NTNU

Norwegian University of
Science and Technology

Analysis of commom cause failures in complex safety instrumented systems

Torbjørn Lilleheier

Master of Science in Physics and Mathematics
Submission date: July 2008
Supervisor: Mette Langaas, MATH
Co-supervisor: Marvin Rausand, IPK

Norwegian University of Science and Technology
Department of Mathematical Sciences

Problem Description

Reliability requirements to safety instrumented systems (SIS) are outlined in the international standard IEC 61508 along with its application-specific standards. Analysis of common cause failures (CCF) is an important part of reliability documentation. IEC 61508 suggest that CCFs are modelled by the beta-factor model. The beta-factor model is adequate for simple systems, but is not able to cover all types of dependencies in complex systems. Several attempts have been made to extend the beta-factor model, for example in the PDS project. The objective of this master thesis is to review existing models and based on these, propose strategies for how to handle the modelling of CCFs with respect to different SIS.

As a part of the thesis, the candidate shall:
- Carry out a litterature survey of CCF modelling and present the results from the survey.
- Assess the quality and the area of application for the different models given in the survey.
- Introduce examples and apply selected CCF-models to these examples.
- Compare the results obtained from the modelling process, and assess the quality (if possible) of the results.
- Assess the quality of the results obtained.

Following agreement with the supervisor, the various items may be given different weights.

Assignment given: 21. January 2008
Supervisor: Mette Langaas, MATH

Analysis of common cause failures in complex safety instrumented systems

Torbjørn Lilleheier

July 28, 2008

Preface

The present thesis is written at the request of the company INERIS in France between February 2008 and July 2008. The thesis is also the finalization of the 5-year master's degree at The Norwegian University of Science and Technology (NTNU). The master's thesis is written at INERIS' facilities in Verneuil-en-Halatte and contains a study about common cause failure analysis in safety instrumented systems. The analysis is based on real systems that INERIS is currently working on.

When the possibility of moving to France to write the master's thesis at INERIS was presented to me, I immediately responded positively. This seemed like a great opportunity, both working with real systems, but also the fact of moving to another country to learn the language and a different culture. As the stay approaches the end, I do not regret my decision and I believe I have learned a lot by spending four months at INERIS.

I would like to thank my supervisor at the department of Mathematical Sciences at NTNU, Assosiate Professor Mette Langaas, for much appreciated advice even though the topic of the thesis is not within her main area of expertice.

I would also like to thank my other supervisor, Professor Marvin Rausand, at the Department of Production and Quality Engineering at NTNU for presenting me with the opportunity of moving to France. In addition, his vast knowledge regarding reliability analysis proved to be an important asset when working on this thesis.

Finally, my supervisor, Mr. Francois Massé and co-worker, PhD. student Florent Brissaud, at INERIS in France have earned my gratitude for creating a good work-environment and for being helpful both with practical and professional difficulties.

Torbjørn Lilleheier, July 28, 2008

Abstract

Common cause failures (CCFs) have been an important issue in reliability analysis for several decades, especially when dealing with safety instrumented systems (SIS). Different approaches have been used in order to describe this CCFs, but the topic is still subject to much research and there does not exist a general consensus as to which method is most suitable for dealing with CCFs. The β-factor model is the most popular method today, even though this method has some well-known limitations. Other, more complicated methods, are also developed to describe situations where the β-factor model is inadequate.

The purpose of this thesis is to develop a strategy to suggest in which situations the different CCF methods are applicable. This is done by making a survey which includes several of the existing methods, before applying these in concrete SIS-examples. Observing the specific system in operation is a valuable tool and may help in acquiring feedback data to describe the lifetime of specific components and the number of failed components conditioned on the fact that the total system is failed. Since such feedback data usually are scarce and in our case totally absent, assessing whether the obtained results are accurate is difficult. Thus, the numerical results obtained from the analysis are compared to each other with respect to the assumptions of the particular model. For instance, the PDS method, a method developed for the Norwegian offshore industry, contains some assumptions which are different from the assumptions of the β-factor model, and the report provides a study with respect to how these different assumptions lead to different results.

Although other methods are introduced, most focus is given to the following four, the β-factor model, the PDS method, Markov analysis and stochastic simulation. For ordinary M out of N architectures with identical components, the PDS method is assumed adequate, and for $N = 2$, the β-factor model works well. Markov analysis and stochastic simulation are also well suited for modelling ordinary M out of N SIS, but because of the higher level of complexity, these approaches are not deemed necessary for simple systems. The need for Markov analysis becomes evident when working with SIS of a more complex nature, for instance non-identical components. Both the β-factor model and the PDS method are not able to describe the system in full when dealing with certain types of systems that have different failure rates.

An even more complex SIS is also included to illustrate when stochastic simulation is needed.

This SIS is modelled by designing a computer algorithm. This computer algorithm describes how the system behaves in the long run, which in turn provides the estimate of interest, namely the average probability of failure on demand (PFD).

Finally, it is always important to remember that if there exist any feedback data or expert knowledge describing the distribution of the number of components that fail in a CCF, this is vital in deciding the most descriptive CCF model. By the term “descriptive model”, we mean a model that both describes the architecture of the system as accurately as possible, and also makes as few assumptions as possible. If it is known, either by applying expert opinion or from feedback data, that if a CCF occurs, all components of the SIS will always be disabled, then the β-factor model is an adequate way of modelling most systems. If such knowledge does not exist, or it is known that a CCF may sometimes disable only a part of the SIS, then the β-factor model will not be the most descriptive model.

Contents

Table of Abbreviations

CCF	Common cause failure
CSU_{TOT}	The total critical safety unavailability
DD	Dangerous detected
DU	Dangerous undetected
DTU_R	Downtime unavailability due to repair of dangerous failures
MBF	Multiple β-factor
$MooN$	M out of N
$MTTF$	Mean time to failure
$MTTR$	Mean time to repair
PBF	Partial β-factor
PDS	Reliability and availability of computer based systems
PFD	The *average* probability of failure on demand
P_{TIF}	the probability of loss of safety due to systematic failures
RPS	Random Probability Shock
SD	Safe detected
SIF	Safety instrumented function
SIL	Safety Integrity Level
SIS	Safety instrumented system
SU	Safe undetected
UPM	(The) Unified Partial Method

Mathematical notation

β	The probability of a CCF given that a failure is observed
λ	The total failure rate
$\lambda^{(c)}$	The failure rate of common cause failures
$\lambda^{(i)}$	The failure rate of individual failures
ν	The rate of shock-rate used in the Shock-models
θ	The probability that $k+1$ components fail in a CCF given that k components have already failed (for the PDS method)
τ	The time (in hours) between maintenance or testing in a system
a_{jk}	The transition rate from state k to state j for Markov analysis
$\overline{A}(t)$	The unavailability of a system or component
C_{MooN}	The modification constant that accounts for different architectures
C_N	The modification constant in the PDS method used to calculate H_N
$f_{j,N}$	The probability that exactly j out of N components fail in a CCF
$g_{j,N}$	The probability that j specific channels out of N have failed
H_N	A constant used when calculating individual failures in the PDS method
$P(\cdot)$	The probability of $(\cdot)$
$P_j(t)$	The probability of a system being in state j at time t for Markov analysis
$\mathbf{T}$	The transition matrix used in Markov analysis
Q	Failure probability of one component
Q_{MooN}	The probability that a $MooN$ configuration is in a failed state

Chapter 1

Introduction

Common cause failures (CCFs) are an important part of reliability analysis, and engineers have been aware of these types of failures since the mid-seventies (Fleming, 1974). Today numerous models exist which explain this concept and which attempt to model the impact such CCFs have on different systems. Even though this topic has been given much attention, it is still considered to be difficult and of a complex nature. CCFs are difficult to quantify correctly, i.e. it is difficult to know if a component fails due to a common root cause that affects several components, or if it fails because it is old and worn out. Usually, not much feedback data exist, so modelling this properly has proven difficult. When referring to feedback data as in the previous sentece, we mean recorded times of when the system fails and the reason for this failure, as well as which components failed. In addition, different systems have different properties meaning that a model that may work for one system, does not necessarily work for another.

The report at hand focuses on the impact CCFs have on safety instrumented systems (SIS), i.e. systems whose purpose is to maintaining the safety of some physical structure (see Section 2.1 for definition). If a critical situation occurs, it is important that the systems which provide the safety are able to function properly.

The objective

The overall aim of the present report is to propose a strategy on how to treat CCFs for different types of SIS. Different SIS may have different architectures, and it is not certain that *one* method proves adequate to handle the vast variety of different architectures. Secondary goals are introduced below as a means to achieve the superior aim, namely proposing a CCF strategy. The primary (·) and secondary (numbered) goals are as follows

- Propose a strategy on how to handle CCF modelling for various types of SIS.

    1. Carry out a literature survey of CCF modelling and present the results from the survey.

2. Assess the quality and the area of application of the different models given in the survey.
3. Introduce different examples and apply selected CCF-models.
4. Compare results obtained from the modelling process, and assess the quality (if possible) of the results.

Limitations

The present thesis aims at presenting a strategy for handling CCFs when working with SIS. This is done by analyzing several systems and architectures which all have different assignments and architectures. As is shown, specific methods may work well for certain architectures, but the same method may prove less suitable when dealing with other architectures.

Within the given framework, i.e. with respect to the goals that are set, there are some limitations. Firstly, not all CCF-models are introduced in the present report. Some of the probably most well-known are included, but other methods are also available.

Sadly, no records of the physical behaviour of the current systems in operation exist. This makes it difficult to assess the quality of the results. As well as lacking behavioural information, other information is also lacking. This includes for instance any registered failure rates and failure rate distribution. As a result, failure rates are collected from different data bases, e.g. OREDA (2002) or Hauge et al. (2006b). For each system introduced in the report, the only information given, was the architecture and the time between periodic testing. In addition, estimates of the failure rates and an estimate of the CCF-rate were applied. As such, all calculations and assessments are based on the mathematical procedure alone with little information about the physical system itself. As such, the report focuses more on the methods and how to apply the mathematics and not so much on the results.

The structure of the report

Some prior knowledge about reliability analysis and the mathematical background required to carry out such analyzes is necessary when reading the following report. Even so, most of the applied methods are described in detail, or references for further reading are provided.

Chapter 2 introduces a few definitions of the expression, "CCF". In addition, mathematical tools and methods which are used in later chapters, are given. Chapter 3 describes some of the existing models that deal with CCFs. Perhaps the most famous model is the β-factor model, and this model is introduced. As is described, the β-factor model has limitations, but different generalizations of the β-factor model exist, and some of these are explained. In particular, the multiple β-factor method is a generalization of the β-factor model that should be applicable for all different M out of N ($MooN$) architectures. The procedure given by the MBF model is later formulated into a method called the PDS method.

There are also other models which may be applied when dealing with CCFs, for instance Shock models and the Unified Partial method. These methods are also described in Section 3.7 and Appendix A.4, respectively.

In some cases the notation used in the present report differs from the notation used in the references. This is done in order to make the notation used in the present report as consistent as possible.

Part II includes several examples where the methods described in Part I are applied. Different methods are applied depending on the architecture, and these examples will hopefully give an indication of which methods are suited for which architectures. For most of the examples several different solutions are provided in order to compare results.

In Part III the obtained results are analyzed more thoroughly. Chapter 7 takes a close look at all the examples given in Part II and provides ideas as to which methods are considered to be reliable for the different examples. Such claims are naturally not easy to make, and the author's opinion is reflected.

Chapter 8 introduces general strategies on how to deal with CCFs. All the derived models and all the examples previously analyzed are presented in order to create a general strategy on how to deal with CCFs for different architectures and with different numerical values. To make a short summary of the most important parts of the report, Chapter 9 includes some closing remarks and final conclusions.

Finally, a section describing different methods of obtaining a "plant-specific" β is also included in Appendix A. This chapter is not applied directly throughout the rest of the report, and it was considered reasonable to move it to the Appendix.

Part I

Basic concepts and methods

Chapter 2

Definitions and mathematical tools

The present chapter describes a few of the tools used when quantitatively analyzing CCFs. First, the concept of CCF is defined. This is followed by methods helping to describe the system in question in order to gain a good overview when applying different methods. Finally, a few mathematical definitions widely used in reliability analysis are introduced.

2.1 Safety instrumented systems and functions

The present report report considers the safety of different systems or components. A safety instrumented system (SIS) is a system which consists of sensors, logic solvers and actuating items. The sensors may for instance be gas detectors, the logic solver could be a computer and the actuating items may be shut down valves. A fire and gas detection system with an alarm or a sprinkler system is an example of a SIS. A SIS is constructed to take the process into a safe state if a dangerous event occurs.

A safety instrumented function (SIF), however, is a function that is implemented by a SIS. A SIS may consist of several SIFs. An example where a SIS consists of two SIFs is given in Chapter 6. Each SIF has to fulfill a requirement which is called safety instrumented level (SIL). Safety integrity is defined as

> the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.
>
> IEC 61508 (2000, Part 4)

The measure is classified into four different discrete levels defined as Safety Integrity Levels (SIL). The SILs are given in Table 2.1. The values stated in the Low demand column represent the *average probability of failure to perform its design function on demand*, while the values represented in the High demand mode equals *the probability of a dangerous failure per hour*. The terms low and high demand mode are defined as

- **Low demand mode:** The frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency.
- **High demand mode:** The frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-test frequency.

Table 2.1: The different SIL levels for Low demand mode and High demand mode.

SIL	Low demand mode	High demand mode
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

If a demand occurs, the probability of the SIS being unable to perform as required equals the probability of failure on demand (PFD), see Section 2.4. By calculating the PFD, we obtain the SIL. Many systems are required to meet a certain SIL. Results later in the report are assigned the corresponding SIL. The examples given in this thesis all belong to the low demand mode category, i.e. shut down valves, heat detectors and the like. We do not expect these systems to be activated very often.

An example of a SIF working in a high demand mode is the braking system of a car. A demand is placed upon this SIF quite frequently, so the SIL is required to be much higher for these types of systems.

2.2 Common cause failures

There are many definitions describing CCFs. Smith and Watson (1980) studied nine different definitions and concluded that there is no "correct" definition, but the best definition depends on the field of use. If a company is to apply CCF modelling, they should use a working CCF definition that is easily understood and readily applied. To that end, they proposed their own definition for CCF.

> Inability of multiple, first-in-line items to perform as required in a defined critical time period due to a single underlying defect or physical phenomena such that the end effect is judged to be a loss of one or more systems.
>
> Smith and Watson (1980)

Naturally, this leads to more definitions like, how long is a critical time period, and what is an underlying defect of physical phenomenon. Rausand and Høyland (2004) proposes a shorter, alternative definition to CCF. This definition is quite similar to the above, but perhaps a bit easier to comprehend.

> A dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause.
>
> Rausand and Høyland (2004)

In the present report, the latter of the two definitions is used.

Other papers also attempt to describe the CCF-concept and also defence strategies against these failures (Lundteigen and Rausand, 2007). The present thesis focuses on the modelling process and not so much on defence strategies, but these strategies are nevertheless important.

Another definition which may be equally adequate, is the following given by the standard IEC 615011 (2003).

> A failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure.
>
> IEC 615011 (2003)

Furthermore, a channel is defined as *element or group of elements that independently perform(s) a function*. This definition does not include the concept of "a limited time interval", and may in some occasions prove to be inaccurate.

2.3 Fault tree analysis

A fault tree is a well arranged method of modelling the failure of a certain (top) event. The failure of a top event depends on other basic (physical) components. The dependencies between the components are modelled in a tree structure using AND- or OR-gates. As an example, consider a system of two components, 1 and 2. A fault tree with an AND-gate is used in the case where the top event (system) fails if both component 1 and 2 fail. This is similar to the parallel structure in a reliability block diagram (see e.g. Rausand and Høyland (2004)). The OR-gate describes the event that the system fails if either component A or B fails. This corresponds to the series structure in a reliability block diagram. There are also other possible gates when dealing with fault trees, but these are not included in the present report. An example of a simple AND- and OR-gate is plotted in Figure 2.1. The fault tree method is thoroughly explained in Vesley et al. (2002).

2.4 Probability of Failure on Demand (PFD)

A common way of measuring the quality of a SIF is to calculate the probability of failure of demand (PFD). This is the estimate which all the models presented in Chapter 3 calculates. Some approximations are usually made when calculating the PFD, and one such is that we are only

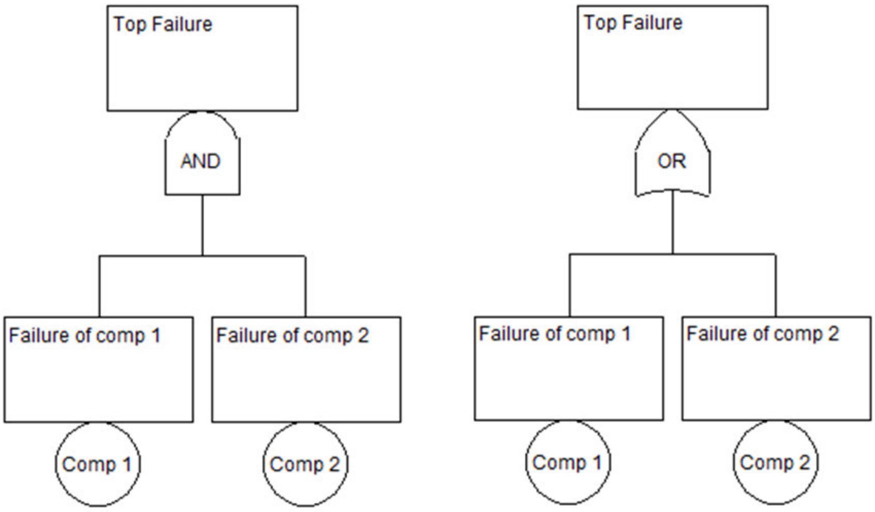

Figure 2.1: An example of an AND gate (left) where both components have to fail in order for the system to fail, and an OR gate (right) where the system fails if one of the two components fail.

considering dangerous undetected (DU) failures, i.e. failures that remain undetected until a demand is made upon the system. This simplification, and others, are more thoroughly explained in Section 3.1. The following introduction to the concept of PFD is similar to that of Rausand and Høyland (2004).

First, we define the safety *unavailability* $\overline{A}(t)$ of the SIF. We are, in the present report, only interested in the availability in an interval $(t, \tau + t)$ so the formula is thus given for an interval. Since we work with systems that are assumed to be as good as new after time τ, we will for simplicity only consider the time interval $(0, \tau)$.

$$\begin{aligned}\overline{A}(t) &= P(\text{a failure has occurred at, or before, time } t) \\ &= P(T \leq t) = F(t)\end{aligned} \tag{2.1}$$

$F(t)$ is the cumulative density function of the component or system. If the SIF is tested at a regular time interval τ and the component is considered to be *as good as new* after each test, the PDF is

$$PFD = \frac{1}{\tau}\int_0^\tau \overline{A}(t)dt = \frac{1}{\tau}\int_0^\tau F(t)dt = 1 - \frac{1}{\tau}\int_0^\tau R(t)dt \tag{2.2}$$

where $R(t)$ is the survivor function ($R(t) = 1 - F(t)$).

