NTNU – Trondheim
Norwegian University of
Science and Technology

Quantification of Reliability Performance: Analysis Methods for Safety Instrumented System

Abraham Almaw Jigar

Master of Science in Mathematics (for international students)

Submission date:	June 2013
Supervisor:	John Sølve Tyssedal, MATH
Co-supervisor:	Marvin Rausand, IPK

Norwegian University of Science and Technology
Department of Mathematical Sciences

NTNU – Trondheim
Norwegian University of
Science and Technology

AkerSolutions™

Master Thesis

Quantification of Reliability Performance: Analysis Methods for Safety Instrumented System

Abraham Almaw

June 2013

Preface

The present report is the master's thesis written at the Department of Mathematical Sciences, Faculty of Information Technology, Mathematics and Electrical Engineering, NTNU. The thesis is part of the two-year international master's program at NTNU.

The title of the thesis is "Quantification of Reliability Performance: Analysis Methods for Safety Instrumented System" and is carried out under the supervision of Professor Marvin Rausand at the Department of Production and Quality Engineering at NTNU. Associate Professor John Sølve Tyssedal was my supervisor at the Department of Mathematical Sciences whose main task was to ensure that the report qualifies the requirements in the department. Moreover, the thesis is written in cooperation with Aker Solutions AS.

The thesis is on the subject of the reliability quantification methods of SIS suggested in annex B of IEC 61508-6 and the reader ought to have some knowledge about this standard. It is assumed that the reader has some basic knowledge about probability, preferably reliability analysis of safety systems, and is familiar with the content of the textbook *System Reliability Theory: Medels, Statistical Methods and Applications* by Rausand and Høyland (2004).

I will express my deepest and sincere gratitude to Professor Marvin Rausand for his excellent guidance, understanding and encouragement throughout my study at NTNU. Without his thoughtful and friendly approach it would have not been possible to produce this report. I would also like to thank my future colleagues at Aker Solutions AS, especially Thomas H. Garten, my advisor in the company, and Christopher A. Lassen for providing me with practical information and assistance through the case study.

Trondheim, June 08, 2013
Abraham Almaw

Abstract

The reliability performance of a safety instrumented system (SIS) can be determined by several analytical methods, such as simplified formulas, fault tree analysis and Markov analysis. These methods are mentioned in annex B of IEC 61508-6, but this part is not normative and the user may choose which method to use based on the specific operational characteristics of the SIS. Moreover, since it does not provide detailed explanations, proofs and generalized formulas for $k$oo$n$ architecture, it is difficult for the users to understand and use it as a guideline. The purpose of this report is to provide background and rationale for these and some other commonly used methods, i.e., the PDS method and Rausand's method, to compare them and suggest alternative methods to overcome some of their weaknesses, and to outline a procedure for their use.

This report provides detailed proofs of the IEC 61508 simplified formulas, i.e., the reliability block diagram approach, and extend them to general $k$oo$n$ architectures. Due emphasis is given to critically evaluate the PDS method and several issues are discussed; for example, the conditional relationship of DU and DD failures. As far as these failures required to be quantified separately, as the PDS method does, an alternative formula is developed that takes this relationship into account. Among the simplified methods the Rausand's method is the least detailed and the PDS method is the most. Nevertheless, the analytical and numerical results show that these simplified methods are very similar except some slight differences resulted from the respective levels of details they consider.

It is recognized that fault tree analysis (FTA) is always a good start during SIS reliability quantification, especially if the SIS is in the design phase. The report sets out a procedure and explores the proper formula in terms of correcting the optimistic approach used in the FTA. It is also noted that a hybrid of FTA and Markov analysis represents a SIS better since some flexibility in the quantification can be taken care of by Markov analysis.

Beside the advantages that has already been explored in Markov analysis, it is acknowledged and exemplified in the report that the model is appropriate to calculate "the average probability that the SIS fails *and* the process demand occurs", whilst the existing tradition is limited to calculating "the average probability that the SIS fails" without directly taking the process demands into account.

All these and other existing methods in the area assume constant failure rate though it is, indeed, unrealistic. This report introduces a new approach to quantify SIS reliability performance under the assumption of other lifetime distributions and is demonstrated thoroughly with Weibull distribution. The approach is verified both analytically and numerically for accuracy.

Furthermore, the report establishes a simple procedure that may help users to choose the most adequate method, among the methods covered in this report, based on the specific operational characteristics of the SIS. This is further demonstrated in a case study.

Finally, the limitations of the present work are noted and suggestions for some areas of further researches are given.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Many operations in the process industry and other application sectors involve inherent risks due to different hazards. A safety instrumented system (SIS) is installed to prevent the development of a hazard to an accident or to reduce the associated consequences. A SIS comprises sensors, logic solvers and final elements as illustrated in Figure 1.1. IEC 61508 [4] and IEC 61511 [5] are the two important standards in the process industry that provide a general framework and requirements for the design, development and operation of a SIS[1].

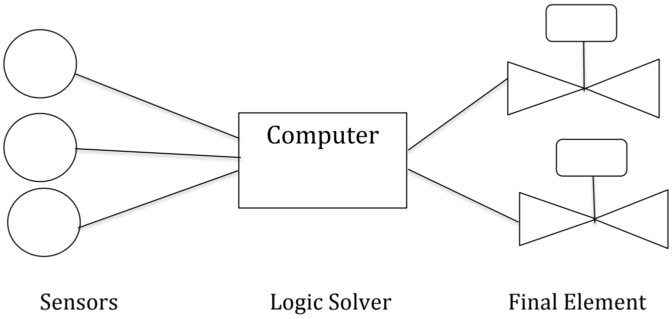

Figure 1.1: A simplified illustration of a safety instrumented system [20]

Beside other qualitative and semi-quantitative measures, the standards require the reliability performance of a SIS to be quantified. For a SIS operating in a low demand, i.e. where the

[1] These standards use the term electrical/electronic/programmable electronic (E/E/PE) safety systems as SISs.

frequency of demands is no greater than once per year, the average probability of failure on demand (PFD_{avg}) is used as a quantitative measure. The PFD_{avg} is the mean unavailability of a SIS to perform the specified safety function when a demand occurs [4].

The PFD_{avg} can be determined on the basis of several analytical methods, such as simplified formulas, fault tree analysis, Markov analysis, and Petri nets. These methods are mentioned in annex B of IEC 61508-6, but this part is not normative and the user may choose which method to use based on the specific operational characteristics of the SIS.

Many users choose the most simplified methods, i.e., the simplified formulas. However, the standard provides formulas only for some typical architectures without proof. It is, therefore, difficult for users to understand and use the standard as a guideline. Some authors [10, 12, 14] provide the proofs for these architectures by using different approaches (simple probabilistic approach and Markov analysis). Nevertheless, none of them provide general formulas for $k$oo$n$ architectures.

Beside IEC 61508, simplified formulas in the PDS method [23], and in Rausand and Høyland (2004) [20], hereafter referred to as Rausand's method[2], are also the commonly used methods. The PDS method is developed to overcome some of the weaknesses of the IEC 61508 simplified formulas and incorporates several factors that affect the unavailability of a SIS. Depending on the characteristics of the SIS under consideration, the most adequate method, among these simplified formulas, can be chosen. Failure to understand their limitations and differences may lead to unnecessary computational burden and/or erroneous results.

IEC 61508 provides a limited discussion on fault tree analysis (FTA) as a PFD_{avg} calculation method. FTA has been used for many years and several references are available such as [2, 18, 20]. A detailed discussion of FTA as a PFD_{avg} calculation method is presented by [16] and ISA [6]. Due to its static nature and the independency assumption of basic events, the method

[2] The approach is proposed by Professor Marvin Rausand. Although it is the foundation for many PFD_{avg} calculation approaches and has been used in many application sectors, the approach has never been mentioned after him.

does not sufficiently capture some relevant system behaviors and maintenance strategies. But, with a hybrid model of FTA and Markov analysis, it is possible to overcome this limitation [1].

Generally, there are two PFD_{avg} calculation methods in Markov analysis [9], i.e., based on time dependent and steady state probabilities. In IEC 61508, the former is regarded as the correct approach though no sufficiently detailed discussion is given. This approach of calculating PFD_{avg} is also cumbersome unless appropriate procedure is implemented to reduce sufficiently the number of states.

The term PFD_{avg} is less appropriate [12] since with the existing methods the average unavailability of a SIS is calculated without directly taking the process demands into account. All methods in the standards and books [4, 5, 6, 19, 20, 23] consider the process demand into account indirectly by roughly classifying the demand rate as low and high. It is argued in [7] that *the explicit incorporation of process demand is necessary to assess SIS safety performance appropriately, and a simple arbitrary division between low demand and high demand is insufficient*; and this argument is supported by some empirical results from Markov analysis.

All the PFD_{avg} calculation methods that have been developed so far are based on the assumption of constant failure rate. The primary argument is that the failure rate function of most equipment during the useful life period is flat so that it can be approximated to a time invariant constant failure rate λ, and exponential distribution can thus be used. Moreover, since the exponential distribution is fully characterized by its mean, the calculation is much more tractable than other lifetime distributions. However, it is recognized by analysts and researchers that the assumption is invalid in most real life situations, especially for rotating equipment.

1.2 Objectives

The main objective of this master thesis is to rationalize and compare selected methods for PFD_{avg} calculation, provide alternative methods to overcome their weaknesses (if any), discuss their applicability in different situations, and give recommendations to their use. To achieve these, we consider the following specific objectives:

1. Describe the background and rationale for the simplified formulas in IEC 61508, the PDS method, and Rausand's method.
2. Provide a detailed comparison of these simplified formulas.
3. Provide a procedure for PFD_{avg} calculation based on FTA.
4. Describe the background and rationale of Markov analysis, and assess and illustrate with examples the different PFD_{avg} calculation approaches.
5. Present and discuss the assumptions that are required to use the methods mentioned above.
6. Develop methodologies to overcome some of the limitations of the methods mentioned above.
7. Provide a procedure to choose the nearest possible approach based on the specific operational characteristics of the SIS.
8. Perform a case study and quantify the PFD_{avg} by each of the method mentioned above, and compare and comment the result.

1.3 Limitations

The focus of this thesis is on the reliability quantification methods of a SIS operating in a low demand mode of operation. It does not include methods for a SIS operating in a high demand mode. Moreover, qualitative and semi-quantitative aspects as well as organization interventions are outside the scope of the thesis.

The thesis uses IEC 61508 as a base and its main principles are inherited in the analysis. The quantification methods are thus based only on the random hardware failures, and so systematic failures are not taken into account in the analysis, as is IEC 61508. Safe failures and software failures are also not part part the analysis. As method evaluation, the thesis does not assess modeling of common cause failure (CCF).

1.4 Structure of the Report

The report is organized as follows: The first two chapters include brief descriptions, based on IEC 61508, on the design, development and operation of a SIS, and some clarification of terms and concepts used in the analyses. Chapter 2 provides a brief overview of parts of IEC 61508, and the requirements in the overall safety life cycle (SLC) as presented in the standard. Chapter 3 discusses the qualitative and quantitative aspects of functional safety requirements. Failure classification, and clarification of the definition and interpretation of the PFD_{avg} are also presented. Chapter 4 provides proofs and assumptions of simplified formulas, i.e., simplified formulas in IEC 61508 and the PDS method, Rausand's method, and an alternative method. Fault tree analysis is treated in Chapter 5. However, some of the important limitations of FTA (e.g., its static nature) are overcome by Markov analysis and it is considered in Chapter 6. It covers time dependent and steady state probabilities, and PFD_{avg} calculation by incorporating the process demand. All the SIS reliability quantification methods are based on constant failure rate assumption and to overcome this limitation a new approach is introduced in Chapter 7. In Chapter 8, the methods considered in the preceding chapters are discussed, compared and summarized. The analyses performed from Chapter 4-8 are demonstrated in a case study in Chapter 9. Finally, Chapter 10 presents concluding remarks and issues require further researches.

Chapter 2

Introduction to Safety Lifecycle

2.1 Introduction

A SIS is installed on the *equipment under control* (EUC) to perform the designated safety function[1]. An EUC can be any equipment (e.g., machinery, apparatus or plant used for manufacturing, processing, transportation and so on) that the SIS is installed for.

Several qualitative and quantitative aspects should be taken into account while implementing a SIS. These aspects normally encompass the whole life span of the SIS, i.e., each relevant activity from cradle to grave. Accordingly, IEC 61508[4] and IEC 61511[5], set out relevant requirements through the overall safety lifecycle (SLC). The focus of this chapter is to present the main issues in the overall SLC established in IEC 61508.

IEC 61508 is a generic standard for all lifecycle activities of systems comprising one or more electrical and/or electric and/or programmable electronic (E/E/PE) elements (SISs). Although the standard is restricted to E/E/PE safety systems, the principles can still be utilized, with special care, to systems that depend on other technologies such as mechanical, hydraulic, pneu-

[1] Safety function is a function to be implemented by a SIS or other risk reduction measures that is intended to achieve or maintain a safe state of the EUC, in respect of a specified hazardous event. Other risk reduction measures are measures to reduce or mitigate risk that is separated and distinct from SIS [4]. For example, in oil, gas and water separator a pressure relief valve may be installed beside the SIS. If the SIS is unable to act upon demand to maintain the safe state of the separator, the pressure level further increases; and then the relief valve may ruptures. It is the worst scenario but keeps the separator against over pressure. It is a typical instance of other risk reduction measure.

matic and so on.

It appears that the overall SLC is the fundamental concept of IEC 61508. Overall technical and nontechnical requirements of a SIS during design, development, operation, and maintenance to decommissioning are addressed using the overall SLC as a framework.

This general framework creates common understanding between involving parties (e.g., suppliers, system integrators, operators, consultants, regulatory bodies and so on) in the life span of the SIS. That is, the requirements in the SLC serve as common references for parties who are taking part in any phase.

The standard provides an overall risk-based approach for the implementation of a SIS. If the risk with respect to a certain hazardous event is above the specified tolerable level, one or more safety systems should be employed to prevent its escalation to an accident and/or to reduce the associated consequences. Thus, the SLC starts out with understanding the EUC and its potential hazards and end up with decommissioning of the implemented SIS. A discussion on the main activities in each phase of the SLC is presented in section 2.4. Before that, we briefly see the parts of the standard and their relationship.

2.2 Parts of IEC61508

In each step of the overall SLC, the standard gives a breadth and depth requirements for both software and hardware parts of a SIS. Examples and guidelines for the application of these requirements are also made available. As can be seen from Table 2.1, the standard consists of seven parts, of which the first three are normative meaning they are required for compliance and the last four are informative which solely provide information and examples.

Figure 2.1 shows the relationship among parts of the standard and phases of the overall SLC activities. Part one is the main part of the standard where the overall SLC is treated. In the realization phase of the overall SLC, part two and three take responsibility to set out the requirements using their respective lifecycle. The remaining parts supplement part one, two and three. The requirements are classified as technical and nontechnical as shown in the figure. To give a little more insight on the main objectives of the parts of the standard, we briefly summarize them as follows.

Table 2.1: Parts of IEC 61508 [4]

Parts	Title
Part 1	General requirements (required for compliance)
Part 2	Requirements for electrical/electronic/programmable electronic safety-related systems (required for compliance)
Part 3	Software requirements (required for compliance)
Part 4	Definitions and abbreviations (supporting information)
Part 5	Examples of methods for the determination of safety integrity levels (supporting information)
Part 6	Guidelines on the application of parts 2 and 3 (supporting information)
Part 7	Overview of techniques and measures (supporting information)

Part one: Fundamental requirements of the standard are presented in this part. One has to understand this part before starts working with the other parts. We have given emphasis on both technical and nontechnical issues presented in this part. This chapter discusses technical requirements through the overall SLC whereas nontechnical requirements are highlighted in Chapter 3.

Part two: This part is devoted to provide the requirements related to the hardware part of a SIS. Hardware related general framework is therefore provided so as to achieve the required safety function. Requirements are presented in a specific hardware SLC along with functional safety and functional safety assessment requirements. This part and part three are intended to be used by manufacturers since requirements are related to design and development of a SIS. It gives also information on installation, commissioning and final safety validation activities. However, it does not include requirements on operation and maintenance, which are covered under part one.

Part three: This part deals with the requirements related to software part of a SIS. Under the scope of part one and part two, softwares that are used in a SIS or used to develop a SIS should obey requirements set out in this part. To implement this part properly, it requires thorough understanding of part one and part two. Like in part two, software requirements are established through software SLC. Requirements are further extended on how to provide information and procedures on the operation, maintenance and modification of softwares to make available to the end users.

Part four: This part contains definitions and explanations of the terms and abbreviations used in the standard. It is important for both experienced and less experienced users to understand and implement the standard correctly.

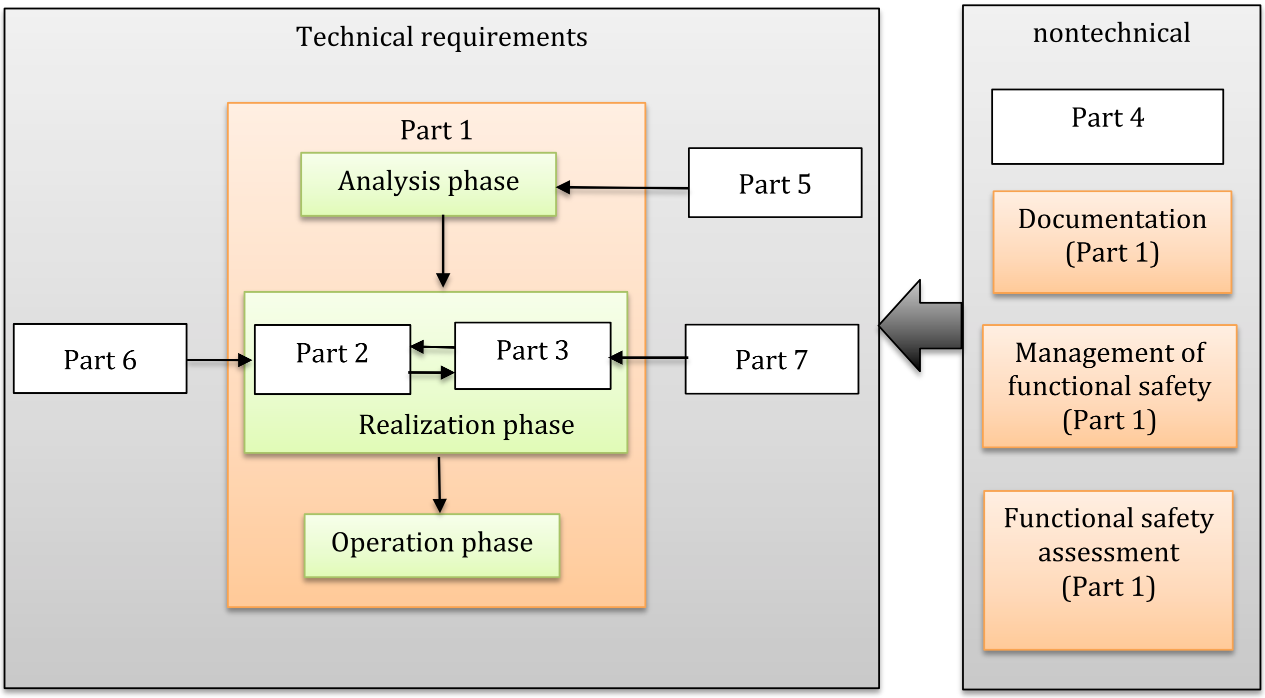

Figure 2.1: Safety lifecycle phases and parts of IEC 61508

Part five: Part five consists of seven informative annexes. These are examples and discussions on the application of part one, particularly on the analysis part of the overall SLC (see

Section 2.3). The focus is on the concepts and methods related to risk based safety integrity level (SIL) determination. A number of quantitative and qualitative methods are discussed with examples.

Part six: This part and part seven provide information and examples on the application of part 2 and part 3. Quantitative and semi-quantitative measures discussed to quantify hardware failures, for example $\mathrm{PFD}_{\mathrm{avg}}$. An example on the application of software integrity is also presented.

Part seven: This part provides information mainly for manufacturers regarding the techniques and measures required during the design and development of a SIS. These are related to controlling of random hardware failures, avoidance of systematic failures, achieving software safety integrity and some other concepts.

2.3 Overall Safety Lifecycle

The overall SLC is the keystone of the requirements in IEC 61508. All requirements and parts of the standard are directly linked to this fundamental concept. Broadly, the purpose is to demonstrate the development and documentation of a safety plan and its execution until decommissioning. It enables to approach all relevant activities during the whole life span of the SIS in a systematic manner so that the required safety performance can be achieved.

The overall SLC is shown in Figure 2.2. It should be noted that activities related to *verification, management of functional safety* and *functional safety assessment* are not shown in the figure for brevity reason. These requirements are however crucial to be considered in all the activities shown in the figure.

The objectives and requirements in each box of the overall SLC are presented in clauses 7.2-7.17 of IEC 61508-1. However, in box 10 a reference is made to part two and three of the standard, and thus the objectives and requirements of the realization phase are presented in these parts.

Note that box 11 is connected through hidden line because it is outside the scope of the standard.

The overall SLC model can roughly be classified into three phases such as analysis, realization and operation. In the first phase all possible hazards in the EUC shall be identified and their associated risk levels should be estimated. All possible risk reducing measures should be assessed, and determine whether or not a SIS is required afterwards. If so, a document called safety requirements specification (SRS) should be established after allocating the overall integrity requirements to the SIS. The second phase is the realization phase that deals with designing and manufacturing of the SIS based on the requirements in the SRS. The last phase encompasses the initial start up through operation, maintenance, repair and modification to final decommissioning.

To implement the standard properly, from the onset the organization should appoint one or more persons who take care of one or more activities in the overall SLC. Persons need to be competent and knowledgeable for the activity they are assigned (see clause 6 of IEC 61508-1).

2.3.1 Analysis

The analysis phase starts out with proper understanding of the EUC, its function and the environment around it. This is a prerequisite to identify comprehensively the likely sources of hazards and harmful events. During hazard identification all modes of operation (including abnormal and infrequent) and all reasonably foreseeable circumstances (including fault conditions, reasonably foreseeable misuses and malevolent or unauthorized actions) should be taken into account. An assessment shall then be done to decide whether or not the identified hazards are worth to be studied further. The following are some important checkpoints that should be considered before commencing a full-scale risk analysis:

- Make sure that the boundary of EUC and its control system are defined such that all equipments and systems associated with the relevant hazards and harmful events are included.

- Make sure that relevant external events are considered.

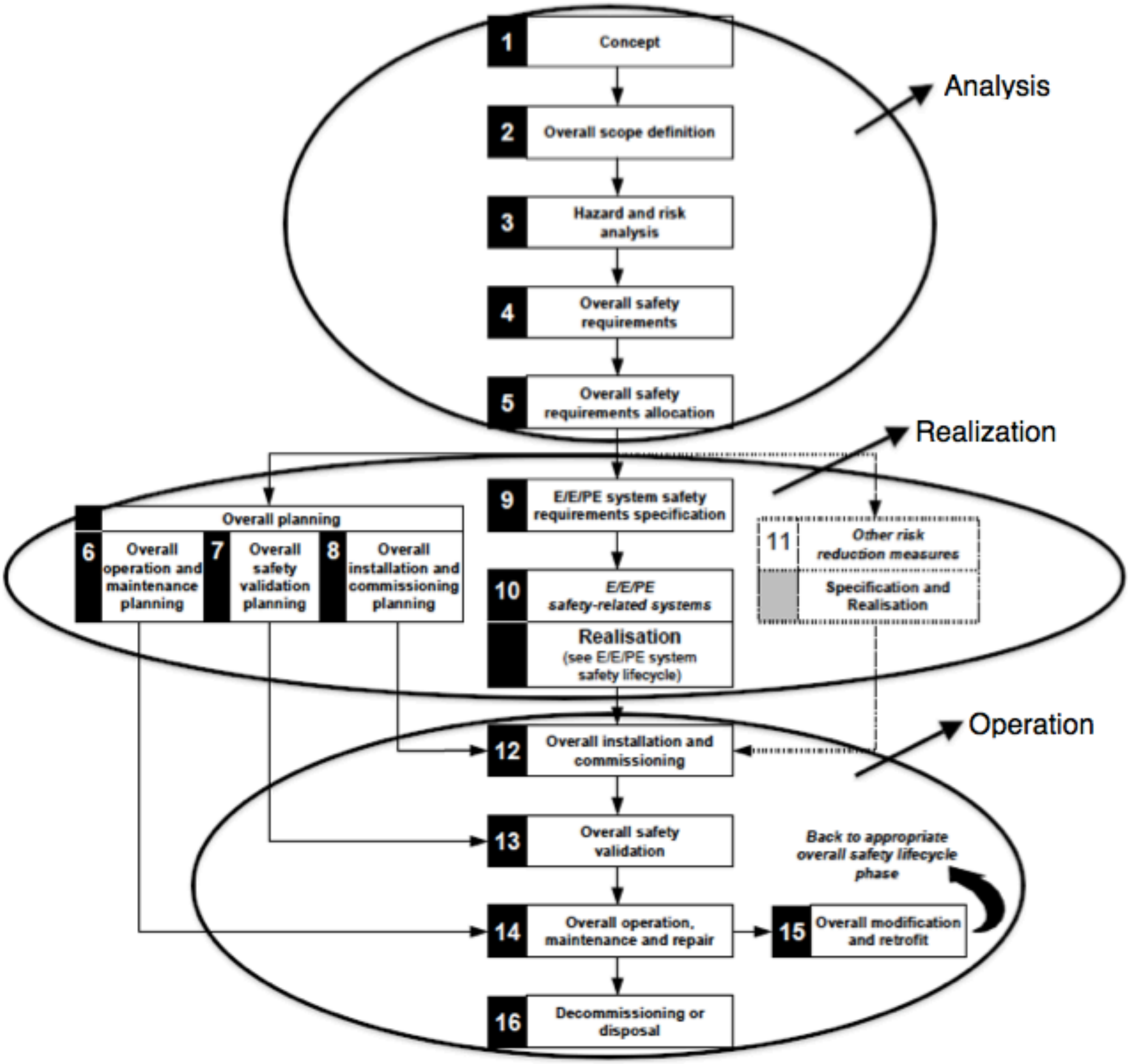
1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall safety requirements allocation
Analysis
Realization
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems
Realisation (see E/E/PE system safety lifecycle)
11 Other risk reduction measures
Specification and Realisation
Operation
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal

Figure 2.2: Overall safety lifecycle [4]

- Interaction of the EUC with other EUC should be taken into account from the development of a hazardous event point of view.
- Make sure that the types of the initiating events are clearly identified.

Once hazards are identified, sequences that lead to a hazardous event should be determined by using an appropriate risk analysis method. IEC 61508-5 suggests some well-known risk analysis techniques. The risk level for each hazardous event, often as a combination of likelihood and consequence, should be estimated. The standard stresses on the things that should be considered while conducting risk analysis (e.g., the tolerable risk for each hazardous event, measures taken to reduce or remove hazards and risks, the assumptions, and so on.). Note that priority should always be given to eliminate any of these event sequences by either modifying the process design or materials used.

Based on the results obtained from risk analysis, overall SRS (in terms of *overall safety function requirements* and *overall safety integrity requirements*) for both safety instrumented functions (SIFs)[2] and other risk reduction measures shall be established. Note that such requirements should be set out for each relevant hazardous event.

Overall safety function requirements at this level are specified in general terms since the method and technology that will be implemented is not yet known. Specifying what function the system is supposed to do when a demand occurs from the EUC is sufficient. For each safety function an overall safety integrity requirements, qualitatively and quantitatively, should then be established.

Risk can be reduced either by reducing the consequence or by reducing the frequency. To achieve the desired risk reduction for a certain hazardous event, one or more SIFs and/or other risk reduction measures may be implemented (see also Figure 3.1).

[2] A SIF is a safety function performed by SIS. A SIS may consist of one or more safety instrumented functions.

Therefore, the overall safety requirements should be allocated to SIFs and other risk reduction measures (the standard is applicable only if the risk reduction is done at least partly by a SIF). First the overall safety function is allocated to SIFs and other risk reduction measures, and then the target failure (safety integrity) is allocated to each safety function carried out by SIFs.

Note that the overall integrity requirement also affects the allocation of the overall safety functions. Consideration shall also be given on the effects of common cause failure (CCF) and whether or not there is dependency among the EUC control system, SIFs and other risk reduction measures. It is also important to consider the skills and resources available during the whole lifetime of the SIS. Allocation is not a straightforward issue, but some methods are suggested in IEC 61508-5.

The safety integrity requirement for each SIF is specified in terms an average probability of a dangerous failure on demand ($\mathrm{PFD}_{\mathrm{avg}}$). As can be seen from Table 2.2, IEC 61508 uses four categories where SIL 1 is the lowest (least reliable) and SIL 4 is the highest (most reliable). After proper allocation, each SIF falls in one of these four levels and the lowest possible probability that can be achieved with the current technology is 10E-5. That is, no single SIF shall claim a probability lower than this value. Together with semi-quantitative and qualitative measures, a SIL measures the reliability a SIF.

Table 2.2: Categories of target failure measures (SIL) for a SIF operating in a low demand mode of operation [4]

Safety Integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function ($\mathrm{PFD}_{\mathrm{avg}}$)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Finally, the safety requirements (in terms of safety function and integrity) shall be established neatly and made available to the developer(s). It shall contain as much relevant information in a clear and precise manner as possible. The standard provides detailed requirements regarding:

- how the structure and expressions of a SRS should look like
- the content related to safety functions requirements specification of SIFs
- the content related to safety integrity requirements specification of SIFs

2.3.2 Realization

This is the phase where the SIS is designed and developed such that requirements in the SRS are met. Part 2 (related to hardware) and part 3 (related to software) of the standard are devoted in realizing the required SIF. This phase can further be classified into three: pre-design and development, design and development, and post-design and development.

Pre-Design and Development

Realization begins with describing the design/architecture of the SIS under the so-called *SIS design requirements specification*. It is primarily derived from the SRS, but in here design requirements are specified at subsystem, element and/or component level. The specification should contain detailed descriptions in terms of hardware and software of the SIS.

Since it is the foundation for the realization of the SIS, ultimate care should be exercised to be able to demonstrate, with reasonable detail, how requirements in the SRS are fulfilled. In addition, appropriate methods shall be implemented to avoid some misspecification problems.

The development of SIS design requirements specification is an iterative process where it is updated over time and becomes more mature as the design progresses. Like in any other activities in the SLC, the document needs to be comprehensive and traceable for those who may use it in any activity in the SLC.

Design and Development

This phase is normally performed parallel with *safety validation planning* (box 7 in Figure 2.2). This is a plan containing proper procedures (activities) to be implemented to validate whether or not the SIS performs the safety function as desired, i.e., a plan to demonstrate, before commissioning, that the SIS satisfies all the requirements in the SRS and SIS design requirements specification. For example, the plan may include the environment under which the test is to take place, the pass/fail criteria (policy), words on how to deal with the results and the like.

Design and development is a broad, time consuming and resource-intense part of the overall SLC. The design, hardware or software, of a SIS shall meet all requirements related to

1. hardware safety integrity
2. systematic safety integrity
3. architecture of integrity circuits (ICs) with one chip redundancy
4. system behavior on detection of a fault
5. data communication processes

A slight overview of the first two requirements is presented below:

1) Hardware Safety Integrity: Hardware safety integrity requirement consists of requirements related to both

A) architectural constraints on hardware safety integrity, and

B) quantification of the random hardware failure

A) Architectural Constraints on Hardware Safety Integrity: Two possible routes have been suggested to achieve the maximum safety integrity level that can be claimed for a SIF.

I) Based on Hardware Fault Tolerance (HFT) and Safe Failure Fraction (SFF) Concepts: Based on the characteristics they possess, elements are classified as type A and B (see IEC 61508-2 p. 24). An element can be regarded as type A if for the components required to achieve the safety function:

- The failure modes of all constituent components are well defined; and
- the behavior of the element under fault conditions can be completely determined; and
- there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met

An element can be regarded as *type B* if for the components required to achieve the safety function

- The failure mode of at least one constituent component is not well defined; or
- The behavior of the element under fault conditions can be completely determined; or
- There is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures.

The estimates for HFT and SFF can be obtained as follows:

- HFT is the number of faults that can be tolerated before loss of the safety function (e.g., A HFT of n means that $n+1$ is the minimum number of faults that could cause a loss of the safety function).
- Procedures to determine SFF are described in Annex C of IEC 61508-2. Accordingly,

$$\mathrm{SFF} = \frac{\sum \lambda_s + \sum \lambda_{DD}}{\sum \lambda_s + \sum \lambda_{DD} + \sum \lambda_{DU}} \tag{2.1}$$

  where λ_s, λ_{DD} and λ_{DU} are safe, dangerous detected and dangerous undetected failure rates respectively.

Once the above attributes are estimated, the maximum possible SIL that can be claimed for a SIF can be determined based on Table 2.3. Moreover, depending on the situation the table can also be used:

- To determine the HFT requirements for an element/subsystem given the required SIL of the safety function and the SFFs of the elements/subsystems used.

- To determine the SFF requirements for elements given the required SIL of the safety function and the HFT of the subsystem.

Table 2.3: Maximum allowable safety integrity by type A and type B element or subsystem [4]

SFF of an element	HFT - Type A			HFT - Type B		
	0	1	2	0	1	2
<60%	SIL 1	SIL 2	SIL 3	Not Allowed	SIL 1	SIL 2
60% − <90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% − <99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

II) Based on Component Reliability Data from Feedback from End Users, Increased Confidence Levels and HFT for Specified SIL: The effect of random hardware failures based on component reliability data is quantified. In here, failure data uncertainty analyses need to be performed in relation to target failure measures. The system then has to be improved to make sure that the confidence of attaining the target failure measure is greater than 90%.

B) Quantification of Random Hardware Failures: For each SIF, the achieved SIL has to be demonstrated through an appropriate reliability quantification method. If the integrity requirement for a particular SIF is not achieved, different factors (e.g., component reliability, diagnostic coverage, test interval, redundancy, and so on) should be reassessed and improved. Several PFD_{avg} calculation methods are studied in detail in Chapter 4-8, and a case study on the application of these methods is presented in Chapter 9.

2) Systematic Failures: During design and development, hardware and software, necessary attentions should be given to avoid systematic failures. Often due to their nature, it is difficult to avoid or control such failures. There are always some residuals left in the system, especially the ones related to operational failures. However, it is possible to reduce their effect up to some extent by exploiting appropriate methods, procedures and/or documentation.

It is also necessary to make sure that the design could not cause other safety system(s) to fail. Analysis should be conducted to determine this, and if it causes the design has to be changed (preferred) or the likelihood has to be reduced.

In most cases employing a proven element/subsystem will reduce the effect of systematic failures. According to the standard, an element/subsystem is said to be proven if it has a clear restricted and specified functionality and when there is adequate documentary evidence to demonstrate that the likelihood of any dangerous systematic faults is low enough that the required safety integrity levels of the safety functions that use the element is achieved.

There are several causes of systematic failures (see Section 3.5.1), and due to their deterministic nature the standard does not require them to be quantified (see Section 3.4). However, the PDS method [23] proposed methods and data to model their effect statistically (see Chapter 4 and 8).

Post-Design and Development

Once the design and development of the SIS is completed, components/elements/subsystems need to be integrated correctly to have a complete SIS. It shall then be tested to see whether they interact each other as intended or not. It should also be tested to see whether or not it performs *only* its intended function. If tests reveal any unpleasant result, design change or modification is required and the procedures should again obey all the requirements. Whenever changes are made, version numbers should be written clearly on the document.

It is part of the realization phase to provide procedures that will be implemented during operation and maintenance activities so as to maintain the achieved performance. It may consist issues related to the proper actions that need to be done by the operators (e.g., during start up, fault condition, shut down), maintenance procedures (e.g., fault diagnoses, repair, revalidation), documentation of system failure and component failure data, and so on.

SIS validation can be considered as the final activity of realization phase. This has to be done according to the plan developed in the beginning of the phase. It encompasses all aspects of the requirements. The integrated system needs to be tested for validity against the requirements in the SRS and SIS design requirements specification as well as the procedures developed to be implemented during operation and maintenance. Note that in some cases validation activity may be performed after installation is completed.

If the validation activity is not satisfactory, appropriate modifications, corrections or enhancements should be done. After these activities the system should be revalidated, reverified and documented with another version.

In parallel with the realization phase, it has suggested in the standard to make an *overall* plan related to

- operation and maintenance,
- safety validation, and
- installation and commissioning

The objectives and requirements of these plans are mentioned in IEC 61508-1, p. 35-38.

2.3.3 Operation

This is the longest phase of the overall SLC. According to our classification, operation phase begins with installation and commissioning. This has to be done according to the plan established earlier. If discrepancies occur during installation, it has to be documented properly— including the decision made to deal with it.

After installation and commissioning, and before proper operation commences, the SIS has to be tested for validation. This is the overall validation activity performed to compare the result with the overall safety requirements. This activity has to be done in accordance with the overall validation plan. If the validation result does not meet with the desired result, the problem area and the decision taken to correct the problem has to be documented.

To maintain the achieved safety performance, the manufacturer should provide a technical document containing proper activities to be done during operation, maintenance and repair. Any failure and corrective actions made during operation, maintenance and repair need to be documented chronologically.

If modification is required, first a procedure needs to be established to make sure that the requirements are maintained during and after the activity. Procedures in turn are based on the results gained from impact analysis, i.e., an assessment to predict whether or not the proposed modification could have effect on the overall functional safety.

The very end activity of the overall SLC will then be decommissioning or disposal. Impact analysis should be conducted to assess whether or not the proposed decommissioning activity has an effect during or after the activity. Based on the result, a decision needs to be made and a detailed procedure shall be established.

Chapter 3

Functional Safety

3.1 Introduction

To be able to install and operate a SIS that complies with IEC 61508, all functional safety requirements need to be satisfied. These requirements are broad that cover the whole lifecycle of the SIS. In this chapter, a brief discussion of functional safety and functional safety requirements is presented.

3.2 What is Functional Safety?

IEC 61508 differentiates the term functional safety from safety and they are defined as follows (IEC 61508-4):

- *Safety* is the freedom from unacceptable risk[1].
- *Functional safety* is part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the SIS and other risk reduction measures.

The standard uses the term functional safety instead of safety [2]. The difference is, however, not clear enough and many use them interchangeably. What conditions demarcate functional

[1] Risk is the combination of the probability of occurrence of harm and the severity of that harm. Harm is a physical injury or damage to the health of people or damage to property or the environment (IEC 61508-4).

[2] It is also believed that the term functional SLC is the correct term instead of just SLC though the adjective *function* is removed

safety from safety? What term do we use in situations where safety depends only on passive systems? An example of passive system may be a separator is equipped with a strong material that resists extreme pressure. Does functional safety limited to the safe state of the *EUC*, and safety does not?

It seems that active and passive systems in the functional safety definition are mixed up since other risk reduction measures can also be passive systems. Safety systems are used as a barrier to cut the development of a hazard to an accident, and these systems are either SISs or other risk reduction measures. This implies that functional safety is a safety that depends on any barrier. However, this does not seem the intention of IEC 6508 to use the term functional safety.

We therefore believe that the definitions can be understood or altered in such a way: Safety, as defined in IEC 61508, is the freedom from unacceptable risk. But, a safety is regarded as a functional safety if it depends on the well functioning of active systems that act upon a demand. That is, a safety that depends on passive systems (e.g., fire wall) cannot be regarded as functional safety.

3.3 Safety Instrumented Systems

Based on the risk calculated for the EUC, a decision should be made on whether or not a SIS is required to achieve the desired functional safety, see Figure 3.1. During risk evaluation, priority must always be given for the elimination of a hazard at source, if possible. If this is not possible, one or more SISs and/or other risk reduction measures needs to be implemented to achieve a tolerable risk level.

A SIF receives requirements in terms of both safety function and safety integrity. Thus, to maintain the desired risk reduction satisfactorily, these two requirements shall be satisfied. The safety function requirements for an SIF imply two things [20]: First, it should perform the intended (predefined) function when a process demand occurs within a reasonable period of time. Second, it should *not* be activated without a process demand from the EUC with respect

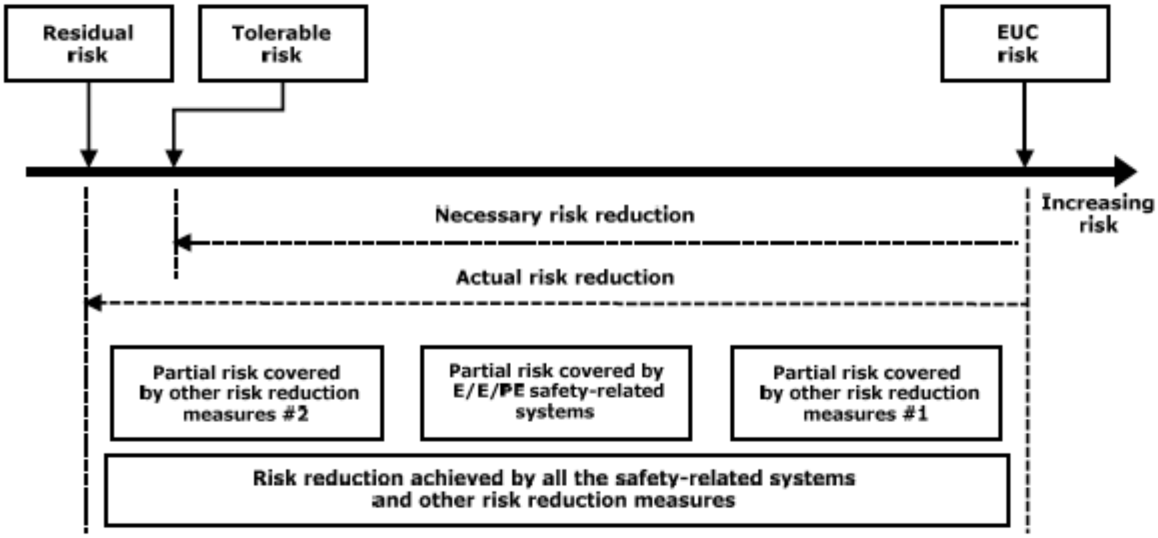
Residual risk
Tolerable risk
EUC risk
Increasing risk
Necessary risk reduction
Actual risk reduction
Partial risk covered by other risk reduction measures #2
Partial risk covered by E/E/PE safety-related systems
Partial risk covered by other risk reduction measures #1
Risk reduction achieved by all the safety-related systems and other risk reduction measures

Figure 3.1: General risk reduction concept [4]

to the hazardous event under consideration.

