Preventive maintenance of Safety-related Systems – modeling, analysis, and optimization

Präventive Instandhaltung sicherheitsbezogener Systeme – Modellierung, Analyse und Optimierung

Vom Fachbereich Elektrotechnik und Informationstechnik
der Technischen Universität Kaiserslautern
zur Verleihung des akademischen Grades
Doktor der Ingenieurwissenschaften (Dr.-Ing.)
genehmigte Dissertation

von
Dipl.-Ing. Konstantin Machleidt
geb. in Nowosibirsk

D 386

Datum der mündlichen Prüfung:	30.10.2015
Dekan des Fachbereichs:	Prof. Dr.-Ing. Hans D. Schotten
Promotionskommision	
Vorsitzender:	Prof. Dr. techn. Gerhard Fohler Technische Universität Kaiserslautern
Berichterstattende:	Prof. Dr.-Ing. habil. Ping Zhang Technische Universität Kaiserslautern
	Prof. Dr.-Ing. Frank Schiller Beckhoff Automation GmbH & Co. KG und East China University of Science and Technology

Abstract: Safety-related Systems (SRS) protect from the unacceptable risk resulting from failures of technical systems. The average probability of dangerous failure on demand (PFD) of these SRS in low demand mode is limited by standards. Probabilistic models are applied to determine the average PFD and verify the specified limits. In this thesis an effective framework for probabilistic modeling of complex SRS is provided. This framework enables to compute the average, instantaneous, and maximum PFD. In SRS, preventive maintenance (PM) is essential to achieve an average PFD in compliance with specified limits. PM intends to reveal dangerous undetected failures and provides repair if necessary. The introduced framework pays special attention to the precise and detailed modeling of PM. Multiple so far neglected degrees of freedom of the PM are considered, such as two types of elementwise PM at arbitrarily variable times. As shown by analyses, these degrees of freedom have a significant impact on the average, instantaneous, and maximum PFD. The PM is optimized to improve the average or maximum PFD or both. A well-known heuristic nonlinear optimization method (Nelder-Mead method) is applied to minimize the average or maximum PFD or a weighted trade-off. A significant improvement of the objectives and an improved protection are achieved. These improvements are achieved via the available degrees of freedom of the PM and without additional effort. Moreover, a set of rules is presented to decide for a given SRS if significant improvements will be achieved by optimization of the PM. These rules are based on the well-known characteristics of the SRS, e.g. redundancy or no redundancy, complete or incomplete coverage of PM. The presented rules aim to support the decision whether the optimization is advantageous for a given SRS and if it should be applied or not.

Zusammenfassung: Sicherheitsbezogene Systeme (SRS) schützen vor unverhälnismäßigen Gefährdungen, die durch Ausfälle technischer Einrichtungen verursacht werden. Die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung (PFD) für die SRS mit niedriger Anforderungsart wird durch Normen begrenzt. Um die mittlere PFD zu ermitteln und die durch Normen vorgeschriebenen Grenzwerte zu verifizieren, werden probabilistische Modelle verwendet. In dieser Dissertation wird eine neue Methode zur probabilistischen Modellierung komplexer SRS entwickelt, mit der die Kenngrößen mittlere, instantane und maximale PFD ermittelt werden können. Für SRS ist die präventive Instandhaltung (PM) unentbehrlich, damit die mittlere PFD die vorgeschriebenen Grenzwerte nicht überschreitet. Durch PM werden die gefahrbringenden unerkannten Ausfälle aufgedeckt und falls erforderlich repariert. Bei der entwickelten Methode wird ein besonderes Augenmerk auf die präzise und detaillierte Modellierung der PM gelegt. Es werden mehrere bisher vernachlässigte Freiheitsgrade der PM berücksichtigt, wie z.B. für jedes Element zwei Typen der PM, jeweils zu beliebigen variablen Zeiten. Wie in Analysen gezeigt wird, haben diese Freiheitsgrade einen signifikanten Einfluss auf die Kenngrößen. Um eine Verbesserung der mittleren oder maximalen PFD oder von beiden

zu erzielen, wird die PM optimiert. Mittels eines Verfahrens der heuristischen nichtlinearen Optimierung (Nelder-Mead-Verfahren) werden die mittlere oder maximale PFD oder eine gewichtete zusammengesetzte Zielfunktion minimiert. Es werden signifikante Verbesserungen der Optimierungsziele und ein besserer Schutz vor Gefährdungen erreicht. Diese Verbesserungen werden mittels verfügbarer Freiheitsgrade der PM erzielt und erfordern keinen Mehraufwand. Zusätzlich werden Regeln bereitgestellt, um abzuschätzen ob für ein SRS signifikante Verbesserungen durch die Optimierung erzielt werden können. Diese Regeln basieren auf den bekannten Merkmalen des SRS, wie z.B. Redundanz oder keine Redundanz, vollständige oder unvollständige Abdeckung der PM. Damit lässt es sich abschätzen, ob der Einsatz der beschriebenen Optimierungsmethoden für ein SRS vorteilhaft sein kann.

Acknowledgments

The work that resulted in this book could not have been accomplished without several persons' assistance, support, and encouragement.

First of all, I would like to thank my doctoral adviser, Professor Lothar Litz, for the opportunity to research and work at his institute. I am deeply grateful for his encouragement, the trust he placed in my work, and the intellectual freedom he has given to me in these years. His guidance and invaluable advice were of great importance to complete this work. The research standards he has propagated were worthy of imitation and influenced me strongly. Tragically, Professor Lothar Litz suddenly passed away this August. This book is dedicated to him.

My sincere thanks go to the members of the evaluation board: Professor Ping Zhang, Technische Universität Kaiserslautern; Professor Frank Schiller, Beckhoff Automation GmbH & Co. KG and East China University of Science and Technology; and the chairman Professor Gerhard Fohler, Technische Universität Kaiserslautern.

During my work as a research associate for the Institute of Automatic Control at the Technische Universität Kaiserslautern I had the privilege to be part of a great team. I am grateful to all my colleagues for the numerous rich and important discussions about research and other interesting topics. Thank you for your friendship, support, and humor. I deeply appreciate the time we had spent together at the institute, on our joint trips, and during the numerous activities apart from work. Many thanks to Stefan Schneider, Thomas Gabriel, Thorsten Rodner, Anna Nehring, Thomas Leifeld, André Teles-Carvalho, and Andreas Haupt for proofreading of the manuscript and hinting at a considerable number of flaws I have eliminated with your help.

During my work for the Institute of Automatic Control, I was part of several industrial projects with the companies KROHNE Messtechnik GmbH, Bayer TechnologyServices GmbH, and BASF SE. I would like to warmly thank all the people who contributed to successfully complete these projects.

My sincere thanks go to Thomas Gabriel, Daniel Düpont, and Andreas Hildebrandt for the numerous interesting and inspiring discussions on the topic of functional safety. I would like to thank Christoph Jötten for his always helpful and inspiring advice. Moreover, I would like to thank my friends and relatives for the support and encouragement they gave me during these years.

Finally, and not the least, I give the heartiest gratitude to Lucia and to my parents for their love, patience, encouragement, and help.

Kaiserslautern, December 2015 Konstantin Machleidt

Contents

Chapter 1

Introduction

1.1 Motivation

In industry, potentially hazardous applications are widely used, e.g. in large-scale plants of the chemical industry. The incorrect functioning of the technical systems related to the potentially hazardous applications threatens the health of humans, the environment, and assets. The potentially hazardous application might require to be put from a "dangerous" into a "safe" state to avoid the mentioned threats.

The *Safety-related Systems* protect from the unacceptable risk resulting from the potentially hazardous applications. An adequate protection has to be achieved through effective Safety-related Systems. To ensure the adequate protection, the safety requirements for effective Safety-related Systems are regulated by international standards, e.g. by the standard [IEC11e] for the electrical/electronic/programmable electronic Safety-related Systems (SRS). The SRSs are a large class of systems applied in many different branches of industry, e.g. chemical and process industry, transportation, nuclear industry.

The failures of an SRS can result in severe accidents. A well-known example for the outcome of an SRS failure is the Deep Water Horizon accident in 2010. On April 20, 2010, a blow-out of hydrocarbons occurred at the offshore oil drilling rig Deep Water Horizon. Eleven people were killed by explosions and the Deep Water Horizon finally sank after the resulting fire could not be extinguished for 36 hours. The accident had such disastrous consequences because the blow-out preventer, which is the critical SRS to prevent an oil spill, failed to seal the drilling well. In total, a huge amount of oil was released and polluted the sea. The oil spill continued for five month until it was stopped.

An effective SRS is designed to exhibit certain characteristics, which ensure an adequate protection for the respective potentially hazardous application. These characteristics have to be built in during design and development, and retained during production and operation of an SRS. The characteristics of an effective SRS are:

1. Ability to continuously perform failure-free for a given appropriately long period of

time

2. Ability to detect failures and be repaired within a given appropriately short period of time

The characteristic 1 ensures that an SRS is effective for a potentially hazardous application that frequently demands the SRS to be put into a safe state. In this case, a failure of the SRS is not tolerated. The characteristic 1 is referred to as *reliability*. In contrast, there are potentially hazardous applications where a failure will be tolerated if it is quickly detected and repaired. Such an application rarely demands the SRS. For example, the blow-out preventer of an oil drilling rig is demanded in the rare event of a blow-out. Hence, the blow-out preventer might fail if the failure is quickly detected and repaired. For such applications, which are called *low demand* applications, the effectiveness of an SRS is ensured by the two characteristics 1 and 2. A quick detection and repair, which is ensured by the characteristic 2, makes an SRS effective as well as the ability not to fail, ensured by the characteristic 1. An SRS will be effective if the characteristics 1 and 2 are balanced, which can be done in various ways. Therefore, a degree of freedom is available that enables the choice of a technically reasonable and economically advantageous SRS. The characteristics 1 and 2 are quantified by a single probabilistic figure of merit, the *probability of dangerous failure on demand* (PFD). The PFD is closely related to the safety-related *availability*. It has to be noted that, the PFD, as well as the characteristics 1 and 2, are probabilistically quantified. This is because these characteristics are not "regular" measurable technical characteristics. For example, the exact period of time, in which an SRS will continuously perform failure-free, can not be determined. A probability can be determined if a given SRS, analyzed at the time of its startup, will continuously perform failure-free for a mission time of 10,000 h. In contrast, a measurable technical characteristic, e.g. the electrical resistance of a given resistor, can be simply determined by measurement.

The SRSs applied in low-demand applications are treated in this thesis. To ensure that an SRS is adequately effective, the safety requirements regulated by [IEC11e] define thresholds for the PFD. The *probabilistic modeling* aims to determine the PFD of an SRS and verify the respective safety requirements. The possibly occurring failures and respective maintenance are evaluated via the probabilistic model. An SRS is built up of multiple possibly dependent elements, which have multiple failure modes and are subject to multiple different maintenance activities. The maintenance activities of an SRS have a significant impact on the PFD. Particularly, the *preventive maintenance* (PM) activities, such as scheduled periodic proof tests and respective repairs, have a crucial impact. This is because the SRSs are prone to the *hidden* or *undetected failures*, not detectable during operation. The PM aims to reveal the undetected failures and provide repair. Various types of PM are applied to the elements of an SRS in the field of industrial applications.

For example, two frequently applied types of PM are the full stroke test and the partial stroke test of a safety valve with respective repairs if necessary. The *PM plan* defines the time schedule of the PM related to an SRS for the time from startup to decommissioning. Two identical SRSs might have strongly varying values of PFD if different PM plans are applied. Hence, a PM plan has to be chosen such that the respective SRS complies with the given threshold for the PFD. An acceptable PM plan is determined and verified via the probabilistic model of the respective SRS.

In this thesis, the probabilistic models based on the *Stochastic and Deterministic Timed Automata* and *Multi-phase Continuous-time Markov Chains* are introduced. These probabilistic models are strongly connected to the concepts of the SRSs and straightforward in application. Additionally, deeper insight is provided into further types of probabilistic models, which feature more or less restrictions. A framework is presented to first model individual SRS elements and then automatically compose the respective model of the entire SRS. Hence, arbitrarily complex SRSs can be modeled, even SRSs that have numerous and dependent elements. Moreover, the introduced probabilistic models are designed to evaluate PM plans that support up to two different types of arbitrarily scheduled PM for each element. Additional degrees of freedom are provided to the PM. The restrictions, which are applied on the PM plans in practice and in literature, are overcome. These restrictions particularly imply the PM to be simultaneous for all elements and periodically scheduled with equal periods. The analysis of the introduced probabilistic models shows that the additional degrees of freedom have a significant impact on the PFD. The choice of a PM plan is formulated as an optimization problem for the available degrees of freedom. The evaluated objective function is the achieved PFD that is calculated via the introduced probabilistic model. The Nelder-Mead method is applied to solve the optimization problem. The choice of a PM plan by solving the respective optimization problem is demonstrated for selected practically relevant types of SRSs, which have a different degree of redundancy, fraction of common-cause failures, and coverage of PM. The PM plans that are determined via optimization in many cases provide significant improvement of the PFD and therefore increase the effectiveness of the respective SRSs. Furthermore, useful general conclusions on the choice of PM plans are provided. Particularly, a set of rules is given to decide for a given SRS if the PFD can be significantly improved via optimization of the PM plan.

1.2 Background and state of the art

1.2.1 Preliminaries

The structure of section 1.2, which deals with the state of the art and the related literature of this thesis, is outlined below. The content of this section is mainly addressed to readers

with fundamental knowledge of the SRSs, functional safety, and probabilistic modeling. The used terms will not be defined in section 1.2, for reasons of improved readability and a compact representation. The definitions of the used terms will be given mainly in chapter 2 and also in the following chapters.

In subsection 1.2.2, the safety requirements on the SRSs and the probabilistic figures of merit are described. The characteristics of the SRSs are described at the beginning of subsection 1.2.3. These characteristics have to be supported by the applied probabilistic modeling. Thereafter, an overview of the probabilistic modeling methods described in literature is provided. The probabilistic modeling methods are reviewed in regard to the support of the identified SRSs characteristics. The advantages and drawbacks of each reviewed method are pointed out. In subsection 1.2.4, the analysis of the probabilistic models is treated and the motivation for the application of optimization is explained.

In the following section 1.3, the main novel contributions and targets of this thesis are presented. Finally, the organization of the thesis is described in section 1.4 to guide the reader.

1.2.2 Safety requirements on Safety-related Systems (SRSs)

The SRS comprises "everything (hardware, software and human elements) necessary to carry out one or more safety functions, where failure of the safety function would give rise to a significant increase in the risk to the safety of persons and/or the environment", as described in [Int14]. An individual set of safety requirements is assigned to every safety function and applies to the related SRS. The safety requirements were regulated by the international standard [IEC11e]. The meaning of acts, regulations, guidelines, and standards related to the SRSs was outlined in [Lit98]. Particularly, the legal situation in Germany was treated in detail. The fundamentals and the terminology related to the field of SRSs were pointed out.

The safety requirements were classified in four *Safety Integrity Levels* (SILs), SIL 1 to SIL 4, see [IEC11e]. The SIL assigned to a safety function depends on the risk, identified via the hazard and risk assessment of the related potentially hazardous application. Thus, the SIL 4 is assigned to a safety function with a high identified risk, in contrast to the SIL 1, which is assigned to a safety function with a low identified risk. The hazard and risk assessment was described in [IEC11c] and [Zio07]. It is not treated with full details in this thesis. Overall, the hazard and risk assessment defines the required safety functions and assigns the appropriate SIL to every safety function. Based on the SIL, the associated set of safety requirements is assigned to the safety functions. These safety requirements are relevant for the respective SRSs, which carry out the safety functions. The relevant safety requirements for an SRS carrying out multiple safety functions are these associated with the highest SIL. The relationship between the risk, SIL, and safety requirements

is illustrated in figure 1.1. In the process industry sector the applications with SIL 4 safety functions are not used. Instead, the related potentially hazardous applications are redesigned to reduce the resulting risk.

Risk	SIL	Safety requirements
	1	Low
	2	Medium
	3	High
	4	Very high

Figure 1.1: Relation of risk and SIL

The safety requirements comprise qualitative and quantitative requirements. A large part of [IEC11e] was designated to the qualitative safety requirements. These requirements have to be followed over the complete life-cycle of an SRS. The activities for the concept development, specification, realization, validation, operation, and decommissioning of the SRSs were regulated by the qualitative requirements defined by [IEC11a]. Complementary, the quantitative requirements provide thresholds for the SRSs quantitative figures of merit. The SRSs are applied to a large variety of categorically different potentially hazardous applications. These applications are categorized based on their SRS mode of operation. Therefore, depending on the mode of operation different figures of merit are relevant for the SRS to be effective. The modes of operation were defined in [IEC11b] as the *low demand mode*, *high demand mode*, and *continuous mode*. The low demand mode is applicable when the safety function is rarely demanded by the related potentially hazardous application, i.e. once per year or less frequent. The potentially hazardous applications generating more frequent demands than once per year are categorized as high demand or continuous mode. The described categorization is motivated to differentiate between applications where a failure at system level is tolerated and such where it is not. That leads to different figures of merit for effective SRSs. For the SRSs with different modes of operation the standard [IEC11a] introduced the relevant figures of merit and respective thresholds. The figures of merit introduced for the low demand mode of operation include the *average probability of dangerous failure on demand* ($\overline{PFD}$) and further figures of merit, e.g. the hardware fault tolerance, etc. For the high demand mode and continuous mode the *average frequency of a dangerous failure* ($\overline{PFH}$) was introduced instead of the $\overline{PFD}$.

The $\overline{PFH}$ and $\overline{PFD}$ are both probabilistic figures of merit, intended for the SRSs with different modes of operation. The $\overline{PFH}$ is the average occurrence rate of failures leading to a hazardous event in the related potentially hazardous application. The $\overline{PFD}$

is the complement of the mean availability referring to the SRS safety function. The $\overline{PFD}$ is determined for the time interval of interest from the instantaneous PFD, denoted by $PFD(t)$. The time interval of interest usually comprises the mission time from the startup until the end of the operation time. Additionally, the maximum PFD for the time interval of interest, denoted by $PFD_{\max}$, was suggested in [IEC11c] to be evaluated. The $PFD_{\max}$ reflects the maximum occurring hazard probability. However, no mandatory thresholds have been provided for the $PFD_{\max}$ so far, in contrast to the $\overline{PFD}$.

This thesis is focused on the SRSs in low demand mode of operation. The probabilistic modeling of SRSs mainly aims to determine the $PFD(t)$. The figures of merit $\overline{PFD}$ and $PFD_{\max}$ are calculated from the $PFD(t)$. Hence, it can be verified if a given SRS meets the respective thresholds. However, the probabilistic models introduced in this thesis can also be applied with minor adjustments to the high demand and continuous modes of operation.

1.2.3 Probabilistic modeling

The SRSs are complex systems build up of *dependent elements*, which are subject to multiple *maintenance actions* and *failure modes*. The dependencies of elements arise from the failures or repairs of one element affecting other elements, e.g. multiple elements might share one repair team, the failures of one element might inhibit the failure detection of other elements, etc. The multiple maintenance actions comprise the *corrective maintenance* (CM), providing repair after *detected failures*, and *preventive maintenance* (PM), revealing the *undetected failures* and providing repair if necessary. The PM comprises up to two different types of PM for each element of an SRS, the *regular* and the *supplementary PM*. Each individual type of the PM provides a different coverage to reveal the undetected failures. For example, the partial stroke test is applied to a valve, providing an incomplete test coverage to reveal failures, and the full stroke test is also applied, providing a higher but still incomplete test coverage to reveal failures. The repair of the revealed failures, if necessary, is part of the PM. The PM related to the elements of an SRS is scheduled via a *PM plan* that specifies the time when each PM activity will be executed. It has to be noted that, no restrictions on the time schedule of the PM are given, i.e. the PM plans other than periodic with equal periods are permitted. The multiple failure modes result from the modeled types of failures that are subject to different maintenance actions. Dependencies within an SRS element are caused by these multiple failure modes. The dependency that is caused by the two failure modes *detected failures* and *undetected failures* is explained in the following example. An undetected failure can only occur if either no detected failures have occurred so far or the occurred detected failures have already been repaired. The state of an element that failed is not influenced by further failures. Hence, the detected and undetected failures of the analyzed element

depend on each other. The dependencies caused by multiple failure modes were treated in [Bir10], where they were referred to as *no further failures at system down*.

The SRSs characteristics outlined above have to be supported by the probabilistic modeling. Different probabilistic modeling methods to determine the $PFD(t)$ and further probabilistic figures of merit can be found in literature, see [IEC11d], [Bir10], [Zio07], and [TE09]. The probabilistic modeling methods in literature are mostly formulated more generally and target at the availability of systems. These methods usually can be adapted to determine the $PFD(t)$ of SRSs. Generally, it is not regulated by standards which method has to be applied to verify the regulated $\overline{PFD}$ thresholds of SRSs. This decision is left to the safety engineer. The different available methods have advantages and drawbacks. The probabilistic modeling methods can be fundamentally classified into

1. Boolean methods,
2. Hybrid methods, and
3. State-based methods.

The *Boolean methods* include the Reliability Block Diagrams (RBDs), Fault Trees (FTs), and further less known methods. For example in [Zio07] the FTs were treated. The PFD of a given SRS is determined via the static logical *Boolean structure function* from the PFDs of the respective SRS elements. An FT modeling the SRS failure, which depends on the SRS elements failures, is shown in figure 1.2. The Boolean methods are limited to model the SRSs consisting of independent elements. The dependencies within an SRS element, caused by multiple failure modes, can not be modeled by Boolean methods. Moreover, the Boolean methods can not model time dependencies of the SRSs elements PFDs, resulting from incomplete diagnosis, undetected failures, and PM. This restriction of the Boolean methods can be overcome by an extension of these methods. Therefore, the Boolean methods are usually extended by complementary modeling methods to model the time dependencies.

The extension of the Boolean methods leads to the *Hybrid methods*. The complementary modeling methods are mostly State-based methods. The principle of the Hybrid methods is illustrated in figure 1.3. The individual SRS elements are modeled by the State-based methods, providing their $PFD(t)$. Subsequently, the $PFD(t)$ of the entire SRS is calculated from the $PFD(t)$ of its individual elements via the Boolean structure function. Hence, the dependencies between elements are not modeled by the Hybrid methods. Moreover, the dependencies caused by the multiple failure modes of elements are not modeled in full details for reasons of simplicity. An SRS element with multiple failure modes is approximated by separately modeling each failure mode and combination of the submodels with a Boolean structure function, as shown in figure 1.4. Thus, the multiple failure modes are modeled equivalent to the independent series elements and the

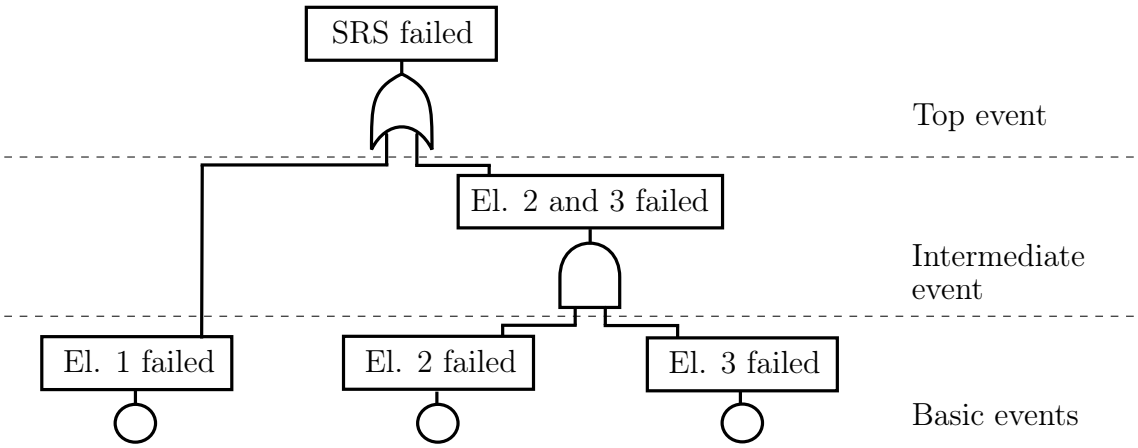

Figure 1.2: Fault tree

respective dependencies are neglected. Frequently, the multiple failure modes are even completely neglected, except one selected "dominant" failure mode. The Hybrid methods are often used in literature. [TE09] used the Hybrid method to model the SRSs behavior and determine the $PFD(t)$ and $\overline{PFD}$. The two failure modes, detected and undetected failures, were modeled. For every element only one type of PM, which provides a complete test coverage and is scheduled by a periodic PM plan with equal periods, was considered. In [BBB12], the Hybrid method was applied to analyze the impact of PM on the $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$. Two types of PM, one with complete test coverage and one with incomplete test coverage, were modeled. The considered PM plans were periodic with equal periods for the PM with high coverage and variable periods for the PM with low coverage. The so-called *α-test policy* was introduced to define the variable periods. The detected failures were neglected. Furthermore, the so-called *simplified equations* (SEs) are frequently used to directly calculate the $\overline{PFD}$. The SEs are mostly based on the Hybrid methods. The most often used SEs were introduced by [IEC11d]. Further important reference to mention is [HLHH10], more detailed SEs were presented in this handbook. Overall, for the SRSs with multiple failure modes, dependencies, and PM the Hybrid methods provide only approximated, inaccurate results. Despite these limitations, easily applicable probabilistic models to approximately calculate the SRSs figures of merit are provided by the Hybrid methods.

The *State-based methods* are capable to overcome the limitations of the Boolean and Hybrid methods described above. The state-based models consider the dependent elements, multiple maintenance actions, and multiple failure modes. The State-based methods comprise the Finite State Automata (FSAs), Markov chains (MCs), Petri nets, etc. The states of the elements of an SRS are represented by the model states. The failures and restorations resulting from the CM and PM are represented by the events triggering the state transitions. An SRS modeled by an FSA is shown in figure 1.5 to illustrate the State-based methods. The occurrence of an event indicating failure, i.e. f_1, f_2, f_3,

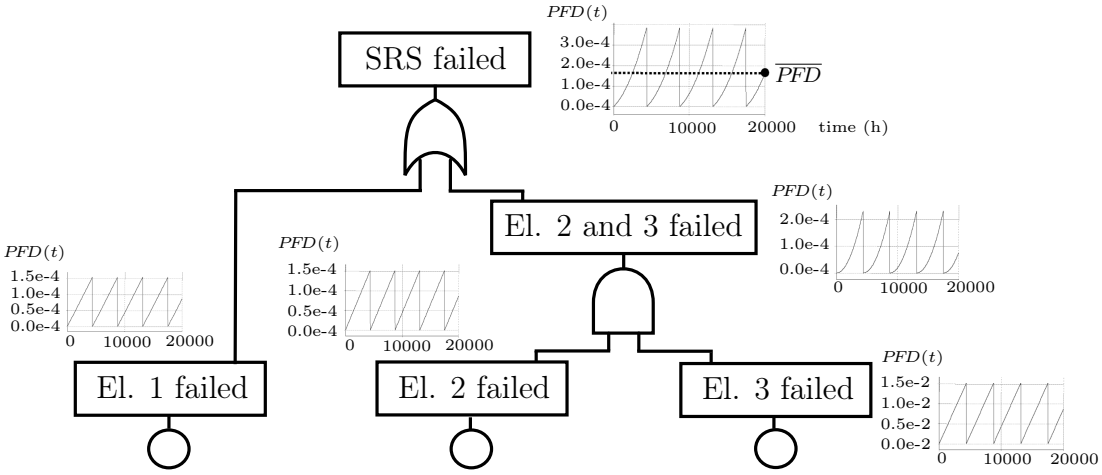

Figure 1.3: Principle of Hybrid methods

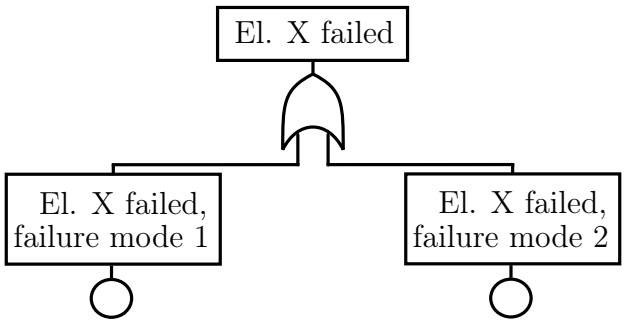

Figure 1.4: Approximation of multiple failure modes via Hybrid method

or restoration, i.e. r_1, r_2, r_3, triggers state transitions. The states set is subdivided into two subsets with the attributes U and $\overline{\text{U}}$, which indicate whether the safety function is available in a given state or not. The $PFD(t)$ is given by the probability of the model states with the attribute $\overline{\text{U}}$. Generally, the challenge of the State-based methods is to cope with the large number of states emerging in models of SRSs with multiple elements and multiple failure modes. This challenge can be dealt with, as was shown in [Gab10] and is shown in this thesis. In [CL08], the Stochastic Timed Automata (STAs) were introduced to model the behavior of systems triggered by discrete and arbitrarily timed events. In fact, the STA is an FSA equipped with a stochastic event timing mechanism. The state transitions of an STA are triggered by the stochastic timed events. An STA enables to separate the model logic function, given by an FSA, from the model event timing, given by a timing mechanism. The timing of events is defined by an arbitrary cumulative distribution function (CDF). Thus, the STA is capable to model an SRS under consideration of arbitrarily timed events. The behavior of a given SRS can be simulated via the STA and the resulting events and states sequences, so-called *random walks*, can be generated.

However, one or even a small number of the random walks are not applicable to determine the figures of merit of interest for a modeled SRS. Either a large number of the random walks has to be generated and evaluated, leading to the *Monte-Carlo methods*,

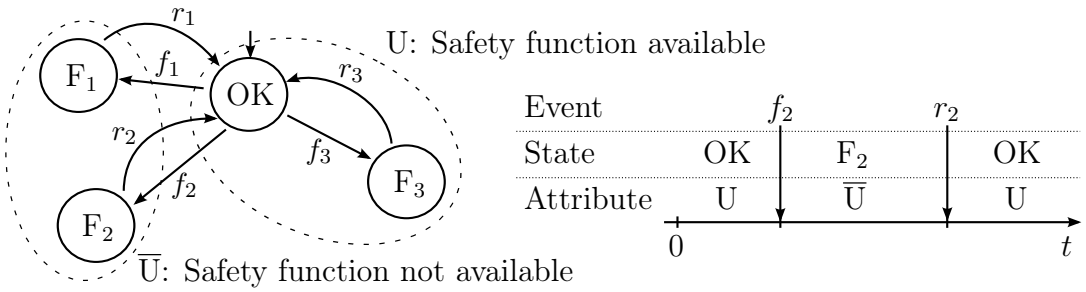

Figure 1.5: Principle of State-based methods

or the probabilistic model has to be analytically evaluated. This thesis follows the latter methodology, although the presented modeling framework is capable of random walks generation and might be used for Monte-Carlo methods. The Monte-Carlo methods were described in [Sob91] and are not further treated in this thesis.

In [CL08], the *stochastic process* generated by the STA was analyzed and identified as equivalent to the *Semi-Markov process*. Hence, the *Semi-Markov chains* can be applied to analytically evaluate the STAs. The $PFD(t)$ is determined by evaluation of the Semi-Markov chains state probabilities. The state probabilities are given by the transient solutions of the relative *integral equations*. These integral equations to calculate the Semi-Markov chains state probabilities can be found in [Bir10]. Overall, the Semi-Markov chains meet the requirements on the probabilistic modeling of SRSs, described at the beginning of the subsection. The application of the Semi-Markov chains is considered by the author to be more complex in comparison to further applicable methods. In [Bir10], the complexity of the Semi-Markov chains was assessed to be higher than that of the ordinary MCs. For that reason, the Semi-Markov chains are not selected to be applied and the review of probabilistic modeling methods is continued.

It was shown by [CL08] that, if the event timing of an STA is restricted to the exponential CDFs, the respective stochastic process will be equivalent to the *Markov process*. In this case, the STAs can be evaluated by the MCs that can be considered as an alternative representation of the STAs. Since it is common to assume the model event timing of an SRS to be distributed by the exponential CDFs, the MCs are widely applied to model the SRSs, e.g. they were applied in [Bir10], [Zio09]. For this purpose, the PM has to be either neglected or approximated by events with exponential CDFs. The state probabilities of the MCs are calculated to determine the $PFD(t)$. Either the *Discrete-time MCs* or the *Continuous-time MCs* can be used for the calculation of the state probabilities. The state probabilities of the Discrete-time MCs are evaluated by matrix multiplications for every time step of a constant step size, see [Gab10], [FF11]. In [FF11], the Discrete-time MCs were compared to the Continuous-time MCs. It was shown that, the Continuous-time MCs provide significantly higher computational efficiency. The state probabilities of the Continuous-time MCs are given by the transient solutions of the *ordinary differential equations* (ODEs). The order of the system of ODEs is given by the respective number

of model states. Efficient numeric ODE solvers are available to compute the transient solutions. The application of the MCs to model and evaluate industrial systems was described in the standard [IEC07]. In [Blu10], the Continuous-time MCs were applied to model and determine the probabilistic figures of merit of SRSs for the high demand mode and continuous mode of operation.

However, the scheduled PM, comprising of periodic proof tests and respective repairs, can not be precisely modeled via the MCs, since the respective event timing is not exponential, but deterministic. A technique to consider the PM by extension of the MCs was published in [BCO94]. For this purpose, the MCs were extended to the *Multi-phase MCs*. The PM is modeled via the so-called *phase transitions*. The phase transitions model the state transitions triggered by the deterministic timed events. This principle is illustrated in figure 1.6. The MC in figure 1.6 exhibits a phase transition that models the impact of a scheduled PM. The scheduled PM is modeled via a deterministic timed event that triggers the related state transition. In [Buk01], the Multi-phase Continuous-time MCs (MP-CMCs) were applied to model the impact of scheduled PM. [Gab10] modeled SRSs via the Multi-phase Discrete-time MCs (MP-DMCs) under consideration of the scheduled PM. In [FF11], the state of the art ODE solvers were applied to determine the $PFD(t)$ of a modeled SRS via evaluation of the MP-CMC state probabilities.

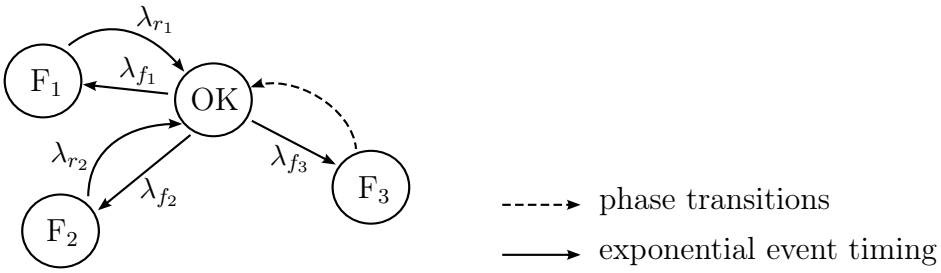

Figure 1.6: Use of phase transitions to model scheduled PM activities

It is concluded by the author that, the MP-CMCs meet the requirements on the probabilistic modeling of SRSs, which are described at the beginning of the subsection. Moreover, the application of the MP-CMCs is considered to be less complex in comparison to the Semi-Markov chains. Therefore, the MP-CMCs are applied in this thesis to determine the $PFD(t)$ of the SRSs. It takes considerable effort to model a given SRS, with the characteristics mentioned above, via the MP-CMCs. Hence, procedures to reduce the modeling effort are highly advantageous and were frequently applied to state-based models in literature. In [Blu10], the MCs modeling independent elements of an SRS were combined via the Kronecker and Cartesian products to determine the MC that models the entire SRS. However, this procedure does not handle dependent elements and phase transitions, which model the PM. [Gab10] proposed a generic approach to automatically generate the MP-DMCs for SRSs. This approach considers the dependencies resulting from multiple failure modes, *combinatorial voting*, *maintenance groups*, *inhibition*, etc.

These dependencies were incorporated in the given algorithm to generate the MP-DMCs for an SRS specified by the introduced formal description language. In this thesis, an alternative procedure to reduce the modeling effort is introduced. A special type of STAs, the *Stochastic and Deterministic Timed Automaton* (SDTA), is introduced and applied to model an SRS that is characterized as described above. The SDTA provides an automata-based probabilistic model that is more straightforward to apply for an engineer. Moreover, the analysis of the SDTA provides further insight into modeling and the relation to further modeling methods is better understood. The timing of events that are modeled via the SDTA are restricted to the exponential CDFs, except the events related to the PM. The latter, the so-called deterministic timed events, exhibit event timing resulting from the PM schedule. The modeling effort, that results from the large number of model states, dependencies of elements, and PM, is reduced by modeling of individual elements via SDTAs and subsequent automatic model composition. The defined parallel composition of SDTAs is applied for the model composition of the SDTAs modeling individual elements to receive the SDTA modeling an entire SRS. The analysis of an SDTA reveals its relation to the Multi-phase MCs. Hence, the MP-CMC can be considered as an alternative representation of the SDTA, which can be evaluated by the MP-CMC. The transformation to derive the respective MP-CMC for a given SDTA is provided in this thesis. Consequently, the MP-CMCs are applied to efficiently calculate the $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ of the SRSs modeled via the SDTAs.

The probabilistic modeling procedure presented in this thesis is illustrated in figure 1.7. In step 1, each element is separately modeled by an individual SDTA. The model of the entire SRS is determined via the introduced automatic composition operation in step 2. After that, this model is transformed in step 3 by means of a defined transformation into an MP-CMC. Finally, the MP-CMC provides efficient probabilistic evaluation of the model. The state probabilities and the figures of merit $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ are calculated.

1.2.4 Model analysis and optimization

The probabilistic models enable to determine the figures of merit $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ for the modeled SRSs. These figures of merit are determined from the set of the probabilistic model parameters of an SRS. The parameters are classified into the *failure parameters* and *maintenance parameters*. The failure parameters originate from the selection and installation of the SRS hardware. A widely accepted method to determine the failure parameters via statistics was presented in [Dü10]. In contrast to the failure parameters, the maintenance parameters are widely independent of the SRS hardware and related to the organizational measures of maintenance. The maintenance is further classified into the *corrective maintenance* (CM) and *preventive maintenance* (PM), as described

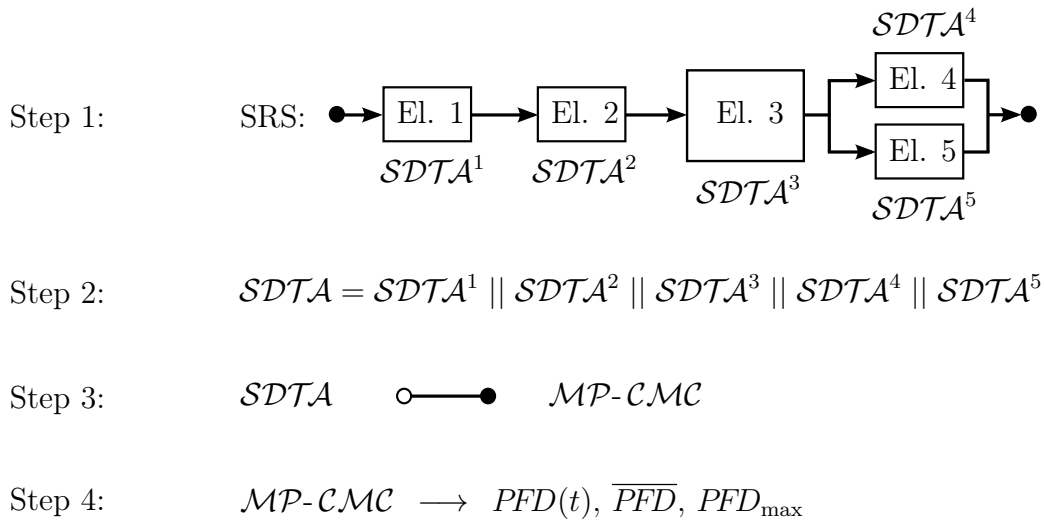

Figure 1.7: Probabilistic modeling procedure of this thesis

in [DIN10]. In this thesis, this classification is applied to the maintenance parameters. The PM is highly relevant for an SRS, as it is crucial to mitigate the undetected failures. Hence, the figures of merit of an SRS are strongly influenced by the PM parameters. The set of PM parameters defines the PM plan that schedules the applied PM activities. The PM plan is crucial for an SRS to meet the threshold for $\overline{PFD}$, which are regulated by [IEC11e]. Therefore, the PM plan has to be chosen to ensure that the mandatory threshold for the $\overline{PFD}$ is met. On the other hand, the PM activities within a PM plan require effort and generate expenses.

The probabilistic models introduced in this thesis support the PM plans with the features outlined hereafter. The supported PM plans are oriented towards those in industrial applications in the chemical and process industry. Up to two different types of PM for each element of an SRS are supported by a PM plan. One type of PM is referred to as the *regular PM activities*, which provide possibly incomplete coverage to reveal the undetected failures and repairs if necessary. For example, the valve in an application with highly poisonous fluids is not accessible to be dismounted, fully checked, repaired if necessary, and re-installed in the framework of a regular PM activity. Instead, the regular PM activity is carried out without dismounting of the valve, resulting in incomplete test coverage. Hence, some failures might remain not revealed. The *supplementary PM activities* are the second type of PM activities that are supported by a PM plan. These PM activities are usually fully automated, require very low effort and exhibit a lower test coverage compared to the regular PM activities. The supplementary PM activities are e.g. partial stroke tests of valves with repairs if necessary, software-based automated self-diagnosis tests of hardware with repairs if necessary, etc. It has to be emphasized that, the regular and supplementary PM activities include repair if necessary. In contrast, the term *proof test* is frequently used in literature. This term occasionally refers only to the PM activities that aim to reveal failures and does not consider repair. The proof test

and the respective repair if necessary are in the following denoted by PM. Eventually, all the PM activities within a supported PM plan might be arbitrarily scheduled for each element. This implies that no restrictions on a PM plan are given, e.g. such as being periodically scheduled with equal periods or simultaneous for all elements.

To the knowledge of the author, probabilistic models of SRSs that support PM plans offering all the outlined features have not been treated in literature. Traditionally, the PM activities scheduled by a PM plan were assumed to exhibit a complete coverage. Meanwhile, this assumption has been relaxed, see [IEC11e]. Additionally, the supplementary PM activities are increasingly considered in PM plans. However, the restriction on the PM activities to be periodically scheduled with equal periods is still common practice. The most PM plans treated in literature exhibit this restriction, see [IEC11e], [HLHH10], [TE09], etc. Just recently, [BBB12] introduced and analyzed the partial relaxation of this restriction. The analyzed PM plans were periodic with equal periods for the regular PM with complete test coverage, but periodic with variable periods for the supplementary PM. The so-called α-test policy was introduced to define the variable periods via a constantly low number of parameters. It was shown, the resulting $\overline{PFD}$ and $PFD_{\max}$ were significantly decreased by the variable periods of the supplementary PM, especially for redundant SRSs. In this thesis it is shown that, the introduced models with the supported PM plans considerably increase the degrees of freedom of the applied PM activities in comparison to the models in literature. The analysis of the introduced models shows that, the increased degrees of freedom might be used to improve the figures of merit and increase the effectiveness of an SRS.

A further target of this thesis is to achieve an improvement of the figures of merit via the increased degrees of freedom of the PM. The optimization was chosen to achieve this target. The introduced probabilistic models provide the relation between the figures of merit, i.e. $\overline{PFD}$ or $PFD_{\max}$, and the model parameters, e.g the applied PM plan, etc. In the field of mathematical optimization, this relation is named an objective function. The optimization aims at maximizing or minimizing the objective function by systematically choosing parameters from within an allowed set. Therefore, a decrease of the evaluated objectives is achieved by minimizing the $\overline{PFD}$, $PFD_{\max}$, or the weighted trade-off between the two former. In literature, the optimization has been previously applied to probabilistic models. An overview of the publications related to the SRSs is given hereafter. [TE09] presented a survey on the optimization of multiple objectives by evaluating numerous parameters, including the failure and PM parameters. A multi-objective Genetic algorithm was applied to the optimization problem. The $\overline{PFD}$, spurious trip rate, and life-cycle costs were used as the objective functions for optimization. The evaluated failure parameters were related to a given set of SRSs elements to select from, in order to construct an SRS that minimizes the given objectives. The considered PM plans contained only regular PM activities with complete test coverage and periodically scheduled with equal

periods. The evaluated PM parameters were the time to first PM activity, period duration of the PM activities schedule, and staggering factor of the PM activities schedules of redundant elements. In [ML11], the optimization was applied to determine the failure and PM parameters. Only periodic PM plans with equal periods and regular PM activities were considered, staggering was not treated. The periods of the PM activities schedule were determined for a given SIL and variable SRS element structure. The optimization problem was solved via an enumeration algorithm. The SRS element structure, consisting of elements from a given set and minimizing the life-cycle costs, was determined. Overall, it is confirmed that an increase in parameters of the objective function, which is the probabilistic model, leads to increased complexity of the optimization problem.

In this thesis, the focus of optimization is put on the parameters related to the PM plans of the introduced probabilistic models. The decision not to consider further parameters, e.g. the failure parameters, for the optimization is motivated by the number of optimization parameters. Due to the detailed modeling of the PM plans by the introduced models, the number of PM parameters is significantly greater than in literature models. Hence, further parameters would increase the complexity of the optimization problem even more and are therefore not considered. Moreover, the focus of optimization on PM parameters is also justified for another reason. The PM parameters are related to organizational measures and therefore easier to vary in contrast to the failure parameters, which are related to hardware. The resulting optimization problems are evaluated via the Nelder-Mead method of heuristic optimization. It is demonstrated that, the applied optimization algorithm effectively evaluates the treated optimization problems via the available computation resources. A framework to determine a PM plan that increases the effectiveness of an SRS is provided.

1.3 Novel contributions

The novel contributions of this thesis are itemized below.

Probabilistic modeling

- Models based on SDTAs and MP-CMCs that are intended for SRSs with PM, multiple failure modes, and dependent elements and provide efficient calculation of $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$

- Modeling framework to model individual elements and automatically compose the model of the entire SRS

- Definition of PM strategies to classify the available degrees of freedom of PM

Model analysis and validation

- Modeling of selected practically relevant SRSs and analysis
- Validation of the introduced models via selected established models from literature
- Sensitivity analysis of parameter variations related to PM

Optimization of PM plans

- Formulation of the optimization problems to minimize $\overline{PFD}$ or $PFD_{\max}$ or trade-off between $\overline{PFD}$ and $PFD_{\max}$ via variation of PM
- Application of Nelder-Mead method to solve the optimization problems
- Optimization of PM for selected practically relevant models of SRSs and analysis of results
- Set of rules to decide for a given SRS if the $\overline{PFD}$ or $PFD_{\max}$ can be significantly improved via optimization of the PM

1.4 Organization

The organization of this thesis is oriented towards the novel contributions formulated in section 1.3.

First, the technical terms and concepts, used in this thesis, are introduced in chapter 2. The used terminology is set in relation to established literature, such as international standards, recent publications, and specialized books.

The chapter 3 extensively treats the introduced models of SRSs. At the beginning, the modeling assumptions are discussed and the SDTA is defined in close connection to the concepts and characteristics of the modeled systems. A modeling procedure is introduced that features separate modeling of possibly dependent elements and composition of the entire model. The models with redundant elements are extended to consider the common-cause failures. Finally, the SDTA as the introduced new type of probabilistic models is discussed, its characteristics are described, and the relation to further models is treated.

In chapter 4, the definition of the MP-CMC is given first and the calculation of the $PFD(t)$ is described. It is based on the calculations of state probabilities. Afterwards, the SDTA transformation into MP-CMC is defined. That enables efficient calculation of $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ for systems modeled via SDTA. Moreover, the PM plans and restrictions of PM plans are defined and discussed. The PM strategies are defined as sets of PM plans with different applied restrictions.

The practically relevant SRS with one or three elements are modeled and analyzed in chapter 5. These models are validated via established literature models and the exclusive

features of the introduced models are demonstrated and discussed. Furthermore, the parameter variations related to the PM are analyzed and discussed.

In chapter 6, the handled optimization problems are first defined. The characteristics of the optimization problems and choice of the optimization algorithm are treated afterwards. Then, the Nelder-Mead method is described. A heuristic approach is introduced that is capable to overcome local minima and improves the minimization of the maximum PFD. The results of the optimization of selected practically relevant models are presented and discussed. Finally, a set of rules is presented to decide if the objectives for a given model can be significantly decreased by optimization.

In the end, the content of the thesis is summarized in chapter 7 in English and German. An outlook on future work is given.

Chapter 2

Safety-related Systems (SRSs)

2.1 Preliminaries

This chapter aims to introduce, clarify, and recapitulate the technical terms and concepts used in this thesis. Additionally, the introduced terminology is set in relation to the literature. Selected fundamental definitions related to the SRSs are introduced immediately hereafter. In section 2.2, the concepts related to the term *failure* are treated. The term failure is defined and subsequently the differentiation of the *random hardware failure* and the *systematic failure* is outlined in subsection 2.2.2. The failure categorization, based on the particular failure effect, failure detection, and the number of affected elements, is discussed in subsection 2.2.3. In conclusion, the failure categorization into *failure modes* is presented and the related events are defined. In section 2.3, the concepts related to *maintenance* are treated. The classification of maintenance into *corrective maintenance* and *preventive maintenance* is described. The events related to maintenance are defined. In section 2.4, the SRSs figures of merit are discussed. The general characteristics reliability and availability are recapitulated and set in relation to the *frequency of a dangerous failure* (PFH) and the *probability of dangerous failure on demand* (PFD).

The definitions given below are formulated according to the standard [IEC11b].

Definition 1 (Safety-related System (SRS)). The *SRS* refers to the system that implements "the required safety functions necessary to achieve or maintain a safe state", see [IEC11b].

The closely related term *Safety Instrumented System* is also often used in literature and specifies an SRS applied in the process industry sector, see e.g. [IEC05]. In practice, an SRS consists of multiple hardware components. The term *element* is introduced below to refer to a particular SRS hardware component or to a group of components.

Definition 2 (Element). The *element* comprises "a single component or any group of components that performs one or more element safety functions", see [IEC11b].

In some references the element is also referred to as *item*, e.g. [DIN10], [Bir10]. The elements subdivide an SRS into individual functional units of arbitrary complexity. Overall, an SRS might consist of one or multiple elements in series – parallel structure. The subdivision of large systems into subsystems complies with good engineering practice. For example, the SRS consisting of multiple elements is subdivided into elements to reduce the modeling complexity and effort. The separate modeling of individual elements is enabled. Subsequently, the element models are combined to obtain the entire SRS model. It has to be mentioned that, this thesis treats dependent elements of an SRS, in contrast to many literature references neglecting dependencies.

The *safety function* specifies the primary SRS functionality that aims to protect from the unacceptable risk.

Definition 3 (Safety function). The *safety function* refers to the function that is "intended to achieve or maintain a safe state", see [IEC11b].

If an individual SRS element is analyzed, the attention will be on its contribution to the safety function. The *element safety function* reflects this contribution.

Definition 4 (Element safety function). The *element safety function* refers to "that part of a safety function which is implemented by an element", see [IEC11b].

In the presence of parallel elements, which is referred to as *redundancy*, multiple elements simultaneously implement the same element safety function.

The following example 2.1 illustrates the terms definitions introduced above.

Example 2.1 (SRS hardware components, elements, safety function, and element safety functions). The SRS to prevent the overfilling of a vessel is illustrated in figure 2.1. The respective hardware components are shown in figure 2.2. The SRS is built up of sensors, barriers, logic solver, barriers, solenoids, and valves. The sensor part is built up of redundant hardware components and the final element part addresses two different vessel inflow pipes. The level in the vessel is measured via the two redundant sensors and the measured values are transferred via the barriers to the logic solver. The logic solver evaluates the measured values signals and generates the commands, transferred via the barriers to the solenoids. The valves are operated by the related solenoids according to the commands of the logic solver. One level sensor, the logic solver, and the final element subsystem, including barriers, solenoids, and valves, could be chosen as distinct elements of the SRS. Depending on the modeling, the exemplarily chosen elements can be merged or split up in further elements.

