf{P}^{(m)} \tag{A.20}$$

$$\mathbf{P}^{(n+1)} = \mathbf{P}^{(n)} \cdot \mathbf{P} \tag{A.21}$$

Satz 2: Sei $(X_n)_{n\in\aleph}$ eine homogene Markov-Kette mit minimalem Zustandsraum $S = \{1,2,.....,k\}$ auf dem Wahrscheinlichkeitsraum (Ω, A, p) mit Anfangsverteilung p_{i_0} und Übergangsmatrix $\mathbf{P}$. Dann gilt für $n \in \aleph_0$ und $i_0, i_1, ..., i_n \in S$ [I05]:

$$p(X_0 = i_0,\ X_1 = i_1, ...,\ X_n = i_n) = p_{i_0} \cdot p_{i_0 i_1} \cdot ... \cdot p_{i_{n-1} i_n} \tag{A.22}$$

Satz 3: Sei $(X_n)_{n\in\aleph}$ eine homogene Markov-Kette mit minimalem Zustandsraum $S = \{1,2,.....,k\}$ auf dem Wahrscheinlichkeitsraum (Ω, A, p) mit Anfangsverteilung p_{i_0} und Übergangsmatrix $\mathbf{P}$. Dann gilt für $n \in \aleph_0$ [I05]:

$$p(X_n = j) = \sum_{i=1}^{k} p_i (\mathbf{P}^n)_{ij} \quad \text{für } \forall j \in S \tag{A.23}$$

Satz 4:

$$p(X_n = i_n \mid X_0 = i_0) = \sum_{\text{alle Pfade von } i_0 \text{ nach } i_n} p_{i_0 i_1} \cdot p_{i_1 i_2} \cdot .... \cdot p_{i_{n-1} i_n} \tag{A.24}$$

Satz 5:

$$p(X_n = i_n) = \sum_{i_0 \in S} \sum_{\text{alle Pfade von } i_0 \text{ nach } i_n} p_{i_0} \cdot p_{i_0 i_1} \cdot .... \cdot p_{i_{n-1} i_n} \tag{A.25}$$

A.1.3 Klassifikation der Zustände einer Markov-Kette

Definition 9: (Eintrittszeit)

Sei $\{X_n, n \geq 0\}$ eine Markov-Kette mit diskretem Zustandsraum S. Für $B \subset S$ ist die Eintrittszeit definiert als:

$$\tau_B = \inf\{n \geq 0 : X_n \in B\} \tag{A.26}$$

Die Eintrittszeit eines Zustands i wird als τ_i bezeichnet.

Definition 10: (Erreichbarer Zustand)

Ein Zustand $j \in S$ heißt erreichbar von einem Zustand $i \in S$, wenn es $n \in \aleph$-Schritte gibt, so dass: $p_{ij} = p(X_n = j \mid X_0 = i) > 0$, Schreibweise: $i \to j$.

Definition 11: (Verbundener Zustand)

Zwei Zustände $i, j \in S$ heißen verbunden, wenn $i \to j$ und $j \to i$ (Abkürzung $i \leftrightarrow j$). Die Beziehung $\leftrightarrow$ ist eine Äquivalenzrelation und zerlegt S in Äquivalenzklassen.

Definition 12: (Wesentlicher Zustand)

Ein Zustand $i \in S$ heißt wesentlich, wenn i aus allen von i erreichbaren Zuständen j ebenfalls erreichbar ist, d.h. wenn gilt $\forall j : i \to j \Rightarrow j \to i$, anderenfalls heißt i unwesentlich.

Definition 13: (Absorbierender Zustand)

Ein Zustand $i \in S$ heißt absorbierend, falls kein anderer Zustand von i aus erreicht werden kann, d.h. $p_{ii} = 1$ [80] [98].

Eine Menge von Zuständen heißt absorbierend, wenn die Kette mit Wahrscheinlichkeit 1 darin verbleibt.

Definition 14: (Periodischer/aperiodischer Zustand)

Ein Zustand $i \in S$ heißt periodisch mit der Periode d, falls d der größte gemeinsame Teiler aller der Zahlen $n \in \mathrm{Z}^+$ ist, für die $p_{ii}^{(n)} > 0$ gilt. Ist $d = 1$, heißt der Zustand i aperiodisch. Falls für alle Zahlen $n \in \mathrm{Z}^+$ $p_{ii}^{(n)} = 0$ gilt, wird $d = \infty$ gesetzt.

Definition 15: (Transienter/rekurrenter Zustand)

Ein Zustand $i \in S$ heißt rekurrent, falls der Prozess bei Start in i mit Wahrscheinlichkeit 1 nach i zurückkehrt, andernfalls ist i transient (die Wahrscheinlichkeit < 1) [80] [98]. Ist j transient, dann gilt $\forall i : \sum_{n=1}^{\infty} p_{ij}^{(n)} < \infty$ und daraus folgt $\lim_{n \to \infty} p_{ij}^{(n)} = 0$. j ist rekurrent nur wenn $\sum_{n=1}^{\infty} p_{ij}^{(n)} = \infty$.

Die Rekurrenzwahrscheinlichkeit ist die Wahrscheinlichkeit, nach Verlassen eines Zustands i jemals wieder zurückzukehren und ist gegeben durch [95]:

$$f_{ii} := \sum_{i=0}^{\infty} f_{ii}^{(n)} = 1 \qquad \textbf{(A.27)}$$

Für $\forall i, j \in S$ seien:

$$f_{ij}^{(n)} := p(X_n = j, X_{n-1} \neq j, ..., X_1 \neq j \mid X_0 = i), \qquad n \geq 2$$
$$f_{ij}^{(1)} := p_{ij} \tag{A.28}$$
$$f_{ij}^{(0)} := 0$$

Die $f_{ij}^{(n)}$ ist die Wahrscheinlichkeit dafür, dass der Zustand j, ausgehend vom Zustand i, zur Zeit n zum ersten Mal erreicht wird. Dann ist $f_{ii}^{(n)}$ eine Wahrscheinlichkeitsverteilung[87] für die erste Rückkehrzeit. Sei μ_i der Erwartungswert dieser Rückkehrzeit und wird wie folgt definiert:

$$\mu_i := \sum_{n=1}^{\infty} n f_{ii}^{(n)} \tag{A.29}$$

Ein rekurrenter Zustand i heißt positiv rekurrent, wenn $\mu_i < \infty$ gilt. Wenn $\mu_i = \infty$ ist, heißt i null-rekurrent, d.h. $\lim_{n\to\infty} p_{ij}^{(n)} = 0$. Sind alle Zustände einer homogenen Markov-Kette rekurrent bzw. positiv rekurrent, heißt die Markov-Kette selbst rekurrent bzw. positiv rekurrent.

Satz 6:

Für $i,\ j \in S$ gelten die folgenden Gleichungen:

$$p_{ii}^{(n)} = \sum_{k=0}^{n} f_{ii}^{(k)} p_{ii}^{(n-k)}, \qquad n \geq 1 \tag{A.30}$$

$$p_{ij}^{(n)} = \sum_{k=0}^{n} f_{ij}^{(k)} p_{jj}^{(n-k)}, \qquad n \geq 0 \text{ und } i \neq j \tag{A.31}$$

A.1.4 Grenzverhalten der Übergangswahrscheinlichkeit einer homogenen Markovschen Kette

Für eine irreduzibel[88], aperiodisch[89] und rekurrente Markov-Kette gilt:

---

[87] Sei Ω eine nichtleere Menge und $A \subseteq P(\Omega)$ eine σ-Algebra. $P(\mathrm{A})$ ist die Wahrscheinlichkeit von Ereignissen $\mathrm{A} \in A$. Dann ist die Abbildung [31]:

$P : A \to [0, \infty]$

$\mathrm{A} \mapsto P(\mathrm{A})$

eine Wahrscheinlichkeitsverteilung auf (Ω, A, P) wenn:

- $P[\bigcup_{i=1}^{\infty} \mathrm{A}_i] = \sum_{i=1}^{\infty} P[\mathrm{A}_i]$
- $P(\Omega) = 1$

[88] Eine homogene Markov-Kette heißt irreduzibel, wenn nur eine Äquivalenzklasse vorhanden ist, d.h. alle Zustände kommunizieren, also ist jeder Zustand von jedem anderen Zustand erreichbar [80].

$$\lim_{n\to\infty} p_{ij}^{(n)} = \begin{cases} \frac{1}{\mu_i} & \text{falls} \quad \mu_i < \infty \\ 0 & \text{sonst} \end{cases} \tag{A.32}$$

Für eine irreduzible und rekurrente Markov-Kette mit der Periode $d > 1$ gilt:

$$p_{ii}^{(nd+k)} = 0 \qquad \forall k \in \{1, 2, ..., d-1\}$$

$$\lim_{n\to\infty} p_{ij}^{(nd)} = \begin{cases} \frac{d}{\mu_i} & \text{falls} \quad \mu_i < \infty \\ 0 & \text{sonst} \end{cases} \tag{A.33}$$

Unter allgemeineren Voraussetzung gilt immer noch:

$$\lim_{n\to\infty} \frac{1}{n+1} \sum_{i=0}^{n} p_{ij}^{(n)} = \begin{cases} \frac{1}{\mu_i} & \text{falls} \quad \mu_i < \infty \\ 0 & \text{sonst} \end{cases} \tag{A.34}$$

Eine homogene Markov-Kette mit endlichem Zustandsraum S hat:

- evtl. transiente Zustände
- mindestens einen rekurrenter Zustand
- keine null-rekurrenten Zustände
- keine wesentlichen transienten Zustände.