Safety integrity requirements can further be classified as qualitative, semi-quantitative and quantitative. Qualitative requirements are mainly concerned with techniques and measures that should be implemented to avoid and control both hardware and software systematic failures (see Section 3.4). Semi-quantitative requirements are related to the behavior of components, and are expressed in terms of architectural constraints (see Section 2.3.2). Quantitative requirements measure the probability that an SIF satisfactorily performs specified safety functions under all the stated conditions within a stated period of time (see Section 3.5).

3.4 Qualitative Requirements

The following are key qualitative requirements to achieve the required functional safety.

- Management of functional safety
- Verification
- Functional safety assessment

The main objectives of the management of functional safety in IEC 61508 as described in Exida[17] are the follows:

- Structure, in a systematic manner, the phases in the overall safety lifecycle that shall be considered in order to achieve the required functional safety of the SISs
- Specify the management and technical activities during the overall, hardware and software SLC phases which are necessary for the achievement of the required functional safety of the SIS.
- Specify the responsibilities of the persons, departments and organizations responsible for each overall, hardware and software SLC phase or for activities within each phase.
- Specify the necessary information to be documented in order that the management of functional safety, verification and the functional safety assessment activities can be effectively performed.
- Document all information relevant to the functional safety of SIS throughout its SLC.
- Document key information relevant to the functional safety of SIS throughout the overall SLC.
- Specify the necessary information to be documented in order that all phases of the overall, hardware and software SLC can be effectively performed.
- Select a suitable set of tools, for the required safety integrity level, over the whole SLC which assists verification, validation, assessment and modification.

Verification is the process of demonstrating by examination that the objectives and requirements of each activity (a box in the SLC) in the SLC (overall, hardware and software) are fulfilled. Given the inputs for an activity the output should by analyzed using appropriate techniques, including logical reasoning, to see whether it is in line with the standard. Note that verification does not have the same meaning as validation. Validation is a process of demonstrating by examination that particular requirements for a specific use are fulfilled.

Functional safety assessment is the process of assessing whether the achieved functional safety by a SIS is adequate enough and compliance with IEC 61508. It is an overall assessment in the sense that all activities in the SLC (overall, hardware and software) including management of functional safety, verification and documentation need to be assessed for adequacy. One or more competent persons may carry out this activity.

3.5 Quantitative Requirements

IEC 61508 requires the failure probability of a SIF due to random hardware failures to be quantified statistically, i.e., the PFD_{avg}. The main factors for the unavailability of a SIF are component failure rate, capability and frequency of function testing, and diagnostic coverage. To quantify the $\mathrm{PFD}_{\mathrm{avg}}$ with reasonable accuracy, better understanding of the nature of failure causes and effects is important.

3.5.1 Classification of Failure

Component failures can be classified as random hardware failures (physical) and systematic failures (nonphysical) based on the nature of their causes. According to the standard, the demarcation feature between them is that the failure rate arising from random hardware failures can be estimated statistically with reasonable accuracy whereas the failure rate arising from systematic failures cannot be estimated with reasonable accuracy due to their deterministic nature. Systematic failures often arise due to design, installation and human error whereas random hardware failures are due to natural degradation (aging) and stress [15]. Some of the respective common causes are shown in Figure 3.2. For detail discussion on the features of systematic failure causes refer ISA [6].

In the PDS method [23] a slightly different and detailed classification is proposed. Unlike IEC 61508, aging is regarded as the only cause for random hardware failures, and failures due to excessive stresses are categorized under systematic failures.

As shown in the figure, random hardware failures and systematic failures can further be clas-

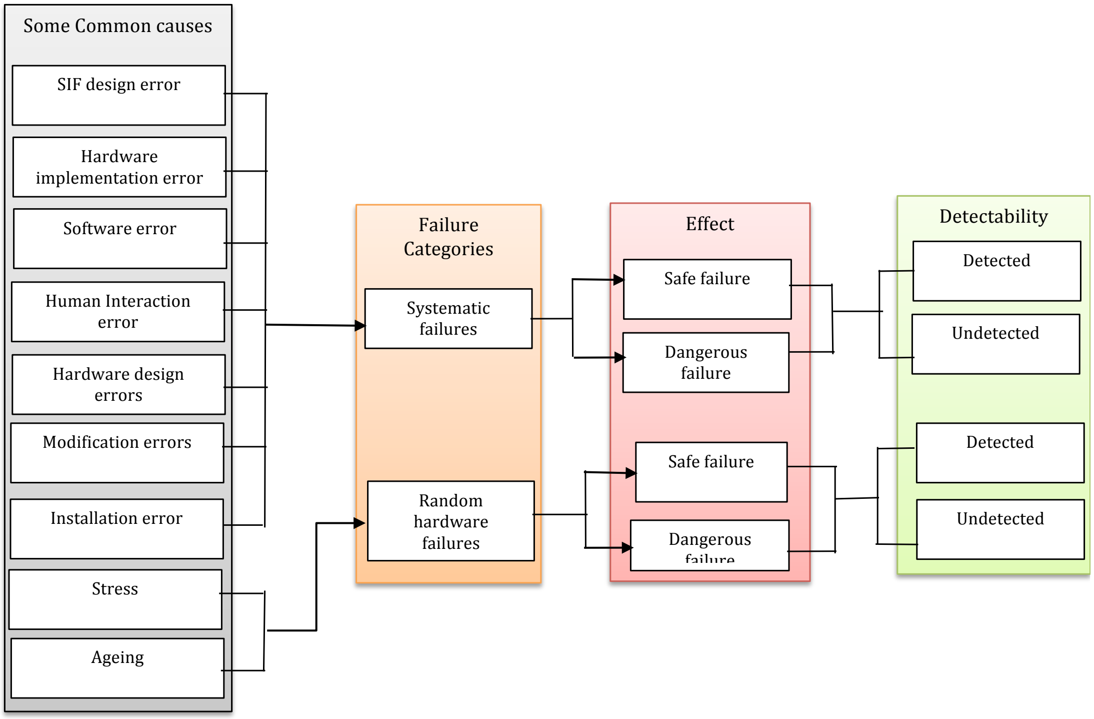

Figure 3.2: Failure classification (adopted from [15])

sified based on their effects as safe/dangerous, and based on detectability as detected/undetected failures.

Dangerous Failure is a failure of a component that:

- prevent a safety function from operating when required (demand mode) such that the EUC is put into a hazardous or potentially hazardous state, or
- decreases the probability that the safe function operates correctly when required

Dangerous Undetected (DU) is a dangerous failure that is revealed only by testing or when a demand occurs.

Dangerous Detected (DD) is a dangerous failure that is detected by diagnostic testing immediately when it occurs.

Safe Failure is a failure of a component that:

- results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state, or

- increases the probability of the spurious operation of the safety function to put the EUC (part thereof) into a safe state or maintain a safe state

These failures can further be classified as

Safe Undetected (SU) is a non-dangerous failure that is not detected by diagnostic testing.

Safe Detected (SD) is a non-dangerous failure that is detected by diagnostic testing.

For a better understanding of the above classification we recommend the reader to consult the discussion and example given by Rausand and Høyland [20] (2004), p. 423-426.

A failure rate splits into detected and undetected failure rates based on the extent to which the diagnostic testing is able to detect immediately when it occurs. This is measures by diagnostic testing coverage factor designated as DC and quantified as percentage. (The method for calculating DC is given in Annex C of IEC 61508-2 and examples are given in Annex C of IEC 61508-6). Mathematically

$$\lambda_{\text{Detected}} = \lambda \cdot \text{DC} \quad \text{and} \quad \lambda_{\text{Undetected}} = \lambda \cdot (1 - \text{DC})$$

Failures can further be classified as failures due to independent causes or common causes. Independent failures are failures that affect a certain component independent of the others whereas common cause failure (CCF) is a concurrent failure that causes more than one components in parallel. Beta factor model is a commonly used approach to model CCF. The factor (β) is used to partition the total failure rate into failures due to independent and CCF. (Annex D of IEC 61508-6 gives informative guidance for the quantification of β).

Beta factor model assumes that a component only fails due to either of these two causes so that $\lambda = \lambda^I + \lambda^C$. Therefore

$$\lambda^{\text{C}} = \beta \cdot \lambda \quad \text{and} \quad \lambda^{\text{I}} = \left(1 - \beta\right) \cdot \lambda, \quad \text{Where} \quad \beta = \frac{\lambda^{\text{C}}}{\lambda^{\text{I}} + \lambda^{\text{C}}}$$

Generally, there are two approaches of modeling beta factor model: the standard and multiple beta factor model. The standard is the simplest approach that assumes given a CCF occurs, all n identical parallel components fail with probability β regardless of the size of n and the type of architecture. IEC 61508, ISA and several standards and guidelines use this approach whereas the PDS method uses multiple beta factor model instead. But, IEC 61508 also suggests multiple beta factor model and some estimates are presented. In this model, for example, given a CCF occurs, the probability that all components in 1oo3 architecture fail is half of the probability that two components in parallel fail. The architecture of a system determines the factor to be used, and there is a non-zero probability that only a subset of components fails, given a CCF occurs. A detailed derivation and discussion as well as comparison with the standard beta factor model is given in the PDS method handbook [23].

In IEC 61508, unlike the PDS method, the beta factor associated with DU failures (β) is distinguished from DD failures (β_D), and a relation $\beta_\mathrm{D} = \frac{1}{\mathrm{M}} \cdot \beta$ is established[3]. Among those failures that are detected by diagnostic testing a fraction that has CCF is equals to β_D.

3.5.2 The Average Probability of Failure on Demand (PFD$_\mathrm{avg}$)

Generally, there are two approaches of calculating PFD$_\mathrm{avg}$ [9]. The average probability can be computed as a steady state probability or as an arithmetic mean of instantaneous probabilities over a certain period of time (usually the test interval). The steady state probability measures the *unavailability* and the arithmetic mean measures the *unreliability* of a system.

IEC 61508 recommends the unreliability approach. Under the assumption of perfect function testing and exponential distribution, since the item is renewed after each function test, the PFD$_\mathrm{avg}$ in the first test interval can represent the rest test intervals (see, e.g., the Rausand's method in Chapter 4).

In the unavailability approach the PFD$_\mathrm{avg}$ is not a function of time since the steady state is achieved by setting the time to infinity. Thus, this approach may not be suitable to quantify the

[3] Often $M = 2$, i.e., if $\beta = 10\%$, then $\beta_\mathrm{D} = 5\%$.

performance of a SIS as it is subject to periodic function testing. The well-known unavailability formula for a single component is

$$\bar{A} = \frac{\lambda}{\lambda + \mu}$$

Where the failure rate (λ) and repair rate (μ) are assumed to be constant with respect to time (refer [22] for the derivation of the formula).

The unreliability approach is used in the methods presented in Chapter 4, 5 and 7, and both unreliability and unavailability approaches are used in Chapter 6.

Several methods have been suggested to calculate PFD_{avg} but none of them fit well with all kinds of systems/situations so that it is up to the analyst to choose the best method for his particular system. Due to its tractable nature all methods assume exponential distribution, i.e., the failure rate is constant with respect to time. A new method of calculating PFD_{avg} under the assumption of other lifetime distributions is proposed in Chapter 7.

Remark: The *probability of failure on demand* measures simply the probability that a SIF fails to perform the intended function. Unless the analyst deliberately includes, no SIS reliability formula takes the the process demand into account. Therefore, the results from these formulas should be interpreted as the probability that a SIF fails — *not as the probability that a SIF fails upon demand*. A method of incorporating a process demand directly into the calculation is discussed in Chapter 6.

Chapter 4

Simplified Formulas

4.1 Introduction

In this chapter some well-known simplified formulas for PFD_{avg} calculation are studied. The first purpose is to make available a sound proof for the *reliability block diagram approach* suggested in IEC 61508 as design, development and operation of a SIS should be in line with this standard. Some authors, for example [10, 14], have provided proof and discussion on this approach. Nonetheless, different approaches have been used and none of them provide a general formula for $k$oo$n$ architecture. We are thus aimed to prove and present the approach in a simple and intuitive manner so that it will be accessible for engineers even outside the field, and further to establish a general formula for $k$oo$n$ architecture.

Moreover, three simplified formulas are discussed: the Rausand's method, the PDS method and a method introduced in this report. Since the Rausand's method explains in a simple manner what we are actually quantifying during PFD_{avg} computation and further the last two methods are dependent on it, we start out our presentation with it. The last two methods are more or less the extension of the Rausand's method.

4.2 Rausand's Method

This method has been widely used in several application sectors. It has also been served as input for other $\mathrm{PFD}_{\mathrm{avg}}$ calculation approaches, for example in fault tree analysis (this is discussed in Chapter 5). The following are the main features of the method:

- It is developed under solid mathematical reasoning.
- It is easy to understand and apply.
- It captures the main contributor of the $\mathrm{PFD}_{\mathrm{avg}}$ (dangerous undetected (DU) failures).

In reliability analyses, formulas are meaningful only if the analyst has due understanding about the underlying assumptions. Before we present the formulas, it is important to look at the assumptions.

- The failure rate of a component is assumed to be constant over its lifetime, i.e., the time to DU failure is assumed to follow the exponential distribution.
- Components are statistically independent, i.e., the failure of one component does not affect the failure of any other component either positively or negatively.
- The average of the instantaneous probabilities is assumed to represent the $\mathrm{PFD}_{\mathrm{avg}}$. Therefore, the resulting probabilities out of this model should always be interpreted on *average*.
- Hidden failures are detected by function testing and its coverage is assumed to be 100%. Moreover, repair actions are assumed to be perfect to restore a failed component without introducing any other potential failures. Therefore, the component is *as good as new* after function testing and repair.
- A component is assumed to be performing its intended function without any problem as long as DU failures are not occurred. This means that either there is no diagnostic testing (all failures are DU) or upon detection of DD failures, it is assumed that the system goes into safe state and/or perfect compensating measures are available.
- The required time to test and repair a component is assumed to be negligible.

- For each subsystem there is a single function test interval.
- The term $\lambda_{\text{DU}} \cdot \tau$ should be small enough to allow $\mathrm{e}^{-\lambda_{\text{DU}} \cdot \tau} \approx 1 - \lambda_{\text{DU}} \cdot \tau$, that is $\lambda_{\text{DU}} \cdot \tau \leq 0.2$ [23].

The approach treats DU failures only. For systems that have significant diagnostic testing with relatively long online restoration this approach cannot solely be used.

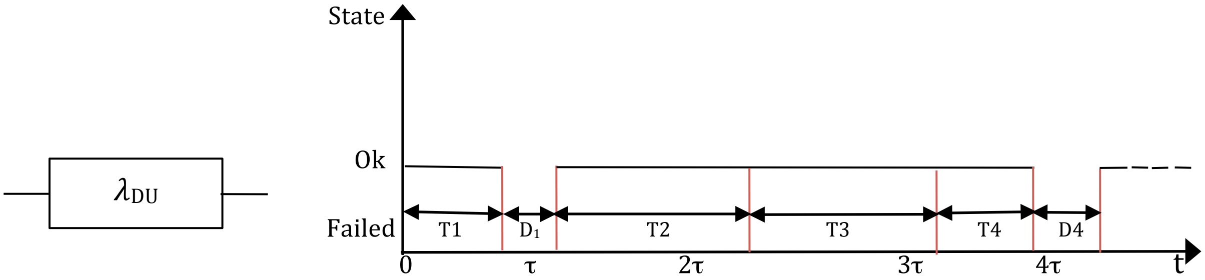

Figure 4.1: Possible DU failure propagation over time

Figure 4.1 shows a possible trajectory on how DU failures could occur over time. As can be seen from the figure, for test interval i we have down time and up time, that are respectively designated as D_i and T_i. The trajectory of course depends on the DU failure rate. Since constant failure rate is assumed, the distribution function of exponential distribution with parameter $\lambda_{\text{DU},i}$ ($F_i(t)$) can be used to generate the probability of the occurrence of DU failure before time t in the i^{th} test interval.

Let T_i be the time to DU failure for a component in the i^{th} test interval. Hence, for $(i-1)\tau \leq t < i\tau$

$$F_i(t) = P(T_i \leq t) = 1 - e^{-\lambda_{\text{DU},i}\, t} = 1 - e^{-\lambda_{\text{DU}}\, t} = F(t)$$

With the assumptions of constant failure rate and perfect function testing, the distribution functions are exactly the same in every test interval. Thus, the above equality holds. Figure 4.2 shows how it appears over several test intervals. It is therefore straightforward that the first test interval can represent all test intervals.

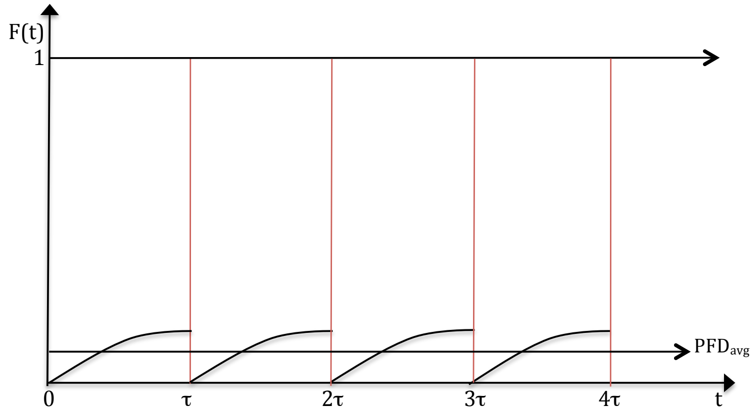

Figure 4.2: A saw tooth curve

It has been a custom to express the failure probability as an *average* probability. It seems more reasonable and handy than expressing it with instantaneous failure probability. It has also an important implication especially when we are working with exponential distribution, i.e., with average failure probability, we can tell the long-run proportion that the system is unavailable. Therefore, as long as proper function testing, repair and maintenance are performed, the system can maintain the calculated failure probability throughout its lifetime. This is one of the reasons why people always tend to assume constant failure rate. However, under the assumption of increasing failure rate, e.g. Weibull distribution, it is not possible to find the long-run proportion that the system is unavailable since the average failure probability increases continuously over the test intervals. This means that if we plot the average PFD over time, it will be a step function plot. This topic is further discussed in detail in Chapter 7.

Averaging can be done by adding instantaneous probabilities in a test interval and divide it by the interval.

$$\mathrm{PFD_{avg}} = \frac{1}{\tau}\int_0^{\tau} F(t)\mathrm{d}t = 1 - \frac{1}{\tau}\int_0^{\tau} R(t)\mathrm{d}t \tag{4.1}$$

Where $R(t)$ is the survival function of a component or system that is equal to $1 - F(t)$. This is simply the *average* proportion of time that the system is down. Intuitively, it is the ratio of expected down time and the test interval (τ) (see Figure 4.1). Mathematically

$$\mathrm{PFD_{avg}} = \frac{\mathrm{E(D)}}{\tau} \qquad \text{Where } \mathrm{E(D)} = \int_0^{\tau} F(t)\mathrm{d}t \text{ is the MDT.} \tag{4.2}$$

We can calculate PFD_{avg} for a single component as

$$\text{PFD}_{\text{avg}} = 1 - \frac{1}{\tau}\int_0^{\tau} e^{-\lambda_{\text{DU}}t}\text{d}t \le \frac{\lambda_{\text{DU}}\tau}{2} \tag{4.3}$$

The PFD_{avg} can thus be interpreted as the product of constant failure rate over time (λ_{DU}) and the expected down time ($\tau/2$) given that the failure occurs in a random point in time in a test interval. With this interpretation, several factors that affect the unavailability of a SIF can be quantified, for example, safety unavailability during planned testing and unplanned testing (it is repeatedly used in the subsequent sections).

Suppose all components in a $k$oo$n$ architecture have the same failure rate. The architecture fails if and only if all $n-k+1$ components fail, and we have $\binom{n}{n-k+1}$ such combinations (MCSs). If all MCSs were independent, PFD_{avg} is the sum of the individual average PFDs. That is,

$$\begin{aligned}\text{PFD}_{\text{avg}} &\approx \binom{n}{n-k+1}\cdot\frac{1}{\tau}\int_0^{\tau}\left(1-\text{e}^{-\lambda_{\text{DU}}t}\right)^{n-k+1}\text{d}t \\ &\approx \binom{n}{n-k+1}\cdot\frac{1}{\tau}\int_0^{\tau}(\lambda_{\text{DU}}t)^{n-k+1}\,\text{d}t = \binom{n}{n-k+1}\cdot\frac{(\lambda_{\text{DU}}\tau)^{n-k+1}}{n-k+2}\end{aligned} \tag{4.4}$$

However, MCSs are not independent since one or more components appear in different MCSs. Consequently, the true PFD_{avg} is always less than (4.4) [20]. If we model CCF explicitly [16] using standard beta factor model, we get

$$\text{PFD}_{\text{avg}} \approx \binom{n}{n-k+1}\cdot\frac{((1-\beta)\lambda_{\text{DU}}\tau)^{n-k+1}}{n-k+2} + \frac{\beta\lambda_{\text{DU}}\tau}{2} \tag{4.5}$$

As shown in Chapter 8, this approach is in line with IEC 61508 in situations where the effect of DD failures is insignificant. This approach is also discussed in relation to FTA in Chapter 5.

4.3 The IEC 61508 Simplifed Formulas

Annex B of IEC 61508-6 provides simplified formulas for 1oo1, 1oo2, 2oo2, 1oo3, 2oo3 and 1oo2D architectures. Neither proof nor generalized formula for $k$oo$n$ architecture is established. In this section, we prove formulas for these architectures and a generalized formula for $k$oo$n$ architecture. Before that, we briefly discuss reliability block diagram (RBD) and the underline assumptions[1].

4.3.1 Reliability Block Diagram

RBD is an intuitive graphical method that represents all possible component combinations (routes) such that if all components in at least one of these routes are functioning, we secure that the system is functioning. It is a success-oriented diagram that often uses series (AND) and parallel (OR) logics to connect individual components. But, we may have a situation where parallel and series logics cannot easily be seen. Nevertheless, it is always possible to make transformation to have a RBD with parallel and series logics since any RBD can be redrawn based on minimal cut sets (MCSs)[2] or based on minimal path sets (MPSs)[3]. In RBD we can describe only one specific function of a system at a time, i.e., if a SIS has more than one SIF we need one RBD for each. Figure 9.3 is a practical instance of RBD that shows how the PSD function for LAHH works.

Based on RBD we can assess system performance measures both qualitatively and quantitatively. A fault tree can be transformed into RBD and vice versa. A discussion on possible analyses that can be performed based on these diagrams is presented in Chapter 5, and for further discussion we recommend the reader to consult IEC 60300 [1].

4.3.2 Assumptions

The following are the assumptions underlying the IEC 61508 simplified formulas:

- The failure rate of a component is assumed to be constant over time.
- Components are statistically independent .

[1] The assumptions can be seen in IEC 61508-6, p. 25-28

[2] A MPS is a set of irreducible components such that if all are functioning, we secure that the system is functioning.

[3] A MCS is a set of irreducible components such that if all components failed, we secure system failure.

- Function testing coverage is assumed to 100%.
- PFD is calculated as average value.
- All channels[4] in an architecture have the same failure rate and diagnostic coverage.
- The overall failure rate of a channel of the subsystem is the sum of the dangerous failure rate and safe failure rate for that channel, which are assumed to be equal.
- The function test interval is at least an order of magnitude greater than the mean repair time (MRT).
- For each subsystem there is a single function test interval and MRT.
- The required time to test a subsystem is assumed to be negligible.
- The expected interval between demand is at least an order of magnitude greater than the function test interval.
- The term $\lambda_{\mathrm{DU}} \cdot \tau$ should be small enough to allow $\mathrm{e}^{-\lambda_{\mathrm{DU}} \cdot \tau} \approx 1 - \lambda_{\mathrm{DU}} \cdot \tau$, that is $\lambda_{\mathrm{DU}} \cdot \tau \leq 0.2$.

The $\mathrm{PFD}_{\mathrm{avg}}$ of a SIF can be determined by summing up the average PFDs of all subsystems that altogether implement the SIF (see Figure 3.2). A SIS often comprises of three subsystems: sensor (S), logic solver (L) and final element (FE). Thus, the $\mathrm{PFD}_{\mathrm{avg}}$ will be

$$\begin{aligned}
\mathrm{PFD}_{\text{avg-SYS}} &= \mathrm{PFD}_{\text{avg-S}} + \mathrm{PFD}_{\text{avg-L}} + \mathrm{PFD}_{\text{avg-FE}} - \mathrm{PFD}_{\text{avg-S}}\mathrm{PFD}_{\text{avg-L}} - \mathrm{PFD}_{\text{avg-S}}\mathrm{PFD}_{\text{avg-FE}} \\
&\quad - \mathrm{PFD}_{\text{avg-L}}\mathrm{PFD}_{\text{avg-FE}} + \mathrm{PFD}_{\text{avg-S}}\mathrm{PFD}_{\text{avg-L}}\mathrm{PFD}_{\text{avg-FE}} \\
&\approx \mathrm{PFD}_{\text{avg-S}} + \mathrm{PFD}_{\text{avg-L}} + \mathrm{PFD}_{\text{avg-FE}} \qquad (4.6)
\end{aligned}$$

The approximation is obvious, regardless of the approach used, since product terms are negligible. Note that we also assumed that subsystems are independent of each other.

Remark: The fundamental idea behind this method is to find a mathematical relationship between $\mathrm{PFD}_{\mathrm{avg}}$ and mean down time (MDT) as shown in Rausand's method in equation 4.3.

[4] Channel is element or group of elements that independently implement an element safety function. The term can be used to describe a complete system, or a portion of a system (for example, sensor or final element).[4]

4.3.3 Equivalent MDT

Notations

t_{cj} MDT for component j in a channel.

t_{CE} Channel equivalent MDT (combined MDT for all components in a channel).

t_{GE} Voted group equivalent MDT for $k$oo$n$ architecture where $n-k+1=2$ (combined MDT for two channels in the voted group).

t_{GjE} Voted group equivalent MDT for $k$oo$n$ architecture where $j=2,3,\ldots,n-k$ provided that $n-k+1>2$ (t_{G2E} is MDT for three channels in the voted group, t_{G3E} is MDT for four channels in the voted group and so on).

Consider an architecture that has one channel with one component. This channel can be seen as two components connected in series as the one shown in Figure 4.3. As can be seen from the figure, the system is down for length $t_{c1}=E(\tau-t'|T\leq\tau)+\text{MRT}$ with probability $\frac{\lambda_{DU}}{\lambda_{DD}+\lambda_{DU}}$ and $t_{c2}=\text{MTTR}$ with probability $\frac{\lambda_{DD}}{\lambda_{DD}+\lambda_{DU}}$, where T is the random variable for time to DU failure and MTTR is the mean time to restoration. Therefore, channel equivalent MDT can be calculated as

$$t_{CE}=\frac{\lambda_{DU}}{\lambda_{DU}+\lambda_{DD}}t_{c1}+\frac{\lambda_{DD}}{\lambda_{DU}+\lambda_{DD}}t_{c2} \tag{4.7}$$

Although it is apparent that the expected time to DU failure is $\tau/2$ due to the randomness assumption, we shall support it mathematically as follows. The unconditional expected downtime $\big(E(D)=E(\tau-t')\big)$ in the interval $(0,\tau]$ can be expressed as $\int_0^\tau(\tau-t')f(t)\mathrm{d}t$ or $\tau-E(t')$. But, our interest here is the expected down time in the interval $[0,\tau]$ given that the component is in failed state at time $t=\tau$. Therefore,

$$E(\tau-t'|T\leq\tau)=\frac{E(\tau-t')}{\mathrm{P}(T\leq\tau)}=\frac{\int_0^\tau(\tau-t')f(x)\mathrm{d}x}{F(\tau)}\approx\frac{\tau}{2} \tag{4.8}$$

The equivalent MDT for 1oo$n$ architecture can be obtained by using the above formula. The proof for (4.8) and for 1oo2 is presented in Appendix D.

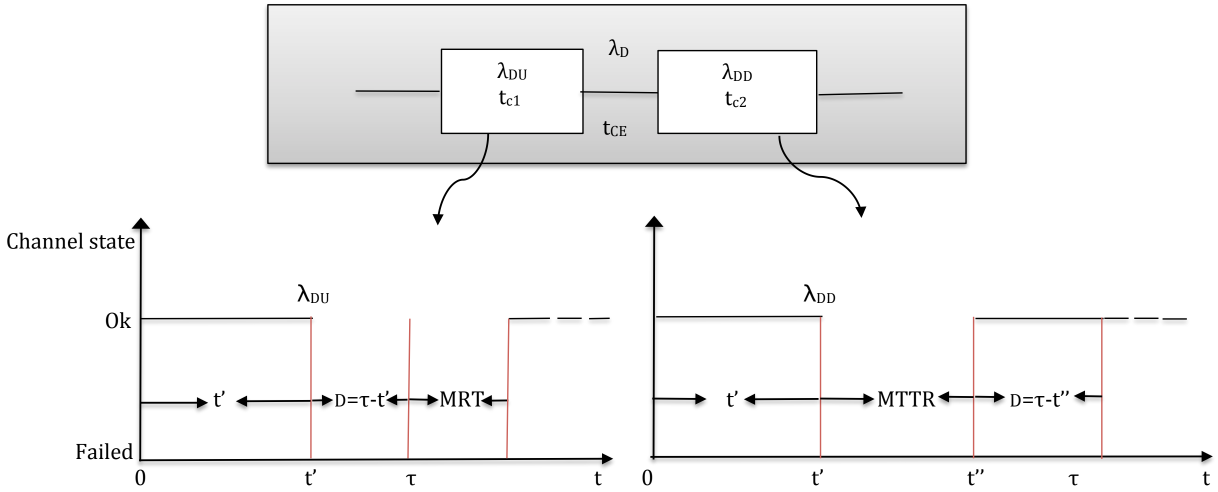

Figure 4.3: Decomposition of dangerous failures (top) and their associated MDT propagation (Bottom)

We can alternatively express (4.8) in a more tractable manner using Rausand's method [20].

$$E(\tau - t'|T \leq \tau) = \frac{E(D)}{F(\tau)} = \frac{\tau}{F(\tau)} \cdot \frac{1}{\tau} \int_0^\tau F(t)\mathrm{d}t = \frac{\tau}{F(\tau)} \cdot \mathrm{PFD_{avg}} \tag{4.9}$$

Hence, for 1oo$n$ architecture,

$$E(\tau - t'|T \leq \tau) \approx \frac{\tau}{\left(1 - \mathrm{e}^{\lambda_{\mathrm{DU}}\tau}\right)^n} \cdot \frac{(\lambda_{\mathrm{DU}}\tau)^n}{n+1} \approx \frac{\tau}{(\lambda_{\mathrm{DU}}\tau)^n} \cdot \frac{(\lambda_{\mathrm{DU}}\tau)^n}{n+1} = \frac{\tau}{n+1} \tag{4.10}$$

For 1oo1, as can be seen from Figure 4.3 and (4.10), the equivalent MDT associated with DU failure is

$$t_{\mathrm{c1}} = \frac{\tau}{2} + \mathrm{MRT}$$

It is evident that the estimate for t_{c2} is $E(t'' - t') = \mathrm{MTTR}$. The equivalent MDT for this architecture is thus obtained by substituting these results into (4.7). Hence

$$t_{\mathrm{CE}} = \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{2} + \mathrm{MRT}\right) + \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR} \tag{4.11}$$

Given the assumptions, the above equation measures the expected length that the architecture is down. It should be noted that t_{CE} is highly dependent on the diagnostic coverage DC factor. That is, for system with high DC the equivalent MDT is significantly low. For example with $\lambda_{\mathrm{D}} = 10\mathrm{E}{-}06, \tau = 8760$, and MRT = MTTR = 8 hrs the expected down time when DC = 0%, 60% 90% and 100% is 4388, 1760, 446, 8 respectively.

We can calculate t_{GE} and $t_{\mathrm{G}j\mathrm{E}}$, respectively, as follows.

$$t_{\mathrm{GE}} = \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{3} + \mathrm{MRT}\right) + \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR} \tag{4.12}$$

and

$$t_{\mathrm{G}j\mathrm{E}} = \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{\tau}{j+2} + \mathrm{MRT}\right) + \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR} \tag{4.13}$$

Some authors established a relation that $t_{\mathrm{GE}} = 0.5 \cdot t_{\mathrm{CE}}$ [10]. This is however problematic because it disagrees with the fact that, for example, for 1oo2 architecture the MDT resulted from DU failures is $\tau/3$. But, according to this relation it will be $\tau/4$

Equivalent MDT in the Density Function

Suppose a channel is down from somewhere in a test interval until function testing and repair, as illustrated in Figure 4.4. Let the length be t_{E}. Due to the assumption of perfect function test, the $\mathrm{PFD_{avg}}$ is equal to the red area under the density curve, and this can be computed as

$$\begin{aligned}
\mathrm{PFD_{avg}} &= \int_{\tau-t_{\mathrm{E}}}^{\tau} f(t)\mathrm{d}t = \int_0^{\tau} f(t)\mathrm{d}t - \int_0^{\tau-t_{\mathrm{E}}} f(t)\mathrm{d}t \\
&= \left(1-\mathrm{e}^{-\lambda_{\mathrm{D}}\tau}\right) - \left(1-\mathrm{e}^{-\lambda_{\mathrm{D}}(\tau-t_{\mathrm{E}})}\right) \\
&\approx \lambda_{\mathrm{D}}\tau - \lambda_{\mathrm{D}}(\tau - t_{\mathrm{E}}) = \lambda_{\mathrm{D}} t_{\mathrm{E}} = \int_0^{t_{\mathrm{E}}} f(t)\mathrm{d}t = F(t_{\mathrm{E}})
\end{aligned} \tag{4.14}$$

This means that regardless of where the equivalent MDT is located the $\mathrm{PFD_{avg}}$ can be calculated as $P(T \le t_{\mathrm{E}}) = F(t_{\mathrm{E}})$, due to the *memoryless* property of exponential distribution. Accordingly, the $\mathrm{PFD_{avg}}$ for a 1oo1 architecture is

$$\mathrm{PFD_{avg}} = \lambda_D t_{\mathrm{CE}} = (\lambda_{\mathrm{DU}} + \lambda_{\mathrm{DU}})\, t_{\mathrm{CE}} \tag{4.15}$$

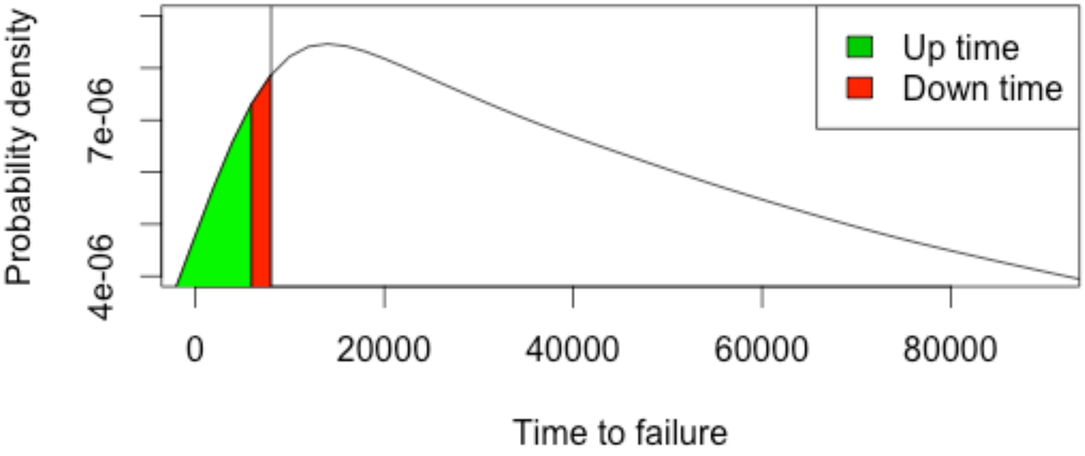

Figure 4.4: Density function for a channel with $\lambda_{\mathrm{D}} = 10\mathrm{E}{-}06, \tau = 8760$, MRT = MTTR = 8hrs and DC = 60%
.

4.3.4 $\mathrm{PFD}_{\mathrm{avg}}$ for Some $k$oo$n$ Architectures

Figure 4.5 shows the RBD and physical block diagram of 1oo2, 2oo2 and 1oo$n$ architectures. If a failure encounters in one channel, the output voting does not update to use the other *ok* channel(s). That is, if a failure occurs in one or more channels the system continues as if nothing has happened. The situation where the output voting updates the diagnostic result is discussed later in 1oo2D architecture.

2oo2

In 2oo2 architecture we need two of them to function for the system to function. Conversely, only one component failure is sufficient for the system to fail. The probability that component 1 OR component 2 fails is actually equal to the sum of the individual probabilities, since the product term is negligible. Therefore

$$\mathrm{PFD}_{\mathrm{avg}} = \lambda_{\mathrm{D}}\, t_{\mathrm{CE}} + \lambda_{\mathrm{D}}\, t_{\mathrm{CE}} = 2\lambda_{\mathrm{D}}\, t_{\mathrm{CE}} = 2(\lambda_{\mathrm{DU}} + \lambda_{\mathrm{DD}})\, t_{\mathrm{CE}} \tag{4.16}$$

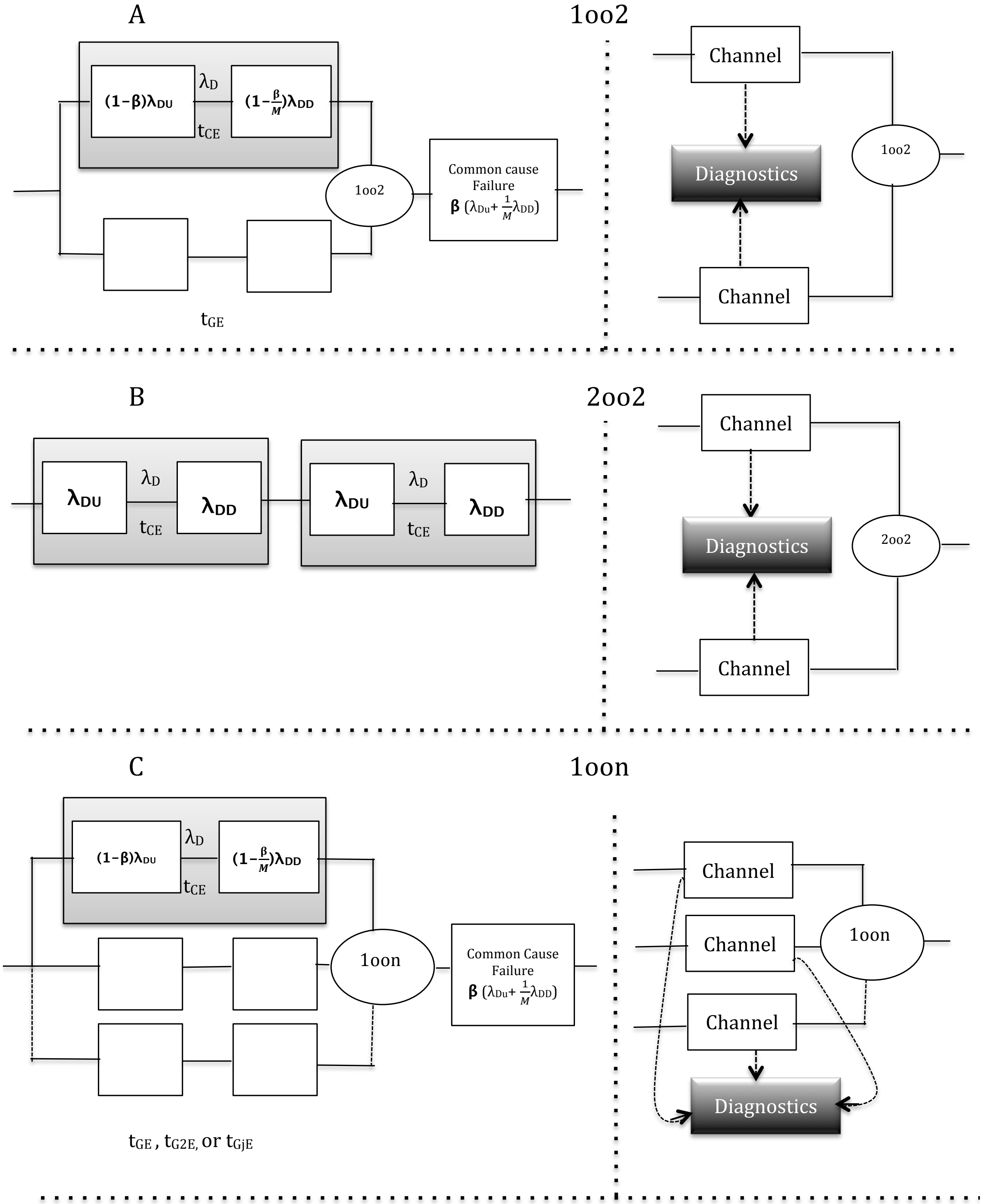

Figure 4.5: Reliability block diagram (left) and physical block diagram (right)

1oo2

Two independent component failures cannot occur at the same time unless it results from shared or common cause failure (CCF)[5]. Upon the second failure, the system fails given that either the first component failed due to DU failure or repair action is not completed after DD failure is encountered.

