4

Methods for determining and processing probabilities

PUBLICATIEREEKS
GEVAARLIJKE STOFFEN

VROM

Publication Series on Dangerous Substances 4 (PGS 4)

Methods for determining and processing probabilities

Ministerie van **Binnenlandse Zaken** *en* **Koninkrijksrelaties**

SZW

Ministerie van Verkeer en Waterstaat

Preface

Starting from June 1st 2004, the Advisory Council on Dangerous Substances (Adviesraad Gevaarlijke Stoffen - AGS) was installed by the Cabinet. At the same time the Committee for the Prevention of Disasters (Commissie voor de Preventie van Rampen- CPR) was abolished.

CPR issued several publications, the so-called CPR-guidelines (CPR-richtlijnen), that are often used in environmental permits, based on the Environmental Protection Law, and in the fields of of labour safety, transport safety and fire safety.

The CPR-guidelines have been transformed into the Publication Series on Dangerous Substances (Publicatiereeks Gevaarlijke Stoffen – PGS). The aim of these publications is generally the same as that of the CPR-guidelines. All CPR-guidelines have been reviewed, taking into account the following questions:

1. Is there still a reason for existence for the guideline or can the guideline be abolished;
2. Can the guideline be reintroduced without changes or does it need to be updated.

This fourth publication in the Series on Dangerous Substances (PGS 4) is not different from the former publication CPR 12E, second edition 1997.

Also on behalf of my colleagues at the Ministries of Transport, Social Affairs and of the Interior, The State Secretary of Housing Spatial Planning and the Environment (VROM).

Drs. P.L.B.A van Geel

[december] 2005

Methods for determining and processing probabilities

'Red Book'

CPR 12E

Principal author	J.C.H. Schüller, m.sc.
Co-authors	J.L. Brinkman, m.sc.
	P.J. Van Gestel, m.sc.
	R.W. van Otterloo, m.sc.

NRG

Utrechtseweg 310, 6812 AR ARNHEM
The Netherlands
Tel. +31 26 356 8526
Fax. +31 36 445 9035

This report was prepared under the supervision of the Committee for the Prevention of Disasters and is published with the approval of

The Director-General for Social Affairs and Employment
The Director-General for Environmental Protection
The Director-General for Public Order and Security
The Director-General for Transport

The Hague, 1997

The Director-General for Social Affairs and Employment

Committee for Prevention of Disasters

Second edition 1997

FOREWORD

The report CPR-12E 'Methods for determining and processing probabilities' was first issued in 1988. In the following years the "Red Book" has proven to be a useful tool in risk analysis. However it became apparent certain subjects should be added or should be covered more elaborately and that in some cases less cumbersome methods could be introduced.
In order to improve the usefulness of the "Red Book" NRG was assigned to prepare a complete revision and update with special emphasis on user friendliness. In this second edition NRG has included many improvements which resulted from the experience it gained in using the "Red Book" in risk analysis.

The revision of the "Red Book" was supervised by a committee in which participated:

Dr. E.F. Blokker, chairman	DCMR Environmental Protection Agency Rijnmond
Mr. ir. K. Posthuma, secretary	Ministry of Social Affairs and Employment
Dr. B.J.M. Ale	RIVM National Institute of Public Health and the Environment
Drs. R. Dauwe	DOW Benelux B.V.
Ir. B.W. Moll	Province of Limburg
Ing. A.J. Muyselaar	Ministry of Housing, Spatial Planning and the Environment
Ing. A.W. Peters	Ministry of Transport, Public Works and Water Management
Drs. Ing. A.F.M. van der Staak	Ministry of Social Affairs and Employment
Dr. P.A.M. Uijt de Haag	RVM National Institute of Public Health and the Environment
Ir M. Vis van Heemst	AKZO Engineering B.V.
Ir. J.H. van Zwol	Ministry of Transport, Public Works and Watermanagement, Traffic Research Centre

With the issue of the second edition of the "Red Book" the Committee for the Prevention of Disasters by Hazardous Materials expects to promote the general use of standardised calculation methods in risk analysis.

The Hague, July 4, 1997

THE COMMITTEE FOR THE PREVENTION OF
DISASTERS BY HAZARDOUS MATERIALS,

Drs. H.C.M. Middelplaats, chairman

Contents

5 **RELIABILITY THEORY**

6 **DATA ANALYSIS**

Keyword	**Chapter(s)**
Absorbing state	11
Accident scenario, or accident sequence	7, 10, 12
Accident sequence	7, 10, 12
Action	14
AND gate	8, 9, 12
Annunciator	14
Availability	5, 9
Available component	5, 9
Average unavaifability	5, 9
Basic event	8, 12
Basic human error probability	14
Bayesian statistics	4, 6
Bayesian update	4, 6
Binomial distribution	4
Boolean algebra	8
Bounding analysis	14
Branch point	10, 12
Burden	14
Cause	6, 13
Checklists	7, 12
Chi-square distribution	4
Classification system	14
Cognition	14
Cognitive behaviour	14
Cognitive response	14
Common cause basic event	13
Common cause component group	13
Common cause event	13
Common cause failure analysis	13
Component	6, 13
Component boundaries	6
Component state	6, 13
Conditional event	3, 10, 12, 13
Conditional human error probability	14
Conditional probability	3, 10, 12

Keyword	Chapter(s)
Confidence Interval	4, 6
Consequence	7, 10, 12
Consequence analysis	7, 12
Continuous probability distribution	4, 15
Correlation	4
Coupling mechanism	13
Data bank or data base	6
Dead time	5, 9
Decision making	14
Defensive strategy	13
Degraded	6
Demand	5, 9
Demand rate	5, 9
Demand related failures	5, 9
Dependability	15
Dependent event	3, 13
Derived human error probability	14
Diagnosis	14
Discrete probability distribution	4, 15
Display	14
Disturbance costs	15
Diversity	13
Effect	7, 10, 12
Error	14
Error of commission	14
Error of omission	14
Event	10, 12
Event sequence	10, 12
Event tree	10, 12
Expected number of failures	5, 9
Expected value	4, 5
Exponential distribution	4
F distribution	4
Fail safe	12
Failed state	11

Keyword	Chapter(s)
Failure	5, 6
Failure cause	6, 13
Failure data	6
Failure density	5
Failure mechanism	6
Failure modes	6
Failure modes and effects analysis	7, 12
Failure modes, effects, and criticality analysis	7
Failure occurrence rate	5, 9
Failure of component	6
Failure rate	5, 9
Failure to danger	5, 9
Fault	5
Fault event	8
Fault tree analysis	8
Final element	12
Front line system	12
Functional state	11
Functional testing	5, 9
Functionally unavailable component	6
Gates	8, 12
Gamma distribution	4
General diagnosis	14
Generic data	6
Hazard	7, 12
Hazard and operability analysis	7, 12
Hazard checklist	7
Hazard evaluation	7
Hazard identification	7
Heading event	10, 12
Hesitancy	14
HRA event tree	14
Human cognitive reliability	14
Human error	14
Human error probability	14

Keyword	Chapter(s)
Human factors	14
Human failure event	14
Human reliability	14
Human reliability analysis	14
Impact vector	13
Incipient failure	6
Independent event	3, 13
Initial state	11
Initiating event group	12
Initiation event	10, 12
Instantaneous unavailability	5, 9
Lapse	14
Latent error	14
Lognormal distribution	4
Life cycle costs	15
Maintainability	15
Mean down time	5, 9
Mean time between failure	5, 9
Mean time to failure	5, 9
Mean time to repair	5, 9
Mean value	4, 5
Median	4, 15
Median response time	14
Minimal cut set	8, 9, 12
Mistake	14
Mode of operation	5, 9
Mutually exclusive events	3, 9
Naming conventions	8
Normal distribution	4
Non-restorable system	11
On-line repairable component	5, 9
Operator	14
OR gate	8
Overt faults	5, 9
Performance shaping factors	14

Keyword	Chapter(s)
Periodically tested component	5, 9
Plant specific data	6
Poisson distribution	4
Population	4, 6
Potentially unavailable component	6
Probability	3
Probability density function	4, 15
Probability distribution	4, 6, 15
Probability of failure	5, 9
Probability of failure on demand	5, 9
Procedure	14
Proof testing	5, 9
Qualitative methods	7, 12
Quantitative methods	7, 12
Quantitative risk analysis	7, 12
RAM program	16
Rare event	8, 9
Recovery	14
Recovery error	14
Redundancy	12
Reliability	5, 9
Repair rate	5, 9
Restorable system	11
Root cause	13
Safety system	12
Scenario	7, 10, 12
Shock	13
Slip	14
Spurious trip	12
Standard deviation	4, 6
Standardized normal distribution	4
State description	11
State label	11
State symbol	11
Stochastic Variable	4, 11

Keyword	**Chapter(s)**
Stress	14
Stressor	14
Success criteria	12
Success likelihood index methodology	14
Support system	12
System	8
System boundaries	8
System initiator	12
System state	11
Task	14
Task analysis	14
Time related failures	5, 9
Time reliability correlation	14
Top event	8, 12
Top logic	12
Transition	11
Transition arrow	11
Transition probability	11
Trigger event	13
Unavailability	5, 8, 9
Unavailable component	6
Unbiased estimator	4
Undeveloped event	8
Unit	11
Uniform and loguniform distribution	4
Unreliability	5, 8, 9
Variance	4, 6
Vigilance	14
Violation	14
Weibul distribution	4

INTRODUCTION

CONTENTS page.

1.1 INTRODUCTION

The operation of (Petro)-Chemical facilities, oil and gas production and nuclear power plants are not possible without acceptance of a certain risk. Risk due to a specific activity can be defined as a measure of an undesired event in terms of both the incident probability and the magnitude of the undesired consequence. In estimating risk, assessments need to be made of the magnitude or severity of the undesired consequence and of the probability of occurrence of this consequence.

In the past various types of analysis techniques have been developed to assess risk. It is important to make distinction between qualitative and quantitative risk analyses techniques. A qualitative technique is based on the experience build up in a certain field of application. Based on this experience one is able to make an assessment about the acceptability of the risk involved in the operation of a certain plant. In a quantitative risk assessment one trien to assess the risk in numerical values; the magnitude of the consequence, e.g. number of casualties and the probability of occurrence.

When a quantitative risk analysis (QRA) is used to assess the risk, risk analysis sets out to answer three questions.

- What can go wrong?

- What is the probability that it will go wrong?

- What are the consequences?

To answer the first question a Hazard identification study has to be performed. Such a study results in the identification of undesired events and the mechanisms by which they occur. For instance potential releases to the environment of Hazardous material.

In a quantitative risk assessment the event sequences that lead to undesired consequences have to be developed.The first event in such a sequence is called the initiating event which can be a pipe or a vessel break or a plant upset or a human error. An important part of a QRA is to calculate the probability of occurrence of each accident sequence which leads to an undesired consequence.

By applying physical models the magnitude of the undesired consequences, i.e. the potential physical effects of the undesired event and the potential damage caused by the undesired consequence have to be calculated.

In all three aspects of consequence analysis; magnitude undesired consequence, potential physical effect and potential damage, probability plays an important role. For instance, depending on the weather conditions, the consequence of the release of a Hazardous material can be more or less severe. Probabilities of occurrence of a limited number of different weather conditions have to be assessed to obtain a realistic picture of the physical effect of the release. Another example is that the physical processes which might occur after the release are not certain. The probabilities of occurrence of each of the potential processes have to be taken into account.

A risk analysis is usually organized on the basis of the diagram in figure 1.1 and consists of:

a: identification of potential undesired events
b: determination of the potential physical effects of these events
c: determination of the damage which can be caused by these effects
d: determination of the probability of occurrence of the undesired consequence, composed of:
- the probability of occurrence of the undesired event
- the probability that the undesired event will lead to the physical effect
- the probability that the physical effect will lead to the damage.

e: calculation of the risk
f: evaluation of the risk.

To create a basis for risk evaluation, the Risk Evaluation Subcommittee organized several studies on various aspects of risk, the result being three books:

Methods for the calculation of physical effects resulting from releases of hazardous materials (liquids and gases), The report is issued by the Secretary of Labour and is known as the “Yellow Book”, reference [1.6].

Methods for Determining of Possible Damage to People and Objects Resulting from Releases of Hazardous Materials (Green Book), The report is also issued by the Secretary of Labour and is known as the “Green Book”, reference [1.5].

The purpose of this book, known as the “Probability Book or Red Book” is to detail methods for determining the probability of undesired events, the effects they cause and any damage which may develop from those effects.

Together with the other two books above, the Probability Book forms a basis for quantitative considerations on the risk caused by an undesired event.

The Probability Book is therefore linked to the book on “Methods for calculating the physical effects of incidental release of hazardous substances” (Yellow Book) but there is a major difference between the two books; the effects dealt with in the “Yellow Book” are dictated by the laws of physics and chemistry. These can give rise to very complicated phenomena, some of which cannot yet be described mathematically but can be observed objectively, are reproducible and thus accessible to calculation

The Probability Book, on the other hand. Deals with the determination of the probability of events in the future on the basis of data from the past and assumptions. Though this determination makes extensive use of mathematical and statistical calculation methods, the basis is always formed by data and assumptions and these inevitably contain some degree of uncertainty and subjectivity. Subjectivity of the data is introduced because there must always be a decision on which data are relevant and must be considered and which data can be disregarded. Assumptions are treated as subjective by definition.

1.2 HOW TO USE THIS DOCUMENT

This document consists of a number of chapters. Each chapter is dealing with a specific subject of risk and reliability analyses.

The various chapters can be divided in a number of categories. These categories are:

- Basic knowledge
- Hazard identification and identification of failure scenario's or accident sequences
- Model development
- Quantification
- Evaluation
- Special topics.

In table 1.1 a cross reference is provided between the categories listed above and the chapters in this document.

Basic knowledge:

Performing risk and reliability analyses requires some basic knowledge of the concept of probability and the rules which can be used to combine probabilities. These issues are explained in chapter 3 "Probability Theory".

To quantify the probability of an undesired event failure data extracted from operational experience is used very often. To process these failure data from operational experience one must be familiar with some statistical concepts and probability density functions Probability density functions also play an important role in uncertainty analyses. The statistical concepts which play an important role in risk and reliability analysis are explained in chapter 4 "Statistics".

To be able to construct a model which represent a failure scenario or an accident sequence one must be familiar with a number of component failure models and the concepts of unavailability and unreliability. Well-known models are the on-line repairable component failure model, the stand by model and the failure on demand model. All three models, unavailability, unreliability and supporting background are explained in chapter 5 "Reliability Theory".

Hazard identification and development of failure scenario's or accident sequences:

An important aspect of a risk analysis is the identification of events which can initiate a failure scenario or an accident sequence. For this reason these events are called initiating events. Examples of initiating events are a pipe break, a vessel breach, a plant upset or a human error. It is possible that an undesired consequence can result from an initiating event directly but for most industrial facilities not only the initiating event must occur but also one or more intermediate events before an undesired consequence, e.g. a release of Hazardous material, will take place.

Model development:

After identification of all potential initiating events and development of the failure or accident sequence scenario's a model has to be constructed to be able to quantify the probability of occurrence in the period of one year of the undesired consequences. To construct a model different ways can be followed depending on the required degree of detail and preferences of the analyst.

One of the possibilities is to construct a fault tree which describes all credible ways in which the accident sequence can occur. Such a fault tree contains as basic events: the initiating event, all intermediate events, human errors and dependent failures. The basic events have to be combined in the right way with "AND" and "OR" gates. Solving the fault tree results in a number of accident sequence cut sets. Each minimal cut set describes the smallest combination of initiating event, component failures, human failures and dependent failures which, if they all occur will cause the accident sequence to occur.

If one is interested in the whole spectrum of undesired consequences, given an initiating event, one has to use the event tree modelling technique. It might be the case that the probability of occurrence of one or more intermediate events can be extracted directly from operational experience or can be estimated directly based on expert opinion. If the probability of occurrence of all events defined in the event tree can be estimated directly, quantification of the event tree is easy. If the probability of occurrence of one or more of the intermediate events have to be determined by the use of fault trees it is recommended to use a special purpose computer code (see section 1.7). The most sophisticated modelling technique which makes use of the event tree technique is described in chapter 12 "Accident Sequence Development and Quantification".

Another possibility to model accident sequences is to make use of Markov processes. Especially if one is interested in the time dependant behaviour of the probability of occurrence of an undesired event, the Markov modelling technique is very suitable. The main disadvantages of the Markov technique are the difficulty to understand the model and the increase in system states if the number of components is increasing. The Markov technique is explained in chapter 11.

One of the modelling techniques which is not treated in this document is the Monte Carlo simulation technique. For a short description of this technique the reader is referred to chapter 15 "Uncertainty, Sensitivity and Importance Analysis".

To model specific issues like human failures and dependent failures the techniques presented in chapter 13 “Dependent Failure Analysis” and chapter 14 “Human Failures” have to be applied.

Quantification:

One of the main issues in the quantification process is the failure data which have to be used. In chapter 6 “Data Analysis” it is explained how to generate plant specific data, how to use generic data and how to combine these two main sources of data with the Bayesian update technique.

If one did use the fault tree modelling technique, whether in combination with the event tree technique or not one has to quantify a number of minimal cut sets. To quantify minimal cut sets one can make use of the quantification techniques described in chapter 9 “Quantification of minimal cut sets” or to model each minimal cut set with a separate Markov diagram “Markov cut set approach”.
Another possibility is to set up a computer simulation process for each minimal cut set (“Monte Carlo simulation technique”).

To quantify human failures and dependent failures the quantification techniques presented in chapter 13 “Dependent Failure Analysis” and chapter 14 “Human Failures” have to be used.

Evaluation:

Evaluation of the results of the quantification process consists of the determination of the dominant contributors in the probability of occurrence of the undesired consequence. This can be an initiating event, a component failure, a human failure or a dependent failure or the probability of occurrence of a physical process given a specific failure scenario.

A sensitivity analysis can be performed to determine how sensitive the results are for input parameter variations. Mostly a sensitivity analysis is performed by changing the input parameter under consideration and performance of a requantification.

An uncertainty analysis is recommended if one is interested in the spread of the results as a function of the uncertainty in the input parameters. This type of analysis is mostly performed by defining a number of probability density distributions for the most important input parameters and performance of a Monte Carlo calculation. The result is a probability density distribution of the probability of occurrence in the period of one year of the undesired consequence.

An importance analysis gives the influence of a specific failure event in the overall result. This is done by assuming the probability of occurrence of one specific failure event to be either one or zero. Both assumptions results in a change in the probability of occurrence of the undesired event. By ranking of these changes, an importance list is generated.

It should be emphasized that the results of an importance analysis for one specific failure event are only valid for the event under consideration by assuming all input parameters of the other components unchanged.

The uncertainty, sensitivity and importance analysis are documented in chapter 15.

Special topics:

One of the special topics in this document is the application of Reliably Availability and Maintainability Specification (RAM specification). Such a specification is useful if one has the intention to order a product which has to fulfil specific reliability, availability or maintainability goals. The potential producer of such a product knows exactly what is expected and is able to generate a competitive design. A RAM specification can also serve as a basis for discussions between the buyer and the producer concerning reliability, availability and maintainability issues. For RAM specification see chapter 16.

Structuring of maintenance is an activity intended to focus maintenance resources on those components that dominate the overall performance of a plant in terms of production loss, safety, and maintenance costs. Distinction has to be made in qualitative and quantitative analyses. The qualitative analysis results in a list of maintenance activities, recommended modifications and staff instructions, including a priority list for all three of them. The next step is to examine the recommendations from the list on their technical and practical feasibility. Subsequently, the feasibility options are subjected to financial scrunity. The financial viability of certain items is assessed as part of the quantitative analysis.

1.3 REFERENCES

[1.1] Premises for Risk Management, Dutch National Environmental Policy Plan, Ministry of Housing, Physical Planning and Environment, Department for Information and International Relations, P.O. Box 20951, 2500 EZ The Hague, VROM 00197/4-90.

[1.2] Risk Assessment in the Process Industries, Second Edition, Edited by Robin Turney and Robin Pitblado, Institute of Chemical Engineers, Davis Building 165-189 Railway Terrace, Rugby, Warwickshire CV213HQ, UK, ISBN 0 85295 323 2.

[1.3] Procedures for conducting probabilistic safety assessments of nuclear power plants (Level I), IAEA safety series No. 50-P-4.

[1.4] Handleiding voor het opstellen en beoordelen van een extern veiligheidsrapport (EVR), Interprovinciaal overleg IPO, Floris Grijpstraat 2, Postbus 97728, 2509 GC Den Haag.

[1.5] Methods for Determining of Possible Damage to People and Objects Resulting from Releases of Hazardous Materials (Green Book), CPR 16E, 1989,
Committee for the Prevention of Disasters, Directorate-General of Labour of the Ministry of Social Affairs, The Hague.

[1.6] Methods for the calculation of physical effects resulting from releases of hazardous materials (liquids and gases), (Yellow book), CPR 14E, Second Edition 1992, Committee for the Prevention of Disasters, Director-General of Labour of of the Ministry of Social Affairs, The Hague.

Figure 1.1: Risk analysis diagram.

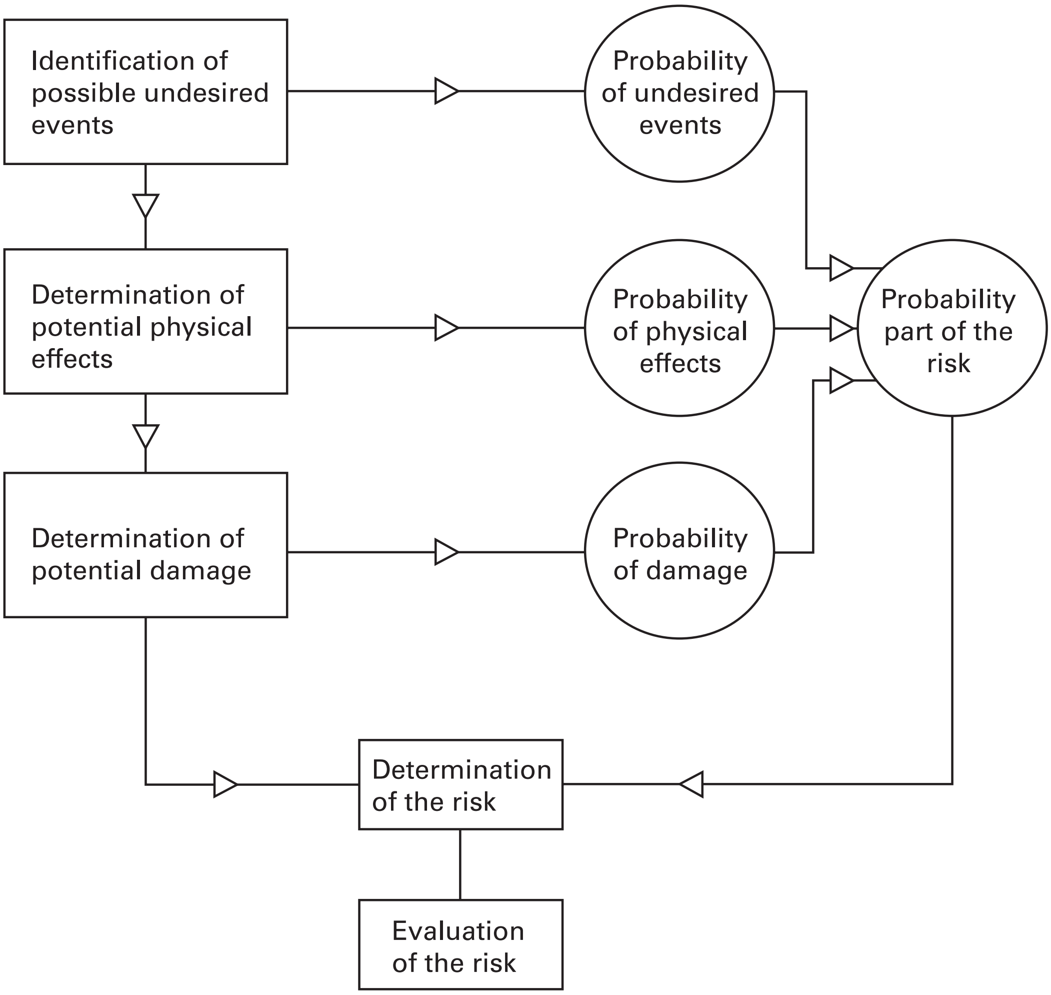

Identification of possible undesired events
Probability of undesired events
Determination of potential physical effects
Probability of physical effects
Probability part of the risk
Determination of potential damage
Probability of damage
Determination of the risk
Evaluation of the risk

Table 1.1: Subjects risk and reliability analyses and related chapters.

No.	Subject	Related chapter
1	Basic knowledge	Ch. 2: Definitions Ch. 3: Probability Theory Ch. 4: Statistics Ch. 5: Reliability Theory
2	Hazard identification and development of failure scenario's	Ch. 7: Methods of identification of failure scenario's Ch. 10: Event Tree Analysis
3	Model development	Ch. 8: Fault Tree Analysis Ch. 11: Markov Processes Ch. 12: Accident Sequence Development and Quantification* Ch. 13: Dependent Failure Analysis Ch. 14: Human Failures
4	Quantification	Ch. 6: Data Analysis Ch. 9: Quantification of minimal cut sets Ch. 11: Markov Processes Ch. 12: Accident Sequence Development and Quantification* Ch. 13: Dependent Failure Analysis Ch. 14: Human Failures
5	Evaluation of the results	Ch. 15: Uncertainty, Sensitivity and Importance Analysis
6	Special Topics	Ch. 16: Reliability Availability and Maintainability Specification Ch. 17: Maintenance Optimization

*: Only for sophisticated risk analyses in which the complete spectrum of all potential undesired consequences have to be taken into account.

DEFINITIONS

CONTENTS **page**

2.1 INTRODUCTION

In order to understand the methodology in this document, it is useful to summarize the terms and definitions. The intention of this chapter is not to provide a comprehensive international accepted set of definitions but to provide concise definitions to achieve understanding of the terms used in this profession.

2.2 PROBABILITY THEORY

Conditional probability P(A|B):
The conditional probability of event A, given event or information B, is the probability of event A occurring, whereby data are available that event B has occurred or information B is valid.

Dependent event:
If an event is not independent, it is defined as a dependent event. Two events, A and B, are dependent only if

$$P(A|B) \neq P(A)$$

$$P(B|A) \neq P(B)$$

As a result this means:

$$P(A \text{ and } B) = P(A) \cdot P(B|A) = P(B)\ P(A|B) \neq P(A) \cdot P(B)$$

Independent event:
Two events A and B are called independent if the probability of A is not affected by whether B occurs or not or an independent event is an event in which a component state occurs, causally unrelated to any other component state. Two events, A and B, are independent if and only if:

$$P(A|B) = P(A)$$

$$P(B|A) = P(B)$$

As a result this means:

$$P(A \text{ and } B) = P(A) \cdot P(B).$$

Mathematical probability theory:
A branch op pure mathematics based on definitions and axioms which are independent of the interpretation of the concept of probability. In practical applications where an interpretation of the probability concept is given, the definition and axioms of mathematical probability theory must be satisfied.

Mutually exclusive events:
Events A and B are mutually exclusive if $P(A \cap B) = 0$ applies.

Probability:
The probability P is a function of a set S to R (R is the set of real numbers). Probability meets the following four fundamental axioms of Kolmogorow:

1: The probability that an event A occurs is a number between zero and unity:

$$0 \le P(A) \le 1$$

2: The probability of a certain event is unity:

$$P(S) = 1$$

3: The probability of the union or sum of the disjoint or mutually exclusive events is: n

$$P(\cup_{i=1}^{n} F_i)\sum_{1}^{n} P(F_i)$$

For two events A and B this formula is:
If $A \cup B = 0$ then $P(A \cup B) = P(A) + P(B)$

4: For all i:

$$F_i \supseteq F_{i+1} \text{ and } \bigcap_{1}^{\infty} F_i = 0 \text{ then } \lim_{i \to \infty} P(F_i) = 0$$

2.3 STATISTICS

Bayesian statistics:
Bayesian statistics is the branch of statistics based on the subjective interpretation of the concept of probability. Probability is regarded as a subjective measure of the belief that a specific event will occur.

Confidence interval:
A confidence interval for a(n) (unknown) parameter is an interval with limits determined in such a way that the probability that this interval contains the (unknown) parameter is equal to a pre-determined value.

Continuous probability distribution:
A probability distribution $F(x) = P(\underline{x} < x)$ where $\underline{x}$ can assume a continuous range of values.

Correlation:
A measure of the interdependence of two statistical variables.

Discrete probability distribution f(x):
A probability distribution $P(\underline{x} = x)$ where $\underline{x}$ can assume a denumerable set of values.

Expected value E(x) or mean value *μ* of a stochastic variable x:
The expected value $E(\underline{x})$ of the stochastic variable $\underline{x}$ is:

- if x has a continuous probability distribution f(x):

$$\mu = E(\underline{x}) = \int_{-\infty}^{+\infty} x\ f(x)\ dx$$

- if x has a discrete probability distribution $f(x_i)$:

$$E\ (\underline{x}) \sum_{i} \quad x_i\ f(x_i)$$

Median:
The value of x for which the distribution function F(x) = 0.5.

Population:
A population is a set of elements satisfying a specific description.

Probability distribution F(x):
The probability distribution of a stochastic variable x means the set of all values x which can assume with the related probabilities $P(\underline{x} \leq x)$.The function $F(x) = P(\underline{x} \leq x)$ is called the distribution function.

Probability density function f(x):
If the distribution function F(x) of the probability distribution f(x) can be written as:

$$F(x) = \int_{-\infty}^{x} f(x)\ dx$$

then f(x) is called probability density function.

Standard deviation:
The standard deviation 6 is the square root of the variance σ^2.

Stochastic variable:
A stochastic variable is a value which, in a given situation, can adopt different values for which it has a probability distribution. It cannot be predicted with certainty what the value of that variable wilt be. A stochastic variable is indicated in this book by underlining the symbol.

Unbiased estimator:
An estimator is unbiased if its expected value is equal to the value of the unknown parameter.

Variance σ^2 or Var (x):
The variance Var($\underline{x}$) or σ^2 of a stochastic variable $\underline{x}$ is:

$$\mathrm{Var}(\underline{x}) = E\left((\underline{x} - \mu)^2\right)$$

or, in other words, this is the expectation of the squared deviation of $\underline{x}$ compared with μ (here $\mu = E(\underline{x})$).

2.4 RELIABILITY THEORY

Availability A(t):
Availability can be defined in two ways:

Definition 1:
The probability that the component is normal at time t, given that it was as good as new at time zero.

Definition 2:
Availability is the fraction of the time period of length T during which the component can perform its required function.

Given the definitions of availability and unavailability the following equation holds:

$$A(t) = 1 - U(t)$$

Average unavailability or probability of failure on demand:
Two different definitions exist for average unavailability. The first definition concerns the average unavailability over a time period of length T or time-average unavailability, and the second definition concerns the limiting average unavailability.

Time-average value:

$$U = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} U(t)\, dt$$

Limiting average value:

$$U = \lim_{t \to \infty} \frac{1}{t} \int_0^t U(t)\, dt$$

Dead time:
The time during which a system or component is not functioning is called dead time.

Demand:
A signal or action that should change the state of a system or a device.

Demand rate:
The number of demands divided by the total elapsed operating time during which the demands occur.

Demand related failures:
Failure of the component due to actuation of the component independent of any exposure times. The probability of failure is independent of any exposure time period, such as the test period or the time the component has existed in stand by.

Expected number of failures in time period (0,t): N(0,t):
The expected number of failures in a certain time period can be obtained by integration of the failure occurrence rate:

$$N(0,t) = \int_0^t \omega\,(\delta)\, d\delta$$

Failure:
A system or component failure occurs when the delivered service deviates from the intended service.The cause of an failure is a fault, which resides, temporarily or permanently in the system or component.

Failure to danger:
An equipment fault which inhibits or delays actions to achieve a safe operational state should a demand occur.The fait-to-danger fault has a direct and detrimental effect on safety.

Failure rate: λ(t)
The small quantity $\lambda(t).dt$ is the probability that the component experiences a failure between t and t + dt, given that the component has survived to time t.

$$\lambda(t)\ dt = P\ [\text{failure occurs between t and t + dt} \mid \text{no prior failure}]$$

Failure density: f(t)
The small quantity f(t).dt is the probability that the component experiences a failure for the first time between t and t + dt, given no failure at time zero.

$$f(t)\ dt = P[\text{first failure occurs between } t \text{ and } t + dt \mid \text{no failure at time zero}]$$

Failure occurrence rate: ω(t)
The small quantity ω(t).dt is the probability that the component experiences a failure between t and t + dt, not necessarily for the first time, given no failure at time zero.

$$\omega(t)\ dt = P[\text{failure occurs between } t \text{ and } t + dt \mid \text{no failure at time zero}]$$

Fault:
The cause of a failure is a fault which resides, temporarily or permanently in the system. Faults can be classified as detected (revealed, overt) or undetected (unrevealed, covert).

Functional testing:
Periodic activity to verify that the system is operating, by testing of the whole system.

Instantaneous and average unavailability:
Dealing with unavailability or probability of failure on demand, one has to make a clear distinction between average values and point-wise or instantaneous values. If unavailability or probability of failure on demand is mentioned as such, the average value is meant in most cases.

- Instantaneous unavailability or probability of failure on demand at time t, U(t) is the probability that the component at time t is not able to operate if called upon.

- Average unavailability U or probability of failure on demand PFD is the time-average probability that the component is not able to operate if called upon.

Mean down time: (MDT)
The mean down time (MDT) is equal to the fraction of the period observed during which the system cannot perform its function.

Mean time between failure (MTBF):
For a stated period in the life of a functional unit, the mean value of the length of time between consecutive failures under stated conditions.

Mean time to failure (MTTF):
The mean time to the occurrence of a component or system failure measured from t=0.

Mean time to repair (MTTR):
The mean time taken to identify the location of a fault and to repair that fault.

Mode of operation:
The way in which a safety-related system is intended to be used with respect to the frequency of demands made upon it in relation to the proof test frequency. The modes of operation are classified as follows:

- *Demand mode:*
  Where the frequency of demands for operation made on a safety-related system is less than the proof check frequency.

- *Continuous/High demand mode:*
  Where the frequency of demands for operation made on a safety-related system is significantly greater than the proof check frequency.

On-line repairable component:
In case of a on-line repairable component repair of the system is started immediately after occurrence of a failure. Logistic time and waiting time are considered to be part of the repair duration.

Overt faults:
Faults that are classified as announced, detected, revealed, etc.

Periodically tested component:
Periodically tested components are usually in a stand-by mode of operation and can be unavailable due to unrevealed faults. To identify an unrevealed fault these type of components have to be tested periodically.

Probability of Failure:
The probability of failure is the probability that, under stated conditions, a system or a component will fail within a stated period of time. Probability of failure is identical to unreliability.

Probability of failure on demand PFD(t):
The probability of failure on demand is defined as the probability that the component is down at time t and unable to operate if called upon. The average probability of a system failing to respond to a demand in a specified time interval is referred to as PFDavg.

Proof testing:
Periodic test performed on the safety-related system. These tests are performed to detect failures in the safety system so that the system can be restored to an ”as new” condition or as close as practical to this condition.

Time related failures:
Time related failure of a component is a failure where the failure is directly related to the exposure time of the component.

Repair rate: μ(t)
The small quantity μ(t).dt is the probability that the component is repaired between t and t + dt, given that the component is under repair until time t.The repair rate is the same type of parameter as the failure rate. But the failure rate is applicable to the failure process and the repair rate is applicable to the repair process.

Reliability R(t):
The probability that the component experiences no failure during the time interval (0,t), given that the component was as good as new at time zero. Reliability is sometimes also called probability of survival. Given the definitions for reliability and unreliability the following equations holds:

$$R(t) = 1 - F(t)$$

Unreliability F(t):
The probability that the component experiences the first failure during the time interval (0,t), given that the component was as good as new at time zero. Reliability as welt as unreliability are probabilities which imply that the associated values must lie between zero and one and are dimensionless. Given the definitions for reliability and unreliability the following equations holds:

$$F(t) = 1 - R(t)$$

Unavailability U(t):
Also, the unavailability can be defined in two different ways:

Definition 1:
Unavailability is the probability that the component is down at time t and unable to operate if called upon.

Definition 2:
Unavailability is the fraction of the time period of lengthT during which the component cannot perform its required function.

Given the definitions for availability and unavailability the following equation holds:

$$U(t) = 1 - A(t)$$

2.5 DATA ANALYSIS

Available component:
The component is available if it is capable of performing its function according to a specified success criterion.

Bayesian update:
Bayesian update is a method of using additional failure data to an existing failure data set.

Component:
A component is an element of plant hardware designed to provide a particular function. Its boundaries depend on the level of detail chosen in the analysis. The hierarchy of the level of detail of modelling a plant in risk and reliability analysis flows from plant, to system, to subsystem, to component, then to failure cause (see definition below). For system modelling purposes, a component is at the lowest level of detail in the representation of plant hardware in the models. Events that represent causes of one or more component states in a system logic model (e.g., fault tree) are found at the level of detail below component.

Active component (Dynamic component):
An active component contributes in a more dynamic manner to the functioning of its parent system by modifying system behaviour in some way. A valve which opens and closes, for example, modifies the system's fluid flow, and a switch has a similar effect on the current in an electrical circuit. Examples of active components are: relays, resistors, pumps, and so forth. An active component originates or modifies a signal. Generally, such a component requires an input signal or trigger for its output signal. In such cases the active component acts as a "transfer function", a term widely used in electrical and mathematical studies. If an active component fails, there may be no output signal or there may be an incorrect output signal.

Passive component (quasi-static component):
A passive component contributes in a more or less static manner to the functioning of the system. Such a component may act as a transmitter of energy from place to place (e.g., a wire or bus-bar carrying current or a steam line transmitting heat energy), or it may act as a transmitter of loads (e.g., a structural member). Examples of passive components are: pipes, bearings, weids, and so forth. A passive component can be considered as the transmitter of a "signal". The physical nature of this "signal" may exhibit considerable variety; for example, it may be a current or force. A passive component may allo be thought of as the "mechanism" (e.g., a wire) whereby the output of one active component becomes the input to a second active component. The failure of a passive component will result in the non-transmission (or, perhaps, partial transmission) of its "signal".

Component boundaries:
Component boundaries define what is included in a component failure. Example: Pump fails to start includes the pump and its driver, but not electric power.

Component state:
Component state defines the component status in regard to the function that it is intended to provide. In this context, the following two general categories of component states are defined; available and unavailable.

Data bank or data base:
A data bank is a collection of data relating to one or more subjects.

Degraded:
The component is in such a state that it exhibits reduced performance but insufficient degradation to declare the component unavailable according to the specified success criterion. Examples of degraded states are relief valves opening prematurely outside the technical specification limits but within a safety margin and pumps producing less than 100% flow but within a stated performance margin.

Failure:
Failure of a component or system is termination of the ability to perform a function.

Failure cause:
These are the conditions during design, manufacture or use which have resulted in failure (for example, incorrect material selection).

Failure of component:
The component is not capable of performing its specified operation according to a success criterion. In order to restore the component to a state in which it is capable of operation, some kind of repair or replacement action is necessary. Additionally, the event may also be considered a failure when a component performs its function when not required or performs its function as required, but does not stop operating once meeting its success criteria. The latter is equivalent to saying that stopping when required is part of the success criterion. Therefore, failure encompasses functioning when not required, as well as not functioning when required.

Failure data:
Failure data are data relating to failure of a system, component or human action.

Failure mechanism:
This is the physical, chemical or mechanical process resulting in failure (for example, corrosion).

Failure modes:
Failure mode describes how the component fails leading to the top undesired event. Example: valve fails to open on demand and valve faits to remain open are two different failure modes of the same component.

Functionally unavailable component:
The component is capable of operation, but the function normally provided by the component is unavailable due to lack of proper input, lack of support function from a source outside the component (i.e., motive power, actuation signal), maintenance, testing, the improper interference of a person.

Generic data:
Data that are built using inputs from various literature sources and commercial databases.

Incipient:
The component is in a condition that, if left unremedied, could ultimately lead to a degraded or unavailable state. An example is the case of an operating charging pump that is observed to have excessive lube oil leakage. If left uncorrected, the tube oil could reach a critical level and result in

severe damage to the pump. A key to distinguishing between degraded and incipient conditions is the knowledge that an incipient condition has not progressed to the point of a noticeable reduction in actual performance, as is the case with a degraded condition. It is important to recognize that potentially unavailable is not synonymous with hypothetical. Both incipient and degraded conditions are indicative of observed, real component states that,without corrective action, would likely lead to unavailable component states.

Plant specific data:
Failure rate data generated from collecting information on equipment failure experience at a specific plant.

Potentially unavailable component:
The component is potentially unavailable if the component is capable of performing its function according to a success criterion, but an incipient or degraded condition exists. Sometimes, although a given success criterion has been met and the component has performed its function according to the success criterion, some abnormalities are observed that indicate that the component is not in its perfect or nominal condition. Although a component in such a state may not be regarded as unavailable, there may exist the potential of the component becoming unavailable with time, other changing conditions, or more demanding operational modes. Events involving these potentially unavailable states provide valuable information about causes and mechanisms of propagation of failures and thus should not be ignored. The concept of potentially unavailable states also serves a practical need to enable the consistent classification of "grey area" cases and difficult-to-classify situations.

Unavailable component:
The component is unable to perform its intended function according to a stated success criterion. It is important to note that the success criterion defined by the analyst to enable him to distinguish between available and unavailable states is not unique. This is because there are cases of several functions and operating modes for a given component, each with a different success criterion. Also, a given event in one plant may be classified differently for a similar component in another plant with different success criteria. Therefore, the specification and documentation of the success criteria and the reconciliation of potential mismatches between the data base and systems models become important tasks of the systems analyst. Two subsets of unavailable states are failure and functionally unavailable. Note that "unavailable" should not be confused with "unavailability".

2.6 METHODS OF IDENTIFICATION OF FAILURE SCENARIOS

Accident scenario, or accident sequence:
An unplanned event or sequence of events that result in undesirable consequences. The first event in an accident sequence is called the initiating event.

Checklists:

Operational checklists:
A detailed list of desired system attributes or steps for a system or operator to perform. Usually

written from experience and used to assess the acceptability or status of the system or operation compared to established norms.

Hazard checklist:
An experience-based list of possible failures of components/systems or human failures to stimulate the identification of hazardous situations for a process or operation.

Consequence analysis:
The analysis of the consequence of incidents outcome cases independent of frequency or probability.

Effect:
An effect is the physical and/or chemical result of an event.

Failure modes and effects analysis (FMEA):
A systematic, tabular method for evaluating and documenting the causes and effects of known types of component failures.

Failure modes, effects, and criticality analysis (FMECA):
A variation of FMEA that includes a quantitative estimate of the significante of consequence of a failure mode.

Hazard:
An inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment.

Hazard evaluation:
The analysis of the significance of hazardous situations associated with a process or activity. Uses qualitative techniques to pinpoint weaknesses in the design and operation of facilities that could lead to accidents.

Hazard identification:
The pinpointing of material, systems, process, and plant characteristics that can produce undesirable consequences through the occurrence of an accident.

Hazard and operability analysis (HAZOP):
The analysis of significance of hazardous situations associated with a process or activity. Uses qualitative techniques to pinpoint weakness in the design and operation of facilities that could lead to accidents.

Qualitative methods:
Methods of design and evaluation developed through experience and/or application of good engineering judgement.

Quantitative methods:
Methods of design and evaluation based on numerical data and mathematical analysis.

Quantitative risk assessment (QRA):
The process of hazard identification followed by numerical evaluation of incident effects and consequences and probabilities, and their combination into overall measures of risk.

Scenario:
The arrangement and sequence of all relevant events which can take place after the occurrence of a selected event is called the scenario.

2.7 FAULT TREE ANALYSIS

AND Gate:
An ”AND”-gate in a fault tree requires the occurrence of all input events to make the output events take place.

Basic event:
An event in a fault tree that represents the lowest level of resolution in the model such that no further development is necessary (e.g., equipment item failure, human failure, or external event).

Boolean algebra:
A branch of mathematics describing the behaviour of linear functions of variables which are binary in nature: on or off, open or closed, true or false. All coherent fault trees can be concerted into an equivalent set of Boolean equations.

Fault event:
A failure event in a fault tree that requires further development.

Fault tree:
A logic model that graphically portrays the combinations of failures that can lead to a specific main failure or accident of interest called the top event.

Fault tree analysis:
A fault tree analysis is the evaluation of an undesired event, called the top event of the fault tree. Given the top event, a fault tree is constructed by a deductive (top-down) method of analysis identifying the cause or combination of causes that can lead to the defined top event. Once the fault tree has been drawn all failure combinations leading to the top event have to be determined. These combinations are called minimal cutsets. Once the minimal cut sets are known the reliability or the unavailability can be calculated by quantification of these minimal cut sets.

Gates:
Gates are defined as the AND and OR symbols used in the fault trees to collect the multiple or single basic events leading to the undesired event.

Minimal cut set:
A term used in Fault Tree Analysis to describe the smallest combination of component and human failures which, if they all occur, will cause the top event to occur. The failure all correspond to basic events or undeveloped events.

Naming conventions:
Naming convention refers to a scheme for developing basic event designators. In most cases the naming convention consists of:

- component identification
- component type identification
- identification of the failure mode.

OR Gate:
The ”OR”-gate in a fault tree requires the occurrence of a minimum of one of the input events to make the output event to occur.

Rare event:
An event or accident whose expected probability of occurrence is very small.

System:
A system is an organized set of components performing one or more functions.

System boundaries:
A system boundary detemines which elements belong to the system under consideration.

Top event:
The undesired event or incident at the ”top” of a fault tree that is traced downward to more basic failures using Boolean logic gates to determine the event’s possible causes. The top event of a fault tree can be the initiating event of an event tree or a heading event of an event tree.

Undeveloped event:
An event in a fault tree that is not developed because it is of no significance or because more detailed information is unavailable.

2.8 EVENT TREE ANALYSIS

Accident sequence:
Accident sequences are combinations of functional successes and failures that result in an undesired outcome.

Branch point:
A node with two paths in an event tree or cause-consequence diagram. One path represents success of a safety function and the other path represents failure of the function.

Consequence:
The direct, undesirable result of an accident sequence usually involving a fire, explosion, or release of toxic material. Consequence descriptions may be qualitative or quantitative estimates of the effects of an accident in terms of factors such as health impacts, economics loss, and environmental damage.

Event:
An occurrence related to equipment performance or human action, or an occurrence external to the system that causes system upset. In this book an event is either the cause of or a contributor to an incident or accident, or is a response to an accident's initiating event.

Event tree:
An event tree is a logic diagram of success and failure combinations of events, used to identify accident sequences leading to all possible consequences of a given initiating event.

Event sequence:
A specific, unplanned series of events composed of an initiating event and intermediate events that may lead to an accident.

Event tree:
A logic model that graphically portrays the combinations of events and circumstances in an accident sequence.

Heading event:
An event in the heading of an event tree that propagates or mitigates the initiating event during an accident sequence.

Initiating event:
The first event in an event sequence. Can result in an accident unless engineered protection systems or human actions intervene to prevent or mitigate the accident.

2.9 MARKOV PROCESSES

Absorbing state:
A state from which, once entered, transitions are not possible. Once in an absorbing state, the system will stay there until in effect it is replaced, as a whole, by a fully functional system.

Failed state:
A system or unit state in which the system or unit does not perform the required function.

Functional state:
A system or unit state in which the system or unit performs the required function.

Initial state:
The system state at time t=0. Following a system failure, the system may be restored to the initial state. Generally, a system starts its operation at t=0 from the complete functional state in which all units of the system are functioning and transits towards the final system state, which is a failed state, via other system functional states having progressively fewer functioning units.

Non-restorable system:
A system, the state transition diagram of which contains only transitions in the direction towards the final system failure state. For a non-restorable system, reliability measures such as reliability and MTTF are calculated.

Restorable system:
A system containing units which can fail and then be restored to their functional state, without necessarily causing system failure. This corresponds to transition in the state diagram in the direction towards the initial state. For this to be possible, the units concerned must operate in redundant configurations.

State symbol:
A state is represented by a circle or a rectangle.

State description:
The state description is placed inside the state symbol and may take the form of words or alphanumeric characters defining those combinations of failed and functioning units which characterize the state.

State label:
A state label is a number in a circle, placed adjacent to the state symbol, or in the absence of a state description, within the symbol itself.

System state:
A system state is a particular combination of unit states.

Transition:
A change from one state to another, usually as a result of failure or restoration. A transition may be also caused by other events such as human errors, external events, etc.

Transition arrow:
The transition arrow indicates the direction of a transition as a result of failure or restoration.

Transition probability:
The probability of transition between state one to another state.

Unit:
A component or set of components, which function as a single entity. As, such, the unit can exist in only two states: functional or failed. For convenience, the term unit state is normally used to denote the state of a unit.

2.10 ACCIDENT SEQUENCE DEVELOPMENT AND QUANTIFICATION

Fail safe:
A concept that defines the failure direction of a component or system as a result of specific malfunctions. The failure direction is towards a safer or less hazardous condition.

Final element:
A device that manipulates a process variable to achieve control.

Front line system:
A system that directly perform a safety function is called a front line system.

Initiating event group:
A group of initiating events that require the same mitigating functions.

Redundancy:
Use of multiple elements or systems to perform the same function. Redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy).

Safety function:
Safety functions are defined by a group of actions that prevent the occurrence of a hazardous event given the occurrence of an initiating event.

Safety system:
Equipment and or procedures designed to limit or terminate an accident sequence, thus mitigating the accident and its consequences.

Spurious trip:
Refers to the shutdown of the process for reasons not associated with a problem in the process that the safety instrument system is designed to protect. Other terms used include nuisance trip and false trip.

Success criteria
The success criteria are defined as the minimum system or component performance required for the successful fulfilment of its function under specific conditions.

Support system
The systems required for the proper functioning of a front line system are called support systems.

System initiator:
Failure in safety or supporting systems that require an immediate plant shutdown.

Top logic:
Top logic is a fault tree logic format, combining several fault trees or functions for tying the functions to system failures and human errors.

2.11 DEPENDENT FAILURE ANALYSIS

Cause:
A cause is simply an explanation for why a component became unavailable or potentially unavailable. In complete, traditional system logic models, the cause level is the most detailed level of analysis and is almost always implicit in the quantification model, being located below the component level. With every cause, there exists a mechanism fully or partially responsible for the state of a component when an event includes a single component state; the cause of the component state is referred to (loosely) as a root cause. In more complex events involving two or more component states, a particular component state or set of component states can result from either a root cause or can be caused by the state of another component; i.e.,component cause.

Common cause event:
In the context of system modelling, common cause events are a subset of dependent events in which two or more component fault states exist at the same time, or in a short time interval, and are a direct result of a shared cause. It is also implied that the shared cause is not another component state because such cascading of component states is normally due to a functional coupling mechanism. Such functional dependencies are normally modelled explicitly in systems models without the need for special common cause event models. The special models that have been developed to model common cause events, such as the beta factor, binomial failure rate, multiple Greek letter, basic parameter, common load, and other models, all apply to root-caused events branching to impact multiple components, but they are generally not applied to component-caused events.

Common cause component group:
A common cause component group is usually a group of similar or identical components that have a significant probability of experiencing a common cause event. In principle, any combination of components could be postulated as having a potential for being involved in such an event.

Common cause basic event:
An event involving common cause failure of a specific subset of components within a common cause component group.

Conditional event:
An conditional event is an event which predisposes a component to failure, or increases its susceptibility to failure, but does not of itself cause failure. Consider a pump failure due to high humidity. The condition event could have been a maintenance error. For instance not sealing the pump control cabinet properly following maintenance. In this case the condition event is latent, but is a necessary contribution to the failure mechanism.

Common cause failure analysis:
An analysis to identify potential failures in redundant systems or redundant sub systems which would undermine the benefits of redundancy because of the appearance of the same failures in the redundant parts.

Coupling mechanism:
A coupling mechanism is a way to explain how a root cause propagates to involve multiple equipment items; e.g., components. The three broad categories of coupling mechanisms are functional, spatial, and human.

Functional Couplings

- **Connected equipment**
  Encompasses plant design involving shared equipment, common input, and loop dependencies plus situations in which the same equipment provides multiple functions.

- **Nonconnected equipment**
  Encompasses interrelated success criteria, such as the relationship between a standby system and the system it is supporting. More subtle forms of nonconnected equipment-couplings are environmental conductors, such as heating, ventilation, and air conditioning systems.

Spatial Couplings

- **Spatial proximity**
  Refers to equipment found within a common room, fire barriers, flood barriers, or missile barriers.

- **Linked equipment**
  Equipment in different locations that, although not functionally related, is similarly affected by an extreme environmental condition possibly due to the breach of a barrier.

Human Couplings
Refers to activities, such as design, manufacturing, construction, installation, quality control, plant management, station operating procedures, emergency procedures, maintenance, testing and inspection procedures, and implementation, etc.

Defensive strategy:
A set of operational, maintenance, and design measures taken to diminish the frequency and/or the consequences of common cause failures. Common cause design review, surveillance testing, and redundancy are therefore examples of tactics contributing to a defensive strategy.

Diversity:
Existence of different means of performing a function (e.g., other physical principles, other ways of solving the same problem).

Impact vector:
An assessment of the impact an event would have on a common cause component group. The impact is usually measured as the number of failed components out of a set of similar components in the common cause component group.

Root cause:
The combinations of conditions or factors that underlie failures, accidents or incidents. The cause of an event can be traced to an event that occurred at some distinct but possibly unknown point in time. These causal events are known as "root cause". There are four general types of root causes.

- Hardware
  Isolated random equipment failures due to causes inherent in the affected component.

- Human
  Errors during plant operations (dynamic interaction with the plant), errors during equipment testing or maintenance, and errors during design, manufacturing, and construction.

- Environmental
  Events that are external to the equipment but internal to the plant that result in environmental stresses being applied to the equipment.

- External
  Events that initiate external to the plant that result in abnormal environmental stresses being applied to the equipment.

Shock:
A concept used to explain how component states other than intrinsic, random, independent failures occur that is used in some common cause models, such as the BFR model. A shock is an event that occurs at d random point in time and acts on the system; i.e., all the components in the system simultaneously. There are two kinds of shocks distinguished by the potential impact of the shock event, as defined below.

a: **Lethal Shock**
A lethal shock is a shock in which all the components in a system are failed, with certainty, any time the shock occurs.

b: **Nonlethal Shock**
A nonlethal shock is a shock for which there is some independent probability that each component in the system fails as a result of the shock. The range of possible outcomes (each having a different probability of occurrence) of a nonlethal shock range from no component failures to all the components failed.

Trigger event:
A trigger event is an event which activates a failure, or initiates the transition to the failed state, whether or not the failure is revealed at the time the trigger events occurs. An event which led to fire in a room and subsequent equipment failure would be such a trigger event. A trigger event therefore is a dynamic feature of the failure mechanism. A trigger event, particularly in the case of common cause events, is usually an event external to the components in question.

2.12 HUMAN FAILURES

Action:
The motions, or decisions, or thinking of one or more people.

Annunciator:
A display that has an audible as well as a visible indication.

Basic human error probability:
The probability of a human error on a task that is considered as an isolated entity, i.e., not influenced by previous tasks.

Bounding analysis:
An analysis in which the best and worst case reliability estimates are obtained by using the results of a best case analysis and worst case analysis.

Burden:
Aspects of the environment or fundamental human mechanism that put loads on human capacities for action or otherwise inhibit performance.

Classification system:
A classification system is a scheme for grouping human errors, such as skill based, rule based and knowledge based type of human errors.

Cognition:
The capacity or mechanisms that lead to knowledge.

Cognitive behaviour:
The mental behaviour of individuals or crews associated with performing a task. Three types of cognitive behaviours have been classified as skill, rule and knowledge. The prevailing type of cognitive processing associated with a given activity is defined as dominant. The concept of dominance permits analysts to ascribe one of three types of cognitive processing to a task for the purpose of estimating the non response probability associated with the task.

Cognitive response:
The operator action associated with a type of cognitive behaviour initiated by an observable stimulus. The stimulus can be as simple as an annunciator alarm going off, or as complex as multiple information inputs within an accident sequence. Depending on the given stimulus and the level of operator experience or training, the cognitive processing may be classified as either skill, rule or knowledge. The times of response by operator crews or individuals appear to be directly related to the type of cognitive processing used.

Conditional human error probability:
The probability of human error on a specific task given failure or, success, on some other task.

Decision making:
The human process of determining the proper course of action.

Derived human error probability:
Estimated human error probability based on extrapolation from human error probabilities or other information collected in different situations from the one of primary interest.

Diagnosis:
The human process of determining the plant state and anticipating its future states.

Display:
A device that indicates a parameter of equipment's status to a person by some perceptual mechanism.

Error:
Any deviation from an intended or desired human performance, or any deviation from a target.

Error of omission:
Error of omission is a passive event where something was not done.

Error of commission:
Error of commission is an active event where something was done that should not have been done.

General diagnosis:
General diagnosis is the thinking process based on information which the operator uses to determine what actions are required.

Human cognitive reliability:
The time dependent function which describes the probability of an operator response in performing a specified task. The human cognitive reliability model permits the analyst to predict the cognitive reliability associated with a non response for a given task, once the dominant type of cognitive processing, the median response time for the task under nominal conditions and performance shaping factors are identified.

Human error:
A human error is the non-performance or incorrect performance of a desired activity, provided that adequate conditions for correct performance are present.

Human error probability:
The probability that an error will occur when a given task is performed. Synonym: human failure probability and task failure probability.

Human factors:
A discipline concerned with designing machines, operations, and work environments so that they match human capacities and limitations and prevent human errors. Among human factors practitioners, the term is considered the general term that includes human factors engineering, procedures, training, selection, and any technical work related to the human factor in man-machine systems.

Human failure event:
An event modelled in a risk assessment that represents a system failure whose proximal cause is the actions or inactions of people.

Human reliability:
The probability of the success of a human action, or some other measure of successful human performance.

Human reliability analysis:
A method used to evaluate whether necessary human actions, tasks, or jobs will be completed successfully within a required time period.

HRA event tree:
A graphical model of sequential events in which the tree limbs designate human actions and other events as well as different conditions or influences upon these events.

Lapse:
Memory failures, omitting planned items, and forgetting intentions.

Latent error:
An erroneous action or decision for which the consequences only become apparent after a period of time when other conditions or events combine with the original error to produce a undesired consequence for the system. Latent errors occur primarily in maintenance or testing, occur prior to an accident, and are most likely slips or an action or event that produces equipment unavailabilities pre incident.

Median response time:
Defined as a measurable or estimated time within which one half of the control room crew faced with the same stimulus would complete a defined action or function. In application, it is the time at a probability of 0.5 that the crew has successfully carried out the required task. Measured median response times for task performance include the impact of performance shaping factors. By adjusting the measured median response time for different performance shaping factors, a measurement in one application could be applied in other situations, with different performance shaping factors, in which a similar task is carried out.

Mistake:
Errors arising from a correct intentions that lead to incorrect action sequences. A mistake is mostly an error in diagnosis or a human error that is a failure in diagnosis, decision making, or planning. Rule based mistakes; misapplication of good rule or application of bad rule. Knowledge based mistakes; many variable forms.

Operator:
An individual responsible for monitoring, controlling, and performing tasks as necessary to accomplish the productive activities of a system. Often used in a generic sense to include people who perform all kinds of tasks.

Performance shaping or influencing factors:
Any factor that influences human performance. Performance shaping factors include factors intrinsic to an individual (personality, skill, etc.) and factors in the work situation (task demands, plant policies, hardware design, training, etc.)

Procedure:
The formal realization of a task, e.g. verbal instructions or written procedure.

Recovery:
The accommodation of a failure or otherwise undesired performance in hardware or software by restoring the failed hardware or software or by finding an alternative to achieving the function of the hardware or software.

Recovery error:
Failure to correct a technical failure or human error before its consequences occur

Slip:
Errors in which the intention is correct but failure occurs when carrying out the activity required. Slips occur at the skill-based level of information processing. A slip is an oversight similar to an error of omission. Attentional failures; intrusion, omission, reversal, misordening and mistiming.

Stress:
The physiological or psychological reaction to loads, burden, or other stressful influences on people.

Stressor:
A stressor is a task intensifying circumstance which increases the probability of human error.

Success likelihood index methodology:
Success Likelihood Index Methodology is based on expert judgment and is a method of normalizing a specific plant operating crew, procedures, training, control room, and control room layout to other equivalent plant factors.

Task:
A series of human activities designed to accomplish a specific goal.

Task analysis:
A human error analysis method that requires breaking down a procedure or overall task into unit tasks and combining this information in the form of tables or event trees. It involves determining the detailed performance required of people and equipment and determining the effects of environmental conditions, malfunctions, and other unexpected events on both.

Time reliability correlation:
Time Reliability Correlation is a curve or function that relates the time available for action and the probability of doing the action. Probability of failure increases with decreasing time.

Vigilance:
Vigilance is a stressor. This stressor results from performance of a task carried out for a long period and consisting of detecting signals which rarely occur but which at the same time are difficult to detect.

Violation:
An error that occurs when an action is taken that contravenes known operational rules, restrictions, and or procedures. The definition of violation excludes actions taken to intentionally harm the system.

2.13 RELIABILITY AVAILABILITY AND MAINTAINABILITY (RAM) SPECIFICATION

Dependability:
Dependability is a collective term used only for non-quantitative descriptions of the reliability, availability and maintainability.

Life cycle costs:
Life cycle costs is the total costs of ownership to the customer for acquisition, operation and maintenance and disposal of a product, for the whole life.

Maintainability:
Maintainability is a measure for the maintenance effort. In RAM analyses normally exposed in terms of time needed for repair (mean time to repair unplanned) and overhaul (mean time to complete overhaul planned).

RAM program:
A RAM program is the work conducted during the project to assure that the reliability, availability and maintainability of the equipment will meet the desired targets.

PROBABILITY THEORY

CONTENTS **Page**

3.1 INTRODUCTION

The probability concept is the basis for a risk analysis or reliability analysis. One must be familiar with this concept to be able to determine the value of the input parameters and to understand the results of a risk or reliability analysis. This chapter deals with the most important concepts of probability. First three definitions of probability and their practical application will be provided. Next the rules for combining events are explained. Mutually exclusive events, complementary events, independent versus dependent events, and conditional events are treated. Essential for risk and reliability analyses are the addition rule for probabilities and the multiplication rule for probabilities. Finally it is explained how the probability of failure of a system which consists of a series of components and/or a number of parallel components have to be calculated using basic probability rules.

Probability distributions and Bayesian statistics are explained in chapter 4.

3.2 NOMENCLATURE

A, B, F	=	events	-
P	=	probability	-
S	=	entire sample space	-
n	=	number of samples in which event A occurred	-
N	=	number of experiments	-
m	=	number of components in series or in parallel	-

Operatíons:

$\cup$: Operation of union

$\cap$: Operation of intersection

$\bar{A}$: Operation of complementation

|: Conditional

Boolean algebra, which is the algebra of events, deals with event operations which are represented by various symbols. Unfortunately, set theoretic symbolism is not uniform; the symbology differs among the fields of mathematics, logic, and engineering as follows:

Operation	**Probability**	**Mathematics**	**Logic**	**Engineering**
Union of A and B:	A or B	$A \cup B$	$A \vee B$	A + B
Intersection of A and B:	A and B	$A \cap B$	$A \wedge B$	A.B or AB
Complement of A:	not A	$\bar{A}$	-A	$\bar{A}$

The symbols used in mathematics and in logic are very similar. The logical symbols are the older. It is unfortunate that engineering has adopted ″+″ for ″$\cup$″ and an implied multiplication for ″$\cap$″. This procedure might arise confusing with the normal use of the symbols ″+″ and “.”.

3.3 PROBABILITIES AND EVENTS

The word probability is used frequently in a loose sense implying that a certain event has a good chance of occurring. In this sense it is a qualitative measure. Mathematically probability is a numerical value that can vary between zero to unity. A probability of zero of event X defines an absolute impossibility that event X will occur. A probability of unity of event X defines an absolute certainty that event X will occur.

Based on definitions and axioms probability theory provides the theoretical propositions about the characteristics of probabilities. This does not cover interpretation of the probability concept. Interpretation is of course necessary for applications. Probability theory also provides the means how to combine probabilities of separate events.

3.3.1 Definition of probability

The most generally accepted approach is to base probability theory on the four fundamental axioms of Kolmogorov. The entire theory is built in a deductive manner on these axioms. This approach has the advantage that, if it is followed carefully, all properties are well defined. As with any other theory or abstract model, the engineering usefulness of the technique is measured by how well it describes problems in the physical world. In order to evaluate the parameters in the axiomatic model one may perform an experiment and utilize the relative-frequency interpretation or evoke a hypothesis on the basis of engineering judgement.

Axiomatic approach begins with a statement of four fundamental axioms of probability P. P is a funtion of a set S to R (R is a real set of numbers):

1: The probability that an event A occurs is a number between zero and unity:

$$0 \leq P(A) \leq 1 \tag{3.1}$$

2: The probability of a certain event is unity:

$$P(S) = 1 \tag{3.2}$$

3: The probability of the union or sum of the highest disjoint or mutually exclusive events is:

$$P\left(\cup_{i=1}^{n} F_i\right) = \sum_{1}^{n} P(F_i) \tag{3.3}$$

For two events A and B this formula is:

$$\text{If } A \cup B = 0 \text{ then } P(A \cup B) = P(A) + P(B) \tag{3.4}$$

4: For all i:

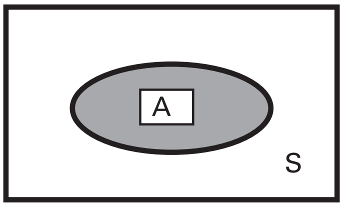
$$\text{If } F_i \supseteq F_{i+1} \text{ and } \bigcap_{1}^{\infty} F_i = 0 \text{ then } \lim_{i\to\infty} P(F_i) = 0 \tag{3.5}$$

In order to understand the meaning of these four statements, one must be familiar with a few basic definitions and results from the theory of sets. The next paragraph introduces these results and explains the use of Venn diagrams.

3.3.2 Set theory and Venn diagrams

A set is simply a collection of objects. The order in which the objects of the set are enumerated is not significant. Each item in the collection is an element of the set. Each set contains a number of sub-sets. The sub-sets are defined by a smaller number of elements selected from the original set. One first defines the largest set of any interest in the problem and calls this the universal set. The universal set contains all possible elements in the problem. In probability theory, the type of sets one is interested in are those which can, at least in theory, be viewed as outcomes of an experiment. These sets are generally called events. It is often more convenient if the events are defined so that they cannot be subdivided. Each event contains only one element. When the concept of universal set is used in probability theory, the term sample space S is generally applied. It is convenient to associate a geometric picture, called a Venn diagram, with these ideas of sample space and event or set and sub-set. In figure 3.1 the area inside the rectangle corresponds to the sample space. The area S encloses or represents the entire sample space being considered. The hatched area inside the rectangle represents the probability of occurrence of event A. By definition:

$$P(A) = \frac{\text{area A}}{\text{area S}} \tag{3.6}$$

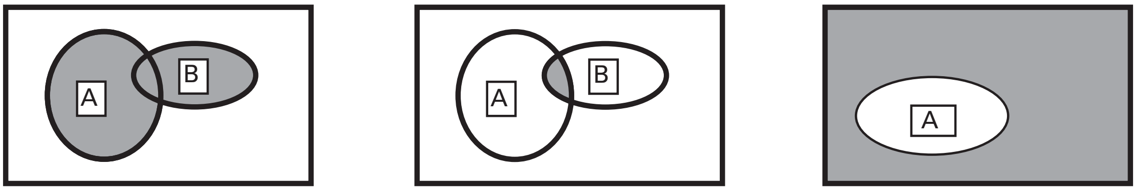


Constrains: P(S) = 1 , P(A) ≥ 0

Figure 3.1: Example of a Venn diagram.

Operations on sets or events can be defined with the help of Venn diagrams. The operation of union is depicted in figure 3.2 (A). The union of two sets of A, B is the set that contains all elements that are either in A or in B or in both, is written as A∪B, and is indicated by the hatched area in figure 3.2 (A).

The operation of intersection is depicted in figure 3.2 (B). The intersection of two sets A, B is the set that contains all elements that are common to A and B, is written as A∩B, and is indicated by the hatched area in figure 3.2 (B). The operation of complementation is depicted in figure 3.2 (C). The complement of a set A is the set that contains all element that are not in A, is written $\bar{A}$, and is indicated by the hatched area in figure 3.2 (C).



(A) The Operation of Union

(B) The Operation of intersection

(C) The Operation of Complementation

Figure 3.2: Operations on sets or events.

3.3.3 **Interpretations of probability**

Three different interpretations of probability will be provided based on three different approaches to the estimation of probabilities. The first and the second interpretation assume that the probability is entirely based on observed information. Probability can be estimated from relative frequency of observed events. The validity of this approach depends on the amount of observed data available.

The third interpretation recognizes that, in addition to observed data, probability is also based on judgement. This is especially necessary when direct observed data are not available.

This approach to estimate probabilities is commonly referred to as the Bayesian approach in which the judgmental information is combined with the observed information for an updated estimation of the probabilities. For explanation of this approach reference is made to the chapters 4 and 6; "Statistics" and "Data Analysis".

Interpretation 1:
If an event can result in N equally likely outcomes, and if the event with attribute A can happen in n of these ways, then the probability of A occurring is:

$$P(A) = \frac{n}{N} \tag{3.7}$$

Interpretation 2:
If in an experiment, an event with attribute A occurs n times out of N experiments, then as N becomes large, n/N approaches the probability of event A, i.e.

$$P(A) = \lim_{N \to \infty} \left(\frac{n}{N}\right) \tag{3.8}$$

Interpretation 3:
Probability is a numerical measure of a state of knowledge, a degree of belief, or a state of confidence about the outcome of an event, based on all available information.

The first interpretation describes the case for which a fixed number of outcomes can be identified, for instance six possible outcomes for the toss of a single die are possible. This definition is not very useful in risk and reliability analysis.

The second interpretation covers typical cases in quality control and reliability if there is a sufficient amount of data available. If one collects data of diesel generators and finds that 20 failures occurred out of 1000 starts, one may feel justified that the probability of failure to start of a diesel generator is 0.02 per demand. However one must be careful in making this type of assertion.

The probability of 0.02 of failure to start in the next demand may be considered as a degree of belief, limited by the size of the sample, in this outcome. This leads to the third, subjective, interpretation of probability (interpretation 3). If, in the 1000 demands, eight of the failures had occurred for a specific type of diesel generator and one has taken corrective action to improve these diesel generators so that such a problem was less likely to occur in future, one might assign some lower probability of failure to the next demand. This subjective approach is quite valid, and is very often necessary in risk and reliability analyses.

Relative frequency approach:
Unknown probabilities can be approximated numerically using the data available. The simplest approximation is that of the fraction of events actually realized. Assume that an event A has occurred n times in N samples. This way of determining the probability of an event is called the

$$\begin{aligned} P(A) &\approx \frac{\text{Number of samples in which event A occurred}}{\text{Total number of samples}} \\ &\approx \frac{n}{N} \end{aligned} \tag{3.9}$$

relative frequency approach.

It should be clear that a probability has no dimension and ranges from 0 to 1.

3.4 RULES FOR COMBINING EVENTS

The area S of a Venn diagram encloses or represents the entire space being considered. There may be two or more events within this space for which the probabilities must be combined. This consideration may be restricted to two events A and B, see figure 3.3. If event A is totally enclosed by event B, then event A is a subset of event B. This is one particular association between events A and B. A more general relationship is that A and B partly overlap or do not overlap at all. In the following paragraphs the different possibilities of combining events A and B will be discussed and the rules for combining events will be provided.

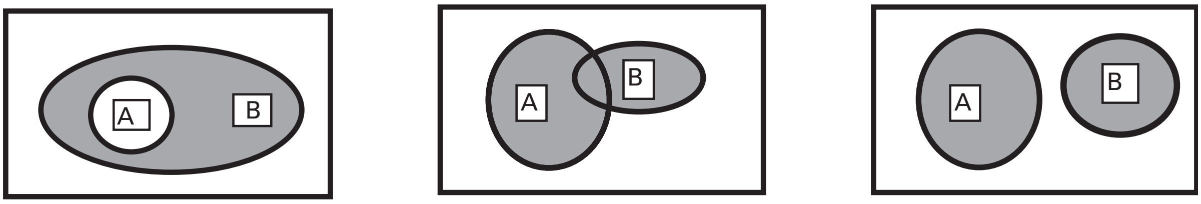
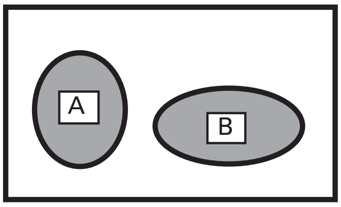


Figure 3.3: Combined events.