The PFD is usually calculated using an approximation. In order to show this, consider a component which has constant failure rate with respect to DU failures, i.e. $z(t) = \lambda_{DU}$. This implies that $R(t) = e^{-\lambda_{DU} t}$. After inserting this expression into Equation (2.2) and integrating, we obtain

$$PFD = 1 - \frac{1}{\lambda_{DU}\tau}\left(1 - e^{-\lambda_{DU}\tau}\right). \tag{2.3}$$

By making use of the Taylor expansion for $e^{-\lambda_{DU}\tau}$ (Rottman, 1995) the following expression is obtained.

$$PFD = 1 - \left(1 - \frac{\lambda_{DU}\tau}{2} + \frac{(\lambda_{DU}\tau)^2}{3!} - \frac{(\lambda_{DU}\tau)^3}{4!} + ...\right) \tag{2.4}$$

If $\lambda_{DU}\tau$ is sufficiently small[1], we use the approximation

$$PFD \approx \frac{\lambda_{DU}\tau}{2}. \tag{2.5}$$

The approximation in Equation (2.5) is widely used and the result is always conservative. This result is used throughout the present report as well. Table 2.2 shows PFD approximations for different architectures ($MooN$). A similar table is also found in Rausand and Høyland (2004, Chapter 10). The results of Table 2.2 are also obtained through the following general formula

Table 2.2: A numerical table for PFD approximations of different architectures.

MooN	$N=1$	$N=2$	$N=3$	$N=4$
$M=1$	$\frac{\lambda_{DU}\tau}{2}$	$\frac{(\lambda_{DU}\tau)^2}{3}$	$\frac{(\lambda_{DU}\tau)^3}{4}$	$\frac{(\lambda_{DU}\tau)^4}{5}$
$M=2$	–	$\lambda_{DU}\tau$	$(\lambda_{DU}\tau)^2$	$(\lambda_{DU}\tau)^3$
$M=3$	–	–	$\frac{3\lambda_{DU}\tau}{2}$	$2(\lambda_{DU}\tau)^2$
$M=4$	–	–	–	$2\lambda_{DU}\tau$

$$PFD_{MooN} \approx \binom{N}{N-M+1}\frac{(\lambda_{DU}\tau)^{N-M+1}}{N-M+2}. \tag{2.6}$$

Note that the PFD is calculated for the SIF and not the SIS. This means that if the system consists of N SIFs, N PFDs have to be calculated.

[1] Sufficiently small meaning $\lambda_{DU} \cdot \tau \leq 0.2$, (Hauge et al., 2006a)

Chapter 3

Existing models for CCF modelling

3.1 Introduction

The concept of CCFs has been addressed by several authors, and different models have been created to attempt to model the impact CCFs have on SIS. The present chapter describes some of these models and the mathematical foundation on which they are based. Naturally the β-factor model, along with its generalizations is included, but other models are also introduced. IEC 61508 (2000) plays an important role in reliability analysis, so notes about this standard is included. The PDS method, which differs slightly from the IEC-standard, is explained along with Markov analysis, which, for reliability analysis, is derived in ISA (2002). In addition Shock models are explained in Hokstad (1988), and the Square-Root method originally given in NUREG-75/014 (1975) is also included to get an overview of some of the first attempt which was made to model dependent failures.

Different types of failures may be classified into different sub-groups. We may for instance consider some types of failures to be dangerous (D), while others are considered safe (S). In addition failures can either be detected (D) or remain undetected (U). This gives the four main groups of failures mentioned in the current thesis, DD, DU, SD and SU. Other types of failures also exist, for instance Spurious Trips, but these are not treated in the present report. Such failures receive well-earned attention in Lundteigen and Rausand (2008).

When describing the following models, dangerous undetected (DU) failures have been focused on, and DU-failures are usually the main focus of authors when dealing with reliability analysis. The reason for this is the fact that detected failures are usually repaired relatively quickly and do not contribute significantly to the unavailability. When the repair time is assumed to be long, DD failures are not neglected, and this is further discussed in Section 3.9.

Another assumption usually made is that following an inspection (at time τ) the SIF is assumed to be “as good as new”. This assumption is also applied in the current report.

3.2 The Square-Root method

The Square-Root Method, originally presented in NUREG-75/014 (1975), but also recited in Rausand and Høyland (2004), is a simple bounding technique used to estimate the effect of CCFs on a system. Since this model perhaps was the first model to deal with CCFs, an example is included for illustrative purposes. Consider a parallel system consisting of two components A_1 and A_2. Let A_i be the situation that component i is in a failed state at time t. The unavailability of the system is defined as $\overline{A} = P(A_1 \cap A_2)$. We have the identity

$$P(A_1 \cap A_2) \leq \min\{P(A_1), P(A_2)\} \tag{3.1}$$

which is an upper bound if A_1 and A_2 are positively dependent [1]. If A_1 and A_2 are independent, then

$$P(A_1 \cap A_2) \leq P(A_1) \cdot P(A_2) \tag{3.2}$$

This gives an upper and lower limit of the unavailability $\overline{A}$.

$$\underbrace{P(A_1) \cdot P(A_2)}_{q_L} \leq \overline{A} \leq \underbrace{\min\{P(A_1), P(A_2)\}}_{q_U} \tag{3.3}$$

The unavailability $\overline{A}^*$ of the system is then approximated using the geometric mean of these limits.

$$\overline{A}^* = \sqrt{q_L \cdot q_U} \tag{3.4}$$

This method has its weaknesses since there is no mathematical support for applying Equation (3.4). The Square-Root Method does not take into account the various degrees of coupling between the components. The Square-Root Method is not used in practice today.

3.3 The β-factor model

The β-factor model is the most commonly used CCF model today, and it was originally proposed by Fleming (1974). This model assumes that a certain percentage of all failures are CCFs. In order to describe the β-factor model, consider a system of N identical components with constant failure rate with respect to DU-failures as λ_{DU}. Using the definition proposed by Rausand and Høyland (2004), a component may fail either due to

- circumstances that concern only that specific component, or
- occurrences of external events which consequently lead to all components failing simultaneously.

[1] Positively dependent means that $P(A_1|A_2) \geq P(A_1)$.

Denote $\lambda_{DU}^{(i)}$ as the failure rate with respect to a single failure and $\lambda_{DU}^{(c)}$ as the failure rate due to a CCF. The total failure rate of a component is written as a sum of the two failure rates

$$\lambda_{DU} = \lambda_{DU}^{(i)} + \lambda_{DU}^{(c)} \tag{3.5}$$

β is called the common cause factor and is defined as

$$\beta = \frac{\lambda_{DU}^{(c)}}{\lambda_{DU}^{(c)} + \lambda_{DU}^{(i)}} = \frac{\lambda_{DU}^{(c)}}{\lambda_{DU}} \tag{3.6}$$

The value β can also be expressed as

$$\beta = P(\text{CCF}|\text{Failure}), \tag{3.7}$$

i.e. β equals the conditional probability that there is a CCF given that there is a failure.

An example of relating the β-factor model and fault tree analysis is given in Figure 3.1. This particular system consists of three redundant and independent components which are exposed to CCFs. The independent- and the CCF-component are separated by an OR-gate, while the independent components are separated by an AND-gate.
The following, simple example is provided in order to illustrate the properties of the β-factor model.

Example 1.
Consider a system with two independent components connected in parallel. Both components have failure rate λ_{DU}. By using a reliability block diagram, the situation can be modelled as in Figure 3.2. The failure rate function of components 1 and 2 is $z_1 = z_2 = (1-\beta)\lambda_{DU}$, and for component C the failure rate function is $z_C = \beta\lambda_{DU}$. The corresponding survivor function, defined as $R(t) = exp\left(-\int_0^t z(u)du\right)$, is

$$R(t) = (1-(1-R_1(t)R_2(t)))\cdot R_C(t) \tag{3.8}$$

By inserting the correct failure rate functions, the survivor function in Equation (3.8) becomes

$$R(t) = 2e^{-\lambda_{DU}t} - e^{-(2-\beta)\lambda_{DU}t} \tag{3.9}$$

The measure of interest is now the PFD and this would for the present example give

$$PFD = \frac{1}{\tau}\int_0^\tau R(t)dt.$$

If we use the approximated results in Table 2.2, we obtain, since we have a $1oo2$ system followed by a $1oo1$ system.

$$PFD \approx \frac{((1-\beta)\cdot\lambda_{DU}\cdot\tau)^2}{3} + \frac{\beta\cdot\lambda_{DU}\cdot\tau}{2} \tag{3.10}$$

The mean time to failure, defined as $MTTF = \int_0^\infty R(t)dt$, is

$$MTTF = \frac{2}{\lambda_{DU}} - \frac{1}{(2-\beta)\lambda_{DU}} \tag{3.11}$$

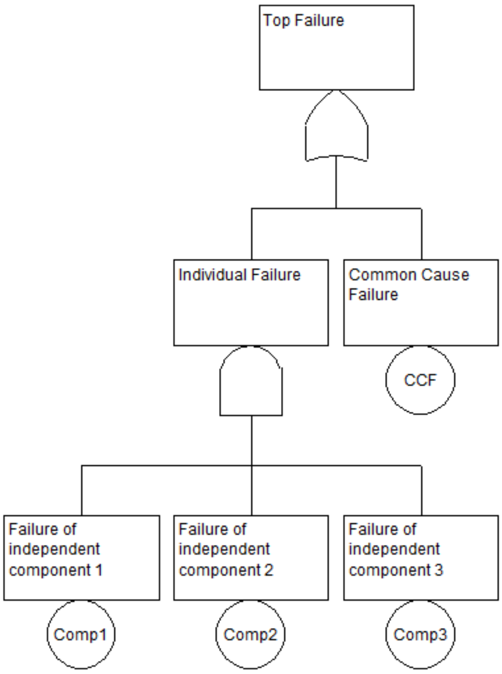
Top Failure
Individual Failure
Common Cause Failure
CCF
Failure of independent component 1
Failure of independent component 2
Failure of independent component 3
Comp1
Comp2
Comp3

Figure 3.1: A fault tree with three independent components in parallel and a CCF term.

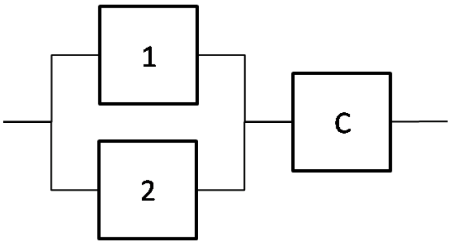

Figure 3.2: Reliability block diagram of two components that are exposed to CCF.

Note: The previous example considered two identical components, but this is not always the case. For instance, two valves in parallel may be subject to different environments or be of different fabricates. This may consequently lead to different failure rates of the two valves. Hauge et al. (2006a, Appendix D) suggests using the geometric mean for the different failure rates in order to handle this problem when the failure rates are very different, with for instance a factor of 10.

If the two components in the previous example had failure rates $\lambda_{DU}^{(1)}$ and $\lambda_{DU}^{(2)}$ with $\lambda_{DU}^{(1)} \neq \lambda_{DU}^{(2)}$, the calculations should be carried out by using $\lambda_{DU} = \sqrt{\lambda_{DU}^{(1)} \cdot \lambda_{DU}^{(2)}}$. Generally, for N redundant components where at least one has different failure rate than the others, the suggested λ_{DU} to be used in general calculations is $\lambda_{DU} = (\lambda_{DU}^{(1)} \cdot \lambda_{DU}^{(2)} \cdots \lambda_{DU}^{(N)})^{\frac{1}{N}}$.

A weaknesses of the β-factor model: If we have a system consisting of more than two components, the β-factor model does not allow for the possibility that more than one, but not all components fail due to a CCF. If a systems consists of 3 components, the β-factor model can not be used to model the event that 2 out of 3 components fail. This is illustrated in Figure 3.3.

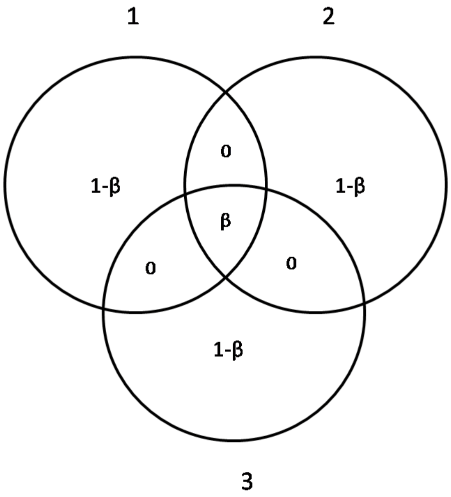

Figure 3.3: The β-factor model of a system consisting of 3 components. The components may either fail independently, or due to a CCF in which all components fail.

3.4 The multiple β-factor model

The multiple β-factor (MBF), described both in Hokstad and Corneliussen (2004) and Hokstad et al. (2006), is a generalization of the β-factor model. As explained in the previous Section, a weakness in the β-factor model becomes evident when we have more than two components in a system. The MBF model, however, allows for the possibility of independent failures and CCFs that destroy j out of N components for $j \leq N$. For $N = 2$ the two models are identical, but they differ when $N \geq 3$.

The MBF model assumes complete uniformity, meaning that all N components have the same constant failure rate independent of time. In addition, all specific combinations of failed components j and not failed components $N - j$ have the same probability of occurring. A further assumption of the MBF model is that removing j of the N components does not influence the failure rate of the remaining components.

In the present model, β_j is defined as

$$\beta_j = P(A_{j+1}|A_1 \cap \ldots \cap A_N) \tag{3.12}$$

i.e. the probability that component A_{N+1} fails given that components $A_1, \ldots, A_N$ have just failed due to a CCF. The probability that j out of N components have failed due a CCF is written as

$$g_{j,N} = P(A_1 \cap A_2 \cap \ldots \cap A_j \cap A^*_{j+1} \cap \ldots \cap A^*_N)$$

where A^*_j is the event that component j has **not** failed in a CCF. This indicates that the probability of exactly j out of N components fail in a CCF is

$$f_{j,N} = \binom{N}{j} g_{j,N} \tag{3.13}$$

We introduce a few new expressions, namely

Q	Failure probability of one component.
Q_{MooN}	The probability that a $MooN$ configuration is in a failed state.

Using Equation (3.13), the probability of a CCF for a $MooN$ system is

$$\begin{aligned} Q_{MooN} &= P(\text{at least } N - M + 1 \text{ components failed due to a CCF}) \\ &= \sum_{j=N-M+1}^{n} f_{j,N} \end{aligned} \tag{3.14}$$

The parameter C_{MooN} is introduced as a configuration factor which accounts for the architecture of the system in question. The probability that a $MooN$ configuration is in a failed state, is given as

$$Q_{MooN} = C_{MooN} \cdot \beta \cdot Q.$$

If the expression $G_{j,N} = \frac{g_{j,N}}{(Q\cdot\beta)}$ is introduced, we obtain

$$G_{j,N} = \frac{g_{j,N}}{(Q\cdot\beta)} = \sum_{i=0}^{N-j}(-1)^i \binom{N-j}{i} \prod_{l=2}^{j-1+i} \beta_l \tag{3.15}$$

for $M = 2,3,..,N$. This gives an explicit expression for the configuration factor C_{MooN}.

$$C_{MooN} = \sum_{j=N-M+1}^{N} \binom{N}{j} G_{j,N} \qquad \text{for } M = 1,2,...,M \tag{3.16}$$

The expression $G_{j,N}$ can be found recursively when starting with $G_{N,N} = \prod_{j=2}^{N-1} \beta_j$. Next it is possible to find $G_{j,N} = G_{j,N-1} - G_{j+1,N}$ for $j = N-1, N-2,...,1$. This approach, including examples, are studied in Hokstad et al. (2006). The expression for C_{MooN} is also available in an easier form, which is found in Hauge et al. (2006a), but that expression is derived from Equation (3.16).

3.5 IEC 61508

IEC 61508 (2000) is an international standard which is widely used when handling functional safety for SIS, and IEC 61508 (2000, Part 6) studies the concept of CCFs.

Failures in systems, and thus CCFs are assumed to arise from two different causes which are

- random hardware failures, and
- systematic failures.

Random hardware failures are caused by general wear and tear. These failures are assumed to occur independently of each other.

The systematic failures, however, may occur as a result of bad design or external stress, which in turn could lead to an early random hardware failure. Such failures are more likely to affect more than one component (in a multi-component system), so CCFs are likely to be a significant factor when addressing the SIL of such systems.

On a qualitative scale, the standard suggests three measures that can be made in order to reduce the probability of dangerous CCFs. These are

1. *Reduce the number of random hardware and systematic failures overall.*
2. *Maximize the independence of the components (separation and diversity).*
3. *Reveal non-simultaneous CCFs while only one, and before a second, component has been affected, i.e. use diagnostic tests or proof test staggering*[1].

Quantitatively, the standard suggests the use of the β-factor model, but states that for many redundant components, this may be inadequate.

[1] Staggered testing is explained in Rausand and Høyland (2004, Chapter 10.3.4)

3.6 The PDS method

Introduction

PDS is a Norwegian acronym for "Reliability and availability of computer based systems". The PDS method is developed for the Norwegian offshore industry, and it differs somewhat from the IEC 61508 standard. The method is considered to be realistic and relatively simple. The PDS method is described in two books published by SINTEF. Hauge et al. (2006a) contains both qualitative and quantitative tools in which to deal with reliabilities regarding safety instrumented systems and thus also common cause failures. Hauge et al. (2006b) contains a short description of the PDS method and how it differs from IEC 61508 (2000). It also contains estimated values for different parameters, such as failure rates (λ_{DU}s) and a few estimated βs to be used in CCF calculations.

Hauge et al. (2006a), which describes the PDS method, includes a classification of failures similar to that of IEC 61508 (2000), but it includes an expansion. This failure structure is found in Figure 3.4. It is assumed as a general rule that random hardware failures are denoted as independent failures while systematic failures may lead to CCFs. A more thorough description of

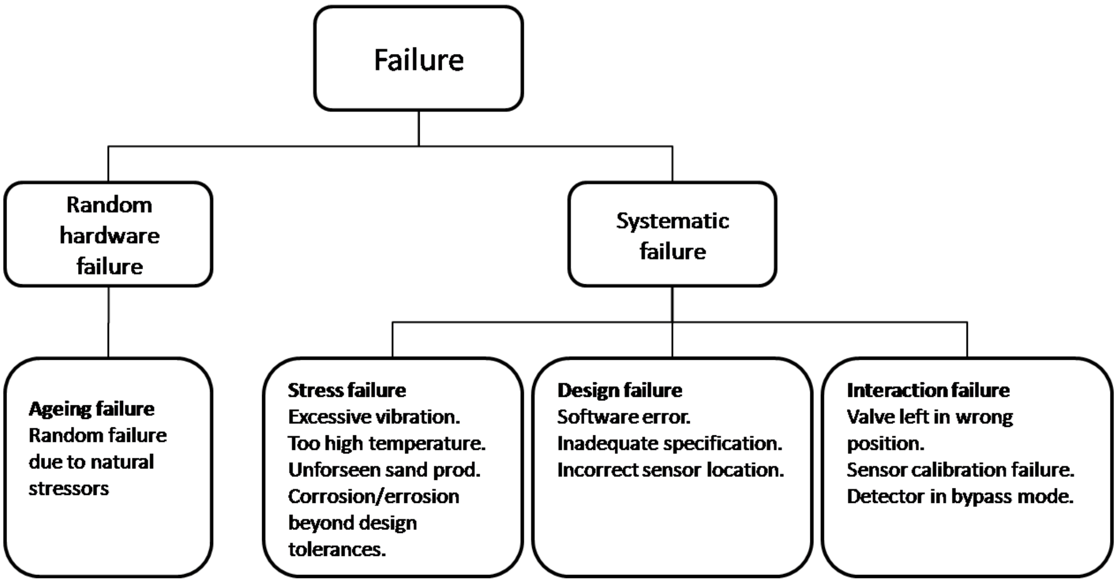

Figure 3.4: The failures considered in the PDS method. The systematic failures are divided into three groups and thus the method differs from the *IEC61508* approach.

the failure modes and what they imply is found in Hauge et al. (2006a).