Definition 16: Eine Markov-Kette heißt regulär, wenn für irgendein $n > 0$ die Matrix $\mathbf{P}^n$ nur positive Elemente enthält.

Bemerkung: Jede reguläre Markov-Kette ist ergodisch, aber nicht jeder ergodische Markov-Kette ist regulär.

Beispiel A.1.1: Die folgende Matrix enthält Null-Element, ist aber regulär, da $\mathbf{P}^3$ nur positive Elemente besitzt:

$$\mathbf{P} = \begin{bmatrix} \frac{1}{2} & \frac{1}{3} & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 \end{bmatrix} \qquad \mathbf{P}^2 = \begin{bmatrix} \frac{5}{12} & \frac{11}{18} & \frac{1}{2} \\ \frac{5}{12} & \frac{5}{18} & \frac{1}{2} \\ \frac{1}{6} & \frac{1}{9} & 0 \end{bmatrix} \qquad \mathbf{P}^3 = \begin{bmatrix} \frac{37}{72} & \frac{55}{108} & \frac{5}{12} \\ \frac{25}{72} & \frac{43}{108} & \frac{5}{12} \\ \frac{5}{36} & \frac{5}{54} & \frac{1}{6} \end{bmatrix}$$

$$\forall (i, j) \in S^2 \; \exists n \in \aleph : p_{ij}^{(n)} > 0$$

[89] Eine Markov-Kette ist aperiodisch, wenn die Beziehung $d_i = 1$ für alle $i \in S$ gilt, wobei der größte gemeinsame Teiler d_i alle $n \in \aleph$ mit $p_{ii}^{(n)} > 0$ die Periode von i ist und periodisch wenn $d_i > 1$. Sie heißt ergodisch, falls sie irreduzibel und aperiodisch ist und alle Zustände positiv rekurrent sind [80].

Definition 17: (Grenzwertsatz für ergodische Markov-Kette) Sei eine homogene Markov-Kette irreduzibel und aperiodisch. Dann sind alle Zustände genau positiv rekurrent und die Markov-Kette besitzt das lineare Gleichungssystem:

$$\begin{aligned} p_j &= \sum_{i \in S} p_i p_{ij} \quad \forall j \in S \\ \sum_{i \in S} p_i &= 1 \end{aligned} \tag{A.35}$$

mit dem Zeilenvektor $\mathbf{p} = (p_j,\ j \in S)$ eine eindeutige, strikt positive Lösung $(p_j > 0, \forall j \in S)$ (stationäre Verteilung[90]) und es gilt:

$$p_j = \frac{1}{\mu_j} = \lim_{n \to \infty} p_{ij}^{(n)} \qquad \forall i, j \in S \tag{A.36}$$

Satz 7: Für eine irreduzibel aperiodische Markov-Kette mit $S = \{0, 1, 2, ..., j, ..., n\}$ existiert eine eindeutige stationäre Verteilung $\mathbf{p} = (p_i)_{i \in S}$ und es gilt:

$$\begin{aligned} \mathbf{P}^{\infty} = \lim_{n \to \infty} \mathbf{P}^{(n)} &= \begin{bmatrix} \lim_{n \to \infty} p_{11}^{(n)} & \lim_{n \to \infty} p_{12}^{(n)} & \dots & \lim_{n \to \infty} p_{1n}^{(n)} \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ \lim_{n \to \infty} p_{n1}^{(n)} & \lim_{n \to \infty} p_{n2}^{(n)} & \dots & \lim_{n \to \infty} p_{nn}^{(n)} \end{bmatrix} \\ &= \begin{bmatrix} p_1 & p_2 & \dots & p_n \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ p_1 & p_2 & \dots & p_n \end{bmatrix} \\ &= \mathbf{p} \end{aligned} \tag{A.37}$$

und:

$$\lim_{n \to \infty} \mathbf{p}^{(n)} = \mathbf{p} \tag{A.38}$$

Ist die homogene Markov-Kette mit $S = \{0, 1, ..., m\}$ irreduzibel aber nicht aperiodisch, gelten folgende Gleichungen:

$$\lim_{n \to \infty} \frac{1}{n+1} \sum_{\nu=0}^{n} p_{ij}^{(\nu)} = p_j \tag{A.39}$$

---

[90] Die Verteilung $\mathbf{p}$ heißt stationäre Verteilung einer Markov-Kette, wenn es $\mathbf{p}^{(n)} = \mathbf{p}^{(n+1)} = \mathbf{p}$ gilt, wobei: $\mathbf{p}^{(n)} = (p_j^{(n)})_{j \in S} = (\mathbf{P}(X_n = j))_{j \in S}$

$$\lim_{n\to\infty}\frac{1}{n+1}\sum_{\nu=0}^{n} p(X_\nu = j) = p_j \qquad \textbf{(A.40)}$$

Eine homogene Markov-Kette heißt ergodisch, wenn die Grenzwerte $\lim_{n\to\infty} p_{ij}^{(n)} = p_j$ unabhängig von $i \in S$ existieren, wobei: $p_j > 0, \forall j \in S, \sum_{j\in S} p_j = 1$.

Bemerkung:

Die Grenzverteilung ist immer stationär, aber die Umkehrung gilt allgemein nicht, d.h., es gibt Prozesse, die stationäre Verteilung hat aber keine Grenzverteilung, z.B.:

$\mathbf{P} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ hat keine Grenzverteilung, weil: $\mathbf{P}^{(2n)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ und $\mathbf{P}^{(2n+1)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Deswegen existieren keine Grenzwerte $\lim_{n\to\infty} p_{ij}^{(n)}$. Aber das Gleichungssystem:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \quad , \qquad p_1 + p_2 = 1 \quad , \qquad p_1,\ p_2 \geq 0$$

hat eine eindeutige Lösung $\begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix}$. Das ist die einzige stationäre Verteilung.

A.1.5 Absorbierende Markov-Kette

Eine Markov-Kette heißt absorbierend, wenn ihr Zustandsraum mindestens einen absorbierenden Zustand hat und wenn jeder Zustand mit Wahrscheinlichkeit > 0 in einen der absorbierenden Zustände gelangen kann [80], [98]. Das bedeutet auch, dass eine absorbierende Markov-Kette nicht irreduzibel und somit auch nicht ergodisch ist.

Sei $\{\underbrace{1, 2, ..., r}_{\text{nicht absorbierenden Zuständen}}, \underbrace{r+1, r+2, ..., r+s}_{\text{absorbierenden Zuständen}}\}$, wird die Übergangsmatrix P einer absorbierenden Markov-Kette in folgender kanonischen Form dargestellt:

$$P = \begin{bmatrix} Q & A \\ 0 & I \end{bmatrix} \qquad \textbf{(A.41)}$$

wobei:

- Die (r, r)-Matrix Q die Übergänge zwischen den nicht absorbierenden (transienten) Zuständen ist.
- Die (r, s)-Matrix A die Übergänge zwischen den nicht absorbierenden und den absorbierenden Zuständen ist.
- Die 0-Matrix 0 die Übergänge zwischen den absorbierenden und den nicht absorbierenden Zuständen ist.

- Die Einheitsmatrix I die Übergänge zwischen den absorbierenden Zuständen (da ein Übergang aus einem absorbierenden Zustand nicht möglich ist) ist.