3.4.1 Mutually exclusive events



Two events A and B are called mutually exclusive events if these events can never occur simultaneously. So if A occurs, B will definitely not occur, see figure 3.4. From the Venn diagram it is clear that the probability of occurrence simultaneously of events A and B is equal to zero. So the following applies to mutually exclusive events:

$$P(A \cap B) = 0 \tag{3.10}$$

Figure 3.4: Mutually exclusive events.

Example:
Consider a redundant safety system, which consists of two components A and B. Testing is performed in sequential order, first component A is tested and component B is tested after completion of the test of component A. The probability that both components are unavailable due to testing is equal to zero, because testing of component A and testing of component B are mutually exclusive events and cannot occur simultaneously.

3.4.2 Complementary events

Two outcomes of an event are called to be complementary if, when one outcome does not

occur, the other must occur. This is depicted by the Venn diagram shown in figure 3.5.
From the Venn diagram, it can be concluded that, if the two outcomes A and B have probabilities P(A) and P(B), the following relation holds:

$$P(A) + P(B) = 1 \quad \text{or} \quad P(B) = P(\bar{A})$$

$P(\bar{A})$ is the probability of A not occurring

Example:
In risk and reliability analyses it is normally assumed that a component has only two modes, for example up or down. By definition these are complementary events.

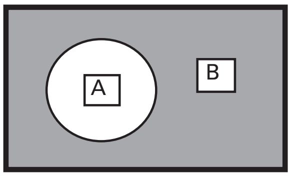


Figure 3.5: Complementary events.

3.4.3 Independent versus dependent events

Two events A and B are called independent if the probability of event A is not affected by whether or not event B occurs. In other words if the information about whether or not B occurs does not provide any additional information about the occurrence of A. Two events are called dependent, if the probability of occurrence of one event is influenced by the probability of occurrence of the other.

$$P(A \mid B) \neq P(A) \tag{3.12}$$

Example:
The failure of two redundant components in a safety system cannot be regarded as independent if both components are identical or if both components are maintained in accordance with the same maintenance procedure on the same day by the same maintenance crew or if both components are vulnerable to the same extreme environmental conditions. A design error or a maintenance error or extreme environmental conditions can be the cause for component failure. In this case both components can be in the failed state due to the same cause.

3.4.4 Conditional probabilities

Conditional events are events which occur conditionally on the occurrence of another event or events. Consider two events A and B and also consider the probability of event A occurring under the condition that event B has occurred, This is described mathematically as P(A | B) in which the vertical bar is interpreted as ″given″ and the complete probability expression is interpreted as the ″conditional probability of event A occurring given that event B has occurred″. This is represented by the intersection depicted in the Venn diagram shown in figure 3.6. In accordance to logic and Bayesian theory all probabilities are conditional.

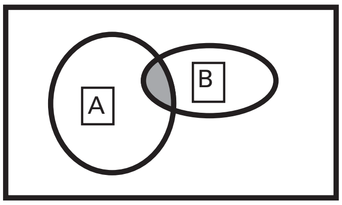


Figure 3.6: Intersection of events A and B.

The value of probability of event A occurring given that condition B has occurred can be deducted from an analysis of the Venn diagram. From the Venn diagram it can be concluded that the following expression holds:

$$P(A \mid B) = \frac{\text{Number of ways events } A \cap B \text{ can occur}}{\text{Number of ways event B can occur}} \tag{3.13}$$

Expression (3.13) is an application of interpretation 1 for probabilities, as given in paragraph 3.3.3, since the total ″numbers of times an experiment is repeated″ is equivalent to event B, some of which will lead to the occurrence of event A together, this being the ″particular outcome″ of interest. The number of ways event A and event B can occur is the hatched area shown in figure 3.6 and is represented mathematically as (A ∩ B), the probability of which can be deducted by again applying equation (3.6) as (see section 3.3.2):

$$P(A \cap B) = \frac{\text{area } (A \cap B)}{\text{area S}} \tag{3.14}$$

$$\text{similary } P(B) = \frac{\text{area B}}{\text{area S}}$$

This can be written as:

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} \tag{3.15}$$

The same expression holds for the probability of event B occurring given that event A has occurred:

$$P(B \mid A) \quad \frac{P(A \cap B)}{P(A)} \tag{3.16}$$

3.5 ALGEBRAIC OPERATIONS WITH PROBABILITIES

3.5.1 Simultaneous occurence of events (Multiplication rule for probabilities)

The simultaneous occurrence of two events A and B is the occurrence of both events A and B. In terms of a Venn diagram, this occurrence is represented by the operation of intersection as depicted in figure 3.6. Mathematically it is expressed as follows:

$$(A \cap B), \quad (A \text{ and } B) \quad \text{or } (AB) \tag{3.17}$$

Rewriting equation (3.15) and (3.16) gives the general multiplication rule for two events:

$$\begin{aligned} P(A \cap B) &= P(A).P(B \mid A) \\ &= P(B).P(A \mid B) \end{aligned} \tag{3.18}$$

In this rule there are two cases to consider, the first is when the two events are independent and the second is when the two events are dependent.

Events are independent:
If A and B are independent, then the following applies:

$$P(A \mid B) = P(A) \quad \text{and} \quad P(B \mid A) = P(B) \tag{3.19}$$

Substitution of equation (3.19) into equation (3.18) gives the multiplication rule for two independent events:

$$P(A \cap B) = P(A).P(B) \tag{3.20}$$

If there are m independent events, equation (3.20) can extended to give:

$$P(A_1 \cap A_2 \cap \quad .... \quad \cap A_m) \quad \prod_{i=1}^{m} P(A_i) \tag{3.21}$$

The m events A_1, A_2 ..., A_m are called independent if knowledge about the occurrence of an arbitrary number of these events does not provide us with information about whether or not the rest occurs.

Events are dependent:
If the two events are dependent the generally valid equation (3.18) can still be used but cannot be simplified as in the case of independent events.

3.5.2 Occurrence of at least one of two events (Addition rule for probabilities)

The occurrence of at least one of two events A and B is the occurrence of event A or the occurrence of event B or the simultaneous occurrence of events A and B. The occurrence of at least one of two events A and B is represented by the hatched area of the Venn diagram depicted in figure 3.7.

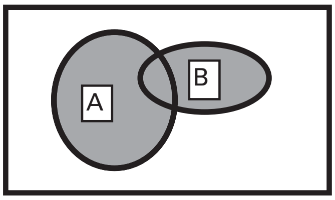


Figure 3.7: Occurrence of at least one of two events.

Mathematically the occurrence of at least one of two events is called the union of two events and is expressed by:

$$(A \cup B), \quad (A \text{ or } B) \quad \text{or} \quad (A + B) \tag{3.22}$$

From the Venn diagram depicted in figure 3.7 the following equation can be deduced:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \tag{3.23}$$

Three cases have to be considered: the events are mutually exclusive, the events are independent and the events are dependent.

Events are mutually exclusive:
If the events are mutually exclusive, then the probability of their simultaneous occurrence $P(A \cap B)$ must be zero by definition. Therefore from equation (3.23):

$$P(A \cup B) = P(A) + P(B) \tag{3.24}$$

This can also be derived from a Venn diagram representation. In this case the Venn diagram is the one depicted in figure 3.4 in which event A and event B do not overlap. It follows that the intersection of the two events is zero.

If there are m countable mutually exclusive events, the following equation yields:

$$P(A_1 \cup A_2 \cup .... \cup A_m) \sum_{i=1}^{m} P(A_i) \tag{3.25}$$

The m events A_1 , A_2, ..., A_m are called mutually exclusive events if each event A_i excludes the event A_j (where $i \neq j$).

Events are independent:
If the events are independent equation (3.20) can be used. Substitution of equation (3.20) into equation (3.23) yields:

$$P(A \cup B) = P(A) + P(B) - P(A).P(B) \tag{3.26}$$

Events are dependent:
If the two events A and B are dependent then the equations (3.15) and (3.16) cannot be simplified. Substitution of equations (3.15) and (3.16) in equation (3.23) results in:

$$\begin{aligned} P(A \cup B) &= P(A) + P(B) - P(A \cap B) \\ &= P(A) + P(B) - P(A).P(B \mid A) \\ &= P(A) + P(B) - P(B).P(A \mid B) \end{aligned} \tag{3.27}$$

3.6 SERIES-PARALLEL SYSTEMS

3.6.1 Series structure of components

The arrangement depicted in figure 3.8 represents a system whose subsystem or components form a series network. If anyone of the subsystem or component fails, the series system experiences an overall system failure.

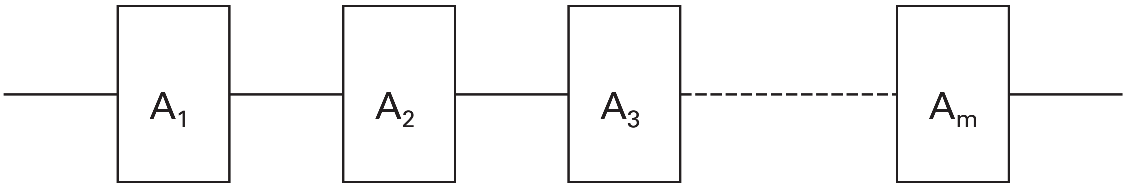


Figure 3.8: Series structure of components. Define the following events:

$\bar{A}$ = Component A is down
A = Component A is up.

If the series system component failures are independent, then the probability that the system is up can be calculated with the following formula:

$$\begin{aligned} P(\text{System is up}) &= P(A_1 \text{ up} \cap A_2 \text{ up} \cap .... \cap A_m \text{ up}) \\ &= P(A_1) \,.\, P(A_2) \,.\, P(A_3) \,...\, P(A_m) \\ &= \prod_{i=1}^{m} P(A_i) \end{aligned} \tag{3.28}$$

The probability that the system will not perform the required function can be calculated with the formula:

$$\begin{aligned} P\,(\text{System is down}) &= 1 - P\,(\text{ System is up}) \\ &= 1 - \prod_{i=1}^{m} - P(A_i) \\ &= 1 - \prod_{i=1}^{m} \{1 - P(\bar{A}_i)\} \end{aligned} \tag{3.29}$$

If one ignores the possibility of any two or more component failure events A_i occurring simultaneously, equation (3.29) reduces to:

$$\begin{aligned} P\,(\text{ System is down}) &= 1 - \prod_{i=1}^{m} \{1 - P(\bar{A}_i)\} \\ &\approx \sum_{i=1}^{m} P(\bar{A}_i) \end{aligned} \tag{3.30}$$

Equation (3.30) is the so-called ”rare event approximation” and is accurate to within about ten per cent of the true probability when $P(\bar{A}) < 0.1$. Furthermore, any error made is on the conservative side, in that the true probability is slightly lower than that given by equation (3.29). The rare event approximation plays an important role in fault tree quantification.

3.6.2 Parallel configuration of components

The parallel configuration of components is shown in figure 3.9. This system will fail if and only if all the units in the system malfunction (one out of m). The model is based on the assumption that all the components are in the same mode of operation. In addition it is assumed that the component failures are independent.

The parallel system experiences an overall system failure if all the subsystems or components have been failed. In terms of probabilities, this can be expressed as follows:

$$
\begin{aligned}
P(\text{System is down}) &= P(A_i\text{down} \cap A_2 \cap \ldots \cap A_m \text{ down}) \\
&= P(\bar{A}_1).P(\bar{A}_2).P(\bar{A}_3) \ldots\ldots\ P(\bar{A}_m) \qquad (3.31) \\
&= \prod_{i=1}^{m} P(\bar{A}_i)
\end{aligned}
$$

Equation (3.31) suggests that the failure probability can be limited to almost zero by putting more components in parallel. In practice this cannot be achieved because of dependencies between the components in parallel. For instance, the components can be identical or the components can be vulnerable to the same environmental influence factors.

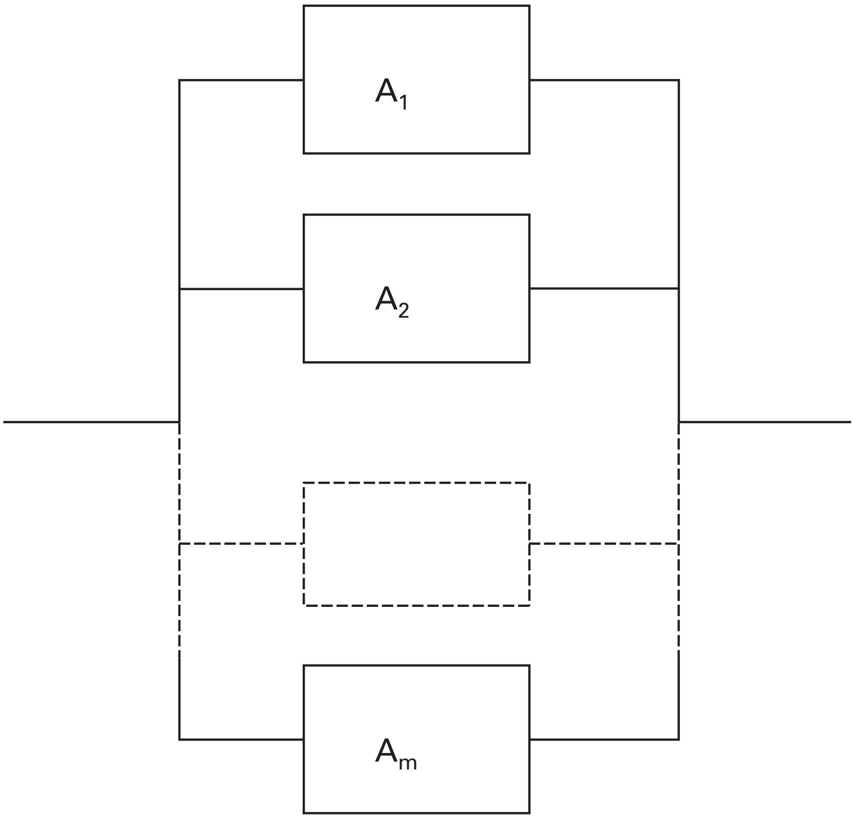


Figure 3.9: Parallel configuration of components.

3.6.3 **Example**

Consider the series-parallel system depicted in figure 3.10. The system consists of six components. The components A, B and C form a two-out-of-three system and the components D and E a one out of two system. The probability of failure of each component is equal to 0.1. The probability of failure of the complete system has to be determined. It is assumed that component failure occurrences are independent.

To calculate the probability of failure, the whole system can be considered as a series structure of three subsystems. The first subsystem is composed of components A, B and C. The second subsystem consists of components D and E. The third subsystem is represented by component F.

Define the following events:

$\bar{A}$ = Failure of component A
$\bar{B}$ = Failure of component B
$\bar{C}$ = Failure of component C
$\bar{D}$ = Failure of component D
$\bar{E}$ = Failure of component E
$\bar{F}$ = Failure of component F

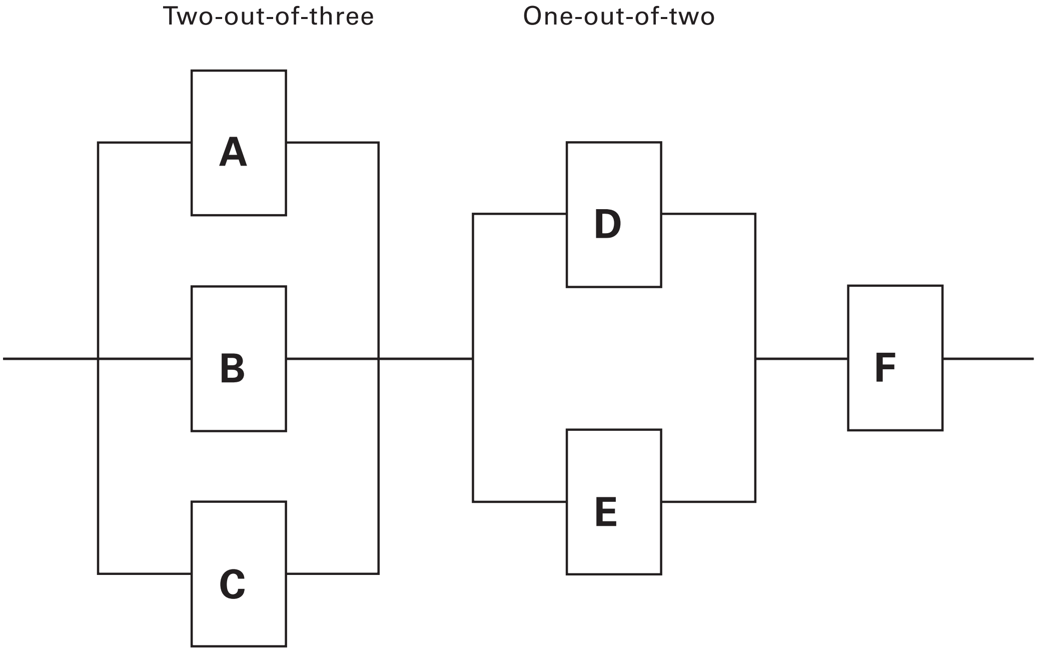


Figure 3.10: Example series-parallel system.

Estimation of the probability of failure of the two-out-of-three-system:
The two-out-of-three-system fails if one of the following combinations of events occur.

$$\begin{gathered}\bar{A}\cap\bar{B}\cap C\\ \bar{A}\cap B\cap\bar{C}\\ A\cap\bar{B}\cap\bar{C}\\ \bar{A}\cap\bar{B}\cap\bar{C}\end{gathered}\tag{3.32}$$

These four combinations of events are mutually exclusive. This implies that equation (3.25) can be used to calculate the probability of failure of the two-out-of-three-system:

$$P(2/3 \text{ fails}) = P(\bar{A}\cap\bar{B}\cap C) + P(\bar{A}\cap B\cap\bar{C}) + P(A\cap\bar{B}\cap\bar{C}) + P(\bar{A}\cap\bar{B}\cap\bar{C}) \qquad (3.33)$$

Because it is assumed that the component failures are independent, equation (3.35) can be rewritten as:

$$\begin{aligned} P(2/3 \text{ fails}) &= P(\bar{A}).P(\bar{B}).\{1 - P(\bar{C})\} + P(\bar{A}).\{1 - P(\bar{B})\}.P(\bar{C}) \\ &\quad + P\{1 - P(\bar{A})\}.P(\bar{B}).P(\bar{C}) + P(\bar{A}).P(\bar{B}).P(\bar{C}) \qquad (3.34) \\ &= P(\bar{A}).P(\bar{B}) + P(\bar{A}).P(\bar{C}) + P(\bar{B}).P(\bar{C}) - 2.P(\bar{A}).P(\bar{B}).P(\bar{C}) \end{aligned}$$

The probability of failure for each component is equal to 0.1 :

$$P(\bar{A}) = P(\bar{B}) = P(\bar{C}) = 0.1 \qquad (3.35)$$

Substitution of (3.35) in equation (3.34) gives the probability of failure of the two-out-of-three system:

$$\begin{aligned} P(2/3 \text{ system fails}) &= 3.\ (0.1)^2 - 2.\ (0.1)^3 \qquad (3.36) \\ &= 0.028 \end{aligned}$$

Equation (3.34) can be deduced directly from a Venn diagram, see figure 3.11. In the Venn diagram the probability of failure of the two-out-of-three system is depicted by the intersection of (A and B) plus the intersection of (A and C) plus the intersection of (B and C). By these three intersections the intersection of the events A, B and C is counted three times. To correct this, one has to subtract twice the intersection of the events A, B and C.

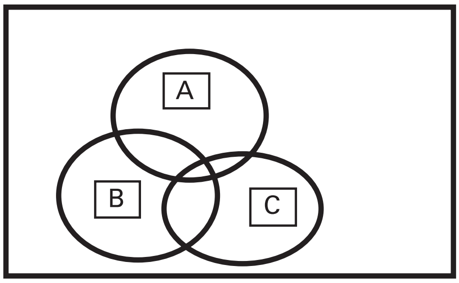


Figure 3.11: Venn diagram two-out-of-three system.

The following equation can be deduced directly from the Venn diagram:

$$\begin{aligned} P(\text{2/3 system fails}) &= P\{(\bar{A}\cap\bar{B})\cup(\bar{A}\cap\bar{C})\cup(\bar{B}\cap\bar{C})\} \\ &= P\ (\bar{A}\cap\bar{B}) + P\ (\bar{A}\cap\bar{B}) + P\ (\bar{B}\cap\bar{C}) - 2.P(\bar{A}\cap\bar{B}\cap 1\bar{C}) \end{aligned} \qquad (3.37)$$

Estimation of the probability of failure of the one-out-of-two system:
The estimation of the probability of failure of the one-out-of-two system is straight forward. Application of equation (3.31) holds:

$$\begin{aligned} P(\text{1/2 system fails}) &= P(\bar{D}).P(\bar{E}) \\ &= 0.\ 1 * 0.1 \\ &= 0.01 \end{aligned} \qquad (3.38)$$

Estimation of the overall system failure probability:
The probability of failure of the whole system can be calculated with equation (3.28):

$$\begin{aligned} P(\text{System fails}) &= 1 - \{1 - P(\text{2/3 fails})\}.\{1 - P(\text{1/2 fails})\}.\{1 - P(F)\} \\ &= 1 - (1 - 0.028).(1 - 0.01).(1 - 0.1) \\ &= 0.134 \end{aligned} \qquad (3.39)$$

Application of the rare event approximation results in:

$$\begin{aligned} P\ (\text{System fails}) &\approx P(\text{2/3 System fails}) + P(\text{1/2 System fails}) + P(F) \\ &\approx 0.028 + 0.01 + 0.1 \\ &\approx 0.138 \end{aligned} \qquad (3.40)$$

As expected, the difference between both results is small and the result calculated with the rare event approximation is conservative.

3.7 REFERENCES

[3.1] Reliability Evaluation of Engineering Systems, Concepts and Techniques, Roy Billington and Ronald Allen, Pitman Advanced Publishing Program, Boston. London. Melbourne, 1983.

[3.2] Fault Tree Handbook, U.S. Nuclear Regulatory Commission NUREG-0492.

[3.3] Terrence L. Fine,
Theories of Probability, An Examination of Foundations, 1973, Academic Press, New York.

[3.4] Roy Weatherford,
Philosophical Foundations of Probability Theory,
1982, Routledge & Kegan Paul, Lodon, ISBN 0-7100-9002-1.

[3.5] E. De Leede, J. Koerts,
On the Notion of Probability: a Survey,
1977, Erasmus University, Rotterdam, report 7704/ES.

[3.6] Harold Jeffreys, Theory of Probability,
3rd edition 1983, Clarendon Press, Oxford, ISBN 0-19-853193-1.

STATISTICS

CONTENTS **Page**

4.1 INTRODUCTION

This chapter deals with methods of processing available failure and accident data to facilitate estimation of the reliability characteristics. The purpose of this chapter is to provide background information and more in-depth knowledge.

First, it will be outlined briefly how these failure and accident data are established. Then the important concepts of randomness and representativeness are discussed at length. Finally, concept of correlation will be explained.

In paragraph 4.4 probability distributions that are frequently used in risk and reliability analyses will be introduced.
Paragraph 4.5 will describe some important concepts used for estimation and in paragraph 4.6 the estimation of time dependent reliability characteristics will be explained.

To combine data from different sources, for instance generic data and plant-specific data, the Baysian update process has to be used. This approach is explained in the last paragraph of this chapter.

4.2 NOMENCLATURE

A	=	event	-
B	=	event	-
E	=	expected value	-
EF	=	error factor	-
F(x)	=	cumulative distribution function	-
f(x)	=	density function	-
L	=	likelihood function	-
n	=	number of samples or number of trials	-
MTTF	=	Mean time to failure	hour
MTBF	=	Mean time between failure	hour
RF	=	range factor	-
P	=	probability	-
t	=	time	hour
x	=	random variable	-
α	=	parameter Weibull distribution	-
β	=	parameter Weibull distribution	-
λ	=	failure rate	-
			hour
θ	=	estimator, characteristic life	-
σ	=	standard deviation	-
μ	=	mean repair duration	hour
X	=	Chi-squared distribution	-

Subscript:

LV	=	lowest value uniform distribution
HV	=	highest value uniform distribution
ml	=	maximum likelihood

4.3 IMPORTANT CONCEPTS IN STATISTICS

4.3.1 Establishment of Failure Data

Failure data can be established in two different ways:

- One way is to carry out an experiment according to a specific test arrangement. In experiments attempts are made to control the conditions as far as possible. An example of this is testing several prototypes under specified conditions. The observations obtained are called experimental data.

  The other way is to collect data from practice. The conditions under which these data are established can differ considerably. The way in which the data are established and recorded is one of the most important aspects in analyzing such data. These data are called *field data.*

In both cases *representativeness* plays a major role; what do the data represent and what can be concluded from them?

- In the case of experiments, the amount of data available is usually limited. From a large group of switches, for example, only 10 new specimens are tested under specified conditions. These 10 switches are regarded as representative of the whole group of switches about which certain statements are to be formulated. It is assumed here that the conditions under which the whole group of switches is used are identical to the test conditions. In statistics, such a whole group of switches is called a *population*. The 10 switches tested are part of this population, called in statistics a *sample.*

4.3.2 Population, sample, non-randomness, representative

A population is a set of elements which satisfy a specific description. The description must be such that it is clear whether any object is an element of the population or not.

For example, all valves of a specific type in a refinery form a population. Assume one is interested in specific data (the MTBF, for example) of such valves. It is not possible to involve all relevant valves in the study, so one has to decide on closer examination of a sample from the valve population.

A sample is one part of a population. But the sample must be really representative of the relevant group of valves. This can be achieved by taking a random sample from the valve population.

A random sample is a sample in which all elements are obtained by random sampling. Random sampling of an element is understood to mean a sampling method in which each qualifying element has the same probability of being selected.

In case of the valves mentioned above, this is achieved by numbering all qualifying valves and selecting some of the numbers by drawing lots. The valves corresponding to the numbers drawn are then included in the examination.

Non-randomness of a sample can come about in different ways. Deliberate selection of what is regarded as representative of the population usually leads to a non-random sample due to the prejudices of the person arranging the study.

The concepts *random* and *representative* often lead to misunderstanding. Yet there is a distinct difference between them. Random relates to the method by which the sample is taken, and representative relates to the result of a sample that was taken. A random sample does not necessarily have to be representative of the population it is taken from. The probability of obtaining a non-representative sample is certainly not very high if the sample size is not too small.

Two examples will be provided of samples which are not random with regard to the characteristic to be examined:

- An insight must be obtained into the distribution of families according to size, based on a sample from a specific group of the population. To this end an arbitrary number of people are selected from the relevant group of the population and asked about the size of the family they come from. This sample is indeed random with regard to the people interviewed but not with regard to the relevant characteristic "family size". Large families are too strongly represented in the sample because, with this sampling method, large families have a relatively higher probability of being included in the sample.

- It is found in a company that the total time spent on machinery repairs has risen in a specific year. To find out whether the cause lies in a higher frequency in the number of repairs or in a longer repair time per case, management decides to examine - by way of a sample on several set days spread over the year - how many repairs are carried out on those dates and how much time they take on average. As far as the repair time is concerned, as in the previous example there will be a distortion in favor of the number of long-term repairs, which can lead unjustly to the impression that the average repair time has increased.

The examples described above relate to homogeneous populations. However in practical situations one may encounter a heterogeneous population. The composition of the population will then have to be taken into account when arranging a random sample.

This is done by dividing the population into several (homogeneous) subpopulations. A random sample is then taken from each subpopulation. The total of these samples forms a random sample.

This will be illustrated with an example:

- An aircraft manufacturer needs to better understand the failure behavior of aircraft he sells in order to be able to organize major overhauls efficiently. Two hundred of a specific type of aircraft are in use all over the world. The manufacturer knows from experience that climatic conditions in particular can cause differences in the type of failures. To obtain a correct picture of this, it is decided to examine this aspect by means of a sample. Three climatic zones are distinguished. The aircrafts sold are distributed among the climatic zones as tabulated in table 4.1.

Table 4.1: Distribution of aircrafts		
Population	Region	Number of aircraft
A	Polar regions	20
B	Temperate zones	100
C	Tropics	80

To achieve a representative sample, the manufacturen must take a random sample from each of the subpopulations (A, B and C), seeing to it that the ratio between sample sizes -say n_A, n_B, and n_C is 1 : 5 : 4. The sample obtained is random with regard to the failure behavior of the aircraft in use in the different climatic zones.

Setting up representative samples is an art in itself. There is excellent literature on this subject, e.g. [4.1].

4.3.3 Correlation

A correlation diagram is often used to indicate the relationship between two variable factors. Consider, for example, the height and weight of 13-week-old baby boys. These two factors are plotted against each other for a group of these children in figure 4.1.

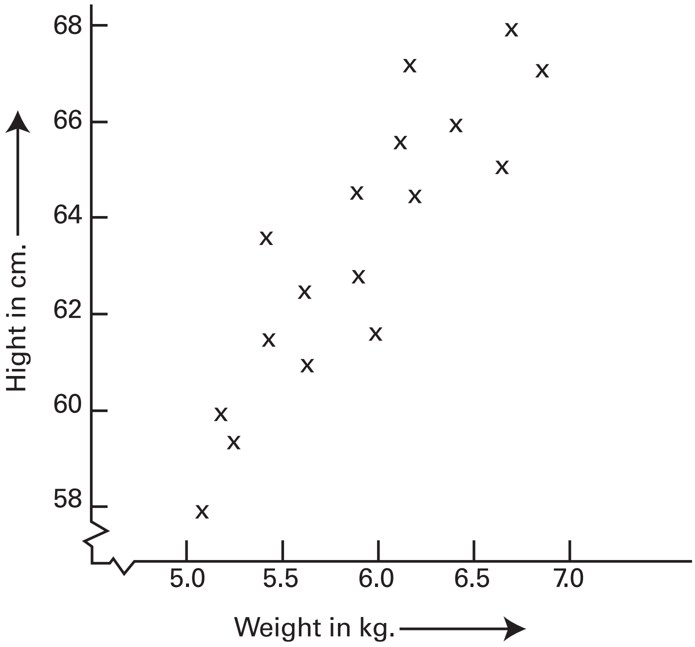


Figure 4.1: A correlation diagram.

The diagram in figure 4.1 shows a reasonable relationship between height and weight. But such a relationship can also develop by accident, so it must be examined first whether it is likely that a certain relationship will exist.

In the search for a (linear) relationship between two variables, a random sample yields pairs of observations (x_i, y_i) from the same population; these are the height and weight of thirteen-week-old baby boys in our example above. So the sample relates to both variables and one cannot earmark of the variables a priori as explanatory of the other; either in other words, it is not known in advance whether a change in one variable directly causes a change in the other.

If an increase in one variable is combined with an increase in the other variable, the variables are called positively correlated. But if an increase in one variable is combined with a decrease in the other, the variables are called negatively correlated.

The existence of correlation does not simply mean that there is a causal relationship between the variables. There can be various other reasons for a statistical relationship which can lead to different interpretations. On the one hand a highly misleading picture can be developed because the observation material is non random, while on the other hand even real statistical coherence does not give a definite answer as to the causes resulting in that coherence.

4.4 PROBABILITY DISTRIBUTIONS

A stochastic variable is a variable which, in a given situation, can adopt different values for which it has a probability distribution. It cannot be predicted with certainty what the value of that variable will be. One can describe the probabilities associated with the stochastic variable by a table of values, but it is easier to write a formula that permits calculation of $P(x_i)$ by substitution of the appropriate value of x_i. Such a formula is called a probability distribution function for the random variable $\underline{x}$.

In this paragraph several probability distributions, which are frequently used in risk and reliability analyses will be explained. Only the main characteristics will be provided; recommended sources for further study are [4.2], [4.3] and [4.4].

4.4.1 Definitions

The cumulative distribution function F(x) is defined as the probability that the random variable x assumes values of less than or equal to the specific value x.

$$F(x) = P(\underline{x} \leq x) \tag{4.1}$$

According to equation (4. l), F(x) is a probability and thus must only assume values between zero and one.

$$0 \leq F(x) \leq 1 \tag{4.2}$$

An important property of the cumulative distribution function is that F(x) never decreases in the direction of increasing x. If x ranges from –∞ to +∞ then:

$$F(-\infty) = 0 \qquad (4.3)$$
$$F(+\infty) = 1$$

For a continuous stochastic variable the probability density function, f(x) is obtained from F(x) by a process of differentiation:

$$f(x) = \frac{d\,F(x)}{dx} \qquad (4.4)$$

An equivalent statement is:

$$F(x) = \int_{-\infty}^{x} f(t)\,dt \qquad (4.5)$$

The properties of probability density functions make it possible to treat the areas under f(x) as probabilities:

$$P\,(x_1 \leq \underline{x} \leq x_2) = \int_{x_1}^{x_2} f(t)\,dt \qquad (4.6)$$

4.4.2 Mean, median and mode of a distribution

For a sample containing n items the sample mean is defined by:

$$\mu = \sum_{i=1}^{n} \frac{x_i}{n} \qquad (4.7)$$

The sample mean can be used to estimate the population mean, which is the average of all outcomes. For a continuous distribution the mean is derived by extending this idea to cover the range -∞ to +∞. The mean of a distribution is usually denoted by μ:

$$\mu = \int_{-\infty}^{+\infty} x\,f(x)\,dx \qquad (4.8)$$

Instead of the mean value often the term expected value, indicated by E, is used. The median value is the mid-point of the distribution, i.e. the point at which half of the measured values fall to either side. The value at which the distribution peaks is called the mode (see figure 4.2).

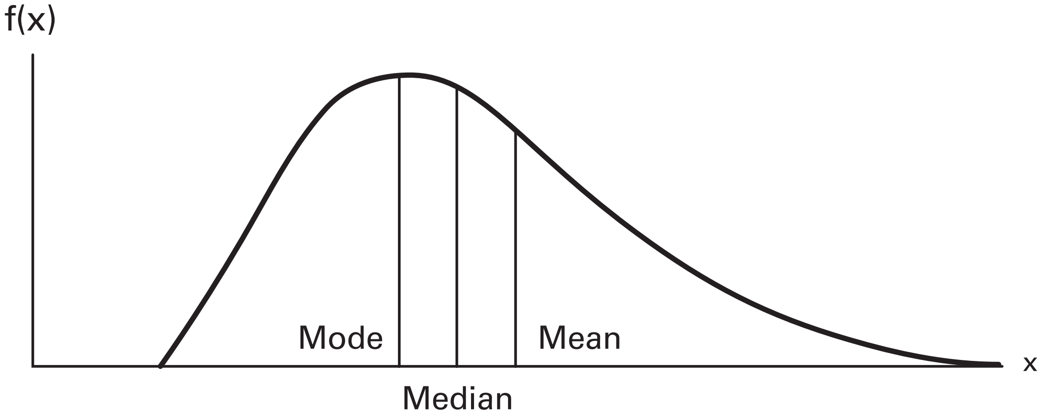


Figure 4.2: Mean, median and mode of a distribution.

4.4.3 **Spread of a distribution**

The spread or the extent to which the valnes which make up the distribution vary, is measured by its variance. For a sample size n the variance (Var(x)), is given by:

$$\mathrm{Var}(x) = \frac{\sum_{i=1}^{n} (x_i - \mu)^2}{n} \qquad (4.9)$$

The variance for a continuous distribution is given by:

$$\sigma^2 = \int_{-\infty}^{+\infty} (x - \mu)^2 f(x)\, dx \qquad (4.10)$$

Sigma (σ) is called the standard deviation.

4.4.4 **Binomial Distribution**

To explain the binomial distribution, consider a system which consists of three redundant identical components (see figure 4.3).

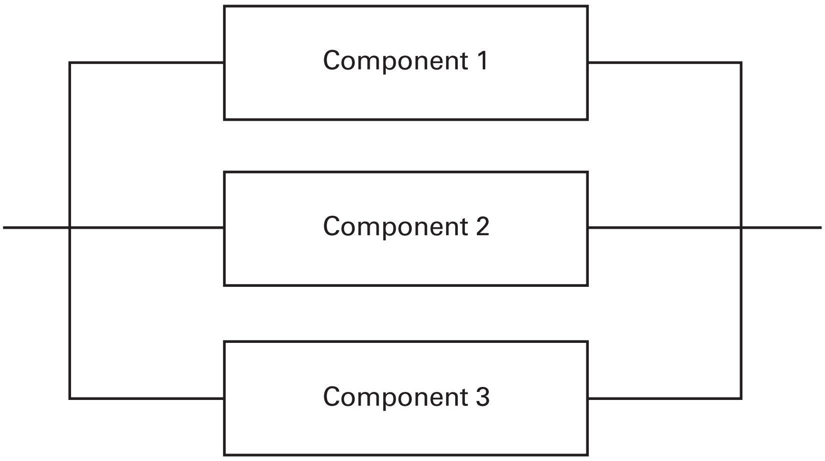


Figure 4.3: Two-out-of-three system.

The system will fail if two out of three components fail (two-out-of-three system). The following ways of system failure are possible:

- failure of components 1 and 2
- failure of components 1 and 3
- failure of components 2 and 3

The probability of having exactly two failures can be calculated as follows:

$$P(1 \text{ and } 2) = p_1\ p_2\ (1 - p_3)$$

$$P(1 \text{ and } 3) = p_1\ p_3\ (1 - p_2) \qquad (4.11)$$

$$P(2 \text{ and } 3) = p_2\ p_3\ (1 - p_1)$$

Assume $p_1 = p_2 = p_3 = p$. Adding all three expressions of formula (4.11) results in:

$$P(\text{Exactly two failures}) = 3\ p^2\ (1 - p) \qquad (4.12)$$

Expression (4.12) can be generalized for an x-out-of-n system. The probability of having exactly x component failures in an equal and independent situation is given by the binomial distribution. The general expression for the binomial distribution in n equivalent and independent situations is:

$$P(\text{Exactly x occurrences in n trials}) = \frac{n!}{x!\ (n-x)!}\ p^x\ (1 - p)^{n-x} \qquad (4.13)$$

The binomial distribution gives the probability of obtaining x occurrences of an event, in a sample of n triais, when the probability of an event is p and the probability of not having the event is (1-p) and the events are independent.

In addition to two components failing, the two-out-of-three system can also fail if three components fail. In general, a k-out-of-n system will fail if k or more components fail. To describe the total failure probability of a k-out-of-m system, the cumulative binomial distribution has to be used:

$$\text{P(At least k occurrences in n trials)} \;=\; \sum_{s=k}^{n} \frac{n!}{s!\,(n-s)!} \quad p^{s}\,(1-p)^{n-s} \tag{4.14}$$

The mean and the variance of the binomial distribution are given by (see reference [4.5], paragraph 3.2.4):

$$\begin{aligned} \mu &= np \\ \text{Var}(x) &= np\,(1-p) \end{aligned} \tag{4.15}$$

It should be emphasized that the binomial distribution can only have values at points where x is an integer.

4.4.5 **Poisson Distribution**

The Poisson distribution together with the exponential distribution forms the statistical basis of many reliability and safety studies in practice. In general, it can be said that the Poisson distribution applies to events occurring in mutual independence in a continuum of space, time, area, length, etc. Some examples of typical Poisson events are:

- the number of alpha particles from a radioactive source recorded per minute by a Geiger counter (number per unit of time).
- the number of yarn breakages per 1000 m in a spinning mill (number per unit of length)
- the number of defects, accidents etc. in a production process (number per unit of time) if at the same time the requirement is satisfied that, after occurrence of such an event, the probability of a new event is just as high as before.

The Poisson distribution can be derived by considering the Poisson distribution as a limiting form of the binomial distribution. The limiting conditions are: n.p is constant, n goes to infinity and p goes to zero. For these conditions two relations can be derived (see appendix A):

$$\text{If:} \quad \begin{aligned} np &= \text{constant} \\ n &\rightarrow \infty \\ p &\rightarrow o \end{aligned} \tag{4.16}$$

$$\text{Then:} \quad \begin{aligned} \frac{n!}{x!(n-x)!} &\approx \frac{n^{x}}{x}\ ! \\ (1-p)^{n-x} &= \exp(-np) \end{aligned} \tag{4.17}$$

Substitution of equations (4.17) in the expression for the Binomial distributions (4.13) holds:

$$P(x) = \frac{n^{x}}{x!}\; p^{x} \exp(-np) \tag{4.18}$$

This can be rewritten as:

$$P(x) \;=\; \frac{(np)^x}{x!}\,\exp(-np) \tag{4.19}$$

Formula (4.19) represents the Poisson distribution. The Poisson distribution gives the probability of exactly x occurrences of a rare event (p → 0) in a large number of trials (n → ∞). The Poisson distribution is a discrete probability distribution and not a probability density distribution.

The expected number of occurrences, also indicated by the mean value μ, is given by:

$$E\,(x) = np \tag{4.20}$$

The Poisson distribution is important not only because it approximates the binomial distribution, but because it describes the behavior of many rare-event occurrences, regardless of their underlying physical processes.

4.4.6 Exponential Distribution

This is a frequently used failure probability distribution in reliability and safety studies. The distribution concerns the time between consecutive failure events, the distribution is characterized by a constant failure rate λ. This implies that the mean time between two consecutive failure events is constant. Another characteristic is that the probability of a future failure event is independent of what has occurred in the past. This is called the memory less characteristic of the exponential distribution.

To derive the expression for the exponential distribution, consider the situation that one is interested in the probability of exactly zero system failures. Applying the Poisson distribution for this situation holds:

$$P(x = 0) = \exp(-np) \tag{4.21}$$

The term np represents the expected number of failures in a large number of trials. Suppose one has field data of system failure occurrences during operating time t. One can state that, on average, a failure occurs every MTTF hours.

$$\text{MTTF} \;=\; \frac{\text{operating time}}{\text{number of failures}} \qquad 4.22)$$

The expected number of failures {n.p(t)} in operating time t can be expressed as:

$$np(t) \;=\; \frac{t}{\text{MTTF}} \tag{4.23}$$

For the exponential distribution it is assumed that:

$$\lambda = \text{constant} \qquad\qquad (4.24)$$

$$\lambda = \frac{1}{\text{MTTF}}$$

Equations (4.23) and (4.24) hold that:

$$np(t) = \lambda t \qquad\qquad (4.25)$$

Substitution of equation (4.25) in the expression of the Poisson distribution for zero failure gives:

$$P(X = 0) = \exp(-\lambda t) \qquad\qquad (4.26)$$

The probability of zero failures in time t {P(x = 0)} represents the reliability of the system:

$$R(t) = P(\text{at } t \in \underline{x} = 0) \qquad\qquad (4.27)$$

The concept of reliability will be explained in more detail in chapter 5.

Expression (4.26) can be rewritten as follows:

$$R(t) = e^{-\lambda t} \qquad\qquad (4.28)$$

The unreliability or the probability of failure in time t, is given by:

$$\begin{aligned} F(t) &= 1 - R(t) \\ &= 1 - e^{-\lambda t} \end{aligned} \qquad\qquad (4.29)$$

And the failure density or the probability density function of the exponential distribution is equal to:

$$\begin{aligned} f(t) &= \frac{dF(t)}{dt} \\ &= \lambda e^{-\lambda t} \end{aligned} \qquad\qquad (4.30)$$

Equation (4.30) is generally referred to as the exponential distribution of time to failure or simply as the exponential distribution. The exponential distribution is frequently used in reliability and safety studies. The distribution is characterized by a constant failure rate and a constant mean time to failure. Another characteristic of the exponential distribution is that the probability of failure in the interval (t,t+Δt) is the same as the probability of failure in any interval of the same length, given that no failure has occurred up to time t. For the exponential distribution it can be stated that the failure history of a component does not influence the failure behavior of the component in the future.

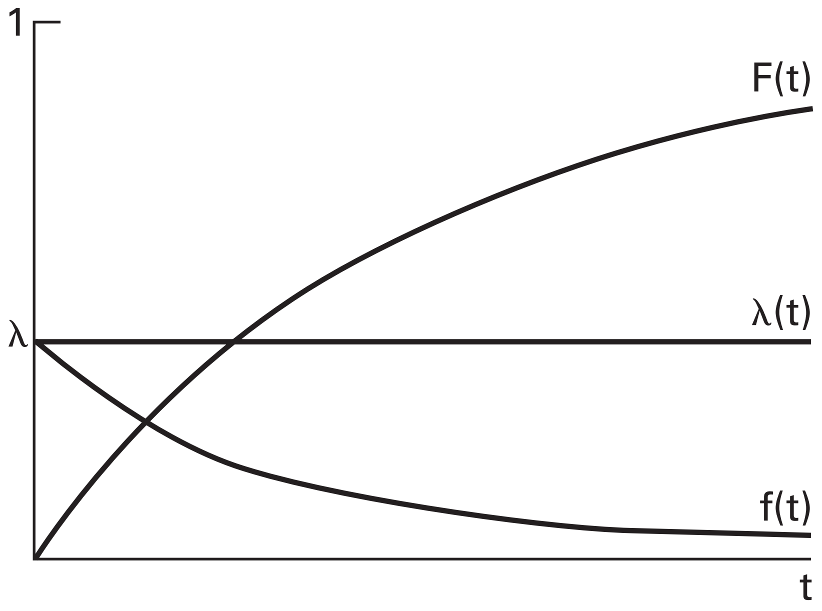


Figure 4.4: Characteristics of the exponential distribution.

4.4.7 Normal Distribution

The normal distribution relates to a stochastic variable which can adopt all values between $-\infty$ and $+\infty$. The probability density function of the normal distribution is:

$$f(x) = \frac{1}{\sigma\sqrt{2\Pi}} \exp[-\frac{1}{2}(\frac{X-\mu}{\sigma})^2] \tag{4.31}$$

The distribution can be characterized by two parameters, i.e. the mean value and the variance.

$$\begin{aligned} x_{mean} &= \mu \\ Var(x) &= \sigma^2 \end{aligned} \tag{4.32}$$

4.4.8 Standardized normal distribution

The normal distribution is extensively tabulated but not in the form of expression (4.31). A direct tabulation would require extensive coverage of values of the parameters μ and σ. To tabulate the normal distribution in a more practical way, one has found a transformation which has the effect of standardizing μ to 0 and σ to 1. This transformation is:

$$\text{Transformation: } z = \frac{x-\mu}{\sigma} \tag{4.33}$$

The corresponding distribution in terms of z is:

$$f(z) \quad = \quad \frac{1}{\sqrt{2\Pi}} \ \exp(-\ \frac{1}{2}\ z^2) \tag{4.34}$$

Expression (4.34) is known as the standardized normal distribution, which forms the basis for all tabulations.

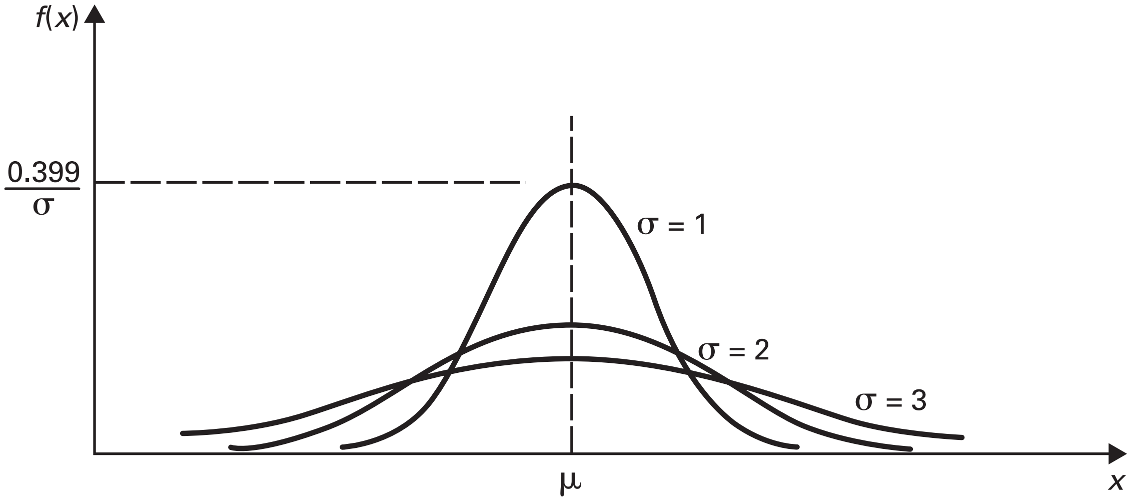


Figure 4.5: Normal distribution.

4.4.9 **Lognormal Distribution**

The lognormal distribution is used quite frequently in reliability and safety studies. The relationship to normal distribution is as follows: if the stochastic variable ln(x) has a normal distribution, x has a lognormal distribution. The probability density function is given by:

$$f(x) \quad = \quad \frac{1}{x\sigma\sqrt{2\Pi}} \quad \exp[-\ \frac{\{\ln(x)-\mu\}^2}{2\sigma^2}\ ] \tag{4.35}$$

The error factor is defined as follows:

$$EF \quad = \sqrt{\frac{x_{0.95}}{x_{0.05}}} \tag{4.36}$$

The median value, mean value and variance are given by:

$$
\begin{aligned}
x_{median} &= \exp(\mu) \\
x_{mean} &= \exp(\mu + 0.5\sigma^2) \\
Var(x) &= \exp(2\mu + \sigma^2)\,\{\exp(\sigma^2)-1\} \\
&= (x_{mean})^2\,\{\exp(\sigma^2)-1\}
\end{aligned}
\tag{4.37}
$$

In most cases the mean value and the error factor are known. The other parameters of the lognormal distribution can be calculated with the following useful expressions:

$$
\begin{aligned}
EF &= \frac{x_{0.95}}{x_{median}} = \frac{x_{median}}{x_{0.05}} \\
\sigma &= \frac{\ln(EF)}{z_{0.95}} = \frac{\ln(EF)}{1.645} \\
\mu &= \ln(x_{mean}) - 0.5\,\sigma^2
\end{aligned}
\tag{4.38}
$$

The relation between the mean value and the median value is given by:

$$
x_{median} = \frac{x_{mean}}{\exp(0.5\,\sigma^2)}
\tag{4.39}
$$

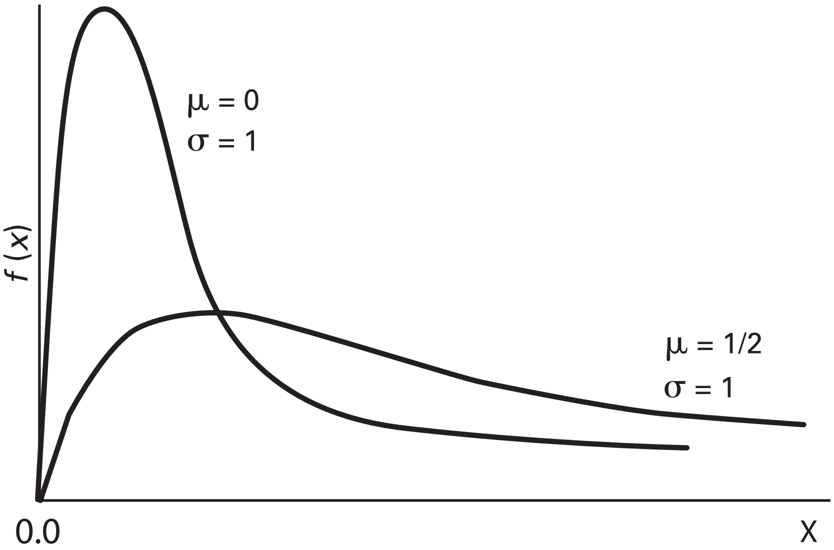


Figure 4.6: Lognormal distribution.

4.4.10 **Uniform and loguniform distributions**

The probability density function of the uniform distribution is given by:

$$f(x) \quad = \quad \frac{1}{x_{HV} - x_{LV}} \tag{4.40}$$

The cumulative distribution function of the uniform distribution can be obtained by integration of equation (4.40):

$$\begin{aligned} F(x) &= \int_{LV}^{x} f(x)\,dx \\ &= \frac{x - x_{LV}}{x_{HV} - x_{LV}} \end{aligned} \tag{4.41}$$

x_{LV} = lowest value of x
x_{HV} = highest value of x

The loguniform distribution can be used if one wants to perform an uncertainty analysis for a parameter which is bounded by a minimum and a maximum value. Considering the expression of the uniform distribution the loguniform distribution is defined by:

$$\begin{aligned} F(x) &= \frac{\ln(x) - \ln(x_{LV})}{\ln(x_{HV}) - \ln(x_{LV})} \\ &= \frac{\ln(x) - \ln(x_{LV})}{\ln(\frac{x_{HV}}{x_{LV}})} \end{aligned} \tag{4.42}$$

A range factor (RF) can be defined as:

$$RF \quad = \quad \sqrt{\frac{x_{HV}}{x_{LV}}} \tag{4.43}$$

Substitution of the range factor in expression (4.42) gives:

$$F(x) \quad = \quad \frac{\ln(x) - \ln(x_{LV})}{2\ln(RF)} \tag{4.44}$$

Differentiation of expression (4.44) gives the probability density function of the loguniform distribution:

$$f(x) = \frac{1}{2 \text{ x } \ln(RF)} \tag{4.45}$$

In practice, mostly the mean value and the range factor are known or have to be selected by the analyst. The following formulas can be used to determine the median values and the lowest and highest values.

$$x_{median} = \frac{2 \; RF \ln(RF)}{RF^2 - 1} \; x_{mean}$$

$$x_{LV} = \frac{x_{median}}{RF} \tag{4.46}$$

$$x_{HV} = x_{median} \; RF$$

4.4.11 **Weibull distribution**

The Weibull distribution has one very important property; the distribution has no specific characteristic shape. Depending upon the values of the parameters in its probability density function, it can be shaped to represent many distributions as weil as to fit sets of experimental data. For this reason the Weibull distribution has a very important role to play in the statistical analysis of experimental data.

The Weibull probability density function is defined as:

$$f(x) = \frac{\beta \, (x - \delta)^{\beta\text{-}1}}{(\theta - \delta)^{\beta}} \; \exp[-(\frac{x - \delta}{\theta - \delta})^{\beta}] \quad \text{where } x \geq \delta \geq 0 \text{ and } \theta > \delta, \; \beta > 0 \tag{4.47}$$

The cumulative distribution function is given by:

$$F(x) = 1 - \exp[-(\frac{x - \delta}{\theta - \delta})^{\beta}] \tag{4.48}$$

If x is replaced by t, in equations (4.47) and (4.48), equation (4.49) describes the failure density function and equation (4.48) the cumulative failure distribution. The failure rate can be derived with the following relation (see chapter 5):

$$\lambda(t) = \frac{f(t)}{1 - F(t)}$$

$$= \frac{\beta \, (t - \delta)^{\beta - 1}}{(\theta - \delta)\beta} \tag{4.49}$$

β = shape parameter
δ = lowest value life parameter
θ = characteristic life

Typical shapes can be produced for the Weibull distribution including the exponential case ($\beta = 1$, $\delta = 0$, $\lambda = 1/\theta$) as shown in figure 4.7.

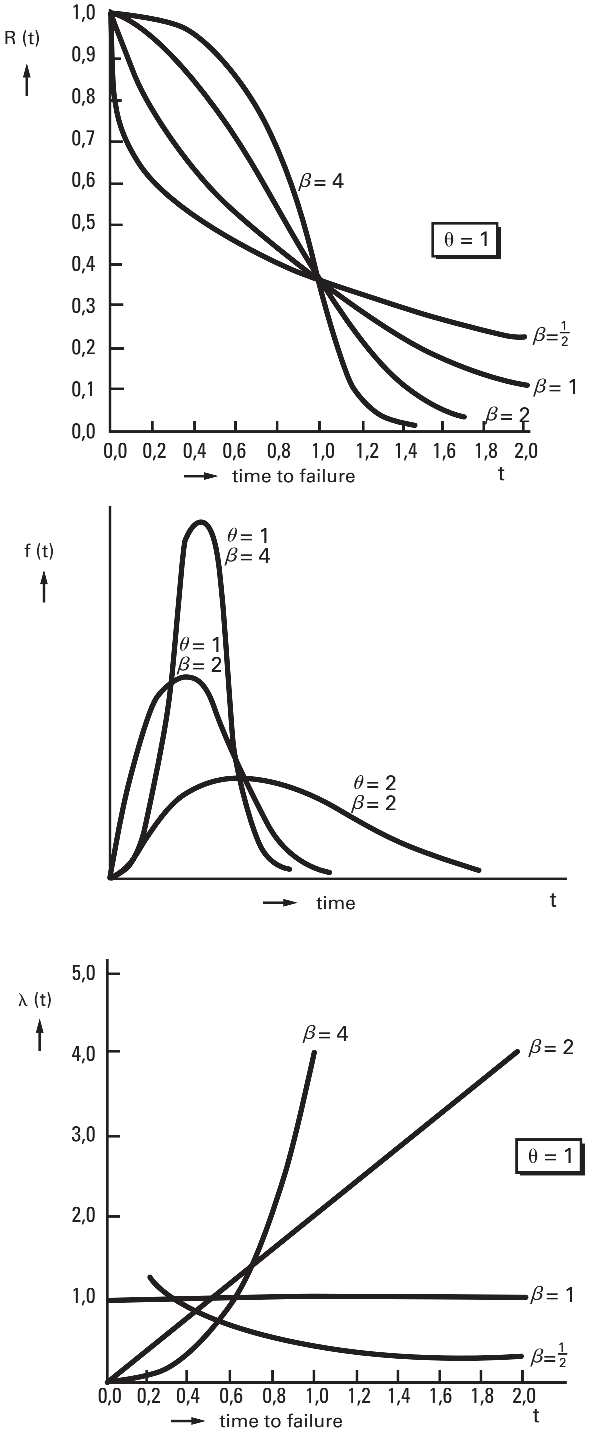


Figure 4.7: Examples of Weibull distribution functions.

4.4.12 Gamma distribution

The probability density function of a gamma distribution is:

$$f(x) \;=\; \frac{1}{\Gamma(r)} \; \lambda^{r}\, x^{r-1} \exp(-\lambda x) \quad \text{for: } x > 0,\, \beta > 0,\, \lambda > 0 \tag{4.50}$$

The gamma function is given by:

$$\Gamma(r) \;=\; \int_{0}^{\infty} t^{r-1}\, e^{-t}\, dt \tag{4.51}$$

The parameter r is known as the shape factor and λ as the scale parameter. The gamma distribution is used in the Baysian update process as describes in section 4.7.0 and chapter 6.

4.4.13 Chi-Square distribution

The probability density function of the Chi-square distribution is given by:

$$f(x) \;=\; \frac{1}{2^{n/2}\,\Gamma(n/2)} \; x^{n/2-1)} \exp(-x/2) \tag{4.52}$$

The parameter n is known as the degree of freedom. Values of the cumulative Chi-square distribution for two percentage probabilities and various values of n are tabulated in appendix A of chapter 6. The Chi-square distribution is used in estimation of the confidence bounds in a plant specific data analysis, see chapter 6.

4.4.14 F distribution

The probability density function of the F-distribution is given by:

$$f(x) \;=\; \frac{\Gamma(\frac{(m+n)}{2})}{\Gamma(\frac{m}{2})\;\Gamma(\frac{n}{2})} \; m^{m/2}\, n^{n/2} \; \frac{x^{(m-2)/2}}{(mx+n)^{(m+n)/2}} \text{ for } x > 0 \tag{4.53}$$

The parameters m and n are known as the degrees of freedom. The F-distribution is used in estimation of the confidence bounds of probabilities of failure on demand in a plant specific data analysis, see chapter 6.

4.5 BASIC CONCEPTS IN ESTIMATION

In this section some basic concepts will be explained which are used in the theory of estimation. This serves as an explanation of the general philosophy on which this theory is based.

Using sample data, one has to try to determine as far as possible the characteristics of a population. This is never a precise science because coincidence plays a role. Not only do the data in a sample differ from each other, any subsequent samples can also give a different picture than the sample taken previously. If the sampling method (i.e. the way in which the sample is taken) results in a thoroughly representative sample, the differences will not be too great as a rule. A population can often be described by a probability distribution. Based on the sample taken - usually limited in size - attempts are made to estimate the parameters of the probability distribution.

4.5.1 Estimation Theory

Estimation theory is the theory developed to determine the parameters in a probabilistic model from statistical data taken on the items governed by the model. The model parameters are computed from certain calculations made with the data. Estimation theory provides guidelines for efficient and accurate computations.

An estimator is a statistic used to estimate the unknown value of a population parameter. The numerical value of the estimator for a given sample is called the estimate of the parameter. To achieve a *good* estimator, it must be stated first what is meant by this. Three requirements can be formulated:

- In the first place it is usually required that the expected value of the estimator be equal to the (unknown) population parameter. Such an estimator is called *unbiased.* This characteristic indicates that, if a sample is taken repeatedly from the population, numerical estimates from these samples are equal to the (unknown) parameters.

- In the second place it may required that the variance of the estimator be small. If more than one unbiased estimator is available, the one with the smallest variance is selected. An unbiased estimator with a minimum of variance is called *efficient.*

- Finally, it is also desirable for an estimator to become more accurate (i.e. for its variance to decrease) with an increasing sample size. If the variance approaches zero when the sample size proceeds to infinite, the estimator is called *consistent.*

In many cases intuition is required to determine which sample size qualifies to act as estimator for a population parameter.

The calculation of expected value and variance is an application of the so-called *method of moments:*

$$(x^k) \;=\; \int_{-\infty}^{\infty} x^k\, f(x)\; dx \qquad (4.54)$$

(x^k) is called the kth moment of the stochastic variable x. Here f(x) is the probability density function of x. The first moment is equal to the expected value or mean value $\mu = E(x)$:

$$(x) \;=\; / \;\; x\, f(x)\; dx \qquad (4.55)$$

The k^{th} central moment of the stochastic variable x is given by:

$$((x - \mu)^k) \;=\; \int_{-\infty}^{\infty} (x - \mu)^k\, f(x)\, dx \qquad (4.56)$$

The second central moment, $E((x - \mu)^2)$ is equal to the variance of the stochastic variable x and indicated by Var (x).

There are various mathematical methods which can be applied for calculating estimators. One of the most widely used methods is the method of maximum likelihood.

4.5.2 Maximum Likelihood

A very important technique for calculating estimators is called the method of maximum likelihood. For large sample sizes under rather general conditions, the maximum likelihood technique yields estimators which are consistent and are both a minimum mean square error estimator and a minimum variance unbiased estimator. Even for moderate or small samples, the maximum likelihood technique yields estimators which are generally usable. The technique is based on the supposition that the particular random sample drawn from the population is the most probable one that could have been selected.

Suppose that random samples are taken from a population that is distributed according to the probability density function $f(x;\theta)$ where θ is some unknown population parameter that is to be estimated. Assume that the sample is $x_1, x_2, x_3,......,x_n$ (size n) and that the sample variables are independent. Using the probability density function, one can write down an expression that gives the probability associated with this particular sample. The likelihood function is now defined by:

$$L(\theta) \;=\; f(x_1, \ldots, x_n;\theta) \;=\; \prod_{i=1}^{n} \; f(x_i;\theta) \qquad (4.57)$$

The likelihood function is no longer equal to the probability of the sample but represents a quantity that is proportional to that probability. The most likely estimator of θ, indicated by the symbol θ, is defined as the value of θ at which the likelihood function $L(\theta$ is maximized. The expression for the maximum value can be determined by setting the derivative of the natural logarithm of the likelihood function $\ln(L(\theta))$ with respect to θ equal to zero and solving for θ.

$$\frac{d}{d\theta} \ln L(\theta) = 0 \quad \text{for } \theta = \hat{\theta} \tag{4.58}$$

Taking the natural logarithm of the likelihood function is simply a matter of convenience because most of the probability density functions encountered in risk and reliability analyses are exponential in form and it is easier to work with the natural logarithm than with the function itself. Substitution of formula (4.57) in formula (4.58) results in:

$$\frac{d}{d\theta} \ln L(\theta) = \frac{d}{d\theta} \sum_{i=1}^{n} \ln f(x_i,\theta) = 0 \quad \text{for } \theta = \hat{\theta} \tag{4.59}$$

Assuming a solution is obtainable, the result is written θ_{ML}, the maximum likelihood estimate of the unknown population parameter θ.

Example:

Consider a number of components for which a constant failure rate is assumed. This implies that the failure behavior can be described with the exponential distribution. Reliability testing has been performed for n components. The question to be answered is what is the mean time to failure (θ) of these components? For this application the probability density function of the exponential distribution is written in the form:

$$f(t;\theta) \quad = \quad \frac{1}{\theta} \; \exp(\frac{-t}{\theta}) \tag{4.60}$$

The time to failure of each of the n components is known. Substitution of equation (4.60) in equation (4.59) gives:

$$\frac{d}{d\theta} \sum_{i=1}^{n} \ln \{ \frac{1}{\theta} \exp(\frac{-t_i}{\theta}) \} = 0$$

$$\frac{d}{d\theta} \sum_{i=1}^{n} \{-\ln(\theta) \;\; \frac{t_i}{\theta} \} = 0$$

$$\frac{d}{d\theta} \{-n \ln (\theta) - \frac{1}{\theta} \sum_{i=1}^{n} t_i \} = 0 \tag{4.61}$$

$$-\frac{n}{\theta} + \frac{1}{\theta^2} \sum_{i=1}^{n} t_i = 0$$

$$\frac{1}{\theta} \sum_{i=1}^{n} t_i = n$$

Solving for θ gives the maximum likelihood estimator for the mean time to failure:

$$\theta_{ML} = \frac{1}{n} \sum_{i=1}^{n} t_i \qquad (4.62)$$

By this it is demonstrated that the mean time to failure is simply the arithmetic mean for the failure data collected.

4.5.3 Confidence Interval

By application of the maximum likelihood method, numerical estimates for unknown parameters can be calculated from sample data. Because the estimates obtained are based on small-sized samples, they have a limited accuracy. The estimators themselves are stochastic vatues, so they can deviate from the actual parameter value.

It is therefore advisable not to restrict the estimate to the value calculated from the sample, also called the point estimate, but to indicate an interval around this estimate which includes the actual parameter value with a certain probability. The construction of such an interval is closely related to the probability distribution of the estimator used. The underlying philosophy of the confidence intervals will be discussed first.

An estimate or confidence interval (θ_1, θ_2) means a stochastic interval around the estimate t_1 calculated from a sample which includes the unknown parameter θ with a certain probability, say $(1 - \alpha)$. The stochastic variables θ_1 and θ_2 are called confidence limits and these must satisfy the condition:

$$P(\theta_1 < \theta < \theta_2) \geq (1 - \alpha) \qquad (4.63)$$

Formula (4.63) indicates the two-sided $(1 - \alpha)$% confidence interval, with upper and lower limits. The following applies to a left one sided or a right one-sided confidence interval, respectively:

$$\begin{aligned} P\ (\theta_1 < \theta) &\geq (1 - \alpha_1) \\ P\ (\theta_2 > \theta) &\geq (1 - \alpha_2) \end{aligned} \qquad (4.64)$$

The limits for a two-sided interval are usually selected in such a way that:

$$\alpha_1 = \alpha_2 = \frac{1}{2}\alpha \qquad (4.65)$$

Customary values for α (also called confidence level) are between 0.001 and 0.10. Selection of a value for α depends on the certainty required for a statement to be made about the interval which contains the unknown parameter θ. In risk and reliability analyses a value of 0.05 is usually selected.

Assume that a sample provides an estimate t for the parameter θ. By selecting α, one can determine the $(1 - \alpha)$ percent confidence interval for θ from the observations, for example:

$$\theta 1 < \theta < \theta 2 \tag{4.66}$$

In principle each new sample provides a different estimate t for the parameter θ and thus another confidence interval as well.

4.5.4 Estimation of failure parameters

The objective of the specific data analysis is to find the number of failures in the plant history plus the associated exposure time or number of demands. Based on this data, it is possible to make a statistical analysis to find an estimate of the failure parameter and an uncertainty interval for this estimate.

The estimation of λ (the constant failure rate, parameter of a Poisson process) is estimated by

$$\lambda_{mean} = \frac{f}{T} \tag{4.67}$$

where f is the number of failures andT the exposure time.

The confidence intervals can be determined using statistical techniques as well.The confidence intervals for the parameter λ (the failure rate) can be calculated by applying the formulas:

$$\lambda_{5\%} = \frac{X^2\,(2f\,,\,0.05)}{2T}$$

$$\lambda_{95\%} = \frac{X^2\,(2f+2\,,\,0.95)}{2T} \tag{4.68}$$

Where:

$\lambda_{5\%}$ = lower bound of confidence interval
$\lambda_{95\%}$ = upper bound of confidence interval
$X^2(v,p)$ = p percentile of a Chi-squared distribution with v degrees of freedom
f = number of failures
T = exposure estimate

Tables are available to calculate the values of the Chi-squared distribution (see chapter 6). In figure 4.8 the confidence intervais as a function of the number of failures are shown. From figure 4.7 it can be concluded that the width of the confidence intervals only depends on the number of failures and not on the exposure time.

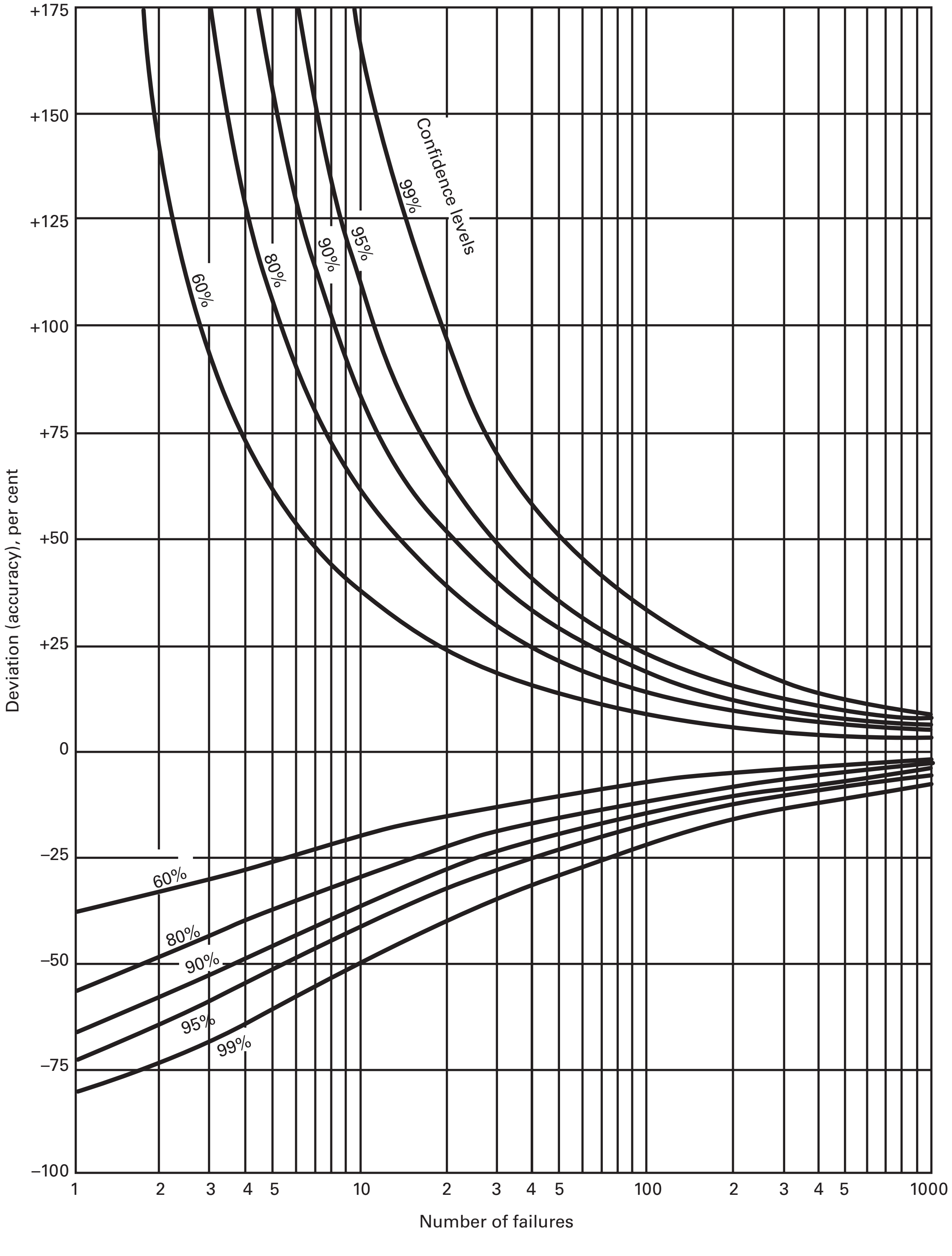


Figure 4.8: Confidence intervals as a function of the number of failures.

4.6 ESTIMATION OF TIME DEPENDENT RELIABILITY CHARACTERISTICS

In this paragraph methods will be provided for estimating some dependent reliability characteristics from the available failure data. These methods can in principle be divided into two groups.