IEC 61508 (2000, Part 6, Annex D) states that only random hardware failures should be quantified. The PDS method also includes the systematic failures even though they may be hard to predict. Systematic failures may for instance be detected by using automatic self-tests or through functional (manual) testing. This is further explained in Section 3.9.

The PDS method introduces something called the total critical safety unavailability (CSU_{TOT}) which is

> the total probability that the module/safety system will fail to automatically carry out successful safety action on the occurrence of a hazardous/accidental event.
>
> Hauge et al. (2006a)

The CSU_{TOT} is given as

$$CSU_{TOT} = PFD + P_{TIF} + DTU. \tag{3.17}$$

P_{TIF} is not included in the present report, but it is a measure describing the probability that the system will fail due to systematic, latent errors. DTU is briefly introduced in Section 3.9 and the DTU measures the "known" downtime unavailability. DTU_T is the planned downtime due to maintenance while DTU_R is the downtime caused by detected failures. DTU_T is not included in the present report and it is, as such, assumed that $DTU \approx DTU_R$.

The PFD, however, is given much attention in the preceding chapters.

PDS formulas

The PDS method applies the same calculations for CCFs as the MBF model discussed in Section 3.4. The PDS method accounts for different architectures with respect to CCFs. Opposed to the β-factor model given in Figure 3.3, the structure given in Figure 3.5 treats a $2oo3$ architecture different than a $1oo3$ architecture with respect to CCFs. The PDS method provides a formula for calculating the configuration factor C_{MooN}. This formula is a paraphrased version of the formulas obtained in Section 3.4. Assuming $\beta_k = \theta, k \geq 3$, the configuration factor is expressed as

$$C_{MooN} = \beta_2 \sum_{j=N-M+1}^{N} \binom{N}{j} \theta^{j-3}(1-\theta)^{N-j}, \qquad M = 1, 2, ..., N-2. \tag{3.18}$$

and

$$C_{(N-1)ooN} = \binom{N}{2}\left(1 - \frac{\beta_2}{\theta}\right) + \beta_2 \sum_{j=2}^{N} \binom{N}{j} \theta^{j-3}(1-\theta)^{N-j} \tag{3.19}$$

β_2 (and θ) is defined in Equation (3.12). A numerical table for C_{MooN} is presented with input values $\beta_2 = 0.3$ and $\theta = 0.5$ The same table is also presented in Hauge et al. (2006a).

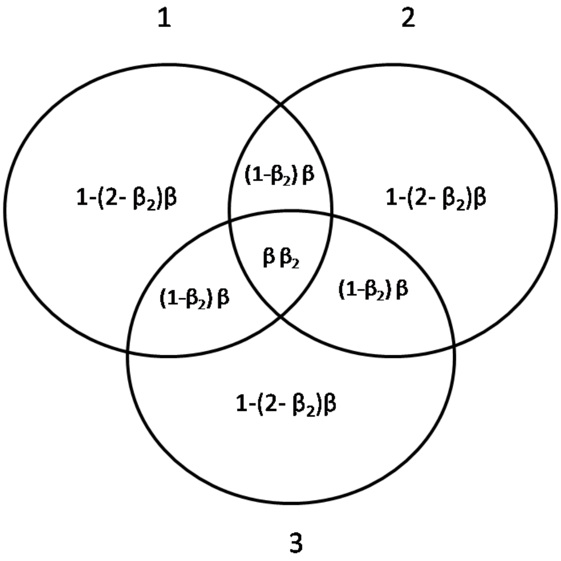

Figure 3.5: The PDS model for 3 components.

Table 3.1: A numerical table for the parameters C_{MooN}, C_N and H_N with $\beta_2 = 0.3$ and $\theta = 0.5$.

$\mathbf{C_{MooN}}$	$M = 1$	$M = 2$	$M = 3$	$M = 4$	$M = 5$	$\mathbf{C_N}$	$\mathbf{H_N}$
$N = 2$	1.00	–	–	–	–	1.0	1.0
$N = 3$	0.30	2.40	–	–	–	2.7	1.7
$N = 4$	0.15	0.75	4.00	–	–	4.9	2.2
$N = 5$	0.08	0.45	1.20	6.00	–	7.7	2.7
$N = 6$	0.04	0.26	1.60	1.60	8.10	10.8	3.2

Hauge et al. (2006a) calculates the PFD for the different voting logics. Using the simplified formulas derived in Section 2.4, the PFD as a consequence of CCFs for an $MooN$ architecture is

$$PFD_{ccf} \approx C_{MooN} \cdot \beta \cdot (\lambda_{DU} \cdot \frac{\tau}{2}), \qquad M < N \tag{3.20}$$

where C_{MooN} is a configuration factor that depends on the architecture. For the special case $M = N$, i.e. a $NooN$ structure, the expression becomes

$$PFD \approx N \cdot \lambda_{DU} \cdot \frac{\tau}{2}. \qquad M = N \tag{3.21}$$

Note that Equation 3.20 does not include independent failures. The contribution from independent failures is given as

$$PFD_{indep} = \frac{N!}{(N-M+2)! \cdot (M-1)!} \cdot (\lambda_{DU}^{(i)} \tau)^{N-M+1}, \qquad M < N; N = 2, 3, \ldots \tag{3.22}$$

Equation (3.21) includes both independent failures and CCFs since the system needs only one component to fail for an $NooN$ system to fail.

Recall that for the β-factor model, $\lambda_{DU}^{(i)} = (1-\beta)\lambda_{DU}$. For the PDS method the expression becomes slightly different with

$$\lambda_{DU}^{(i)} = (1 - H_N \beta)\lambda_{DU} \tag{3.23}$$

where H_N is given as

$$H_N = \frac{1}{N}\left(C_N + C_{(N-1)ooN}\right) \tag{3.24}$$

The term $C_{(N-1)ooN}$ is given in Equation (3.19) and C_N is

$$C_N = \sum_{M=1}^{N-1} C_{MooN}. \tag{3.25}$$

Table 3.1 provides values for both C_N and H_N.

3.7 Shock models

There are also other methods of treating CCFs which differ from the various β-factor models. Shock models, described by (Hokstad, 1988), is a slightly different approach. Three shock models, The Multinomial Failure Rate (MFR) model, The Binomial Failure Rate (BRF) model and The Random Probability Shock (RPS) model are discussed in the following sections.

3.7.1 The Multinomial Failure Rate model

In the MFR model, two different causes for failures exist. Components may fail individually, for instance from aging or other causes. The individual failure rate without specifying the type of failure, of component i, is denoted by $\lambda^{(i)}$. The system is also susceptible to shocks caused by external events. Such external shocks, denoted v, may cause damage to all the components in the system. There is a probability f_k that exactly k out of N components fail due to such a shock. The obvious bound

$$\sum_{k=1}^{N} f_k = 1$$

applies to these probabilities. Now it is possible to assign the rate for failures of exactly k components of the system s.

$$\begin{aligned} \lambda^{s(1)} &= N \cdot \lambda^{(i)} + v f_1 \\ \lambda^{s(k)} &= v f_k \qquad k = 2, 3, ..., N \end{aligned} \tag{3.26}$$

The total failure rate for one specific component i is

$$\frac{\lambda^{s(N)}}{N} = \lambda^{(i)} + \frac{v f_1}{N}$$

and the total rate of dependent failures, $\lambda^{(c)}$ is

$$\lambda^{(c)} = v \sum_k \frac{k}{N} f_k = \sum_k \frac{k}{N} \lambda^{s(k)}.$$

By adjusting the parameters in the MFR model, we are able to obtain both the β-factor model and the Greek letter model (Apostolakis and Moieni, 1987). An advantage when using the MFR model is the possibility of choosing the probabilities f_k so they fit observed data (if there is any).

3.7.2 The Binomial Failure Rate model

The Binomial Failure Rate Model (BFR) assumes that all components have the same probability p to fail in a shock. If a shock occurs, the components thus fail independently of each other. The number of failed components k is assumed to be binomially distributed with parameters p and N.

$$f_k = \binom{N}{k} p^k (1-p)^{N-k} \tag{3.27}$$

The rate at which shocks occur, is still v which provides

$$\lambda^{(c)} = vp$$

for the failure rate of a component with respect to shocks. The total failure rate of one component, when including the possibility of independent failures, is

$$\lambda = \lambda^{(i)} + vp$$

3.7.3 The Random Probability Shock model

As previously discussed, the β-factor model assumes that a CCF disables all components. Shocks are the equivalent to a CCF, but all components are not necessarily disabled by a shock. If a shock occurs when using the BFR model, components fail independently. Hokstad (1988) introduced a new model, the Random Probability Shock (RPS) model, which allows for various degrees of dependency between the components. In fact, the β-factor model and the BFR model are special (extreme) cases of the RPS model.

The RPS model assumes that the parameter p in the BFR model is itself a random variable with a probability distribution. This follows from the assumption that p may vary from shock to shock. It is further assumed that p is beta-distributed as follows.

$$g(p) = \frac{\Gamma(r+s)}{\Gamma(r)\Gamma(s)} p^{r-1}(1-p)^{s-1} \tag{3.28}$$

r and s are parameters which can be estimated from a suggested mean and variance (Rydén and Rychlik, 2006, Chapter 6). Further, it is assumed that x conditioned on a certain p, i.e. $f(x|p)$, has a binomial distribution. By integrating out p we are able to obtain the unconditional probability distribution for $f(X=x)$

$$f(X=x) = \binom{N}{x} \frac{\Gamma(r+s)\Gamma(x+r)\Gamma(N-x+s)}{\Gamma(r)\Gamma(s)\Gamma(r+s+N)} \tag{3.29}$$

This gives the RPS model, and information is only needed about the parameters r and s. Hokstad (1988) also presents a different parametrization which is more comprehensible. By introducing the two new parameters

$$O = \frac{r}{r+s} \qquad \text{and} \qquad D = \frac{1}{r+s+1}$$

we acquire a more understandable model since O is the probability that a component fail due to a shock averaged over all possible shocks, and D describes the correlation between the different components with respect to shocks. If $D = 1$ and a shock occurs, all components share the same fate, i.e. if one component fails, all fail. The situation $D = 1$ equals the β-factor model. If a shock occurs with the other extreme, $D = 0$, components fail independently, i.e. as in the BFR model.

Failure rates for failures of multiplicity k is

$$\lambda(1) = \quad N \cdot \lambda_i + \nu f_1 \tag{3.30}$$

$$\lambda(k) = \quad \nu \cdot f_k \tag{3.31}$$

Another method which could be modified to include the different "environments" the components were exposed to is given by Hughes (1987). As elegant as this method is mathematically speaking, it requires information about the system which is rarely available and is thus not given further attention in the present report.

3.8 Markov analysis

Markov analysis represents a different angle of reliability modelling for SIS. A complete introduction to Markov models is considered too extensive to be given in this report, but certain concepts relating to CCFs are explained. An advantage when using Markov models is the great diversity these methods are able to provide. It is possible to model different repair strategies and fairy dynamic models while the downside is the complexity which becomes evident when the number of components increases. For instance, if the model includes both DD- and DU-failures, the number of states are nearly doubled. For each state or component susceptible to both dependent and independent failures, we need one state for detected failures and one for undetected failures.

Much focus has previously been given to model production systems, like for instance pumps or generators which keep production going (Rausand and Høyland, 2004). These systems (or components of the system) fail at a certain rate and are repaired again at another rate. This is somewhat different when dealing with DU-failures where all repairs are performed at regular time intervals τ.

As such, this report will focus mostly on DU-failures when dealing with Markov analysis. When dealing with DU failures, the system is repaired at regular time intervals τ and not at once. In order to be able to model this by a Markov model, the repair rate is given as the mean downtime $E(D)$ in a test interval$[t, t+\tau]$. A derivation of this formula is found in Rausand and Høyland (2004, Chapter 10) and the result is approximated with

$$E(D) = \frac{\tau}{F(\tau)} \cdot PFD. \tag{3.32}$$

When the repair rate is found by using Equation (3.32), the system can be modelled by using standard Markov analysis. By observing Equation (3.32), much information is needed in order to calculate $E(D)$. We will for instance need to calculate the PFD before it is possible to describe the repair rate. This makes this strategy complicated so it is not pursued further.

It is possible, however, to use Markov analysis to obtain the PFD directly. As explained in ISA (2002, Part 4), it can even be done in two different fashions. One way is to transform the rates into discrete time steps, while the other solves the differential equations which follow directly.

3.8.1 The Matrix Multiplication method

The first approach, named the Matrix Multiplication method is by far the most practical for large systems. This method transforms the rates into discrete time-steps and calculates the PFD directly. In order to illustrate, an example is employed.

Example 2.
We have a system of two identical components in parallel that are also exposed to CCFs. Only DU-failures are included when working with the following example. Assuming the Markov property

Table 3.2: The different states in which the system may reside for the $1oo2$ system.

Assigned number	Condition
1	Both components are able to function.
2	One component has failed while the other works.
3	Both components have failed.

holds, and also assuming the system is as good as new following a periodic inspection at time τ, the following numerical values are given.

$$\begin{aligned}\lambda_{DU} =& 1.0 \cdot 10^{-6}\ hours^{-1}\\ \beta =& 0.05\\ \tau =& 8760\ hours\\ \Delta t =& 1\ hour\end{aligned} \tag{3.33}$$

The $1oo2$ system with periodic repair may reside in 3 possible states. These states are given in Table 3.2. Based on the states in Table 3.2, we construct the transition diagram given in Figure 3.6. The next step is to construct a transition matrix which includes the rates in Figure 3.6. In order to make the system more suitable for reliability calculations , we "transfer" the rates in Figure 3.6 into probabilities. This is done by multiplying the rate by an interval Δt, with Δt small enough so that the probability of multiple failures within same the interval can be neglected. For calculation simplicity, the value $\Delta t = 1$ hour is chosen[2]. This procedure means that we move from continuous time Markov analysis to discrete time Markov analysis.

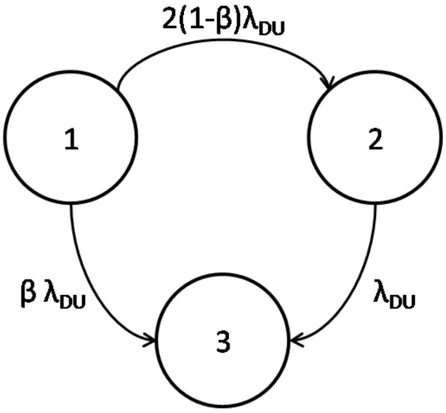

Figure 3.6: Transition diagram for a system of two identical components which are also exposed to CCFs.

[2] $\Delta t = 1$ hour is coincident with ISA (2002)

Transferring the values from Figure 3.6 when including Δt and making sure the diagonal is one minus the rest of the current row, the transition matrix becomes.

$$\mathbf{T} = \begin{pmatrix} 1-(2-\beta)\lambda_{DU}\Delta t & (2(1-\beta)\lambda_{DU})\Delta t & \beta\lambda\Delta t \\ 0 & 1-\lambda_{DU}\Delta t & \lambda_{DU}\Delta t \\ 0 & 0 & 1 \end{pmatrix} \tag{3.34}$$

If we assume that both components are able to function when put into operation, i.e. $P(0) = [1,0,0]$*, the probability of the system being in either state* 1, 2 *or* 3 *at time t is given by*

$$\mathbf{P}(t) = \mathbf{P}(0)\mathbf{T}^t. \tag{3.35}$$

The value $\mathbf{T}^t$ *is in practice impossible to calculate by hand for large values of t, for instance* $t = \tau$*, but it is easily obtained by using a computer. For the present example, we obtain*

$$\mathbf{P}(\tau) = \left[9.831 \cdot 10^{-1}, 1.643 \cdot 10^{-2}, 5.065 \cdot 10^{-4}\right]$$

which is the probability of the system being in state 1, 2 *or* 3 *at time* τ.

The average PFD is, which is the measure of interest, is

$$PFD = \frac{1}{\tau}\int_0^\tau P_3(t)dt \tag{3.36}$$

Since state 3 equals the fact that the system is down, the PFD is obtained when studying the mean time spent in this state. The value is obtained through numerical integration, namely having a computer calculate $P_3(t)$ *for all* $t \in (0,\tau)$.

$$PFD = \frac{1}{\tau}\sum_{t=1}^{\tau} P_3(t) = 2.42 \cdot 10^{-4} \tag{3.37}$$

The MTTF can be found by applying the Fourier analysis-method suggested in Rausand and Høyland (2004, Chapter 8). This derivation is not included in the present thesis, but the result is

$$MTTF = \frac{3-2\beta}{(2-\beta)\lambda_{DU}} \tag{3.38}$$

Markov models are also easily applied when dealing with detected failures and the repair rate is known as is usually the case for production systems, i.e. not SIS. There is a lot of literature dealing with such cases, for instance Rausand and Høyland (2004, Chapter 8) or Ross (2003). The aim of the previous example was to apply Markov analysis through a less common approach.

A similar introduction to the one presented in the current section which follows the same principles as Example 2 is given in Bukowski and Goble (1995). In that paper the flexibility of Markov methods is argued, and it is also stated that the ISA 84.02 subcommittee has chosen Markov analysis as the preferred technique for safety and availability evaluation.

3.8.2 The differential equations method

The system given in Example 2 will now be solved without transforming the failure rates into discrete probabilities. The method applies the continuous rates directly and thus makes less assumptions than the previous one. An example of the same manner is given in ISA (2002, Part 5) but in that example, the differential equations are solved by making use of the Laplace transformation (Rausand and Høyland, 2004, Appendix B). In the present paper, however, the differential equations are solved directly.