The safety function of the SRS is the following: The inflow valves to the vessel will be shut down if the level exceeds the given limit. The element safety function of the element level sensor is to provide a sufficiently exactly measured level value.

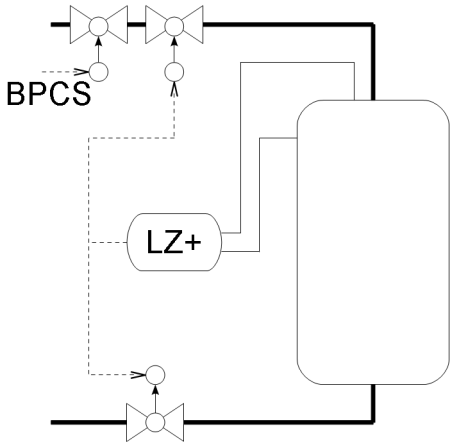

Figure 2.1: P&ID of SRS to prevent overfilling of a vessel; [Gab10]

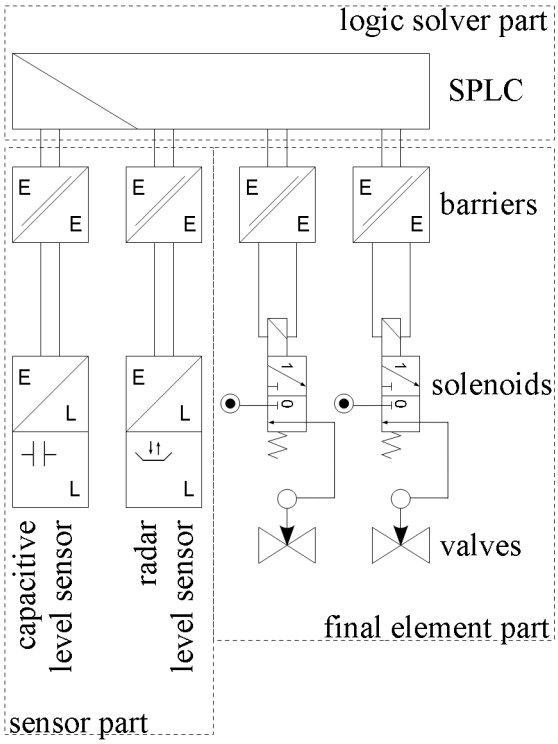

Figure 2.2: SRS hardware structure related to figure 2.1; [Gab10]

2.2 Failure

2.2.1 Definition

The definition given below is formulated according to the standard [IEC11b].

Definition 5 (Failure). The *failure* is the event that terminates the "ability of a functional unit to provide a required function", see [IEC11b].

In this thesis, the term *functional unit*, used in definition 5, refers to an SRS element. The term *required function* is intentionally not equivalent to the element safety function, introduced in definition 4. The required function refers to the perfect functionality of the respective SRS element, often denoted by *as good as new* or *operating as required*. Particularly, the following functions of an SRS are included in the required function: (1) to provide the safety function and (2) to avoid spurious operation of the SRS. However, the ability to provide the safety function is the most crucial part of the ability to provide the required function.

2.2.2 Random hardware failure vs. systematic failure

Next, the failures of an SRS are differentiated between the *random hardware failures* (RHFs) and the *systematic failures* (SFs). The RHFs and the SFs have different failure

mechanisms and consequently require different procedures to deal with. Therefore, it has become common to strictly differentiate between the RHFs and the SFs. For example, in [IEC11b] the RHFs and the SFs were defined and strictly differentiated. The procedures to deal with these failures were given.

The definitions given below are formulated according to [IEC11b] and [HLHH10].

Definition 6 (Random hardware failure (RHF)). The *RHF* results "from the natural degradation mechanisms", see [HLHH10]. Additionally, for the RHF it is assumed that "the operating conditions are within the design envelope of the system".

Definition 7 (Systematic failure (SF)). The *SF* is "related to a particular cause other than natural degradation and foreseen stressors", [HLHH10]. The SF "can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors", see [IEC11b].

Occasionally, the RHFs are alternatively named *physical failures* in literature, even though this term does not definitely characterize the RHFs. In contrast, the SFs are alternatively named *non-physical failures*. The same remark as above holds here.

The differentiation between the RHFs and the SFs appears reasonable from theoretical point of view, but in practice it is often difficult to differentiate between them. In the following, further characteristics and examples are given to clearly contrast the RHFs with the SFs. The RHFs are not present at the startup of an SRS. In contrast, at least the causes of the SFs are initially present at startup. An SF might prevent the related element from performing its required function even though it is still able to operate, as shown in the following example 2.2.

Example 2.2 (SF of pressure transmitter). A pressure transmitter failure occurs due to a plugged sensing line. Then, the pressure transmitter failure is caused by wrong design of the sensing line, which has been initially present at startup.

Example 2.3 (SF of flow transmitter). The unforeseen vibration of a pump causes a failure of the flow transmitter, which is located on the connected piping.

The pressure transmitter failure of example 2.2 is clearly indicated as an SF and the alternative denotation as a *non-physical failure* fits very well. Contrarily to example 2.2, an SF might also result in a *physical failure*. Evidently, a *physical failure* of the flow transmitter occurs in example 2.3. Nevertheless, the failure of the flow transmitter is clearly indicated as an SF.

The RHFs arise over time and can be causally traced back to the affected element of the respective SRS. The following examples 2.4 and 2.5 illustrate two possible RHFs.

Example 2.4 (RHF of sensor converter). A sensor converter failure occurs due to a transistor failure that is caused by aging of the semiconductor.

Example 2.5 (RHF of relay). A relay failure occurs due to wear out within operating conditions.

The RHFs always occur at a random time. For the SFs it holds that, as stated in [Bir10], "they can appear as if they were randomly distributed in time". In such cases the SFs might be erroneously classified as RHFs, e.g. if a failure occurs due to faulty software. If the software sequence related to the failure is infrequently executed, it will appear as if this failure is randomly distributed in time. An RHF occurs when an element has "degraded to a point of failure where it is not able to operate and thus needs to be changed or repaired", [HLHH10]. Multiple elements are never simultaneously affected by RHFs. In contrast, the SFs can simultaneously affect multiple elements. These SFs are referred to as *common-cause failures*. The SFs can be eliminated by use of suitable countermeasures, e.g. these regulated by the standard [IEC11e]. At least, they have to be reduced to a negligible number by the applied countermeasures. The SFs mostly cannot be quantified. In contrast, the RHFs can not be eliminated by means of the countermeasures for the SFs. Thus, the RHFs are dealt with by quantifying them.

The differentiation of RHFs and SFs is outlined above. However, some failures require unreasonable effort to fit into the above classification or may not fit at all. The failure classes RHFs and SFs overlap in practice, as pointed out in [HLHH10]. Hence, it is very difficult to classify an observed failure as an aging failure, i.e. RHF, or as a stress failure, i.e. SF.

The question, whether the characteristics of an SRS have to be quantified only based on RHFs, is controversial. It is further discussed below. To quantify the characteristics of an SRS only based on RHFs seems to be straightforward and has been frequently proposed in literature. In particular, [IEC11e] recommends this procedure. The SFs are neglected, motivated by the mandatory regulations to eliminate them and the difficulties to quantify them. However, a gap between the predicted SRSs figures of merit compared to the observed figures of merit or the experience-based figures of merit occurs. This is explained by the procedure to strictly differentiate between RHFs and SFs. A considerable amount of the SFs may be not completely excluded by the applied countermeasures to eliminate them. Nevertheless, these failures are excluded from the quantitative evaluations of the SRSs characteristics. Some RHFs are therefore often erroneously classified as SFs, especially by the manufacturer of the SRSs. Due to that, the parameter estimations regarding the RHFs may provide too optimistic results. In consequence, the predicted SRSs figures of merit, which are based on the estimated parameters, do not match with the actual ones.

In [HLHH10], it was proposed to determine the SRSs figures of merit in a more realistic way, in consideration of the RHFs and all quantifiable SFs. It has to be emphasized that, it is widely accepted to quantify the SFs threatening multiple elements via the common-cause failures, see [IEC11e], [HLHH10]. In the same way, the failures applied in this thesis

to quantify the SRSs figures of merit are not limited to the RHFs, but also include the quantifiable SFs. To simplify notation, the term *failure* is used in the following to denote all quantifiable failures, including RHFs and SFs. Nevertheless, appropriate regulations to eliminate the SFs, especially the non-quantifiable ones, or at least to reduce these to a sufficient low level are still mandatory, see [IEC11e].

2.2.3 Failure modes

Within the classifications and definitions, given in the previous section 2.2.2, the failures treated in this thesis are further categorized in the following to model the impact of each individual failure category on the SRS. The *failure modes* that are differentiated for modeling are based on the failure categorization given below. Three dimensions for failure categorization are identified. The failures are categorized based on (1) the failure effect on the element safety function, (2) the failure detection, and (3) the number of affected elements.

First, the failure categorization based on (1) is described. The resulting failure categories are *dangerous failure*, *safe failure*, and *no-effect failure*. The failure categories are based on those differentiated by [IEC11b]. The *dangerous failure* is characterized to "prevent a safety function from operating", see [IEC11b]. The *safe failure* is characterized to "result in the spurious operation of the safety function", see [IEC11b]. The *no-effect failure* is characterized as a "failure of an element that plays a part in implementing the safety function, but has no direct effect on the safety function", [IEC11b].

The second dimension for the failure categorization is based on the failure detection. *Detected failure*, *undetected failure*, and *non-revealable failure* are differentiated. The *detected failure* is detected by the automatic on-line diagnostic tests or through normal operation. The characteristic of the detected failure is in accordance with the definition of the property *detected* in [IEC11b]. The *undetected failure* is not detected by the automatic on-line diagnostic tests or through normal operation. This failure can be revealed by the PM or upon a demand. The property *undetected* is accordingly defined in [IEC11b]. The *non-revealable failure* is neither detected by the automatic on-line diagnostic tests nor through normal operation or revealed by the PM. This failure can be revealed only upon a demand. The non-revealable failure results from the non-perfect PM, which provides incomplete coverage to reveal failures and is not able to completely reveal all the undetected failures, as mentioned in [IEC11d]. Overall, the coverage of the PM to reveal failures has a significant impact on the SRS and has to be modeled to obtain a precise model. It has to be emphasized that, in the standard [IEC11d] the non-revealable failures were not explicitly defined. Instead, the non-perfect PM, referred to as *proof test*, was considered via the proof test coverage (PTC) parameter. The extended categorization into undetected and non-revealable failures is proposed in this thesis. In earlier publica-

tions the non-revealable failures were occasionally denoted by *non-detectable failures*, e.g. in [ML12]. The non-revealable failures were also considered in [HLHH10], denoted by *test independent failures*.

Finally, the *common-cause failure* and *single element failure* are differentiated. The *common-cause failures* are the simultaneous failures of two or more separate redundant SRS elements that independently implement the same element safety function. These failures are "leading to system failure", see [IEC11b]. The *single element failure* is the failure of a single SRS element, complementary to the common-cause failures.

The failure categorization based on (1), (2), and (3) is illustrated in figure 2.3. It provides the basis to define the failure modes applied in this thesis for modeling of an SRS. The no-effect failures do not have an impact on the safety function or spurious operation of an SRS and are not further considered. The failure modes are defined in the following.

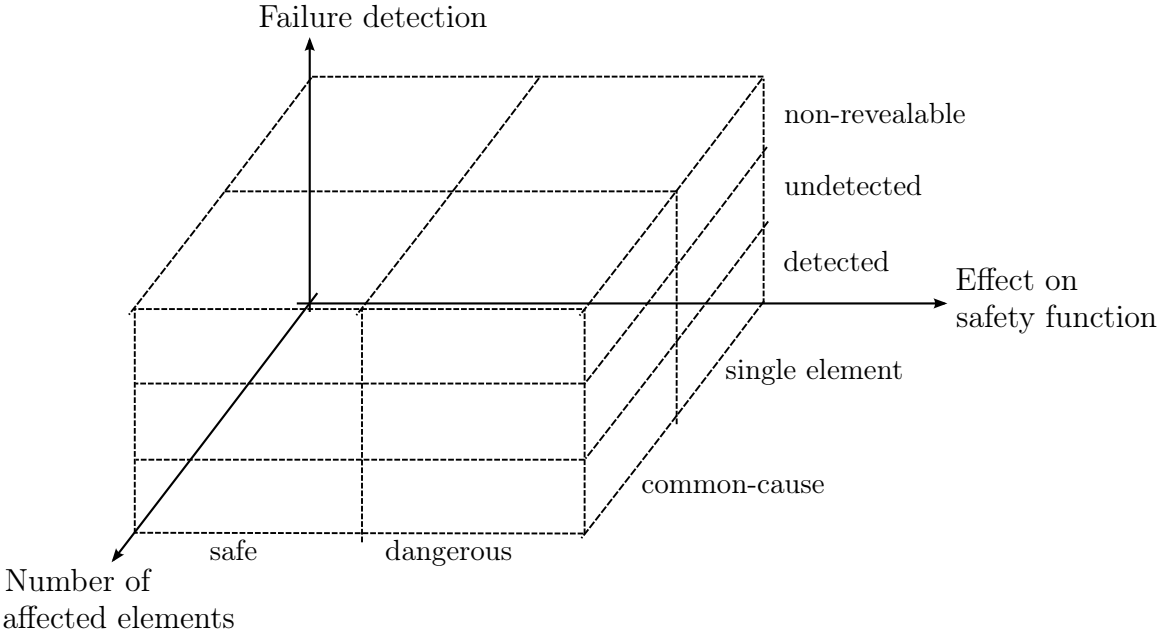

Figure 2.3: Failure categorization

Definition 8 (Safe failure mode (s)). The failures classified into the *safe failure mode* always cause *spurious operation* of the respective SRS element and are immediately detected. These failures are referred to as s-failures.

The *spurious operation of an SRS element* refers to the activation of the SRS element without the presence of a process demand. The *spurious operation of the SRS* might be caused by the spurious operation of an SRS element, depending on the SRS configuration. The concept of spurious activation of SRSs was described in [LR08].

Example 2.6 (s-failure of sensor). An s-failure will occur if a sensor provides an erroneous signal, that the monitored measurement of the potentially hazardous application

has exceeded the given threshold. This is referred to as spurious operation of the SRS element "sensor". The erroneous signal triggers the SRS to initiate a shut down of the potentially hazardous application, as if a true demand occurred. This erroneous initiation of the SRS is named spurious operation of the SRS.

It is further mentioned that, in some references, e.g. [HLHH10], the s-failures were further subdivided into *safe detected failures* and *safe undetected failures*. The latter were considered as "undetected" failures in terms of the categorization given above and cause spurious operation. The former were considered as "detected" failures and do not cause spurious operation.

Definition 9 (Dangerous detected failure mode (dd)). The failures classified into the *dangerous detected failure mode* prevent the element safety function from operating and are detected by the automatic on-line diagnostic tests or through normal operation. These failures are referred to as dd-failures.

Example 2.7 (dd-failure of sensor). A sensor gets stuck and is not able to respond upon a process demand. If this failure is detected by the automatic on-line diagnostic tests or through normal operation, it will be a dd-failure.

The dangerous and undetected failures, resulting from the failure categories described above, are further categorized in this thesis. In literature, these failures are not further categorized. The further categorization, introduced below, aims to consider two different applicable types of PM for each element of an SRS. Hence, the SRS is modeled more detailed. The two considered types of PM are

- PM type A, introduced as the *regular PM activities*;
- PM type B, introduced as the *supplementary PM activities*.

The PM type B provides a lower coverage to reveal failures, compared to the PM type A. However, the failures revealed by the PM type B are also revealed by the PM type A. Moreover, it is assumed that some failures might be "non-revealable" and might be revealed neither by the PM type A nor type B. These failures might be revealed only upon a true demand of the SRS. This implies that, the introduced PM might provide an incomplete coverage to reveal failures. The resulting failure modes are defined below and illustrated by examples.

Definition 10 (Dangerous undetected failure mode AB (duab)). The failures classified into this failure mode prevent the element safety function from operating and are not detected by the automatic on-line diagnostic tests or through normal operation. These failures are revealed by the PM type A and type B and are referred to as duab-failures.

Example 2.8 (duab-failure of sensor). The duab-failure of a sensor is a dangerous and undetected failure, which is revealed either by the regular PM activities, e.g. a proof test, or by the less effective supplementary PM activities, e.g. an online field check and examination.

Definition 11 (Dangerous undetected failure mode A (dua)). The failures classified into this failure mode prevent the element safety function from operating and are not detected by the automatic on-line diagnostic tests or through normal operation. These failures are revealed only by the PM type A and are referred to as dua-failures.

Example 2.9 (dua-failure of sensor). The dua-failure of a sensor is a dangerous and undetected failure, which is revealed only by the regular PM activities.

Definition 12 (Dangerous non-revealable failure mode (dn)). The failures classified into this failure mode prevent the element safety function from operating and are not detected by the automatic on-line diagnostic tests or through normal operation. Moreover, these failures are neither revealed by the PM type A nor type B. These failures are revealed only upon a true demand and are referred to as dn-failures.

Example 2.10 (dn-failure of valve). The dn-failure is the failure of a valve, which closes during regular testing, but due to insufficient actuator force does not close upon a process demand situation, e.g. due to high process pressure.

The failure classification into failure modes, applied in this thesis, is illustrated in figure 2.4. It is compared with the failure classification introduced by [IEC11e]. The comparison shows that the failures classified as du*-failures by [IEC11e] are further subclassified in this thesis. Since the dangerous undetected failures are highly relevant for the probabilistic figures of merit, the introduced failure modes enable more precise modeling. Hence, the impact of two types of PM is modeled. Despite the safe failures were further subclassified by [IEC11e] into sd*- and su*-failures, these failures were not used for modeling. In contrast, the s-failures are used for the models presented in this thesis.

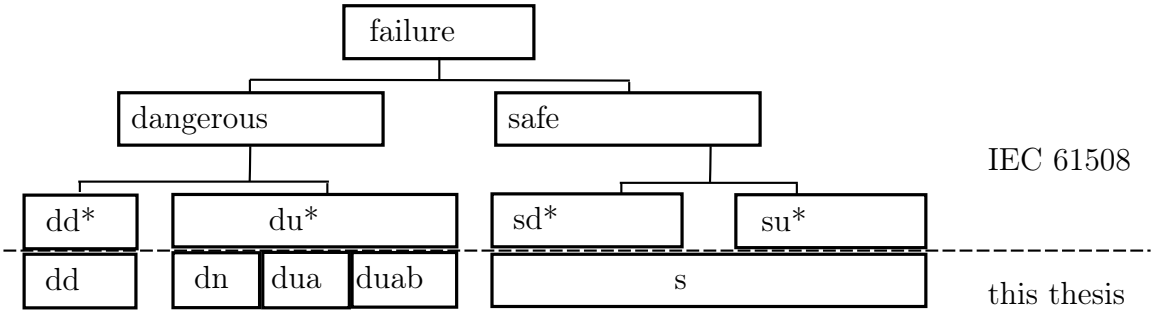

Figure 2.4: Comparison of failure classifications used by [IEC11e] and this thesis

Hereafter, events are defined for the introduced failure modes to proceed with the modeling of SRSs. An SRS with k elements is considered. The events set indicating single element failures is given by

$$\mathcal{E}_{SF} = \left\{ s_i, dd_i, duab_i, dua_i, dn_i : i \in \{1, \ldots, k\} \right\} , \tag{2.1}$$

where s_i denotes the s-failure of the element i, etc. The failures of $\mathcal{E}_{SF}$ are named analogously to the respective failure mode defined above.

The common-cause failures are related to the groups of redundant SRSs elements. These failures are denoted by cc-failures. Let the m groups of elements, which independently implement the same element safety function and are subject to common-cause failures, be denoted by the elements numbers set $\mathcal{GE}_j$,

$$\mathcal{GE}_j = \left\{ p, \ldots, r : p, \ldots, r \in \{1, \ldots, k\} \right\} , \tag{2.2}$$

where $p, \ldots, r$ denote the elements included in the group $j \in \{1, \ldots, m\}$ of redundant SRS elements and $p \neq r$ holds. The following assumptions hold for the common-cause failures.

Assumption 1 (Groups of elements do not overlap). It is assumed that

$$\mathcal{GE}_h \cap \mathcal{GE}_j = \emptyset, \quad \forall h, \forall j \in \{1, \ldots, m\},\ h \neq j, \tag{2.3}$$

i.e. an element can be assigned to only one group of redundant SRS elements.

Assumption 2 (Common-cause failure modes). The common-cause failures occur only for identical failure modes.

The events set indicating common-cause failures is given by

$$\mathcal{E}_{CF} = \left\{ s_{GEj}, dd_{GEj}, duab_{GEj}, dua_{GEj}, dn_{GEj} : j \in \{1, \ldots, m\} \right\} . \tag{2.4}$$

2.3 Maintenance

2.3.1 Preliminaries

The term *maintenance* was defined as the "combination of all technical, administrative and managerial actions during the life cycle of an item intended to retain it in, or restore it to, a state in which it can perform the required function", see [DIN10]. In this thesis the *items* addressed by maintenance are the elements of an SRS. The *required function*

that is restored by maintenance refers to the *maintenance objectives*. The latter include the restoration of the ability to perform the element safety function and the elimination of the spurious operation. Numerous *maintenance activities* were defined in [DIN10] to detail the maintenance actions. In this thesis, the individual maintenance activities are not addressed. Instead, the two maintenance types *corrective maintenance* (CM) and *preventive maintenance* (PM) are considered. These maintenance types are treated as entities including all the maintenance activities required to achieve the maintenance objectives. Overall, the CM and PM describe the processes eliminating the consequences of failures and resulting in *restoration*.

Definition 13 (Restoration). The *restoration* is defined as the "event at which the ability to perform as required is re-established, after a failure", see [DIN10].

In this thesis, the term *ability to perform as required*, used in definition 13, refers to the SRS condition when the maintenance objectives have been achieved. In the subsequent sections 2.3.2 and 2.3.3, the CM and PM are defined and discussed in more details. The given definitions are formulated in the style of the standard [DIN10].

2.3.2 Corrective maintenance

Definition 14 (Corrective maintenance (CM)). The *CM* is defined as the maintenance that is carried out after failure detection and intends to put the related element "into a state in which it can perform a required function", see [DIN10].

It has to be mentioned that, for the term *required function*, used in definition 14, the remark given in section 2.3.1 holds. For instance, when an s-failure or a dd-failure is detected, the CM will be immediately initiated and continue until restoration will occur. The failure detection time delay, resulting from the delay of the failure detection after the failure occurrence, is neglected. The CM events set of an SRS with k elements is given by

$$\mathcal{E}_{CM} = \left\{ cmdd_i, cms_i : i \in \{1, \ldots, k\} \right\} , \tag{2.5}$$

where $cmdd_i$, cms_i denote the events indicating that the CM of the element i has been completed after a dd-failure or an s-failure. The maintenance objectives for the element i have been achieved by then. Hence, the events $cmdd_i$, cms_i indicate restoration.

Example 2.11 (CM event $cmdd_i$). The element i is observed and assumed to be subject to dd-failures only. The element is new and failure-free at the time $t = 0$ when the observation is started. A dd-failure occurs at the time $t = t_{dd}$. During the time period from $t = t_{dd}$ until $t = t_{cmdd}$, the element i is not able to perform its element safety function. At the time $t = t_{cmdd}$, the CM event $cmdd_i$ occurs and indicates the restoration of the element i. From the occurrence of the CM event on, the element is able to perform

its element safety function until the next failure event will occur. It has to be emphasized that, the CM event can only occur after the dd-failure has occurred and as long as this failure has not been restored. The event sequence described above, related to failure and restoration, is visualized in figure 2.5.

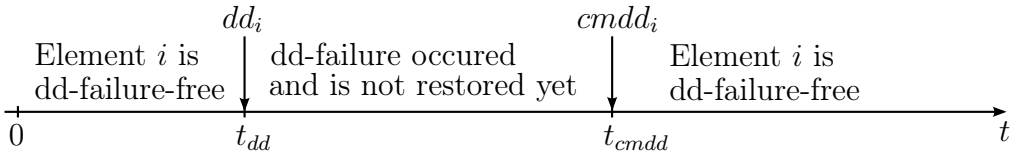

Figure 2.5: Sequence of CM events of example 2.11

2.3.3 Preventive maintenance

Definition 15 (Preventive maintenance (PM)). The *PM* is defined as the "maintenance carried out at predetermined intervals" and intends to "reduce the probability of failure or the degradation of the functioning" of the related element, see [DIN10].

It has to be noted that, the presented definition 15 implies multiple aspects of the PM. These aspects were specified in [Bir10]. The PM is considered to be necessary to (I) "avoid wearout failures" and (II) "to identify and repair undetected failures", see [Bir10]. The focus of the PM treated in this thesis is on (II), the *wearout failures* are not treated.

The PM that is treated in this thesis aims to reveal the undetected failures, i.e. the dua-, duab-failures, and to achieve restoration of the affected elements. The PM consists of two parts:

1. PM activities to reveal the failures,
2. PM activities that provide repair and achieve restoration.

This two-part structure is reflected by the defined PM events that indicate the termination of each PM part. The PM events set of an SRS with k elements is given by

$$\mathcal{E}_{PM} = \left\{ pma1_i, pma2_i, pmb1_i, pmb2_i : i \in \{1, \ldots, k\} \right\} , \tag{2.6}$$

where $pma1_i$ is the event indicating the revealing of the dua- or duab-failure of the element i via the PM type A. The revealing of the failure via the PM is assumed to be instantaneously and is modeled via the respective event. As soon as a failure is revealed, the PM activities to achieve restoration will be initiated. When the PM activities to achieve restoration are completed, the event $pma2_i$ will occur. Respectively, the event $pmb1_i$ indicates the revealing of the duab-failure of the element i via the PM type B and $pmb2_i$ indicates the restoration. It has to be emphasized that, the introduced framework neglects the duration of the PM activities to reveal failures. It is assumed that, the

failures are revealed immediately when the respective PM activities are initiated. Thus, the events $pma1_i$, $pmb1_i$ indicate the initiation of the PM activities and the revealing of failures if these are present.

The times of the events $pma1_i$ and $pmb1_i$ are deterministic and assumed to be scheduled in advance within a *PM plan*. Particularly, the PM plan defines the times of $pma1_i$ and $pmb1_i$, for all $i \in \{1, \ldots, k\}$, that comprise the k elements of an SRS. Moreover, the PM plans are categorized into *PM strategies*. The PM strategies imply restrictions on the PM plans, e.g. the times of $pma1_i$ and $pmb1_i$ being restricted to be periodic with equal periods, etc. The PM strategies treated in this thesis will be introduced in the chapter 4, subsection 4.4. Until then, arbitrary PM plans without further restrictions are assumed.

The event $pma1_i$ or $pmb1_i$ will always occur at the predetermined times, given by the PM plan, whether a failure occurs or not. In contrast, the event $pma2_i$ or $pmb2_i$ will only occur if the event $pma1_i$ or $pmb1_i$ occurs before. This is comparable to the CM events, i.e. $cmdd_i$, cms_i, that will only occur if the respective failure event, i.e. dd_i, s_i, occurs before. The following examples 2.12, 2.13 illustrate the event characteristics described above.

Example 2.12 (PM events $pma1_i$, $pma2_i$ occur after failure). The element i is observed and assumed to be subject to the dua-failures only. A dua-failure of the observed element occurs, i.e. the event dua_i occurs. After some time the PM is carried out. Within the first part of the PM the dua-failure of the element i is revealed, i.e. the event $pma1_i$ occurs. Immediately after the failure is revealed, the PM activities to achieve restoration are initiated. When these PM activities are completed, the event $pma2_i$ will occur. The sequence of PM events results in condition changes of the observed element. The figure 2.6 visualizes the sequence of PM events.

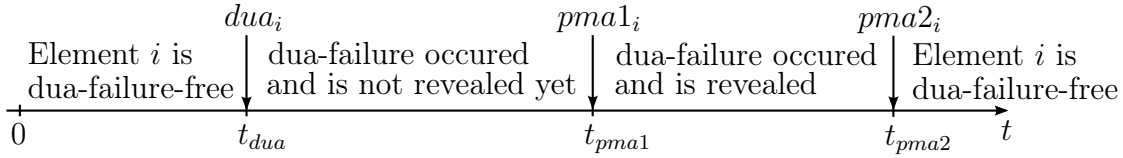

Figure 2.6: Sequence of PM events of example 2.12

Example 2.13 (PM event $pma1_i$ occurs when element is failure-free). The element i is observed and the same assumptions as in example 2.12 hold. The time $t = t_{pma1}$ of the scheduled in advance PM activities arrives when no dua-failures of the element i have occurred. Then, the event $pma1_i$ will occur and there will be no condition change of the observed element, as shown in figure 2.7. Thus, in contrast to the CM events, e.g. $cmdd_i$, the PM events $pma1_i$, $pmb1_i$ occur independently of the element failures. This is not the case for the PM events $pma2_i$, $pmb2_i$, which can only occur successively to the events $pma1_i$, $pmb1_i$.

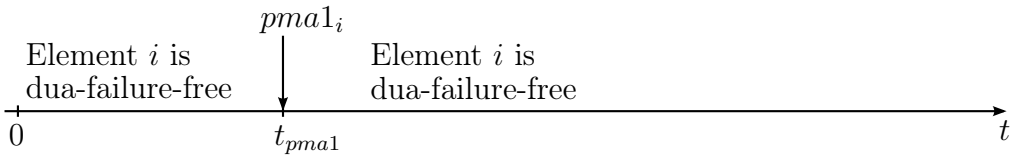

Figure 2.7: Sequence of PM events of example 2.13

2.4 Figures of merit

2.4.1 Preliminaries

The introduced events, that are related to the failures and maintenance, influence the condition of an SRS. In the subsequent sections 2.4.2 and 2.4.3, the figures of merit definitions that are applied to the SRSs are discussed. The given definitions are formulated in the style of [Bir10] and [Lit01].

2.4.2 Reliability and frequency of a dangerous failure (PFH)

The *lifetime distribution function* $F(t)$ is given by

$$F(t) = \Pr(T_F \leq t) \ , \tag{2.7}$$

where T_F is the random variable of the time in which the SRS continuously performs its assigned safety function or is in spurious operation. The *reliability function* $R(t)$ is the complementary function to $F(t)$,

$$R(t) = \Pr(T_F > t) = 1 - F(t) \ . \tag{2.8}$$

The ability of an SRS to continuously remain able to provide its safety function during the time interval $(0, t]$ is quantified by $R(t)$ or $F(t)$. The spurious operation is permitted during this time. Usually, the $R(t)$ and $F(t)$ are determined *bottom-up*, by mathematical modeling of T_F.

The mean of the random variable T_F is referred to as the *mean time to failure* ($MTTF$), given by

$$MTTF = \mathbb{E}\left[T_F\right] = \int_0^\infty R(t)\, dt \ . \tag{2.9}$$

The $MTTF$ characterizes the random variable T_F and the functions $R(t)$, $F(t)$ by use of a single figure. Furthermore, the $MTTF$ can be estimated *top-down*, by observation of the analyzed SRS, e.g. by mean estimation via the method of moments from [HEK09]. The estimate of $MTTF$ is given by

$$\hat{MTTF} = \frac{1}{n} \sum_{i=1}^{n} t_{Fi} \ , \tag{2.10}$$

where $t_{F1}, \ldots, t_{Fn}$ are the realizations of T_F for the analyzed SRS. The estimated figure $\hat{MTTF}$ is applied to characterize the SRSs with unknown $R(t)$ and $F(t)$.

The *frequency of a dangerous failure* (PFH) was provided by the standard [IEC11e], as the relevant figure of merit for the SRSs in high demand- or continuous mode of operation. The PFH was referred to as the *probability of dangerous failure per hour* in numerous older references, leading to the abbreviation PFH that is still in use today. The instantaneous PFH is given by

$$PFH(t) = \lim_{\Delta t \to 0} \frac{F(t + \Delta t) - F(t)}{\Delta t} \ . \tag{2.11}$$

The $PFH(t)$ reflects the gradient of the lifetime distribution function $F(t)$ at the point t. Particularly, the $\overline{PFH}$, the average PFH for an analyzed time interval, is applied as the relevant figure of merit for the SRSs in high demand- or continuous mode of operation. The thresholds for the $\overline{PFH}$ were regulated by [IEC11e]. However, the focus of this thesis is on the SRSs in low demand mode of operation. Therefore, the PFH is not further treated. In the subsequent section 2.4.3, the availability and PFD are discussed.

2.4.3 Availability and probability of dangerous failure on demand (PFD)

The *availability function* $A(t)$ is given by

$$A(t) \ = \ \Pr\left(Z(t) = 1\right) \ , \tag{2.12}$$

where $Z(t)$ is the discrete random variable defined by

$$Z(t) \ = \ \begin{cases} 1, & \text{SRS either able to perform its safety function} \\ & \text{or in spurious operation at time } t \\ 0, & \text{otherwise} \end{cases} \ . \tag{2.13}$$

The ability of an SRS to perform its safety function or to be in spurious operation at a stated instant of time t is completely characterized by use of $A(t)$. Usually, the $A(t)$ is determined *bottom-up*, by mathematical modeling of $Z(t)$.

The average availability in the time interval $(t_1, t_2]$ is given by

$$\overline{A(t_1, t_2)} = \frac{1}{t_2 - t_1} \cdot \mathbb{E}\left[T_U(t_1, t_2)\right] = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(\tau) \, d\tau \ , \tag{2.14}$$

where $T_U(t_1, t_2)$ is the random variable of the time in which an SRS performs its safety function or is in spurious operation during the time interval $(t_1, t_2]$. The mean of $T_U(t_1, t_2)$ is denoted by $\mathbb{E}\left[T_U(t_1, t_2)\right]$. The $\overline{A(t_1, t_2)}$ can be estimated *top-down*, by observation of

the analyzed SRS. The estimate of $\overline{A(t_1, t_2)}$ is given by

$$\hat{\overline{A(t_1, t_2)}} = \frac{1}{t_2 - t_1} \cdot \hat{\mathbb{E}}\left[T_U(t_1, t_2)\right] \ , \tag{2.15}$$

where the estimate $\hat{\mathbb{E}}\left[T_U(t_1, t_2)\right]$ is given by

$$\hat{\mathbb{E}}\left[T_U(t_1, t_2)\right] = \frac{1}{n} \sum_{i=1}^{n} t_{U,i} \tag{2.16}$$

and $t_{U,1}, \ldots, t_{U,n}$ are the realizations of $T_U(t_1, t_2)$ for the analyzed SRS. The estimated figure $\hat{\overline{A(t_1, t_2)}}$ is applied to characterize an SRS with unknown $\overline{A(t_1, t_2)}$.

For the SRSs in low demand mode of operation the *probability of dangerous failure on demand* (PFD) was provided by [IEC11e] as the relevant figure of merit. The instantaneous PFD is given by

$$PFD(t) = 1 - A(t) \ . \tag{2.17}$$

The $PFD(t)$ is the complementary function to the $A(t)$ and reflects the instantaneous *unavailability*. Particularly, the $\overline{PFD}$, the average PFD for an analyzed time interval, is applied as the relevant figure of merit for the SRSs in low demand mode of operation. The $\overline{PFD}$ is given by

$$\overline{PFD}(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} PFD(t)\, dt \ . \tag{2.18}$$

The time interval $(t_1, t_2]$, which is considered for the $\overline{PFD}$ calculation, usually comprises the mission time interval $(0, t_m]$ of the analyzed SRS. The mission time interval starts with the startup and lasts for the mission time until the SRS is decommissioned or replaced. In some references, the mission time is also referred to as *useful life time*.

In addition to the $\overline{PFD}$, in [IEC11c] it was proposed to evaluate the $PFD_{\max}$ over the mission time of the analyzed SRS. However, no requirements have been specified for the $PFD_{\max}$. From the point of view of the author the $PFD_{\max}$ is an important additional figure of merit to quantify the effectiveness of an SRS. The $PFD_{\max}$ over the mission time interval is given by

$$PFD_{\max} = \max(PFD(t)) \quad 0 \leq t < t_m \ . \tag{2.19}$$

Overall, the $PFD(t)$ is considered in this thesis as the figure of merit of major interest for the analysis of an SRS. The further figures of merit, such as $\overline{PFD}$ and $PFD_{\max}$, can be directly determined from the $PFD(t)$. The relation of the $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ is shown in figure 2.8 for an SRS with redundancy and PM.

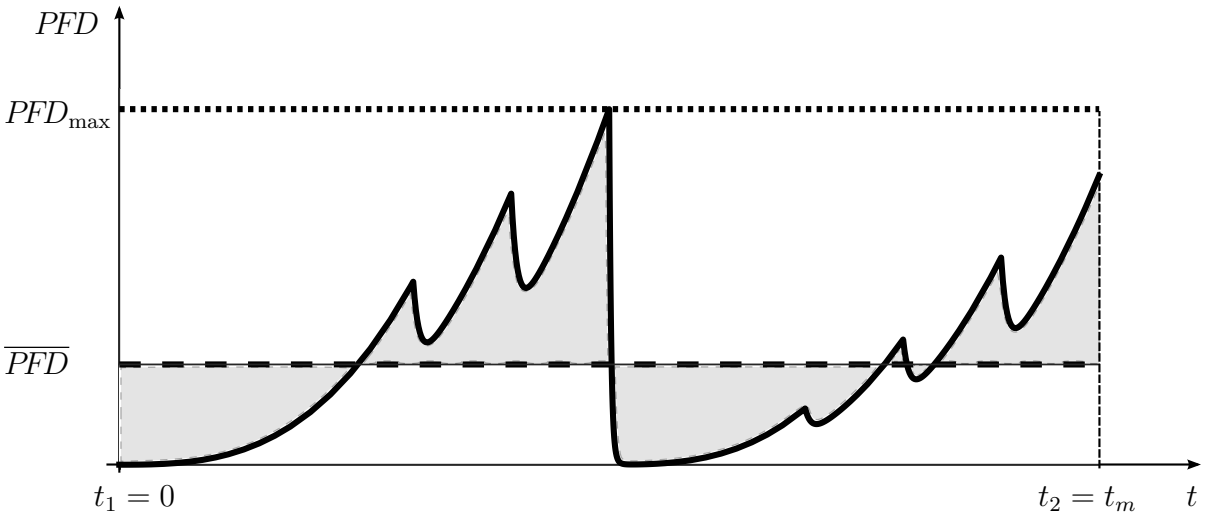

Figure 2.8: Relation of the $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$

Chapter 3

Modeling via Stochastic and Deterministic Timed Automata (SDTAs)

3.1 Preliminaries

The SDTA that models an SRS is introduced in this chapter. First, the modeling assumptions are described immediately hereafter. In section 3.2, the definition of SDTA is given. The procedure to determine the SDTA for an SRS with multiple elements is presented in section 3.3. Eventually, the SDTAs are further characterized and discussed in section 3.4.

Now, the modeling assumptions are treated. The events that influence an SRS were described in chapter 2. These events are related to failures, CM, and PM. The state transition of a probabilistic model reflects an SRS condition change that is caused by an occurring event. A discrete state model will be applicable to model an SRS if the following assumption holds.

Assumption 3 (Model states and transitions). The SRS is characterized by a finite number of states. All state transitions are deterministic. Thus, for every state an occurring event causes a state transition to a unique adjacent state.

Usually, the probabilistic model is evaluated for the time interval that begins at startup of the respective SRS. At startup an SRS is considered to be failure-free. Therefore, the following assumption is introduced.

Assumption 4 (Initial model state). The initial state of the SRS model is the fully operational and failure-free state.

The failures of an SRS are classified into multiple failure modes, as described in subsection 2.2.3 of the last chapter. The following assumption is introduced for the failures

of an SRS element. This assumption is also frequently used in literature. For instance, it was introduced in [Bir10], where it was referred to as *no further failures at system down*.

Assumption 5 (No further failures). No further failures occur in an SRS element as long as the repair after the previous failure has not been completed.

The following assumption results directly from the definition of the PM, see subsection 2.3.3.

Assumption 6 (PM times). The PM is carried out at scheduled times irrespective of the current SRS state.

At first glance it might appear useless to carry out PM if the SRS is in a failure-free state. This assumption is better to understand if the objective of the PM is recapitulated. That objective is to reveal undetected failures, i.e. the dua- and duab-failures, and provide repair if necessary. Because of the undetected failures the current SRS state is usually not known. Hence, the PM is carried out though the respective SRS might be in a failure-free state.

3.2 SDTA definition

3.2.1 Preliminaries

The events, which were described in sections 2.2 and 2.3, are classified into the *deterministic timed events* or *exponential stochastic timed events*. The former are treated in subsection 3.2.2 and the latter in subsection 3.2.3. The events are classified in order to model the event timing of each event class separately. In subsection 3.2.4, the definition of an SDTA for an arbitrary number of elements is introduced. Moreover, examples are given to illustrate the definition.

3.2.2 Deterministic timed events

The set of the *deterministic timed events* of an SRS model with k elements is given by

$$\mathcal{E}_{det} = \left\{ pma1_i, pmb1_i : i \in \{1, \ldots, k\} \right\} . \tag{3.1}$$

The events $pma1_i$, $pmb1_i$ are related to the PM of the i-th element of an SRS and were described in subsection 2.3.3.

Definition 16 (Deterministic timed event (DTE)). The DTE h is deterministically timed via the SDTA timing mechanism for a given deterministic clock sequence $\mathcal{V}_h$.

The set of the deterministic clock sequences $\mathcal{V}_h$ is given by

$$\mathcal{V} = \{\mathcal{V}_h : h \in \mathcal{E}_{det}\} , \tag{3.2}$$

where $\mathcal{V}_h = (v_{h,1}, \ldots, v_{h,ne_h})$ is the deterministic clock sequence of the DTE h. The deterministic clocks are characterized by $v_{h,j} \in \mathbb{R}^+$, for all $j \in \{1, \ldots, ne_h\}$. The length ne_h of the deterministic clock sequence $\mathcal{V}_h$ denotes the execution number of the PM related to the DTE h. It has to be noted that, the PM plan of an SRS that is modeled by an SDTA is specified by $\mathcal{V}$. The deterministic clocks $v_{h,1}$, ..., v_{h,ne_h} give the relative times from the activation to the occurrence of the DTE h.

Here, the activation and occurrence of events has to be briefly explained. This subject will be detailed in subsection 3.2.4. An event becomes "active" when the SDTA enters a state where the event is permitted to occur. Once an event is active, the SDTA might enter a state where the event is not permitted to occur. In this case the event gets deactivated and becomes "not active". It has to be emphasized that, in this thesis the DTEs of an SDTA permanently remain active. This characteristic is the consequence of assumption 6 and ensures that the PM is carried out "at predetermined intervals", see definition 15. Hence, once a DTE becomes active, it will definitely occur when the time of the respective deterministic clock will be passed. In contrast to the DTEs, the *exponential stochastic timed events*, treated in subsection 3.2.3, do not permanently remain active.

The deterministic clock sequence of a DTE is illustrated by the following example.

Example 3.1 (Deterministic clock sequence). Let the deterministic clock sequence of $pma1$ be given by $\mathcal{V}_{pma1} = (1000\text{ h}, 500\text{ h}, 700\text{ h})$. Hence, the PM, related to $pma1$, will be executed $ne_{pma1} = 3$ times. The deterministic clocks define the relative times from the activation to the occurrence of $pma1$. Hence, $pma1$ will occur at the absolute times $t_1 = 1000$ h, $t_2 = 1500$ h, and $t_3 = 2200$ h. Because $pma1$ permanently remains active, the resulting t_1, t_2, t_3 are determined by summation of the given deterministic clocks.

3.2.3 Exponential stochastic timed events

The set of the *exponential stochastic timed events* of an SRS model with k elements is given by

$$\mathcal{E}_{stoch} = \{\mathcal{E}_{PMstoch} \cup \mathcal{E}_{SF} \cup \mathcal{E}_{CF} \cup \mathcal{E}_{CM}\} , \tag{3.3}$$

where $\mathcal{E}_{PMstoch} = \{pma2_i, pmb2_i : i \in \{1, \ldots, k\}\}$ is the set of the exponential stochastic timed PM events. These events were described in subsection 2.3.3. The sets of events $\mathcal{E}_{SF}$, $\mathcal{E}_{CF}$, and $\mathcal{E}_{CM}$ are related to the single failures, common-cause failures, and CM events. These events were described in subsections 2.2.3 and 2.3.2.

Definition 17 (Exponential stochastic timed event (STE)). The STE h is stochastically timed via the SDTA timing mechanism for a given stochastic clock sequence $\mathcal{W}_h$.

The set of the stochastic clock sequences $\mathcal{W}_h$ is given by

$$\mathcal{W} = \{\mathcal{W}_h : h \in \mathcal{E}_{stoch}\} \ , \tag{3.4}$$

where $\mathcal{W}_h = (w_{h,1}, w_{h,2}, \dots)$ is the stochastic clock sequence of the STE h. The stochastic clocks $w_{h,j} \in \mathbb{R}^+$, for all $j \in \{1, 2, \dots\}$, are realizations of the random variables $W_{h,j}$. The random variables $W_{h,j}$ are characterized by the set of CDFs given by

$$\mathcal{G} = \{G_h : h \in \mathcal{E}_{stoch}\} \ , \tag{3.5}$$

where each CDF $G_h(t)$, which is assigned to the STE h, is given by

$$G_h(t) = \Pr(W_{h,j} \leq t) = 1 - e^{-\lambda_h t} \ . \tag{3.6}$$

The parameter λ_h is the rate parameter of the exponential CDF. It is assumed that, the stochastic clock sequences $\mathcal{W}_h = (w_{h,1}, w_{h,2}, \dots)$ of arbitrary length will be generated via the given set of CDFs $\mathcal{G}$.

The stochastic clock sequence of an STE is illustrated by the following example.

Example 3.2 (Stochastic clock sequence). Let the stochastic clock sequence $\mathcal{W}_{dd}$ be determined by random number generation via the given exponential CDF with $\lambda_{dd} = 1.14 \cdot 10^{-6}$ h^{-1}. The random result is $\mathcal{W}_{dd} = (1.8078 \cdot 10^6 \text{ h}, 7.9372 \cdot 10^4 \text{ h}, 1.1416 \cdot 10^6 \text{ h})$. The stochastic clocks of $\mathcal{W}_{dd}$ will define the relative times from the activation to the occurrence of the STE *dd* if the event does not get deactivated.

3.2.4 Model of an SRS

The SDTA models an SRS that consists of an arbitrary number of elements.

Definition 18 (Stochastic and Deterministic Timed Automaton (SDTA)). The SDTA is the seven-tuple $\mathcal{SDTA}$, given by

$$\mathcal{SDTA} = (\mathcal{X}, \mathcal{E}, f_{\text{tr}}, \Gamma, x_{\text{init}}, \mathcal{V}, \mathcal{G}) \ . \tag{3.7}$$

The first five parameters of the SDTA define the *Finite State Automaton* (FSA) that is given by definition 19. The FSA is driven by the DTEs and STEs, which are fully specified by $\mathcal{V}$ and $\mathcal{G}$. The DTEs and STEs are timed by the SDTA timing mechanism that will be introduced in definition 20.

Definition 19 (Finite State Automaton (FSA)). The FSA is the five-tuple $\mathcal{FSA}$, given by

$$\mathcal{FSA} = (\mathcal{X}, \mathcal{E}, f_{\text{tr}}, \Gamma, x_{\text{init}}) \ . \tag{3.8}$$

The parameters of the FSA are as follows:

$\mathcal{X}$ is the set of states, $\mathcal{X} = \{1, 2, \dots\}$, $x \in \mathcal{X}$;

$\mathcal{E}$ is the set of events that can be expressed as the union of the two disjoint sets of events $\mathcal{E}_{det}$ and $\mathcal{E}_{stoch}$, i.e. $\mathcal{E} = \{\mathcal{E}_{det} \cup \mathcal{E}_{stoch}\}$, where $\mathcal{E}_{det} \cap \mathcal{E}_{stoch} = \{\}$;

f_{tr} is the transition function, $f_{\text{tr}} : \mathcal{X} \times \mathcal{E} \to \mathcal{X}$;

Γ is the active event function, $\Gamma : \mathcal{X} \to 2^{\mathcal{E}}$;

x_{init} is the initial state.

Example 3.3 (FSA). The FSA of an SDTA that models an SRS, which consists of one element, is discussed. The states/transitions diagram of the FSA is shown in figure 3.1. The set of states is $\mathcal{X} = \{1, 2, 3, 4\}$ and the initial state is $x_{\text{init}} = 1$. The set of events is $\mathcal{E} = \{cmdd, dd, dua, pma1, pma2\}$, where $pma1$ is the only DTE. The indices that indicate the relative element are omitted for clarity. The transition function for the state $x = 1$ is given by

$$f_{\text{tr}}(x = 1, h) = \begin{cases} 1 \text{ if } h = pma1 \ , \\ 2 \text{ if } h = dd \ , \\ 3 \text{ if } h = dua \ , \end{cases} \qquad h \in \Gamma(x = 1) \ ,$$

where the active event function for $x = 1$ is $\Gamma(x = 1) = \{pma1, dd, dua\}$. The rest of the FSA parameters can be easily derived from the states/transitions diagram. The FSA models the dd- and dua-failures, which might occur in the initial state. The dd-failures are repaired by CM and restoration is indicated by *cmdd*. The dua-failures are first revealed by PM indicated by $pma1$. After that, repair is carried out and restoration is indicated by $pma2$. The active events in one particular state trigger the transitions to the adjacent states. In the states/transitions diagram it is clearly visible that, the set of events that might occur in a state x is a subset of the set of events $\mathcal{E}$. The active event function $\Gamma(x)$ defines the set of events that might occur in a state x. It has to be emphasized that, the PM event $pma1$ might occur in every state due to assumption 6. In some states the occurrence of $pma1$ triggers a state transition to the same state, e.g. for $x \in \{1, 2, 4\}$. These state transitions reflect the PM activities that are carried out when no dua-failure has occurred.

The state transitions of an FSA are triggered by the occurring events, i.e. the DTEs and STEs. The event timing mechanism determines the next occurring event and the respective time. These are determined based on the active events in the current state and the respective event characteristics. The active events of a state x are given by the active event function $\Gamma(x)$. The FSA of an SDTA has to ensure that the DTEs

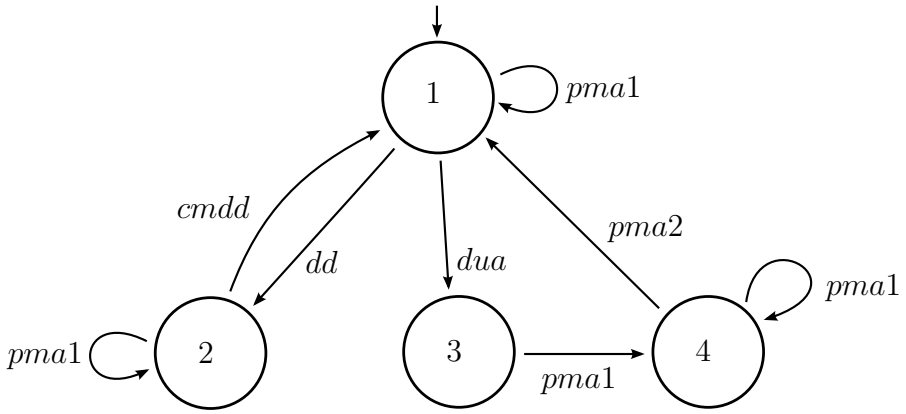

Figure 3.1: States/transitions diagram of the FSA in example 3.3

remain permanently active in all states. Hence, the FSA definition 19 is completed by the following restriction:

$$h \in \Gamma(x), \qquad \forall h \in \mathcal{E}_{det},\ \forall x \in \mathcal{X}. \tag{3.9}$$

The *SDTA event timing mechanism* is based on the *STA event timing mechanism* defined in [CL08]. The SDTA event timing mechanism provides event timing to the logical model that is given by the FSA. In this thesis, the defined SDTA event timing mechanism differentiates between STEs and DTEs. In contrast, the STA event timing mechanism defined in [CL08] does not differentiate. The following notation is adopted to avoid excessive use of subscripts:

x is the current state,

e is the most recent event (causing transition to state x).