On the one hand, the reliability characteristics can be estimated direct from the failure data; these estimation procedures are called *direct* methods. They have the advantage that they are quite fast and easy to carry out. The disadvantage is that they cannot always be used for accurate estimates.

On the other hand, a distribution function can first be determined using failure data, from which the reliability characteristics can then be calculated. These so-called *indirect* methods have the disadvantage that sufficient failure data must be available. Moreover, there is not always an easy way of determining the distribution function. An advantage of the indirect procedure is that reliability characteristics can be estimated for any moment required by using the distribution function obtained.

4.6.1 Direct methods

Selection of the estimation method is dictated to a large extent by the sample size. So one must give a criterion for the sample size on which a selection can then be based. A distinction has to be made between two cases:

- large sample, i.e. more than 30 observations
- small sample, i.e. 30 or fewer observations

Large Sample:
The estimating method used here consists of preparing a frequency table and a histogram. F(t), R(t) and f(t) immediately follow from there. Then $\lambda(t)$ can be calculated from f(t) and R(t), i.e. $\lambda(t) = f(t)/R(t)$. This method can be used only if large numbers of observations are available in life tests. If data are available from a large sample, preference is given to an indirect method, i.e. estimation using a known distribution function. This involves more arithmetic of course, but the advantages are that a distribution function can give more insight into the underlying failure process and the reliability characteristics can be estimated for any moment required.

Small Sample:
A common method here is estimating F(t) by using the mean rank or median rank method. This method is explained by an example. Assume the data tabulated in table 4.2 from a sample consisting of three specimens is available:

Table 4.2: Data of three specimens

Failure sequence	t_i: life in days	$F(t_i)$
1	23	0.33
2	51	0.67
3	92	1.00

(t) is estimated on the basis of a frequency table. F(92) = 1.00 implies that all specimens in the population from which the sample is taken have a life shorter than or equal to 92 days. This does not seem a very realistic estimate. If a sample of three specimens were taken from the population a large number of times, it is not impossible that one would observe a life already achieved of more than 92 days. If one uses F(92) = 1.00, that possibility is excluded. How can one now achieve a more realistic estimate? This is possibie by including the failure sequence in the estimate. For this the time axis is divided into four intervals:

I : 0- 23 days
II : 24- 51 days
III : 52 - 92 days
IV : $\geq$ 93 days

Now the question is in which interval any new observation will end up. As a first approximation, one assumes that the probability of a new observation ending up in a specific interval would on average be equal for all four intervals. In this case, the probability would be 0.25.

Taking this as a basis, a new table can be compiled, see table 4.3:

Table 4.3: Modified data of three specimens

Failure sequence	t_i: life in days	$F(t_i)$
1	23	0.25
2	51	0.50
3	92	0.75

Table 4.3 can be interpreted as follows:
On average, 25 per cent of specimens from the relevant population fail in the first 23 days, 50 per cent fail within 51 days, 75 per cent fail within 92 days and 25 per cent lasts longer than 92 days. The estimate for $F(t_i)$ in table 4.3, the column with $F(t_i)$, is called the *mean rank.*

This approach can be generalized for a sample consisting of N specimens. As an estimator for $F(t_i)$, one takes:

$$\frac{i}{N+1} = \text{mean rank} \tag{4.69}$$

where i relates to the i^{th} observation in the series of increasing observations (i = 1, ..., N). The theory on which this method is based [4.4] uses a symmetrical failure probability distribution. As failure probability distributions are usually skew in practice, it is better to use the *median rank* as an estimator for F(t), rather than the *mean rank.*

For using the median rank approximation formula, the reliability characteristics can be estimated as follows (see reference [4.4]):

$$F(t_i) = \frac{i - 0.3}{N + 0.4} \tag{4.70}$$

$$R(t_i) = 1 - F(t_i)$$

$$= \frac{N - i + 0.7}{N + 0.4} \tag{4.71}$$

$$f(t_i) = \frac{R(t_i) - R(t_{i+1})}{(t_i{+}1 - t_i)} \tag{4.72}$$

$$= \frac{i_{t+1} - i_t}{(N + 0.4)\,(t_{i+1} - t_i)} \tag{4.72}$$

$$\lambda(t_i) = \frac{f(t_i)}{R(t_i)} \tag{4.73}$$

$$= \frac{i_{t+1} - i_t}{(t_{i+1} - t_i)\,(N - i + 0.7)} \tag{4.73}$$

An application of these formulae will be provided in the following example.

Assume that a life test generates the following data, presented in the first two columns of table 4.4, originating from a sample consisting of 1000 specimens. Estimates for $R(t_i)$, $f(t_i)$ and $\lambda(t_i)$ according to the formulae are provided in the last three columns of table 4.4:

Table 4.4: ReDability characteristics.

Time	Number of failures	$F(t_i)$	$f(t_i)$	$\lambda(t_i)$
0	0	0.000	0.020	0.020
5	100	0.100	0.010	0.011
10	150	0.150	0.012	0.014
15	211	0.211	0.007	0.009
20	247	0.247	0.000	0.000
25	247	0.247	0.005	0.007
30	270	0.270	0.023	0.032
35	385	0.385	0.041	0.067
40	589	0.589	0.082	0.200
45	1000	1.000	0.000	0.000
50	1000	1.000	-	-

Note that estimates for $f(t_{50})$ and $\lambda(t_{50})$ cannot be provided at the achieved life of t = 50 because in formulae (4.72) and (4.73) use is made of the differences $t_{i+1} - t_i$. The calculated values are plotted in figure 4.9.

Incomplete data:

In the second part of this paragraph the estimation of the reliability characteristics in case not all specimens in the sample have failed will be explained. It is not unusual for reliability characteristics to be estimated on the basis of incomplete data - in other words, there are on the one hand components which have already failed and on the other components which still operate. This can be the case for life tests in which all tests are started simultaneously and in which conclusions must be reached before the test is completed. All components which have already failed have a life that is shorter than the operating time of the Components still remaining. One can then easily estimate the reliability characteristics using the method given earlier, where one confines oneself to the life of components which have already failed. In this way one achieves a conservative estimate for F(t). But at a certain moment some of the components which have not yet failed may have an operating time shorter than the life of components which have already failed. For example, the operating time of component C is shorter than the life of components A and D (see table 4.5)

Table 4.5: Example of incomplete data

Component	Failed	Operating time in days
A	yes	274
B	yes	84
C	no	91
D	yes	122

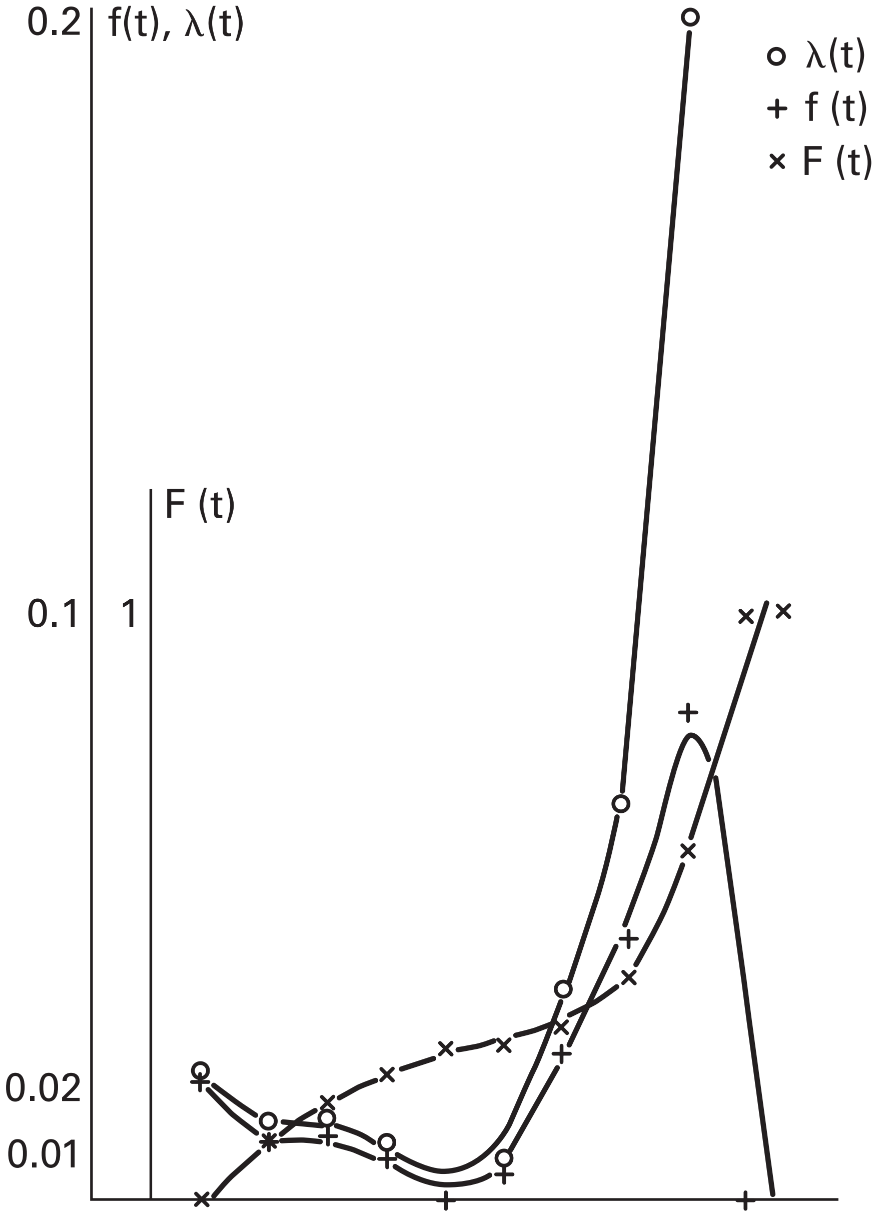


Figure 4.9: l(t), f(t) and F(t) of example.

This will occur for instance in the case of:

- Observations in practice: if components are started up at different moments, if components have in the meantime been replaced preventively or if components fail due to failure mechanisms other than the one examined
- Tests in a laboratory: where a test cannot be completed due to a mistake or a defect.

One can disregard the components which have not yet failed but in doing so valuable information is disregarded as well. Particularly in the case of small samples one may be reluctant to miss out on such information. However it is possible to make use of information concerning the operating time of components which have not yet failed. See paragraph 4.7 and reference [4.4].

4.6.2 **Indirect Methods**

In essence indirect methods amount to determining the type of distribution function and estimating the parameter(s) for the distribution function selected. The reliability characteristics can then be determined by using the estimated failure probability distribution function. As already stated in the introduction, the indirect methods have the advantage that the reliability characteristics can be estimated for any moment. Moreover, a better insight has been gained into the underlying failure process by using an indirect method.

A condition for using these methods is that sufficient observations are available, i.e. preferably 20 or more. This is important in determining the type of distribution function and accurately estimating the parameter(s) for the distribution function.

If, from previous experience or other sources, one has an idea about the type of distribution function characterizing the failure process, fewer observations may be sufficient. But a minimum of 15 observations must be available. One will find the reason for this minimum in the theory of testing statistical hypotheses.

An indirect method can be described by the following steps, in which it is assumed that all specimens in the sample have failed.

Step 1:
Starting from failure data, a specific type of distribution function has to be selected. This selection is carried out on the basis of:

a: own experience
b: reference sources, such as [4.6], [4.7] or
c: comparison of the graphs for the failure probability density (= histogram) or the failure rate relating to the data and the theoretical graphs for the failure probability density or the failure rate associated with the various types of distribution functions.

It is wise to apply this last criterion in almost all cases. Comparison of the relevant graphs should be regarded as indicative.

Step 2:
After selecting a specific type of failure probability distribution (e.g. exponential, lognormal, Weibull), the parameter(s) of the distribution function are estimated using the data. Various methods are available here (see [4.2] and [4.3]).

Step 3:
In order to test whether the observations made concur with the failure probability distribution selected, various methods can be used (see [4.2] and [4.3]). By far the simplest method is the graphic method. Another well-known test is the Chi-square test, which will also be discussed.

Step 4:
The last step consists of indicating the confidence limits for the distribution function or its parameter(s). But testing the selected distribution function against the observations can also lead to reassessing the parameter(s) or to selecting another type of distribution function, which means the relevant steps have to be carried out once more.

4.6.3 Graphic Method

With this method one can quickly and efficiently gain some idea of the type of distribution function. Selection and testing of the type of distribution function actually coincide in this method. It is also possible to estimate the parameter(s) of the distribution function selected. One disadvantage of the method is that it is less accurate and more subjective than analytical methods such as the maximum likelihood method and methods given in [4.2] and [4.3]. Before explaining the procedure for this method, the minimum required number of observations is given to which the method may be applied. As a rule of thumb the minimum required number of observations for each type of distribution is provided in table 4.6.

Table 4.6: Minimum required number of observations for graphic method.

No.	Type of distribution	Minimum number of observations
1	Exponential distribution	6
2	Normal distribution	7
3	Lognormal distribution	7
4	Weibull distribution	8

Procedure for the execution of the graphic method:

The probability of failure (or cumulative percentage of failed components) is plotted against time (or another basis to which the observations relate, such as length, etc.). Usually several points are obtained through which a curve can be fitted. But if certain transformations (usually logarithmic transformations) are made to the distribution function and time and these are plotted against each other, a straight line will develop when plotting the observations, provided the observations follow the distribution function selected. If the observations do not satisfy the equation, this will be shown by a deviating shape of the line (in other words, a straight line does not develop after transformation). Another type of distribution function must then be selected, which implies that another transformation must be made on F(t) and t. The values of the characteristic parameters can often also be derived from the slope and point of intersection with the co-ordinate axes.

Exponential distribution:
If the observations follow an exponential distribution, a straight line is developed by plotting In(1 – F(t)) against t on ordinary graph paper. The slope of the straight line is an estimate for $-\lambda$, where λ is the distribution parameter.

Normal distribution:
If the observations follow a normal distribution, special *normal probability paper* can be used. The y-axis is a scale for values of F(t). The so-called fifty per cent point t_{50} is an estimate for μ (the α per cent point t_α is the point to which $F(t_\alpha) = \alpha$ applies). The parameter σ is estimated by dividing the difference between the 84 per cent point t_{84} and the 16 per cent point t_{16} by 2, in other words:

$$\sigma \quad = \quad \frac{t_{84} - t_{16}}{2} \tag{4.74}$$

These estimates are based on the fact that $P(\underline{x} \leqslant \mu) = 0.5$; $P(\underline{x} \leqslant \mu{-}\alpha) = 0.16$ and $P(\underline{x} > \mu{+}\alpha) = 0.84$ apply to a stochastic variable $\underline{x}$ with a normal distribution.

Lognormal distribution:
If the observations follow a lognormal distribution, normal probability paper can also be used, on which one plots F(t) against In(t). The estimates for μ and α then follow in the same way as for the normal distribution. There is also *lognormal probability paper.* Its y-axis is the same as for normal probability paper but the x-axis is on a logarithmic scale.

Weibull distribution:
If observations follow a Weibull distribution, a straight line develops by plotting in(1/(1-F(t)) against In(t) on ordinary graph paper. The slope of the straight line is an estimate of the shape parameter β. The point of intersection with the y-axis can be used to estimate the scale parameter θ.

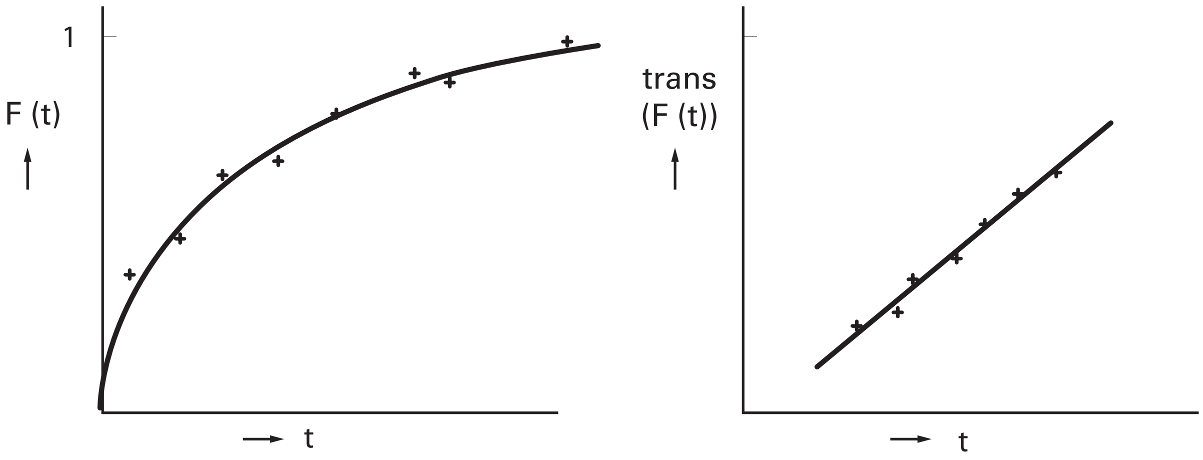


Figure 4.10: Example of the graphic method.

4.6.4 Testing

Various methods can be used for testing whether the observations made agree with the failure probability distribution selected. In this paragraph the Chi-square goodness-of-fit test is discussed. Special tests have been developed for specific cases, such as for the Weibull distribution. See reference [4.3].

The Chi-square goodness-of-fit test is generally applicable.The test statistic is determined on the basis of a frequency table or a histogram. The number of observations per class from the frequency table is compared with the expected number of observations per class based on the estimated distribution function.

The Chi-squared statistic is:

$$X^2 = \sum_{i=1}^{k} \frac{(W_i - G_i)^2}{G_i} \tag{4.75}$$

where:

W_i = the number of observations in class i

G_i = the expected number of observations in class i based on the estimated distribution function

X = the number of classes in the frequency table or in the histogram

G_i is determined as follows. The probability that an observation will end up in class i can be determined by using the estimated distribution function. This probability is called P_i. The expected number of observations in class i from a sample of size N is then $G_i = N . p_i$.

In fact k is smaller than or equal to the number of classes in the frequency table; if the expected number of observations G_i is smaller than 1, certain adjacent classes must be joined to ensure that the expected number of observations in this joint class is at least 1. The test statistic Chi-square is positive. If the observations made do not fit well in the estimated distribution function, the result will be that $(W_i - G_i)^2$ is high:. This means that the selected distribution function will be rejected for high values of Chi-square.

The number of degrees of freedom is the parameter on which the Chi-square distribution is based (the distribution of the test statistic in this case). The number of degrees of freedom is given by:

$$\text{Number of degrees of freedom} = k - s - 1 \tag{4.76}$$

k = number of classes

s = number of parameters of the selected distribution function to be estimated

Confidence intervals

Designing confidence intervals is definitely no simple matter, particularly not for parameters of failure probability distributions such as those of the Weibull distribution. If one is interested in determining the confidence intervalsr reference is made to reference [4.4] section 11.2.3.

4.7 BAYESIAN UPDATING TECHNIQUE

The objective of the Bayesian update method is to combine generic data and plant-specific data in such a way that the influence of the plant-specific data on the updated data increases with the lengthening of the period in which data is collected or the number of failures increases. The method is specially useful if little plant-specific data is available or little confidence in the plant-specific data exists.

The generic information is referred to as knowledge "prior" to the plant-specific data. The prior knowledge is an uncertainty distribution about the possible value of the component failure parameter: λ or p. The Bayesian update process changes the generic uncertainty distribution into a "posterior" distribution by incorporating the plant-specific data. Both the mean value of this distribution and its spread (the uncertainty) might change during the update process. This is illustrated in figure 4.11.

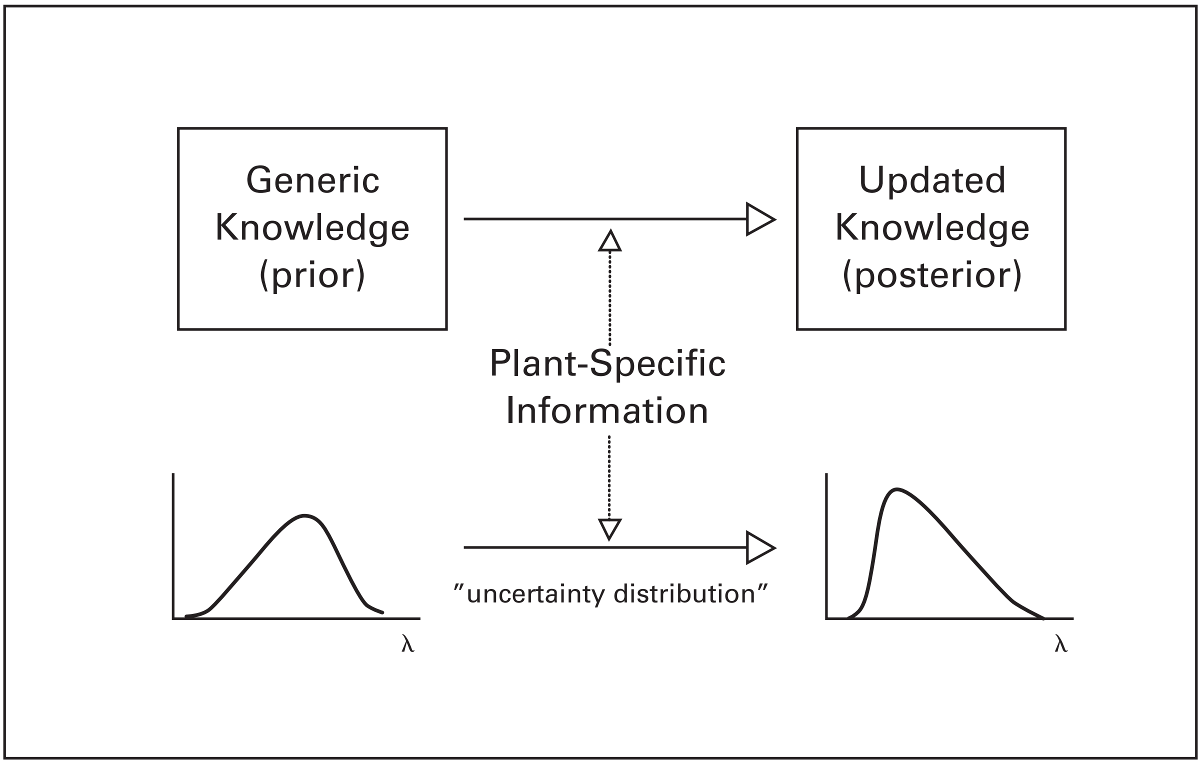


Figure 4.11: Bayesian update process.

The Bayesian update process consists of the following steps:

- For each basic event group, the plant-specific data and the mean and error factor of the generic distributions are collected. The generic distribution can be assumed to be lognormal or for example a gamma distribution.

- From this input data a new failure rate and error factor, or variance, for the basic event group are calculated. The theory behind the formulas that are used for the Bayesian update process is explained below.

In the following this process will be explained. This explanation is applicable for the failure parameter λ. For the failure on demand probability, other formulas must be applied. More information can for example be found in NUREG/CR-2300 [4.8].

4.7.1 Theoretical background

Consider the probability equation for an intersection:

$$P(A\cap B) = P(A)\ P(B|A) = P(B)P(A|B) \tag{4.77}$$

This expression is true for any two arbitrary events A and B. Thus, one can write:

$$P(A_i\cap B) = P(A_i)\ P(B|A_i) = P(B)\ P(A_i|B) \tag{4.78}$$

This can be written as:

$$P(A_i|B) = \frac{P(A_i)\ P(B|A_i)}{P(B)} \tag{4.79}$$

Let's consider that one has a set of generic failure data for type-A components. The data can be classified in a number of classes. The events A_i must be exhaustive and mutually exclusive. Exhaustive implies that every conceivable outcome is included in the prior distribution. Considering A_i as class i, the following conditions hold:

$$\sum_{i=1}^{n} P(A_i|B) = 1 \tag{4.80}$$

Combining equation (4.79) and equation (4.80) and rewriting gives:

$$P(B) = \sum_{i=1}^{n} P(A_i)\ P(B|A_i) \tag{4.81}$$

Substitution of expression (4.81) in expression (4.79) gives:

$$P(A_i|B) = P(A_i)\ \frac{P(B|A_i)}{\sum_{i=1}^{n} P(A_i)\ P(B|A_i)} \tag{4.82}$$

Expression (4.82) is Bayes' theorem. The equation is valid in general for any number of events A_i, A_2, ..., A_n. It is important to understand the meaning of the various terms in expression (4.82):

B	:	Collected plant-specific data.
$P(A_i)$	:	Probability of A;, prior to learning fact B. (Available generic data)
$P(B|A_i)$	:	The probability of the observation, given that A, is true. (Updated failure data)
$P(A|B)$	:	Probability of A'after learning fact B.

4.7.2 Continuous distributions

The following inputs are required.

Generic failure data : Failure rate
Error factor

Plant-specific data : Number of failures
Exposure (operating time or calendar time)

The generic error factor (EF) is a measure of the uncertainty in the generic information. It is the square root of the ratio of the 95 per cent percentile and the 5 per cent percentile. The percentiles are the upper and lower value of the uncertainty interval.

$$EF = \sqrt{\frac{P_{95\%}}{P_{5\%}}} \qquad (4.83)$$

Other representations of the generic information are possible as well. What is at least required an estimate of the parameter (failures and exposure) plus an uncertainty indicator.

The posterior density function for A, f(λ|E), combining the generic and the specific information is calculated using the Bayesian update formula:

$$f(\lambda|E) = \frac{f(\lambda)\ f(E|\lambda)}{\int_0^\infty f(\lambda)\ f(E|\lambda)\ d\lambda} \qquad (4.84)$$

f(λ) = distribution of A prior to collection of evidence E
f(E|λ) = distribution of evidence E given a value of A (likelihood function)
f(λ|E) = distribution of A after collection of evidence E

The prior distribution f(λ) reflects the generic knowledge. The function f(λ|E) is called the likelihood function. This function expresses the probability of observing E, the plant specific failure data, given that λ is the true value. The likelihood is the Poisson function, as λ is the parameter of a Poisson process (continuously operating with constant failure rate).

The resulting posterior distribution f(λ|E) can be established exactly by numerical integration the denominator. An example of this approach is given in the example described in section 4.7.4.

To avoid this numerical integration, an approximation is often used with a Gamma distribution The following five steps are performed for the most general case in which the generic information is represented as a lognormal distribution, with given mean value and error factor This lognormal distribution is approximated with a Gamma distribution that is easily updated reflect the specific information. The update process is used in the first example described section 4.7.3. More examples are presented in chapter 6.

Step 1:
Determination of the logarithmic standard deviation and variance of the generic data's lognormal uncertainty distribution

$$\sigma = \frac{\ln(EF)}{Z_{0.95}} \qquad (4.85)$$

$$Var = (x_{mean})^2 \{\exp(\sigma^2)-1\}$$

where:
σ = logarithmic standard deviation
EF = log normal error factor of the generic data uncertainty distribution
$Z_{.95}$ = 95th percentile of the standard normal distribution (1.645)
Var = variance of the generic data's lognormal uncertainty distribution
X_{mean} = mean of the generic data's lognormal uncertainty distribution

Step 2:
The prior lognormal distribution is approximated with a Gamma distribution. The reason for this is that with a Gamma prior distribution the update process does not require numerical integration. The Gamma approximation (see reference [4.8]) is performed by preservation of the mean and the variance. Determination of the prior distribution parameters α and β of a Gamma distribution using this approach is as follows:

$$\alpha = \frac{(x_{mean})^2}{Var}$$

$$\beta = \frac{x_{mean}}{Var} \qquad (4.86)$$

Step 3:
Using the Gamma prior distribution, it possible to perform straightforward updating, without numerical calculations. Calculation of the posterior distribution parameters α' and β' is an addition of the specific data:

$$\alpha' = \alpha + f_T$$

$$\beta' = \beta + T \qquad (4.87)$$

where:
f_T : number of time-related failures
T : time interval over which f_T failures occurred

Thus, in this Bayesian approach, the gamma parameters α and β have a very appealing interpretation: the α represents the number of failures, while the β represents the exposure time.

Step 4:
Determination of the mean and variance of the posterior distribution

$$x'_{mean} = \frac{\alpha'}{\beta'}$$

$$Var' = \frac{\alpha'}{(\beta')^2} \tag{4.88}$$

where:
x'_{mean} : posterior mean
Var' : posterior variance

Step 5:
Calculation of the log normal error factor of the posterior distribution (EF')

$$EF' = \exp\left[Z_{.95} \sqrt{\ln(1 + \frac{Var'}{(x'_{mean})^2}} \right] \tag{4.89}$$

In general the error factor be will reduced in the Bayesian update process when more information is available. It is interesting to note that if a large amount of plant-specific failure data is available, the application of a Bayesian update process is approximately the same as the result of statistical estimation techniques.

4.7.3 Example one (Spurious opening of a safety valve)

One of the possible causes of a failure scenario can be the spurious opening of a safety valve as a pressure vessel. In this example, a data analysis is performed for these safety valves.

The basic assumption in this data analysis is that the valve failure can be described by an exponential distribution. This means that the failure rate, which describes the spurious opening of a safety valve, is assumed to be constant. As the safety valve failure is an initiating event only the parameter λ, the failure rate, must be assessed.

Inputs:

- Assume that from other plants where similar safety valves are used, no such failures the safety relief valves are known. The total number of valve operating years, cumulative over all plants with these safety valves installed, is 463 years. Note that if one plant has more than one safety valve, the plant operating time must be multiplied by the number of safety valves installed to find the valve operating years.

- A plant specific data analysis shows that 5 safety valves are installed at the specific plant under consideration and during the plant’s operating history of 20 years, a spurious opening has occurred.

The generic input (0 failures in 463 years) must be translated into an uncertainty distribution. The statistical estimate and the statistically calculated confidence bounds do not provide the best solution: $\lambda = 0/463 = 0$ failures per year, and the lower confidence bound is zero as well. Another approach, the Bayesian update process, will be used.

Theoretical analysis based on the Bayesian update process teaches that if no failures have occurred in 463 years and if this is the only information available, then this can be interpreted as one failure likely to occur in the: double number of operating hours: 926 years.This theoretically means that a ”non-informative prior” is combined with the generic information [4.8]. It can be shown that in this approach, the generic information is represented by a distribution with the following mean and variance:

$$\begin{aligned} x_{mean} &= 1.08\ 10^{-3} \\ \mathrm{Var} &= 2.3\ 10^{-6} \end{aligned} \tag{4.90}$$

A gamma distribution is used with the following parameters.

$$\begin{aligned} \alpha_0 &= \frac{(x_{mean})^2}{\mathrm{Var}} = 0.5 \\ \beta_0 &= \frac{x_{mean}}{\mathrm{Var}} = 463 \end{aligned} \tag{4.91}$$

This is the generic prior distribution, which can be updated with the plant-specific data. It is interesting to see that the ratio α_0/β_0, the mean of the gamma distribution, reflects the assumption that a failure would have occurred in twice the number of exposure hours (926 years).

The Bayesian update process, step 3 in the previous section, now calculates the posterior mean and variance of a gamma distribution as follows:

$$\begin{aligned} x_{mean}' &= \frac{\alpha_0 + 0}{\beta_0 + 100} = 8.9\ 10^{-4} \\ \mathrm{Var}' &= \frac{\alpha_0 + 0}{(\beta_0 + 100)^2} = 1.6\ 10^{-6} \end{aligned} \tag{4.92}$$

What is established now is an uncertainty distribution about λ in which both the specific and the generic information are incorporated. If the risk model contains the initiating event; spurious opening of a safety valve, the uncertainty distribution for the initiating event frequency would be the posterior gamma distribution calculated above.

4.7.4 Example two (Coolant pump fails to run)

This example describes the failure rate estimation of a coolant recycle pump in the risk study of a chemical plant. The recycle pump is a medium sized centrifugal pump that operates continuously and pumps cooling fluid from a chiller through a heat exchanger. It is driven by sealed electric motor that can be used in unsheltered applications. The pump is located outdoors. It is generally not exposed to harsh environments. Its service is mild; that is, the flue is not exceptionally heavy or viscous. The recycle pump is inspected by plant personnel once every work shift.

The failure mode of interest for this pump is failure to continue pumping during operation. This may occur from such causes as motor winding faults or bearing seizure. The recycle pump has never failed in 10 years.

Here one has a case where there is some plant-specific information on pump performance. Theevidence is that there have been no failures in ten year of operation.

E : No spurious failures in 10 years of operation.

One could calculate the upper bound of a statistical confidence interval and use this as an estimator for the failure rate. For instance, at the 95% confidence level, the upper bound frequency estimate is 0.1 per year.

However, with the additional knowledge about the type of component under consideration, its operating environment, and the fluid being pumped, one can obtain a more realistic range uncertainty by using Bayesian techniques. For example, it is judged here that the reliability of this pump must be better than that of an average pump in the plant because it is not exposed a harsh environment nor to stressful operating conditions. Furthermore, the pumped flue characteristics closely resemble those of water. Therefore, to establish the *prior* failure frequency distribution, $\Pi_0(\lambda)$, one could use experience from nuclear industry with medium-sized centrifugal, motor-driven, continuously operating pumps. The distribution developed for the category of pumps is as follows:

5 per cent percentile	: 2.00E-06	- / hour	(about one failure per 57 years)
95 per cent percentile	: 98.3E-06	- / hour	about one failure per year)

One needs to fit a parametric distribution to these bounds. The choice of a parameter distribution family can be based on criteria. Extensive experience in other industries indicates that, for failure rates, a lognormai distribution [4.4] is a reasonable choice because it provides a great deal of flexibility with ranges of variability that could span several orders of magnitude. In this example, lognormal is used to represent the prior distribution with the given 5 per cent and 95 per cent percentile values.

The posterior density function for λ, $f(\lambda|E)$, is calculated by using the Bayesian update formula (4.84).

The resulting posterior, after numerical integration of the denominator, has the following characteristics:

5 per cent percentile	:	8.5E-07	- / hour	(once per 134 years)
95 per cent percentile	:	1.7E-05	- / hour	(once per 7 years)
Mean	:	7.8E-06	- / hour	(once per 15 year)

Both the prior and posterior distribution are shown in figure 4.12. The uncertainty in the failure frequency is reduced and the overall distribution has shifted towards lower values. This is because the recycle pump's performance (i.e. no failures in 10 years) has been better than anticipated by prior distribution.

A well-known property of Bayes' updating mechanism is that the degree toiwhich the shape and location of the posterior distribution would be influenced by the plant-specific evidence depends on the strength of that evidence relative to the prior distribution. Therefore, if there is a large database of plant-specific information, the effect of the prior (generic) distribution (information) would be minimal.

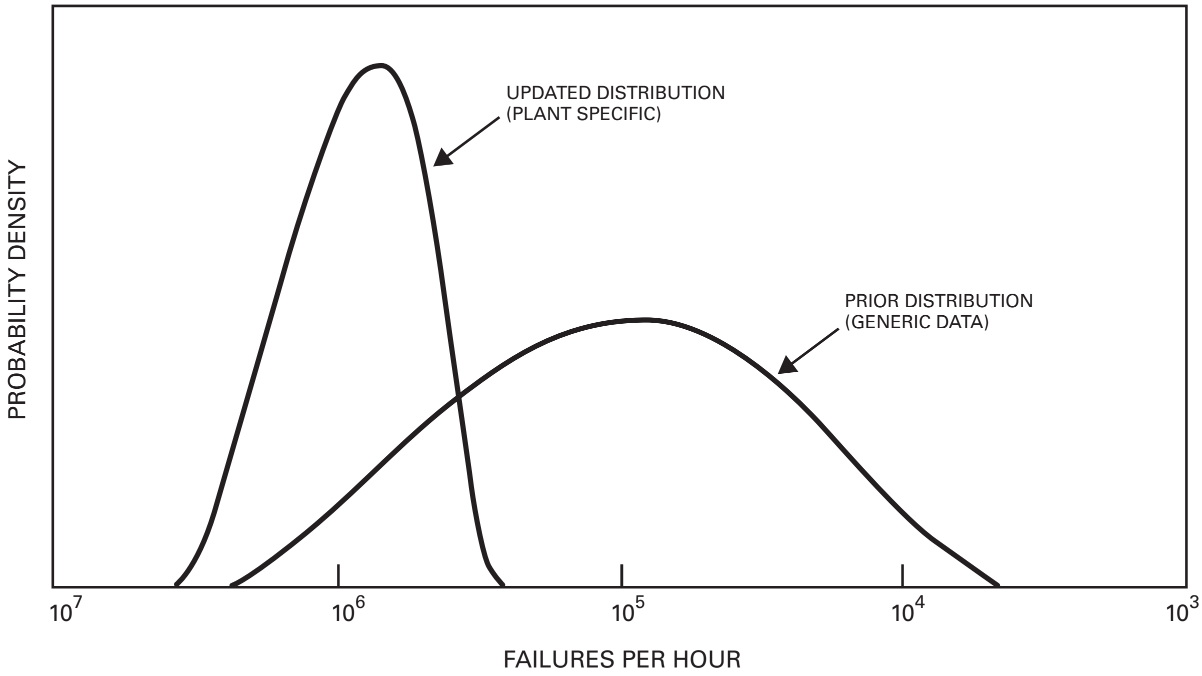


Figure 4.12: Prior and Posterior distribution for the pump failure frequency.

4.7 REFERENCES

[4.1] Sampling Techniques, Cochran, Wiley, 1963

[4.2] Survival Distributions: Reliability Applications in the Biomedical Sciences,
Gross and Clark, Wiley, 1975

[4.3] Methods for Statistical Analysis of Reliability and Life Data,
Mann, Schafer and Singpurwalla, Wiley, 1974.

[4.4] K.C. Kapur and L.R. Lamberson, Reliability in engineering design
Department of Industrial Engineering and Operations Research,
Wayne State University, Detroit, Michigan 48202.
John Wiley & Sons, New York, 1977.

[4.5] Reliability Evaluation of Engineering Systems, Concepts and Techniques,
Roy Billington, Ronald N Allan, Pitman Advanced Publishing Program,
Boston, London, Melbourne, 1985.

[4.6] Bittner, ”Mathematische Methoden bei der Informations-beschaffung und -bewertung für die Instandhaltung”, ”Fertigungstechnik und Betrieb”, 27, (1977), No. 3, pp. 160 - 162

[4.7] Yoshikawa, ”Fundamentals of mechanical reliability and its application to computer-aided design”, Annals of the CIRP, Vol. 24, (1975), No. 1, pp. 297 - 302

[4.8] PRA Procedures Guide
A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants.
U.S. Nuclear Regulatory Commission, NUREG/CR-2300
Final Report, January 1983.

[4.9] Kansrekeningen en statistiek, Dr. A.G.P.M. Nilst en J.Th.M Wijnen
Wolters-Noordhof, ISBN 90 01 657206.

APPENDIX A:

Derivation A:

$$\frac{n!}{x!(n\text{-}x)!} = \frac{n\,(n\text{-}1)\,(n\text{-}2)\,(n\text{-}3)}{x!\,(n\text{-}x)\,(n\text{-}x\text{-}1)\,(n\text{-}x\text{-}2)\,(n\text{-}x\text{-}3)\,......}$$

$$= \frac{n\,(n\text{-}1)\,(n\text{-}2)\,......\,(n\text{-}x\text{+}1)}{x!} \qquad (4.93)$$

$$= \frac{n^x}{x!} \qquad n \gg x$$

Derivation B:

Binomial series development results in:

$$(1\text{-}p)^{n\text{-}x} = 1 - (n\text{-}x)*p + \frac{(n\text{-}x)\,(n\text{-}x\text{-}1)}{2!}*p^2 - \frac{(n\text{-}x)\,(n\text{-}x\text{-}1)\,(n\text{-}x\text{-}2)}{3!}*p^3 + \,......$$

$$\approx 1 - np + \frac{n^2p^2}{2!} - \frac{n^3p^3}{3!} + \,......\ (n\rightarrow\infty,\ p\rightarrow 0,\ np = \text{finite}) \qquad (4.94)$$

$$\approx 1 - np + \frac{(np)^2}{2!} - \frac{(np)^3}{3!} + \,......$$

The Taylor series for e^x is:

$$e^x = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \,...... \qquad (4.95)$$

From formulas (4.94) and (4.95) it can concluded that:

$$(1\text{–}p)^{n\text{-}x} \approx e^{\text{-}np} \qquad (4.96)$$

RELIABILITY THEORY

CONTENTS **Page**

5.1 INTRODUCTION

In this chapter the basic elements that are necessary to understand the probabilittic concepts through quantitative reliability analysis will be presented. This material will also serve as the basis for cut-set quantification as explained in chapter 9 "Quantification of minimal cut-sets". Before one begins studying this chapter, one must be familiar with the theory presented in chapter 3 "Probability Theory" and with probability distribution theory as explained in chapter 4 "Statistics".

The theory presented in this chapter mainly deals with components, but the same principles and reliability characteristics can be derived for systems. First a number of reliability characteristics with the dimension per hour will be treated, like the failure rate, the failure density and the failure occurrence rate. Next, the reliability characteristics which are probabilities are explained; reliability, unreliability, availability, unavailability and the probability of failure on demand. The last reliability characteristic which will be explained is the expected number of failures within a certain time interval. This is of course not a reliability but fust a number without any dimension.

An important issue in quantification is the identification of the most appropriate reliability characteristic that must calculated. Depending on the reliability problem one has to calculate the reliability within a certain time interval (0,t) or the probability of failure on demand or the unavailability. In general the following guidelines can be followed:

- The probability of failure on demand must be calculated for a safety system that is demanded randomly over time.

- The reliability or the unreliability must be calculated if the system under consideration has to perform an active function for a certain period of time (mission) without any failure.

- The unavailability and the expected number of failures are the correct reliability characteristics to describe the reliability of a production unit which is in a continuous mode of operation.

It must be emphasized that these guidelines only give some guidance, the analyst has to evaluate for each separate case very carefully which reliability characteristics provide the right information about the reliability of the system under consideration.

5.2 NOMENCLATURE

			Dimension
λ	-	failure rate	-/hour
ω	-	failure occurrence rate	-/hour
μ	-	repair rate	-/hour
f	-	failure density	-/hour
τ	-	test duration in which the component is not available	hour
θ	-	repair duration	hour
A	-	availability	-
A(t)	-	limiting average availability	-
Q	-	probability of failure per demand	-
P	-	probability	-
PFD	-	probability of failure on demand	-
F(0,t)	-	unreliability at time t	-
N(0,t)	-	expected number of failures during (0,T)	-
U	-	time average unavailability	-
U(t)	-	unavailability at time t	-
T	-	test period	hour
MTTF	-	mean time to failure	hour
MDT	-	mean down time	hour
MTBF	-	mean time between failures	hour
MTTR	-	mean time to repair	hour

Superscript

m	-	mission

Subscript

LD	-	low demanded
HD	-	high demanded

5.3 MODELLING OF COMPONENT FAILURES

The models of interest in this chapter are those describing the stochastic failure behavior of components of systems. The definition of what constitutes a component failure requires the specification of some attributes of components. This specification delineates the assumed component boundary and defines the mode of failure. The mode of failure is given as an undesirable state of component performance.

In general the component models estimate the probability that a component will not perform its intended function and they depend on the mode of operation of the system to which the components belong. Component failure models can be divided into two general types: time-related models and demand-related models. Time-related models are used to model failure mechanisms which can be associated with exposure times, like fatigue or corrosion. The demand model is used when failures are not related to exposure time, for instance a human action. This paragraph defines both types of models and explains their application.

5.3.1 Time related failures

To model time-related failures, the failure rate concept has been introduced in risk and reliability analysis. The failure rate concept is used to describe the probability of failure of the component due to time-related failure phenomena.

Three parameters are of interest, failure rate, failure density and the failure occurrence rate. All three parameters have the same dimension, per hour. The difference between these parameters is that they are applicable to different populations of components. The repair rate also has the dimension per hour but is applicable to the repair process. For each parameter a definition and the application will be given.

Failure rate: A(t)
The small quantity $\lambda(t)$.dt is the probability that the component experiences a failure between t and t + dt, given that the component has survived to time t.

$$\lambda(t)\ dt = P[\text{failure occurs between } t \text{ and } t + dt \mid \text{no prior failure}] \tag{5.1}$$

The failure rate describes the components which have survived until time t. The failure rate is applicable to the population of the components that have not failed.

Failure density: f(t)
The small quantity f(t).dt is the probability that the component experiences a failure for the first time between t and t + dt, given no failure at time zero.

$$f(t)\ dt = P[\text{first failure occurs between } t \text{ and } t + dt \mid \text{no failure at time zero}] \tag{5.2}$$

The failure density is applicable to the whole population of components, failed or not. This is in contrast with the failure rate, which is only applicable to the components that have not failed.

The failure density is normalized in terms of the size of the original population of components and the failure rate is normalized with respect to the average number of components successfully functioning at time t. This can be expressed with the following formulas in which n(t) represents the number of components functioning at time t:

$$\lambda(t) \;=\; \lim_{\Delta t \to 0} \frac{n(t) - n(t+\Delta t)}{n(t)\,\Delta t} \tag{5.3}$$

$$f(t) \;=\; \lim_{\Delta t \to 0} \frac{n(t) - n(t+\Delta t)}{n(t=0)\,\Delta t} \tag{5.4}$$

Failure occurrence rate: ω(t)
The small quantity ω(t).dt is the probability that the component fails between t and t + dt, not necessarily for the first time, given no failure at time zero.

$$\omega(t)\,dt = P[\text{failure occurs between t and t +dt} \mid \text{no failure at time zero}] \tag{5.5}$$

In the definition of the failure occurrence rate, it is not given that the component has operated without failure to time t, as was the case for the failure rate definition. If the component is repairable then it may have failed many times previously. For an non-repairable component the failure density and the failure occurrence rate are equal.

To demonstrate the difference in the various parameters defined in this paragraph the failure rate and the failure density applicable to human beings is provided in figure 5.1. The basis for the density plots in figure 5.2 is the mortality data provided in reference [5.1].

The failure density at an age of 60 gives the probability of death between the age of 60 and 65, given birth. The failure rate at an age of 60 gives the probability of death between the age of 60 and 65, given survival until the age of 60 years.

Repair rate: μ(t)
The small quantity μ(t).dt is the probability that the component is repaired between t and t + dt, given that the component is under repair until time t. The repair rate is the same type of parameter as the failure rate. But the failure rate is applicable to the failure process and the repair rate is applicable to the repair process.

Remark:
The definitions of the various parameters defined above are given for components. But similar definitions can be formulated for minimal cut-sets and for systems.

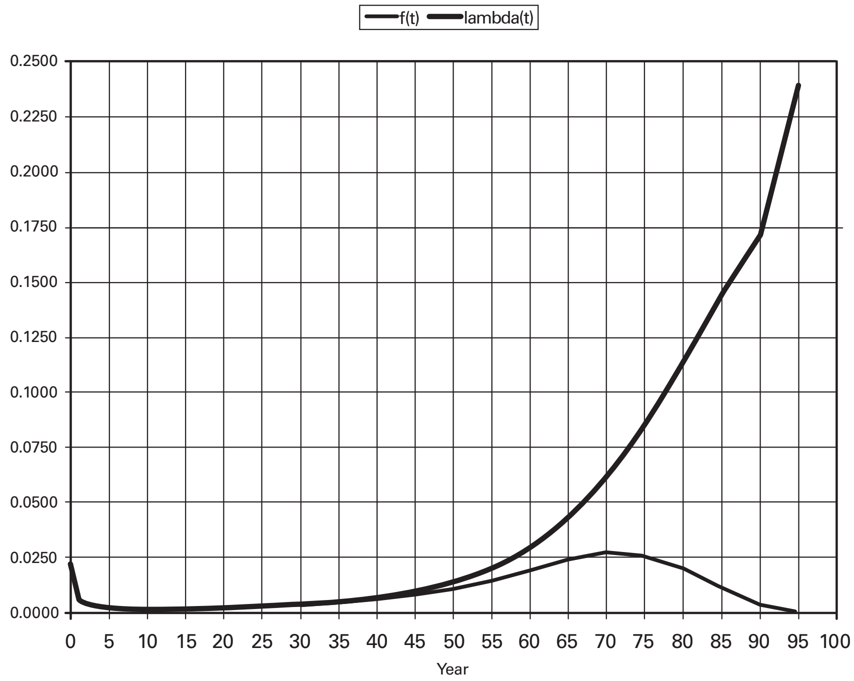


Figure 5.1: Failure rate and failure density of human beings.

5.3.2 Demand related failures

Another type of model for describing component failures is the demand model. It is used to describe the failure of a component at the time of a demand for its use. Mostly these are inactive components which have to change in condition when a demand occurs; from inactive to operating. These are usually components of a protection systems such as pressure relief valves, check valves, etc. Human error is also often characterized as failure on demand given the requirement of a specific operator action. The probability of failure on demand is designated with Q. It must be emphasized that Q is a conditional probability, i.e. the probability of failure given a demand.

The probability of failure given n demands is described by the binomial distribution. The underlying assumption is that at each demand the probability of failure is independent of whether or not a failure occurred at any previous demand.

The expression which describes the binomial distribution is as follows:

$$P(x) = \frac{n!}{(n - x)!\, x!} \quad Q^{x} (1 - Q)^{(n - x)} \tag{5.6}$$

Expression (5.6) gives the probability of x failures in n independent trials, given that the constant probability of failure in a single trial is Q. The probability of failure per demand is assumed to be independent of any exposure time interval, such as the time interval between tests or the time that the component has existed in stand-by.

The demand model is applied when failures are inherent to the component and are not caused by external mechanisms that are associated with exposure time. A well-known example of the Q model is the probability of failure of the operator who is supposed to take corrective action.

5.3.3 **Bath-tub curve**

In general the quantities defined in section 5.3.1 are not constant over time. The progress of failure rate as a function of time can be classified into three periods in the component life, indicated by the names of the early failure period, the random failure period and the wear-out failure period. For a typical example see figure 5.2.

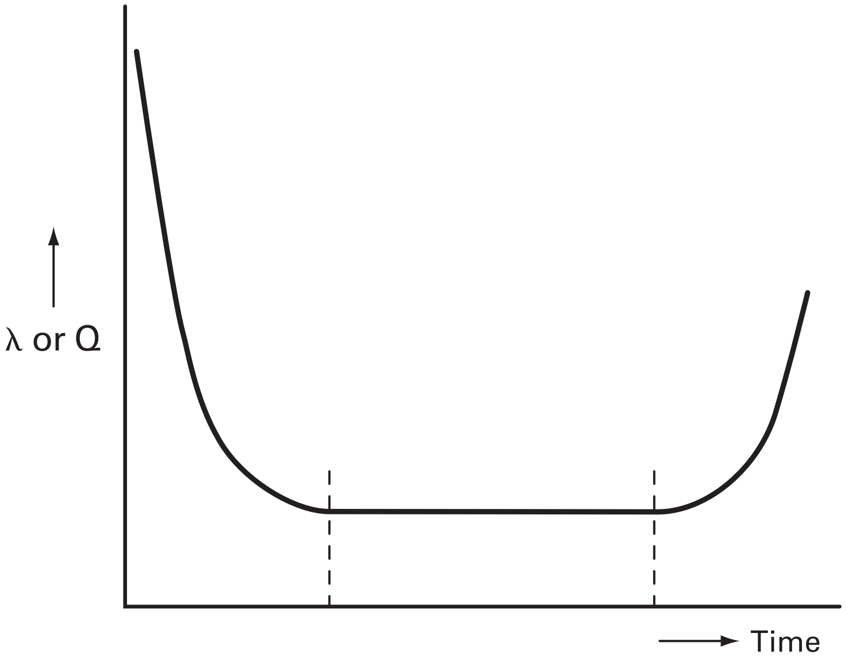


Figure 5.2: Relationship between failure rate λ(t) or Q(t) and life t.

Early failure period (decreasing failure rate):
After start-up of a component it may be expected that several failures will occur due to design and manufacturing faults, installation faults, faults during start-up and operating faults. To a large extent these can be eliminated after a certain burn-in period. It is characteristic of these failure causes that - after an initially high failure rate - the failure rate will decrease with time. This period is also called the running-in or burn-in period.

Random failure period (constant failure rate):
There follows a period in the life of components when failures occur due to accidental causes. These can include external failure causes and incidental design or operating errors, faults during maintenance or occasional overload. If these failures together are based on pure coincidence, the period is characterized by a constant failure rate. The period can cover a major part of the component life.

Wear-out failure period (increasing failure rate):
During the last phase of the component life, failure causes are predominantly time-dependent. Major failure causes are wear, corrosion, fatigue and creep. The result is a decrease in the strength and other material characteristics of the component, leading to an increased probability of failure. An increasing failure rate is characteristic of this period.

The bath-tub curve is an idealized picture of reality. To construct a bath-tub curve for a certain type of component one has to collect data for a large number of that type of components during the whole lifetime of those components. In most cases this is not possible in practice. For this reason the failure rate and repair rate are mostly assumed to be constant over time in reliability analysis.

Uncertainties:
A failure rate for a component is determined in most cases by statistical processing of test results for a large group of identical components (electrotechnical components) or by statistical processing of maintenance data for a limited group of components over an adequately long period (mechanical components).

The failure rates obtained in this way are seldom entirely applicable. The latest construction changes are never expressed in the available data. Moreover, the number of failure data for components is limited and the component descriptions for which data are available do not always correspond with the component descriptions which are the subject of study.

This means that the failure data available are uncertain and have to be considered as distributions rather than as point values.

5.4 RELIABILITY CHARACTERISTICS

In reliability analysis the following parameters are used to characterize the reliability of a component or a system:

- Reliability or probability of survival	:	R(t)
- Unreliability or probability of failure	:	F(t)
- Unavailability	:	U(t)
- Probability of failure on demand	:	PFD
- Expected number of failures	:	N(t)

Depending on the type of component or system one has to decide which reliability parameter gives the desired information. In this respect it is important to make a distinction between safety systems and systems which are in a continuous mode of operation. Safety systems are normally in a stand-by mode of operation and can fait unrevealed. Systems in a continuous mode of operation will normally fail revealed. For each reliability parameter the definition and the application will be given. They are defined for components but an equivalent definition can be formulated for system reliability characteristics.

5.4.1 Reliability and unreliability.

The definitions of reliability and unreliability are as follows:

Reliability R(t):
The probability that the component experiences no failure during the time interval (0,t), given that the component was as good as new at time zero. Reliability is sometimes also called probability of survival.

In practice it can happen that repair of the system is not possible, for instance an aircraft engine or a satellite. During the mission, the system has to perform its function without failure. In this case the unreliability or the probability of failure during the mission time period is the right characteristic reliability parameter.

Unreliability F(t):
The probability that the component experiences the first failure during the time interval (0,t), given that the component was as good as new at time zero. Reliability as well as unreliability are probabilities which imply that the associated values must lie between zero and one and are dimensionless.

Since the component either remains normal or experiences its first failure at time t, the following conditions holds:

$$R(t) + F(t) = 1 \tag{5.7}$$

Suppose that for a certain type of component a large number of failures as functions of operating time are available. For this component reliability and unreliability can be assessed with the following two formulas:

$$R(t) \cong \frac{1 - n_f(t)}{n_0} \tag{5.8}$$

$$F(t) \cong \frac{n_f(t)}{n_0} \tag{5.9}$$

n_f : number of failures before time t
n_0 : total number of components.

Application:
These reliability characteristics are applicable to systems which fulfil their functions continuously for a stated period of time. The period refers to operating time if the system operates for part of the day (month, year) or to calendar time if the system operates continuously. In figure 5.3 reliability (probability of survival) and unreliability (probability of mortality) are plotted for human beings, based on the data provided in reference [5.1].

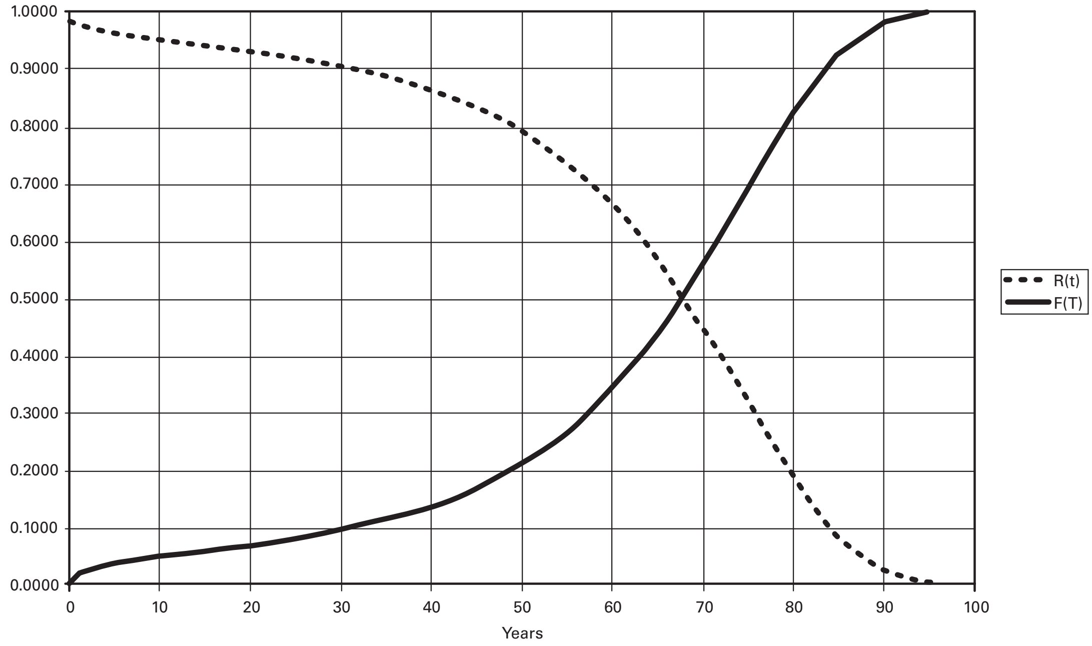


Figure 5.3: Probability of survival R(t) and probability of mortality F(t) of human beings.

5.4.2 General relation between failure rate, failure density and unreliability.

Consider the following generally valid multiplication rule for probabilities:

$$P(A \cap C) = P(C)\ P(A \mid C) \tag{5.10}$$

If one limits oneself to a population with a certain property W, equation (5.10) can be rewritten as:

$$P(A \cap C \mid W) = P(C \mid W)\ (PA \mid C,W) \tag{5.11}$$

Rearranging equation (5.11) yields:

$$P(A \mid C,W) = \frac{P(A \cap C \mid W)}{P(C \mid W)} \tag{5.12}$$

Consider the events A,C and W, which are defined as follows:
A: the component fails during (t,t+dt)
C: the component has been normal until time t
W: the component was as good as new at time zero

The quantity $\lambda(t).dt$ coincides with the conditional probability $P(A \mid C,W)$. The probability $P(C \mid W)$ is the reliability $R(t) = 1\text{-}F(t)$. Further more $P(A \cap C \mid W)$ is given by $f(t).dt$.

Substitution in formula (5.12) yields:

$$\lambda(t)\ dt = \frac{f(t)\ dt}{1 - F(t)} \tag{5.13}$$

This expression can be rewritten as:

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \tag{5.14}$$

From expression (5.14) it can be concluded that the failure rate is always greater than the failure density.

5.4.3 **Availability, unavailability and probability of failure on demand.**

The definitions of avaliability, unavailability and probability of failure per demand can be formulated as follows:

Availability A(t):
Availability can be defined in two ways:

Definition 1:
The probability that the component is normal at time t, given that it was as good as new at time zero.

Definition 2:
Availability is the fraction of the time period of length T during which the component can perform its required function.

Unavailability U(t):
Also, the unavailability can be defined in two different ways:

Definition 1:
Unavailability is the probability that the component is down at time t and unable to operate if called upon.

Definition 2:
Unavailability is the fraction of the time period of length T during which the component cannot perform its required function.

Probability of failure on demand PFD(t):
The probability of failure on demand is defined as the probability that the component is down at time t and unable to operate if called upon.

Application of the various definitions:
In principle both definitions are equivalent, the first definition is very useful in the case of safety devices. Because a safety device is demanded randomly over time, the probability of not performing the required safety function is a useful parameter to describe the reliability of such a safety device. In practice this type of unavailability is also called the probability of failure on demand.

It is also possible to apply the second definition on a safety device. In this case unavailability can be defined as the fraction of time the production unit, which is protected by the safety device, cannot operate due to spurious actions (nuisance trips) of the safety device.

In general, the second definition of unavailability is most useful for a system which is in a continuous mode of operation. For this type of application unavailability is equal to the fraction of time the system was not able to operate.

Instantaneous and average unavailability:
Dealing with unavailability or probability of failure on demand, one has to make a clear distinction between average values and point-wise or instantaneous values. If unavailability or probability of failure on demand is mentioned as such, the average value is meant in most cases.

- Instantaneous unavailability or probability of failure on demand at time t, U(t) is the probability that the component at time t is not able to operate if called upon.

- Average unavailability U or probability of failure on demand PFD is the time-average probability that the component is not able to operate if called upon.

Average unavailability or probability of failure on demand:
Two different definitions exist for average unavailability. The first definition concerns the average unavailability over a time period of length T or time-average unavailability, and the second definition concerns the limiting average unavailability.

Time-average value:

$$U = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} U(t)\, dt \qquad (5.15)$$

Limiting average value:

$$U = \lim_{T \to \infty} \frac{1}{T} \int_{0}^{T} U\,(t)\, dt \qquad (5.16)$$

In the following paragraphs no distinction will be made between time average and limiting average unavailability. This can be justified by the fact that for realistic on-line repairable components the limiting average unavailability is reached very quickly in time.

The relation between unavailability and MTBF, MTTF en MDT:
Consider a repairable component. After the occurrence of a failure there will be a period of time that the component is not available. After completion of the repair the component will be available again until the next failure occurs. In figure 5.4 this has been represented graphically.

From figure 5.4 it can be concluded directly that the following relation holds between the repair duration, the uptime and the time between failures:

$$z = x + y \tag{5.17}$$

Taking the expected value resuits into:

$$\bar{z} = \bar{x} + \bar{y} \tag{5.18}$$

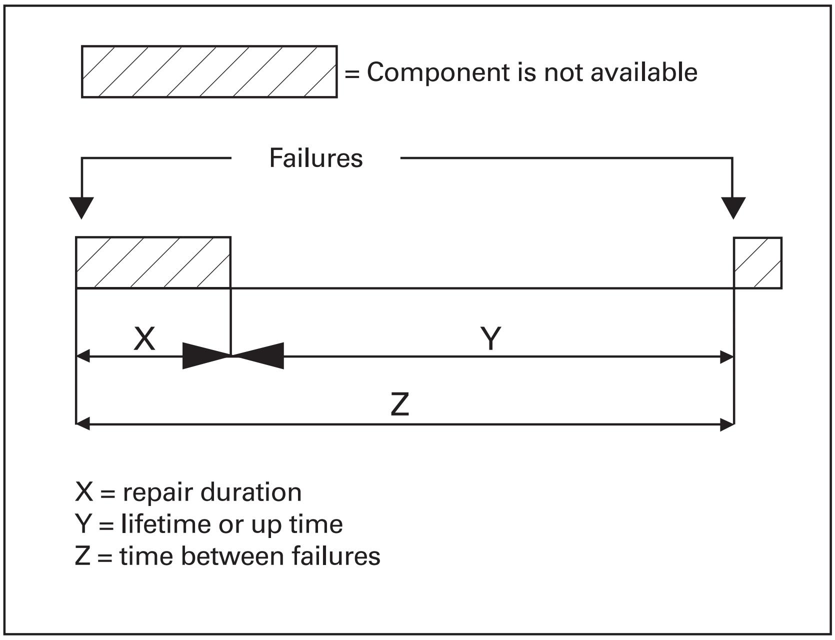


Figure 5.4: Definition of time intervals x, y and z.

In equation (5.18) $\bar{z}$ is the mean time between failures (MTBF). The parameter $\bar{x}$ is the mean time to repair MTTR or the mean down time MDT. The parameter $\bar{y}$ is the mean up time or the mean time to failure MTTF. Formula (5.18) can now be rewritten as:

$$\text{MTBF} = \text{MDT} + \text{MTTF} \tag{5.19}$$

Taking into account the second definition of unavailability, the following expression holds to calcuiate time-average unavailability:

$$U = \frac{\text{MDT}}{\text{MTTF} + \text{MDT}} \tag{5.20}$$

5.4.4 Contributors to unavailability

Three main causes can be identified for component or system unavailability:

Unrevealed failure:
In case of an unrevealed failure there will be a period of time that the component is not able to operate while this is not known. During this period the component is unavailable. This time period is ended by a test or a demand.

Testing or maintenance:
When a component is periodically tested or maintained, during which time the component is not available or only partly available, the component is unavailable or partly unavailable due to testing or maintenance. The unavailability of a redundant component will be increased during testing or maintenance. It is common practice to test redundant components in sequential order. By doing this the n redundant components will be (n-1) redundant components during testing or maintenance.

Repair:
A failed component has to be repaired or replaced. Repair or replacement requires some time during which the component is not available. During repair a single component is not available. The unavailability of redundant components will be higher if more components are taken out of service simultaneously.

5.4.5 Expected number of failures.

Expected number of failures in time period (O,t): N(0,t)
The expected number of failures in a certain time period can be obtained by integration of the failure occurrence rate:

$$N(0,t) = \int_0^t \omega(\delta)\, d\delta \tag{5.21}$$

It must be emphasized that the expected number of failures is not a probability. The expected number of failures can be higher than 1, which is not possible for a probability.

For a non-repairable component the failure probability during time period (0,t) and the expected number of failures during time period (0,t) are equal.

5.4.6 General relation between failure rate, failure occurrence rate and unavailability.

Consider equation (5.12):

$$P(A \mid C,W) = \frac{P(A \cap C \mid W)}{P(C \mid W)} \qquad (5.22)$$

Define the events A,C and W as follows:

A: the component fails during (t,t+dt)
C: the component is normal at time t
W: the component jumped into the normai state at time zero.

According to the definitions of unavailability, failure rate and failure occurrence rate, the following relations are applicable:

$$\begin{aligned} P(A \cap C \mid W) &= \omega(t)\ dt \\ P(A \mid C,W) &= \lambda(t)\ dt \qquad (5.23) \\ P(C \mid W) &= 1 - U(t) \end{aligned}$$

Substitution of equation (5.23) into equation (5.22) and elimination of dt results in the generally valid expression:

$$\lambda(t) = \frac{\omega(t)}{1 - U\ (t)} \qquad (5.24)$$

In practice the unavailability will be a small number. From equation (5.24) it can be concluded that in most practical cases the failure occurrence rate wilt be almost equal to the failure rate.

$$\text{If } U(t) < 0.01 \text{ then : } \lambda(t) \approx \omega(t) \qquad (5.25)$$

5.5 COMPONENT FAILURE MODELS

To model time-related failures, the constant failure rate model is mostly used. It is used basically for two reasons:

- Both the theory and the required calculations are simple

- The lack of information concerning the failure behavior over time for almost all type of components.

In this paragraph the equations valid for the constant failure rate model will be provided. Also, a number of component models that make use of the constant failure rate concept will be described.

At the end of this paragraph the reliability characteristics of the constant demand model will be provided.

5.5.1 Characteristics of constant failure rate model

Application of the constant failure rate model greatly simplifies relationships between the various reliability characteristics. In this paragraph important relations will be derived which play an essential rose in cut-set quantification (chapter 9).

Reliability and Unreliability.
To derive the expressions for reliability and unreliability, given a constant failure rate, expression (5.13) is used as a basis.

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \tag{5.26}$$

The failure density is given by:

$$f(t) = \frac{dF(t)}{dt} \tag{5.27}$$

Eliminating the failure density in expression (5.26) by using expression (5.27) yields:

$$\begin{aligned} \lambda \, dt &= \frac{[-dF(t)]}{1 - F(t)} \\ &= \frac{-d[1 - F(t)]}{1 - F(t)} \end{aligned} \tag{5.28}$$

Integration of both sides over time interval (0,t) results in:

$$\begin{aligned} \lambda \, t &= - \ln[1 - F(t)] \Big|_{F(0)}^{F(t)} \\ &= - \ln\,[1 - F(t)] + \ln(1) \\ &= - \ln\,[1 - F(t)] \end{aligned} \tag{5 29}$$

Expression (5.29) is equivalent with equation:

$$\begin{aligned} \ln[1 - F(t)] &= -\lambda t \\ 1 - F(t) &= e^{-\lambda t} \end{aligned} \tag{5.30}$$

Rearranging equation (5.30) gives the unreliability function for a component with a constant failure rate:

$$F(t) = 1 - e^{-\lambda t} \tag{5.31}$$

In practice the following simplification is used very often:

$$\begin{aligned} F(t) &= 1 - e^{-\lambda t} \\ &= 1 - [1 - \lambda T + \frac{(\lambda T)^2}{(2!)} - \frac{(\lambda T)^3}{3!} + ...] \\ &= \lambda T - \frac{(\lambda T)^2}{2!} + \frac{(\lambda T)^3}{3!} \quad .... \\ &\approx \lambda T \quad \lambda T < 0.01 \end{aligned} \tag{5.32}$$

The reliability function is given by:

$$\begin{aligned} R\ (t) &= 1 - F(t) \\ &= e^{-\lambda t} \end{aligned} \tag{5.33}$$

Failure density:
The failure density can be obtained by differentiation of formula (5.31):

$$f(t) = \lambda e^{-\lambda t} \tag{5.34}$$

Mean time to failure:
The mean time to failure can be calculated by means of the equation:

$$\begin{aligned} MTTF &= \int_0^\infty t\ f(t)dt \\ &= \int_0^\infty t\lambda e^{-\lambda t}dt \end{aligned} \tag{5.35}$$

To perform the integration the following standard integration solution can be used

$$\int_0^\infty t^n\ e^{-a\ t}\ dt = \frac{n!}{a^{n+1}} \quad \text{for : } a,n > 0 \quad \text{and n integer} \tag{5.36}$$

The result is:

$$\begin{aligned} MTTF &= \frac{\lambda}{\lambda^2} \\ &= \frac{1}{\lambda} \end{aligned} \tag{5.37}$$

Formulas (5.31), (5.33), (5.34) and (5.37) represent an exponential failure distribution. The exponential failure distribution gives the distribution of time between independent events occurring at a constant failure rate. A typical example of the characteristics of the constant failure rate model (A = 1.0E-05 -/hour) is presented in figure 5.5.

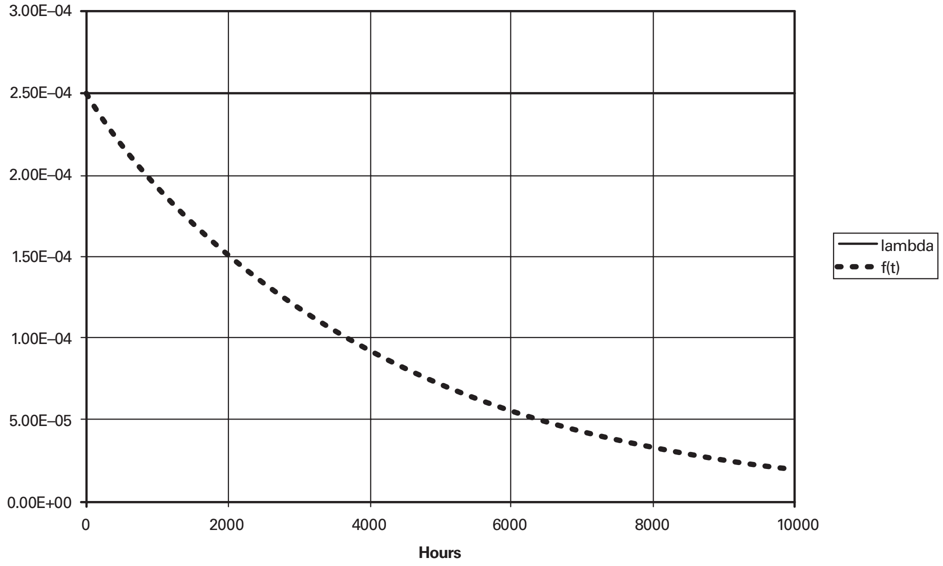


Figure 5.5: Typical example of the failure rate and failure density as a function of time (constant failure rate).

5.5.2 Periodically tested stand-by components

Many components in a safety system are in stand-by mode of operation. This means that they are not used until demanded or tested. Often such components are assumed to fail over time white in this stand-by mode of operation. To detect a failure in stand-by mode of operation, it is necessary to test the component. For this reason stand-by components have to be tested periodically. Such a test can be performed, for example, once a month or perhaps once a year. The time between tests is the length of time during which the component is exposed to failure without detection, which explains the term "fault-exposure time". This time is called the test interval and is often designated by T. The test interval is usually determined from plant procedures.