At time $t = 0$, we know that the system is in state 1, i.e. $P_1(t = 0) = 1$. In addition we are aware of the fact that

$$P_1(t) + P_2(t) + P_3(t) = 1, \tag{3.39}$$

i.e. the process must always be in one of the three states. We are thus able to use the state-equations derived from the Kolmogorov forward equations found in Rausand and Høyland (2004, p. 312) or Ross (2003, p. 367). The steady state equation is for state j, assuming we have r different states, given as

$$\frac{dP_j(t)}{dt} = \dot{P}_j(t) = \sum_{k=1}^{r} a_{kj} P_k(t) \tag{3.40}$$

where a_{kj} is the rate at which the system goes from state k to j. For $k = j$, a_{jj} becomes

$$a_{jj} = \sum_{\substack{i=0 \\ i \neq j}}^{r} -a_{ji}.$$

By applying Equation (3.40) to the components in Figure 3.6, we obtain the following equations

$$\dot{P}_1(t) = -(2-\beta)\lambda_{DU} \cdot P_1(t) \tag{3.41}$$

$$\dot{P}_2(t) = 2(1-\beta)\lambda_{DU} \cdot P_1(t) - \lambda_{DU} \cdot P_2(t) \tag{3.42}$$

$$\dot{P}_3(t) = \beta\lambda_{DU} \cdot P_1(t) + \lambda_{DU} \cdot P_2(t) \tag{3.43}$$

Since we have three unknowns, we need only chose two of the above equations in addition to Equation (3.39). Equation (3.41) is solved easily, and when also applying the fact that $P_1(t = 0) = 1$ we obtain

$$P_1(t) = e^{-(2-\beta)\cdot\lambda_{DU}\cdot t} \tag{3.44}$$

We now choose to solve Equation (3.42). This equation is more complicated so we apply a technique called “an integrating factor”. For this linear first order differential equation, we want the left side of the equation to be equal to the derivative of a product. This technique is described in several introductory calculus books, e.g. Edwards and Penny (1990).

With this in mind the equation is rearranged, the value for $P_1(t)$ obtained in Equation (3.44) is inserted, and the expression is multiplied by $e^{\lambda}_{DU} \cdot t$. This gives

$$e^{\lambda_{DU}\cdot t} \cdot \dot{P}_2(t) + e^{\lambda_{DU}\cdot t} \cdot \lambda_{DU} \cdot P_2(t) = e^{\lambda_{DU}\cdot t} \cdot 2(1-\beta) \cdot \lambda_{DU} \cdot e^{-(2-\beta)\cdot\lambda_{DU}\cdot t}$$

The left side of the equation is now the derivative of a product, and after integrating with respect to t on both sides, we obtain

$$e^{\lambda_{DU}\cdot t}P_2(t) = -2\cdot e^{-(1-\beta)\lambda_{DU}\cdot t} + C,$$

where C is an integrating constant we need to determine. It is assumed that the system is as good as new at time $t = 0$ which makes $P_2(t = 0) = 0$. Isolating the $P_2(t)$-term on the left side of the equation, we are finally able to obtain $P_2(t)$.

$$P_2(t) = 2\left(e^{-\lambda_{DU}\cdot t} - e^{-(2-\beta)\lambda_{DU}\cdot t}\right) \tag{3.45}$$

$P_3(t)$ is found by inserting the values for $P_1(t)$ and $P_2(t)$ into Equation (3.39). This produces the estimate

$$P_3(t) = 1 - 2\cdot e^{-\lambda_{DU}\cdot t} + e^{-(2-\beta)\lambda_{DU}\cdot t}. \tag{3.46}$$

The average PFD is calculated by taking the average of $P_3(t)$ over the time interval $(0,\tau)$ and using λ_{DU} from Equation (3.33) . This gives

$$PFD = 2.42\cdot 10^{-4}. \tag{3.47}$$

The result obtained through this approach is equal (within a factor of 10^{-6}) to that of Equation (3.37). At least for the studied example, we may "safely" use the discrete-time approximation instead of the differential equations. The discrete-time approximation is also used in the following chapters and the this approximation is assumed to provide sufficient results. The same approximation is also assumed throughout ISA (2002, Part 4). Figure 3.7 shows the difference of $PFD(t)$ for each t in the interval $(0,\tau)$ of the two methods. As seen, the difference between the two methods are in the order of 10^{-9}.

3.9 Non-negligible repair time and diagnostics testing

The current section explains a bit closer the difference between DU-failures and DD-failures and the tools which are being used to detect some of the failures, namely diagnostics testing. In the previous chapters, it has been assumed that $MTTR << \tau$. This consequently leads to the fact that detected failures are ignored. We now address the case where DD-failures are not neglected.

Including diagnostics testing

Many different SIS have a "built-in" diagnostics system which frequently perform tests. This comes in addition to the periodic tests performed at time $x\cdot\tau$ for $x = 1,2,...$. These diagnostic safe-tests are performed frequently and are assumed to discover a certain percentage of the failures. This is called diagnostic coverage (DC). Applying the DC is done straight forward by adding the term to the failure rate.

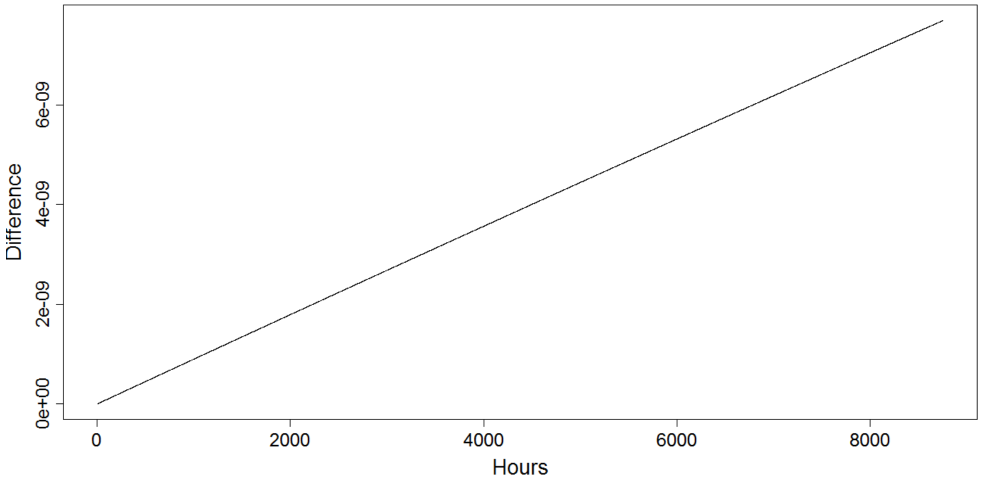

Figure 3.7: The difference obtained for $PFD(t)$ when applying the matrix multiplication method and the differential equation method, i.e. $PFD_{\text{Matrix multiplication method}}(t) - PFD_{\text{Differential equations method}}(t) \propto 10^{-9}$.

Both Hokstad (2005) and IEC 61508 (2000, Part 6) give examples of diagnostics testing. The concept is handled slightly different in the two literatures, so the main concept of both are given below. IEC 61508 (2000) operates with the diagnostic coverage

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC); \qquad \lambda_{DD} = \frac{\lambda}{2}DC.$$

When dealing with CCFs, (IEC 61508, 2000) introduces β_D to account for the detected common cause failures. In addition if the repair time is not neglected, the mean time to repair must be included, i.e. $MTTR$ must be included in the PFD calculation for detected failures.

The PDS method (Hauge et al., 2006a, Appendix E) does not use the notation β_D, only the standard β. Instead it includes the possibility for different diagnostic coverage with respect to individual failures and CCFs. This makes the rate for DU failures

$$\begin{aligned} \lambda_{DU}^{(i)} &= (1 - DC^{(i)}) \cdot (1 - \beta) \cdot \lambda_D \\ \lambda_{DU}^{(c)} &= (1 - DC^{(c)}) \cdot \beta\lambda_D \end{aligned} \tag{3.48}$$

We observe that this is a way to calculate the fraction λ_{DU} of λ_D. The remaining part thus makes up λ_{DD}, i.e. dangerous failures which are detected in a diagnostic test. For systems with very good DC, most dangerous failures are DD-failures and only a small part are DU-failures. For more on this topic, there is an introduction given in Rausand and Høyland (2004, Chapter 10).

Non-negligible repair time

We now investigate the case where we do not disregard DD-failures, but include these in the reliability calculations. Both IEC 61508 (2000, Part 6) and Hauge et al. (2006a) give examples on how to treat these types of failures, and the main difference between the two is that the PDS method includes the specific voting logic while the IEC-method does not. In addition, the PDS method separates the expressions so that the contribution obtained from when repairing DD-failures, called Downtime Unavailability (DTU_R), is calculated separately.

This separation makes, according to the author's opinion, the procedure much more surveyable and is therefore chosen in the present report. The PFD is calculated normally, but in addition an additional term, DTU_R, is included.

If a DD-failure occurs in a safety system, we are aware of this fact, and in some cases the system may be shut down or put into a safe state at once. In some situations, however, this is either impossible (an airplane in the air), or it is considered to be too expensive. If the SIS has good redundancy the system is still able to provide safety even though some components have failed due to a DD-failure. For instance if we have a $1oo2$ system, and one component is being repaired due to a DD-failure, the system is still able to perform its designated function since one component is functional. A DU-failure to the component not being repaired component, however, would leave the system unable to function if a demand occurs. If DD-failures occur to both components of a $1oo2$ safety system, one would be wise to shut down the operation since the system is unprotected if a demand occurs. Consequently it is assumed that if a DD-failure occurs in a $NooN$ system, operation is shut down until the failure is repaired.

If given an $MooN$ system and the aim is to calculate the DTU_R, we need to include the fact that a DD-failure has occurred AND the possibility of DU failures disabling the rest of the $Moo(N-1)$ system. Naturally, the DU-failures must occur while the DD-failed component is under repair, i.e. in a time interval of length $MTTR$. For a $1oo2$ system, we thus have

$$DTU_R = 2\lambda_{DD} \cdot MTTR \cdot \lambda_{DU} \cdot \tau/2 \tag{3.49}$$

which is the probability that a DD failure has occurred multiplied by the PFD of a $1oo1$ system.

If we have a $2oo3$ system and a DD failure occurs, we now have a degraded $2oo2$ system which handles the safety function. DTU_R is now the probability that a dangerous failure has occurred, multiplied with the PFD for a $2oo2$ system.

$$DTU_R = 3\lambda_{DD} \cdot MTTR \cdot \lambda_{DU} \cdot \tau. \tag{3.50}$$

As Hauge et al. (2006a) points out, certain $2oo3$ systems may be designed to function as $1oo1$ system and is able to provide safety even though two components have failed due to DD-failures. Such systems are, however, not given any attention in the present report. Also, we do not include a CCF-term for the DD-failures since we assume the strategy that if all components fail due to DD-failures, production is shut down since the safety system is no longer able to provide protection.

If deemed possible, Equation (3.50) also allows for different failure rates for DU failures when a DD-failure has occurred. It may for instance be that if a repair crew is working on repairing one component, they are more aware of DU-failures on the remaining. Consequently, λ_{DU} is in reality lower in the time interval of repair. The other case may also be true. By repairing one component, the remaining components are more vulnerable to damage during this time interval. This is an issue which has to be assessed for the specific system and not on a general basis.

In order to illustrate this concept and what sort of numerical values we may expect, we make us of an example where we include DD-failures. The values for λ_{DD} and λ_{DU} are obtained from Hauge et al. (2006b).

Example 3.
We assume we have two pressure switches connected in parallel which are also subject to CCFs. Yearly inspections are performed, and the system is assumed to be as good as new following such an inspection. If a DD-failure is discovered, repair is commenced and the mean time to repair MTTR is assumed to be significant. If we consider the following numerical values,

$$\begin{aligned}\lambda_{DU} =& 1.6\cdot 10^{-6}\ hours^{-1}\\ \lambda_{DD} =& 0.7\cdot 10^{-6}\ hours^{-1}\\ \beta =& 0.02\\ MTTR =& 730\ hours\\ \tau =& 8760\ hours,\end{aligned} \tag{3.51}$$

we see that the mean time to repair is one month. The CSU_R is found by inserting the numerical values into Equation (3.49). This gives

$$DTU_R = 2\cdot 0.7\cdot 10^{-6}\cdot 730\cdot 1.6\cdot 10^{-6}\cdot 8760/2 \approx 7.16\cdot 10^{-6} \tag{3.52}$$

We observe that, the total PFD for the entire system is

$$PFD = \frac{\left((1-\beta)\lambda_{DU}\cdot\tau\right)^2}{3} + \frac{\beta\cdot\lambda_{DU}\cdot\tau}{2} \approx 2.03\cdot 10^{-4} \tag{3.53}$$

which is large (28 times larger) in comparison. (CSU_{TOT}) is thus given as

$$CSU_{TOT} = PFD + DTU_R = 2.03\cdot 10^{-4} + 7.16\cdot 10^{-6} \approx 2.10\cdot 10^{-4}. \tag{3.54}$$

Note If we want to calculate the DTU_R for a $2oo4$ system, we must include the possibility of one DD-failure and two DD-failures and the two degenerated systems respectively

$$\begin{aligned}DTU_R =& P\left(0 \text{ components have failed due to a DD-failure}\right)\cdot 4\lambda_{DD}\cdot MTTR\cdot PFD_{2oo3}\\ &+P\left(1 \text{ component has failed due to a DD-failure}\right)\cdot 3\lambda_{DD}\cdot MTTR\cdot PFD_{2oo2}\end{aligned} \tag{3.55}$$

where PFD_{2oo3} and PFD_{2oo2} are the PFD a $2oo3$ and a $2oo2$ architecture, respectively. The first term of Equation (3.55) is usually the most dominant since the probability of 0 components having failed due to DD-failure is usually much greater than the probability of one component having failed.

3.10 Summarizing the derived models

The models that are derived in the present chapter, are all applied in reliability analysis to a greater or lesser degree. For instance the Square-Root method (NUREG-75/014, 1975) is not widely used today because of the lacking proper mathematical foundation and its limited area of application.

The shock models are thoroughly derived (Hokstad, 1988), but these models are not widely used in practice today. Initial information is needed about the shock-rate and the probability of different components being disabled if a shock occurs. Such information is usually not available, and this makes the simpler models more preferable.

The β-factor model is the most popular model today, and the simplicity of the model contributes to this fact. Since this model is widely used, a lot of data has been collected to describe the input parameters λ and β, e.g. OREDA (2002). The β-factor model is assumed to be adequate for $1oo2$ systems but it is insufficient for systems with $N > 2$.

For larger, more complicated systems, a slightly more complicated model is preferred. The PDS method is built on the same foundation as the β-factor method, and in addition it accounts for different architectures, i.e. different Ms in $MooN$ architectures. This is a well documented method which is widely used in the offshore industry, (Hauge et al., 2006a). The PDS method also uses the same input values as the β-factor model and should thus be considered as a better alternative for large $MooN$ systems where little information is provided. Exceptions may naturally be made if expert knowledge leads one to believe that when a CCF occurs, all components will always be disabled.

Markov analysis is yet another approach, slightly more complicated than the aforementioned. It is highly capable of modelling a variety of systems, and it is the preferred method of the standard ISA (2002). In addition to $MooN$ systems, the method is also highly capable of modelling more advanced systems. Two alternative derivations were introduced in Section 3.8, and for the purpose of reliability analysis we saw in Section 3.8 that the matrix multiplication method is, at least for the studied example, by far adequate.

Markov analysis is slightly more complicated than the β-factor model and the PDS method, but when using the matrix multiplication method we have seen that it is quite straight-forward. It is, however, not very complicated when using the matrix multiplication method. In addition, some approximation formulas for the PFD, analogous to the approximation formulas of Section 2.4, are introduced in Bukowski (2005). Markov analysis may also be applied when dealing with systems of repairable components, and the repair time is assumed **not** to be exponentially distributed. Bukowski (2006) addresses this issue.

Part II

Assessing specific systems with respect to CCF modelling

Introduction

The present part discusses working examples where CCF modelling is applied. The examples are collected from actual systems, and an estimate for the PFD when including CCFs is needed. The presented examples are quite different in architecture and functionality, and this is done on purpose in order to show which strategy is best suited to model different types of problems.

For the different examples, numerous methods are applied, and because of the lack of feedback data it is difficult to claim that some results are more accurate than others. It is, however, possible to investigate how the results differ when using different methods and then assess this variation.

The following examples include most of the methods given in Chapter 3, but not all. For instance, the Square-Root method was included to illustrate the first attempts of modelling CCFs and will not be included in the examples of Part II.

Necessary assumptions for Part II

A few assumptions are needed when calculating the PFD for the following examples. Some of these assumptions are already mentioned when deriving the formulas. These and other assumptions are summarized in the current section.

For all models

- The failure rates of all components are assumed constant with respect to time.
- Reparations occur at time intervals τ, and all components are assumed to function as good as new following a repair.
- The test period at time τ, and eventual repairs, are assumed to be short compared to τ and is thus neglected.
- The state of one component is independent from the state of the others, i.e. if one component fails, this will not affect the other components. (This can be modified when using Markov models).
- DD-failures are assumed not to contribute to the safety unavailability either because $MTTR << \tau$ or the system is placed in a safe state if a DD-failure occurs. (This assumption is not included in Section 3.9.)
- If a SIS consists of more than one SIF, the PFD is calculated separately for each SIF.
- All the systems in the following examples are systems working in a low demand mode (see Section 2.1).

For the PDS method and the β-factor model

- The PFD formula given in Section 2.4 is assumed, i.e. $\lambda_{DU} \cdot \tau$ is small enough to allow $e^{\lambda_{DU} \cdot \tau} \approx 1 - \lambda_{DU} \cdot \tau$. For this assumption to be valid we must, according to Hauge et al. (2006a), have $\lambda_{DU} \cdot \tau \leq 0.2$.
- The contributions from different PFD-terms, for instance PFD_{ccf} and PFD_{indep} are assumed to be small enough for $1 - (1 - PFD_{ccf}) \cdot (1 - PFD_{indep}) \approx PFD_{ccf} + PFD_{indep}$.

For Markov analysis

- The Markov assumption is assumed to hold, i.e. the probability of in which state the system resides in the next time step $(t + \Delta t)$, depends on the current time step only (t) and is independent of previous ones $(t - x \cdot \Delta t$ for $x = 1, 2, 3, ...)$.
- The fail states are absorbing states, i.e. when the system has failed, it stays failed until it is repaired at time τ.

Chapter 4

A system to detect low oil pressure

Consider a function designed to detect if lube oil pressure is low. The architecture of this function given in Figure 4.1 and it consists of four components and one logic unit. The logic unit also activates an actuating item, but this is not included here. Components 1 and 2 are in a parallel structure, called an inner system, while components 3 and 4 are connected in parallel to the inner system. The logic unit shuts down the system if it receives 2 warnings of low lube oil pressure. Component 1 is a pressure detector, while components 2, 3 and 4 are pressure switches. The logic unit is assumed to work perfectly.

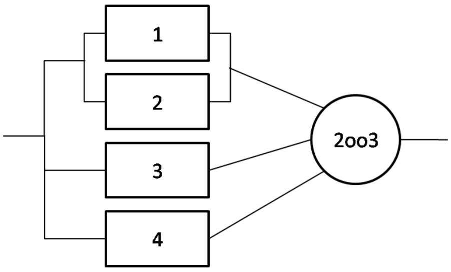

Figure 4.1: A system designed to detect if lube oil pressure gets low.

4.1 Applying the β-factor model

The current architecture can not be treated as a normal $2oo3$ system since components 1 and 2 are in a separate parallel structure. To that end, we define two concepts which are used in the present Chapter.