Weil die Markov-Kette absorbierend ist, gilt für alle Zeilensummen der Matrix Q^n: $\sum_{j=1}^{r} q_{ij} < 1$

für $\forall i = 1, ..., r$

Dann gilt für die Zeilensummennorm von Q^n: $\left\| Q^n \right\| = \max_{i=1, ..., r} \sum_{j=1}^{s} q_{ij} < 1$

Also sind die Beträge aller Eigenwerte von Q kleiner als 1 und $I - Q$ ist invertierbar. Für die Inverse N der Matrix $I - Q$ gilt:

$$N = (I - Q)^{-1} = I + Q + Q^2 + ... \qquad \textbf{(A.42)}$$

Die Inverse N heißt Fundamentalmatrix der absorbierenden Markov-Kette und wird als Neumannsche Reihe von Q dargestellt. Strebt Q^n gegen 0, wird die Kette mit Wahrscheinlichkeit 1 absorbiert.

A.1.6 Absorptionswahrscheinlichkeit und Absorptionszeit

Definition 18: Sei b_{ij} die Wahrscheinlichkeit, dass die Markov-Kette im transienten Zustand i startet und im absorbierenden Zustand j endet. Dann wird die Absorptionswahrscheinlichkeit nach [80] wie folgt definiert:

$$\mathbf{B} = (\mathbf{I} - \mathbf{Q})^{-1}\mathbf{A} = \mathbf{NA} = \sum_{k} n_{ik} a_{kj} \qquad \textbf{(A.43)}$$

wobei:

$\mathbf{A}$: die Übergänge von transienten zu absorbierenden Zuständen und

$\mathbf{Q}$: die Übergänge zwischen transienten Zuständen sind

Definition 19: Sei m_{ij} die mittlere Anzahl von Schritten, die gebraucht werden, um den Zustand j zum ersten Mal zu erreichen, wenn der Prozess im Zustand i gestartet ist. Diese Werte ergeben sich $\forall j$, wenn aus j ein absorbierender Zustand gemacht wird, dann gilt: $m_{ij} = \tau_i$. Sei $\boldsymbol{\tau}$ der Spaltenvektor von τ_i, dann gilt die Gleichung:

$$\boldsymbol{\tau} = \mathbf{Nc} \qquad \textbf{(A.44)}$$

wobei:

$\mathbf{c}$: Vektor enthält nur 1.

A.2 Markov-Kette mit kontinuierlicher Zeit

Definition 20: Ein Semi-Markov-Prozess ist ein stochastischer Prozess, dessen Zustände sich wie bei einer Markov-Kette mit diskreter Zeit verändern, der aber in jedem Zustand für einen zufällig verteilten Zeitraum verweilt [98].

Definition 21: Eine Markov-Kette mit kontinuierlicher Zeit ($t \in [0,\infty)$) ist ein Semi-Markov-Prozess, dessen Übergangszeiten exponentiell verteilt sind [98].

Alternative Definition: Eine Markov-Kette mit kontinuierlicher Zeit (stetige Markov-Kette, $t \in [0,\infty)$) ist ein Markov-Prozess mit $\forall n \geq 0$, $\forall t > s > s_n > ... > s_0 > 0$ gilt:

$$p(X(t) = j \mid X(s) = i,\ X(s_n = i_n, ..., X(s_0) = i_0) = p(X(t) = j \mid X(s) = i) \tag{A.45}$$

Für beliebige $i,\ j \in S$ wird die Übergangswahrscheinlichkeit wie folgt dargestellt:

$$p_{ij}(s,t) = p(X(t) = j \mid X(s) = i) \tag{A.46}$$

Eine stetige Markov-Kette heißt homogen, wenn die Übergangswahrscheinlichkeit $p_{ij}(s,t)$ nur von der Differenz $t - s \geq 0$ abhängt. D.h.:

$$\begin{aligned} p_{ij}(t+s) &= p(X(t+s) = j \mid X(s) = i) \\ &= p(X(t) = j \mid p(X(0) = i) \\ &= p_{ij}(0,t) = p_{ij}(t) \end{aligned} \tag{A.47}$$

Bemerkung: $p_{ij}(t)$ entspricht $p_{ij}^{(t)}$ (t-schrittige Übergangswahrscheinlichkeit) bei Markov-Ketten mit diskreter Zeit.

Für die Übergangswahrscheinlichkeit von Zustand i nach Zustand j im Zeitraum t gelten die Gleichung (A.48) und die Voraussetzung (A.49):

$$\sum_{j \in S} p_{ij}(t) = 1 \qquad , \ p_{ij}(t) \geq 0 \tag{A.48}$$

$$p_{ij}(t) = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases} \tag{A.49}$$

Die Verteilung zum Zeitpunkt t ist:

$$p_i(t) = p(X(t) = i) \tag{A.50}$$

Analog wie bei der Markovschen Kette mit diskreter Zeit wird die Matrix $\mathbf{P}(t)$ definiert durch:

$$\mathbf{P}(t) = (p_{ij}(t))_{i,j\in S} = \begin{bmatrix} p_{11}(t) & \dots & p_{1s_0}(t) \\ \vdots & \dots & \vdots \\ p_{s_0 1}(t) & \dots & p_{s_0 s_0}(t) \end{bmatrix} \tag{A.51}$$

Die Wahrscheinlichkeitsverteilung nach der Zeit t ist:

$$\left(p_1(t), ..., p_{s_0}(t)\right) = \left(p_1(0), ..., p_{s_0}\right) \cdot \begin{bmatrix} p_{11}(t) & \dots & p_{1s_0}(t) \\ \vdots & \dots & \vdots \\ p_{s_0 1}(t) & \dots & p_{s_0 s_0}(t) \end{bmatrix} \tag{A.52}$$

A.2.1 Chapman-Kolmogorov-Gleichungen

Satz 8: Für $\forall n \in \aleph,\ \forall 0 \le t_0 < t_1 < ... < t_n \in \Re^+,\ i_0, i_1, ..., i_n \in S$ [80]:

$$p(X(t_n) = i_n, ..., X(t_1) = i_1 \mid X(t_0) = i_0) = p_{i_0 i_1}(t_1 - t_0) \cdot ... \cdot p_{i_{n-1} i_n}(t_n - t_{n-1}) \tag{A.53}$$

$$\begin{aligned} &p(X(t_n) = i_n, ..., X(t_1) = i_1, X(t_0) = i_0) \\ &= p(X(t_0) = i_0) \cdot p_{i_0 i_1}(t_1 - t_0) \cdot ... \cdot p_{i_{n-1} i_n}(t_n - t_{n-1}) \end{aligned} \tag{A.54}$$

$$p_{ij}(t_1, t_2) = \sum_{k\in S} p_{ik}(t_1) p_{kj}(t_2) \tag{A.55}$$

In Matrixschreibweise wird die Gleichung (A.55) nach der Gleichung (A.56) dargestellt:

$$\mathbf{P}(t_1 + t_2) = \mathbf{P}(t_1)\mathbf{P}(t_2) \tag{A.56}$$

und:

$$\begin{aligned} \mathbf{P}(X(t) = j) &= \sum_{i\in S} \mathbf{P}(X(0) = i) p_{ij}(0,t) \\ &= \sum_{i\in S} \mathbf{P}(X(0) = i) p_{ij}(t) \end{aligned} \tag{A.57}$$

Eine Menge $\{\mathbf{P}(t) : t \ge 0\}$ von Übergangsmatrixen heißt stetige Halbgruppe von Übergangsmatrizen (Transition Semigroup), falls alle darin enthaltenen Matrizen die Chapman-Kolmogorov-Gleichungen erfüllen und:

$$\lim_{t\to 0} \mathbf{P}(t) = \mathbf{P}(0) = \mathbf{I} \tag{A.58}$$

mit $\mathbf{I}$ die Einheitsmatrix ist

Satz 9: Es sei eine homogene Markov-Kette mit kontinuierlicher Zeit mit Übergangsmatrix $\mathbf{P}(t)$. Eine reelle Matrix $\mathbf{\Lambda}$, die die Beziehung erfüllt:

$$e^{\mathbf{\Lambda}t} = \mathbf{P}(t), \qquad t \ge 0 \tag{A.59}$$

wobei:

$$e^{\mathbf{\Lambda}} = \sum_{k=0}^{\infty} \frac{t^k}{k!}\mathbf{\Lambda}(t) = \mathbf{I} + t\mathbf{\Lambda} + \frac{t^2}{2}\mathbf{\Lambda}^2 + \ldots$$
$$= \lim_{n\to\infty}\left(\mathbf{I} + \frac{t^2}{n}\mathbf{\Lambda}\right)^n \qquad \textbf{(A.60)}$$

ist, dann heißt $\mathbf{\Lambda}$ Intensitätsmatrix (Generatormatrix) der homogenen stetigen Markov-Kette.