The most interesting reliability characteristic of the stand-by component model is the probability of failure on demand. After determining an appropriate test interval T for each component that is modelled to fail over time during stand-by, it is necessary to define the probability of failure on demand due to each component's random failure distribution in time.

The expression for the probability of failure on demand of a component that fails in time over a period T is given by the cumulative function of the time-to-failure distribution for that component.

$$PFD(t) = F(t) \qquad (5.38)$$

For example, if a component is found to have a constant failure rate, then the instantaneous probability of failure on demand is given by:

$$\begin{aligned}
PDF(t) &= 1 - e^{-\lambda t} \\
&= 1 - [1 - \lambda T + \frac{(\lambda T)^2}{2!} - \frac{(\lambda T)^3}{3!} + ...] \\
&= \lambda T - \frac{(\lambda T)^2}{2!} + \frac{(\lambda T)^3}{3!} .... \\
&\approx \lambda T \quad \lambda T < 0.01
\end{aligned} \tag{5.39}$$

It must be emphasized that the λ in expression (5.39) represents the failure for unrevealed failures.

In general the demand on safety systems and components occurs randomly over time. Thus, it is necessary to evaluate the probability of failure on demand function during the fault exposure time T. If it is assumed that the demand can occur with equal probability at any point during the test interval, as it usually does, the probability that should be used is the frequency-weighted probability of failure on demand over time period T. Thus:

$$PFD_{mean} = \frac{1}{T} \int_0^T PDF\ (t)\ dt \tag{5.40}$$

For the constant failure rate model this results in:

$$\begin{aligned}
PFD &= \frac{1}{T} \int_0^T (1 - e^{-\lambda t})dt \\
&= 1 + \frac{1}{\lambda T} (e^{-\lambda T)} - 1)
\end{aligned} \tag{5.41}$$

Simplification of formula (5.41) results in the welf known formula:

$$\begin{aligned}
PFD &= 1 + \frac{1}{\lambda T} (e^{-\lambda T)} - 1) \\
&= \frac{\lambda T}{2!} - \frac{(\lambda T)^2}{3!} + \frac{(\lambda T)^3}{4!} - .... \\
&\approx \frac{\lambda T}{2}
\end{aligned} \tag{5.42}$$

Note that the above presented, often-used approximation of the frequency-weighted or time-averaged component probability of failure on demand assumes that:

- the failure rate is constant (exponential failure density function)
- the higher order terms of the exponential are negligible.

5.5.3 On-line repairable components

Failure is detected immediately for components in a continuous mode of operation. For instance a component which is part of a production unit. The probability that such a component is not available if needed is related to the frequency of failure and the average time needed to return the component to service (mean repair duration).

For this type of component two processes are important; the failure process and the repair process. The failure process can be described by a constant failure rate and the repair process by a constant repair rate.

Mean time to repair.
In case of a constant repair rate, the following expression holds:

$$\text{MTTR} = \theta = \frac{1}{\mu} \tag{5.43}$$

It is assumed that the mean time to repair covers the total time to respond to the failure, repair the component, and return it to service.

Unavailability and availability:
The expression for unavailability can be derived very easily by means of a Markov process (see chapter 11).

$$U(t) = \frac{\lambda}{\lambda + \mu} \left(1 - e^{-(\lambda + \mu)t}\right) \tag{5.44}$$

The limiting average unavailability is given by:

$$\begin{aligned} U &= \lim_{t \to \infty} \left[\frac{\lambda}{\lambda + \mu} \left(1 - e^{-(\lambda + \mu)t}\right)\right] \\ &= \frac{\lambda}{\lambda + \mu} \end{aligned} \tag{5.45}$$

For almost all cases in practice, equation (5.44) can be simplified as follows:

$$\text{If} \quad \mu \gg \lambda \quad \text{and } t \geq \frac{3}{\mu} \quad \text{then} \quad U(t) \approx \frac{\lambda}{\mu}$$

Or: (5.46)

$$\text{If} \quad \theta \ll \text{MTTF} \quad \text{and } t \geq 3\,\theta \quad \text{then} \quad U(t) \approx \lambda\,\theta$$

The expression for availability can be derived as follows:

$$A(t) = 1 - U(t)$$

$$= \frac{\mu + \lambda\ e^{-(\lambda + \mu)t}}{\lambda + \mu} \tag{5.47}$$

The limiting average availability is given by:

$$A \ = \lim_{t \to \infty} \left[\frac{\mu + \lambda\ e^{-(\lambda + \mu)t}}{\lambda + \mu} \right]$$

$$= \frac{\mu}{\lambda + \mu} \tag{5.48}$$

Failure occurrence rate:
Substitution of equation (5.44) into equation (5.24) gives the expression for the failure occurrence rate of a component with a constant failure rate:

$$\omega(t) \ = \frac{\lambda\ \mu}{\lambda + \mu} + \frac{\lambda^2}{\lambda + \mu}\ e^{-(\lambda + \mu)t} \tag{5.49}$$

In practice it will mostly be the case that the mean time to failure of a component is much greater than the mean time to repair of that component. So, the following expression will hold in general:

$$\mu \gg \lambda \tag{5.50}$$

Considering formulas (5.49) and (5.50), the failure occurrence rate can be approximated by the failure rate:

$$\omega \approx \lambda \tag{5.51}$$

Number of failure occurrences:
The expected number of failures in time interval (0,t) can be calculated by the formula:

$$N\ (0,t) \ = \int_0^t \ \omega\ (t)\ dt \tag{5.52}$$

Substitution of equation (5.49) into equation (5.52) and integration gives the expected number of failure occurrences (constant failure rate model):

$$N(0,t) = \frac{\lambda\mu}{\lambda + \mu}\ t + \frac{\lambda^2}{(\lambda + \mu)^2}\ [1 - e^{-(\lambda + \mu)t}] \tag{5.53}$$

In general μ » λ will be applicable and the formula above can be simplified to:

$$N(0,t) \approx \lambda\ t \tag{5.54}$$

From formulas (5.32) and (5.54) it can be concluded that the probability of failure in time period (0,t) and the number of failure occurrences in time period (0,t) are equal, if the time period (0,t) is short. It must be emphasized that the probability of failure is always less than or equal to one, white the expected number of failure occurrences can be greater than one (see figure 5.6).

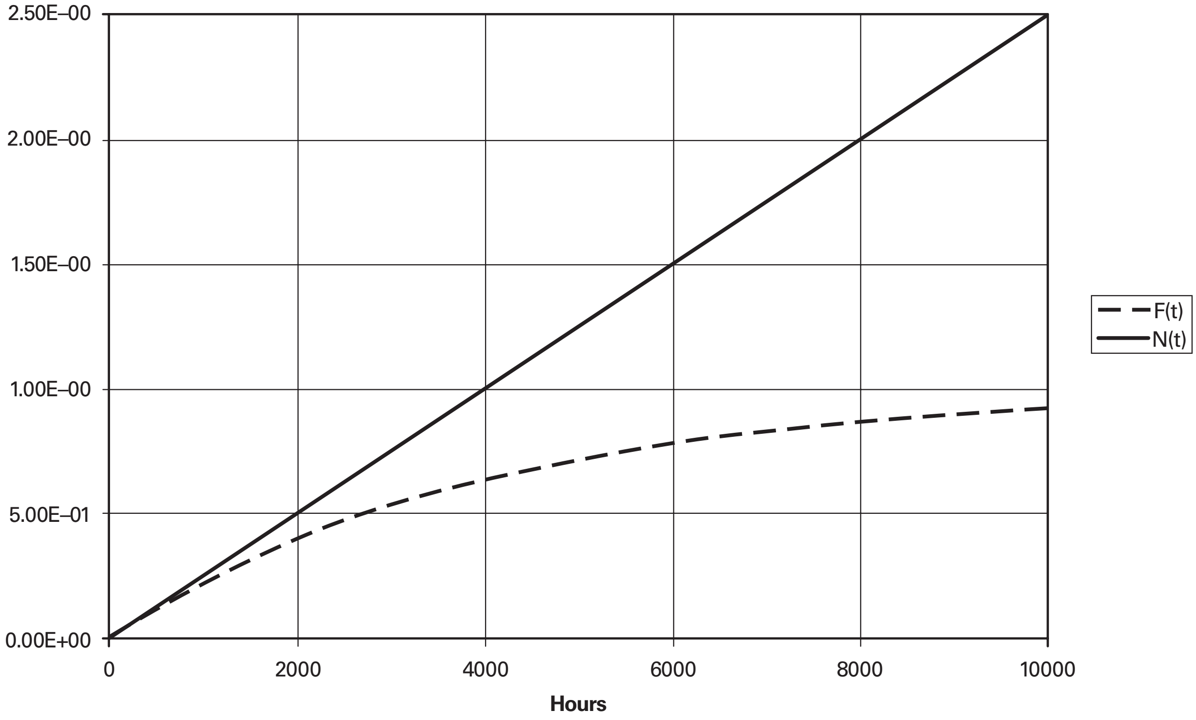


Figure 5.6: Typical example N(0,t) and F(0,t) of constant failure rate model.

5.5.4 Mission-type components

It is often necessary to evaluate the probability of component failure after a successful start, but before completing its mission. An example of such a component is an emergency diesel generator. The mission time is here designated as T^m. The probability that a component fails before T^m is given by the cumulative distribution function. The following equation holds for components with a constant failure rate (exponential distribution):

$$\begin{aligned} F(T^m) &= 1 - e^{-\lambda t} \\ &\approx \lambda T \qquad \lambda T < 0.01 \end{aligned} \tag{5.55}$$

It should emphasized that the failure rate A in this case is not the same as the failure rate in stand-by. To estimate the failure rate for failures occurring after a successful start, the analyst must take into account any adverse environment as well as recognize differences between the rates of stand-by and operation failures.

5.5.5 Constant demand model

The reliability characteristics for the Q model are straightforward and are all based on the characterizing probability of failure per demand Q.

For n demands in time interval (0,t) and assuming independent failures, the unreliability and unavailability can be derived very easily from formula (5.6):

$$F(0,t) = U(0,t) = P\ (x = 1) = n\ Q\ (1 - Q)^n \tag{5.56}$$

If one limits oneself to only one demand in time interval (0,t), which is the most practical case for a component of a safety system, unreliability and unavailability are given by:

$$F(0,t) = U(0,t) = Q \tag{5.57}$$

Several very important factors should be taken into account when using the demand model. If the event being considered really could occur before the demand, then using the demand model "lumps" the failure rate into the instantaneous time of the demand. Thus, for different demand rates the probability of failure on demand would actually be different, and if the demand model is used, a reasonable estimate is obtained only if the demand rates are similar. A component that behaves exactly as the demand model will have the same probability of failure on demand, whether the demand occurs once per hour or once per decade.

If it is necessary to obtain a new probability of failure on demand, Q2, for a new test period T2; the new failure on demand probability is given by (see reference [5.2]):

$$Q_2 = 1 - (1 - Q_1)^{T2/T1} \tag{5.58}$$

5.6 PFD HIGH DEMANDED SYSTEMS

For a large number of industrial facilities operation is not possible without accepting a certain risk level. This acceptable risk level is mostly achieved by application of one or more safety systems. Calculation of the risk involved is possible by performing a risk analysis. Important items in a risk analysis are the demand rate and the probability of failure on demand of the safety systems. In case of a single safety device the Hazard rate can be calculated with the formula:

$$f_H = f_D\ PFD_{SD} \tag{5.59}$$

f_H : HAZARD rate (undesirable event frequency).

f_D : Demand rate on the safety system. The frequency of the undesirable event associated with the risk that exists without any safety system.

PFD_{SD} : Probability of failure on demand of the safety device.

The demand rate and the probability of failure on demand can only be considered as independent if the demand rate is low in comparison with the test frequency of the safety device. In case of a high-demanded system (more than one demand per test period), the demand rate and the probability of failure on demand cannot be considered independent.

Probability of failure on demand.
A safety device can be in a failed state while this is not noticed by the operators. For this reason safety devices have to be tested periodically. Just after the test the probability of failure on demand will be zero. During the course of the test interval the probability of failure will increase. So in general the probability of failure on demand will be a function of time.

$$PDF = PDF\ (t) \qquad (5.60)$$

In figure 5.7 a typical example of the probability of an unrevealed failure as a function of time is depicted.

Probability of failure on demand, low-demanded safety systems:
As explained in section 5.5.2 the demand on the safety device occurs randomly over time. For this reason it is necessary to calculate the time-average probability of failure on demand over the test period T. If it is assumed that the demand can occur with equal probability at any point in the test period; the correct formula to calculate the time average probability of failure on demand is:

$$PFD_{LD} = \frac{1}{T} \int_0^T PDF\ (t)\ dt \qquad (5.61)$$

For low-demanded (LD) components with a constant failure rate the welf known formula can be derived to calculate the probability of failure on demand:

$$PFD_{LD} = \frac{1}{2} \lambda T \qquad (5.62)$$

This formula is only valid in case the number of demands per test period is equal to or less than one. In case of multiple demands, formula (5.62) is not correct.

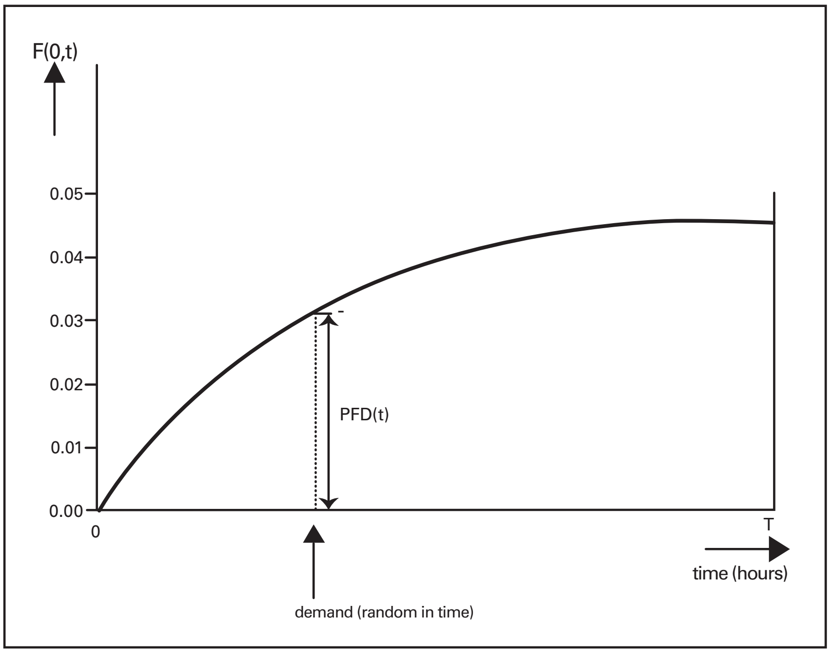


Figure 5.7: Probability of failure on demand as function of time (typical example).

Probability of failure on demand, high-demanded safety systems:
To calculate the probability of failure on demand for a high-demanded component, two assumptions have to be formulated:

Assumption 1:
It is assumed that the probability of dangerous failure of a safety system is independent of the number of demands on that safety system.

Assumption 2:
It is assumed that in case of a demand followed by a failure of the safety device the process is stopped and the safety device is repaired before operation is continued.

At time t1 a demand is made on the safety device. The probability of failure on demand is equal to PFD(t1). In accordance with assumption 2, the second demand at time t2 can only occur if the demand at time t1 is handled properly. This implies that in case of a demand at time t2, the safety device did not fail in time period (0,t1).

In this case the test interval T indicates the proof test interval. Proof test are performed to detect failures in the safety system so the system can be restored to an ”as new” condition or as close as practical to this condition. If separate channels are used, a proof test implies that each channel is tested separately.

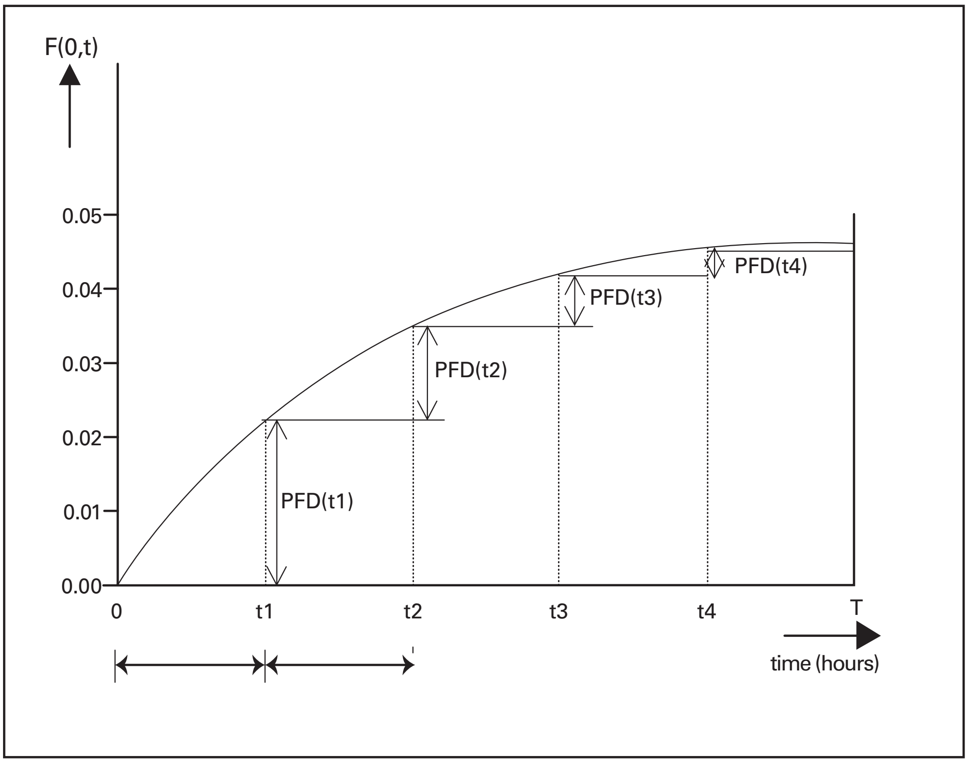


Figure 5.8: Multiple demands in one test period.

The probability of a failure on demand at time t1 is equal to:

$$PDF\ (t1) = F\ (t1) \tag{5.63}$$

Considervthe time periods A (0,t1) and B (t_1, t_2). The probability of an unrevealed failure in time interval A or B is equal to:

$$\begin{aligned} F(t2) &= p(A \cup B) \\ &= P(A) + P(B) - P(A \cap B) \\ &= PFD(t1) + PFD(t2) - 0 \end{aligned} \tag{5.64}$$

The term $P(A \cap B) = 0.0$ because, in accordance with assumption 2, it is not possible that a unrevealed failure occurs in time interval A as well as in time interval B (mutually exclusive events).

$$PFD(t2) = F(t2) - PFD(t1) \tag{5.65}$$

Generalization of formula (5.60) gives:

$$\sum_{i=1}^{n} PFD(ti) = F(T) \tag{5.66}$$

n = number of demands in one test interval.

The mean probability of failure on demand for a high-demanded (HD) safety system can be calculated as follows:

$$PFD_{HD} = \frac{F(T)}{n} \tag{5.67}$$

F(T) = the probability of a unrevealed failure in one test interval
T = test period
n = the number of demands in one test interval.

Hazard rate high-demanded component:
To calculate the Hazard rate in case of a high-demanded safety system, the following formula can be used:

$$f_H = f_D \quad \frac{F(T)}{n} \tag{5.68}$$

f_H = Hazard rate -/year
f_D = Demand rate -/year

5.7 REFERENCES

[5.1] E.J. Henley, H. Kumamoto, Reliability Engineering and Risk Assessment, New York, IEEE Press, 1992.

[5.2] PRA Procedures Guide
A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants. U.S. Nuclear Regulatory Commission, NUREG/CR-2300
Final Report, January 1983.

[5.3] IAEA, International Atomic Energy Agency,
The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, Safety series No. 106, 1992.

[5.4] Fault Tree Handbook
U.S. Nuclear Regulatory Commission NUREG-0492, January 1981.

DATA ANALYSIS

CONTENTS **page**

6.1 INTRODUCTION

Along with the establishment of the system model (fault tree or Markov process), a data analysis has to be performed to quantify the basic events or the transition rates of the model. The objective is to find not only estimates of the failure parameters but also uncertainty intervals for these estimates. In this chapter only the basic events involved in hardware component failures are of concern.

A reliability analysis requires the following input parameters as a minimum of quantitative data:

- failure rates or probabilities of failure on demand for the components modelled
- test durations and test intervals
- repair durations
- maintenance durations and maintenance intervals.

In a lot of cases this set of data has to be expanded by quantitative data concerning human error probabilities, dependent failure probabilities and, a risk analysis is being undertaken, with initiating event frequencies.

In general, one can make use of three different sources of data to determine quantitative estimates of the input parameters.

Generic data:
Generic data is generally developed from previous reliability or risk studies or from generic data bases.

Plant-specific data:
Plant-specific data is collected from the plant under consideration. It reflects the operating experience within a time window for the plant operating mode that is considered.

Expert or subjective judgement:
If neither physical nor theoretical models are available and failure data is unavailable as well, subjective judgement is the only alternative to assess a probability. Expert judgement requires experts having extensive experience with component and system outage failure occurrences of the system under consideration.

It is preferable to use plant-specific data as much as possible. This is not always possible because of a lack of plant-specific data due to financial constraints or shortage of operational history. Therefore in general the data analysis consists of a combination of generic data, plant-specific data and data based on expert opinion.

The purpose of this section is to describe the methods for analyzing data to assess the component failure parameters (A and Q), the maintenance unavailabilities and the initiating event frequencies and the associated uncertainty. It should be noted that estimation of common cause failure probabilities and human error probabilities are not discussed in this section.

It should be emphasized that the numerical quantities obtained by the procedures of this section are in a very strict sense estimates; that is, these quantities should be considered judgments of the values for the numerical quantities of interest.

Before failure data can be collected or analyzed, one must be familiar with the different failure modes which can occur and the failure classification applicable to the components modelled in the reliability model. Section 6.3 covers this aspect.

In section 6.4 and 6.5 the analysis and treatment of generic and plant-specific data will be described. The use of subjective judgement is explained in section 6.6.

The establishment of the final component failure parameter estimate from these inputs, combining data from different sources, is described in section 6.7. The techniques used to combine generic and plant-specific data or data obtained by expert judgement is called "Bayesian updating".

These techniques are not only applicable for the quantification of component failure events, but can be used in the estimation of maintenance unavailability and initiating events as well.

Repair durations, test durations and test intervals, maintenance durations and maintenance intervals cannot be extracted from generic data sources because of the differences in maintenance and test practices between the different plants. To obtain estimates for these type of input parameters, use has to be made of plant-specific data or expert judgement. The same holds for initiating event frequencies.

6.2 NOMENCLATURE

			Dimension
λ	-	failure rate	-/hour
ω	-	failure occurrence rate	-/hour
μ	-	repair rate	-/hour
f	-	failure density	-/hour
α	-	prior parameter Bayesian update process	-
β	-	prior parameter Bayesian update process	-
α'	-	posterior parameter Bayesian update process	-
β'	-	posterior parameter Bayesian update process	-
τ	-	test duration in which the component is not available	hour
θ	-	repair duration	hour
EF	-	error factor	-
Q	-	probability of failure per demand	-
P	-	probability	-
T	-	test interval	hour
MTTF	-	mean time to failure	hour
MDT	-	mean down time	hour
MTBF	-	mean time between failures	hour
MTTR	-	mean time to repair	hour
Var	-	Variance	-

6.3 FAILURE CLASSIFICATION

The failure of a component or system is the termination of the ability to perform a required function. This termination may involve either total loss (breakdown) or partial loss of that function (no longer satisfying the standards, specifications or requirements). Hence, for both situations it can be determined whether or not there is a failure.

To analyze the failure of a component or a system, it is desirable that the failure be described as comprehensively as possible. This usually comprises a definition of the failure, the failure cause, the failure mechanism, the failure mode and the consequences of the failure.

To define failure, a description is first required of the function with which failure is connected. After all, components and systems can have several functions. Total loss of the function is an unequivocal fact but exceeding limit values is based on criteria whose the determination is of a subjective nature. Thus, it is possible to state that a pump fails if:

- a gland seal leaks
- the pump does not reach its capacity
- the pump no longer delivers.

6.3.1 Fault and failure

Each failure form has its own cause, frequency and consequences. The failure cause comprises the conditions during design, manufacture or use which have led to failure. These conditions are termed "faults". A failure occurs because the component or the system is erroneous. A failure occurs when the delivered service deviates from the intended service. From these descriptions it can be seen that fault, and failure are part of a chain (fault ...... failure). An error is thus the manifestation of a fault in the system, and a failure is the effect on the intendant service

6.3.2 Primary and secondary failures

In general, two different faults can be distinguished, i.e. primary and secondary faults.

Primary failure:
A primary failure is understood to be failure of a component not caused (directly or indirectly) by failure of another component.

Secondary failure:
Secondary failure then comprises failure of a component which is caused (directly or indirectly) by failure of another component. Secondary failure then comprises failure of a component which is caused (directly or indirectly) by failure of another component.

6.3.3 Failure mechanism

Failure mechanism is defined as the physical, chemical or mechanical process resulting in failure, such as wear and fatigue.

6.3.4 Failure mode

A failure mode is defined as the effect by which a failure is observed to occur; it is usually characterized by a description of the manner in which a failure occurs. A failure mode provides a descriptive characterization of the failure event in generic terms - not in terms of the failure mechanism, but in terms of the failure effect.

Some examples of failure modes are:
- failure to start of a diesel generator
- failure to run of a motor
- failure to open on demand of a safety valve
- spurious opening of a safety valve.

In determining the correct probability of failure of the system in question, a description of the consequences may also be relevant. A safety valve, for example, may open too soon, too late, at the wrong pressure or not at all (failure cause). The nature and seriousness of the consequences greatly depend on that. So, to determine the probability of the specific failure of the system in question, data must be used which refer to that specific failure mode.

The effect of a failure within a system may be propagated to higher and lower levels of assembly or the system design may erevent such propagation. Failure modes and effects analysis is a formal approach of the analysis of failure modes and their propagated effects; it involves the toss or degradation of function and also the effects of failures on system safety.

In risk and reliability analysis it is important to describe which failure mode is represented by the basic events in the fault trees or by the transition rates in a Markov model. To determine the failure rate or the probability of failure on demand, the right failure mode has to be taken into consideration. In general the failure mode ”spurious operation” of an air-operated valve has a different failure rate than the failure mode ”failure to operate on demand” of the same air operated valve. If only the total failure rate is provided, an estimate has to be made of which part of the failure rate represents spurious operation and which part represents failure to operate on demand. It is obvious that a database providing numbers for each failure mode separately is to be preferred.

6.3.5 Critical, degraded and incipient failure

A distinction is made between hardware failures, software failures and human failures. In this section only hardware failures are considered. For the classification of human failures reference is made to the section ”Human Reliability Analysis”. In generic databases mostly the following classification for hardware failures is used:

Critical failures:
A critical failure is a failure whereby the function of the component is considered to be lost. Critical failures include failures of the type: Pump will not start on demand or stops spuriously.

It should be emphasized that for safety devices critical failures include failures like failure on demand of a safety device as well as spurious operation of a safety device.

Degraded failures:
A degraded failure implies that the component under consideration is still capable of functioning but certain characteristics that are not crucial to the function have been degraded. Examples of ”degraded failures” are: external leakage, vibrations. This type of failures does not always lead to immediate repair; repair is often postponed to some convenient occasion.

Incipient failures:
An incipient failure is one in which the complete function of the component concerned cannot be maintained. One can often expect that the failure will be getting worse if no measures are taken, which means that repairs should be made without too much delay. Examples of incipient failures are considerable vibrations and loss of lubricant. Since it is difficult to distinguish incipient from critical failures, the incipient failures are often considered as ”critical failures”.

6.3.6 **Random versus systematic failures**

Random failures:
Failures, occurring at random times, which result from a variety of degrading mechanisms.

There are many degradation mechanisms occurring at different rates in different components and since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of a total equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Systematic failure:
Failures due to errors which cause the component to fail under some particular combinations of inputs or under some particular environmental condition.

A major distinguishing feature between random failures and systematic failures, is that component failure rates, arising from random failures, can be predicted with reasonable accuracy but systematic failure rates by their very nature cannot be accurately predicted.

6.4 **GENERIC DATA ANALYSIS**

Generic data can be obtained from literature, other risk and reliability studies and data banks. Generic data may be available in many forms. The analyst may have raw failure data or reduced failure rate data in the form of point or interval estimates, percentiles, and so forth. A number of books are available which provide failure rates or probabilities of failure on demand for a large number of components. It is important to realize that the quality of all databases is not equal. The quality of a database is higher if more of the requirements listed in table 6.1 are fulfilled.

Table 6.1: Requirements for databases.

No.	Requirement
1	Component type
2	Clear description of the failure mode
3	Description of the component boundary
4	Mean value
5	Median value
6	Uncertainty bound
7	Description of component population

If in a certain database only the component type is provided with a failure rate, the information is not very valuable. In most risk and reliability analyses a failure rate of a specific failure mode is required. Also, it must be clear what is considered to be included in the figure provided. For instance, consider a motor driven pump; is the motor included and are the control circuits excluded, or not? A clear definition of the component boundary is very important to avoid these type of questions. An example of a high quality database is presented in table 6.2.

6.4.1 **Sources of generic data**

To collect generic data, the following methods can be used:
- literature search
- membership of a database organization
- review of existing risk and reliability studies.

Given the effort required to collect failure data it is impractical to collect the data in such a way that bath tube curves can be generated. For this reason the mean value must be considered as a mean value containing both burn-in failures and wear-out failures.Therefore it is normally assumed that the failure rate and the probability of failure on demand are constant in time. A large number of data books are available. A short description of a number of books will be provided.

Table 6.2: Example of a generic database.

Component and Failure Modes	Mean	Median	Error Factor	Component Boundary
Pumps				
Motor-driven				Pump and motor; excludes control circuits.
Failure to start	3E-3/d	1 E-3/d	10	
Failure to run, given start				
Normal Environment	3E-5/h	1 E-5/h	10	
Extreme Environment	3E-3/h	1 E-3/h	10	
Turbine-driven				Pump, turbine, steam and throttle valves, and governor.
Failure to start	3E-2/d	1 E-2/d	10	
Failure to run, given start	1 E-5/h	1 E-5/h	3	
Diesel-driven				Pump,diesel, lube-oil system, fuel oil, suction and exhaust air, and starting system.
Failure to start	1 E-3/d	1E 3/d	3	
Failure to run, given start	8E-4/h	1 E-4/h	30	

1 **NUCLARR**
Nuclear Computerized Library for Assessing Reactor Reliability
NUREG/CR -4639, EGG-2458, Volume 5, Rev 3, 1990, Part 3, hardware component failure data (HCFD).

The Nuclear Computerized Library for assessing Nuclear Power Plants reliability data is an automated data management system used to process, store, and retrieve human and hardware reliability data in a ready-to-use format. The Nuclarr system was developed by the U.S. Nuclear Regulatory Commission (NRC) to provide the risk analysis community with a repository of reliability data that can be used to support a variety of risk assessment activities. The system maintains a broad range of database management functions for input and retrieval of data, including computational algorithms for aggregating the source data and routines for report generation. All data and related information available from the PC-based system are also accessible in hard-copy format.

2 **IEEE Std 500-1984**
IEEE Guide to the collection and presentation of electrical, electronic, and sensing component reliability data for nuclear power generating stations.
IEEE Standards Board, The institute of Electrical and Electronics Engineers, Inc. 345 East 47 Street, New York, NY 10017

This guide applies to reliability data of electrical, electronic, sensing component, and mechanical equipment. The purpose of this guide is to establish one method of collecting and presenting reliability data for use in nuclear power generating units reliability calculations and risk analyses.

3 **Eireda**
European Industry Reliability Data Bank, H. Procaccia, P. Aufort, S. Arsenis, Volume 2, Edition SFER, Paris, 1995.

This book aims to satisfy the requirements of quantitative risk and safety studies on industrial systems for documented estimates of reliability parameters of system components. It presents point and interval estimates for failure rates and probabilities of failure on demand for components operating in industrial plants.

4 **T-book**
Reliability Data of Components in Nordic Nuclear Power Plants, The ATV Office and Studsvik AB, 4th edition, Sweden.

Data collected in the Swedish nuclear power plants. Contains clear definitions of component boundaries. Almost all requirements listed in table 6.1 are fulfilled. The T-book is important because it can be considered as an independent source of data not related to the data collected in U.S. nuclear power plants.

5 **OREDA**
Offshore Reliability Data Handbook, 1994 P.O.Box 370, N-1322-HØVIK, Norway

The data in this book has been collected in the offshore industry. Clear component boundaries are provided. Besides failure rates, repair durations are given as well. It is one of the few high quality data books outside the nuclear industry.

6 **RDF 93**
Handbook of reliability data for electronic components, France Telecom CNET, June 1993.

This handbook is specifically designed as an aid to research into how to maximise equipment reliability, and to assist in the design of the equipment, by introducing various influencing factors.

The reliability data contained in this handbook is taken mainly from field data concerning electronic equipment operating in the following kinds of environment:

- equipment for stationary use on the ground in weather-protected locations, operating permanently or otherwise.
- equipment for stationary use on the ground in non-weather-protected locations
- equipment for non-stationary use on the ground.

7 **MIL-HDBK-217F**
Military Handbook: Reliability Prediction of Electronic Equipment Department of Defense, 1992, USA.

This book provides two methodologies to determine the reliability characteristics of electronic systems: 'Tart Stress Analysis" and "Parts Count Analysis". Both methodologies are based on a basic failure rate and a number of influence factors. For the part stress analysis a lot of information concerning the quality, the complexity and the environmental conditions of the system are required. The second methodology requires less information but gives mostly conservative results.

8 **AMINAL**
Handbook Probability figures, version 1
Ministry of Physical Planning and the Environment, Belgium, 1994

By order of the Ministry of Physical Planning and the Environment, a large number of data sources have been reviewed. The data collected is presented in this book. Uncertainty bounds are provided in most cases. This book is mainly intended to provide failure rates to calculate the probability of a release of some fluid contained in the component under consideration. For instance, external leakage, catastrophic failure of a vessel or a pipe rupture.

9 **NUREG/CR-1278**
Handbook of human reliability analysis with emphasis on nuclear power plant applications, A.D. Swain H.E. Guttman,
SAND 80-200, RX, AN, August 1983, U.S. Nuclear Regulatory Commission.

Section 20 of this book contains a number of tables which apply to the probability of human failure in different circumstances. Most of the data provided is based on subjective judgement. Uncertainty intervals are provided, but it is stated that distributions are unknown. This book is a must for all analysts who have to perform a human reliability analysis.

6.4.2 Uncertainty bounds of generic data

Generic data is extracted from a large number of plants with different maintenance policies, test frequencies, operating conditions and operating hours. This implies that all kind of data is mixed up. For instance, burn-in failures, wear-out failures, failures of components which have been replaced; all are part of the same data set. As a consequence, generic data will have a large uncertainty bound due to these differences. For this reason the mean value, presented in a generic database, has to be considered as a mean value for the population for which the data is collected.

If one selects a numerical figure for one specific type of component from different databases one must not expect to find the same figure in all databases. Reference [6.3] presents the ranges of failure rates or probabilities of failure on demand for a number of components that are usually considered in risk studies. Table 6.3 contains some typical examples. As can be seen in table 6.3, the ranges can vary between 3 and 100. Possible causes for these ranges are:

- differences in design
- differences in manufacturer
- differences in maintenance policies
- differences in environmental and operating conditions
- differences in definition in component boundaries.

Table 6.3: Example of ranges for pumps.

Component type	**Failure mode**	**Range**
Diesel-driven pump	Fail to start Fail to run	3E-4 - 3E-2 -/d 1E-3 - 3E-2 -/h
Motor-driven pump	Fail to start Fail to run	3E-4 - 3E-2 -/d 1E-4- 3E-4-/h
Turbine-driven pump	Fail to start Fail to run	3E-3 - 3E-2 -/d 1E-5 - 1E-3 -/h

6.4.3 Generic data analysis procedure

To extract data from generic sources the following steps have to be performed:

1: Identification of data requirements

2: Grouping of similar components

3: Identification of appropriate generic data

4: Aggregation of generic input to parameter estimate

Each step will be described in detail.

Step 1: Identification of data requirements

The data analysis task is performed parallel to the construction of event trees and fault trees. For each of the basic events in the model, a specification of the component involved is required, which should be as complete as possible. This means that not only the component type must be described, but also the component boundaries and the failure mode. An example regarding the component boundaries is the question whether the breakers in a pump or a diesel generator are included in the basic event as modelled in the risk and reliability analyses. When defining these component boundaries, the component boundaries generally used in generic databases must be taken into account. The failure mode of the component must be made explicit as welt. For example, the probability of a valve which fails to open might be different from the probability that a valve fails to close when required.

The failure mode also determines whether a failure frequency or a failure probability must be assessed for the basic event under consideration. For example, a diesel generator has two different failure modes: "failure to start" and "failure to run". For the "failure to start" failure mode, a probability of failure when demanded, Q, must be assessed whereas a failure frequency during operation, λ, must be assessed for the failure mode "failure to run".

Step 2: Grouping of similar components

As generic data will not be found for each very specific component as used in a particular system of the plant, it is useful to group the components according to component type and failure mode. Other groupings are possible as well, but generic sources will not use distinctions based on for example application types (system function, operating or stand-by) or engineering parameters (size, environment). The grouping based on component type and failure mode must be consistent with the generic databases.

Step 3: Identification of appropriate generic data

Generic data is searched for each of the component groups. There is a large number of generic data sources of varying quality available (both nuclear and non-nuclear). The data found in the generic data sources must be assessed for applicability. The following aspects can be considered:

Origin: Distinguish between data from nuclear and non-nuclear fields, data from different type of plants, from different manufacturers, different ages of the plant, etc.

Scope: Consider the amount of failure data included in the establishment of the generic database.

Quality: Consider the extent to which the real data can be accessed (i.e. whether the exposures and failures are documented or only a computerized summary).

Step 4: Aggregation of generic data to parameter estimate

From the generic data, either a selection must be made or an aggregation to find the required parameter estimate. In this step the following two considerations must be taken into account: data relevance and data confidence.

If one decides to combine a number of generic data sources, an aggregation methodology has to be selected. Not only the point value but also the uncertainty bounds have to be taken into account, see figure 6.1.

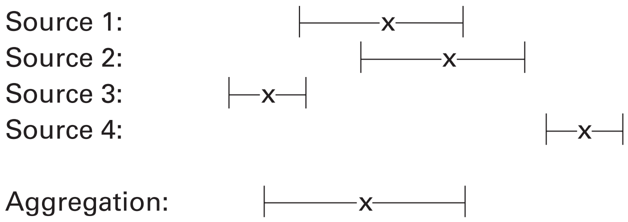


Figure 6.1: Aggregation of data from different sources.

A large number of aggregation methodologies have been proposed. In this section two rather simple methods will be provided: the weighted arithmetic average and the weighted geometric average.

Weighted arithmetic average:

$$\lambda_{mean} = \sum_{i=1}^{n} \lambda_i W_i$$

$$\sum_{i=1}^{n} W_i = 1 \qquad (6.1)$$

Weighted geometric average:

$$\lambda_{mean} = \prod_{i=1}^{n} (\lambda_i)^{W_i}$$

$$\sum_{i=1}^{n} W_i = 1 \qquad (6.2)$$

λ_i = failure rate source i
W_i = weighting factor source i
n = number of generic data sources.

The formulas presented above can be used to calculate the mean value, the lower bound and the upper bound. It is important to note that the formula to calculate the geometric average value assumes statistically independent sources.

If the different generic data sources are judged to be of equal importance, the weighting factor can be calculated using the formula:

$$W_i = \frac{1}{n} \tag{6.3}$$

Another possiblilty is to calculate the weighting factor as a function of the uncertainty bound. A high weighting factor for sources with a narrow range and a low weighting factor for sources with a large range. In this case the weighting factor reduces the influence of data sources with large ranges and vice versa increases the impact of data with narrow ranges. Data sources with wide ranges might indicate insufficient data or data from an immature database.

The following formula can be used to calculate the weighting factor as a function of the uncertainty bound expressed by an error factor:

$$W_i = \frac{\dfrac{1}{\{\ln(EF_i)\}^2}}{\sum_{i=1}^{n} \dfrac{1}{\{\ln(EF_i)\}^2}} \tag{6.4}$$

Care should be taken when applying formula (6.4). This might be the case with certain components for a specific application; a database with a wide range best represents the component under consideration white a potential database with a narrow range does not represent the actual component very well. A wide range of uncertainty must be taken into account in this situation.

6.4.4 **Failure on demand versus failure rate model**

Several important factors should be taken into account when using the demand model. If the event being considered really could occur before the demand, then using the demand model ”lumps” the failure rate into the instantaneous time of the demand. Thus, for different demand rates the probability of failure would actually be different, and if the demand model is used, a reasonable estimate is obtained only if the demand rates are similar. A component that behaves exactly as the demand model will have the same probability of failure on demand, whether the demand occurs once per hour or once per decade. In practice this will generally not be the case. So, the probabilities of failure on demand provided in generic databases cannot be used for components which are subjected to another test interval or another demand rate. If the demand rate is more or less the same (low-demanded systems) the probability of failure on demand can be modified to account for different test intervals.

To modify the probability of failure on demand given in the generic database, the following formula can be used (see reference [6.1]):

$$Q_2 = 1 - (1 - Q_1)^{T_2/T_1} \tag{6.5}$$

Q_1 = probability of failure on demand
T_1 = test interval of generic database
Q_2 = probability of failure on demand with test interval T_2
T_2 = test period in current situation.

In almost all generic databases the test interval for which the probability of failure has been determined is not provided. For databases based on nuclear experience, a test period between one and three months can be assumed.

Example:

A generic database contains the following information:

Q	=	1.0 E-02	per demand
T	=	720	hours (one month)

The component under consideration is tested on a annual basis. The corrected probability of failure on demand is:

$$\begin{aligned} Q_2 &= 1 - \{1 - (1 * 10^{-2})\}^{12} \\ &= 0.11 \end{aligned} \tag{6.6}$$

It is clear that a much higher value has to be used than that provided in the generic database.

6.5 PLANT-SPECIFIC DATA ANALYSIS

In general, generic data provides estimates based on a large population of components with different maintenance policies, different process conditions and different environmental conditions. Given the background of generic data, the uncertainty bounds will be wide. To obtain representative figures for the plant under consideration, plant-specific failure data has to be collected. By collecting the number of failure occurrences and the exposure time for a large number of components, plant-specific failure rates and plant-specific probabilities of failure on demand can be generated. Collecting plant-specific data is a time-consuming effort. It requires reporting of the failure occurrences and the processing of all those reports to obtain the required figures. The reporting must provide sufficient detail of the failure occurred to be able to identify the failure mode and to be able to classify the failure occurred.

6.5.1 Plant-specific data analysis procedure

A plant-specific data analysis can be divided into a number of separate steps:

1: Identification of data requirements

2: Collection of plant-specific information

3: Determining failure counts

4: Estimation of exposures and number of demands

5: Reducing data to reliability parameters.

Step 1. Identification of data requirements

Before the plant-specific data analysis task can be started, the scope of the plant-specific data collection has to be clearly defined. The definition of the scope depends on the information available at the plant and on the financial resources.

Component populations have to be defined by tabulating the following information about each component contained in the plant-specific data analysis scope that is referenced in the reliability model:

- System equipment tag number
- Component type
- Fault trees that contain the component
- Plant systems that contain the component.

Component boundaries have to be defined by specifying the scope of each item to be considered as a single entity for the purpose of the data analysis. For example, all pieces of a motor-operated valve are typically considered to be single ”components” when collecting reliability data, even though the valve consists of various piece parts (e.g., electric motor, gearbox, limit switches, torque switches, reversing contacts and coils, stem, disc, valve body, etc.) that may be separately identified in the plant maintenance records. The component boundaries in the plant-specific data analysis task have to be consistent with the reliability model and preferably with the generic data as well.

All component populations have to be sorted by component type as specified by the component population definitions (i.e., collect all motor-operated valves, manual valves, etc.). The component populations have to be documented in the plant-specific data analysis documentation.

In most cases it will not be possible to collect plant-specific data for all components in the reliability model. A selection has to be made. In table 6.4, an (incomplete) list is given of components for which plant-specific data is likely to be found. For each of the components several component types can be distinguished. The failure mode is a further differentiation which must be considered in the data collection task. This provides a grouping of components consistent with the generic data analysis task and with the generic databases.

Table 6.4: Components for which in general plant-specific data can be collected.

Component	Type	Failure mode
Diesel Generator		- Fail to run - Fail to start
Pumps	- Motor-driven -Turbine-driven	- Fail to run - Fail to start
Valves	- Motor-operated - Medium-operated - Check - Relief - Manual - Safety	- Fail to open - Fail to close

Step 2: Collection of plant-specific information

Sources of plant-specific information have to be identified. Typical sources include, but are not limited to, maintenance work-orders, Control Room Logs, Monthly Operating Reports and plant personnel experience.

A data window has to be established after review of the plant operating history and discussions with plant personnel. The data window will encompass, as a minimum, the most recent calender years of operating history. It has to be documented in the plant-specific data analysis documentation, along with the rationale used to establish its limits.

Finally, all information needed to complete the data analysis task is collected by execution of the following steps:

- For the component population determined by step 1 retrieve from the plant-specific sources all failure records that have occurred during the data window established.

- Collect the plant operating history by gathering all Monthly Operating Reports issued during the data window.

It must be realized that collecting plant-specific information is the greatest burden on the data analysis team.

Step 3: Determining failure counts

In the failure count, the data analyst must discriminate between catastrophic failures, degraded failures and incipient failures. Time-related versus demand-related failures. Single-component versus multiple-component failures.

Reports of maintenance of components are potential sources of data on failures, repair times after failure, and other unavailabilities due to maintenance. These reports typically include the following:

- A plant identification number for the component undergoing maintenance and a description of the component.

- A description of the reason for maintenance.

- A description of the work performed.

- An indication of the time required for the work or the duration of the component's unavailability.

The report may indicate that maintenance was needed because the component failed to operate adequately or was completely inoperable. Such an event may then be added to the count of component failures. The maintenance report often gives information about the failure mode and mechanism as well as the amount of time spent on repair after the failure was discovered. Such information must be interpreted carefully, because the actual repair time may cover only a fraction of the time the component was unavailable between the detection of the failure and the completion of repairs. In addition, the repair time is often given in terms of man-hours, which means that the actual time spent on repair could be shorter, depending on the size of the work crew; the use of recorded man-hours would therefore lead to a conservative estimate of repair time. The complete out-of-service time for the component can, however, be derived, because the maintenance record often states the date on which the failure was discovered and the date on which the component was made available after repair.

Maintenance reports that record preventive maintenance can be used to estimate the contributions of these actions to component unavailability. Again, the report may show that a component was taken out of service on a certain date and restored some time later, giving a sample of the duration of maintenance. The frequency of these events can be derived from the number of preventive-maintenance reports in the calendar time considered.

Unfortunately, sometimes the information given in the maintenance reports is incomplete. Often the descriptions of a component's unavailability or of the work performed are unclear (or missing altogether), requiring guess work as to whether an non-failed component was made unavailable by maintenance or whether the maintenance was the result of component failure. An additional problem that has already been mentioned is the difficulty in matching the failures recorded in maintenance reports with the demands or operating times reported in other documents.

Step 4: Estimation of exposures and number of demands

The establishment of exposure estimates is different for Bemand-related failures and time-related failures. The number of demands, and the number of operating hours respectively, must be assessed. The considerations and sources of information are summarized in table 6.5.

Table 6.5: Exposure estimates for demand-related and time-related failures

Demand-related failures	**Time-related failures**
Period testing	Component operation vs. system operation
Automatic and manual initiation	System operation vs. plant operation
Failure-related maintenance	Plant history: trips, shutdowns, refueling, start-ups
Interfacing maintenance	

Periodic test reports and procedures are a potential source of data on demands and operating time for components that are tested periodically. Test reports for key components or systems typically contain a description of the test procedure and a checklist to be filled out by the tester as the steps are being performed. For example, in an operating test of an emergency diesel generator, the procedure may call for starting the diesel and running it for two hours. The record of a specific test would report whether or not the diesel started and whether it ran successfully for the entire two hours. Another example is a test of emergency system performance, in which the procedure calls for the tester to give an emergency signal that should open certain flow paths by moving some motor-operated valves and starting one or more pumps. The position of the valves and the operation of the pump are then verified, giving records of whether the valves and pumps of periodic tests provide a self-contained tally of demands on some components, as well as the failure (and success) of the component given these demands.

If the records of actual periodic tests are not readily available, the test procedure can be used to estimate the number of testing demands or the operating time during tests for a component over a period of time. To do this, the number of demands or the operating time of a single test can be multiplied by the frequency of the test and the pertinent calendar time. Of course, this approach is valid only if the tests are conducted at the prescribed frequency. Some tests may in fact be conducted at more frequent intervals than those stated in the procedures. Plant personnel should be interviewed to determine what adjustments are necessary.

Operating procedures can be used to estimate the number of demands on certain components in addition to demands occurring during periodic tests. This estimate is obtained by multiplying the number of demands imposed on a component during a procedure by the number of times the procedure was carried out during the calendar time of interest. Unfortunately, the latter number is not always easily obtained. For procedures followed during plant startup or shutdown, the number of times the procedure was performed should be readily obtainable, but for procedures followed during operation, this information will be available only from the control-room log.

Many of the gaps in a component reliability database compiled from test and maintenance records can be filled by examining the control room log, which is a chronological record of important events at the plant. For example, the log has records of demands made (e.g. pumps and diesel generators) at other times than during periodic tests. It notes the starting and stopping times for these components, thus supplying operating-time data. The log also notes the initiation of various operating procedures, thus adding to the information about demand. Furthermore, it records periods when certain components and systems are out of service, and in this respect the log is often more accurate than the maintenance reports.

There is, however, a problem with using the control room log as a source of component data: all events in the log are listed chronologically, without being separated by system, type of event, or any other category. The analyst must therefore search through many irrelevant entries to find those needed for the database. The additional accuracy that is provided to the estimates of component-failure parameters by data from the log may not be worth the effort needed to search through several years of the plant history recorded in the log.

Step 5: Reducing data to reliability parameters

The objective of this task is to reduce the plant-specific data collected in step 2 and step 3 to component-level reliability parameters. A distinction has to be made between the estimation of failure rates and the estimation of probabilities of failure on demand.

Failure rates:

To calculate the point estimate and the confidence bounds of time-related failures, the following formulas can be used. These formulas are valid under the assumption that the failure rate is constant.

$$\lambda = \frac{f_T}{T} \tag{6.7}$$

$$\lambda_{0.05} = \frac{X^2\,(2\,f_T\,,\,0.05)}{2T} \tag{6.8}$$

$$\lambda_{0.95} = \frac{X^2\,(2\,f_T+2\,,\,0.95)}{2T} \tag{6.9}$$

here:

λ = failure rate mean value

$\lambda_{0.05}$ = failure rate lower confidence bound
$\lambda_{0.95}$ = failure rate upper confidence bound
$X^{2}(v,p)$ = pth percentile of a Chi-square distribution with v degrees of freedom
f_T = number of time-related failures
T = time interval over which the f_T failures occurred

In appendix 6-A a table is provided to calculate the Chi-square distribution.

Demand probabilities:
To calculate the point estimate and confidence bounds of demand-related failures,
the following formulas are valid. Also, in this case it is assumed that the probability of failure on demand is constant.

$$Q = \frac{f_D}{D} \tag{6.10}$$

$$Q_{0.05} = \frac{f_D\ F_{0.05}(2\ f_D\ ,\ 2D - 2f_D + 2)}{D - f_D + 1 + f_D\ \ F_{0.05}(2f_D,\ 2D - 2f_D + 2)} \tag{6.11}$$

$$Q_{0.95} = \frac{(f_D + 1)\ F_{0.95}(2\ f_D + 2,\ 2D - 2f_D)}{D - f_D + (f_D\ \ +1)\ F_{0.95}(2f_D,\ +2,\ 2D - 2f_D)} \tag{6.12}$$

where:

Q	=	failure-on-demand probability of mean value
$Q_{0.05}$	=	failure-on-demand-probability of lower confidence bound
$Q_{0.95}$	=	failure-on-demand-probability of upper confidence bound
$F_p(v_1,v_2)$	=	pth percentile of an F distribution with v_1 and v_2 degrees of freedom
f_D	=	number of demand-related failures
D	=	number of demands over which the f_D failures occurred.

In appendix 6-A tables are provided to calculate the F distribution.

6.5.2 **Example**

This example concerns a data analysis to determine the probability of failure on demand for the emergency diesel generators of six coal-fired power units (A, B, C, D, E, F).

During normal operation the emergency diesel generators are not in operation but in a stand-by mode of operatien. After failure of the power supply the emergency diesel generators receive an actuation signal to start. Every diesel generator is tested once a month. All Goal fired units are in possession of a diesel logbook. In this logbook the number of tests and the number of demands are reported. Also, the number of failures are reported in this logbook.

All logbooks have been reviewed very carefully to identify the type of failures and to count the number of failures to start on demand. The results of this investigation are reported in table 6.6

Table 6.6: Results plant-specific data collection.

Plant	Power DG (kVA)	Number of demands	Number of failures
A	600	520	1
B	1000	653	2
C	200	408	1
D	200	408	9
E	2500	199	2
F	100	943	16

By application of the formulas to calculate the point value and confidence bounds for demand related failures, the probability of failure on demand and the corrsponding confidence bounds can be calculated for each coal-fired unit separately. The results are tabulated in table 6.7.

Table 6.7: Results mean, lower bound and upper bound.

Plant	Number of demands	Number of failures	Mean (-/d)	Lower bound (5%)	Upper bound (95%)	Error Factor
A	520	1	1.9E-03	9.9E-05	9.1E-03	9.6
B	653	2	3.1E-03	5.41E-04	9.61E-03	4.2
C	408	1	2.5E-03	1.3E-04	1.2E-02	9.6
D	408	9	2.2E-02	1.2E-02	3.8E-02	1.8
E	199	2	1.0E-02	1.8E-03	3.1E-02	4.2
F	943	16	1.7E-02	1.1E-02	2.6E-02	1.6

In figure 6.2 the results for each separate diesel generator have been plotted. Both point value for the calculated mean value and the lower and upper confidence bounds are plotted.

In spite of the large differences in power of the six emergency diesel generators (200 kVA and 2500 kVA) the differences in the probability of failure on demand are rather small for plants A, B and C and for plants D, E and F. One gets the impression that the diesel generators for plants A, B and C on the one hand and the diesel generators D, E and F on the other belong to different populations.

Review of the technical information of the diesel generators showed that the diesel generators in plants A, B and C are equipped with a start repeater. If the first starting attempt is not successful, a second attempt and if necessary a third attempt will be made. After three failures the starting process is stopped. The failure data shows that start repeaters reduce the probability of failure on demand considerably. Two populations are defined; one of diesel generators with start repeaters and one without start repeaters.

For each population the arithmetic and geometrie mean and confidence bounds can be calculated. The final resuits are listed in table 6.8. The calculated arithmetic and geometrie avarages are almost equal for each population.

Table 6.8: Results data analysis of diesel generators.

Population	Average	Mean (-/d)	Lower bound (5 %)	Upper bound (95%)	Error factor
A, B, C	Arithmetic	2.48E-03	2.56E-04	1.01E-02	6.3
	Geometrie	2.44E-03	1.89E-04	1.00E-02	7.3
D, E, F	Arithmetic	1.64E-02	8.00E-03	3.17E-02	2.0
	Geometrie	1.56E-02	6.04E-03	3.13E-02	2.3

Evaluation:

Based on the information available at the plants; it was possible to determine the main contributors to the ”failure to start” probabilities:

Fuel system	:	18 per cent
Starting system	:	18 per cent
Control system	;	18 per cent
Heating	:	12 per cent
Unknown	:	25 per cent

The lessons learned are:

- differences in manufacturers do not result in differences in ”failure-to-start” probabilities
- differences in design can be of major importante to the failure-to-start probability.

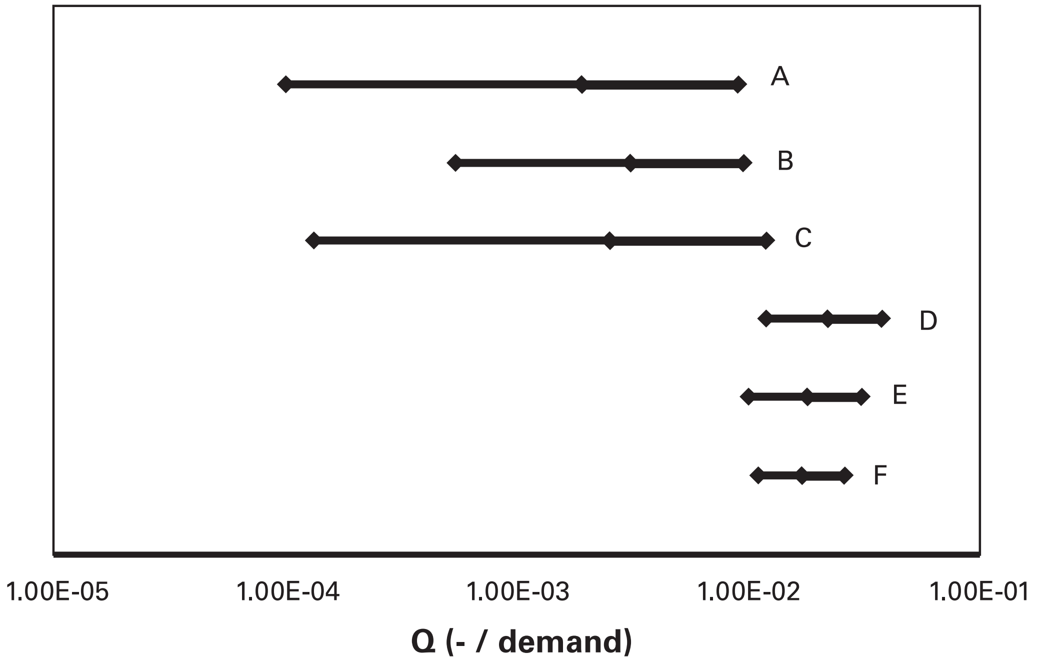


Figure 6.2: Estimated probabilities of failure on demand and uncertainty bounds.

6.6 USE OF EXPERT OPINION

6.6.1 Introduction

Often ”hard, objective” data are not available and one is forced to make use of expert-opinions, which by their nature are subjective. Although consulting experts is nothing new -it is commonly known as ”Engineering Judgement”- the use of expert opinion still raises the question of the quality of this kind of data. It will be clear that this quality will depend on the quality of the experts interviewed and the quality of the elicitation process itself. A careful choice of experts, if possible calibrated, and of the elicitation procedure and a good preparation of the interview session are therefore paramount.

In the section 6.6.3 the sources of biases in expert opinion and the means to prevent, reduce or quantify them are discussed. Section 6.6.5 summarizes the different elicitation methodologies and quantification models. An example is given in the final section.

6.6.2 Conditions for use of data

In order to use data based on expert opinion in an accountable way ”engineering judgement” will have to be replaced by a more structured process of elicitation. This means amongst other things that the following should be stated:

- the criteria used to select the experts
- the elicitation process
- whether or not difference is made between ”better” and ”worse” experts; and how this is done
- the method used to combine the opinions of different experts.

Also, the uncertainty in the answers given by the experts should be stated explicitly. Point estimates contain in general not enough information to base decisions on. The expert’s knowledge should therefore be modelled as a probability distribution.

Two items concerning quality are of importance in determining and using such probability distributions:

- how good is the knowledge of the expert in the area of concern ?
- how capable is the expert in expressing his knowledge, and translating and relating it into probabilities ?

In other words: how good is the estimated mean value or median, and estimated confidence interval?

6.6.3 Expert opinion and biases

Manifestation of biases:

Subjective estimates of uncertain variables will always contain biases. These biases influence the accuracy of the expert’s estimate in a negative way. Two different biases can be discerned:

over/underestimation : the expert tends to underestimate or overestimate (extreme) incidents, resulting in a too optimistic or too pessimistic value of the estimated median value

overconfidence : the tendency of the expert to estimate the confidence interval to narrowly. Underconfidence is of course also possible.

This is illustrated graphically in the figure below:

```
real situation                    x---------------  o   -------------x
overconficence                                x---  o  -------x
overestimation                               x---------------  o   -------------x
example of expert’s estimation                          x---   o   -------x
```

Both biases are equally important for the quality of the data. The methods used to elicit expert opinion can contribute significantly to reducing the biases. In addition to this interpretation problems play an important role. It will be clear that the phrasing of the questions as well as the way of posing them can exercise great influence on reducing or enlarging biases.

Causes of biases and solutions:

The causes of biases are many and in references [6.6], [6.7] and [6.8] an array of types are discerned:

1 **Expert level:**
A distinct cause for both biases is the fact that the expert in the worst case is not an expert at all.

2 **Probabilism:**
The expert is unfamiliar with probabilism. The probabilistic aspect causes a discrepancy between knowledge of the expert and estimated values.

3 **Anchoring:**
Anchoring is the phenomenon that in the estimation process a starting value is chosen, which is then corrected insufficiently.

4 **Systems:**
The tendency to estimate the probability of success of a series system too high and of a parallel system too low.

5 **Availability:**
Some events are more readily available than others, because they are easier to envisage or have a special meaning to the expert.

6 **Representativeness:**
Only part of the information available and necessary is used.

7 **Base-rate fallacy:**
Part of the underlying assumptions is not taken into account; Stereotyping is a special case.

8 **Control:**
The feeling to be able to control events results in too optimistic estimates.

9 **Motivation:**
The (un)conscious drive for a certain estimate or outcome of the analysis.

This list is not complete, but gives the most important causes for biases. More causes, illustrated with examples, can be found in references [6.5], [6.6], [6.7] and [6.8].

There are two ways to cope with the possible biases:

- prevent or reduce bias during the elicitation session
- quantify the biases and take them into account.

The solutions to prevent and reduce biases in the elicitation phase are partly trivial, but certainly not unimportant and are of a qualitative nature:

- the recognition of the existence of biases and the underlying causes reduces in itself the influence to a large extent
- the analyst has to probe for the background and scenarios on which the expert "bases" his or her estimates
- complex parameters and parameters with implicit conditions should be broken down
- the relation between parameters and objective of the analysis has to be disguised for the experts
- the expert needs to understand probabilism.

These measures will reduce the influence of all causes except cause 1 : "expert level".To cope with this problem a different, quantitative approach is needed. This approach is discussed in section 6.6.5, where models to process and combine expert opinions are discussed.

6.6.4 **The interview session**

The above list of causes and solutions to biases shows that in order to obtain reliable and thus useful data based on expert opinion, the set-up and implementation of the elicitation interview is very important. References [6.7] as well as [6.8] address this topic and give practical guidelines to streamline the process.

Motivation:
Problem, objective and approach should be explained to the expert as well as the way in which his answers will be processed. It should be clear to the expert that it is not the intention to predict a value, but to elicit his knowledge and opinion. The importance of a good estimation of the uncertainty bounds should also be made clear.

Format of question and answers:
The format of the questions as well as the answers should appeal to the expert. In general a preference exists for giving answers graphically, for instance by putting tick marks in a box or along a scale.The straightforward question to elicit numbers is less effective.The units have to be the expert's choice. His preferente can be numerical, for instance a failure rate per hour, per week or year, or a description: high or low. Going through one or two example questions can effectively clarify the whole process.

Clear questions:
It is not easy to formulate clear and unambiguous questions. Nevertheless, it is of the utmost importance to prevent interpretation problems and irritation (to the expert the analyst seems not to know what he wants). One way to test questions on the subject of unambiguity is the clairvoyance test, see reference [6.8]. Starting point is a clairvoyant person, who knows the correct answer to every question. In a mental experiment the question is examined whether the clairvoyant can answer the question directly or if additional information is needed. In the latter

case the question is not formulated accurately enough or has to be broken down.

Testing:
Testing of the questions generally improves them.

Coaching:
The expert is the expert, not the analyst.

Duration:
Experience shows that an interview session should not exceed one or two hours. If more time is needed it is better to organize a second session.

6.6.5 **Models**

Obtaining data from expert opinions consists in principle of two parts. The first part is the elicitation process of obtaining the opinion of one expert. The second part is the process of evaluating and combining the different opinions.

Elicitation:

The elicitation process can be direct or indirect. The differente is mainly caused by the method of questioning to gather the expert's opinions. In case of direct elicitation the expert is asked directly to state a probability (of exceeding) for a certain value or a value for a given probability. This kind of questioning needs (some) probabilistic feeling of the expert.
In the case of indirect elicitation no values and probabilities are asked. The expert is asked to compare events with other events. Part of the events have known probabilities. The advantage of the indirect way of questioning is that the questions are simple: a relative, qualitative judgement is asked for. Furthermore no probabilistic knowledge is necessary. It can be a problem to find sufficient events of a known probability, with relevance to the subject under question.

Evaluation and combination:

Evaluation and combination techniques can be divided into two groups:
- consensus techniques
- mathematical techniques.

Consensus techniques:
Consensus techniques attempt to reach iteratively a mutual point of view of all experts by way of discussions and feedback of the results. The best known method using this principle is undoubtedly DELPHI

The DELPHI method

This is a method to combine the knowledge of a group of experts and is characterized by (see reference [6.4]):

- a group of experts and an organizing team
- a questionnaire, which is formulated in consultation with the group of experts
- guaranteed anonymity of the answers and sometimes of the experts themselves
- a possibility to adjust one's view, based on the summary of the group's results
- two to five iterative cycles.

Using the DELPHI method, experts do not meet each other and so the estimates are made individually. The individual estimates are processed, giving all experts the same weight.

The Nominal Group Technique

This is basically the same as DELPHI, except that direct interaction between the experts is possible. The problems concerning dominant personalities are said to have been limited, as no joint estimate is generated during the discussions. Every group member makes his own estimate after the discussion.

The Consensus Group Technique

This takes the discussion even further than the Nominal Group Technique, by making the estimate also part of the discussion.

The advantage of DELPHI over the Nominal and Consensus Group Techniques is the fact that experts do not have to meet, resulting in a minimum effort on their part. Also, the negative effects of group processes (dominant personalities, personal aversion etc.) are circumvented. On the other hand, clear disadvantages are the fact that interpretation differences between the experts will not surface easily, nor will hidden agendas etc. Finding the optimum between full and no interaction is the crux when using consensus techniques. Controlling and directing the group processes is one of the main tasks of the analyst.

The main drawback of all consensus techniques is the Jack of information about the quality of the experts. In references [6.9] and [6.10] consensus techniques are criticized because they do not yield better results for the mean value than the mathematical mean value approach, in principle the first step of DELPHI, and because they have a tendency of creating over-confidence in other words, too small confidence bounds. This is especially a point of attention to the analyst.

Mathematical techniques:

Mean value, without weighting

This is a technique in which the experts do not meet and estimates are made individually. The estimates are aggregated statistically by calculating for instance the geometrical mean value. The consistency between the various experts can be analyzed using for instance analysis of the variance.

The main disadvantage of the method is the equal weight of the experts. In the consensus techniques the expert do not have equal weights, although it is impossible to check and say why, how much, and which experts are assigned more weight than others.

Mean value, including weighting

Assigning weights to experts can be considered if a substantial difference is expected in the quality of the various estimates. Mathematically this can be expressed as follows. Suppose p_i is the probability density function of expert i, p_{tot} is the total probability density function over all experts n, and w_i is the normalized weighting factor:

linear:

$$p_{tot} \quad = \quad \sum_{i=1}^{n} w_i \, p_i \, ; \qquad\qquad \sum_{i=1}^{n} w_i \;\; 1 \; = \; w_i \geq 0 \qquad (6.13)$$

log-linear:

$$\log p \quad = \quad \sum_{i=1}^{n} w_i \log p_i \qquad (6.14)$$

The value of the weighting factor w_i can be determined in various ways. Experience, age or number of publications can for instance be used as criterion for a (supposed) level of knowledge. Another commonly used method is self assessment, possibly in combination with the assessment of the other experts. All these methods of assessment are subjective.

A method to obtain objective weighting factors is calibration (see reference [6.11]). The weighting factor of an expert is determined on the basis of the expert's score on test variables, using classical statistical tests. The basic assumption is that the achievement of the expert in generating an estimate of something unknown can be judged by his the achievement on known subjects.

The main problem using this method is the test variables. They should be relevant to the analysis and their real values should be known or become known at short notice.

It is not recommended to use formula (6.4) to calculate the weighting factors, because a large uncertainty bound does not imply a poor expert. A narrow uncertainty bound can indicate overconfidence of the expert.

Bayes

Another technique using weighting in combining expert opinions employs Bayes theorem of updating the prior distribution with the expert opinion to a posterior distribution.

In this case the use of test variables is necessary as well. As a general qualification of Bayesian models it can be stated that the number of assumptions is large, reducing the value of the outcome, or that the number of test variables is large. Furthermore, due to the enormous amount of calculus, the applicability is limited to a maximum of two or three experts.

No interaction between experts is used in the mathematical techniques. The quality of experts is taken into account by using weights. The most commonly used techniques and easiest to apply weights are based on subjective data. Their subjective nature makes them prone to criticism. The use of objective weights, however, is complicated by the need for test variables with relevance to the analysis in question.

6.6.6. **Example**

From the Reliability-Centred Maintenance analysis (RCM analysis, see section 17, Structuring of Maintenance) of a chemical plant, it became apparent that for a number of components the use-based maintenance intervals could be optimized. The calculation of the optimal maintenance intervals would be greatly facilitated by good estimates of some of the service lives of the components involved.

As no plant and maintenance records were available to draw relevant information from, expert opinion was used to obtain service life estimates.

			X					
		X	X	X				
X		X	X	X	X	X		
3	3.5	4	4.5	5	5.5	6	6.5	7

Figure 6.3 Estimates (in years) of expert 1 for component D.

Elicitation was accomplished using the consensus group technique, with three experts.The outline of the procedure used is as follows:

- the experts list reasons and conditions liable to increase or decrease the service life of the component;
- the experts estimate minimum and maximum service lives for each component;
- the experts estimate the likely service life between these two extremes by inserting crosses representing a 10% chance of a component lasting for the period in question. In figure 6.3 an example of such an estimation is given.

Based on these estimations, the analysis can be taken one step further by fitting the data to e.g. a Weibull distribution to obtain mean values and if necessary confidence bounds. In figure 6.4 the results of such an analysis are shown for component D.

An example of these last estimates is given in figure 6.4. The figure shows the results for component D.

- if the experts differ significantly in their estimates, the matter is discussed with a view to arriving at a consensus.

The first three steps were done independently by all three experts. In table 6.9 the estimates for six components are summarized. Interestingly, for every component one of the experts (but not always the same) disagreed with the other two. The deviant estimate is marked grey in table 6.9. The differences are sometimes rather large; for component D the difference is a factor of five.

Table 6.9: Estimated mean service life according to experts (weeks).

Component	Type	Expert 1	Expert 2	Expert 3
A	filter	15	38	13
B	solenoid valve	180	207	509
C	brake system	220	118	213
D	bearing	48	245	51
E	pump	20	53	54
F	transport cylinder	19	17	10

The following conclusions were drawn, after discussions with the experts.

Component A, filter.
Expert 2 estimated the filter's service life to be relatively long compared with the other experts, because he classified early failure problems as random failures, which could not be prevented by (use-based) maintenance. As such random failures have nothing to do with the failure mechanisms (ageing) of the component, he disregarded the early failures. Experts 1 and 3 agreed to amend their estimates for the filter, to take account of the influential factors from outside the component only identified by expert 2, resulting in a final estimation close to the earlier estimation of expert 2.

Component B, solenoid valve:
The differences between experts 1 and 2, and expert 3 became clear during the discussion: they were talking about different types of solenoid valves. As a result, this component was split into two groups, with life expectancies of approximately 200 and 500 weeks.

Component C, brake system:
Experts 1 and 3 made similar predictions regarding the service life of the brake system; their predictions corresponded closely to the few data available. Expert 2 was more pessimistic about the component, but was prepared to modify his estimate as a result of the arguments used by the other experts.

Component D, bearing:
Again, expert 2 disagreed with his colleagues, but this time the disagreement was very substantial. As no consensus could be reached, a different maintenance approach was chosen rather than going for the shortest estimated life expectancy. Although RCM analysis advised use based maintenance, alternatively condition-based maintenance was recommended for a short period. The service life estimate could then be adjusted in due course on the basis of the inspection results at every stoppage. When better insight into the life expectancy is gained, one should switch back to use-based maintenance.

Components E and F, pump and transport cylinder:
Although differences existed between the experts' estimates, no discussion was held as irrespective of the differences the same optimum maintenance interval was calculated: at every scheduled stoppage.