The equivalent MDT for 1oo2 architectures is t_{GE} (marked as red in Figure 4.6) and is expected to occur with rate $2\lambda_{\text{D}}$. Before the repair action is completed for the first failed component, the second must fail (its equivalent MDT is t_{CE} that occurs with rate λ_{D} and marked as yellow in Figure 4.6) to secure system failure. Therefore, the average PFD due to independent failures is

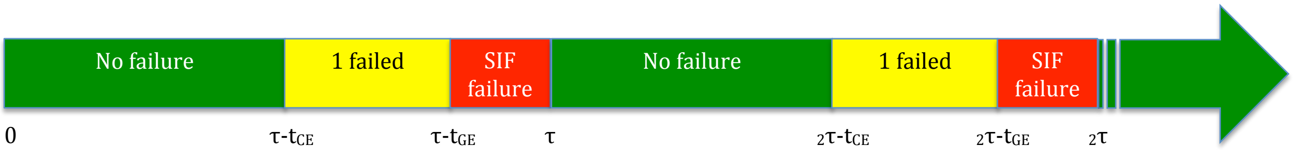

Figure 4.6: Failure development in a 1oo2 architecture

$$\begin{aligned} \text{PFD}_{\text{avg}}^{\text{I}} &= (1-\text{e}^{2\lambda t_{\text{GE}}})(1-\text{e}^{\lambda t_{\text{CE}}}) \approx 2\lambda_{\text{D}} t_{\text{GE}} \cdot \lambda_{\text{D}} t_{\text{CE}} \\ &\approx 2\lambda_{\text{D}}^2 t_{\text{CE}} t_{\text{GE}} = 2\left((1-\beta)\lambda_{\text{DU}} + (1-\beta_{\text{D}})\lambda_{\text{DD}}\right)^2 t_{\text{CE}} t_{\text{GE}} \qquad (4.17) \end{aligned}$$

where β_{D} is the common cause factor associated with DD failure. As seen from Figure 4.5 A, common cause can be treated as 1oo1 architecture by its own right. Then, the corresponding equivalent MDT can be written as

$$t_{\text{CE}}^{\text{C}} = \frac{\beta\lambda_{\text{DU}}}{\beta\lambda_{\text{DU}} + \beta_{\text{D}}\lambda_{\text{DD}}}\left(\frac{\tau}{2} + \text{MRT}\right) + \frac{\beta_{\text{D}}\lambda_{\text{DD}}}{\beta\lambda_{\text{DU}} + \beta_{\text{D}}\lambda_{\text{DD}}}\text{MTTR} \qquad (4.18)$$

[5] A CCF is a failure that the result of one or more events, causing concurrent failure of two or more separate channels in a multiple channel system, leading to system failure [4] whereas failures outside this are independent failures.

Thus, the average PFD due to CCF is

$$\mathrm{PFD}^{\mathrm{C}}_{\mathrm{avg}} = \left(\beta\lambda_{\mathrm{DU}} + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\right) t^{\mathrm{C}}_{\mathrm{CE}} = \beta\lambda_{\mathrm{DU}}(\frac{\tau}{2} + \mathrm{MRT}) + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR} \tag{4.19}$$

Hence

$$\begin{aligned} \mathrm{PFD}_{\mathrm{avg}} &= PFD^{\mathrm{I}}_{\mathrm{avg}} + PFD^{\mathrm{C}}_{\mathrm{avg}} \\ &= 2\left((1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\right)^2 t_{\mathrm{CE}} t_{\mathrm{GE}} + \beta\lambda_{\mathrm{DU}}(\frac{\tau}{2} + \mathrm{MRT}) + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR} \quad (4.20) \end{aligned}$$

2oo3

RBD for 2oo3 architecture can normally be redrawn as three 1oo2 architectures connected in series. The failure of one of these combinations is sufficient for the system to fail. Therefore, $\mathrm{PFD}_{\mathrm{avg}}$ for 2oo3 architecture is three times that of the $\mathrm{PFD}_{\mathrm{avg}}$ for 1oo2 architecture.

$$\mathrm{PFD}_{\mathrm{avg}} = 6((1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}})^2 t_{\mathrm{CE}} t_{\mathrm{GE}} + \beta\lambda_{\mathrm{DU}}(\frac{\tau}{2} + \mathrm{MRT}) + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR} \tag{4.21}$$

1oo3

As seen in Figure 4.7, system failure occurs if the third channel fails before no restoration on the previously failed channels is completed. The equivalent mean down time for 1oo3 architecture is t_{G2E} with rate $3\lambda_{\mathrm{D}}$. After one of these channels failed the system continues as 1oo2, and its equivalent MDT is t_{GE} with rate $2\lambda_{\mathrm{D}}$. After one of these two channels failed, the system runs with one channel, and its equivalent MDT is t_{CE} with rate λ_{D}. Therefore

$$\mathrm{PFD}^{\mathrm{I}}_{\mathrm{avg}} = (3\lambda_{\mathrm{D}} t_{\mathrm{G2E}}) \cdot (2\lambda_{\mathrm{D}} t_{\mathrm{GE}}) \cdot (\lambda_{\mathrm{D}} t_{\mathrm{CE}}) = 6\lambda^3_{\mathrm{D}} t_{\mathrm{CE}} t_{\mathrm{GE}} t_{\mathrm{G2E}} \tag{4.22}$$

Hence

$$\mathrm{PFD}_{\mathrm{avg}} = 6((1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}})^3 t_{\mathrm{CE}} t_{\mathrm{GE}} t_{\mathrm{G2E}} + \beta\lambda_{\mathrm{DU}}(\frac{\tau}{2} + \mathrm{MRT}) + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR} \tag{4.23}$$

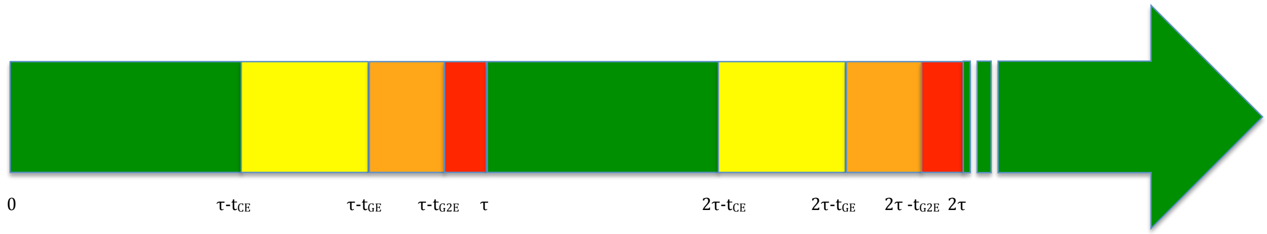

Figure 4.7: Failure development in a 1oo3 architecture

1oo2D

As it is shown in Figure 4.7 and described in the standard that during normal operation, both channels need to demand the safety function before it can take place. In addition, if the diagnostic tests in either channel detect a failure then the output voting is adapted so that the overall output state then follows that given by the other channel. If the diagnostic tests find failures in both channels or a discrepancy that cannot be allocated to either channel, then the output goes to the safe state. In order to detect a discrepancy between the channels, either channel can determine the state of the other channel via a means independent of the other channel. The channel comparison / switching over mechanism may not be 100% efficient therefore k represents the efficiency of this inter-channel comparison/ switching mechanism, i.e. the output may remain on the 2oo2 voting even with one channel detected as failed [4].

In addition to those failures considered in a channel in the previous architectures, in 1oo2D we have safe detected failures as illustrated in Figure 4.8 B. This failure occurs when both channels are detected failure or a diagnostic result that cannot be allocated to one of the channels. Whenever this failure is encountered the channel is down for MTTR and thus detected failures, in this case, is the sum of safe and dangerous detected failures. Therefore, channel equivalent MDT will be

$$t_{\mathrm{CE}'} \quad = \quad \frac{\lambda_{\mathrm{DU}}\left(\frac{\tau}{2}+\mathrm{MRT}\right)+(\lambda_{\mathrm{DD}}+\lambda_{\mathrm{SD}})\mathrm{MTTR}}{\lambda_{\mathrm{DU}}+(\lambda_{\mathrm{DD}}+\lambda_{\mathrm{SD}})} \tag{4.24}$$

Unlike other architectures, 1oo2D updates the results gained from diagnostic testing. If the diagnostic tests find failure in one channel, the system continues with the other channel so that

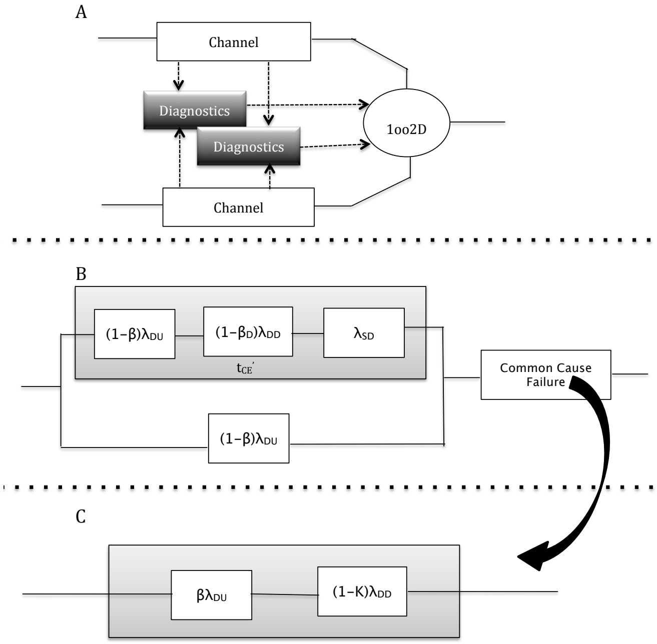

Figure 4.8: Physical block diagram (A), reliability block diagram (B) and reliability block diagram for the common cause (C), for a 1oo2D architecture

detected failures have no contribution in the voted group equivalent MDT. Therefore

$$t_{\text{GE'}} = \frac{\tau}{3} + \text{MRT} \tag{4.25}$$

Hence

$$\text{PFD}^{\text{I}}_{\text{avg}} = 2\lambda_{\text{DU}}\, t_{\text{GE}'} \cdot (\lambda_{\text{DU}} + \lambda_{\text{DD}} + \lambda_{\text{SD}})\, t_{\text{CE}'} = 2\lambda_{\text{DU}}(\lambda_{\text{DU}} + \lambda_{\text{DD}} + \lambda_{\text{SD}})\, t_{\text{CE}'}\, t_{\text{GE}'} \tag{4.26}$$

Authors, for example [10, 14], treated $t_{\text{GE'}}$ in the same way as they treat t_{GE}. But, no argument is given why they tend to compute it in this manner. The first reference treats in such a way that $t_{\text{GE'}} = 0.5 \cdot t_{\text{CE'}}$ and the second

$$t_{\text{CE'}} \quad = \quad \frac{\lambda_{\text{DU}}\left(\frac{\tau}{3} + \text{MRT}\right) + (\lambda_{\text{DD}} + \lambda_{\text{SD}})\text{MTTR}}{\lambda_{\text{DU}} + (\lambda_{\text{DD}} + \lambda_{\text{SD}})}$$

The efficiency of the switching over mechanism or $(1-k)$ determines the proportion of DD failures that leads to architecture failure. A channel compares itself with the other channel *inde-*

pendently so that malfunctioning can be either in channel 1 and 2. Therefore, CCF related to DD failure occurs at a rate of $(1-k)\cdot 2\cdot \lambda_{\mathrm{DD}}$. Total CCF rate for this architecture will then be $\lambda_{\mathrm{C}}^{'} = \beta\lambda_{\mathrm{DU}} + 2(1-k)\lambda_{\mathrm{DD}}$, and the corresponding equivalent MDT is

$$t_{\mathrm{CE}'}^{\mathrm{c}} = \frac{\beta\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{CC}}^{'}}\left(\frac{\tau}{2} + \mathrm{MRT}\right) + \frac{2(1-k)\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{CC}}^{'}}t_{\mathrm{CE}'} \tag{4.27}$$

Therefore

$$\mathrm{PFD}_{\mathrm{avg}}^{\mathrm{C}} = \lambda_{\mathrm{CC}}^{'}t_{\mathrm{CE}'}^{\mathrm{cc}} = \beta\lambda_{\mathrm{DU}}\left(\frac{\tau}{2} + \mathrm{MRT}\right) + 2(1-k)\lambda_{\mathrm{DD}}t_{\mathrm{CE}'} \tag{4.28}$$

Hence

$$\begin{aligned}\mathrm{PFD}_{\mathrm{avg}} \;&=\; 2((1-\beta)\lambda_{\mathrm{DU}})((1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}} \\ &\quad +\lambda_{\mathrm{SD}})t_{CE'}t_{GE'} + \beta\lambda_{\mathrm{DU}}(\frac{\tau}{2} + \mathrm{MRT}) + 2(1-K)\lambda_{\mathrm{DD}}t_{\mathrm{CE}'}\end{aligned} \tag{4.29}$$

4.3.5 Generalized Formula for $k$oo$n$ Architectures

A $k$oo$n$ architecture has $\binom{n}{n-k+1}$ MCSs and each of them are of order $n-k+1$. The architecture fails if and only if all channels in any of these MCSs are failed. Following previous arguments, $\mathrm{PFD}_{\mathrm{avg}}^{\mathrm{I}}$ for a MCS $(1\mathrm{oo}(n-k+1))$ is

$$\begin{aligned}\mathrm{PFD}_{\mathrm{avg}}^{\mathrm{I}} \;&=\; \big((n-k+1)\lambda_{\mathrm{D}}t_{\mathrm{G}(n-k)\mathrm{E}}\big)\cdot\big((n-k)\lambda_{\mathrm{D}}t_{\mathrm{G}(n-k-1)\mathrm{E}}\big) \\ &\quad \cdot\big((n-k-1)\lambda_{\mathrm{D}}t_{G(n-k-2)\mathrm{E}}\big)\ldots(2\lambda_{\mathrm{D}}t_{\mathrm{GE}})\cdot(\lambda_{\mathrm{D}}t_{\mathrm{CE}}) \\ &=\; (n-k+1)!\lambda_{\mathrm{D}}^{n-k+1}t_{\mathrm{G}(n-k)\mathrm{E}}t_{G(n-k-1)\mathrm{E}}t_{\mathrm{G}(n-k-2)\mathrm{E}}\cdots t_{\mathrm{G2E}}t_{\mathrm{CE}}\end{aligned} \tag{4.30}$$

For $k$oo$n$

$$\begin{aligned}\mathrm{PFD}_{\mathrm{avg}}^{\mathrm{I}} \;&=\; \frac{n!}{(k-1)!(n-k+1)!}(n-k+1)!\lambda_{\mathrm{D}}^{n-k+1}t_{\mathrm{G}(n-k)\mathrm{E}}t_{\mathrm{G}(n-k-1)\mathrm{E}}t_{\mathrm{G}(n-k-2)\mathrm{E}}\cdots t_{\mathrm{G2E}}t_{\mathrm{CE}} \\ &=\; \frac{n!}{(k-1)!}\lambda_{\mathrm{D}}^{n-k+1}t_{\mathrm{G}(n-k)\mathrm{E}}t_{\mathrm{G}(n-k-1)\mathrm{E}}t_{\mathrm{G}(n-k-2)\mathrm{E}}\cdots t_{\mathrm{G2E}}t_{\mathrm{CE}}\end{aligned} \tag{4.31}$$

Thus for $k < n$

$$\begin{aligned}\mathrm{PFD_{avg}} &= \frac{n!}{(k-1)!}((1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}})^{n-k+1}\, t_{\mathrm{G}(n-k)\mathrm{E}}\, t_{\mathrm{G}(n-k-1)\mathrm{E}} \cdot \ldots t_{\mathrm{G2E}}\, t_{\mathrm{CE}} \\ &\quad + \beta\lambda_{\mathrm{DU}}(\frac{\tau}{2} + \mathrm{MRT}) + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR} \qquad (4.32)\end{aligned}$$

For $k = n$

$$\mathrm{PFD_{avg}} = n\lambda_{\mathrm{D}}\, t_{\mathrm{CE}} = n(\lambda_{\mathrm{DU}} + \lambda_{\mathrm{DD}})\, t_{\mathrm{CE}} \qquad (4.33)$$

4.4 The PDS Method

The focus of this section is to assess in detail the arguments of the PDS[6] method in relation to $\mathrm{PFD_{avg}}$ calculation. However, in this section we refrain from providing proves (mathematically) for formulas in detail due the following reasons:

- The method utilizes the basic ideas in the above two methods in a slightly different way, and it can thus be seen more or less as a hybrid of the above two.
- Since the method is aimed to provide information for engineers even who are outside the field, formulas are presented in a detailed and intuitive manner.

Therefore, we strongly recommend the reader to consult the handbook throughout this section.

4.4.1 How the PDS Method Addresses the Weaknesses of IEC 61508 Formulas

The PDS method has tried to address the weaknesses of IEC 61508 formulas by

- using a more detailed failure classification,
- using a multiple beta factor model,
- incorporating systematic failures in the quantification,
- modeling imperfect function testing,

[6] PDS is a Norwegian acronym for reliability of safety instrumented systems

- incorporating the time required for function testing into the model, and
- providing a technique that takes into account a particular operational philosophy

Attempt is made to develop a model that includes all possible factors that contribute to the unavailability of a SIF. Unlike IEC 61508, a model is developed to include systematic failures and a slightly more detailed failure classification is established. Systematic failures are further classified as software failures, design related failures, installation failures, excessive stress failures and operational failures. However, it is not clear that the PDS method adopts IEC 61508 definitions for random hardware failures and systematic failures. According to IEC 61508, random hardware failures are random in nature resulted from one or more degradation mechanisms in the hardware, whereas systematic failures are related to a certain cause in a *deterministic* way. The same definition applies also in ISA [6].

In the PDS method, random hardware failures are failures resulting from the natural degradation mechanism of the component whereas systematic failures are failures resulting from causes outside this. Accordingly, in the PDS method failures due to excessive stresses are categorized under systematic failures since it is not due to natural degradation (though it is a hardware (physical) failure). Thus, it does not seem that it is in line with the definitions of IEC 61508.

Systematic failures are classified as detected/undetected and safe/dangerous. According to the PDS method, DU failure rate (λ_{DU}) consists of DU random hardware failures and DU systematic failures. Mathematically

$$\lambda_{\text{DU}} = \lambda_{\text{DU-RH}} + \lambda_{\text{DU-SYS}} \tag{4.34}$$

where $\lambda_{\text{DU-SYS}} = (1-r)\lambda_{\text{DU}}$ and thus $1-r$ is the fraction of DU failure rate originated from systematic failures, and data is available in the PDS handbook for the estimates of λ_{DU} in this case.

The arguments behind such an intention to quantify systematic failures is that since most systematic failures are operation related, the failure probability calculation in the design phase without considering future operating environments cannot be realistic. This means that failure probability calculations should not be limited to the intrinsic characteristics of the system, but what it might face in the operational phase shall also be considered. If we are able to do so, the result reflects the actual risk reduction that may be experienced in the operational phase.

Once the estimate for λ_{DU} based on (4.34) is obtained, ordinary formula can be used to quantify its contribution. It is pointed out that while applying formulas to calculate the probability, splitting of λ_{DU} is not necessary. Thus, λ_{DU} in this case can simply be considered as a conservative estimate of DU failure rate that incorporates systematic failures.

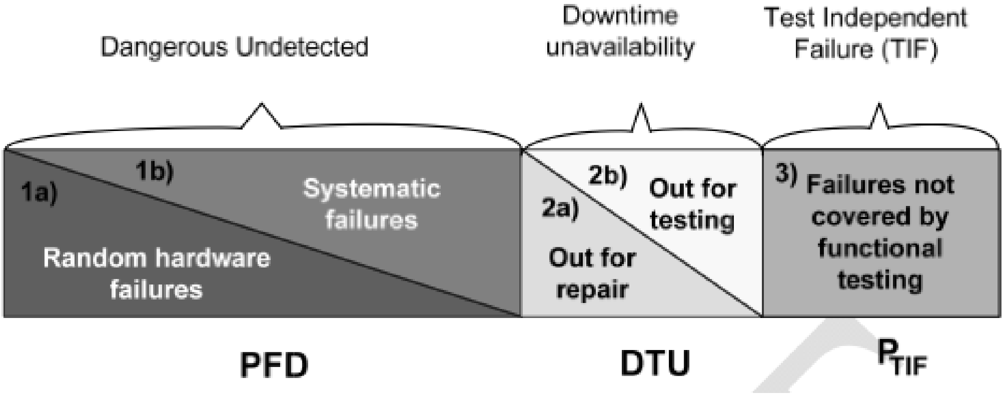

Figure 4.9: Loss of safety contributors [23]

In addition to this, since emphasis is given in the PDS method to incorporate all possible factors that affect the unavailability of a SIF (loss of safety), the model is developed to include them explicitly. In the PDS method, the term *critical safety unavailability (CSU)* is used to measure the quantitative reliability performance of a SIS and has three contributors as shown in Figure 4.9. These are

- PFD - Unavailability due to DU failures.
- DTU - Unavailability due to known or planned downtime. It is further classified as
  - $\mathrm{DTU}_{\mathrm{R}}$ - due to repair of dangerous failures (DU and DD), and
  - $\mathrm{DTU}_{\mathrm{T}}$ - due to function testing/preventive maintenance.

- P_{TIF} - Unavailability due to TIF (test independent failures)

Since the product terms are negligible, we have

$$\text{CSU} = \text{PFD} + \text{DTU}_R + \text{DTU}_T + P_{TIF} \tag{4.35}$$

In line with IEC 61508, an extended (multiple) beta factor model is introduced. Unlike the standard beta factor model, this model distinguishes the effect of CCF in different types of architectures. Accordingly, the following relation is established for $k$oo$n$ architecture, where $k < n$.

$$\beta(k\text{oo}n) = C_{k\text{oo}n}\beta \tag{4.36}$$

$C_{k\text{oo}n}$ is the modification factor for various architectures and β is a factor for 1oo2 architecture. Proof and discussion of the factor is given in Annex B of the PDS method handbook [23]. The estimates of $C_{k\text{oo}n}$ for some typical architectures is presented in Table 4.1.

Table 4.1: $C_{(k\text{oo}n)}$ factors for different architectures [23]

k \ n	2	3	4	5	6
1	1.0	0.5	0.3	0.2	0.15
2	-	2.0	1.1	0.8	0.6
3	-	-	2.8	1.6	1.2
4	-	-	-	3.6	1.9
5	-	-	-	-	4.5

Given that CCF occurs, the probability that two components in parallel fail is β ($C_{1oo2} = 1$). But, given CCF occurs, the probability that three components in parallel fail is $0.5 \cdot \beta$, that is $C_{1oo3} = 0.5$. However, in the IEC 61508 formulas, it is assumed that given CCF occurs the probability that n components in parallel fail is β, regardless of the size of n and the voting.

Terms in (4.35) are determined based on Rausand's method in one way or another. A simplified description about the terms are presented below. The first term (PFD) that is due to DU failures is given by

$$\text{PFD}_{\text{avg}} \approx \binom{n}{n-k+1} \cdot \frac{(\lambda_{\text{DU}}\tau)^{n-k+1}}{n-k+2} + \frac{C_{k\text{oo}n}\beta\lambda_{\text{DU}}\tau}{2} \tag{4.37}$$

This is exactly the same as (4.5) except two modifications related to CCF. First, it is chosen to use a conservative failure rate for independent failures by eliminating the reduction by common cause factor, for example λ_{DU} instead of $(1-\beta)\lambda_{\mathrm{DU}}$ for 1oo2 architecture. Second, architecture specific beta factor ($\mathrm{C}_{k\mathrm{oo}n}\beta$) is implemented in the CCF term.

$\mathrm{DTU_R}$ is also calculated in the same way except replacing the mean down time $(\tau/(n-k+2))$ by MTTR. For example, for 1oo1 architecture $\mathrm{DTU_R} = \lambda_{\mathrm{D}} \cdot \mathrm{MTTR}$. In the handbook $\mathrm{DTU_R}$ formulas are developed for some typical architecture by considering the operational philosophies.

A similar approach is also applied for $\mathrm{DTU_T}$. The mean down time associated with this contributor is just t, time required for function testing, if the philosophy is to test all channels at the same time. Therefore, for $k$oo$n$ architecture, $\mathrm{DTU_T} = \lambda_{\mathrm{D}} \cdot t$. For philosophies other than this, the handbook provided formulas for some typical architectures.

When it comes to quantifying the contribution from TIF, two methods are suggested, i.e., based on TIF formula or incorporating function testing coverage (FTC) into the $\mathrm{PFD_{avg}}$. TIF formula for $k$oo$n$ architecture is $\mathrm{C}_{k\mathrm{oo}n}\cdot\beta\cdot\mathrm{P_{TIF}}$, and $n\cdot\mathrm{P_{TIF}}$ for $n$oo$n$. $\mathrm{P_{TIF}}$ can be estimated based on expert judgment. But, for some typical components data is available in the PDS method handbook.

The second alternative, for example for 1oo1 architecture, is given by

$$\mathrm{PFD_{avg}} = \mathrm{FTC} \cdot \left(\frac{\lambda_{DU}\tau}{2}\right) + (1-\mathrm{FTC}) \cdot \left(\frac{\lambda_{DU}T}{2}\right) \tag{4.38}$$

where T is the assumed interval of *complete* testing when the residual failure modes can be detected. Note that in this case $\mathrm{PFD_{avg}}$ is a function of time and always increasing. A sufficiently detailed discussion of the approaches is presented in the handbook.

4.5 Alternative Method

The mean down time of a component originated from DU failures is $\tau/2$, given it is known that DD failures do not occur. In other words, if DD failure occurs, the mean down time will obviously be less than $\tau/2$ depending on when DD failure is encountered in a test interval. Based on this argument a mathematical relation is established such that the conditional relationship of DU and DD failures is maintained.

Let us define the following events

A be the event that the system fails due to DU failure, and

B be the event that the system fails due to DD failure.

Rausand's formula gives us the conditional PFD$_{\text{avg}}$ given it is known that DD failures do not occur, that is $P(\text{A}|\text{B}^{\text{c}})$, where B$^{\text{c}}$ is the complement of event B. As we shall see in Chapter 8, IEC 61508 and the PDS method reduce to Rausand's formula if we ignore other contributors except DU failures. An extension is made here in the formula by including the contribution during repairing of DU failures (MRT). It is the product of average system failure rate and MRT (the last term in the equation below).

$$\begin{aligned} P(\text{A}|\text{B}^{\text{c}}) &= \binom{n}{n-k+1}\frac{\big((1-\beta)\lambda_{\text{DU}}\tau\big)^{n-k+1}}{n-k+2}+\frac{\beta\lambda_{\text{DU}}\tau}{2}+\binom{n}{n-k+1}\lambda_{\text{DU}}^{n-k+1}\tau^{n-k}\text{MRT} \\ &= \binom{n}{n-k+1}\tau^{n-k+1}\left(\frac{\big((1-\beta)\lambda_{\text{DU}}\big)^{n-k+1}}{n-k+2}+\frac{\lambda_{\text{DU}}^{n-k+1}\text{MRT}}{\tau}\right)+\frac{\beta\lambda_{\text{DU}}\tau}{2} \qquad (4.39) \\ &\approx \binom{n}{n-k+1}(\lambda_{\text{DU}}\tau)^{n-k+1}\left(\frac{1}{n-k+2}+\frac{\text{MRT}}{\tau}\right)+\frac{\beta\lambda_{\text{DU}}\tau}{2} \end{aligned}$$

Similarly, P(B) can be calculated as the product of average system failure rate and the expected down time while detecting and repairing of DD failures (MTTR).

$$\text{P(B)} = \binom{n}{n-k+1}\big((1-\beta_{\text{D}})\lambda_{\text{DD}}\big)^{n-k+1}\tau^{n-k}\text{MTTR}+\frac{\beta_{\text{D}}\lambda_{\text{DD}}\tau}{2} \qquad (4.40)$$

Our interest is to find P(A∪B) that measures PFD$_{\text{avg}}$ due to DU failures or DD failures or both.

Mathematically

$$P(\mathrm{A} \cup \mathrm{B}) = P(\mathrm{A}) + P(\mathrm{B}) - P(\mathrm{A} \cap \mathrm{B}) \tag{4.41}$$

We know from Baye's theorem that

$$P(\mathrm{A}|\mathrm{B}^{\mathrm{c}}) = \frac{P(A) - P(A \cap B)}{1 - P(B)} \tag{4.42}$$

After rearranging we get

$$P(A \cup B) = P(A|B^{\mathrm{c}})(1 - P(\mathrm{B})) + P(\mathrm{B}) \tag{4.43}$$

Hence,

$$\mathrm{PFD}_{\mathrm{avg}} = \mathrm{PFD}_{\mathrm{avg}}^{\mathrm{DU}}\left(1 - \mathrm{PFD}_{\mathrm{avg}}^{\mathrm{DD}}\right) + \mathrm{PFD}_{\mathrm{avg}}^{\mathrm{DD}} \tag{4.44}$$

As expected the contribution of DU failure is reduced by a factor of $\left(1 - \mathrm{PFD}_{\mathrm{avg}}^{\mathrm{DD}}\right)$ though it can be approximated to one.

Chapter 5

Fault Tree Analysis

5.1 Introduction

In Chapter 4, we discussed quantification methods based on simplified formulas. The simplified formulas are developed using reliability block diagrams (RBDs). As a graphical representation, RBD and fault tree represent the same thing, but in opposite ways. In RBD we think of all the possible ways the functionality of a system can be secured whereas in fault tree it is the other way around. Any fault tree can be converted to a RBD and vice versa, as long as only AND and OR gates are used. Thus, the result we get out of these models is the same. Although fault tree and RBD are transposable, it should be noted that starting with fault tree is always advantageous and recommended [20].

In IEC 61508, the method for simplified formulas named as “the RBD approach”. However, the quantification principle is not directly related to the diagram. It is therefore important to note that the RBD approach and the FTA approach are different in principle. In this chapter we discuss fault tree analysis (FTA) as SIS reliability quantification method.

5.1.1 Why FTA?

With fault tree we can graphically represent possible causes of system failure. It shall be constructed in such a way that the undesired event (Top event) is stated beforehand in a specific and unambiguous manner, and failure (fault) breakdown is carried out to find all possible routes (combinations of events) that contribute to the occurrence of the Top event. Top event is an outcome of combinations of input events [2]. In SIS reliability quantification, it may be stated as *SIF fails to act upon demand during normal operation.*

FTA is a mature technique, and one of the recommended methods in IEC 61508. It has been used in several application sectors both qualitatively and quantitatively. Construction and qualitative analysis of fault tree are straightforward, and several references are available, for example [2, 6, 18, 16, 20]. Of course, it requires extra caution, for example, when there is a rather complex dependency between components. A simple example of such scenarios may be, in 2oo4 architecture, when two components are dependent and the other two are independent of any. A plain way of modeling such situations may lead to an overwhelmingly big fault tree and/or unable to represent the reality.

FTA has had a great success in the reliability quantification theory of SISs. The reasons for this are three:

1. Graphical representation of the logical developments of component failures to system failure is easily conceivable and communicable. It is understandable even by engineers who are not trained in risk and reliability analysis. It therefore helps to deal with system performance from different point of view, as it facilitates communication among different specialists such as design engineers, system engineers, maintenance personnel, and so on.

2. Since it has widely been used for many years, references are sufficiently available such as books, articles, handbooks, standards, guidelines, and the like.

3. Several efficient algorithms have been developed to carry out the analysis both qualitatively and quantitatively, for example RiskSpectrum.

5.1.2 Assumptions

The assumptions listed here are influenced by [6].

- The failure rate is constant over time
- The failures of individual components are statistically independent; this means that the failure of any component does not affect the failure of any other component
- The expected interval between demands is at least an order of magnitude greater than the function test interval
- Function test coverage is assumed to be 100%
- The function test interval is at least an order of magnitude greater than the MRT
- For each subsystem there is a single function test interval and MRT
- A component can only fail again after it has first been repaired
- If DD failure occurs, the SIF will take the process to a safe state or plant personnel will take necessary action to ensure the process is safe

5.2 Fault Tree Analysis Procedures

The objective of fault tree construction is to establish the relationships between the lowest level events and the Top event. The lowest level events are called *basic events* and usually related to component failure or human error that are located at the bottom of the tree. The reliability quantification of a SIS based on fault tree may be carried out in six steps:

1. SIF familiarization
2. Top event identification
3. Decision on how to model systematic failures and CCF
4. Construction of the fault tree
5. Qualitative analysis of the fault tree
6. Quantitative analysis of the fault tree

5.2.1 SIF Familiarization

Like any other risk and reliability analysis techniques, FTA starts out with thorough understanding of the system under consideration. The first thing to do is to identify the SIF, its function and system behavior in different modes of operation such as normal, activation, testing, repair, start-up, fault and so on. It should be well understood how the SIF responds to a process demand, and further how and to which extent a component's functionality is required in order for the SIF to function. It is also crucial at this stage to understand how individual components fail, for example due to normal degradation, misuse, excessive stresses from operation or the environment [16] and so on.

IEC 61025 recommends FTA to be carried out by personnel with detailed knowledge about the system, its design features and operation; as well as by those who are trained in FTA and other relevant reliability modeling techniques. Lack of engineering knowledge of the product design and potential failure modes will produce a FTA that might not be a true representation of the product functionality and, thus, the analytical results would become meaningless [2].

5.2.2 Top Event Identification

Once the system is fully understood, the next step is to identify and state the Top event as precisely as possible, since it is the event that the whole analysis depends on. It is the state of a SIF where it is not able to perform the required functions under the stated conditions. The description of the Top event must be clear, unambiguous and should answer the questions *what, where*, and *when* [20].

Before commencing construction of the fault tree, the scope of the analysis and system boundary need to be established, given that the overall objective is met. Scope definition may in this case be the extent to which the analysis is going to take care of the attributes that may affect the unavailability of the SIF. For example,

- how to treat systematic failures and common cause failures
- coverages of function testing and self diagnostic testing

- online or offline testing and repair
- significance of the time requires for testing and repair
- human error (skills and knowledge of operators and maintenance personnel)
- environmental and operational stresses, and so on

The physical boundary [2], such as electrical, mechanical and operational interfaces with the system, shall be identified and stated in an unambiguous manner. One has to have a clear idea about these and other relevant factors before commencing the next step.

In quantitative FTA, consideration is given to those factors for which failure data is available and have significant effect on the Top event. However, for qualitative judgment it may be important to consider several factors that affect the unavailability of SIF, even if it is known that failure data is unavailable or their effect is insignificant.

5.2.3 Systematic and Common Cause Failures

It is not a straightforward issue to quantify systematic failures and common cause failures. From the onset, it requires to understand the system in terms of its operation, maintenance, diagnostic testing, and so on to identify systematic failures and common cause failures that should be included in the fault tree[6]. Second, there must be a clear understanding on how to incorporate them in the model. Different authors have different views, and the common ones are presented below. We suggest the reader to first look at a discussion on failure classification in Chapter 3.

Systematic Failures

According to IEC 61508, systematic failures are controlled by qualitative measures. However, if these qualitative measures are not secured properly, the PFD_{avg} value will be too optimistic.

As discussed in Chapter 4, failure classification and thus the PFD_{avg} calculation in the PDS method is different from IEC 61508. In the PDS method, DU failures encompass both random hardware failures and systematic failures. To be able to include systematic failures in the PFD_{avg}

calculation, no explicit modeling is required since DU failures are conservative to take into account systematic failures.

In ISA [6], two possible ways are suggested to model systematic failures in a fault tree:

- Explicitly by adding systematic failures in the fault tree as independent events, or
- By using conservative failure rates to take into account the effect of systematic failures in the analysis. This is analogous to the PDS method.

Unlike the above approaches, OLF 070[19] requires a separate quantification for systematic failures called probability of systematic failure (PSF). The argument is that while having several major contributors to the unavailability of a SIF related to systematic failure, calculating PFD_{avg} without considering them is senseless. The following are examples of systematic failures listed in the OLF 070 to illustrate the above argument:

- Failure of detector to react due to "wrong" location of detectors
- Failure of detector to discriminate between true and false alarm
- Insufficient functional test procedure
- Human error during functional test
  - detector left in by-pass
  - wrong calibration of transmitter
- Failure of shutdown valve to close since operator has left the isolation valve on the bleed off line in closed position
- Failure to execute safety function due to software error

Thus, according to OLF 070, safety unavailability is the sum of PSF and PFD, where PFD is based on random hardware failure that can be calculated, for example, by IEC 61508 formula.

Common Cause failures

We have two ways of modeling CCF depending on the situation: explicitly and implicitly [6, 16, 18]. In situations where components are identical, with the same CCF, it is straightforward to include in the fault tree. For example, a $k\text{oo}n$ architecture has $\binom{n}{n-k+1}$ cut sets with an order of $n-k+1$ each so that the corresponding fault tree can be depicted as Figure 5.1. This is the simplest situation where CCF can be modeled *explicitly*.

In order to reduce the effect of CCF, diversified components could be used. Moreover, we may have a SIF that has more than one type of components in a subsystem, say sensor. For example, smoke detectors and temperature detectors can be used in a SIF to protect the EUC against fire. In such situations, explicit modeling is no longer practical since more than one type of dependency appear in a MSC. For these and situations like these we should use implicit modeling.

Implicitly we can model CCF in two ways:

- CCFs can be treated as basic events and integrated into the MCSs that are already obtained from the fault tree. This approach is discussed further in detail in [16].
- The contribution of CCFs can be treated indirectly by adding their failure rate into the respective DU failures [6]. This is analogous to modeling systematic failures [6, 23].

In most standards and guidelines [4, 19, 23], the beta factor model is adopted to model CCF. There are two different ways of thinking, as we discussed in Chapter 3. In the standard beta factor model, which is the commonly used model, $\beta \cdot \lambda_{DU}$ is the failure rate of the CCF, regardless of the type of the architecture. But, in the PDS method, an architecture factor $\left(\mathrm{C}_{(k\text{oo}n)}\right)$ is implemented such that $\beta_{(k\text{oo}n)} = \beta \cdot \mathrm{C}_{(k\text{oo}n)}$. The estimates of $\mathrm{C}_{(k\text{oo}n)}$ can be seen from Table 4.1 for some typical architectures.

5.2.4 Fault Tree Construction

Construction is carried out in such a way that the specified Top event is broken down into lower level failures (faults) connected through logic gates in a binary fashion. It assumes only two states, failed or not failed. This is the static nature of the model and that can be considered as one of its demerits. In principle, fault tree construction continues until all basic events are identified. However, as far as quantitative FTA is concerned, the inclusion of those basic events with very low probability to affect the Top event is not only waste of time but also increment of the uncertainty of the Top event probability — "too much detail, too much uncertainty" [18]. Thus, we should exclude those events that have insignificant effect on the Top event. The continuation also depends on how far detailed analysis is required. Figure 5.1 shows a fault tree for a $koon$ architecture with identical components using standard beta factor modeling.

In a fault tree we only deal with one failure mode. It is thus important to keep this in mind all the time going down to basic events. Caution should also be exercised not to switch to different failure modes.

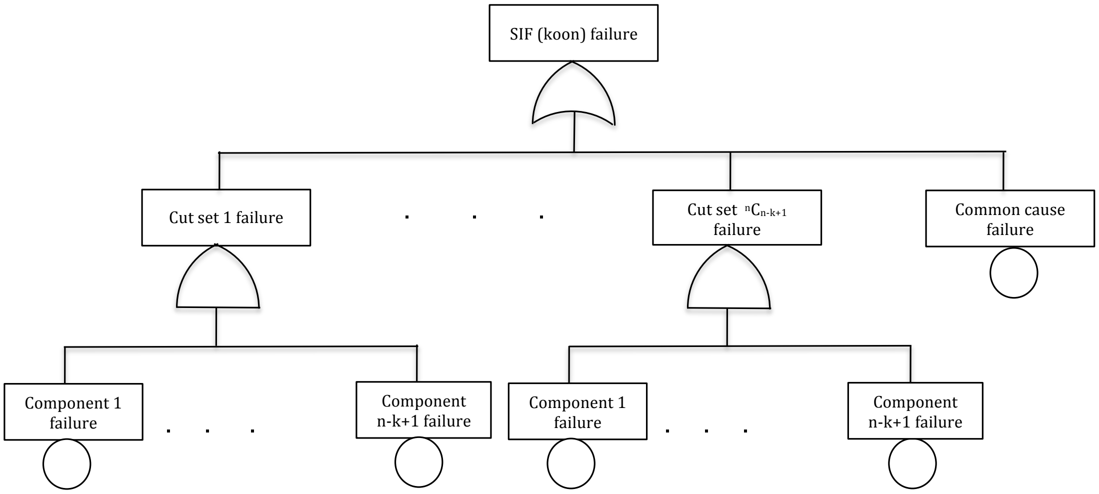

Figure 5.1: Fault tree for $koon$ architecture with identical components

Before going further in the analysis, the constructed fault tree should be confirmed for completeness and adequacy. There is no way that an inadequate fault tree gives adequate result. Therefore, due emphasis should be given during construction. An adequate fault tree shows comprehensively how failure of basic events could develop into the Top event.

5.2.5 Qualitative Analysis of Fault Tree

In some applications, for example nuclear industries, identifying potential causes that contribute to the Top event is sufficient, without further performing any quantitative analysis [2]. Qualitative analysis is a qualitative judgment on MCSs. A MCS is a set containing irreducible number of basic events such that the failure of all such events leads directly to the occurrence of Top event. As far as this kind of analysis is concerned, the likelihood of the occurrence of the Top event may be manifested in terms of two dimensions, the *number* and *nature* of basic events in a MCS.