Falls eine Generatormatrix existiert, wird sie eindeutig bestimmt und wegen der Gleichungen (A.59) und (A.60) gilt:

$$\mathbf{\Lambda} = \lim_{t\to 0}\frac{\mathbf{P}(t) - \mathbf{I}}{t} = \mathbf{P}'(0) \qquad \textbf{(A.61)}$$

Ist $\{\mathbf{P}(t) : t \geq 0\}$ eine stetige Halbgruppe von Übergangsmatrizen einer stetigen Markov-Kette, dann existieren für alle Zustände $i,\ j \in S$ die Grenzwerte:

$$\lambda_{ii} := \lim_{t\to 0}\frac{1 - p_{ii}(t)}{t} = -p_{ii}'(0) \in [0, \infty] \qquad \textbf{(A.62)}$$

$$\lambda_{ij} := \lim_{t\to 0}\frac{p_{ij}(t)}{t} = p_{ij}'(0) \in [0, \infty),\ i \neq j \qquad \textbf{(A.63)}$$

$$\lambda_{ii} = \sum_{i\neq j}\lambda_{ij} \qquad \textbf{(A.64)}$$

In Matrixdarstellung lauten diese Gleichungen wie folgt:

$$\mathbf{P}'(0) = \lim_{t\to 0^+}\frac{\mathbf{P}(t) - \mathbf{I}}{t} = \mathbf{\Lambda} \qquad \textbf{(A.65)}$$

wobei:

$$\mathbf{\Lambda} = \begin{bmatrix} -\lambda_{11} & \lambda_{12} & \cdots & -\lambda_{1n} \\ \lambda_{21} & -\lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{n1} & \lambda_{n2} & \cdots & -\lambda_{nn} \end{bmatrix}$$
$$= \begin{bmatrix} \mathbf{\Lambda}_1 & \mathbf{\Lambda}_2 \\ 0 & \mathbf{\Lambda}_3 \end{bmatrix} \qquad \textbf{(A.66)}$$

wobei:

$\mathbf{\Lambda}_1$: nicht absorbierende Zustände und

$0, \mathbf{\Lambda}_2, \mathbf{\Lambda}_3$: absorbierende Zustände sind

A.2.2 Grenzverhalten der Übergangswahrscheinlichkeiten stetiger homoger Markov-Kette

Satz 10: Es sei $(X_t)_{t\geq 0}$ eine homogene Markov-Kette mit der Generatormatrix Λ sowie $(Y_n)_{n\in\mathbb{N}_0}$ die zugehörige eingebettete Markov-Kette, dann gelten die folgenden Gleichungen.

Ist die Markov-Kette $(Y_n)_{n\in\mathbb{N}_0}$ irreduzibel und positiv rekurrent, dann existiert:

$$\lim_{t\to\infty}\mathbf{P}(t)=\begin{pmatrix}\boldsymbol{\pi}^T\\ \boldsymbol{\pi}^T\\ \vdots\end{pmatrix} \qquad \text{wobei } \boldsymbol{\pi} \text{ die stationäre Verteilung von } (X_t)_{t\geq 0} \text{ ist} \tag{A.67}$$

p ist die stationäre Verteilung von $(X_t)_{t\geq 0}$, wenn $\boldsymbol{\pi}^T\Lambda=0$.

A.2.3 Absorptionswahrscheinlichkeiten und Absorptionszeit

Definition 22: Eine alternative Definition der Absorptionswahrscheinlichkeit und der Absorptionszeit wird in [24], [83], [98] gegeben. Sei:

$\boldsymbol{\pi}_{na}(0)$: die Anfangsverteilung der nicht absorbierenden Zustände

$\boldsymbol{\pi}_{na}(t)$: die Verteilung der nicht absorbierenden Zustände zum Zeitpunkt t

Nach der Gleichung (A.17) und der Gleichung (A.59) wird die Verteilung der nicht absorbierenden Zustände zum Zeitpunkt t wie folgt bestimmt:

$$\boldsymbol{\pi}_{na}(t)=\boldsymbol{\pi}_{na}(0)e^{\Lambda_1 t} \tag{A.68}$$

Die Absorptionswahrscheinlichkeit ist:

$$F(t)=1-\sum\boldsymbol{\pi}_{na}(t) \tag{A.69}$$

$$\begin{aligned}\Rightarrow F'(t)&=(1-\sum\boldsymbol{\pi}_{na}(t))'\\ &=-(\sum\boldsymbol{\pi}_{na}(0)e^{\Lambda_1 t})'\\ &=-\boldsymbol{\pi}_{na}(0)\cdot e^{\Lambda_1 t}\cdot\Lambda_1\cdot \mathrm{e}\end{aligned} \tag{A.70}$$

Daraus folgt die Wahrscheinlichkeitsdichte[91] der Zeit bis zur Absorption:

[91] Die Wahrscheinlichkeitsdichte $f(x)$ ist die erste Ableitung der Verteilungsfunktion $F(x)$: $f(x)=\frac{dF(x)}{x}$. Die Verteilungsfunktion ist wie folgt definiert: $F(x)=\int_{-\infty}^{x}f(x')dx'$

$$\Rightarrow f(t) = F'(t) = \mathbf{p}_{na}(0) \cdot e^{t\Lambda_1}(-\mathbf{\Lambda}_1 \mathrm{e}) \tag{A.71}$$

wobei:

$\mathrm{e} = (1, ..., 1)$

Die Absorptionszeit T_A ist der Erwartungswert der Zeit bis zur Absorption, d.h. die Zeit, die eine Markov-Kette braucht, um in einen absorbierenden Zustand zu gelangen und wird wie folgt berechnet:

$$\begin{aligned} T_A &= \int_0^\infty t \cdot \mathrm{p}_{na}(0) \cdot e^{\Lambda_1 t} \cdot (-\Lambda_1 \mathrm{e}) dt \\ &= -t \cdot \mathrm{p}_{na}(0) \cdot e^{\Lambda_1 t} \cdot \mathrm{e}\Big|_0^\infty + \int_0^\infty \mathrm{p}_{na}(0) \cdot e^{\Lambda_1 t} \cdot \mathrm{e} dt \\ &= \mathrm{p}_{na}(0) \cdot \Lambda_1^{-1} e^{\Lambda_1 t} \cdot \mathrm{e}\Big|_0^\infty \\ &= \mathrm{p}_{na}(0) \cdot (-\Lambda_1)^{-1} \cdot \mathrm{e} \end{aligned} \tag{A.72}$$

Ist die Anfangsverteilung im Zustand 1 konzentriert, so ist:

T_A = Zeilensumme der ersten Zeile von $(-\mathbf{\Lambda}_1)^{-1}$

Da Verweilzeiten[92] in jedem Zustand exponentialverteilt sind, ist die Absorptionszeit gerade Erlang-verteilt[93] mit n Phasen. Vor der Absorption werden genau n Zustände durchlaufen, alle mit gleicher exponentieller Verweilzeitverteilung [80].

[92] Das Verweilen in einem Zustand $i \in S$ lässt sich als Bernoulli-Experiment mit Erfolgswahrscheinlichkeit p_{ii} interpretieren.

[93] Die Erlang-Verteilung ist die Verteilung der Summe von n unabhängigen Exponentialverteilungen mit Parameter $\lambda > 0$.