Remarks
From the foregoing it is clear that a good definition of the component is of paramount importance. Most of the time stating the type of equipment only will not be sufficient, as environment, manufacturer and sub-type can have a major influence on the life expectancy.

Causes of failure and failure mechanisms should not be restricted to internal ones. The relative contribution of random failures (i.e. random for the component) can determine the choice of the maintenance strategy and the estimated life expectancy. A complete list of factors influencing the life should be available and all experts should use the same list as a reference.
estimated life (week)

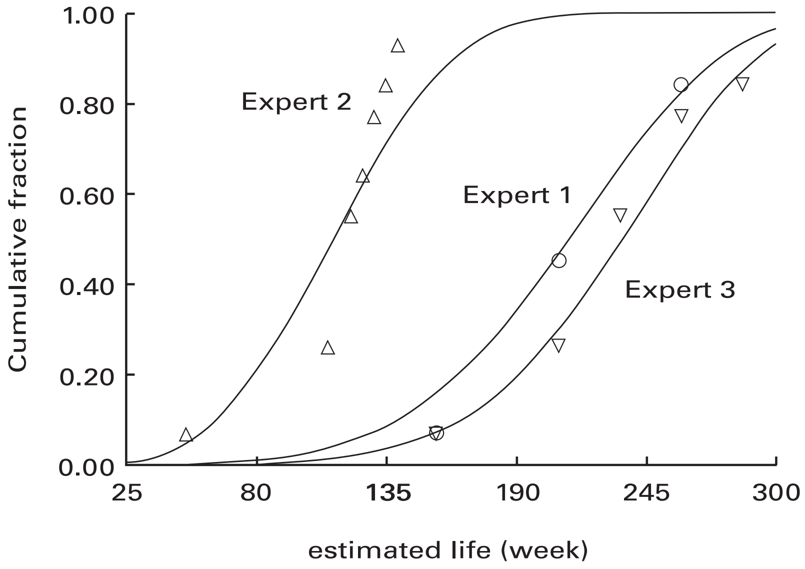


Figure 6.4: Cumulative frequency plots of life estimates and corresponding Weibull-2 fit; Median ranking is used on the data as obtained from plots as given in figure 6.3.

6.7 BAYESIAN UPDATING TECHNIO.UE

Both generic data and plant-specific data have their advantages and disadvantages. The pros and cons of generic and plant-specific data are:

Generic data:

- Generic data banks are based on a large number of failure occurrences.

- Generic data banks contain a wide range of component types.

- Generic data is rarely conservative in nature. For example, many generic data sources have been created by using sources that restrict the number of reportable component failures and, thus, underestimate the true component failure characteristics.

- Generic data banks provide estimates based on a large population of components with different maintenance policies, different test frequencies and different process and environmental conditions. This implies that the uncertainty bound wilt be wide.

- The data extracted from a generic database is more or less accepted in the international community.

Plant-specific data:

- Plant-specific data best represents the failure behavior of the components under consideration.

- The inclusion of plant-specific data in a risk or reliability analysis lends credibility to the study. Moreover, it allows for comparison of plant performance with other plants.

- It is not possible to collect plant-specific data for all components or initiating events addressed by the reliability model. Extremely reliable components (e.g. instrumentation, control circuits or other equipment with long mean time between failures) may never have failed in the history of the plant or within the time window considered. The lack of failure history makes it difficult to estimate the true failure rate or probability. In addition, it is impossible to collect a meaningful exposure spectrum on certain components (for example, the number of demands placed on a relay) using the existing plant records.

It is clear that plant-specific failure data best represents the failure behavior of the system to be analyzed. Therefore, it is advisable to make use of plant-specific data to the extent possible. A well-known problem is that only a limited amount of plant-specific failure data will be available if the population consists of only one or a few plants. The optimum result can be achieved by combining the little plant-specific evidence available with the generic data available. The underlying philosophy of a data analysis should therefore be to use plant-specific data whenever possible, as dictated by the availability of relevant information and good statistical practice.

At the point where for all component groups either generic estimates, plant-specific estimates are or both are established, a selection or a combination of these must be made. If no maintenance records are available or if the budget is not sufficient, one must use generic data. If a lot of plant-specific evidence is available one is able to calculate reliability parameters completely based on plant-specific failures using the classical approach (Chi-squared, see section 6.5). In case of little plant-specific evidence or figures based on expert judgement one has to perform a Bayesian update process to get as much information from the data as possible.

Note that the question whether plant-specific data is collected must also be answered positively when an exposures estimate is made in which zero failures occurred. The criterion whether statistical information is sufficient or not, relies on good statistical practice.

The objective of the Bayesian update method is to combine generic data and plant-specific data in such a way that the influence of the plant-specific data in the updated data grows as the period in which data is collected or the number of failures grows. The method is especially useful if little plant-specific data is available or little confidence exist in the plant-specific data.

The generic information is referred to as knowledge "prior" to the plant-specific data. The prior knowledge is an uncertainty distribution about the possible value of the component failure parameter: λ or Q. The Bayesian update process changes the generic uncertainty distribution into a "posterior" distribution by incorporating the plant-specific data. Both the mean value of this distribution and its spread (the uncertainty) might change during the update process. This is illustrated in figure 6.5.

Prior distribution:
A probability distribution which describes the knowledge one has about the failure rate of a component based on generic data or based on subjective judgement.

Posterior distribution:
A probability distribution which describes the knowledge one has about the failure rate of a component after data of the component failures have been taken into account.

Non-informative distribution:
A prior distribution which contains as little information as possible about the failure rate of a component in relation to the information which can be expected in the future failure statistics of the component in question.

Generic distribution:
A probability distribution which describes an uncertainty which is relevant for a broader population than the one to which the current plant belongs.

The generic prior data must be reduced to a form that permits the selection of a specific prior distribution from a suitable famlily. For example, if a lognormal family has been selected, the two lognormal parameters must be determined from the generic data. If there are multiple sets of generic prior data, these must likewise be reduced to a common consensus prior.

Using the Bayesian update technique requires numerical integration. Only for a few specific distribution functions are closed-form solutions are possible. For both failure rates and probabilities of failure on demand the closed-form solutions will be provided in this section. The mathematical background can be found in reference [6.1] and chapter number 4.

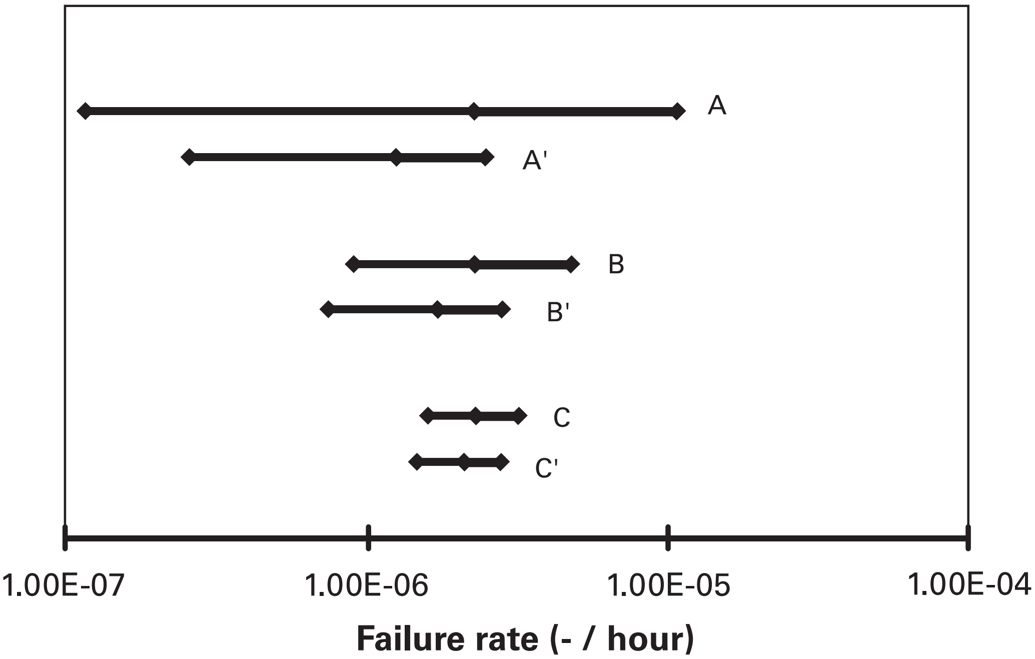


Figure 6.5 : Principle of the Bayesian update method.

6.7.1 Bayesian update process procedure

Step 1: Calculation of variance in prior distribution.

To perform the Bayesian update, first the logarithmic standard deviation of the generic data's uncertainty distribution has to be calculated:

$$\sigma = \frac{\ln(EF)}{1.645} \tag{6.15}$$

where:
σ = logarithmic standard deviation
EF = log-normal error factor of the generic data's uncertainty distribution

Second, the variance of the generic data's uncertainty distribution has to be determined:

$$\mathrm{Var} = x^2 \{\mathrm{EXP}\ (\sigma^2) - 1\} \tag{6.16}$$

where:
Var = variance of the generic data's uncertainty distribution
x = mean of the generic data's uncertainty distribution
σ = logarithmic standard deviation

Step 2: Estimation of prior α and β.

The prior distribution parameters α and β have to be estimated. If failure rates are being updated, then α and β are parameters of a gamma distribution. If failure probabilities are being updated, then α and β are the parameters of a beta distribution, see reference [6.1]. Alpha can be interpreted as the prior number of failures in beta prior total operating time or as the prior number of failures in beta prior demands.

Failure rates:

$$\begin{aligned} \alpha &= \frac{x^2}{\mathrm{Var}} \\ \beta &= \frac{x}{\mathrm{Var}} \end{aligned} \tag{6.17}$$

Failure probabilities on demand:

$$\begin{aligned} \alpha &= \frac{x^2\ (1 - x)}{\mathrm{Var}} - x \\ \beta &= \frac{x\ (1 - x)^2}{\mathrm{Var}} - 1 + x \end{aligned} \tag{6.18}$$

Step 3: Estimation of posterior α' and β'.

Bayesian update is performed by calculating the posterior distribution parameters α' and β'.

Failure rates:

$$\begin{aligned} \alpha' &= \alpha + f_T \\ \beta' &= \beta + T \end{aligned} \tag{6.19}$$

Failure probabilities on demand:

$$\alpha' = \alpha + f_D$$
$$\beta' = \beta + D - f_D \qquad (6.20)$$

f_T = number of time-related failures
T = time interval over which the f_T failures occurred
f_D = number of demand-related failures
D = number of demands over which the f_D failures occurred.

Step 4: Estimation of posterior mean and variance.

The posterior distribution's mean and variance can be calculated with the formulas:

Failure rates:

$$x' = \frac{\alpha'}{\beta'}$$
$$Var' = \frac{\alpha'}{(\beta')^2} \qquad (6.21)$$

Failure probabilities on demand:

$$x' = \frac{\alpha'}{\alpha' + \beta'}$$
$$Var' = \frac{\alpha' * \beta'}{(\alpha' + \beta' + 1)\ (\alpha' + \beta')^2} \qquad (6.22)$$

x = posterior mean value
Var = posterior variance

Step 5: Estimation of lower and upper bound.

Failure rates:

$$x'_{0.05} = \frac{X^2\ (2\ \alpha'\ ,\ 0.05)}{2\ \beta'}$$
$$x'_{0.95} = \frac{X^2\ (2\ \alpha'\ ,\ 0.95)}{2\ \beta'} \qquad (6.23)$$

Failure probabilities on demand:

$$x'_{0.05} = \frac{\alpha'}{\alpha' + \beta' \, F_{0.05} \, (2\,\beta', 2\alpha')}$$

$$x'_{0.95} = \frac{\alpha' \, F_{0.95} \, (2\alpha', 2\beta')}{\beta' + \alpha' \, F_{0.95} \, (2\alpha', 2\beta')} \tag{6.24}$$

An estimate of the error factor for the posterior distribution can be calculated with the formula:

$$EF' = \sqrt{\frac{x'_{0.95}}{x'_{0.05}}} \tag{6.25}$$

6.7.2 **Example of Bayesian updata**

To demonstrate the Bayesian update technique, a numerical example will be provided concering updating the generic failure rate of a transformer with three different options of plant-specific evidence. The generic information is as follows:

λ	=	10^{-6}	-/hour
EF	=	3	
MTTF	=	114	year

Three different options are considered for the plant-specific evidence. Option one considers one failure over an exposure time of 50 years, option two considers 5 failures over an exposure time of 250 years and option three 25 failures over an exposure time of 1250 years. In Table 6.10 the plant-specific evidence is tabulated.

Table 6.10: Plant-specific evidence.

Options	Exposure time (years)	Number of failures
A	50	1
B	250	5
C	1250	25

Classical evalution:

Given the plant-specific evidence, the mean value, lower confidence bound and upper confidence bound can be calculated with the formulas presented in section 6.5. The results are listed in Table 6.11.

Table 6.11: Chi-squared evaluation.

Option	Mean (-/hour)	Lower bound (-/hour)	Upper bound (-/hour)	EF
A	2.28E-06	1.17E-07	1.08E-05	9.6
B	2.28E-06	9.00E-07	4.80E-06	2.3
C	2.28E-06	1.59E-06	3.19E-06	1.4

As expected, wide uncertainty bounds are found for option A (only one failure occurrence) and a narrow uncertainty bound for option C (25 failure occurrences). Corresponding error factors are calculated: a high value for option A and a low value for option C.

Bayesian update:

To perform the Bayesian update process, the five steps described in section 6.7.1 have to be performed.

$$\sigma = \frac{\ln(EF)}{1.645} = \frac{\ln(3)}{1.645} = 0.67 \tag{6.26}$$

Step 1: logarithmic standard deviation and variance

$$Var = x^2 \{EXP(\sigma^2)\text{-}1\} = (1.0E\text{-}06)^2 \{EXP(0.67\ 0.67) - 1\} = 5.62\ E\text{-}13 \tag{6.27}$$

Step 2: Prior alpha and beta.

$$\alpha = \frac{x^2}{Var} = \frac{(1.0E - 06)^2}{5.62E - 13} = 1.78 \qquad (6.28)$$

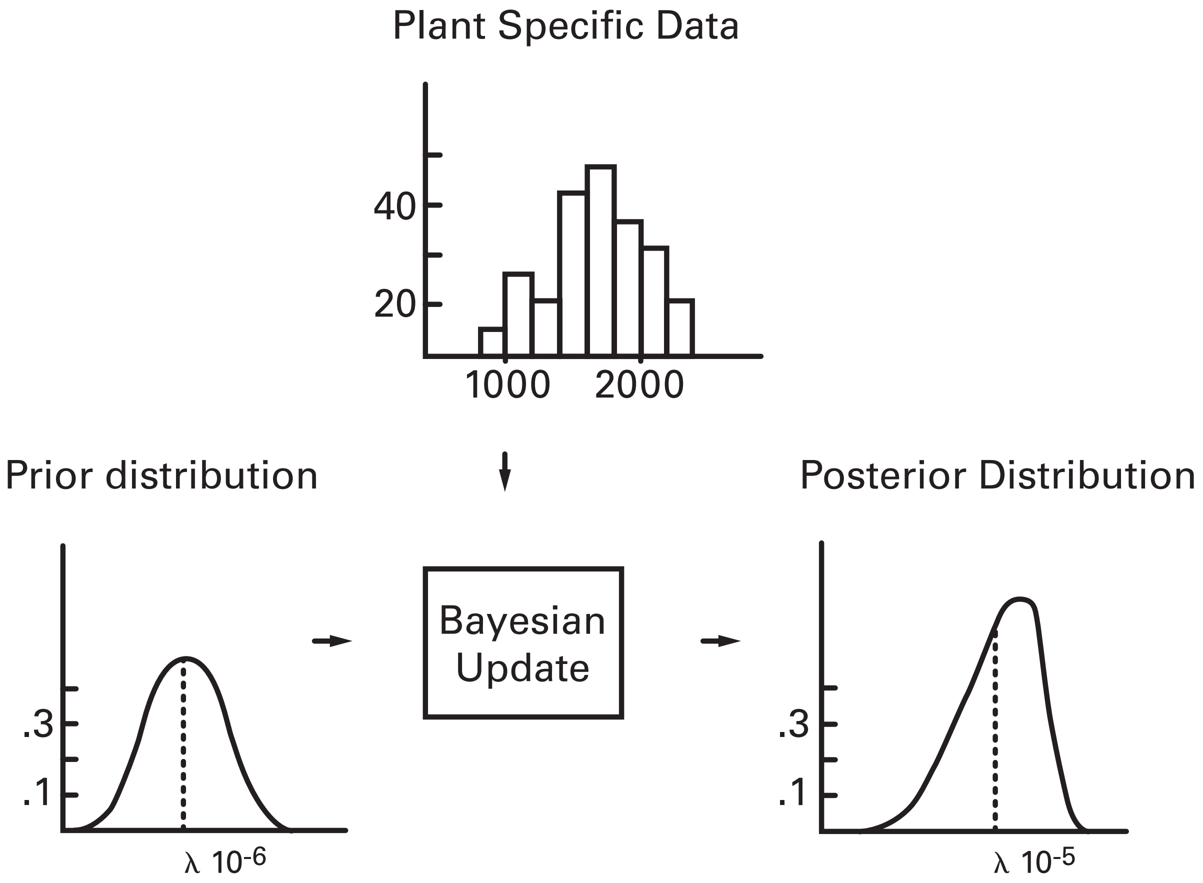
$$\beta = \frac{x}{Var} = \frac{1.0E - 06}{5.62E - 13} = 1.8E+6 \qquad (6.29)$$

Remaining steps:
The posterior alpha, beta, mean, lower and upper bound and error factor have to be calculated. In Table 6.12 the results are listed.

Table 6.12: Results of Bayesian update.

Option	α'	β'	Mean (-/hour)	Lower bound (-/hour)	Upper bound (-/hour)	MTTF (years)	EF
A'	2.78	2.22E+06	1.25E-06	2.58E-07	2.50E-06	91	3.1
B'	6.78	3.97E+06	1.71E-06	7.42E-07	2.82E-06	67	1.9
C'	26.78	1.27E+07	2.10E-06	1.46E-06	2.79E-06	54	1.4

From Table 6.12 it can be concluded that the posterior error factor for option A has been reduced considerably in comparison with the error factor based on the Chi-squared analysis (see Table 6.11). It can be concluded also from Table 6.12 that the Bayesian update process is usefull only if a limited amount of plant-specific failure data is available. In case of a lot of plant-specific failure data (option C) the posterior error factor is almost equal to the error factor based on the Chi-squared approach. In Figure 6.6 the results are graphically presented.



Fígure 6.6: Example of Bayesian update technique.

6.8 ASSESSMENT OF COMPONENT DOWNTIME

The mean time to repair is not so easy to assess. In generic data banks, generally no information can be found on the time necessary to repair a component or system. When the plant records are investigated for information, it often appears that the occurrence of a failure and the associated request for maintenance are documented, but the lapse of time until the component was really repaired is not reported.

The best approach is therefore to organize interviews with the experienced plant operators, shift supervisors and maintenance personnel. This is easy to implement but often time-consuming and difficult to validate. In these interviews, the aim is to find not only a best estimate of the repair time but also to ask about the variation in the repair times. The experts are, for example, asked to remember the shortest and longest period of time that a component was out of operation due to repair activities.

In general, there are two problems in assessing the uncertainty about the mean time to repair:

- The time necessary to repair a component can vary widely in practical situations
- The subjective expert interviews often exhibit a pessimistic or an optimistic bias and the confidence intervals are generally too narrow in the assessment.

Experience indicates that several hours are required for each interview. The experienced people who should cooperate are generally in great demand and may not be available during the time required to perform the interview.

The problems related to the validity of the assessment must consider the bias of an expert. The first type of bias is the "location bias", estimates can be optimistic or pessimistic, and the second type of bias is called "scale bias", referring to the fact that the experts are generally overconfident with respect to their assessments. The location bias can be great: In some studies using expert opinion, the analysts discovered that the 65 per cent percentile was frequently a more desirable estimate of the true probability than other measures like mean or median (50 per cent percentile). Studies on the scale bias indicate that, people think that they can estimate values with much greater accuracy than is actually the case.

Accounting for the location bias can be done by interviewing the experts about a component with a known outage history. This event is called an anchor event or seed variable. The various expert's opinions are combined based on the assessment that is made by each expert. The assumption underlying this approach is that the bias indicated by each expert, relative to the anchor event, is the same as for all other components that are investigated in the same way.

The scale bias is accounted for by an interview methodology which stretches the responder to the extent of credibility about the extremest high and low values. This is carried out by challenging the responses with additional questions, such as "Are you certain that this is the greatest/smallest quantity you can remember?". This technique examines the expert's confidence in the boundary he sets and encourages him to push his thoughts to farther and farther bounds.

Thus, for both the failure frequency λ and the repair time θ, an uncertainty distribution (best estimate plus interval) is established.

The uncertainty distribution for the unavailability of the component due to maintenance, $U = \lambda\theta$, is now characterized by the following mean and variance:

$$\begin{aligned} E(U) &= E(\lambda)\, E(\theta) \\ Var(U) &= Var(\lambda)\, Var(\theta) + Var(\lambda)\, E(\theta)^2 + Var(\theta)\, E(\lambda)^2 \end{aligned} \tag{6.30}$$

If a lognormal distribution is used for the two parameter uncertainties λ and θ, then the uncertainty distribution for the unavailability U is again a lognormal distribution. This is the reason why the lognormal distribution is often used in risk and reliability studies.

6.9 ASSESSMENT OF INITIATING EVENT FREQUENCIES

Initiating events are the occurrences that initiate an accident sequence. The desired measure for such events is frequency. A plant may experience dozens of these events per year or only one in 10,000 years. The objective of this task is to assess the initiating event frequencies based on both the plant-specific data and the generic data.

The assumption made about initiating events is that they occur randomly over time at a constant rate: the initiating event frequency. However, data on events that occur more frequently indicate that the rate of occurrence may be higher during the plant's first years than during subsequent years. For the purpose of initiating event frequency quantification, the techniques described in section 6.5 to assess a constant failure frequency λ of a component, can be used.

The initiating events are either single events or modelled by means of a fault tree. The latter possibility refers to the case where there are more causes for the initiating event occurrence. The quantification of such a fault tree with frequencies of occurrence might be different from the quantification of an ordinary fault tree in which basic event probabilities are combined.

The following sources of information consulted for the initiating event quantification:

Plant-specific data
Monthly operating reports of the specific plant, over a selected time window.

Estimates from other nuclear experience (Generic data)

- Previous risk analyses
- Analyses of pipe break fracture mechanics
- etc.

In some cases it will be very useful to perform a Bayesian update. This makes it possible to combine frequency estimates from generic data sources with the plant-specific operating experience.

6.10 REFERENCES

[6.1] PRA Procedures Guide
A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants.
U.S. Nuclear Regulatory Commission, NUREG/CR-2300 Final Report, January 1983.

[6.2] IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations, The institute of Electrical and Electronics Engineers, Inc.
345 East 47 Street, New York, NY 10017

[6.3] IAEA-TECDOC-508,
Survey of ranges of component reliability data for use in probabilistic safety assessment International Atomic Energy Agency, Vienna 1989.

[6.4] Linstone, H. A. and Turoff, M. The Delphi Method: Techniques and Applications. Reading, 1975

[6.5] Kahneman, D., Slovic, P., Tversky, A., (eds.) Judgement Under Uncertainty, Heuristics and Biases, Cambridge, 1982

[6.6] Mosleh, A, Bier, V.M., Apostolakis, G, A Critique of Current Practise for the Use of Expert Opinions in Probabilistic Risk Assessments, Reliability Engineering and Systems Safety Volume 20, (1988), pp 63-85

[6.7] Cooke, R.M., Experts in Uncertainty, New York, 1991

[6.8] McNamee, P, Celona, J., Decision Analysis with Supertree, San Fransisco, 1990

[6.9] Sackman, H., Delphi Critique, Expert Opinion, Forecasting and Group Processes, Lexington, 1975

[6.10] Fischer, G.W., When Oracles Fail, Organisational Behaviour and Human Performance, Volume 9 (1973), pp 96-110

[6.11] Steen, van, J.F.J., Oortman Gerlings, P.D., Expert Opinions in Safety studies, Volume 2, Literature Survey Report, Delft University of Technology, 1989

APPENDIX 6- A: TABLES CHI-SQUARED AND F-DISTRIBUTION

Table 6-A-1: Chi-Square distibution.

V	P		V	P	
	0.05	0.95		0.05	0.95
1	0.00393	3.84	19	10.1	30.1
2	0.103	5.99	20	10.9	31.4
3	0.352	7.81	21	11.6	32.7
4	0.711	9.49	22	12.3	33.9
5	1.15	11.1	23	13.1	35.2
6	1.64	12.6	24	13.8	36.4
7	2.17	14.1	25	14.6	37.7
8	2.73	15.5	26	15.4	38.9
9	3.33	16.9	27	16.2	40.1
10	3.94	18.3	28	16.9	41.3
11	4.57	19.7	29	17.7	42.6
12	5.23	21.0	30	18.5	43.8
13	5.89	22.4	31	19.3	45.0
14	6.57	23.7	32	20.1	46.2
15	7.26	25.0	33	20.9	47.4
16	7.96	26.3	34	21.7	48.6
17	8.67	27.6	35	22.5	49.8
18	9.39	28.9			

Table 6-A-2: F-Distribution 0.05 percentiles.

	v_1									
v_2	**2**	**4**	**6**	**8**	**10**	**20**	**40**	**60**	**120**	**1000**
2	0.0526	0.1440	0.1944	0.2243	0.2437	0.2863	0.3094	0.3174	0.3255	0.3328
4	0.0520	0.1565	0.2206	0.2606	0.2875	0.3489	0.3837	0.3960	0.4086	0.4200
6	0.0517	0.1623	0.2334	0.2793	0.3108	0.3848	0.4281	0.4436	0.4598	0.4745
8	0.0516	0.1655	0.2411	0.2909	0.3256	0.4087	0.4587	0.4769	0.4959	0.5134
10	0.0516	0.1677	0.2463	0.2988	0.3358	0.4259	0.4814	0.5019	0.5234	0.5434
12	0.0515	0.1692	0.2500	0.3045	0.3433	0.4391	0.4991	0.5215	0.5453	0.5676
14	0.0515	0.1703	0.2528	0.3089	0.3491	0.4494	0.5134	0.5376	0.5634	0.5877
16	0.0515	0.1711	0.2550	0.3123	0.3537	0.4579	0.5253	0.5509	0.5785	0.6047
18	0.0514	0.1718	0.2567	0.3151	0.3574	0.4649	0.5353	0.5623	0.5916	0.6195
20	0.0514	0.1723	0.2581	0.3174	0.3605	0.4708	0.5438	0.5721	0.6029	0.6325
22	0.0514	0.1728	0.2593	0.3194	0.3631	0.4758	0.5512	0.5806	0.6129	0.6440
24	0.0514	0.1732	0.2603	0.3210	0.3653	0.4802	0.5577	0.5882	0.6217	0.6544
26	0.0514	0.1735	0.2612	0.3224	0.3673	0.4840	0.5635	0.5949	0.6297	0.6637
28	0.0514	0.1738	0.2619	0.3237	0.3689	0.4874	0.5686	0.6009	0.6368	0.6722
30	0.0514	0.1740	0.2626	0.3247	0.3704	0.4904	0.5733	0.6064	0.6434	0.6800
40	0.0514	0.1749	0.2650	0.3286	0.3758	0.5015	0.5907	0.6272	0.6688	0.7111
60	0.0513	0.1758	0.2674	0.3327	0.3815	0.5138	0.6108	0.6518	0.6998	0.7508
120	0.0513	0.1767	0.2699	0.3370	0.3876	0.5273	0.6343	0.6815	0.7397	0.8074
1000	0.0513	0.1776	0.2722	0.3410	0.3932	0.5406	0.6590	0.7146	0.7890	0.9012

Table 6-A-3: F-Distribution 0.95 percentiles.

	v_1									
v_2	**2**	**4**	**6**	**8**	**10**	**20**	**40**	**60**	**120**	**1000**
2	19.0000	19.2467	19.3295	19.3709	19.3959	19.4457	19.4707	19.4791	19.4873	19.4948
4	6.9443	6.3882	6.1631	6.0410	5.9644	5.8025	5.7170	5.6878	5.6581	5.6317
6	5.1432	4.5337	4.2839	4.1468	4.0600	3.8742	3.7743	3.7398	3.7047	3.6732
8	4.4590	3.8379	3.5806	3.4381	3.3472	3.1503	3.0428	3.0053	2.9669	2.9324
10	4.1028	3.4780	3.2172	3.0717	2.9782	2.7740	2.6609	2.6211	2.5801	2.5430
12	3.8853	3.2592	2.9961	2.8486	2.7534	2.5436	2.4259	2.3842	2.3410	2.3017
14	3.7389	3.1122	2.8477	2.6987	2.6022	2.3879	2.2663	2.2229	2.1778	2.1365
16	3.6337	3.0069	2.7413	2.5911	2.4935	2.2756	2.1507	2.1058	2.0589	2.0157
18	3.5546	2.9277	2.6613	2.5102	2.4117	2.1906	2.0629	2.0166	1.9681	1.9232
20	3.4928	2.8661	2.5990	2.4471	2.3479	2.1242	1.9938	1.9464	1.8963	1.8497
22	3.4434	2.8167	2.5491	2.3965	2.2967	2.0707	1.9380	1.8894	1.8380	1.7899
24	3.4028	2.7763	2.5082	2.3551	2.2547	2.0267	1.8920	1.8424	1.7896	1.7401
26	3.3690	2.7426	2.4741	2.3205	2.2197	1.9898	1.8533	1.8027	1.7488	1.6978
28	3.3404	2.7141	2.4453	2.2913	2.1900	1.9586	1.8203	1.7689	1.7138	1.6615
30	3.3158	2.6896	2.4205	2.2662	2.1646	1.9317	1.7918	1.7396	1.6835	1.6299
40	3.2317	2.6060	2.3359	2.1802	2.0773	1.8389	1.6928	1.6373	1.5766	1.5175
60	3.1504	2.5252	2.2541	2.0970	1.9926	1.7480	1.5943	1.5343	1.4673	1.3994
120	3.0718	2.4472	2.1750	2.0164	1.9105	1.6587	1.4952	1.4290	1.3519	1.2675
1000	3.0047	2.3808	2.1076	1.9476	1.8402	1.5811	1.4063	1.3318	1.2385	1.1097

APPENDIX 6- B: Generic Component Failure Data Base

This appendix provides a generic data base for a large number of components and failure modes. To generate these generic data the following data books have been used.

Source **Description**

(1) Guidelines for Process Equipment Reliability Data, with data tables, Center for Chemical Process Safety of the American Institute of Chemical Engineers, 345 East 47th Street, New York, New York 10017, ISBN 0-8169-0422-7.

(2) IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations, IEEE Std 500-1984, The Institute of Electrical and Electronics Engineers, Inc, 345 East 47th Street, New York, NY 10017, ISBN 471-80785-0.

(3) OREDA, Offshore Reliability Data Handbook, 2nd Edition, Det Norske Veritas Industri Norge as DNV Technica, P.O. Box 300, N-1322 HOVIK, NORWAY, ISBN 82 515 0188 1.

(4) T-book, 4rd edition, Reliability Data of Components in Nordic Nuclear Power Plants, Prepared by TUD-kansliet, Studsvik Eco & Safety AB and Pórn Consulting, The ATV office Vattenfall AB, 162 15 Vállingby, Sweden, ISBN 91-7186-303-6.

(5) Eireda, European Industry Reliability Data, Industrial Plants, Volume 2, Second Edition, 1995, Electricite de France - Direction des Etudes et Recherches Departement Retour d'Experience Mesures Essais, 93206 Saint-Denis (Paris) France, ISBN 2-9509092-0-5.

(6) Component Failure Rate Comparison and Recommendations for various processing fluids, S.A. Eide, L.C. Cadwallader, and J.N. Wilkinson, Idaho National Engineering Laboratory, P.O. Box 1625, Idaho Falls, ID, USA, 83415.

(7) Handboek kanscijfers ten behoeve van het opstellen van een Veiligheidsrapport, AMINAL Dienst Gevaarlijke Stoffen en Risicobeheer, Ministerie van de vlaamse gemeenschap, Departement leefmilieu en infrastructuur.

(8) Handleiding voor het opstellen en beoordelen van een extern veiligheidsrapport (EVR), IPO-publikatienummer 73, Interprovinciaal overleg IPO, Floris Grijpstraat 2, Postbus 977278, 2509 GC Den Haag.

(9) Auditing and Safety Management for Safe Operations and Land Use Planning: A Cross-national comparison and validation exercise, A Report for the Commission of the European Comminities, Contract EV5V-CT92-0068, Environmental Programme, 20 december 1995.

To compile this database the mean value and the lower and upper bound for each data source has been determined. Using the methodology explained in section 6.4.3 the uniform weighted arithmetic and uniform weighted geometric average has been calculated. The final numbers, presented in the database, have been determined by using the following procedure:

Mean value:	select highest value from arithmetic and geometric means.
Lower bound:	select lowest lower bound from arithmetic and geometric lower bounds.
Upper bound:	select highest upper bound from arithmetic and geometric upper bounds.
Median value:	calculated by using the formulas presented in section 4.4.9.

For pipe and vessel breaks no uncertainty data was presented in the available data source. The uncertainty figures presented in "Component Failure Rate Comparison and Recommendations for various processing fluids", by S.A. Eide, L.C. Cadwallader, and J.N. Wilkinson, has been used. Given a mean value and an error factor the other figures can be generate by assuming a lognormal distribution.

	Component and	Mean	LB	Median	UB	EF	Sources
	failure mode	(h-1)	(h-1)	(h-1)	(h-1)	__	
1	Sensors						
1.1	Pressure						
1.1.1	*Fails to operate*	6.3E-07	6.5E-08	3.2E-07	1.6E-06	4.9	1,2,3,4
1.1.2	*Spurious operation*	6.6E-07	2.9E-08	1.8E-07	1.1E-06	6.1	1,2,3,4
1.2	Temperature						
1.2.1	*Fails to operate*	2.6E-06	8.5E-08	8.3E-07	8.0E-06	9.7	1,2,3,4
1.2.2	*Spurious operation*	1.0E-06	9.3E-08	5.4E-07	3.2E-06	5.9	1,2,3,4
1.3	Flow						
1.3.1	*Fails to operate*	2.7E-06	2.4E-07	1.5E-06	9.9E-06	6.4	1,2,3,4
1.3.2	*Spurious operation*	1.1E-06	4.5E-07	8.5E-07	1.6E-06	1.9	1,2,3,4
1.4	Level						
1.4.1	Fails to operate	6.9E-07	2.0E-07	4.8E-07	1.2E-06	2.4	1,2,3,4
1.4.2	*Spurious operation*	5.2E-07	8.0E-08	2.9E-07	1.1E-06	3.7	1,2,3,4
2	Transmitters						
2.1	Pressure						
2.1.1	*Fails to obtain signal*	7.3E-07	2.4E-07	5.9E-07	1.4E-06	2.4	2,3,4
2.2	Temperature						
2.2.1	*Fails to obtain signal*	5.3E-07	9.6E-08	3.9E-07	1.6E-06	4.0	2,3,4
2.3	Flow						
2.3.1	*Fails to obtain signal*	3.2E-06	1.4E-06	2.7E-06	5.4E-06	2.0	2,3,4
2.4	Level						
2.4.1	*Fails to obtain signal*	8.9E-07	1.2E-07	5.2E-07	2.3E-06	4.3	2,3,4
3	Valves						
3.1	Air operated valves						
3.1.1	*Fails to operate*	1.7E-05	5.5E-06	1.2E-05	2.8E-05	2.3	3,4,5,7
3.1.2	*Spurious operation*	1.7E-06	2.3E-07	1.5E-06	1.0E-05	6.7	1,2,3,5,6
3.2	Solenoid						
3.2.1	*Fails to operate*	2.6E-07	8.2E-08	1.9E-07	4.2E-07	2.3	4
3.2.2	*Spurious operation*	6.3E-07	1.4E-07	6.2E-07	2.7E-06	4.3	1,2,6
3.3	Motor operated valves						
3.3.1	*Fails to operate*	6.8E-06	2.2E-06	5.1E-06	1.2E-05	2.3	3,4
3.3.2	*Spurious operation*	9.5E-07	1.6E-07	7.5E-07	3.4E-06	4.6	1,2,3
3.4	Control valve						
3.4.1	*Fails to operate*	5.9E-06	3.7E-06	5.9E-06	9.5E-06	1.6	3,4
3.4.2	*Spurious operation*	8.3E-07	6.5E-08	5.3E-07	4.4E-06	8.3	3,5
3.5	Check valve						
3.5.1	*Fails to open*	1.1E-07	9.6E-09	5.2E-08	2.8E-07	5.4	3,4,5
3.5.2	*Fails to close*	2.2E-07	2.4E-08	1.0E-07	4.1E-07	4.1	3,4,5
3.6	Safety valve, spring operated						
3.6.1	*Fails to open*	6.2E-08	3.3E-09	3.3E-08	3.4E-07	10.3	1,5,7
3.6.2	*Spurious opening*	8.6E-07	2.1E-07	1.1E-06	5.5E-06	5.1	4,5
3.7	Safety valve, pilot operated						
3.7.1	*Fails to open*	4.8E-07	1.0E-08	1.3E-07	1.8E-06	13.2	1,4,5
3.7.2	*Spurious opening*	4.4E-06	8.6E-07	5.6E-06	3.6E-05	6.5	4,5

	Component and failure mode	Mean (h-1)	LB (h-1)	Median (h-1)	UB (h-1)	EF	Sources
4	Pumps						
4.1	Pumps, centrifugal, motor driven						
4.1.1	*Fails to start*	2.6E-05	6.0E-06	1.7E-05	4.7E-05	2.8	3,4,6
4.1.2	*Fails to run*	6.4E-05	1.7E-06	2.4E-05	3.3E-04	13.8	1,2,3,4,6
4.2	Pumps, reciprocating, motor driven						
4.2.1	*Fails to start*	2.3E-05	5.0E-06	1.5E-05	4.8E-05	3.1	3,4
4.2.2	*Fails to run*	4.3E-05	1.2E-05	3.2E-05	9.0E-05	2.8	3
4.3	Pumps, turbine driven						
4.3.1	*Fails to start*	9.9E-06	1.2E-06	6.2E-06	3.3E-05	5.3	1,3,6
4.3.2	*Fails to run*	5.6E-04	5.4E-05	2.4E-04	1.1E-03	4.4	1,3,6
4.4	Pumps, diesel driven						
4.4.1	*Fails to start*	5.1E-05	6.0E-06	2.0E-05	6.8E-05	3.4	3,6
4.4.2	*Fails to run*	2.5E-03	1.0E-04	1.6E-03	2.5E-02	15.9	3,6
5	Compressors						
5.1	Compressor, motor driven						
5.1.1	*Fails to start*	1.4E-05	2.8E-06	1.4E-05	7.0E-05	5.0	6
5.1.2	*Fails to run*	1.0E-04	1.0E-05	1.0E-04	1.0E-03	10.0	6
5.2	Compressor, turbine driven						
5.2.1	*Fails to start*	1.8E-05	3.2E-06	9.9E-06	3.0E-05	3.1	1,3
5.2.2	*Fails to run*	No data available					
6	Batteries, rectifiers, inverters						
6.1	Batteries						
6.1.1	*Fails to provide power*	1.2E-06	2.3E-07	9.2E-07	3.6E-06	4.0	1,3,4,5
6.2	Rectifier						
6.2.1	*Loss of output*	9.9E-07	2.3E-07	6.7E-07	2.0E-06	2.9	1,3,4
6.3	Inverter						
6.3.1	*Loss of output*	1.4E-05	1.5E-06	8.2E-06	4.3E-05	5.3	1,3,4,5
7	Switches						
7.1	Relay						
7.1.1	*Fails to operate*	3.5E-08	2.4E-09	2.9E-08	3.4E-07	11.9	2,6
7.1.2	*Spurious operation*	2.0E-07	1.5E-08	1.9E-07	2.3E-06	12.3	1,2,6
7.2	Electronic limit switch						
7.2.1	*Fails to operate*	5.9E-08	6.4E-09	2.9E-08	1.3E-07	4.6	4,6
7.2.2	*Spurious operation*	7.2E-07	1.6E-07	9.2E-07	5.3E-06	5.8	4,6
8	Breakers						
8.1	Breakers, 6-10 kV						
8.1.1	*Fails to operate*	2.5E-06	2.8E-07	1.1E-06	4.1E-06	3.8	3,4
8.1.2	*Spurious operation*	1.2E-06	1.8E-07	6.9E-07	2.6E-06	3.8	3,4
8.2	Breakers, < 1 kV						
8.2.1	*Fails to operate*	1.9E-07	8.5E-08	1.8E-07	3.9E-07	2.1	3,4
8.2.2	*Spurious operation*	1.6E-07	6.4E-08	1.3E-07	2.8E-07	2.1	3,4

	Component and failure mode	Mean (h-1)	LB (h-1)	Median (h-1)	UB (h-1)	EF	Sources
9	Busbar						
9.1	Busbar, 6 < U < 20 kV						
9.1.1	*Fails to provide power*	4.1E-07	1.1E-07	3.1E-07	8.6E-07	2.8	4
9.2	Busbar, < 1 kV						
9.2.1	*Fails to provide power*	1.7E-07	7.6E-08	1.5E-07	3.0E-07	2.0	4
10	Diesel driven generators						
10.1	*Fails to start*	1.5E-04	2.8E-05	9.8E-05	3.5E-04	3.5	1,3,4,6
10.2	*Fails to run*	3.4E-03	6.3E-04	3.6E-03	2.0E-02	5.7	1,4,6
11	Transformers						
11.1	Power transformers						
11.1.1	*Fails to provide power*	1.7E-06	2.3E-07	1.2E-06	6.1E-06	5.2	1,2,4,5,6
11.2	Instrument transformers						
11.2.1	*Fails to provide power*	6.7E-07	1.0E-07	7.6E-07	5.5E-06	7.2	2,6
12	Fuses						
12.1	*Fails to open*	2.8E-09	2.8E-10	2.8E-09	2.8E-08	10.0	6
12.2	*Premature opening*	3.7E-07	1.6E-08	1.6E-07	1.7E-06	10.2	1,6
13	Pipings						
13.1	D<75mm						
13.1.1	*Leakage*	5.7E-10	2.1E-11	2.1E-10	2.1E-09	10.0	9
13.1.2	*Break*	1.1E-10	4.5E-13	1.3E-11	4.0E-10	30.0	9
13.2	75<D<150mm						
13.2.1	*Leakage*	2.3E-10	8.6E-12	8.6E-11	8.6E-10	10.0	9
13.2.2	*Break*	3.4E-11	1.3E-13	4.0E-12	1.2E-10	30.0	9
14	Static Pressure Vessels						
14.1	*Basic Failure Rate*	1.1E-10	4.3E-13	1.3E-11	3.9E-10	30.0	9
14,2	*Catastrophic failure instantaneous release*	5.7E-11	2.2E-13	6.7E-12	2.0E-10	30.0	9
14.3	*Catastrophic failure short continuous release*	5.7E-11	2.2E-13	6.7E-12	2.0E-10	30.0	9
14.4	*Leakage trom a 10 mmm hole*	1.1E-09	4.1E-11	4.1E-10	4.1E-09	10.0	9
15	Static single walled vessels						
15.1	*Catastrophic failure*	1.1E-09	4.3E-12	1.3E-10	3.9E-09	30.0	9
16	Reactor vessels and process vessels (e.g.heat exchangers)						
16.1	*Basic Failure Rate*	1.1E-09	4.3E-12	1.3E-10	3.9E-09	30.0	9
16.2	*Catastrophic failure instantaneous release*	5.7E-10	2.2E-12	6.7E-11	2.0E-09	30.0	9
16.3	*Catastrophic failure short continuous release*	5.7E-10	2.2E-12	6.7E-11	2.0E-09	30.0	9
16.4	*Leakage from a 10 mm hole*	1.1E-08	4.1E-10	4.1E-09	4.1E-08	10.0	9

	Component and failure mode	Mean (h-1)	LB (h-1)	Median (h-1)	UB (h-1)	EF	Sources
17	Filters						
17.1	*Plugged*	7.5E-06	1.2E-06	6.5E-06	3.4E-05	5.2	3.6.7
17.2	*Fail open*	3.1E-06	4.3E-07	3.8E-06	3.3E-05	8.9	3.6.7

METHODS OF IDENTIFICATION OF FAILURE SCENARIOS

CONTENTS **Page**

7.1 INTRODUCTION

A Hazard can be defined as a physical condition that has the potential causing damage to people, property, or environment (see reference [5]). This definition includes danger to people arising within a short timescale (e.g. fire or explosion) and also types of danger that have a long term effect on a person's health (e.g release of toxic substance).

Hazard identification consists of the identification of serious incidents which may result in danger to employees or the public or environment or in financial loss.

Fundamental methods can be used to identify the underlying root causes which can lead to the undesired consequences, as welt as to identify those incidents which could lead to problems related to operability, maintainability and other problems. Considering accident sequences or failure scenarios, the first event of the scenario is called the initiating event.The initiating event can be a pipe rupture or some other plant disturbance. Intermediate events can be operator failure or failure of one or more safety devices.

Risk is defined as the unwanted consequences of a particular activity in relation to the probability that this may occur (See Reference [6]). So the risk consists of two characteristic variables: the magnitude of the consequence and the probability that these may occur. A risk analysis usually consists of the identification of all equipment failures or plant upsets and identification of the intermediate failure events leading to undesired consequences and calculation of the probability of occurrence of these undesired consequences.

In the past a large number of analysis techniques have been developed for Risk or Hazards identification and evaluation. It is important to make a distinction between qualitative and quantitative analysis techniques. Both type of techniques are used to reduce risk or to avoid Hazardous situations.

A qualitative analysis technique is mostly used for Risk or Hazard identification and accident sequence development. Evaluation of Risk or Hazards can be done by either a qualitative technique or a quantitative technique. If a qualitative method is used, a risk graph is sometimes used to classify the risk into a number of categories.

In this book qualitative analysis techniques are primarily used to identify Hazardous situations and to identify failure scenarios which can lead to unwanted consequences. A quantitative method is used to calculate the probability of occurrence of the unwanted consequence for a period of one year.

Based on references [7.1] to [7.11] the most important risk and reliability analysis techniques will be described in this chapter.

The purpose of this chapter is to provide brief descriptions of the most important hazard or risk identification and evaluation techniques which are often employed by modern system safety practitioners. A number of techniques which are of minor importance or are not very well known are listed in appendix 7-A.

Subject-specific analysis techniques such as: Data Analysis, Human Error Analysis and Dependent Failure Analysis are not included in this chapter. For those techniques reference is made to the relevant chapters in this book.

The Hazard and Risk identification and evaluation techniques which will be covered in this chapter are:

Qualitative Analysis Techniques:
- Safety Review
- Checklist Analysis - Relative Ranking
- Preliminary Hazard Analysis
- What-If Analysis
- Hazard and Operability Analysis
- Failure Modes and Effects Analysis
- Criticality Analysis.

From a perspective of completeness it is important that the most important undesired consequences have been identified and taken into account in the Hazard evaluation or risk assessment. Completeness depends on how sophisticated the identification technique is and how well known the Hazards are. For existing technology the Hazards may be known form past experience and a simpte identification technique will be sufficient to identify the important Hazards. For new applications a more detailed analysis technique like the HAZOP or the FMEA technique will be necessary to attain sufficient confidence that all important Hazards have been identified.

Quantitative Analysis Techniques:
- Fault Tree Analysis
- Markov Processes
- Event Tree Analysis
- Monte Carlo Simulation.

The most common way to model accident sequences is the event tree approach. This is particularly useful if the plant upset or equipment failure can result in different consequences from a risk standpoint. If only one consequente needs to be analysed, all our quantitative methods can be applied.

If the probability of failure on demand of a safety system has to be calculated, the fault tree technique, or the Markov Processes or the Monte Carlo simulation can be used. If applied properly, all three methodologies will generate the same results, taking into account the constraints of each methodology and a proper comparison of the results generated with the different approaches.

Information Presentation

A common method of information presentation will be applied to describe each evaluation technique, in order to facilitate comparisons and selections. The method of information presentation follows this pattern:

Description:
A succinct statement of the process which must be followed to apply the technique is provided. This description is a digest of information drawn from the references coupled.

Application:
Special system/subsystem/component areas to which the technique may be applicable are noted, as are processes/activities/procedures. Areas of inapplicability are also delineated. where this has been appropriate. Techniques which are especially applicable to manned systems, activities and procedures are so identified. (Objective descriptions of areas of application are difficult to assemble for all but the more highly specialized techniques: the practitioners of a given technique have often developed diversified methods for using it which will have given it the appearance of being universally applicable.)

Solidity:
By their nature, some techniques are well suited to broad and/or rapid, superficial studies, while others lend themselves to finely detailed, in-depth explorations. Comments on these aspects of thoroughness are provided.

Expertise Required:
Some techniques lend themselves to easy application by the untrained novice, whereas others may require formal study and some practical experience. An attempt has been made to indicate the degree of preparation required for the successful use of each technique.

Difficulty of Application:
Presuming that a given technique has been adequately mastered and that it is not mis-applied, its use may produce acceptable results either with relative ease or at great expense in time and resources. Comments on these features are provided here.

Comments:
Miscellaneous notes and precautions drawn largely from discussions with practitioners of techniques are presented where applicable.

7.2 OVERVIEW OF QUALITATIVE EVALUATION TECHNIQUES

Qualitative evaluation techniques are normally applied to identify any potential Hazard as a consequence of the operation of a facility. For existing technology and an experienced Hazard evaluation team a simple qualitative evaluation technique may be sufficient to identify all conceivable Hazards. For new technology applications of limited past experience the Hazard evaluation team may ”brainstorm” on potential failures, using techniques like ”What-If” analyses. Once a design progresses into the pre-engineering phase, a more detailed technique like the Hazop or FMEA is preferable for Hazard identification and evaluation.

7.2.1 Safety review

Description:
This technique, which can also be referred to as a Process Safety Review, a Design Review or a Loss Prevention review, can be used at any stage during the life cycle of the plant. When performed on existing facilities, the safety review typically involves a walk-trough inspection that can vary from informal, routine visual examination, to a formal examination performed by a team, which takes several weeks. For plants that are still being designed, a design project team might, for example, review a set of documents and drawings during a meeting.

Application:
Safety Reviews are intended to identify plant conditions or operating procedures that could lead to an accident and result in injuries, significant property damage, or environmental impacts. A typical Safety Review includes interviews with many people in the plant: operators, maintenance staff, engineers, management, safety staff, and others, depending upon the plant organization. Safety Reviews should be viewed as cooperative efforts to improve the overall safety and performance of the plant, rather than as an interface to normal operations or as a reaction to a perceived problem.

Solidity:
For a comprehensive review, the team members will need access to applicable codes and standards, previous safety studies, detailed plant descriptions, such as P&ID's and flowcharts, plant procedures for start-up, shutdown, normal operation, maintenance records, such as critical instrument checks, pressure relief vaive tests, and pressure vessel inspections and material characteristics.

Expertise Required:
The personeel assigned to Safety Review inspections must be very familiar with safety standards and procedures. Special technical skills and experience are helpful for evaluating instrumentation, electrical systems, pressure vessels, process materials and chemistry, and other special topics.

Difficulty of Application:
Cooperation is essential; people are likely to become defensive unless a considerable effort is made to present the review as a benefit to affected plant personnel and designers.

7.2.2 Checklist analysis

Description:
A Checklist Analysis uses a written list of items or procedural steps to verify the status of a system. Checklists contain possible failures and causes of hazardous events. Checklists are based on operating experience and are often used in risk analyses. Traditionally, checklists vary widely in their level of detail and are frequently used to indicate compliance with standards and practices.

Application:
The purpose of a checklist is to provide a stimulus to critical appraisal of all aspects of the system rather than to lay down specific requirements. As a minimum, a checklist can be used to ensure that the design is in accordance with standard practices. In general a checklist is most useful to identify customarily recognized hazards.

Solidity:
Checklists are limited by their author's experience; therefore, they should be developed by authors with varied backgrounds who have extensive experience with the system they are analysing. Frequently, checklists are created by simply organizing information from currently relevant codes, standards and regulations. Checklists should be considered as living documents and should be audited and updated regularly.

Expertise Required:
The Checklist Analysis is easy to use. But it should be clear that the use of checklists depends critically on the expertise and judgement of the engineer selecting and applying the checklist. As a result decisions taken by the engineer with regard to the checklist selected, and any additional or superfluous questions, should be fully documented and justified.

Difficulty of Application:
Given the availability of experience in the field of application, the use of checklists is straightforward and uncomplicated.

7.2.3 **Relative ranking**

Description:
Relative ranking is actually an analysis strategy rather than a single, well-defined analysis method. This strategy allows hazard analysts to compare the attributes of several processes or activities to determine whether they possess hazardous characteristics that are significant enough to warrant further study. These comparisons are based on numerical values that represent the relative level of significance that the analyst gives to each hazard.

Application:
Relative ranking studies should normally be performed early in the life of a process, before the detailed design is completed, or early in the development of an existing facility's hazard analysis program.

Solidity:
The main purpose of using relative ranking methods is to determine the process areas or operations that are most significant with respect to the hazard of concern in a given study. The philosophy behind relative ranking approaches is to address these risk analysis questions to determine the relative importance of processes and activities from a safety standpoint, before performing additional and more costly hazard evaluation or risk analysis studies.

Expertise Required:
A relative ranking study can be carried out by a single analyst. Several analysts can work together on a large, complex process when they are experienced in working with the relative

ranking technique and have access to all of the input data needed. To obtain consistent results, it is crucial that all analysts are ”calibrated” in the same way.

Difficulty of Application:
A technique is easy to apply for an analyst who is familiar with the process and well trained in applying the relative ranking methodology.

7.2.4 **Preliminary Hazard analysis**

Description:
As a broad, initial study, identify apparent hazards, feasibility of controlling them, and methods which might be applied to effect the control. Alternatively, apply any hazard analysis techniques, singly or in combination, very early in the system life cycle, preferably during formulation of the design concept.

Application:
Preliminary hazard analyses may be applied universally to all systems, subsystems, components, procedures, interfaces, etc. To satisfy the definition, they must be performed preliminarily - i.e. prior to or as an initial step of design, shakedown, operation, maintenance, refurbishment etc.

Solidity:
Solidity depends upon the technique(s) used and the depth to which they are employed.

Expertise Required:
Acquiring competence is dependent upon the technique(s) selected with which to perform the Preliminary Hazard Analysis.

Difficulty of Application:
Selection of technique(s) to be used determines the difficulty of application. The Preliminary Hazard Analysis is not a discrete technique. Instead, it is the application of any technique, or any group of them, performed preliminarily, e.g. prior to the specific life cycle phase to which that analysis applies.

7.2.5 **What-If analysis**

Description:
The What-If analysis technique is a brainstorming approach in which a group of experienced people familiar with the subject process ask questions or voice concerns about possible undesired events. It is not as inherently structured as some other techniques like HAZOP or FMEA. The What-If Analysis concept encourages the team to think of questions that begin with ”What if”. However, any process safety concern can be questioned, even if it is not phrased as a question.

Application:
The purpose of a What-If Analysis is to identify hazards, hazardous situations or specific accident events that could produce an undesirable consequence. Since What-If analysis is so flexible, it can be performed at any stage of the process life cycle, using whatever process information and knowledge is available.

Solidity:
A What-If analysis can be a powerful procedure if the staff is experienced, otherwise the results are likely to be incomplete.

Expertise Required:
The analysts must have a good understanding of the process intention, along with the ability to mentally combine possible deviations from the design intent that could result in an accident.

Difficulty of Application:
Analyst must have detailed knowledge of the process under consideration and must be able to conceive abnormal process conditions.

7.2.6 **Hazard and operability analysis**

Description:
The Hazard and Operability study was developed to identify and evaluate safety hazards in a process plant, and to identify operability problems which, although not hazardous, could comprise the plant's ability to achieve design productivity. In HAZOP analysis, an interdisciplinary team uses a creative, systematic approach to identify hazard and operability problems resulting from deviations from the design intent of the process that could lead to undesirable consequences. An experienced team leader systematically guides the team through the plant design using a fixed set of "guide words". These guide words are applied at specific points in the plant design and are combined with specific process parameters to identify potential deviations from the plant's intended operation. After agreement about the deviation, possible causes of the deviations, the consequences of the deviations, and the possible mitigation actions are investigated. If necessary the team might formulate a follow-up action for management consideration. The results of a HAZOP Analysis are the team findings which are normally recorded in a column-format table.

Application:
The purpose of a HAZOP Analysis is to carefully review a process or operation in a systematic fashion to determine whether process deviations can lead to undesirable consequences. The Hazop team lists potential causes and consequences of the deviations as well as existing safeguards protecting against the deviation. If the team comes to the conclusion that inadequate protection exists against a credible deviation, it usually recommends that action be taken to reduce the risk. The HAZOP methodology is very time consuming and for that reason rather expensive.

Solidity:
Solidity is determined by:
- the extent to which interactions are known
- the degree of detail of the analysis
- the degree to which the consequences are identified and explored.

Expertise Required:
The HAZOP analysis technique is easy to understand. Success depends on the knowledge the team members have of the process and their ability to evaluate and discuss possible deviations without any constraints or presuppositions.

Difficulty of Application:
Difficulty is determined by process complexity and the knowledge of the behaviour of the process in abnormal situations.

7.2.7 Failure modes and effects analysis

Description:
The technique evaluates the ways in which equipment can fait and the effect these failures can have on an installation. These failure descriptions provide analysts with a basis for determining where changes can be made to improve a system design. Single equipment failures are defined by the analysts and the effects of such failures, both locally and on the system as a whole, are investigated. Each individual failure is considered as an independent occurrence with no relation to other failures in the system, except for the subsequent effects that it might produce.

Application.
The technique is universally applicable to systems, subsystems, components, procedures, interfaces etc. The technique is most suited to installations where the danger comes from mechanical equipment, electrical failures etc, but not from the dynamics of the procesces. This is in contrast to the HAZOP technique which is applied to whole processes, whereby the danger comes from hazardous materials in chemical process systems.

Solidity:
Solidity is dictated by:

- the degree to which failure modes are identified and explored,
- the degree to which effect avenues are identified and to which they are explored, for each failure mode
- the degree to which the effects of multiple co-existent failure modes are analyzed.

Expertise required.
The principles of an FMEA analysis are easy to understand and to learn. It is more important that the analysts are familiar with the components of the system to be analyzed. They must know the failure modes of the components and the effects of those failure modes on the system as a whole.

Difficulty of Application:
The technique is not difficult to apply. It is, however, enormously time-consuming. Although only failure modes (e.g. component faults) are explored, both type of failure modes which wilt and those which will not result in great harm must be investigated to develop the analysis fully.

7.2.8 Criticality analysis

Description:
Rank the damage potential of system elements according to a scale which represents the harm each element might cause in case of failure.

Application:
The purpose of a criticality analysis is to rank the criticality of components which could result in injury, damage or system degradation through single-point failures, in order to identify those components which might need special attention and control measures during design or operation. The technique is universally applicable to all systems, processes, procedures and their elements.

Solidity:
As the criticality generally depends on the probability of occurrence of the undesired event and on the severity of the undesired event, it might be possible that the same criticality will be calculated for a low probability event with very severe consequences and a high probability event with less severe consequences. Although the same criticality is calculated, the two cases do not have to be equal because of additional considerations or judgements. In this respect calibration of the calculation scheme to determine the criticality is very important.

Expertise Required:
Once the methodology is understood, the technique is easy to apply. Success depends on the effort spent to calibrate the methodology and to instruct the analysts how to use the calculation scheme.

Difficulty of Application:
Application is readily accomplished for cases in which failure modes have been identified. However, the use of Criticality Analysis is practical, system cases must presuppose that the specific failures to which it is to be applied have been identified. If they have not, application of an adjunct technique then becomes a necessity, and the difficulty of applying the adjunct technique predominates.

Comments:
This technique is quite often combined, in practice, with the Failure Modes and Effects Analysis.

7.3 OVERVIEW OF QUANTITATIVE EVALUATION TECHNIQUES

For systems for which the probability of occurrence of an undesired consequence has to be calculated it is necessary to perform a quantitative analysis in addition to the qualitative analyses described in section 7.2. The quantitative approach can be used to:

- identify and analyse accident sequences, initiated by a plant disturbance, which may contribute to the overall plant risk

- identify those components or plant systems whose unavailability significantly contributes to the overall plant risk and to isolate the underlying causes of their significance

- identify weak links in the operating, test, maintenance and emergency procedures which contribute significantly to the overall plant risk

Quantitative analyses can be performed for new designs, modifications to existing systems, or evaluations of existing installations.

7.3.1 **Fault tree analysis**

Description:
Fault tree analysis focuses on one particular accident or main system failure (top event), and provides a method for determining causes of that event. The fault tree is a graphical model that displays the various combinations of equipment failures (minimal cut-sets), dependent failures and human failures that can result in the top event of interest. Boolean logic rules are used to determine the minimal cut-sets. Quantification of the minimal cut-sets is possible by various means, e.g. direct estimation of the basic event probability, kinetic theory, Markov processes or Monte Carlo simulation.

Application:
The strength of fault tree analysis as a qualitative tool is its ability to identify the combinations of equipment failures, dependent failures and human failures that can lead to an undesired consequence. This allows the analyst to focus preventive measures on basic causes to reduce the probability of occurrence. The technique is universally applicable to systems of all kinds.

Solidity:
Important limitations of the technique are:
- the presumption that the relevant undesirable events have been identified
- the presumption that contributing factors have been adequately identified and explored in sufficient depth.

Apart from these limitations, the technique as usually practised is regarded as being among the most thorough of those prevalent for general system application.

Expertise Required:
The basis of the fault tree technique is easy to understand and to apply in simple cases. Some years of experience are required to be able to perform a fault tree analysis of a complicated system. Prior knowledge of Boolean algebra and/or the use of logic gates is helpful.

Difficulty of Application:
Application, though time-consuming, is not difficult once the technique has been mastered. Computer aids are available. Unlike Event-Tree Analysis and Failure Modes & Effects Analysis, the technique explores only those faults and conditions leading to the undesired (top) event.

7.3.2 Markov processes

Description:
A state diagram of a system is constructed. The state diagram represents the status of the system with regard to its failure states. A specific failure state is represented by one node of the state diagram. The arrows between nodes, which represent the failure events or repair events, are weighted with the corresponding failure rates or repair rates.

Application:
The Markov technique is most beneficial for analyzing systems where the sequence of failure is important or where repair is done on a continuous basis. The Markov technique can also be applied to the analysis of standby redundancies and state-dependent failure rates. For reliability calculations the Markov process is taken as a discrete-state, continuous-time model. Each discrete state is normally given as a unique, well-defined condition of the relevant system components. In the simplest cases, the formulae which describe the probabilities of the system are readily available in the literature or can be calculated manually. In more complex cases, some methods of simplification can be applied. Results can be calculated also by computer simulation (numerical integration) of the graph.

Sofidity:
The Markov technique is one of the most advanced quantitative analysis techniques in risk and reliability analysis. Especially in the case of analyzing different repair strategies the Markov technique is a powerful tool to support the reliability analyst. The disadvantage of this approach is that great care must be taken to eliminate possible dependent events. Dependency can be properly handled by the Markov technique if the system is modelled correctly.

Expertise Required:
The technique is among the more difficult ones. Successful application to complex systems cannot be undertaken without formal study over a period of time, combined with practical experience.

Difficulty of Application:
Care must be taken to ensure that the state diagram is a realistic representation of the system. If this hurdle is passed, the solution can easily be obtained by the application of a suitable computer code.

7.3.3 Event tree analysis

Description:
Event Tree analysis evaluates the potential of an accident occurring as result of a general equipment failure or process upset, known as initiating event. Event tree analysis is an inductive process in which the analyst begins with an initiating event and develops the possible sequences of events that lead to different consequences, ranging from normal plant response to accidents. Event trees provide a systematic way of recording the accident sequences and defining the relationship between the initiating events and subsequent events that result in accidents. Given an initiating event, all possible consequences are in principle considered in an event tree analysis.

Application:
The technique is universally applicable to systems of all kinds, with the limitation that unwanted events (as well as wanted events) must be anticipated to produce meaningful analytical results.

Solidity:
The technique can be exhaustively thorough, Solidity has only two theoretical limits, i.e. the presumptions that:
- all system events have been anticipated
- all consequences of those events have been explored.

Expertise Required:
The technique is among the more difficult. Successful application to complex systems cannot be undertaken without formal study over a period of time, combined with practical experience.

Difficulty of Application:
The technique is not particularly difficult to apply. It is, however, time-consuming. It must be recognized that the exploration of all wanted events and their consequences increases the effort substantially.

Comments:
Of the techniques presented in this chapter. Event-Tree Analysis is beyond question the most exhaustive, if properly applied. Axiomatically, the use of these techniques also consumes large quantities of resources.Their use, therefore, is well reserved for systems in which risks are thought to be high and well concealed (i.e. not amenable through analysis by simpler methods).

7.3.4 **Monte carlo simulation**

Description:
Some practical problems in risk and reliability analysis cannot be solved by analytical methods and require numerical simulation.Thus, rather than attempt to analytically analyse the effects on inputs described with probability distributions, e.g. failure rates of components, Monte Carlo techniques represent the distributions as sequences of discrete random values. The technique consists of building, usually with a computer code, a probabilistic model of the system under investigation. A trial run of the model is repeated many times, and each time one discrete value of the performance of the simulated system is recorded. After a sufficiently large number of computer runs, these discrete values can be combined into one probability distribution which describes the system parameter of interest.

Application:
The technique requires the building of a probabilistic model of the system, translation of this model into a computer model, estimation of the probability distributions of the input parameters and composition and interpretation of the output probability distribution. It will be clear that this is a time-consuming process and requires various skills. For this reason it is advisable to use the Monte Carlo technique only in those cases where analytical methods fail.

Sofidity:
Very realistic results can be generated with the Monte Carlo technique. Almost all aspects can be incorporated into the probabilistic model.

Expertise Required:
Analysts need to be familiar with system reliability techniques and need to have a detailed understanding of probability distributions. In most cases some computer programming is necessary to model the probabilistic system model. Interpretation of the results requires analysts to be familiar with median, mean and upper and lower bounds of probability distributions.

Difficulty of Application:
The analyst must be familiar with probability distribution and random number generators. Also some computer programming is required in most cases.
In the case of very reliable systems a large number of computer runs are required to generate a probability distribution. New techniques have been developed to save computer time.

7.4 DESCRIPTION OF THE HAZARD AND OPERABILITY ANALYSIS TECHNIQUE

7.4.1 Introduction

HAZOP analysis was originally developed for the chemical industry. It is a systematic technique for identifying hazards and operability problems throughout an entire facility. It is particularly useful to identify unwanted hazards designed into facilities due to lack of information, or introduced into existing facilities due to changes in process conditions or operating procedures.

The objectives of a HAZOP study are to detect any predictable deviation (undesirable event) in a process or a system. This purpose is achieved by a systematic study of the operations in each process phase. Also, the interactions of the various components or systems are considered.

The system is divided into functional blocks. Subsequently every part (action, system) of the process is questioned in order to discover how deviations from the design intention can occur. The deviations are considered in order to decide whether they can cause any hazard or inconvenience. The questioning is done by a team of experts on all phases in the process.

The questioning is focused on every phase of the process. Each system and person that plays a part in a phase is subjected to questions formulated around guide words. The use of Guide words ensures that every conceivable way in which a process could deviate from the process intention is found. Each deviation is considered to decide how it could be caused and what the consequences would be.

Some causes of a deviation may be unrealistic and some consequences may be trivial. However, other causes and consequences may be conceivable and hazardous. For these hazards (preventive) actions are defined.

7.4.2 Definitions

Because the analysis has to be systematic and structured, it is necessary to use certain terms in a precise and disciplined way. The most important terms are:

Function or Intention The function or intention defines how the part (component, subsystem or human) is expected to operate. This can take several forms and can be either descriptive or diagrammatic.

Deviation A departure from the design and operating intention.

Failure cause This is a reason why a deviation might occur.

Consequence This is the loss caused by a deviation, should it occur (local and end effects).

Measure Action taken or to be taken in order to prevent (reduce the probability of) the cause or reduce the consequences of a deviation. It is mentioned explicitly whether or not the action has already been taken.

Consequences These are the results of the deviations, should they occur.

Guide Words These are simple words which are used to qualify the intention in order to guide and stimulate the creative thinking process and thereby discover deviations. A list of guide words is given in Table 7.1.

Hazard and operability Study The application of a formal systematic critical examination of the process and engineering intentions of new or existing facilities to assess the hazard potential of operation or malfunction of individual items of equipment and their consequential effects on the facility as a whole.

Design and operating intentions The way the process and equipment is intended to work under both normal and anticipated abnormal conditions.

Hazard An inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment.

Examination sessions Periods of time (usually about three hours) during which the study team systematically analyses the design to detect hazards.

Team discussion The part of an examination session which follows the application of a guide word to a design intention and during which the team members derive meaningful deviations, decide whether these are hazardous and what action should be taken as a consequence.

Evaluation and action session
Under certain circumstances, it is inappropriate to take firm decisions during examination sessions and instead, a series of questions are posed for subsequent evaluation. Under these circumstances further meetings are held in which each question is reviewed, the results of any investigation are reported and decisions taken.

Technical team members
Those members of a study team whose main contribution consists of explaining the design, using their knowledge, experience and imagination during team discussions and taking decisions on changes.

Team leader
A person trained in the methodology of Hazard and Operability Studies who will advise and assist the study in general and in particular, use the guide words, stimulate the team discussion and ensure comprehensive coverage during examination sessions. In the absence of a study secretary (see below) he will also note actions or questions which arise during these sessions.

7.4.3 The basic concept

The examination procedure consists of:

- the composition of a concise description of the process
- systematical questioning every part of it to discover how deviations from the design intention can occur
- decisions as to whether these deviations can give rise to hazards.

The questioning is focused in turn on every part of the design. Each part is subjected to a number of questions formulated around a number of guide words, which are derived from method study techniques. In effect, the guide words are used to ensure that the questions, which are posed to test the integrity of each part of the design, will explore every conceivable way in which that design could deviate from the design intention. This usually produces a number of theoretical deviations and each deviation is then considered in order to decide how it could be caused and what would be the consequences.

Having examined one part of the design and recorded any potential hazards associated with it, the study progresses to focus on the next part of the design. The examination is repeated until the whole plant has been studied.

The purpose of the examination is to identify all possible deviations from the way the design is expected to work and all the hazards associated with these deviations. In addition, some of the hazards can be resolved. If the solution is obvious and is not likely to cause adverse effects on other parts of the design, a decision can be taken and the design modified on the spot. This is not always possible; for example, it may be necessary to obtain further information. Thus the output from examinations normally consists of a mixture of decisions and questions to be answered at subsequent meetings.

7.4.4 Timing of a HAZOP study

The principles of HAZOP studies can be applied to process plants and batch operated plants in operation or in various stages of design. A HAZOP study carried out during the initial phase of design can frequently provide a guide to safer detailed design.

A HAZOP study may highlight specific deviations for which mitigating measures need to be developed. For those cases where mitigating measures are not obvious or where they are potentially very costly, the results of the HAZOP study identify the initiating events necessary for further risk analysis.

The most appropriate time for carrying out a Hazop in the design stage is when the P&I diagrams have been produced, but before actual construction.

Hazard and Operability Studies can also be carried out when construction has been largely completed, but before start up. Studies at this stage are particularly useful as a check on operating instructions. However, the correction of design faults at this stage can be expensive and will lead to delays.

Studies can also be carried out on existing plant. The main benefit in that case is that operating methods may be improved.

Although the approach as described may appear to generate many hypothetical deviations in a rather mechanistic way, success or failure depends on four aspects:
- the accuracy of drawings and other data used as the basis for the study
- the technical skills and insights of the team
- the ability of the team to use the approach as an aid to their imagination in visualising deviations, causes and consequences
- the ability of the team to maintain a sense of proportion, particularly when assessing the seriousness of the hazards which are identified

7.4.5 The procedure for a study

A HAZOP study involves the following steps:

1. Definition of the objectives and scope of the study, e.g. hazards having only off-site impact or only on-site impact, areas of the plant to be considered, etc.

2. Assembly of a HAZOP study team. This team must consist of design and operation personnel with technical expertise to evaluate the effects of deviations from intended operation.

3. Collection of the required documentation, drawings and process description. This includes process flowsheets, piping and instrument drawings, equipment, piping and instrument specifications, process control logic diagrams, layout drawings, operating and maintenance Procedures, emergency response procedures, etc.