Keeping other factors constant, a MCS of order 1 is more “important” than a MCS of order 2 or more; a MCS of order 2 is more “important” than a MCS of order 3 or more, and so on. For example, in Figure 5.1 there is a MCS containing only one basic event, i.e., the CCF. Therefore, effort on the reduction of the likelihood of the occurrence of this event would substantially reduce the likelihood of the occurrence of the Top event.

The reliability of basic events in a MCS is also equally valuable on the decision to identify the most critical MCSs. For example, we may have a situation where a MCS of order 1 with basic event that is as strong as two basic events in parallel (order 2). In this case we cannot say that the former is more important than the second. Thus, nature and number of basic events are both equally important to be considered simultaneously. Beside the number of basic events in a MCS, in [20] it is described that the nature of basic events can be ranked as human error, active equipment failure and passive equipment failure according to their importance respectively. The assumption behind this ranking is that human errors are more frequent than active components and active components are more frequent than passive ones.

5.2.6 Quantitative Analysis of Fault Tree

Quantitative FTA, especially PFD calculation, requires a clear understanding of the underlining assumptions; otherwise the mathematics is rather easy. Failure to understand the assumptions leads to wrong perception of the results gained.

In quantitative FTA, we employ basic set mathematics and Boolean algebra on the MCSs. Once they are identified from the constructed fault tree it can easily be transformed into a RBD as a series structure of those minimal cut sets, like the one shown in Figure 5.2. Such transformation is important because it is easier to visualize and change it into mathematical equation than fault tree. Assume now that a minimal cut set contains r identical and independent components. The average PFD is

$$\begin{aligned}\mathrm{PFD_{avg}} &= \frac{1}{\tau}\int_0^{\tau}\left(1-\mathrm{e}^{\lambda_{\mathrm{DU}}t}\right)^r \mathrm{d}t \\ &\approx \frac{1}{\tau}\int_0^{\tau}(\lambda_{\mathrm{DU}}t)^r\,\mathrm{d}t = \frac{(\lambda_{\mathrm{DU}}\tau)^r}{r+1}\end{aligned} \tag{5.1}$$

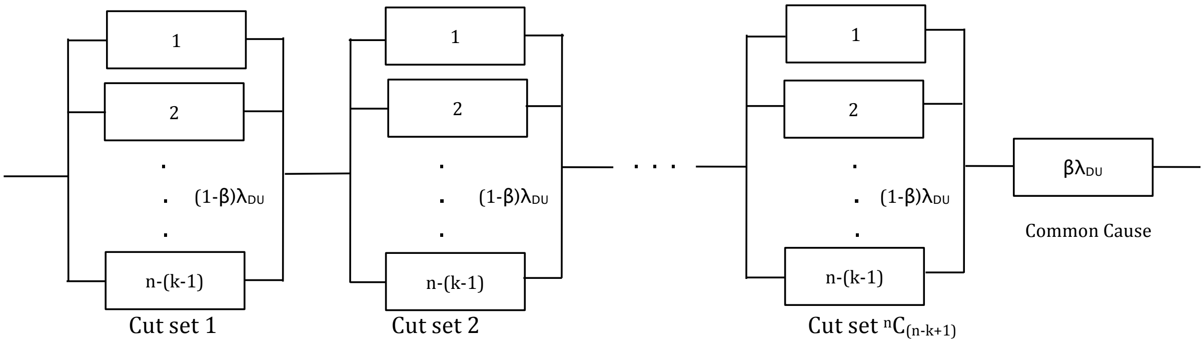

Figure 5.2: Corresponding RBD of *k*oo*n* architecture based on MCSs

Note that the above result is valid only for small $\lambda_{DU}\tau$. If we now assume that MCSs are independent, we can calculate PFD$_{avg}$ for an architecture that has M MCSs (including CCFs) as

$$\mathrm{PFD_{avg}} \approx 1-\prod_{i=1}^{M}\left(1-\mathrm{PFD}_{\mathrm{avg},i}\right) \tag{5.2}$$

If the product terms are negligible, we can simply combine them as

$$\mathrm{PFD}_{\mathrm{avg}} \approx \sum_{i=1}^{M} \mathrm{PFD}_{\mathrm{avg},i} \tag{5.3}$$

In the above two equations we assumed independency between MCSs, which is not of course true as a component(s) may appear in more than one MCSs. The formulas thus give an upper bound of the *true* $\mathrm{PFD}_{\mathrm{avg}}$ and consequently they are called *upper bound approximation formulas*. The validity of the inequality in (5.2) is shown in [20]. It can also be verified that (5.3) is more conservative than (5.2), and hence (5.2) is more closer to the true value.

It is important to understand that the above formulas take the dependency among components into account *twice*. It is normally considered as a product of events by simple probability formula and again by CCF. However, this does not cause serious problem in the calculation since the product terms are almost always negligible and that presumes it is taken care of by only CCF.

Notice that the above result is obtained by averaging after computing the failure probability of a MCS. But, if the averaging is carried out before finding the failure probability of a MCS, the result will be wrong (optimistic). For 1oo1 architecture, $\mathrm{PFD}_{\mathrm{avg}} = \frac{\lambda_{\mathrm{DU}}\tau}{2}$, thus

$$\mathrm{PFD}_{\mathrm{avg}} = \left(\frac{\lambda_{\mathrm{DU}}\tau}{2}\right)^{r} \tag{5.4}$$

It is straightforward to see that (5.4) gives lower result than (5.1). A numerical comparison and discussion on these approaches is presented in part 3 of [6]. In IEC 61508 this approach is considered as wrong.

Several computer programs, including the CARA FaultTree program, compute Top event probability based on (5.4) and (5.2). Although we are sure that for a MCS (5.4) gives optimistic result, it is not possible to say that the final $\mathrm{PFD}_{\mathrm{avg}}$ based on (5.4) and (5.2) is optimistic. This is because the optimistic results in (5.4) may be compensated afterwards by the conservative result from (5.2). To make the calculation safer, nonetheless, we shall impose the correction factor in (5.4) as

$$\frac{(\lambda_{\mathrm{DU}}\tau)^r}{r+1} = \frac{\frac{(\lambda_{\mathrm{DU}}\tau)^r}{r+1}}{\left(\frac{\lambda_{\mathrm{DU}}\tau}{2}\right)^r} \cdot \left(\frac{\lambda_{\mathrm{DU}}\tau}{2}\right)^r = \frac{2^r}{r+1}\left(\frac{\lambda_{\mathrm{DU}}\tau}{2}\right)^r \tag{5.5}$$

Therefore, the correction factor $\frac{2^r}{r+1}$ multiplies the $\mathrm{PFD}_{\mathrm{avg}}$ in each MCS to arrive at the correct solution.

In some large fault trees with many AND and OR gates, the Top event probability may not be reasonably accurate. This accuracy problem is serious, especially, when high-probability events appear in the fault tree [18]. In such situations, binary decision diagram (BDD) can be used and gives an efficient and exact result. It is an alternative way of analyzing fault tree based on disjoint minimal paths instead of MCSs. Since the analysis is based on disjoint minimal paths, the result is exact. However, notice that the standard FTA approach is important for both qualitative and quantitative analyses whereas BDD is important mainly to get accurate Top event probability in an efficient way.

Chapter 6

Markov Analysis

6.1 Introduction

The methods discussed in Chapter 4 and 5 represent the static nature of a system, i.e., time or sequence independent picture of a system. In other words, a component/system has two states (failed or functioning) and there are always sufficient repairmen and resources available to restore failed components. It is thus difficult with these methods to model complex system behaviors and maintenance strategies (e.g., prioritization, resources availability, the minimum number of failed components required to initiate repair action, and so on) [1, 3].

Markov analysis can model the time-dependent movement or transition of a system from one state to another state by taking into account the behavior of the system and attributes related to maintenance strategies and the performance of the repair actions.

Markov analysis can also be used together with the methods that we discussed in Chapter 4 and 5. That is, the solution for a subsystem obtained from Markov analysis can be plugged into RBD and FTA models. But, caution is required here to preserve the independency assumption between events in the RBD and FTA models.

In this chapter we present the theoretical background of Markov analysis and examples to illustrate some possible SIS reliability quantification approaches.

6.2 Assumptions and Limitations

6.2.1 Assumptions

An important assumption of Markov analysis is that the transition rates (failure and repair) from one state to another state are constant with respect to time. But, since repair times are not exponentially distributed, it requires justification before modeling unless the mean time to restoration of components is very small in comparison with the corresponding mean times to failure [3]. A comparative research in [8] shows that the steady state probabilities for constant and non-constant repair times are identical. Therefore, a conclusion is made that in the situations where steady state probabilities are used as a measure of PFD_{avg}, a model with constant repair rate assumption can be used and will give identical results as non-constant repair rate.

It should also be noted that a Markov process is memoryless, i.e., the future state of a system depends only on the state it has today and is independent of all the states it had before. This is the fundamental property of the Markov analysis that users need to understand, and a discussion of a Markov process is given in Section 6.3.

6.2.2 Limitations

Although the flexible nature of Markov analysis enables to incorporate relevant system behaviors in the analysis, the number of states increases exponentially as the number of components increases. This creates intractability problem (especially when time dependent solutions are required) and that may also lead to erroneous results due to wrong specification of states and transitions. It is therefore important to employ appropriate procedures to keep the number of states as small as possible.

In [11] a step-wise technique is presented to generate a Markov model for complex system in a simple manner. The technique simplifies the number of states mainly by eliminating the intermediate states. A straightforward approach is also suggested in IEC 61165 [3]. It recommends that before defining the states, a RBD shall be drawn, and collect any group of n series elements in one element with failure rate $\lambda_1 + \lambda_2 + ... + \lambda_n$ and restoration rate $(\lambda_1 + ... + \lambda_n)/(\lambda_1/\mu_1 + ... + \lambda_n/\mu_n)$, provided that $\lambda_i \ll \mu_i$. This procedure simplifies the calculation to a great extent, and is applied in Chapter 9.

One of the potential limitations of Markov analysis, in reliability analysis, is that it is difficult for users to apply and it requires specific computer programs [1].

6.3 Markov Process

Consider a 1oo2 architecture with identical components, and assume that there is no CCF. It is thus natural to have three states as shown in Table 6.1. The following discussion is influenced by [20, 22].

Table 6.1: Simplified states of a 1oo2 architecture

States	Description
2	Both are functioning
1	One functioning and one is failed
0	None is functioning

Consider a discrete time for the moment. Let $X(t)$ be the state of the 1oo2 architecture and takes a value either 0,1 or 2 in each time period $t \in \{0, 1, 2, 3, ...\}$. The SIF is able to perform the required function if it is either in state 2 or 1, and fails if it is in state 0. That is, $P(X(t) = 0)$ tells us the probability that the SIF is not able to perform the safety function at time t. The purpose is therefore to establish a probability model that represents successive values of $X(t)$.

One could assume independency between these values to simplify the modeling, but it hardly represents the realty as it is not reasonable to say the state of a system at time $t+1$ is independent of the states at times $t \in [0, 1, 2, ..., t]$. For example, in order for the system to be in state 0 at time $t+1$, the system has to be in state 1 at time t. Therefore, $X(t)$ are obviously not independent. It is, of course, reasonable to assume that the state of the system at time $t+1$ is *only* dependent on the state of the system at time t. This means that today's information is sufficient to predict for tomorrow. In other words, given the present state, the future is independent of the past. This assumption characterizes a type of stochastic process called *Markov chain*.

So far, we considered a discrete time, called *discrete-time Markov chain*, to make the discussion smoother. For the purpose of estimating the reliability of a SIS, however, from now on we consider a *continuous-time Markov chain* with finite state space. A state space is a set containing all possible values of $X(t)$ and is designated as Ω.

Based on the argument above, we can define a continues-time Markov chain $X(t)$ such that given the present $X(s)$ and the history of the system up to, but not including, time s $X(u), 0 \leq u < s$, the conditional distribution of $X(t+s)$ depends only on the present and is independent of the history [20]. Mathematically,

$$\begin{aligned} P\left(X(t+s)=j|X(s)=i, X(u)=x(u), 0 \leq u < s\right) &= P\left(X(t+s)=j|X(s)=i\right) \\ &= P_{ij}(s, s+t) \quad \forall u : 0 \leq u < s \end{aligned} \tag{6.1}$$

The above relation is the fundamental equation of the Markov process. We can further impose stationarity (in time) in the process and gives us

$$P_{ij}(s, s+t) = P\left(X(t+s)=j|X(s)=i\right) = P\left(X(t)=j|X(0)=i\right) = P_{ij}(t) \quad \forall s, t \geq 0 \tag{6.2}$$

A Markov process satisfying (6.2) is said to have *stationary* or *homogenous transition probabilities*. This is an important property of the Markov process for our problems because if we let the transition probabilities being dependent of the global time, the model will not obviously be tractable due to environmental, operational, and other seasonal factors [20]. Therefore, from now on, we assume stationarity.

If P_{ij} is the probability that the system makes a transition from state i to j and r is the number of possible states, it satisfies the following:

$$0 \le P_{ij}(t) \le 1 \quad \text{and}$$
$$\sum_{j=0}^{r} P_{ij}(t) = 1 \quad \forall i \in \Omega$$

The equality is intuitive since given the system is in state i, will make transition to either one of the rest of the states or stay in state i with probability 1—*exhaustivity.* It is commonly given in matrix form as

$$\mathbb{P}(t) = \left(\begin{array}{cccccc} P_{00}(t) & P_{01}(t) & . & . & . & P_{0r}(t) \\ P_{10}(t) & P_{11}(t) & . & . & . & P_{1r}(t) \\ . & . & . & & & . \\ . & . & & . & & . \\ . & . & & & . & . \\ P_{r0}(t) & P_{r1}(t) & . & . & . & P_{rr}(t) \end{array}\right)$$

where $\mathbb{P}(t)$ is called the probability transition matrix (PTM).

As we already assumed, the probability of being in any state i at time t depends on the time independent transition rates. A famous differential equation is developed, by a Russian mathematician Andrey N. Kolmogorov in 1931, which characterizes the random dynamic Markov process as

$$\lim_{\Delta t \to 0} \frac{P_{ij}(t+\Delta t) - P_{ij}(t)}{\Delta t} = \dot{P_{ij}}(t) = \sum_{k=0}^{r} \alpha_{kj} P_{ik}(t) \tag{6.3}$$

or in matrix form

$$\dot{\mathbb{P}}(t) = \mathbb{P}(t) \cdot \mathbb{A} \tag{6.4}$$

where $\dot{\mathbb{P}}(t)$ is a time derivative of the transition probability at time t and $\mathbb{A}$ is a transition rate matrix. Thus, (6.4) can be rewritten in matrix form as

$$\begin{pmatrix} \dot{P}_{00}(t) & \dot{P}_{01}(t) & . & . & . & \dot{P}_{0r}(t) \\ \dot{P}_{10}(t) & \dot{P}_{11}(t) & . & . & . & \dot{P}_{1r}(t) \\ . & . & . & & & . \\ . & . & & . & & . \\ . & . & & & . & . \\ \dot{P}_{r0}(t) & \dot{P}_{r1}(t) & . & . & . & \dot{P}_{rr}(t) \end{pmatrix} = \begin{pmatrix} P_{00}(t) & P_{01}(t) & . & . & . & P_{0r}(t) \\ P_{10}(t) & P_{11}(t) & . & . & . & P_{1r}(t) \\ . & . & . & & & . \\ . & . & & . & & . \\ . & . & & & . & . \\ P_{r0}(t) & P_{r1}(t) & . & . & . & P_{rr}(t) \end{pmatrix} \cdot \begin{pmatrix} \alpha_{00}(t) & \alpha_{01}(t) & . & . & . & \alpha_{0r}(t) \\ \alpha_{10}(t) & \alpha_{11}(t) & . & . & . & \alpha_{1r}(t) \\ . & . & . & & & . \\ . & . & & . & & . \\ . & . & & & . & . \\ \alpha_{r0}(t) & \alpha_{r1}(t) & . & . & . & \alpha_{rr}(t) \end{pmatrix}$$

where

$$\alpha_{jj} = -\sum_{\substack{k=0 \\ k\neq j}}^{r} \alpha_{kj}$$

This is called the Kolmogorov forward equation (KFE). The proof of backward and forward Kolmogorov equations is provided in Appendix D, and can also be seen from [20, 22].

In SIS reliability quantification, the aim is to predict the performance the system given that the system is at a specific state at time 0. Therefore, we can simplify the differential equation (6.3) as

$$\dot{P}_j(t) = \sum_{k=0}^{r} \alpha_{kj} P_k(t) \tag{6.5}$$

or in matrix form

$$\begin{pmatrix} \dot{P}_0(t) & \dot{P}_1(t) & . & . & . & \dot{P}_r(t) \end{pmatrix} = \begin{pmatrix} P_0(t) & P_1(t) & . & . & . & P_r(t) \end{pmatrix} \cdot \begin{pmatrix} \alpha_{00}(t) & \alpha_{01}(t) & . & . & . & \alpha_{0r}(t) \\ \alpha_{10}(t) & \alpha_{11}(t) & . & . & . & \alpha_{1r}(t) \\ . & . & . & & & . \\ . & . & & . & & . \\ . & . & & & . & . \\ \alpha_{r0}(t) & \alpha_{r1}(t) & . & . & . & \alpha_{rr}(t) \end{pmatrix} \tag{6.6}$$

Hence, (6.6) is an important equation that shows the relationship between probabilities and transition rates, and is the key to find several system performance measures.

6.4 Unreliability and Unavailability

As discussed in Chapter 3, the performance of a SIS can be computed in terms of unreliability or unavailability (steady state probability). The $\mathrm{PFD}_{\mathrm{avg}}$ computed in Chapters 4 and 5 is the average unreliability of a system in a test interval. Due to the assumption of perfect function testing, however, it turns out that the $\mathrm{PFD}_{\mathrm{avg}}$ is considered as an average long-run unavailability. In Markov analysis, these two concepts have entirely different approaches and interpretations [9].

In the unreliability approach, the $\mathrm{PFD}_{\mathrm{avg}}$ is computed as a time dependent solution for the state(s) where the system is unavailable and then arithmetically averaged over the test interval [20]. Mathematically (assuming test intervals are the same):

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{1}{\tau}\int_0^{\tau} P\left(X(t) \in \mathrm{F}\right)\mathrm{d}t \tag{6.7}$$

where F is a set containing the states where the system is unavailable for safety. In IEC 61508, this approach is considered to be the correct approach of computing $\mathrm{PFD}_{\mathrm{avg}}$ and is discussed further with examples in Section 6.5.1.

In the unavailability approach, we compute the steady state probabilities of the states where the system is unavailable for safety and their arithmetic sum will then be the $\mathrm{PFD}_{\mathrm{avg}}$. Mathematically:

$$\mathrm{PFD}_{\mathrm{avg}} = \sum_{i\in \mathrm{F}} P\left(X(t) = i\right) \tag{6.8}$$

This is by far the easier and faster way of calculating $\mathrm{PFD}_{\mathrm{avg}}$. We have discussed this approach in section 6.5.2.

6.5 Examples

This section presents some examples to illustrate SIS reliability quantification approaches in terms of both unreliability and unavailability. We consider 1oo1 and 1oo2 architectures. Notice that the same architectures are also treated in the cases study in Chapter 9. In this section, no state reduction is employed, but an appropriate procedure [3] is employed in the case study. Therefore, by comparing the analysis in this chapter with Chapter 9, the reader can see how the analysis will be complicated if the number of states is not reduced.

6.5.1 Time Dependent Solution

With time dependent solutions we can quantify two types of system performance.

Type 1: The average probability that the SIS is unavailable for safety regardless of the occurrence of the process demand from the EUC.

Type 2: The average probability that the SIS fails *and* the process demand occurs from the EUC.

Neither IEC 61508 [4] nor ISA [6] requires the reliability quantification methods to take directly the process demand into account. Except the classification of demand rates as low, high and continuous, in all the suggested methods the performances of SISs are quantified regardless of the characteristics of the process (condition) in which they operate, i.e., type 1. Nevertheless, with simple probabilistic approach it is possible to estimate type 2 probability, roughly, as

$$\text{PFD}_{\text{avg, type 1}} = \text{PFD}_{\text{avg, type 2}} \cdot \lambda_{\text{P}} \tag{6.9}$$

where λ_{P} is the demand rate.

However, it is argued in [7] that such a simple classification of demand rates is not sufficient and an explicit incorporation of demand rate (λ_{P}) in the models is necessary. It is further argued that *the issue in determining acceptable risk is not in measuring the probability that the SIS is in a failed (dangerously) state regardless of whether or not a shutdown is required but in measuring the probability that the SIS is in a failed state and the process requires shutdown* (type 2). The potential limitation of this approach is, however, the fact that data for process demand rate is hardly available.

Unlike (6.9), with Markov analysis an exact estimate of type 2 probabilities is possible. Below we present examples of both type 1 and type 2 quantification techniques.

Type 1

Example 1: 1oo1 Architecture

As can be seen from the RBD of this architecture in Figure 4.3, the system fails due to one of the two mutually exclusive failure modes, i.e., dangerous detected or dangerous undetected. The state transition diagram is shown in Figure 6.1.

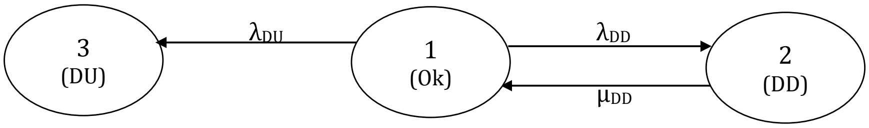

Figure 6.1: State transition diagram for a 1oo1 architecture

The state equations based on (6.6) will be

$$\begin{pmatrix} \dot{P}_1(t) & \dot{P}_2(t) & \dot{P}_3(t) \end{pmatrix} = \begin{pmatrix} P_1(t) & P_2(t) & P_3(t) \end{pmatrix} \cdot \begin{pmatrix} -(\lambda_{\mathrm{DU}}+\lambda_{\mathrm{DD}}) & \lambda_{\mathrm{DD}} & \lambda_{\mathrm{DU}} \\ \mu_{\mathrm{DD}} & -\mu_{\mathrm{DD}} & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{6.10}$$

Therefore

$$\dot{P}_1(t) = -(\lambda_{\mathrm{DU}}+\lambda_{\mathrm{DD}})P_1(t)+\mu_{\mathrm{DD}}P_2(t) \tag{6.11}$$

$$\dot{P}_2(t) = \lambda_{\mathrm{DD}}P_1(t)-\mu_{\mathrm{DD}}P_2(t) \tag{6.12}$$

$$\dot{P}_3(t) = \lambda_{\mathrm{DU}}P_1(t) \tag{6.13}$$

To establish state equations, we do not need to remember (6.6) all the time. For example, to be in state 1 at time $(t+\Delta t)$, either the system is in state 2 at time t and make transition to state 1 with probability $1-\mathrm{e}^{-\mu_{\mathrm{DD}}\Delta t} \approx \mu_{\mathrm{DD}}\Delta t$, OR in state 1 at time t and make no transition to anywhere, i.e., with probability $1-(\lambda_{\mathrm{DU}}+\lambda_{\mathrm{DD}})\Delta t$. Mathematically

$$\begin{aligned} P_1(t+\Delta t) &= [1-(\lambda_{\mathrm{DU}}+\lambda_{\mathrm{DD}})\Delta t]P_1(t)+\mu_{\mathrm{DD}}\Delta t P_2(t) \\ \lim_{\Delta t\to 0}\frac{P_1(t+\Delta t)-P_1(t))}{\Delta t} &= -(\lambda_{\mathrm{DU}}+\lambda_{\mathrm{DD}})P_1(t)+\mu_{\mathrm{DD}}P_2(t) \\ \dot{P}_1(t) &= -(\lambda_{\mathrm{DU}}+\lambda_{\mathrm{DD}})P_1(t)+\mu_{\mathrm{DD}}P_2(t) \end{aligned}$$

Any way, to solve the above differential equations we make use of Laplace transformation and their transform, respectively, is

$$\begin{aligned} sP_1(s) - 1 &= -(\lambda_{\text{DU}} + \lambda_{\text{DD}})P_1(s) + \mu_{\text{DD}}P_2(s) && (6.14)\\ sP_2(s) - 0 &= \lambda_{\text{DD}}P_1(s) - \mu_{\text{DD}}P_2(s) && (6.15)\\ sP_3(s) - 0 &= \lambda_{\text{DU}}P_1(s) && (6.16) \end{aligned}$$

From (6.15) we have

$$(s+\mu_{\text{DD}})P_2(s) = \lambda_{\text{DD}}P_1(s) \Rightarrow P_2(s) = \frac{\lambda_{\text{DD}}}{s+\mu_{\text{DD}}}P_1(s) \tag{6.17}$$

Substituting this into (6.14) gives

$$\begin{aligned} P_1(s) &= \frac{s+\mu_{\text{DD}}}{s^2 + s(\mu_{\text{DD}} + \lambda_{\text{DU}} + \lambda_{\text{DD}}) + \mu_{\text{DD}}\lambda_{\text{DU}}}\\ &= \frac{s+\mu_{\text{DD}}}{(s+r_1)(s+r_2)} && (6.18) \end{aligned}$$

where

$$\begin{aligned} r_1 &= -\frac{1}{2}\left(-(\mu_{\text{DD}} + \lambda_{\text{DU}} + \lambda_{\text{DD}}) - \sqrt{(\mu_{\text{DD}} + \lambda_{\text{DU}} + \lambda_{\text{DD}})^2 - 4\mu_{\text{DD}}\lambda_{\text{DU}}}\right) && (6.19)\\ r_2 &= -\frac{1}{2}\left(-(\mu_{\text{DD}} + \lambda_{\text{DU}} + \lambda_{\text{DD}}) + \sqrt{(\mu_{\text{DD}} + \lambda_{\text{DU}} + \lambda_{\text{DD}})^2 - 4\mu_{\text{DD}}\lambda_{\text{DU}}}\right) && (6.20) \end{aligned}$$

If we substitute (6.18) into (6.17), we get

$$P_2(s) = \frac{\lambda_{\text{DD}}}{(s+r_1)(s+r_2)} \tag{6.21}$$

and if we do the same into (6.16), we get

$$P_3(s) = \frac{\lambda_{\text{DU}}}{(s+r_1)(s+r_2)} + \frac{\lambda_{\text{DU}}\mu_{\text{DD}}}{s(s+r_1)(s+r_2)} \tag{6.22}$$

Now we need to transform the equations from Laplace domain back to time domain, and we need the following inverse Laplace transforms, where a and b are constants:

$$
\begin{aligned}
\frac{1}{(s+a)(s+b)} &= \frac{1}{b-a}\left(\mathrm{e}^{-at}-\mathrm{e}^{-bt}\right) && (6.23)\\
\frac{s}{(s+a)(s+b)} &= \frac{1}{b-a}\left(a\mathrm{e}^{-at}-b\mathrm{e}^{-bt}\right) && (6.24)\\
\frac{1}{s(s+a)(s+b)} &= \frac{1}{ab}\left(1-\frac{b}{b-a}\mathrm{e}^{-at}-\frac{a}{b-a}\mathrm{e}^{-bt}\right) && (6.25)
\end{aligned}
$$

Therefore, the probability that we find the system in state $i=1,2,3$ at time t, can be obtained, respectively, as follows:

$$
\begin{aligned}
P_1(t) &= \frac{1}{r_2-r_1}\left(r_1\mathrm{e}^{-r_1t}-r_2\mathrm{e}^{-r_2t}\right)+\frac{\mu_{\mathrm{DD}}}{r_2-r_1}\left(\mathrm{e}^{-r_1t}-\mathrm{e}^{-r_2t}\right)\\
&= \left(\frac{r_1+\mu_{\mathrm{DD}}}{r_2-r_1}\right)\mathrm{e}^{-r_1t}-\left(\frac{r_2+\mu_{\mathrm{DD}}}{r_2-r_1}\right)\mathrm{e}^{-r_2t} && (6.26)\\
P_2(t) &= \frac{\lambda_{\mathrm{DD}}}{r_2-r_1}\left(\mathrm{e}^{-r_1t}-\mathrm{e}^{-r_2t}\right) && (6.27)\\
P_3(t) &= \frac{\lambda_{\mathrm{DU}}}{r_2-r_1}\left(\mathrm{e}^{-r_1t}-\mathrm{e}^{-r_2t}\right)+\frac{\lambda_{\mathrm{DU}}\mu_{\mathrm{DD}}}{r_1r_2}\left(1-\frac{r_2}{r_2-r_1}\mathrm{e}^{-r_1t}+\frac{r_1}{r_2-r_1}\mathrm{e}^{-r_2t}\right)\\
&= 1+\left(\frac{\lambda_{\mathrm{DU}}-r_2}{r_2-r_1}\right)\mathrm{e}^{-r_1t}+\left(\frac{r_1-\lambda_{\mathrm{DU}}}{r_2-r_1}\right)\mathrm{e}^{-r_2t} && (6.28)
\end{aligned}
$$

We can observe that $P_1(\infty)=0$, $P_2(\infty)=0$. But, $P_3(\infty)=1$, i.e., the system will eventually goes to state 3 and get trapped there forever.

Since λ and μ are too small to allow $\mathrm{e}^{rt}\approx 1-rt$, we have for state 2

$$\mathrm{PFD}_{\mathrm{avg-2}}=\frac{1}{\tau}\int_0^\tau P_2(t)\mathrm{d}t\approx\frac{\lambda_{\mathrm{DD}}}{\tau(r_2-r_1)}\int_0^\tau(r_2-r_1)t\mathrm{d}t=\frac{\lambda_{\mathrm{DD}}\tau}{2} \qquad (6.29)$$

and similarly for state 3

$$
\begin{aligned}
\mathrm{PFD}_{\mathrm{avg-3}} &= \frac{1}{\tau}\int_0^\tau P_3(t)\mathrm{d}t\\
&\approx 1+\left(\frac{\lambda_{\mathrm{DU}}-r_2}{r_2-r_1}\right)\left(1-\frac{r_1\tau}{2}\right)+\left(\frac{r_1-\lambda_{\mathrm{DU}}}{r_2-r_1}\right)\left(1-\frac{r_2\tau}{2}\right) && (6.30)
\end{aligned}
$$

Therefore, the average SIS unreliability is

$$\mathrm{PFD}_{\mathrm{avg}}=\mathrm{PFD}_{\mathrm{avg-2}}+\mathrm{PFD}_{\mathrm{avg-3}} \qquad (6.31)$$

Example 2: 1oo2 Architecture

The RBD of a 1oo2 architecture is shown in Figure 4.5. Under the assumption that two repairmen are available, the state transition diagram is shown in Figure 6.2.

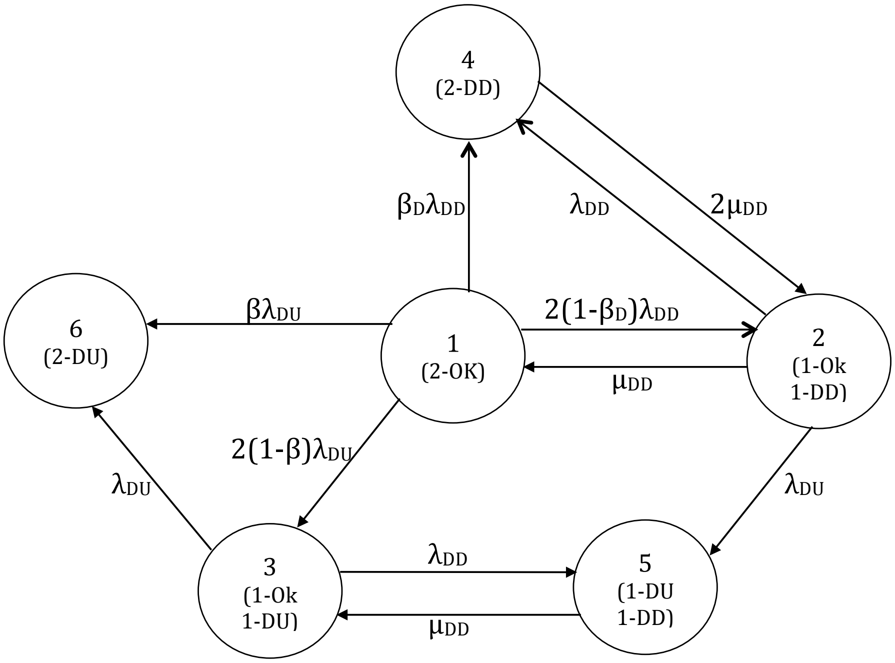

Figure 6.2: State transition diagram for a 1oo2 architecture

The state equations are

$$
\begin{aligned}
\dot{P}_1(t) &= -\left(2(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}} + 2(1-\beta)\lambda_{\mathrm{DU}} + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}} + \beta\lambda_{\mathrm{DU}}\right) P_1(t) + \mu_{\mathrm{DD}} P_2(t) \\
\dot{P}_2(t) &= 2(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}} P_1(t) - \left(\lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}} + \mu_{\mathrm{DD}}\right) P_2(t) + 2\mu_{\mathrm{DD}} P_4(t) \\
\dot{P}_3(t) &= 2(1-\beta)\lambda_{\mathrm{DU}} P_1(t) - (\lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}}) P_3(t) + \mu_{\mathrm{DD}} P_5(t) \\
\dot{P}_4(t) &= \beta_{\mathrm{D}}\lambda_{\mathrm{DD}} P_1(t) + \lambda_{\mathrm{DD}} P_2(t) - 2\mu_{\mathrm{DD}} P_4(t) \\
\dot{P}_5(t) &= \lambda_{\mathrm{DU}} P_2(t) + \lambda_{\mathrm{DD}} P_3(t) - \mu_{\mathrm{DD}} P_5(t) \\
\dot{P}_6(t) &= \beta\lambda_{\mathrm{DU}} P_1(t) + \lambda_{\mathrm{DU}} P_3(t)
\end{aligned}
$$

The solution of the above set of differential equations is computed in Maple, but it is too large to be presented in this report. A time dependent analytical solution for a Markov process with five or more states is always very hard. However, it is still possible to find a numerical solution using an appropriate software, and thus the required probability will be

$$\text{PFD}_{\text{avg}} = \text{PFD}_{\text{avg}-4} + \text{PFD}_{\text{avg}-5} + \text{PFD}_{\text{avg}-6} \tag{6.32}$$

Type 2

In this section we offer the state transition diagrams and the corresponding state equations of the examples considered above when demand rate is incorporated. The computational procedure is the same as the one shown above to the 1oo1 architecture.

Example 1: 1oo1 Architecture

The accident occurs only if the process demand occurs *and* the SIS is either in state 2 or state 3 in Figure 6.1. Therefore, the state transition diagram can be redrawn as shown in Figure 6.3, and the state equations can be established accordingly as follows:

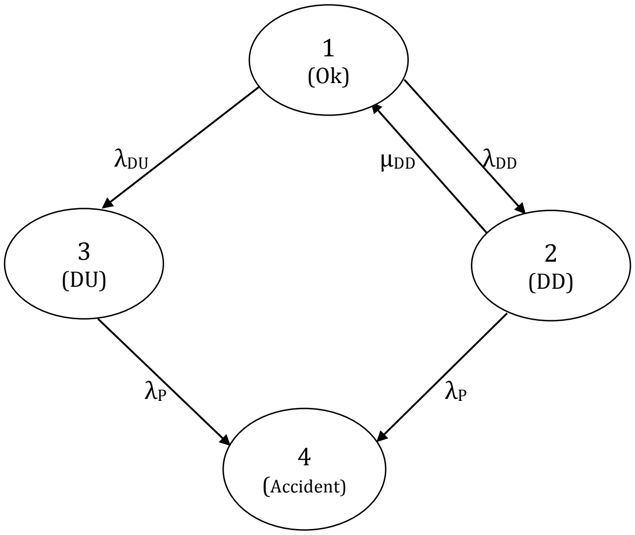

Figure 6.3: State transition diagram for a 1oo1 architecture (with process demand)

$$\begin{aligned}
\dot{P}_1(t) &= -(\lambda_{\text{DU}} + \lambda_{\text{DD}})P_1(t) + \mu_{\text{DD}}P_2(t) \\
\dot{P}_2(t) &= \lambda_{\text{DD}}P_1(t) - (\mu_{\text{DD}} + \lambda_{\text{P}})P_2(t) \\
\dot{P}_3(t) &= \lambda_{\text{DU}}P_1(t) - \lambda_{\text{P}}P_3(t) \\
\dot{P}_4(t) &= \lambda_{\text{P}}P_2(t) + \lambda_{\text{P}}P_3(t)
\end{aligned}$$

Therefore, the probability that the SIS is in a failed state *and* the process requires activation is

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{1}{\tau}\int_0^{\tau} P_4(t)\,\mathrm{d}t \tag{6.33}$$

Example 2: 1oo2 Architecture

Figure 6.4 shows the state transition diagram for a 1oo2 architecture taking into account the demand rate. In the diagram, state 7 represents the accident resulted from SIS failure due to either DD, DU or a combination of them *and* a demand occurs from the EUC. The corresponding state equations are as follows:

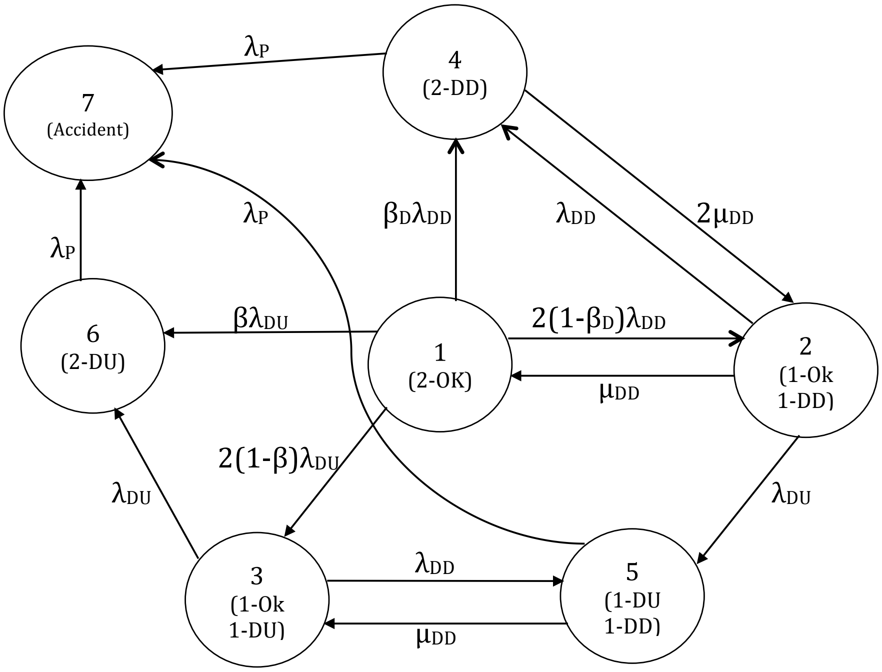

Figure 6.4: State transition diagram for a 1oo2 architecture (with process demand)

$$\begin{aligned}
\dot{P}_1(t) &= -\big(2(1-\beta_\mathrm{D})\lambda_\mathrm{DD} + 2(1-\beta)\lambda_\mathrm{DU} + \beta_\mathrm{D}\lambda_\mathrm{DD} + \beta\lambda_\mathrm{DU}\big)\,P_1(t) + \mu_\mathrm{DD}P_2(t) \\
\dot{P}_2(t) &= 2(1-\beta_\mathrm{D})\lambda_\mathrm{DD}P_1(t) - \big(\lambda_\mathrm{DD} + \lambda_\mathrm{DU} + \mu_\mathrm{DD}\big)\,P_2(t) + 2\mu_\mathrm{DD}P_4(t) \\
\dot{P}_3(t) &= 2(1-\beta)\lambda_\mathrm{DU}P_1(t) - (\lambda_\mathrm{DD} + \lambda_\mathrm{DU})\,P_3(t) + \mu_\mathrm{DD}P_5(t) \\
\dot{P}_4(t) &= \beta_\mathrm{D}\lambda_\mathrm{DD}P_1(t) + \lambda_\mathrm{DD}P_2(t) - (2\mu_\mathrm{DD} + \lambda_\mathrm{P})P_4(t) \\
\dot{P}_5(t) &= \lambda_\mathrm{DU}P_2(t) + \lambda_\mathrm{DD}P_3(t) - (\mu_\mathrm{DD} + \lambda_\mathrm{P})P_5(t) \\
\dot{P}_6(t) &= \beta\lambda_\mathrm{DU}P_1(t) + \lambda_\mathrm{DU}P_3(t) - \lambda_\mathrm{P}P_6(t) \\
\dot{P}_7(t) &= \lambda_\mathrm{P}P_4(t) + \lambda_\mathrm{P}P_5(t) + \lambda_\mathrm{P}P_6(t)
\end{aligned}$$

Hence, the probability that the SIS is in a failed state *and* the process requires activation is

$$\mathrm{PFD}_\mathrm{avg} = \frac{1}{\tau}\int_0^\tau P_7(t)\mathrm{d}t \tag{6.34}$$

6.5.2 Steady State Solution

If a Markov process is irreducible[1] and positive recurrent[2], then [22]

$$\lim_{t\to\infty} P_k(t) = P_k \quad \text{for } k = 1,2,3,\ldots,r \tag{6.35}$$

Now, take a limit to infinity on both sides in (6.5), that is

$$\lim_{t\to\infty} \dot{P}_j(t) = \lim_{t\to\infty} \sum_{k=0}^{r} \alpha_{kj}P_k(t) \tag{6.36}$$

But, the left hand side in (6.36) converges to 0 since otherwise (6.35) does not hold. Therefore

$$0 = \sum_{k=0}^{r} \alpha_{kj}P_k \tag{6.37}$$

[1] A Markov Process is said to be irreducible if, starting in state i, there is a positive probability of ever being in state j, for all i, j.