Additionally, the following two variables associated with each event $h \in \mathcal{E}$ are defined:

n_h is the current score of event h, $n_h \in \{0, 1, \dots\}$;

y_h is the current clock value of event h, $y_h \in \mathbb{R}^+$.

The "next" state, event, event time, score, and clock value are denoted using the prime ($'$) notation as given in the following:

x' is the next state, given by $x' = f_{\mathrm{tr}}(x, e')$;

e' is the next event, it is $e' \in \Gamma(x)$;

$n_h{}'$ is the next score of the event h (after event e' occurs);

$y_h{}'$ is the next clock value of the event h (after event e' occurs).

The initial conditions are defined to determine the first event that occurs after the initialization of an SDTA. The initial event clock values y_h, for all $h \in \Gamma(x_{\text{init}})$, are given by

$$y_h = \begin{cases} v_{h,1} & \text{if } h \in \Gamma(x_{\text{init}}) \text{ AND } h \in \mathcal{E}_{det} \ , \\ w_{h,1} & \text{if } h \in \Gamma(x_{\text{init}}) \text{ AND } h \in \mathcal{E}_{stoch} \ . \end{cases} \tag{3.10}$$

The event clock values y_h, for all $h \notin \Gamma(x_{\text{init}})$, are undefined. The initial event scores n_h, for all $h \in \mathcal{E}$, are given by

$$n_h = \begin{cases} 0 & \text{if } h \notin \Gamma(x_{\text{init}}) \ , \\ 1 & \text{if } h \in \Gamma(x_{\text{init}}) \ . \end{cases} \tag{3.11}$$

The SDTA event timing mechanism iteratively generates the timed event sequence $\{\dots, e, e', e'', \dots\}$. It is assumed that the most recent event is e, the current state is x, the current event scores are n_h, and the current clock values are y_h, for all $h \in \mathcal{E}$. The next event e' and interevent time y^* are determined via the SDTA event timing mechanism given below. In the initial state the most recent event e is undefined.

Definition 20 (SDTA event timing mechanism). The next occurring event e' is given by

$$e' = \arg \ \min\{y_h : h \in \Gamma(x)\} \ . \tag{3.12}$$

The interevent time y^*, which is the period of time between the previous event e and the next event e', is given by

$$y^* = \min\{y_h : h \in \Gamma(x)\} \ . \tag{3.13}$$

The next state x' is determined via the transition function of the SDTA, $x' = f_{\text{tr}}(x, e')$, from the current state x and the next occurring event e'. The next clock values ${y_h}'$, for all $h \in \Gamma(x')$, are given by

$${y_h}' = \begin{cases} y_h - y^* & \text{if } h \neq e' \text{ AND } h \in \Gamma(x) \ , \\ v_{h,n_h+1} & \text{if } (h = e' \text{ OR } h \notin \Gamma(x)) \text{ AND } h \in \mathcal{E}_{det} \ , \\ w_{h,n_h+1} & \text{if } (h = e' \text{ OR } h \notin \Gamma(x)) \text{ AND } h \in \mathcal{E}_{stoch} \ . \end{cases} \tag{3.14}$$

For all $h \notin \Gamma(x')$ the ${y_h}'$ are undefined. The next event scores ${n_h}'$, for all $h \in \mathcal{E}$, are given by

$${n_h}' = \begin{cases} n_h & \text{if } h \neq e' \text{ AND } h \in \Gamma(x) \ , \\ n_h + 1 & \text{if } h = e' \text{ OR } h \notin \Gamma(x) \ . \end{cases} \tag{3.15}$$

Afterwards, the event e'', which is next to the event e', is determined starting the next iteration. The stochastic state sequence $\{x_{\text{init}}, \dots, x, x', x'', \dots\}$ is iteratively generated by the SDTA.

The definition of the SDTA event timing mechanism and generation of a state sequence appear complex at first view. However, the complexity mostly results from the formal notation. The basic idea is quite straightforward, as pointed out below. The SDTA is initialized via the equations (3.10), (3.11) and the following steps are iteratively executed to generate the state sequence:

1. Compare clock values for active events and determine the next occurring event e' via equation (3.12) and the interevent time y^* via equation (3.13);
2. Update the state via the transition function $x' = f_{\mathrm{tr}}(x, e')$, given by definition 19;
3. Update the clock values and event scores via equations (3.14), (3.15);
4. The "next" variables e', y_i', n_i', x' become current and the next iteration is restarted at step 1.

The following example illustrates the state sequence generated by an SDTA.

Example 3.4 (SDTA state sequence). The SDTA is considered that consists of the FSA in example 3.3. Let $\mathcal{V}$, $\mathcal{G}$ be given by

$$\begin{aligned}\mathcal{V} &= \{\mathcal{V}_{pma1} = (35040\text{ h}, 8760\text{ h}, 140160\text{ h})\}\ ,\\ \mathcal{G} &= \{G_{cmdd}, G_{dd}, G_{dua}, G_{pma2}\}\ ,\end{aligned}$$

where the rate parameters of the exponential CDFs in $\mathcal{G}$ are given by

$$\lambda_{cmdd} = 0.014\text{ h}^{-1},\ \lambda_{dd} = 1.5 \cdot 10^{-6}\text{ h}^{-1},\ \lambda_{dua} = 1.5 \cdot 10^{-6}\text{ h}^{-1},\ \lambda_{pma2} = 0.014\text{ h}^{-1}\ .$$

Let the respective stochastic clock sequences be

$$\begin{aligned}\mathcal{W}_{cmdd} &= (20\text{ h})\ ,\\ \mathcal{W}_{dd} &= (148530\text{ h}, 45524\text{ h}, 65964\text{ h})\ ,\\ \mathcal{W}_{dua} &= (29185\text{ h}, 2583500\text{ h}, 60405\text{ h})\ ,\\ \mathcal{W}_{pma2} &= (30\text{ h})\ .\end{aligned}$$

The random event and state sequences are iteratively generated by the SDTA. The steps described above are followed to determine the sequences. These sequences are illustrated in figure 3.2. The solid arrows mark the active events of a respective current state. The clock value of an active event is reflected by the length of an arrow. The dotted arrows mark an event that is deactivated. The respective times of the occurring events are given in table 3.1.

A note on the simultaneously occurring events has to be given because these are not considered by the timing mechanism in definition 20. First, it has to be noted that, two or

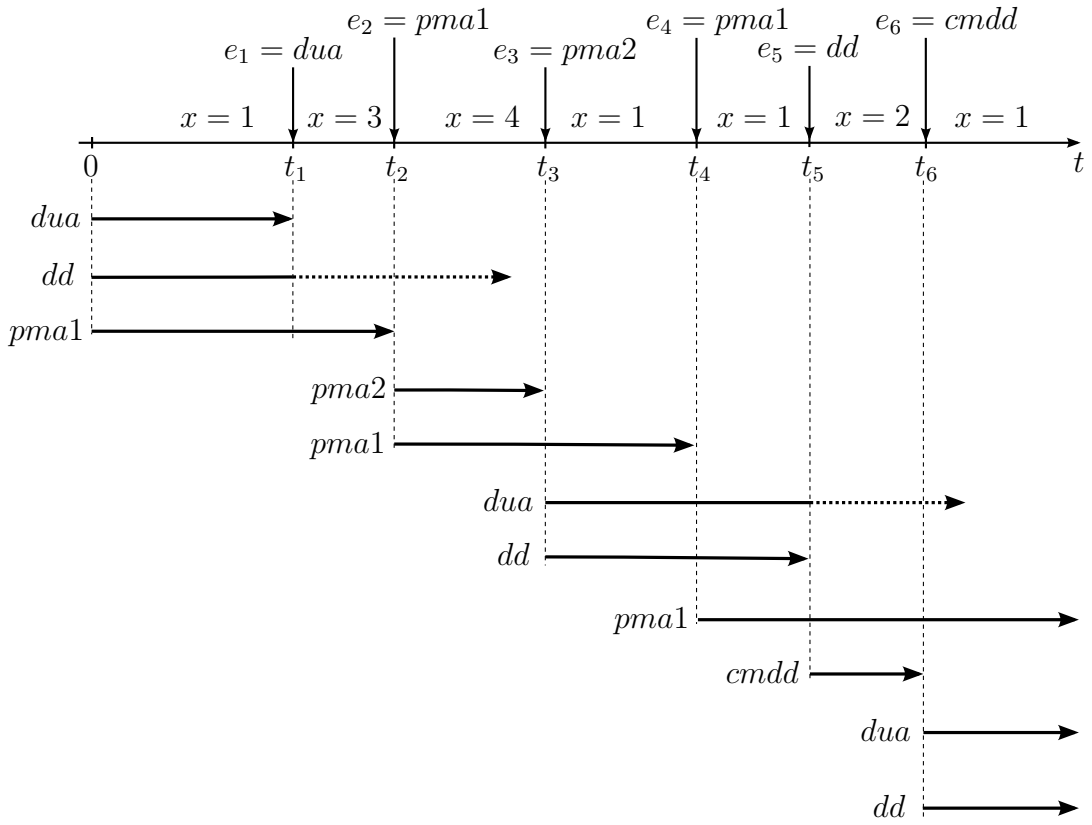

Figure 3.2: Timed sequence of events and states for example 3.4

t_1	t_2	t_3	t_4	t_5	t_6
29185 h	35040 h	35070 h	43800 h	80594 h	80614 h

Table 3.1: Event times of example 3.4

more STEs can occur at exactly the same time only with probability zero. This is implied by the respective CDFs being continuous over $[0, \infty)$. The same holds for a DTE and an STE that occur at the same time. However, multiple distinct DTEs might occur at the same time if e.g. the PM of multiple elements is carried out simultaneously. Therefore, it is assumed that priority rules over the event set $\mathcal{E}_{det}$ are given. These rules define which simultaneous DTE will affect the state first and also the sequence of the further DTEs, in case of more than two. Anyway, the final target state resulting from the sequence of simultaneous DTEs is independent of the priority rules for the treated models. This is due to the absence of DTE dependencies in the models that is indicated by each DTE being active in all states. Hence, the priority rules might be arbitrarily chosen for model implementation and evaluation of simultaneous DTEs.

The classification of SDTA states in regard to the safety function of the respective SRS is required to calculate the $PFD(t)$. It is introduced hereafter.

Definition 21 (State classification regarding safety function). The function that

classifies the states of an SDTA is given by $f_{\text{safety}} : \mathcal{X} \rightarrow \mathcal{A}_{\text{safety}}$,

$$f_{\text{safety}}(x) = \begin{cases} \text{U} & \text{if in state } x \text{ SRS is either able to provide its} \\ & \text{safety function or in spurious operation,} \\ \overline{\text{U}} & \text{otherwise.} \end{cases} \tag{3.16}$$

Each state x is related to a safety attribute from the set $\mathcal{A}_{\text{safety}} = \{\text{U}, \overline{\text{U}}\}$. If x is related to U or $\overline{\text{U}}$ is determined by the elements safety attributes and the elements structure. The elements safety attributes of the state x are given by the function $f_{\text{el safety}}(x)$, see definition 22. The set of k-tuples of element safety attributes is given by $\mathcal{U}$, which defines the relation of x to U or $\overline{\text{U}}$. Therefore, the function $f_{\text{safety}}(x)$ is specified by $\mathcal{U}$,

$$f_{\text{safety}}(x) = \begin{cases} \text{U} & \text{if } f_{\text{el safety}}(x) \in \mathcal{U} \text{ ,} \\ \overline{\text{U}} & \text{otherwise.} \end{cases} \tag{3.17}$$

Hence, the SDTA states, where the respective SRS is able to provide its safety function or is in spurious operation, are characterized by $\mathcal{U}$. The set $\mathcal{U}$ is usually specified by the safety engineer. $\mathcal{U}$ is illustrated for an SRS with a 1oo2 element structure in example 3.5. The state classifications of further *M*oo*N* element structures that are treated in this thesis are defined in appendix B.

Definition 22 (State classification regarding element safety functions). Each state of an SDTA is related via the function $f_{\text{el safety}} : \mathcal{X} \rightarrow \underbrace{\mathcal{A}_{\text{el safety}} \times \cdots \times \mathcal{A}_{\text{el safety}}}_{k}$ to a k-tuple of element safety attributes, where the set of element safety attributes is given by $\mathcal{A}_{\text{el safety}} = \{\text{U}_{\text{el}}, \overline{\text{U}_{\text{el}}}\}$. The function $f_{\text{el safety}}$ is given by

$$f_{\text{el safety}}(x) = (\mathcal{AV}_{\text{el safety,1}}, \ldots, \mathcal{AV}_{\text{el safety,i}}, \ldots, \mathcal{AV}_{\text{el safety,k}}) \text{ ,}$$

where

$$\mathcal{AV}_{\text{el safety,i}} = \begin{cases} \text{U}_{\text{el}} & \text{if in state } x \text{ element } i \text{ is either able to provide its} \\ & \text{element safety function or in spurious operation,} \\ \overline{\text{U}_{\text{el}}} & \text{otherwise.} \end{cases} \tag{3.18}$$

Example 3.5 (State classification). The SDTA that models an SRS with $k = 2$ elements with the 1oo2 element structure is given. The 1oo2 element structure implies that two redundant elements provide the same element safety function. The set $\mathcal{U}$ for the given model is given by

$$\mathcal{U} = \{(\text{U}_{\text{el}}, \text{U}_{\text{el}}), (\text{U}_{\text{el}}, \overline{\text{U}}_{\text{el}}), (\overline{\text{U}}_{\text{el}}, \text{U}_{\text{el}})\} \text{ ,}$$

see appendix B for the definitions of $\mathcal{U}$ for further element structures. The set $\mathcal{U}$ includes tuples of the element safety attributes. These tuples characterize the states where the SRS is able to provide its safety function or is in spurious operation. The given specification of $\mathcal{U}$ implies that, a state x will be classified by U if at least one element is able to provide its element safety function or is in spurious operation.

It has to be noted that, each SDTA state $x \in \mathcal{X} \setminus \{x_{\text{init}}\}$ reflects the information about the occurred failure events in the k elements of the modeled SRS. The only exception is the initial failure-free state x_{init}. This information is stored via k-tuples of element failure mode attributes, which will be introduced in subsection 3.3.2.

3.3 Procedure to model SRS with multiple elements

3.3.1 Preliminaries

The SDTA aims to model an SRS that consists of multiple possibly dependent elements. The modeling procedure to determine the SDTA for such an SRS usually requires high effort due to the large number of states and dependencies between the elements. The separate modeling of individual elements and automatic composition of the entire model reduce the effort of modeling. In the following, a suitable procedure is presented. In subsection 3.3.2, the SDTA that models an SRS element is introduced. The composition operation for SDTAs is presented in subsection 3.3.3. The modeling of dependent SRS elements is treated in subsection 3.3.4. Based on that, the dependencies that are caused by common-cause failures are modeled in subsection 3.3.5. Furthermore, the modeling of selected dependencies between elements, such as repair priorities and inhibition, are covered in appendices C.1 and C.2.

3.3.2 The SRS element

Let an SRS consist of k elements. The i-th SRS element, $i \in \{1, \ldots, k\}$, is modeled by the SDTA that is defined hereafter.

Definition 23 (SDTA modeling the i-th SRS element). The SDTA is given by

$$\mathcal{SDTA}^i = (\mathcal{X}^i, \mathcal{E}^i, f^i_{\text{tr}}, \Gamma^i, x^i_{\text{init}}, \mathcal{V}^i, \mathcal{G}^i) \,, \tag{3.19}$$

where the parameters are as follows:

$\mathcal{X}^i = \{1, 2, 3, 4, 5, 6\}$;

$\mathcal{E}^i = \mathcal{E}^i_{det} \cup \mathcal{E}^i_{stoch}$, where $\mathcal{E}^i_{det} = \{pma1_i, pmb1_i\}$ and
$\mathcal{E}^i_{stoch} = \{s_i, dd_i, duab_i, dua_i, dn_i, cms_i, md_i\}$;

$$\mathcal{V}^i = \{(v_{pma1_i,1}, \ldots, v_{pma1_i,ne_{pma1_i}}), (v_{pmb1_i,1}, \ldots, v_{pmb1_i,ne_{pmb1_i}})\};$$

$$\mathcal{G}^i = \{G_{s_i}, G_{dd_i}, G_{duab_i}, G_{dua_i}, G_{dn_i}, G_{cms_i}, G_{md_i}\}.$$

It has to be mentioned that, the set of STEs that is given by $\mathcal{E}^i_{stoch}$ is defined in appendix A. In contrast to the set of STEs that was introduced in equation (3.3) of subsection 3.2.3, the former set $\mathcal{E}^i_{stoch}$ includes modifications to reduce the number of SDTA states. These modifications are in detail described in appendix A and lead to the SDTA that models the i-th SRS element. The states/transitions diagram of this SDTA is shown in figure 3.3. The transitions that are triggered by the STEs and DTEs are drawn by the solid and dashed arrows respectively. The set of element failure mode attributes is given by

$$\mathcal{A}_{\text{el fm}} = \{\text{OK}, \text{S}, \text{DR}, \text{DUAB}, \text{DUA}, \text{DN}\}\ . \tag{3.20}$$

The element failure mode attributes are related to the failure modes applied in this thesis, see subsection 2.2.3. Additionally, the modifications introduced in appendix A are applied.

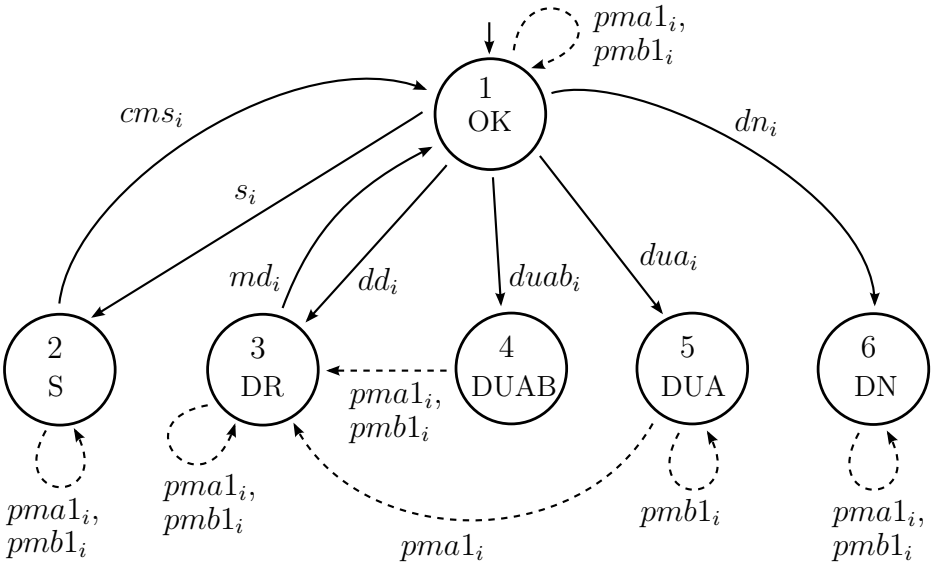

Figure 3.3: States/transitions diagram of the SDTA modeling an SRS element

Definition 24 (Element failure mode attributes). The elements of the set $\mathcal{A}_{\text{el fm}}$ are defined as follows:

OK: Element is fully operational and able to provide its element safety function;

S: An s-failure occurred and has not been restored yet, i.e. spurious operation of element safety function;

DR: A dd-, dua-, or duab-failure occurred, has been detected or revealed, and has not been restored yet, i.e. element safety function is prevented from operating;

DUAB: A duab-failure occurred, has not been revealed, and has not been restored yet, i.e. element safety function is prevented from operating;

DUA: A dua-failure occurred, has not been revealed, and has not been restored yet, i.e. element safety function is prevented from operating;

DN: A dn-failure occurred, i.e. element safety function is prevented from operating.

A k-tuples of element failure mode attributes is related to each SDTA state via the state elements failure mode classification function $f_{\text{el fm}}$, given in definition 25. The function $f_{\text{el fm}}$ is defined for an SDTA that models an SRS consisting of k elements.

Definition 25 (State classification regarding failure modes). Each state of an SDTA is related via the function $f_{\text{el fm}} : \mathcal{X} \to \underbrace{\mathcal{A}_{\text{el fm}} \times \cdots \times \mathcal{A}_{\text{el fm}}}_{k}$ to a k-tuple of element failure mode attributes. The function $f_{\text{el fm}}$ is given by

$$f_{\text{el fm}}(x) = (\mathcal{AV}_{\text{el fm},1}, \ldots, \mathcal{AV}_{\text{el fm},j}, \ldots, \mathcal{AV}_{\text{el fm},k}) \ ,$$

where

$$\mathcal{AV}_{\text{el fm},j} = \begin{cases} \text{OK} & \text{if in state } x \text{ element } j \text{ is characterized by OK,} \\ \text{S} & \text{if in state } x \text{ element } j \text{ is characterized by S,} \\ \text{DR} & \text{if in state } x \text{ element } j \text{ is characterized by DR,} \\ \text{DUAB} & \text{if in state } x \text{ element } j \text{ is characterized by DUAB,} \\ \text{DUA} & \text{if in state } x \text{ element } j \text{ is characterized by DUA,} \\ \text{DN} & \text{if in state } x \text{ element } j \text{ is characterized by DN.} \end{cases} \tag{3.21}$$

Example 3.6 (State classification of an SDTA regarding failure modes). The SDTA that models an SRS with $k = 1$ element is given. The SDTA is specified by definition 23 and illustrated by the states/transitions diagram in figure 3.3. The respective element failure mode attributes are given by definition 24. The function $f_{\text{el fm}}$ is given by

$$f_{\text{el fm}}(x) = \begin{cases} \text{OK} & \text{if } x = 1, \\ \text{S} & \text{if } x = 2, \\ \text{DR} & \text{if } x = 3, \\ \text{DUAB} & \text{if } x = 4, \\ \text{DUA} & \text{if } x = 5, \\ \text{DN} & \text{if } x = 6. \end{cases}$$

The state elements safety classification function $f_{\text{el safety}}$ is given by the definition 22. Hence, the respective $f_{\text{el safety}}$ for the treated SDTA is given by

$$f_{\text{el safety}}(x) = \begin{cases} \mathrm{U}_{\text{el}} & \text{if } x \in \{1,2\}, \\ \overline{\mathrm{U}}_{\text{el}} & \text{if } x \in \{3,4,5,6\}. \end{cases}$$

3.3.3 Parallel composition

The SDTAs that model individual elements are combined to the SDTA that models an entire SRS via the *parallel composition of SDTAs* that is introduced below. This operation is based on the *parallel composition of deterministic automata*, which was presented in [CL08]. Let the k elements of an SRS be given by $\mathcal{SDTA}^i = (\mathcal{X}^i, \mathcal{E}^i, f_{\text{tr}}^i, \Gamma^i, x_{\text{init}}^i, \mathcal{V}^i, \mathcal{G}^i)$, for all $i \in \{1, \ldots, k\}$. The parallel composition of SDTAs of $\mathcal{SDTA}^p$ and $\mathcal{SDTA}^r$, where $p, r \in \{1, \ldots, k\}$, is defined hereafter.

Definition 26 (Parallel composition of SDTAs). The SDTA that results via the parallel composition of SDTAs is given by

$$\mathcal{SDTA}^p \,||\, \mathcal{SDTA}^r = (\mathcal{X}, \mathcal{E}, f_{\text{tr}}, \Gamma, x_{\text{init}}, \mathcal{V}, \mathcal{G}) \,, \tag{3.22}$$

where the individual parameters are determined as follows:

The set of states is given by $\mathcal{X} = \{\mathcal{X}^p \times \mathcal{X}^r\}$;

The set of events is given by $\mathcal{E} = \{\mathcal{E}^p \cup \mathcal{E}^r\}$;

The transition function f_{tr} is given by

$$f_{\text{tr}}((x^p, x^r), e) := \begin{cases} (f_{\text{tr}}^p(x^p, e), f_{\text{tr}}^r(x^r, e)) & \text{if } e \in \Gamma^p(x^p) \cap \Gamma^r(x^r) \,, \\ (f_{\text{tr}}^p(x^p, e), x^r) & \text{if } e \in \Gamma^p(x^p) \setminus \mathcal{E}^r \,, \\ (x^p, f_{\text{tr}}^r(x^r, e)) & \text{if } e \in \Gamma_r(x^r) \setminus \mathcal{E}^p \,; \end{cases}$$

The active event function is given by

$$\Gamma(x^p, x^r) = [\Gamma^p(x^p) \cap \Gamma^r(x^r)] \cup [\Gamma^p(x^p) \setminus \mathcal{E}^r] \cup [\Gamma^r(x^r) \setminus \mathcal{E}^p] \,;$$

The initial state is given by $x_{\text{init}} = (x_{\text{init}}^p, x_{\text{init}}^r)$;

The set of deterministic clock sequences is given by $\mathcal{V} = \{\mathcal{V}^p \cup \mathcal{V}^r\}$;

The set of CDFs is given by $\mathcal{G} = \{\mathcal{G}^p \cup \mathcal{G}^r\}$.

An example is given hereafter to illustrate the parallel composition of SDTAs. It has to be noted that, the SDTAs that are composed in example 3.7 possess only *private events*. This is because these SDTAs are models of independent SRS elements. The dependent elements will be treated in subsection 3.3.4.

Example 3.7 (Parallel composition of SDTAs). The two given SDTAs, $\mathcal{SDTA}^1$ and $\mathcal{SDTA}^2$, are combined via the parallel composition of SDTAs. The states/transitions diagrams of $\mathcal{SDTA}^1$, $\mathcal{SDTA}^2$ are shown in figure 3.4. Let the SDTA that results via the parallel composition be $\mathcal{SDTA} = \mathcal{SDTA}^1 \,||\, \mathcal{SDTA}^2$. The $\mathcal{SDTA}$ is determined via the definition 26. Selected parameters of the $\mathcal{SDTA}$ are the following:

$$\mathcal{X} = \{\hat{1}, \hat{2}\} \times \{1, 2, 3\} = \{(\hat{1}, 1), (\hat{1}, 2), (\hat{1}, 3), (\hat{2}, 1), (\hat{2}, 2), (\hat{2}, 3)\};$$

$$\mathcal{E} = \{dd_1, md_1\} \cup \{dua_2, md_2, pma1_2\};$$

$$x_{\text{init}} = (\hat{1}, 1).$$

The full expressions of the relative transition function $f_{\text{tr}}(x, e)$ and active event function $\Gamma(x)$ are omitted in this example. These functions can be deduced from the given states/transitions diagram. The states/transitions diagram of the $\mathcal{SDTA}$ is shown in figure 3.5.

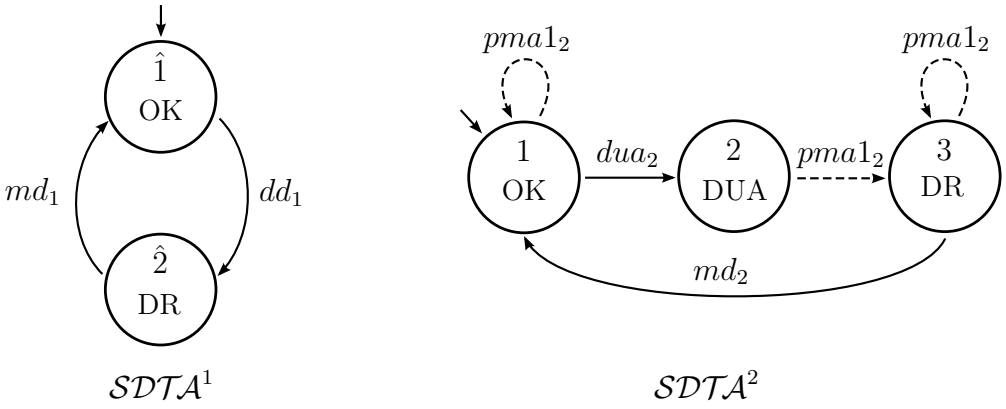

Figure 3.4: States/transitions diagrams of $\mathcal{SDTA}^1$, $\mathcal{SDTA}^2$

3.3.4 Dependent SRS elements

The introduced modeling framework comprising the SDTA and parallel composition provides features that enable to treat elements which depend on each other. It has to be emphasized that, two types of events are differentiated by the parallel composition of SDTAs, defined in subsection 3.3.3. The *private events* are these events, which appear only in one of the combined SDTAs, i.e. $e \in \Gamma^p(x^p) \setminus \mathcal{E}^r$ or $e \in \Gamma_r(x^r) \setminus \mathcal{E}^p$. In contrast, the *common events* appear in both SDTAs, i.e. $e \in \Gamma^p(x^p) \cap \Gamma^r(x^r)$. The private and common events are treated differently in the parallel composition of SDTAs. It is clearly

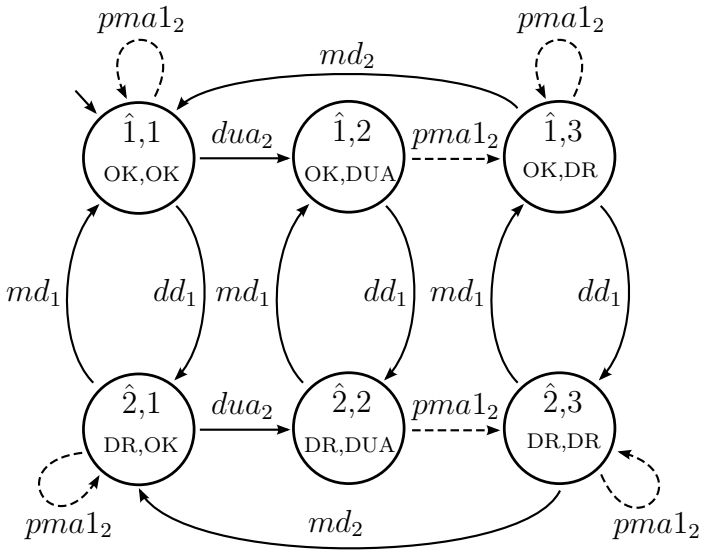

Figure 3.5: States/transitions diagram of $\mathcal{SDTA} = \mathcal{SDTA}^1 \,||\, \mathcal{SDTA}^2$

evident in definition 26, where the transition function f_{tr} is determined. The private events are not subject of constraints in the parallel composition and can occur independently. Independent elements have only this type of events. A common event can only simultaneously occur in both elements. The respective SDTAs are synchronized by the parallel composition. Hence, both elements participate on the common events. These events can be applied to model dependencies between elements.

Dependencies of elements might strongly influence the probabilistic figures of merit of a system. Therefore, it is important to model dependencies if these are present. However, SRS elements might depend on each other in many different ways that can all not be treated in this thesis. Selected dependencies of elements are described, such as common-cause failures, repair priorities, and inhibition, see subsection 3.3.5 and appendix C.

3.3.5 SRS elements with common-cause failures

The groups of two or more redundant elements of an SRS, which independently implement the same element safety function, are subject to the common-cause failures. The common-cause failures are not part of an individual element model. Thus, the common-cause failures are considered to be caused by dependencies between elements. Accordingly, the common-cause failure can not be modeled by combination of the SDTAs of independent elements. The additional state transitions, which result from the common-cause failures, have to be separately modeled.

The common-cause failures were described in subsection 2.2.3. The groups of redundant SRS elements are specified in equation (2.2). The events that indicate the common-cause failures are defined in equation (2.4). The procedure to model a group of redundant SRS elements with common-cause failures is described below.

It is assumed that, the SDTA that models an SRS with a group of redundant elements is given. Let the group of redundant elements have the elements number set $\mathcal{GE}_j$, as defined by equation (2.2). In total, the entire treated SRS might include m groups of redundant elements, i.e. $j \in \{1, \ldots, m\}$. The common-cause failures are modeled by additional state transitions that are inserted into the respective SDTA. These transitions are triggered by the STEs that are related to the common-cause failures. Altogether, one additional transition for each failure mode is introduced. The additional transitions connect the initial failure-free state with the states where failures of the relevant identical failure mode occurred in all redundant elements. In total, five additional transitions per group of redundant elements are introduced.

Finally, the rate parameters of the introduced STEs, which are related to the common-cause failures, are determined. In this thesis, the so-called *Beta model*, which was described in [IEC11d], is applied to determine the rate parameters. The *Beta model extension*, which was introduced in [HLHH10] to consider the varying sensitivity of different element structures of SRSs to the common-cause failures, is applied as well. The rate parameters of the common-cause failures are determined from the rate parameters of single failures of the redundant elements, by use of the following equations:

$$\begin{aligned}
\lambda_{s_{GEj}} &= C_{MooN} \cdot \beta_{s_{GEj}} \cdot \min\{\lambda_h : h \in \mathcal{E}_s\}, & \mathcal{E}_s &= \{s_i : i \in \mathcal{GE}_j\} \ , \\
\lambda_{dd_{GEj}} &= C_{MooN} \cdot \beta_{dd_{GEj}} \cdot \min\{\lambda_h : h \in \mathcal{E}_{dd}\}, & \mathcal{E}_{dd} &= \{dd_i : i \in \mathcal{GE}_j\} \ , \\
\lambda_{duab_{GEj}} &= C_{MooN} \cdot \beta_{duab_{GEj}} \cdot \min\{\lambda_h : h \in \mathcal{E}_{duab}\}, & \mathcal{E}_{duab} &= \{duab_i : i \in \mathcal{GE}_j\} \ , \\
\lambda_{dua_{GEj}} &= C_{MooN} \cdot \beta_{dua_{GEj}} \cdot \min\{\lambda_h : h \in \mathcal{E}_{dua}\}, & \mathcal{E}_{dua} &= \{dua_i : i \in \mathcal{GE}_j\} \ , \\
\lambda_{dn_{GEj}} &= C_{MooN} \cdot \beta_{dn_{GEj}} \cdot \min\{\lambda_h : h \in \mathcal{E}_{dn}\}, & \mathcal{E}_{dn} &= \{dn_i : i \in \mathcal{GE}_j\} \ .
\end{aligned} \tag{3.23}$$

The index $j \in \{1, \ldots, m\}$ is related to the j-th group of redundant elements with common-cause failures. The parameter C_{MooN} is the modification factor, which was introduced in [HLHH10]. It depends on the respective element structure of the group. The parameters $\beta_{s_{GEj}}$, $\beta_{dd_{GEj}}$, $\beta_{duab_{GEj}}$, $\beta_{dua_{GEj}}$, $\beta_{dn_{GEj}}$ denote the fractions of common-cause failures for the respective failure modes.

The example 3.8 illustrates the procedure to model the common-cause failures.

Example 3.8 (Common-cause dd-failures). Let the two SDTAs, $\mathcal{SDTA}^1$ and $\mathcal{SDTA}^2$, be given. The respective states/transitions diagrams are given in figure 3.6. Moreover, the states/transitions diagram of $\mathcal{SDTA}$ is also shown in this figure. The $\mathcal{SDTA}$ is the model that consists of the two elements given by $\mathcal{SDTA}^1$ and $\mathcal{SDTA}^2$. Let the two elements be redundant elements that are subject to the common-cause failures. Hence, the $\mathcal{SDTA}$ is extended by additional transition to model the common-cause failures. The states/transitions diagram of the extended $\mathcal{SDTA}$ is given in figure 3.7. The additional transition that is relative to the common-cause failures is drawn by the bold arrow. The rate parameter of the respective STE dd_{GEj} is calculated via the equation (3.23) and is

given by

$$\lambda_{dd_{GEj}} = C_{1oo2} \cdot \beta_{dd_{GEj}} \cdot \min\{\lambda_{dd_1}, \lambda_{dd_2}\} \ .$$

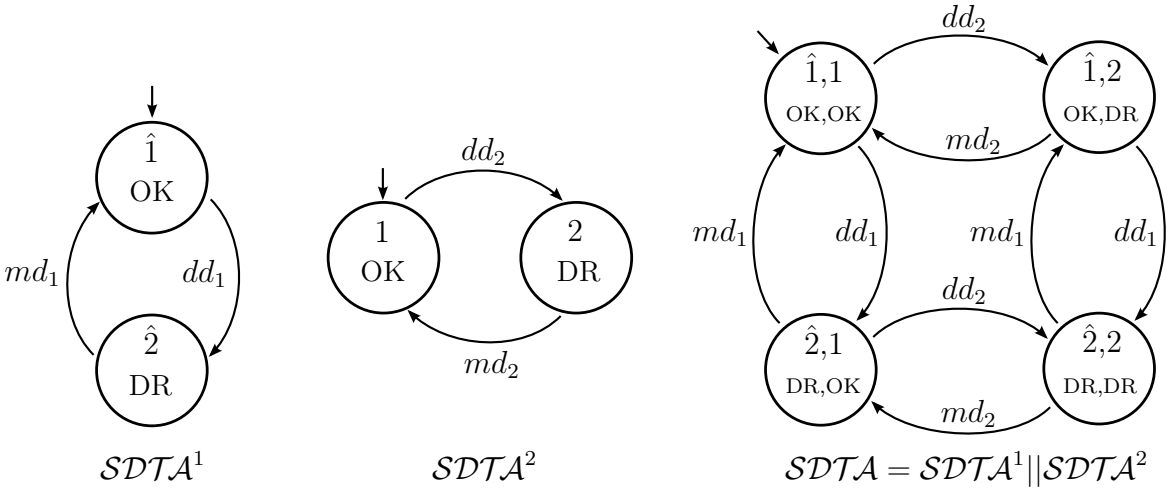

Figure 3.6: States/transitions diagrams of $\mathcal{SDTA}^1$, $\mathcal{SDTA}^2$, and $\mathcal{SDTA}$

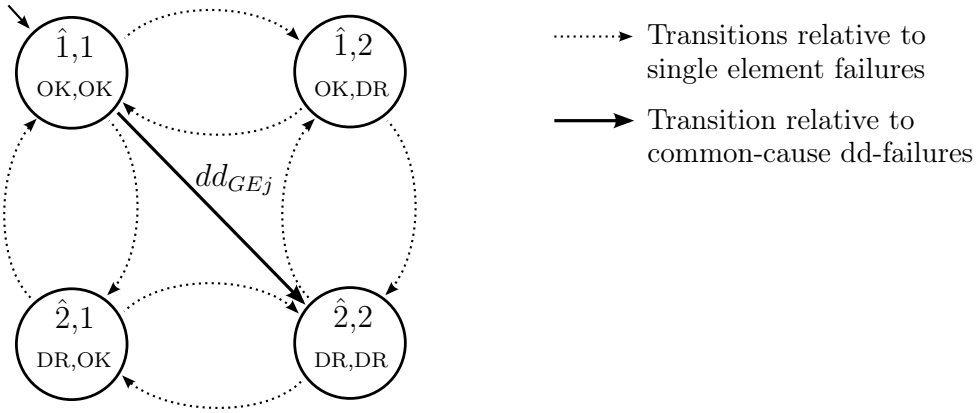

Figure 3.7: States/transitions diagram of $\mathcal{SDTA}$ modeling common-cause dd-failures

3.4 Discussion on SDTAs

The introduced SDTA is discussed in this section. An SDTA generates random event and state sequences that were demonstrated in example 3.4. This example and the discussion of the state sequence generation provided deep insight into the SDTAs. In the following, the relation of an SDTA to further models and probabilistic evaluation is discussed. The focus is to provide efficient calculation of the state probabilities and $PFD(t)$.

An SDTA is based on the *Stochastic Timed Automaton with Poisson clock structure* (STAP) that was defined in [CL08]. It results from the extension of the STAP by an additional type of events, the DTEs. If the set of deterministic clock sequences is empty,

the SDTA will be identical to an STAP. Moreover, if the set of exponential stochastic clock sequences is empty, the SDTA will be an automaton with purely deterministic timing (DTA). The SDTA is understood as a model where an STAP and a DTA are embedded. These two are sequentially evaluated within the SDTA. The following example illustrates that.

Example 3.9 (SDTA decomposition). The SDTA of example 3.4 is given. It is decomposed into the embedded STAP and DTA. In figure 3.8, two states/transitions diagrams are given to illustrate the respective automata. On the left, the diagram shows the STAP that is triggered by STEs. The diagram on the right shows the DTA that is triggered by the DTEs, which is here $pma1$.

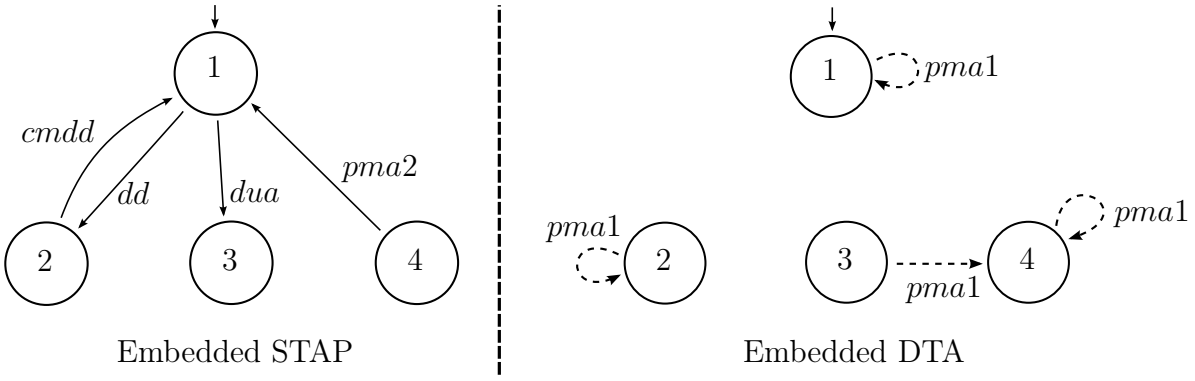

Figure 3.8: Embedded automata of SDTA in example 3.9

The state transitions of the SDTA that are triggered by the STEs or DTE are evaluated by the STAP or DTA, respectively. Let the SDTA be initialized and the STE *dua* occur after that. A transition from state 1 to state 3 is triggered in the embedded STAP. Let now the DTE $pma1$ occur. This triggers the DTA to be initialized in state 3 and a transition from state 3 to state 4. After that, the STAP is reinitialized in state 4 and remains there until the next STE occurs or until the next DTE will trigger the DTA.

The described nature of an SDTA will be used for its probabilistic evaluation. A further characteristic of the SDTA is essential for that: The DTEs remain permanently active in all states and therefore occur in predetermined intervals. This characteristic is part of the SDTA definition, see equation (3.9). The predetermined intervals define the time intervals where the embedded STAP of the SDTA is active. In these intervals, the STAP exclusively defines the occurring events and state transitions of the SDTA. In between, the embedded DTA is initialized and triggers transitions related to the DTEs. The state probabilities will be calculated based on the embedded STAP and DTA. The state probabilities of the STAP were investigated in literature, see [CL08], via the Markov chains (MCs). This method can be applied in the predetermined intervals between the DTEs to calculate the state probabilities of the SDTA. In addition to that, the state transitions triggered by DTEs occur at predetermined times. These state transitions

can not be modeled via MCs. Therefore, the *phase transitions* of the MCs have to be introduced. These enable to model the state transitions triggered by DTEs. The state probabilities of the SDTA will be calculated via the MCs with phase transitions, the so-called Multi-phase MCs.

It has been investigated in literature that the Multi-phase MCs provide an efficient calculation of state probabilities, see [FF11]. In the next chapter, they will be applied to calculate the state probabilities of the SDTAs. However, the application of the SDTA provides numerous advantages for probabilistic modeling of SRSs. It provides a close connection to the concepts of the SRSs and enables straightforward modeling of an SRS under consideration of the dependencies of individual elements. Individual elements can be modeled separately and composed to the entire model. Furthermore, insight into further types of probabilistic models is provided, which are based on automata and feature different timing of events.

Chapter 4

Probabilistic evaluation of the SDTAs via Multi-phase Continuous-time Markov Chains (MP-CMCs)

4.1 Preliminaries

The last chapter treated the modeling of an SRS via the SDTA. A modeling procedure was introduced to determine the SDTA for an SRS that consists of multiple possibly dependent elements. This chapter treats the probabilistic evaluation of a determined SDTA. The $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ are determined based on state probability calculations of the *Multi-phase Continuous-time Markov Chains*. The provided framework for the probabilistic evaluation will be applied in chapters 5, 6 to analyze the models and optimize the PM plans.

The structure of the chapter is outlined hereafter. First, the MP-CMC definition is introduced in section 4.2. The procedure to determine the $PFD(t)$ via the MP-CMC is described. In section 4.3, the transformation to determine the MP-CMC for a given SDTA is presented. Finally, the PM plans and PM strategies, which imply restrictions on the PM plans, are introduced in section 4.4.

4.2 MP-CMC definition

The MP-CMC is closely related to the MP-DMC. The MP-DMCs were applied in [Gab10], referred to as the *Safety Multiphase Markov Models*. The extension of the MP-DMCs for continuous-time leads to the MP-CMCs. The MP-CMCs enable the use of variable-step ODE solvers providing efficient computation of the state probabilities.

Definition 27 (Multi-phase Continuous-time Markov Chain (MP-CMC)). The

MP-CMC that models an SRS with k elements is the seven-tuple $\mathcal{MP}\text{-}\mathcal{CMC}$, given by

$$\mathcal{MP}\text{-}\mathcal{CMC} = (\mathcal{X}_{MC}, \boldsymbol{p}_{\text{init}}, \boldsymbol{Q}, \mathcal{T}, \mathcal{M}, \boldsymbol{c}_{PFD}, t_m) \; . \tag{4.1}$$

The parameters of the MP-CMC are as follows:

$\mathcal{X}_{MC} = \{1, \ldots, n\}$ is the set of states, $|\mathcal{X}_{MC}| = n$;

$\boldsymbol{p}_{\text{init}} = \begin{bmatrix} p_{\text{init},1} & \ldots & p_{\text{init},n} \end{bmatrix}$ is the initial state probabilities row vector of dimension n, where $\sum_{j=1}^{n} p_{\text{init},j} = 1$;

$\boldsymbol{Q}$ is the square transition rates matrix of dimension $n \times n$;

$\mathcal{T} = (\mathcal{T}_{a,1}, \mathcal{T}_{b,1}, \ldots, \mathcal{T}_{a,k}, \mathcal{T}_{b,k})$ is the sequence of phase transition time sequences $\mathcal{T}_{h,r}$, where $\mathcal{T}_{h,r} = (t_{h,r,1}, \ldots, t_{h,r,ne_{h,r}})$, $h \in \{a, b\}$, $r \in \{1, \ldots, k\}$;

$\mathcal{M} = (\boldsymbol{M}_{a,1}, \boldsymbol{M}_{b,1}, \ldots, \boldsymbol{M}_{a,k}, \boldsymbol{M}_{b,k})$ is the sequence of phase transition matrices $\boldsymbol{M}_{h,r}$, where the phase transition time sequence $\mathcal{T}_{h,r}$ is related to each $n \times n$ phase transition matrix $\boldsymbol{M}_{h,r}$, $h \in \{a, b\}$, $r \in \{1, \ldots, k\}$;

$\boldsymbol{c}_{PFD}$ is the state selection column vector of dimension n that is used to select the states where the modeled SRS is not able to provide its safety function;

t_m is the SRS mission time that is evaluated to determine the PFD.

The $\mathcal{MP}\text{-}\mathcal{CMC}$ is applied in this thesis to determine the relevant figures of merit of a modeled SRS. The $PFD(t)$ is determined first. Afterwards, the $\overline{PFD}$ and $PFD_{\max}$ are determined from the $PFD(t)$ under consideration of the given mission time t_m, see subsection 2.4.3. The $PFD(t)$ reflects the instantaneous probability that the SRS is in a state, where it is not able to provide its safety function. Consequently, the $PFD(t)$ is determined via

$$PFD(t) = \boldsymbol{p}(t) \cdot \boldsymbol{c}_{PFD} \; , \tag{4.2}$$

where $\boldsymbol{p}(t) = \begin{bmatrix} p_1(t) & p_2(t) & \ldots & p_n(t) \end{bmatrix}$ is the state probabilities row vector. The relevant states to determine the $PFD(t)$ are selected via the state selection vector $\boldsymbol{c}_{PFD}$. In equation (4.2), the relevant state probabilities are summed up and yield the $PFD(t)$.

The state probabilities vector $\boldsymbol{p}(t)$ of a given $\mathcal{MP}\text{-}\mathcal{CMC}$ has to be calculated to determine the respective $PFD(t)$. The $\boldsymbol{p}(t)$ is characterized by the system of ordinary differential equations (ODEs) that is given by

$$\dot{\boldsymbol{p}} = \boldsymbol{p}(t) \cdot \boldsymbol{Q} \; . \tag{4.3}$$

The system of ODEs in equation (4.3) is linear and homogeneous. It is based on the balance of the state probability flows in the $\mathcal{MP}\text{-}\mathcal{CMC}$. The balance of the state probability

flows of the state i is given by the ODE

$$\frac{\mathrm{d}p_i(t)}{\mathrm{d}t} = \underbrace{\sum_{\substack{j=1 \\ j\neq i}}^{n} p_j(t) q_{j,i}}_{\text{inflows}} - \underbrace{p_i(t) \sum_{\substack{j=1 \\ j\neq i}}^{n} q_{i,j}}_{\text{outflows}} , \tag{4.4}$$

where $q_{j,i}$ are the transition rates related to the inflows and $q_{i,j}$ are related to the outflows. In figure 4.1, the state probability inflows and outflows of the state i are illustrated. The transition rates related to the inflows are located in the i-th column of the matrix $\boldsymbol{Q}$ and these related to the outflows are located in the i-th row. In equation (4.4), the derivation of the state probability of state i equals the total state probability inflow minus the total outflow. The equation (4.4) can be rewritten by

$$\frac{\mathrm{d}p_i(t)}{\mathrm{d}t} = \sum_{\substack{j=1 \\ j\neq i}}^{n} p_j(t) q_{j,i} + p_i(t) q_{i,i} , \tag{4.5}$$

since the diagonal elements of $\boldsymbol{Q}$ are equal to the negative sum of the transition rates related to the outflows,

$$q_{i,i} = -\sum_{\substack{j=1 \\ j\neq i}}^{n} q_{i,j} . \tag{4.6}$$

The i-th diagonal element of $\boldsymbol{Q}$, which is denoted by $q_{i,i}$, reflects the negative transition rate for a state transition from the state i to an arbitrary adjacent state. The state probabilities behave as conserved quantities that were initialized by $\boldsymbol{p}_{\text{init}}$. Hence, the sum of the elements of $\boldsymbol{Q}$ that are located in one row equals zero.