- Inner system: Components 1 and 2 in a parallel ($1oo2$) structure.

- Outer system: The total 2*oo*3 system in which the inner 1*oo*2 system is treated as a single component.

For the present system testing is conducted once a year, i.e. $\tau = 8760$ hours, and the different λs are

$$\begin{aligned}\lambda^{(1)} =& 1.7\cdot 10^{-6} \text{ hours}^{-1}\\ \lambda^{(2)} =& 6.0\cdot 10^{-6} \text{ hours}^{-1}\\ \lambda^{(3)} =& 3.4\cdot 10^{-5} \text{ hours}^{-1}\\ \lambda^{(4)} =& 3.4\cdot 10^{-5} \text{ hours}^{-1}.\end{aligned}$$

Component 3 and 4 are identical, while 1 and 2 are different. We assume that both the inner and outer systems are prone to CCFs. It is possible that the inner system fails due to a CCF without disabling the functionality of the system. It is also possible to have a CCF when looking at the outer system, i.e. treating the inner system as **one** component. A CCF on the outer system could knock out components $\{1,2,3\}$, $\{1,2,4\}$, $\{3,4\}$ or $\{1,2,3,4\}$. The fraction of failures that are caused by a CCF is assumed to be 5%, i.e. $\beta = 0.05$.

The inner system

The purpose of the current Section is to find the failure rate function $z(t)$ for the inner system when including CCFs and then using this information to evaluate the PFD for the outer system.

The inner system consists of two components in parallel and a CCF term. This is essentially the same system as the one given in Figure 3.2. The only difference in the present case is the different failure rates, i.e. $\lambda^{(1)} \neq \lambda^{(2)}$. According to Hauge et al. (2006a, Appendix D), this problem can be solved by using the geometric mean of the λs. This gives the failure rate for the inner system as $\lambda^{(is)} = \sqrt{\lambda^{(1)}\cdot\lambda^{(2)}}$.

The failure rate function is defined by its survivor function as

$$z(t) = -\frac{\frac{d}{dt}R(t)}{R(t)} \tag{4.1}$$

The survivor function is similar to the one found in Equation 3.9, with $\lambda^{(is)}$ instead of λ. After differentiating $R(t)$, inserting the expression into Equation 4.1 and simplifying the result slightly, we obtain the failure rate for the inner system

$$z(t) = \frac{\lambda^{(is)}\left(2-(2-\beta)e^{-(1-\beta)\lambda^{(is)}t}\right)}{2-e^{-(1-\beta)\lambda^{(is)}t}} \tag{4.2}$$

This function is a monotonely increasing function and taking the limit yields

$$\lim_{t\to\infty} z(t) = \lambda^{(is)}.$$

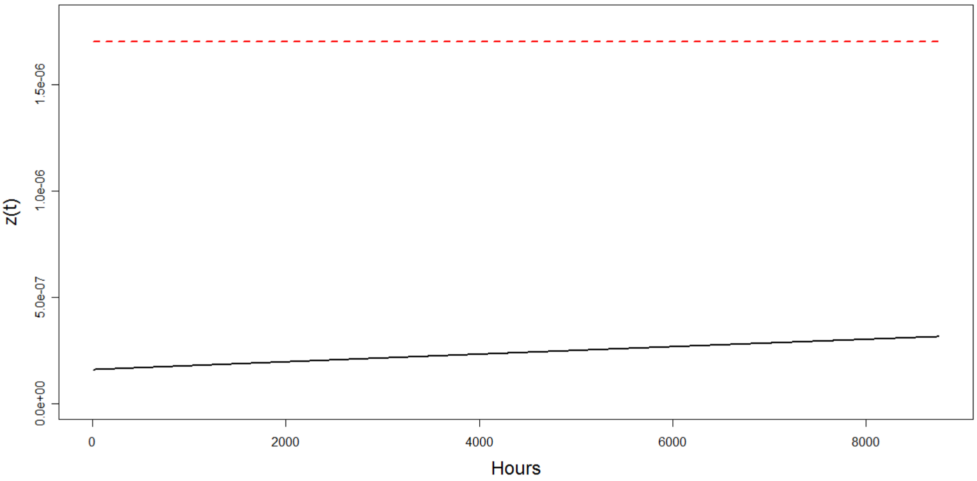

Figure 4.2: Plot of the failure rate function $z(t)$ for the inner system (solid-drawn line) and the independent failure rate for component 2 (dotted line).

This function increases very slowly, and with $\beta = 0.05$ and $\tau = 8760$ hours, $z(\tau)$ is nowhere near its limit. For the period of one year, $z(t)$ is not even close to $\lambda^{(1)} = 1.7 \cdot 10^{-6}$, the more reliable of the two components. This can be observed in Figure 4.2. The function $z(t)$ reaches its maximum at $t = \tau$, and the maximum value is

$$z(\tau) = 3.15 \cdot 10^{-7} \text{ hours}^{-1}. \tag{4.3}$$

The complete failure rate function in Equation 4.2 is too complex to be used in practical applications when calculating the PFD for the outer system. It is, however, required that an estimate is used. Naturally one could use the conservative estimate obtained in Equation (4.3), but since the estimate of interest is the average PFD, the average value for $z(t)$ over the time interval $(0, \tau)$ is used. This gives

$$z_{mean}(t) = 2.38 \cdot 10^{-7} \text{ hours}^{-1}. \tag{4.4}$$

The outer system

We are now faced with a normal 2$oo$3 system which is prone to CCFs. At least two obvious methods present themselves for calculating the PFD. The β-factor method and the PDS method. The failure rate for the outer system is, as previously, assumed to be the geometric mean of the failure rates of the three components [2]. This yields

$$\lambda^{(os)} = \left(\lambda^{(is)} \cdot \lambda^{(3)} \cdot \lambda^{(4)}\right)^{\frac{1}{3}} = 6.51 \cdot 10^{-6} \text{ hours}^{-1} \tag{4.5}$$

The β-factor model does not differ between a $2oo3$ voting and a $1oo3$ voting with respect to CCFs. The PFD is calculated by assuming that a hypothetical CCF term is connected in series with the $2oo3$ architecture. By making use of Table 2.2, we obtain

$$\begin{aligned} PFD &= \frac{\beta\lambda^{(os)}\tau}{2} + ((1-\beta)\lambda^{(os)}\tau)^2 \\ &= 1.42 \cdot 10^{-3} + 2.93 \cdot 10^{-3} \\ &= 4.36 \cdot 10^{-3} \end{aligned} \tag{4.6}$$

For a $2oo3$ system, the survivor function is given as

$$R_{2oo3}(t) = 3e^{-(2-\beta)\lambda t} - 2e^{-(3-2\beta)\lambda t}. \tag{4.7}$$

The mean time to failure is thus

$$MTTF = \int_0^\infty R_{2oo3}(t)dt = \frac{3}{(2-\beta)\lambda} - \frac{2}{(3-2\beta)\lambda}. \tag{4.8}$$

Using $\lambda = \lambda^{(os)}$ and $\beta = 0.05$, the mean time to failure is

$$MTTF = 130460 \; hours \tag{4.9}$$

4.2 The PDS approach

By investigating Figure 4.1, we see that the system is in a failed state if three components fail, regardless of which components fail. The system is also in a failed state if component 3 and 4 fail, but any other of the five possible combinations of two failed components will not disable the system. This means that if two components fail, the system fails with probability $\frac{1}{6}$. The system can thus be treated as a $3oo4$ system with probability $\frac{1}{6}$ and a $2oo4$ system with probability $\frac{5}{6}$. The PFD for DU failures with respect to CCFs, PFD_{ccf} is

$$PFD_{ccf} = (\frac{1}{6}C_{3oo4} + \frac{5}{6}C_{2oo4}) \cdot \frac{\beta\lambda_{DU}\tau}{2}. \tag{4.10}$$

For the current system we have $\beta = 0.05$, $\tau = 8760$ hours and $\lambda_{DU} = (\lambda^{(1)} \cdot \lambda^{(2)} \cdot \lambda^{(3)} \cdot \lambda^{(4)})^{\frac{1}{4}} = 1.04 \cdot 10^{-5}$ hours^{-1}, and the values for C_{MooN} are given in Table 3.1. This provides the estimate

$$PFD_{ccf} = 2.94 \cdot 10^{-3} \tag{4.11}$$

[2] The inner system treated as a component and components 3 and 4.

The contribution from independent failures is calculated as in Section 3.6. Firstly, we need to obtain $\lambda_{DU}^{(i)}$, and by using values given in Table 3.1, we have

$$\lambda_{DU}^{(i)} = (1 - H_N\beta)\lambda_{DU} = 9.256 \cdot 10^{-6} \text{ hours}^{-1}$$

Proceeding similarly as in Equation (3.22) yields,

$$PFD_{indep} = \frac{1}{6}\frac{4!}{3! \cdot 2!}(\lambda_{DU}^{(i)}\tau)^2 + \frac{5}{6}\frac{4!}{4! \cdot 1!}(\lambda_{DU}^{(i)}\tau)^3 = 2.64 \cdot 10^{-3}. \tag{4.12}$$

The total PFD is thus

$$PFD = PFD_{indep} + PFD_{ccf} = 5.58 \cdot 10^{-3} \tag{4.13}$$

As shown, the PDS method modifies the β-factor model. For further reading, an example with 3 components in parallel is given in Hokstad et al. (2006).

4.3 A shock model approach

In addition to the two preceding models, the shock model approach is also applied to the inner system. For the shock model approach, it is assumed that a shock occurs according to a Poisson process with rate $\nu = \beta\lambda$. The probability that a component fails in a shock averaged over all possible shock is assumed to be 0.25, and the correlation between the components is assumed to be 0.5. This gives the parameters $O = 0.25$ and $D = 0.5$.

There are a few difficulties when applying shock models. Shocks are assumed to be Poisson distributed with parameter ν. This indicates that the waiting time between shocks is exponentially distributed with the same parameter, ν. When a shock occurs, Equation (3.29) gives the probability that exactly $X = x$ components fail. These results, especially for the values of O and D chosen above, implies that many of the shocks go unnoticed. Nevertheless, estimates are obtained using the shock model and stochastic simulation with the numerical values previously given.

$$PFD_{ccf} = 5.70 \cdot 10^{-4} \tag{4.14}$$

For the independent failures, we recall Equation (3.30). The last part of that equation, $\nu \cdot f_1$, is already included in the simulation that leads to the result obtained in Equation (4.14), but the first part must be included. When looking at the first part, it is clear that this is the same as independent failures in the β-factor model so we have $PFD_{indep} = 2.93 \cdot 10^{-3}$. This gives the total PFD of

$$PFD = 2.93 \cdot 10^{-3} + 5.70 \cdot 10^{-4} = 3.50 \cdot 10^{-3} \tag{4.15}$$

4.4 Markov approach

An alternative methodology is to apply Markov analysis as derived in Section 3.8. As previously, DD-failures are ignored. First, we begin by initially classifying all the different states. Initially

Table 4.1: The different states of the lube oil pressure system when including the aforementioned simplifications.

Assigned number	Condition
1	All components are able to function.
2	Comp. 3 or 4 has failed.
3	Comps. 1 and 2 have failed.
4	Comps. 3 and 4 have failed.
5	Comps. 1 and 2 and 3 or 4.
6	All components have failed.

we see that we can ignore all the states where either component 1 or 2, but not both have failed since this does not influence the functionality of the SIF. This means that we need to make use of the ”inner system“ used in Section 4.1. This gives the average failure rate for the system of two components in parallel. This simplification is by no means necessary (if the system was constructed differently), but it simplifies the calculations without changing the result. The different states are given in Table 4.1. Since components 3 and 4 are identical, the notation used to describe these is $\lambda^*_{DU} = 3.4 \cdot 10^{-5}$. The matrix which provides the instantaneous transition rates is given as

$$\mathbf{T} = \begin{pmatrix} 1-x & 2\lambda^*_{DU}(1-\beta) & \lambda^{(is)}_{DU} & \beta\lambda^*_{DU} & 0 & 0 \\ 0 & 1-(\lambda^*_{DU}+\lambda^{(is)}_{DU}) & 0 & \lambda^*_{DU} & \lambda^{(is)}_{DU} & 0 \\ 0 & 0 & 1-(2-\beta)\lambda^*_{DU} & 0 & 2\lambda^*_{DU}(1-\beta) & \beta\lambda^*_{DU} \\ 0 & 0 & 0 & 1-\lambda^{(is)}_{DU} & 0 & \lambda^{(is)}_{DU} \\ 0 & 0 & 0 & 0 & 1-\lambda^*_{DU} & \lambda^*_{DU} \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \end{pmatrix} \tag{4.16}$$

where

$$x = ((2-\beta)\lambda^*_{DU} + \lambda^{(is)}_{DU})$$

is simply introduced for aesthetic reasons. Similar to Equation (3.34), the term $\Delta t = 1$ hour is introduced to transform the rates into probabilities. $\Delta t = 1$ is assumed to be small enough so that the probability of more than one error in the same 1 hour interval may be neglected. In practice, the transformation is done by multiplying Δt by every term in **T** except the 1s on the diagonal. When $\Delta t = 1$, no changes are actually made to the matrix **T**, but the values are now probabilities and not rates. We have moved from continuous time Markov analysis to discrete time Markov analysis.

If a demand occurs and the system is in either state 4, 5 or 6, it is unable to perform its designated function. We assume that the system is fully functional at $t = 0$, i.e. $P_0 = [1,0,0,0,0,0]$. In addition, we have the assumption $P(t) = P_0 T^t$. By saving the value for all values $t \in (0,\tau)$, we obtain the plot given in Figure 4.3. The mean value of the PFD over the interval $(0,\tau)$ is

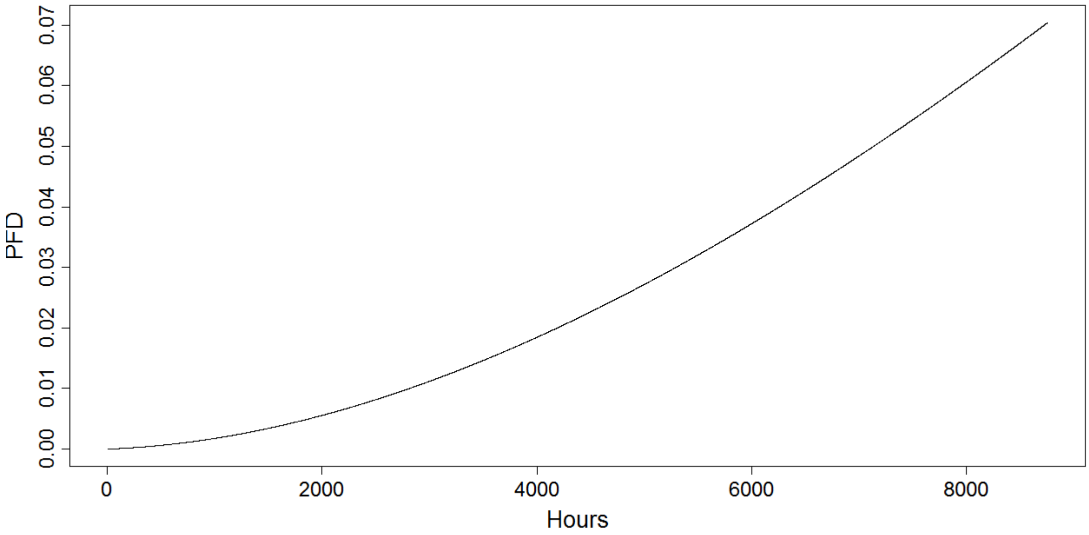

Figure 4.3: The probability of failure on demand when applying Markov analysis plotted against the number hours in operation.

$$PFD = 2.61 \cdot 10^{-2} \tag{4.17}$$

Notice that this result is significantly higher than all the previous ones. When taking a closer look at the different states and how much they contribute to the PFD, we see that at time $t = \tau$ the probability that the system is residing in any of the failed states is

$$\begin{aligned} P_4(\tau) =& 6.95 \cdot 10^{-2} \\ P_5(\tau) =& 7.83 \cdot 10^{-4} \\ P_6(\tau) =& 1.45 \cdot 10^{-4}. \end{aligned} \tag{4.18}$$

State 4, i.e. when components 3 and 4 have failed, is by far the main contributor to the PFD since it is approximately 100 times larger than the other two.

Chapter 5

A system of speed sensors

Consider a system of speed sensors which is mounted to an engine and is designed to turn off the engine if the recorded speed is too high. A reliability block diagram of the system is given in Figure 5.1. The system consists of two $2oo3$ systems in parallel. All six components are identical. The numerical values for the present system are.

$$\begin{aligned} \beta =& 0.02 \\ \lambda_{DU} =& 2.3 \cdot 10^{-6} \text{ hours}^{-1} \\ \tau =& 8760 \text{ hours.} \end{aligned} \tag{5.1}$$

5.1 A PDS approach

The aim is as always to calculate the PFD for the entire system, and this can be done similarly as in Section 4.2. An identical example is given in Hauge et al. (2006a, Appendix D.2) although that example ignores the contribution which comes from independent failures. This is called a $2oo3 \times 1oo2$ architecture. If five or six components fail, the system fails. If four components fail, then the system fails if two are located on one cluster, and the other two are located on the other cluster. This means that the system is in a failed state if either four or five components fail. The system can be considered as a $2oo6$ system with probability $\frac{6}{15}$ and $3oo6$ system with probability $\frac{9}{15}$. The probability $\frac{6}{15}$ is found by counting the different ways four components can fail in the current architecture.

The CCF-part of the PFD is thus

$$PFD_{ccf} = (\frac{6}{15}C_{2oo6} + \frac{9}{15}C_{3oo6}) \cdot \frac{\beta\lambda_{DU}\tau}{2} = 1.21 \cdot 10^{-4} \tag{5.2}$$

For the individual failures we can use the same logic. By using Equation (3.22), we obtain the general formula for independent failures. The last step is to assign $\lambda_{DU}^{(i)}$ according to Equation

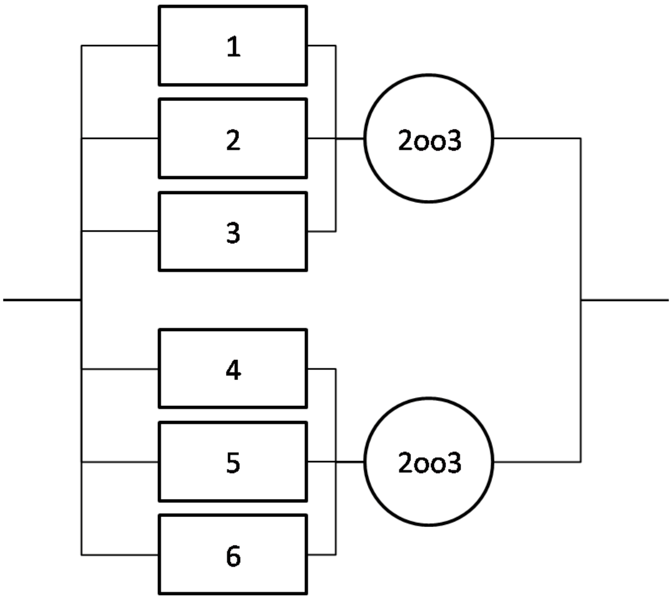

Figure 5.1: A system of speed sensors.