[2] A Markov process is said to be positive recurrent if, starting in any state, the mean time to return to that state is finite.

or in matrix form

$$\begin{pmatrix} 0 & 0 & . & . & . & 0 \end{pmatrix} = \begin{pmatrix} P_0 & P_1 & . & . & . & P_r \end{pmatrix} \cdot \begin{pmatrix} \alpha_{00}(t) & \alpha_{01}(t) & . & . & . & \alpha_{0r}(t) \\ \alpha_{10}(t) & \alpha_{11}(t) & . & . & . & \alpha_{1r}(t) \\ . & . & . & & & . \\ . & . & & . & & . \\ . & . & & & . & . \\ \alpha_{r0}(t) & \alpha_{r1}(t) & . & . & . & \alpha_{rr}(t) \end{pmatrix} \tag{6.38}$$

and we also have

$$\sum_{k=0}^{r} P_k = 1 \tag{6.39}$$

Therefore, $r-1$ linear equations from (6.38), and (6.39) can be used to solve the steady state probabilities. The steady state probability P_k is the long-run probability that the system stays in state k. In other words, P_k is the long-run proportion of time that the process is in state k. Note that the steady state probabilities are independent of the periodic function testing (τ).

Example 1: 1oo1 Architecture

To be able to quantify the steady state probabilities, we must first establish an irreducible state transition diagram for the architecture under consideration. Assume that upon detection of the DU failures during function test, a repair action initiates and restore the system back to functioning state, i.e., state 1 (note however that this duration is assumed to be exponentially distributed). Thus, Figure 6.1 can be amended as shown in Figure 6.5. Thus, the state equations

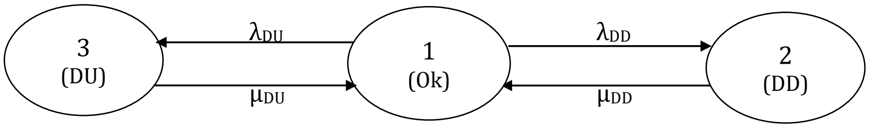

Figure 6.5: State transition diagram for a 1oo1 architecture

are

$$\begin{pmatrix} 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_1 & P_2 & P_3 \end{pmatrix} \cdot \begin{pmatrix} -\lambda_{\mathrm{D}} & \lambda_{\mathrm{DD}} & \lambda_{\mathrm{DU}} \\ \mu_{\mathrm{DD}} & -\mu_{\mathrm{DD}} & 0 \\ \mu_{\mathrm{DU}} & 0 & -\mu_{\mathrm{DU}} \end{pmatrix} \tag{6.40}$$

and we also have

$$\sum_{k=0}^{r} P_k = 1 \tag{6.41}$$

It is always advisable to eliminate a column that has most non-zero elements to make the calculation easy. Hence,

$$\begin{aligned} 0 &= \lambda_{\mathrm{DD}} P_1 - \mu_{\mathrm{DD}} P_2 \\ 0 &= \lambda_{\mathrm{DU}} P_1 - \mu_{\mathrm{DU}} P_3 \\ 1 &= P_1 + P_2 + P_3 \end{aligned}$$

The steady state probabilities are therefore,

$$P_1 = \frac{\mu_{\mathrm{DD}}\mu_{\mathrm{DU}}}{\mu_{\mathrm{DD}}\mu_{\mathrm{DU}} + \lambda_{\mathrm{DD}}\mu_{\mathrm{DD}} + \lambda_{\mathrm{DD}}\mu_{\mathrm{DU}}} \tag{6.42}$$

$$P_2 = \frac{\lambda_{\mathrm{DD}}\mu_{\mathrm{DU}}}{\mu_{\mathrm{DD}}\mu_{\mathrm{DU}} + \lambda_{\mathrm{DD}}\mu_{\mathrm{DD}} + \lambda_{\mathrm{DD}}\mu_{\mathrm{DU}}} \tag{6.43}$$

$$P_2 = \frac{\lambda_{\mathrm{DD}}\mu_{\mathrm{DD}}}{\mu_{\mathrm{DD}}\mu_{\mathrm{DU}} + \lambda_{\mathrm{DD}}\mu_{\mathrm{DD}} + \lambda_{\mathrm{DD}}\mu_{\mathrm{DU}}} \tag{6.44}$$

The above probabilities tell us the proportion of times that we find the system in a particular state at a random point of time. For example, P_3 is the long-run proportion of time that the system is in a dangerously undetected failed state.

Example 2: 1oo2 Architecture

Assume that upon detection of DU failures in both channels, the repair crews restore both channels to a functioning state (state 1), i.e., full restoration. We further assumed that the time required to do the restoration is exponentially distributed with rate μ_{DU}. The situation in Figure 6.2 is modified accordingly and produce an irreducible state transition diagram as shown in Figure 6.6.

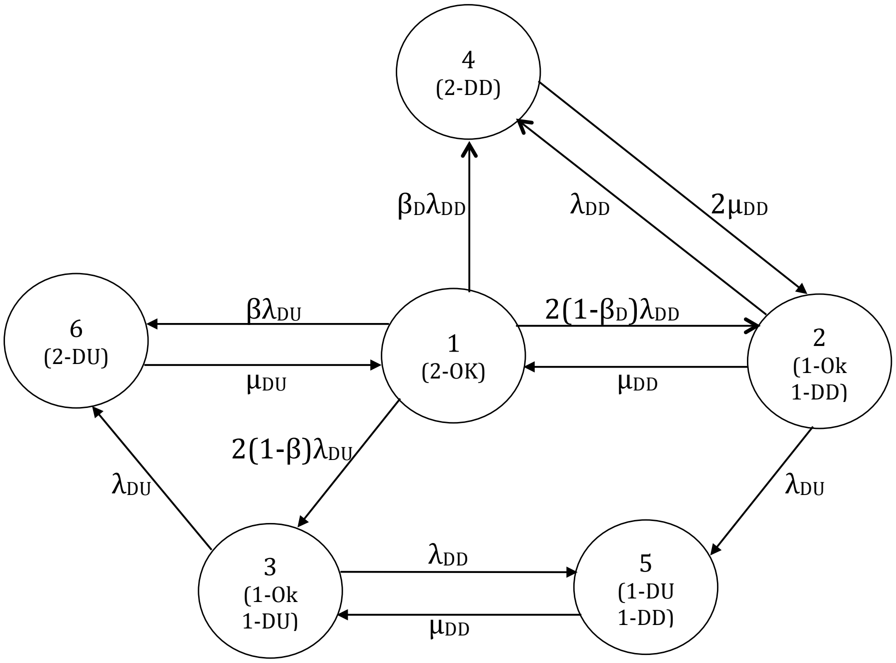

Figure 6.6: State transition diagram for a 1oo2 architecture

The state equations therefore are (the first linear equation is eliminated)

$$\begin{aligned}
0 &= 2(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}P_1 - \left(\lambda_{\mathrm{DD}}+\lambda_{\mathrm{DU}}+\mu_{\mathrm{DD}}\right)P_2 + 2\mu_{\mathrm{DD}}P_4\\
0 &= 2(1-\beta)\lambda_{\mathrm{DU}}P_1 - (\lambda_{\mathrm{DD}}+\lambda_{\mathrm{DU}})P_3 + \mu_{\mathrm{DD}}P_5\\
0 &= \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}P_1 + \lambda_{\mathrm{DD}}P_2 - 2\mu_{\mathrm{DD}}P_4\\
0 &= \lambda_{\mathrm{DU}}P_2 + \lambda_{\mathrm{DD}}P_3 - \mu_{\mathrm{DD}}P_5\\
0 &= \beta\lambda_{\mathrm{DU}}P_1 + \lambda_{\mathrm{DU}}P_3 - \mu_{\mathrm{DD}}P_6\\
1 &= P_1+P_2+P_3+P_4+P_5+P_6
\end{aligned}$$

Since the analytical solutions for the steady state probabilities are large, we only present the solution for P_6, which is an important solution from a safety viewpoint.

$$P_6 = \frac{2\lambda_{\mathrm{DU}}\left(\beta\lambda_{\mathrm{DD}}^2+\mathrm{A}+\mathrm{B}\right)}{\lambda_{\mathrm{DD}}^3\left(2\beta_{\mathrm{D}}-2\right)+\mathrm{C}+\mathrm{D}+\mathrm{E}} \tag{6.45}$$

Where

$$
\begin{aligned}
\mathrm{A} &= \lambda_{\mathrm{DD}}\left(2\beta\lambda_{\mathrm{DU}}-2\beta\lambda_{\mathrm{D}}-\beta_{\mathrm{D}}\lambda_{\mathrm{DU}}-\beta\mu_{\mathrm{DD}}\right)\\
\mathrm{B} &= -2\beta\lambda_{\mathrm{DU}}\lambda_{\mathrm{D}}-2\beta\lambda_{\mathrm{DU}}\mu_{\mathrm{DD}}+2\lambda_{\mathrm{DU}}\lambda_{\mathrm{D}}+2\lambda_{\mathrm{DU}}\mu_{\mathrm{DD}}+\beta\lambda_{\mathrm{D}}\mu_{\mathrm{DD}}+\beta\lambda_{\mathrm{D}}^{2}\\
\mathrm{C} &= \lambda_{\mathrm{DD}}^{2}\left(6\beta\lambda_{\mathrm{DU}}-3\beta_{\mathrm{D}}\lambda_{\mathrm{D}}+2\lambda_{\mathrm{D}}+\beta_{\mathrm{D}}\mu_{\mathrm{DD}}-4\lambda_{\mathrm{DU}}-2\mu_{\mathrm{DD}}\right)\\
\mathrm{D} &= \lambda_{\mathrm{DD}}(-2\beta_{\mathrm{D}}\lambda_{\mathrm{DU}}^{2}+4\beta\lambda_{\mathrm{DU}}^{2}-2\beta_{\mathrm{D}}\lambda_{\mathrm{DU}}\mu_{\mathrm{DD}}+4\lambda_{\mathrm{DU}}\mu_{\mathrm{DD}}-2\mu_{\mathrm{DD}}^{2}-\beta_{\mathrm{D}}\lambda_{\mathrm{D}}\mu_{\mathrm{DD}}-2\beta_{\mathrm{D}}\lambda_{\mathrm{D}}\lambda_{\mathrm{DU}}\\
&\quad +8\lambda_{\mathrm{D}}\lambda_{\mathrm{DU}}-8\beta\lambda_{\mathrm{D}}\lambda_{\mathrm{DU}}+\lambda_{\mathrm{D}}^{2}\beta_{\mathrm{D}}-2\beta\lambda_{\mathrm{DU}}\mu_{\mathrm{DD}})\\
\mathrm{E} &= 4\lambda_{\mathrm{DU}}\mu_{\mathrm{DD}}^{2}-2\beta\lambda_{\mathrm{DD}}\lambda_{\mathrm{DU}}\lambda_{\mathrm{D}}+2\beta\lambda_{\mathrm{DU}}\lambda_{\mathrm{D}}^{2}-4\beta\lambda_{\mathrm{DU}}\mu_{\mathrm{DD}}^{2}-4\beta\lambda_{\mathrm{DU}}^{2}\lambda_{\mathrm{D}}-4\beta\lambda_{\mathrm{DU}}^{2}\mu_{\mathrm{DD}}+4\lambda_{\mathrm{DU}}^{2}\mu_{\mathrm{DD}}\\
&\quad +2\lambda_{\mathrm{D}}^{2}\mu_{\mathrm{DD}}+4\lambda_{\mathrm{DU}}\lambda_{\mathrm{D}}\mu_{\mathrm{DD}}+4\lambda_{\mathrm{DU}}^{2}\lambda_{\mathrm{D}}+2\lambda_{\mathrm{D}}\mu_{\mathrm{DD}}^{2}
\end{aligned}
$$

It should be noted that once the state transition diagram is drawn, the numerical solution for steady state probabilities is not difficult at all, regardless of the number of states.

Chapter 7

What if the Failure Rate is not Constant

7.1 Introduction

Most, if not all, risk and reliability analysis techniques are based on the assumption of constant failure rate, i.e., a component is *as good as new* during its useful life period. The main argument of the assumption results from the fact that the failure rate distribution of most components look like a bathtub curve as illustrated in Figure 7.1. The curve decreases during the burn-in (infant mortality) period, as some design and manufacturing problems are revealed over time, and increases in the wear-out period due to aging. However, during the useful life period the failure rate appears to be flat and thus is approximated to a time invariant failure rate λ, and so exponential distribution can be used.

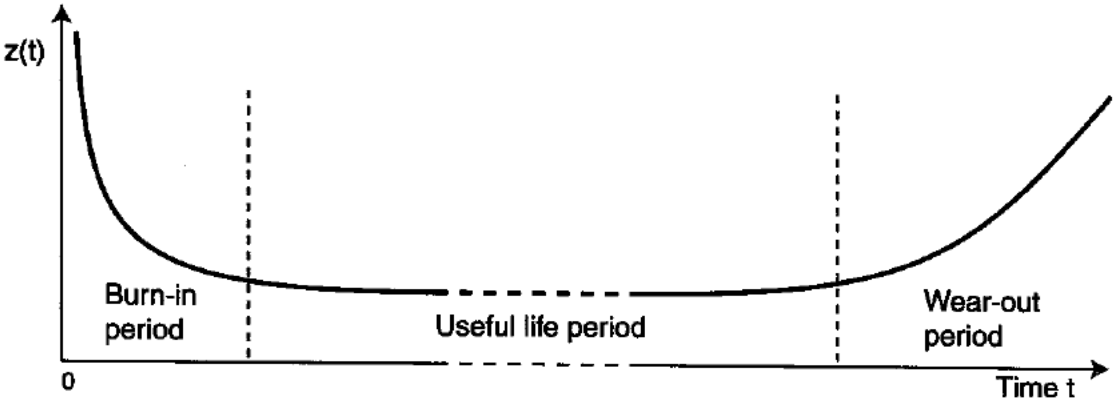

Figure 7.1: Bathtub curve [20]

With the assumption of exponential distribution the mean fully characterizes the distribution. However, with other lifetime distributions, e.g. Weibull, usually two parameters describe the distribution. Since existing reliability databases are not too sufficient to estimate these parameters with reasonable accuracy, it has been a challenge to work with more realistic lifetime distributions, and even an attempt may lead to a result that is susceptible to high uncertainty. In 1998 a research [21] is conducted to study the consequence of estimating the PFD_{avg} under the assumption of Weibull distribution. The result shows that, due to lack of data to estimate the parameters with reasonable accuracy, the estimates were non-robust. This and its computational tractability contribute for exponential distribution to widespread in system reliability analysis.

Nevertheless, it is not simply deniable the fact that the reliability of man-made equipment deteriorate over time. Even in the useful life period, the failure rate of the majority of mechanical components increases over time [20] though the extent may vary over the types of components that we are looking at. For example, for rotating equipment this assumption hardly represents the reality.

It is evident in most cases that the assumption suppresses the value of *time*. For example, preventive maintenance can not be done since a component is as good as new, i.e., as long as a component is functioning no repair or maintenance is required. However, since this assumption has been perpetuated in all the standards, guidelines, books, articles and so on, its feasibility is overlooked.

We are not, however, trivializing the role of exponential distribution in reliability analysis and not also aimed to argue on its pitfalls, but the aim is to provide a generalized method for PFD_{avg} calculation that is not limited to constant failure rate assumption.

7.2 Proposed Method

Assumptions:

- All components in a $1\text{oo}k$ architecture are independent and identical. It implies that individual components in a MCS follow the same distribution with identical parameters.
- In a test interval, the distribution of the time to failure (T) for a $1\text{oo}k$ architecture inherits the distribution of $1\text{oo}1$ architecture with appropriate parameters.

The cumulative distribution functions (CDF) of $1\text{oo}k$ and $1\text{oo}1$ architectures are illustrated in Figure 7.2. In each time point there exists a multiplier $\mathrm{A}(t)$ that equates the two CDFs. We can mathematically express it as

$$F_{1\text{oo}k}(t) = \frac{1}{\mathrm{A}(t)} \cdot F_{1\text{oo}1}(t) \tag{7.1}$$

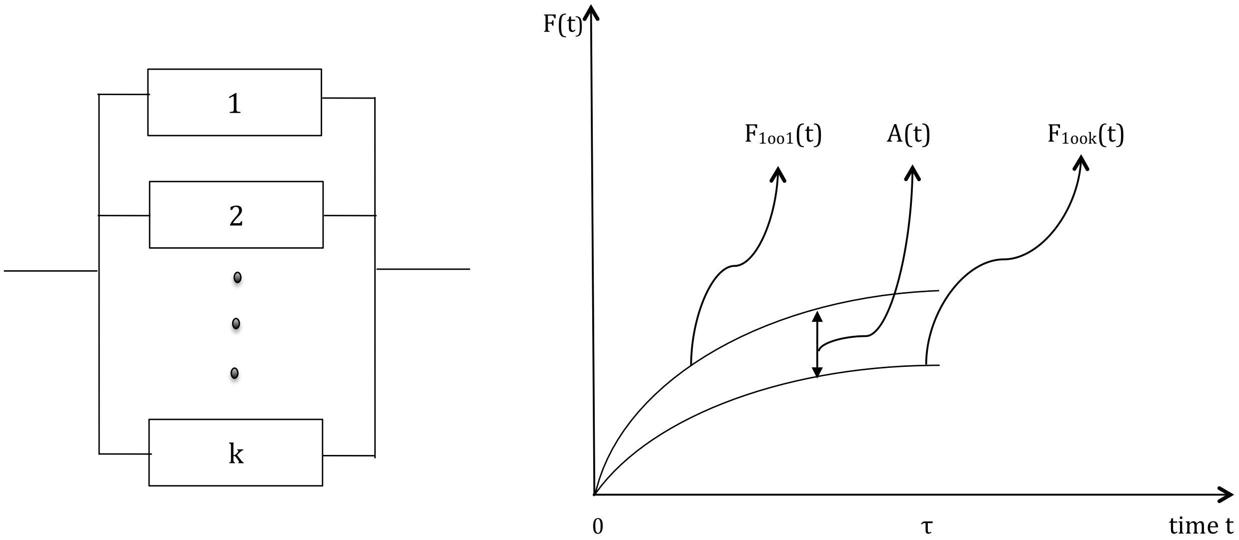

Figure 7.2: RBD for a $1\text{oo}k$ architecture (left), and the CDFs of $1\text{oo}1$ and $1\text{oo}k$ architectures (right)

The implication of the proposed method can be seen under the assumption of Weibull distribution. Throughout this chapter we consider this distribution but the basic principle could also be applied under the assumption of other lifetime distributions.

7.3 The PFD_{avg} Under Weibull Distribution

Weibull distribution was first described in detail by the Swedish Professor Waloddi Weibull and so named after him. It is a very flexible lifetime distribution that has been widely used in several areas where lifetime analysis is important. Exponential distribution is the special case of this distribution. The density, survival and cumulative distribution functions are presented as follows, respectively.

$$\begin{aligned} f(t) &= \alpha(\lambda)^\alpha t^{\alpha-1} \mathrm{e}^{1(\lambda t)^\alpha} && (7.2) \\ R(t) &= \mathrm{e}^{-(\lambda t)^\alpha} && (7.3) \\ F(t) &= 1 - \mathrm{e}^{-(\lambda t)^\alpha} && (7.4) \end{aligned}$$

where λ and α are referred to as scale and shape parameters, respectively. If $\alpha = 1$ Weibull distribution reduces to exponential distribution, i.e., constant failure rate. If $\alpha > 1$, the failure rate function is increasing, and decreasing if $\alpha < 1$.

Let $F_k(t)$ and $F_n(t)$, $k \geq n$, be the CDFs of $1\mathrm{oo}k$ and $1\mathrm{oo}n$ architectures respectively (from now on we use i instead of $1\mathrm{oo}i$). The ratio of these distributions can thus be simplified as follows:

$$\frac{F_k(t)}{F_n(t)} = \frac{1-\mathrm{e}^{-(\lambda_k t)^\alpha}}{1-\mathrm{e}^{-(\lambda_n t)^\alpha}} \approx \frac{(\lambda_k t)^\alpha}{(\lambda_n t)^\alpha} = \left(\frac{\lambda_k}{\lambda_n}\right)^\alpha = \left(\frac{\frac{1}{\lambda_n}\Gamma(\frac{1}{\alpha}+1)}{\frac{1}{\lambda_k}\Gamma(\frac{1}{\alpha}+1)}\right)^\alpha = \left(\frac{\mu_n}{\mu_k}\right)^\alpha \tag{7.5}$$

where μ is the mean of the distribution. The approximation is obvious because λt is always small and so is $(\lambda t)^\alpha$ (since $\alpha \geq 1$ for all components).

Consider 1oo1 and 1oo2 architectures. $F_1(t)$ is the probability that a component fails before time t, and $F_2(t)$ is the probability that both components fail before time t. The ratio (multiplier) of this probabilities at time t is $(\mu_1/\mu_2)^\alpha$. However, this multiplier is conditional on the second component failure in a 1oo2 architecture and that occurs with probability $F(t)$. In other words, the multiplier manifests upon the failure of the second component after the first has already failed. Therefore

$$F_2(t) = \left[\left(\frac{\mu_1}{\mu_2}\right)^\alpha F(t)\right] F_1(t) \tag{7.6}$$

Notice that since we assumed that components are identical, $F(t)$ and $F_1(t)$ are identical but their purpose is different, as it shall be seen later.

If we express 1oo3 with respect to 1oo2, we get

$$\begin{aligned} F_3(t) &= \left[\left(\frac{\mu_2}{\mu_3}\right)^{\alpha} F(t)\right] F_2(t) \\ &= \left[\left(\frac{\mu_2}{\mu_3}\right)^{\alpha} F(t)\right]\left[\left(\frac{\mu_1}{\mu_2}\right)^{\alpha} F(t)\right] F_1(t) = \left[\left(\frac{\mu_1}{\mu_3}\right)^{\alpha} (F(t))^2\right] F_1(t) \qquad (7.7) \end{aligned}$$

We can thus generalize for 1oo$k$ architecture as

$$F_k(t) = \left[\left(\frac{\mu_1}{\mu_k}\right)^{\alpha} (F(t))^{k-1}\right] F_1(t) \qquad (7.8)$$

Now let us find a simplified expression for the multiplier in (7.5). The survival function for 1oo$k$ architecture is given by:

$$R_k(t) = 1 - \left(1 - \mathrm{e}^{-(\lambda t)^{\alpha}}\right)^k$$

If we use binomial expansion, we get

$$\begin{aligned} R_k(t) &= 1 - \sum_{x=0}^{k} \binom{k}{x} \left(-\mathrm{e}^{-(\lambda t)^{\alpha}}\right)^x \\ &= \sum_{x=1}^{k} \binom{k}{x} (-1)^{x+1} \left(\mathrm{e}^{-(\lambda t)^{\alpha}}\right)^x \\ &= \sum_{x=1}^{k} \binom{k}{x} (-1)^{x+1} \left(\mathrm{e}^{-(x^{\frac{1}{\alpha}} \lambda t)^{\alpha}}\right) \end{aligned}$$

Therefore,

$$\begin{aligned} \mu_k &= \sum_{x=1}^{k} \binom{k}{x} (-1)^{x+1} \int_0^{\infty} \mathrm{e}^{-(x^{\frac{1}{\alpha}} \lambda t)^{\alpha}} \mathrm{d}t \\ &= \sum_{x=1}^{k} \binom{k}{x} (-1)^{x+1} \frac{1}{\lambda x^{\frac{1}{\alpha}}} \Gamma(\frac{1}{\alpha} + 1) \\ &= \frac{1}{\lambda} \Gamma(\frac{1}{\alpha} + 1) \sum_{x=1}^{k} \binom{k}{x} (-1)^{x+1} x^{-\frac{1}{\alpha}} \qquad (7.9) \end{aligned}$$

Let $\mathrm{A}_k^{\mathrm{W}}$ denotes a multiplier for a 1oo$k$ architecture where all components have a Weibull time to failure. Hence

$$\mathrm{A}_k^{\mathrm{W}} = \left(\frac{\mu_1}{\mu_k}\right)^{\alpha} = \left[\sum_{x=1}^{k} \binom{k}{x} (-1)^{x+1} x^{-\frac{1}{\alpha}}\right]^{-\alpha} \tag{7.10}$$

As (7.10) shows, the multiplier depends only on the shape parameter (α) and the order of the architecture (k), as it should be. A table consists of the values of $\mathrm{A}_k^{\mathrm{W}}$ for some selected α's (1.0-5.0) versus the first fifteen 1oo$k$ architectures is presented in Appendix B.

Hence (7.8) can be rewritten as

$$F_k(t) = \left[\mathrm{A}_k^{\mathrm{W}} \left(F(t)\right)^{k-1}\right] F_1(t) \tag{7.11}$$

The above equation should be interpreted as the *expected* CDF of 1oo$k$ architecture as seen from 1oo1 architecture.

Let $\mathrm{PFD}_{\mathrm{avg},ki}$ be the average PFD for 1oo$k$ architecture in the t^{th} test interval. Thus, $\mathrm{PFD}_{\mathrm{avg},ki}$ is the arithmetic average of the CDF of 1oo$k$ architecture from $(i-1)\tau$ to $i\tau$. But, for the first test interval we have (for other test intervals see Section 7.4)

$$\begin{aligned}\mathrm{PFD}_{\mathrm{avg},k1} &= \left[\mathrm{A}_k^{\mathrm{W}} \left(F(\tau)\right)^{k-1}\right] \frac{1}{\tau} \int_0^{\tau} F_1(t)\mathrm{d}t \\ &= \left[\mathrm{A}_k^{\mathrm{W}} \left(F(\tau)\right)^{k-1}\right] \mathrm{PFD}_{\mathrm{avg},k1} \end{aligned} \tag{7.12}$$

Therefore, (7.12) signifies that to calculate the $\mathrm{PFD}_{\mathrm{avg}}$ for any architecture, what we all need to calculate is the $\mathrm{PFD}_{\mathrm{avg}}$ for a single component and then multiply with the constant. We can further simplify (7.12) as

$$\begin{aligned}\mathrm{PFD}_{\mathrm{avg},k1} &= \frac{\mathrm{A}_k^{\mathrm{W}}}{\tau} \left(1 - \mathrm{e}^{-(\lambda\tau)^{\alpha}}\right)^{k-1} \int_0^{\tau} 1 - \mathrm{e}^{-(\lambda t)^{\alpha}} \mathrm{d}t \\ &\approx \frac{\mathrm{A}_k^{\mathrm{W}}}{\tau} (\lambda\tau)^{\alpha(k-1)} \frac{\lambda^{\alpha}\tau^{\alpha+1}}{\alpha+1} \\ &\approx \frac{\mathrm{A}_k^{\mathrm{W}}}{\alpha+1} (\lambda\tau)^{\alpha k} \end{aligned} \tag{7.13}$$

For an architecture with n MCSs with all order k, the $\text{PFD}_{\text{avg},k1}$ is

$$\text{PFD}_{\text{avg},k1} \approx n \cdot \frac{\text{A}_k^{\text{W}}}{\alpha + 1} (\lambda\tau)^{\alpha k} \tag{7.14}$$

Particularly, for $M$oo$N$ architecture the PFD_{avg} can be calculated as

$$\text{PFD}_{\text{avg},k1} \approx \binom{N}{N-M+1} \cdot \frac{\text{A}_k^{\text{W}}}{\alpha + 1} (\lambda\tau)^{\alpha k} \tag{7.15}$$

Where $k = M - N + 1$

7.3.1 Comparison with Rausand's Method

If $\alpha = 1$, we get exponential distribution with parameter λ and thus the multiplier (A_k^{W}) reduces to

$$\text{A}_k^{\text{E}} = \left[\sum_{x=1}^{k} \binom{k}{x} \frac{(-1)^{x+1}}{x} \right]^{-1} \tag{7.16}$$

where E stands for exponential distribution, and (7.15) reduces to

$$\text{PFD}_{\text{avg},k1} = \binom{N}{N-M+1} \frac{\text{A}_k^{\text{E}}}{2} (\lambda\tau)^{k} \tag{7.17}$$

Remember that Rausand method is given by (see Section 4.2):

$$\text{PFD}_{\text{avg},k1} = \binom{N}{M-N+1} \frac{(\lambda\tau)^{k}}{k+1} \tag{7.18}$$

Table 7.1 shows the $\text{PFD}_{\text{avg},\cdot 1}$ for some typical architecture based on the two methods. Rausand's formulas are differentiated by bracket below each proposed formula. The second row is the multiplier for the first five 1oo$k$ architectures (see the second raw in the A_k^{W} table in Appendix B). As can be seen from the table that the proposed method is almost exactly identical with Rausand method. If we have to compare, however, the proposed method gives a slightly conservative result than Rausand's method.

Table 7.1: PFD$_{\text{avg}}$ for some $M$oo$N$ architectures when $\alpha = 1$; elements in bracket are based on Rausand's method

M \ N	1	2	3	4	5
(A_k^E)	1	$\frac{2}{3}$	$\frac{6}{11}$	$\frac{12}{25}$	$\frac{60}{137}$
1	$\frac{\lambda\tau}{2}$	$\frac{(\lambda\tau)^2}{3}$	$\frac{3(\lambda\tau)^3}{11}$	$\frac{6(\lambda\tau)^4}{25}$	$\frac{30(\lambda\tau)^5}{137}$
	$\left(\frac{\lambda\tau}{2}\right)$	$\left(\frac{(\lambda\tau)^2}{3}\right)$	$\left(\frac{(\lambda\tau)^3}{4}\right)$	$\left(\frac{(\lambda\tau)^4}{4}\right)$	$\left(\frac{(\lambda\tau)^5}{6}\right)$
2	-	$\lambda\tau$	$(\lambda\tau)^2$	$\frac{12(\lambda\tau)^3}{11}$	$\frac{6(\lambda\tau)^4}{5}$
	-	$(\lambda\tau)$	$\left((\lambda\tau)^2\right)$	$\left((\lambda\tau)^3\right)$	$\left((\lambda\tau)^4\right)$
3	-	-	$\frac{3\lambda\tau}{2}$	$2(\lambda\tau)^2$	$\frac{30(\lambda\tau)^3}{11}$
	-	-	$\frac{3\lambda\tau}{2}$	$2(\lambda\tau)^2$	$\frac{10(\lambda\tau)^3}{4}$
4	-	-	-	$2\lambda\tau$	$\frac{10(\lambda\tau)^2}{3}$
	-	-	-	$(2\lambda\tau)$	$\left(\frac{10(\lambda\tau)^2}{3}\right)$
5	-	-	-	-	$\frac{5\lambda\tau}{2}$
	-	-	-	-	$\left(\frac{5\lambda\tau}{2}\right)$

7.3.2 Empirical Conformation of the Proposed Method

We shall now see numerically whether or not the proposed method is valid, especially when $\alpha \neq 1$. Comparing the results that we get from the proposed method with the *exact* values carries out the validation. We have done for 1oo2, 1oo3 and 1oo4 architectures by using some typical parameters and test intervals (Table 2 & 3).

The exact PFD$_{\text{avg},\cdot 1}$ values for these architectures are calculated, respectively, based on the following formulas:

$$\text{PFD}_{\text{avg},21} = 1 - \frac{1}{\tau}\int_0^\tau 2\mathrm{e}^{-(\lambda t)^\alpha} - \mathrm{e}^{-(2\lambda t)^\alpha}\mathrm{d}t \tag{7.19}$$

$$\text{PFD}_{\text{avg},31} = 1 - \frac{1}{\tau}\int_0^\tau 3\mathrm{e}^{-(\lambda t)^\alpha} - 3\mathrm{e}^{-2(\lambda t)^\alpha} + \mathrm{e}^{-3(\lambda t)^\alpha}\mathrm{d}t \tag{7.20}$$

$$\text{PFD}_{\text{avg},41} = 1 - \frac{1}{\tau}\int_0^\tau 4\mathrm{e}^{-(\lambda t)^\alpha} - 6\mathrm{e}^{-2(\lambda t)^\alpha} + 4\mathrm{e}^{-3(\lambda t)^\alpha} - \mathrm{e}^{-4(\lambda t)^\alpha}\mathrm{d}t \tag{7.21}$$

The last column in the table shows the percentage change in the proposed method with respect to (wrt) the exact, for example, 100% means that the proposed method is twice as large as the exact value. As can be seen from the tables, it is evident that the proposed method is almost exact by itself.

Table 7.2: $\text{PFD}_{\text{avg},21}$ under Weibull distribution

Specification				methods		Proposed wrt Exact in %
Architecture	τ	β	α	Exact	Proposed	
1oo2	4380	5.0E-06	0.1	2.140E-01	2.130E-01	-0.448
			0.5	9.742E-03	9.711E-03	-0.316
			1	1.577E-04	1.569E-04	-0.182
			1.5	2.619E-06	2.613E-06	-0.253
			2.5	8.395E-10	8.369E-10	-0.307
		2.5E-05	0.1	2.680E-01	2.660E-01	-0.792
			0.5	4.233E-02	4.163E-02	-1.648
			1	3.684E-03	3.651E-03	-0.907
			1.5	3.197E-04	3.180E-04	-0.533
			2.5	2.616E-06	2.607E-06	-0.343
	8760	5.0E-06	0.1	2360E-01	2.340E-01	-0.590
			0.5	1.858E-02	1.844E-02	-0.767
			1	6.189E-04	6.166E-04	-0.364
			1.5	2.087E-05	2.080E-05	-0.303
			2.5	2.685E-08	2.677E-08	-0.313
		2.5E-05	0.1	2.930E-01	2.910E-01	-0.954
			0.5	7.642E-02	7.442E-02	-2.619
			1	1.361E-02	1.336E-02	-1.803
			1.5	2.439E-03	2.412E-03	-1.093
			2.5	8.264E-5	8.222E-05	-0.500

7.4 Forecasting the $\text{PFD}_{\text{avg},ki}$

With exponential distribution, since the failure rate is constant with respect to time, the PFD_{avg} of the first test interval serves as a long-run PFD_{avg}. But, with the proposed method (when $\alpha \neq 1$), we are able to calculate only a time dependent PFD_{avg} for a particular test interval. We understand that this method cannot easily be welcomed by practitioners since it requires an update in each test interval for each SIF, and also whenever any change/modification is carried

Table 7.3: $\text{PFD}_{\text{avg},31}$ and $\text{PFD}_{\text{avg},41}$ under Weibull distribution

Specification				methods		Proposed wrt Exact in %
Architecture	τ	β	α	Exact	Proposed	
1oo3	4380	5.0E-06	0.1	9.956E-02	1.011E-01	1.581
			0.5	1.080E-03	1.150E-03	6.482
			1	2.558E-06	2.782E-06	8.772
			1.5	6.165E-09	6.757E-09	9.593
			2.5	≈ 0	≈ 0	-
		2.5E-05	0.1	1.394E-01	1.407E-01	0.915
			0.5	9.700E-03	1.009E-02	4.097
			1	2.882E-04	3.098E-04	7.507
			1.5	8.289E-06	9.044E-06	9.109
			2.5	7.314E-09	8.069E-09	10.324
	8760	5.0E-06	0.1	1.154E-01	1.168E-01	1.303
			0.5	2.836E-03	2.997E-03	5.673
			1	1.994E-05	2.162E-05	8.455
			1.5	1.385E-07	1.517E-07	9.506
			2.5	7.583E-12	8.401E-12	10.778
		2.5E-05	0.1	1.601E-01	1.610E-01	0.603
			0.5	2.339E-02	2.395E-02	2.362
			1	2.029E-03	2.151E-03	5.944
			1.5	1.737E-04	1.878E-04	8.142
			2.5	1.296E-06	1.426E-06	10.054
1oo4	8760	5.0E-05	0.1	1.046E-01	1.073E-01	2.592
			0.5	2.198E-02	2.329E-02	5.997
			1	3.655E-03	4.074E-03	11.459
			1.5	6.337E-04	7.329E-04	15.678
			2.5	1.941E-05	2.317E-05	19.407
		7.5E-05	0.1	1.158E-01	1.185E-01	2.301
			0.5	3.960E-02	4.101E-02	3.564
			1	1.333E-02	1.431E-02	7.411
			1.5	4.996E-03	5.541E-03	10.908
			2.5	7.854E-04	9.107E-04	15.957
	13140	5.0E-05	0.1	1.158E-01	1.185E-01	2.301
			0.5	3.960E-02	4.101E-02	3.565
			1	1.332E-02	1.431E-02	7.417
			1.5	5.000E-03	5.541E-03	10.832
			2.5	7.839E-04	9.107E-04	16.182
		7.5E-05	0.1	1.260E-01	1.305E-01	2.001
			0.5	6.843E-02	6.892E-02	0.712
			1	4.232E-02	4.302E-02	1.648
			1.5	3.027E-02	3.111E-02	2.751
			2.5	1.885E-02	1.969E-02	4.475

out. However, we hope in the future that this would be easy when softwares are developed to do the calculations.

As far as the proposed method is concerned, there are two types of PFD_{avg} that are worth to quantify; the current and the i step ahead conditional PFD_{avg}.

7.4.1 The Current $\text{PFD}_{\text{avg},ki}$

We want to compute the average PFD for 1oo$k$ architecture in the i^{th} test interval while we are standing at time $(i-1)\tau$. It actually depends on what has been done to the architecture from time 0 to $(i-1)\tau$. If changes are done during this period, we should update the CDF accordingly. However, this report does not cover the updating mechanisms and is left for other researchers.

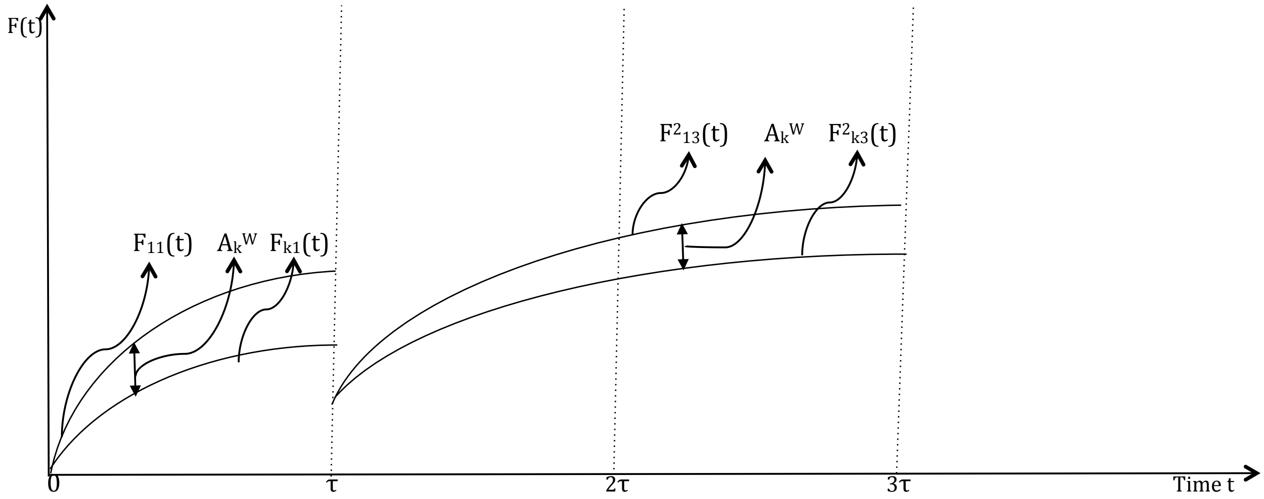

Figure 7.3: Possible propagation of CDFs over test intervals

Let $F^p_{ki}(t)$ be the CDF for 1oo$k$ architecture and is updated in the p^{th} test interval, at the latest. It should, therefore, be used to calculate the $\text{PFD}_{\text{avg},k}$ for the i^{th} test interval and denote it as $\text{PFD}^p_{\text{avg},ki}$ where $i \geq p$.

Consider a simple situation where the change is made in the first test interval and the CDF is updated accordingly in the beginning of the second test interval $(p = 2)$ as illustrated in Figure 7.3. Since the multiplier is independent of time t and the failure rate, we presume that it is independent of the change.

Suppose we are at time 2τ and want to calculate the average PFD, i.e., $\text{PFD}^2_{\text{avg},k3}$. We must thus find the probability that a component fails in the interval $(2\tau, 3\tau]$ and is equal to $F^2(3\tau) - F^2(2\tau)$. Therefore, (7.12) can be modified as follows:

$$\begin{aligned}\text{PFD}^2_{\text{avg},k3} &= \left[\text{A}^{\text{W}}_k \left(F^2(3\tau) - F^2(2\tau)\right)^{k-1}\right] \frac{1}{\tau}\int_{2\tau}^{3\tau} F^2_{13}(t)\text{d}t \\ &= \left[\text{A}^{\text{W}}_k \left(F^2(3\tau) - F^2(2\tau)\right)^{k-1}\right] \text{PFD}^2_{\text{avg},13} \qquad (7.22)\end{aligned}$$

Thus, given no change is ever made since the p^{th} test interval, the average PFD for 1oo$k$ architecture in the i^{th} test interval is

$$\begin{aligned}\text{PFD}^p_{\text{avg},ki} &= \left[\text{A}^{\text{W}}_k \left(F^p(i\tau) - F^p((i-1)\tau)\right)^{k-1}\right] \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} F^p_{1i}\text{d}t \\ &= \left[\text{A}^{\text{W}}_k \left(F^p(i\tau) - F^p((i-1)\tau)\right)^{k-1}\right] \text{PFD}^p_{\text{avg},1i} \qquad (7.23)\end{aligned}$$

To simplify the notation in (7.23), assume that whenever the CDF is updated, the test interval counter starts from 1, i.e., $p = 1$ and i starts counting from this test interval. Thus, (7.23) can be rewritten as

$$\text{PFD}_{\text{avg},ki} = \left[\text{A}^{\text{W}}_k \left(F(i\tau) - F((i-1)\tau)\right)^{k-1}\right] \text{PFD}_{\text{avg},1i} \qquad (7.24)$$

Therefore,

$$\text{PFD}_{\text{avg},ki} \approx \frac{\text{A}^{\text{W}}_k \lambda^\alpha}{(1+\alpha)\tau}\left[(i\tau)^{\alpha+1} - ((i-1)\tau)^{\alpha+1}\right]\left[(\lambda i\tau)^\alpha - (\lambda(i-1)\tau)^\alpha\right]^{k-1} \qquad (7.25)$$

Note that if we set $i = 1$ then (7.25) reduces to (7.13), and further if we set $\alpha = 1$ then we get Rausand's formula.