B Sicherheitsparameter

B.1 Ausfallrate

Die Norm IEC 61508 [48] definiert in Teil 4 einen Ausfall als den Verlust der Fähigkeit eines Systems, die spezifizierte Funktion zu erfüllen. Um die Wahrscheinlichkeit zu berechnen, wird die Ausfallrate $\lambda(t)$ berechnet, wobei das System im Intervall $[t, t+\delta t]$ ausfällt, unter der Bedingung, dass es zur Zeit $t = 0$ eingeschaltet war und im Intervall $[0, t]$ nicht ausgefallen ist. Es gilt:

$$\lambda(t) = \frac{f(t)}{1 - P(t)} \qquad \textbf{(B.1)}$$

wobei:

$$R(t) = 1 - P(t) \qquad \textbf{(B.2)}$$

mit:

- $f(t)$: die Ausfalldichte[94]
- $R(t)$: die Zuverlässigkeitsfunktion
- $P(t)$: die Ausfallwahrscheinlichkeit

Die Ausfallrate $\lambda(t)$ muss in den meisten Fällen experimentell bestimmt werden. Sehr oft, besonders bei elektronischen Komponenten, lässt sich die Ausfallrate in drei Phasen unterteilen: [48], [16], [15], [10]

- Frühausfälle mit fallender Ausfallrate: die Ausfallrate nimmt mit zunehmender Lebensdauer ständig ab.
- Zufallsausfälle mit konstanter Ausfallrate: diese Phase beschreibt das Normalverhalten der Komponenten und ist Basis der Berechnung aller Zuverlässigkeitskenngrößen.
- Verschleißausfälle mit steigender Ausfallrate: diese Phase ist dadurch gekennzeichnet, dass die Ausfallrate aufgrund von Alterungs- und Verschleißerscheinungen wieder ansteigt. Sie ist gleichbedeutend mit dem Ende der Betriebsdauer.

Dieses Verhalten wird durch eine so genannte Wannenkurve (Abbildung B.1) beschrieben.

---

[94] *f(t)* ist die dazugehörige Verteilungsdichte der Verteilungsfunktion *P(t)* und es gilt: $P(t) = \int_{-\infty}^{\infty} f(x)dx$

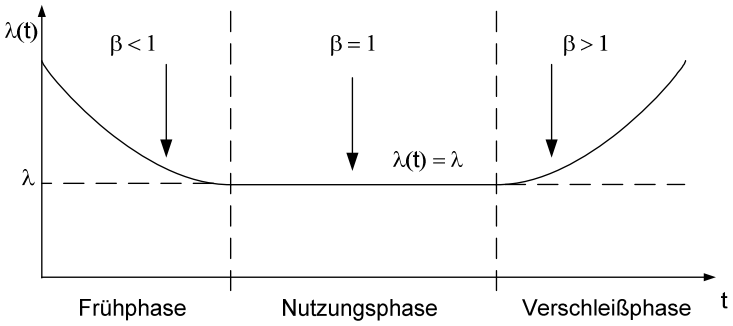

Abbildung B.1: Wannenkurve der Ausfallrate [48], [16], [15], [10]

Die Ausfallrate λ des gesamten Systems wird in die sicheren Ausfälle λ_S und in die gefährlichen Ausfälle λ_D aufgeteilt. Die Aufteilung der Ausfallraten wird in der folgenden Abbildung gezeigt.

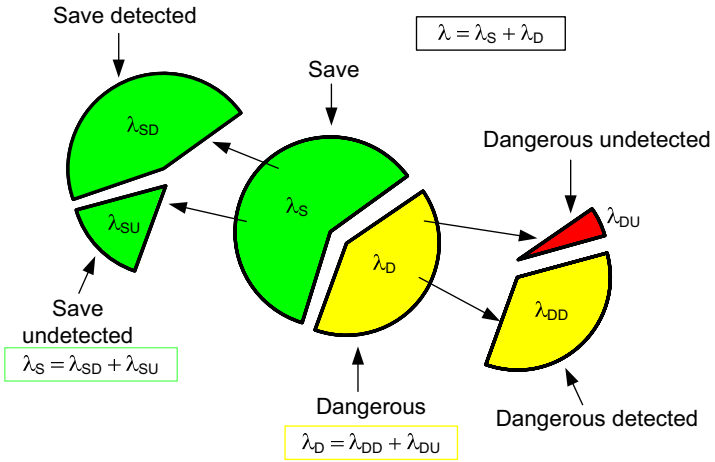

Abbildung B.2: Verteilung der Ausfallrate [48], [16], [15]

B.2 Zuverlässigkeit

Die Zuverlässigkeit $R(t)$ einer Komponente (oder eines Systems) ist die Wahrscheinlichkeit dafür, dass die Komponente (oder das System) im Intervall $[0,t]$ oder länger fehlerfrei funktioniert. Sie ist die Überlebenswahrscheinlichkeit bis zum Zeitpunkt t oder länger. Die Zuverlässigkeit ist von vielen Faktoren, wie z.B. Produktion, Test, Umwelteinflüsse (Temperatur oder mechanische Beanspruchung) und insbesondere von der Missionsdauer, abhängig. Wie

für Wahrscheinlichkeiten liegt die Zuverlässigkeit im Bereich: $0 \le R(t) \le 1$. Eine Wahrscheinlichkeit von ***0*** steht für das Unmögliche, eine von ***1*** für das sichere Eintreten [16].

Die Zuverlässigkeitsfunktion $R(t)$ wird durch die Ausfallrate $\lambda(t)$ vollständig bestimmt.

$$R(t) = e^{-\int_0^{\infty} \lambda(t) \cdot dt} \tag{B.3}$$

Ist die Ausfallwahrscheinlichkeit nach der Weibull-Verteilung verteilt, wird die Zuverlässigkeitsfunktion mit folgender Gleichung dargestellt:

$$\begin{aligned} R(t) &= 1 - P(t) \\ &= e^{-\left(\frac{t-t_0}{T-t_0}\right)^{\beta}} \end{aligned} \tag{B.4}$$

B.3 Ausfallwahrscheinlichkeit

Die Ausfallwahrscheinlichkeit $P(t)$ ist die Wahrscheinlichkeit, dass die Betriebszeiten T bis zum Ausfall nicht länger als ein vorgegebener Zeitraum t sind. Die Ausfallwahrscheinlichkeit $P(t)$ ist das Komplement der Zuverlässigkeitsfunktion und wird als eine Exponential-Verteilung bezeichnet [16], [15], [10]:

$$P(t) = 1 - R(t) = 1 - e^{-\lambda \cdot t} \tag{B.5}$$

Im Allgemeinen wird die Ausfallwahrscheinlichkeit in der Form der Weibull-Verteilung definiert:

$$P(t) = W(t;\beta;t_0,T) = 1 - e^{\left[-\frac{t-t_0}{T-t_0}\right]^{\beta}} \tag{B.6}$$

mit:

- t: Zeit
- β: Ausfallsteilheit
- t_0: Abzugsgröße oder Korrekturparameter
- T: charakteristische Lebensdauer oder Lageparameter

PFD steht für die Wahrscheinlichkeit eines Fehlers bei der Anforderung einer Sicherheitsfunktion und gibt die Güte eines Systems in Bezug auf Fehlerfreiheit an. Je kleiner der PFD-Wert ist, desto sicherer ist das System [16], [15].

Annahme: Nicht alle Ausfälle können ermittelt werden, denn in jedem technischen System gibt es keine 100 %-Sicherheit.

Die Berechnung des PFD-Wertes eines Systems erfolgt für einen Zeitraum zwischen zwei Wartungsintervallen und somit wird die PFD-Funktion wie folgt definiert:

$$PFD(t_i) = P(t_i) \qquad \textit{für} \quad \begin{cases} 0 \le t_1 \le T \\ T \le t_2 < 2 \cdot T \\ \ldots\ldots \\ (i-1) \cdot T \le t_i \le i \cdot T \end{cases} \tag{B.7}$$

mit $i \in (1, 2, \ldots, n)$

Mit dem ersten Wartungsintervall $i = 1$ wird die Güte eines Systems hinreichend untersucht und die Gleichung (B.7) lässt sich vereinfachen:

$$PFD(t_1) = P(t_1) = \lambda_D \cdot t_1 \qquad \textit{für } 0 \le t_1 \le T \tag{B.8}$$

Zur Beurteilung und zum Vergleich von Systemen wird meist der PFD-Mittelwert, PFD_{avg}, angegeben. PFD_{avg} wird über das gesamte Prüfintervall T gerechnet.

$$\begin{aligned} PFD_{avg} &= \frac{1}{T}\int_0^T P(t) \cdot dt \\ &= \frac{1}{T}\int_0^T \lambda_D \cdot t \cdot dt \\ &= \frac{1}{2} \cdot \lambda_D \cdot T \end{aligned} \tag{B.9}$$

B.4 Verfügbarkeit

Rakowsky [76] definiert die Verfügbarkeit als Wahrscheinlichkeit, eine Einheit zu einem gegebenen Zeitpunkt in einem Zustand anzutreffen, in dem sie eine geforderte Funktion unter gegebenen Bedingungen erfüllen kann, vorausgesetzt, dass die erforderlichen äußeren Mittel bereitgestellt sind. Die mittlere Verfügbarkeit wird durch das Integral über die Zeit T ermittelt.

$$A_{avg} = \frac{1}{T}\int_0^T A(t)dt \tag{B.10}$$

Storey [91] definiert die Verfügbarkeit eines Systems als die Wahrscheinlichkeit für eine korrekte Funktion im Sinne der Zuverlässigkeit mit Berücksichtigung von Reparatur.

$$A = \frac{MTTF}{MTTF + MTTR} \tag{B.11}$$

mit:

- $MTTF$: Mean Time To Failure
- $MTTR$: Mean Time To Repair

$$MTTF = \int_0^\infty R(t) \cdot dt \qquad \textbf{(B.12)}$$

Die Verfügbarkeit wird im Internationalen Elektrotechnischen Wörterbuch IEV [I04] nicht als Wahrscheinlichkeit, sondern als eine Eigenschaft, die durch „*das Zusammenwirken der Funktionsfähigkeit, der Instanz-Haltbarkeit und der Instandhaltungsbereitschaft*“ bestimmt wird.