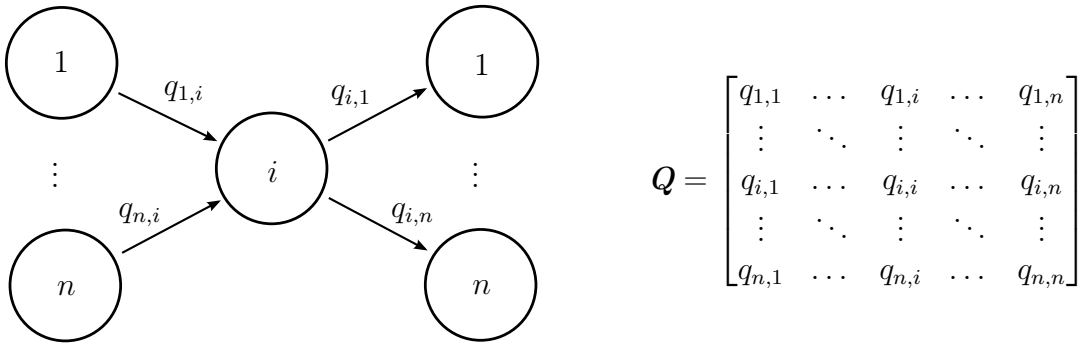

Figure 4.1: State probability flows of state i and transition rates matrix $\boldsymbol{Q}$

The state probabilities vector $\boldsymbol{p}(t)$ is piecewise defined due to the discontinuities caused by the phase transitions. The procedure to piecewise calculate $\boldsymbol{p}(t)$ is described hereafter. For the time interval $0 \leq t < t_{h,r,1}$, before the first phase transition has occurred, $\boldsymbol{p}(t)$ is the solution of the *initial value problem* given by the ODEs in equation (4.3) and the

initial condition given by

$$\boldsymbol{p}(t=0) = \boldsymbol{p}_{\text{init}} = \begin{bmatrix} p_{\text{init},1} & p_{\text{init},2} & \dots & p_{\text{init},n} \end{bmatrix} . \tag{4.7}$$

For each phase transition that occurs at $t = t_{h,r,s}$, the state probabilities vector $\boldsymbol{p}(t)$ is instantly manipulated via

$$\boldsymbol{p}(t_{h,r,s}) = \boldsymbol{p}(t_{h,r,s}{}^{-}) \cdot \boldsymbol{M}_{h,r}, \qquad \forall t_{h,r,s} \in \mathcal{T}_{h,r} , \tag{4.8}$$

where $\boldsymbol{p}(t_{h,r,s}{}^{-})$ is the left-sided limit that is given by

$$\boldsymbol{p}(t_{h,r,s}{}^{-}) = \lim_{t \to t_{h,r,s}} \boldsymbol{p}(t) . \tag{4.9}$$

It is the limit of $\boldsymbol{p}(t)$ as t increases in value approaching $t_{h,r,s}$.

It is evident that, the phase transitions redistribute the state probabilities at the times $t_{h,r,s}$, for all $h \in \{a, b\}$, $r \in \{1, \dots, k\}$, and $s \in \{1, \dots, ne_{h,r}\}$. The state probabilities vector is modified by multiplication with the phase transition matrices $\boldsymbol{M}_{h,r}$, see equation (4.8). The phase transitions describe the impact of the PM on the SRS behavior, which is characterized by the state probabilities vector $\boldsymbol{p}(t)$. The initial condition for the next time interval, for $t_{h,r,s} \leq t$, is given by $\boldsymbol{p}(t_{h,r,s})$. It is determined in equation (4.8) by multiplication of the state probabilities $\boldsymbol{p}(t_{h,r,s}{}^{-})$ of the previous time interval with a phase transition matrix. The vector $\boldsymbol{p}(t)$ is calculated for the next time interval by solving the initial value problem with the updated initial condition. Step by step, $\boldsymbol{p}(t)$ is piecewise calculated over the mission time t_m. The phase transitions cause discontinuities of $\boldsymbol{p}(t)$. The described procedure to piecewise calculate $\boldsymbol{p}(t)$ is illustrated by the following example.

Example 4.1 (Calculation of the state probabilities vector of an $\mathcal{MP}$-$\mathcal{CMC}$). The $\mathcal{MP}$-$\mathcal{CMC}_1$ is given, which models an SRS that consists of one element. Only the undetected failures were modeled. These failures are revealed and the SRS is immediately repaired via the PM. The repair duration is neglected, i.e. the restoration instantly occurs after a failure is revealed. The states/transitions diagram of the $\mathcal{MP}$-$\mathcal{CMC}_1$ is shown in figure 4.2. The $\mathcal{MP}$-$\mathcal{CMC}_1$ parameters are given as follows:

$$\mathcal{X}_{MC} = \{1, 2\};\ \boldsymbol{p}_{\text{init}} = \begin{bmatrix} 1 & 0 \end{bmatrix};\ \boldsymbol{Q} = \begin{bmatrix} -\lambda & \lambda \\ 0 & 0 \end{bmatrix};\ \boldsymbol{c}_{PFD} = \begin{bmatrix} 0 & 1 \end{bmatrix};\ t_m = 60000 \text{ h};$$

$$\mathcal{T} = (\mathcal{T}_{a,1}),\ \mathcal{T}_{a,1} = (t_{a,1,1}),\ t_{a,1,1} = 20000 \text{ h};$$

$$\mathcal{M} = (\boldsymbol{M}_{a,1}),\ \boldsymbol{M}_{a,1} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}.$$

The system of ODEs, which characterizes the state probabilities vector $\boldsymbol{p}(t) = \begin{bmatrix} p_1 & p_2 \end{bmatrix}$ of the $\mathcal{MP}\text{-}\mathcal{CMC}_1$, is given by

$$\begin{bmatrix} \dot{p}_1 & \dot{p}_2 \end{bmatrix} = \begin{bmatrix} p_1 & p_2 \end{bmatrix} \cdot \begin{bmatrix} -\lambda & \lambda \\ 0 & 0 \end{bmatrix} .$$

The time intervals of the piecewise defined state probabilities $p_1(t)$, $p_2(t)$ are given by

$$\begin{aligned} &\text{Interval 1:} && 0 \text{ h} \leq t < 20000 \text{ h} , \\ &\text{Interval 2:} && 20000 \text{ h} \leq t < 60000 \text{ h} . \end{aligned}$$

The initial condition of the initial value problem that defines $\boldsymbol{p}(t)$ for the interval 1 is given by

$$\begin{bmatrix} p_1(t=0) & p_2(t=0) \end{bmatrix} = \boldsymbol{p}_{\text{init}} = \begin{bmatrix} 1 & 0 \end{bmatrix} ,$$

and the initial condition for the interval 2 is given by

$$\begin{bmatrix} p_1(t=t_{a,1,1}) & p_2(t=t_{a,1,1}) \end{bmatrix} = \begin{bmatrix} p_1(t=t_{a,1,1}{}^{-}) & p_2(t=t_{a,1,1}{}^{-}) \end{bmatrix} \cdot \boldsymbol{M}_{a,1} .$$

The calculated state probabilities $p_1(t)$, $p_2(t)$ are plotted in figure 4.3 for the transition rate $\lambda = 1.5 \cdot 10^{-5}$. The discontinuities that are caused by the phase transition appear in the plots of $p_1(t)$ and $p_2(t)$ for $t = 20000$ h. The $PFD(t)$ equals the state probability of the state 2, i.e. $p_2(t) = PFD(t)$.

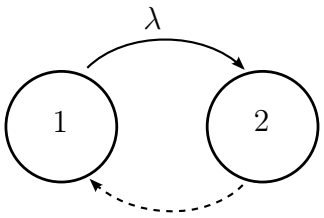

Figure 4.2: States/transitions diagram of $\mathcal{MP}\text{-}\mathcal{CMC}_1$

4.3 SDTA transformation into MP-CMC

The transformation to determine the MP-CMC for a given SDTA is introduced below. Before the transformation is introduced, two particular characteristics of SDTAs are discussed. These characteristics have to be considered to ensure that the SDTA transformation into MP-CMC exists for a given SDTA.

It has to be noted that, the state transition from state i to state j of an SDTA might be triggered by multiple STEs. This is not reasonable for modeling of SRSs, but permitted by automata theory. In that case, in order to enable the SDTA transformation into MP-CMC, the multiple STEs have to be replaced by a single substitutional STE. The rate

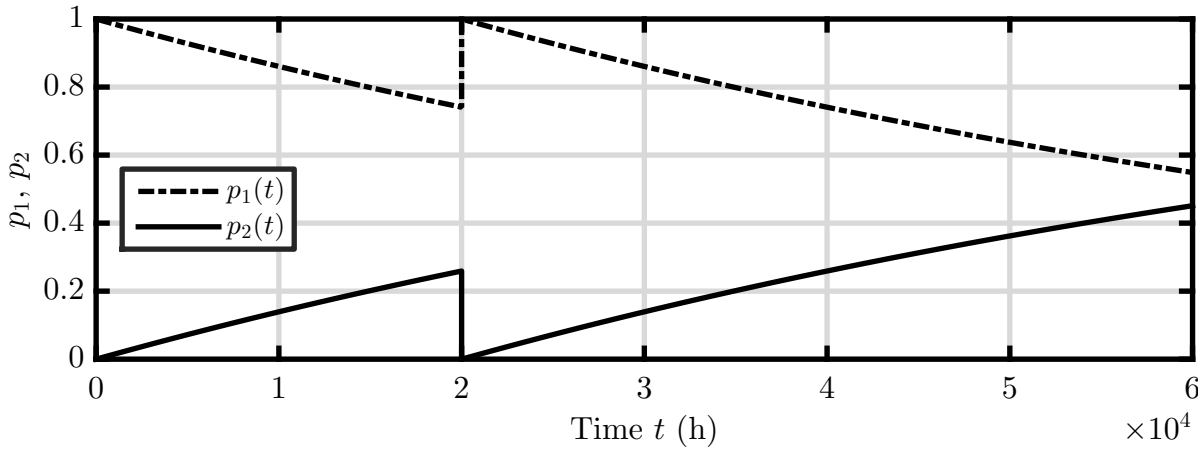

Figure 4.3: State probabilities p_1, p_2 of $\mathcal{MP}$-$\mathcal{CMC}_1$ in example 4.1

parameter of the substitutional STE is calculated as the sum of the rate parameters of all the multiple STEs for a given state transition. This calculation is enabled by the superposition of exponential CDFs.

Another characteristic of the SDTAs also has to be discussed. An STE that triggers state transitions with the same start and end state might occur, i.e. from state i to state j, where $i = j$. Such STEs are permitted by automata theory. However, these STEs do not have any impact that is relevant for state probabilities calculation. Hence, these STEs are not considered for the transformation of an SDTA into the MP-CMC.

Let an SDTA be given by $\mathcal{SDTA} = (\mathcal{X}, \mathcal{E}, f_{\text{tr}}, \Gamma, x_{\text{init}}, \mathcal{V}, \mathcal{G})$, equivalent to the definition 18. The respective $\mathcal{MP}$-$\mathcal{CMC} = (\mathcal{X}_{MC}, \boldsymbol{p}_{\text{init}}, \boldsymbol{Q}, \mathcal{T}, \mathcal{M}, \boldsymbol{c}_{PFD}, t_m)$ is denoted equivalent to the definition 27. The definitions given below enable to determine the parameters of the $\mathcal{MP}$-$\mathcal{CMC}$ from the parameters of the given $\mathcal{SDTA}$.

Definition 28 (Calculation of $\mathcal{X}_{MC}$). The states set $\mathcal{X}_{MC}$ is given by

$$\mathcal{X}_{MC} = \mathcal{X} = \{1, 2, \ldots, n\} \; . \tag{4.10}$$

The $\mathcal{MP}$-$\mathcal{CMC}$ states set $\mathcal{X}_{MC}$ is identical to the $\mathcal{SDTA}$ states set $\mathcal{X}$.

Definition 29 (Calculation of $\boldsymbol{p}_{init}$). The initial state probabilities vector $\boldsymbol{p}_{\text{init}} = \begin{bmatrix} p_{\text{init},1} & p_{\text{init},2} & \ldots & p_{\text{init},n} \end{bmatrix}$ is given by

$$p_{\text{init},i} = \begin{cases} 1 & \text{if } i = x_{\text{init}} \\ 0 & \text{else} \end{cases} \quad , \qquad i \in \{1, 2, \ldots, n\} \; . \tag{4.11}$$

The $\boldsymbol{p}_{\text{init}}$ is determined from the initial state x_{init} of the $\mathcal{SDTA}$.

Definition 30 (Calculation of $\boldsymbol{Q}$). The transition rates matrix $\boldsymbol{Q}$ is given by

$$q_{i,j} = \begin{cases} \lambda_h & \text{if transition from state } i \text{ to state } j \text{ exists and} \\ & \text{is triggered by STE } h \text{ with rate parameter } \lambda_h, \qquad i \neq j \ , \\ 0 & \text{otherwise,} \end{cases} \tag{4.12}$$

$$q_{i,i} = -\sum_{\substack{j=1 \\ j \neq i}}^{n} q_{i,j} \ ,$$

where $q_{i,j}$ with the indices $i, j \in \{1, 2, \ldots, n\}$ are the elements of the $n \times n$ matrix $\boldsymbol{Q}$.

The matrix $\boldsymbol{Q}$ is related to the adjacency matrix of the $\mathcal{SDTA}$ states/transitions diagram that includes only the transitions triggered by an STE. In contrast to an adjacency matrix, the entries of $\boldsymbol{Q}$ are weighted by the rate parameters of the respective STEs, see definition 30. As mentioned at the beginning of the current section, the STEs that trigger state transitions with the same start and end state are not considered. The diagonal elements of $\boldsymbol{Q}$ are determined via equation (4.6). Moreover, each state transition is assumed to be triggered by only one STE. Otherwise, the transition rate matrix $\boldsymbol{Q}$ can not be determined via definition 30. Therefore, a substitutional STE can be introduced for each state transition that is triggered by multiple STEs.

Definition 31 (Calculation of $\mathcal{T}$). Let $\mathcal{T}_{a,r}$, $\mathcal{T}_{b,r}$, $r \in \{1, \ldots, k\}$, be the phase transition time sequences related to the element r. The elements of $\mathcal{T}_{h,r} = (t_{h,r,1}, \ldots, t_{h,r,ne_{h,r}})$, $h \in \{a, b\}$, are given by

$$\begin{aligned} t_{a,r,s} &= \sum_{i=1}^{s} v_{pma1_r,i} \ , \qquad s \in \{1, \ldots, ne_{a,r}\} \ , \\ t_{b,r,s} &= \sum_{i=1}^{s} v_{pmb1_r,i} \ , \qquad s \in \{1, \ldots, ne_{b,r}\} \ , \end{aligned} \tag{4.13}$$

where $v_{pma1_r,i}$, $v_{pmb1_r,i}$ are the i-th deterministic clocks of the DTEs $pma1_r$, $pmb1_r$.

It has to be noted that, a time of a given phase transition time sequence $\mathcal{T}_{h,r} = (t_{h,r,1}, \ldots, t_{h,r,ne_{h,r}})$ will have an impact on the $PFD(t)$ within the evaluated time interval only if it complies with the inequality given by,

$$0 < t_{h,r,s} < t_m \ , \tag{4.14}$$

for all $h \in \{a, b\}$, $r \in \{1, \ldots, k\}$, and $s \in \{1, \ldots, ne_{h,r}\}$. The given inequality is explained by the fact that, a PM that is carried out before startup or after decommissioning has no impact on the $PFD(t)$ of an SRS during the time span of interest. Hence, only these times $t_{h,r,s}$ that comply with the given inequality are considered to calculate the $PFD(t)$.

Definition 32 (Calculation of $\mathcal{M}$). Let $\boldsymbol{M}_{a,r}$, $\boldsymbol{M}_{b,r}$, $r \in \{1,\ldots,p\}$, be the phase transition matrices related to the element r. The elements of $\boldsymbol{M}_{a,r}$, $\boldsymbol{M}_{b,r}$ are given by

$$m_{i,j} = \begin{cases} 1 & \text{if transition from state } i \text{ to state } j \text{ exists} \\ & \text{and is triggered by the relevant DTE,} \\ 0 & \text{otherwise,} \end{cases} \tag{4.15}$$

with the indices $i, j \in \{1, 2, \ldots, n\}$. The relevant DTE for $\boldsymbol{M}_{a,r}$ is $pma1_r$ and respectively $pmb1_r$ for $\boldsymbol{M}_{b,r}$.

The matrices $\boldsymbol{M}_{a,r}$, $\boldsymbol{M}_{b,r}$ are these adjacency matrices of the $\mathcal{SDTA}$ states/transitions diagram, where only the state transitions that are triggered by $pma1_r$, $pmb1_r$ are considered. The phase transition time sequence that is related to $\boldsymbol{M}_{h,r}$ is $\mathcal{T}_{h,r}$, $h \in \{a, b\}$.

Definition 33 (Calculation of $\boldsymbol{c}_{PFD}$). The states selection vector $\boldsymbol{c}_{PFD}$, where $\boldsymbol{c}_{PFD} = \begin{bmatrix} c_{PFD,1} & c_{PFD,2} & \ldots & c_{PFD,n} \end{bmatrix}^T$, is given by

$$c_{PFD,i} = \begin{cases} 1 & \text{if } f_{\text{safety}}(i) = \overline{\text{U}}, \\ 0 & \text{otherwise,} \end{cases} \qquad i \in \{1, 2, \ldots, n\} \; . \tag{4.16}$$

The introduced definitions enable to determine the MP-CMC for a given SDTA. An example is given hereafter to illustrate the SDTA transformation into an MP-CMC.

Example 4.2 (SDTA transformation into MP-CMC). Let the SDTA be given that was treated in examples 3.3 and 3.4. The respective MP-CMC was determined. The states set is given by $\mathcal{X}_{MC} = \{1, 2, 3, 4\}$. The initial state probabilities vector is given by $\boldsymbol{p}_{\text{init}} = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}$. The elements of the 4×4 transition rates matrix $\boldsymbol{Q}$, which are not equal to zero, are given by

$$\begin{aligned} &q_{1,1} = -(\lambda_{dd} + \lambda_{dua}), \quad q_{1,2} = \lambda_{dd}, \qquad q_{1,3} = \lambda_{dua}, \\ &q_{2,1} = \lambda_{cmdd}, \qquad\quad q_{2,2} = -\lambda_{cmdd}, \\ &q_{4,1} = \lambda_{pma2}, \qquad\qquad\qquad\quad q_{4,4} = -\lambda_{pma2} \; . \end{aligned}$$

The phase transition time sequence is given by $\mathcal{T}_a = (35040, 43800, 183960)$, where the respective times are specified in hours (h). The relevant DTE to determine the phase transition matrix is $pma1$. The elements of the phase transition matrix $\boldsymbol{M}_a$, which are not equal to zero, are given by

$$m_{1,1} = 1, \quad m_{2,2} = 1, \quad m_{3,4} = 1, \quad m_{4,4} = 1 \; .$$

The states selection vector is given by $\boldsymbol{c}_{PFD} = \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix}$. The determined MP-CMC

enables to calculate the state probabilities vector $\boldsymbol{p}(t)$, $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ for a given interval of interest $0 \leq t < t_m$.

4.4 Preventive maintenance (PM) plans and strategies

4.4.1 Preliminaries

A PM plan was described above in subsection 2.3.3. After that, it has been briefly mentioned that the PM plan is specified by the set of deterministic clock sequences of an SDTA. In this section, the PM plan is defined based on an MP-CMC. First, the definition of a PM plan is introduced immediately hereafter. Afterwards, the restrictions on a PM plan are discussed, formulated and defined. Finally, the PM strategies, which will be treated in this thesis, are defined. The PM strategies are based on the introduced restrictions.

4.4.2 Definition of PM plan

A PM plan defines the schedule of the applied PM to a given SRS. The applied PM includes for each element the PM type A and B, where each includes the PM activities that reveal failures and the PM activities that provide repair and result in restoration if necessary. Let the model of an SRS with k elements be given by an MP-CMC as in definition 27.

Definition 34 (PM plan). The *PM plan* is given by the sequence of phase transition time sequences $\mathcal{T} = (\mathcal{T}_{a,1}, \mathcal{T}_{b,1}, \ldots, \mathcal{T}_{a,k}, \mathcal{T}_{b,k})$.

Each phase transition time sequence $\mathcal{T}_{h,i} = (t_{h,i,1}, \ldots, t_{h,i,ne_{h,i}})$, for all $h \in \{a, b\}$, $i \in \{1, \ldots, k\}$, specifies the times of the phase transitions that are related to the PM type A or B of the i-th SRS element. The particular impact of a PM type A or B of element i is given by the phase transition matrix $\boldsymbol{M}_{h,i}$. It has to be noted that, the impact of each PM type A or B is considered to be build in into the SRS and therefore it can not be varied. In contrast, the times of the PM are considered to be variable.

4.4.3 Restrictions on PM plans

The restrictions on the PM plans are treated in this thesis for the purposes to: (1) illustrate the characteristics of the introduced models and (2) identify, classify, and analyze the restrictions. The probabilistic models, which are applied in literature, imply several restrictions on the PM plans, such as simultaneous PM for all elements and periodically scheduled with equal periods. These restrictions mostly aim to reduce the complexity of the models and are only rarely motivated by application-related restrictions. One

important objective of this thesis is to find out if it is beneficial to overcome particular restrictions. The treated restrictions on a PM plan are introduced hereafter.

The first restriction aims to limit the effort that is required for the PM. It will be enabled to compare different PM plans with identical characteristics in regard to this effort. Therefore, the execution numbers of each particular PM type A or B of each element of a PM plan are restricted to be constant.

Definition 35 (Constant execution numbers of PM). Each execution of a PM is modeled by a respective phase transition. The numbers of the phase transition times are specified for a PM plan and remain constant. These numbers are given by $ne_{h,i}$, for all $h \in \{a, b\}$, $i \in \{1, \ldots, k\}$.

The next two restrictions result in simultaneously executed PM type A or B for all elements of an SRS.

Definition 36 (Simultaneous PM type A). The phase transition time sequences $\mathcal{T}_{a,i}$, which are related to PM type A for all elements, are given by the phase transition time sequence $\mathcal{T}_{a,SRS}$,

$$\mathcal{T}_{a,SRS} = (t_{a,SRS,1}, \ldots, t_{a,SRS,ne_{a,SRS}}) \, . \tag{4.17}$$

Hence, it is $\mathcal{T}_{a,i} = \mathcal{T}_{a,SRS}$ for all $i \in \{1, \ldots, k\}$.

Definition 37 (Simultaneous PM type B). The phase transition time sequences $\mathcal{T}_{b,i}$, which are related to PM type B for all elements, are given by the phase transition time sequence $\mathcal{T}_{b,SRS}$,

$$\mathcal{T}_{b,SRS} = (t_{b,SRS,1}, \ldots, t_{b,SRS,ne_{b,SRS}}) \, . \tag{4.18}$$

Hence, it is $\mathcal{T}_{b,i} = \mathcal{T}_{b,SRS}$ for all $i \in \{1, \ldots, k\}$.

Example 4.3 (Simultaneous PM type A). Let the $\mathcal{MP}$-$\mathcal{CMC}$ of an SRS with three elements be given. The phase transition time sequences that are related to the PM type A of each element are given by $\mathcal{T}_{a,i} = (t_{a,i,1}, t_{a,i,2})$, for all $i \in \{1, 2, 3\}$. The restriction of definition 36 is applied to provide simultaneously executed PM type A for all three elements. Hence, the phase transition time sequences $\mathcal{T}_{a,i}$, for all $i \in \{1, 2, 3\}$, are equal and given by $\mathcal{T}_{a,SRS} = (t_{a,SRS,1}, t_{a,SRS,2})$, where $t_{a,SRS,1} = 3.5$ years and $t_{a,SRS,2} = 7$ years.

In example 4.3 it is shown that, the simultaneous PM results in equal phase transition time sequences of all phase transitions that are related to this particular PM. Hence, all these phase transitions will occur simultaneously.

The next two restrictions effect the periodicity of the PM type A or B. The PM are restricted to be periodically scheduled with equal periods.

Definition 38 (PM type A periodic with equal periods). Let a phase transition time sequence related to PM type A be given by $\mathcal{T}_{a,i} = (t_{a,i,1}, \ldots, t_{a,i,ne_{a,i}})$, for all $i \in \{SRS, 1, \ldots, k\}$. The initial phase transition time $t_{a,i,1}$ is given by

$$t_{a,i,1} = \frac{t_m}{ne_{a,i} + 1} \,, \tag{4.19}$$

for all $ne_{a,i} \in \mathbb{N}$, where $ne_{a,i}$ is the number of phase transition times. It is assumed that $0 < t_{a,i,j} < t_m$. If it is $ne_{a,i} = 0$, the $t_{a,i,1}$ will be undefined and the respective phase transition time sequence empty, i.e. $\mathcal{T}_{a,i} = ()$. In the case of $ne_{a,i} > 1$, the further phase transition times will be given by the recursion

$$t_{a,i,j+1} = t_{a,i,j} + t_{a,i,1} \,, \tag{4.20}$$

for all $j \in \{1, \ldots, ne_{a,i} - 1\}$.

A phase transition that is related to a PM type A is restricted by definition 38 to occur periodically with the equal period $t_{a,i,1}$, which is given by equation (4.19).

Example 4.4 (PM type A periodic with equal periods). Let a PM type A be periodic with equal periods, according to the restriction of definition 38. Hence, the phase transition time sequence is given by $\mathcal{T}_{a,i}$, $i \in \{SRS, 1, \ldots, k\}$. Let the mission time be $t_m = 10$ years and the number of transition times be $ne_{a,i} = 1$. The sequence $\mathcal{T}_{a,i} = (5)$ years is determined via the equation (4.19). The phase transition will occur periodically with the equal period $t_{a,i,1} = 5$ years.

Definition 39 (PM type A and B periodic with equal periods). Let a phase transition time sequence that is related to PM type A be given by $\mathcal{T}_{a,i}$, $i \in \{SRS, 1, \ldots, k\}$. The sequence $\mathcal{T}_{a,i}$ is restricted via definition 38. It has to be noted that, the case of $ne_{a,i} = 0$ and the sequence $\mathcal{T}_{a,i}$ being empty, i.e. $\mathcal{T}_{a,i} = ()$, might occur. A phase transition time sequence that is related to PM type B is given by $\mathcal{T}_{b,i} = (t_{b,i,1}, \ldots, t_{b,i,ne_{b,i}})$. The initial phase transition time $t_{b,i,1}$ is given by

$$t_{b,i,1} = \begin{cases} \frac{t_m}{ne_{b,i}+1} & \text{if } ne_{a,i} = 0 \,, \\ \frac{t_{a,i,1}}{m_i+1} & \text{if } ne_{a,i} \neq 0 \,, \end{cases} \tag{4.21}$$

for all $ne_{b,i}, m_i \in \mathbb{N}$, where the $ne_{b,i}$ is the number of phase transition times in $\mathcal{T}_{b,i}$ that occur within the period $0 < t_{b,i,j} < t_m$. If it is $ne_{a,i} \neq 0$, the number of phase transition times in $\mathcal{T}_{b,i}$ that occur within the period $0 < t_{b,i,j} < t_{a,i,1}$ will be given by m_i,

$$m_i = \frac{ne_{b,i}}{ne_{a,i} + 1} \,, \tag{4.22}$$

where $m_i \in \mathbb{N}_0$. If it is $m_i = ne_{b,i} = 0$, the $t_{b,i,1}$ will be undefined, the respective phase

transition time sequence empty, i.e. $\mathcal{T}_{b,i} = ()$. In the case of $ne_{a,i} = 0$, m_i will equal $ne_{b,i}$, i.e. $m_i = ne_{b,i}$. The further phase transition times of the sequence $\mathcal{T}_{b,i}$ are given by the recursion

$$t_{b,i,j+1} = \begin{cases} t_{b,i,j} + t_{b,i,1} & \text{if} \quad \text{mod}\left(\frac{j}{m_i}\right) \neq 0 \,, \\ t_{b,i,j} + 2 \cdot t_{b,i,1} & \text{if} \quad \text{mod}\left(\frac{j}{m_i}\right) = 0 \,, \end{cases} \tag{4.23}$$

for all $j \in \{1, \ldots, ne_{b,i} - 1\}$, for $ne_{b,i} > 1$ and $m_i \neq 0$.

In definition 39 it is obvious that, the phase transition times related to PM type B, which is periodic with equal periods, depend on the phase transition times related to the respective PM type A, which is periodic with equal periods. Particularly in equation (4.22) it is noticeable that, $ne_{b,i}$ depends on $ne_{a,i}$. It has to be emphasized that, a phase transition related to PM type B occurs periodically with equal periods either within the period of the PM type A or within the period of the mission time t_m.

Example 4.5 (PM type A and B periodic with equal periods). Let a PM type A be periodic with equal periods, as in example 4.4. Therefore, it is $t_m = 10$ years, $ne_{a,i} = 1$, and $\mathcal{T}_{a,i} = (5)$ years. For a phase transition that is related to a PM type B it is assumed that $m_i = 1$. Hence, $ne_{b,i} = 2$ results from equation (4.22). The sequence $\mathcal{T}_{b,i}$ is determined via the equations (4.21), (4.23). The result is given by $\mathcal{T}_{b,i} = (2.5, 7.5)$ years.

4.4.4 Definition of PM strategies

The restrictions that were defined above are applied to PM plans. The PM strategies are introduced as the sets of PM plans with different applied restrictions. These PM strategies are defined hereafter in ascending order for increasing number of restrictions.

Definition 40 (PM strategy I). The PM type A and B have a constant execution number $ne_{h,i} \in \mathbb{N}_0$, for all $h \in \{a, b\}$, $i \in \{1, \ldots, k\}$, see definition 35. The set of PM plans that are classified into the PM strategy I is given by

$$\mathcal{S}_I = \{(\mathcal{T}_{a,1}, \mathcal{T}_{b,1}, \ldots, \mathcal{T}_{a,k}, \mathcal{T}_{b,k}) \mid \mathcal{T}_{h,i} = (t_{h,i,1}, \ldots, t_{h,i,ne_{h,i}})\} \,, \tag{4.24}$$

where $t_{h,i,j} \in \mathbb{R}^+$.

The set of PM plans that are classified into the PM strategy I is further restricted to determine the set of PM plans classified into PM strategy II.

Definition 41 (PM strategy II). The PM type A and B have a constant execution number, see definition 35. The PM type A is simultaneously executed for all elements, see definition 36. The set of PM plans that are classified into the PM strategy II is given by

$$\mathcal{S}_{II} = \{(\mathcal{T}_{a,SRS}, \mathcal{T}_{b,1}, \ldots, \mathcal{T}_{b,k}) \mid \mathcal{T}_{h,i} = (t_{h,i,1}, \ldots, t_{h,i,ne_{h,i}})\} \,, \tag{4.25}$$

where $h \in \{a, b\}$, $i \in \{SRS, 1, \ldots, k\}$, and $t_{h,i,j} \in \mathbb{R}^+$.

The set of PM plans that are classified into the PM strategy II is further restricted to determine the sets of PM plans classified into PM strategy IIIa or IIIb. Different restrictions are applied in each case to define the PM strategy IIIa or IIIb, respectively.

Definition 42 (PM strategy IIIa). The PM type A and B have a constant execution number, see definition 35. The PM type A and B are simultaneously executed for all elements, see definitions 36 and 37. The set of PM plans that are classified into the PM strategy IIIa is given by

$$\mathcal{S}_{IIIa} = \{(\mathcal{T}_{a,SRS}, \mathcal{T}_{b,SRS}) \mid \mathcal{T}_{h,SRS} = (t_{h,SRS,1}, \ldots, t_{h,SRS,ne_{h,SRS}})\} \,, \tag{4.26}$$

where $t_{h,SRS,j} \in \mathbb{R}^+$.

Definition 43 (PM strategy IIIb). The PM type A and B have a constant execution number, see definition 35. The PM type A are simultaneously executed for all elements and periodic with equal periods, see definitions 36 and 38. The set of PM plans that are classified into the PM strategy IIIb is given by

$$\mathcal{S}_{IIIb} = \{(\mathcal{T}_{b,1}, \ldots, \mathcal{T}_{b,k}) \mid \mathcal{T}_{b,i} = (t_{b,i,1}, \ldots, t_{b,i,ne_{b,i}})\} \,, \tag{4.27}$$

where $i \in \{1, \ldots, k\}$, $t_{b,i,j} \in \mathbb{R}^+$. The sequence $\mathcal{T}_{a,SRS}$ is uniquely specified by $ne_{a,SRS}$.

The set of PM plans that are classified into the PM strategy IIIa or IIIb are further restricted to determine the sets of PM plans classified into PM strategy IV.

Definition 44 (PM strategy IV). The PM type A and B have a constant execution number, see definition 35, and are simultaneously executed for all elements, see definitions 36, 37. The PM type A is periodically executed with equal periods, see definition 38. The set of PM plans that are classified into the PM strategy IV is given by

$$\mathcal{S}_{IV} = \{(\mathcal{T}_{b,SRS}) \mid \mathcal{T}_{b,SRS} = (t_{b,SRS,1}, \ldots, t_{b,SRS,ne_{b,SRS}})\} \,, \tag{4.28}$$

where $t_{b,SRS,j} \in \mathbb{R}^+$. The sequence $\mathcal{T}_{a,SRS}$ is uniquely specified by $ne_{a,SRS}$.

The last PM strategy includes PM plans that are restricted by all introduced restrictions.

Definition 45 (PM strategy V). The PM type A and B have a constant execution number, see definition 35, and are simultaneously executed for all elements, see definitions 36, 37. Moreover, the PM type A and B are periodically executed with equal periods, see definitions 38, and 39. The set of PM plans that are classified into the PM strategy

V includes a single PM plan. This PM plan is uniquely determined by the specified execution numbers $ne_{h,SRS}$ of the PM A and B, for all $h \in \{a, b\}$. The respective set is denoted by $\mathcal{S}_V$.

It has to be emphasized that, the available degrees of freedom of a model for the PM are classified by the PM strategies. Usually, the PM plans of a PM strategy with more restrictions are included in that with less restrictions. In particular, it is

$$\mathcal{S}_V \subset \mathcal{S}_{IV} \subset \mathcal{S}_{IIIa}, \mathcal{S}_{IIIb} \subset \mathcal{S}_{II} \subset \mathcal{S}_I \ . \tag{4.29}$$

Furthermore, it has to be noted that the choice of the PM strategies is explained by the different characteristics of the PM type A or B. The PM type B is considered to require less effort to vary the respective schedule compared to those of type A. That is because PM type B is usually fully automated and does not require human interaction. The PM type A usually requires human interaction and even an interruption of operation might be required. Therefore, changes of the PM type A schedule are sometimes just not possible for various reasons. In general, a framework is provided that enables to treat SRSs with different degrees of freedom for PM plans. In the next chapter the $PFD(t)$ will be analyzed for different degrees of freedom.

Chapter 5

Model analysis and validation

5.1 Preliminaries

Selected SRSs with different structures and characteristics were modeled via the methods introduced in previous chapters. These models are discussed and analyzed in this chapter. The one element and three element models with a 1oo3, 2oo3, and 3oo3 element structure are treated in section 5.2. In section 5.3, the treated models are validated versus the models that are available in literature. Finally, sensitivity analysis is applied to the treated models in section 5.4.

5.2 Analyzed models

5.2.1 Preliminaries

The remarks on the motivation of the choice of analyzed models are given immediately hereafter. After that, the parameters of the analyzed models are introduced in this subsection. In subsection 5.2.2, the one element model is described and analyzed. The three element models with a 1oo3, 2oo3, and 3oo3 element structure are treated in subsection 5.2.3. The analysis results of the treated models are presented in subsection 5.2.4.

Choice of analyzed models

The one element model is chosen to show the model features that are related to an element, such as multiple failure modes, two types of PM, etc. The three element model provides a large variety of possible element structures with a varying degree of redundancy, i.e 1oo3, 2oo3, and 3oo3. Hence, the three element models are chosen to show the model features that appear for multiple elements. The common-cause failures are not considered in this chapter. These usually dominate the behavior of models with redundancies and would interfere further characteristics.

The dependent elements are not treated in this chapter, in order to put the focus on the models with independent elements. However, the introduced models, the presented analysis and optimization methods are capable to treat dependent elements. Selected dependent elements are described in appendix C.

Parameters of analyzed models

The transition rates of an MP-CMC correspond to the rate parameters of the exponential CDF that is related to the STE that triggers the respective transition of the SDTA. The rate parameters of the STEs *dd*, *duab*, *dua*, and *dn* are given by

$$\begin{aligned} \lambda_{dd} &= dc \cdot \lambda_d \ , \\ \lambda_{duab} &= tcb \cdot (1 - dc) \cdot \lambda_d \ , \\ \lambda_{dua} &= (tca - tcb) \cdot (1 - dc) \cdot \lambda_d \ , \\ \lambda_{dn} &= (1 - tca) \cdot (1 - dc) \cdot \lambda_d \ , \end{aligned} \tag{5.1}$$

where the parameters λ_d, dc, tca, and tcb are introduced to express the rate parameters. The indices that indicate the relative SRS element are omitted for clarity. The parameters λ_d, dc, tca, and tcb are characterized in the following:

dc is the diagnostic coverage factor, given by

$$dc = \frac{\lambda_{dd}}{\lambda_{dd} + \lambda_{duab} + \lambda_{dua} + \lambda_{dn}} \ ; \tag{5.2}$$

λ_d is the rate parameter of the STEs that indicate dangerous failures, i.e. *dd*, *duab*, *dua*, and *dn*; λ_d is given by

$$\lambda_d = \lambda_{dd} + \lambda_{duab} + \lambda_{dua} + \lambda_{dn} \ ; \tag{5.3}$$

tca is the coverage of the PM type A, given by

$$tca = \frac{\lambda_{duab} + \lambda_{dua}}{\lambda_{duab} + \lambda_{dua} + \lambda_{dn}} \ ; \tag{5.4}$$

tcb is the coverage of the PM type B, given by

$$tcb = \frac{\lambda_{duab}}{\lambda_{duab} + \lambda_{dua} + \lambda_{dn}} \ . \tag{5.5}$$

The parameters λ_d, dc, and tca were also used by the standard [IEC11e] as parameters of probabilistic models. The parameter tca was denoted by PTC and referred to as *proof test coverage*. Additionally, the parameter tcb is introduced in this thesis to quantify the

coverage of the PM type B. In [BBB12], a comparable parameter was introduced, denoted by E, and referred to as the *efficiency of the partial test*.

5.2.2 One element model

The one element model is given by $\mathcal{MP}\text{-}\mathcal{CMC}_{1EL} = (\mathcal{X}_{MC}, \boldsymbol{p}_{\text{init}}, \boldsymbol{Q}, \mathcal{T}, \mathcal{M}, \boldsymbol{c}_{PFD}, t_m)$. This model was determined from the $\mathcal{SDTA}$, which was given in definition 23, via the SDTA transformation into MP-CMC, which was introduced in section 4.3. The parameters of the $\mathcal{MP}\text{-}\mathcal{CMC}_{1EL}$ are introduced below.

The set of states $\mathcal{X}_{MC}$ and the initial state probabilities vector $\boldsymbol{p}_{\text{init}}$ are given by

$$\mathcal{X}_{MC} = \{1, 2, 3, 4, 5, 6\} , \qquad \boldsymbol{p}_{\text{init}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} .$$

The transition rates matrix $\boldsymbol{Q}$ is given by

$$\boldsymbol{Q} = \begin{bmatrix} q_{1,1} & q_{1,2} & \cdots & q_{1,6} \\ q_{2,1} & q_{2,2} & \cdots & q_{2,6} \\ \vdots & \vdots & \ddots & \vdots \\ q_{6,1} & q_{6,2} & \cdots & q_{6,6} \end{bmatrix} .$$

The elements of $\boldsymbol{Q}$ that are not equal to zero are given by

$$\begin{aligned} & q_{1,2} = \lambda_s, \quad q_{1,3} = \lambda_{dd}, \quad q_{1,4} = \lambda_{duab}, \quad q_{1,5} = \lambda_{dua}, \quad q_{1,6} = \lambda_{dn}, \\ & q_{2,1} = \lambda_{cms}, \\ & q_{3,1} = \lambda_{md}, \\ & q_{1,1} = -(q_{1,2} + q_{1,3} + q_{1,4} + q_{1,5} + q_{1,6}), \quad q_{2,2} = -q_{2,1}, \quad q_{3,3} = -q_{3,1}, \end{aligned}$$

where λ_{dd}, λ_{duab}, λ_{dua}, and λ_{dn} are given in equations (5.1). Hence, the parameters of the matrix $\boldsymbol{Q}$ are λ_s, λ_{cms}, λ_{md}, dc, λ_d, tca, and tcb. The indices that indicate the relative SRS element are omitted for clarity. The state selection vector $\boldsymbol{c}_{PFD}$ is given by

$$\boldsymbol{c}_{PFD} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}^T .$$

The i-th element of $\boldsymbol{c}_{PFD}$ is zero if in state i either the safety function is provided or the SRS is in spurious operation. Otherwise, the i-th element of $\boldsymbol{c}_{PFD}$ is one if the safety function is not provided in state i.

The parameters $\mathcal{T}$, $\mathcal{M}$ are related to the phase transitions that model the PM. The sequence of the phase transition time sequences, which is given by $\mathcal{T} = (\mathcal{T}_a, \mathcal{T}_b)$, defines the schedule of the phase transitions and the PM plan. $\mathcal{M}$ is the sequence of the phase transition matrices that specifies the impact of each phase transition on the states of the $\mathcal{MP}\text{-}\mathcal{CMC}_{1EL}$. $\mathcal{M}$ is given by $\mathcal{M} = (\boldsymbol{M}_a, \boldsymbol{M}_b)$. The phase transitions specified by $\boldsymbol{M}_a$,

$\boldsymbol{M}_b$ model the PM type A, B.

The $PFD(t)$ is calculated via the state probabilities of the $\mathcal{MP}$-$\mathcal{CMC}_{1EL}$, see section 4.2. The respective system of ODEs is piecewise solved via the MATLAB ODE solver *ode23tb*. This solver uses a variable step size that depends on the precision settings for the calculation. Particularly, the ode23tb efficiently solves stiff ODEs. The stiff ODEs result from the elements of the matrix $\boldsymbol{Q}$ that differ by large orders of magnitude, e.g. the rate parameters λ_{dua} and λ_{md}, which indicate failure and restoration, usually strongly differ.

The calculated $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ are shown in figure 5.1. The $\overline{PFD}$, $PFD_{\max}$ are plotted using a dashed line and a dotted line, respectively. The parameters that were used for the model evaluation are given in table 5.1. The phase transition time sequences $\mathcal{T}_a$, $\mathcal{T}_b$ are given in table 5.2. In figure 5.1, the results for the PM plans 1 and 2 of table 5.2 are shown in black or blue. The phase transition matrices $\boldsymbol{M}_a$, $\boldsymbol{M}_b$ are not explicitly given. The PM plan 1 is classified into the PM strategy V, given by definition 45. Hence, the $PFD(t)$ plot of the PM plan 1, in figure 5.1, shows that the phase transitions related to the PM type A and B occur periodically with equal periods. The PM plan 2 is classified into the PM strategy IIIa, where the periods between the phase transitions do not have to be equal.

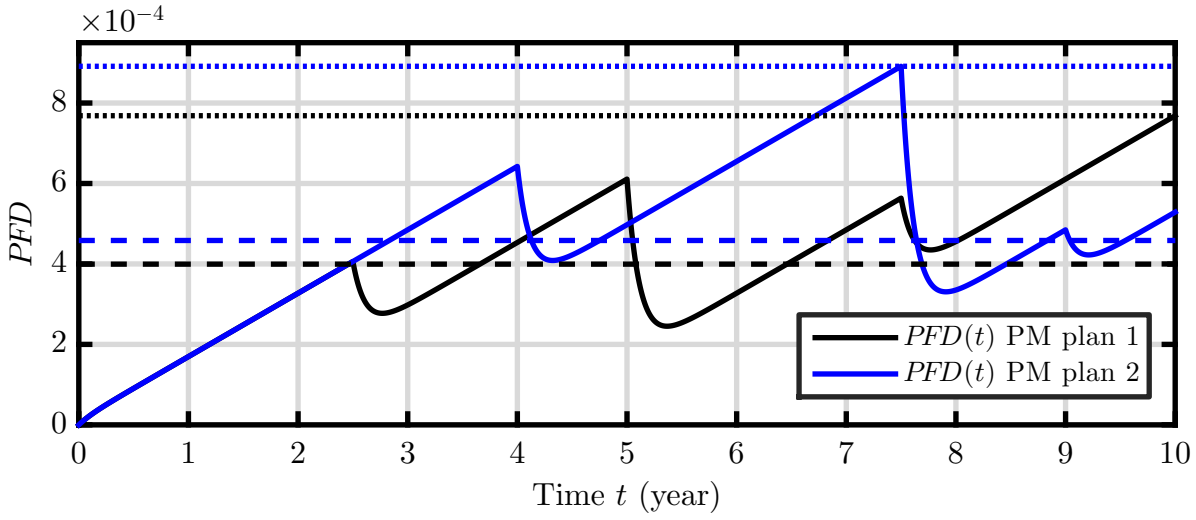

Figure 5.1: $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ of one element model

λ_s (h^{-1})	λ_d (h^{-1})	dc	tca	tcb	λ_{cms} (h^{-1})	λ_{md} (h^{-1})	t_m (year)
$300 \cdot 10^{-9}$	$30 \cdot 10^{-9}$	0.4	0.8	0.48	$5 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	10

Table 5.1: Parameters of one element model

	PM plan 1	PM plan 2
$\mathcal{T}_a$ (year)	(5)	(7.5)
$\mathcal{T}_b$ (year)	(2.5, 7.5)	(4, 9)

Table 5.2: PM plans 1, 2 of one element model

5.2.3 Three element model

The three element model is given by $\mathcal{MP}\text{-}\mathcal{CMC}_{3EL} = (\mathcal{X}_{MC}, \boldsymbol{p}_{\text{init}}, \boldsymbol{Q}, \mathcal{T}, \mathcal{M}, \boldsymbol{c}_{PFD}, t_m)$. A three element model can have the 1oo3, 2oo3, or 3oo3 element structure. This model was determined from the respective $\mathcal{SDTA}$ that was transformed into the $\mathcal{MP}\text{-}\mathcal{CMC}_{3EL}$. The $\mathcal{SDTA}$ was determined via the parallel composition from the $\mathcal{SDTA}^i$ for all $i \in \{1, 2, 3\}$. The parameters of $\mathcal{MP}\text{-}\mathcal{CMC}_{3EL}$ are introduced below.

The set of states $\mathcal{X}_{MC}$ and the initial state probabilities vector $\boldsymbol{p}_{\text{init}}$ are given by

$$\mathcal{X}_{MC} = \{1, 2, \ldots, 216\} , \qquad \boldsymbol{p}_{\text{init}} = \begin{bmatrix} 1 & 0 & \ldots & 0 \end{bmatrix} .$$

The transition rates matrix $\boldsymbol{Q}$ is a 216×216 matrix and is therefore not explicitly given. The parameters of the matrix $\boldsymbol{Q}$ are λ_{s_i}, λ_{cms_i}, λ_{md_i}, λ_{d_i}, dc_i, tca_i, tcb_i, for all $i \in \{1, 2, 3\}$. The index i indicates the relative element of a parameter. The state selection vector $\boldsymbol{c}_{PFD}$ is a column vector with 216 elements. The element structure of the model is reflected by $\boldsymbol{c}_{PFD}$. Hence, $\boldsymbol{c}_{PFD}^{1oo3}$, $\boldsymbol{c}_{PFD}^{2oo3}$, and $\boldsymbol{c}_{PFD}^{3oo3}$ are differentiated. These state selection vectors were determined based on the state classification regarding the safety function, see definition 33.

The PM plan is defined by $\mathcal{T}$. That is $\mathcal{T} = (\mathcal{T}_{a,1}, \mathcal{T}_{b,1}, \mathcal{T}_{a,2}, \mathcal{T}_{b,2}, \mathcal{T}_{a,3}, \mathcal{T}_{b,3})$ the sequence of the phase transition time sequences, where $\mathcal{T}_{a,i}$ is the time sequence scheduling the phase transition that models the PM type A of the element i. Respectively, $\mathcal{T}_{b,i}$ is related to the PM type B. Due to the presence of multiple elements, the PM plans can be classified in more PM strategies compared to a one element model. The PM type A or B might be separately executed for each element, i.e. *elementwise* PM. In contrast, the PM might be simultaneously executed for all elements. The sequence of phase transition matrices is given by $\mathcal{M} = (\boldsymbol{M}_{a,1}, \boldsymbol{M}_{b,1}, \boldsymbol{M}_{a,2}, \boldsymbol{M}_{b,2}, \boldsymbol{M}_{a,3}, \boldsymbol{M}_{b,3})$. The phase transitions specified by $\boldsymbol{M}_{a,i}$, $\boldsymbol{M}_{b,i}$ model the PM type A, B of the element i.

The calculated $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ are shown for the 1oo3, 2oo3, and 3oo3 element structures in figures 5.2, 5.3, and 5.4. The parameters that were used for the model evaluation are given in table 5.3. The phase transition time sequences $\mathcal{T}_{a,i}$, $\mathcal{T}_{b,i}$, for all $i \in \{1, 2, 3\}$, which define the evaluated PM plans 1 and 2, are given in table 5.4. The PM plan 1 implies simultaneous PM type A and B, in contrast to the PM plan 2 with elementwise PM. The evaluated PM plans 1, 2 are classified into the PM strategy V or PM strategy I, respectively.