Note also that the simplest situation in this type of calculation is that if no change has ever been made until $(i-1)\tau$ so that the CDF established in the first test interval, i.e. $F_{11}(t)$, is used to calculate the current $\text{PFD}_{\text{avg},ki}$ (see also Figure 7.3).

7.4.2 The i Step Ahead Conditional PFD$_{\text{avg},k}$

It is also worth to calculate the PFD$_{\text{avg}}$ one or more test intervals ahead given that the system is functioning till the end of the preceding test interval. We want to answer the question: *What is the PFD$_{\text{avg}}$ for a 1oo$k$ architecture in the i^{th} test interval given that the system is survived the first* $(i-1)$ *test intervals?* Let us denote this as PFD$_{\text{avg},ki}\,(i\tau|\cdot)$. Assume that i starts counting from the latest CDF update.

The conditional survival probability for a 1oo$k$ architecture in the i^{th} test interval is

$$P_{ki}\,(T \geq t+(i-1)\tau|T \geq (i-1)\tau) = \frac{P_{ki}(T \geq t+(i-1)\tau \cap T \geq (i-1)\tau)}{P_{ki}(T \geq (i-1)\tau)} = \frac{P_{ki}(T \geq t+(i-1)\tau)}{P_{ki}(T \geq (i-1)\tau)}$$

Thus,

$$R_{ki}\,(t+(i-1)\tau|(i-1)\tau) = \frac{R_{ki}(t+(i-1)\tau)}{R_{ki}((i-1)\tau)} \tag{7.26}$$

Hence,

$$\begin{aligned}
\text{PFD}_{\text{avg},ki}\,(i\tau|\cdot) &= \text{A}_k^{\text{W}} \cdot (1-P\,(T \geq i\tau|T \geq (i-1)\tau))^{k-1} \cdot \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} (1-P_{1i}\,(T \geq t+(i-1)\tau|T \geq (i-1)\tau))\mathrm{d}t \\
&= \frac{\text{A}_k^{\text{W}}}{\tau} \cdot (1-R(i\tau|(i-1)\tau)^{k-1} \cdot \int_{(i-1)\tau}^{i\tau} (1-R_{1i}(t+(i-1)\tau|(i-1)\tau)\,\mathrm{d}t \\
&= \frac{\text{A}_k^{\text{W}}}{\tau} \cdot \left(1-\frac{R(i\tau)}{R((i-1)\tau)}\right)^{k-1} \cdot \int_{(i-1)\tau}^{i\tau} \left(1-\frac{R_{1i}(t+(i-1)\tau)}{R_{1i}((i-1)\tau)}\right)\mathrm{d}t \\
&= \text{A}_k^{\text{W}} \cdot \left(1-\frac{R(i\tau)}{R((i-1)\tau)}\right)^{k-1} \cdot \left(1-\frac{1}{\tau R_{1i}((i-1)\tau)}\int_{(i-1)\tau}^{i\tau} R_{1i}(t+(i-1)\tau)\mathrm{d}t\right) \qquad (7.27)
\end{aligned}$$

This measures the conditional long-run reliability performance of a SIS.

Chapter 8

Discussion

8.1 Introduction

No single reliability analysis method can effectively comprehend all relevant system features in a complete and flexible manner. To obtain a reasonably meaningful result it is important to consider several qualitative/quantitative as well as bottom-up/top-down approaches altogether. In this report four SIS reliability quantification approaches are discussed from Chapter 4-7, namely simplified formulas, FTA, Markov analysis and a newly proposed approach, respectively. Four simplified formulas (methods) are also discussed in Chapter 4, which are Rausand, IEC 61508, the PDS method, and a newly (another) proposed method. The methods covered in this report are shown in Figure 8.1.

Many users prefer the simplified formulas. In the Norwegian petroleum industry, the PDS method has been widely used. In this chapter, we compare the simplified formulas each other with especial emphasis on the PDS method. However, before that we shall start with the first level approaches (see Figure 8.1).

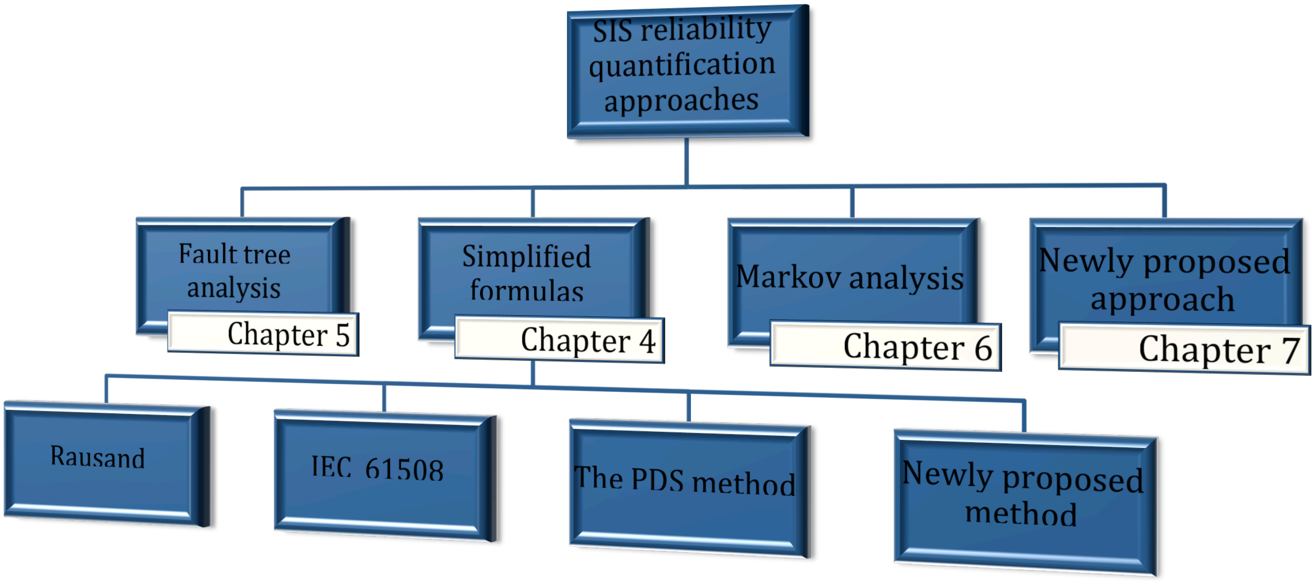

Figure 8.1: Summary of the methods covered in this report

8.2 Comparison of the Methods

It has always been a challenge to choose the right approach for a particular situation. It has been practically proven that performing the top-down and bottom-up analyses together for a particular problem is an effective approach [1]. Inevitably, FMECA is used effectively as input for more complex quantitative analysis techniques like FTA and Markov analysis [13].

Consider FMECA and FTA in the reliability quantification of SISs. The benefit is twofold: first to secure completeness, i.e., to make sure that all relevant causes are taken into account in the FTA since FMECA is a bottom-up analysis and FTA is a top-down. For example, a single failure found in the FMECA that leads to system failure should appear in the FTA as a single MCS. Secondly, FMECA enables to perform complete hazard identification at component level and some safety standards require single failure analysis [2].

As discussed in Chapter 5, FTA can be performed qualitatively and quantitatively. Moreover, since we think in terms of failure while we are establishing a fault tree, we get a better understanding of all potential causes of failure [16, 20]. It is thus an important method, in addition to quantifying the PFDavg, to suggest proactive actions to be performed in eliminating the causes at source by design modification or some other techniques. Therefore, in SIS reliability quantification process FTA, especially in combination with FMECA, is always a good start.

Moreover, all other approaches, i.e., simplified formulas [4], Markov analysis [3] and the proposed approach require RBD to be established beforehand. Fault tree and RBD are transposable but as argued above and in [20] RBD should be derived from fault tree – not in other way around.

The obvious limitations of FTA, nonetheless, as described in IEC 60300 [1], are

- It is not able to represent time or sequence dependency of events correctly.
- It has limitations with respect to architecture or state dependent behavior of the system.

With FTA we can only represent the instantaneous behavior of a system. Therefore, complex system behavior and maintenance strategies cannot be modeled. This problem is often overcome by Markov analysis either fully or as a hybrid of the two. A simple example of a hybrid of FTA and Markov analysis is illustrated in Figure 8.2.

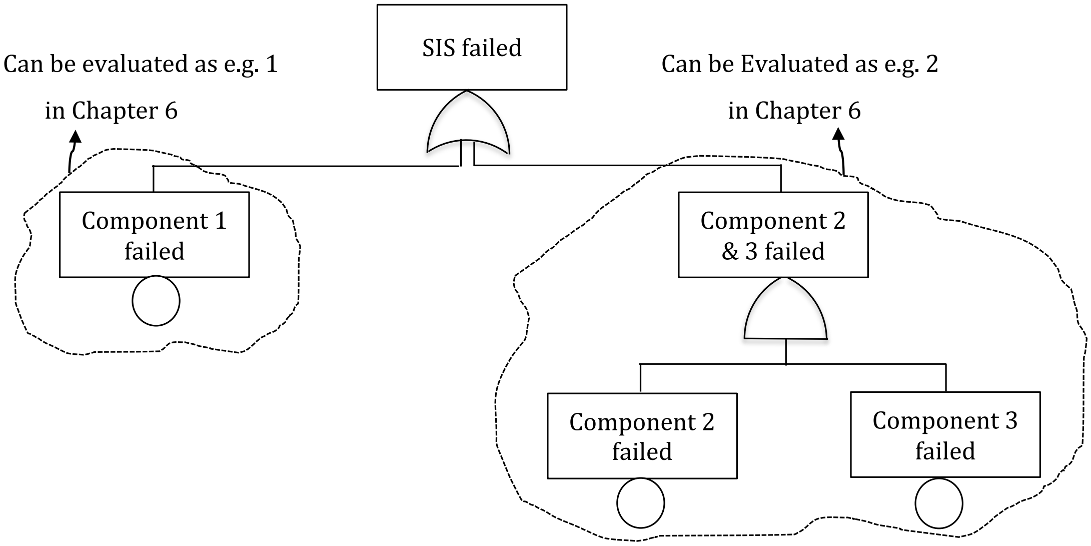

Figure 8.2: A simple hybrid model of FTA and Markov analysis

The system fails if either component 1 fails or component 2 *and* 3 fail. These two MCSs (1oo1 and 1oo2) can be evaluated by Markov analysis as example 1 and 2 presented in Chapter 6, respectively. Then, the average probability that the SIS fails is evaluated by using the upper bound approximation formula. Note that the part of fault tree that is analyzed by Markov analysis is considered as a basic event in the FTA.

Therefore, if FTA is not a sufficient method for a particular SIS, based on the complexity of the system and its operational characteristics, we look for Markov analysis or simplified formulas, or a combination of both.

The IEC 61508 simplified formulas can be seen as a simplified version of Markov analysis and an extension of quantitative FTA. The average system failure rate and equivalent mean down times are the inputs used to derive the IEC 61508 formulas, and equivalent mean down times in turn can be derived by Markov analysis [12, 24]. All other simplified formulas are also considered as the extension of the quantitative FTA because with the simplified formula we can take into account both DU and DD failures. But, due to the assumption of independency between basic events we cannot model DU and DD failures directly in the fault tree.

All the approach discussed so far are based on the assumption of constant failure rate. The newly introduced approach is based on Weibull distribution and the aim is to relax the restrictive assumption of constant failure rate.

8.3 Simplified Formulas

8.3.1 Introduction

In this section, we discuss how the simplified formulas can be applied in real life situations. To be able to choose one against the others, it is important to understand the major differences among them. The primary difference among the first three methods is the extent to which factors that affect the unavailability of SIF are included. Rausand's method is the least detailed and the PDS method is the most. The new method is, however, closely related to IEC 61508. The only difference is the manner in which DD and DU failures are treated.

Attempt is made to evaluate critically the PDS method as a method and also by comparing it with other methods. We finally conclude the section by establishing a procedure to choose the nearest possible method based on the operational characteristics of the system under consideration.

8.3.2 Brief Comments on the PDS Method

Is it Worth/Practical to Model Systematic Failures?

1. According to IEC 61508 [4] and ISA [6], the major distinguishing feature between random hardware failures and systematic failures is that system failure rates arising from random hardware failures can be predicted with reasonable accuracy *but* systematic failures, by their very nature, cannot be accurately predicted. The reason for this is that the events that lead to systematic failures do not occur randomly.

   Randomness is the key assumption in probability distributions. That is, probability distributions, including exponential, are practical only for *random* variables (stochastic variables). Therefore, modeling of systematic failures is not a question of data availability or choice of appropriate statistical model, it is rather the *deterministic nature* of the events leading to these type of failure. It is not justified in the PDS method that with what statistical ground that these two different failures are combined just like (4.34) and used exponential distribution afterwards. Does randomness assumed to systematic failures? If so, how far is this assumption valid?

   It seems that the PDS method is likely to high uncertainty due to the non-randomness effect of systematic failures since they are modeled implicitly with DU random hardware failures. *No limit or caution is also stated in the handbook to remind the users if the inclusion in case causes some modeling problem.*

   However, unlike the PDS method, in ISA an explicit way of modeling systematic failures is suggested. Accordingly, if data for systematic failures is available, it can be treated, with special care, as DU failures. The average PFD is thus the sum of average PFDs due to independent failures, CCFs, during repair action and systematic failures. Mathematically

$$\text{PFD}_{\text{avg}} = \text{PFD}_{\text{avg-ind}} + \text{PFD}_{\text{avg-CCF}} + \text{PFD}_{\text{avg-repair}} + \text{PFD}_{\text{avg-sys}} \tag{8.1}$$

Where $\text{PFD}_{\text{avg-sys}} = \lambda_{\text{D}-\text{sys}} \cdot \tau/2$ regardless of the type of architecture, as $\text{PFD}_{\text{avg-CCF}}$, which is equal to $\beta \cdot \lambda_{\text{DU}} \cdot \tau/2$, and $\lambda_{\text{D}-\text{sys}}$ is dangerous systematic failure rate.

Remark: Some systematic failures do not manifest themselves randomly, but exist since the first time the system is installed (e.g., installation failure). Therefore, the expected down time will be τ, and then $\text{PFD}_{avg-sys} = \lambda_{\text{D}-\text{sys}} \cdot \tau$ [6].

In situations where treating $\text{PFD}_{\text{avg-sys}}$ at subsystem level is inappropriate, ISA suggested to incorporate the contribution at system level. That is

$$\text{PFD}_{\text{avg-SYS}} = \text{PFD}_{\text{avg-S}} + \text{PFD}_{\text{avg-LS}} + \text{PFD}_{\text{avg-FE}} + \text{PFD}_{\text{avg-sys}} \tag{8.2}$$

where the first three terms are the average PFDs for the sensor, logic solver and final element respectively.

It is repeatedly mentioned in the standard that systematic failures are hard to model statistically with reasonable accuracy. Therefore, rather strict qualitative measures are established to reduce their effect sufficiently to a tolerable level. These qualitative measures are developed by the system integrator and made available to the system operator in a manual form.

2. Even if we assume that randomness assumption is satisfied and then modeled according to the PDS method, it gives unnecessary confidence for decision makers. One of the arguments in the PDS method for the inclusion of systematic failures is that they are often dominant contributors towards the overall failure probability. If we quantify them in this

manner, the attention towards qualitative measures set out in IEC 61508 would eventually be dropped.

3. Furthermore, since it is the nature of systematic failures to cause redundant components simultaneously, their effect is partly taken care of by CCF [4, 23]. This shows that dependent failures (CCF) are overly modeled. Surprisingly, we quantify them three times:
   (a) as CCF (partly),
   (b) as systematic failures and
   (c) when we combine average PFDs of the MCSs that are due independent failures

How Significant is 2b)?

It is explicitly mentioned in the standard that the required time to detect and repair DD failures is MTTR. However, how to deal with the required time to detect DU failures (function testing) is not explicitly mentioned. To use IEC 61508 formulas we need to assume that the required time for function testing is negligible. If the operational philosophy is to test all components at the same time, its contribution to the safety unavailability is simply t/τ, regardless of the type of architecture, where t is the required time for testing. This is more or less the worst contribution, in comparison with other operational philosophies, that we may encounter since λ_{DU} is almost always by far less than $1/\tau$ (see DTU_{T} formulas in the PDS method handbook [23]). Consider the following example.

Example: Consider 1oo1, 1oo2 and 2oo3 architectures with $t = 5$ hours, $\tau = 8760$ hours and λ_{DU}= 5.0E-6. If we are testing all components at a time the contribution will be 5· 1.14E-4=5.70E-4. But, if the philosophy is to test one component at a time, the contributions are approximately $t \cdot \lambda_{\text{DU}}$=2.5E-5 and $t \cdot 2\lambda_{\text{DU}}$=5.0E-5, respectively, for 1oo2 and 2oo3 architectures. The most significant contributor for 1oo1 architectures is $\lambda_{\text{DU}}\tau/2 = 2.2\text{E-}2$ and for 1oo2 and 2oo3 it is $\beta\lambda_{\text{DU}}\tau/2 = 1.1\text{E-}3$ (according to the PDS formula for 2oo3 it is $\text{C}_{2oo3}\beta\lambda_{\text{DU}}\tau/2 = 2.2\text{E-}3$).

As can be seen from the above example, with philosophies other than testing all channels at a time, the contribution of DTU_{T} is almost always negligible that can be neglected. Thus, this cannot be a sufficient reason to deviate from IEC 61508 formulas since t/τ can simply be added on it.

Therefore, the following conclusions are drawn:

- If the philosophy is to test all channels at the same time and t/τ is significant, it is evident that it should be added to any PFD_{avg} formula (e.g., IEC 61508 or Rausand's formulas) since the associated down time is independent of any contributor (or simply independent of the failure rates).
- If the philosophy is to test one at a time (or while some other channels are operating), the contribution is always insignificant. For example, for 1oo2 architecture it is easy to see the order of magnitude difference between $\beta\tau/2$ and t. The former is at least two orders of magnitude higher than the second. Therefore, formulas to quantify this have no worth than making the formulas complicated.

Imperfect Testing

It is always important to have a clear idea about the extent to which function testing is perfect. Although it is not practical in most cases to assume all hidden failures are detected during function testing, most formulas persist working under this assumption. Thus, the PDS method has been devoted to find a mathematical relation to quantify the contribution of failures which remains undetected after function testing.

To get more realistic prediction we must also ask ourselves another obvious question in relation to the reliability of a SIS in the next term after function testing is performed. Suppose τ =1 year and we are able to manage to have 100% coverage to uncover all hidden failures. The question is then: Is it realistic to believe that the SIS is *as good as new* in the coming year? In one of the suggested methods, i.e. incorporating the FTC into the already computed PFD_{avg}, we get a time dependent PFD. Thus, our comment in this regard is that if we are willing to deal with time dependent PFD_{avg}, FTC is not the only one which is responsible for that, we should also look at how far constant failure rate assumption is valid. Obviously, it is not a valid assumption in most situations since a component that has been used for one or two years is *hardly* possible to be as good as new.

Conditionality

Like the PFD_{avg} is conditional on FTC, it is also conditional on DTU due to repair of DD failures. Despite the fact, this conditionality has never been stated or used in any PFD_{avg} calculation where DD and DU failures are treated separately, for example in [6, 19, 23]. The conditionality is obvious because if DD failures occur, a repair or replace action initiates immediately to restore it in an *as good as new* state so that the contribution of DU failures should be reduced accordingly. We cannot simply add two events where one is conditional on the other.

In IEC 61508 this conditionality is treated in a systematic manner. The equivalent mean down times balance the unavailability of safety due to DU and DD failures according to their rates, i.e., if DD failures are likely the contribution from DU failures decreases (see equations for MDTs in section 4.3.3).

We believe that a correct mathematical approach should be employed to combine the contributions from DU and DD failures or if it is believed that its impact is small, an assumption should be made. Accordingly, in this paper a new approach is introduced and is presented in Section 4.5.

8.3.3 Pairwise Comparison

The PDS Method Versus Rausand Method

The PDS method uses the main principle advocated in Rausand's method but four more factors (factors other than DU failures) and multiple beta factor model are introduced. It is a more conservative method than the Rausand's method since in the PDS method

1. contribution from systematic failures is implicitly incorporated in the DU failures,

2. contribution during repair of dangerous failures is added (DTU_{R}),

3. contribution during function testing is added ($\mathrm{DTU_T}$),
4. contribution from imperfect testing is added, and
5. multiple beta factor model is used against standard beta factor model

Both methods are in line with IEC 61508 under the respective assumptions. In real life situation the choice depends on whether the above five points have significant impact or not

The PDS Method and IEC 61508

The most significant differences between these two methods are the following:

- Unlike the PDS method, IEC 61508 formulas incorporate only DU and DD failures, and a standard beta factor model is employed. The standard, however, suggests point 4 and 5 above to be treated with appropriate formulas.
- Two methods are suggested in the PDS method to handle point 4, and one of them, i.e. using FTC, is recommended in the standard.
- Although it is suggested in the standard to consider the type of architecture while using beta factor model, it is not far from presenting the associated correction factors in a table (Table D.5 of IEC 61508-6). However, in the PDS method a relatively detailed discussion and formulas are developed. A slightly different results from IEC 61508 are also gained.
- In the standard no explicit statement or formula is established for point 3 but it is intuitive, as long as its effect is significant, that the associated down time should be considered. In the PDS handbook due emphasis is given to quantify the effect and formulas are developed.
- Systematic failures are hard to quantify statistically and that is repeatedly mentioned in the standard. But in the PDS method they are quantified in such a way that DU systematic failure rate and DU hardware failure rate are combined together and Rausand's formula is then used.

- The developments of formulas in these approaches are quite different thought they give almost identical results (see also IEC 61508 vs. Rausand's method below). In the PDS method the probabilities for factors are quantified explicitly whereas in the standard they are treated implicitly through the so-called equivalent mean down time. Moreover, in the standard the repair time due to DU failure (MRT) and DD failure (MTTR) are differentiated. But, in the PDS method only MTTR is used to measure a *planned down time* due to both DU and DD failure.

- Unlike IEC 61508, in the PDS method relevant operational philosophies during test and repair are considered, and formulas are developed accordingly. In IEC 61508, it is assumed that all channels have a single MRT, and it is perhaps the worst scenario among other operational philosophies.

- In IEC 61508 a clear approach of incorporating CCF related to DD failures is provided and the factor is designated as β_{D}. But, the PDS method does not distinguish these types of CCFs and thus lets the users to use *the most applicable* β.

IEC 61508 Versus Rausand's Method

The differences between Rausand's method and IEC 61508 formulas are just two:

- In IEC 61508, DD failures are considered whilst in Rausand's method it is assumed that the system is functioning as long as DU failures do not not occurred, and

- In IEC 61508, the time to repair due to DU failures (MRT) is considered whilst in Rausand's method it is assumed to be negligible

Under the above two assumptions favorable to Rausand's method, if we reduce IEC 61508 formula, the equivalent mean down times will get the following forms:

$$t_{\mathrm{CE}} = \frac{\tau}{2}, \;\; t_{\mathrm{GE}} = \frac{\tau}{3}, \;\; t_{\mathrm{G2E}} = \frac{\tau}{4} \;\text{ and }\; t_{\mathrm{G}j\mathrm{E}} = \frac{\tau}{j+1} \;\text{ for } j > 2$$

The IEC 61508 formula (4.32) will then be reduce to

$$\mathrm{PFD_{avg}} = \frac{n!}{(k-1)!(n-k+2)!}\left((1-\beta)\lambda_{\mathrm{DU}}\tau\right)^{n-k+1} + \frac{\beta\lambda_{\mathrm{DU}}\tau}{2} \tag{8.3}$$

and if k=n

$$\mathrm{PFD_{avg}} = \frac{n\lambda_{\mathrm{DU}}\tau}{2} \tag{8.4}$$

Remember that Rausand's method for $k$oo$n$ architecture, where $k \leq n$, can be rewritten as

$$\begin{aligned} \mathrm{PFD_{avg}} &= \frac{n!}{(k-1)!(n-k+1)!}\frac{((1-\beta)\lambda_{\mathrm{DU}}\tau)^{n-k+1}}{n-k+2} + \frac{\beta\lambda_{\mathrm{DU}}\tau}{2} \\ &= \frac{n!}{(k-1)!(n-k+2)!}(1-\beta)\lambda_{\mathrm{DU}}\tau)^{n-k+1} + \frac{\beta\lambda_{\mathrm{DU}}\tau}{2} \end{aligned} \tag{8.5}$$

As can be seen above, both methods are *absolutely* the same although they are developed based on different concepts. As we have seen in section 4.2, Rausand's formula is developed in such a way that failure distribution of an architecture is computed, as such, and then averaged over the test interval whereas IEC 61508 formulas are developed based on the concept that the $\mathrm{PFD_{avg}}$ is the product of average system failure rate and equivalent mean down time. Since we already have confirmed that Rausand's method is in line with IEC 61508, under the conditions mentioned above, we recommend the users to apply this formula — as it is easy to manipulate.

Note that we can extend Rausand's formula by including the contributions from MRT and MTTR as we did in section 4.5.

8.3.4 Procedure for Method Identification

We are concerned in this section to develop a simple procedure while choosing an appropriate method based on specific operational characteristics of the SIS under consideration.

It should be noted that the procedure set out here does not take into account modeling of CCF and systematic failures. Modeling of CCF is out side the scope of this report so that no assessment is done to see the appropriateness of the multiple beta factor model against the standard or any other possible models. Moreover, no sufficient reason is mentioned either in the PDS method or IEC 61508 why we use multiple beta factor model against the standard. We are therefore *neutral* when it comes to CCF modeling to choose an appropriate method.

We believe that implicit modeling of systematic failures may lead to high uncertainty as we have discussed in section 4.2.2. Thus, in this section in the PDS method λ_{DU} measures only dangerous hardware undetected failure rate.

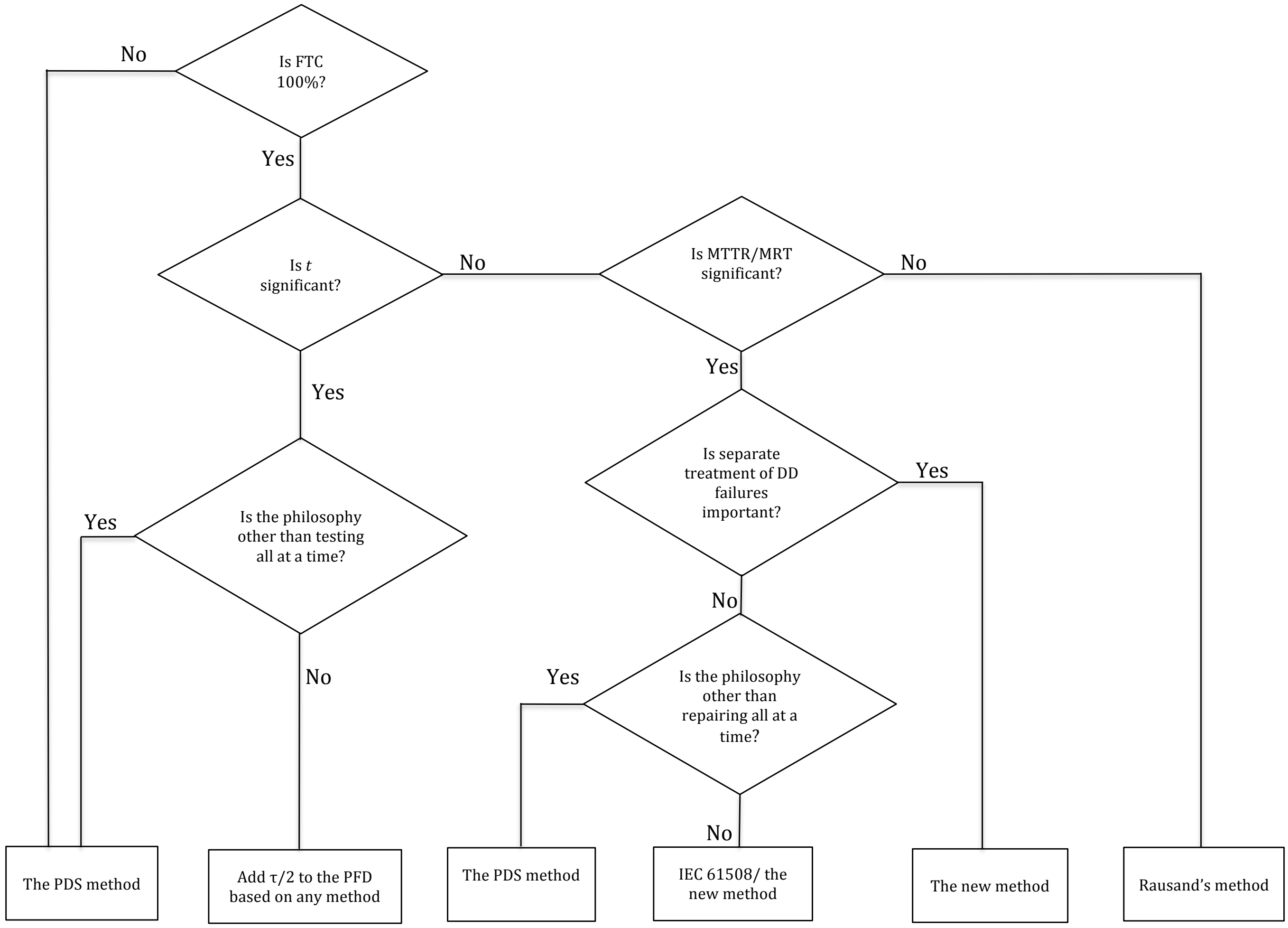
Is FTC 100%?
No
Yes
Is *t* significant?
No
Is MTTR/MRT significant?
No
Yes
Yes
Is separate treatment of DD failures important?
Yes
Yes
Is the philosophy other than testing all at a time?
No
No
Yes
Is the philosophy other than repairing all at a time?
No
The PDS method
Add τ/2 to the PFD based on any method
The PDS method
IEC 61508/ the new method
The new method
Rausand's method

Figure 8.3: Flowchart for the decision to choose the nearest possible method

.

If there is, however, a strong reason to quantify systematic failures and data is available, we recommend the users to calculate the associated mean down time carefully by taking the potential causes into account. The appropriate choice for most systematic failures may be τ rather than $\tau/2$. There should also be a clear idea whether or not it is a shared cause for several channels in parallel. If so, we must treat this probability as we treat the probability of CCF. It is also our recommendation that the users should consult at least IEC 61508[4], IEC 61511[5], PDS[23], ISA[6] and OLF[19] handbooks for the better understanding and modeling of such failures.

The flowchart in Figure 8.3 is constructed to suggest the easiest (nearest) method based on the factors that we want to include or believe that they have significant affect on the unavailability of the system. It should be noted however that the identified method is not the only best method. For example, the figure directs to the PDS method if the function testing coverage (FTC) is not perfect. It is true that SIF unavailability due to this failure is treated only in the PDS method but one can use one of the other methods and then incorporate the contribution with some appropriate techniques.

As it has been mentioned above, Rausand's method is the least detailed and easiest method so that if we have the characteristics of a system that let the figure to direct to this method, we should make use of this method otherwise utilizing other models is waste of time and resource. This situation happens if the following three conditions are fulfilled altogether (see also the figure):

- the function testing coverage is 100%,
- the time required to detect and restore DD failures (MTTR) is negligible or the system goes into safe state upon DD failures, and
- either
  - the required time for testing is negligible
  - the test in all channels performs at the same time, or
  - the process is shut down during function testing

The new method and IEC 61508 use the same parameters. If there are situations where the probability of DU and DD failures are required to be quantified separately or are already quantified by some other methods, the new method is useful to combine them with sound mathematical reasoning.

A numerical analysis based on these four methods is performed using some typical architectures such as 1oo1, 1oo2, 1oo3 and 2oo3. We compared numerically how these three methods deviate from IEC 61508[1], and the results are shown in Appendix C. In all computations we used MTTR=MRT=8 hours. Multiple beta factor model is employed in case of the PDS method (but no CCF related to DD failures) whilst standard beta factor model is used for the rest three methods. In Rausand's method we used only DU failures and ignored the contribution from DD failures.

The purpose of this numerical analysis is not to conclude that methods that deviate from IEC 61508 are wrong or less important. It is rather to provide information on how big the differences will be for some selected architectures and parameters. Accordingly, Rausand's formula is not that far from IEC 61508 even for architectures with 90% diagnostic test, but remember that restoration period is just 8 hours. Thus, it is evident that for architectures with relatively small restoration time, Rausand's formula is good enough. Although we employed multiple beta factor model in the PDS method, the results (in many cases) are not far from IEC 61508. As can be seen from the last columns, the new method more or less systematically increases over diagnostic coverage. This means that it is highly sensitive to the changes from DD failures, unlike the PDS method.

[1] Note that in the last three columns, for example 100% means that the PFD_{avg} based on that method is two times higher /lower than the PFD_{avg} based on IEC 61508, depending on the sign.

Chapter 9

Case Study

9.1 Introduction

A SIS has been widely used in the oil and gas industry to achieve a certain safety level for a specific hazard. Such a system is installed to act upon a process demand so that its escalation can be stopped before it develops into an uncontrollable situation. Since they are used to protect people, environment and assets against unwanted events, their reliability is important. That is, if a SIS is unable to act upon a demand, the associated fatalities, environmental damages and material costs may be significant.

There are several standards and guidelines that deal with the qualitative and quantitative requirements of a SIS to achieve satisfactorily the desired functional safety, but IEC 61508 and IEC 61511 are the prominent ones. This report assessed several methods to measure the quantitative requirement of a SIS, namely the PFD_{avg}, with special focus on the IEC 61508 formulas.

In this chapter a case study from Aker Solutions AS is carried out. The objective is twofold: first to see how the methods discussed in this report can be applied for compliance, and second to give some suggestions that whether or not the SIF fulfills the quantitative requirement, keeping other qualitative and semi-quantitative requirements constant.

The SIF considered here is a process shutdown (PSD) function intended to protect a subsea compressor against liquid inflow. As can be seen from Figure 9.1 that when an excess liquid level in the separator is detected by either of the two level transmitters, the SIF is required to stop the compressor and at the same time to close the two inlet valves to the separator. The SIL requirement for this function is SIL 2, i.e., $\text{PFD}_{\text{avg}} \le 0.01$. It should be noted that for the sake of confidentiality the system is slightly changed and anonymized, and the data used in the analysis are the generic ones — not project specific.

As discussed in Chapter 8, among the methods, FTA is an appropriate method to start with since it helps to visualize, understand and communicate the system. We therefore start with FTA to analyze the reliability of the SIF.

9.2 Fault Tree Analysis

This section is a continuation of chapter 5. The assumptions listed in Section 5.1.2 govern the validity of the result gained from this method. The last assumption may not be realistic since the system does not shut down the process upon DD failures and also the MTTR is relatively long as most components are located subsea. For this system, therefore, SIL compliance based on this method may not be adequate.

9.2.1 SIF Familiarization

Figure 9.1 shows a simplified schematic diagram of the SIF under consideration. The figure is prepared based on the drawings and descriptions of the actual SIF that is made available by the company as well as through thorough discussion with engineers. It should be noted that the actual SIF is by far more complex than the one shown here. In here, only components that are thought to have significant effect on the reliability quantification of the SIF are included. Other components either have nothing to do with the PFD_{avg} (e.g., compressor downstream valve and pump downstream valve) or have negligible contribution to the PFD_{avg} (e.g., communication items like jumpers, junction boxes, switches, modems and so on). Therefore, in the figure such valves are not connected to SEMs. However, it should be noted that in practice it might be reasonable to close them upon a demand since the process is supposed to be closed. For brevity

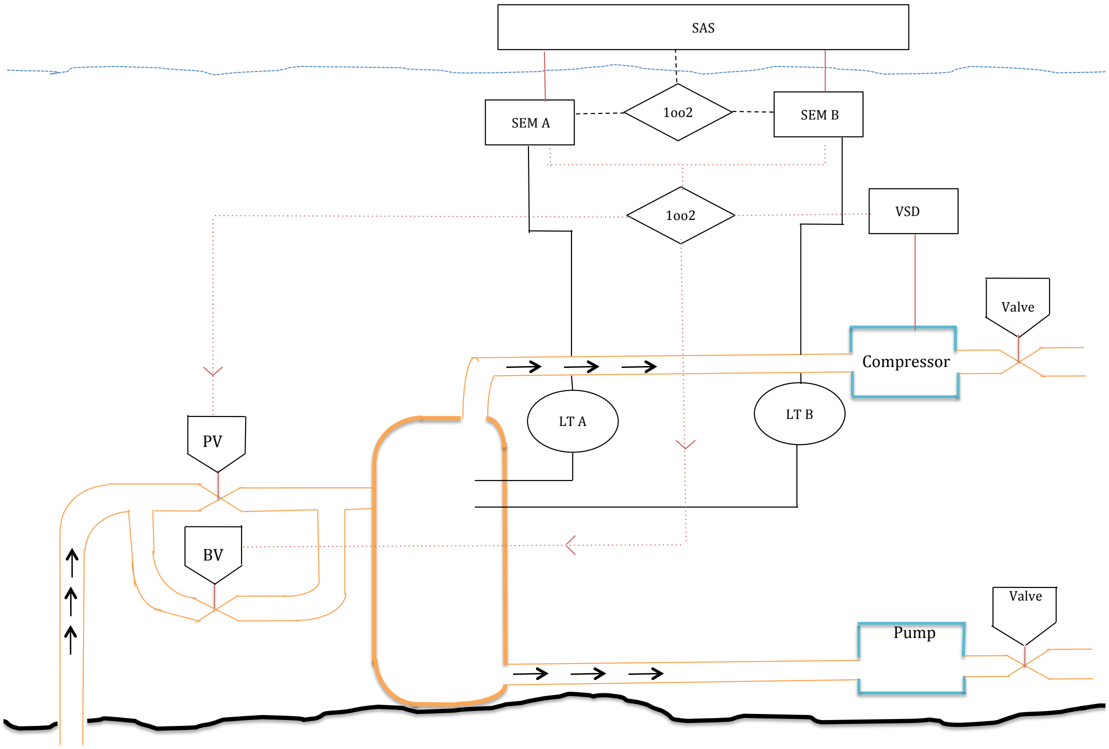

Figure 9.1: Simplified schematic representation of the PSD function

communication items are not shown at all. Notice also that all items, except the SAS are located subsea.

The unwanted event *liquid enters into the compressor* may occur only if the level is increased beyond the specified limit, and that could happen as a consequence of two different causes. The first is due to failure from the Process Control System (PCS). The PCS regulates the amount of liquid in the separator based on the readings from level transmitters. The level is maintained by speeding up the pump upon high level readings. The second cause is due to the pump, OR its downstream valve spurious tripping, OR any blockage of this outlet. If one of these causes occurs, the level increases to/beyond the specified level and then the SIF is supposed to act at a reasonable speed.

We have two inlet valves: the Primary valve and the Bypass valve. In normal operation, the bypass valve is closed and the production proceeds while the primary valve (only) is opened.

It might be reasonable not to include the bypass valve in the PFD$_{\text{avg}}$ calculation since it is already closed. However, there are situation where this valve may erroneously be kept open by the operator or due to some other reasons. We, therefore, consider a conservative avenue such that the two valves are treated as if both are functioning during normal operation. This means that the PFD$_{\text{avg}}$ we get from this calculation will obviously be larger than the PFD$_{\text{avg}}$ that can be calculated with a single inlet valve. For the calculation, we assume that the probability that the bypass valve is erroneously opened at any time t is 0.5, and thus its failure rate is half of the failure rate of the primary valve.

To summarize how the SIF is designed, there are two level transmitters from which signal transmits through the respective SEM to the topside logic (SAS), which is the master PSD controller. After the logic a signal transmit back to SEMs. The received signals in the SEMs will then be forwarded to the valves (to stop inflow to the separator) and the VSD to open the relay (de-energize) so that the compressor will stop.

Items included in the analysis are described as follows:

Level Transmitter (LT): is used to measure the level (liquid-gas interface) in the separator. If the level reaches at the specified high level, a signal goes to the respective SEM. There are two redundant level transmitters that are connected in series to their own SEMs.

SEM A/B: is a subsea electronic module that contains several components. The failure of one of these components leads the SEM to fail so that its failure rate is the result of the combination of all the failure rates of these components.

SAS: is the topside master process shutdown (PSD) controller and all actions are thus initiated from here. It is a 1oo2 logic and if demand occurs the action initiation message will normally go through SEMs.

Separator Inlet Valve (PV/BV): is a fail-safe valve to stop inflow to the separator upon demand. In normal operation, the primary valve is open and the bypass is closed.

VSD: contain a fail-safe relay used to stop the compressor upon demand.

9.2.2 Definition of the Top event

It is an interesting discussion that whether the two final elements should be designed in series, parallel or stopping the compressor only is sufficient. If we connect them in series, it means that two actions that are stoppage of the compressor and closure of the inlet valves to the separator need to take place simultaneously to achieve a safe state upon demand. The question here is, do we necessarily need both actions at the same time?