(3.23).

$$\lambda_{DU}^{(i)} = (1 - H_N\beta) \cdot \lambda_{DU} = 2.15 \cdot 10^{-6} \text{ hours}^{-1}$$

provides the rate for independent failures which is in turn employed when calculating the PFD for independent failures.

$$PFD_{indep} = \frac{6}{15}\frac{6!}{6!1!}(\lambda_{DU}^{(i)}\tau)^5 + \frac{9}{15}\frac{6!}{5! \cdot 2!}(\lambda_{DU}^{(i)}\tau)^4 = 2.29 \cdot 10^{-7} \tag{5.3}$$

This gives in total PFD of

$$PFD = PFD_{indep} + PFD_{ccf} \approx 1.21 \cdot 10^{-4}. \tag{5.4}$$

With such high degree of redundancy and $\lambda_{DU} \cdot \tau << 1$, independent failures contribute little to the total PFD.

Mathematically, this is a more precise way of handling the current problem than by using the β-factor model, which has no way of accounting for the current architecture. The β-factor model is included, however, in order to further illustrate the differences.

5.2 A β-factor approach

It seems natural to calculate the PFD when using the β-factor model as in Section 4.1, namely by introducing an ”inner system“ and then treat these two super-components as a $1oo2$ system.

But, we need to stop and think about what we are actually calculating before we progress. According to the β-factor model, a component is exposed to CCFs with a certain fraction (β). This means that we must calculate this percentage from the original failure rate, λ_{DU}. Taking 2% of the failure rate of the $2oo3$ system is far too optimistic. In accordance to the β-factor model one should calculate the CCF term based on λ_{DU} and the independen failures by the same manner as in Equation (5.3).

The preceding reasoning provides, for the CCF term,

$$PFD_{ccf} = \frac{\beta \lambda_{DU} \tau}{2} = 2.015 \cdot 10^{-4},$$

for the independent failures, we know that $\lambda_{DU}^{(i)} = (1-\beta)\lambda_{DU}$,

$$PFD_{indep} = \frac{6}{15}\frac{6!}{6!1!}(\lambda_{DU}^{(i)}\tau)^5 + \frac{9}{15}\frac{6!}{5! \cdot 2!}(\lambda_{DU}^{(i)}\tau)^4 = 2.75 \cdot 10^{-7}$$

which makes the total PFD

$$PFD = PFD_{indep} + PFD_{ccf} = 2.018 \cdot 10^{-4} \approx 2.02 \cdot 10^{-4} \tag{5.5}$$

5.3 A Markov approach

The architecture given in Figure 5.1 is also applicable for Markov analysis. As previously, we begin to assess the different states of the system. Since the components are identical, this process is mostly straightforward. State 5 and 6 includes the same situation as treated in Equation (5.2) in Section 5.1. As previously, the focus is given to DU-failures.

Table 5.1: The different states of the speed sensor system.

Assigned number	Condition
1	All components are able to function.
2	1 component has failed.
3	2 components have failed.
4	3 components have failed.
5	4 components have failed, but the system still works.
6	4 components have failed and the system is down.
7	5 components have failed.
8	All components have failed.

For the handling of CCFs, we may chose several strategies. For instance when in state 1, independent failures with rate $6\lambda_{DU}(1-\beta)$ lead to state 2, and if using the β-factor method, a CCF term with rate $\beta\lambda_{DU}$ leads to state 8. It is naturally possible to assume that CCFs only disable some components and not all. When in state 1, the CCF term can for instance be split into 5 parts with rates $\frac{\beta\lambda_{DU}}{5}$ leading to states 3, 4, 5 or 6, 7 and 8. Another possibility is to assume a tenancy in these CCF probabilities, i.e. if a CCF occurs, the probability of knocking out all components is greater than the probability of disabling only 2 components. Since not much is known about the system, the assumption that a CCF disables $2,3,...,8$ with the same probability is applied. This gives the following transition matrix

$$\mathbf{T} = \begin{pmatrix} a_{1,1} & 6\lambda_{DU}^{(i)} & \frac{1}{5}\lambda_{DU}^{(c)} & \frac{1}{5}\lambda_{DU}^{(c)} & \frac{6}{15\cdot 5}\lambda_{DU}^{(c)} & \frac{9}{15\cdot 5}\lambda_{DU}^{(c)} & \frac{1}{5}\lambda_{DU}^{(c)} & \frac{1}{5}\lambda_{DU}^{(c)} \\ 0 & a_{2,2} & 5\lambda_{DU}^{(i)} & \frac{1}{4}\lambda_{DU}^{(c)} & \frac{6}{15\cdot 4}\lambda_{DU}^{(c)} & \frac{9}{15\cdot 4}\lambda_{DU}^{(c)} & \frac{1}{4}\lambda_{DU}^{(c)} & \frac{1}{4}\lambda_{DU}^{(c)} \\ 0 & 0 & a_{3,3} & 4\lambda_{DU}^{(i)} & \frac{6}{15\cdot 3}\lambda_{DU}^{(c)} & \frac{9}{15\cdot 3}\lambda_{DU}^{(c)} & \frac{1}{3}\lambda_{DU}^{(c)} & \frac{1}{3}\lambda_{DU}^{(c)} \\ 0 & 0 & 0 & a_{4,4} & \frac{3\cdot 6}{15}\lambda_{DU}^{(i)} & \frac{3\cdot 9}{15}\lambda_{DU}^{(i)} & \frac{\lambda_{DU}^{(c)}}{2} & \frac{\lambda_{DU}^{(c)}}{2} \\ 0 & 0 & 0 & 0 & a_{5,5} & 0 & 2\lambda_{DU}^{(i)} & \lambda_{DU}^{(c)} \\ 0 & 0 & 0 & 0 & 0 & a_{6,6} & 2\lambda_{DU}^{(i)} & \lambda_{DU}^{(c)} \\ 0 & 0 & 0 & 0 & 0 & 0 & a_{7,7} & \lambda_{DU} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \end{pmatrix} \tag{5.6}$$

with

$$\begin{aligned} \lambda_{DU}^{(i)} =& (1-\beta)\lambda_{DU} \\ \lambda_{DU}^{(c)} =& \beta\lambda_{DU} \\ a_{i,i} =& 1 - \sum_{j=i+1}^{8} a_{i,j} \end{aligned} \tag{5.7}$$

As previously, the rates are multiplied by $\Delta t = 1$ hour, ignoring the probability of more than one failure (1 CCF counts as one failure) within an interval of 1 hour. The system fails to function if it enters ether state 6, 7 or 8. In order to obtain a smaller transition matrix these 3 states could have been combined into one state and lead to the same answer for the PFD, namely

$$PFD = 1.07 \cdot 10^{-4} \tag{5.8}$$

The PFD value is thus a little smaller, but not unlike the one obtained through the PDS method given in Equation (5.4). Combining failed states as mentioned above is done in Section 6.2.3.

Chapter 6

A complex system of heat detectors

The current Chapter considers a gas outlet surrounded by 24 heat detectors. These heat detectors have two different tasks to perform, i.e. there are two different SIFs present.

1. Detect if there is a significant temperature difference throughout the gas.

2. Detect if the temperature is higher than a 120°C.

SIF 1 is treated separately from SIF 2.

6.1 Temperature distribution in gas

A SIF which makes sure that the temperature is constant throughout the exhaust gas is modelled by assuming that the SIF fails if three adjacent components fail. This can not be modelled as a standard $MooN$ system. If so, what would M be? Another question is how CCFs should be modelled in this situation. The PDS method is applicable for $MooN$ systems, but this is an architecture where M is not specified. It is naturally possible to make simplifications, and one such conservative simplification is to assume that the function has a $22oo24$ structure. Since the SIF fails if three adjacent components fail, a $22oo24$ architecture only allows for two failures. This is, however, a conservative estimate and the aim is to find something more exact.

A simple solution is to use stochastic simulation when solving the current problem. The failure rate λ_{DU} is given (identical components), and the time between each inspection τ is also provided. As previously, all components are assumed to be as good as new after each inspection.

The complex structure of the system makes it difficult to find a precise way of modelling the CCFs. For this reason the β-factor model is applied so that all components fail if a CCF occur. The β-factor gives a conservative estimate since the possibility of a CCF only disabling a few of the components, is excluded. The numerical values applied for the present system are

$$\begin{aligned} \beta =& 0.02 \\ \lambda_{DU} =& 5.8 \cdot 10^{-6} \text{ hours}^{-1} \\ N =& 24 \\ \tau =& 8760 \text{ hours.} \end{aligned} \tag{6.1}$$

The algorithm that was used to perform the modelling is given below. t_G and t_B represent the amount of time the system is working and the amount of time it is not working, respectively. The number of iterations is represented by it.

Algorithm 1.

1. *Assign initial values* $\tau, \lambda_{DU}, N, it = 0, \beta, t_G = 0$ *and* $t_B = 0$.
2. $t_G = t_G + \tau$
3. *Draw N waiting times* t_N^w *from the distribution* $exp((1-\beta)\lambda_{DU})$.
4. *Check if* 3 *adjacent waiting times,* $t_{i-1}^w, t_i^w, t_{i+1}^w$ *are smaller than* τ *(waiting time* 1 *is adjacent to waiting time* 24*). If so,* $\widehat{t}^w = \tau - max\{t_{i-1}^w, t_i^w, t_{i+1}^w\}$ *otherwise* $\widehat{t}^w = 0$.
5. *Draw* 1 *waiting time* t^c *from* $exp(\beta\lambda_{DU})$.
6. *Check if* $t^c < \tau$. *If true,* $\widehat{t}^c = \tau - t^c$, *otherwise* $\widehat{t}^c = 0$.
7. *If* $\widehat{t}^w > 0$ *or* $\widehat{t}^c > 0$. $t_B = t_B + max\{\widehat{t}^w, \widehat{t}^c\}$ *and* $t_G = t_G - max\{\widehat{t}^w, \widehat{t}^c\}$.
8. $it = it + 1$ *and return to Step 2 until sufficient iterations are performed.*
9. *Calculate* $PDF = \frac{t_B}{t_G + t_B}$.

For the given initial values and for 1000000 iterations, the PDF was calculated to be

$$PDF = 1.21 \cdot 10^{-3}. \tag{6.2}$$

Next, the algorithm is run two additional times, one time where the CCF-term is left out and another where the individual term is left out. This is done in order to see which part contribute the most to the PFD. The results were

$$PFD_{indep} = 7.06 \cdot 10^{-4}$$

and

$$PFD_{ccf} = 5.07 \cdot 10^{-4}.$$

The consistency of the different results is assured by drawing the exact same random numbers in all three simulations.

6.2 Detecting high temperature

The SIS also detects if the temperature increases above 120°C (SIF2). In this case, four blocks, each consisting of three components, have to function. Each block is made up of three specific components that all have to function for the block to function. This SIF thus consists of eight blocks where four have to function for the system to function. One block is modelled as a series structure of three individual components. The failure rate for one block is then obtained by adding the failure rates for the three components which give a $4oo8$ structure.

A $4oo8$ structure can be handled numerous ways. Recall Equation (2.6) which provided the general formula for $MooN$ systems for calculating the PFD with respect to DU-failures.

$$PFD_{MooN} \approx \binom{N}{N-M+1} \frac{(\lambda_{DU} \cdot \tau)^{N-M+1}}{N-M+2} \tag{6.3}$$

The following sections present three different methods of modelling this SIF, known as SIF 2. Firstly, we look at the PDS method before stochastic simulation and Markov analysis is applied.

6.2.1 A PDS approach

The PDS approach introduced in Chapter 3.6 is easily applied for the present problem. We have a $4oo8$ system with numerical values

$$\begin{aligned} \beta =& 0.02 \\ \lambda_{DU} =& 3 \cdot 5.8 \cdot 10^{-6} = 1.74 \cdot 10^{-5} \text{ hours}^{-1} \\ N =& 8 \\ M =& 4 \\ \tau =& 8760 \text{ hours.} \end{aligned} \tag{6.4}$$

The suggested values for β_2 and θ and Equation (3.18) yield $C_{4oo8} = 0.87$. The PFD_{ccf} is calculated by using Equation (3.20) and is

$$PFD_{ccf} = 1.33 \cdot 10^{-3} \tag{6.5}$$

When calculating the independent failures, $\lambda_{DU}^{(i)}$ given in Equation (3.23) should be applied. After determining the correct value for H_N, the PFD_{indep} is given by Equation (3.22). When inserting the numerical values we find that $H_N = 3.99$ for $N = 8$ which in turn gives

$$\lambda_{DU}^{(i)} = (1 - 3.99 \cdot 0.02)1.74 \cdot 10^{-5} = 1.60 \cdot 10^{-5} \text{ hours}^{-1}.$$

Finally we are able to obtain

$$PFD_{indep} = \frac{8!}{(8-4+2)!(4-1)!}(1.60 \cdot 10^{-5} \cdot 8760)^{8-4+1} = 5.05 \cdot 10^{-4} \tag{6.6}$$

The total PFD is thus

$$PFD = PFD_{indep} + PFD_{ccf} = 1.835 \cdot 10^{-3} \approx 1.84 \cdot 10^{-3} \tag{6.7}$$

6.2.2 Stochastic simulation

Another method is found by using stochastic simulation. The algorithm is quite simple and can be modified both to different architectures and different failure rates. As it is formulated in Algorithm 2, it is similar to the β-factor model so the values when using the β-factor model are also included to illustrate the similarity.

Constant failure rates, as assumed in the present case, give exponential waiting times, but the algorithm can easily be modified to draw from other distributions. The stochastic simulation given in Algorithm 2 assumes a β-factor model when handling CCFs.

Algorithm 2.

1. *Assign initial values to* $N, M, \lambda_{DU}, \tau, it = 0, t_G = 0$ *and* $t_B = 0$.
2. *Set* $t_G = t_G + \tau$.
3. *Draw N random numbers* $t_i^w, i = 1, ..., N$ *from the distribution* $exp(\lambda_{DU})$.
4. *Draw one random number* t^c *from the distribution* $exp(\beta \cdot \lambda_{DU})$.
5. *Check if more than N−M of the numbers* t_i^w *are smaller than* τ. *If so,* $\widehat{t}^w$ = *the Mth smallest value.*
6. *If the last point was true,* $t_G = t_G - (\tau - \min\{\widehat{t}^w, t^c\})$ *and* $t_B = t_B + (\tau - \min\{\widehat{t}^w, t^c\})$.
7. $it = it + 1$ *and go back to Step 2 until sufficient iterations are done.*

This provided the estimate

$$PFD = 1.84 \cdot 10^{-3}. \tag{6.8}$$

As in Section 6.1, the algorithm is run two additional times with the same random numbers in order to isolate the contribution from independent failures and CCFs. This gives

$$PFD_{indep} = 3.81 \cdot 10^{-4}$$

and

$$PFD_{ccf} = 1.42 \cdot 10^{-3}.$$

By using standard β-factor analysis, the estimate

$$PFD_{indep} = 6.94 \cdot 10^{-4}$$

and

$$PFD_{ccf} = 1.52 \cdot 10^{-3}$$

Table 6.1: The different states of the speed sensor system when applying Markov analysis.

Assigned number	Condition
1	All components are able to function.
2	1 component has failed.
3	2 components have failed.
4	3 components have failed.
5	4 components have failed.
6	5, 6, 7 or 8 components have failed and the system is down.

are also obtained. The total average PFD for the standard β-factor model is thus

$$PFD = PFD_{indep} + PFD_{ccf} \approx 2.22 \cdot 10^{-3}. \tag{6.9}$$

The stochastic simulation gave basically an identical value for the PFD as the PDS method did, while the calculated β-factor model gave a slightly greater value. The PDS method includes the fact that a CCF not necessarily disable all components. A $4oo8$ structure has good redundancy which means that the PDS estimate is lower than the β-factor estimate.

The reason for the stochastic simulation estimate being lower than the β-factor estimate is simply that the approximation formulas produce a conservative estimate, while the stochastic simulation does not.

6.2.3 Markov analysis

A regular $4oo8$ system is naturally applicable to Markov analysis. As in Section 5.3, a CCF is assumed to have the same probability of knocking out $2, 3, ..., N$ components. As always, the first step is to assign the different states as done in Table 6.1. In order to reduce the complexity and increase the speed of the computation process, the different states where the system is unable to function, is combined into a single state. From Table 6.1 we see that state 6 is made up of four different failure possibilities, and this is accounted for when defining the transition rates. The transition matrix is

$$\mathbf{T} = \begin{pmatrix} a_{1,1} & 8\lambda_{DU}^{(i)} & \frac{\lambda_{DU}^{(c)}}{7} & \frac{\lambda_{DU}^{(c)}}{7} & \frac{\lambda_{DU}^{(c)}}{7} & \frac{4\lambda_{DU}^{(c)}}{7} \\ 0 & a_{2,2} & 7\lambda_{DU}^{(i)} & \frac{\lambda_{DU}^{(c)}}{6} & \frac{\lambda_{DU}^{(c)}}{6} & \frac{4\lambda_{DU}^{(c)}}{6} \\ 0 & 0 & a_{3,3} & 6\lambda_{DU}^{(i)} & \frac{\lambda_{DU}^{(c)}}{5} & \frac{4\lambda_{DU}^{(c)}}{5} \\ 0 & 0 & 0 & a_{4,4} & 5\lambda_{DU}^{(i)} & \lambda_{DU}^{(c)} \\ 0 & 0 & 0 & 0 & a_{5,5} & 4\lambda_{DU} \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \end{pmatrix} \tag{6.10}$$

with

$$\begin{aligned}
\lambda_{DU}^{(i)} &= (1-\beta)\lambda_{DU} \\
\lambda_{DU}^{(c)} &= \beta\lambda_{DU} \\
a_{i,i} &= 1 - \sum_{j=i+1}^{6} a_{i,j}
\end{aligned} \tag{6.11}$$

As previously, the rate matrix is transformed into probabilities by multiplying $\Delta t = 1$ by all terms except the 1s on the diagonal. Δt is assumed to be small enough for the probability of more than one failure in the duration of one hour to be of importance. The system is assumed to be fully functioning at time $t = 0$ so in accordance with the formulas of Section 3.8, $\mathbf{P}(0) = [1,0,0,0,0,0]$ and $\mathbf{P}(t) = \mathbf{P}(0)\mathbf{T}^t$. PFD is for the system in question; the average amount of time spent in state 6 during the time interval $(0,\tau)$. With the help of a computer, the result of interest is

$$PFD = 1.35 \cdot 10^{-3}. \tag{6.12}$$

The result in Equation (6.12) is not very different from the one obtained through the PDS approach given in Equation (6.7). Both the PDS method and the Markov approach yield significantly lower values for the PFD than when using stochastic simulation. The reason is simply that when using simulation, we assumed a β-factor model which, compared to the PDS method and the Markov method, punishes systems with good redundancy when assuming that all CCFs disable all components.