4. Analysis of each major item of equipment, and all supporting equipment, piping and instrumentation, using documents collected in step 3. The process design intent is first defined; subsequently, for each line and item of equipment. Each guide word (see table 7.1) has to be combined with relevant process parameters, such as temperature, pressure, flow, level and chemical composition, and applied at each point, e.g. study node, process section, or operating step, in the process that is being examined. The principle to identify a deviation can be presented is as follows:

Guide Word		**Parameter**		**Deviation**
NO	+	Flow	=	No Flow
MORE	+	Pressure	=	High Pressure

Once a deviation is identified, the specific cause of this deviation are sought. Depending on the seriousness of the consequences in a qualitative sense, various provisions or actions may be identified.

5. Documentation of the consequences of any deviation from normal and highlights of those deviations which are considered hazardous and credible. In addition, an identification is made of means to detect and/or prevent the deviation. This documentation is usually done on HAZOP worksheets. A sample of such a worksheet for the guide word ”Not, No” applied to ”flow” is shown in Table 7.2.

Table 7.1 Minimum list of Guide Words used in a HAZOP

GUIDE WORDS	MEANINGS	COMMENTS
NO or NOT	The complete negation of these intentions	No part of the intentions is achieved but nothing else happens
MORE LESS	Quantitative increase or decrease	These refer to quantities and properties such as flow rates and temperatures as well as activities like ”HEAT” and ”REACT”
AS WELL AS	A qualitative increase	All the design and operating intentions are achieved together with some additional activity
PART OF	A qualitative decrease	Only some of the intentions are achieved
REVERSE	The logical opposite of the intention	This is mostly applicable to activities, for example reverse flow or chemical reaction. It can also be applied to substances, eg. ’POISON’ instead of ’ANTIDOTE’
OTHER THAN	Complete substitution	No part of the original intention is achieved. Something quite different happens.

7.4.6 Team composition

Hazard and Operability Studies are normally carried out by multi-disciplinary teams. There are two types of team members, namely those who wilt make a technical contribution and those who play a supporting and structuring role.

The examination requires the team to have detailed knowledge of the way the plant is intended to work. This means a combination of those concerned with the design of the plant and those concerned with its operation. The technique of using guide words generates a very large number of questions. For most purposes it is essential that the team has enough members with sufficient knowledge and experience to answer the majority of those questions without recourse to further expertise.
This group should contain sufficient expertise to provide the necessary technical input. Additionally, if some members of the team are drawn from those who also have some responsibility for the design of a plant, they will be particularly motivated to produce a successful design and a safe operating procedure. Normally these members of the team will have the necessary authority to make changes. The combination of disciplines will vary with the type of project.

The study leader has a role to play throughout the study. He should help whoever has commissioned the study to define its scope. He may help with the selection and training of the team. He will advise on the assembly of the necessary data and may help convert this into a suitable form. However, his most obvious role emerges during the examination sessions, in which he guides the systematic questioning and must be thoroughly selected for this job. It is not desirable that he should be responsible for making a major technical contribution. If possible, he should not have been closely associated with the subject of the study as there is a danger of developing blind spots and failing to use the technique objectively. But he should have sufficient technical knowledge to be able to understand and control the team discussions.

It is imperative that the team as a whole should have a positive and constructive attitude towards a study, as its success ultimately depends upon the imaginative thinking of the members. This positive attitude must be developed from the definition stage onwards. Suitable training is a great help and should create a climate in which the team members are anxious to start the study. At times during the examination sessions, some team members feel the approach is tedious but a well-led team ultimately derives considerable satisfaction from its design work receiving such a thorough analysis.

Examination sessions are highly structured with the study leader controlling the discussion by following his predetermined plan. If the approach is based on the flow sheet he selects the first object and asks the team to explain its broad function. This is not always straightforward but until every member of the team knows exactly what something is supposed to do, deviations cannot be generated. A similar approach is used if the study sequence is based on operating instructions.

The study leader then applies the first guide word and the team discussion starts. It is sometimes necessary, particularly with an inexperienced team, for the study leader to stimulate the team discussion by asking further questions such as 'Can the flow stop?' or 'Does it matter if it stops?' As far as possible, only probing questions should be asked by the study leader. The team should not only provide the technical answers but be encouraged to be creative and think of all the deviations and hazards themselves.

7.4.7 **Reporting**

An important activity of the study team is to record the results of the study.The results of a HAZOP are normally recorded in a HAZOP work sheet. The work sheet is divided into a number of columns. Each column describes a certain aspect of the identified deviations, e.g. the guide word used or a description of the deviation or a description of the consequences of the deviation. Although the format of the HAZOP worksheet can vary from study to study, the following information should be available:

Heading:
- Part of the system analysed
- The design intention of that part of the system.

Columns:
- Guide word applied
- Deviation from the intended function
- Possible causes of this deviation
- Consequences for the system as a whole or for the environment depending on the objectives of the HAZOP study
- Actions required.

An example of a HAZOP work sheet for a pump is provided in table 7.2.

Table 7.2: Sample HAZOP Work sheet for Guide word "Not, No"

Component : Pump
Intention : To generate flow

Guide word	Deviation	Possible Causes	Consequences	Action Required
Not, No	No flow	1. No feed material available	Reduced output Polymer will be formed	a) Ensure good communication with operator b) Provide low level alarm on setting tank
		2. Pump fails (variety of reasons)	As for 1.	As for b)
		3. Line blockage or valve closed in error or control valve fails shut	As for 1. Pump will overheat	Install recirculation line on each pump

7.5 DESCRIPTION OF THE CRITICALITY ANALYSIS

Criticality is a combination of severity of an effect and the probability or expected frequency of occurrence. The objective of a criticality analysis is to quantify the relative importance of each failure effect, so that priorities for action to reduce the probability of occurrence or to mitigate the severity of the effect can be taken. Criticality is evaluated by a subjective measure of the severity of the effect and an estimation of the probability of occurrence. Depending on the subject of the study, the formula to calculate the criticality can be defined. The following formula is only presented as an example which wijl be applicable in a large number of cases:

$$Cr = P \beta S \tag{7.1}$$

Cr : Criticality number
P : Probability of occurrence of the identified deviation over a period of one year
β : Conditional probability that the Beverest consequence will occur, given occurrence of the deviation
S : Severity of the severest consequence.

The severity is an assessment of the seriousness of the consequente. Severity applies only to the consequente and not to its probability of occurrence.

It should be emphasized that the criticality number can only be used to rank the identified deviations in a HAZOP or FMEA study from most serious to less serious. It cannot be used as a risk measure because the criticality number is the product of three rough estimates. The primary usefulness is to identify which items should be given more attention to eliminate or mitigate the identified hazard.

Before a criticality analysis can be performed guidelines have to be developed on how to determine the probability of occurrence (P), the conditional probability that the severest consequence will occur (beta) and the rating scheme for the severity (S). There are no generally accepted criteria for criticality applicable to a system, because this concept is fundamentally linked to that of the severity of consequences and their probability of occurrence. The severity concept itself can be defined in various ways depending on whether the objective is related to safety of life, consequential damage or loss, or service availability.

7.5.1 Example of a framework

An example of a framework to assess the criticality will be presented in this section. This framework can be modified, to the extent necessary, depending on the specific preferences of the reader. In this framework four categories are defined for each parameter in formula (7.1), see table 7.3. As can be seen in this table, the rating of each parameter varies from 1 to 4.

Application of formula (7.1) shows that multiplication of the probability, severity and Beta, results in 16 possible outcomes, ranging from 1 to 64. This categorization allows ranking of the deviations.

To make the criticality analysis consistent, the terms listed in table 7.3 have to be defined more precisely. This has been done in tables 7.4, 7.5 and 7.6. If necessary, the definitions in these tables have to be extended.

Table 7.3: Categories for Probability, Beta and Severity.

Probability		Beta		Severity	
very rare	1	very low	1	low	1
rare	2	low	2	significant	2
likely	3	significant	3	high	3
frequent	4	high	4	very high	4

Table 7.4: Interpretation of the categories for probability

Probability	Meaning
very rare	less than once in 100 years
rare	between once in 10 years and once in 100 years
likely	between once a year and once in 10 years
frequent	more frequent than once a year

Table 7.5: Interpretation of the categories for Beta.

Beta	Meaning
very low	less than once every 1000 occurrences of the cause
low	less than once every 100 occurrences of the cause
significant	less than once every 10 occurrences of the cause
high	more than once every 10 occurrences of the cause

Table 7.6: Interpretation of the categories for severity.

Severity	Meaning
low	No or minor economical loss Small, non-permanent environmental damage
significant	considerable economical loss considerable non-permanent environmental damage slight non-permanent injury
high	major economical loss considerable release of hazardous material serious non-permanent injury
very high	major release of hazardous material permanent injury or worse

After execution of the criticality analysis, a list of undesired consequences has been generated ranging from a high criticality to a low criticality. Now a decision has to be made on the undesired consequences for which additional measures will be defined. This can be done on a case-by-case basis if only one HAZOP study is carried out. If for a number of plants a generally, applicable framework has to be developed, a criterion has to be formulated to determine for which items additional actions have to be performed. Table 7.7 is an attempt to categorize criticality as a function of the criticality number only. For instance, all undesired consequences with a criticality number lower than or equal to X are acceptable. The values for X and Y have to be determined by a decision-maker. It might be necessary to formulate some additional criteria, for instance: every deviation for which the severity is classified as "very high severity" shall be evaluated to investigate the possibilities of reducing the undesired consequences.

Table 7.7: Interpretation of the categories for criticality.

Criticality	Judgement	Meaning
Cr < X	Acceptable	No action required: e.g. all has been done to prevent a deviation with a low probability and very high severity
X < Cr <Y	Consider modifications	Should be mitigated within a reasonable time period unless costs demonstrably outweigh benefits
Cr >Y	Not acceptable	Should be mitigated as soon as possible

7.6 DESCRIPTION OF THE FAILURE MODES & EFFECTS ANALYSIS TECHNIQUE

7.6.1 Introduction

Failure modes and effects analysis (FMEA) is a standard evaluation procedure for systematically identifying potential failures in an equipment/system design and analysing the resulting effects on the performance of the equipment/system. The FMEA is useful in identifying the critical problem areas of a design and design improvements or operational modifications necessary in order to achieve the required equipment/system performance throughout the plant's life cycle, and it is also a very useful preliminary step in system model development (e.g. fault trees).

FMEA is an inductive method of reliability analysis and is based on the question 'What happens if ...?'. It considers one (single) failure within the equipment/system at a time. As such, it provides a better appreciation of the functioning of the equipment/system and its potential failure Modes. FMEA has the disadvantage of being a relatively labourious method. However, it is a systematic method for analysing and clarifying the effects of component failures on the system functions.

7.6.2 Definition of terms

Failure mode The manner in which the function of a component can fail (e.g. for an isolation valve one failure mode is 'fail to close on command').

Effect The consequences of failure on a subsystem, a system or the plant as a whole.

Component The specific subdivision of the plant or system under consideration in the analysis. Unless defined by contractual or regulatory requirements, the definition of components is at the discretion of the analyst for any given analysis.

Function The specified working requirements of a component within a system (e.g. the functions of an isolating valve may be to open and close a particular flow path upon command and to keep the pressure boundary of that path intact).

7.6.3 Purpose of FMEA

The primary Purpose in performing an FMEA in the context of risk and reliability analysis is to provide qualitative information on the various ways and modes in which a system can fail, and hence it constitutes an input for system modelling. Additional uses of FMEA include:

- comparison of Various design alternatives and Configurations
- confirmation of the ability of the system to meet its design reliability criteria
- identification of problem areas such as:
    - single failure modes that can cause system failure
    - cross links between systems
    - areas requiring additional redundancy
- input data for establishing corrective action. Priorities and trade off studies

- providing an objective evaluation of the design requirements related to redundancy, failure detection and annunciation systems, fail-safe characteristics, and automatic and manual override features.

In addition, FMEA provides historical documentation for future reference to aid in the analysis of field failures, the evaluation of design changes and the comparison between in-service performance and predicted performance.

7.6.4 Prerequisites for performing an FMEA

Before performing an FMEA, the analyst must define what constitutes the system under analysis and the extent or level of resolution of the analysis. The definition will include:
- the functional performance requirements of the system
- the environmental and operational conditions under which the system is to perform
- a clear statement of the Physical bounds and Interfaces
- a definition of system failure
- the level of resolution (subsystems or components) at which the analysis starts
- the level of resolution (major system or overall plant) at which the analysis stops.

In addition to the foregoing, the objectives of the analysis and the assumptions must be clearly stated. The objectives of the analysis will dictate the level of resolution. Furthermore, it is recommended that a review of relevant operational experience should be conducted, to help identify all applicable failure Modes of the Components of the system.

7.6.5 Format of the analysis

A tabular Work sheet format is recommended. Figure 7.2 depicts a typical format. The detailed design of the work sheet is at the discretion of the analyst or may be dictated by company procedures. However, it should allow the analyst to present the following information:

1: The name of the system element under analysis

2: The function performed by the system element

3: The identification number of the system element

4: The failure mode identified

5: The probable causes for this failure mode

6: A complete description of the effect of the failure mode at the subsystem level and, where relevant, at the system and overall plant level. If different effects occur under different environmental conditions, then a separate description must be written for each set of conditions, with a clear statement of the different effects

7: A complete description of the failure symptoms, alarms and indications that would alert an operator to the failure

8: A qualitative statement of failure significance and alternative provisions by which the effects of the failure may be alleviated.

Further additions are permissible as required by company policies, analytical details etc., but no omissions from this list should be considered. Items (6), (7), (8) and (9) are iterative in nature; i.e. is as an analysis progresses, more failure modes with similar indications may be found and lists may need to be revised.

7.6.6 **Method of analysis**

The analysis proceeds in a series of logical steps, as follows:

(1) Gather all relevant design information for the system under consideration: design Manuals, flow sheets, Instrument loop diagrams, elementary electrical diagrams, etc;

(2) Determine the level at which the component breakdown is to be made for the initial iteration and list the system components;

(3) Using the work sheet format, identify for each component the possible functional failure modes, with their probable causes.

(4) Trace the effects of each failure to determine its effect at the relevant subsystem level; in the process, identify other failures with the same or very similar effects and indications;

(5) Check the diagnostic actions necessary to isolate the effects to a particular failure mode;

(6) Determine the corrective actions necessary;

(7) Repeat steps (4), (5) and (6) for each set of operating conditions that modify the effects of a failure mode;

(8) When the process is complete at the subsystem level, trace the effects of the failure through the system level and the overall plant level, as dictated by the requirements of the analysis.

Table 7.8: Example of an FMEA work sheet.

Equipment name	Function	Ident. No.	Failure mode	Failure cause	Failure effect		Failure detection	Alternative provisions
					Local effect	End effect		

7.6 REFERENCES

[7.1] Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples, Center for Chemical Process Safety of the American Institute of Chemical Engineers 345 East 47th Street, New York, NY 10017 (ISBN 0-8169-0491-X).

[7.2] Guidelines for Chemical Process Quantitative Risk Analysis,
Center for Chemical Process Safety of the American Institute of Chemical Engineers, 345 East 47th Street, New York, NY 10017 (ISBN 0-8169-0402-2).

[7.3] A compendium of Hazard identification and evaluation techniques for System Safety Application, P.L. Clemens, Hazard Prevention, March/April 1982.

[7.4] Vesely, W.E., et al; Fault-Tree Handbook, NUREG-0492; U.S. Government Printing Office; January 1981.

[7.5] Guidelines for Safe Automation of Chemical Processes, Center for Chemical Process Safety of the American Institute of Chemical Engineeers, 345 East 47th Street, New York, NY 10017. (ISBN 0-8169-0554-1).

[7.6] Premises for Risk Management, Dutch National Environmental Policy Plan, Ministry of Housing, Physical Planning and Environment, Department for Information and International Relations, P.O. Box 20951, 2500 EZ The Hague, The Netherlands.

[7.7] Procedures for Conducting Probabilistic Safety Assessment of Nuclear Power Plants (Level I), Safety Series No. 50-P-4, International Atomic Energy Agency, Vienna, 1992,
(ISBN 92-0-102392-8).

[7.8] Analysis techniques for system reliability - Procedures for failure mode and effects analysis (FMEA), Publication 812, International Electrotechnical Commission IEC Standard, First Edition 1985.

[7.9] Potential Failure Mode and Effects Analysis (FMEA), An Instruction Manual, Ford Motor Company, September 1988.

[7.10] Reliability of systems, equipment and components, Part 5. Guide to failure modes, effects and criticality analysis (FMEA and FMECA), British Standard, BS 5760: Part 5: 1991.

[7.11] A Guide to Hazard and Operability Studies, Chemical Industry Safety & Health Council of the Chemical Industries Association Limited, London.

[7.12] Hazard and Operability Study Why? When? How?, Report of the Directorate-General of Labour, First Edition 1982, Publication of the Directorate-General of Labour of the Ministry of Social Affairs and Employment, P.O. Box 69, 2270 MA Voorburg, the Netherlands, (ISBN 0166-8935 AIR 3E/8207).

[7.13] AMIR/SPAR, System Engineering Monte-Carlo based advanced software, Malchi Science Sci. Ltd. 1992, P.O. Box 1194, Beer-Sheva, Israel.

[7.14] A Manual of HAZARD & Operability Studies, The Creative Identification of Deviations and Disturbances, Chemetics International Company Ltd, 1992.

APPENDIX 7- A: SOME OTHER ANALYSIS TECHNIQUES

The appendix contains a number of evaluation techniques which are of minor importance or are not used very often in risk and Hazard evaluation. The evaluation techniques described in this appendix are based on reference 3.

7-A.1 **Change analysis**

Description:
Consider an existing, known system as a baseline. Examine the nature of all contemplated or real changes, and analyze the probable effect of each change (singly) and all changes (collectively) upon system risks.

Application:
Although originally conceived for management system applications, Change Analysis has come to be applied to systems of all kinds. It can only be applied, of course, if system design change or actual alteration has occurred or is contemplated. It is well applied as a means of optimizing tile selection of a preferred change from among several candidate changes, or in aiding the design of a needed change. The technique can be applied meaningfully only to a system for which the baseline risk has been established (e.g, as a result of prior analysis).

Solidity:
Solidity is constrained by the detail treated in performing the analysis. Solidity required to analyse a given change is governed by the extent of the change itself. Effectiveness cannot exceed that of prior analysis(es) used in establishing baseline risk.

Expertise Required:
Understanding of the physical principles governing behaviour of the system being changed is essential, so that the effects of the change can be determined with a degree of confidence adequate to the purposes of the analysis. Assuming that the complexity of the changes does not appreciably exceed that of the system prior to alteration, mastery of the baseline analytical technique becomes sufficient.

Difficulty of Application:
Difficulty is determined largely by the extent to which the system has undergone (or will undergo) change in combination with system complexity.

Comments:
The chief advantage of the technique lies in its shortcut approach: i.e. only the effects of change(s) need be analysed, rather than the system as a whole. In this advantage also lies the technique's chief shortcoming: i.e. the presumption that the baseline analyses has been carried out adequately.

7-A.2 Contingency analysis

Description:
Identify the credible mishaps that might occur in a given system, and examine the existence and adequacy of emergency measures and protective equipment with which control can be established and/or harm can be avoided in the event of each credible mishap.

Application:
Contingency Analyses may be applied universally to all systems, subsystems, components, procedures, interfaces, etc. To satisfy the definition, they must be performed for the specialized purpose of examining the existence and the suitability of system contingency features. In general system applications, the Contingency Analysis may be considered as an effective means to aid in disciplining the approach to evaluating the adequacy of back-up elements and/or control paths intended to mitigate failures. It is also of particular value in assessing the adequacy of disaster response plans and equipment.

Solidity:
Solidity is determined largely by (1) the degree to which mishap modes have been identified and (2) the adjunct technique(s) employed to examine the existence and adequacy of mitigation features within, or available to, the system (See Comments below).

Difficulty of Application:
Selection of technique(s) to be used determines the difficulty of application (See Comments below.)

Comments:
The Contingency Analysis is not a discrete technique. Instead it is the application of any technique, or any group of them, performed for the specific purposes of determining the need for, the existence of, and the adequacy of, system contingency features.

7-A.3 Critical incident technique

Description:
Interview operationally experienced personnel (and/or use questionnaires) to collect information on past mistakes, hazards and near misses. Identify dominant high-risk cases.

Application:
The technique may be applied, without restriction, to any system having human operators or observers, for which a reasonable background of historical operational experience has been accumulated.

Solidity:
The technique is limited in thoroughness by (1) the degree to which near misses which are likely ultimately to result in, or to contribute to, a critical Incident wilt have been experienced and (2) the fidelity with which those instances will have been noted, remembered, and reported by competent operators or observers.

Expertise Required:
Expertise on gathering objective data from subjective interviews in a sine qua non. Moreover a solid basis in the principles of system safety and risk assessment is necessary.

Difficulty of Application:
Given proper preparation (see Expertise Required, above), application of the technique is straightforward and uncomplicated.

Comments:
This technique has come to enjoy a more favourable reputation than the other ″what-if″ methods: cf Scenario and Maximum Credible Event/Worst-Case Condition.

7-A.4 **Energy analysis**

Description:
Identify all sources of energy within a system, and examine the adequacy of barriers to the unwanted flow of that energy to ″targets″ which might suffer harm.

Application:
The technique can be applied to all systems which contain, make use of, or which store energy in any form or forms (e.g. potential or kinetic mechanical energy, electrical energy, ionizing radiation, chemical energy, thermal energy etc.). In conjunction with other techniques Energy Analysis is applicable also to systems which control the containment, use, storage or flow of energy. The technique cannot be applied - without use of special interpretations - to the discovery and analysis of hazards which are not energy-related, and exclusive reliance upon its use can leave important hazards undiscovered (e.g. the presence of asphyxiants in confined spaces).
* ″Critical Incidents″ are known to the Department of Energy as ″Reported Significant Observations″, or ″Unusual Operating Reports″.

Solidity:
The likelihood of oversight in cataloguing the sources of energy within the system is small. (Checklists are available in the literature as aids to the process.) The likelihood of oversight in identifying system vulnerability to external sources of energy can be great, however. The effects of rates of energy application and of frequency or total number of cycles of application are sometimes overlooked (e.g. shock loading and fatigue), as are combined energy effects (e.g. a vessel whose walls are simultaneously exposed to a pressure differential and a thermal gradient).

Expertise Required:
Inconsequential preparation is required for cataloguing energy sources within a system. However, use of the method also requires recourse to the expertise needed to judge the adequacy of barriers to the unwanted flow of that energy.

Difficulty of Application:
The cataloguing of energy sources is carried out with relative ease. Analysis of the adequacy of static barriers can be accomplished, in many cases, by simple comparison of the physical characteristics of the system with requirements levied by codes, regulations and standards. (Ordinarily, this will have been done and documented during system design.) Application becomes more difficult in systems in which process controls play a part in restraining the unwanted flow of energy. The adequacy of such controls - whether automatic or manned - is not amenable to straightforward analysis by this technique, and other methods must be used to support it.

Comments:
The method is of special value as a quickly applied first look technique. It is inclined to focus exclusively upon energy sources within the system being analysed. External sources (e.g. from adjacent systems or forces of nature) are often overlooked. When applied in the making of ”safe-to-enter” decisions, special adaptations are necessary to ensure that it will support life, even though the environment is free from unrestrained sources of energy likely to cause harm.

7-A.5 **Flow analysis**

Description:
Consider the confined or unconfined flow of fluids or energy - intentional or unintentional - from one component/subsystem/system to another. Find and evaluate opportunities
for that flow to occur without intended constraint, in ways which might result in harm.

Application:
The technique is applicable to all systems, which transport, or which control the flow of, fluids or energy. Adjunct techniques are often essential to success in the use of Flow Analysis (e.g. in analysing fluid flow control systems to determine unwanted modes of flow and their probabilities).

Solidity:
The likelihood of oversight in cataloguing intentional flows of fluids or energy within a system is small. The likelihood of oversight in identifying opportunities for unintentional flows is great, however. Even greater is the likelihood of oversight in identifying opportunities for combined unintentional flows.

Expertise Required:
Inconsequential preparation is necessary to enable a straightforward cataloguing of the intentional flows of fluids or energy within a system. However, some expertise must be acquired on judging the adequacy of barriers to unintentional flows. If adjunct techniques are to be used (see Application above) they must also be mastered.

Difficulty of Application:
The cataloguing of energy fluid flows within a system is carried out with relative ease. Analysis of the adequacy of static barriers can be accomplished, in many cases, by simple comparisons of the physical characteristics of the system with requirements levied by codes, regulations and standards. Application becomes more difficult in systems in which process controls play a part in restraining the undesired flow of fluid or energy. The adequacy of such controls - whether automatic or manned - is not amenable to straightforward analysis by this technique, and adjunct methods must be used to support it.

Comments:
This technique is inclined to focus exclusively upon fluid and energy flows within the system being analysed. External sources of such flows (e.g., from adjacent systems or forces of nature) are often overlooked.

7-A.6 **Interface analysis**

Description:
Seek physical and functional incompatibilities between adjacent/interconnected/interacting elements of a system which, if allowed to persist under all conditions of operation, would cause hazards which could result in mishaps.

Application:
Interface analysis is universally applicable to systems of all kinds above the least-component level. Interfaces treated may be inter-machine, intra-machine, man-machine etc., without restriction.

Solidity:
Solidity is determined by the extent to which interfaces are known (or can be anticipated) and the degree to which candidate incompatibilities can be identified. Solidity increases as additional, adjunct techniques are brought to bear to support Interface Analyses. (See Comments below.)

Expertise Required:
Understanding of the physical principles underlying the behaviour of the interconnected system elements is essential. Expertise of adjunct techniques, if they are to be used to support the analysis (see Comments below) is an obvious requirement.

Difficulty of Application:
The difficulty is determined by the system complexity and by the nature of such adjunct techniques as may be used. (See Comments below.)

Comments:
Use of adjunct techniques to support Interface Analysis is markedly beneficial - e.g. application of Failure Modes and Effects Analysis at each of many intra-system interfaces can serve to identify incompatibilities not discovered through Interface Analysis alone. A principal weakness of Interface Analysis lies in the presumption that incompatibilities between system elements can be identified, prior to failures, for all conditions of operations.

7-A.7 **Job safety analysis**

Description:
Analyse job (or work process/system/operation) element by element, identifying hazards associated with each element. (Classically, this is done by a worker-supervisor-safety engineer team.)

Application:
The technique is applicable to - and limited to - human operator functions. Those functions must be proceduralized in ways which provide assurance that they will not vary significantly, or anticipated variations in them must be accounted for in the analysis.

Solidity:
Solidity is limited by: (1) the degree to which job elements are explored, and (2) the degree to which variations in/from procedural job elements are considered.

Expertise Required:
Elementary analyses may be performed by the uninitiated analysts. More complex jobs, having many possible variations in job elements, require the use of formalized techniques and training experience commensurate with the complexity.

Difficulty of Application:
The technique is quite readily applied to jobs having little opportunity for variation in the structure of individual job elements, but becomes difficult to apply when such variation exists and must be taken into account. (If such variation exists and is not taken into account, thoroughness suffers.)

7-A.8 **Management oversight & risk tree analysis**

Description:
Apply a pre-designed, systematized logic tree to the identification of total system risks, those inherent in physical equipment and processes as well as those which arise from operational/management inadequacies.

Application:
The pre-designed tree - intended as a comparison tool - generally describes all phases of a safety program and is applicable to systems and processes of all kinds. The technique is of particular value in accident/incident investigation as a means of discovering system or program weaknesses or errors which provide an environment conducive to mishaps.

Solidity:
Design of the ”model” tree, against which comparison judgments are made, is exhaustive. As a result, thoroughness is limited only by the degree to which the analysis explores the existing or contemplated system, in mirroring it against the model tree.

Expertise Required:
One day of formal instruction leads to capability in applying the technique. One-week courses, including various exercises in practical application, are viewed as preferable.

Difficulty of Application:
Although tedious and time-consuming, the technique is not difficult to apply once mastery has been achieved (see above). Graphic aids and explanatory texts are available.

7-A.9 Maximum credible accident/worst-case condition

Description:
Visualize the severest mishap that might reasonably be expected to occur in a system. Consider all potential contributors to the mishap in their worst-ease states and examine the probability that the mishap itself might evolve as a result of its occurrence.

Application:
The technique has universal application to systems and subsystems of all kinds, whether manned or unmanned.

Solidity:
The technique lacks thoroughness chiefly to the degree that it relies upon the exercise of intuitive skills in imagining the nature of sometimes complex events that have not yet been experienced. A converse argument, favouring thoroughness, can also be put forward: use of the technique induces consideration of system failures for which no historical basis is at hand.

Expertise Required:
The technique is often practised with success by the newly initiated novice. (See cautionary note under Comments below.)

Difficulty of Application:
Application is accomplished with little difficulty. presuming that the practitioner is adequately versed in the system and its environment of use.

Comments:
Spontaneity of thought is essential to the practice of the technique. That same spontaneity can give rise to the visualization of ″worst cases″ which lack reasonable credibility. The practitioner must guard against uselessly expending resources in pursuing analyses of conceivable but unlikely cases.

7-A.10 Naked man

Description:
Consider the primordial system, with all existing safety features and mishap countermeasures removed. Examine theoretical baseline hazards in that state, and determine which ones are eliminated or appropriately suppressed - or which new ones might be added - as existing countermeasures are restored or new ones are applied.

Application:
The technique is universally applicable to system and subsystems, whether Manned or unmanned. It is recognized as especially useful in developing and/or analysing confined-space entry safeguards and procedures.

Solidity:
The technique tends to be exhaustively thorough, unless practised superficially.

Expertise Required:
Use of the system is readily mastered, requiring less than one day of instruction and practice with demonstration cases.

Difficulty of Application:
Assuming the availablilty of a sufficiently detailed logging and documentation system, the technique is readily applied. It is, however, enormously time-consuming.

Comments:
Of the techniques presented in this compendium. Network Logic Analysis, Event-Tree Analysis and use of the Naked Man principle are beyond question the most exhaustive, properly applied. Axiomatically, their use also consumes large quantities of resources. Their use, therefore, is well reserved for systems in which risks are thought to be high and well-concealed (i.e., not amenable to analysis by simpler methods).

7-A.11 **Network logic analysis**

Description:
Describe system operation as a network of logic elements, and develop Boolean expressions for proper system functions. Analyse the network and/or expressions to identify elements of system vulnerability to mishap.

Application:
The technique can be universally applied to all systems, whether manned or unmanned, having components and/or operations which can be adequately represented in bi-modal elemental form.

Solidity:
The technique can be exhaustively thorough. Solidity rests on the degree to which system components and or operations wilt have been represented in network form. (Note: peripheral service failures - e.g. utilities - and interface effects are often overlooked in the application of this technique.)

Expertise Required.
The technique is among the more difficult. A working knowledge of Boolean algebra is essential. Successful application to complex systems cannot be undertaken without formal study over a period of several days to several weeks, combined with some practical experience.

Difficulty of Application:
Once mastery is achieved. the technique is not particularly difficult to apply. It is, however, enormously time-consuming. Because the technique expiores all wanted as well as unwanted system performance eventualities, it requires substantially more effort than Fault-Tree Analysis or Failure Modes and Effects Analysis.

7-A.12 **Procedure analysis (task analysis)**

Procedure Analyses are often designated by the activity to be analysed, e.g.: "Test Safety (Hazard) Analysis", "Operation Safety (Hazard) Analysis", Waintenance Safety (Hazard) Analysis". - cf. Job Safety Analysis.

Description:
Review, step by step, the actions that must be performed (generally in relation to mission tasks, equipment that must be operated, and the environment in which personnel must exist) seeking possibilities of mishaps as a result of those actions, e.g.: (1) the possibilities of harm to operators by the systems, and (2) the possibilities of harm to the system by the operators.

Application:
Application is limited to systems involving procedures followed by human operators. Those procedures must be sufficiently documented, or otherwise formalized so as to lend themselves to the necessary analysis with reasonable confidence that the step-by-step protocol will not be violated. Alternatively, additional analyses must be performed to evaluate the effects of protocol violation.

Solidity:
Solidity is limited by: (1) the degree to which procedural steps/sub-elements are explored, and (2) the degree to which error options are considered (e.g. embedded) step performed out of sequence, step omitted, false step inserted.)

Expertise Required:
Elementary analyses may be performed by the uninitiated analyst. More complex procedures having many error avenues require the use of formalized techniques and training/experience commensurate with the complexity.

Difficulty of Application:
The method is quite readily applied to operations having few error options, but becomes difficult to apply when multiple error options must be considered, or when single error options at multiple points in time or at separated operating stations must be dealt with in combination.

7-A.13 **Prototype**

Description:
Construct and operate, under widely varying conditions, system subsystem mock-ups/models, and examine operation for evidence of failure under appropriately varied operating conditions.

Application:
The technique is applicable to systems, subsystems and components, whether electrical/electronic, or mechanical. Man-machine systems are also analysed in prototype versions - e.g. using operational simulators. The cases, however, particularly where operator stress is a factor, require analysis.

Solidity:
Solidity depends entirely upon the degree of system replication achieved in the construction and operation of the prototype. Expertise Required: a finely detailed understanding of the system and its intricacies is essential in order for it to be modelled effectively in the prototype version.

Difficulty of Application:
Prototype analysis tends to be costly in resources and time, which is especially true at levels above the subsystem. For that reason, its application is customarily reserved for suspected high-severity cases which are not amenable to adequate treatment by other techniques.

Comments:
Manned control functions for mass transportation systems are often dealt with in prototype, using simulators which also serve as training devices.

7-A.14 **Scenario**

Description:
A mass, spontaneous ideas (often generated by members of a group) describing conceivable accidents and/or their contributors. Discard those ideas which are deemed wholly unreasonable, and pursue the remainder by refining descriptions of their causes and consequences and judgments of their likelihood.

Application:
Manned and unmanned systems and subsystems are amenable to treatment by this technique. The technique is of special value in cases where system features are novel and as a result, there is no historical database for guidance or comparison.

Solidity:
The technique is limited in thoroughness only by the ability of the practitioner to conceive mishaps and combinations of events, conditions and actions that might induce them.

Expertise Required:
An unfettered mind and an active imagination lead to mastery. (It can be argued that overfamiliarity with the system under analysis restricts the freedom of thought processes necessary to successful application.)

Difficulty of Application:
Application is accomplished with ease in all but obscure cases.

Comments:
Because the method relies upon spontaneity, it lacks the appearance of methodical discipline. Detractors view this as a weakness.

7-A.15 Single-point failure analysis

Often called ”what-if-ing” or ”brainstorming”; cf. Maximum Credible Accident/Worst-Case Condition.

Description:
Examine system, element by element. Identify those discrete elements and/or interfaces whose malfunctions/failures, taken individually, would induce system failure.

Application:
The technique is equally applicable to hardware systems, software systems, and formalized human operator procedures.

Solidity:
Solidity by simple ”inspection” methods is usually viewed as marginal or inadequate for systems having more than an arbitrarily small number of elements. When performed as an adjunct to another method (see Comments below), thoroughness is dictated by the depth to which that other, primary analysis is pursued.

Expertise Required:
Expertise by simple ’inspection’, methods is readily found in the competent system analyst/designer. Expertise as an adjunct to other methods. (see Comments below) requires reasonable expertise on those other methods.

Difficulty of Application:
Difficulty by ”inspection” methods increases rapidly as system complexity (i.e., number of elements) increases. Difficulty when practised as an adjunct to other methods (see Comments below) generally requires little effort beyond that expended to practise those other methods.

Comments:
Single-Point Failure Analysis is a natural consequence of the application of Fault-Tree Analysis, as used to determine cut sets. Single-Points Failure Analysis is also often accomplished through Event-Tree Analysis or Failure Modes and Effects Analysis.

7-A.16 Sneak-circuit analysis

Description:
Examine circuits (or command/control functions), searching out unintended paths (or control sequences) which - without component failure - can result in undesired operations, or in desired operations at inappropriate times, or which can inhibit desired operations.

Application:
Sneak-Circuit Analysis is applicable to control and energy-delivery circuits of all kinds, whether electronic/electrical, pneumatic or hydraulic. Adaptations of the technique also find application in the analysis of software logic algorithms.

Solidity:
The technique, when applied to a given system, tends to be exhaustively thorough in identifying all sneak paths of previously prescribed kinds. More problematical is the discovery of paths which lie outside previously prescribed classes.

Expertise Required:
A basic understanding of control circuit theory is essential. Beyond that, little is required for analysis of uncomplicated systems. Several weeks of study and practice of application are necessary to develop mastery adequate for the analysis of more complex logic circuitry, however.

Difficulty of Application:
Though quite time-consuming, application is uncomplicated once mastery has been achieved, (Computer-assisted methods are available.)

Comments:
The technique enjoys a favourable reputation among control system designers who recognize it as a disciplined approach to the discovery of inadvertent design flaws.

7-A.17 **Systematic inspection**

Description:
Using checklists, codes, regulations, industry consensus standards and guidelines, prior mishap experience and common sense, methodically examine a design/system/ process, identifying discrepancies representing hazards.

Application:
The technique is the single, most widely practised of the many hazard discovery methods. Its application is virtually without limit.

Solidity:
Solidity of application is determined by the degree to which codified checklists etc. (see Method above) are available, the degree to which the ones available are applicable to the system at hand, and furthermore the degree to which they are actually applied in practice.

Expertise Required:
Competent system designers will have developed the mastery required, simply as a result of having carried out the designs. Because a rote process is involved, mastery by others is easily achieved, except for complex designs.

Difficulty of Application:
Application most often involves a readily applied use of checklist data in a rote process.

Comments:
Many system safety practitioners regard Systematic Inspection as an essential preliminary step to the application of any other technique.

FAULT-TREE ANALYSIS

CONTENTS **Page**

8.1 INTRODUCTION

In the course of risk and reliability analysis it is often desirable to know the probability of occurrence of a certain event, the conditions on which this occurrence depends and how this probability of occurrence can be influenced. Such an event can be the probability of failure on demand of a safety device. One of the analyses techniques to generate this information is the fault tree technique.

The fault tree technique can be described as an analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur.

Fault tree analysis is a deductive failure analysis which focuses on one particular undesired event and which provides a method for determining causes of this event. The undesired event constitutes the top event in a fault tree diagram constructed for the system, and generally consists of a complete, or catastrophic, failure of the system under consideration. Careful formulation of the top event is important to the success of the analysis.

The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with component hardware failures, human errors, or any other pertinent event which can contribute to the top event.

It is important to understand that a fault tree is not a model of all possible system failures or all possible causes of system failure. A fault tree is tailored to its top event, which corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event.

It is also important to point out that a fault tree is not in itself a quantitative model. It is a qualitative model that can be evaluated quantitatively. The qualitative results generated with a fault tree are the minimal cut-sets and the qualitative insights which can be derived by evaluating the cut-sets.

A minimal cut-set is defined as a smallest combination of basic events that, if they all occur, will cause the top event to occur (for instance failure of a safety device). One speaks of a first-order minimal cut-set in case a single basic event causes the top event to occur. A second-order minimal cut-set is a combination of two single failures that, if they both occur, will cause the top event to occur.

A fault tree is a complex of entities known as ″gates″ which serve to permit or inhibit the passage of a fault logic up the troth gates show the relationships of events needed for the occurrence of a ″higher″ event. The ″higher″ event is the ″output″ of the gate ; the ″lower″ events are the ″inputs″ to the gate. The gate symbol denotes the type of relation of the input events required for the output event to occur. The lowest level events are called primary or basic events. Basic or primary events are singular events for which a probability of occurrence can be determined or estimated. These basic events can be associated with component hardware failure, human errors, maintenance or test unavailabilities or any other pertinent event that can contribute to the top event.

The minimal cut-sets generated with a fault tree can be quantified to calculate the various reliability measures of a system, like probability of failure on demand, unavailability or reliability. To quantify the minimal cut-sets, different quantification techniques can be used. For instance, by application of a number of standard formulas (see chapter 9) or by the application of Markov processes (see chapter 11) or by Monte Carlo simulation (see chapter 15).

In this chapter the construction of fault trees and the theoretical background of the generation of minimal cut-sets will be explained. Also, the quantification of a simple example will be carried out by using the formulas provided in chapter 9.

8.2 NOMENCLATURE

λ_i	=	Failure rate for component i	-/hour
β	=	Beta factor	-
τ_i	=	Test duration for component i	hour
θ_i	=	Repair duration for component i	hour
θ_i	=	Mean repair duration for component i	hour
PFD	=	Probability of failure on demand	-
Q_i	=	Probability of failure on demand for component i	-
T	=	Test interval	hour

Subscript

ccf	=	common cause failure
shv	=	shut-off valves
sol	=	solenoid valves
ps	=	pressure switches

8.3 FAULT TREE ANALYSIS

To perform a fault tree analysis, a number of tasks have to be performed. In chronological order these tasks are:

Qualitative analysis:

- System familiarization.
  Before a fault tree can be constructed, one has to know in detail how the system operates and which failure modes have to be taken into account.

- Definition of the top event and construction of the fault tree.

- Determination of the minimal cut-sets.

Quantitative analysis:

- Collecting all relevant failure, repair, test and maintenance data.

- Quantification of the minimal cut-sets.

- Evaluation of the results.

In the next few paragraphs these steps are explained in further detail by means of a simple example.

When the system to be analyzed becomes complex, or in case more than one fault tree must be constructed by different fault tree analysts, it will be useful to apply a number of guide-lines.These guidelines are explained in section 8.4.

8.3.1 System familiarization

The first step in a fault tree analysis is to get familiar with the system to be analyzed. Before one can construct a fault tree one has to know exactly how the system works and how the various components within the system can fait. If there is only a limited amount of information available on the system under consideration it might be necessary to perform a failure modes and effects analysis to identify all possible failures within the system.

To explain the different steps in a fault tree analysis, the safety system as depicted in figure 8.1 will be analyzed.

The safety system consists of two sensors which for proper functioning require power supply E2. In case the maximum tolerable temperature is exceeded, the sensors send a signal to the one-out-of-two logic solver.This logic solver has a different power supply (E1) and in its turn sends a signal to two identical final elements (A1 and A2), which have the same power supply (E2). Only one of the final elements is needed to stop the process and prevent a hazard occurring.

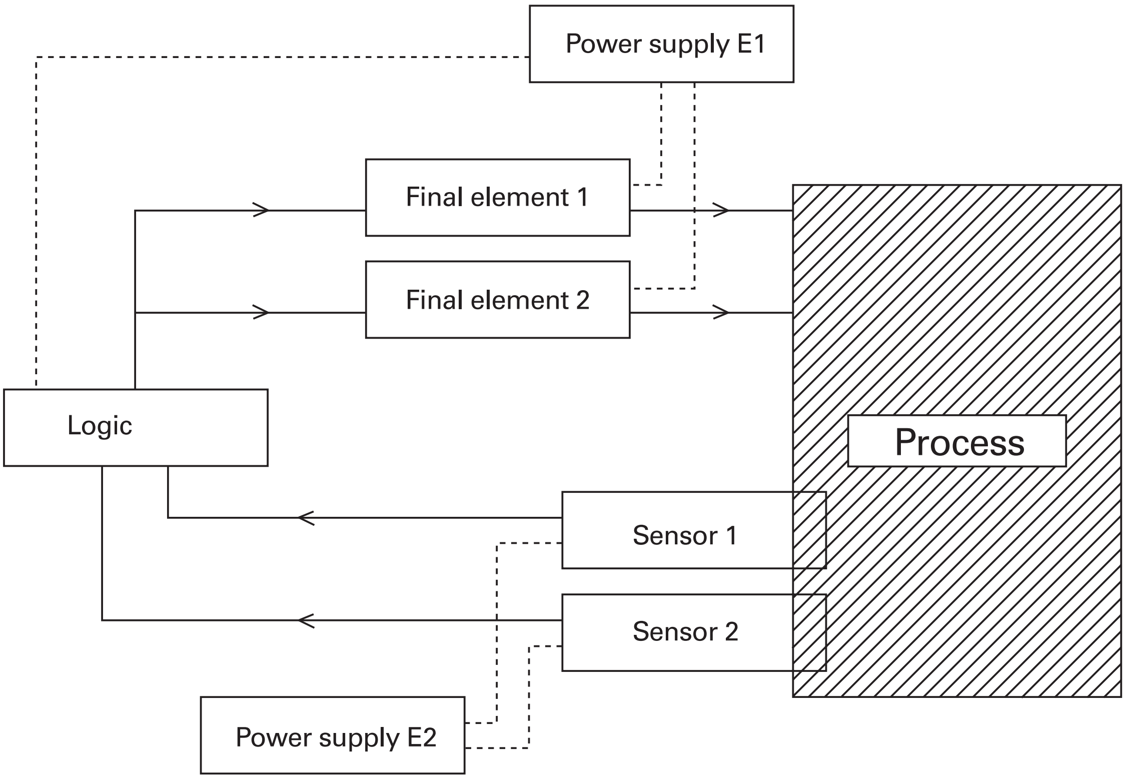


Figure 8.1: Safety system to be analyzed.

The failure modes to be considered in this example for the various components are:

Sensors	:	Failure to generate a signal given a high temperature
Logic	:	Failure to generate a trip signal to the final elements given one or two trip signals from the sensors
Final elements	:	No action given a demand
Power supply	:	No output

The construction of a fault tree starts with the definition of the top event. The top event is the top of the fault tree and must be defined unequivocally and can refer to only one specific operational state of the system. For the safety system under consideration the top event is defined as follows:

> "Safety device fails on demand"

This means that if the maximum tolerable temperature is exceeded the safety system fails to stop the process.

If one is interested in the probability of a spurious action of the safety system, the top event should be defined as:

" Spurious failure of the safety system".

This means that the process is stopped by the safety system without the occurrence of a demand. Both top events require the construction of different fault trees.

After definition of the top event the fault tree has to be constructed. The aim of the fault tree construction is to identify all causes that contribute to the occurrence of the top event. To construct a fault tree reviewing of system drawings and system descriptions is necessary. Also it is often necessary to consult the supervisor, operator or maintenance crew of the system to identify all contributors to the top event.

It should be realized that the fault tree relates to only one specific failure mode of the system. In this case the safety device fails to function given a high temperature. Before fault tree construction can continue the symbols that are used to depict a fault tree have to be explained.

8.3.2 Fault tree symbology

A fault tree is generated by making a drawing using the symbols depicted in table 8.1. The construction of a fault tree always starts with the top event as the output of a logic gate. Next, all input events of the "top event gate" have to be identified. These input events are represented by either new intermediate events or by one or more basic events. In fault trees basic events are end points. New intermediate events are again divided into "lower" intermediate events and/or basic events. The basic events and intermediate events are mostly joined by "and" or "or" gates. This depends on the way in which they influence the output event.

The application of the "AND" and "OR" gate will be explained with the electrical diagram which is depicted in figure 8.2

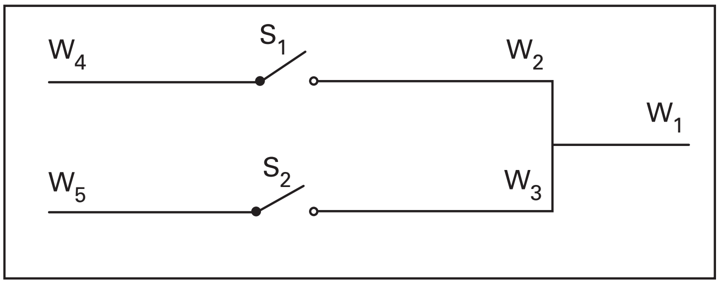
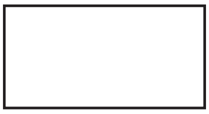
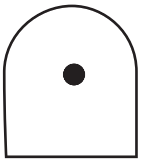
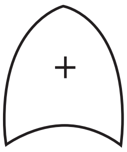
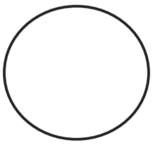
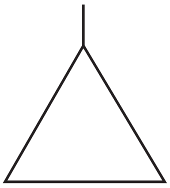
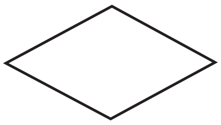


Figure 8.2: Electrical diagram.

In the electrical diagram of figure 8.2, there is no power at W1 if there is no power present at W2 and no power present at W3. In a fault tree this fault condition have to be represented by an "AND" gate. Both input fault events "No power at W2" and "No power at W3" have to occur to cause the top event "No power at W1" to occur. This is depicted in figure 8.3.

Table 8.1: Fault Tree Symbols

Symbol	Description
	**Intermediate event** A fault event that occurs because of one or more antecedent causes acting through logic gates have occurred.
	**And gate** The AND-gate is used to show that the output event occurs only if all the input events occur.
	**Or gate** The OR-gate is used to show that the output event occurs only if one or more of the input events occur.
	**Basic Event** A basic event that requires no further development because the appropriate limit of resoiution has been reached.
	**Transfer** A triangle indicates that the tree is developed further at the occurrence of the corresponding transfer symbol.
	**Undeveloped Event** A diamond is used to define an event which is not further developed either because it is of insufficient consequence or because information is unavailable.

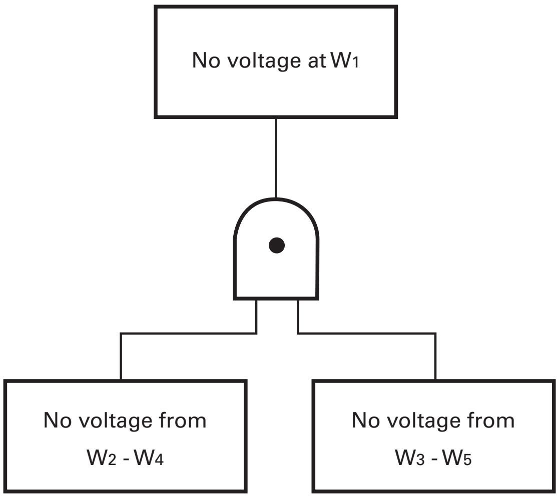


Figure 8.3: Example of an "AND" gate.

In the electrical diagram of figure 8.2, there is no power at W2 if switch S1 fails to close or there is no power at W4. In a fault tree this fault condition have to be represented by an "OR" gate. One out of two input fault events "Switch fails to close" or "No power at W4" have to occur to cause the top event "No power at W2" to occur. This is depicted in figure 8.4.

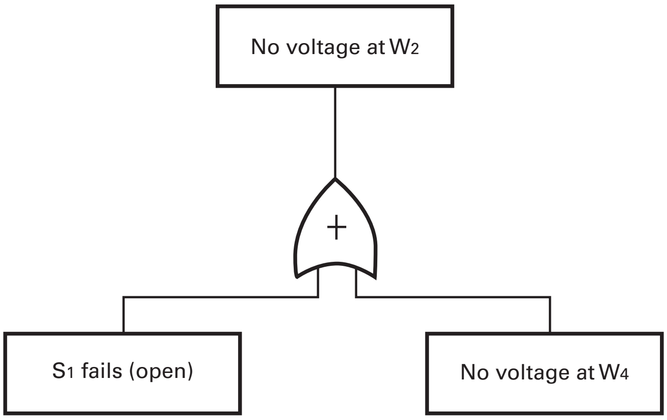


Figure 8.4: Example of an "OR" gate.

8.3.3 Rules for fault tree construction

Fault tree construction is a process that can be performed in many ways depending on the experience and preferences of the fault tree analyst. To avoid errors in fault tree construction and to give guidance to the fault tree analysts a number of basic rules have been developed. Following these rules a fault tree can be obtained which is correct and easy to understand.

The rules can be summarized as follows:

Rule 1: Correct definition of top event.
The top event of the fault tree must be defined unequivocally and can refer to only one mode of operation and one specific fault condition of the system.

Rule 2: Construction from top to bottom.
A fault tree is always constructed from top to bottom. One starts with the top event and then works downwards, dissecting the system until one reaches the basic events.

Rule 3: Consistently going upstream.
Given the top event, one must move very consistently upstream through all flow paths. Whether they are electric, hydraulic or pneumatic currents or flows is irrelevant. It will become apparent that there is always some flow to be found. Each component fault is then taken into account. By applying this rule the probability of making errors is decreased as much as possible and components are treated in the right order.

Rule 4: Complete the gate.
All inputs into a particular gate should be completely defined before further analysis of any one of them is undertaken.

Rule 5: No gate to gate connections.
Gate inputs should be properly defined fault events, and gates should not be directly connected to other gates.

Rule 6: No miracles.
One might find, in the course of a system analysis, that the propagation of a particular fault sequence could be blocked by miraculous and totally unexpected failure of some other component. For instance it is not allowed to suppose a ”failure to open” of a check valve in the discharge line of a pump after a spurious actuation of the pump. The correct assumption to make is that the component functions normally, thus allowing the passage of the fault sequence in question. However, if the normal functioning of a component acts to block the propagation of a fault sequence, then the normai functioning must be defeated by faults if the fault sequence is to continue up the tree

Rule 7: Required level of detail.
In general it can be stated that the level of detail is sufficient in case the failure data of a certain event is known or if the probability of occurrence of a certain event is negligible compared to the probability of occurrence of the other events.

8.3.4 Fault tree construction example

A fault tree is an organized graphical representation of the conditions or other factors causing or contributing to the occurrence of a defined undesirable event, referred to as the ”top event”. For the safety system under consideration the top event is defined as follows (see section 8.3.1):

“Safety device fails on demand”

The corresponding fault tree is depicted in figure 8.5.

Given rule 2, one needs to start at the point where the safety system interacts with the process. In this example the final elements 1 and 2 stop the process. So this must be the starting point of the fault tree construction. Given that one out of two final elements are required to stop the process, the process is not stopped if both final elements fail to operate. This implies that one has to start with an ”and-gate” because both final elements 1 and 2 have to fail in order to cause the top event to occur.

Two intermediate events can be defined as input event for gate G 1. Final element 1 fails to operate on demand and final element 2 fails to operate on demand. Next, one has to identify all causes why final element 1 is not able to operate. During this investigation one has to move upstream all process flows which are required for proper functioning of final element 1. Three causes can be identified why final element 1 is not able to operate on demand:

- internal failure of final element 1
- no power supply from power supply E1
- no actuation signal from the one-out-of-two logic.

The occurrence of each of these three causes is sufficient to cause the intermediate event described by gate G2 to occur. This implies that gate G2 must be an ”or-gate”. The same holds for gate G3.

Three input events have to be drawn for gate G2 and gate G3. Two input events are basic events which describe successively internal failure of the final element and failure of power supply 1. The third input event is the output event of gate G4 which represents the failure of the actuation signal.

It must be emphasized that for gate G2 and gate G3 a distinction has to be made between internal failure of final element 1 and internal failure of final element 2. No distinction has to be made between power supply 1 for both gates G2 and G3 because it concerns failure of the same power supply.

A transfer symbol to gate G4 is added to gate G2. This symbol means that the branch represented by the output of G4 is also applicable as input event for G3.

Next, all failure causes of the actuation signal have to be identified. Careful review of the safety system shows that three causes can be identified:

- internal failure of the one-out-of-two logic
- failure of power supply 1
- no signal to the logic from both sensors.

internal failure of the logic is represented by basic event BE4 and failure of the power supply E1 by basic event BE3. Given the design of the logic (one out of two) an ”and-gate” has to be used to describe failure of both actuation signals from the sensors.

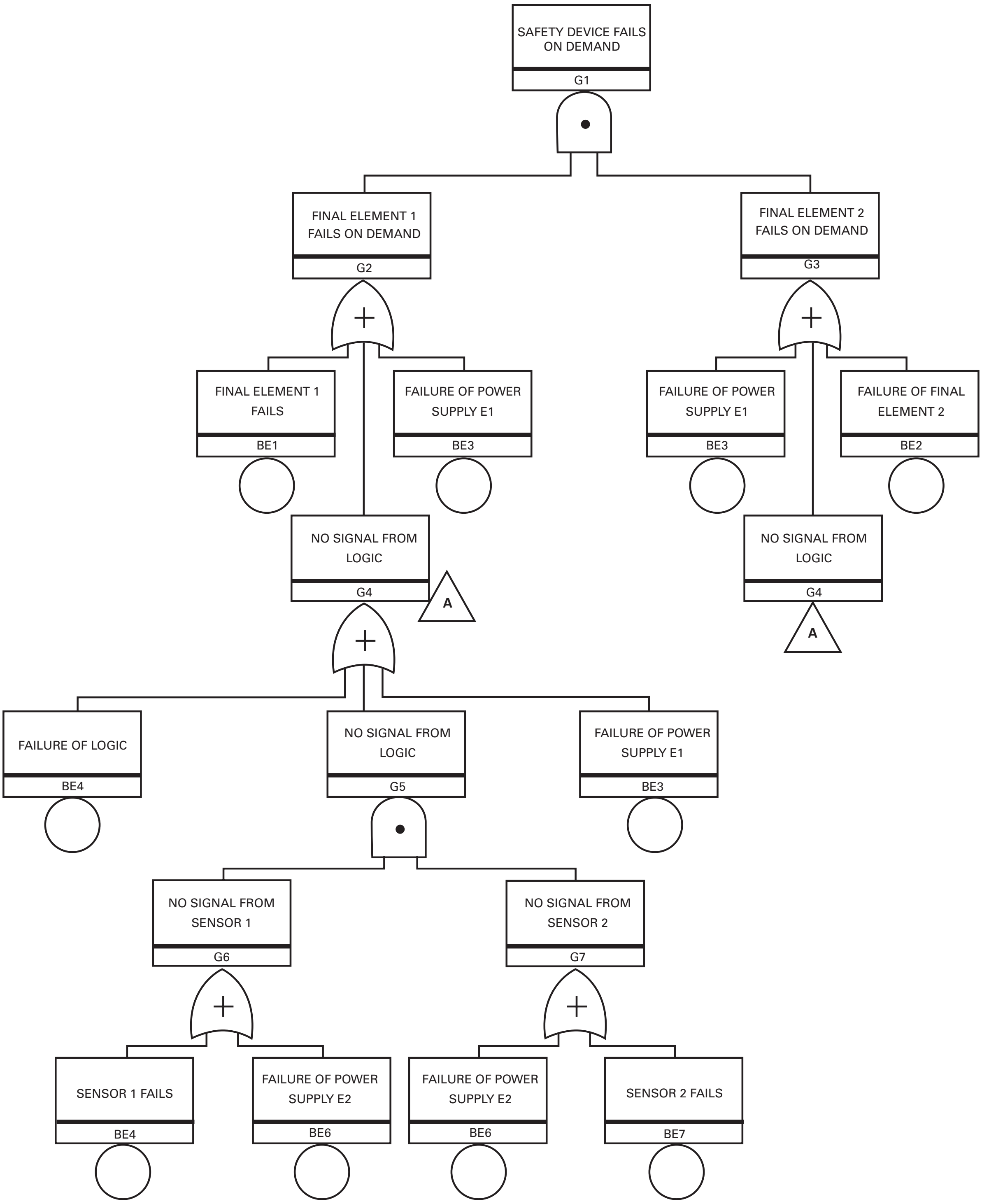

SAFETY DEVICE FAILS ON DEMAND
G1
FINAL ELEMENT 1 FAILS ON DEMAND
G2
FINAL ELEMENT 2 FAILS ON DEMAND
G3
FINAL ELEMENT 1 FAILS
BE1
FAILURE OF POWER SUPPLY E1
BE3
FAILURE OF POWER SUPPLY E1
BE3
FAILURE OF FINAL ELEMENT 2
BE2
NO SIGNAL FROM LOGIC
G4
A
NO SIGNAL FROM LOGIC
G4
A
FAILURE OF LOGIC
BE4
NO SIGNAL FROM LOGIC
G5
FAILURE OF POWER SUPPLY E1
BE3
NO SIGNAL FROM SENSOR 1
G6
NO SIGNAL FROM SENSOR 2
G7
SENSOR 1 FAILS
BE4
FAILURE OF POWER SUPPLY E2
BE6
FAILURE OF POWER SUPPLY E2
BE6
SENSOR 2 FAILS
BE7

Figure 8.5: Fault tree safety system.

Going upstream the signal flow, two different causes can be identified why sensor 1 does not generate an actuation signal. The first cause is an internal failure of the sensor and the second cause is a failure of the power supply E2. So, to describe the failure of sensor 1 to generate an actuation signal, an ″or-gate″ G6 has to be added. Inputs for gate G6 are the basic events BE5 (sensor 1 fails) and BE6 (failure of power supply E2). The same rationale holds for failure of the actuation signal from sensor 2.

The complete fault tree is depicted in figure 8.5. The next step is to determine all minimal cut-sets.

8.3.5 Determination of the minimal cut-sets

A minimal cut-set is defined as the smaltest combination of basic events which, if they all occur, will cause the top event to occur.

By the definition, a minimal cut-set is thus a combination (intersection) of basic events sufficient for the top event. The combination is a ″smallest″ combination in that all failures are needed for the top event to occur; if one of the failures in the cut-set does not occur, then the top event will not occur by this combination.

For any fault tree a finite number of minimal cut-sets can be determined, which are unique for the top event defined for that fault tree.

The one basic event minimal cut-sets (first order), if there are any, represent those single failures which cause the top event to occur. The two basic event minimal cut-sets (second order) represent those double failures which, if both occur, cause the top event to occur. For a n-basic event minimal cut set, all n basic events within that cut-set have to occur in order to cause the top event to occur.

The cut-sets are normally determined by application of a computer code. The fault tree logic in terms of gates and basic events is used as a input for such computer programs. In this chapter the theoretical background for cut-set determination wilt be explained. One important element of cut-set determination is the application of Boolean algebra.

Boolean algebra:

In order to explain the cut-set determination of a fault tree, it is necessary to be familiar with the most important rules concerning Boolean algebra. In fact, a fault tree can always be translated into an entirely equivalent set of Boolean equations. Thus an understanding of the rules of Boolean algebra contributes materially towards the construction and simplification of fault trees. In the following part of this section the most important Boolean rules and their application to fault tree analysis are discussed. For an extensive discussion of Boolean algebra and application to fault tree analysis, the reader is referred to reference [8.1].

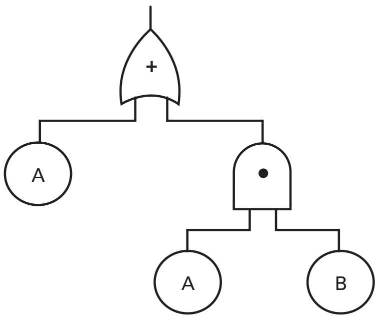
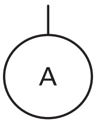
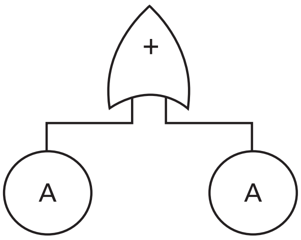
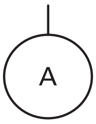
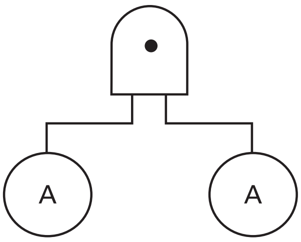
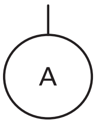
Assume that events A and B represent two basic events. For example, event A stands for ″pump A fails to start″ and event B for ″circuit breaker B fails to open″. Using Boolean algebra, the plus sign (+) is to be read as ″or″ and the dot (.) is to be read as ″and″, the valid rules are tabulated in table 8.2.

The Boolean rules one and two "cancel out" any redundanties of the same event. The third rule can be expressed in words as: The occurrence of basic event A or the combination of basic events A and B is equivalent to the occurrence of basic event A.

Basic events identification:

For proper cut-set determination it is important to use the same name for the same basic events that represent the failure of the same component in the different branches within the fault tree. For instance, the basic event that represents the failure of power supply 1 as inputs for gates G2, G3 and G4 (see figure 8.5) must have the identification (BE3). On the other hand, the basic events BE1 and BE2 represent failures of two different components and for that reason must have a different identification.

Table 8.2: Rules Boolean algebra.

No.	Fault tree left term	Rule	Fault tree right term
1		A + A = A	
2		A.A = A	
3		A + A.B = A	

It is not feasible to name the basic events, as has been done within the rectangles in figure 8.5. Therefore, in general the labels for the basic events need to be short. In the example the basic events are labeled from BE1 up to BE7. Depending on the computer program to be used, longer names might be possible.

One unique identification for each equivalent basic event is important because the second Boolean rule can be applicable. Take for example basic event BE3. The gate G1 is an ”and-gate”.This means that all basic events beneath gate G2 must be combined with the basic events beneath gate G3, so amongst others BE3 must be combined with BE3. This suggests a second order cut-set, but this is not true because rule 2 states BE3.BE3 = BE3.

After identification of the basic events the minimal cut-sets can be determined. The use of a computer program facilitates this process and in the case of large fault trees this aid is indispensable. In the case of the example, the minimal cut-sets are determined by hand.

8.3.6 Determination of minimal cut-sets example

To determine the minimal cut-sets of a fault tree, the tree is first translated into its equivalent Boolean equations and then either the ”top-down” or the ”bottom-up” substitution method is used. The methods are straightforward and they involve substituting and expanding Boolean expressions. The first and second Boolean rules are used to remove the redundancy of the same basic event. This process wilt be executed for the fault tree of the example safety system as depicted in figure 8.5. The top event from the fault tree depicted in figure 8.5 can be expressed as (using Boolean algebra):

TOP = (BE1 + BE3 + A) . (BE3 + BE2 + A) with

A = BE3 + BE4 + (BE5 + BE6) . (BE6 + BE7)

This expression can also be rewritten as:

TOP	:	BE1	.	BE3	+
		BE1	.	BE2	+
		BE1	.	A	+
		BE3	.	BE3	+
		BE3	.	BE2	+
		BE3	.	A	+
		A	.	BE3	+
		A	.	BE2	+
		A	.	A	

The expression for the occurrence of the top event is now described by a number of intersections, but not as minimal cut-sets. In order to determine the minimal cut-sets, the intersections need to be simplified by using the three rules from Boolean Algebra.

Intersection BE3.BE3 occurs if basic event BE3 occurs. This means that the subset BE3.BE3 is not the simplest way to express the occurrence of the top event, in relation to basic event BE3 (Rule 2).

Applying rule 2 yields:

TOP	:	BE1	.	BE3	+
		BE1	.	BE2	+
		BE1	.	A	+
		BE3	.		+
		BE3	.	BE2	+
		BE3	.	A	+
		A	.	BE3	+
		A	.	BE2	+
		A			

Given a first order minimal cut-set, the top event will occur; according to rule 3 it serves no purpose at all to examine that basic event in combination with other basic events. In this case the top event will occur despite the occurrence of other basic events. Here BE3 and A are first-order minimal cut-sets. This means that the intersections:

BE1	.	BE3
BE1	.	A
BE3	.	BE2
BE3	.	A
A	.	BE3
A	.	BE2

are meaningless. The expression for the occurrence of the top event now becomes:

TOP = BE1.BE2 + BE3 + A

With A:

A = BE3 + BE4 + BE5.BE6 + BE5.BE7 + BE6.BE6 + BE6.BE7

Applying rule 2 yields:

A = BE3 + BE4 + BE5.BE6 + BE5.BE7 + BE6 + BE6.BE7

Applying rule 3 yields:

A = BE3 + BE4 + BE5.BE7 + BE6

Substitution of A into the expression for the occurrence of the top event yields:

TOP = BE1.BE2 + BE3 + BE3 + BE4 + BE5.BE7 + BE6

Applying rule 1 and rearranging the results holds:

TOP = BE3 + BE4 + BE6 + BE1.BE2 + BE5.BE7

On purely qualitative grounds, the number of intersections cannot be limited any further, so the minimal cut-sets are found.

The minimal cut sets are:

First order:	BE3	(failure of power supply E1)
	BE4	(failure of logic)
	BE6	(failure of power supply E2)
Second order:	BE1 . BE2	(failure of both final elements)
	BE5 . BE7	(failure of both sensors)

As stated in the introduction, the minimal cut-sets represent the ways in which the system can fail. It is recommended always to check if the minimal cut-sets represent the correct failure possibilities of the system under consideration.

8.3.7 Collecting failure, repair, test and maintenance data

In order to be able to quantify a fault tree, additional information concerning the components, the operation and maintenance of the system is necessary. In general this additional information comprises:

- failure frequencies or probabilities of failure on demand of the components
- the types of components; stand-by or on-line repairable
- the test interval (T)
- the repair duration (θ)
- the test duration (τ).

In case of the example problem, table 8.3 present the necessary data which is the result of the consultation of failure data banks and the consultation of the maintenance crew.

Table 8.3: Data of the example safety system.

Component	Basic event	λ -/hour	τ hour	θ hour	T hour	Q -/demand
Final Elements	BE1 , BE2	10^{-5}	1	10	730	-
Power supply	BE3 , BE6	10^{-6}	-	10	-	-
Sensors	BE5 , BE7	10^{-5}	5	2	2190	-
Logic	BE4	-	0	1	2190	10^{-4}

8.3.8 Quantification of the minimal cut sets

One of the most important aspects in quantifying a fault tree is establishing the nature of the problem. Which reliability parameters have to be calculated? The unavailability of a system in a continuous mode of operation, the probability of failure on demand or the expected number of failures within a stated period of time. The analyst has to make the right selection of the appropriate parameters to be calculated. For a safety device this wilt mostly be the probability of failure on demand.

The quantification process is explained by quantification of the minimal cut-sets of the example problem of the safety device. In this case the probability of failure on demand has to be calculated. The probability of failure on demand is equal to the unavailability of the safety device. So, to calculate the probability of failure on demand, the formulas which are derived to calculate the unavailability have to be used.

To determine the probability of failure on demand, the expression for the occurrence of the top event is needed:

TOP = BE3 + BE4 + BE6 + BE1 . BE2 + BE5.BE7

The top event will occur in case power supply E1 fails (BE3) or the logic fails (BE4) or power supply E2 fails (BE6) or both the final elements fail (BE1 . BE2) or both the sensors fail (BE5.BE7).

The probability of failure needs to be determined by using probability rules:

P(TOP) = P(BE3 + BE4 + BE6 + BE1.BE2 + BE5.BE7)

= P(BE3) + P(BE4) + P(BE6) + P(BE1.BE2) + P(BE5.BE7) + Higher Order terms

In practical cases the "rare event approximation" can mostly be applied, which means that the higher order terms are neglected. This is tolerable in case the probabilities of occurrence of a single basic event within the minimal cut-sets are very low.

The probability of failure on demand of the safety system is now determined by adding the probability of failure on demand of each separate minimal cut-set.

P(TOP) = P(BE3) + P(BE4) + P(BE6) + P(BE1.BE2) + P(BE5.BE7)

To quantify the minimal cut-sets, a number of standard formulas have been derived, see chapter 9, "Quantification of minimal cut-sets". In the following paragraph these standard formulas will be used to calculate the probability of failure on demand for the example safety system.

Minimal cut set BE3 (failure of power supply E1):

This minimal cut-set describes the situation where power supply E1 is in a failed condition. The power supply is monitored by means of an audiovisual signal in the control room. The control room is continuously occupied by an operator, who upon the signal's occurrence immediately calls for a service engineer and has the defect repaired. As soon as the fault occurs, the repair procedure is started and the repair period starts. Maintenance of power supply E1 is carried out only at times when the process is shut down and therefore does not contribute to system unavailability. Hence, the only contributor to system unavailability is repair of the power supply after occurrence of a power supply failure. This implies that formula A2, given in the appendix of chapter 9, has to be used. For the sake of convenience formula A2 is repeated here:

COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
A2 λ o.r.	–	–	$\lambda\theta$

o.r. = On-line repairable.

From table 8.3 it follows that:

λ	$= 10^{-6}$ -/hour	
θ	= 10	hour

Substitution of these values into formula A2 yields:

Unavailability: BE3 $= 0.1\ 10^{-4}$ (-)

Minimal cut-set BE4 (failure of logic):

This minimal cut-set describes the failure of the one-out-of-two logic. In table 8.3 a probability of failure on demand is provided for this component. This implies that formula A3 from the appendix of chapter 9 has to be used.

COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
A3 Q –	Q	$\frac{\tau}{T}$	$\frac{Q\theta}{T}$

From table 8.3 it follows that:

Q	=	10^{-4}	-/demand
τ	=	0	hour
θ	=	1	hour
T	=	2190	hour

Substitution of these values into formula A3 yields:

Unavailability: BE4 $= 1.0\ 10^{-4} + 0.0 + 0.0005\ 10^{-4}$

$\approx 10^{-4}$ (-)

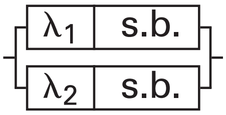
Minimal cut-set BE6 (failure of power supply E2):

In this case electric power supply E2 has failed. Exactly the same conditions apply to this situation as to power supply E1. Thus the unavailability is the same:

Unavailability: BE6 $= 0.1\ 10^{-4}$ (-)

Minimal cut-set BE1.BE2 (both final elements failed):

Both final elements 1 and 2 are failed. The final elements are entirely identical, they can both fail and remain in the failed condition without this being immediately obvious. Therefore periodical testing is applied, which is scheduled once a month. First final element 1 is tested and then final element 2 is tested. If during testing final element 1 proves to be defective, it is repaired immediately, even before device 2 is tested. From the foregoing it can be concluded that formula B1, see the appendix to chapter 9, is to be used:

COMPONENTS	UNAVAILABILITY		
FAILURE	TESTING	REPAIR	
B1  	$\frac{1}{3}\ \lambda_1\lambda_2T^2$	$\lambda_2\tau_1$	$\lambda_1\lambda_2\theta_1T$

s.b. = Periodically tested stand-by component.