Das Gegenteil dazu ist die Nichtverfügbarkeit. Die Nichtverfügbarkeit ist die Wahrscheinlichkeit, dass das System nicht in der Lage ist ihre vorgesehene Funktion zu einem bestimmten Zeitpunkt auszuführen.

Zuverlässigkeit ist ein Maß für die meist nicht reparierbaren Systeme, aber Verfügbarkeit wird für reparierbare Systeme gebraucht. Es ist zu beachten, dass eine Komponente zu einem bestimmten Zeitpunkt nicht verfügbar ist, weil sie entweder ausgefallen ist oder weil sie gewartet wird (vorbeugende Wartung, Test oder Reparatur). Dies bedeutet, die Verfügbarkeit ist eine Funktion der internen Zuverlässigkeit der Komponente und der Wartbarkeit. Zusammenfassend ist Nichtverfügbarkeit ein Maß für Ausfallzeiten.

B.5 Diagnose

Sicherheitssysteme haben in der Regel über einen integrierten Hardware- und / oder Software-Mechanismus eine automatische Erkennung von internen Fehlern. Dies wird Diagnose genannt [48], [23]. Der Diagnosedeckungsgrad (diagnostic coverage factor DC) ist das Verhältnis zwischen erkennbarer Ausfallrate und totaler Ausfallrate einer Komponente oder eines Subsystems durch automatischen diagnostischen Test.

$$\begin{aligned} \lambda_{Detected} &= DC \cdot \lambda_B = \lambda_{SD} + \lambda_{DD} \\ \lambda_{Undetected} &= (1 - DC) \cdot \lambda_B = \lambda_{SU} + \lambda_{DU} \end{aligned} \qquad \textbf{(B.13)}$$

Für Sicherheitsapplikationen werden nur gefährliche Ausfallraten in der DC-Berechnung betrachtet.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \qquad \textbf{(B.14)}$$

C Veröffentlichungen

[01] J.Börcsök, P.Holub, M.H.Schwarz, N.T.Dang Pham, “Determine PFD-values for Safety Related Systems Overview”, Risk, Reliability and Societal Safety; European Safety and Reliability Conference Proceedings, ESREL, Stavanger, 2007.

[02] Krini O., Börcsök J., Russo L., El Bahri M., Dang Pham N.T., 2012, “A New Software-Tool for Determining the Safety-Parameters of Components.” In Proceedings of International Symposium on Security and Safety of Complex Systems, 25-26 May 2012, Agadir, Morocco.

[03] N.T. Dang Pham, Michael Schwarz, Josef Börcsök, “Evaluation of Spurious Trip Rate of SIS dependent on demand rate”, WSEAS, Mathematical Methods and Systems in Science and Engineering, Teneriffa, 2015

[04] Thao Dang, Michael Schwarz, Josef Börcsök, “Effect of Demand Rate on Evaluation of Spurious Trip Rate of a SIS”, International journal of mathematical models and methods in applied sciences, Volume 9, Pages 487 – 498, 2015

Literaturverzeichnis

A Bücher/Monographien

[01] Abele Marcus, “Modellierung und Bewertung hochzuverlässiger Energiebordnetz-Architekturen für sicherheitsrelevante Verbraucher in Kraftfahrzeugen ”, Dissertation Uni Kassel, 2008.

[02] Ando T., “Safety and availability, easier and simpler SIS selection”, Tokyo, Japan, 2005.

[03] Andrews J.D., Bartlett LM., “A branching search approach to safety system design optimisation”, Reliability Engineering System Safety, 2005, 87: 23-30.

[04] Andrews J.D., Ericson II Clifton A., “Fault tree and Markov analysis applied to various design complexities”, Proceedings of the 18th International System Safety Conference, 2000.

[05] ANSI/ISA 84.01, “Application of Safety Instrumented Systems for the Process Industries”, 1996, Instrument Society of America, Research TrianGl.e Park, NC, USA

[06] ANSI/ISA-TR84.00.02-2002, Part 1-5, 2002

[07] ANSI/ISA-TR84.00.03-2002, 2002

[08] ANSI/ISA-TR84.00.04-2005, 2005

[09] Bauer Heinz, “Wahrscheinlichkeitstheorie und Grundzüge der Maßtheorie”, Walte de Gruyter & Co. Berlin, 1968.

[10] Bertsche Bernd, “Reliability in Automotive and Mechanical Engineering”, VDI-Buch, Springer-Verlag Berlin Heidelberg, 2008.

[11] Birolini Alessandro, “Reliability Engineering – Theory and Practice”, Fifth Edition, Springer-Verlag, 2006.

[12] Bodsberg L., Hokstad P., “A system approach to reliability and life-cycle cost process safety-systems”, IEEE Transactions on Reliability, Volume 44, Issue 2, Jun 1995.

[13] Bodsberg L., Hokstad P., “A system approach to reliability and life-cycle cost of process safety-systems”, IEEE Transactions on Reliability, Volume 44, Issue 2, Page(s): 179-186, 1995.

[14] Bodsberg L., Hokstad P., “Transparent reliability model for fault-tolerant safety systems”, Reliability Engineering and System Safety, Volume 55, Issue 1, Page(s): 25-38, 1997.

[15] Börcsök J., “Elektronic Safety Systems”, Hüthig publishing company, 2004.

[16] Börcsök J., “Elektronische Sicherheitssysteme – Hardwarekonzepte, Modelle und Berechnung”, Hüthig Verlag, 2004.

[17] Börcsök J., “Funktionale Sicherheit, Grundzüge sicherheitstechnischer Systeme“, Hüthig Verlag, 2006.

[18] Börcsök J., “HIMA Lexikon Sicherheitstechnik”, Heidelberg, Hüthig, 2009.

[19] Börcsök J., Ugljesa E., Machmur D., “Calculation of MTTF values with Markov Models for Safety Instrumented Systems”, 7th WSEAS International Conference on Applied Computer Science, Venice, Italy, November 21-23, 2007.

[20] Bukowski J. V., “Modelling and Analyzing the Effects of Periodic Inspection on the Performance of Safety-Critical Systems”, IEEE Transactions on Reliability, Vol. 50, No. 3, pp 321-329, September 2001.

[21] Bukowski J. V., Goble M. William, “Defining Mean-Time-to-Failure in a Particular Failure-State for Multi-Failure-State Systems”, IEEE Transactions on Reliability, Vol. 50, No. 2, June 2001

[22] Bukowski J.V., “A comparison of techniques for computing PFD average”, Proceedings Annual Reliability and Maintainability Symposium, Page(s): 590-595, 2005.

[23] CCPS, “Safe and Reliable Instrumented Protective Systems”, Center for Chemical Process Safety Wiley Interscience, New Jersey, USA, 2007.

[24] Chemia J.P., “A-Processus déterministes :Les Réseaux de Petri”, Modélisation et analyse des systèmes de production, Polytech’Tours département Productique 2ème année.

[25] Cheng C.-Y., Wang M., Lee B: L., “The impacts of common cause failures for two-unit parallel systems from RAMS+C point of view”, IEEE International Conference on Industrial Engineering and Engineering Management, Page(s) 1256-1260, 2011.

[26] Dhillon B.S., “Life Cycle Costing – Techniques, Models and Applications”, Gordon and Breach Science Publishers S.A., Amsterdam, Netherlands, 1989.