Part III

Assessing the results and proposing strategies for dealing with CCFs

Chapter 7

Discussion

The following chapter assesses the results obtained in Chapters 4, 5 and 6. As previously stated, it is difficult to know which results are the most ”correct“ for these particular systems since no feedback data exist. The aim is then to study which results are obtained with respect to which assumptions that are made. For instance, the β-factor always assumes that all components fail in a CCF while the PDS method does not. These different assumptions lead to different results when dealing with various architectures.

Throughout the report, except in Section 3.9, it is assumed that $MTTR << \tau$, which makes $DTU_R << PFD$. Section 3.9 shows that even with $MTTR = 730$ hours, the term DTU_R is still small compared to the PFD. This will naturally also depend on the failure rate λ_{DD} and λ_{DU} but we may in general disregard DTU_R for systems where most failures are repaired within a couple of days or a week. If $MTTR$ is much longer than this, we may still be able to neglect the term DTU_R, but some extra consideration is needed.

7.1 The methods of Chapter 4

Table 7.1 summarizes the values obtained for the PFD in Chapter 4. These values are divided into contributions from independent and dependent failures, except when using Markov analysis. As seen in Table 7.1, no method provides the same exact result. The Shock model provided the smallest value for the PFD, and this is especially due to the CCF-part of the PFD. The independent part is equal to the β-factor, but the values applied for shocks, $\nu = \beta\lambda_{DU}$ were too small to provide values in the same range as for the PDS method or the β-factor. This comes as a natural consequence since many of the shocks go unnoticed. Even when adjusting the parameters Y and D, there is still a relative large probability of zero components failing due to a shock, and this probability is not accounted for in the estimated failure rates applied in the other models. The shock model is easily expanded to account for all $MooN$ architectures[1], but if one wants

[1] Adjust n in Equation (3.29)

Table 7.1: The numerical values obtained for the PFD of the lube oil pressure system when applying different methods.

Method	PFD_{indep}	PFD_{ccf}	PFD	SIL
β-factor	$2.93 \cdot 10^{-3}$	$1.42 \cdot 10^{-3}$	$4.36 \cdot 10^{-3}$	2
PDS method	$2.64 \cdot 10^{-3}$	$2.94 \cdot 10^{-3}$	$5.58 \cdot 10^{-3}$	2
Shock model	$2.93 \cdot 10^{-3}$	$5.70 \cdot 10^{-4}$	$3.50 \cdot 10^{-3}$	2
Markov approach	-	-	$2.61 \cdot 10^{-2}$	1

it to provide the same results as the β-factor model or the PDS method, the rate v should be increased.

The β-factor model follows next with the second smallest value, but the result is quite similar to that of the PDS method. Even though the β-factor method and the PDS method are quite similar, the applied strategies used in Chapter 4 are quite different. In Section 4.1 the average failure rate function for the "inner system" is obtained while in Section 4.2, since the PDS method is able to distinguish between different architectures to a greater degree, applies the probability of the system either being either a $2oo4$ or a $3oo4$ system. When working with a system with relatively bad redundancy, ($3oo4$) the PDS method "punishes" such systems since there in the PDS method is a relatively larger probability of a CCF occurring. For a $3oo4$ system, only 2 components need to fail for the system to fail, so this system does not have a great deal of redundancy.

The largest value for the PFD was obtained when using Markov analysis. We notice that for this method, we are not able to distinguish between independent and dependent failures. This follows as a natural consequence of the Markov assumption[2].

There is one simplification which was made for all methods except when using Markov analysis, and this proves to be of some consequence. The simplification in question is that all other methods apply the geometric mean and thus use *one* estimated failure rate instead of the actual ones. For the current example this simplification proves to be decisive when determining the SIL, since the system fails if components 3 and 4 (see Figure 4.1) fail. These two components have failure rates equaling $3.4 \cdot 10^{-5}$ and not $1.04 \cdot 10^{-5}$ as estimated when using the PDS method or $6.51 \cdot 10^{-6}$ as estimated in Section 4.1.

The Markov analysis does in this case present a model which bear the closest resemblance to the real, physical system. As a consequence the estimate provided by Markov analysis is considered to be the most reliable.

The β-factor model, the PDS method and the Shock model use a simplification which pro-

[2] The probability of the system being in state $i+1$ is only dependent of state i and independent of state $i-1$, see (Rausand and Høyland, 2004, Chapter 8).

vides severely different values for the PFD compared to the Markov analysis, namely the geometric mean between the different components when calculating the "average" failure rate. This leads to a series of strange results. The average failure rate for the inner system was calculated to be $z_{mean}(t) = 2.38 \cdot 10^{-7}$ hours^{-1}. After taking the geometric mean, the total failure rate for the entire system was obtained, $\lambda^{(os)} = 6.51 \cdot 10^{-6}$ hours^{-1}. When applying the β-factor model, the system is susceptible to CCFs at a rate of $\beta \cdot \lambda^{(os)} = 3.26 \cdot 10^{-7}$ hours^{-1}. This means, according to this model, that CCFs will disable the components of the inner system more often than the actual failure rate of the inner system. This must be incorrect and the geometric mean is thus not ideal when working with failure rates which are very different from one another. In such situations, Markov analysis seems to be a more sensible approach.

7.2 The methods of Chapter 5

Chapter 5 studies the system given in Figure 5.1 and proposes a few different strategies on how to handle CCFs. The same strategies as in Chapter 4 are applied, except Shock models. The Shock model was not included based on the fact that the rate at which shock occurs $\nu = \beta \cdot \lambda_{DU}$ is not comparable with the rest of the models. If the shock model is to be applied, a different value must be utilized.

Table 7.2 shows the results obtained by applying the β-factor model, the PDS method and Markov analysis. Chapter 5 first applied the PDS method before continuing with the β-factor model.

Table 7.2: The numerical values obtained for the PFD of the speed sensor system when applying three different methods.

Method	PFD_{indep}	PFD_{ccf}	PFD	SIL
β-factor	$2.75 \cdot 10^{-7}$	$2.015 \cdot 10^{-4}$	$2.02 \cdot 10^{-4}$	3
PDS method	$2.29 \cdot 10^{-7}$	$1.21 \cdot 10^{-4}$	$1.21 \cdot 10^{-4}$	3
Markov approach	-	-	$1.07 \cdot 10^{-4}$	3

These methods are handled similarly, except for the fact that a CCF when applying the β-factor model always disables all components. Finally Markov analysis is applied with respect to the system in Chapter 5 and the PFD value given in Table 7.2 is obtained by using a similar CCF technique as the PDS method applies. As previously mentioned, Markov analysis is flexible and by adjusting Equation (5.6), a number of different tactics could have been applied for dealing with CCF.

Table 7.2 indicates that the PDS method and the Markov analysis gave relatively similar answers while the β-factor provided an answer almost twice as large. This is explained by the CCF-tactic employed by the different methods. Since the system in question has good redundancy, a relative large number of components (four or five) need to fail in order for the system to fail. As a natural consequence, the β-factor model produces a higher value for the PFD.

It is difficult to state bombastically that any of these methods is more correct than the others without analyzing feedback data from the actual system in operation. If the CCFs are observed to be of the same nature described by the β-factor model, then there is no need for any of the other models. If on the other hand, CCFs occur at different multiplicities, the β-factor model is not the right choice and one of the other models would fit better. These evaluation needs to be made for each system based on feedback data or previous knowledge.

We also observe that the contribution to the PFD from independent failures is negligible when we have this many components. This is not the case for the oil pressure system in Chapter 4 where the independent failures and CCFs are of the same order.

7.3 The methods of Chapter 6

The SIS which is given in Chapter 6 consists of two SIFs, one which controls the temperature distribution and another which makes sure the temperature stays beneath a set limit. The SIF in Section 6.1 is much more complicated than the one in Section 6.2, since the latter of the two is treated as a regular $MooN$ system.

7.3.1 Temperature distribution

The first SIF is of such complex structure that a customized simulation algorithm is created in order to compute the PFD. Algorithm 1 is a recipe on how to create this function in a computer program. The algorithm draws 24 waiting times from the exponential distribution and checks if three adjacent waiting times are smaller than τ. If three adjacent waiting times are smaller than τ, the time the system was unable to function is recorded as well as the time it was able to function. This is repeated many times in order to see the general behaviour of the system in a long time perspective.

The procedure described just now will, however, only provide the independent failures and not CCFs. The method for handling CCFs, which is also described in Algorithm 1, is similar to that of the β-factor model. The algorithm may be modified if one wishes to chose a different CCF tactic.

A waiting time is drawn from the exponential distribution with parameter $\beta \cdot \lambda_{DU}$, and if this waiting time is smaller than τ, a CCF occurs. This CCF may knock out all components, or some condition can be placed upon it. One may for instance assume that the CCF disables a component by a certain probability. In practice, this is accomplished by drawing 24 random numbers between 0 and 1 and see how many of these numbers are lower than the probability of failure. Such a method gives the number of failed components as well as which specific components fail. The last step is to combine independent and CCFs over the time interval τ and see if 3 adjacent have failed.

As shown in Chapter 6, by simulating the system for 10^6 years, we are able to obtain

$$PDF = 1.21 \cdot 10^{-3} \tag{7.1}$$

$$PFD_{indep} = 7.06 \cdot 10^{-4} \tag{7.2}$$

$$PFD_{ccf} = 5.07 \cdot 10^{-4} \tag{7.3}$$

which equals SIL 2. Even though $PFD_{indep} + PFD_{ccf} \neq PFD$ since there sometimes are overlaps, i.e. in some iterations there are both independent failures and a CCF. This difference is so small that it may be disregarded, so it is safe to use

$$PFD \approx PFD_{indep} + PFD_{ccf}.$$

By comparison, we may perform standard PFD analysis on a $22oo24$ system and see the difference. The PDS method provides the estimate

$$PFD_{ccf} = C_{22oo24} \frac{\beta \lambda_{DU} \cdot \tau}{2} \approx 1.22 \cdot 10^{-3}$$

and

$$PFD_{indep} = \frac{24!}{4! \cdot 21!} \left((1 - H_N \cdot \beta) \lambda_{DU}^{(i)} \cdot \tau \right)^3 \approx 3.30 \cdot 10^{-2}$$

which results in the total PFD of

$$PFD = PFD_{indep} + PFD_{ccf} \approx 3.42 \cdot 10^{-2} = \text{SIL 1} \tag{7.4}$$

We see that when assuming a $22oo24$ structure, the PFD given by the PDS method is high compared to the stochastic simulation. The greatest contributor to this part comes from independent failures. By studying the CCF-term when using the regular β-factor model we are able to see that

$$PFD_{ccf} = \frac{\lambda_{DU} \beta \cdot \tau}{2} \approx 5.08 \cdot 10^{-4}$$

which is essentially the result obtained through stochastic simulation in Equation (7.3). As expected, the stochastic simulation provides similar results as the approximation formula, but the estimates from the approximation formula are a bit higher (more conservative).

7.3.2 Detecting high temperature

Four different approaches were applied when calculating the PFD for det safety system which detects high temperature. The system is modelled as a normal $4oo8$ system with eight identical components. The modelling resulted in the estimates repeated in Table 7.3. We observe that the highest value for the PFD is given by the standard β-factor model. The simulated version, i.e. the less conservative β-factor approach, provides the same result as the PDS method. The Markov

Table 7.3: The numerical values obtained for the PFD for the SIF that detects high temperature. Four different methods are applied.

Method	PFD_{indep}	PFD_{ccf}	PFD	SIL
β-factor	$6.94 \cdot 10^{-4}$	$1.52 \cdot 10^{-3}$	$2.22 \cdot 10^{-3}$	2
Simulated β-factor	$3.81 \cdot 10^{-4}$	$1.42 \cdot 10^{-3}$	$1.84 \cdot 10^{-3}$	2
PDS method	$5.05 \cdot 10^{-4}$	$1.33 \cdot 10^{-3}$	$1.84 \cdot 10^{-3}$	2
Markov approach	-	-	$1.35 \cdot 10^{-3}$	2

approach, which assumes a similar CCF-strategy as the PDS method, provides the lowest estimate. The reason why the Markov estimate gives a lower estimate than the PDS method, originates in the fact that the PDS method also uses a conservative approximation formula. Even though the PDS method accounts for different voting logics, the approximation formula in Section 2.4 is still employed.

It is naturally difficult to evaluate which estimate is the most correct when there are no feedback data and in addition, the difference between the estimates is not especially large.

Again the CCFs are treated differently for the β-factor model and the PDS method with respect to the number of components that fail when a CCF occurs. If some previous knowledge of the system exists with respect to CCFs, this should naturally be utilized in deciding the correct strategy. If nothing is known about the system, the Markov approach and the simulated β-factor model are mathematically more correct than both the PDS approach and the β-factor model since no approximation formula is used.

The simulated β-factor model provides different estimates from time to time since random numbers are drawn even though the difference from time to time is relatively small. The Markov approach however, provides a fixed estimate and is a more flexible model.

Chapter 8

Recommendations when applying CCF-modelling

8.1 Introduction

The present thesis has introduced different methods of handling CCFs and examples where these models are applied. Chapter 4 provided an example with different failure rates and an inner and outer system (see Figure 4.1), while Chapter 5 involved two 2$oo$3 architectures in parallel (Figure 5.1). Chapter 6 introduced two different SIFs, one where three adjacent components out of 24 had to fail for the system to fail, and another which is treated as a regular 4$oo$8 system.

The present chapter reviews the assessments in Chapter 7 and aims at providing advice on how to model CCFs for different systems. As previously mentioned, there is not **one** model which is best suited for all situations. If more than one approach is possible, it may also be difficult to claim that one is better than the other especially when feedback data are absent. Since no feedback data are available for the current examples, the previously obtained results are not verified in any way, and the suggested strategies reflect the author's personal opinion. Firstly, if feedback data are available, the data should be considered and taken into account when performing reliability analysis. Feedback data may be helpful when determining variables such as, λ_{DU}, β and so forth. Additionally, if there are any data or expert opinion available to describe the nature of the CCFs, this may help in choosing the most descriptive model.

8.2 Reviewing the models

Chapter 3 introduced several of the existing models that deal with CCFs. Some of these models, and others, are also covered in the PhD. thesis (Zitrou, 2006).

8.2.1 Models not included

The Square-Root model in Chapter 3 is only included for illustrative purposes and not applied to the examples in Part II. The Square Root method has a poor mathematical foundation, and it is difficult to handle advanced structures when using this method.

The Shock model was introduced and also applied in Chapter 4 for the system that detects low oil pressure. This model has not been subject to much previous research, and it is difficult to assess whether the general values available (λ and β) apply for this model since many shocks go unnoticed. It is, however, an interesting model, but for systems where little information is available, it is perhaps not preferable.

8.2.2 The main models

Four of the introduced models were deemed relevant for some, or all, of the selected examples. The simplest of these are β-factor model. The remaining models employ the same input parameters, namely λ, β, M and N.

To summarize the difference between these models shortly with respect to CCF modelling, one may say that the β-factor model and the PDS method work for standard $MooN$ system but only the latter of the two account for different values of M. Stochastic simulation and Markov methods may be used to "copy" either the β-factor model or the PDS method but without the approximation made in Section 2.4. In addition, stochastic simulation and Markov methods may also be used to model other, more complicated structures more accurately.

More generally, the β-factor model is undoubtedly applicable for for $N = 2$ components. The question becomes evident when the number of components increase and the architectures differ, i.e. architectures such as $2oo9$, $4oo9$, $8oo9$ and so forth. Preferably, one should know the distribution of number of components that fail due to a CCF, but this is usually not the case. Intuitively, one would think that a $2oo9$ system should not be treated similarly as a $8oo9$ system with respect to CCFs. Since the $2oo9$ system has greater redundancy than the $8oo9$ system, it seems less likely for the $2oo9$ to be as prone to CCFs as the $8oo9$ system. Thus, the PDS method is preferable instead of the β-factor model when $N > 2$. As seen in the different examples, the calculus involved when applying the PDS method is relatively simple. The independent failures are slightly more complicated when dealing with the PDS method, but these may be disregarded if the system has good redundancy.

Both stochastic simulation and Markov methods are applicable for general $MooN$ methods, and both models are, in fact, mathematically more accurate since none of these make the conservative assumption derived in Section 2.4. This claim is supported by the results obtained in for instance Section 6.2 where the stochastically simulated β-factor model and the Markov approach provided a lower result than the β-factor model and the PDS method, respectively.

The downside when using these models (stochastic simulation or Markov) is that they are slightly more complicated than the β-factor model and the PDS method. For Markov methods, when "converting" from continuous time to discrete time, the complexity severely decreases and even large systems may be treated with relative ease. This simplification does, however, introduce the need for a computer and the knowledge of a programming language (for instance MATLAB or **R**) since the procedure involves calculating the power of a matrix numerous times.

Stochastic simulation naturally also includes the use of a computer and programming skills to implement the algorithms previously presented. This is not particularly difficult for someone who knows a suitable programming language, but it may prove a challenge for someone who is not familiar with programming.

When applying Markov methods, it is naturally necessary to investigate whether the system in question fulfills the Markov assumption. This should, however, be the case for most regular systems and thus not cause great difficulties, but it is important to be aware of this fact. When dealing with the PDS method and the β-factor model, the size of $\lambda_{DU} \cdot \tau$ is critical since these methods assume an approximation formula. For small $\lambda_{DU}s$, this approximation does not cause significant deviations, but a Markov approach or stochastic simulation omits this approximation entirely.

A downside which presents itself for Markov approaches is when we are dealing with both detected and undetected failures. This vastly increases the complexity of the transition matrix and the number of states.

For non-identical failure rates, as the for the system in Chapter 4, it is important to proceed with care, especially when the difference is large. In such cases, Markov analysis is valuable and preferable compared to the β-factor model and the PDS method. Chapter 4 presented a $2oo3$ system where two of the components had a significantly higher failure rate than the ones given in the "inner system". Since only the two components with high failure rate need to fail for the system to fail, the strategy of taking the geometric mean of all components result in a too low PFD. Markov analysis is thus better at accounting for the diversity of such systems.

In some situations, stochastic simulation is definitely preferable instead of any of the other presented approaches. When dealing with architectures like the one presented in Section 6.1, even though an analytic solution probably exists, the easiest approach is to program the behaviour of the system in the long run. Since the system in question is not a regular $MooN$ system, other approaches are not able to model its complexity.

Independent failures

For simplicity, Hauge et al. (2006a) suggested not to include independent failures for $N > 3$. This is not always adequate as seen in Section 7.3.1 where a $22oo24$ system was introduced to compare results with the stochastic simulation. On the other hand, the contribution from independent failures for the system in Chapter 5 is small compared to that of the CCFs (see

Table 7.2). As previously stated, the system in Chapter 5 may be treated as a combination of a $2oo6$ system and a $3oo6$ system and has as such good redundancy. This is certainly not the case for a $22oo24$ system which has relatively poor redundancy.

As a first approximation to investigate whether independent failures are relevant, compare Equation (3.20) with Equation (3.22) when using λ_{DU} instead of $\lambda_{DU}^{(i)}$ in Equation (3.22). As a rule of thumb for general $MooN$ systems, one may ignore independent failures if the system has very good redundancy. It is up to each individual to decide when the system has good redundancy, but since the procedure of including independent failures only requires a minimal amount of work, it is strongly suggested that this is done.