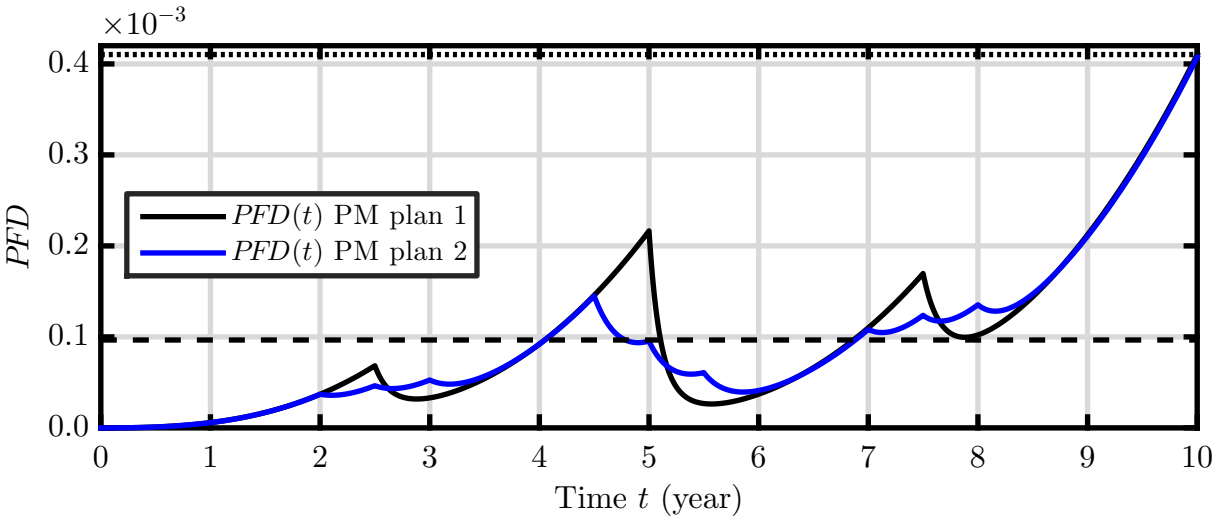

Figure 5.2: $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ of three element 1oo3 model

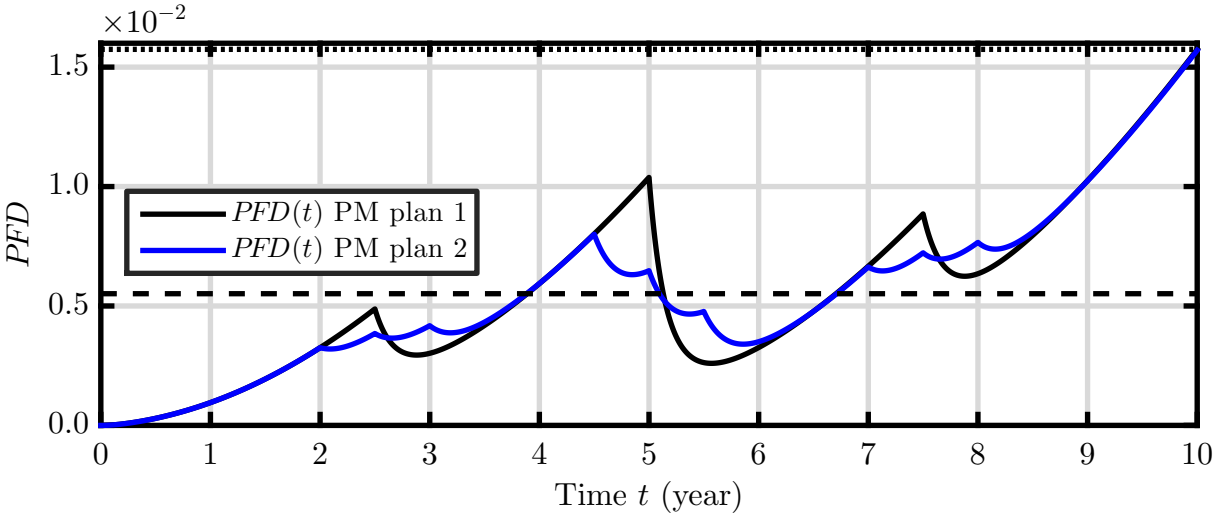

Figure 5.3: $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ of three element 2oo3 model

5.2.4 Results

Overall, each $PFD(t)$ plot in figures 5.1, 5.2, 5.3, and 5.4 shows a similar trend. The $PFD(t)$ starts at zero in the origin, is increasing from there along the x-axis, and is decreased by phase transitions. No jump discontinuities are present in the $PFD(t)$ plots in contrast to example 4.1. This is explained by the duration of repair after the failures were revealed by the PM. Due to that, the respective models have no direct phase transitions from a state where the safety function is not available to a state where it is. It is shown in the states/transitions diagram in figure 3.3. The occurring phase transitions cause

λ_{s_i} (h^{-1})	λ_{d_i} (h^{-1})	dc_i	tca_i	tcb_i	λ_{cms_i} (h^{-1})	λ_{md_i} (h^{-1})	t_m (year)
$300 \cdot 10^{-9}$	$3000 \cdot 10^{-9}$	0.4	0.8	0.48	$5 \cdot 10^{-3}$	$0.5 \cdot 10^{-3}$	10

Table 5.3: Parameters of three element model

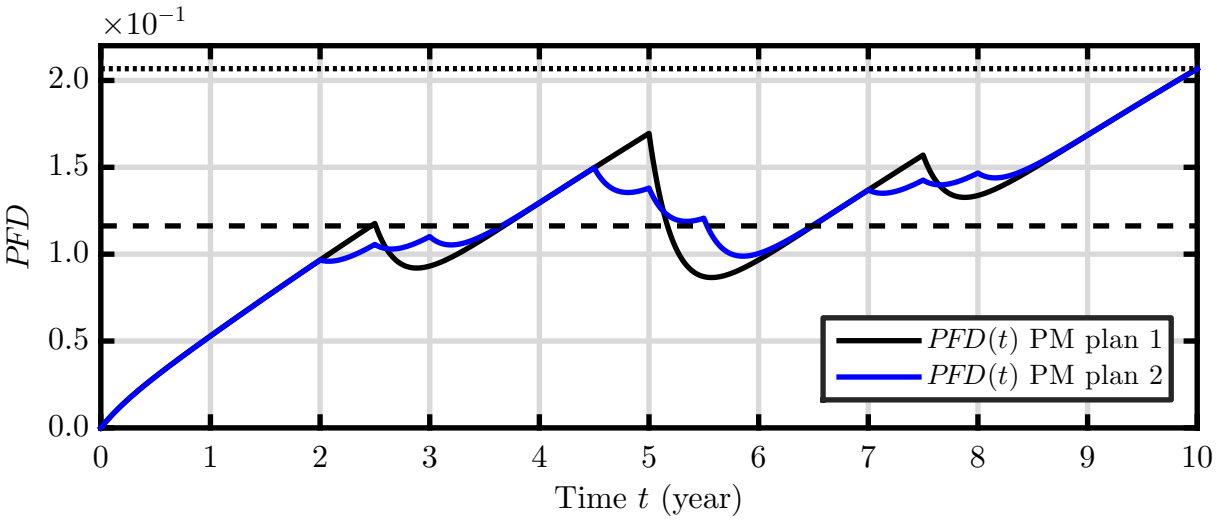

Figure 5.4: $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$ of three element 3oo3 model

		PM plan 1	PM plan 2
Element 1	$\mathcal{T}_{a,1}$ (year)	(5)	(4.5)
	$\mathcal{T}_{b,1}$ (year)	(2.5, 7.5)	(2, 7)
Element 2	$\mathcal{T}_{a,2}$ (year)	(5)	(5)
	$\mathcal{T}_{b,2}$ (year)	(2.5, 7.5)	(2.5, 7.5)
Element 3	$\mathcal{T}_{a,3}$ (year)	(5)	(5.5)
	$\mathcal{T}_{b,3}$ (year)	(2.5, 7.5)	(3, 8)

Table 5.4: PM plans 1, 2 of three element model

discontinuities of the derivative of the $PFD(t)$. A jump of the gradient of the $PFD(t)$ is caused.

The figures of merit $\overline{PFD}$, $PFD_{\max}$ were applied to characterize the $PFD(t)$ via its average and maximum values. If it is $PFD_{\max} > \overline{PFD}$, there will exist a time interval $t_1 \leq t < t_2$, where the $PFD(t)$ and $\overline{PFD}(t_1, t_2)$ are greater than the $\overline{PFD}$. Hence, it might be not sufficient to analyze only the $\overline{PFD}$ in order to assess the $PFD(t)$ for the entire mission time interval. For example, refer to the $PFD(t)$ plot of the PM plan 1, given in figure 5.1. In the time intervals $4 \leq t < 5$ and $8 \leq t < 10$ the $PFD(t)$ and $\overline{PFD}(t_1, t_2)$ are greater than the $\overline{PFD}$. Therefore, it is required to analyze the $\overline{PFD}$ and $PFD_{\max}$, in order to assess the $PFD(t)$ for the entire mission time interval and ensure that it is sufficiently low.

Now, the focus is put on the characteristics of the $PFD(t)$ plots that result from the analyzed element structures. The figures 5.2, 5.3, and 5.4 were analyzed and compared. It can be stated that, with decreasing redundancy the $PFD(t)$ plot becomes more similar in shape to the $PFD(t)$ plot of the one element model, shown in figure 5.1. Moreover, the $PFD_{\max}$ is significantly greater in relation to the $\overline{PFD}$ for the 1oo3 element structure, in comparison to the 2oo3 or 3oo3 element structures. Further, the gradient of the $PFD(t)$ is discussed without the consideration of its changes due to phase transitions. It can

be stated that, the gradient of the $PFD(t)$ faster increases over time for an increasing redundancy, i.e. for 2oo3, 1oo3 element structures. In contrast, the gradient of the $PFD(t)$ remains constant or even decreases over time for the analyzed models without redundancy, see figures 5.1, 5.4.

Furthermore, the degrees of freedom of the analyzed models in regard to the PM were demonstrated. These degrees of freedom, such as elementwise PM of individual elements and arbitrarily variable individual periods, impact the $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$.

5.3 Validation

5.3.1 Preliminaries

Selected probabilistic models, which were introduced in literature, are briefly described in the following subsections. Particularly, the models of [TE09], [BBB12], and [IEC11d] are described in subsections 5.3.2, 5.3.3, and 5.3.4. These literature models are applied to validate the models introduced in this thesis. The validation results are presented in subsection 5.3.5.

5.3.2 Model of Torres-Echeverría et al.

The model of Torres-Echeverría et al. is based on the Hybrid method, see subsection 1.2, and was introduced in [TE09]. The $PFD(t)$ is calculated as the result of the two independent series elements, which model the two failure modes dd- and du-failures. The dd-failures with respective repair are quantified by a constant contribution to the $PFD(t)$. The du-failures are revealed by PM with a complete coverage and repaired thereafter. Only one type of PM was considered for each element in [TE09]. However, let this PM be the PM type A, for the purpose of comparison with the models introduced in this thesis. The PM schedule was specified in [TE09] via the functional test cycle that is shown in figure 5.5. The time to the first test after the startup at $t = 0$ is given by t_p, the respective interval in figure 5.5 is denoted by (1). After that, the test (2), repair (3), and standby (4) intervals cyclically follow each other until the end of mission time at $t = t_m$. The test time is denoted by t_t, the repair time by t_r, and the period between two PM executions by TI_a. If the time to the first test is $t_p = TI_a$, the PM will be periodic with equal periods TI_a.

The $PFD(t)$ of a one element SRS was calculated by a piecewise defined equation, see [TE09]. Due to the equal periods between two PM executions and the complete test coverage, the $PFD(t)$ is a periodic function for $t \geq t_p$. The $PFD(t)$ for an SRS with multiple elements is determined by multiplication or summation of the $PFD(t)$ of individual elements, for parallel or serial elements, respectively. The PM periods were assumed to be equal for all elements, i.e. TI_a. However, the times to the first test can

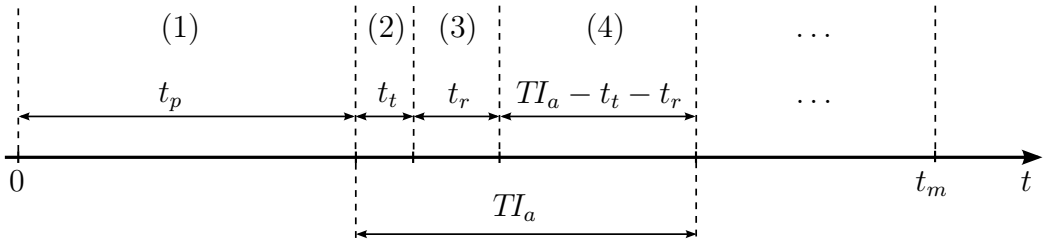

Figure 5.5: Functional test cycle, [TE09]

be individually parametrized for each element to enable the so-called *staggered* PM of an SRS with multiple elements. The staggered PM is illustrated in figure 5.6 for an SRS with three elements.

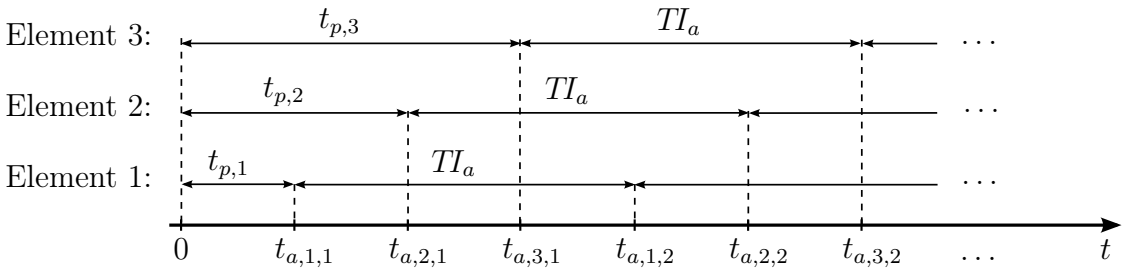

Figure 5.6: Staggered PM of three elements

5.3.3 Model of Brissaud et al.

The model of Brissaud et al. is also based on the Hybrid method. This model was introduced in [BBB12]. It is capable to model two types of PM for each element, in contrast to the model from [TE09]. Let these two types be the PM type A and B, for the purpose of comparison with the models introduced in this thesis. The PM type A, modeled by [BBB12], is restricted to a complete coverage. Similarly to [TE09], the $PFD(t)$ is calculated as the result of the two independent series elements, which model the two failure modes duab- and dua-failures. The former failures are revealed either by the PM type A or by the PM type B. In contrast, the latter are revealed only by the PM type A. The dd-failures are neglected by [BBB12]. Moreover, the test time of the PM type A or B and the repair duration of the failures, which were revealed by the PM type A or B, are neglected as well. The PM type A is restricted to be periodic with equal periods. The times of the PM type B are identically located in each period of the PM type A. These times are specified by a recursion that is referred to as the α-test policy, see [BBB12]. The motivation to use the α-test policy is the reduced number of parameters to specify the schedule of the PM type B.

The $PFD(t)$ of the one element SRS was calculated by a piecewise defined equation, see [BBB12]. Due to the equal periods between two executions of the PM type A and the complete coverage, the $PFD(t)$ is a periodic function for the period of the PM type A.

Further equations were given to calculate the $PFD(t)$ for an SRS with multiple identical elements and a given element structure, see [BBB12]. The times of the PM type A and B are restricted to be equal for all elements, i.e. the PM is simultaneous for all elements.

5.3.4 Model of IEC 61508

The model of IEC 61508 is based on the Simplified equations, see subsection 1.2, and was introduced in [IEC11d]. This model calculates the $\overline{PFD}$ as the result of the independent series elements that model the following failure modes: dd-failures, du-failures, and dn-failures, if necessary. Let the du-failures be revealed by the PM type A with an arbitrary coverage, for the purpose of comparison with the models introduced in this thesis. The incomplete coverage of the PM type A leads to the dn-failures. The dn-failures were modeled to be revealed by the occurring demands of the SRS. Here, the dn-failures are assumed to remain effective until the end of the mission time, to enable comparison between the model introduced in [IEC11d] and the models introduced in this thesis.

It has to be emphasized that, the model of IEC 61508 is not capable to calculate the $PFD(t)$. The PM type B is not supported as well. The schedule of the PM type A is restricted to be periodic with equal periods. SRS that consist of multiple elements with widely used element structures, where the redundant elements are identical, were treated via the respective equations to calculate the $\overline{PFD}$, see [IEC11d].

5.3.5 Results

Selected one and three element models were evaluated, the results are presented hereafter. The literature models, which were described in subsections 5.3.2, 5.3.3, and 5.3.4, are applied to validate the models that are introduced in this thesis. Moreover, the presented validation results demonstrate selected important features of the introduced models, such as the PM type A, B with incomplete coverage, elementwise for each element, and arbitrarily scheduled, not restricted to be periodic with equal periods.

Case 1: One element model, subject to PM type A with complete coverage

The evaluated one element model is subject to the PM type A with complete coverage and periodic with equal periods. The model parameters are according to table 5.1, except the coverage of the PM type A, which is given by $tca = 1$ that reflects the complete coverage. The PM plan is derived from the PM plan 1, which is given in table 5.2, where the PM type B is omitted, i.e. $\mathcal{T}_b = ()$. The calculated results of the $PFD(t)$ are plotted in figure 5.7. The respective figures of $\overline{PFD}$, $PFD_{\max}$ are given in table 5.5. The presented results were calculated via the literature models and the model of this thesis.

The literature models and the models of this thesis provide similar results, as clearly

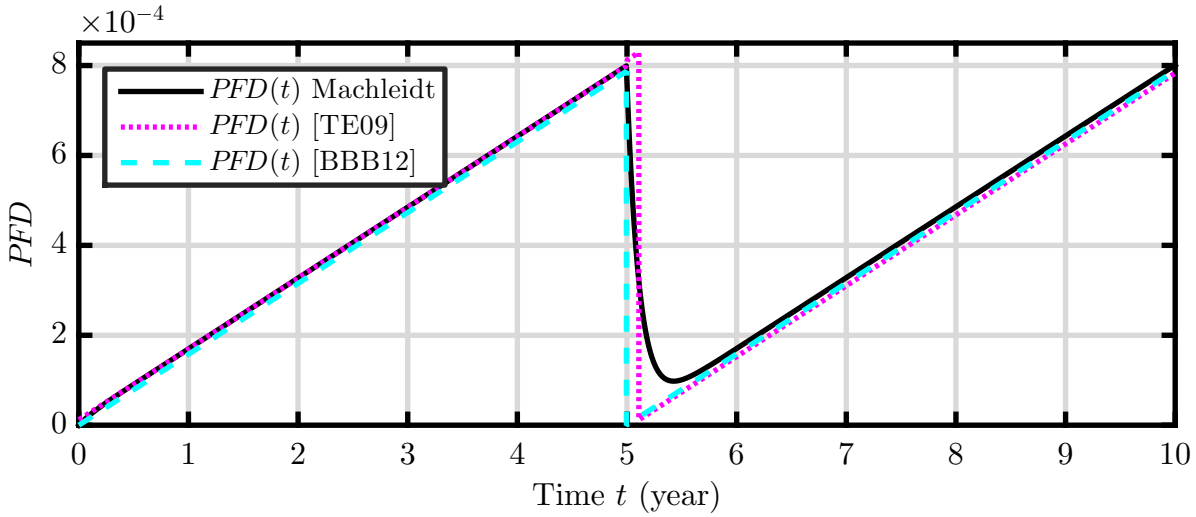

Figure 5.7: $PFD(t)$ of one element model in case 1

	Case 1		Case 2		Case 3	
	$\overline{PFD}$	$PFD_{\max}$	$\overline{PFD}$	$PFD_{\max}$	$\overline{PFD}$	$PFD_{\max}$
Machleidt	$4.1 \cdot 10^{-4}$	$8 \cdot 10^{-4}$	$3.2 \cdot 10^{-4}$	$6.1 \cdot 10^{-4}$	$4 \cdot 10^{-4}$	$7.7 \cdot 10^{-4}$
[TE09]	$4.1 \cdot 10^{-4}$	$8.3 \cdot 10^{-4}$	$4.1 \cdot 10^{-4}$	$8.3 \cdot 10^{-4}$	$3.3 \cdot 10^{-4}$	$6.7 \cdot 10^{-4}$
[BBB12]	$3.9 \cdot 10^{-4}$	$7.9 \cdot 10^{-4}$	$3.0 \cdot 10^{-4}$	$6.0 \cdot 10^{-4}$	$2.2 \cdot 10^{-4}$	$4.4 \cdot 10^{-4}$
[IEC11d]	$4.2 \cdot 10^{-4}$	-	$4.2 \cdot 10^{-4}$	-	$5 \cdot 10^{-4}$	-

Table 5.5: $\overline{PFD}$, $PFD_{\max}$ of one element models in case 1, 2, and 3

evident in figure 5.7 and table 5.5. The $PFD(t)$ plots slightly differ at the time of the PM, due to the differently modeled repair process that is related to the PM. Instant repair was modeled in [BBB12] and the repair time was neglected. In [TE09], an average repair duration was modeled. During the repair duration, failures might occur that will be completely revealed and restored when the repair duration is over. In this thesis, the occurred failures are revealed by the PM and repaired after that. The time of repair is random and distributed via a given exponential CDF. In contrast to [TE09], the failures that occur during a repair will remain unrevealed and will not be restored by the running repair activities. These failures will be revealed by the next PM.

Case 2: One element model, subject to PM type A with complete coverage and B

The evaluated one element model is equivalent to that of case 1, except the PM plan that is now equivalent to the PM plan 1, which is given in table 5.2. The calculated results of the $PFD(t)$ are plotted in figure 5.8. The respective figures of $\overline{PFD}$, $PFD_{\max}$ are given in table 5.5.

The $PFD(t)$ plot in figure 5.8 that is related to the model of [TE09] is equivalent to that in figure 5.7. Moreover, the values of $\overline{PFD}$, $PFD_{\max}$ of the models of [TE09] and

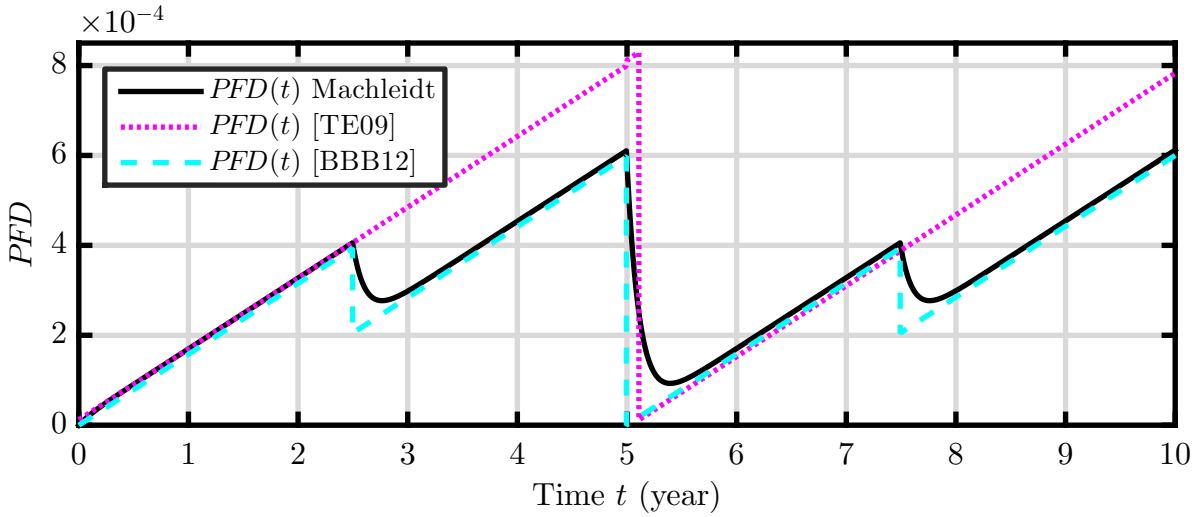

Figure 5.8: $PFD(t)$ of one element model in case 2

[IEC11d] remain unchanged in case 2, in comparison to case 1, see table 5.5. It is clearly evident that, the models of [TE09] and [IEC11d] do not consider the PM type B.

Case 3: One element model, subject to PM type A with incomplete coverage and B

The evaluated one element model is equivalent to that of case 2, except the coverage of the PM type A, which is now incomplete. The coverage of the PM type A is given by $tca = 0.8$, which is equivalent to 80%. The calculated results of the $PFD(t)$ are plotted in figure 5.9. The respective values of $\overline{PFD}$, $PFD_{\max}$ are given in table 5.5.

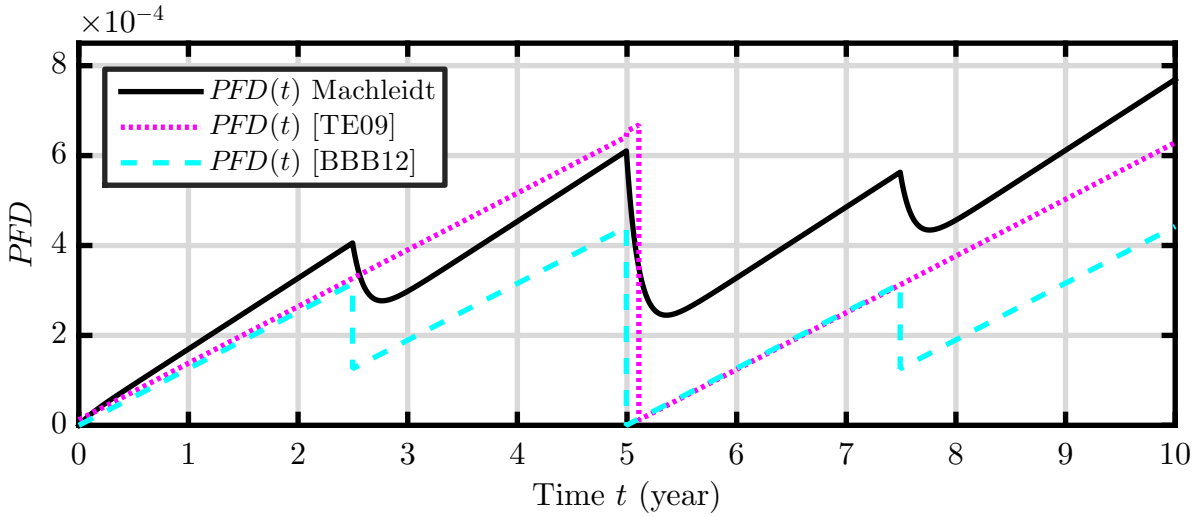

Figure 5.9: $PFD(t)$ of one element model in case 3

In figure 5.9, the $PFD(t)$ plot that is related to the model of this thesis shows a greater gradient. Moreover, the decrease in $PFD(t)$ that is caused by the PM type A is significantly less, compared to the models of [TE09] and [BBB12]. It is clearly evident

that, the models of [TE09] and [BBB12] do not consider the incomplete coverage of the PM type A and the resulting dn-failures. This feature is modeled by the model of [IEC11d], which is unable to model PM type B, see table 5.5.

Case 4: Three element model, subject to simultaneous PM type A

The evaluated three element model is subject to the PM type A with complete coverage, periodic with equal periods, and simultaneous for all elements. The model parameters are according to table 5.3, except the coverage of the PM type A, which is given by $tca = 1$ that reflects the complete coverage. The PM plan is derived from the PM plan 1, which is given in table 5.4, where the PM type B is omitted, i.e. $\mathcal{T}_{b,i} = ()$ for all $i \in \{1, 2, 3\}$. The calculated results of the $PFD(t)$ for the 1oo3 element structure are plotted in figure 5.10. The respective values of $\overline{PFD}$, $PFD_{\max}$ are given in in tables 5.6, 5.7, and 5.8 for the 1oo3, 2oo3, and 3oo3 element structures.

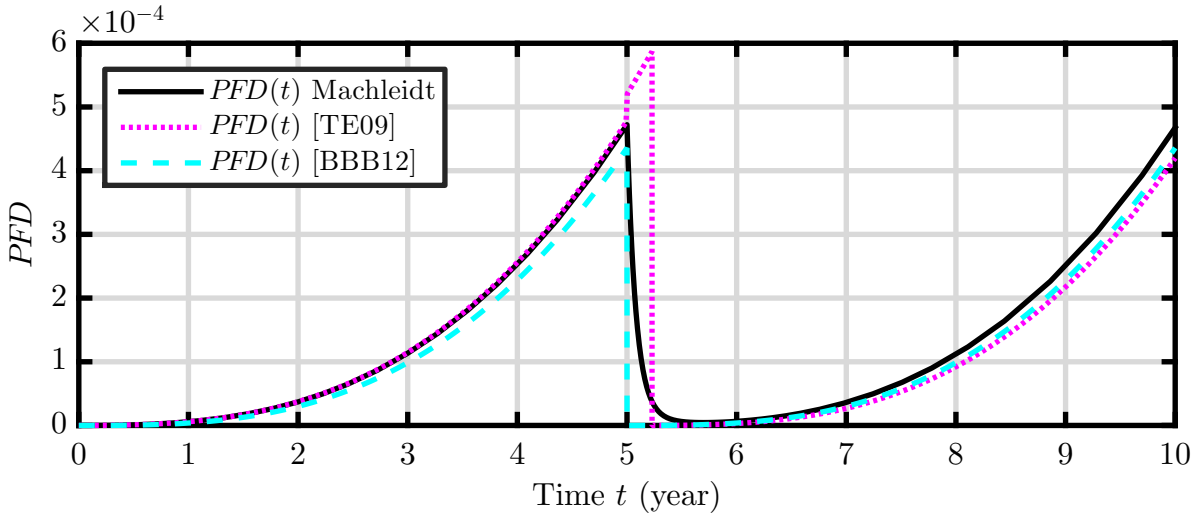

Figure 5.10: $PFD(t)$ of three element model in case 4, 1oo3 element structure

	Case 4		Case 5		Case 6	
	$\overline{PFD}$	$PFD_{\max}$	$\overline{PFD}$	$PFD_{\max}$	$\overline{PFD}$	$PFD_{\max}$
Machleidt	$1.3 \cdot 10^{-4}$	$4.7 \cdot 10^{-4}$	$1.1 \cdot 10^{-4}$	$4.2 \cdot 10^{-4}$	$0.5 \cdot 10^{-4}$	$2.1 \cdot 10^{-4}$
[TE09]	$1.3 \cdot 10^{-4}$	$5.9 \cdot 10^{-4}$	$1.1 \cdot 10^{-4}$	$4.6 \cdot 10^{-4}$	$1.1 \cdot 10^{-4}$	$4.2 \cdot 10^{-4}$
[BBB12]	$1.1 \cdot 10^{-4}$	$4.4 \cdot 10^{-4}$	$1.1 \cdot 10^{-4}$	$4.4 \cdot 10^{-4}$	$0.4 \cdot 10^{-4}$	$2.0 \cdot 10^{-4}$
[IEC11d]	$2.3 \cdot 10^{-4}$	-	$2.3 \cdot 10^{-4}$	-	$2.3 \cdot 10^{-4}$	-

Table 5.6: $\overline{PFD}$, $PFD_{\max}$ of three element model in case 4, 5, and 6, 1oo3 element structure

In figure 5.10, it is clearly visible that the plot related to the model of [TE09] significantly differs from the plot related to the model of this thesis, due to the differently modeled repair process. It has to be noted that, the difference is greater compared to the one element model that is analyzed above. The $PFD(t)$ plot that is related to the model

	Case 4		Case 5		Case 6	
	$\overline{PFD}$	$PFD_{\max}$	$\overline{PFD}$	$PFD_{\max}$	$\overline{PFD}$	$PFD_{\max}$
Machleidt	$6.3 \cdot 10^{-3}$	$17 \cdot 10^{-3}$	$6.1 \cdot 10^{-3}$	$17 \cdot 10^{-3}$	$3.7 \cdot 10^{-3}$	$10 \cdot 10^{-3}$
[TE09]	$6.5 \cdot 10^{-3}$	$21 \cdot 10^{-3}$	$6.0 \cdot 10^{-3}$	$17 \cdot 10^{-3}$	$6.0 \cdot 10^{-3}$	$17 \cdot 10^{-3}$
[BBB12]	$5.6 \cdot 10^{-3}$	$16 \cdot 10^{-4}$	$5.6 \cdot 10^{-3}$	$16 \cdot 10^{-3}$	$3.2 \cdot 10^{-3}$	$10 \cdot 10^{-3}$
[IEC11d]	$8.8 \cdot 10^{-3}$	-	$8.8 \cdot 10^{-3}$	-	$8.8 \cdot 10^{-3}$	-

Table 5.7: $\overline{PFD}$, $PFD_{\max}$ of three element model in case 4, 5, and 6, 2oo3 element structure

	Case 4		Case 5		Case 6	
	$\overline{PFD}$	$PFD_{\max}$	$\overline{PFD}$	$PFD_{\max}$	$\overline{PFD}$	$PFD_{\max}$
Machleidt	0.12	0.22	0.12	0.22	0.10	0.17
[TE09]	0.12	0.25	0.12	0.22	0.12	0.22
[BBB12]	0.11	0.21	0.11	0.21	0.08	0.16
[IEC11d]	0.14	-	0.14	-	0.14	-

Table 5.8: $\overline{PFD}$, $PFD_{\max}$ of three element model in case 4, 5, and 6, 3oo3 element structure

of [BBB12] slightly differs from the plot related to the model of this thesis. This can be explained by the neglected dd-failures. It has to be emphasized that, the $\overline{PFD}$ that was calculated via the model of [IEC11d] is significantly greater in comparison to those figures calculated via the other evaluated models, see table 5.6. An increase of approx. 75% occurs for the 1oo3 element structure.

Case 5: Three element model, subject to elementwise PM type A

The evaluated three element model is equivalent to that of case 4, except the PM that is now executed elementwise for each element. The respective PM plan is equivalent to the PM plan 2, which is given in table 5.4, where the PM type B is omitted, i.e. $\mathcal{T}_{b,i} = ()$ for all $i \in \{1, 2, 3\}$. The calculated results of the $PFD(t)$ for the 1oo3 element structure are plotted in figure 5.11. The respective values of $\overline{PFD}$, $PFD_{\max}$ are given in in tables 5.6, 5.7, and 5.8 for the 1oo3, 2oo3, and 3oo3 element structures.

The $PFD(t)$ plot in figure 5.11 that is related to the model of [BBB12] is equivalent to that in figure 5.10. Moreover, the values of $\overline{PFD}$, $PFD_{\max}$ of the models of [BBB12] and [IEC11d] remain unchanged in case 2, in comparison to case 1, see tables 5.6, 5.7, and 5.8. It is clearly evident that, the models of [BBB12] and [IEC11d] do not model the elementwise PM type A. In contrast, the model of [TE09] is capable to model the elementwise PM type A for the case of the staggered PM, see subsection 5.3.2.

Case 6: Three element model, subject to elementwise PM type A and B

The evaluated three element model is equivalent to that of case 5, except the PM plan that now includes PM type A and B, which are both executed elementwise. The respective PM plan is equivalent to the PM plan 2, which is given in table 5.4. The calculated results

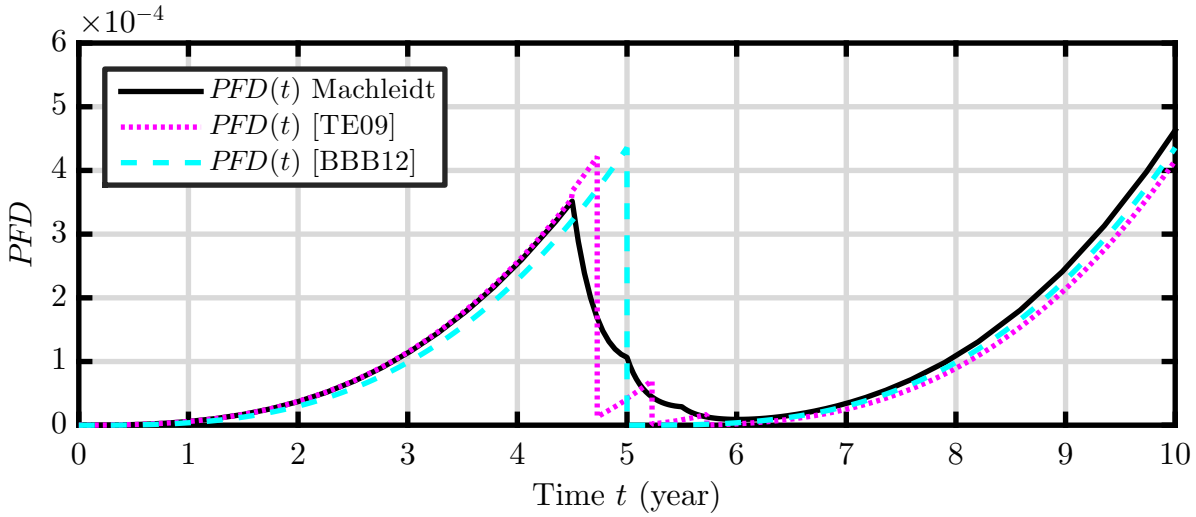

Figure 5.11: $PFD(t)$ of three element model in case 5, 1oo3 element structure

of the $PFD(t)$ for the 1oo3 element structure are plotted in figure 5.12. The respective values of $\overline{PFD}$, $PFD_{\max}$ are given in in tables 5.6, 5.7, and 5.8 for the 1oo3, 2oo3, and 3oo3 element structures.

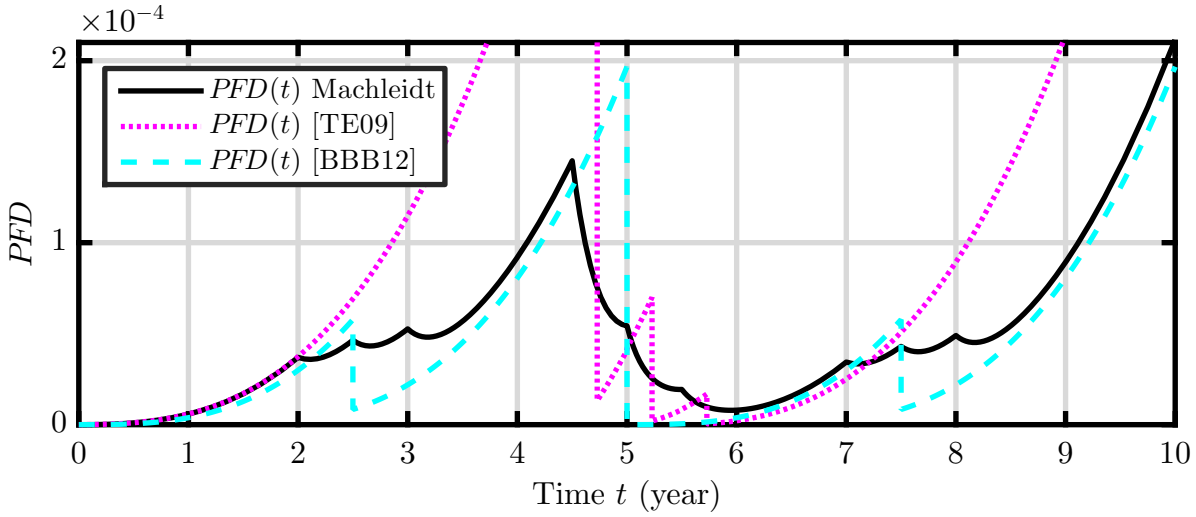

Figure 5.12: $PFD(t)$ of three element model in case 6, 1oo3 element structure

In figure 5.12 it is clearly visible that, the plot that is related to the model of this thesis significantly differs from the plots related to the other models. It is clearly evident that, the elementwise PM type B is only modeled by the model that is introduced in this thesis.

Conclusions

Due to the analyzed and discussed results it is concluded that, the models that are introduced in this thesis provide plausible results. It was shown that, significant deviations of the results between the compared models have occurred. These deviations were analyzed

and discussed. Different missing features of the literature models in comparison to the introduced models were identified to cause the deviations. None of the evaluated literature models was capable of modeling the PM type A and B with incomplete coverage, executed elementwise for each element, and arbitrarily scheduled. Furthermore, the introduced models exhibit further features, such as s-failures, dependencies resulting from the multiple failure modes, etc. These further features additionally impact the $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$, where the particular impact depends on parametrization. Overall, less approximations and restrictions are required by the introduced models, particularly in regard to the PM.

5.4 Sensitivity analysis

5.4.1 Preliminaries

The parameters of a probabilistic model influence the $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$. This section aims to analyze the deviations of the parameters. Particularly, the impact of the deviations on the $\overline{PFD}$ or $PFD_{\max}$ is analyzed. In subsection 5.4.2, the theoretical framework of the applied sensitivity analysis procedure is given. The results of the sensitivity analysis are presented in subsection 5.4.3. The presented results treat the one and three element models.

5.4.2 Theoretical framework

The system sensitivity theory was introduced in [Fra78]. The *analytical* procedures of sensitivity analysis are frequently applied in literature, particularly in [Fra78]. These procedures apply linearization and therefore only small parameter deviations can be analyzed. In contrast, the sensitivity analysis procedure that is applied in this thesis is *simulative*. It does not require linearization and enables to analyze arbitrary parameter deviations. The procedure is applied to the parameters that are related to the PM plans. These parameters are mainly focused in this thesis because they are related to purely organizational measures and easily adaptable. In general, arbitrary parameters can be analyzed via the described procedure.

The sensitivity measures are introduced and defined below. Let the $\overline{PFD}$ and $PFD_{\max}$ be given via an $\mathcal{MP}$-$\mathcal{CMC}$ and the procedure to calculate the state probabilities of the $\mathcal{MP}$-$\mathcal{CMC}$, which was described in section 4.2. The $\overline{PFD}(\boldsymbol{\alpha})$ and $PFD_{\max}(\boldsymbol{\alpha})$ are considered to be the scalar-valued functions of the actual parameter vector $\boldsymbol{\alpha} = \begin{bmatrix} \alpha_1 & \alpha_2 & \dots \end{bmatrix}^T$, which might deviate from its nominal values. Let the vector of the nominal parameter values be given by $\boldsymbol{\alpha}_0 = \begin{bmatrix} \alpha_{1,0} & \alpha_{2,0} & \dots \end{bmatrix}^T$. The $\overline{PFD}(\boldsymbol{\alpha})$ for an arbitrary actual parameter

vector $\boldsymbol{\alpha}$ is given by

$$\overline{PFD}(\boldsymbol{\alpha}) = \overline{G}(\boldsymbol{\alpha}_0, \boldsymbol{\alpha}) \cdot \overline{PFD}(\boldsymbol{\alpha}_0) \ . \tag{5.6}$$

The ability of a deviation of the nominal parameter vector to cause a deviation of the nominal $\overline{PFD}$ is given by the gain of the $\overline{PFD}$, which is denoted by $\overline{G}(\boldsymbol{\alpha}_0, \boldsymbol{\alpha})$ and defined hereafter. In an analogous manner, the gain of the $PFD_{\max}$ is defined afterwards.

Definition 46 (Gain of $\overline{PFD}$). The gain of the $\overline{PFD}$ is given by

$$\overline{G}(\boldsymbol{\alpha}_0, \boldsymbol{\alpha}) = \frac{\overline{PFD}(\boldsymbol{\alpha})}{\overline{PFD}(\boldsymbol{\alpha}_0)} \ , \tag{5.7}$$

as the ratio of the $\overline{PFD}$ for the actual and nominal parameter vectors $\boldsymbol{\alpha}$ and $\boldsymbol{\alpha}_0$.

Definition 47 (Gain of $PFD_{\max}$). The gain of the $PFD_{\max}$ is given by

$$G_{\max}(\boldsymbol{\alpha}_0, \boldsymbol{\alpha}) = \frac{PFD_{\max}(\boldsymbol{\alpha})}{PFD_{\max}(\boldsymbol{\alpha}_0)} \ , \tag{5.8}$$

as the ratio of the $PFD_{\max}$ for the actual and nominal parameter vectors $\boldsymbol{\alpha}$ and $\boldsymbol{\alpha}_0$.

In this thesis the deviation of one parameter at a time is analyzed. Let the deviation of a particular parameter from its nominal value be given by $\Delta\alpha_j$, the respective actual parameter vector will be $\boldsymbol{\alpha} = \begin{bmatrix} \alpha_{1,0} & \dots & \alpha_{j,0} + \Delta\alpha_j & \dots \end{bmatrix}^T$. The respective sensitivity measures are given by $\overline{G}(\boldsymbol{\alpha}_0, \Delta\alpha_j)$, $G_{\max}(\boldsymbol{\alpha}_0, \Delta\alpha_j)$.

The relation of the $\overline{G}(\boldsymbol{\alpha}_0, \Delta\alpha_j)$, $G_{\max}(\boldsymbol{\alpha}_0, \Delta\alpha_j)$ to the *performance index sensitivity*, which was defined in [Fra78], is described below. Let the performance index of interest be $\overline{G}(\boldsymbol{\alpha}_0, \Delta\alpha_j)$, the respective sensitivity in regard to the parameter α_j is given by

$$s_{\overline{G},\alpha_j}(\boldsymbol{\alpha}_0) = \lim_{\Delta\alpha_j \to 0} \frac{\overline{G}(\boldsymbol{\alpha}_0, \Delta\alpha_j) - \overline{G}(\boldsymbol{\alpha}_0, 0)}{\Delta\alpha_j} \ . \tag{5.9}$$

In equation (5.9) it is clearly noticeable that, the performance index sensitivity reflects the gradient of the performance index $\overline{G}(\boldsymbol{\alpha}_0, \Delta\alpha_j)$ over $\Delta\alpha_j$, at the point $\Delta\alpha_j = 0$, i.e. for the nominal parameter values. This relation is illustrated in figure 5.13. In contrast to the respective performance-index sensitivities, the sensitivity measures $\overline{G}(\boldsymbol{\alpha}_0, \Delta\alpha_j)$, $G_{\max}(\boldsymbol{\alpha}_0, \Delta\alpha_j)$ are not restricted to infinitesimal parameter deviations $\Delta\alpha_j \to 0$ and enable to analyze arbitrary $\Delta\alpha_j$. It has to be noted that, the vector of the nominal parameter values $\boldsymbol{\alpha}_0$ will be omitted in the notation of the sensitivity measures, i.e. $\overline{G}(\Delta\alpha_j)$, $G_{\max}(\Delta\alpha_j)$.

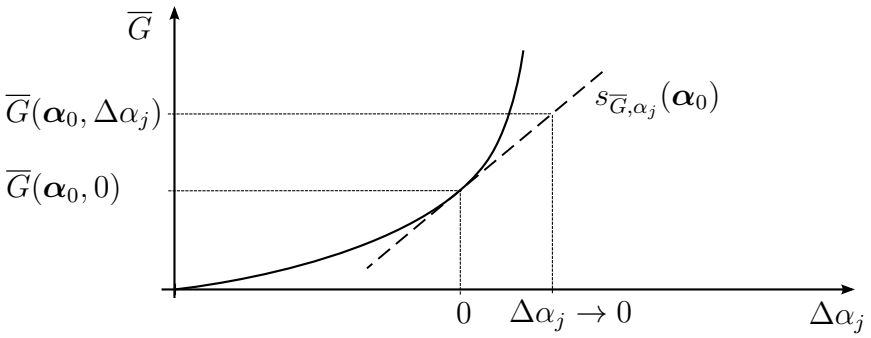

Figure 5.13: Performance index sensitivity $s_{\overline{G},\alpha_j}(\boldsymbol{\alpha}_0)$ as gradient of $\overline{G}(\boldsymbol{\alpha}_0, \Delta\alpha_j)$

5.4.3 Results

One element model

The deviations of parameters of the one element model are analyzed via the introduced sensitivity measures. The analyzed one element model is equivalent to that, which was discussed in case 3 of subsection 5.3.5. The parameters that are related to the PM plan are analyzed. The nominal PM plan is given by $\mathcal{T} = (\mathcal{T}_a, \mathcal{T}_b)$, $\mathcal{T}_a = (t_{a,1})$, $\mathcal{T}_b = (t_{b,1}, t_{b,2})$, where the times of PM are $t_{a,1} = 5$, $t_{b,1} = 2.5$, and $t_{b,2} = 7.5$ years. The $\overline{G}(\Delta t_{h,j})$, $G_{\max}(\Delta t_{h,j})$ are plotted in figures 5.14, 5.15 for the deviations $\Delta t_{h,j} \in \{\Delta t_{a,1}, \Delta t_{b,1}, \Delta t_{b,2}\}$.

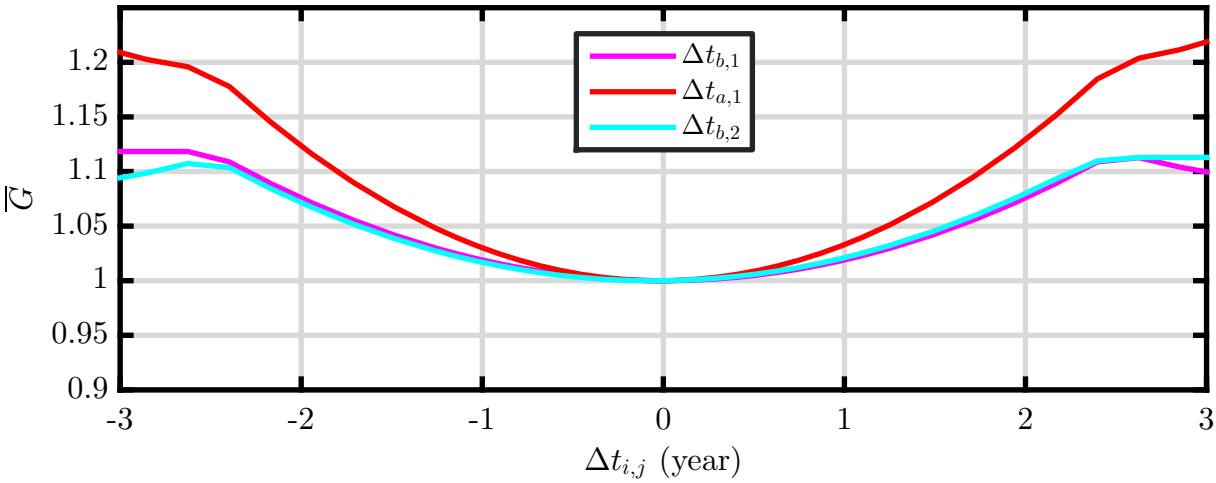

Figure 5.14: Gain of $\overline{PFD}$ of one element model

It is clearly noticeable that, a deviation of a particular time $t_{h,j}$ from its nominal value results in $\overline{G}(\Delta t_{h,j}) \geq 1$, see figure 5.14. Hence, the deviation of a particular time $t_{h,j}$, while the other times of the PM plan remain constant, does not decrease the $\overline{PFD}$ in comparison to the nominal $\overline{PFD}$. The $\overline{PFD}$ will increase if the deviation $\Delta t_{h,j}$ is increased.

In contrast to $\overline{G}(\Delta t_{h,j})$, for some positive deviations $\Delta t_{a,1}$, $\Delta t_{b,2}$ it is $G_{\max}(\Delta t_{h,j}) < 1$, see figure 5.15. The $PFD_{\max}$ might increase or decrease for a given deviation $\Delta t_{a,1}$ or $\Delta t_{b,2}$. The $PFD_{\max}$ remains constant for a deviation $\Delta t_{b,1}$.

An example is given below to illustrate the influence of the deviation $\Delta t_{b,2}$.

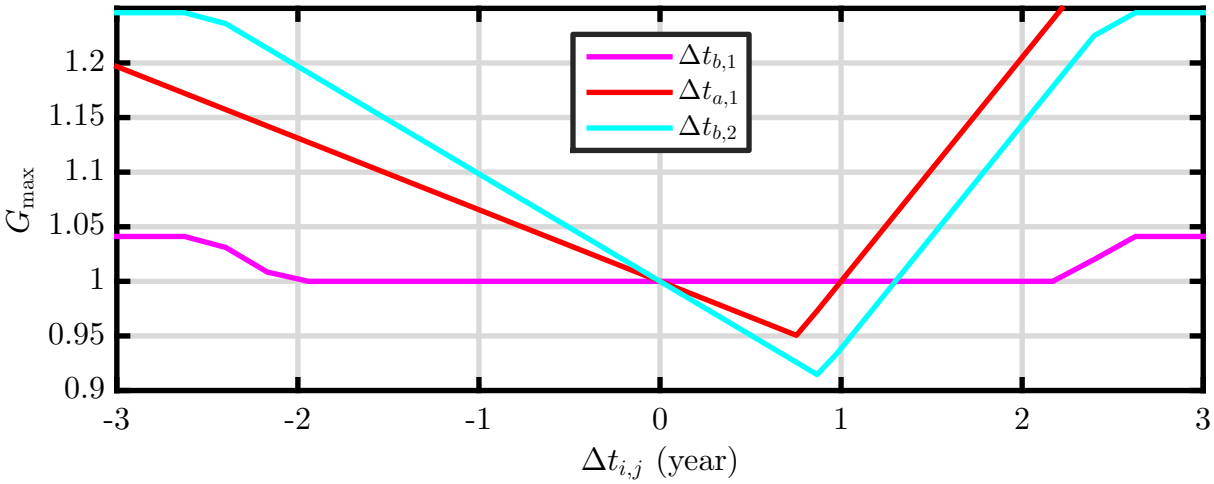

Figure 5.15: Gain of $PFD_{\max}$ of one element model

Example 5.1 (Deviation $\Delta t_{b,2}$ of one element model). The deviation of the time $t_{b,2}$ by $\Delta t_{b,2} = 0.88$ year is analyzed. In figure 5.16, the $PFD(t)$ plot for the nominal PM plan is compared to that for the PM plan with the deviation $\Delta t_{b,2}$. It is clearly noticeable that the $\overline{PFD}$ is slightly increased and the $PFD_{\max}$ is significantly decreased by the deviation $\Delta t_{b,2}$. These results are consistent to the sensitivity measures for $\Delta t_{b,2} = 0.88$ year in figures 5.14, 5.15, where $\overline{G}(\Delta t_{b,2} = 0.88) \approx 1.03$ and $G_{\max}(\Delta t_{b,2} = 0.88) \approx 0.92$. Hence, the $\overline{PFD}$ is increased by approx. 3% and $PFD_{\max}$ is decreased by approx. 8%.