Since our aim is to protect the compressor, stopping the compressor (only) can be a sufficient action. If we secure this, it does not matter actually whether or not the inlet valves are closed because the pressure in the separator is always higher than the upstream pressure, and that eventually leads the liquid flow to achieve a steady state.

What will happen to the compressor if the SIF manage to close the inlet valves but not to stop the compressor? In this case, the safe state depends mainly on three inter-related conditions: the upcoming liquid pressure (speed), the distance between the separator and the inlet valves, and the distance between the level at which the alarm rises and the level at which the liquid makes contact with the compressor. These three conditions can collectively be measured as *the speed of the SIF to stop inflow before the liquid in the separator makes contact with the compressor.* Therefore, if we can achieve this with a reasonable speed to protect the compressor, we can use it as redundant measure — *and this is the case in this case study.* We thus have two final elements in parallel.

Therefore, the Top event is *the SIF failed to stop the compressor AND the inflow to the separator when the liquid-gas interface level is too high in the separator during normal operation.*

9.2.3 Fault Tree Construction

As discussed in Chapter 5, due care must be given while modeling CCFs in the FTA. There are two ways of modeling [16], explicitly where a CCF is included as a (basic) event in the fault tree or implicitly where it is incorporated after identifying the MCSs. Implicit modeling is helpful if the system under consideration is rather complex, having different types of CCFs in a MCS. However, in our case, explicit modeling is sufficient as it can be seen from Figure 9.2 (drawn with the CARA FaultTree software). The adequacy of the fault tree is communicated before going to further analyses.

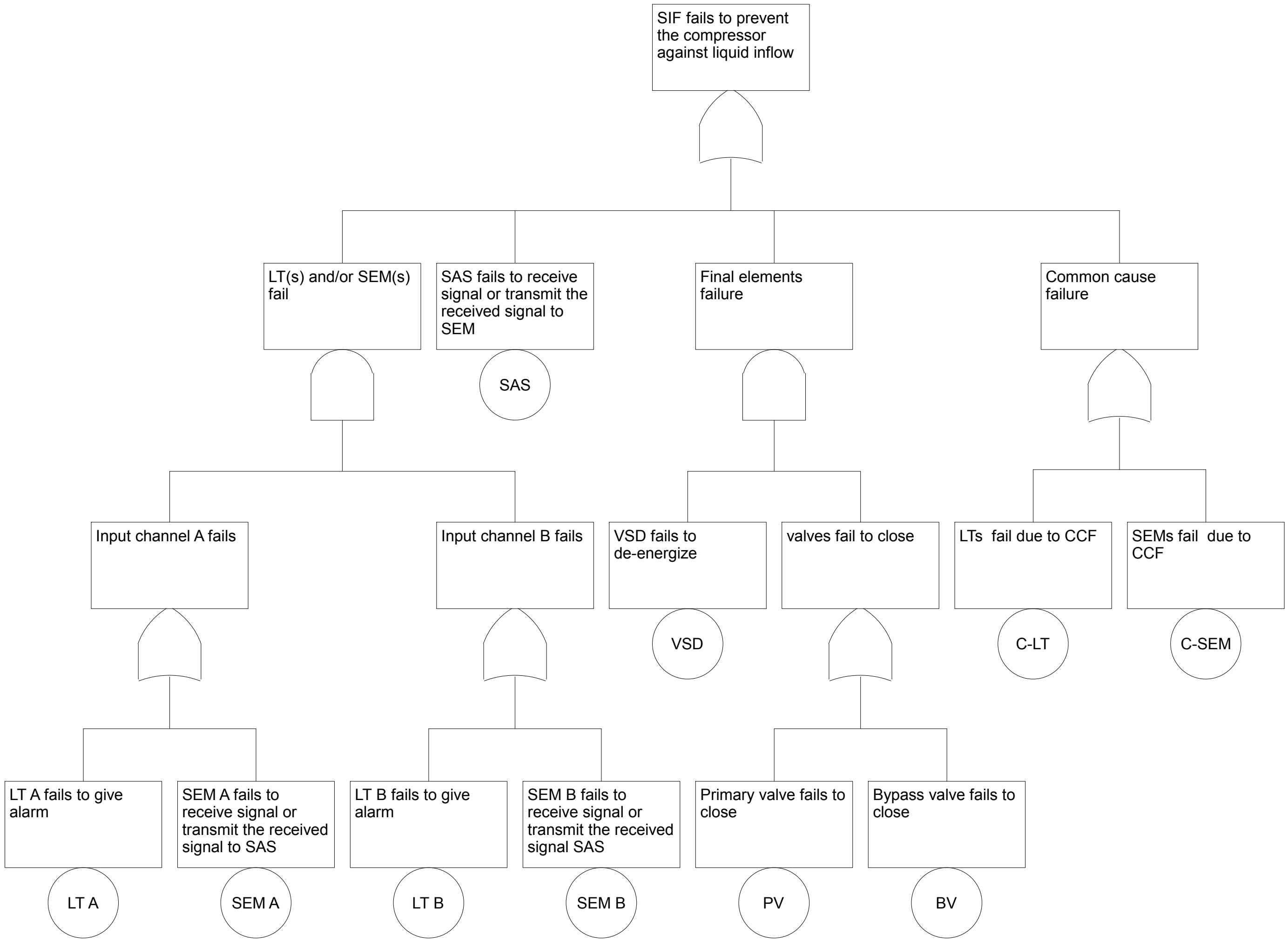
SIF fails to prevent the compressor against liquid inflow
LT(s) and/or SEM(s) fail
SAS fails to receive signal or transmit the received signal to SEM
SAS
Final elements failure
Common cause failure
Input channel A fails
Input channel B fails
VSD fails to de-energize
VSD
valves fail to close
LTs fail due to CCF
C-LT
SEMs fail due to CCF
C-SEM
LT A fails to give alarm
LT A
SEM A fails to receive signal or transmit the received signal to SAS
SEM A
LT B fails to give alarm
LT B
SEM B fails to receive signal or transmit the received signal SAS
SEM B
Primary valve fails to close
PV
Bypass valve fails to close
BV

Figure 9.2: Fault tree for the PSD function

It is almost always a good idea to transform the constructed fault tree into RBD before commencing any further analysis. It can easily be transformed to a series structure of all MCSs where components in a MCS are in parallel. The SIF has nine MCSs.

Figure 9.3 shows the equivalent RBD of the fault tree. Such transformation is helpful at least for two reasons: first it can be used as a cross-check for the adequacy of the fault tree, and

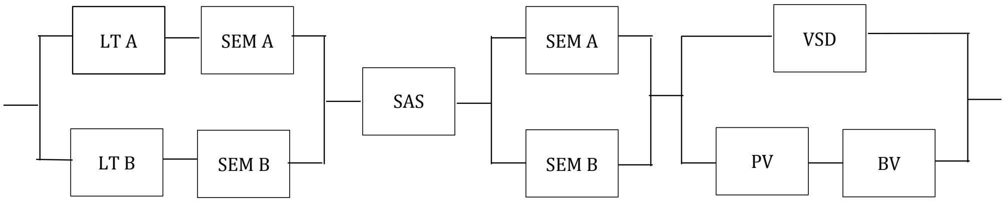

Figure 9.3: RBD for the PSD function

second, it is easier in the RBD than in the fault tree to visualize the MCSs and how the system functions as well as to establish associated formulas.

9.2.4 PFD$_{\text{avg}}$ Calculation

PFD$_{\text{avg}}$ calculations are performed based on all possible alternatives to point out how they deviate from the correct one. As discussed in Chapter 5, averaging before logic is a wrong way of calculating PFD$_{\text{avg}}$ but still some computer programs, including CARA FaultTree, uses this approach. With this approach PFD$_{\text{avg}}$ is 1.12E-03. With the correct approaches we also tried to see how the result varies for the IEC 61508 and the PDS method[1].

The PDS method advocates multiple beta-factor model but this does not bring any difference in our analysis since the maximum order of the MCSs is two. The only difference is that the PDS method uses (not strictly) a conservative failure rate for independent failures, i.e., λ instead of $(1-\beta)\lambda$ for the 1oo2 architecture. This does not even bring any significant difference since the beta factors are small. We, therefore, ended up with identical result from these methods, i.e., PFD$_{\text{avg}}$ = 1.14E-03.

The last row in Table 9.1 is based on (5.3) where we simply sum up the individual average PFDs of all the MCSs. As expected, they are identical with the results from the exact formula (5.2) since the product terms are negligible.

[1] Note that the PDS method suggests both formulas with and without the CCF factor in the PFD$_{\text{avg}}$ due to independent failures.

Table 9.1: PFD_{avg} calculation based on different possible approaches

MCS	MCS	Average before		Average After logic			
No.		logic		IEC 61508		the PDS method	
(order)		Formula	Estimate	Formula	Estimate	Formula	Estimate
1(1)	{C-SEM}	$\frac{\lambda^{C}_{DU}\tau}{2}$	9.81E-05	$\frac{\lambda^{C}_{DU}\tau}{2}$	9.81E-05	$\frac{\lambda^{C}_{DU}\tau}{2}$	9.81E-05
2(1)	{C-LT}	"	2.63E-04	"	2.63E-04	"	2.63E-04
3(1)	{SAS}	$\frac{\lambda_{DU}\tau}{2}$	7.01E-04	$\frac{\lambda_{DU}\tau}{2}$	7.01E-04	$\frac{\lambda_{DU}\tau}{2}$	7.01E-04
4(2)	{LT A, LT B}	$\frac{(\lambda^{I}_{DU}\tau)^2}{4}$	5.54E-06	$\frac{(\lambda^{I}_{DU}\tau)^2}{3}$	7.39E-06	$\frac{(\lambda_{DU}\tau)^2}{3}$	8.02E-06
5(2)	{SEM A, SEM B}	"	1.18E-05	"	1.57E-05	"	1.72E-05
6(2)	{LT A, SEM A}	$\frac{\lambda^{I}_{DU,1}\lambda^{I}_{DU,2}\tau^2}{4}$	1.18E-05	$\frac{\lambda^{I}_{DU,1}\lambda^{I}_{DU,2}\tau^2}{3}$	1.57E-05	$\frac{\lambda_{DU,1}\lambda_{DU,2}\tau^2}{3}$	1.72E-05
7(2)	{LT B, SEM B}	"	2.49E-05	"	3.32E-05	"	3.68E-05
8(2)	{VSD, PV}	"	9.98E-07	"	1.33E-06	"	1.33E-06
9(2)	{VSD, BV}	"	4.99E-07	"	6.65E-07	"	6.65E-07

PFD_{avg} based on (5.2)	1.12E-03	1.14E-03	1.14E-03
PFD_{avg} based on (5.3)	1.12E-03	1.14E-03	1.14E-03

Conclusion

- The function meets the requirement of SIL 2 since $1.14\text{E}-03 < 1.00\text{E}-02$.

- Almost 93% of the PFD_{avg} is consumed by the first three MCSs individually with 8.6%, 23% and 61%, respectively. On one hand, the function can be considered as good, because the result implies that system failure occurs mainly due to SAS failure, but it is known that computers are more reliable than detectors and final elements. Furthermore, unlike the other components, the SAS is located topside. On the other hand, such huge amount of consumption by one component may be considered as the weakness of the design. With this and other qualitative and semi-quantitative measures, appropriate decision should be made on whether or not reallocation is required to improve the reliability of the system.

9.3 Simplified Formulas

Four simplified formulas are covered in Chapter 4. The suitability of the formulas depend on the specific operational characteristics of the system, and this issue is discussed in Chapter 8. For this particular system:

- The FTC is assumed to be 100% (this assumption is partly influenced by lack of data).

- The safety unavailability contribution during function testing is negligible as argued in Chapter 8. However, sensitivity analysis can be performed by incorporating t/τ into the already computed PFD_{avg}.

- There is no diagnostic coverage for the final elements, i.e., for the VSD and the valves.

- There is no special desire to separately quantify the safety unavailability due to DU and DD failures.

As can be seen from Figure 8.1, the above points lead to either the PDS method or IEC 61508 (for all subsystems). However, we proceed by using the IEC 61508 formula. The calculation will then be based on the assumptions listed in Section 4.3.2, and further we assume that the subsystems are statistically independent.

The RBD in Figure 9.3 is subjected to the functionality path of the system and can thus be redrawn by eliminating the redundant MCS {SEM A, SEM B}. Figure 9.4 shows the resulting RBD that also takes into account the failure modes. Note that in the first subsystem both channels are identical.

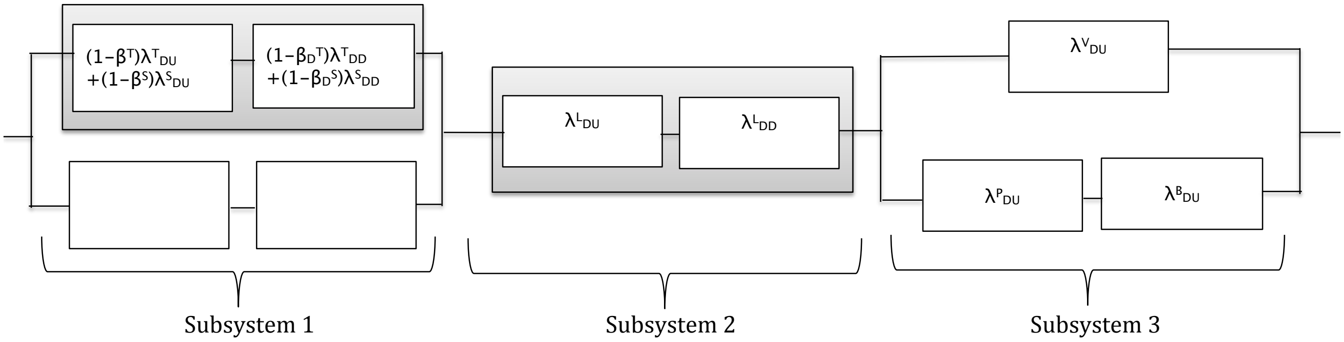

Figure 9.4: Reduced RBD for PSD function

The fifth assumption of IEC 61508 in Section 4.3.2 states that all channels have the same failure rate and diagnostic coverage. As can be seen from Figure 9.4, the final elements violate this assumption, and no IEC 61508 formula is available for this case. Let us now digress to see what will happen to the IEC 61508 formula if the channels were equipped with a built-in diagnostic testing having different DC factors. The PFD$_{\text{avg}}$ formula can thus be modified as follows:

$$\text{PFD}^{\text{FE}}_{\text{avg}} = \left(\lambda^{\text{V}}_{\text{D}} t^{\text{V}}_{\text{CE}}\right) \cdot \left(\lambda^{\text{PB}}_{\text{D}} t^{\text{PB}}_{\text{GE}}\right) + \left(\lambda^{\text{PB}}_{\text{D}} t^{\text{PB}}_{\text{CE}}\right) \cdot \left(\lambda^{\text{V}}_{\text{D}} t^{\text{V}}_{\text{GE}}\right) \tag{9.1}$$

where

$$\begin{aligned}
t^{\text{V}}_{\text{CE}} &= \frac{\lambda^{\text{V}}_{\text{DU}}}{\lambda^{\text{V}}_{\text{D}}}\left(\frac{\tau}{2} + \text{MRT}\right) + \frac{\lambda^{\text{V}}_{\text{DD}}}{\lambda^{\text{V}}_{\text{D}}}\text{MTTR} \\
t^{\text{PB}}_{\text{CE}} &= \frac{\lambda^{\text{P}}_{\text{DU}} + \lambda^{\text{B}}_{\text{DU}}}{\lambda^{\text{P}}_{\text{D}} + \lambda^{\text{B}}_{\text{D}}}\left(\frac{\tau}{2} + \text{MRT}\right) + \frac{\lambda^{\text{P}}_{\text{DD}} + \lambda^{\text{B}}_{\text{DD}}}{\lambda^{\text{P}}_{\text{D}} + \lambda^{\text{B}}_{\text{D}}}\text{MTTR} \\
t^{\text{PB}}_{\text{GE}} &= \frac{\lambda^{\text{P}}_{\text{DU}} + \lambda^{\text{B}}_{\text{DU}}}{\lambda^{\text{P}}_{\text{D}} + \lambda^{\text{B}}_{\text{D}}}\left(\frac{\tau}{3} + \text{MRT}\right) + \frac{\lambda^{\text{P}}_{\text{DD}} + \lambda^{\text{B}}_{\text{DD}}}{\lambda^{\text{P}}_{\text{D}} + \lambda^{\text{B}}_{\text{D}}}\text{MTTR} \\
t^{\text{V}}_{\text{GE}} &= \frac{\lambda^{\text{V}}_{\text{DU}}}{\lambda^{\text{V}}_{\text{D}}}\left(\frac{\tau}{3} + \text{MRT}\right) + \frac{\lambda^{\text{V}}_{\text{DD}}}{\lambda^{\text{V}}_{\text{D}}}\text{MTTR} \quad \text{and} \\
\lambda^{\text{PB}}_{\text{D}} &= \lambda^{\text{P}}_{\text{DU}} + \lambda^{\text{P}}_{\text{DD}} + \lambda^{\text{B}}_{\text{DU}} + \lambda^{\text{B}}_{\text{DD}}
\end{aligned}$$

where FE is the final element; and V and PB stands for VSD channel and valves (primary and bypass) channel respectively.

But, for the system under consideration $\lambda_{\text{DD}} = 0$, therefore (9.1) reduces to

$$\begin{aligned}
\text{PFD}^{\text{FE}}_{\text{avg}} &= \left(\lambda^{\text{V}}_{\text{DU}}\left(\frac{\tau}{2} + \text{MRT}\right)\right) \cdot \left(\lambda^{\text{PB}}_{\text{DU}}\left(\frac{\tau}{3} + \text{MRT}\right)\right) + \left(\lambda^{\text{PB}}_{\text{DU}}\left(\frac{\tau}{2} + \text{MRT}\right)\right) \cdot \left(\lambda^{\text{V}}_{\text{DU}}\left(\frac{\tau}{3} + \text{MRT}\right)\right) \\
&= 2\lambda^{\text{PB}}_{\text{DU}}\lambda^{\text{V}}_{\text{DU}}\left(\frac{\tau}{2} + \text{MRT}\right)\left(\frac{\tau}{3} + \text{MRT}\right) \qquad (9.2)
\end{aligned}$$

(Note that if MRT=0, then (9.2) reduces to Rausand's formula, i.e., $\lambda^{\text{V}}_{\text{DU}}(\lambda^{\text{P}}_{\text{DU}} + \lambda^{\text{B}}_{\text{DU}})/3$)

Hence, the PFD_{avg} for the system is

$$\begin{aligned}
\text{PFD}_{\text{avg}} &= 2\left((1-\beta^{\text{T}})\lambda_{\text{DU}}^{\text{T}} + (1-\beta^{\text{S}})\lambda_{\text{DU}}^{\text{S}} + (1-\beta_{\text{D}}^{\text{T}})\lambda_{\text{DD}}^{\text{T}} + (1-\beta_{\text{D}}^{\text{S}})\lambda_{\text{DD}}^{\text{S}}\right)^2 t_{\text{CE}}^{\text{TS}} t_{\text{GE}}^{\text{TS}} \\
&\quad + \lambda_{\text{D}}^{\text{L}} t_{\text{CE}}^{\text{L}} \\
&\quad + 2\lambda_{\text{DU}}^{\text{PB}} \lambda_{\text{DU}}^{\text{V}} \left(\frac{\tau}{2} + \text{MRT}\right)\left(\frac{\tau}{3} + \text{MRT}\right) \\
&\quad + \beta^{\text{T}} \lambda_{\text{DU}}^{\text{T}} (\frac{\tau}{2} + \text{MRT}) + \beta_{\text{D}}^{\text{T}} \lambda_{\text{DD}}^{\text{T}} \text{MTTR} \\
&\quad + \beta^{\text{S}} \lambda_{\text{DU}}^{\text{S}} (\frac{\tau}{2} + \text{MRT}) + \beta_{\text{D}}^{\text{S}} \lambda_{\text{DD}}^{\text{S}} \text{MTTR}
\end{aligned} \tag{9.3}$$

The first three terms are contributions from independent failures of the subsystems shown in Figure 9.4, respectively. The last two terms are contributions from the CCF of level transmitters and SEMs respectively. T, S, and L stand for level transmitter, SEM and SAS, respectively. The equivalent MDTs are computed as follows:

$$\begin{aligned}
t_{\text{CE}}^{\text{TS}} &= \frac{\lambda_{\text{DU}}^{\text{T}} + \lambda_{\text{DU}}^{\text{S}}}{\lambda_{\text{D}}^{\text{T}} + \lambda_{\text{D}}^{\text{S}}}\left(\frac{\tau}{2} + \text{MRT}\right) + \frac{\lambda_{\text{DD}}^{\text{T}} + \lambda_{\text{DD}}^{\text{S}}}{\lambda_{\text{D}}^{\text{T}} + \lambda_{\text{D}}^{\text{S}}}\text{MTTR} \\
t_{\text{GE}}^{\text{TS}} &= \frac{\lambda_{\text{DU}}^{\text{T}} + \lambda_{\text{DU}}^{\text{S}}}{\lambda_{\text{D}}^{\text{T}} + \lambda_{\text{D}}^{\text{S}}}\left(\frac{\tau}{3} + \text{MRT}\right) + \frac{\lambda_{\text{DD}}^{\text{T}} + \lambda_{\text{DD}}^{\text{S}}}{\lambda_{\text{D}}^{\text{T}} + \lambda_{\text{D}}^{\text{S}}}\text{MTTR} \\
t_{\text{CE}}^{\text{L}} &= \frac{\lambda_{\text{DU}}^{\text{L}}}{\lambda_{\text{D}}^{\text{L}}}\left(\frac{\tau}{2} + \text{MRT}\right) + \frac{\lambda_{\text{DD}}^{\text{L}}}{\lambda_{\text{D}}^{\text{L}}}\text{MTTR}^*
\end{aligned}$$

In the calculations, we assumed that $\beta = 2 \cdot \beta_{\text{D}}$, $\lambda_{\text{DU}}^{\text{P}} = 2 \cdot \lambda_{\text{DU}}^{\text{B}}$ and $\text{MRT} = \text{MTTR} = 2 \cdot \text{MTTR}^*$ (remember that all except SAS are located subsea).

Table 9.2: Some PFD_{avg} estimates for various values of MTTR and τ (hours)

MTTR τ	16	183	365	548
4380	5.68E-04	7.56E-04	9.64E-04	1.18E-03
8760	1.16E-03	1.36E-03	1.58E-03	1.80E-03
13140	1.78E-03	1.99E-03	2.22E-03	2.46E-03

The calculation is performed in Excel and some results are presented in Table 9.2. Sensitivity analysis is also performed to see whether or not t/τ has significant effect on the PFD_{avg} results. For example, if we assume that the required time for function testing is 8 hours, the unavailability contribution to be added on the PFD_{avg} results will be 9.13E-04 (if all the subsystems are tested at the same time) and 3*9.13E-04=2.74E-03 (if the subsystems are tested staggeringly). It is thus evident that the SIF fulfills the SIL 2 requirement even for large test intervals, MTTRs as well as with online function testing with 8 hour duration.

9.4 Markov Approach

In Chapter 6, we discussed three approaches of calculating system performance by using Markov analysis, i.e., using type 1, type 2 and steady state probabilities as a measure of PFD_{avg} (see Section 6.5.1). As can be seen from the examples in that chapter, Markov analysis is cumbersome unless a simplification technique is employed to reduce the number of states. In this case study we employed the suggestion given by IEC 61165 [3]. Accordingly, series components in a subsystem are combined and treated as a single component as shown in Figure 9.5. That is, the failure rate of a channel is the sum of the failure rates of the components in that channel, and the repair rate is computed as $(\lambda_1 + ... + \lambda_n)/(\lambda_1/\mu_1 + ... + \lambda_n/\mu_n)$, provided that $\lambda_i \ll \mu_i$

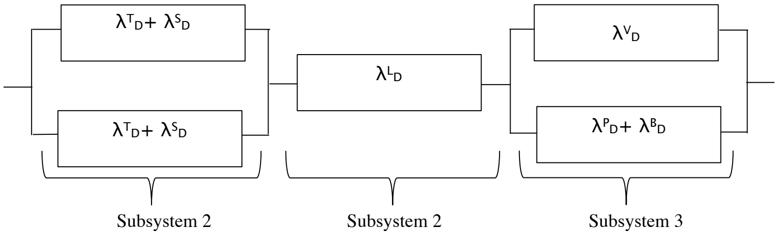
$\lambda^T_D + \lambda^S_D$
$\lambda^T_D + \lambda^S_D$
λ^L_D
λ^V_D
$\lambda^P_D + \lambda^B_D$
Subsystem 2
Subsystem 2
Subsystem 3

Figure 9.5: Further reduced RBD for the the PSD, for the purpose of Markov analysis

With this technique we cannot calculate type 1 probability since the Markov process will not have an absorbing state. That is, since the DD and DU failures are combined, the process can always leave that state with some positive probability. Therefore, in the following section we calculate steady state probability and type 2 probability.

We assumed that there are two repair crews available to restore failed channel(s). Upon failure of two channels, the one that is repaired first will start performing the safety function regardless of the status of another channel.

9.4.1 Steady State Solution

Figure 9.6 shows the state transition diagrams of the subsystems shown in Figure 9.5. Now, let us calculate the repair rates. Since constant repair rate is assumed, for DU failures the repair rate is 1/MRT and for DD failure it is 1/MTTR. The minimum repair time we used in the calculation is 8 hours (for SAS) that gives a rate of 9.13E-04 and is significantly greater than the failure rates. Therefore, the repair rate for the first subsystem can be calculated as

$$\mu_{\mathrm{D}}^{\mathrm{TS}} = \frac{\lambda_{\mathrm{DU}}^{\mathrm{T}} + \lambda_{\mathrm{DD}}^{\mathrm{T}} + \lambda_{\mathrm{DU}}^{\mathrm{S}}\lambda_{\mathrm{DD}}^{\mathrm{S}}}{\lambda_{\mathrm{DU}}^{\mathrm{T}} / \left(\mathrm{MRT}^{\mathrm{T}}\right)^{-1} + \lambda_{\mathrm{DD}}^{\mathrm{T}} / \left(\mathrm{MTTR}^{\mathrm{T}}\right)^{-1} + \lambda_{\mathrm{DU}}^{\mathrm{S}} / \left(\mathrm{MRT}^{\mathrm{S}}\right)^{-1} + \lambda_{\mathrm{DD}}^{\mathrm{S}} / \left(\mathrm{MTTR}^{\mathrm{S}}\right)^{-1}}$$

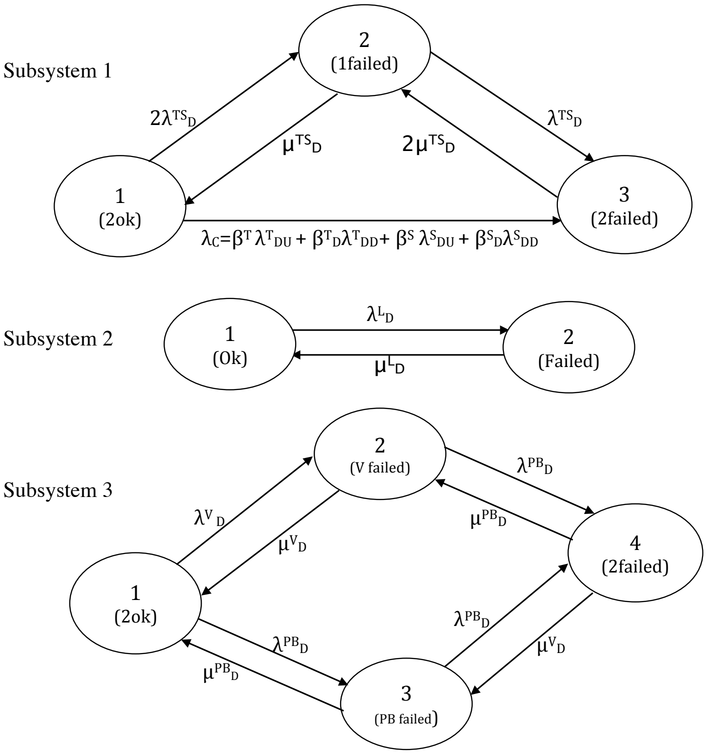

Figure 9.6: State transition diagrams of the subsystems of the PSD function

But, we assumed for all components that MRT = MTTR = $2 \cdot \text{MTTR}^*$, where MTTR^* is for SAS and hence

$$
\begin{aligned}
\mu_{\text{D}}^{\text{TS}} &= \mu_{\text{D}}^{\text{V}} = \mu_{\text{D}}^{\text{PB}} = \frac{1}{\text{MTTR}} && (9.4)\\
\mu_{\text{D}}^{\text{L}} &= \frac{\lambda_{\text{D}}^{\text{L}}}{\text{MTTR}\left(\lambda_{\text{DU}}^{\text{L}} + 2\lambda_{\text{DD}}^{\text{L}}\right)} && (9.5)
\end{aligned}
$$

Let P_i^j be the steady state probability that the system is in state i, and j is used to indicate the subsystem. Therefore,

$$\text{PFD}_{\text{avg}} = P_3^1 + P_2^2 + P_4^3 \tag{9.6}$$

The corresponding state equations are established as follows:

$$\begin{pmatrix} 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_1^1 & P_2^1 & P_3^1 \end{pmatrix} \cdot \begin{pmatrix} -\left(2\lambda_{\text{D}}^{\text{TS}} + \lambda_{\text{C}}\right) & 2\lambda_{\text{D}}^{\text{TS}} & \lambda_{\text{C}} \\ \mu_{\text{D}}^{\text{TS}} & -\left(\mu_{\text{D}}^{\text{TS}} + \lambda_{\text{D}}^{\text{TS}}\right) & \lambda_{\text{D}}^{\text{TS}} \\ 0 & 2\mu_{\text{D}}^{\text{ST}} & -2\mu_{\text{D}}^{\text{ST}} \end{pmatrix} \quad \text{and}$$

$$P_1^1 + P_2^1 + P_3^1 = 1 \tag{9.7}$$

$$\begin{pmatrix} 0 & 0 \end{pmatrix} = \begin{pmatrix} P_1^2 & P_2^2 \end{pmatrix} \cdot \begin{pmatrix} -\lambda_{\text{D}}^{\text{L}} & \lambda_{\text{D}}^{\text{L}} \\ \mu_{\text{D}}^{\text{L}} & -\mu_{\text{D}}^{\text{L}} \end{pmatrix} \quad \text{and}$$

$$P_1^2 + P_2^2 = 1 \tag{9.8}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_1^3 & P_2^3 & P_3^3 & P_4^3 \end{pmatrix} \cdot \begin{pmatrix} -\left(\lambda_{\text{D}}^{\text{V}} + \lambda_{\text{D}}^{\text{PB}}\right) & \lambda_{\text{D}}^{\text{V}} & \lambda_{\text{D}}^{\text{PB}} & 0 \\ \mu_{\text{D}}^{\text{V}} & -\left(\mu_{\text{D}}^{\text{V}} + \lambda_{\text{D}}^{\text{PB}}\right) & 0 & \lambda_{\text{D}}^{\text{PB}} \\ \mu_{\text{D}}^{\text{PB}} & 0 & -\left(\mu_{\text{D}}^{\text{PB}} + \lambda_{\text{D}}^{\text{PB}}\right) & \lambda_{\text{D}}^{\text{PB}} \\ 0 & \mu_{\text{D}}^{\text{PB}} & \mu_{\text{D}}^{\text{V}} & -\left(\mu_{\text{D}}^{\text{PB}} + \mu_{\text{D}}^{\text{V}}\right) \end{pmatrix} \quad \text{and}$$

$$P_1^3 + P_2^3 + P_3^3 + P_4^3 = 1 \tag{9.9}$$

The steady state probabilities are computed in R for some selected MTTR values and the results are shown in Table 9.3. The table depicts that the function satisfies well the SIL 2 requirement. The second subsystem, namely the SAS, consumes the majority of PFD$_{\text{avg}}$ as we already saw in FTA.

Table 9.3: Some PFD$_{\text{avg}}$ estimates for various values of MTTR (hours)

MTTR τ	16	183	365	548
P_3^1	1.35E-06	1.73E-05	3.80E-05	6.25E-05
P_2^2	4.86E-05	5.55E-04	1.11E-03	1.66E-03
P_4^3	3.76E-06	4.29E-05	8.57E-05	1.30E-04
PFD$_{\text{avg}}$	5.37E-05	6.15E-04	1.23E-03	1.86E-03
SIL	SIL 4	SIL 3	SIL 2	SIL 2

9.4.2 Time Dependent Solution - Type 2

In this section, we tried to calculate a time dependent probability as a PFD$_{\text{avg}}$ measure. Let λ_{P} be process demand rate. The state transition diagrams for the subsystems are illustrated in Figure 9.7.

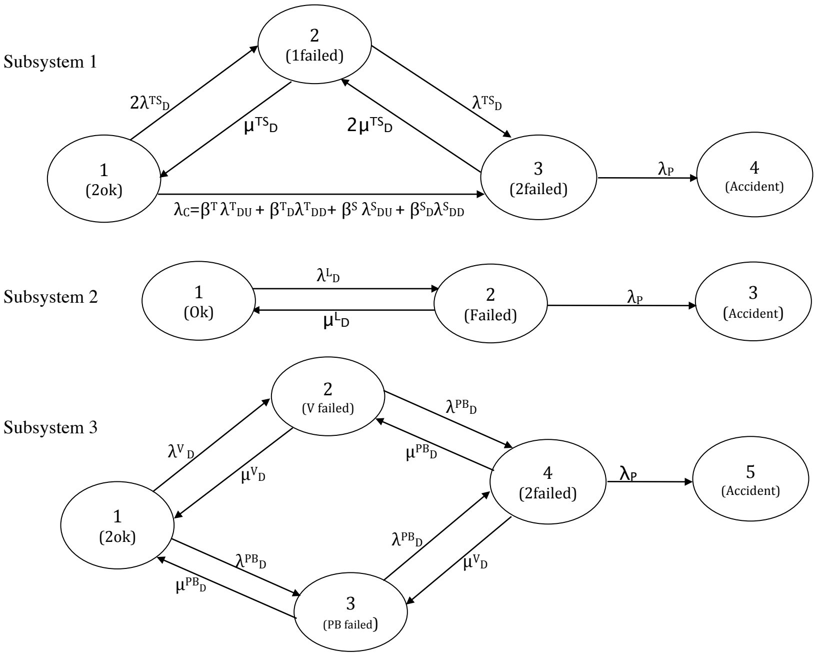

Figure 9.7: State transition diagrams of the subsystems of the PSD function (with process demand)

The corresponding set of differential equations for each subsystem respectively are

$$\begin{pmatrix} \dot{P}^1_1(t) \\ \dot{P}^1_2(t) \\ \dot{P}^1_3(t) \\ \dot{P}^1_4(t) \end{pmatrix} = \begin{pmatrix} -\left(2\lambda^{\mathrm{TS}}_{D}+\lambda_{\mathrm{C}}\right) & \mu^{\mathrm{TS}}_{\mathrm{D}} & 0 & 0 \\ 2\lambda^{\mathrm{TS}}_{\mathrm{D}} & -\left(\mu^{\mathrm{TS}}_{\mathrm{D}}+\lambda^{\mathrm{TS}}_{\mathrm{D}}\right) & 2\mu^{\mathrm{ST}}_{\mathrm{D}} & 0 \\ \lambda_{\mathrm{C}} & \lambda^{\mathrm{TS}}_{\mathrm{D}} & -\left(2\mu^{\mathrm{ST}}_{\mathrm{D}}+\lambda_{\mathrm{P}}\right) & 0 \\ 0 & 0 & \lambda_{\mathrm{P}} & 0 \end{pmatrix} \cdot \begin{pmatrix} P^1_1(t) \\ P^1_2(t) \\ P^1_3(t) \\ P^1_4(t) \end{pmatrix} \tag{9.10}$$

$$\begin{pmatrix} \dot{P}^2_1(t) \\ \dot{P}^2_2(t) \\ \dot{P}^2_3(t) \end{pmatrix} = \begin{pmatrix} -\lambda^{\mathrm{L}}_{\mathrm{D}} & \mu^{\mathrm{L}}_{\mathrm{D}} & 0 \\ \lambda^{\mathrm{L}}_{\mathrm{D}} & -\left(\mu^{\mathrm{L}}_{\mathrm{D}}+\lambda_{\mathrm{P}}\right) & 0 \\ 0 & 2\lambda_{\mathrm{P}} & 0 \end{pmatrix} \cdot \begin{pmatrix} P^2_1(t) \\ P^2_2(t) \\ P^2_3(t) \end{pmatrix} \tag{9.11}$$

$$\begin{pmatrix} \dot{P}^3_1(t) \\ \dot{P}^3_2(t) \\ \dot{P}^3_3(t) \\ \dot{P}^3_4(t) \\ \dot{P}^3_5(t) \end{pmatrix} = \begin{pmatrix} -\left(\lambda^{\mathrm{V}}_{\mathrm{D}}+\lambda^{\mathrm{PB}}_{\mathrm{D}}\right) & \mu^{\mathrm{V}}_{\mathrm{D}} & \mu^{\mathrm{PB}}_{\mathrm{D}} & 0 & 0 \\ \lambda^{\mathrm{V}}_{\mathrm{D}} & -\left(\mu^{\mathrm{V}}_{\mathrm{D}}+\lambda^{\mathrm{PB}}_{\mathrm{D}}\right) & 0 & \mu^{\mathrm{PB}}_{\mathrm{D}} & 0 \\ \lambda^{\mathrm{PB}}_{\mathrm{D}} & 0 & -\left(\mu^{\mathrm{PB}}_{\mathrm{D}}+\lambda^{\mathrm{PB}}_{\mathrm{D}}\right) & \mu^{\mathrm{V}}_{\mathrm{D}} & 0 \\ 0 & \lambda^{\mathrm{PB}}_{\mathrm{D}} & \lambda^{\mathrm{PB}}_{\mathrm{D}} & -\left(\mu^{\mathrm{PB}}_{\mathrm{D}}+\mu^{\mathrm{V}}_{\mathrm{D}}+\lambda_{\mathrm{P}}\right) & 0 \\ 0 & 0 & 0 & \lambda_{P} & 0 \end{pmatrix} \cdot \begin{pmatrix} P^3_1(t) \\ P^3_2(t) \\ P^3_3(t) \\ P^3_4(t) \\ P^3_5(t) \end{pmatrix} \tag{9.12}$$

and their Laplace transforms are

$$\begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -\left(2\lambda^{\mathrm{TS}}_{\mathrm{D}}+\lambda_{\mathrm{C}}+s\right) & \mu^{\mathrm{TS}}_{\mathrm{D}} & 0 & 0 \\ 2\lambda^{\mathrm{TS}}_{\mathrm{D}} & -\left(\mu^{\mathrm{TS}}_{\mathrm{D}}+\lambda^{\mathrm{TS}}_{\mathrm{D}}+s\right) & 2\mu^{\mathrm{ST}}_{\mathrm{D}} & 0 \\ \lambda_{\mathrm{C}} & \lambda^{\mathrm{TS}}_{\mathrm{D}} & -\left(2\mu^{\mathrm{ST}}_{\mathrm{D}}+\lambda_{\mathrm{P}}+s\right) & 0 \\ 0 & 0 & \lambda_{\mathrm{P}} & s \end{pmatrix} \cdot \begin{pmatrix} P^1_1(s) \\ P^1_2(s) \\ P^1_3(s) \\ P^1_4(s) \end{pmatrix} \tag{9.13}$$

$$\begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -\left(\lambda^{\mathrm{L}}_{\mathrm{D}}+s\right) & \mu^{\mathrm{L}}_{\mathrm{D}} & 0 \\ \lambda^{\mathrm{L}}_{\mathrm{D}} & -\left(\mu^{\mathrm{L}}_{\mathrm{D}}+\lambda_{\mathrm{P}}+s\right) & 0 \\ 0 & 2\lambda_{\mathrm{P}} & s \end{pmatrix} \cdot \begin{pmatrix} P^2_1(s) \\ P^2_2(s) \\ P^2_3(s) \end{pmatrix} \tag{9.14}$$

$$\begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -\left(\lambda^{\mathrm{V}}_{\mathrm{D}}+\lambda^{\mathrm{PB}}_{\mathrm{D}}+s\right) & \mu^{\mathrm{V}}_{\mathrm{D}} & \mu^{\mathrm{PB}}_{\mathrm{D}} & 0 & 0 \\ \lambda^{\mathrm{V}}_{\mathrm{D}} & -\left(\mu^{\mathrm{V}}_{\mathrm{D}}+\lambda^{\mathrm{PB}}_{\mathrm{D}}+s\right) & 0 & \mu^{\mathrm{PB}}_{\mathrm{D}} & 0 \\ \lambda^{\mathrm{PB}}_{\mathrm{D}} & 0 & -\left(\mu^{\mathrm{PB}}_{\mathrm{D}}+\lambda^{\mathrm{PB}}_{\mathrm{D}}+s\right) & \mu^{\mathrm{V}}_{\mathrm{D}} & 0 \\ 0 & \lambda^{\mathrm{PB}}_{\mathrm{D}} & \lambda^{\mathrm{PB}}_{\mathrm{D}} & -\left(\mu^{\mathrm{PB}}_{\mathrm{D}}+\mu^{\mathrm{V}}_{\mathrm{D}}+\lambda_{\mathrm{P}}+s\right) & 0 \\ 0 & 0 & 0 & \lambda_{\mathrm{P}} & s \end{pmatrix} \cdot \begin{pmatrix} P^3_1(t) \\ P^3_2(t) \\ P^3_3(t) \\ P^3_4(t) \\ P^3_5(t) \end{pmatrix} \tag{9.15}$$

We assume the process demand rate to be once every two years, i.e., λ_{P}=5.71E-05. However, the numerical analysis performed in Maple is turned out to be zero since the probabilities are negligible.