From table 8.3 it follows that:

λ_1	=	10^{-5}	-/hour
λ_2	=	10^{-5}	-/hour
τ_1	=	1	hour
θ_1	=	10	hour
T	=	730	hour

Substitution of these values into formula B2 yields:

Unavailability:

BE1.BE2 $= 0.18\ 10^{-4} + 0.1\ 10^{-4} + 0.007\ 10^{-4}$
$\approx 0.3\ 10^{-4}$ (-)

Minimal cut-set BE5.BE7 (failure of both sensors):

Both sensor 1 and 2 are now in a failed condition. The sensors are identical and remain in the failed condition until a test is performed. For this reason the sensors are tested periodically. In order to test a sensor it must be removed and tested in a test rig. This is done four times a year for each sensor. The sensors are tested one immediately after the other. In this way one sensor is always present to operate if necessary. From the foregoing it can be concluded that formula B1 from the appendix of chapter 9 has to be used.

From table 8.3 it follows that:

λ_1	=	10^{-5}	-/hour
λ_2	=	10^{-5}	-/hour
τ_1	=	5	hour
θ_1	=	2	hour
T	=	2190	hour

Substitution into formula B1 yields:

Unavailability:

$$\text{BE5.BE7} = 1.6\ 10^{-4} + 0.5\ 10^{-4} + 0.004\ 10^{-4}$$

$$\approx 2.1\ 10^{-4} \quad (-)$$

The total probability of failure on demand or the total unavailability is the sum of the contributions of each of the minimal cut-set:

BE3	$0.1\ 10^{-4}$	(failure of power supply E1)
BE4	$1.0\ 10^{-4}$	(failure of one out of two logic)
BE6	$0.1\ 10^{-4}$	(failure of power supply E2)
BE1 . BE2	$0.3\ 10^{-4}$	(failure of both final elements)
BES . BE7	$2.1\ 10^{-4}$	(failure of both sensors)

The total probability of failure on demand of the safety system equals:

$$\text{PFD} = 3.6\ 10^{-4}$$

This means that given a demand the probability that the safety system will not stop the process is equal to $3.6\ 10^{-4}$. This implies that on average the safety system fails to stop the process approximately once per three thousand demands.

8.3.9 Evaluation, sensitivity and uncertainty analysis

Quantification of the fault tree provides information not only about the value of the system reliability parameter, but also of the main and minor contributors to the system reliability parameter. This means that it is often possible to identify whether a system change is actually an improvement or not. For example, in order to reduce the probability of failure on demand, it is useless to aim for a shorter repair time for power supply E1. Halving the repair time (e.g. having a spare power supply available) has practically no effect on the total probability of failure on demand.

For the example safety system, the main contributors to the probability of failure on demand are the sensors and the one-out-of-two logic.

Sensitivity studies are performed to assess the impact of variations or changes to the component data or to the fault tree model. It is particularly convenient to assess effects of component data variations using the formulas presented in chapter 9, because they explicitly contain component failure rates, test intervals, repair duration and test duration as variables. In sensitivity analysis different values may be assigned to these variables to determine the difference in any result.

As a type of sensitivity study, scoping-type evaluations can also be performed by using a high failure rate and a low failure rate for a particular basic event in the fault tree. If the system reliability parameter calculated does not change significantly, then the basic event is not important and no more attention needs to be paid to it. If the system reliability parameter does change significantly, then more precise data must be obtained or the event must be further developed into more basic causes.

If, for the example safety system, the testing interval is increased from 4 times a year to 8 times a year, the contribution of the sensors to the probability of failure on demand is reduced from 2.1 E-04 to 9 E-05, and therefore the total probability of failure on demand becomes: 2.4 E-04.

The above quantification is one that works with point values. In reality there are uncertainties in the numerical values of the system reliability parameter to be calculated. This means that there are probability distributions and that an analysis performed as above only results in an average value. It must be emphasized that the point values generated with a quantitative reliability analysis must not be regarded as fixed numbers. The calculated value for a certain system reliability parameter is always an estimated value, subject to a certain error spread. Taking into account the uncertainty in the input parameters, the uncertainty in the calculated system reliability parameter can be estimated. The most commonly applied technique to determine this uncertainty is the Monte Carlo simulation technique. To perform such an analysis, the reader is referred to chapter 15.

8.4 GUIDELINES FOR FAULT TREE DEVELOPMENT

This chapter presents guidelines and other considerations to be taken into account in fault tree development. Although these rules are always important when performing a Fault Tree analysis, they become indispensable as the system to be analyzed gets complex or when more than one fault tree is needed. This chapter originates from the nuclear field of fault tree analysis but is also applicable in the non-nuclear field of fault tree analysis.

8.4.1 General guidelines for fault tree development

If a number of fault trees have to be constructed for one or maybe more plants, it is useful to make a task plan so as to be sure that all fault trees are constructed with the same degree of detail and that all fault trees are constructed with the same generally applicable assumptions. The following issues merit special consideration in the development of fault trees:

- *Fault tree analysis task plan:*
  Methods and procedures for the construction of fault trees should be agreed and documented in a fault tree analysis task plan at the beginning of a fault tree analysis project. This is necessary in order to guarantee consistency of the analysis. Items to be considered in this context are: system boundaries, logic symbols, event coding and representation of human errors and common cause failures.

- *Assumptions:*
  All assumptions made in the process of constructing a fault tree should be documented together with the source of all design information used. In this way, consistency will be promoted throughout the analysis and traceability will be maintained.

- *Computer programs:*
  Computerized methods should be used for handling the solution and quantification of fault trees to ensure consistency, comprehensiveness, efficiency and quality.

- *Definition of system boundaries:*
  It is clear that precise definitions of system boundaries need to be established before the analysis begins. These definitions should be adhered to during the analysis and should be included in the final documentation covering system modeling. The interface points with the support systems, like instrument air, power supply and actuation signals, for example, could be located as follows:
  - for electrical power supply, at the buses from which components considered within the system are fed
  - for actuation signals, at the appropriate output cabinets of the actuation system
  - for support systems, providing various media (water, oil, air), at the main header line of the support system.

  In cases where equipment or piping is shared between several systems, guidance with respect to proper establishment of boundary conditions is usually provided by system descriptions and drawings. This aspect has to be carefully checked in order to avoid possible omissions and/or double counting.

- *Standard coding basic events:*
  It is important that a standardized format is employed for coding basic events in the fault trees. Whichever scheme is used, it should be compatible with the computer code selected for the systems analysis and also enable the basic events to be clearly related to the following:
  - component failure mode
  - specific component identification and type
  - specific system in which the component is located.
  - plant codings for the components.

8.4.2 Specific guidelines for fault tree development

In general the fault trees should reflect all possible failure modes that may contribute to failure of the system. This should include contributions due to outages for testing and maintenance. Human errors associated with failure to restore equipment to its operable state following testing and maintenance.

The fault tree analyst has to take notice of all available information collected in the plant familiarization process. Important are descriptions of all types of failures that have occurred at the plant being analyzed and at similar plants, in order to gain a direct awareness of the potential for independent or dependent failures in the systems and of the potential for system interactions.

Based on experience a number of specific guidelines have been developed which should be followed during the fault tree development process. These guidelines are:

- *Level of detail.*
  In a fault tree analysis, it is important to include all components which may contribute to the probability of failure. Taking this into account, fault trees should be developed down to a level where appropriate failure data exists.

- *Identification of dependencies between systems:*
  When systems are not modeled in detail and system level reliability data is used, failure events in common with other systems should be separated out and explicitly considered.

- *Undeveloped events:*
  To simplify and reduce the size of the fault trees, certain events are often excluded as a result of their low probability in comparison with other events (passive versus active components).

- *Test procedures:*
  The testing procedures used must be closely examined to see whether they introduce potential failure modes. All such potential failure modes identified must be documented. An example of such a failure would be if in the course of testing, the flow path through a valve is isolated, and at the end of the test the flow path remains closed (possibly due to human error) and there is no indication that the flow path is stil) closed.

- *Component protection:*
  Trips of pumps and other safeguards intended to protect a component must be carefully identified. These can be a source of common mode failure.

- *Human failure events:*
  Human-related failure events that occur prior to the start of an accident (i.e. latent human failure) should be included in the fault tree at a train or system level.

- *Testing and maintenance:*
  Equipment unavailability due to testing or maintenance when the plant is operating has to be included in the fault tree. Basic events representing such unavailabilities should reflect unavailability at the train or system level. Component level testing or maintenance unavailabilities should be avoided if possible.

- *Pipe breaks:*
  Pipe breaks do not have to be modeled in the trees unless they cause total failure of a system, all trains must be affected by the pipe break.

- *Check valves:*
  Normally check valves will be modeled for failure to open, failure to remain open (transfer closed), and failure to prevent reverse flow (only if such a failure prevents a system from performing its required functions).

- *Flow diversion:*
  Flow diversion paths for fluid systems should be considered only if they could seriously degrade or fail the system.

- *Recirculation paths:*
  Minimum recirculation paths need to be modeled if required to ensure component operability during mission time.

- *Position faults:*
  Position faults prior to a demand are not included if the component receives an automatic signal to return to its operable state under accident conditions.

- *Treatment of dependencies:*
  In general, dependent failures are important contributors to system failure. For this reason aspects of dependent failures have to be reflected in the fault trees. The most important dependencies in the system analysis task are:
  - common support system faults affecting more than one component through functional dependencies
  - human errors associated with common test and maintenance activities
  - redundancy achieved by identical components.

  In fault tree analysis two types of modeling of dependent events have to be distinguished, viz. explicit and implicit modeling.

  Multiple failure events for which a clear cause-effect relation can be identified have to be explicitly modeled in the fault tree model: the root cause events should be included in the system fault tree so that no further special dependent failure model is necessary. This applies to multiple failures caused by internal equipment failure (such as cascade failures and functional unavailability events caused by components) and multiple failures due to failure of common support systems.

  Multiple failure events that are susceptible to dependencies, and for which no clear root cause event can be identified, can be modeled using implicit methods such as the parametric models (see chapter 13). Examples of such types of dependencies are dependencies between identical redundant equipment.

8.4.3 Documentation of a fault tree analysis

A detailed documentation of the fault tree analysis task is very important.

For most safety systems, essential information should be provided concerning:

- the instrumentation for monitoring the performance of the process
- the control logic associated with any of the components of the system
- the minimal information needed to identify support system dependencies
- other auxiliaries such as instrumentation and control systems and their relation to system operation should also be discussed.

Every assumption made during fault tree construction should be documented very carefully and the reference of all failure data used should be clearly stated in the documentation.

For safety systems, a description of the system should include a list of the parameters that are monitored, the mitigatory actions initiated by the system and the components that are activated. Information should also be provided about the fait safe principle for major components and the failure warning system.

The composition and organization of the instrumentation, including sensors and transmitters, signal processing channels, logic modules and load relay drivers, should be described. Separation and diversity of transmitters should be discussed. Manual override or actuation possibilities should also be discussed.

As a minimum, the fault tree documentation should include the following items:

- *Sources of information:*
  The sources of system design data that were used in the analysis should be specified together with the discussion related to the actuality and sufficiency of the information.

- *System function:*
  A brief description of the purpose of the system is given. The principal function that the system helps to perform.

- *Design basis:*
  A simple description of the piping/wiring configuration should be given, accompanied by a schematic diagram depicting the major components of the system. Piping/wiring segments should be noted in the diagram. This discussion should clarify system boundaries used in the modeling. If certain flow paths have been ignored, these should be noted and a justification should be given. Technical data such as physical dimensions, locations, capacities will be included if important to the system's operation.

- *System description:*
  A concise description of the system layout is appropriate. Component details should be provided to the extent necessary to support the selection of generic failure data for the fault trees.

- *Interfaces:*
  Detailed lists of the interfaces with other systems or support systems, including all those necessary for operation, should be provided. The specific interfaces and impacts of supporting system failures should be described.

- *System operation:*
  Operation of the system in various operating modes of interest should be provided. The discussion should specify which equipment changes the state to initiate the system, what signals cause the system to actuate, and any required operator actions. If the operator is to perform any backup actions, these should be discussed, together with the indications that the operator would have in the control room or locally to perform the action. Recovery actions available to the operator are discussed for major component or system failure modes. The portions of the emergency operating procedures relevant to this system are summarized.

- *System and Component Boundaries:*
  Component boundaries ought to be defined. Although this question may primarily belong to the component data section, it also is very important for the modeling of the fault trees. Thus, it is suggested that component boundaries are defined and that those definitions are referenced in the systems analysis.

- *Testing and maintenance:*
  General schedule for system tests, the type of test procedure and the changes in system configuration during these tests is described. The maintenance schedule and procedures with respect to availability of system components are discussed. The system configuration during maintenance should be described.

- *Technical specifications:*
  A summary of the technical specification requirements and of other limiting conditions for operation is provided.

- *System actuation:*
  The parameters and set points used for automatic system actuation, the names of initiating signals with statements of the effects of these signals (such as open the valve, close the valve, check position of the valve), the names of start systems that are activated.

- *Component trips:*
  The parameters and set points used to initiate component operation automatically, information that the operator receives, reasons for component trips.

- *Fault tree presentation:*
  The fault tree presentation should include:
  - graphical representation and a description of the detailed fault tree model.
  - additional qualitative and quantitative information related to logic elements used in the model (provided in tabular form), including:
    - description and data for all hardware failures (failure rate, mean time between demands or duration time, mean unavailability)
    - description and data for human errors (event type, failure probability)
    - description and data for maintenance events (mean frequency, mean duration, unavailability)
    - description and data for dependent failures included in the fault tree model.

8.5 EXAMPLES

8.5.1 Example of a system in a continuous mode of operation

This example concerns the electrical supply of railway track equipment, like signal posts, points and actuators of level-crossing barriers (see figure 8.6). In this case the electrical supply consists of two 3000 Volt cables on each side of the track. Each 3000 Volt cable is fed by a cabinet, in which a transformer and a fuse is mounted. The cabinets are fed from two power supplies of the local 380 Volt grid. These two power supplies are fully dependent. To prevent a blackout in case of a grid failure, a diesel generator set is installed.

System familiarization:
During normal operation the railway track equipment is fed by the upper 3000 Volt cable (K1). In case of a failure of this power supply the electronic device will connect the railway track equipment to the lower 3000 Volt cable. In case of a failure of the power supply from the grid the diesel generator will be started and will be connected to cable K2 by the electronic device E2. To perform a reliability analysis, the system is simplified to the system as drawn in figure 8.7.

Fault tree construction:
Fault tree construction has to start at the point where the 110 Volt is supplied. So the following top event has been defined:

”No_110_volt”

Two branches have to be analyzed, one going into the direction of cable K1 and one going into the direction of cable K2. The resulting fault tree is depicted in appendix 8-A.

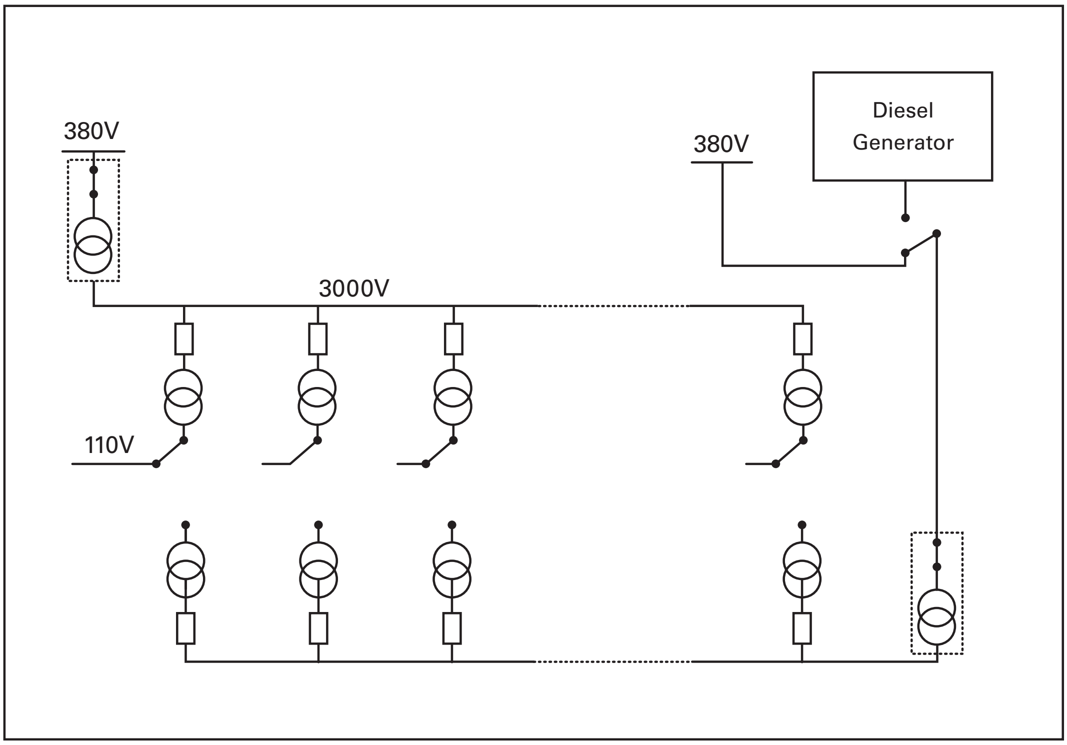


Figure 8.6: Example of a system in continuous mode of operation

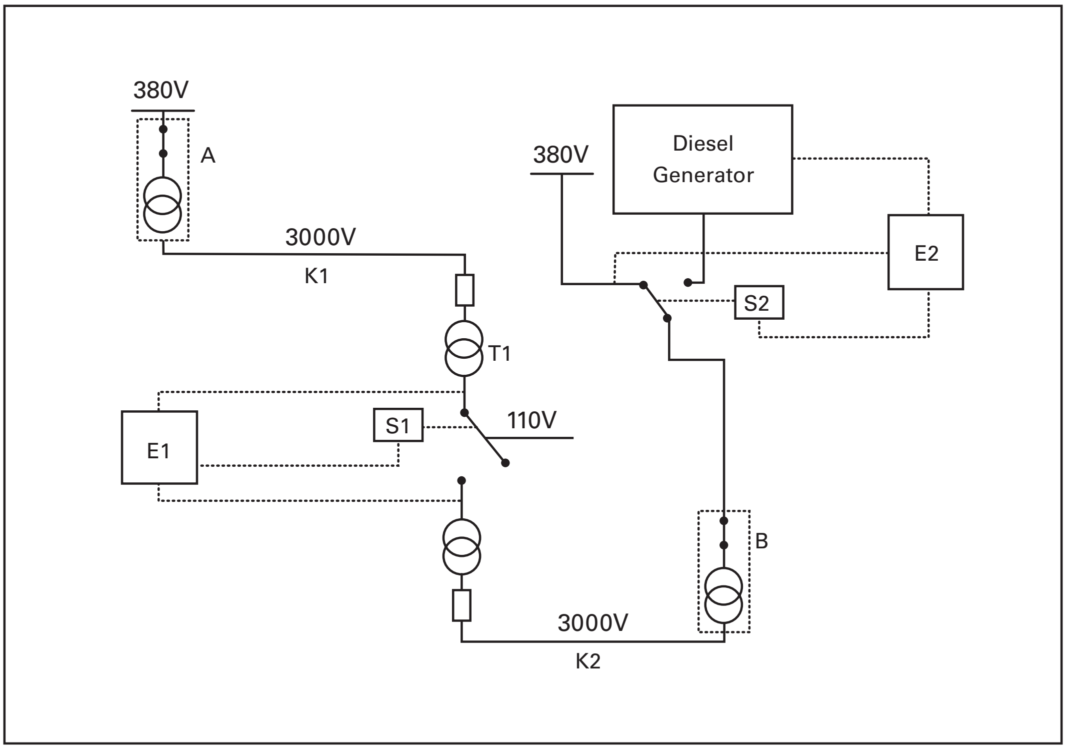


Figure 8.7: Modified system layout for fault tree construction.

Minimal cut-set determination:

Cut-set determination will be done by application of a fault tree analysis computer code. The input fault tree structure is as follows:

```
Gate                Type     Input events

NO-110-VOLT         OR       SWITCH_S1_OPEN     NO_E_SUPPLY
NO_E_SUPPLY         AND      NO_SUPPLY_Tl       NO_SUPPLY_T2
NO_SUPPLY_T1        OR       NO_SUPPLY_TO_T1    FAILURE_OF_Tl
NO_SUPPLY_TO_T1     OR       FAILURE_OF_K1      FAILURE_OF_KA       FAILURE_380_VOLT
NO_SUPPLY_T2        OR       NO_SUPPLY_TO_T2    S1_FAIL_TO_CLOSE
S1_FAIL_TO_CLOSE    OR       FAILURE_OF_S1      FAILURE_OF_E1
NO_SUPPLY_TO_T2     OR       NO_SUPPLY_TO_KB    FAILURE_OF_T2       FAILURE_OF_K2
                             FAILURE_OF_KB
NO_SUPPLY_TO_KB     OR       NO_SUPPLY_TO_S2    SWITCH_S2_OPEN
NO_SUPPLY_TO_S2     AND      FAILURE_380_VOLT   NO-SUPPLY DIESEL
NO_SUPPLY_DIESEL    OR       S2_FAIL_TO_CLOSE   DIESEL_FAILURE
S2_FAIL_TO_CLOSE    OR       FAILURE_OF_S2      FAILURE_OF_E2
```

The following cut-set report is generated by the fault tree computer program:

Cut-set report:

```
Order                 Combinations     Cut-sets
First order     :          1               1
Second order    :          2              27
Higher order    :          0               0

Total           :          3              28
```

First-order minimal cut-sets:

```
SWITCH_S1_OPEN
```

Second-order minimal cut-sets:

Combination 1:

```
FAILURE_OF_Kl        FAILURE_OF_El
FAILURE_OF_KA        FAILURE_OF_K2
FAILURE_OF_Tl        FAILURE_OF_KB
                     FAILURE_OF_S1
                     FAILURE_OF_T2
                     SWITCH_S2_OPEN
```

Combination 2:

```
FAILURE_380_VOLT      DIESEL_FAILURE
                      FAILURE_OF_E1
                      FAILURE_OF_E2
                      FAILURE_OF_K2
                      FAILURE_OF_KB
                      FAILURE_OF_S1
                      FAILURE_OF_S2
                      FAILURE_OF_T2
                      SWITCH_S2_OPEN
```

Remark:
The computer program used to determine the minimal cut-sets reports the minimal cut-sets in blocks. For combination 1 of the set of second-order minimal cut-sets this implies that every basic event in the first column constitutes a minimal cut-set with each basic event in the second column. Combination 1 represents eighteen minimal cut-sets. The advantage of this type of presentation is that a large number of cut-sets can be documented on one page and that the cut-sets can be checked very easily.

Interpretation of second-order minimal cut-sets:
The first block of combination 1 represents failure of the power supply via cable K1. The second block of combination 1 represents failure of the restoration of the power supply after failure of the power supply via cable K1. The second block of combination 2 describes failure to restore power supply after a grid failure.

Component database:
To quantify the generated minimal cut-sets, all relevant component data has to be collected. If necessary, generic data has to be used or combined with plant-specific data to achieve an accurate result. To calculate the unavailability of a system in a continuous mode of operation, accurate repair durations are important. The collected data is presented in table 8.4.

Quantification of minimal cut-sets:
The system reliability characteristics of interest in this example are; the expected number of failures per year and the unavailability. To calculate the expected number of failures per year the formulas in tables C and D in the appendix of chapter 9 have to be used.

Table 8.4: Component failure data example 1.

Component	**λ (-/hour)**	**Q -**	**T (hour)**	**θ (hour)**
Switch S1 transfers open	1.0E-06	-	-	1
Switch S2 transfers open	1.0E-06	-	-	1
Switch fails on demand	-	1.0E-04	-	0
Switch fails on demand	-	1.0E-04	-	0
Electronic device EI	1.0E-06	-	8760	4
Electronic device E2	1.0E-08	-	8760	4
Cable K1	1.8E-05	-	-	24
Cable K2	1.8E-05	-	-	24
Cabinet KA	1.0E-06	-	-	8
Cabinet KB	1.0E-06	-	-	8
Transformer T1	1.0E-06	-	-	8
Transformer T2	1.0E-06	-	-	8
Grid failure	2.5E-06	-	-	1
Diesel fails in stand-by	4.0E-06	-	8760	8
Diesel fails to start	-	2.5E-03	-	0
Diesel fails to run	8.0E-04	-	-	0

Remark: It should be emphasized that the data presented in table 8.4 is for illustrative purposes only and cannot be regarded as valid data.

The results of the quantification are as follows:

Expected number of failures per year:

Contributions:

First-order minimal cut-sets	:	8.76E-03	53.60%
Second-order minimal cut-sets	:	7.54E-03	46.40%
Higher-order minimal cut-sets	:	0.0	0.00%
Total	:	1.63E-02	

The fifteen most important minimal cut-sets determining the expected number of failures per year are:

	Cut-set	Contribution	Per cent	Formula
1	SWITCH_S1_OPEN	8.76E-03	53.60	D2
2	FAILURE_380_VOLT DIESEL_FAILURE	4.56E-03	27.94	See note
3	FAILURE_OF_E1 FAILURE_380_VOLT	9.64E-04	5.88	D2
4	FAILURE_OF_E2 FAILURE_380_VOLT	9.64E-04	5.88	D2
5	FAILURE_OF_E1 FAILURE_OF_K1	6.95E-04	4.25	D2
6	FAILURE_OF_Kl FAILURE_OF_K2	1.37E-04	0.83	D3
7	FAILURE_380_VOLT FAILURE_OF_K2	9.90E-05	0.60	D3
8	FAILURE_OF_E1 FAILURE_OF_KA	3.85E-05	0.24	D2
9	FAILURE_OF_El FAILURE_OF_T1	3.85E-05	0.24	D2
10	FAILURE_380_VOLT FAILURE_OF_SI	2.19E-05	0.13	DS
11	FAILURE_380_VOLT FAILURE_OF_S2	2.19E-05	0.13	D3
12	FAILURE_OF_K1 FAILURE_OF_SI	1.58E-05	0.10	D3
13	FAILURE_OF_K1 FAILURE_OF_KB	5.05E-06	0.03	D3
14	FAILURE_OF_K1 FAILURE_OF_T2	5.05E-06	0.03	D3
15	FAILURE_OF_KA FAILURE_OF_K2	5.05E-06	0.03	D3

Unavailability:

Unavailability can be calculated with the formulas provided in tables A and B in the appendix of chapter 9. The results are:

Contributions:

First-order minimal cut-sets	:	1.00E-06	24.04%
Second-order minimal cut-sets	:	3.16E-06	75.96%
Higher-order minimal cut-sets	:	0.0	0.0%
Total	:	4.16E-06	

The fifteen most important minimal cut-sets describing the unavailability of the system are:

	Cut-set	Contribution	Per cent	Formula
1	FAILURE_OF_EI FAILURE_OF_K1	1.89E-06	45.54	B2
2	SWITCH_Sl_OPEN	1.00E-06	24.04	A2
3	FAILURE_380_VOLT DIESEL_FAILURE	5.21E-07	12.53	See note
4	FAILURE_OF_Kl FAILURE_OF_K2	3.73E-07	8.97	B3
5	FAILURE_OF_El FAILURE_380_VOLT	1.10E-07	2.64	B2
6	FAILURE_OF_E2 FAILURE_380_VOLT	1.10E-07	2.64	B2
7	FAILURE_OF_K1 FAILURE_OF_S1	4.32E-08	1.04	B5
8	FAILURE_OF_E1 FAILURE_OF_KA	3.51E-08	0.84	B2
9	FAILURE_OF_E1 FAILURE_OF_T1	3.51E-08	0.84	B2
10	FAILURE_380_VOLT FAILURE_OF_K2	1.13E-08	0.27	B3
11	FAILURE_OF_K1 FAILURE_OF_KB	4.61E-09	0.11	B3
12	FAILURE_OF_Kl FAILURE_OF_T2	4.61E-09	0.11	B3
13	FAILURE_OF_KA FAILURE_OF_K2	4.61E-09	0.11	B3
14	FAILURE_OF_T1 FAILURE_OF_K2	4.61E-09	0.11	B3
15	FAILURE_380_VOLT FAILURE_OF_S1	2.50E-09	0.06	B5

Note:
The quantification of the minimal cut-set that describes a grid failure and a failure of the diesel generator has to be done with the formulas derived in chapter 11, 'Warkov processes". In paragraph 11.8 the following formula is presented to quantify the unavailability of a stand-by system like the diesel generator in this example.

$$U_{mcs} = (\lambda_1\ \Theta_1\ \lambda_2 + \lambda_1\ Q_2)\ \theta_1 \tag{8.1}$$

The formula to calculate the failure occurrence rate for the same cut-set can be derived from formula (8.1):

$$\omega_{mes} = \lambda_1\ \Theta_1\ \lambda_2 + \lambda_1\ Q_2 \tag{8.2}$$

Component 1 represents the grid and component 2 represents the diesel generator set. The second term in formula (8.2) describes a failure to start of the diesel generator after failure of the grid and the first term describes a failure to run of the diesel generator during repair of the grid.

The expected number of failures per year can be calculated with the formula:

$$N(0,T)_{mcs} = (\lambda_1\ \Theta_1\ \lambda_2 + \lambda_1\ Q_2)\,T \tag{8.3}$$

Evaluation of the analysis

The numerical results are:

Expected number of failures	:	1.6E-02	-/year
Unavailability	:	4.2E-06	-

The mean time between failures of this system is equal to 60 years. The mean down time can be calculated with the following formula:

$$\begin{aligned} MDT &= \frac{U\ 8760}{N} \\ &= \frac{4.2\ 10^{-6}\ 8760}{1.6\ 10^{-2}} \qquad (8.4) \\ &= 2.2 \quad \text{hours} \end{aligned}$$

The dominant contributors to the failure frequency are failure of switch S1, failure of the grid and failure of the diesel generator set.

The dominant contributors to unavailability are: failure of cable K1, failure of electronic device E1, failure of switch S1 and failure of the grid.

8.5.2 Example of a high-integrity pressure protection system (HIPPS)

In figure 8.8 an example of the layout of a high-pressure protection system is provided. The objective of a high-pressure protection system is to protect the low-pressure part of the system against over pressure by closing of at least one of the two shut-off valves. The shut-off valves are spring-return valves and are operated by solenoid valves. The spring will close the shut-off valve after loss of the air supply. The complete system is designed fail-safe against loss of power supply or loss of air supply.

The solenoid valves are de-activated by a logic element. Pressure switches are used as input of the one-out-of-two logic element. If a preset pressure level is reached and the pressure switches detect this situation, the solenoid valves are de-activated by the logic element. De-activation of the solenoid valves releases air pressure from the shut-off valves, which in turn will be closed by the springs.

For this example a fault tree analysis will be performed to calculate the probability of failure on demand, given a high-pressure situation.

System familiarization:
The system is tested periodically over a test period of one year. Testing is performed during annual maintenance. Review of the test procedure showed that a part of the logic is not covered by the annually performed test. This part is only tested during an overhaul performed every ten years. The same procedures are used to calibrate the pressure switches and calibration of the pressure switches is performed by the same maintenance team. Both pressure switches are calibrated on a single day. Also, the solenoid valves and the shut-off valves are maintained in accordance with the same procedures and by the same maintenance team. This implies that the pressure switches as well as the solenoid valves and the shut-off valves are vulnerable to dependent failures. For this reason dependent failures have to be included in the fault tree.

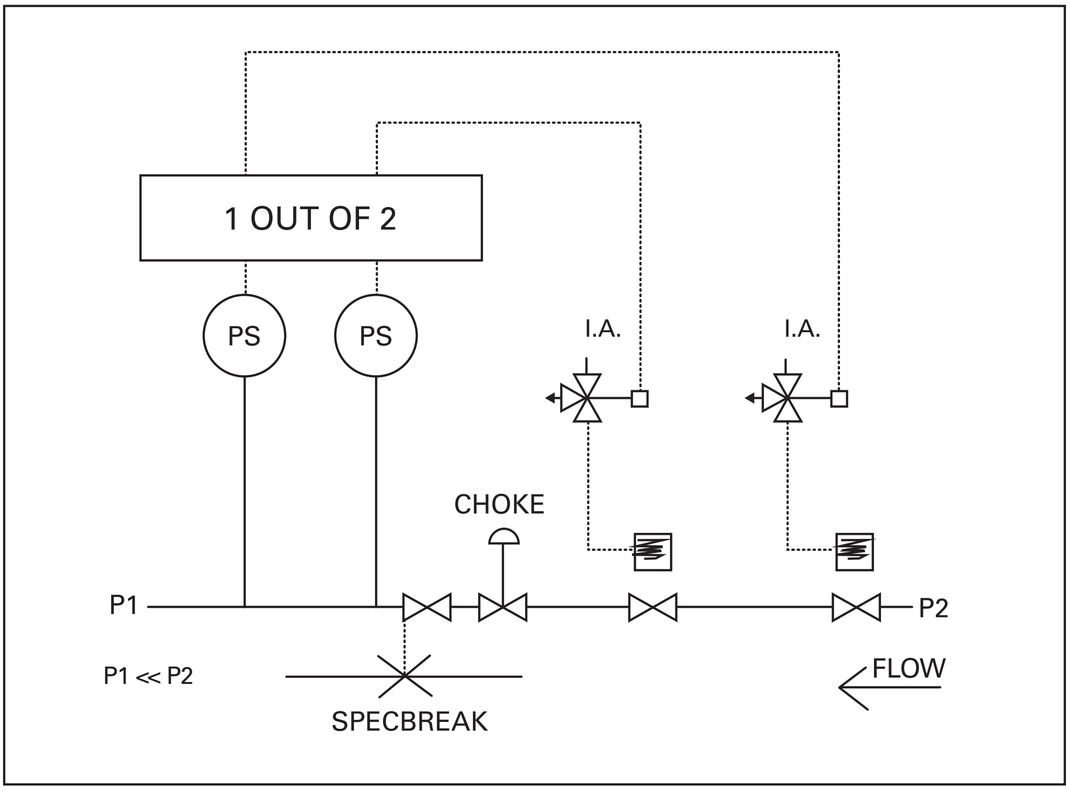


Figure 8.8: Layout of high-integrity pressure protection system.

Fault tree structure:
At least one of the two shut-off valves have to be closed to prevent over pressure of the low-pressure part of the system. This implies that the fault construction has to begin by considering that both shut-off valves will not be closed, given an over pressure situation. The fault tree for this system is depicted in appendix 8-B. The fault tree logic can be described as follows:

Gate	Type	Input Events		
TOP	AND	SHT_OFF_VAL1_FTC	SHT_OFF_VAL2_FTC	
SHT_OFF_VAL1_FTC	OR	SH_VAL1_FAILS	CCF_SH_VALVES	NO_DEPRESS_SOL1
SHT_OFF_VAL2_FTC	OR	SH_VAL2_FAILS	CCF_SH_VALVES	NO_DEPRESS_SOL2
NO_DEPRESS_SOL1	OR	SOL_VAL1_FAILS	CCF_SOL_VALVES	NO_SIGNAL_LOGIC
NO_DEPRESS_SOL2	OR	SOL_VAL2_FAILS	CCF_SOL_VALVES	NO_SIGNAL_LOGIC
NO_SIGNAL_LOGIC	OR	LOGIC_FAILS	NO_SIGNAL_SENSOR	
LOGIC_FAILS	OR	LOGIC1_FAILS	LOGIC2_FAILS	
NO_SIGNAL_SENSOR	AND	NO_SIGNAL_SEN1	NO_SIGNAL_SEN2	
NO_SIGNAL_SEN1	OR	SENSOR1_FAILS	CCF_SENSORS	
NO_SIGNAL_SEN2	OR	SENSOR2_FAILS	CCF_SENSORS	

Cut-set determination:
The minimal cut-sets have been determined by application of a computer program. The results are:

First-order minimal cut-sets

CCF_SENSORS
CCF_SH_VALVES
CCF_SOL_VALVES
LOGICI_FAILS
LOGIC2_FAILS

Second-order minimal cut-sets

SH_VAL1_FAILS	-	SH_VAL2_FAILS
SH_VAL1_FAILS	-	SOL_VAL2_FAILS
SOL_VAL1_FAILS	-	SH_VAL2_FAILS
SOL_VAL1_FAILS	-	SOL_VAL2_FAILS
SENSORI_FAILS	-	SENSOR2_FAILS

Data analysis:
A data analysis can be divided into a generic and a plant-specific data collection. If a limited amount of plant specific data is available, a Bayesian update process has to be performed to combine the generic and plant specific data. The results of this data analysis are presented in table 8.5.

To calculate the failure rates representing dependent failure of the two shut-off valves, the two solenoid valves and the two pressure switches, the beta factor model (see chapter 13) has been applied:

$$\lambda_{ccf,shv} = \beta \,.\, \lambda_{shv}$$

$$\lambda_{ccf,sol} = \beta \,.\, \lambda_{sol}$$

$$\lambda_{ccf,ps} = \beta \,.\, \lambda_{ps}$$

A beta factor of 0.1 has been used in this example. The transition rates can be calculated with the formulas listed above and the data provided in table 8.5. The results are presented in the last three rows of table 8.5. It should be emphasized that the data presented in this paragraph is for illustrative purpose only and has no practical value.

Table 8.5: Component failure data example 2.

Component	Failure rate (-/hour)	Test period (hour)
Pressure switch	2.0 E-06	8760
Shut-off valve	5.0 E-06	8760
Solenoid valve	1.0 E-06	8760
Logic-1	8.0 E-08	8760
Logic-2	2.0 E-08	87600
CCF sensors	2.0 E-07	8760
CCF shut-off valves	5.0 E-07	8760
CCF Solenoid valves	1.0 E-07	8760

Remarks:

- It should be emphasized that the data presented in table 8.5 are for illustrative purposes only and cannot be regarded as valid data.
- CCF : Common Cause Failures

Quantification of minimal cut-sets:
The system reliability characteristic for example 2 is the probability of failure on demand. The probability of failure on demand can be calculated by application of the formulas A and B presented in the appendix of chapter 9 "Quantification of minimal cut-sets". The results are:

Contributions:

First-order minimal cut-sets	: 4.7260E-03	82.20%
Second-order minimal cut-sets	: 1.0232E-03	17.80%
Higher-order minimal cut-sets	: 0.0	0.00%
Total	: 5.7491E-03	

The separate contributions of each cut-set are:

```
    Cut-set             Contribution    Per cent   Formula

1   CCF_SH_VALVES       2.19E-03        38.04      Al
2   CCF_SENSORS         8.76E-04        15.23      Al
3   LOGIC2_FAILS        8.75E-04        15.23      Al
4   SH_VAL1_FAILS       6.39E-04        11.12      B1
    SH_VAL2_FAILS
5   CCF_SOL_VALVES      4.38E-04        7.62       Al
6   LOGICI_FAILS        3.50E-04        6.09       Al
7   SH_VAL1_FAILS       1.28E-04        2.22       B1
    SOL_VAL2_FAILS
8   SOL_VAL1_FAILS      1.28E-04        2.22       B1
    SH_VAL2_FAILS
9   SENSORI_FAILS       1.02E-04        1.78       B1
    SENSOR2_FAILS
10  SOL_VAL1_FAILS      2.56E-05        0.44       B1
    SOL_VAL2_FAILS
```

Importance analysis:

To determine the dominant contributors to the probability of failure on demand, the Fussel Vesely importance will be calculated. The Fussel Vesely importance measure of a component X is defined as the fractional contribution to the probability of failure on demand by component X.

The Fussel Vesely importance can be expressed as follows (see chapter 15):

$$I_{FV}(X) \quad = \quad \frac{PFD - PFD\ (X = 0)}{PFD} \tag{8.5}$$

PFD : Calculated probability of failure on demand

PFD(X=0) : Calculated probability of failure on demand, given that the failure rate of component X is assumed to be zero.

The results of the importante analysis are:

```
    Basic Event       Fussel-Vesely

1   CCF_SH_VALVES       3.80E-01
2   CCF_SENSORS         1.52E-01
3   LOGIC2_FAILS        1.52E-01
4   SH_VAL1_FAILS       1.33E-01
5   SH_VAL2_FAILS       1.33E-01
6   CCF_SOL_VALVES      7.62E-02
7   LOGICI_FAILS        6.09E-02
8   SOL_VAL1_FAILS      2.67E-02
9   SOL_VAL2_FAILS      2.67E-02
10  SENSORI_FAILS       1.78E-02
11  SENSOR2_FAILS       1.78E-02
```

From the results it can be concluded that the dominant contributors are: dependent failure of both shut-off valves, the logic that is tested once every ten years, dependent failure of the pressure switches and independent failure of the shut-off valves.

Interpretation of results:
The calculated probability of failure on demand of the high-integrity pressure protection system is equal to 5.5 E-03 per demand. The results are dominated by dependent failures and failure of the shut-off valves.

8.5.3 Example toss of containment due to corrosion

In this examples a generic fault tree is presented which describes the toss of containment due to corrosion. The fault tree is depicted in appendix 8-C. The basic events in this fault tree [8.9] can be described as follows [8.8]:

- Protection not maintained:
  This basic event applies to both the inside and the outside of the containment. The selected protection requires maintenance. This can be necessary because of wear and tear of the protection or because the protection is not fully resistant to the corrosive environment. When the protection is not maintained the containment wilt start to corrode eventually leading to loss of containment.

- Accelerated deterioration of protection:
  The basic event applies to both the inside and the outside of the containment. Due to some change in the environment or the process, the quality of the protection changes rapidly. This can be an unwanted reaction or introduction of a wrong chemical or external contact with chemicals. The accelerated deterioration is not detected in time because it is unforeseen. Losing the protection leads to corrosion of the containment and eventually loss of containment.

- Installation error:
  The basic event applies to both the inside and the outside of the containment. Due to an installation error the wrong material is used for protection giving an unsuitable type of protection. Most likely it will be using the wrong type of material, but it can also be a wrong form of application of the material to the containment. The error is not detected and leads to loss of containment.

- Design error
  The material of the containment requires protection. The basic event applies to both the inside and the outside of the containment. Due to a design error the wrong material is used for protection giving an unsuitable type of protection. It is most likely, that in the design phase the aspect of corrosion is treated well enough. The error is not detected and leads to loss of containment.

- Damaged
  The basic event applies to both the inside and the outside of the containment. The protection is damaged, for instance by impact of the outside of the containment, or impact by a stirring device on the inside of an enamel lined reactor. The protection is not replaced or repaired or by neglecting it or by not knowing that the damage has occurred. So in case damage can occur, inspection is necessary.

- Containment not maintained
  The containment is not protected against corrosion. The basic event applies to both the inside and the outside of the containment. Choosing not to protect the equipment can be for economie reasons, because the corrosion is very slow or can easily be repaired. When containment in that case is not properly maintained it can lead to loss of containment.

- Changes in external environmental accelerate corrosion
  The containment is not protected against corrosion. The basic event applies to the outside of the containment. Some change in the external environment causes an accelerated corrosion. This can be caused by for instance emissions of a neighbouring plant or an incident in the near environment. The accelerated corrosion is not accounted for and will lead to loss of containment.

- Installation error
  The basic event applies to both the inside and the outside of the containment. An accelerated corrosion takes place because of an installation error. Often it will be installing the wrong material. The mistake is not detected and leads to loss of containment. An example is galvanic corrosion which occurs when different kinds of metal are in direct contact. Another example is installing an unsuitable metal type that looks very similar to the type the design specifies.

- Design error
  The containment is not protected against corrosion. The basic event applies to both the inside and the outside of the containment. An accelerated corrosion takes place because of a design error. Often it will be a selection of wrong material due to lack of knowledge of the properties of the material.

- Caused by other agents
  The basic event applies to the inside of the containment. An agent that should not have been brought in the containment is brought in and leads to accelerated corrosion and subsequently loss of containment. Also the agent can deliberately be brought in the containment, but knowledge of corrosive properties was insufficient.

- Caused by product
  The basic event applies to the inside of the containment. The accelerated corrosion is caused by a product that is intended to be in the containment and usually is. Accelerated corrosion can than occur of instance by an increased temperature. The temperature is above the intended of normal level. This does not affect the containment, but gives in increased corrosion rate, leading to loss of containment.

8.6 COMPUTER PROGRAMS

A large assortment of computer codes exist to perform fault tree analyses. Important capabilities to be considered by a fault tree analysis code are:

- Is the code able to determine minimal cut sets?
- Is the code able to quantify minimal cut sets?
- Is the code able to generate a plot of the fault tree?

- Which reliability models to calculate basic event unavailabilities and reliabilities are supported by the code?
- What is the maximum size of the fault tree which can be handled by the code?
- What are the capabilities of the code to perform an uncertainty, sensitivity and importance analysis?

One of the most advanced code developed in Europe is RISK SPECTRUM (reference [8.7]). Well-known codes developed in the United States of America are the NUPRA code (reference [8.6]) and the CAFTA code (reference [8.5]). All three codes support as well fault tree analysis as event tree analysis and have plotting capabilities and support importance and uncertainty analyses.

The FTA code developed by KEMA supports cut set determination, cut set quantification and uncertainty and importance analyses. Sensitivity analyses can be performed by manually changing the input parameters and requantification of the fault tree (see reference [8.4]).

8.7 REFERENCES

[8.1] Fault Tree Handbook
U.S. Nuclear Regulatory Commission NUREG-0492, January 1981.

[8.2] Procedures for conducting probabilistic safety assessment of nuclear power plants
(Level I), Safety series No. 50-P-4
IAEA, Vienna 1992

[8.3] Henley E.J. & Kumamoto H.
Probabilistic Risk Assessment; Reliability Engineering, design and Analysis, IEEE Press, New York. 1992

[8.4] Manual Fault Tree Analysis code FTA,
J.C.H. Schüller, KEMA Nuclear, 40721-NUC-94-4582, 11 January 1995.

[8.5] CAFTA User's manual,
Science Applications International Corporation, 4920 El Camino Real, Los Altos, California 94022, USA.

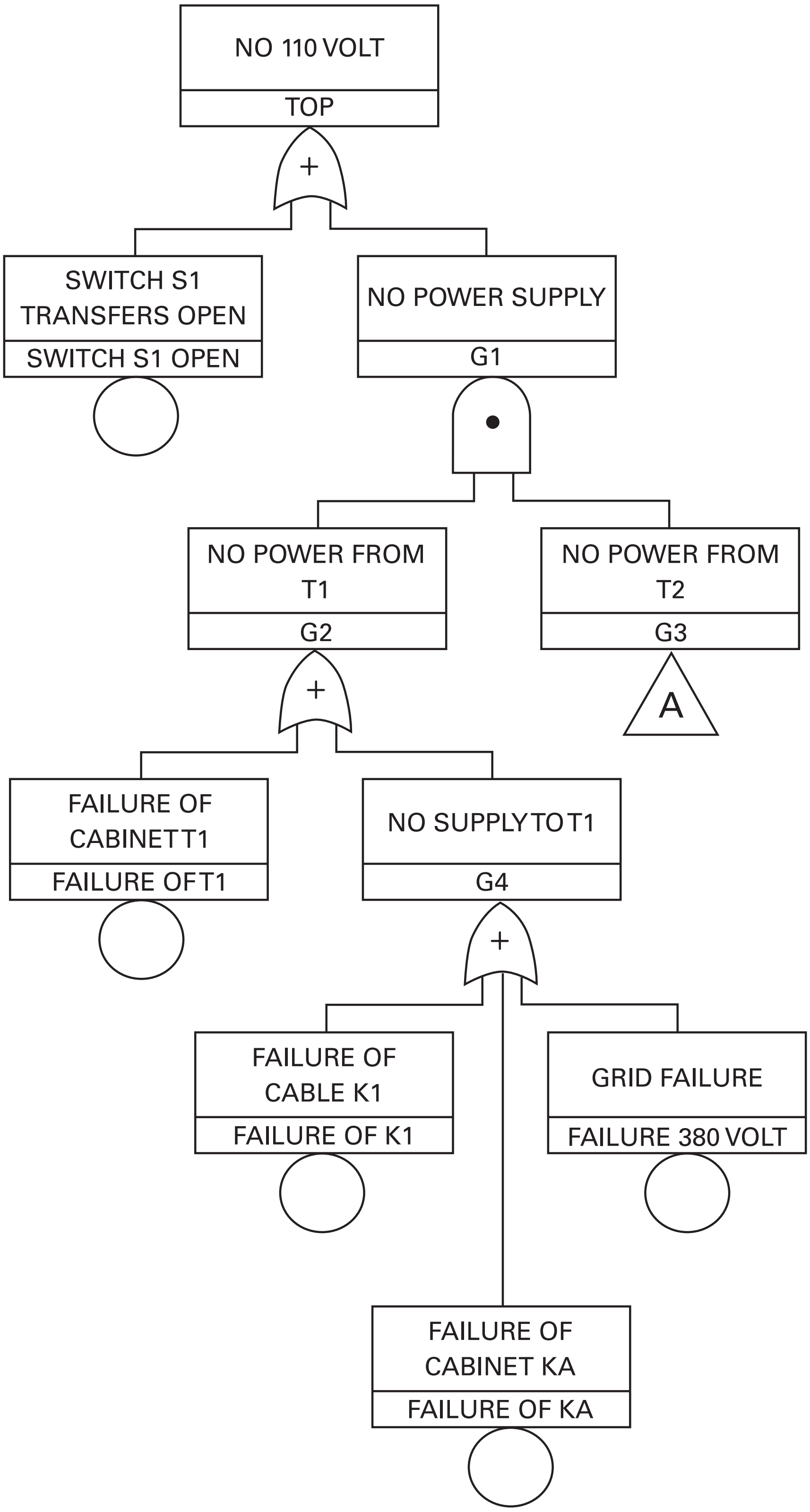
[8.6] NUPRA User's manual,
Halliburton NUS Corporation, 910 Clopper Road, P.O. Box 6032, Gaithersburg, MD 20877-0962, USA.

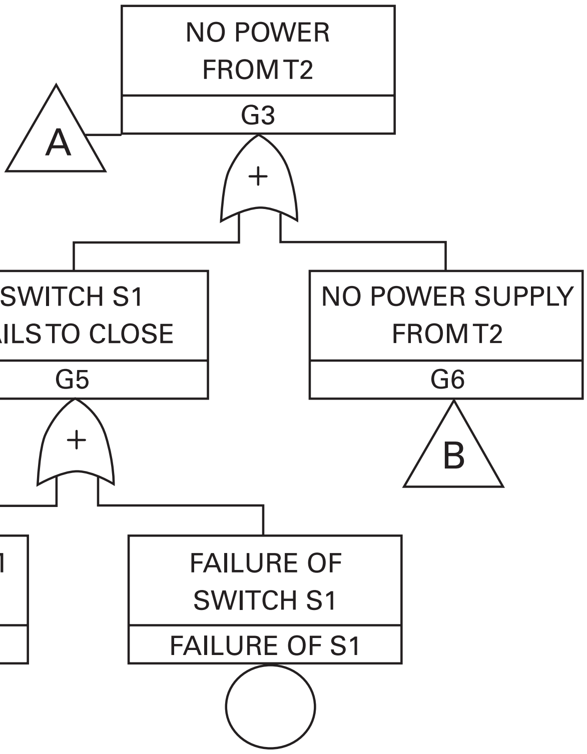
[8.7] RISK SPECTRUM, Professional Risk & Reliability Software, RELCON AB, P.O. Box 1288, S-17225 Sundbyberg, Sweden.

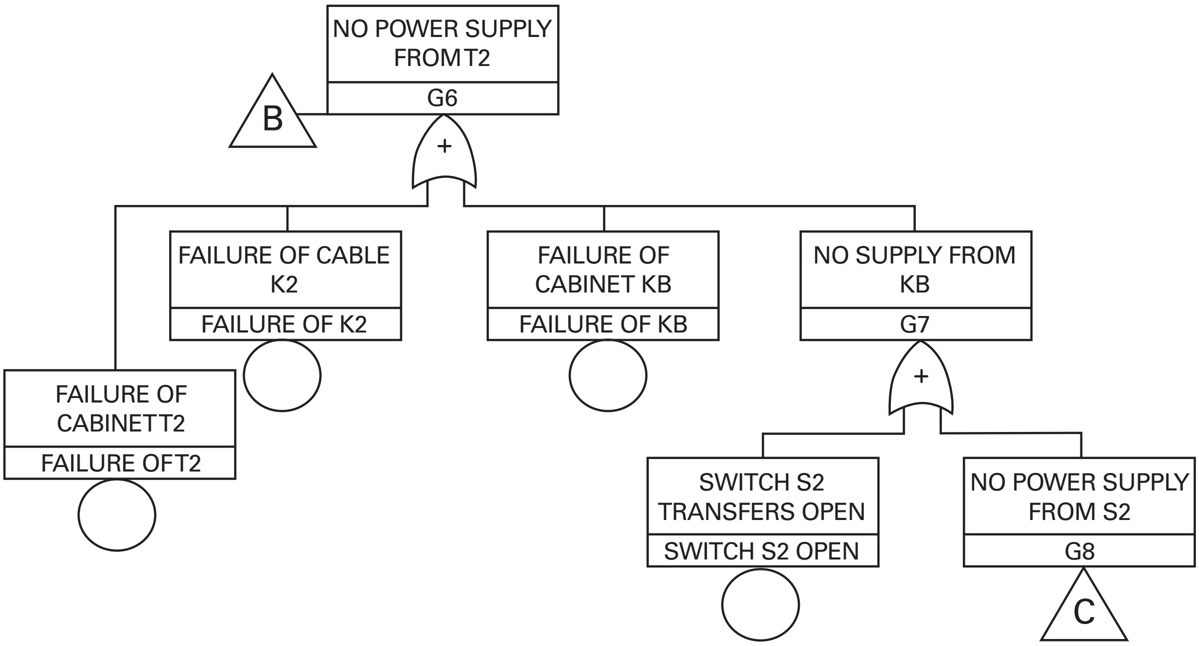
[8.8] AVRIM 2, Assessment and inspection method, Ministry of Social Affairs and Employment, Save, version 1.0 1996.

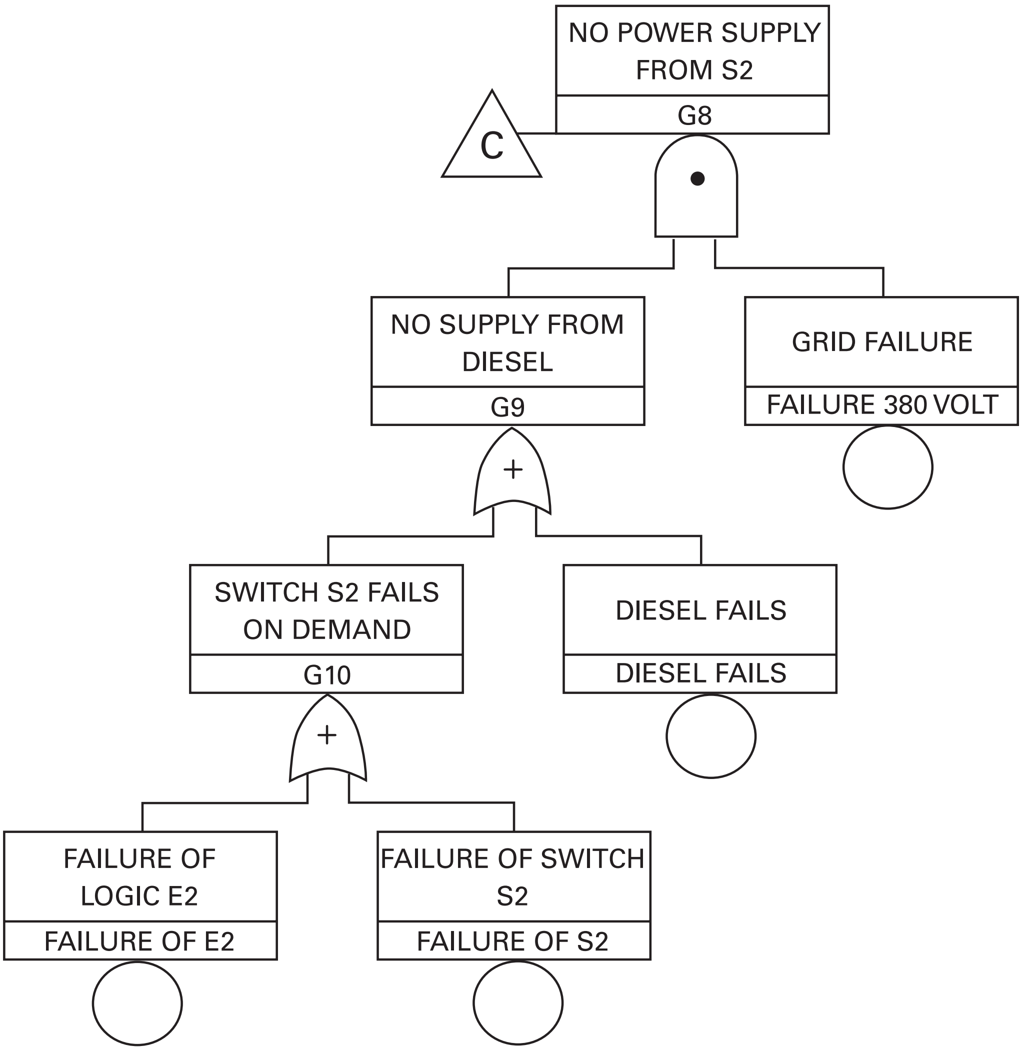
[8.9] Generic Fault Trees and the Modeling of Management and Organisation, R.van der Mark, Delft University of Technology, August 25, 1996, Delft.

Appendix 8-A: Fault tree of example 1.

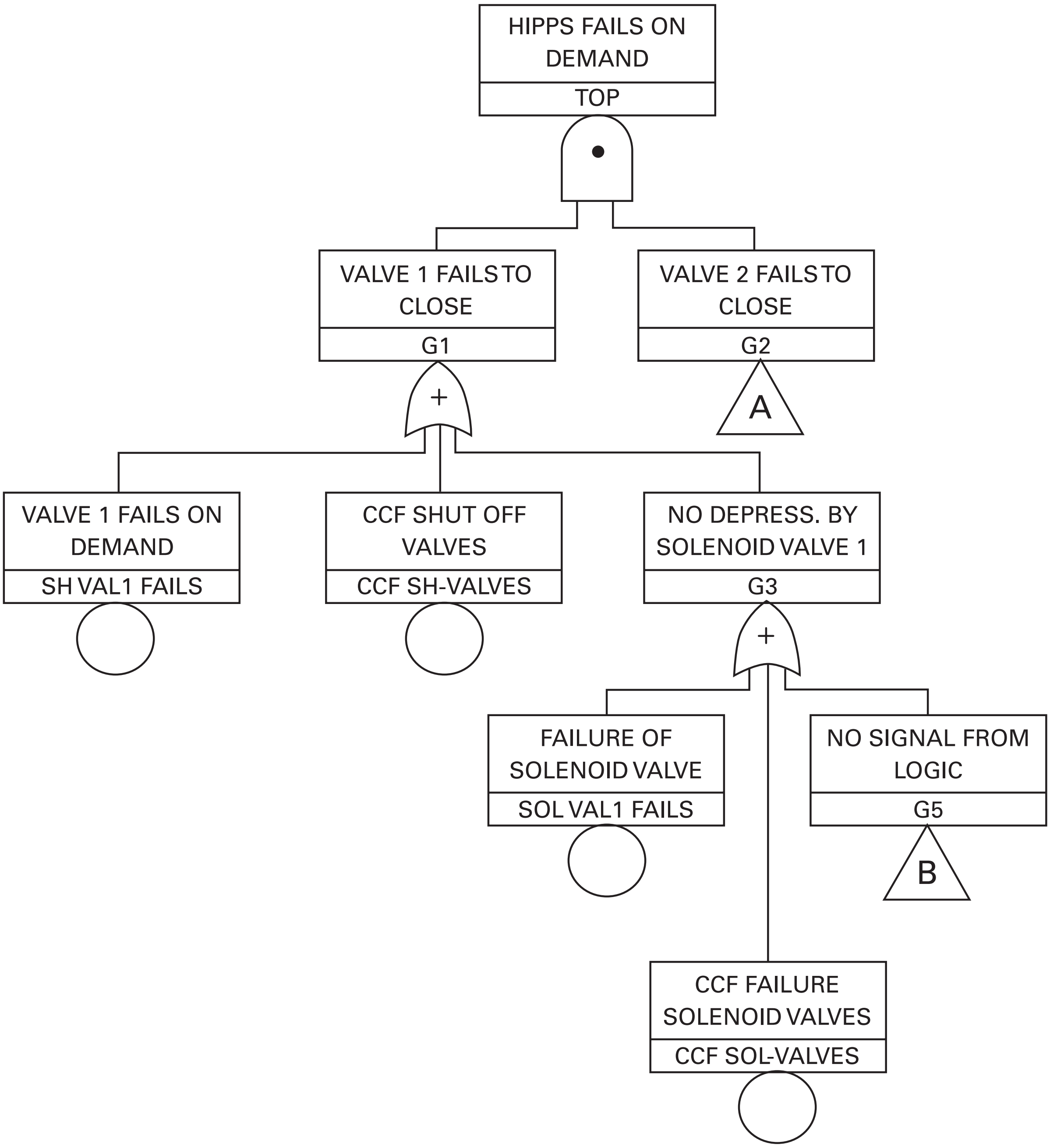


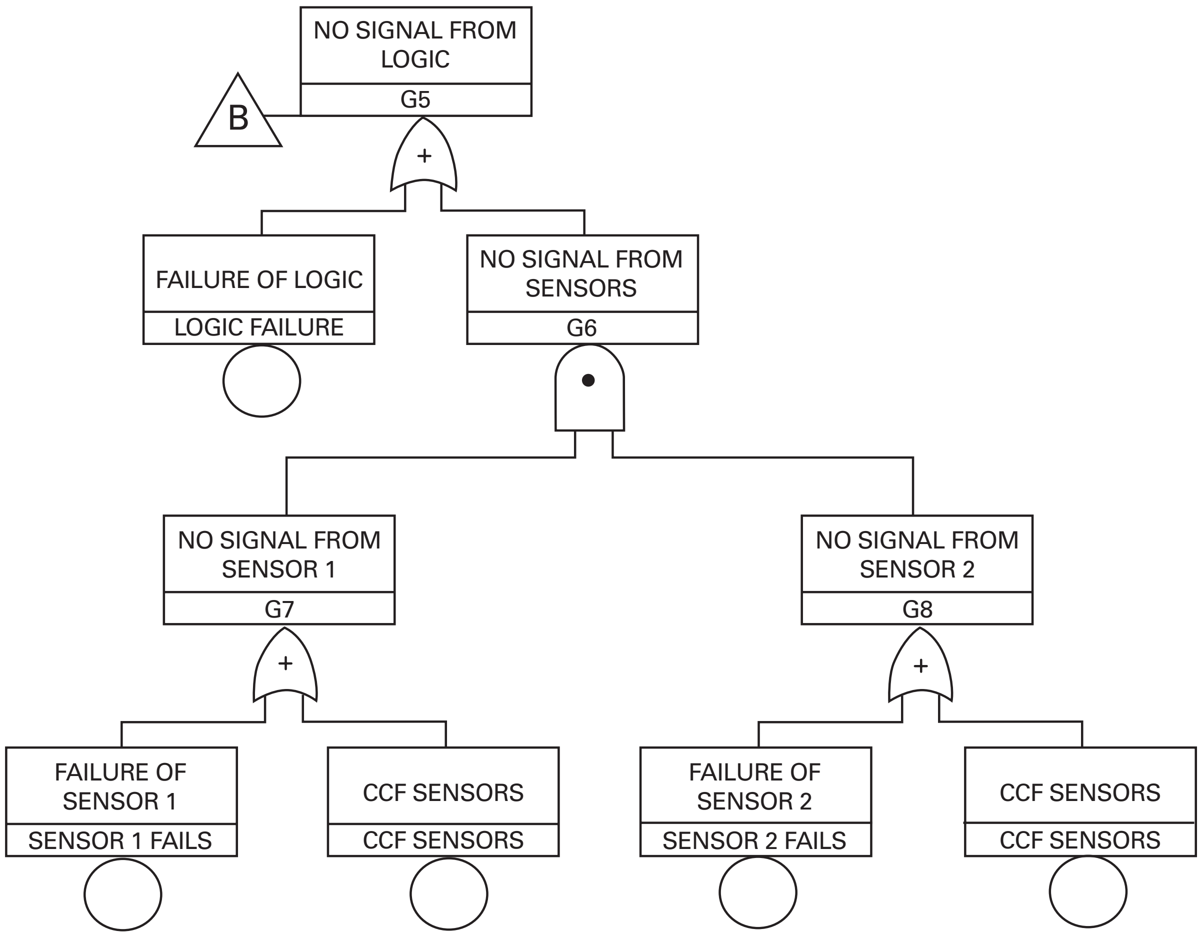

NO POWER FROM T2
G3
A
+
SWITCH S1 FAILS TO CLOSE
G5
NO POWER SUPPLY FROM T2
G6
B
+
NO POWER FROM E1
FAILURE OF E1
FAILURE OF SWITCH S1
FAILURE OF S1

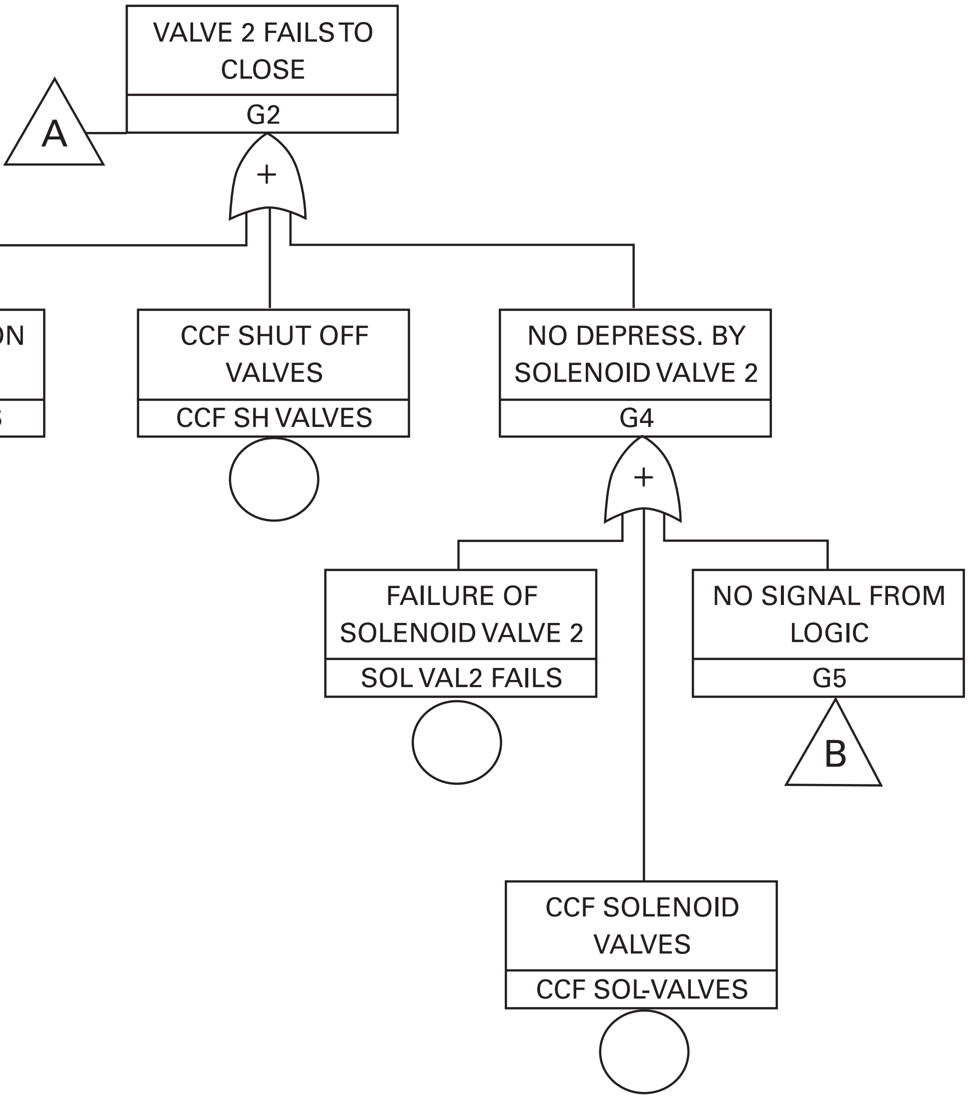

NO POWER SUPPLY FROM T2
G6
B
+
FAILURE OF CABINET T2
FAILURE OF T2
FAILURE OF CABLE K2
FAILURE OF K2
FAILURE OF CABINET KB
FAILURE OF KB
NO SUPPLY FROM KB
G7
+
SWITCH S2 TRANSFERS OPEN
SWITCH S2 OPEN
NO POWER SUPPLY FROM S2
G8
C


NO POWER SUPPLY FROM S2
G8
C
NO SUPPLY FROM DIESEL
G9
GRID FAILURE
FAILURE 380 VOLT
SWITCH S2 FAILS ON DEMAND
G10
DIESEL FAILS
DIESEL FAILS
FAILURE OF LOGIC E2
FAILURE OF E2
FAILURE OF SWITCH S2
FAILURE OF S2

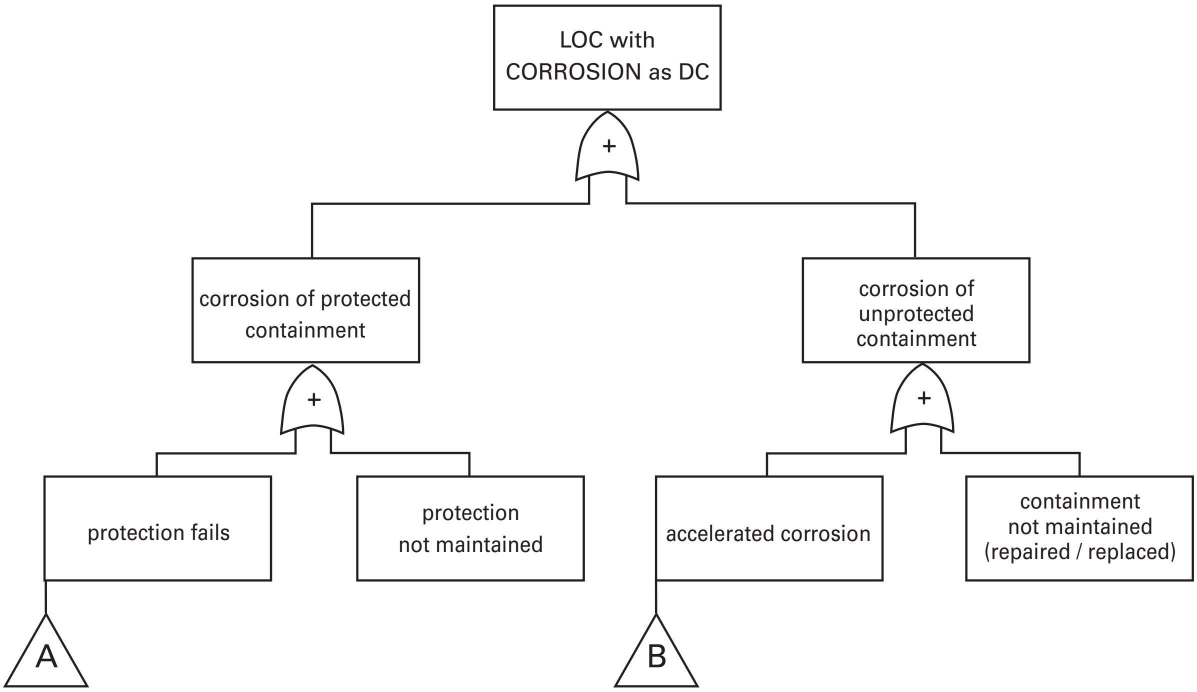
Appendix 8-B: Fault tree of example 2.