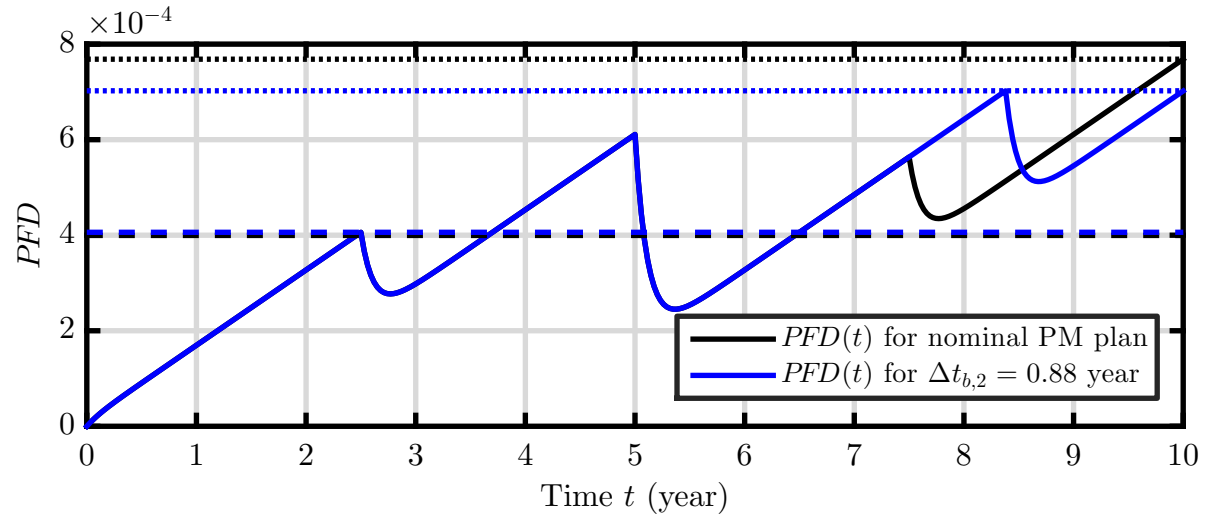

Figure 5.16: Influence of $\Delta t_{b,2} = 0.88$ year on $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$

Three element model

The deviations of parameters of the three element model is analyzed. The analyzed three element model is equivalent to that, which was introduced in subsection 5.2.3. The element structure of the model is 1oo3. The PM plan 1 in table 5.4 is given as the nominal

PM plan. The $\overline{G}(\Delta t_{h,i,j})$, $G_{\max}(\Delta t_{h,i,j})$ are plotted in figures 5.17, 5.18 for the deviations $\Delta t_{h,i,j} \in \{\Delta t_{a,1,1}, \Delta t_{b,1,1}, \Delta t_{b,1,2}\}$.

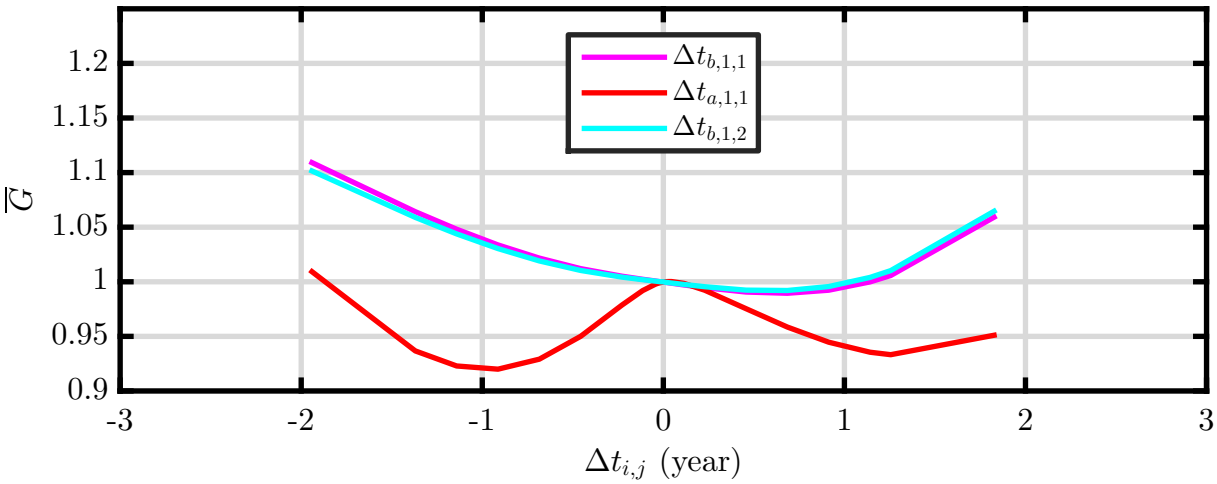

Figure 5.17: Gain of $\overline{PFD}$ of three element 1oo3 model

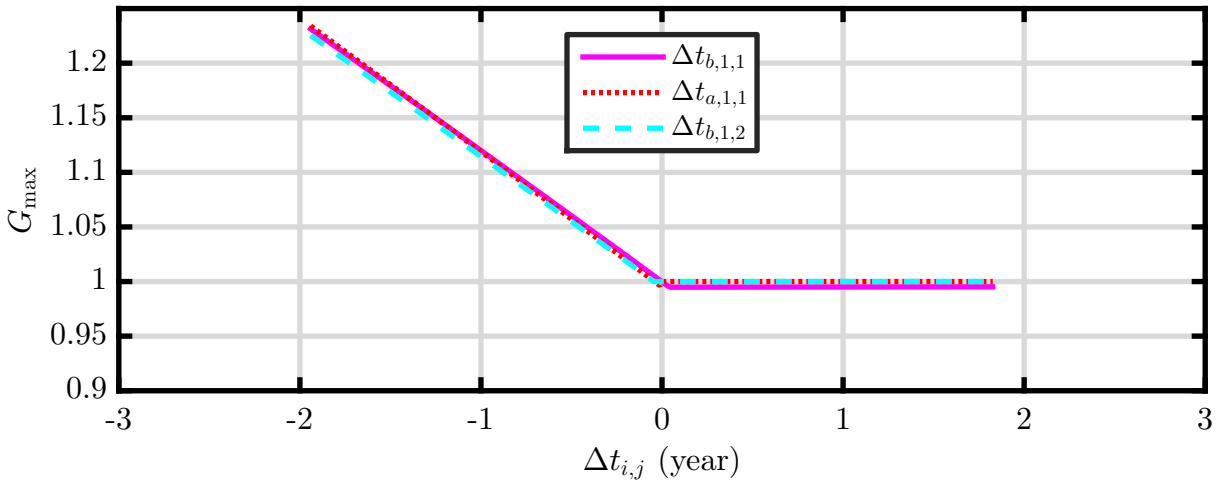

Figure 5.18: Gain of $PFD_{\max}$ of three element 1oo3 model

In figure 5.17 it is noticeable that, the $\overline{PFD}$ can be significantly decreased via the deviation $\Delta t_{a,1,1}$. Since the elements of the model are identical, the deviation $\Delta t_{a,2,1}$ or $\Delta t_{a,3,1}$ will provide identical results as $\Delta t_{a,1,1}$. A deviation $\Delta t_{b,1,1}$ or $\Delta t_{b,1,2}$ might slightly decrease the $\overline{PFD}$. This also holds for the deviation $\Delta t_{b,2,1}$, $\Delta t_{b,2,2}$, $\Delta t_{b,3,1}$, and $\Delta t_{b,3,2}$.

The deviation $\Delta t_{h,i,j}$, $\Delta t_{h,i,j} \in \{\Delta t_{a,1,1}, \Delta t_{b,1,1}, \Delta t_{b,1,2}\}$, does not decrease the $PFD_{\max}$ in comparison to the nominal $PFD_{\max}$. For a negative deviation $\Delta t_{h,i,j}$ the $PFD_{\max}$ is significantly increased. The $PFD_{\max}$ remains constant for a positive deviation $\Delta t_{h,i,j}$, see figure 5.18.

Conclusions

The introduced sensitivity measures $\overline{G}$ and $G_{\max}$ enable to analyze the impact of a parameter deviation on the $\overline{PFD}$ or $PFD_{\max}$. It was observed that the $\overline{PFD}$ or $PFD_{\max}$

might be significantly changed by the deviation of a parameter that is related to the PM plan. It is concluded that, a given model with a nominal PM plan can be analyzed via the introduced sensitivity measures if the parameter deviations decrease the $\overline{PFD}$ or $PFD_{\max}$.

It has to be emphasized that, the deviation of only one parameter at a time was analyzed. The introduced PM plans and probabilistic models provide the degrees of freedom to arbitrarily vary the available parameters, also multiple parameters at a time. The available degrees of freedom span a multi-dimensional space that is explored in only one direction via the introduced procedure. This is illustrated in figure 5.19, where the contour plot of the $PFD_{\max}$ of the one element model is shown over $\Delta t_{a,1}$ and $\Delta t_{b,2}$. The time $t_{b,1}$ remained constant, i.e. $\Delta t_{b,1} = 0$. The plots of the $G_{\max}(\Delta t_{a,1})$ or $G_{\max}(\Delta t_{b,2})$ in figure 5.15 reflect the movement along the y-axis or x-axis of the contour plot. As shown in figure 5.19, all available dimensions have to be explored to determine the deviations $\Delta t_{a,1}$ and $\Delta t_{b,2}$, which provide the minimum of the $PFD_{\max}$. This requires a high effort that grows exponentially with the number of dimensions. Therefore, heuristic optimization will be applied to explore the multi-dimensional space that is spanned by the degrees of freedom and search for the minima of the $\overline{PFD}$ or $PFD_{\max}$.

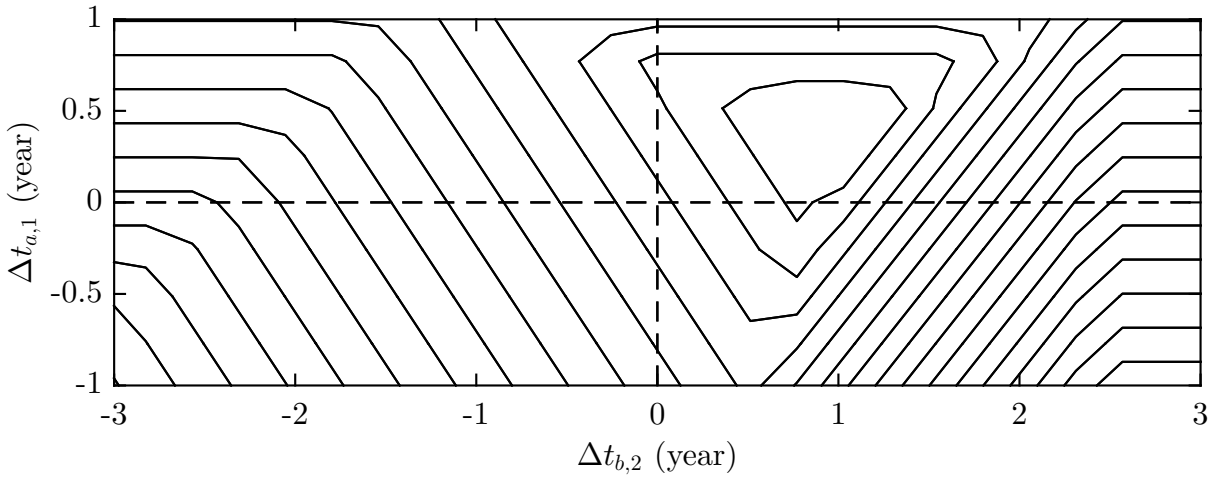

Figure 5.19: Contour plot of $PFD_{\max}$ over $\Delta t_{a,1}$, $\Delta t_{b,2}$

Chapter 6

Optimization of preventive maintenance plans

6.1 Preliminaries

In section 5.4 it was shown that, the $\overline{PFD}$ and $PFD_{\max}$ might be significantly changed by a change of the respective PM plan. Particularly, the degrees of freedom of the PM plans that were not treated by other models were analyzed, such as elementwise PM of individual elements and arbitrarily variable individual periods, which are not restricted to be equal, of PM. In this chapter a heuristic optimization algorithm is applied to vary an initial PM plan within the given degrees of freedom to decrease the $\overline{PFD}$ or $PFD_{\max}$.

The organization of this chapter is outlined below. First, the treated optimization problems are defined in section 6.2. In section 6.3, the Nelder-Mead method is described, which is the applied heuristic optimization algorithm. A heuristic approach to overcome the local extrema and effectively minimize the $PFD_{\max}$ is introduced in section 6.4. In section 6.5, the optimization results are presented and discussed. The general conclusions that are given in section 6.6 were derived from the optimization results. Particularly, a useful set of rules is given to decide for a given SRS if the $\overline{PFD}$ or $PFD_{\max}$ can be significantly decreased via optimization of the PM plan.

6.2 Optimization problems

Let the probabilistic model of an SRS be given. $\mathcal{T} \in \mathcal{S}$ is a PM plan of the given model and $\mathcal{S}$ is a given PM strategy. The PM strategies that are applied in this thesis were defined in section 4.4. The choice of a PM plan from the set that is given by a PM strategy is formulated as the optimization problem given by

$$\min\{f(\mathcal{T}) \,|\, \mathcal{T} \in \mathcal{S}\} \,, \tag{6.1}$$

where the function $f(\mathcal{T}) : \mathcal{S} \subset \mathbb{R}^n \to \mathbb{R}$ is an objective function with the domain $\mathcal{S}$. The objective functions are evaluated via the given probabilistic model. The $\overline{PFD}$ and $PFD_{\max}$ are calculated via the respective $\mathcal{MP}$-$\mathcal{CMC}$, as in section 4.2. It is assumed that, the parameters except the PM plan remain constant and the $\overline{PFD}(\mathcal{T})$ and $PFD_{\max}(\mathcal{T})$ are functions of $\mathcal{T}$. The treated objective functions are introduced immediately hereafter.

Objective function quantifying $\overline{PFD}$

The objective function that quantifies the $\overline{PFD}$ is given by

$$\overline{PFD}(\mathcal{T}) : \mathcal{S} \subset \mathbb{R}^n \to \mathbb{R} \, . \tag{6.2}$$

The respective optimization problem is defined by $\min\{\overline{PFD}(\mathcal{T}) \,|\, \mathcal{T} \in \mathcal{S}\}$.

Objective function quantifying $PFD_{\max}$

The objective function that quantifies the $PFD_{\max}$ is given by

$$PFD_{\max}(\mathcal{T}) : \mathcal{S} \subset \mathbb{R}^n \to \mathbb{R} \, . \tag{6.3}$$

The respective optimization problem is defined by $\min\{PFD_{\max}(\mathcal{T}) \,|\, \mathcal{T} \in \mathcal{S}\}$.

Objective function quantifying the weighted trade-off between $\overline{PFD}$ and $PFD_{\max}$

The two objective functions introduced above are combined to define the objective function that quantifies the weighted trade-off between $\overline{PFD}(\mathcal{T})$ and $PFD_{\max}(\mathcal{T})$. The respective objective function

$$WT(\mathcal{T}) : \mathcal{S} \subset \mathbb{R}^n \to \mathbb{R} \, , \tag{6.4}$$

is given by

$$WT(\mathcal{T}) = c \cdot \frac{\overline{PFD}(\mathcal{T})}{\overline{PFD}(\mathcal{T}_{\overline{PFD}})} + (1 - c) \cdot \frac{PFD_{\max}(\mathcal{T})}{PFD_{\max}(\mathcal{T}_{PFD_{\max}})} \, . \tag{6.5}$$

where $c \in \mathbb{R}$, $0 \leq c \leq 1$, is a given trade-off factor and $\mathcal{T}_{\overline{PFD}}$, $\mathcal{T}_{PFD_{\max}}$ are the arguments of the solutions of the two former optimization problems defined above, $\mathcal{T}_{\overline{PFD}} = \arg\left(\min\{\overline{PFD}(\mathcal{T}) \,|\, \mathcal{T} \in \mathcal{S}\}\right)$ and $\mathcal{T}_{PFD_{\max}} = \arg\left(\min\{PFD_{\max}(\mathcal{T}) \,|\, \mathcal{T} \in \mathcal{S}\}\right)$. The respective optimization problem is defined by $\min\{WT(\mathcal{T}) \,|\, \mathcal{T} \in \mathcal{S}\}$.

6.3 Optimization algorithm

6.3.1 Preliminaries

This subsection treats the optimization algorithm that is applied to the optimization problems. First, the choice of the optimization algorithm is motivated. After this, the

Nelder-Mead method, which is the chosen optimization algorithm, is described in subsection 6.3.2.

The choice of the optimization algorithm is based on the characteristics of the respective optimization problem. The treated optimization problems are nonlinear because of the nonlinear objective functions and no derivatives of the objective functions are available. Moreover, the objective functions are not explicitly defined due to the complexity of an explicit definition. Instead, it is preferred to implicitly specify an objective function via a given model. A robust and easy to apply optimization algorithm is required that can handle nonlinear objective functions and does not require derivatives of objective functions. Several optimization algorithms might be applied to the optimization problems with the described characteristics, e.g. *evolutionary algorithms* or *direct search* methods, see [LTT00]. This thesis does not aim to find the best available optimization algorithm, but to apply a robust algorithm that converges to a local or possibly global minimum. Therefore, the Nelder-Mead method is chosen in this thesis to be applied to the treated optimization problems.

6.3.2 Nelder-Mead method

The Nelder-Mead method was introduced in [NM65]. In [LRWW98], the convergence properties of the Nelder-Mead method were analyzed. This optimization algorithm is available in the optimization toolbox of MATLAB, the numerical computing software developed by MathWorks. The Nelder-Mead method is widely applied to minimize a scalar-valued nonlinear objective function of n real variables. Only the objective function values are used for the optimization and no derivative information is required. The Nelder-Mead method is usually applied to unconstrained optimization problems. However, the treated optimization problems imply constraints for the times of a PM plan. These times are intended to be within the mission time interval, i.e. $0 \leq t \leq t_m$. Because the constraint violations are penalized by the objective functions, the respective optimization problems can be treated as unconstrained optimization problems.

The algorithm of the Nelder-Mead method is outlined hereafter. Let us consider an objective function of n variables and a given initial value. First, the initial simplex that is specified by its $n + 1$ vertices is determined from the given initial value. The initial value is the first vertex of the initial simplex. The other n vertices are calculated by adding 5% of each component to the initial value. The objective function values of the $n + 1$ vertices are calculated. After that, the algorithm computes at each iteration an updated simplex. A set of procedures is available to compute the updated simplex. These procedures are illustrated in figures 6.1 and 6.2 for $n = 2$ variables. The current simplex is drawn by dashed lines and the respective updated simplex by solid lines. The illustrated procedures are defined in [LRWW98]. Basically, that vertex of the simplex,

where the objective function value is greater than that of other vertices, is moved to a point with a less objective function value. The applied procedure to compute the updated simplex is selected based on the relative ranks of the objective function values. This is a characteristic feature of the direct search methods, numerical values are not used. The iterative computation will terminate if the termination constraints are met. If the difference in the objective function values of the simplex is less than f_{tol} and the difference between the current best point and the other points of the simplex is less than x_{tol}, the algorithm will terminate. The termination constraints f_{tol} and x_{tol} have to be specified. Further termination constraints are the maximum number of iterations and the maximum number of evaluations of the objective function. The best computed value is returned as the solution of the evaluated optimization problem.

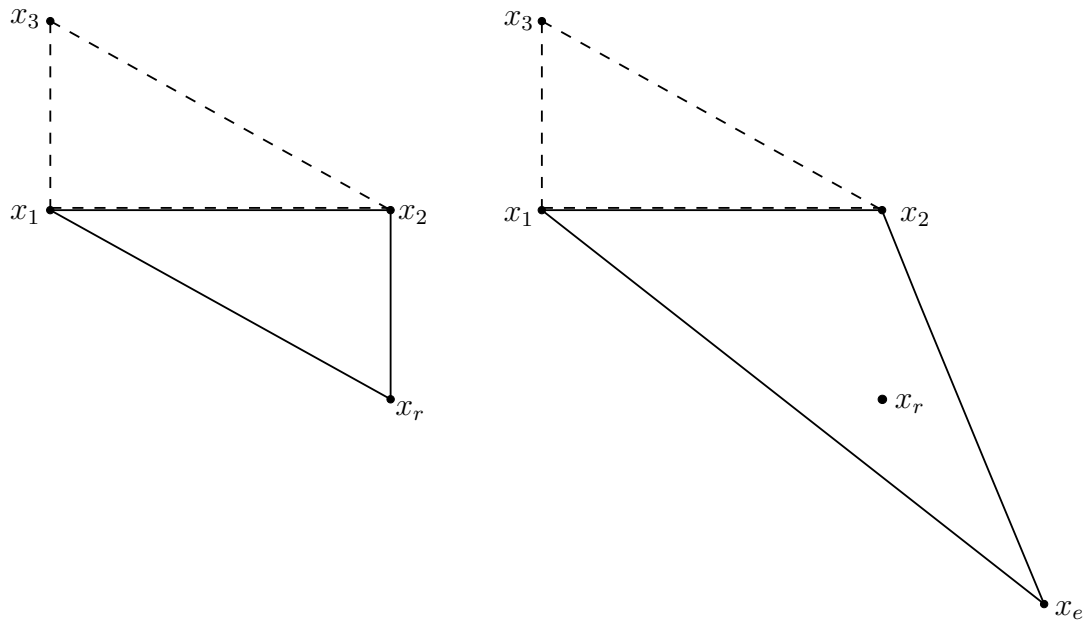

Figure 6.1: Reflexion and expansion iterations of Nelder-Mead method; [LRWW98]

The drawbacks of the Nelder-Mead method have also to be mentioned. The Nelder-Mead method might result in a slow convergence towards the solution of an evaluated optimization problem. This is especially the case for high-dimensional optimization problems and in comparison to optimization algorithms that use derivatives of the objective function. Moreover, similar to all existing nonlinear optimization algorithms, it can not be guaranteed that the Nelder-Mead method will overcome the possibly existing local extrema and find the global extremum.

In example 6.1 the convergence of the Nelder-Mead method is illustrated for the minimization of $PFD_{\max}$.

Example 6.1 (Convergence of Nelder-Mead method towards a minimum). Let the one element model be given, which was discussed in case 3 of subsection 5.3.5. The initial PM plan is given by $\mathcal{T}_{\text{init}} = (\mathcal{T}_a, \mathcal{T}_b)$, $\mathcal{T}_a = (t_{a,1})$, $\mathcal{T}_b = (t_{b,1}, t_{b,2})$, where the times

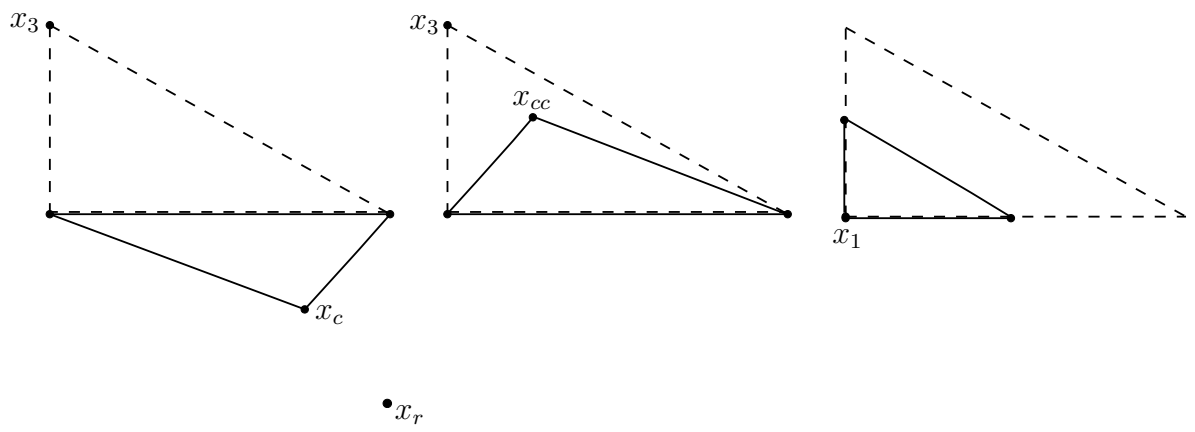

Figure 6.2: Outside contraction, inside contraction, and shrink iterations of Nelder-Mead method; [LRWW98]

of PM are $t_{a,1} = 5$, $t_{b,1} = 2.5$, and $t_{b,2} = 7.5$ years. The time $t_{b,1}$ remains constant and the times $t_{a,1}$, $t_{b,1}$ are varied by the Nelder-Mead method to minimize the $PFD_{\max}$. The contour plot of the $PFD_{\max}$ is shown over $\Delta t_{a,1}$ and $\Delta t_{b,2}$ in figure 6.3. The first six iterations of the Nelder-Mead method are shown in the contour plot of figure 6.3. The initial point is placed at the origin. It is clearly noticeable that the points computed by the Nelder-Mead method converge towards the minimum.

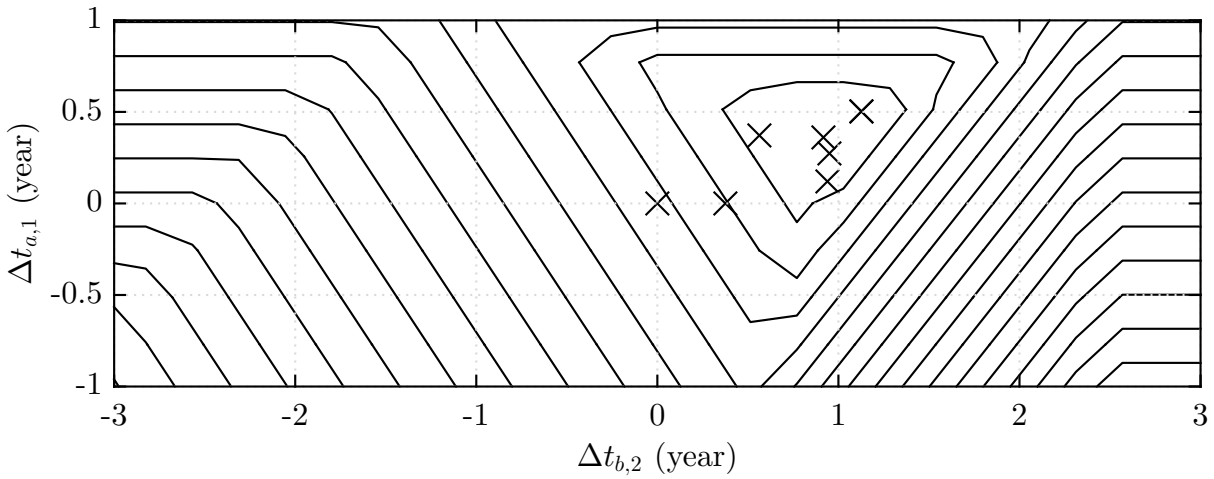

Figure 6.3: Convergence of Nelder-Mead method in example 6.1

It has to be noted that, for nonlinear optimization problems the convergence of an optimization algorithm towards an extremum strongly depends on the chosen initial point. The explored domain of the objective function might have multiple basins of attraction, where the optimization algorithm would converge to a local extremum and be stucked there. This problem occurred for some of the optimization problems that are treated in this thesis. The next section describes the applied heuristic approach to overcome this problem.

6.4 Heuristic approach to minimize the maximum PFD

The drawbacks of the Nelder-Mead method were mentioned above. Particularly, the inability to overcome local extrema is an important disadvantage. It was observed that, local minima frequently occurred for the *direct minimization* of the $PFD_{\max}$, especially for an increasing number of dimensions, i.e. the number of varied times of a PM plan. An exemplary case is shown in figure 6.4. The $PFD(t)$ plots for the initial PM plan and the PM plan that was determined by the direct minimization of the $PFD_{\max}$ are shown. The one element model of example 6.1 was treated. The initial PM plan is given by $\mathcal{T}_{\text{init}} = (\mathcal{T}_a, \mathcal{T}_b)$, $\mathcal{T}_a = (t_{a,1}, \ldots, t_{a,4})$, $\mathcal{T}_b = ()$, where the times of PM type A are $t_{a,1} = 2$, $t_{a,2} = 4$, $t_{a,3} = 6$, and $t_{a,4} = 8$ years. It is clearly noticeable that, the peaks of the blue $PFD(t)$ plot that results from direct minimization of $PFD_{\max}$ are not equal. As will be shown below, a PM plan with equal peaks provides a value of $PFD_{\max}$ that is less than that in figure 6.4. Hence, the algorithm was terminated although it is evident that the minimum of the $PFD_{\max}$ was not found. The algorithm must have computed a local minimum that could not be overcome. Different initial PM plans have been evaluated and the algorithm usually got stuck in a local minimum. An initial PM plan that will provide convergence to the global minimum is not available for all types of models.

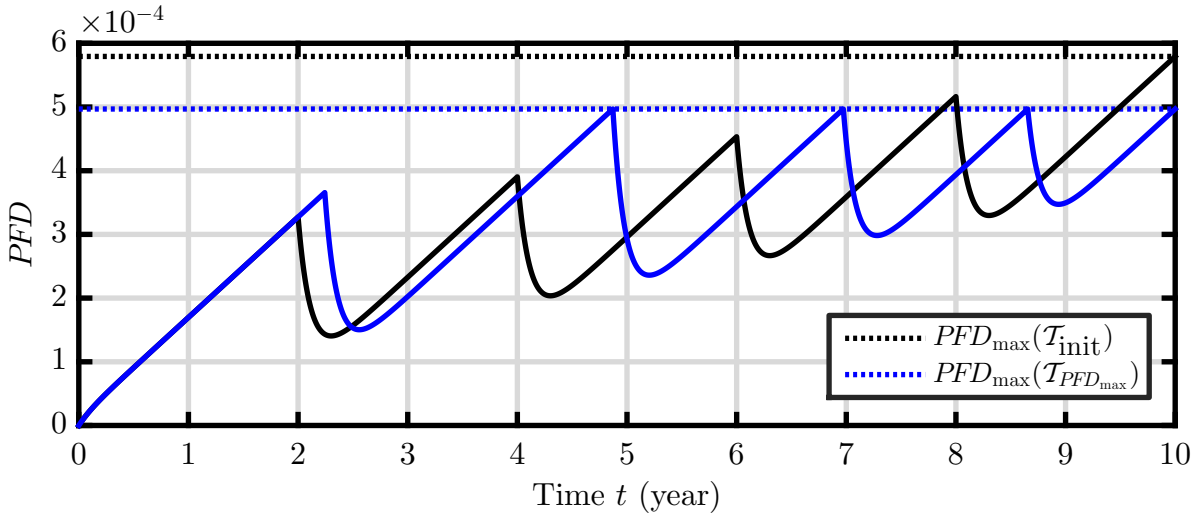

Figure 6.4: Result of direct minimization of $PFD_{\max}$

In contrast to the minimization of $PFD_{\max}$, no obvious problems with local extrema occurred for the minimization of $\overline{PFD}$. Different initial PM plans were evaluated and led to very similar computed solutions. It can be explained by the different properties of the objective functions that quantify $PFD_{\max}$ or $\overline{PFD}$. Overall, it can not be assured that no local minima have occurred for the minimization of $\overline{PFD}$, but the respective optimization problem seems to be less problematic in this regard. Therefore, the PM plans, which are periodic with equal periods and simultaneous for all elements, will be used as initial PM plans for the minimization of $\overline{PFD}$.

The heuristic approach described below is applied to improve the computation of the optimization problem to minimize the $PFD_{\max}$ and overcome the local extrema. The numerical ODE solver, which is applied to calculate the state probabilities and $PFD(t)$ of an $\mathcal{MP}$-$\mathcal{CMC}$, is utilized by the heuristic approach. The basic idea is to determine a PM plan with equal peaks and this will be the PM plan that minimizes the $PFD_{\max}$. The applied numerical ODE solver has the so-called *event location property*. That will stop the integration if a given upper bound of the $PFD(t)$ is reached. When the given upper bound is reached and the number of the phase transitions is not exceeded, the integration will be stopped and the next phase transition triggered to occur. The heuristic approach is to minimize the $PFD_{\max}$ by variation of the upper bound. If the upper bound is too low, the phase transitions will occur too early and the $PFD(t)$ will increase to a high value, resulting in a high $PFD_{\max}$. If the upper bound is too high, the phase transitions will not occur at all and the $PFD_{\max}$ will also be high. If the upper bound is right, the peaks of the $PFD(t)$ will be equal and the $PFD_{\max}$ will be less than in the previous cases. It has to be emphasized that, the sequence of the phase transitions is an additional restriction that is required for the heuristic approach. It is assumed that this sequence is identical to the initial PM plan. Each phase transition reflects an individual PM within the PM plan. The resulting optimization problem is of dimension one. Hence, the PM plan with equal peaks, which minimizes the $PFD_{\max}$ is determined.

The described heuristic approach is illustrated in figure 6.5. A PM plan with only one time of PM is considered. The respective phase transition will occur if the given upper bound PFD_b is reached, i.e. at the time $t_{a,1}$ in figure 6.5. By variation of the PFD_b the time of the phase transition that minimizes the $PFD_{\max}$ will be determined. For example, if the upper bound PFD_b in figure 6.5 is increased, the $PFD_{\max}$ will be decreased.

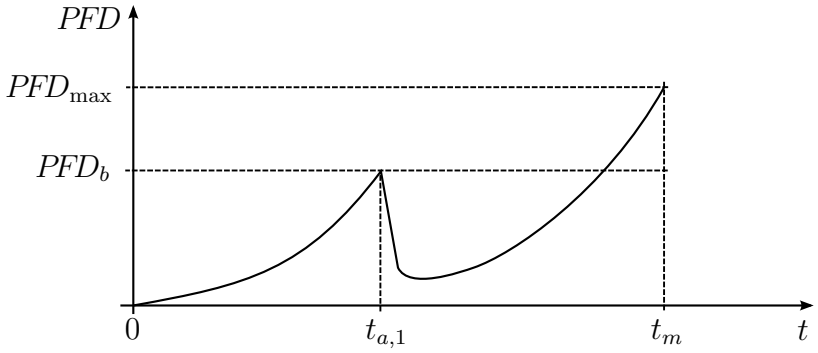

Figure 6.5: Heuristic approach to minimize $PFD_{\max}$

It has to be emphasized that, a different optimization problem is solved via the heuristic approach in comparison to the direct minimization of the $PFD_{\max}$. The objective function of the heuristic approach is given by

$$PFD_{\max}(PFD_b) : \mathbb{R} \to \mathbb{R} \; . \tag{6.6}$$

Hence, the respective optimization problem is given by $\min\{PFD_{\max}(PFD_b) \mid PFD_b \in \mathbb{R}\}$. It is clearly noticeable that the dimension of the optimization problem is always one. In contrast, the dimension of the direct minimization of $PFD_{\max}$ depends on the initial PM plan and is usually multi-dimensional, see definition in section 6.2.

The described heuristic approach was applied to the exemplary optimization case that is shown in figure 6.4, where a local minimum occurred. The result is shown in figure 6.6. The peaks of the blue $PFD(t)$ plot are equal. The determined PM plan provides the $PFD_{\max}(\mathcal{T}_{PFD_{\max}})$ that is less than the result of direct minimization in figure 6.4. The introduced heuristic approach is effective to overcome local extrema and is applied in this thesis to minimize the $PFD_{\max}$.

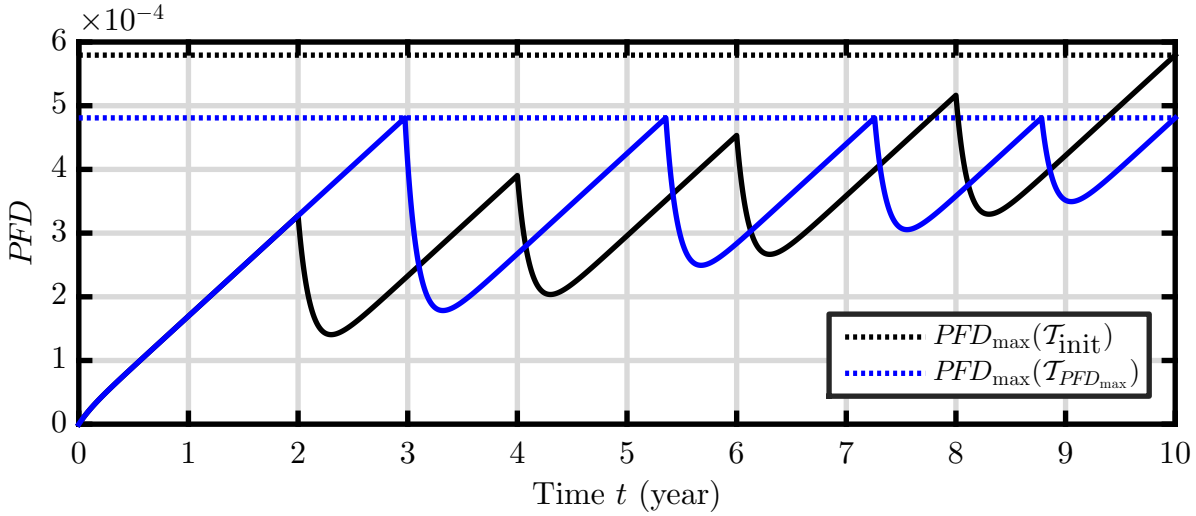

Figure 6.6: Result of minimization of $PFD_{\max}$ via heuristic approach

6.5 Results

6.5.1 Preliminaries

The Nelder-Mead method was applied to search for a PM plan from a given set to minimize a given objective. The optimization results are presented below and in the following subsections. The evaluated optimization problems were formulated in section 6.2. Particularly, the minimized objectives are the $\overline{PFD}$, $PFD_{\max}$, and the weighted trade-off between the $\overline{PFD}$ and $PFD_{\max}$.

The organization of section 6.5 is briefly outlined. A description of the optimization procedure, which was applied to all treated models, and an overview of the results of the 1oo3 model are given directly hereafter. The optimization results of further models with different element structures, degrees of redundancy, coverages of PM, and fractions of cc-failures are presented and discussed in the following subsections. The models without redundancy, which have the 1oo1 or 3oo3 element structure, are treated in subsection

6.5.2. The treated models are additionally classified into these with a complete coverage of the PM type A or an incomplete coverage. In subsection 6.5.3, the models with redundancy, which have the 1oo3 or 2oo3 element structure, are treated in a similar manner. After that, the models with redundancy and common-cause failures are treated in subsection 6.5.4.

The applied optimization procedure is described. First, the $\overline{PFD}$ was minimized. A conventional PM plan, which is periodic with equal periods and simultaneous for all elements, was used as the initial PM plan. After that, the $PFD_{\max}$ was minimized via the heuristic approach that was presented in section 6.4. Finally, the trade-off was minimized with the PM plan that minimizes the $PFD_{\max}$ as initial PM plan. These three minimization runs were executed for different PM strategies. A PM strategy defines the available degrees of freedom for the minimization. The PM plan that minimizes the $\overline{PFD}$, $PFD_{\max}$, or weighted trade-off is denoted by $\mathcal{T}_{\overline{PFD}}$, $\mathcal{T}_{PFD_{\max}}$, or $\mathcal{T}_{WT}$. Each PM plan $\mathcal{T} \in \{\mathcal{T}_{\overline{PFD}}, \mathcal{T}_{PFD_{\max}}, \mathcal{T}_{WT}\}$ is characterized by the respective values of the two objective functions $\overline{PFD}(\mathcal{T})$ and $PFD_{\max}(\mathcal{T})$. These are given relatively to the respective values of the initial PM plan, i.e. $\overline{G}(\mathcal{T}) = \overline{PFD}(\mathcal{T})/\overline{PFD}(\mathcal{T}_{\text{init}})$ and $G_{\max}(\mathcal{T}) = PFD_{\max}(\mathcal{T})/PFD_{\max}(\mathcal{T}_{\text{init}})$ in figure 6.7. Due to the relative representation, the results are independent on the number of PM of an initial PM plan. For example, the gains $\overline{G}(\mathcal{T}_{\overline{PFD}})$, $G_{\max}(\mathcal{T}_{\overline{PFD}})$ quantify the impact of the minimization of $\overline{PFD}$ on $\overline{PFD}(\mathcal{T}_{\text{init}})$ or $PFD_{\max}(\mathcal{T}_{\text{init}})$ for an arbitrary initial PM plan with equal characteristics. The results given below can be generalized for initial PM plans $\mathcal{T}_{\text{init}} \in \mathcal{S}_V$, where $\mathcal{T}_{a,i} = (t_{a,i,1}, \ldots, t_{a,i,ne_{a,i}})$, $\mathcal{T}_{b,i} = (t_{b,i,1}, \ldots, t_{b,i,ne_{b,i}})$, and $ne_{b,i} = 2ne_{a,i}$. The initial PM plan that was used for the optimization is given by $\mathcal{T}_{a,i} = (5)$ years, $\mathcal{T}_{b,i} = (2.5, 7.5)$ years, for all $i \in \{1, \ldots, k\}$ of a model with k elements.

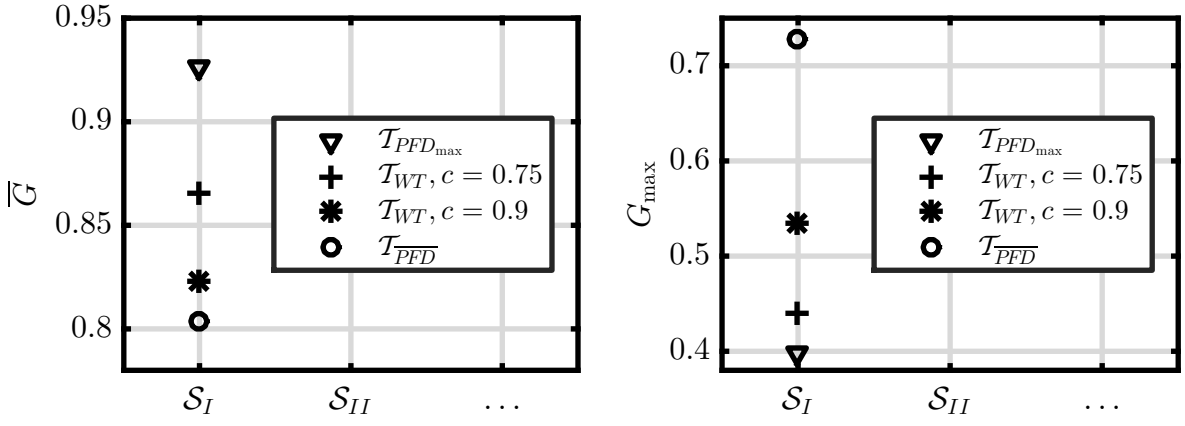

Figure 6.7: Overview of optimization results of 1oo3 model

The results of the 1oo3 model with complete coverage of PM type A are shown in figure 6.7. The gains $\overline{G}$ and $G_{\max}$ are shown for each PM plan $\mathcal{T}_{\overline{PFD}}$, $\mathcal{T}_{WT}$, and $\mathcal{T}_{PFD_{\max}}$. Only the results for the PM strategy I are given in this overview, i.e. $\mathcal{T}_{\overline{PFD}}, \mathcal{T}_{WT}, \mathcal{T}_{PFD_{\max}} \in \mathcal{S}_I$. First, the minimization of $\overline{PFD}$ is discussed. The $\overline{PFD}$ is decreased by approx. 20%.

The $PFD_{\max}$ is decreased by approx. 25% through the minimization of $\overline{PFD}$. Now, the minimization of $PFD_{\max}$ is discussed. The $PFD_{\max}$ is decreased by approx. 60% and the $\overline{PFD}$ is decreased by approx. 7% through the minimization of $PFD_{\max}$. It has to be noted that, the lowest determined values of $\overline{G}$ and $G_{\max}$ did not occur simultaneously. It indicates that the objectives to minimize the $\overline{G}$ or $G_{\max}$ are conflictive. The minimization results of the weighted trade-off between $\overline{PFD}$ and $PFD_{\max}$ are given for selected values of c. The choice of the weighting factor c enables to determine a PM plan that provides the desired trade-off between the minimal $\overline{PFD}$ and $PFD_{\max}$. Overall, it is demonstrated that, the introduced optimization framework is effective to significantly decrease the $\overline{PFD}$ or $PFD_{\max}$, and for this model even both of them simultaneously.

6.5.2 Models without redundancy

PM type A with complete coverage

The optimization results of models without redundancy, with the 1oo1 or 3oo3 element structure, are presented and discussed below. These models feature a complete coverage of the PM type A. The minimization of $\overline{PFD}$ or $PFD_{\max}$ is treated. In figure 6.8, the results of the 1oo1 model are shown. It has to be noted that, the simultaneous PM are not applicable to the 1oo1 model due to only one element. Hence, the PM strategies explored by optimization are limited to the PM strategies IIIb and I. In contrast, for models with multiple elements all the PM strategies, defined in section 4.4, were explored. The results of the 3oo3 model are shown in figure 6.9.

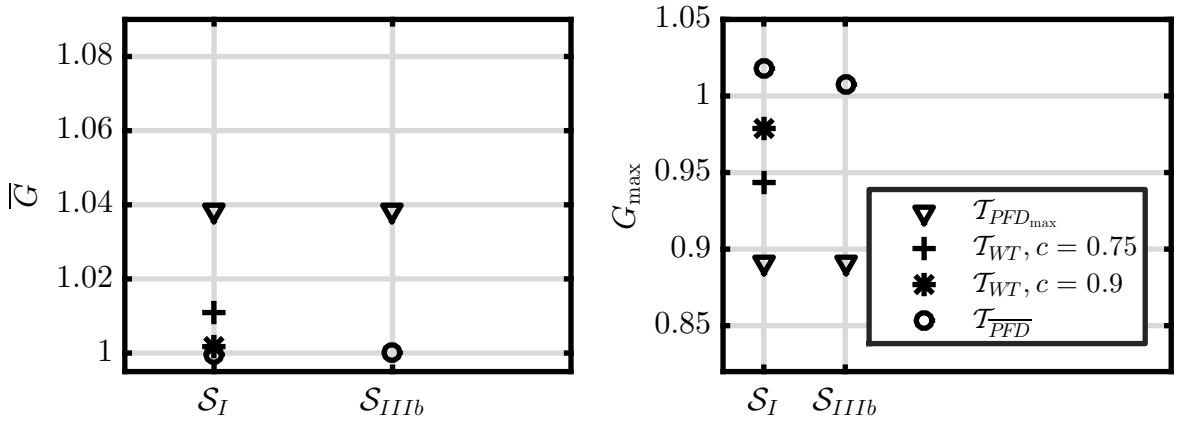

Figure 6.8: Optimization results of 1oo1 model with complete coverage

The results of the minimization of $\overline{PFD}$ are discussed first. The decrease in $\overline{PFD}$ is less than 0.1% for the 1oo1 and 3oo3 models, as shown in figures 6.8 and 6.9. This decrease is considered to be negligible. In comparison to the initial PM plan, the minimization of $\overline{PFD}$ does not significantly decrease the $\overline{PFD}$. Moreover, the $PFD_{\max}$ is increased by approx. 2-4% through the minimization of $\overline{PFD}$.

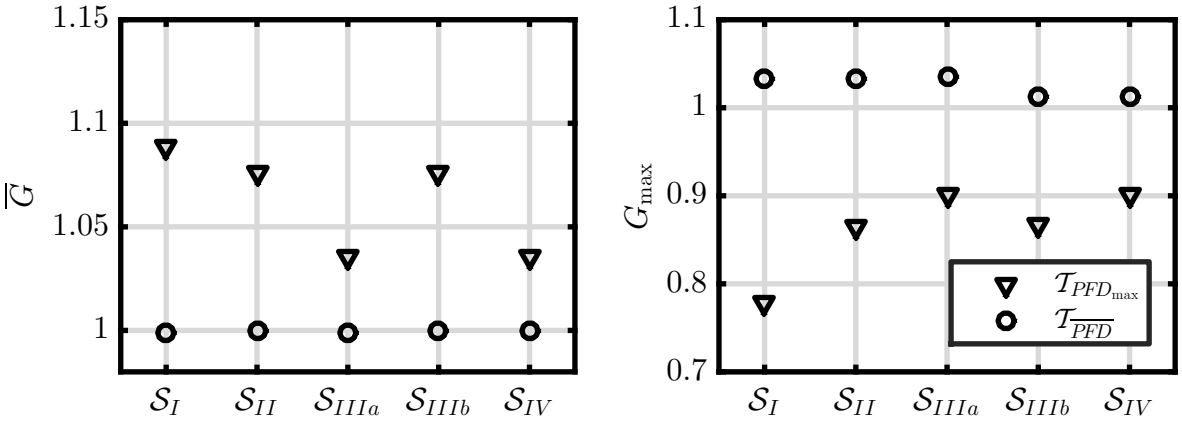

Figure 6.9: Optimization results of 3oo3 model with complete coverage

The discussed results are explained below. The observed negligible decrease in $\overline{PFD}$ is explained by the shape of the respective $PFD(t)$ plots, see figures 6.10, 6.11. The $PFD(t)$ plots have an approx. constant gradient. For the 1oo1 model it is caused by the comparably small rate parameters of failures and large rate parameters of repairs. This leads to an approx. constant probability flow to the states of the $\mathcal{MP}$-$\mathcal{CMC}$, where the safety function is not provided. For the 3oo3 model, the total $PFD(t)$ is the sum of the $PFD(t)$ of each element. In general it can be stated that, the models without redundancy have a $PFD(t)$ plot with an approx. constant gradient for usual practically relevant values of the rate parameters. For an approx. constant gradient of the $PFD(t)$, a periodic PM plan with equal periods will provide a comparable low $\overline{PFD}$ that can not be further significantly decreased by optimization. Furthermore, if the number of the PM executions per element is equal, a PM plan that is simultaneous for all elements will be appropriate to provide low $\overline{PFD}$. However, for some particular values of the rate parameters the minimization of $\overline{PFD}$ might determine a PM plan that significantly decreases the $\overline{PFD}$.

Now, the results of the minimization of $PFD_{\max}$ are discussed. The greatest decrease in $PFD_{\max}$ equals approx. 10% or 22% for the 1oo1 or 3oo3 models, as shown in figures 6.8 and 6.9. The $\overline{PFD}$ is increased by approx. 4% or 9% through the minimization of $PFD_{\max}$. For the 1oo1 model only two PM strategies were evaluated. Hence, in order to analyze all available PM strategies we focus on the 3oo3 model. The results are compared, starting with the PM strategy with the most restrictions, i.e. IV and continue to that with the least, i.e. I. The detailed analysis of figure 6.9 identifies that, the decrease in $PFD_{\max}$ occurred in three steps. In a first step, the $PFD_{\max}$ is decreased by approx. 10% via optimization for the explored PM strategy IV or IIIa. A further decrease by approx. 3% is achieved for the explored PM strategy IIIb or II. Finally, the total decrease in $PFD_{\max}$, by approx. 22%, is achieved for the explored PM strategy I.