[27] Dilger E., Dieterle W., “Fehlertolerante Elektronikarchitekturen für sicherheitsgerichtete Kraftfahrzeugsysteme”, at – Automatisierungstechnik, Seiten 375 – 381, Ausgabe 50/2002,.

[28] Duduit Y., Innal F., Rauzy A., Signoret J-P., “Probabilistic assessments in relationship with safety integrity levels by using Fault Trees”, Reliability Engineering and System Safety, Volume 93, Issue 12, Page(s): 1867-1876, 2008.

[29] Dugan J., Bavuso S., Boyd M., “Dynamic fault tree models for fault tolerant computer systems”, IEEE Transactions on Reliability, Volume 41, Issue 3, Page(s): 363-377, 1992.

[30] Dunford N. and Schwartz J.T., “Linear Operators, Part I: General Theory”, Interscience, 1958.

[31] Eberle Andreas, “Einführung in die Wahrscheinlichkeitstheorie”, Vorlesung, WS 2009/2010, Uni Bonn.

[32] Esparza Alejandro, Hochleitner Monica Levy, “A brief discussion over safety costs in new enterprises”, exida.com, LLC, August 2010.

[33] Faghih-Roohi S., Xie M., Ng K. M., Yam R. C.M., “Dynamic availability assessment and optimal component design of multi-state weighted k-out-of-n systems”, Reliability Engineering and System Safety, Volume 123, Page(s) 57-42, 2014.

[34] Gabriel Thomas, Litz Lothar, Schrörs Bernd, “A formal approach to derive configurable Markov models for arbitrarily structures safety loops”, Processdings of the 9th International Conference on Probabilistic Safety Assissment and Management (PSAM9), Hong Kong, 2009.

[35] Goble W. M., “Control System Safety Evaluation & Reliability”, Research Triangle Park, NC: ISA-The Instrumentation, Systems and Automation Society, US, 1998.

[36] Goble W.M, Cheddie Harry L., “Safety Instrumented Systems Verification”, Research Triangle, NC: ISA-The Instrumentation, Systems and Automation Society, US, 2005.

[37] Goble W.M., “Control Systems Safety Evaluation & Reliability”, 3rd, North Carolina: Instrumented Society of America, 2010.

[38] Grøtan Tor Olav, Jaatun Martin Gilje, Øien Knut, Onshus Tor, “The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems”, SINTEF Technology and Society Safety and Reliability, 2007.

[39] Gruhn P., “Safety Instrumented Systems: Design, Analysis and Justification”, 2nd edn, Research Triangle Park, NC: ISA-The Instrumentation, Systems and Automation Society, US, 2007.

[40] Gruhn P., Cheddie Harry L., “Safety Instrumented Systems: Design, Analysis and Justification”, 2nd edn, Research Triangle Park, NC: ISA- The Instrumentation, Systems and Automation Society, US, 2006.

[41] Guo H., Yang X., “A simple reliability block diagram method for safety integrity verification”, Reliability Engineering and System Safety, Volume 92, Issue 9, Page(s):1267-1273, 2007.

[42] Heuser, H., “Funktionalanalysis, Theorie und Anwendung”, B. G. Teubner Verlag, 4., durchgesehene Auflage November 2006.

[43] Hildebrand A, “Berechnung der Probability of Failure on Demand (PFD) einer heterogenen 1-aus-2-Struktur in Anlehnung an die EN 61508”, atp – Automatisierungstechnische Praxis, 10: 73-80, 2007.

[44] Hokstad P., Corneliussen K., “Loss of safety assessment and the IEC 61508 standard”, Reliability Engineering and System Safety, 83(1): 111-120, 2004.

[45] Holub P., Börcsök J., “Advanced PFH Calculation for Safety Integrity Systems with High Diagnostic”, ICAT 2009 XXII International Symposium on Information, Communication and Automation Technologies, 2009.

[46] Houtermans M., “Reliability Engineering & Data Collection, To Improve Plant Safety & Availability”, Second International Conference on Systems (ICONS’07), IEEE, 2007.

[47] Houtermans M., “Safety Availability versus Process Availability, Introduction Spurious Trip Levels™”, White paper, Risknowlogy Expert in Risk, Reliability and Safety, May 2006.

[48] IEC 61508, “Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems”, Part 1-7, Deutsche Fassung EN 61508: 2010.

[49] IEC 61511, “Functional safety: safety instrumented systems for the process industry sector”, Part 1-3, CDV versions, 2003.

[50] IEC 62061, “Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems, First edition, 2005-01.

[51] ISO 26262, “Road verhicles – Functional Safety”, Part 1 -10, ISO Standard, 2011.

[52] Jin Hui, Lundteigen Mary Ann, Rausand Marvin, “Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation”, Reliability Engineering and Safety, Volume 96, Issue 3, Page(s): 365-373, 2011.

[53] Kang Hyun Gook, Kim Hee Eun, “Unavailability and spurious operation probability of k-out-of-n reactor protection systems in consideration of CCF”, Annals of Nuclear Energy, Volume 49, Page(s) 102-108, 2012.

[54] Kawachi Yoshio, Rausand Marvin, “Life cycle cost (LCC) analysis in oil and chemical process industries”, Norwegian University of Science and Technology, 06/1999.

[55] Knetering B., Brombacher A., “Application of micro Markov models for quantitative safety assessment to determine safety integrity levels as defined by IEC 61508 standard for functional safety”, Reliability Engineering and System Safety, Volume 66, Issue 2, Page(s) 171-175, 1999.

[56] König Wolfgang, “Erfolgsgeschichte eines stochastischen Prozesses: Die Brown’sche Bewegung”, Sächsische Akademie der Wissenschaften, 28. Juni 2008.

[57] Kumar M., Verma A. K., Srividya A., “Modeling demand rate and imperfect proof-test and analysis of their effect on system safety”, Reliability Engineering and System Safety, Volume 93, Page(s) 1720-1729, 2008.

[58] Kumar M., Verma A. K., Srividya, “Analyzing effect of demand rate on safety of systems with periodic proof-tests“, International Journal of Automation and Computing, Page(s) 335-341, October 2007.

[59] Liu Yiliu, Rausand Marvin, “Reliability assessment of safety instrumented systems subject to different demand modes”, Journal of Loss Prevention in the Process Industries 24, Page(s): 49-56, 2011.

[60] Liu Yiliu, Rausand Marvin, “Reliability effects of test strategies on safety-instrumented systems in different demand modes”, Reliability Engineering and System Safety, Volume 119 , Page(s): 235-243, 2013.

[61] Lu L., Lewis G., “Configuration determination for k-out-of-n partially redundant systems”, Reliability Engineering and System Safety, Volume 93, No. 11, Page(s) 1594-1604, 2008.

[62] Lu L., Lewis G., “Reliability evaluation of standby safety systems due to independent and common cause failures”, Procs IEEE International Conference on Automation Science and Engineering, Shanghai, China, Page(s) 264-269, October 2006.

[63] Lu und Jiang, “Analysis of on-line maintenance strategies for k-out-of-n standby safety systems”, Reliability Engineering System Safety, 92: 144-155, 2007.

[64] Lubcke Wolfgang, “Methods to interconnect functional safety and selfmonitoring of field devices in process control loops”, 4th. European Conference on Electrical and instrumentation Applications in the Petroleum & Chemical Industry, Page(s) 1-4, 2007 (PCIC Europe 2007).

[65] Lundteigen M. A., Rausand M., “Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas”, Reliability Engineering and System Safety 93, Page(s): 1208-1217, 2008.

[66] Lundteigen M.A., Rausand M., “Architectural containts in IEC 61508: Do they have the intended effect?”, Reliability Engineering and System Safety 2008.

[67] Lyndersen S., Aaro R., “Life cycle cost prediction handbook, computer-based process safety system”, SINTEF report STF7 A89024 Trondheim, Norway, 1989.

[68] Macdonald Dave, “Practical Hazops, Trips and Alarms”, IDC Technologies, Netherlands, 2004.

[69] Machleidt Konstantin, Litz Lothar, “An optimization approach for safety instrumented system design”, Proceeding – Annual Reliability and Maintainability Symposium (RAMS), Page(s) 1-6, 2011.

[70] Martorell S., Sanchez A., Carlos S., Serradell V., “Simultaneous and multi-criteria optimization of TS requirements and maintenance at NPPs”, Annals Nuclear Energy, Volume 29, Issue 2, Page(s): 147-168, 2002.