As can be seen from all the results, the SIF is in accordance with the SIL 2 requirement, and the SAS is the huge contributor of the PFD_{avg}. Thus, an appropriate measure should be carried out to improve the reliability of the system by taking into account these results and other qualitative and semi-quantitative aspects.

Chapter 10

Conclusions and Recommendations for Further work

10.1 Conclusion

Several methods, with different backgrounds, assumptions and limitations, are available to quantify the reliability of a SIS. The PFD_{avg} result depends on the choice of a method, its assumptions and limitations, and the assumptions made to simplify the calculation. The result is "lame" if the calculation is carried out without understanding the assumptions and the limitations of the method employed. Theoretical and empirical analyses indicate that if two analysts, independently, calculate the PFD_{avg} for the same SIS, they will likely come up with different results. If so, what is the point of the calculation then? After all, the calculation is performed as a basis for decision-making about the reliability performance of the SIS.

We have documented the background, rationale, assumptions, limitations and applications of several analytical methods that are available for analysts. The analytical methods suggested in IEC 61508, except Petri net, are presented, discussed and compared to each other, and further two approaches are introduced. Moreover, a procedure is set up to choose and apply these methods, and is demonstrated in a case study, i.e., a SIF installed to prevent a subsea compressor against liquid inflow.

Proper understanding of the nature of failure causes and operational characteristics of the SIS will substantially reduce the computational burden and increase the accuracy of the result. It is always beneficial to start with FTA, especially if the SIS is in the design phase, because of four reasons. Firstly, since we think in terms of failure while constructing the fault tree, we have the opportunity to uncover and understand failure causes. Secondly, since the method is intuitive, it gives the chance to communicate among several experts. Thirdly, FTA can fully be utilized as a PFD_{avg} calculation method under the respective assumptions. Fourthly, a hybrid of FTA and Markov analysis gives a good estimate of the PFD_{avg}, especially for a relatively complex SIS. Thus, the report provides a procedure to implement FTA and distinguishes the associated optimistic and pessimistic approaches to calculate the PFD_{avg}.

It is recognized that many users choose the most simplified formulas; particularly, in the Norwegian petroleum industry, the PDS method is the most common method. A detailed proof of the IEC 61508 simplified formulas and an extension to $k$oo$n$ architectures are performed. Rausand's formula is absolutely the same as the IEC 61508 formula under the assumptions that *MRT is negligible* and *the SIS is functioning as long as DU failures are not occurred.* Some factors incorporated in the PDS method, e.g., DTU_{T}, are shown to be less significant to require deviation from the IEC 61508 formulas. Moreover, the conditional relationship of DU and DD failures is overlooked. An alternative formula is suggested in this report that utilizes this conditionality. Nonetheless, the analytical and numerical analyses show that these methods are very similar except some slight differences resulted from their level of details. To the extent that simplified methods are considered appropriate for PFD_{avg} calculation, with these four approaches, a procedure is developed to choose the nearest possible method based on the specific operational characteristics of the SIS.

For a more complex SIS with complex maintenance strategies, Markov analysis gives a better result though the computation is difficult and requires some special computer programs. We have shown some practical examples to calculate both time dependent and steady state probabilities as a measure of PFD_{avg}. It is also exemplified that the number of states increases exponentially as the number of components increase and its consequence in calculating a time dependent solution. It is always a problem to calculate a time dependent solutions if the number of states is greater than five so that care has to be exercised to keep it as small as possible. Based on the suggestion from IEC 61165, i.e., by collecting all series component in one component, the number of states can significantly be reduced. This is illustrated in the case study.

Most PFD_{avg} calculation methods do not directly take the process demands into account. In this report it is shown that the *average probability that the SIS fails and the process demand occurs* can be computed rigorously with Markov analysis, provided that reliable data for the demand rate is available.

Although it is recognized that the constant failure rate assumption is unrealistic, all PFD_{avg} formulas are persisting with it. A new approach is introduced in this report that enables us to calculate PFD_{avg} under the assumption of other lifetime distributions and is demonstrated under Weibull distribution. The analytical and numerical verifications indicated that the approach estimates the PFD_{avg} with high degree of accuracy.

10.2 Recommendations for Further Work

With Markov analysis, the PFD_{avg} can be computed in terms of time dependent probability (unreliability) or steady state probability (unavailability). In IEC 61508 the unreliability approach is considered as the correct approach but its computational burden is incomparably higher than the unavailability approach. Therefore, research should be performed to explore and provide a firm conclusion on the consequences of the unavailability approach.

The PFD_{avg} calculation under the assumption of Weibull distribution is dependent on the availability of data to estimate the parameters. It is, therefore, important to collect data such that model parameters can be estimated with reasonable accuracy. Moreover, further studies are necessary to verify the proposed approach as well as to extend it to other lifetime distributions, for example lognormal.

Appendix A

Acronyms

CCF common cause failure

CDF cumulative distribution function

DC diagnostic coverage

FTC function testing coverage

E/E/PE electrical/electronic/programmable electronic

EUC equipment under control

FMECA failure modes, effects, and criticality analysis

FTA fault tree analysis

IEC international Electrotechnical Commission

KBS kolmogorov backward equations

KFE kolmogorov forward equations

LT level transmitter

MDT mean down time

MTTR mean time to restoration

MTTF mean time to failure

PCS process control system

PFD probability of failure on demand

PSD process shutdown

SAS safety and automation system

SEM subsea electronic module

SIF safety instrumented function

SIL safety integrity level

SIS safety instrumented system

SLC safety lifecycle

SRS safety requirements specification

Appendix B

Some Typical Values of the Multiplier $\left(\mathrm{A}_k^{\mathrm{W}}\right)$

The approximated PFD formula for a $M\mathrm{oo}N$ architecture under the assumption of Weibull distribution is given by

$$\mathrm{PFD}_{\mathrm{avg},k1} \approx \binom{N}{N-M+1} \cdot \frac{\mathrm{A}_k^{\mathrm{W}}}{\alpha+1} (\lambda\tau)^{\alpha k}$$

Where $k = M - N + 1$ and $\mathrm{A}_k^{\mathrm{W}}$ is a multiplier that is given by

$$\mathrm{A}_k^{\mathrm{W}} = \left[\sum_{x=1}^{k} \binom{k}{x} (-1)^{x+1} x^{-\frac{1}{\alpha}}\right]^{-\alpha}$$

The table below provides the values of the multiplier for various values of α and k. Note that $\mathrm{A}_1^{\mathrm{W}} = 1$, for all $\alpha > 0$.

Note that we presented the values only for increasing failure rate ($\alpha \geq 0$), which follows from the fact that all components, at least for our purpose, have increasing failure rate.

Table B.1: The values of $\mathrm{A}_k^{\mathrm{W}}$ for some typical α and k

α \ k	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1.0	0.667	0.545	0.480	0.438	0.408	0.386	0.368	0.353	0.341	0.331	0.322	0.314	0.308	0.301
1.1	0.656	0.533	0.468	0.426	0.397	0.374	0.357	0.343	0.331	0.321	0.312	0.304	0.298	0.292
1.2	0.646	0.523	0.457	0.416	0.387	0.365	0.347	0.333	0.322	0.312	0.303	0.296	0.289	0.283
1.3	0.638	0.514	0.448	0.407	0.378	0.356	0.339	0.325	0.314	0.304	0.296	0.288	0.282	0.276
1.4	0.630	0.506	0.440	0.399	0.371	0.349	0.332	0.318	0.307	0.298	0.289	0.282	0.276	0.270
1.5	0.624	0.498	0.433	0.392	0.364	0.343	0.326	0.312	0.301	0.292	0.283	0.276	0.270	0.264
1.6	0.618	0.492	0.427	0.386	0.358	0.337	0.320	0.307	0.296	0.286	0.278	0.271	0.265	0.259
1.7	0.612	0.486	0.421	0.381	0.353	0.332	0.315	0.302	0.291	0.282	0.274	0.267	0.261	0.255
1.8	0.607	0.481	0.416	0.376	0.348	0.327	0.311	0.298	0.287	0.278	0.270	0.263	0.257	0.251
1.9	0.602	0.476	0.412	0.372	0.344	0.323	0.307	0.294	0.283	0.274	0.266	0.259	0.253	0.248
2.0	0.598	0.472	0.407	0.367	0.340	0.319	0.303	0.290	0.280	0.271	0.263	0.256	0.250	0.245
2.1	0.594	0.468	0.404	0.364	0.336	0.316	0.300	0.287	0.277	0.268	0.260	0.253	0.247	0.242
2.2	0.591	0.464	0.400	0.360	0.333	0.313	0.297	0.284	0.274	0.265	0.257	0.250	0.245	0.239
2.3	0.587	0.461	0.397	0.357	0.330	0.310	0.294	0.281	0.271	0.262	0.255	0.248	0.242	0.237
2.4	0.584	0.457	0.394	0.354	0.327	0.307	0.292	0.279	0.269	0.260	0.252	0.246	0.240	0.235
2.5	0.582	0.455	0.391	0.352	0.325	0.305	0.289	0.277	0.266	0.258	0.250	0.244	0.238	0.233
2.6	0.579	0.452	0.388	0.349	0.322	0.302	0.287	0.275	0.264	0.256	0.248	0.242	0.236	0.231
2.7	0.576	0.449	0.386	0.347	0.320	0.300	0.285	0.273	0.262	0.254	0.246	0.240	0.234	0.229
2.8	0.574	0.447	0.384	0.345	0.318	0.298	0.283	0.271	0.260	0.252	0.244	0.238	0.232	0.227
2.9	0.572	0.445	0.381	0.343	0.316	0.296	0.281	0.269	0.259	0.250	0.243	0.236	0.231	0.226
3.0	0.570	0.443	0.380	0.341	0.314	0.295	0.280	0.267	0.257	0.249	0.241	0.235	0.229	0.224
3.1	0.568	0.441	0.378	0.339	0.313	0.293	0.278	0.266	0.256	0.247	0.240	0.234	0.228	0.223
3.2	0.566	0.439	0.376	0.337	0.311	0.292	0.276	0.264	0.254	0.246	0.239	0.232	0.227	0.222
3.3	0.564	0.437	0.374	0.336	0.309	0.290	0.275	0.263	0.253	0.245	0.237	0.231	0.226	0.221
3.4	0.562	0.435	0.373	0.334	0.308	0.289	0.274	0.262	0.252	0.243	0.236	0.230	0.224	0.219
3.5	0.561	0.434	0.371	0.333	0.307	0.287	0.272	0.260	0.251	0.242	0.235	0.229	0.223	0.218
3.6	0.559	0.432	0.370	0.332	0.305	0.286	0.271	0.259	0.249	0.241	0.234	0.228	0.222	0.217
3.7	0.558	0.431	0.368	0.330	0.304	0.285	0.270	0.258	0.248	0.240	0.233	0.227	0.221	0.216
3.8	0.557	0.429	0.367	0.329	0.303	0.284	0.269	0.257	0.247	0.239	0.232	0.226	0.220	0.216
3.9	0.555	0.428	0.366	0.328	0.302	0.283	0.268	0.256	0.246	0.238	0.231	0.225	0.220	0.215
4.0	0.554	0.427	0.365	0.327	0.301	0.282	0.267	0.255	0.246	0.237	0.230	0.224	0.219	0.214
4.1	0.553	0.426	0.364	0.326	0.300	0.281	0.266	0.254	0.245	0.236	0.229	0.223	0.218	0.213
4.2	0.552	0.425	0.362	0.325	0.299	0.280	0.265	0.254	0.244	0.236	0.229	0.223	0.217	0.212
4.3	0.551	0.424	0.361	0.324	0.298	0.279	0.264	0.253	0.243	0.235	0.228	0.222	0.216	0.212
4.4	0.550	0.422	0.361	0.323	0.297	0.278	0.264	0.252	0.242	0.234	0.227	0.221	0.216	0.211
4.5	0.549	0.422	0.360	0.322	0.296	0.278	0.263	0.251	0.242	0.233	0.226	0.220	0.215	0.210
4.6	0.548	0.421	0.359	0.321	0.296	0.277	0.262	0.251	0.241	0.233	0.226	0.220	0.214	0.210
4.7	0.547	0.420	0.358	0.320	0.295	0.276	0.261	0.250	0.240	0.232	0.225	0.219	0.214	0.209
4.8	0.546	0.419	0.357	0.320	0.294	0.275	0.261	0.249	0.240	0.232	0.225	0.219	0.213	0.209
4.9	0.545	0.418	0.356	0.319	0.293	0.275	0.260	0.249	0.239	0.231	0.224	0.218	0.213	0.208
5.0	0.544	0.417	0.355	0.318	0.293	0.274	0.260	0.248	0.238	0.230	0.223	0.217	0.212	0.207

Appendix C

Numerical Comparison Between Simplified Formulas

Table C.1: Comparison between the methods, 1oo1 architecture

Parameter Specification			Approaches				Comparison with IEC in %		
Test Int.	λ_D	DC	IEC 61508	PDS	Rausand	New	PDS	Rausand	New
4380 hr	5.0E-06	0%	1.28E-02	1.10E-02	1.10E-02	1.28E-02	-14.29	-14.29	0.00
		60%	7.30E-03	6.57E-03	4.38E-03	7.29E-03	-10.00	-40.00	-0.15
		90%	4.56E-03	4.38E-03	1.10E-03	4.56E-03	-4.00	-76.00	-0.09
	2.5E-05	0%	6.39E-02	5.48E-02	5.48E-02	6.39E-02	-14.29	-14.29	0.00
		60%	3.65E-02	3.29E-02	2.19E-02	3.62E-02	-10.00	-40.00	-0.77
		90%	2.28E-02	2.19E-02	5.48E-03	2.27E-02	-4.00	-76.00	-0.46
	1.0E-05	0%	2.56E-02	2.19E-02	2.19E-02	2.56E-02	-14.29	-14.29	0.00
		60%	1.46E-02	1.31E-02	8.76E-03	1.46E-02	-10.00	-40.00	-0.31
		90%	9.13E-03	8.76E-03	2.19E-03	9.11E-03	-4.00	-76.00	-0.18
8760 hr	5.0E-06	0%	2.37E-02	2.19E-02	2.19E-02	2.37E-02	-7.69	-7.69	0.00
		60%	1.17E-02	1.10E-02	8.76E-03	1.17E-02	-6.25	-25.00	-0.18
		90%	5.66E-03	5.48E-03	2.19E-03	5.65E-03	-3.23	-61.29	-0.14
	2.5E-05	0%	1.19E-01	1.10E-01	1.10E-01	1.19E-01	-7.69	-7.69	0.00
		60%	5.84E-02	5.48E-02	4.38E-02	5.79E-02	-6.25	-25.00	-0.89
		90%	2.83E-02	2.74E-02	1.10E-02	2.81E-02	-3.23	-61.29	-0.69
	1.0E-05	0%	4.75E-02	4.38E-02	4.38E-02	4.75E-02	-7.69	-7.69	0.00
		60%	2.34E-02	2.19E-02	1.75E-02	2.33E-02	-6.25	-25.00	-0.36
		90%	1.13E-02	1.10E-02	4.38E-03	1.13E-02	-3.23	-61.29	-0.28

Table C.2: Comparison between the methods, 1oo2 architecture

Parameter Specification				Approaches				Comparison with IEC in %		
Int.	λ_D	DC	β	IEC 61508	PDS	Rausand	New	PDS	Rausand	New
4380	5.0E-06	0%	2%	4.79E-04	3.73E-04	3.73E-04	4.11E-04	-22.29	-22.29	-14.29
			10%	1.47E-03	1.22E-03	1.22E-03	1.26E-03	-16.49	-16.49	-14.29
		60%	2%	2.07E-04	1.75E-04	1.12E-04	2.12E-04	-15.57	-45.81	2.52
			10%	6.94E-04	6.95E-04	4.59E-04	8.18E-04	0.11	-33.93	17.86
		90%	2%	9.59E-05	9.62E-05	2.34E-05	1.86E-04	0.34	-75.55	93.84
			10%	3.26E-04	4.46E-04	1.11E-04	6.62E-04	36.65	-66.04	103.01
	2.5E-05	0%	2%	6.88E-03	4.93E-03	4.93E-03	5.89E-03	-28.24	-28.24	-14.29
			10%	1.11E-02	8.71E-03	8.71E-03	9.52E-03	-21.57	-21.57	-14.29
		60%	2%	2.69E-03	1.74E-03	1.05E-03	2.24E-03	-35.34	-60.93	-16.89
			10%	4.95E-03	4.23E-03	2.71E-03	5.12E-03	-14.38	-45.25	3.57
		90%	2%	1.23E-03	6.53E-04	1.48E-04	2.24E-03	-46.88	-87.96	82.03
			10%	2.32E-03	2.38E-03	5.80E-04	4.51E-03	2.99	-74.95	94.82
	1.0E-05	0%	2%	1.41E-03	1.05E-03	1.05E-03	1.21E-03	-25.20	-25.20	-14.29
			10%	3.31E-03	2.71E-03	2.71E-03	2.84E-03	-18.20	-18.20	-14.29
		60%	2%	5.80E-04	4.36E-04	2.73E-04	5.42E-04	-24.75	-52.83	-6.49
			10%	1.54E-03	1.47E-03	9.59E-04	1.74E-03	-4.56	-37.57	13.27
		90%	2%	2.67E-04	2.10E-04	4.99E-05	5.02E-04	-21.42	-81.27	88.40
			10%	7.21E-04	9.07E-04	2.24E-04	1.44E-03	25.84	-68.90	100.39
8760	5.0E-06	0%	2%	1.22E-03	1.05E-03	1.05E-03	1.13E-03	-13.97	-13.97	-7.69
			10%	3.00E-03	2.71E-03	2.71E-03	2.77E-03	-9.85	-9.85	-7.69
		60%	2%	4.11E-04	3.55E-04	2.73E-04	4.74E-04	-13.58	-33.41	15.31
			10%	1.24E-03	1.21E-03	9.59E-04	1.68E-03	-1.87	-22.39	35.78
		90%	2%	1.35E-04	1.30E-04	4.99E-05	3.75E-04	-3.78	-62.96	177.90
			10%	4.51E-04	5.66E-04	2.24E-04	1.33E-03	25.34	-50.32	194.03
	2.5E-05	0%	2%	2.11E-02	1.75E-02	1.75E-02	1.95E-02	-16.79	-16.79	-7.69
			10%	2.76E-02	2.39E-02	2.39E-02	2.55E-02	-13.55	-13.55	-7.69
		60%	2%	6.03E-03	4.49E-03	3.33E-03	5.70E-03	-25.54	-44.75	-5.52
			10%	9.72E-03	8.41E-03	6.45E-03	1.13E-02	-13.45	-33.60	15.92
		90%	2%	1.76E-03	1.05E-03	3.73E-04	4.55E-03	-40.30	-78.89	157.73
			10%	3.25E-03	3.19E-03	1.22E-03	9.08E-03	-1.89	-62.35	179.20
	1.0E-05	0%	2%	3.94E-03	3.33E-03	3.33E-03	3.64E-03	-15.48	-15.48	-7.69
			10%	7.27E-03	6.45E-03	6.45E-03	6.71E-03	-11.25	-11.25	-7.69
		60%	2%	1.22E-03	9.81E-04	7.43E-04	1.28E-03	-19.50	-39.02	5.04
			10%	2.82E-03	2.66E-03	2.08E-03	3.64E-03	-5.85	-26.25	28.97
		90%	2%	3.79E-04	3.00E-04	1.12E-04	1.02E-03	-20.80	-70.38	168.52
			10%	1.00E-03	1.17E-03	4.59E-04	2.90E-03	16.50	-54.23	189.24

Table C.3: Comparison between the methods, 2oo3 architecture

Parameter Specification				Approaches				Comparison with IEC in %		
Int.	λ_D	DC	β	IEC 61508	PDS	Rausand	New	PDS	Rausand	New
4380	5.0E-06	0%	2%	9.27E-04	8.89E-04	6.80E-04	7.95E-04	-4.09	-26.70	-14.29
			10%	1.84E-03	2.54E-03	1.48E-03	1.58E-03	37.55	-19.55	-14.29
		60%	2%	3.73E-04	3.35E-04	1.61E-04	3.30E-04	-10.13	-56.73	-11.47
			10%	8.42E-04	1.37E-03	5.00E-04	9.22E-04	62.69	-40.58	9.52
		90%	2%	1.71E-04	1.80E-04	2.65E-05	3.17E-04	5.22	-84.48	85.36
			10%	3.95E-04	8.79E-04	1.13E-04	7.82E-04	122.87	-71.27	98.25
	2.5E-05	0%	2%	1.81E-02	1.35E-02	1.26E-02	1.55E-02	-25.45	-30.22	-14.29
			10%	2.06E-02	1.96E-02	1.52E-02	1.76E-02	-4.56	-26.10	-14.29
		60%	2%	6.84E-03	3.12E-03	2.28E-03	5.18E-03	-54.38	-66.65	-24.27
			10%	8.63E-03	7.96E-03	3.74E-03	7.71E-03	-7.85	-56.63	-10.72
		90%	2%	3.10E-03	9.89E-04	2.25E-04	5.50E-03	-68.12	-92.76	77.45
			10%	4.03E-03	4.47E-03	6.45E-04	7.51E-03	10.96	-83.99	86.58
	1.0E-05	0%	2%	3.20E-03	2.68E-03	2.28E-03	2.74E-03	-16.16	-28.69	-14.29
			10%	4.82E-03	5.77E-03	3.74E-03	4.13E-03	19.60	-22.34	-14.29
		60%	2%	1.24E-03	8.14E-04	4.70E-04	1.01E-03	-34.48	-62.19	-18.48
			10%	2.13E-03	2.85E-03	1.12E-03	2.15E-03	34.05	-47.10	1.33
		90%	2%	5.66E-04	3.68E-04	6.22E-05	1.03E-03	-34.95	-89.01	81.04
			10%	9.94E-04	1.77E-03	2.35E-04	1.92E-03	77.57	-76.42	93.55
8760	5.0E-06	0%	2%	2.72E-03	2.68E-03	2.28E-03	2.51E-03	-1.43	-16.16	-7.69
			10%	4.27E-03	5.77E-03	3.74E-03	3.94E-03	35.15	-12.25	-7.69
		60%	2%	8.09E-04	7.27E-04	4.70E-04	8.07E-04	-10.11	-41.87	-0.15
			10%	1.59E-03	2.41E-03	1.12E-03	1.97E-03	51.74	-29.24	23.79
		90%	2%	2.44E-04	2.37E-04	6.22E-05	6.42E-04	-2.81	-74.49	163.36
			10%	5.51E-04	1.11E-03	2.35E-04	1.57E-03	101.29	-57.42	185.42
	2.5E-05	0%	2%	5.85E-02	4.95E-02	4.83E-02	5.40E-02	-15.39	-17.53	-7.69
			10%	5.92E-02	5.66E-02	4.98E-02	5.47E-02	-4.49	-15.89	-7.69
		60%	2%	1.60E-02	9.41E-03	8.25E-03	1.40E-02	-41.11	-48.40	-12.32
			10%	1.86E-02	1.65E-02	1.06E-02	1.85E-02	-11.16	-42.93	-0.51
		90%	2%	4.49E-03	1.55E-03	6.80E-04	1.12E-02	-65.57	-84.87	150.11
			10%	5.74E-03	5.82E-03	1.48E-03	1.52E-02	1.39	-74.16	164.79
	1.0E-05	0%	2%	9.93E-03	8.97E-03	8.25E-03	9.17E-03	-9.65	-16.97	-7.69
			10%	1.23E-02	1.43E-02	1.06E-02	1.14E-02	16.10	-14.00	-7.69
		60%	2%	2.81E-03	2.03E-03	1.53E-03	2.62E-03	-27.73	-45.58	-6.96
			10%	4.24E-03	5.27E-03	2.75E-03	4.80E-03	24.20	-35.24	13.25
		90%	2%	8.15E-04	5.10E-04	1.61E-04	2.09E-03	-37.40	-80.21	156.12
			10%	1.40E-03	2.25E-03	5.00E-04	3.88E-03	60.33	-64.29	177.02

Table C.4: Comparison between the methods, 1oo3 architecture

Parameter Specification				Approaches				Comparison with IEC in %		
Int.	λ_D	DC	β	IEC 61508	PDS	Rausand	New	PDS	Rausand	New
4380	5.0E-06	0%	2%	1.33E-04	1.12E-04	2.21E-04	2.22E-04	-15.59	67.08	67.70
			10%	6.42E-04	5.49E-04	1.10E-03	1.10E-03	-14.53	70.73	70.83
		60%	2%	7.43E-05	9.38E-05	8.78E-05	1.54E-04	26.28	18.19	107.23
			10%	3.66E-04	3.53E-04	4.38E-04	7.67E-04	-3.55	19.69	109.49
		90%	2%	4.61E-05	5.43E-05	2.19E-05	1.22E-04	17.80	-52.46	164.13
			10%	2.29E-04	2.28E-04	1.10E-04	6.03E-04	-0.15	-52.08	164.01
	2.5E-05	0%	2%	1.24E-03	8.47E-04	1.40E-03	1.51E-03	-31.66	13.27	21.58
			10%	3.66E-03	2.94E-03	5.71E-03	5.79E-03	-19.68	56.17	58.35
		60%	2%	5.22E-04	1.05E-03	4.58E-04	8.39E-04	100.43	-12.24	60.76
			10%	1.96E-03	2.27E-03	2.21E-03	3.89E-03	15.87	12.72	98.82
		90%	2%	2.84E-04	4.81E-04	1.10E-04	7.57E-04	69.41	-61.32	166.76
			10%	1.19E-03	1.32E-03	5.48E-04	3.15E-03	11.37	-53.94	164.60
	1.0E-05	0%	2%	2.94E-04	2.38E-04	4.58E-04	4.64E-04	-18.97	55.73	57.98
			10%	1.31E-03	1.11E-03	2.21E-03	2.21E-03	-15.25	68.70	69.09
		60%	2%	1.56E-04	2.44E-04	1.76E-04	3.11E-04	56.57	13.10	99.46
			10%	7.38E-04	7.56E-04	8.77E-04	1.54E-03	2.34	18.77	108.06
		90%	2%	9.48E-05	1.29E-04	4.38E-05	2.51E-04	36.56	-53.79	164.52
			10%	4.59E-04	4.75E-04	2.19E-04	1.21E-03	3.34	-52.32	164.07
8760	5.0E-06	0%	2%	2.65E-04	2.38E-04	4.58E-04	4.61E-04	-10.25	72.51	73.75
			10%	1.21E-03	1.11E-03	2.21E-03	2.21E-03	-8.29	82.56	82.77
		60%	2%	1.21E-04	1.67E-04	1.76E-04	3.10E-04	37.54	45.72	155.60
			10%	5.88E-04	5.97E-04	8.77E-04	1.53E-03	1.64	49.25	161.21
		90%	2%	5.73E-05	7.57E-05	4.38E-05	2.46E-04	32.09	-23.54	328.99
			10%	2.84E-04	2.92E-04	2.19E-04	1.21E-03	3.03	-22.75	326.31
	2.5E-05	0%	2%	4.70E-03	3.49E-03	4.66E-03	5.07E-03	-25.72	-0.83	7.94
			10%	8.65E-03	7.09E-03	1.29E-02	1.32E-02	-18.09	48.67	52.35
		60%	2%	1.12E-03	2.10E-03	1.03E-03	1.90E-03	87.03	-7.74	69.50
			10%	3.37E-03	4.06E-03	4.50E-03	7.95E-03	20.56	33.58	136.00
		90%	2%	3.75E-04	8.00E-04	2.21E-04	1.83E-03	113.12	-40.97	386.78
			10%	1.49E-03	1.83E-03	1.10E-03	6.57E-03	22.35	-26.62	339.22
	1.0E-05	0%	2%	6.99E-04	5.91E-04	1.03E-03	1.06E-03	-15.44	47.87	51.63
			10%	2.55E-03	2.29E-03	4.50E-03	4.52E-03	-9.95	76.80	77.60
		60%	2%	2.68E-04	4.52E-04	3.61E-04	6.37E-04	68.72	34.54	137.59
			10%	1.20E-03	1.30E-03	1.76E-03	3.08E-03	8.39	47.04	157.61
		90%	2%	1.19E-04	1.93E-04	8.78E-05	5.22E-04	62.44	-26.29	338.09
			10%	5.71E-04	6.21E-04	4.38E-04	2.44E-03	8.77	-23.26	327.97

Appendix D

Supplementary Derivations

This appendix provides some supplementary mathematical derivations for the mean down times due to DU failure for some architectures and kolmogorov differential equations.

D.1 Equivalent MDT

The equivalent MDT are derived in a simple manner in Chapter 4. It has also been shown with Markov analysis [12, 24]. Moreover, they can also be derived based on the approach presented below:

1oo1

The exponential probability density function of 1oo1 architecture is $f(t) = \lambda_{\mathrm{DU}}\mathrm{e}^{-\lambda_{\mathrm{DU}}t}$. Thus, the expected down time given that the architecture is failed at time τ is (see also Figure 4.3)

$$\begin{aligned} E(\tau - t|T \leq \tau) &= \frac{E(\tau - t)}{\mathrm{P}(T \leq \tau)} = \frac{\int_0^\tau (\tau - t) f(t)\mathrm{d}t}{F(\tau)} \\ &= \frac{\int_0^\tau (\tau - t')\lambda_{\mathrm{DU}} e^{-\lambda_{\mathrm{DU}}t}\mathrm{d}t}{1 - \mathrm{e}^{-\lambda_{\mathrm{DU}}\tau}} \\ &= \frac{\lambda_{\mathrm{DU}}\tau + \mathrm{e}^{-\lambda_{\mathrm{DU}}\tau} - 1}{\lambda_{\mathrm{DU}}\left(1 - \mathrm{e}^{-\lambda_{\mathrm{DU}}\tau}\right)} \end{aligned} \tag{D.1}$$

If we take second order Maclaurins series for the numerator and first order for the denominator, we get

$$E(\tau - t|T \leq \tau) \quad \approx \quad \frac{\lambda_{\mathrm{DU}}\tau - \lambda_{\mathrm{DU}}\tau + (\lambda_{\mathrm{DU}}\tau)^2/2}{\lambda_{\mathrm{DU}}^2\tau} = \frac{\tau}{2} \tag{D.2}$$

1oo2

The probability density function for this architecture is $f(t) = 2\lambda_{DU}(e^{-\lambda_{DU}t} - \mathrm{e}^{-2\lambda_{DU}t})$.

$$\begin{aligned}
E(\tau - t|T \leq \tau) &= \frac{E(\tau - t)}{\mathrm{P}(T \leq \tau)} = \frac{\int_0^\tau (\tau - t) f(t)\mathrm{d}t}{F(\tau)} \\
&= \frac{\int_0^\tau (\tau - t')2\lambda_{DU}(e^{-\lambda_{DU}t} - e^{-2\lambda_{DU}t})\mathrm{d}x}{\int_0^\tau 2\lambda_{DU}(e^{-\lambda_{DU}t} - e^{-2\lambda_{DU}t})\mathrm{d}x} \\
&= \frac{2\lambda_{\mathrm{DU}}\tau - \mathrm{e}^{-2\lambda_{\mathrm{DU}}\tau} + 4\mathrm{e}^{-\lambda_{\mathrm{DU}}\tau} - 3}{2\lambda_{\mathrm{DU}}\mathrm{e}^{-2\lambda_{\mathrm{DU}}\tau}\left(\mathrm{e}^{\lambda_{\mathrm{DU}}\tau} - 1\right)}
\end{aligned}$$

If we take third order Maclaurins series for the numerator and second order for the denominator, we get

$$\begin{aligned}
E(\tau - t|T \leq \tau) &\approx \frac{2\lambda_{\mathrm{DU}}\tau - 1 + 2\lambda_{\mathrm{DU}}\tau - (2\lambda_{\mathrm{DU}}\tau)^2/2 + (2\lambda_{\mathrm{DU}}\tau)^3/6 + 4(1 - \lambda_{\mathrm{DU}}\tau + (\lambda_{\mathrm{DU}}\tau)^2/2 - (\lambda_{\mathrm{DU}}\tau)^3/6) + 3}{2\lambda_{\mathrm{DU}}\left(1 - 2(1 - \lambda_{\mathrm{DU}}\tau + (\lambda_{\mathrm{DU}}\tau)^2/2) + (1 - 2\lambda_{\mathrm{DU}}\tau + (2\lambda_{\mathrm{DU}}\tau)^2/2)\right)} \\
&\approx \frac{2(\lambda_{\mathrm{DU}}\tau)^3/3}{2\lambda_{\mathrm{DU}}(\lambda_{\mathrm{DU}}\tau)^2} = \frac{\tau}{3}
\end{aligned} \tag{D.3}$$

We can thus apply a similar procedure to find the MDTs of any architecture.

D.2 Kolmogorov Differential Equations

The following derivations are strongly influenced by [22]. Let

α_i transition rate from state i, or departure rate from state i.

α_{ij} transition rate from state i to j.

P_{ij} the probability that the process makes a transition from state i to j

Then, we have the following relations:

$\alpha_{ij} = \alpha_i P_{ij}$ and $\alpha_i = \sum_j \alpha_i P_{ij} = \sum_j \alpha_{ij} \Rightarrow P_{ij} = \frac{\alpha_{ij}}{\alpha_i} = \frac{\alpha_{ij}}{\sum_j \alpha_{ij}}$

and $\alpha_{jj} = -\alpha_j$

This shows that given the transition rates from i to j, we can determine system performance characteristics.

Consider the following results:

1. $\lim_{\Delta t \to 0} \frac{1-P_{ii}(\Delta t)}{\Delta t} = \alpha_i \quad \Rightarrow \quad 1 - P_{ii}(\Delta t) = \Delta t \alpha_i + o(\Delta t)$
2. $\lim_{\Delta t \to 0} \frac{P_{ij}(\Delta t)}{\Delta t} = \alpha_{ij} \quad \Rightarrow \quad P_{ij}(\Delta t) = \Delta t \alpha_i P_{ij} + o(\Delta t)$ where $i \neq j$
3. $P_{ij}(t+s) = \sum_{k=0}^{\infty} P_{ik}(t) P_{kj}(s)$ for all $s, t \geq 0$ (Chapman-Kolmogorov equation)

Where $o(\Delta t)$ is very small compared to Δt.

A. Kolmogorov Backward Equations

As can be seen from Figure D.1, the probability of being in state j at time $t + \Delta t$ given transition from state i at time 0 is

$$\begin{aligned}
P_{ij}(t+\Delta t) &= \sum_{k=0}^{r} P_{ik}(\Delta t) P_{kj}(t) \\
P_{ij}(t+\Delta t) - P_{ij}(t) &= \sum_{k=0}^{r} P_{ik}(\Delta t) P_{kj}(t) - P_{ij}(t) \\
&= \sum_{\substack{k=0 \\ k \neq i}}^{r} P_{ik}(\Delta t) P_{kj}(t) - (1 - P_{ii}(\Delta t)) P_{ij}(t) \\
&= \sum_{\substack{k=0 \\ k \neq i}}^{r} [\alpha_{ik} \Delta t + o(\Delta t)] P_{kj}(t) - [\alpha_i \Delta t + o(\Delta t)] P_{ij}(t)
\end{aligned}$$

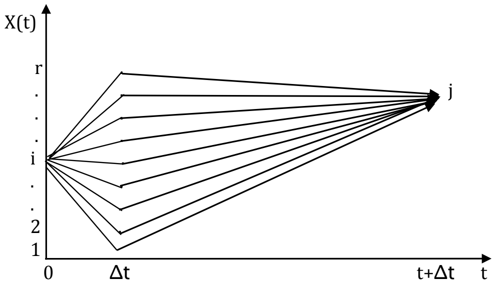

Figure D.1: Markov transition (KBE)

Hence, if we divide both sides by Δt, we get

$$\frac{P_{ij}(t+\Delta t) - P_{ij}(t)}{\Delta t} = \sum_{\substack{k=0 \\ k \neq i}}^{r} \left(\alpha_{ik} P_{kj}(t) + \frac{o(\Delta t)}{\Delta t} \right) - \left(\alpha_i P_{ij}(t) + \frac{o(\Delta t)}{\Delta t} \right)$$

But, $\lim_{\Delta t \to 0} \frac{o(\Delta t)}{\Delta t} = 0$, thus if we take the limit, we get

$$\dot{P}_{ij}(t) = \sum_{\substack{k=0 \\ k \neq i}}^{r} \alpha_{ik} P_{kj}(t) - \alpha_i P_{ij}(t) = \sum_{k=0}^{r} \alpha_{ik} P_{kj}(t) \tag{D.4}$$

B. Kolmogorov Forward Equations

The derivation of KFE is similar with the derivation of KBE, except the initial condition. Thus, we only present the result. The probability of being in state j at time $t + \Delta t$ can be written as (see also Figure D.2)

$$P_{ij}(t + \Delta t) = \sum_{k=0}^{r} P_{ik}(t) P_{kj}(\Delta t)$$

If we following similar procedure as above, we get

$$\dot{P}_{ij}(t) = \sum_{k=0}^{r} \alpha_{kj} P_{ik}(t) \tag{D.5}$$

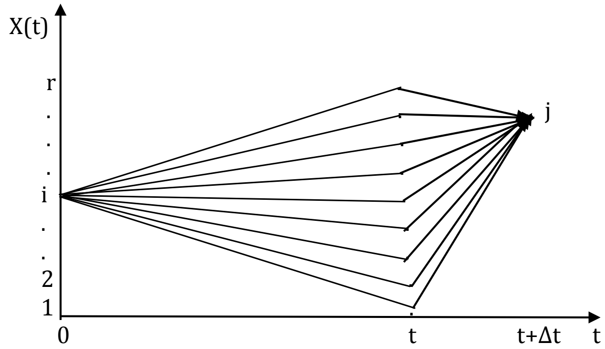

Figure D.2: Markov transition (KFE)

Notice that both (4.37) and (4.38) have the same unique solution.

Bibliography

[1] IEC 60300. *Dependability Management Part 3-1: Application Guide Analysis Techniques for Dependability Guide on Methodology*. International Electrotechnical Commission, Geneva, 2003.

[2] IEC 61025. *Fault Tree Analysis (FTA)*. International Electrotechnical Commission, Geneva, 2006.

[3] IEC 61165. *Application of Markov Techniques*. International Electrotechnical Commission, Geneva, 2006.

[4] IEC 61508. *Functional safety of electrical/electronic/programmable electronic safety-related systems*. International Electrotechnical Commission, Geneva, 2010.

[5] IEC 61511. *Functional safety - Safety Instrumented Systems For the Process Industry sector*. International Electrotechnical Commission, Geneva, 2003.

[6] ISA TR 84.00.02. *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques. Parts 1–5*. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 2002.

[7] Julia V Bukowski. Incorporating process demand into models for assessment of safety system performance. In *Annual Reliability and Maintainability Symposium, 2006. RAMS'06.*, pages 577–581. IEEE, 2006.

[8] Julia V Bukowski. Using markov models to compute probability of failed dangerous when repair times are not exponentially distributed. In *Annual Reliability and Maintainability Symposium, 2006. RAMS'06.*, pages 273–277. IEEE, 2006.

[9] Julia V Bukowski, Jan Rouvroye, and WM Goble. What is PFD$_{avg}$. *Exida library*, 2002.

[10] Haitao Guo and Xianhui Yang. A simple reliability block diagram method for safety integrity verification. *Reliability Engineering & System Safety*, 92(9):1267–1273, 2007.

[11] Haitao Guo and Xianhui Yang. Automatic creation of markov models for reliability assessment of safety instrumented systems. *Reliability Engineering & System Safety*, 93(6):829–837, 2008.

[12] Fares Innal. *Contribution to modelling safety instrumented systems and to assessing their performance Critical analysis of IEC 61508 standard*. PhD thesis, University of Bordeaux, Bordeaux, France, 2008.

[13] Rouvroye J. L. and van den Bliek E. G. Comparing safety analysis techniques. *Reliability Engineering & System Safety*, 75(3):289–294, 2002.

[14] Wei Long, Tie Ling ZHANG, and Masaki Oshima. Quantitative evaluation on safety-related systems. *tc*, 2(1):1–1, 2002.

[15] Mary Ann Lundteigen. *Safety instrumented systems in the oil and gas industry*. PhD thesis, Trondheim: Department of Production and Quality Engineering, 2009.

[16] Mary Ann Lundteigen and Marvin Rausand. Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study. *International Journal of Reliability, Quality and Safety Engineering*, 16(02):187–212, 2009.

[17] Peter Müller and Peter Süderblom. Results of the IEC 61508 functional safety assessment. *Exida*, 2011.

[18] NASA. *Fault Tree Handbook with Aerospace Applications*. NASA Office of Safety and Mission Assurance, Washington DC, 2002.

[19] OLF-070. *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*. The Norwegian Oil Industry Association, Stavanger, Norway, 2004.

[20] Marvin Rausand and Arnljot Høyland. *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley, Hoboken, New Jersey, 2nd edition, 2004.

[21] Marvin Rausand and Jørn Vatn. Reliability modeling of surface controlled subsurface safety valves. *Reliability Engineering & System Safety*, 61(1):159–166, 1998.

[22] Sheldon M. Ross. *Introduction to Probability Models*. Academic Press, 10th edition, 2010.

[23] SINTEF. *Reliability Prediction Methods for safety Instrumented system, PDS Data Handbook*. SINTEF, Trondheim, Norway, 2013 edition.

[24] Tieling Zhang, Wei Long, and Yoshinobu Sato. Availability of systems with self-diagnostic components–applying markov model to iec 61508-6. *Reliability Engineering & System Safety*, 80(2):133–141, 2003.