The discussed results of the minimization of $PFD_{\max}$ are explained below. The decrease in $PFD_{\max}$, which is related to the first step of decrease, is achieved via the variation of the simultaneously executed PM B, permitted by the PM strategy IV. No further significant

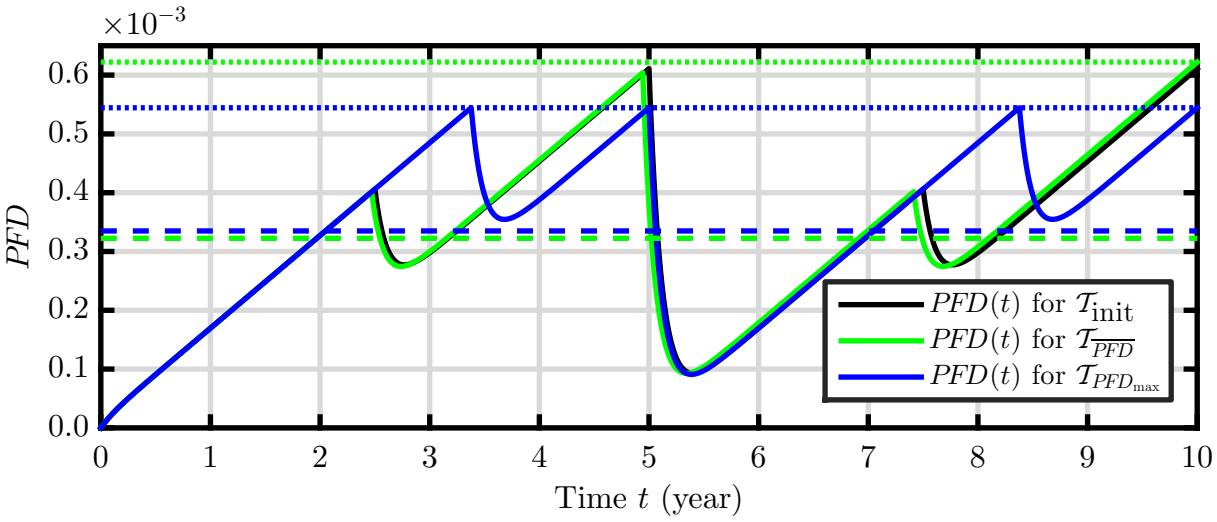

Figure 6.10: $PFD(t)$ for optimized PM plans of 1oo1 model with complete coverage

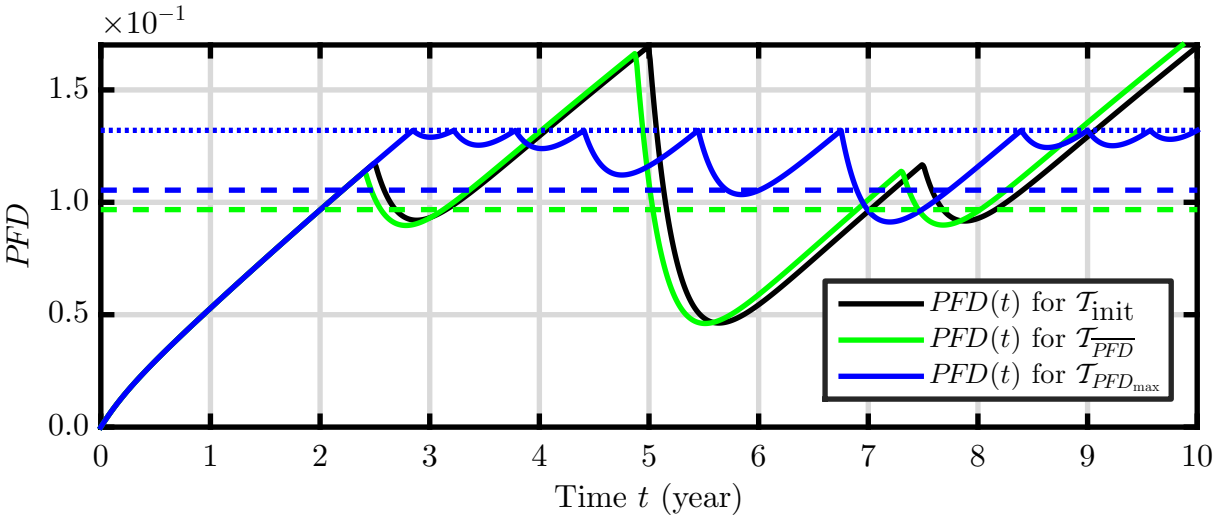

Figure 6.11: $PFD(t)$ for optimized PM plans of 3oo3 model with complete coverage

decrease is achieved via the additional variation of the simultaneously executed PM A, permitted by the PM strategy IIIa. A further decrease is achieved via the additional variation of the elementwise executed PM B, permitted by the PM strategy IIIb. Again, no further significant decrease is achieved via the additional variation of the simultaneously executed PM A, permitted by the PM strategy II. Finally, a further decrease is achieved via the additional variation of the elementwise executed PM A, permitted by the PM strategy I. Overall, the significant total decrease in $PFD_{\max}$ is explained via the greater total number of phase transitions for the elementwise PM A and B. The greater number of phase transitions more effectively prevents the $PFD(t)$ from an increase to high values.

The results of the minimization of the trade-off between $\overline{PFD}$ and $PFD_{\max}$ are shown in figure 6.8 for selected weighting factors. The $PFD(t)$ plots of the 1oo1 or 3oo3 models are shown in figures 6.10, 6.11. The $PFD(t)$ plots for the PM plans that minimize the $\overline{PFD}$ or $PFD_{\max}$ are shown in comparison to the $PFD(t)$ for the initial PM plan. The

initial PM plan is periodic with equal periods and simultaneously executed PM. The $\overline{PFD}$ and $PFD_{\max}$ are shown for the PM plans, which were determined by optimization.

PM type A with incomplete coverage

Now, the models that feature the PM type A with an incomplete coverage of 80% are treated. The minimization of $\overline{PFD}$ and $PFD_{\max}$ is treated in a similar way as above. In figures 6.12, 6.13 the results of the 1oo1 or 3oo3 model are shown.

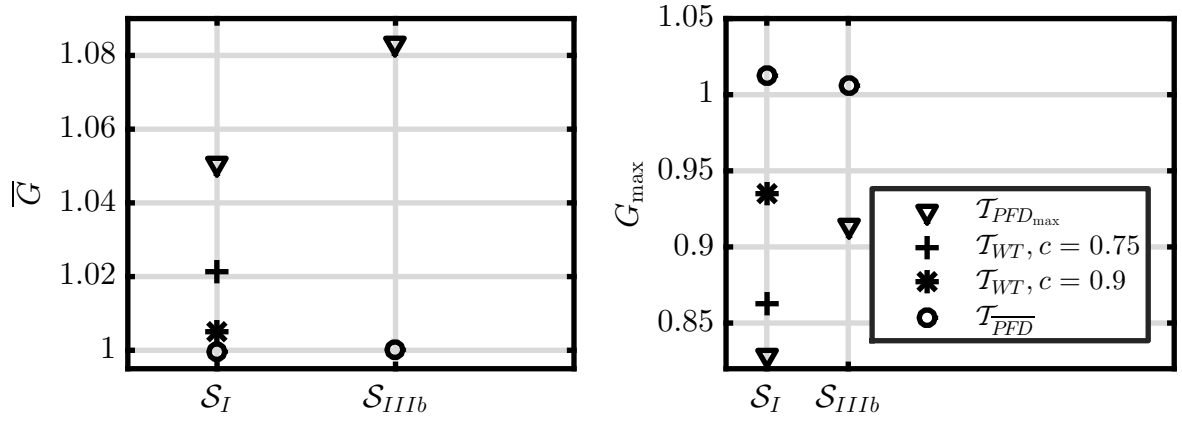

Figure 6.12: Optimization results of 1oo1 model with incomplete coverage

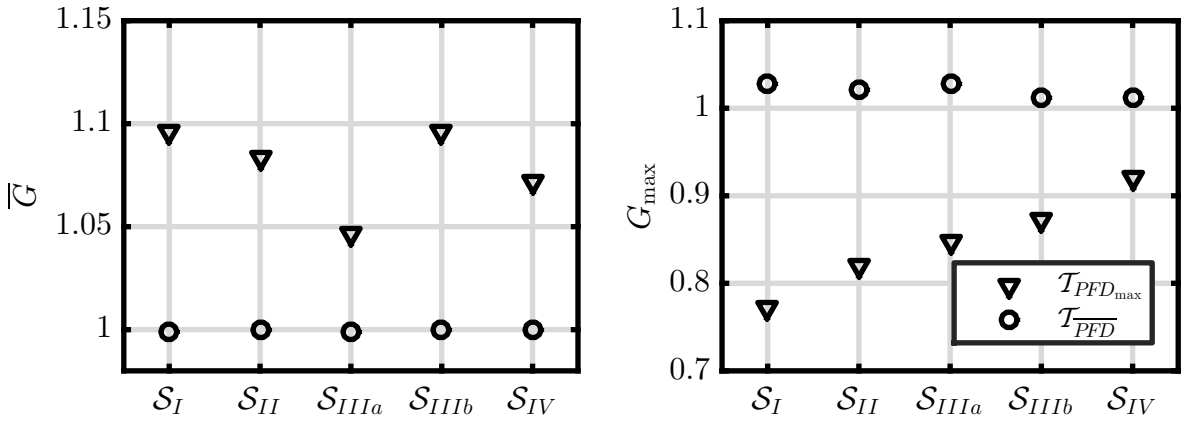

Figure 6.13: Optimization results of 3oo3 model with incomplete coverage

The results of the minimization of $\overline{PFD}$ are very similar to the results of the models with complete coverage of PM, which were discussed above. Hence, the derived findings are equivalent to those that were given above.

The results of the minimization of $PFD_{\max}$ differ from those of the models with complete coverage of PM. The differences are described below. Each explored PM strategy with less restrictions on the respective PM plans provided a significant decrease in $PFD_{\max}$. It is clearly noticeable for the PM strategies IV, IIIb, IIIa, II, and I, see figure 6.13. However, for some PM strategies a disproportionately large increase in $\overline{PFD}$ was caused through the minimization of $PFD_{\max}$. This is the case for the PM strategies IV and

IIIb. Furthermore, the $\overline{PFD}$ is overall slightly greater increased through the minimization of $PFD_{\max}$, in comparison to the results of the models with complete coverage of PM, see figure 6.9.

The discussed results of the minimization of $PFD_{\max}$ are explained below. The disproportionately large increase in $\overline{PFD}$ through the minimization of $PFD_{\max}$ is treated first. This is explained by the times of the PM A, which are not varied by the optimization for the given PM strategies IV and IIIb. The variation of the times of PM A enables to achieve a greater decrease in $PFD_{\max}$ for a less increase in $\overline{PFD}$. Finally, the overall greater increase in $\overline{PFD}$ through the minimization of $PFD_{\max}$ is explained by the incomplete coverage of the PM type A. Therefore, the PM plans require greater changes (i.e. a greater shift to the right on the time axis) to minimize the $PFD_{\max}$, in comparison to the models with complete coverage of PM.

The $PFD(t)$ plots of the 3oo3 model with an incomplete coverage of PM are shown in figure 6.14.

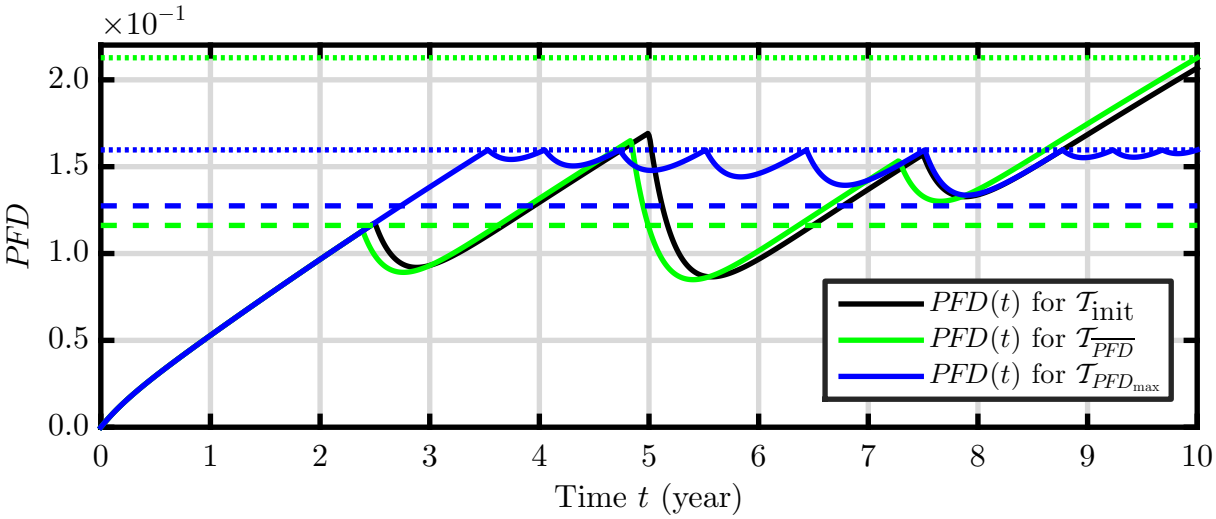

Figure 6.14: $PFD(t)$ for optimized PM plans of 3oo3 model with incomplete coverage

6.5.3 Models with redundancy

PM type A with complete coverage

The optimization results of models with redundancy, with the 1oo3 or 2oo3 element structure, are presented and discussed below. The treated models feature a complete coverage of the PM type A. The minimization of $\overline{PFD}$ or $PFD_{\max}$ is treated in a similar way as described above for the models without redundancy. In figure 6.15, the results of the 1oo3 model are shown. The results of the 2oo3 model are shown in figure 6.16.

The results of the minimization of $\overline{PFD}$ are discussed first. The greatest decrease in $\overline{PFD}$ equals approx. 20% or 5% for the 1oo3 or 2oo3 models, as shown in figures 6.15 and

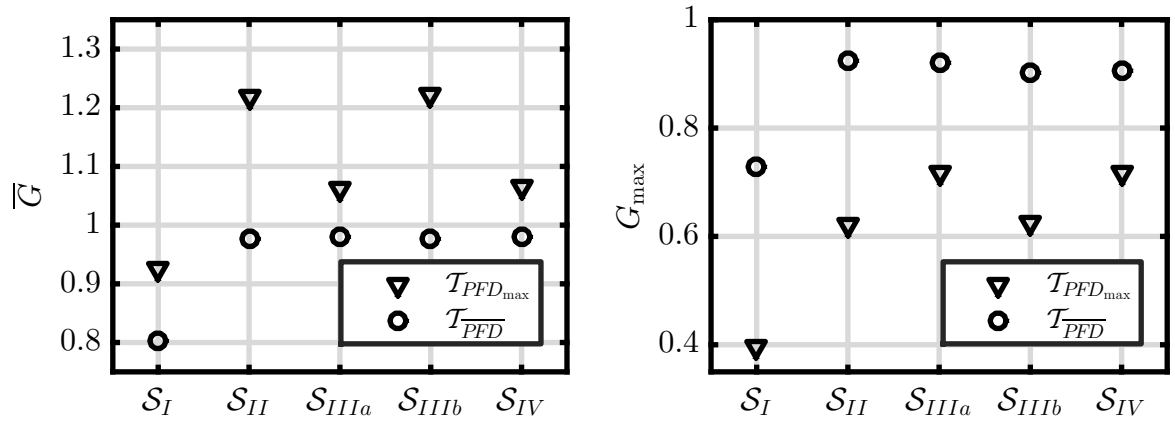

Figure 6.15: Optimization results of 1oo3 model with complete coverage

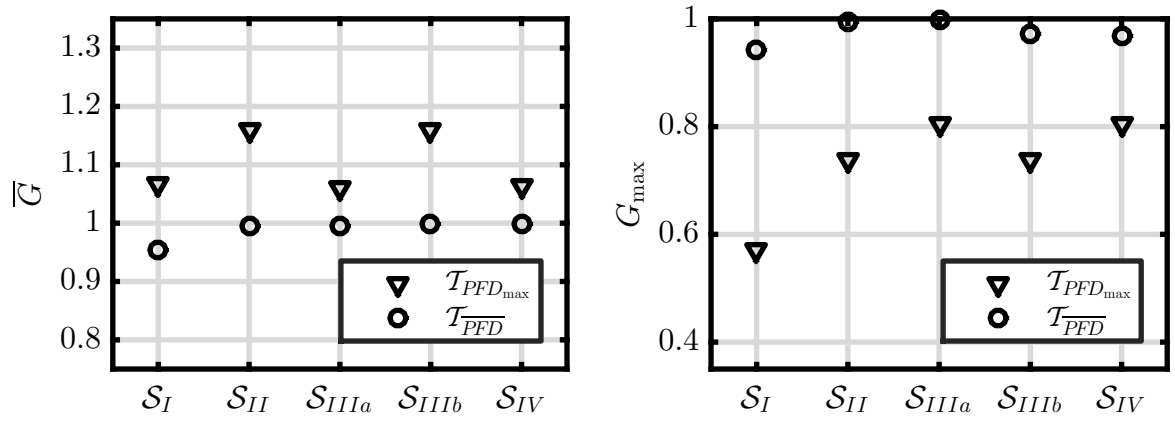

Figure 6.16: Optimization results of 2oo3 model with complete coverage

6.16. The $PFD_{\max}$ is decreased by approx. 27% or 7% through the minimization of $\overline{PFD}$. The detailed analysis of the figures 6.15 and 6.16 identifies that, the decrease in $\overline{PFD}$ was mainly achieved via optimization for the explored PM strategy I.

The discussed results are explained below. For the 1oo3 model, the decrease in $\overline{PFD}$ is significant because the PM type A of each element is also a PM type A of the entire 1oo3 model, even with a complete coverage. Hence, a PM plan with elementwise PM type A provides a greater total number of PM that are applied to the model, in comparison to a PM plan with simultaneous PM. For the 2oo3 model the achieved decrease in $\overline{PFD}$ is significantly less compared to the 1oo3 model. This is explained by the elementwise PM type A, which are only PM with incomplete coverage of the entire 2oo3 model.

Now, the results of the minimization of $PFD_{\max}$ are discussed. The greatest decrease in $PFD_{\max}$ equals approx. 60% or 40%, see figures 6.15 and 6.16. It has to be noted that, the achieved decrease in $PFD_{\max}$ is significantly greater than for models without redundancy. Through the minimization of $PFD_{\max}$, the $\overline{PFD}$ is decreased by approx. 5% or increased by approx. 5%. The detailed analysis of figures 6.15, 6.16 in regard to the explored PM strategies identifies that, the decrease in $PFD_{\max}$ occurs in three steps, as for the models without redundancy and with complete coverage of PM, see subsection

6.5.2.

The discussed results of the minimization of $PFD_{\max}$ are explained below. The evaluated PM strategies provide similar results as those of the models without redundancy and with complete coverage of PM, see subsection 6.5.2. Hence, the derived findings are equivalent to those given above. The significantly greater achieved decrease in $PFD_{\max}$ is explained by the increasing gradient of $PFD(t)$ of the models with redundancy. The increasing gradient leads to high peaks of $PFD(t)$ and a greater initial $PFD_{\max}$ that enables a greater decrease.

The $PFD(t)$ plots of the 1oo3 or 2oo3 model with complete coverage of PM are shown in figures 6.17, 6.18.

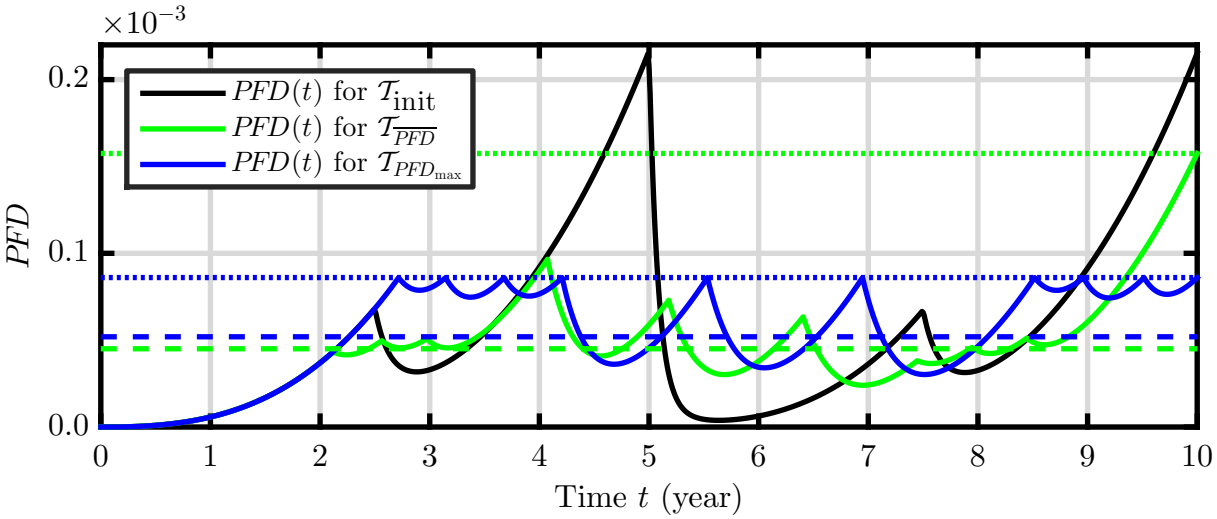

Figure 6.17: $PFD(t)$ for optimized PM plans of 1oo3 model with complete coverage

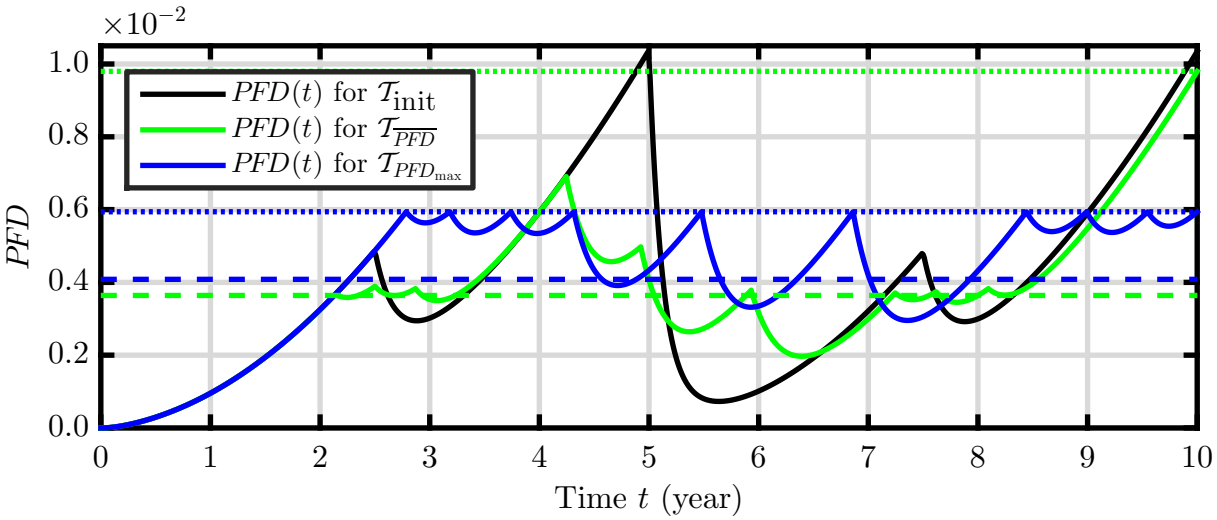

Figure 6.18: $PFD(t)$ for optimized PM plans of 2oo3 model with complete coverage

PM type A with incomplete coverage

The models with redundancy and a PM type A with an incomplete coverage of 80% are treated below. The minimization of $\overline{PFD}$ and $PFD_{\max}$ is treated in a similar way as above. In figure 6.19, the results of the 1oo3 model are shown. The results of the 2oo3 model are shown in figure 6.20.

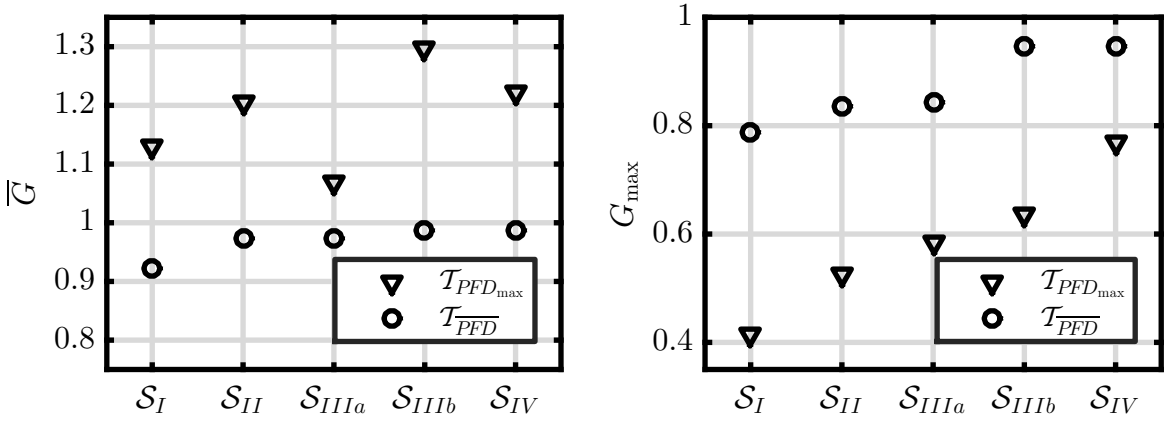

Figure 6.19: Optimization results of 1oo3 model with incomplete coverage

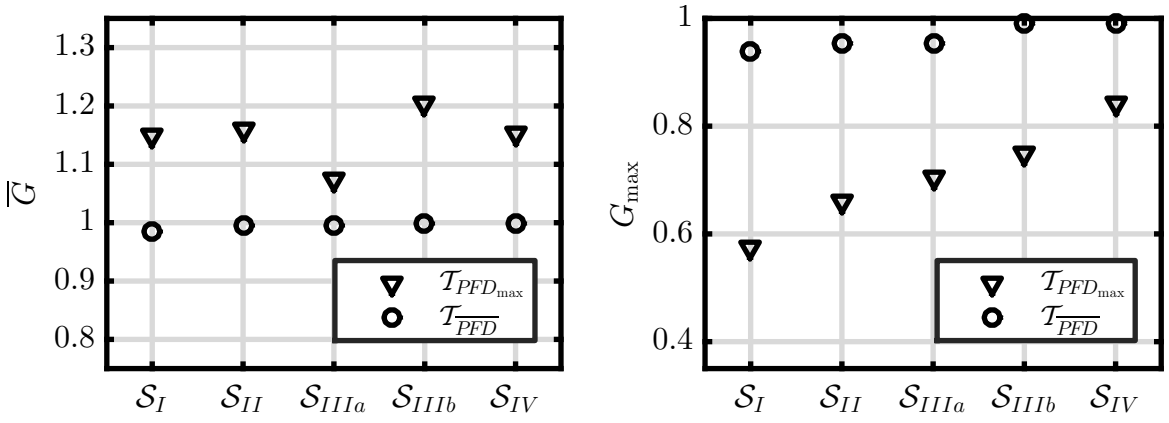

Figure 6.20: Optimization results of 2oo3 model with incomplete coverage

The results of the minimization of $\overline{PFD}$ are discussed first. The greatest decrease in $\overline{PFD}$ equals approx. 8% or 3% for the 1oo3 or 2oo3 models, as shown in figures 6.19 and 6.20. Compared to the models with redundancy and complete coverage of PM, which were treated above, the achieved decrease in $\overline{PFD}$ is significantly less. The $PFD_{\max}$ is significantly decreased by approx. 20% or 8% through the minimization of $\overline{PFD}$.

The discussed results are explained below. The occurred less decrease in $\overline{PFD}$ is explained by the less coverage of PM. The dn-failures that are caused by the incomplete coverage can not be revealed by PM. These failures significantly contribute to the total $\overline{PFD}$ and this contribution can not be influenced by the PM. Hence, the decrease that can be achieved is less.

Now, the results of the minimization of $PFD_{\max}$ are discussed. The greatest decrease in $PFD_{\max}$ equals approx. 60% or 40% for the 1oo3 or 2oo3 models, as shown in figures 6.19 and 6.20. The results are comparable to those of models with redundancy and complete coverage of PM, which were discussed above. It has to be noted that, through the minimization of $PFD_{\max}$ the $\overline{PFD}$ is increased significantly greater than for models with redundancy and complete coverage of PM.

The discussed results of the minimization of $PFD_{\max}$ are explained below. The mentioned greater increase in $\overline{PFD}$ through the minimization of $PFD_{\max}$ is explained by the incomplete coverage of PM type A. Therefore, the PM plans that minimize the $PFD_{\max}$ require a greater shift to the right on the time axis and this causes a greater increase in $\overline{PFD}$. Moreover, an observation, that also occurred for models with incomplete test coverage and without redundancy, has to be mentioned here. It was described in subsection 6.5.2. For the PM strategies IV and IIIb, a disproportionately large increase in $\overline{PFD}$ is caused through the minimization of $PFD_{\max}$. This observation was explained above.

The $PFD(t)$ plots of the 1oo3 and 2oo3 models with incomplete coverage of PM are shown in figures 6.21, 6.22.

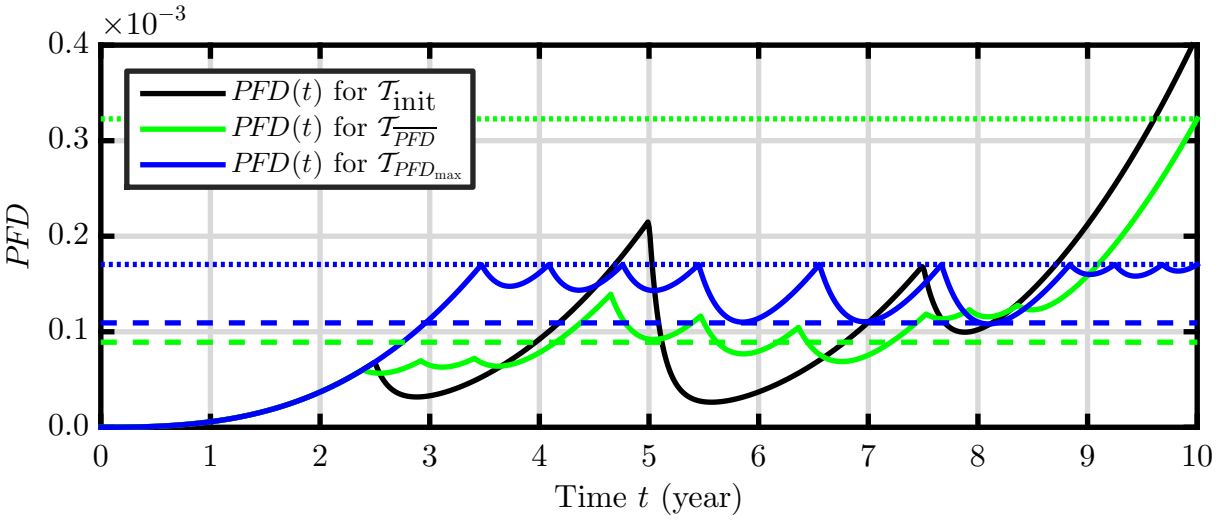

Figure 6.21: $PFD(t)$ for optimized PM plans of 1oo3 model with incomplete coverage

6.5.4 Models with redundancy and common-cause failures

1oo3 element structure

The impact of the cc-failures on the optimization results that were treated above is analyzed. The minimization of $\overline{PFD}$ or $PFD_{\max}$ was evaluated for a gradually increasing fraction of the cc-failures β. The evaluated values of β were equal for all failure modes and given by 0, 0.01, 0.05, or 0.1. These values were denoted in %, i.e. 0%, 1%, etc. The PM strategy I was explored via optimization. Further PM strategies were not explored,

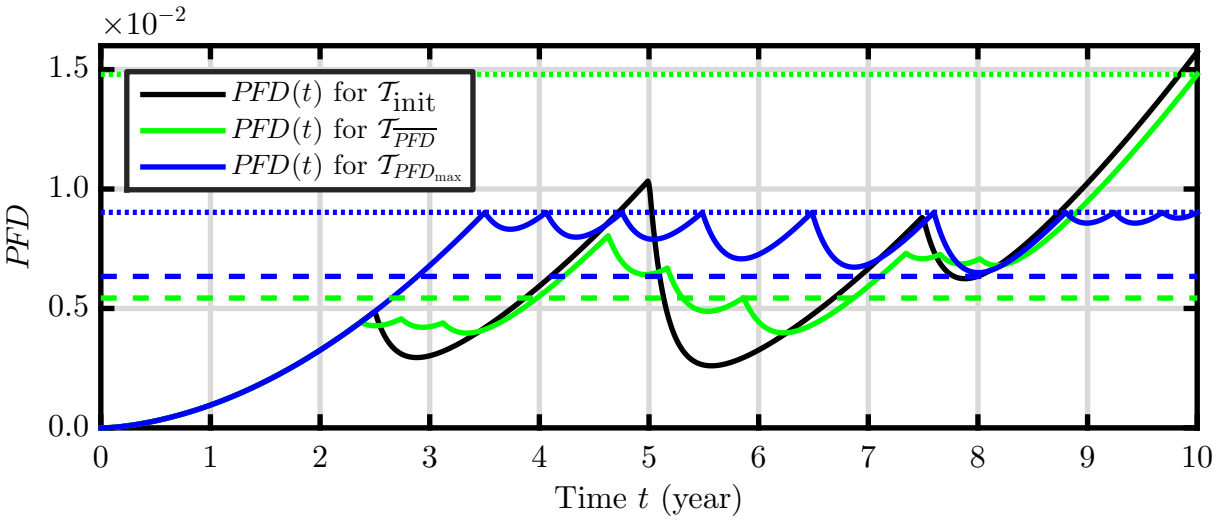

Figure 6.22: $PFD(t)$ for optimized PM plans of 2oo3 model with incomplete coverage

in contrast to the results of models without cc-failures, which were presented above. In figures 6.23, 6.24, the results of the 1oo3 model are given for a complete or an incomplete coverage of PM.

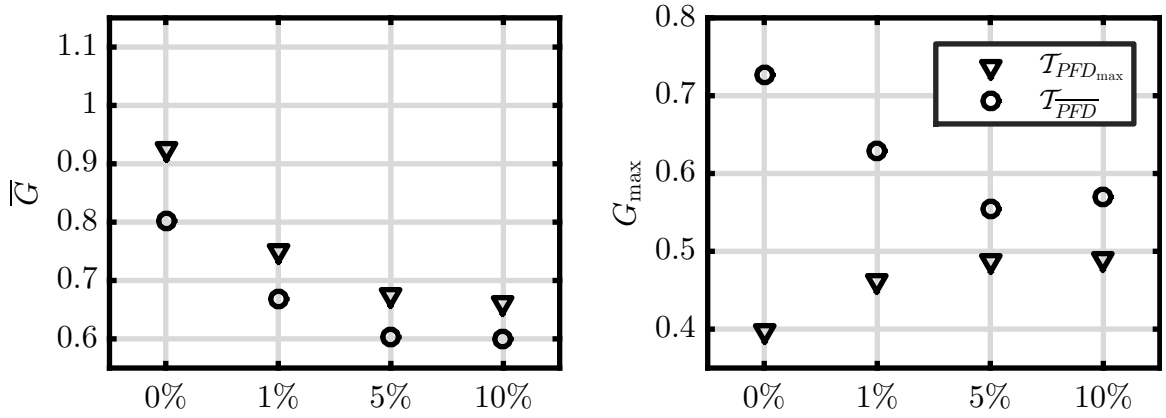

Figure 6.23: Optimization results of 1oo3 model, complete coverage and cc-failures

The results of the minimization of $\overline{PFD}$ are discussed first. For an increased fraction of cc-failures, a greater decrease in $\overline{PFD}$ is achieved. Additionally, a greater decrease in $PFD_{\max}$ is achieved for an increased fraction of cc-failures through the minimization of $\overline{PFD}$.

The discussed results are explained below. The elementwise PM of 1oo3 model effectively reveal the cc-failures. Hence, if the fraction of cc-failures is increased, the achieved decrease in $\overline{PFD}$ will be greater.

Now, the results of the minimization of $PFD_{\max}$ are discussed. For an increased fraction of cc-failures, a less decrease in $PFD_{\max}$ is achieved. Additionally, a greater decrease in $\overline{PFD}$ is achieved for an increased fraction of cc-failures through the minimization of $PFD_{\max}$.

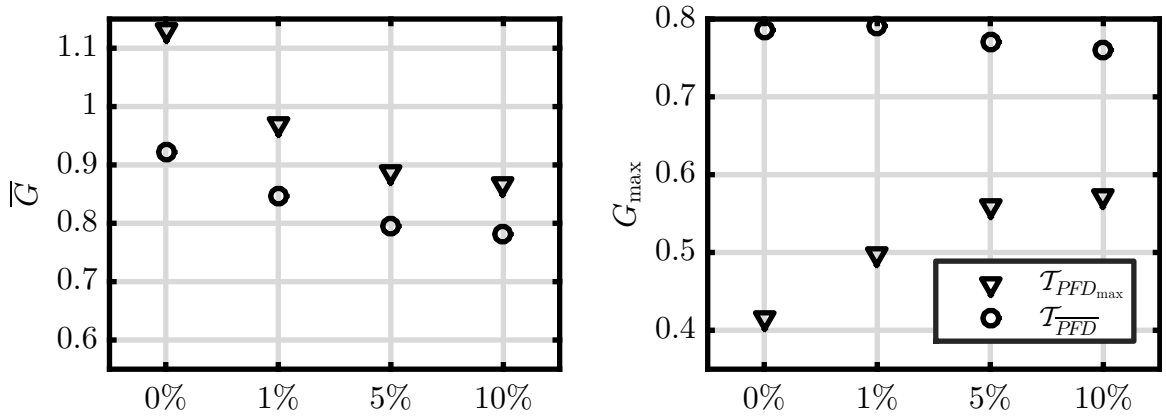

Figure 6.24: Optimization results of 1oo3 model, incomplete coverage and cc-failures

The discussed results of the minimization of $PFD_{\max}$ are explained below. An increased fraction of cc-failures results in a less decreasing gradient of $PFD(t)$, since the redundancy of the model is weakened. Its behavior gets similar to a model without redundancy, where the initial $PFD_{\max}$ is less than that of a model with redundancy. The reduced initial $PFD_{\max}$ results in the decreased ability of the model to reduce $PFD_{\max}$.

2oo3 element structure

In figures 6.25, 6.26, the impact of the cc-failures on the optimization results of the 2oo3 model is illustrated for a complete and an incomplete coverage of PM.

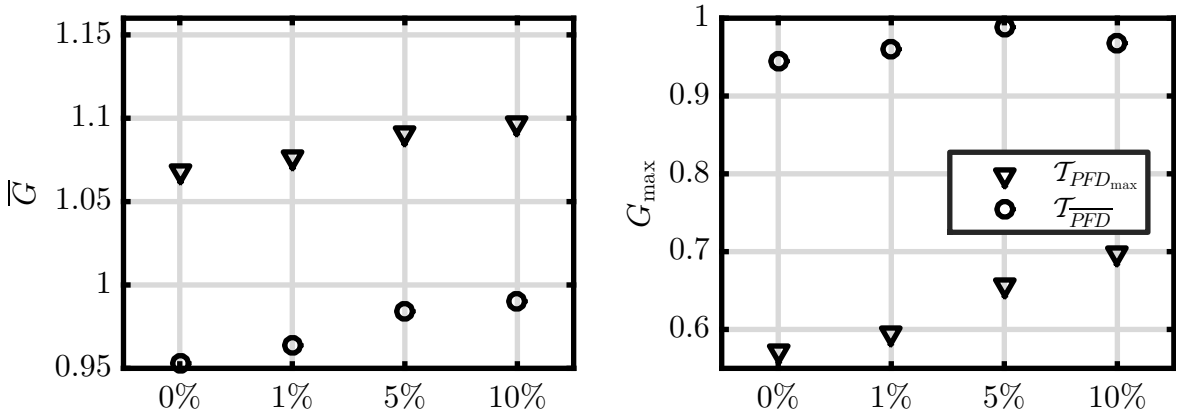

Figure 6.25: Optimization results of 2oo3 model, complete coverage and cc-failures

The results of the minimization of $\overline{PFD}$ are discussed first. For an increased fraction of cc-failures, a less decrease in $\overline{PFD}$ is achieved. Additionally, a less decrease in $PFD_{\max}$ is achieved for an increased fraction of cc-failures through the minimization of $\overline{PFD}$.

The discussed results are explained below. In contrast to the 1oo3 model, the element-wise PM do not effectively reveal the cc-failures. That is because at least two elements are required to provide the safety function. Hence, if the fraction of cc-failures is increased, the achieved decrease in $\overline{PFD}$ will be less.

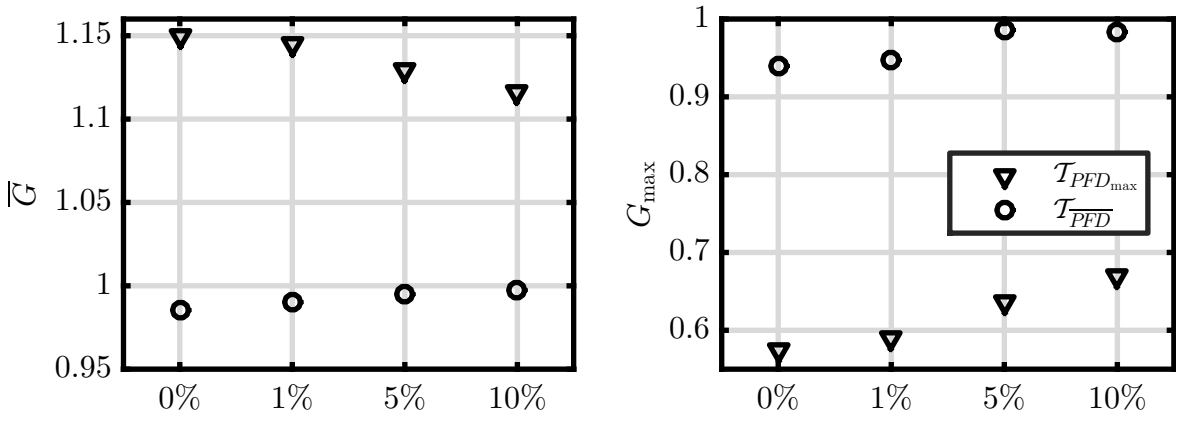

Figure 6.26: Optimization results of 2oo3 model, incomplete coverage and cc-failures

Now, the results of the minimization of $PFD_{\max}$ are discussed. For an increased fraction of cc-failures, a less decrease in $PFD_{\max}$ is achieved. These results are comparable to those of the 1oo3 model with cc-failures, which were discussed above. Additionally, no clear tendency was observed for the changes in $\overline{PFD}$ through the minimization of $PFD_{\max}$.

The discussed results of the minimization of $PFD_{\max}$ are explained below. The findings on the reduced decrease in $PFD_{\max}$ are equivalent to those of the 1oo3 model with cc-failures, which were given above.

6.6 General conclusions

Preliminaries

As demonstrated in section 6.5, an effective framework is provided to determine a PM plan via optimization, for the objective to minimize the $\overline{PFD}$, $PFD_{\max}$, or weighted trade-off between the $\overline{PFD}$ and $PFD_{\max}$. This framework has been applied to selected types of SRS models and the results were discussed in section 6.5. The general conclusions that were derived from these results are presented in this section. The practically relevant types of SRSs are treated. These SRSs have a conventional PM plan that is periodic with equal periods and simultaneous for all elements. Particularly, a set of rules is given to decide for a given SRS if the $\overline{PFD}$ or $PFD_{\max}$ can be significantly decreased via optimization of the PM plan. These rules are based on the characteristics of an SRS, such as the degree of redundancy, coverage of the PM, fraction of cc-failures, etc. Furthermore, the degrees of freedom of a PM plan are specified, which have to be modified to achieve the desired decrease. These degrees of freedom comprise elementwise PM of individual elements and arbitrarily variable individual periods, which are not restricted to be equal, of a PM. The provided rules enable to decide if the introduced framework should be applied to a given SRS or not. Each of the following subsections treats an objective that will be minimized.

PM plans to minimize $\overline{PFD}$

The examined SRSs are classified into the SRSs without redundancy or with redundancy, in order to decide if the $\overline{PFD}$ can be decreased. For an SRS without redundancy the $\overline{PFD}$ can not be significantly decreased. In contrast, for an SRS with redundancy the $\overline{PFD}$ can be significantly decreased and even the $PFD_{\max}$ will be simultaneously decreased. It was shown that, the $\overline{PFD}$ is decreased by up to 20% for an SRS with the 1oo3 element structure and complete coverage of the PM type A. The desired decrease is achieved by the following modifications of the PM plan: elementwise PM type A and B and variable individual periods of the PM type A and B. It has to be noted that, if these modifications are not applicable to a given SRS, most likely no significant decrease in the $\overline{PFD}$ will be achieved. The achieved decrease in the $\overline{PFD}$ will be declined by the decreased degree of redundancy and coverage of the PM type A. The increased fraction of cc-failures might enhance or decline the decrease in the $\overline{PFD}$, depending on the degree of redundancy. For a higher degree of redundancy, e.g. 1oo3, the decrease in the $\overline{PFD}$ will be significantly enhanced by the increased fraction of cc-failures. In contrast, the decrease in the $\overline{PFD}$ will be declined by the increased fraction of cc-failures for a lower degree of redundancy, e.g. 2oo3.

PM plans to minimize $PFD_{\max}$

The $PFD_{\max}$ can be significantly decreased for a given SRS independent of its characteristics. However, the $\overline{PFD}$ will be most likely simultaneously increased. It was shown that, the $PFD_{\max}$ is decreased by up to 60% for an SRS with the 1oo3 element structure and complete coverage of the PM type A. The desired decrease is achieved by a set of modifications of the PM plan, where each modification contributes to the decrease, as outlined below. The examined SRSs are classified into the SRSs with the complete or incomplete coverage of the PM type A. For a complete coverage, the following sets of modifications provide an ascending decrease in $PFD_{\max}$:

- variable individual periods of the simultaneous PM type B,
- variable individual periods of the elementwise PM type B,
- variable individual periods of the elementwise PM type A and B.

The greatest decrease in $PFD_{\max}$ will be achieved via the latter modifications, but the less decrease that will be achieved via the two former will be significant as well. For an SRS with an incomplete coverage, the sets of modifications are the following, in ascending order:

- variable individual periods of the simultaneous PM type A and B,

- variable individual periods of PM type A and B, where PM type A is simultaneous, and PM type B is elementwise,
- variable individual periods of the elementwise PM type A and B.

As above, the greatest decrease will be achieved via the latter modifications and each set will provide a significant decrease. It has to be noted that, further modifications, which are related only to the PM type B, will also provide a significant decrease in $PFD_{\max}$, but for a disproportionately large increase in $\overline{PFD}$. Therefore, these modifications are not recommended for the SRSs with the incomplete coverage of the PM type A. In general, the decrease in the $PFD_{\max}$ will be declined by the decreased degree of redundancy and increased fraction of cc-failures.

PM plans to minimize the trade-off between $\overline{PFD}$ and $PFD_{\max}$

The objectives to minimize the $\overline{PFD}$ or $PFD_{\max}$ are usually conflictive, e.g. the minimization of the $PFD_{\max}$ leads to a significant increase in the $\overline{PFD}$ and vice versa. Hence, the objective to minimize the weighted trade-off between the $\overline{PFD}$ and $PFD_{\max}$ is effective to simultaneously consider both objectives. The objective function of the trade-off has a weighting factor that quantifies the priorities of the two objectives.

In particular, for an SRS the $PFD_{\max}$ can be significantly decreased for a slight simultaneous increase in $\overline{PFD}$. This ability is independent of the characteristics of the SRS. The desired decrease is achieved by the following modifications of the PM plan: elementwise PM type A and B and variable individual periods of the PM type A and B. This set of modification provides the degrees of freedom to achieve most favorable trade-off between the $\overline{PFD}$ and $PFD_{\max}$. If some of the mentioned modifications are not available, the achieved trade-off will be significantly worse.

Chapter 7

Summaries

7.1 Summary in English

Probabilistic modeling

The probabilistic models of the Safety-related Systems (SRS) were introduced in this thesis. An SRS is build up of multiple possibly dependent elements, which are subject to multiple maintenance actions and failure modes. The failure modes comprise the safe, dangerous detected, dangerous undetected, and dangerous non-revealable failures. The introduced models focus on the detailed modeling of the preventive maintenance (PM). The PM intends to reveal the undetected failures of an SRS and provides repair if necessary. Up to two different types of PM for each element of the SRS were modeled, where each type has a different coverage to reveal the undetected failures. The PM is scheduled via a given PM plan that specifies the times when each particular type of PM of each element of an SRS will be executed. A framework was provided to first model individual elements of an SRS and afterwards automatically compose the respective model of the entire SRS. A new class of probabilistic models, the Stochastic and Deterministic Timed Automata (SDTA) were defined to enable the elementwise modeling and composition. The SDTA are strongly connected to the concepts of the SRSs and enable straightforward modeling of an SRS under consideration of the dependencies of individual elements. Moreover, an insight is provided into further automata-based types of probabilistic models, which feature more or less restrictions on the timing of events. The probabilistic figures of merit of the modeled SRS were efficiently computed via the Multi-phase Continuous-time Markov Chains (MP-CMC). For this purpose the SDTAs were transformed into the MP-CMCs by means of a transformation that was introduced in this thesis. The computed figures of merit were the instantaneous, average, and maximum probability of dangerous failure on demand (PFD), denoted by $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$.

Model analysis and validation

The introduced framework to model the SRSs was applied to multiple selected SRSs with practically relevant element structures and characteristics. These models were validated via selected established models from the literature. It was shown that, the introduced models provide plausible results and exhibit various exclusive features in comparison to the literature models. These exclusive features, such as the detailed modeling of the PM, were demonstrated and discussed. A procedure that is based on sensitivity analysis was introduced and applied to analyze the parameter variations of the models. The analysis has shown that, the parameter variations related to the PM have a significant impact on the $PFD(t)$, $\overline{PFD}$, and $PFD_{\max}$. Particularly, the parameter variations that are related to the exclusive features of the introduced models were analyzed. It was concluded that, additional degrees of freedom are available for the PM plans of the SRSs, such as elementwise PM of individual elements and arbitrarily variable individual periods, which are not restricted to be equal. These degrees of freedom can be used to decrease the $\overline{PFD}$ or $PFD_{\max}$ or both in order to make an SRS more effective.

Optimization of PM plans

The choice of a PM plan within the available degrees of freedom for a given SRS was formulated as an optimization problem. Different optimization objectives that are minimized were introduced, such as the $\overline{PFD}$ or $PFD_{\max}$ or the weighted trade-off between the $\overline{PFD}$ and $PFD_{\max}$. The objective functions, which quantify the objectives, were given via the respective probabilistic models. The Nelder-Mead method was applied to compute the treated optimization problems. For selected practically relevant types of SRS, the respective optimization problems were computed to demonstrate the effectiveness of the Nelder-Mead method. It has been shown that, the determined PM plans provide most likely a significant decrease in the $\overline{PFD}$ or $PFD_{\max}$ or a favorable trade-off between the two former. A set of rules was given to decide based on the characteristics of a given SRS if the $\overline{PFD}$ or $PFD_{\max}$ can be significantly decreased via optimization. These rules address practically relevant types of SRSs. The required degrees of freedom of PM to decrease the desired objective were identified and evaluated. The presented rules aim to support the decision if the optimization of a PM plan should be applied to a given SRS or not.

7.2 Outlook

In this thesis, it has been shown that the probabilistic model of an SRS can be determined via the SDTA. A model is provided that is based on automata and reflects the discrete states and events, which are related to failure, repair, and restoration of the SRS. The

events are classified to be either deterministic or exponential stochastic timed. The state probabilities of the probabilistic model are efficiently calculated via the MP-CMC, which is done to determine the $PFD(t)$ and related figures of merit.

A promising research topic for future work is to extend the introduced probabilistic model to arbitrarily timed events. This will lead to the Stochastic Timed Automaton (STA), which was defined in [CL08]. The STA provides a probabilistic model, where the events are timed by arbitrary CDFs and not restricted to be either deterministic or exponential stochastic timed. This enables to model systems with failure and repair processes that are not restricted to be deterministic or exponential. However, the numerical calculation of the probabilistic figures of merit is expected to be more complex and less efficient.

7.3 Extended summary in German – Kurzfassung in deutscher Sprache

Motivation und wichtige Beiträge der Dissertation

In der Industrie werden zahlreiche technische Einrichtungen und Geräte, z.B. Maschinen, Apparate oder Anlagen, betrieben. Ausfälle und Störungen dieser technischen Einrichtungen können eine Gefährdung von Mensch, Umwelt, Produktionsmitteln und Gütern verursachen. Zum Schutz vor diesen Gefährdungen muss eine technische Einrichtung bei einem Ausfall aus einem gefährlichen in einen sicheren Zustand überführt werden. Diese wichtige Aufgabe erfüllen die sogenannten *sicherheitsbezogenen Systeme*. Durch den Einsatz dieser Systeme wird das Risiko von den beschriebenen Gefährdungen auf ein tolerierbares Maß herabgesetzt. Auf diese Weise können diese technischen Einrichtungen unter Beherrschung der von ihnen ausgehenden Gefährdungen und dem damit verbundenen Risiko betrieben werden. Die sicherheitsbezogenen Systeme sind in vielen verschiedenen Industriezweigen im Einsatz, z.B. in der Prozessindustrie, Automobilindustrie, etc. und schließen eine Vielzahl von unterschiedlichen Systemen ein.