The consideration of when to include and when not to include independent failures is not needed for Markov analysis. This follows naturally since, if proceeding in the same manner as presented in the present report, one only obtains the total PFD and not the different contributions.

DD-failures

Section 3.9 introduced DD-failures and non-negligible repair time. This is included to account for systems with very long repair time and as seen in the example, not even a repair time of 1 month had a significant impact on CSU_{TOT} in the derived example. This naturally also depends on the choice λ_{DD} and λ_{DU}. For a large value of λ_{DD} the DTU_R becomes more relevant than with a small value.

In general, the inclusion of the DTU_R is not deemed necessary because the contribution to CTU_{TOT} is negligible compared to the PFD. As such, the DTU_R is only necessary for special systems when the repair rate of DD-failures is extremely long. This may for instance be the case for different sub-sea equipments or other systems that are not accessible for repair. It is, however, necessary to be aware of this fact because the system has reduced protection in this time interval. In addition if for instance two components in a $2oo3$ system have failed dangerously, the system is unable to provide the necessary safety if a demand occurs.

Chapter 9

Final conclusions

The present report deals with reliability modelling for SIS and focuses on calculating the PFD, and special attention is given to CCFs. The strategy chosen in doing so, is to survey a few of the existing models that deal with CCFs, apply these models for various examples, and based on the obtained results, propose strategies for how to deal with CCF modelling. Real-life examples with very different architectures are chosen to account for the great variety of SIS found in different industries.

After reviewing a large number of existing models, some of whom are presented in Chapter 3, four "models" were given more careful attention, namely the β-factor model, the PDS method, Markov analysis and stochastic simulation.

We may conclude that for regular $MooN$ systems, the β-factor fails to describe the system properly when $N > 2$. The PDS method yields relatively similar results as Markov analysis except for the fact that the PDS method uses an approximation that is not included when applying Markov analysis. This fact ensures that the PDS method provides a more conservative estimate for the PFD. For standard $MooN$ systems with identical components it is the author's belief that the PDS method is adequate. If any data exist which indicate the distribution of the number of failed components in a CCF, the parameter θ may be changed to account for this.

For systems with additional properties, for instance different failure rates or other attributes that require a more dynamic model, Markov analysis (if possible) is preferred. Working with a system consisting of multiple failure rates may give strange results when applying the geometric mean as an estimate (see Table 7.1). Two different methods of applying Markov analysis is introduced, and for the example in Chapter 3.8, the results were very similar.

In special circumstances we may need to design a specific algorithm in order to correctly handle the complexity of the system in question. Section 6.1 provides such an example where the other approaches are inadequate.

Even though the β-factor model and the PDS method are not applicable for all architectures where Markov analysis or stochastic simulation is used, the opposite is not the case. Both Markov analysis and stochastic simulation are very well suited for modelling general $MooN$ architectures (see e.g. Section 6.2).

Finally it is always important to retrieve as much information as possible about the system in question. Operating with a failure rate that correctly reflect the reliability of the components in the system is important when calculating the PFD. The distribution of CCFs are also important since this provides clues in deciding the parameters used in CCF-modelling.

Appendix A

Methods of estimating β

The methods described in Chapter 3 introduced different methods for modelling CCFs. These methods, like the β-factor model and the generalizations of the β-factor model require the use of a given β. IEC 61508 (2000) suggest, based on experience, that the best case scenario for the value of β is $\beta = 0.01$ while the worst case scenario is $\beta = 0.3$. The current chapter suggests a few methods of deciding a suitable plant specific β.

In addition, a method called The Unified Partial method, which is somewhat different from the methods previously mentioned, is introduced in Section A.4.

The present chapter is not directly applied in the report since assigning a plant specific β requires some knowledge about the physical system. Since such information is not available in the present case, this chapter moved to the Appendix and may be applied when dealing with a specific system where both expert opinion and (or) feedback data are available. In addition to the methods presented below, there are other more general descriptions available on how to reasonably apply expert knowledge of a system, e.g. Wisse et al. (2008). The following reviews are not to be considered complete, and the provided references should be consulted for further reading.

A.1 Partial β-factor model

Johnston (1987) proposed a method of estimating the β which is combined with qualitative analysis. Not much information was obtained with respect to this approach, but the main facts are mentioned here. The following points are qualitative measures which can be taken to minimize the risk of CCFs. The points are merely suggested facts to be aware of.

- Development of system logic.
- Identification of components affected by common attributes/environments.
- Check whether any cutset of the fault tree contains two or more affected components.

- Assessment of component defences against the cause of the dependency.

- Evaluation of the effect on system reliability, reflecting as much as possible, the detailed qualitative analysis.

The β-value derived from the partial β-factor method (PBF) is constructed through expert opinions of the defences of the model at hand. The different aspects of the model is broken down in parts (partial βs), and each part is considered separately. All the different defences are assigned with a numerical value, and the product yields the β. The different defences which are assigned values, are given in Table A.1.

Table A.1: The partial β-factor method listing different defences and the assigned reference values. The product of all 19 values yield the specified β.

Defences	Reference values
Design control	0.6
Design review	0.8
Functional diversity	0.2
Equipment diversity	0.25
Fail-safe design	1.0
Operational interfaces	0.8
Protection and segregation	0.8
Redundancy and voting	0.9
Proven design and standardization	0.9
Derating and simplicity	0.9
Construction control	0.8
Testing and commissioning	0.7
Inspection	0.9
Construction standards	0.9
Operational control	0.6
Reliability monitoring	0.8
Maintenance	0.7
Proof test	0.7
Operations	0.8
	$\prod_{i=1}^{19} \beta_i = 0.001$

The partial β-factor model may thus be a tool of qualitatively gaining an estimate for the β that is used e.g. in the β-factor model.

This model is not the most rigorous, mathematically speaking, but it might be helpful if there is no information available regarding CCFs. For more information about this model and the strengths and weaknesses is found in Johnston (1987).

The model may be difficult to quantify correctly since not much information other than Johnston (1987) is available. For instance, what does the values of Table A.1 signify? If the system is deemed "better" than average with respect to, for instance design control, the value (0.6) should be reduced, but by how much? This uncertainty makes this method difficult to apply.

A.2 The IEC method for determining a plant specific β

IEC 61508 (2000, Part 6, Annex D) provides a method of finding a plant specific β. This method is based on engineering judgement when inspecting the system in question. A score function $S = X + Y$ is used to obtain a plant specific β. For each of the topics listed below, a number of questions are given and the user should sum the Xs and Ys if the question applies to the system in question.

1. Separation/segregation
2. Diversity/redundancy
3. Complexity/design/application/maturity/experience
4. Assessment/analysis and feedback data
5. Procedures/human interface
6. Competence/training/safety culture
7. Environmental control
8. Environmental testing

The ratio $X : Y$ represent to which extent diagnostic testing (explained in Section 3.9) would improve the defence against CCFs. In some cases there is no value given for X. This indicates that diagnostic testing have no influence for that particular measure, and the Y-value should be chosen.

As an example we choose the first question for the topic *Separation/segregation*. The question is as follows:*Are all signal cables for the channels routed separately at all positions?*

If the answer for the system in question is *yes*, we need to know if that system has diagnostics testing. If the system does not have diagnostics testing, we add the term X into our score function. If the answer to the question is *yes*, and the system in question also has diagnostics testing, we add the term Y. The same question is asked both for the logical sub system of the SIS and the sensors and final elements of the SIS. After repeating this process for all questions given under all the different topics, we end up with a sum, $S = X + Y$ for all X and Y. The value for β may then be decided by using the values in Table A.2. This table is also found in IEC 61508 (2000, Part 6, Annex D).

Table A.2: The plant specific value for β calculated by the corresponding score function S.

S	Logic subsystem	Sensors or final elements
120 or above	0.5%	1 %
70 to 120	1 %	2 %
45 to 70	2%	5%
Less than 45	5%	10 %

A.3 The PDS approach for determining a plant specific β

The PDS method suggests a way of determining an application specific value for β. Firstly, Hauge et al. (2006b) lists several "average" β values for different safety instrumented systems. However, this value may not be valid for all systems. The notation β^* is used for the application specific β, and the relationship

$$\beta^* = k_\beta \cdot \beta$$

is assumed. k_β is a parameter describing the system's protection against CCFs and β represent an "average" value for the protection for a SIS of the type in question. Section A.2, (IEC 61508, 2000, Part 6, Annex D, Table D1) presented a number of topics to take into consideration when determining β^*. The PDS method argues that only the first two topics, *Separation/segregation* and *Diversity/redundancy* are relevant for the current calculation. The remaining topics are only relevant for determining the application specific λ_{DU}. The two relevant topics are to be assessed by expert engineering judgement and quantified according to Table A.3. Other values than the ones presented in Table A.3 may naturally be utilized, but as the method states, $k_\beta = 0.1$ requires extreme measures of protection and does not seem likely in practice. A more thorough descrip-

Table A.3: Typical values for k_β when applying the PDS method of finding the application specific β, i.e. β^*.

k$_\beta$	**Protection**	**Comments**
0.1	Very high protection	Separation/segregation and diversity/redundancy fully implemented
0.5	Extended protection	Some additional protection implemented and documented
1.0	Normal protection	Average level of protection - current practice
5.0	Reduced protection	Less protection than typically implemented

tion of the two topics considered (separation/segregation and diversity/redundancy) is given in Hauge et al. (2006a, Appendix C).

A.4 The Unified Partial method

The Unified Partial method (UPM) is the main approach for modelling CCFs in the UK. The method is given in Zitrou and Bedford (2003), but the notation is somewhat modified in Zitrou et al. (2007), so a review of the latter of the two approaches is given in the present report. UPM is based on the β-factor method in the sense that a CCF disables all components in the system. In the UPM eight different defences are suggested. These are listed in Figure A.1. The defences are denoted $D_1, \dots, D_8$ and each D_i is assigned a value x_k, $x_k \in \{1, \dots, 5\}$ by consulting experts. Each defence is then given a score, s_i which indicates the importance of each defence. In addition, a scaling factor d is introduced. This gives an estimator for β.

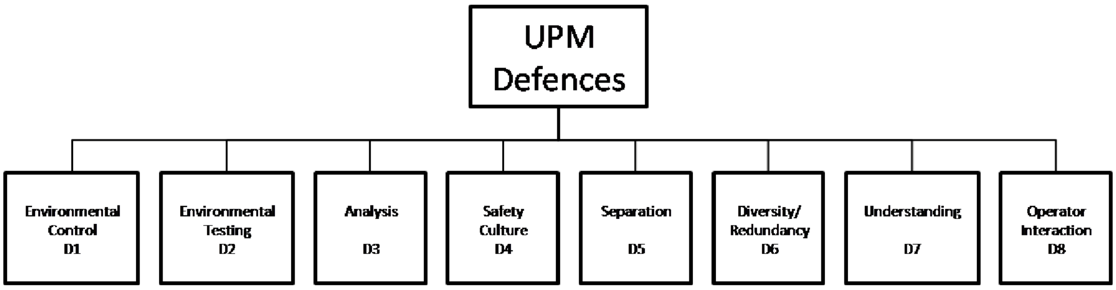

Figure A.1: The different UPM defences numbered from 1 to 8.

$$\hat{\beta} = \frac{s_1(x_1) + \dots + s_8(x_8)}{d} \tag{A.1}$$

A.4.1 An ID extension of UPM

An extension of the UPM applies Influence Diagrams (IDs). IDs are an extension of Bayesian Belief Networks. A more general introduction to Bayesian Belief Networks is given in Quigley et al. (2001).

The ID extension method, (Zitrou et al., 2004), assumes that there are two main factors that result in the occurrence of a CCF. The first is the occurrence of a root cause while the second is the existence of a coupling factor that creates dependency conditions among the components and induces these to fail due to the same root cause. The two types of failures have the following sub-groups

- Root cause events

  design

human

internal to component

maintenance

procedures

external environment

- Coupling factor events

  operational

  hardware

  environment.

In addition, the ID extension model considers different defensive measures which can be taken, see Figure A.1. Defence actions may be applied at reducing root causes, coupling factors or both.

The variables in the ID network are now given as:

- The root causes which lead to CCFs
- The coupling factors that create the conditions for CCFs to occur
- The defence actions
- A chosen reliability rate or CCF rate

The ID network will portray the cause-and-effect relationship between the root causes and the coupling factors with the CCF rate. In addition, there are also the defence measures against the root causes and/or the coupling factors. The defence parameters are deterministic variables representing different decision alternatives. These variables may be adjusted according to later improvements or such.

The UPM further assumes that failures occur independently and with a constant rate. The failure events caused by root cause i is given as a Poisson process with rate R_i, $i = 1, ..., 6$. The probability of a failure event due to root cause i resulting in a CCF through a coupling mechanism j, $j = 1,2,3$, is expressed as

$$P_{ij} = P(\text{CCF via coupling mechanism } j | \text{event due to root cause } i).$$

The CCFs that result from a root cause i occur according to an independent Poisson process with rate

$$\Lambda_i = R_i \sum_{j=1}^{3} P_{ij}. \tag{A.2}$$

The next assumption is that a CCF event occurs due to only one root cause event and through only one coupling mechanism. Based on this assumption, the total rate for CCF events becomes

$$\Lambda = \sum_{i=1}^{6} \Lambda_i. \tag{A.3}$$

The construction of the ID network is done by consulting experts. This includes deciding which defences are relevant (and applied) for the different root causes or coupling factors. The level of defence also has to be addressed. In addition, the dependencies between the different defences must be investigated. Zitrou et al. (2007) provides a thorough description of the different aspects that are relevant and the process of designing the network.

The quantitative analysis which follows once the network is constructed, is perhaps the most complicated. The Phd.Thesis by Zitrou (2006, Chapter 5 and 6), describes the quantitative Bayesian approach in detail. The Bayesian model produces an estimate for $\lambda^{(c)}$, i.e. the failure rate at which common cause failures occur. The ID extension does not estimate β, but instead the method estimates the failure rate directly.

Bibliography

Apostolakis, G. and Moieni, P. (1987). The foundations of models of dependence on probabilistic safety assessment. *Reliability Engineering*, 18:177–195.

Bukowski, J. V. (2005). A comparison of techniques for computing pfd average. *Reliability and Maintainability Symposium*, Annual edition:590–595.

Bukowski, J. V. (2006). Using markov models to compute probability of failed dangerous when repair times are not exponentially distributed. *Reliability and Maintainability Symposium*, Annual Volume:273–277.

Bukowski, J. V. and Goble, W. M. (1995). Using markov model for safety analysis of programmable electronic systems. *ISA Transactions*, 34:193–198.

Edwards, C. H. and Penny, D. E. (1990). *Calculus and Analytic Geometry*. Prentice Hall College Div, 3. edition.

Fleming, K. (1974). A reliability model for common mode failures in redundant safety systems. Technical Report GA-A–13284, General Atomic Co., San Diego, Calif. (USA).

Hauge, S., Hokstad, P., Langseth, H., and Øien, K. (2006a). *Reliability Prediction Method for Safety Instrumented Systems. PDS Method Handbook.* SINTEF, NO-7465 Trondheim, NORWAY.

Hauge, S., Langseth, H., and Onshus, T. (2006b). *Reliability Prediction Method for Safety Instrumented Systems. PDS Data Handbook.* SINTEF, NO-7465 Trondheim, NORWAY.

Hokstad, P. (1988). A shock model for common-cause failures. *Reliability Engineering and System Safety*, 23:127–145.

Hokstad, P. (2005). Probability of failure on demand (pdf) - the formulas of iec61508 with focus on the 1oo2d voting. In *ESREL 2005, Gdansk, Polen.*

Hokstad, P. and Corneliussen, K. (2004). Loss of safety assessment and the iec 61508 standard. *Reliability Engineering and System Safety*, 83:111–120.

Hokstad, P., Maria, A., and Tomis, P. (2006). Estimation of common cause factors from systems with different numbers of channels. *IEEE Transactions on Reliability*, 55(1):18–25.

Hughes, R. P. (1987). A new approach to common cause failure. *Reliability Engineering*, 17:211–236.

IEC 615011 (2003). *IEC 61511 Standard. Functional safety - safety instrumented systems for the process industry sector.*

IEC 61508 (2000). *IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commision (IEC), Geneva. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.

ISA (2002). *ISA-TR84.00.02. Safety Instrumented Functions (SIF) - Safety Integrity Levels (SIL) Evaluation Techniques.* The Instrumentation, Systems, and Automation Society, 67 Alexander Drive P.O. Box 12277 Research Triangle Park, North Carolina 27709.

Johnston, B. D. (1987). A structured procedure for dependent failure analysis (dfa). *Reliability Engineering*, 19:125–136.

Lundteigen, M. A. and Rausand, M. (2007). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *Journal of Loss Prevention in the process industries*, 20:218–229.

Lundteigen, M. A. and Rausand, M. (2008). Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. *Reliability Engineering & System Safety*, 93(8):1208–1217.

NUREG-75/014 (1975). Reactor safety: An assessment of accident risk in us commercial nuclear power plants. Technical report, U.S. Nuclear Regulatory Commission, WASH-1400, Washington, DC.

OREDA (2002). *Offshore Reliability Data.* SINTEF Industrial Management, NO-7465 Trondheim, Norway, 4. edition.

Quigley, J., Sigurdsson, J., and Walls, L. (2001). Bayesian belief nets for managing expert judgement and modelling reliability. *Quality and Reliability Engineering International*, 17:181–190.

Rausand, M. and Høyland, A. (2004). *System Reliability Theory.* John Wiley & Sons, Inc., Hoboken, New Jersey, USA, 2. edition.

Ross, S. M. (2003). *Introduction to Probability Models.* Academic Press, 525 B Street, Suite 1900, San Diego, CA 92101 - 4495, USA, 8. edition.

Rottman, K. (1995). *Matematisk formelsamling.* Bracan forlag.

Rydén, J. and Rychlik, I. (2006). *Probability and Risk Analysis.* Springer-Verlag Berlin Heidelberg.

Smith, A. M. and Watson, I. A. (1980). Common cause failures - a dilemma in perspective. *Reliability Engineering*, 1:127–142.

Vesley, W., Dugan, J., Fragola, J., Minarick, J., and Railsback, J. (2002). *Fault tree handbook with aerospace applications.* NASA, Washington, DC 20546, 1.1 edition.

Wisse, B., Bedford, T., and John, Q. (2008). Expert judgement combination using moment methods. *Reliability Engineering and System Safety*, 93:675–686.

Zitrou, A. (2006). *Exploring a bayesian approach for structural modelling of common cause failures.* PhD thesis, The University of Strathclyde.

Zitrou, A. and Bedford, T. (2003). Foundations of the upm common cause method. *Safety & Reliability, ESREL 2003*, pages 1769–1775.

Zitrou, A., Bedford, T., and Walls, L. (2004). Developing soft factors inputs to common cause failure models. *PSAM 7/ESREL 04.*

Zitrou, A., Bedford, T., and Walls, L. (2007). An influence diagram extension of the unified partial method for common cause failures. *Quality Technology & Quantitative Management*, 4(1):111–128.