[71] Martorell S., Villanueva J.F., , Carlos S., Nebot Y., Sanchez A., Pitchard J.L., Serradell V., “RAMS+C Informed Decision-Making with Application to Multi-objective Optimization of Technical Specifications and Maintenance Using Genetic Algorithms”, Reliability Engineering and System Safety, Volume 87, Issue 1, Page(s): 65-75, 2005.

[72] Meintrup D., Schäffler S., “Stochastik – Theorie und Anwendungen”, Springer-Verlag Berlin Heidelberg, 2005.

[73] Miller, Curt, Win-Win, “A manager’s guide to functional safety”, Sellersville, exida.com LLC, 2008.

[74] Onshus T., Bodsberg L., “Reliability of computerbased safety systems”, A First International Conference on the Use of Programmable Electronic Systems in Safety Related Applications Computers and Safety, Page(s) 8-12, 1989.

[75] Pateli M., Crossley P.A., “Reliability assessment of SIPS based on safety integrity level and spurious trip level”, International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012), Page(s) 1-7, Hangzhou, 2012.

[76] Rakowsky Uwe Kay, “System-Zuverlässigkeit, Terminologie-Methoden-Konzept”, Life-Long Learning Hagen, 2002.

[77] Rausand Marvin, “Reliability of Safety-Critical: Theory and Applications”, Verlag John Wiley & Sons, Canada, 2014.

[78] Rouvroye J.L., van den Bliek E.G., “Comparing safety analysis techniques”, Reliability Engineering and System Safety, Volume 75, Issue 3, Page(s): 289-294, 2002.

[79] Rouvvroye J., Brombacher A., “New quantitative safety standards; different techniques, different results?”, Reliability Engineering and System Safety, Volume 66, Issue 2, Page(s) 121-125, 1999.

[80] Sandmann Werner, “Kapitel 4 Markovketten”, Universität Bamberg, WS 07-08.

[81] Schneeweiss W.G., “Tutorial: Petri nets as a graphical description medium for many reliability scenarios”, IEEE Transaction on reliability, 50(2): 159-164, 2001.

[82] Schulz Daniel, “Eine Einführung in zeit-diskrete homogene Markov-Ketten”, Fakultät für Informatik Otto-von-Guericke Universität Magdeburg, November 2010.

[83] Sheskin Theodore J., “Computing absorption probabilities for a Markov chain”, INT. J. MATH. EDUC. SCI. TECHNOL., Vol. 22, No. 55, Page(s) 799-805, 1991.

[84] Signoret J-P., Duduit Y., Rauzy A., “High Integrity Protection Systems (HIPS): Methods and tools for efficient Safety Integrity Level (SIL) analysis and calculation”, Procs. European Safety and Reliability Conference ESREL 2007, Norway.

[85] Sikora D.S., Jones R.L., “Emergency shutdown system”, IEEE Transactions on Industry Applications, Page(s) 254-256, Volume 27, Issue 2, 1991.

[86] SINTEF, “Reliability prediction method for safety instrumented systems”, PDS Method Handbook, 2003 Edition”, SINTEF 2003.

[87] SINTEF, “Reliability prediction method for safety instrumented systems”, PDS Method Handbook, 2006 Edition”, SINTEF 2006.

[88] SINTEF, “Reliability prediction method for safety instrumented systems”, PDS Method Handbook, 2010 Edition”, SINTEF 2010.

[89] Sonnleitner Kurt, “75 Jahre RAG, die Sicherheitsanforderungen im Wandel der Zeit”, 2010.

[90] Stapelberg Rudolph Frederick, “Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design”, Springer-Verlag London Limited, 2009.

[91] Storey N., “Safety-critical Computer Systems”, Addison Wesley Longman New York, USA, 1996.

[92] Torres- Echevarría A.C., Martorell S,, Thompson H.A., “Multi-objective optimization of design and testing of safety instrumented systems with MooN voting architectures using a genetic algorithm”, Reliability Engineering and System Safety 106, Page(s): 45-60, 2012.

[93] Torres- Echevarría A.C., Martorell S., Thompson H.A., “Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy”, Reliability Engineering and System Safety, 94(2): 167-179, 2009.

[94] Torres- Echevarría A.C., Martorell S., Thompson H.A., “Modelling and optimization of proof testing policies for safety instrumented systems”, Reliability Engineering and System Safety, 94(2): 838-854, 2009.

[95] Torres- Echevarría A.C., Thompson H.A., “Multi-objective genetic algorithm for optimization of system safety and reliability based on IEC 61508 requirements: a practical approach”, Proceedings of the IMechE Part O: Journal of Risk and Reliability, 221(O3): 193-205, 2007.

[96] Üstoğlu İ., Kaymakçı Ö.T., Börcsök. J, “Effects of Varying Diagnostic Coverage on Functional Safety”, In Proceedings IEEE International Symposium on Fundamentals of Electrical Engineering 2014 (ISFEE 2014), Bucharest, Romania, 27-29 November 2014.

[97] Wacker H.-D., Holub P., Börcsök J., 2013: Optimization of Diagnostics with Respect to the Diagnostic Coverage and the Cost Function. In Proceedings ICAT 2013, Sarajevo, Bosnia and Herzegovina., October 30 – November 1, 2013.

[98] Wacker Hans-Dieter, “Markovsche Ketten und Markovsche Prozesse und ihre Anwendung in der Risikoanalyse”, Probevorlesung zur Habilitation, 2010.

[99] Wang Peng, Bai Yan, “Safety and Availability Optimization of Safety Instrumented System”, 9th International Conference on Reliability, Maintainability and Safety (ICRMC), Page(s): 560-564, 2011.

[100] Winkovich T., Eckardt D., “Reliability Analysis of Safety Systems Using Markov-Chain Modelling”, European Conference on Power Eletronics and Applications, Page(s): 10pp-P.10, 2005.

[101] Xie L.Y., James M.N., Zhao Y.X. and Qian W.X., “Research on Spurious Trip of 1oo2 Safety Instruments of Petrochemical Installation with Repair Considered” , Advanced Materials Research (Volumes 118 - 120), Materials and Product Technologies II, Page(s) 596-600, June, 2010.

[102] Yoshimura Itaru and Sato Yoshinobu, “Safety achieved by the safe failure fraction (SFF) in IEC 61508”, IEEE Transactions on Reliability, Volume 57, Issue 4, Page(s) 662-669, 2008.

[103] Zhang T., Long W., Sato Y., “Availability of systems with self-diagnostics components – Apply Markov model to IEC 61508-6”, Reliability Engineering and System Safety, 80(2): 133-141, 2003.

[104] Zhang T., Wang Y., Xie M., “Analysis of the Performance of Safety-Critical Systems with Diagnosis and Periodic Inspection”, Reliability and Maintainability Symposium 2008, RAMS 2008, Annual 2008, Page(s): 143-148.

[105] Zierke Erik, “Absorptionswahrscheinlichkeiten und Absorptionszeiten der Brownschen Bewegung als Grenzwerte von Irrfahrtsproblemen ”, Dissertation, Otto-von-Guericke-Universität Magdeburg, 1999.

B Internet-Adressen

[I01] Buddy Creef, “Selection of an SIS for Maximum Process Availability”, (http://www.rtpcorp.com/documents/SafetyvsAvailability_000.pdf, Stand: 12/03/2014)

[I02] http://fahto.com/instandhalungsgebiete/sicherheit/index.html, Stand: 28/01/2016

[I03] http://www.rf-sicherheit.de/index.php/component/content/article/54, Stand: 12/03/2014

[I04] http://www.dke.de/de/Online-Service/DKE-IEV/Seiten/IEV-Woerterbuch.aspx, Stand: 28/01/2016

[I05] http://www.siegel-christian.de/seiten/facharbeit/markow.html, Stand: 23/05/2011

[I06] Alfred Beer, Marcus Rau, “Qualität und Zuverlässigkeit elektronischer Systeme am Beispiel von x-by-wire Systemen“, TÜV Automotive GmbH, http://www.tuev-sued.de/uploads/images/1134986818079365489049/09_beer.pdf, Stand: 11/01/2012

[I07] http://www.vde.com/de/Technik/fs/Documents/FAQdemand.pdf, Stand 28/01/2016

[I08] http://www.automation.siemens.com/w1/efiles/automation-technology/pi/SIL/SIL_Broschuere_de.pdf, Stand 28/01/2016

ISBN 978-3-7376-0204-4