Aufgrund der hohen Bedeutung der sicherheitsbezogenen Systeme werden durch internationale Normen besondere Forderungen an diese gestellt. Unter anderem in der Norm [IEC11e] werden diese Forderungen beschrieben. Damit soll sichergestellt werden, dass eine ausreichende Risikoreduktion für vorhandene Gefährdungen gewährleistet wird. Die vorgegebenen Forderungen an ein sicherheitsbezogenes System richten sich nach dem Risiko der Gefährdung, die von der zu überwachenden technischen Einrichtung ausgeht. Dabei werden für technische Einrichtungen mit kontinuierlicher, hoher oder niedriger Anforderungsart an ein sicherheitsbezogenes System unterschiedliche Forderungen gestellt. In dieser Dissertation wird die niedrige Anforderungsart betrachtet, das bedeutet dass ein sicherheitsbezogenes System im Mittel nicht häufiger als einmal im Jahr von der über-

wachten technischen Einrichtung angefordert wird. Eine wichtige Forderung aus der Norm an solche sicherheitsbezogenen Systeme gibt risikoabhängige Grenzwerte für die mittlere *Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung* (PFD, engl. Probability of Dangerous Failure on Demand) vor. Ein rechnerischer Nachweis wird gefordert, dass die vorgegebenen Grenzwerte für die mittlere PFD nicht überschritten werden. Die PFD ist eine probabilistische Kenngröße, welche mittels geeigneter probabilistischer Modelle berechnet wird.

Das Verhalten von sicherheitsbezogenen Systemen unter Berücksichtigung von Ausfall und Wiederherstellung wird durch probabilistische Modelle modelliert. Mehrere Arten von Ausfällen werden unterschieden: ungefährliche, gefahrbringende, erkannte sowie unerkannte. Insbesondere die *gefahrbringenden unerkannten Ausfälle* beeinträchtigen die PFD erheblich. Als Gegenmaßnahme wird die *präventive Instandhaltung* eingesetzt. Damit sind die Maßnahmen gemeint, welche zur Aufdeckung von gefahrbringenden unerkannten Ausfällen und ggf. Wiederherstellung durchgeführt werden. Die präventive Instandhaltung von sicherheitsbezogenen Systemen ist von hoher Bedeutung, da sie deren Funktionsfähigkeit und damit einen ausreichenden Schutz vor Gefährdungen gewährleistet. Diese Dissertation legt ein besonderes Augenmerk auf die Modellierung der präventiven Instandhaltung sicherheitsbezogener Systeme. Es werden dazu geeignete probabilistische Modelle entwickelt. Diese Modelle ermöglichen insbesondere eine präzisere und detailliertere Modellierung der präventiven Instandhaltung als die in der Literatur verwendeten Modelle. Die damit gewonnenen Freiheitsgrade werden analysiert und mittels Optimierung dazu verwendet die PFD zu verbessern. Das Risiko von den jeweiligen Gefährdungen kann damit deutlich herabgesetzt werden und der Schutz verbessert werden.

Die wichtigen Beiträge dieser Dissertation werden in folgende Kategorien unterteilt:

- Probabilistische Modellierung von sicherheitsbezogenen Systemen zur Berechnung der probabilistischen Kenngrößen mittlere, instantane und maximale PFD unter detaillierter Berücksichtigung der präventiven Instandhaltung,

- Validierung der eingeführten probabilistischen Modelle durch Literaturmodelle und Analyse der Einflüsse präventiver Instandhaltung auf die probabilistischen Kenngrößen unter Berücksichtigung der gewonnenen, bisher vernachlässigten Freiheitsgrade,

- Optimierung der präventiven Instandhaltung durch die Formulierung geeigneter Optimierungsprobleme zur Minimierung ausgewählter probabilistischer Kenngrößen und deren Lösung unter Verwendung des Nelder-Mead-Verfahrens.

Jede Kategorie wird im Folgenden ausführlicher erläutert.

Probabilistische Modellierung

Die probabilistischen Modelle in dieser Dissertation basieren auf den zeitbewerteten Automaten mit exponentialverteilten und deterministischen Verweilzeiten sowie den zeitkontinuierlichen Mehrphasen-Markov-Ketten. Die erstgenannte Modellklasse wird in dieser Arbeit zur Modellierung der sicherheitsbezogenen Systeme eingeführt. Dabei wird ein enger Zusammenhang zu den jeweiligen Konzepten und Begrifflichkeiten hergestellt, wie beispielsweise mehrere Arten von Ausfällen sowie verschiedene relevante Instandhaltungstätigkeiten, z.B. Prüfungen, Instandsetzung, Wiederherstellung, usw. Dieses Modell entspricht der Denkweise eines Ingenieurs in einem höheren Maße als Markov-Ketten, die dafür eine effiziente Berechnung der probabilistischen Kenngrößen ermöglichen. Darüber hinaus lässt sich mittels der eingeführten zeitbewerteten Automaten die Verbindung zu weiteren Modellklassen herstellen, welche entweder mehr oder weniger Einschränkungen an die Verweilzeiten enthalten.

Insgesamt wird in dieser Dissertation eine ganzheitliche Methode zur probabilistischen Modellierung präsentiert, welche die getrennte Modellierung einzelner Teile eines Systems ermöglicht, die dann automatisch zu dem Gesamtmodell zusammengesetzt werden können. Dabei lassen sich auch Abhängigkeiten der einzelnen Teile modellieren. Dies wird am Beispiel eines gemeinsamen Reparaturteams für mehrere Teilsysteme verdeutlicht. Das gewonnene Modell in Form eines zeitbewerteten Automaten lässt sich mit einer definierten Transformation in die entsprechende Mehrphasen Markov-Kette überführen. Damit können die probabilistischen Kenngrößen instantane, mittlere und maximale PFD effizient berechnet werden.

Validierung und Analyse der probabilistischen Modelle

Die eingeführten probabilistischen Modelle werden zur Modellierung von mehreren Systemen mit praxisrelevanten *M*oo*N*-Strukturen und Eigenschaften verwendet. Diese werden mittels ausgewählter etablierter Literaturmodelle validiert. Es werden die Unterschiede zu den Literaturmodellen diskutiert, insbesondere im Hinblick auf die detailliertere Modellierung der präventiven Instandhaltung. Eine Analyse der gewonnenen Freiheitsgrade auf Basis einer Sensitivitätsanalyse wird durchgeführt. Damit wird gezeigt, dass sich die gewonnenen Freiheitsgrade der präventiven Instandhaltung signifikant auf die probabilistischen Kenngrößen auswirken.

Optimierung der präventiven Instandhaltung

Auf Basis der verfügbaren Freiheitsgrade der präventiven Instandhaltung werden mehrere *Strategien präventiver Instandhaltung* definiert. Die Pläne präventiver Instandhaltung werden in Klassen mit unterschiedlichen Freiheitsgraden eingeteilt. Mit einem *Plan der*

präventiven Instandhaltung werden alle jeweiligen Maßnahmen für ein System terminiert und die resultierenden probabilistischen Kenngrößen können berechnet werden.

Die Pläne präventiver Instandhaltung werden optimiert, um eine Verbesserung der probabilistischen Kenngrößen zu erzielen. Es werden die mittlere oder maximale PFD oder alternativ eine zusammengesetzte, gewichtete Zielfunktion aus der mittleren und maximalen PFD minimiert. Die Minimierung erfolgt durch die Variation eines Plans präventiver Instandhaltung innerhalb der durch die jeweilige Strategie präventiver Instandhaltung verfügbaren Freiheitsgrade. Das Nelder-Mead-Verfahren wird zur Lösung der Optimierungsprobleme verwendet. Es handelt sich dabei um einen heuristischen Optimierungsalgorithmus aus der Kategorie der Hillclimbing- oder Downhill-Suchverfahren.

Die Optimierung wird für ausgewählte, praktisch relevante Modelle durchgeführt und die Ergebnisse analysiert. Die Performanz eines Systems, im Hinblick auf die mittlere und maximale PFD, lässt sich in den meisten Fällen signifikant verbessern. Aus den Ergebnissen werden wichtige Schlussfolgerungen mit Relevanz für die Praxis gewonnen. Durch die in dieser Dissertation bereitgestellten Regeln lässt sich abschätzen, ob die mittlere oder maximale PFD eines sicherheitsbezogenen Systems durch die Optimierung signifikant verbessert werden kann. Diese Regeln basieren auf den Merkmalen des Systems, wie z.B. Redundanz oder keine Redundanz, vollständige oder unvollständige Abdeckung der präventiven Instandhaltung, usw. Mit dieser Entscheidungshilfe kann ein Ingenieur abschätzen, ob der Einsatz der beschriebenen Optimierungsmethoden für ein System vorteilhaft sein kann.

Ausblick

Für die weitere Forschung im Bereich der probabilistischen Modellierung von sicherheitsbezogenen Systemen erscheint eine Verallgemeinerung der hier verwendeten zeitbewerteten Automaten interessant. Durch die Ausweitung auf beliebig verteilte stochastische Verweilzeiten können auch Ausfall- und Instandsetzungsprozesse mit Verweilzeiten, die nicht exponentialverteilt oder deterministisch sind, berücksichtigt werden. Damit wird jedoch die numerische Berechnung der probabilistischen Kenngrößen voraussichtlich erschwert und weniger effizient.

Appendix A

Model of SRS element with reduced number of states

The SDTA that models an SRS element is introduced below. The SDTA has been determined to have a low number of states as possible on one hand and on the other hand to provide a sufficiently precise model.

The events introduced to model an SRS were defined in chapter 2. Let the SDTA of the i-th SRS element be discussed. The CM event $cmdd_i$ and the PM events $pma2_i$, $pmb2_i$ are closely related, as outlined hereafter. All these events are STEs and indicate restoration due to a completed CM or PM after the element previously suffered from a dd-, dua-, or duab-failure. The dd-failures are immediately detected, in contrast to the dua- and duab-failures, revealed only by the respective PM activities. However, once the dua- or duab-failures are revealed, these are treated just like the dd-failures. The respective maintenance activities are immediately initiated and last for the period of time until the restoration is achieved. This is modeled by the respective events $cmdd_i$, $pma2_i$, and $pmb2_i$, which become active and occur. The states/transitions diagram to illustrate the reasoning above is given in figure A.1. The events $cmdd_i$, $pma2_i$, and $pmb2_i$ trigger the individual transitions of the state 2* to state 1, 3* to 1, and 6* to 1 respectively. Thus, the maintenance activities to achieve restoration in consequence of the dd-failures, the revealed dua-, and duab-failures are modeled individually. Due to that, the rate parameters of $cmdd_i$, $pma2_i$, and $pmb2_i$ can be individually parametrized and reflect the respective characteristics of the maintenance activities.

In practical applications, the maintenance activities to achieve restoration in consequence of the dd-failures, or the revealed dua-, duab-failures have equal characteristics. This feature is used in the following to reduce the number of states of the SDTA and reduce the complexity of the model. Therefore, the following assumption is formulated.

Assumption 7 (Restoration of dd-, dua-, and duab-failures). The maintenance activities to achieve restoration in consequence of the dd-failures, the revealed dua-, and

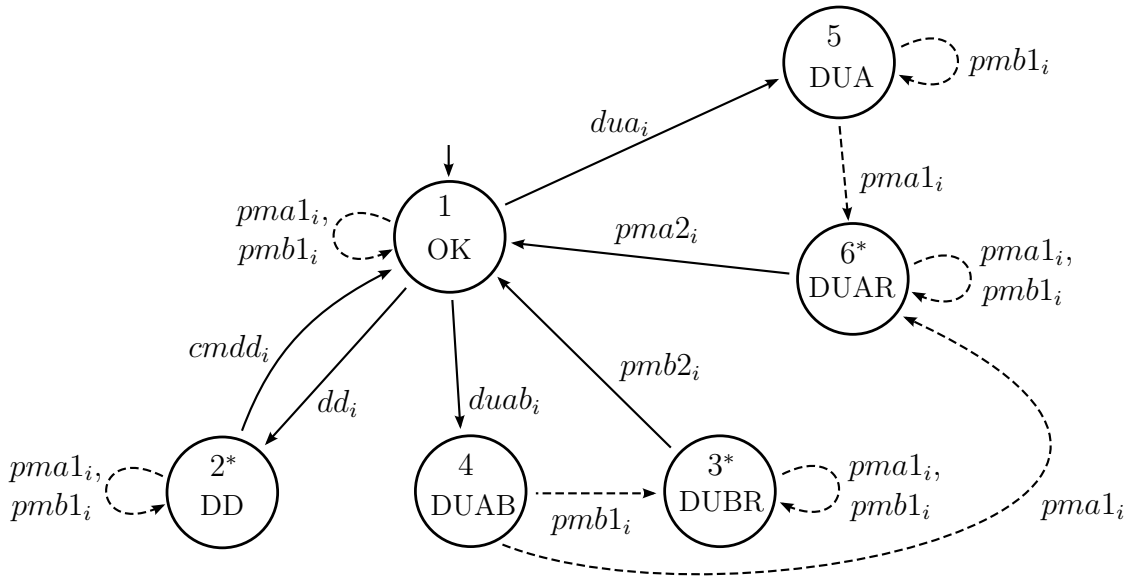

Figure A.1: States/transitions diagram of SDTA modeling an SRS element, limited to dd-, dua-, and duab-failures

duab-failures have equal characteristics. Hence, the rate parameters of $cmdd_i$, $pma2_i$, and $pmb2_i$ are equal, i.e.

$$\lambda_{cmdd_i} = \lambda_{pma2_i} = \lambda_{pmb2_i} \ .$$

Due to the explanation given above and assumption 7, the events $cmdd_i$, $pma2_i$, and $pmb2_i$ do not have to be longer differentiated. Instead, these events are combined and considered as one event that is denoted by md_i. Additionally, the states of the SDTA, where a dd-failure occurred, or a dua-, duab-failure occurred and has been revealed, are melted to one state and no longer differentiated. The states that are melted to one state are shown in figure A.1 and have the state attributes DD, DUAR, and DUBR. The resulting states/transitions diagram of the reduced number of states SDTA that models the i-th SRS element is shown in figure A.2. It is clearly evident that the number of states is reduced in comparison to figure A.1 and the mentioned states were melted to a single state with the state attribute DR.

It has to be mentioned that, due to the combined states it is not any more possible to decide whether a dd-, dua-, or duab-failure has occurred once the SDTA is in the state with the attribute DR. However, due to the reduced model complexity and sufficient precision, the reduced number of states SDTA that models an SRS element is applied in this theses. Particularly, the SDTA that is introduced in section 3.3.2 is based on the reduced number of states SDTA outlined above.

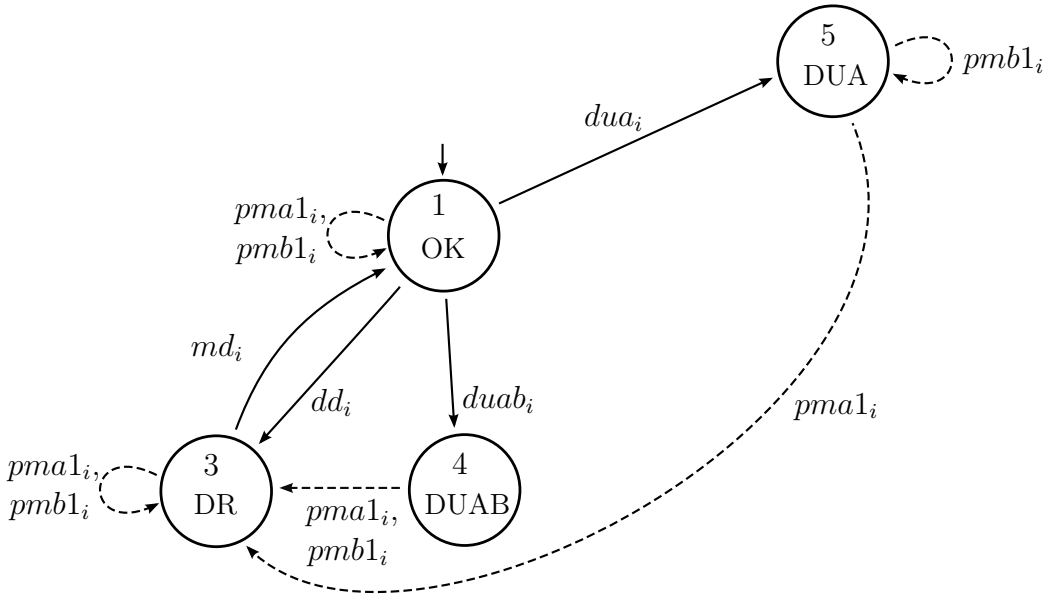

Figure A.2: States/transitions diagram of the reduced number of states SDTA modeling an SRS element

Appendix B

State classification of selected *M*oo*N* element structures

The set of the k-tuples of element safety attributes, which is denoted by $\mathcal{U}$, defines the state classification of the model in regard to the safety function of the respective SRS. The sets $\mathcal{U}_{MooN}$ of the *M*oo*N* element structures that are treated in this thesis are defined below.

B.1 1oo1 element structure

The set $\mathcal{U}_{1oo1}$ is given by

$$\mathcal{U}_{1oo1} = \{(\mathrm{U_{el}})\} \; . \tag{B.1}$$

B.2 1oo2 element structure

The set $\mathcal{U}_{1oo2}$ is given by

$$\mathcal{U}_{1oo2} = \{(\mathrm{U_{el}}, \mathrm{U_{el}}), (\mathrm{U_{el}}, \overline{\mathrm{U}}_{\mathrm{el}}), (\overline{\mathrm{U}}_{\mathrm{el}}, \mathrm{U_{el}})\} \; . \tag{B.2}$$

B.3 2oo2 element structure

The set $\mathcal{U}_{2oo2}$ is given by

$$\mathcal{U}_{2oo2} = \{(\mathrm{U_{el}}, \mathrm{U_{el}})\} \; . \tag{B.3}$$

B.4 1oo3 element structure

The set $\mathcal{U}_{1oo3}$ is given by

$$\begin{aligned}\mathcal{U}_{1oo3} = \{&(\mathrm{U_{el}}, \mathrm{U_{el}}, \mathrm{U_{el}}), (\mathrm{U_{el}}, \mathrm{U_{el}}, \overline{\mathrm{U}}_{\mathrm{el}}), (\mathrm{U_{el}}, \overline{\mathrm{U}}_{\mathrm{el}}, \mathrm{U_{el}}), (\overline{\mathrm{U}}_{\mathrm{el}}, \mathrm{U_{el}}, \mathrm{U_{el}}),\\ &(\mathrm{U_{el}}, \overline{\mathrm{U}}_{\mathrm{el}}, \overline{\mathrm{U}}_{\mathrm{el}}), (\overline{\mathrm{U}}_{\mathrm{el}}, \mathrm{U_{el}}, \overline{\mathrm{U}}_{\mathrm{el}}), (\overline{\mathrm{U}}_{\mathrm{el}}, \overline{\mathrm{U}}_{\mathrm{el}}, \mathrm{U_{el}})\} .\end{aligned} \tag{B.4}$$

B.5 2oo3 element structure

The set $\mathcal{U}_{2oo3}$ is given by

$$\mathcal{U}_{2oo3} = \{(\mathrm{U_{el}}, \mathrm{U_{el}}, \mathrm{U_{el}}), (\mathrm{U_{el}}, \mathrm{U_{el}}, \overline{\mathrm{U}}_{\mathrm{el}}), (\mathrm{U_{el}}, \overline{\mathrm{U}}_{\mathrm{el}}, \mathrm{U_{el}}), (\overline{\mathrm{U}}_{\mathrm{el}}, \mathrm{U_{el}}, \mathrm{U_{el}})\} . \tag{B.5}$$

B.6 3oo3 element structure

The set $\mathcal{U}_{3oo3}$ is given by

$$\mathcal{U}_{3oo3} = \{(\mathrm{U_{el}}, \mathrm{U_{el}}, \mathrm{U_{el}})\} . \tag{B.6}$$

Appendix C

Models of selected dependent SRS elements

C.1 Repair priorities

In practice, separate repair teams are not available for the individual SRS elements, contrary to the often used assumption. Consequently, the SRS elements are dependent. Whether an element is repaired immediately after a detected failure or only after the restoration of another element, depends on the current state of another element. In this thesis, it is assumed that *repair priorities* were defined for the case, when the repair team is required by multiple failed elements of an SRS. The repair priorities define the sequence of elements to be repaired. The modeling of repair priorities is illustrated via the example given below. The given example is based on the example 3.7. The SRS element 1*, with a higher repair priority over the element 2, is introduced in example C.1 to replace the element 1 of example 3.7.

Example C.1 (SRS consisting of elements with repair priority). Let the two SDTAs, $\mathcal{SDTA}^{1*}$ and $\mathcal{SDTA}^{2}$, be given. The states/transitions diagrams of the given SDTAs are shown in figure C.1. It has to be noted that, the respective SRS elements are dependent due to only one available repair team. The defined repair priority is in favor of the element 1*, i.e. if the elements 1* and 2 fail, the element 1* will be repaired first. That is modeled via the supplementary transition in $\mathcal{SDTA}^{1*}$ that is triggered by the event md_2, which is also relative to $\mathcal{SDTA}^{2}$. Therefore, the event md_2 is common and it appears in $\mathcal{SDTA}^{1*}$ and $\mathcal{SDTA}^{2}$, in contrast to example 3.7, where it is a private event of $\mathcal{SDTA}^{2}$. The given SDTAs are combined via the parallel composition of SDTAs to determine the $\mathcal{SDTA}^{*}$. The result is shown in figure C.2. In contrast to the figure 3.5, no transition from the state $(\hat{2}, 3)$ to the state $(\hat{2}, 1)$ is present in figure C.2. This transition is missing due to the one available repair team and the defined higher repair priority of the element 1*. The missing transition results in the repair of the element 1* until its

restoration, before the repair of the element 2 will be carried out and its restoration will be achieved.

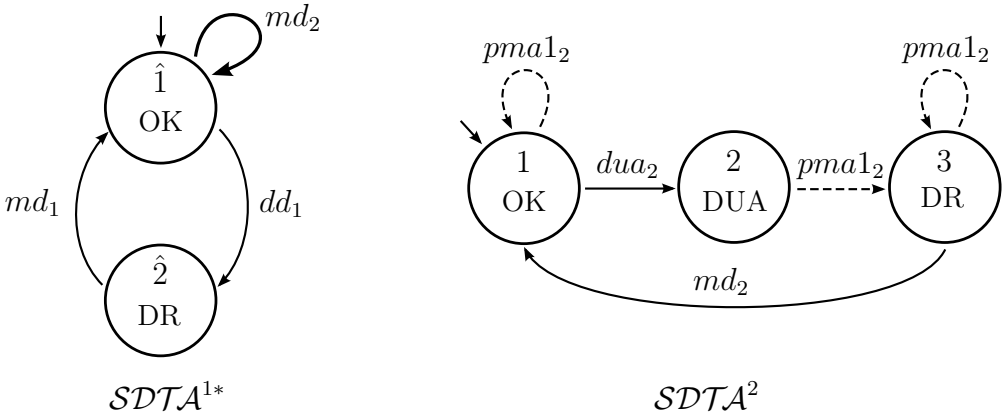

Figure C.1: States/transitions diagrams of $\mathcal{SDTA}^{1*}$ and $\mathcal{SDTA}^2$

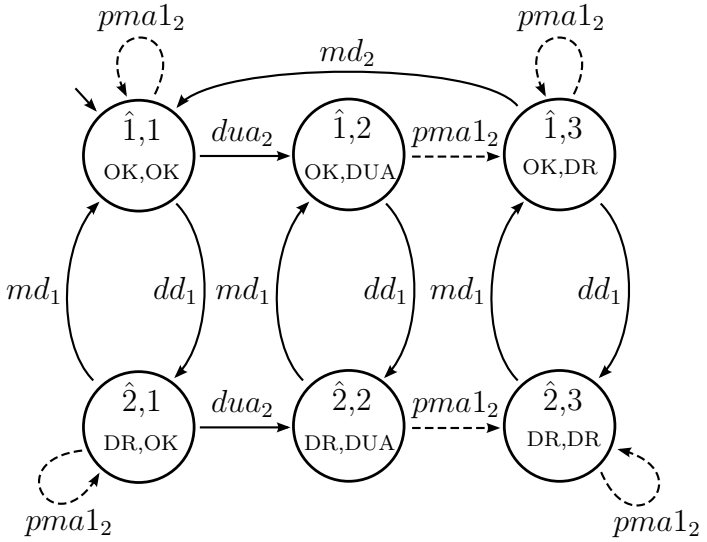

Figure C.2: States/transitions diagram of $\mathcal{SDTA}^* = \mathcal{SDTA}^{1*} \,||\, \mathcal{SDTA}^2$

The SDTA that models an independent SRS element, introduced in subsection 3.3.2, is now extended to consider repair priorities. Let us consider an SRS consisting of k elements. Let the focus be on the elements with the indices $i, p, r \in \{1, \ldots, k\}$. The element i has repair priority over the elements p and r. The repair priority is modeled via the SDTA extension by additional transitions triggered by common events, as described in example C.1. The SDTA of the element i is illustrated in figure C.3. Compared to the figure 3.3, it is evident that additional transitions are present in figure C.3. These additional transitions are triggered by the common events h, for all $h \in \mathcal{E}_{RP} = \{cms_p, md_p, cms_r, md_r\}$, indicating restoration of the elements p, r. The additional transitions are self-loop transitions, which appear in states, where the repair team would not be occupied by the maintenance activities of the element i. Moreover, the SDTA of the element p or r has to be extended to model the repair priority of these elements.

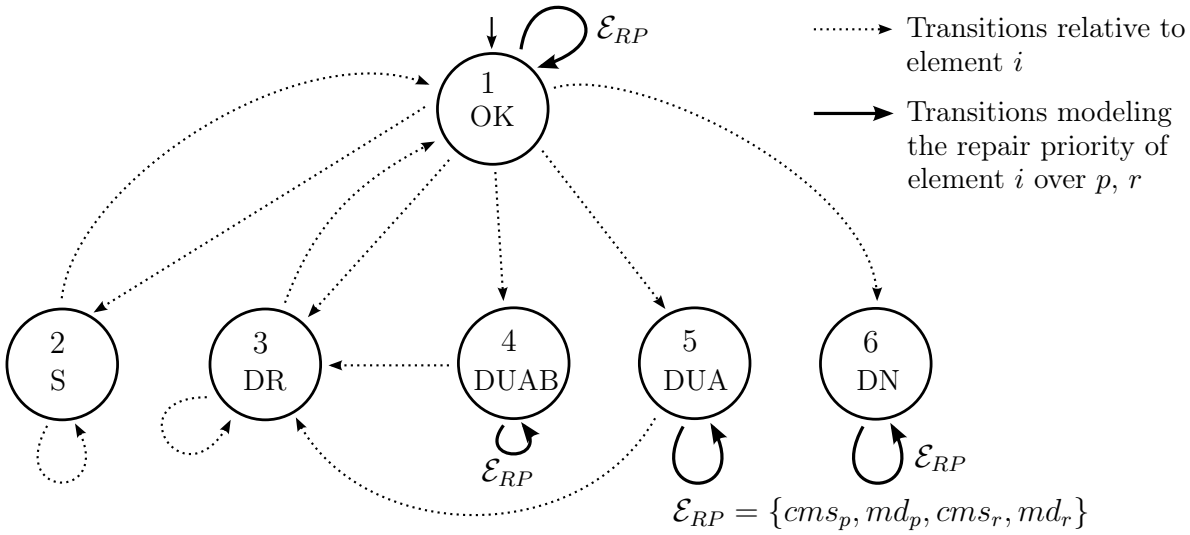

Figure C.3: SDTA modeling SRS element i with repair priority

It has to be noted that, the self-loop transitions triggered by an STE are of no relevance for the respective SDTA. It becomes evident in figure C.3. The self-loop transitions do not cause state transitions and can be ignored if only the SDTA that models the element i is analyzed.

C.2 Inhibition effect

The *inhibition effect* is relevant for the failure detection of SRS elements in series. If one element fails undetected, the failure detection of the further series elements might be *inhibited*. Due to the failed element, the failure detection signal of the series elements is interrupted on its way to the safety programmable logic controller. Hence, the dd-failures of these elements, though being detected, take an effect comparable to the undetected failures. The failure detection of these failures is inhibited and repair can not be initiated. Instead, these failures are only revealed by the PM of the element, which caused the inhibition. The inhibition effect results in dependencies between SRS elements. Whether an element is repaired immediately after a detected failure, depends on the current state of another element. The inhibition effect was analyzed and described in [Gab10].

An SRS that consists of the two series elements p and r is considered. Let the element p be subject to the inhibition effect, which is caused by the element r. The inhibition effect is modeled by the SDTA introduced below. In figure C.4, the SDTA that models the inhibition effect of the two elements p and r is given. By use of the SDTA in figure C.4, the SDTA that models the entire SRS, which consists of the two elements that are subject to the inhibition effect is easily determined. First, the SDTA that models the two elements is determined via the parallel composition, just as for elements without the inhibition effect. After that, the obtained SDTA is combined via the parallel composition

with the SDTA given in figure C.4, which models the inhibition effect. The result is the SDTA that models the SRS, which consists of the two elements that are subject to the inhibition effect.

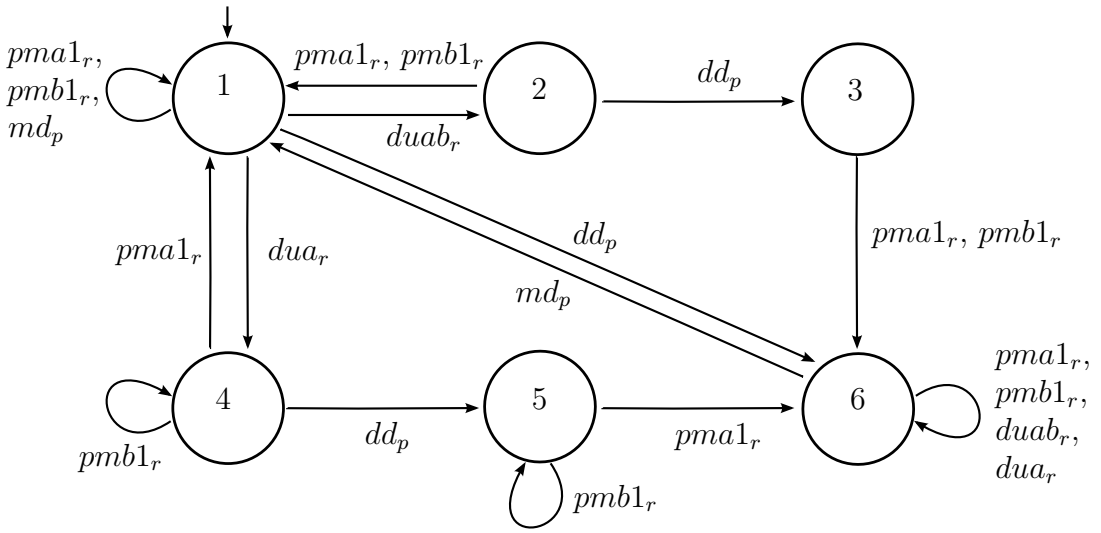

Figure C.4: States/transitions diagram of SDTA modeling inhibition effect

The inhibition effect of the two elements p and r is specified via the SDTA in figure C.4. The dd-failure of the element p will not be detected if previously a duab- or dua-failure of the element r occurs. This behavior is incorporated in the SDTA, shown in figure C.4. The SDTA is initiated in state 1 where both elements are fully operational. Further it is differentiated whether a duab- or dua-failure of the element r or a dd-failure of the element p occurs. These failures trigger the state transitions to the states 2, 4, or 6 respectively. After the dd-failure of the element p the repair is immediately started and after its completion the state transition back to the state 1 is triggered. If the duab- or dua-failure of the element r has occurred and afterwards the dd-failure of the element p triggers the state transitions to the states 3 or 4, the repair of the element p is delayed. The repair of the element p will only start after the duab- or dua-failure of the element r will be revealed by the respective PM. Hence, the state transitions from the state 3 or 5 to the state 6 will be triggered. After the repair of the element p is completed, the state transition to the state 1 is triggered.

It has to be noted that, the SDTA of figure C.4, which models the inhibition effect, is not intended to be evaluated on its own. Instead, it aims to extend the behavior of two independent elements by the inhibition effect.

Appendix D

Nomenclature

D.1 Acronyms

cc Common-cause, page 28

CDF Cumulative distribution function, page 9

CM Corrective maintenance, page 29

dd Dangerous detected failure mode, page 26

dn Dangerous non-revealable failure mode, page 27

DTA Automaton with deterministic timing, page 55

DTE Deterministic timed event, page 39

dua Dangerous undetected failure mode A, page 27

duab Dangerous undetected failure mode AB, page 27

FSA Finite State Automaton, page 8

FT Fault Tree, page 7

MC Markov chain, page 8

MP-CMC Multi-phase Continuous-time Markov Chain, page 58

MP-DMC Multi-phase Discrete-time Markov Chain, page 11

ODE Ordinary differential equation, page 10

PFD Probability of dangerous failure on demand, page 34

PFH Frequency of a dangerous failure, page 33

PM Preventive maintenance, page 30

RBD Reliability Block Diagram, page 7

RHF Random hardware failure, page 22

s Safe failure mode, page 25

SDTA Stochastic and Deterministic Timed Automaton, page 40

SE Simplified equation, page 8

SF Systematic failure, page 22

SIL Safety Integrity Level, page 4

SRS Safety-related System, page 19

STA Stochastic Timed Automaton, page 9

STAP Stochastic Timed Automaton with Poisson clock structure, page 40

STE Exponential stochastic timed event, page 40

D.2 Functions and operators

Γ Active event function of $\mathcal{SDTA}$ or $\mathcal{FSA}$, page 41

$\hat{\mathbb{E}}\left[T_U(t_1, t_2)\right]$ Estimate of $\mathbb{E}\left[T_U(t_1, t_2)\right]$, page 34

$\widehat{\overline{A(t_1, t_2)}}$ Estimate of $\overline{A(t_1, t_2)}$, page 34

$\hat{MTTF}$ Estimate of mean time to failure, page 33

$\mathbb{E}\left[T_U(t_1, t_2)\right]$ Mean of $T_U(t_1, t_2)$, page 33

$\mod\left(\frac{a}{b}\right)$ Modulo operation, a modulo b, page 68

$\overline{A(t_1, t_2)}$ Average availability in the time interval $(t_1, t_2]$, page 33

$\overline{G}(\Delta\alpha_j)$ Gain of $\overline{PFD}$ for deviation of parameter α_j, page 87

$PFD(t)$ Instantaneous probability of dangerous failure on demand, page 34

$\overline{PFD}(\mathcal{T})$ Objective function quantifying average PFD for given PM plan, page 94

$\overline{PFD}(t_1, t_2)$ Average probability of dangerous failure on demand over the time interval $(t_1, t_2]$, page 34

$PFD_{\max}(\mathcal{T})$ Objective function quantifying maximum PFD for given PM plan, page 94

$PFH(t)$ Instantaneous frequency of a dangerous failure, page 33

$WT(\mathcal{T})$ Objective function quantifying trade-off between average and maximum PFD for given PM plan, page 94

$A(t)$ Availability function, page 33

$F(t)$ Lifetime distribution function, page 32

$f_{\text{el fm}}$ Function of state classification regarding element failure modes, page 49

$f_{\text{el safety}}$ Function of state classification regarding element safety functions, page 46

f_{safety} Function of state classification regarding safety function, page 46

f_{tr} Transition function of $\mathcal{SDTA}$ or $\mathcal{FSA}$, page 41

$G_{\max}(\Delta\alpha_j)$ Gain of $PFD_{\max}$ for deviation of parameter α_j, page 87

$R(t)$ Reliability function, page 32

D.3 Mathematic symbols latin

$\boldsymbol{c}_{PFD}$ State selection column vector, page 58

$\boldsymbol{M}_{a,r}$ Phase transition matrix, related to PM type A of element r, page 58

$\boldsymbol{M}_{b,r}$ Phase transition matrix, related to PM type B of element r, page 58

$\boldsymbol{p}(t)$ State probabilities row vector, page 58

$\boldsymbol{p}_{\text{init}}$ Initial state probabilities row vector, page 58

$\boldsymbol{Q}$ Transition rates matrix, page 58

$\mathcal{AV}_{\text{el fm},j}$ Value of element failure mode attribute of element j, page 49

$\mathcal{AV}_{\text{el safety},i}$ Value of element safety attribute of element i, page 46

$\mathcal{A}_{\text{el fm}}$ Set of element failure mode attributes, page 48

$\mathcal{A}_{\text{el safety}}$ Set of element safety attributes, page 46

$\mathcal{A}_{\text{safety}}$ Set of safety attributes, page 46

$\mathcal{E}$ Set of events of $\mathcal{SDTA}$ or $\mathcal{FSA}$, page 41

$\mathcal{E}_{CF}$ Events set indicating common-cause failures, page 28

$\mathcal{E}_{CM}$ CM events set of an SRS, page 29

$\mathcal{E}_{det}$ Set of deterministic timed events, page 38

$\mathcal{E}_{PMstoch}$ Set of exponential stochastic timed PM events, page 39

$\mathcal{E}_{PM}$ PM events set of an SRS, page 30

$\mathcal{E}_{SF}$ Events set indicating single element failures, page 28

$\mathcal{E}_{stoch}$ Set of exponential stochastic timed events, page 39

$\mathcal{FSA}$ Finite State Automaton, page 41

$\mathcal{GE}_i$ Elements numbers set indicating the elements of group i, page 28

$\mathcal{G}$ Set of CDFs characterizing the set of stochastic clock sequences, page 40

$\mathcal{MP}$-$\mathcal{CMC}$ Multi-phase Continuous-time Markov Chain, page 58

$\mathcal{M}$ Sequence of phase transition matrices, page 58

$\mathcal{SDTA}$ Stochastic and Deterministic Timed Automaton, page 40

$\mathcal{S}_I$ Set of PM plans of PM strategy I, page 68

$\mathcal{S}_{IIIa}$ Set of PM plans of PM strategy IIIa, page 69

$\mathcal{S}_{IIIb}$ Set of PM plans of PM strategy IIIb, page 69

$\mathcal{S}_{II}$ Set of PM plans of PM strategy II, page 69

$\mathcal{S}_{IV}$ Set of PM plans of PM strategy IV, page 69

$\mathcal{S}_V$ Set of PM plans of PM strategy V, page 70

$\mathcal{T}$ Sequence of phase transition time sequences and PM plan, page 58

$\mathcal{T}_{\overline{PFD}}$ PM plan minimizing average PFD, page 94

$\mathcal{T}_{PFD_{\max}}$ PM plan minimizing the maximum PFD, page 94

$\mathcal{T}_{\text{init}}$ Initial PM plan for optimization, page 97

$\mathcal{T}_{WT}$ PM plan minimizing trade-off between average and maximum PFD, page 101

$\mathcal{T}_{a,SRS}$ Phase transition time sequence, related to simultaneous PM type A of all SRS elements, page 66

$\mathcal{T}_{a,r}$ Phase transition time sequence, related to PM type A of element r, page 58

$\mathcal{T}_{b,SRS}$ Phase transition time sequence, related to simultaneous PM type B of all SRS elements, page 66

$\mathcal{T}_{b,r}$ Phase transition time sequence, related to PM type B of element r, page 58

$\mathcal{U}$ Set of k-tuples of element safety attributes, page 46

$\mathcal{V}$ Set of deterministic clock sequences, page 39

$\mathcal{V}_h$ Deterministic clock sequence of event h, page 39

$\mathcal{W}$ Set of exponential stochastic clock sequences, page 40

$\mathcal{W}_h$ Stochastic clock sequence of event h, page 40

$\mathcal{X}$ Set of states of $\mathcal{SDTA}$ or $\mathcal{FSA}$, page 41

$\mathcal{X}_{MC}$ Set of states of $\mathcal{MP}$-$\mathcal{CMC}$, page 58

$\overline{\mathrm{U}}$ Attribute of states, complementary to U, page 46

$\overline{PFD}$ Average probability of dangerous failure on demand over the SRS mission time interval, page 34

$PFD_{\max}$ Maximum probability of dangerous failure on demand over the SRS mission time interval, page 34

$\overline{PFH}$ Average frequency of a dangerous failure, page 33

U Attribute of states, where SRS is either able to provide its safety function or in spurious operation, page 46

C_{MooN} Structure-related modification factor of common-cause failure fraction, page 53

$cmdd_i$ Event indicating that CM of element i has been completed after a dd-failure, page 29

cms_i Event indicating that CM of element i has been completed after an s-failure, page 29

dc Diagnostic coverage factor, page 72

dd_i Event indicating dd-failure of element i, page 28

dd_{GEi} Event indicating common-cause dd-failure of group i, page 28

dn_i Event indicating dn-failure of element i, page 28

dn_{GEi} Event indicating common-cause dn-failure of group i, page 28

dua_i Event indicating dua-failure of element i, page 28

dua_{GEi} Event indicating common-cause dua-failure of group i, page 28

$duab_i$ Event indicating duab-failure of element i, page 28

$duab_{GEi}$ Event indicating common-cause duab-failure of group i, page 28

e Most recent event of $\mathcal{SDTA}$ (causing transition to state x), page 43

e' Next event of $\mathcal{SDTA}$ (causing transition to state x'), page 43

G_h CDF characterizing the stochastic clock sequence of event h, page 40

$MTTF$ Mean time to failure, page 32

n_h Current score of event h, page 43

ne_h Length of deterministic clock sequence of DTE h, page 39

$ne_{a,i}$ Number of phase transition times related to PM type A of element i, page 66

$ne_{b,i}$ Number of phase transition times related to PM type B of element i, page 66

$p_i(t)$ State probability of state i, page 58

$pma1_i$ Event indicating the revealing of a dua- or duab-failure of element i via PM type A, page 30

$pma2_i$ Event indicating that PM of element i has been completed after a dua- or duab-failure, page 30

$pmb1_i$ Event indicating the revealing of duab failure of element i via PM type B, page 30

$pmb2_i$ Event indicating that PM of element i has been completed after a duab-failure, page 30

$q_{j,i}$ Element of transition rate matrix $\boldsymbol{Q}$ with the indices i, j, page 59

s_i Event indicating s-failure of element i, page 28

s_{GEi} Event indicating common-cause s-failure of group i, page 28

T_F Continuous random variable of the time the SRS continuously performs its assigned safety function or is in spurious operation, page 32

t_m SRS mission time, page 34

$t_{a,SRS,j}$ Phase transition time, j-th element of the sequence $\mathcal{T}_{a,SRS}$, page 66

$t_{a,r,j}$ Phase transition time, j-th element of the sequence $\mathcal{T}_{a,r}$, page 58

$t_{b,SRS,j}$ Phase transition time, j-th element of the sequence $\mathcal{T}_{b,SRS}$, page 66

$t_{b,r,j}$ Phase transition time, j-th element of the sequence $\mathcal{T}_{b,r}$, page 58

t_{Fi} i-th realization of random variable T_F, page 33

$t_{U,i}$ i-th realization of $T_U(t_1, t_2)$, page 34

$T_U(t_1, t_2)$ Random variable of the time the SRS performs its safety function or is in spurious operation during the time interval $(t_1, t_2]$, page 33

tca Coverage of PM type A, page 72

tcb Coverage of PM type B, page 72

$v_{h,j}$ Deterministic clock j of event h, page 39

$W_{h,j}$ Random variable of stochastic clock $w_{h,j}$, page 40

$w_{h,j}$ Stochastic clock j of event h, page 40

x Current state of $\mathcal{SDTA}$, page 43

x' Next state of $\mathcal{SDTA}$, given by $x' = f_{\mathrm{tr}}(x, e')$, page 43

x_{init} Initial state of $\mathcal{SDTA}$ or $\mathcal{FSA}$, page 41

y^* Interevent time between the events e and e', page 43

y_h Current clock value of event h, page 43

$Z(t)$ Discrete random variable indicating SRS condition, page 33

$n_h{}'$ Next score of event h, page 43

$y_h{}'$ Next clock value of event h, page 43

DN Element failure mode attribute of SDTA states, page 49

DR Element failure mode attribute of SDTA states, page 49

DUA Element failure mode attribute of SDTA states, page 49

DUAB Element failure mode attribute of SDTA states, page 49

OK Element failure mode attribute of SDTA states, page 49

S Element failure mode attribute of SDTA states, page 49

D.4 Mathematic symbols greek

$\beta_{dd_{GEj}}$ Common-cause failure fraction of dd-failures for j-th group of elements, page 53

$\beta_{dn_{GEj}}$ Common-cause failure fraction of dn-failures for j-th group of elements, page 53

$\beta_{dua_{GEj}}$ Common-cause failure fraction of dua-failures for j-th group of elements, page 53

$\beta_{duab_{GEj}}$ Common-cause failure fraction of duab-failures for j-th group of elements, page 53

$\beta_{s_{GEj}}$ Common-cause failure fraction of s-failures for j-th group of elements, page 53

$\boldsymbol{\alpha}$ Actual parameter vector, page 87

$\boldsymbol{\alpha}_0$ Nominal parameter vector, page 87

λ_h Rate parameter of exponential CDF G_h, page 40

λ_{cms_i} Rate parameters of STE cms_i, page 73

λ_{dd_i} Rate parameters of STE dd_i, page 72

λ_{dn_i} Rate parameters of STE dn_i, page 72

λ_{dua_i} Rate parameters of STE dua_i, page 72

λ_{duab_i} Rate parameters of STE $duab_i$, page 72

λ_{md_i} Rate parameters of STE md_i, page 73

λ_{s_i} Rate parameters of STE s_i, page 73

Bibliography

[BBB12] Florent Brissaud, Anne Barros, and Christophe Bérenguer. Probability of failure on demand of safety systems: impact of partial test distribution. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 226(4):426–436, 2012.

[BCO94] G. Becker, L. Camarinopoulos, and W. Ohlmeyer. Discontinuities in homogeneous markov processes and their use in modelling technical systems under inspection. *Microelectronics Reliability*, 34(5):771–788, 1994.

[Bir10] Alessandro Birolini. *Reliability Engineering*. Springer, 2010.

[Blu10] Michael Blum. *Effizienter Sicherheitsnachweis für mechatronische Systeme*. PhD thesis, Technische Universität München, 2010.

[Buk01] J.V. Bukowski. Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems. *IEEE Transactions on Reliability*, 50(3):321–329, 2001.

[CL08] C.G. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems*. SpringerLink Engineering. Springer, 2008.

[Dü10] Daniel Düpont. *Merging Bottom-up and Top-down Availability for realistic Analysis of Safety-related Loops*. PhD thesis, TU Kaiserslautern, 2010.

[DIN10] Maintenance – Maintenance terminology; Trilingual version EN 13306, December 2010.

[FF11] F. Felgner and G. Frey. Multi-phase markov models for functional safety prediction: Efficient simulation of markov models used for safety engineering and the online integration of individual systems' diagnostic and maintenance history. In *Dependable Control of Discrete Systems (DCDS), 2011 3rd International Workshop on*, pages 133–140, 2011.

[Fra78] Paul M. Frank. *Introduction to System Sensitivity Theory*. Academic Press, 1978.

[Gab10] Thomas Gabriel. *Generic Construction of Availability Calculation Models for Safety Loops in Process Industry.* PhD thesis, TU Kaiserslautern, 2010.

[HEK09] Joachim Hartung, Bärbel Elpelt, and Karl-Heinz Klösener. *Statistik: Lehr- und Handbuch der angewandten Statistik.* Oldenbourg, München, 15 edition, 2009.

[HLHH10] Stein Hauge, Mary Ann Lundteigen, Per Hokstad, and Solfrid Håbrekke. *Reliability Prediction Method for Safety Instrumented Systems PDS Method Handbook 2010 edition.* SINTEF, 2010.

[IEC05] Functional safety – Safety instrumented systems for the process industry sector – Parts 1-3. Standard IEC 61511:2003 + Corrigendum 2004, May 2005.

[IEC07] Application of Markov techniques (IEC 61165:2006); German version EN 61165:2006. Standard IEC 61165:2006, February 2007.

[IEC11a] Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements. Standard IEC 61508-1:2010, January 2011.

[IEC11b] Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations. Standard IEC 61508-4:2010, January 2011.

[IEC11c] Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels. Standard IEC 61508-5:2010, January 2011.

[IEC11d] Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3. Standard IEC 61508-6:2010, January 2011.

[IEC11e] Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 1-7. Standard IEC 61508:2010, January 2011.

[Int14] International Electrotechnical Comission. IEC 61508 Ed. 2.0 – Key concepts. `http://www.iec.ch/functionalsafety/faq-ed2/page5.htm`, 2014.

[Lit98] Lothar Litz. Grundlagen der sicherheitsgerichteten Automatisierungstechnik. *at - Automatisierungstechnik*, 46:56–68, 1998.

[Lit01] Lothar Litz. *Wahrscheinlichkeitstheorie für Ingenieure: Grundlagen, Anwendungen, Übungen.* Hüthig, Heidelberg, 2001.

[LR08] Mary Ann Lundteigen and Marvin Rausand. Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. *Reliability Engineering & System Safety*, 93(8):1208–1217, 2008.

[LRWW98] Jeffrey C. Lagarias, James A. Reeds, Margaret H. Wright, and Paul E. Wright. Convergence properties of the Nelder-Mead simplex method in low dimensions. *SIAM J. on Optimization*, 9(1):112–147, May 1998.

[LTT00] Robert Michael Lewis, Virginia Torczon, and Michael W. Trosset. Direct search methods: then and now. *Journal of Computational and Applied Mathematics*, 124(1–2):191–207, 2000. Numerical Analysis 2000. Vol. IV: Optimization and Nonlinear Equations.

[ML11] K. Machleidt and L. Litz. An optimization approach for safety instrumented system design. In *Reliability and Maintainability Symposium (RAMS), 2011 Proceedings - Annual*, pages 409–414, Januar 2011.

[ML12] K. Machleidt and L. Litz. Optimal prooftests for safety instrumented systems based on maintenance models. In *Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference*, volume 7, pages 6011–6020, June 2012.

[NM65] J. A. Nelder and R. Mead. A simplex method for function minimization. *The Computer Journal*, 7(4):308–313, January 1965.

[Sob91] I.M. Sobol. *Die Monte-Carlo-Methode*. VEB Deutscher Verlag der Wissenschaften, 1991.

[TE09] Alejandro Carlos Torres-Echeverría. *Modelling and optimization of Safety Instrumented Systems based on dependability and cost measures*. PhD thesis, University of Sheffield, Department of Automatic Control and Systems Engineering, 2009.

[Zio07] Enrico Zio. *An introduction to the basics of reliability and risk analysis*, volume 13 of *Series on quality, reliability & engineering statistics*. World Scientific, Singapore, reprint. edition, 2007.

[Zio09] Enrico Zio. *Computational methods for reliability and risk analysis*. Series on quality, reliability & engineering statistics. World Scientific, 2009.

About the author

Konstantin Machleidt was born in Nowosibirsk, Russia. As a child he emigrated with his parents to Germany. In 2007 he graduated from the Technische Universität Kaiserslautern with a Dipl.-Ing. degree (equivalent to Master of Science) in electrical engineering, with the majors mechatronics and automatic control. He then joined BASF SE Ludwigshafen, where he worked as an automation engineer with the Center of Technical Expertise for Automation Technology. In 2009 he took a full-time position as a research associate at the Institute of Automatic Control of the Technische Universität Kaiserslautern, where he focused on safety-related automation technology. The major field of his research was the probabilistic modeling, analysis, and optimization of Safety-related Systems. The research work in that field resulted in this book as a doctoral thesis. In October 2015 Konstantin Machleidt defended his doctoral thesis to be awarded Doktor der Ingenieurwissenschaften (Dr.-Ing.).