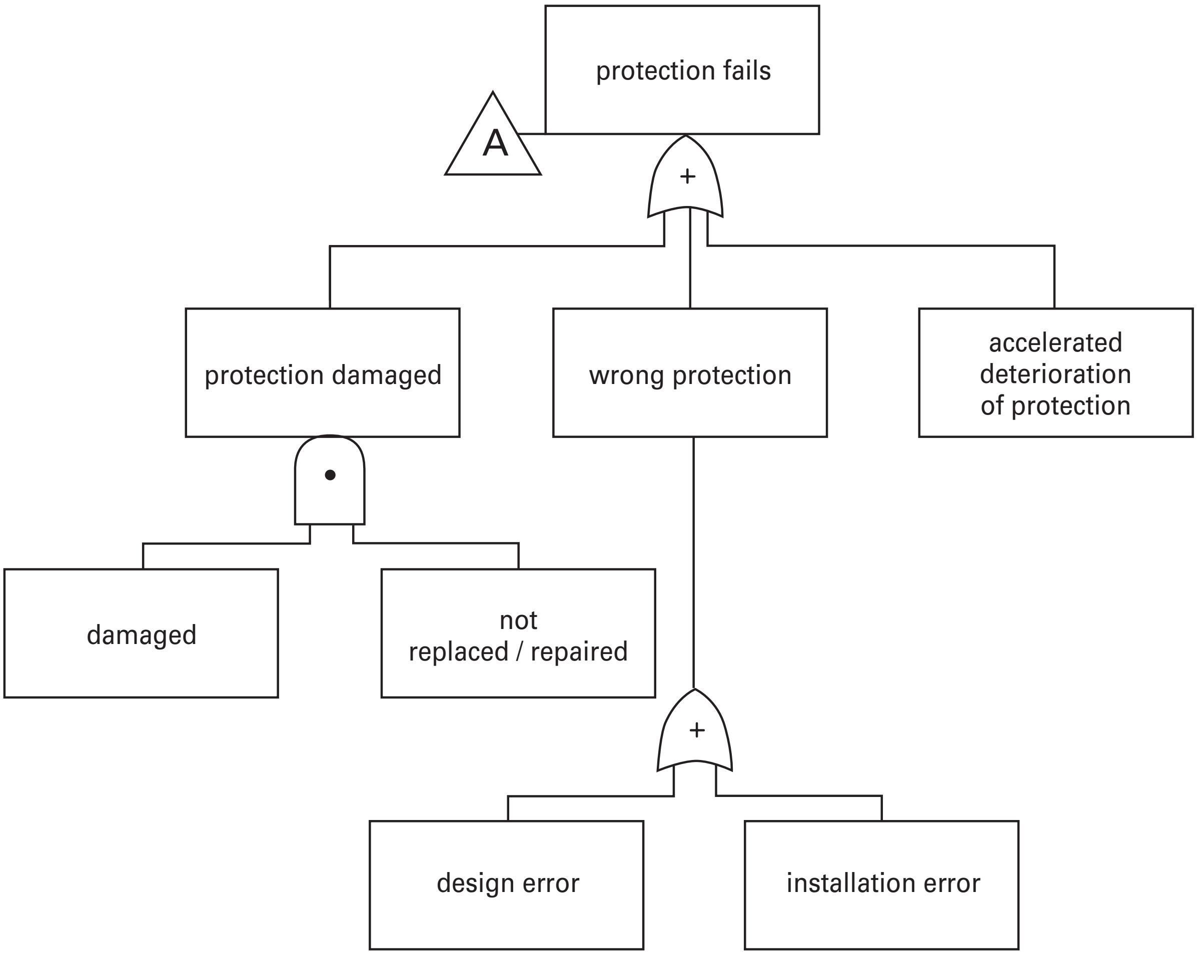


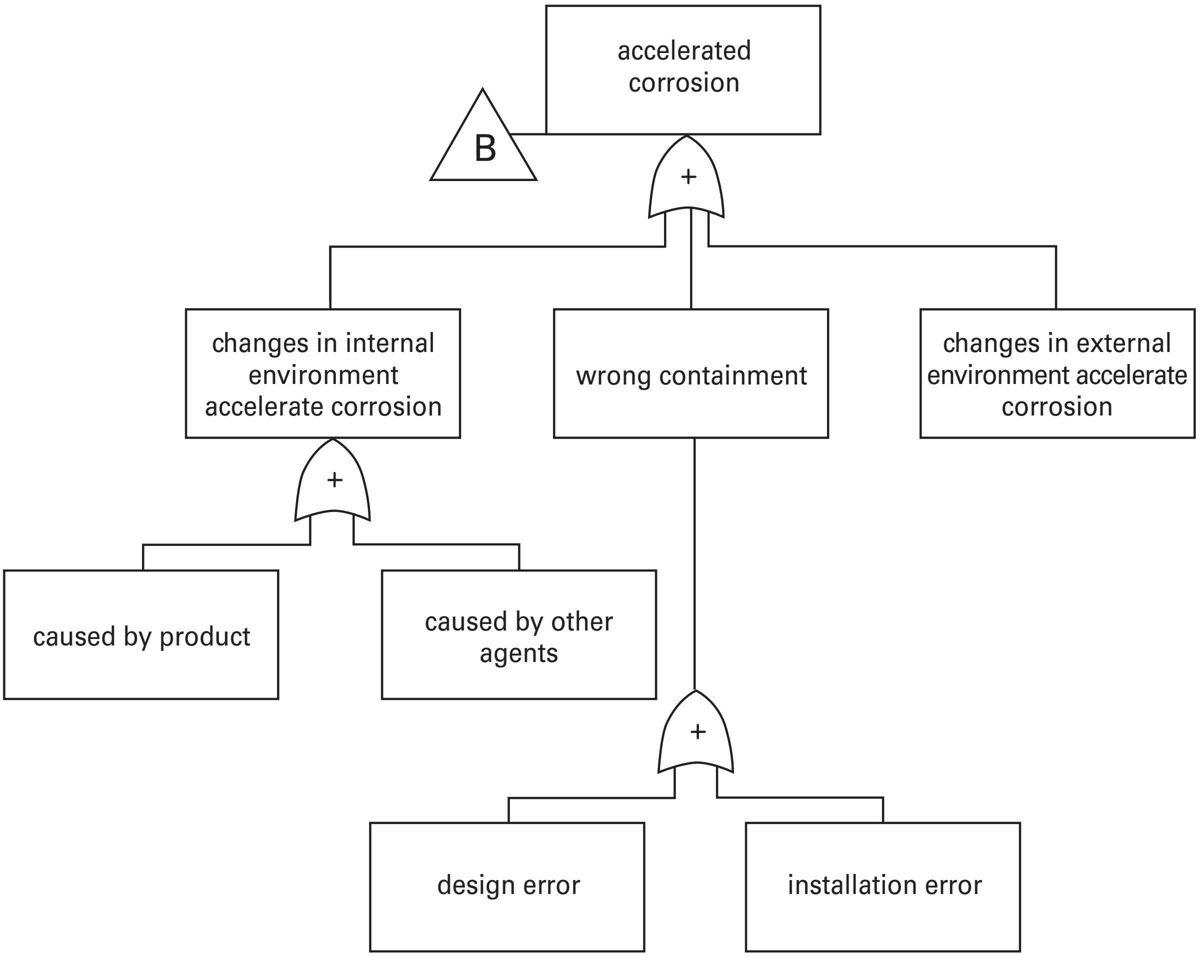

NO SIGNAL FROM LOGIC
G5
B
+
FAILURE OF LOGIC
LOGIC FAILURE
NO SIGNAL FROM SENSORS
G6
NO SIGNAL FROM SENSOR 1
G7
+
NO SIGNAL FROM SENSOR 2
G8
+
FAILURE OF SENSOR 1
SENSOR 1 FAILS
CCF SENSORS
CCF SENSORS
FAILURE OF SENSOR 2
SENSOR 2 FAILS
CCF SENSORS
CCF SENSORS


VALVE 2 FAILS TO CLOSE
G2
A
+
VALVE 2 FAILS ON DEMAND
SH VAL2 FAILS
CCF SHUT OFF VALVES
CCF SH VALVES
NO DEPRESS. BY SOLENOID VALVE 2
G4
+
FAILURE OF SOLENOID VALVE 2
SOL VAL2 FAILS
NO SIGNAL FROM LOGIC
G5
B
CCF SOLENOID VALVES
CCF SOL-VALVES

Appendix 8-C: Fault tree of example 3.


LOC with CORROSION as DC
+
corrosion of protected containment
corrosion of unprotected containment
+
+
protection fails
protection not maintained
accelerated corrosion
containment not maintained (repaired / replaced)
A
B


protection fails
A
+
protection damaged
wrong protection
accelerated deterioration of protection
•
damaged
not replaced / repaired
+
design error
installation error


accelerated corrosion
B
+
changes in internal environment accelerate corrosion
wrong containment
changes in external environment accelerate corrosion
+
caused by product
caused by other agents
+
design error
installation error

QUANTIFICATION OF MINIMAL CUT SETS

CONTENTS **Page**

9.1 INTRODUCTION

A minimal cut set consists of a combination of basic events (component failures) that constitute the smallest combinations of basic events causing occurrence of the undesired event. This undesired event can be the top event of a fault tree or a specific accident sequence. In case the undesired event is an accident sequence one of the basic events in the cut set represents the occurrence of the initiating event of the corresponding accident sequence.

The quantification technique presented in this chapter is focused on quantification of cut sets generated by fault trees; however accident sequences can be quantified in the same way. Each accident sequence represents a logical AND gate of the initiating event and subsequent safety system failures. Thus, each accident sequence can be thought of as a separate fault tree with the accident sequence description as the top event, followed by an AND gate containing the initiating event and all the contributing safety system failures.

A fault tree analysis can be divided into two parts, a qualitative part and a quantitative part. The outcome of the qualitative part of a fault tree analysis are the minimal cut sets.
The quantitative part deals with the quantification of those minimal cut sets. Quantification of minimal cut sets consists of the following basic tasks:

Task 1: Select or derive a quantification formula for each of the minimal cut sets. The quantification formula must take into account test, repair and maintenance procedures. Failure to observe the proper handling procedure for the components in practice is one of the main sources of errors in cut set quantification.

Task 2: Task two consists of collecting all failure, repair, test and maintenance data for components belonging to the minimal cut set which has to be quantified.

Task 3: Performance of the calculations by applying the right formula and using the component failure data.

The theory for cut set quantification presented in this chapter is based on the information provided in references [9.1], [9.2], [9.3], [9.4] and [9.5]. To understand the theory presented in this chapter, one must be familiar with the theory presented in the chapters: probability theory and reliability theory.

In appendix 9-A a number of standard formulas to quantify first and second order minimal cut sets are presented. Formulas are given to quantify unavailability and the failure occurrence rate of minimal cut sets.

Other methods that can be used for cut set quantification are the Monte Carlo simulation and Markov Processes. The Markov Processes will be explained in chapter 1 1. For a short explanation of Monte Carlo simulation, reference is made to chapter 15 on importance, sensitivity and uncertainty analysis.

In this chapter always the dimension per hour will be applied for those parameters which has the dimension per unit time.

9.2 NOMENCLATURE

			Dimension
λ	-	failure rate	-/hour
ω	-	failure occurrence rate	-/hour
μ	-	repair rate	-/hour
f	-	failure density	-/hour
τ	-	test duration with the component not being available	hour
θ	-	repair duration	hour
Q	-	probability of failure per demand	-
P	-	probability	-
F(0,t)	-	unreliability at time t	-
N(0,t)	-	expected number of failures during (0,T)	-
U	-	time-average unavailability	-
U(t)	-	instantaneous unavailability at time t	-
T	-	test period	hour
T_P	-	the time during which a failure can occur and the state of the component is unknown	hour
MTTF	-	mean time to failure	hour
MDT	-	mean down time	hour
MTBF	-	mean time between failures	hour
MTTR	-	mean time to repair	hour

<u>Subscript</u>

mcs	- applicable to cut sets
sys	- applicable to system
fld	- unavailability due to failure on demand
unr	- unavailability due to unrevealed failure
rep	- unavailability due to repair
tst	- unavailability due to testing

9.3 BASIC FORMULAS FOR CUT SET GUANTIFICATION

In this paragraph basic formulas will be provided that can be used to derive formulas for cut set quantification. To derive the various formulas a number of restrictive assumptions have to be made. These assumptions are:

Restrictive assumptions:

- The failure rate is assumed to be constant in time.

- The average repair and test duration are assumed to be constant in time.

- Redundant components are subjected immediately to testing, one after the other, and are always tested in the same sequence. If the component that is tested first is found to have failed, will be repaired before the redundant component is tested.

- The mean time to failure is assumed to be much longer than the mean time to repair.

- The formulas derived for periodically tested stand-by components are only valid if: $\lambda t < 0.01$. - The test period is assumed to be constant.

- The test procedure always results in proper classification of the component status. This implies that if a component has failed, this will always be detected in the test and therefore the human error probability is assumed to be zero.

- It is assumed that the number of tests do not influence the failure behavior of the component.

- The test duration is negligible compared with the test period.

- Test and repair are completed before the next scheduled test and they restore the component in as-good-as-new condition.

- In case of unavailability due to a revealed fault, it is assumed that repair will start just after occurrence of the failure. Waiting time and logistic time are assumed to be incorporated into the repair duration.

- In case of the probability of failure per demand model it is assumed that during one test period only one demand can occur. For most safety applications this is in accordance with normal practice.

- For higher order cut sets it is assumed that component failures are independent. In a fault tree analysis this corresponds to independent occurrence of various basic events. Practice, however, shows that there are limits to this independence. In advanced systems designed with a high theoretical reliability common-cause failures are often the major contributors to system unavailability. In these cases a detailed common-cause failure analysis has to be performed.

- The formulas derived in this chapter are based on a number of conservative assumptions (see reference [9.5]). In general, the over prediction can become significant if:
  - the unavailability of an on-line repairable component is evaluated to be less than twice the mean repair time
  - the unavailability of a periodically tested stand-by component is evaluated to be more than one tenth of the mean time to failure.
  - the cut set unavailabilities are greater than 0.1.

9.3.1 Failure occurrence rate of a minimal cut set: w ncjt)

All parameters applicable to a minimum cut set will be identified with the subscript mcs. To calculate the failure occurrence rate of a second order minimal cut set consider the following minimal cut set:

$$C = A\ B \tag{9.1}$$

This minimal cut set wilt occur in time interval (t,t+dt) if component B is not available at time t and component failure of A occurs during the time interval (t,t+dt), or if component A is not available at time t and component failure of B occurs during time interval (t,t+dt). This can be formulated as follows:

$$\begin{aligned} &\text{P [C fails during } (t,t+\Delta t)] = \\ &\qquad \text{P[A fails during } (t,t+\Delta t)]\ \text{P[B unavailable at t]} + \\ &\qquad \text{P[B fails during } (t,t+\Delta t)]\ \text{P[A unavailable at t]} \end{aligned} \tag{9.2}$$

In the expression above the higher-order terms can be neglected because these are mutually exclusive events. The probability of occurrence of basic event A or B during time interval (t,t+Δt) is given by:

$$\begin{aligned} &\text{P[A occurs during } (t,t+\Delta t)] = \omega_A(t)\ \Delta t \\ &\text{P[B occurs during } (t,t+\Delta t)] = \omega_B(t)\ \Delta t \end{aligned} \tag{9.3}$$

The probability of A and B not being available at time t is given by:

$$\begin{aligned} &\text{P[A unavailable at t]} = U_A(t) \\ &\text{P[B unavailable at t]} = U_B(t) \end{aligned} \tag{9.4}$$

Substitution of equations (9.3) and in (9.4) in equation (9.2) results in:

$$\text{P[C occurs during } (t,t+\Delta t)] = \omega_A\ \Delta t\ U_B(t) + \omega_B\ \Delta t\ U_A(t) \tag{9.5}$$

Dividing the left-hand side of equation (9.5) by Δt gives the failure occurrence rate of a second-order minimal cut set C.

$$\omega_{mcs}(t) = \omega_A (t)\ U_B (t) + \omega_B (t)\ U_A (t) \tag{9.6}$$

Generalization of equation (9.6) gives the general formula to calculate the failure occurrence rate of a higher-order minimal cut set:

$$\omega_{mcs}(t) = \sum_{j=1}^{n} \omega_j \prod_{\substack{k=1 \\ k\neq j}}^{n} U_k(t) \tag{9.7}$$

n = number of basic events.

9.3.2 The expected number of failures of a minimal cut set: $N_{mcs}(0,t)$

The general expression for the expected number of failures of a minimal cut set in time period (0,t) is given by:

$$N_{mcs}(0,t) = \int_0^t \omega_{mcs}(t)\ dt \tag{9.8}$$

In case of a constant failure occurrence rate $\omega_{mcs}(t)$, formula (9.8) can be rewritten as:

$$N_{mcs}(0,t) = \omega_{mcs}\ t \tag{9.9}$$

9.3.3 Instantaneous unavailability of a minimal cut set: $U_{mcs}(t)$

Consider the second-order minimal cut set:

$$C = A\ .\ B \tag{9.10}$$

The minimal cut set C is unavailable at time t if basic event A is unavailable at time t and basic event B is unavailable at time t. In case the unavailability of both components is independent, the unavailability of the minimal cut set can be written as:

$$\begin{aligned} P\ (C \text{ unavaible}) &= P\ (A \text{ unavailable} \cap B \text{ unavailable}) \\ &= P\ (A \text{ unavailable})\ P\ (B \text{ unavailable})\ (A \text{ and } B \text{ independent}) \end{aligned} \tag{9.11}$$

$$U_{mcs}(t) = U_A(t)\ U_B(t) \tag{9.12}$$

Transition to the correct symbols for unavailability results in:

Equation (9.12) can be generalized for higher order minimal cut sets as follows:

$$U_{mcs}(t) = \prod_{j=1}^{n} U_j (t) \tag{9.13}$$

n = number of basic events

9.3.4 Time-averaged unavailability of a minimal cut set: U_{mcs}

The general expression for the time-averaged unavailability is given by:

$$U_{mcs} = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} U_{mcs}(t)\, dt \tag{9.14}$$

Substitution of equation (9.13) in equation (9.14) gives the expression to calculate the time-averaged unavailability of a higher-order minimal cut set:

$$U_{mcs} = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \prod_{j=1}^{n} U_j(t)\, dt \tag{9.15}$$

n = number of basic events.

It must be emphasized that equation (9.15) is only valid in case the failure occurrences of the basic events are independent.

Only in case that the instantaneous unavailabilities of the various components are independent in time, the time-averaged unavailability of the cut set can be calculated by multiplication of the time-averaged unavailabilities of the individual components. In formula:

$$\begin{aligned} U_{mcs} &= \prod_{j=1}^{n} \left[\frac{1}{t_2 - t_1} \int_{t_1}^{t_2} U_j(t)\, dt \right] \\ &= \prod_{j=1}^{n} U_j \quad \text{(only if } U_j \text{ j=1,n are time-independent)} \end{aligned} \tag{9.16}$$

n = number of basic events.

9.3.5 Mean down time of a minimal cut set: Mean Down Time (MDT_{mcs})

The time-averaged unavailability of a minimal cut set for steady-state conditions can be written as:

$$U_{mcs} = \frac{MDT_{mcs}}{MTTF_{mcs} + MDT_{mcs}} \tag{9.17}$$

By approximation one can write:

$$MTTF_{mcs} \approx \frac{1}{\omega_{mcs}} \tag{9.18}$$

Substitution of formula (9.18) in formula (9.17), and neglection of MDT_{mcs} in relation to $MTTF_{mcs}$ results in the following expression to calculate the mean down time of a cut set:

$$MDT_{mcs} \approx \frac{U_{mcs}}{\omega_{mcs}} \tag{9.19}$$

9.3.6 The quantification of system parameters

Quantification of system reliability parameters can be done by applying the rare event approximation. To explain the rare event approximation, consider a system consisting of two components in series. The top event of this system can be written as two first order minimal cut sets (A and B). To calculate the probability of occurrence of the top event the probability law has to be used:

$$P(TOP) = P(A) + P(B) - P(A \cap B) \tag{9.20}$$

The rare event approximation consists of only keeping the first contribution, which is the sum of the individual cut set probabilities. This approximation will always be conservative and is generally reasonably accurate (for realistic components the probabilities P(A) and P(B) will be very small). So application of the rare event approximation holds:

$$P(TOP) \approx P(A) + P(B) \tag{9.21}$$

In general this will be valid. Besides one can prove that the neglected part has a negative contribution to the probability of occurrence of the top event. Thus application of the rare event approximation implies that a conservative result is generated.

The failure occurrence rate of a system can be calculated using the formula:

$$\omega_{sys}\,(t) \approx \sum_{i=1}^{m} \omega_i\,(t) \tag{9.22}$$

m = number of minimal cut sets

The unavailability of a system is given by the expression:

$$U_{sys}\,(t) \approx \sum_{i=1}^{m} U_i\,(t) \tag{9.23}$$

The average mean time to failure is given by:

$$MTTF_{sys} = \frac{1}{\omega_{sys}} \tag{9.24}$$

The average down time of the system can be calculated using the formula:

$$MDT_{sys} = \frac{U_{sys}}{\omega_{sys}} \tag{9.25}$$

The mean time between failures of a system is given by:

$$MTBF_{sys} = MTTF_{sys} + MDT_{sys} \tag{9.26}$$

9.4 QUANTIFICATION OF THE UNAVAILABILITY OF FIRST ORDER MINIMAL CUT SETS

9.4.1 Mode of operation

During the process of deriving formulas for cut set quantification, one must be sure to describe the failure behavior of the component in practice as accurately as possible. In this respect it is important to make a distinction between the different modes of operations of the component. Two modes of operation are usually identified, viz. the stand-by mode of operation and the continuons mode of operation.

Stand-by mode of operation:
A component in a stand-by mode of operation is mostly part of a safety system. The major reliability measure of interest for a safety system is unavailability on demand. A component in a stand-by mode of operation can be unavailable due to unrevealed faults. For this reason a system in a stand-by mode of operation has to be tested periodically. If the component is tested periodically, the unavailability becomes a periodic function of time and the average unavailability of the component is equal to the average unavailability during the period between tests.

An alternative model that has been proposed for components during the stand-by period is that of constant unavailability or constant failure probability per demand. This model assumes that the failure of the component is only caused by immediate influences related to the demand. The unavailability does not change with time, nor is it affected by tests or actual demands. In fact, tests should be avoided if this model holds.

The failure mechanism of most components includes elements of a time dependent process and elements of a demand related process. However, the fractional influence of each is difficult to assess. Moreover, if this dual aspect is introduced in the modeling, very specific data are needed. Studies have not supported such analyses. It is therefore recommended to use a time-dependent model that can include, where quantified on the basis of real data, both time-dependent influences and indirectly demand-related features. The time-dependent feature allows the inclusion in the model of the influence of the frequency of periodic testing.

Continuous mode of operation:
Components in a continuous mode of operation are mostly part of a production unit. The reliability characteristic of interest of such a unit is generally the expected number of failures per time period. Components in a continuous mode of operation can be divided into two main groups: non-repairable components and repairable components.

The following classification can be used to derive formulas for the quantification of first-order minimal cut sets:

- tested stand-by component
- untested stand-by component
- non-repairable component
- on-line repairable component.

For each class of components a quantification formula to quantify a first order minimal cut set will be derived.

9.4.2 **Tested stand-by component.**

These types of components are usually in a stand-by mode of operation and have to be tested periodically to limit the unavailability due to unrevealed faults. If during testing the component is found to be unavailable due to an unrevealed fault, the component will be repaired immediately. Three types of contributions to component unavailability can be identified (see figure 9.1):

- unavailability due to unrevealed faults
- unavailability due to testing or maintenance.
- unavailability due to repair.

If during testing or repair the complete system is taken out of service, the contribution to the unavailability of testing and repair can be dropped. The contribution due to maintenance can be treated similarly as the contribution due to testing of the component.

Contribution due to unrevealed faults:

The contribution due to unrevealed fauits can be derived in two ways. A simple engineering approach can be used or a more sophisticated probabilistic approach. First, the engineering approach will be explained.

Engineering approach:

The contribution to the unavailability due to unrevealed faults can be derived from the formula for unavailability (see chapter 5):

$$U_{unr} = \frac{MDT_{unr}}{MTTF + MDT} \tag{9.27}$$

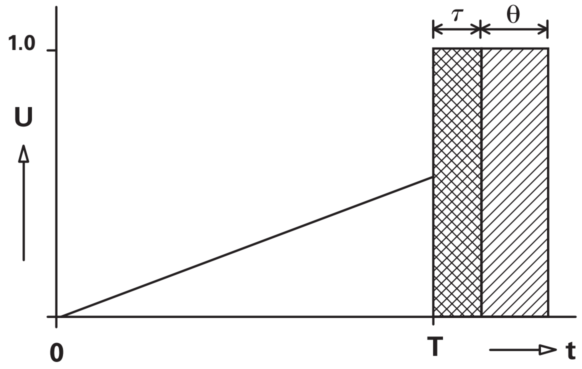


Figure 9.1: Tested stand-by component.

For periodic tests performed at intervals of T, the instantaneous unavailability rises from a low value immediately after a test is performed to a high value immediately before the next test is performed.

Assuming a constant failure rate and assuming that the demand on the component may occur uniformly at any time in the test period, the average down time will be half the test period.

$$MDT_{unr} = \frac{1}{2} \; T \tag{9.28}$$

For components with a constant failure rate the relation between the mean time to failure and the failure rate is given by the expression:

$$\text{MTTF} = \frac{1}{\lambda} \qquad \text{9.29)}$$

Substitution of formulas (9.28) and (9.29) in formula (9.27) gives the contribution to the unavailability due to unrevealed faults.

$$U_{unr} = \frac{1}{2} \lambda T \qquad (9.30)$$

The contribution to the unavailability due to testing is equal to the fraction of the test period which is required for testing:

$$U_{tst} = \frac{\text{Test duration}}{T + \text{Test duration}} \qquad (9.31)$$

In practice the test duration will be much smaller than the test period. For this reason the test duration in the denominator can be neglected in comparison with the test period. The test duration is normally denoted by τ. Formula (9.31) can therefore be written as:

$$U_{tst} = \frac{\tau}{T} \qquad (9.32)$$

The following expression holds for the contribution due to repair.

$$U_{rep} = \frac{\text{MDT}_{rep}}{\text{MTTF} + \text{MDT}} \qquad (9.33)$$

For practical situations the mean down time in the denominator can be neglected in comparison with the mean time to failure. The mean down time is equal to the mean repair time and is denoted by θ. The mean time to failure is given by formula (9.29). The final expression is:

$$\begin{aligned} U_{rep} &= \frac{\theta}{\text{MTTF}} \\ &= \frac{\theta}{\frac{1}{\lambda}} \qquad (9.34) \\ &= \lambda\,\theta \end{aligned}$$

The total unavailability of a single component that might be unavailable due to unrevealed faults is given by the sum of (9.30), (9.32) and (9.34). The resulting expression is:

$$U = \frac{1}{2} \lambda T + \frac{T}{T} + \lambda \theta \tag{9.35}$$

Probabilistic approach:
The general expression for the time-averaged unavailability is given by formula (9.14):

$$U = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} U(t)\, dt \tag{9.36}$$

In this case the upper and lower bounds are:

$$\begin{aligned} t_1 &= 0 \\ t_2 &= T + T + \theta \end{aligned} \tag{9.37}$$

Rewriting of formula (9.37) results in:

$$\begin{aligned} U = & \frac{1}{T + T + \theta} \int_{0}^{T + T + \theta} U(t)\, dt \\ \approx & \frac{1}{T} \int_{0}^{T + T + \theta} U(t)\, dt \\ \approx & \frac{1}{T} \left[\int_{0}^{T} U_{unr}(t)\, dt + \int_{T}^{T+T} U_{tst}(t)\, dt + \int_{T+T}^{T+T+\theta} U_{rep}(t)\, dt \right] \end{aligned} \tag{9.38}$$

The instantaneous unavailabilities due to unrevealed faults and due to testing are given by:

$$\begin{aligned} U_{unr}\,(t) &= \lambda\, t \\ U_{tst}\,(t) &= 1 \end{aligned} \tag{9.39}$$

A test will be followed with a repair of the component if the component has failed during the test period. In practice this wilt not be the case for most test periods. Per test period there is a probability of failure. This probability of failure is equal to λ.T.

The instantaneous unavailability due to repair can now be written as:

$$\begin{aligned} U_{rep}(t) &= P\text{ (repair in test period) } (U_{rep}(t) \mid \text{Given repair}) \\ &= \lambda T\ 1 \qquad (9.40) \\ &= \lambda T \end{aligned}$$

Substitution of the three instantaneous unavailabilities in formula (9.38) and integration gives the expression of the unavailability of a component that can be unavailable due to unrevealed faults (9.35).

9.4.3 Untested stand-by components

If a stand-by component is never tested, the instantaneous unavailability is equal to the probability of failure in time period (0,t):

$$U(t) = 1 - e^{-\lambda\, t} \qquad (9.41)$$

The time-averaged unavailability, within the fault exposure time, can be calculated as follows:

$$\begin{aligned} U &= \frac{1}{T_p} \int_0^{T_p} 1 - e^{-\lambda\, t}\, dt \\ &= 1 - \frac{1 - e^{-\lambda T_p}}{\lambda T_p} \end{aligned} \qquad (9.42)$$

In this formula, the fault exposure time T_p (the time during which a failure can occur and the state of the component is unknown) has to be set equal to the plant life. However, it often happens that the component is indirectly tested or renewed. For example, if the system to which the component belongs is called upon to operate, the state of the untested component might be detectable (operating or failed) when the system is demanded. In this case the mean fault exposure time for the untested component can be set equal to the mean time to challenge the system to which it belongs. In other cases the component might be replaced every time some other tested component is replaced. The mean fault exposure time in that case can be set equal to the mean time to failure of the tested component.

9.4.4 Non repairable component.

This type of component can be used to model a component that has to perform a mission during a certain period of time, the mission time. The basic expression for probability of failure is given by the expression for unreliability (see chapter 5):

$$U = 1 - e^{-\lambda\, T} \qquad (9.43)$$

9.4.5 On line repairable component.

This type of components are normally in a continuous mode of operation. A failure will be detected as soon as it occurs (failure due to a revealed failure). It is said that this type of component can be unavailable due to revealed faults. It is assumed that repair will start immediately after occurrence of a failure. Waiting time and logistic time are expected to be incorporated into the repair duration. The only contribution to unavailability is the unavailability due to repair (see figure 9.2).

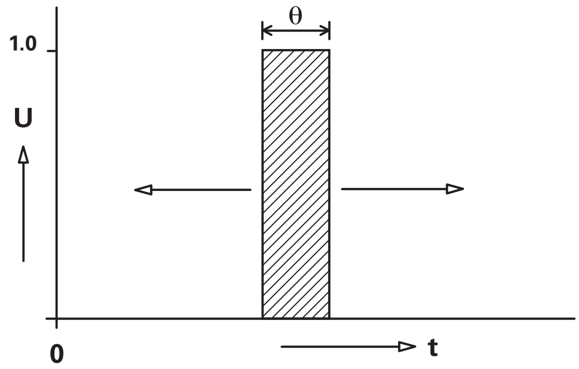


Figure 9.2: On-line repairable component.

The following expression holds:

$$U = \frac{MDT_{Repair}}{MTTF + MDT_{Repair}} \tag{9.44}$$

In the denominator the mean down time due to repair can be neglected in comparison with the mean time to failure. The mean down time due to repair is denoted by θ and the mean time to failure is given by formula (9.29). Substitution in expression (9.44) results in:

$$
\begin{aligned}
U &\approx \frac{\theta}{MTTF} \\
&\approx \frac{\theta}{\frac{1}{\lambda}} \\
&\approx \lambda\,\theta
\end{aligned}
\tag{9.45}
$$

Formula (9.45) gives the unavailability of a component that is unavailable due to revealed faults.

9.4.6 **Probability of failure on demand model.**

Instead of modeling a component failure with a constant failure rate per hour, one can use a constant failure per demand model. In the constant failure per demand model, the component is assumed to have a constant probability of failing when it is demanded. This probability of failure per demand, which is denoted by Q, is independent of any exposure time interval, such as the time interval between tests or the time that the component has existed in stand-by. The constant failure per demand model can be applied when failures are inherent to the component and are not caused by external mechanisms that are associated with exposure time. In practice, the demand model has been applied to relatively few components, such as motor operated valves and human errors.

One has to realize that the probability of failure per demand Q is a conditional probability, i.e. the probability of failure given a demand. The formulas derived in this chapter for unavailability and probability of failure in the case of a failure on demand are conditional. In other words, the unavailability of the component is determined, given the system is demanded.

The contributors to the unavailability for the probability of failure on demand models are:
- unavailability due to failure given a demand
- unavailability due to testing of the component
- unavailability due to repair of the component.

Given a constant probability of failure, it does not appear logical to perform a test for these types of components because testing does not result in a lower probability of failure. In practice, however, almost all components will show some time-related failure behavior. For this reason also, these types of components can be more or less unavailable due to unrevealed faults. To detect these unrevealed faults, a test has to be performed. In this respect it is important to realize that the probability of failure on demand given in a number of databases is related to the test period of the components from which the data is derived. For nuclear databases a test interval can be assumed to be between one and three months.

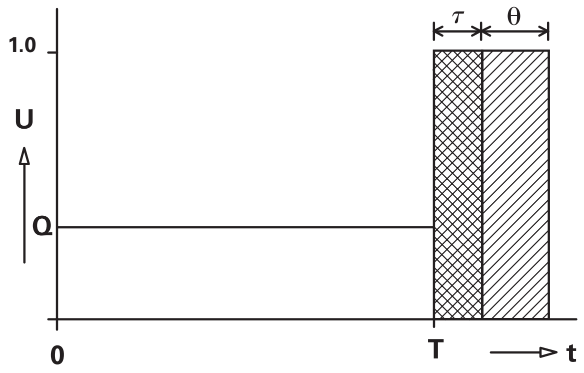


Figure 9.3: Probability of failure on demand.

Assuming a maximum of one demand per test period, the unavailability due to failure on demand is given by the probability of failure per demand Q:

$$U_{fld} = Q \tag{9.46}$$

The probability of failure per demand Q is assumed to be constant in time. The unavailability due to testing is given by the expression:

$$U_{tst} = \frac{\text{Test duration}}{T + \text{Test duration}} \tag{9.47}$$

In the denominator the test duration can be neglected in comparison with the test period. The test duration is denoted by τ. Substitution gives the unavailability due to testing:

$$U_{tst} \approx \frac{\tau}{T} \tag{9.48}$$

To test the component, it is assumed that the component is demanded once. Given a demand, there is a probability that the component will fail. After occurrence of the failure, the component has to be repaired.

The expression for the unavailability due to repair is now given by:

$$U_{rep} = P \text{ (repair per test period) } \frac{\text{Repair duration}}{\text{Test period}} \tag{9.49}$$

The probability of failure given one demand is equal to the probability of failure on demand Q. The

$$U_{rep} = Q \quad \frac{\theta}{T} \tag{9.50}$$

repair duration is denoted by θ. Substitution in formula (9.49) gives:
The total unavailability for the demand model is given by the expression:

$$U = Q + \frac{T}{T} \quad + Q \quad \frac{\theta}{T} \tag{9.51}$$

Remark:

Only one demand is considered to test the component. This might not be the case in reality, but one has to realize that the contribution due to repair can be neglected in comparison with the contribution due to failure or testing.

9.5 QUANTIFICATION OF THE UNAVAILABILITY OF HIGHER-ORDER CUT SETS

To calculate the unavailability of a higher-order cut set, the general formula (9.15) has to be applied. Application to a second-order minimal cut set holds:

$$U_{mcs} = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} U_1(t) \; U_2(t) \, dt \tag{9.52}$$

Now a distinction has to be made between the different types of components. Consider the following three different types of components:

- stand-by components
- on-line repairable components and
- components with a probability of failure per demand.

If one limits oneself to these three different types of components, six different types of formulas

Table 9.1: Formulas to quantify the unavailability of second order minimal cut sets

Formula number	Component 1	Component 2
B1	Stand-by	Stand-by
B2	On-line repairable	Stand-by
B3	On-line repairable	On-line repairable
B4	Stand-by	Probability of failure per demand
B5	On-line repairable	Probability of failure per demand
B6	Probability of failure per demand	Probability of failure per demand

For each combination given in table 9.1, a quantification formula has to be derived. In this paragraph the derivation will be provided for the first combination only.The formulas for the other combinations can be derived in similar fashion. The formulas to calculate the unavailability of second-order minimal cut sets are given in the appendix 9-A in tables B-1 up to B-6.

9.5.1 Both components in stand-by

Consider a second order minimal cut set in which both components can be unavailable due to unrevealed faults (see figure 9.4). It is assumed that component one is tested first and if necessary repaired. Next, component two is tested and if necessary repaired. Application of the general formula (9.15) holds:

$$t_1 = 0$$

$$t_2 = T + \tau_1 + \theta_1 + \tau_2 + \theta_2 \tag{9.53}$$

$$U_{mcs} = \frac{1}{T + \tau_1 + \theta_1 + \tau_2 + \theta_2} \int_0^{T + \tau_1 + \theta_1 + \tau_2 + \theta_2} U_1(t)\, U_2(t)\, dt$$

$$\approx \frac{1}{T} \int_0^{T + \tau_1 + \theta_1 + \tau_2 + \theta_2} U_1(t)\, U_2(t)\, dt \tag{9.54}$$

This integral can be separated into five integrals describing:
- both components unavailable due to unrevealed faults
- testing of component one and component two unavailable due to an unrevealed fault
- repair of component one and component two unavailable due to an unrevealed fault
- testing of component two and component one unavailable due to an unrevealed fault
- repair of component two and component one unavailable due to an unrevealed fault.

For each situation the integral (9.54) has to be resolved.

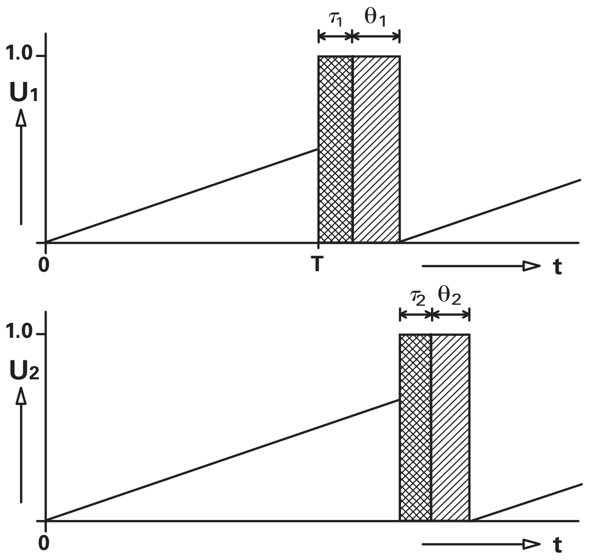


Figure 9.4: **Adopted test and repair sequence of two stand-by components tested.**

Unavailability of both components due to unrevealed faults in period (0,T)

In this period both components can be unavailable due to unrevealed faults. The instantaneous unavailabilities of the components due to unrevealed faults in time period (0,T) are:

$$U_1(t) = \lambda_1 \, t \qquad U_2(t) = \lambda_2 \, t \tag{9.55}$$

The time-averaged unavailability can be determined by resolving the integral in period (0,T):

$$\begin{aligned}[U_{mcs}]_T &= \frac{1}{T} \int_0^T U_1(t) \; U_2(t) \; dt \\ &= \frac{1}{T} \int_0^T \lambda_1 \; t \; \lambda_2 \; t \; dt \\ &= \frac{1}{3} \; \lambda_1 \; \lambda_2 \; T^2 \end{aligned} \tag{9.55}$$

Testing of component one, period (T , $T+\tau_1$)

Component one is not available due to testing and component two can be unavailable due to unrevealed failure. The instantaneous unavailabilities in this period are:

$$U_1(t) = 1.0$$

$$U_2(t) = \lambda_2 \, t \qquad (9.57)$$

Resolving the integral expression gives the time-averaged unavailability due to testing of component one.

$$[\ U_{mcs}]_{\tau_1} = \frac{1}{T} \int_{T}^{T+\tau_1} U_1(t)\, U_2(t)\, dt$$

$$= \frac{1}{T} \int_{T}^{T+\tau_1} \lambda_2 \ t\, dt$$

$$= \lambda_2 \ \tau_1 \ \ \frac{\lambda_2 \ \tau_1^{\,2}}{2 \ T}$$

In practice the test period T will always be much greater than the test duration of component one. This implies that the second term in the expression above can be neglected in comparison with the first term.

Repair of component one, period ($T+\tau_1$, $T+ \tau_1$, θ_1)

Component one does not need to be repaired every test period. There is a probability that the component has failed during the test period. The instantaneous unavailability for component one is given by:

$$U_1(t) = \text{P (component 1 faits in test period) } (U_{rep}(t) \mid \text{given repair})$$

$$= \lambda_1 \ T \ 1 \qquad (9.59)$$

$$= \lambda_1 \ T$$

The instantaneous unavailability of component two is equal to:

$$U_2(t) = \lambda_2 \ t \qquad (9.60)$$

The time-averaged unavailability due to repair of component one can be calculated as follows:

$$
\begin{aligned}
[\ U_{mcs}]_{\theta_1} &= \frac{1}{T} \int_{T+\tau_1}^{T+\tau_1+\theta_1} U_1(t)\, U_2(t)\, dt \\
&= \frac{1}{T} \int_{T+\tau_1}^{T+\tau_1+\theta_1} \lambda_1\, \lambda_2\, dt \\
&= \lambda_1\ \lambda_2\ (T+\tau_1)\ \theta_1 + \frac{\lambda_1\ \lambda_2\ \theta_1^2}{2} \\
&= \lambda_1\ \lambda_2\ T\,\theta + \frac{\lambda_1\ \lambda_2\ \theta_1^2}{2}
\end{aligned}
\tag{9.61}
$$

The second term of the last line of formula (9.61) is valid only if the repair duration is assumed to be a constant.

Testing of component two, period $(T + \tau_1 + \theta_1, T + \tau_1 + \theta_1 + \tau_2)$

Component one can be unavailable due to an unrevealed fault and component two is unavailable due to testing. The instantaneous unavailability in this period is given by:

$$
\begin{aligned}
U_1(t) &= \lambda_1\ t \\
U_2(t) &= 1.0
\end{aligned}
\tag{9.62}
$$

Care has to be taken to use the correct lower and upper bounds in the integral.

$$
\begin{aligned}
[\ U_{mcs}]_{\tau_2} &= \frac{1}{T} \int_{T+\tau_1+\theta_1}^{T+\tau_1+\theta_1+\tau_2} U_1(t)\, U_2(t)\, dt \\
&= \frac{1}{T} \int_{0}^{\tau_2} \lambda_1\ t\ dt \\
&= \frac{\lambda_1\ \tau_2^2}{2\ T}
\end{aligned}
\tag{9.63}
$$

Repair of component two, period $(T + \tau_1 + \theta_1, + \tau_2, T + \tau_1 + \theta_1 + \tau_2 + \theta_2)$
Component one can be unavailable due to an unrevealed fault and there is a certain probability that component two needs to be repaired. The instantaneous unavailabilities for this period are equal to:

$$
\begin{aligned}
U_1(t) &= \lambda_1 \; t \\
U_2(t) &= P \text{ (component 2 fails in test period) } 1.0 \\
&= \lambda_2 \, (T + \tau_1 + \theta_1) \\
&\approx \lambda_2 \; T
\end{aligned}
\qquad (9.64)
$$

The time-averaged unavailability can be calculated using the following formula:

$$
\begin{aligned}
[\; U_{mcs}]_{\theta_2} &= \frac{1}{T} \int\limits_{T + \tau_1 + \theta_1 + \tau_2}^{T + \tau_1 + \theta_1 + \tau_2 + \theta_2} U_1(t) \, U_2(t) \; dt \\
&= \frac{1}{T} \int\limits_{\tau_2}^{\tau_2 + \theta_2} \lambda_1 \; t \; \lambda_2 \; T \; dt \\
&= \lambda_1 \; \lambda_2 \; \tau_2 \; \theta_2 \quad \frac{\lambda_1 \; \lambda_2 \; \theta_2^{\,2}}{2}
\end{aligned}
\qquad (9.65)
$$

The second term of the last line of formula (9.65) is valid only if the repair duration of component two is assumed to be a constant.

Total time-averaged unavailability
The total time-averaged unavailability for a second order cut set consisting of two components that can be unavailable due to unrevealed faults is given by the expression:

$$
\begin{aligned}
U_{mcs} &= \frac{1}{3} \quad \lambda_1 \; t \; \lambda_2 \; T^2 \\
&+ \quad \lambda_2 \; \tau_1 \; \frac{\lambda_2 \; \tau_1^{\,2}}{2 \; T} \\
&+ \quad \lambda_1 \; \lambda_2 \; T \; \theta_1 \quad \frac{\lambda_1 \; \lambda_2 \; \theta_1^{\,2}}{2} \\
&+ \quad \frac{\lambda 1 \; \tau_2^{\,2}}{2 \; T} \\
&+ \quad \lambda_1 \; \lambda_2 \; \tau_2 \theta_2 \; + \; \frac{\lambda_1 \; \lambda_2 \; \theta_2^{\,2}}{2}
\end{aligned}
\qquad (9.66)
$$

In practice the following relation will be valid:

$$T \text{ » } \tau_1 \, , \tau_2 \, , \theta_1 \, , \theta_2 \tag{9.67}$$

This implies that a number of terms in formula (9.66) can be neglected. Rewriting of formula (9.66) results in:

$$U_{mcs} \;=\; \frac{1}{3} \; \lambda_1 \; \lambda_2 T^2 + \lambda_2 \; \tau_1 \; + \; \lambda_1 \; \lambda_2 \; \theta_1 \; T \tag{9.68}$$

9.6 QUANTIFICATION OF THE FAILURE OCCURRENCE RATE AND THE EXPECTED NUMBER OF FAILURES OF A CUT SET

If the top event of a fault tree represents the failure of a system in a continuous mode of operation, not only the unavailability is of interest but also the expected number of failures of the system in a specified time period. For each minimal cut set the expected number of failure occurrences has to be calculated. The easiest way to calculate the expected number of failure occurrences of a minimal cut set is to calculate the failure occurrence rate first. The general expression to calculate the failure occurrence rate of a minimaf cut set is given by formula (9.7):

$$\omega_{mcs}(t) \;=\; \sum_{j=1}^{n} \omega_j \prod_{\substack{k=1 \\ k \neq j}}^{n} U_k(t) \tag{9.69}$$

The minimal cut set occurrence rate is strictly applicable when all components have a per-hour failure rate. The probability of failure per demand model does not have any explicit time-associated behavior. The expression (9.69) can be applied to minimal cut sets having per demand models only if the per-demand model is considered to be demanded. This is not always straightforward, which is why for a number of cut set combinations no generally valid quantification formula can be derived.

9.6.1 First-order minimal cut sets

In practice the unavailability can be regarded as small. This implies that the failure occurrence rate can be approximated by the failure rate (see chapter 5):

$$\omega \approx \lambda \quad \text{if} \quad U \leq 0.01 \tag{9.70}$$

The general expression of the expected number of failures is given by:

$$\begin{aligned} N(0,T) \;&=\; \int_0^T \lambda \; dt \\ &=\; \lambda \; T \end{aligned}$$

Formula (9.71) gives the expected number of failures for a first-order cut set if the contributions due to testing, repair or maintenance are not taken into account. The same formula holds for on-line repairable components.

9.6.2 Second-order minimal cut sets

For second-order minimal cut sets equation (9.69) can be written as:

$$\omega_{mcs} = \omega_1(t)\ U_2(t) + \omega_2(t)\ U_1(t) \tag{9.72}$$

If the unavailability is smalt, the following expression can be derived (see chapter 5):

$$\omega \approx \lambda \quad \text{if} \quad U \leq 0.01 \tag{9.73}$$

Substitution of expression (9.73) in formula (9.72) gives:

$$\omega_{mcs} = \lambda_1\ U_1(t) + \lambda_2\ U_1(t) \tag{9.74}$$

In principle a formula to calculate the failure occurrence rate should be derived for each type of component combinations as tabulated in table 9.1. This is rather complicated if one or both of the components have a probability of failure per demand. The problem is that the number of demands have to be known to be able to calculate a failure occurrence rate. Also, it is important to know how the components are handled after a demand. For instance are they tested or not after a demand ?. These types of considerations make it impossible to derive a generally valid formula to calculate the failure occurrence rate if one of the components has a probability of failure on demand. For each of the first three combinations given in table 9.1 a formula will be derived.

<u>Both components fail due to unrevealed faults:</u>
The following expression holds for both components (see chapter 5):

$$\begin{aligned} U_1(t) &= \lambda_1\ t \\ U_2(t) &= \lambda_2\ t \end{aligned} \tag{9.75}$$

Substitution of expression (9.75) in formula (9.74) gives:

$$\begin{aligned} \omega_{mcs} &= \lambda_1\ \lambda_2\ t + \lambda_2\ \lambda_1\ t \\ &= 2\ \lambda_1\ \lambda_2\ t \end{aligned} \tag{9.76}$$

The expected number of minimal cut set failures in time period (0,T) can be calculated using formula (9.8):

$$N_{mcs}(0,T) = \int_0^T \omega_{mcs}(t)\ dt$$

$$= \int_0^T 2\ \lambda_1\ \lambda_2\ t\ dt \qquad (9.77)$$

$$= \lambda_1\ \lambda_2\ T^2$$

<u>Component one faits due to a revealed fault and component two faits due to a unrevealed fault:</u>
The instantaneous unavailabilities are:

$$U_1(t) = \lambda_1\ \theta_1$$
$$U_2(t) = \lambda_2\ t \qquad (9.78)$$

Substitution in formula (9.72) results in:

$$\omega_{mcs} = \lambda_1\ \lambda_2\ t + \lambda_2\ \lambda_1\ \theta_1 \qquad (9.79)$$

The expected number of minimal cut set failures in time period (0,T) can be calculated as follows:

$$N_{mcs}(0,T) = \int_0^T \omega_{mcs}(t)\ dt$$

$$= \int_0^T \lambda_1\ \lambda_2\ t + \lambda_1\ \lambda_2\ \theta_1)\ dt \qquad (9.80)$$

$$= \frac{1}{2}\ \lambda_1\ \lambda_2 T^2 + \lambda_1\ \lambda_2\ \theta_1\ T$$

The second term in formula (9.80) can be neglected in comparison with the first term.

<u>Both components fail due to revealed faults:</u>
In this situation the instantaneous unavailabilities are:

$$U_1(t) = \lambda_1\ \theta_1$$
$$U_2(t) = \lambda_2\ \theta_2 \qquad (9.81)$$

Substitution in formula (9.72) holds:

$$\begin{aligned}\omega_{mcs} &= \lambda_1 \lambda_2 \theta_2 + \lambda_2 \lambda_1 \theta_1 \\ &= \lambda_1 \lambda_2 (\theta_1 + \theta_2)\end{aligned} \tag{9.82}$$

The expected number of minimal cut set failures in time period (0,T) are:

$$\begin{aligned}N_{mcs}(0,T) &= \int_0^T \omega_{mcs}(t)\, dt \\ &= \int_0^T \lambda_1 \lambda_2 (\theta_1 + \theta_2)\, dt \\ &= \lambda_1 \lambda_2 (\theta_1 + \theta_2)\, T\end{aligned} \tag{9.83}$$

9.7 REFERENCES

[9.1] IAEA, International Atomic Energy Agency,
The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, Safety series No. 106, 1992.

[9.2] PRA Procedures Guide
A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants.
U.S. Nuclear Regulatory Commission, NUREG/CR-2300
Final Report, January 1983.

[9.3] Probabilistic Risk Assessment; Reliability Engineering, design ans Analysis, IEEE Press, New York, 1992.

[9.4] Fault Tree Handbook
U.S. Nuclear Regulatory Commission NUREG-0492, 1981.

[9.5] How to Hand Calculate System Reliability and Safety Characteristics, Fussell, J., IEEE Trans. on Reliability, R-24, No. 3, 1975.

[9.6] Reliability Evaluation of Engineering Systems, R. Billington, R.N. Allan
Pitman Advanced Publishing Program, Boston-London-Melbourne, 1983,
(ISBN 0-273-08484-4).

[9.7] Reliability and Risk Analysis, N.J. Mc Cormick, Academic Press,
New York 1081.e t.

APPENDIX 9-A: QUANTIFICATION FORMULAS

In tables A,B,C and D a number of standard quantification formulas are provided. Table A contains formulas to calculate the time-average unavailability of first order minimal cut sets. In table B formulas to calculate the time-average unavailability of second order minimal cut sets are given. Tables C and D contain formulas to calculate the expected number of failure occurrences in time period (0,T) for first and second order minimal cut sets. Tables C and D can also be used to calculate the probability of failure in time period (0,T) if the calculated value is less than approximately 0.1.

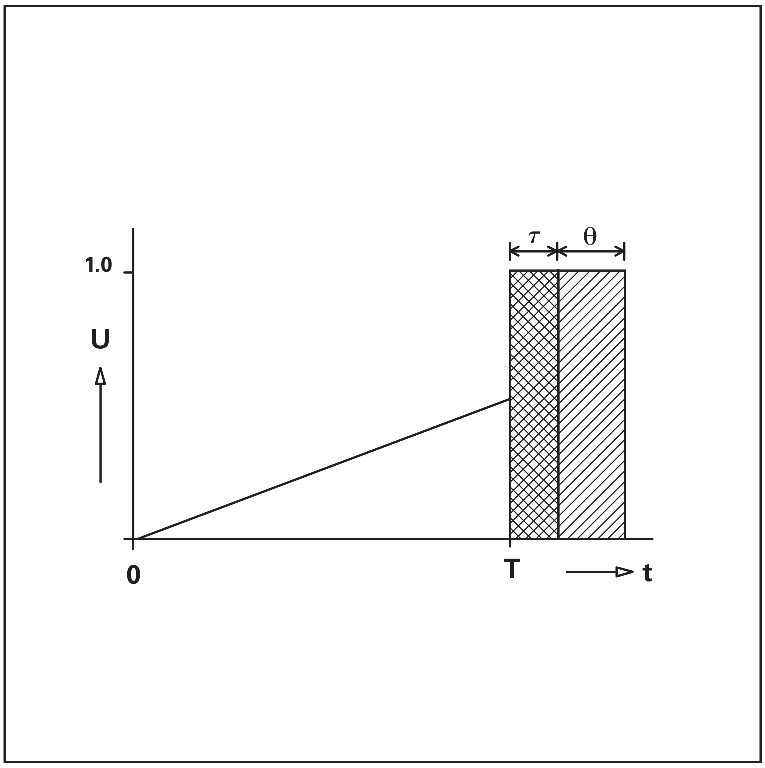
During the derivation process of the quantification formulas a number of assumptions have to be made. The most important assumptions are:

- The failure rate is assumed to be constant in time.
- The average repair and test durations are assumed to be constant in time.
- For the formulas to be used to calculate time-averaged unavailability, it is assumed that the number of demands is less than the test frequency.
- In the case of a second-order minimal cut set with both components tested periodically, it is assumed that the test period is equal for both components.
- In tables B, C and D only the most important terms are given.
- For second order cut sets, it is assumed that failure of the components is independent.
- It is assumed that the test procedure always results in proper classification of the component status. This implies that if a component has failed, this will always be detected in the test and therefore the human error probability is assumed to be zero.

TABLE A: UNAVAILABILITY FIRST-ORDER MINIMAL CUT SETS

FORMULA: A1

Formula Al applies to a periodically tested stand-by component. If during testing the component is found to have failed, it will be repaired immediately.



COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
A1 λ u.f.	$\frac{1}{2}\ \lambda T$	$\frac{T}{T}$	$\lambda\theta$

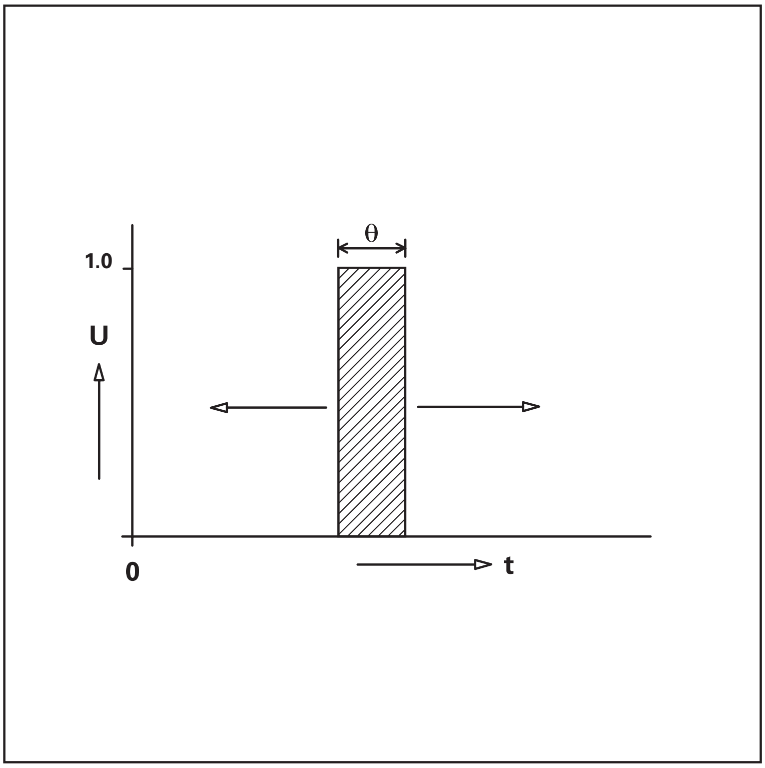
u.f. = Unrevealed faults.

r.f. = Revealed faults.

CONTINUATION OF TABLE A: UNAVAILABILITY FIRST-ORDER MINIMAL CUT SETS

FORMULA: A2

Formula A2 applies to an on-line repairable component. After failure the of the component, repair is started immediately. Logistic, and waiting time are assumed to be incorporated in the repair duration.



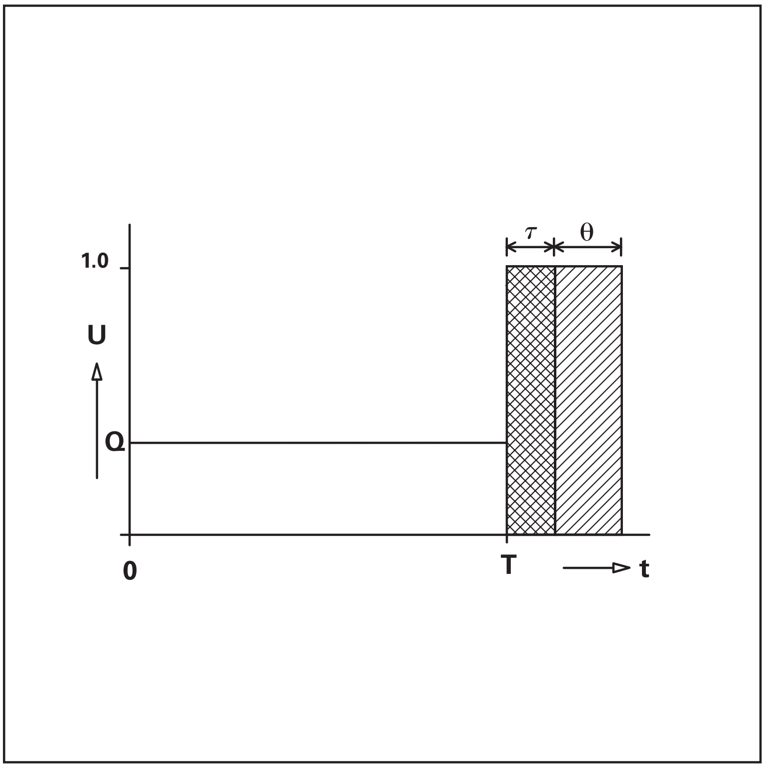
COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
A2 λ r.f.	–	–	λθ

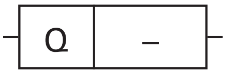
u.f. = Unrevealed faults.
r.f. = Revealed faults.

CONTINUATION OF TABLE A : UNAVAILABILITY FIRST-ORDER MINIMAL CUT SETS

FORMULA: A3

Formula A3 applies to a component with a probability of failure on demand. The component is tested periodically. If during testing the component is found to have failed, repair is started immediately.



COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
A3 	Q	$\frac{T}{T}$	$\frac{Q\theta}{T}$

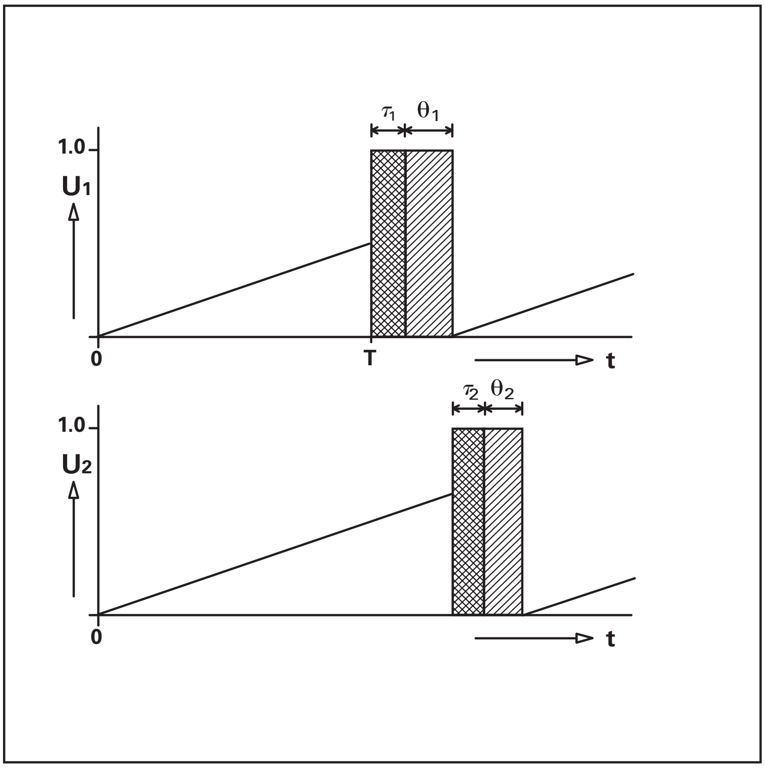
u.f. = Unrevealed faults.

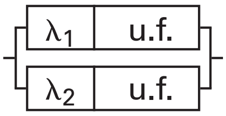
r.f. = Revealed faults.

TABLE B : UNAVAILABILITY SECOND-ORDER MINIMAL CUT SETS

FORMULA: B1

Both components are periodically tested stand-by components. First, component one is tested and, if necessary, repaired; next, component two is tested and, if necessary, repaired.



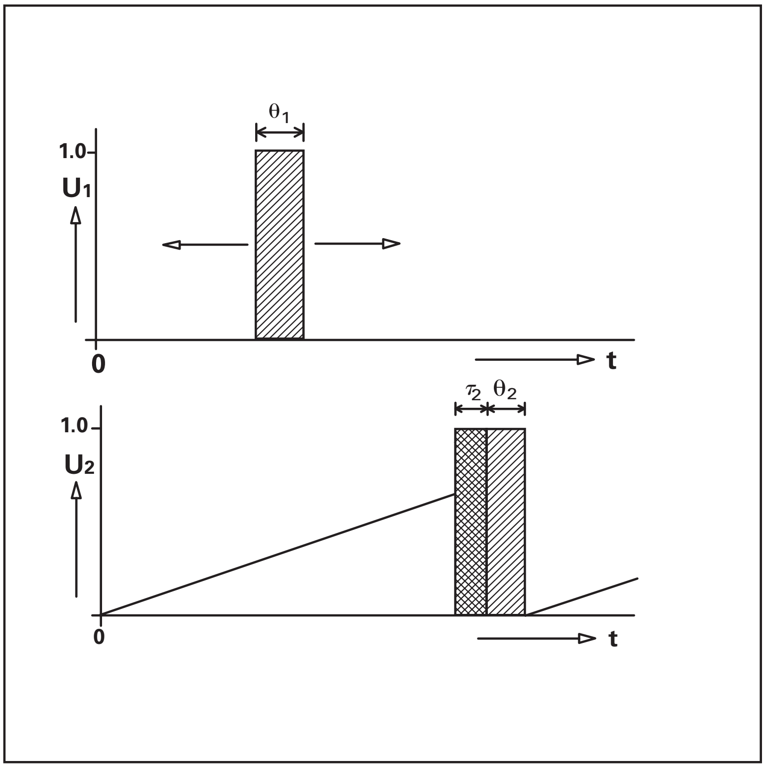
COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
B1  	$\frac{1}{3}\ \lambda_1\lambda_2T^2$	$\lambda_2 T_1$	$\lambda_1\lambda_2\theta_1T$

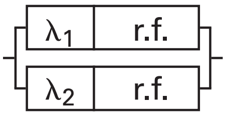
u.f. = Unrevealed faults.
r.f. = Revealed faults.

CONTINUATION OF TABLE B: UNAVAILABILITY SECOND-ORDER MINIMAL CUT SETS

FORMULA: B2

Both components have a failure rate. Component one is an on-line repairable component and component two is a periodically tested stand-by component. After failure of component one, repair is started immediately. During repair of component one, testing of component two wilt be postponed.



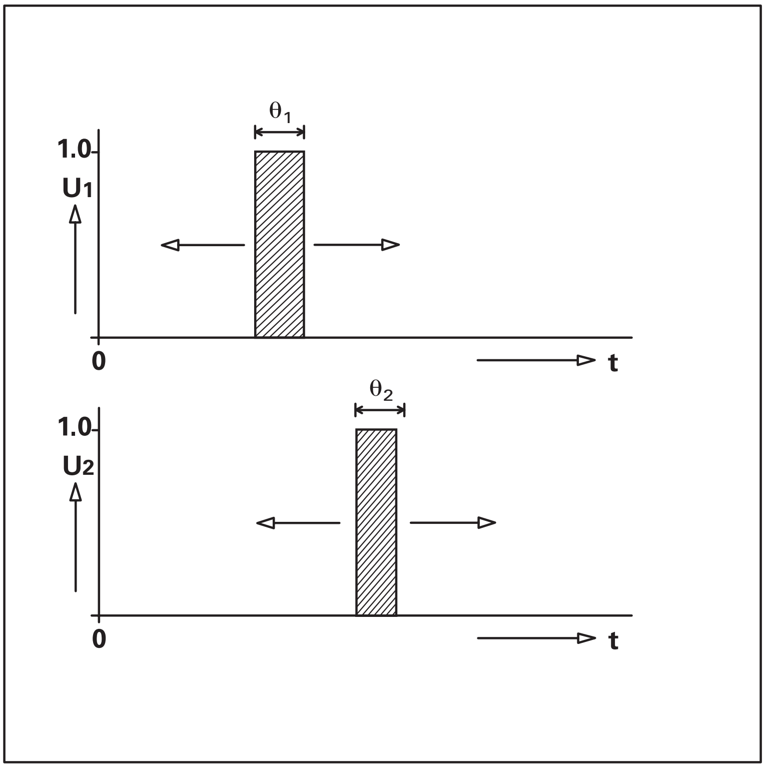
COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
B2 	–	$\frac{\lambda_1 T_2^2}{2T}$	$\frac{1}{2} \quad \lambda_1\lambda_2\theta_1 T$

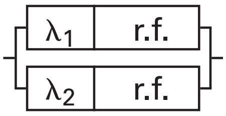
u.f. = Unrevealed faults.
r.f. = Revealed faults.

CONTINUATION OF TABLE B: UNAVAILABILITY SECOND-ORDER MINIMAL CUT SETS

FORMULA: B3

Both components are on-line repairable components. After failure of a component, repair is started immediately. If both components are in a failed state, the component with the smallest repair duration will be repaired first.



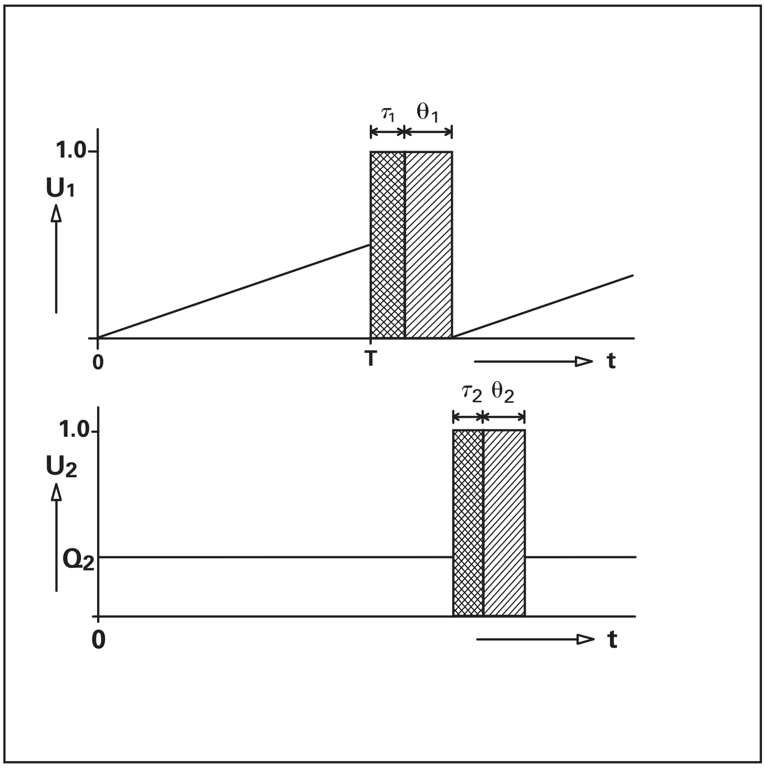
COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
B3 	–	–	$\lambda_1\lambda_2\theta_A(\theta_A+\theta_B)$ $\theta_A=\min(\theta_1,\theta_2)$ $\theta_B=\max(\theta_1,\theta_2)$

u.f.	= Unrevealed faults.
r.f.	= Revealed faults.

CONTINUATION OF TABLE B: UNAVAILABILITY SECOND-ORDER MINIMAL CUT SETS

FORMULA: B4

Component one is a periodically tested component and component two has a probability of failure on demand. First, component one is tested and, if necessary, repaired; next, component two is tested and, if necessary, repaired.



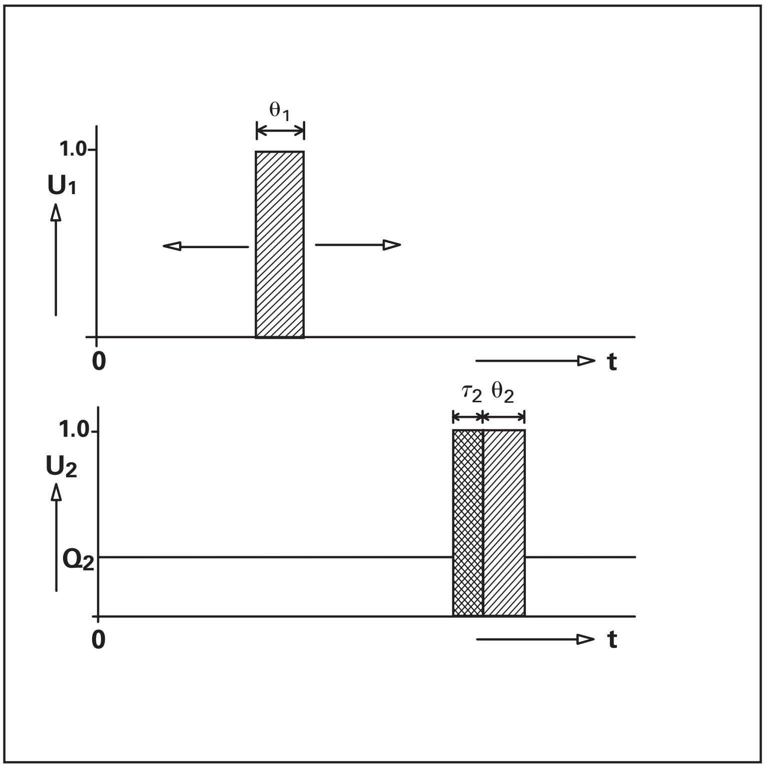
COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
B4 λ_1 u.f. Q_2 –	$\frac{1}{2}\ \lambda_1 T Q_2$	$\frac{\tau_1 Q_2 0.5 \lambda_1 \tau_2^2}{T}$	$\lambda_1 \theta_1 Q_2$

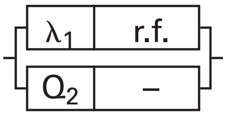
u.f. = Unrevealed faults.
r.f. = Revealed faults.

CONTINUATION OF TABLE B: UNAVAILABILITY SECOND-ORDER MINIMAL CUT SETS

FORMULA: B5

Component one has a failure frequency and is periodically tested. Component two has a probability of failure on demand and is periodically tested. If component one faits, repair is started immediately. During repair of component one, testing of component two is postponed.



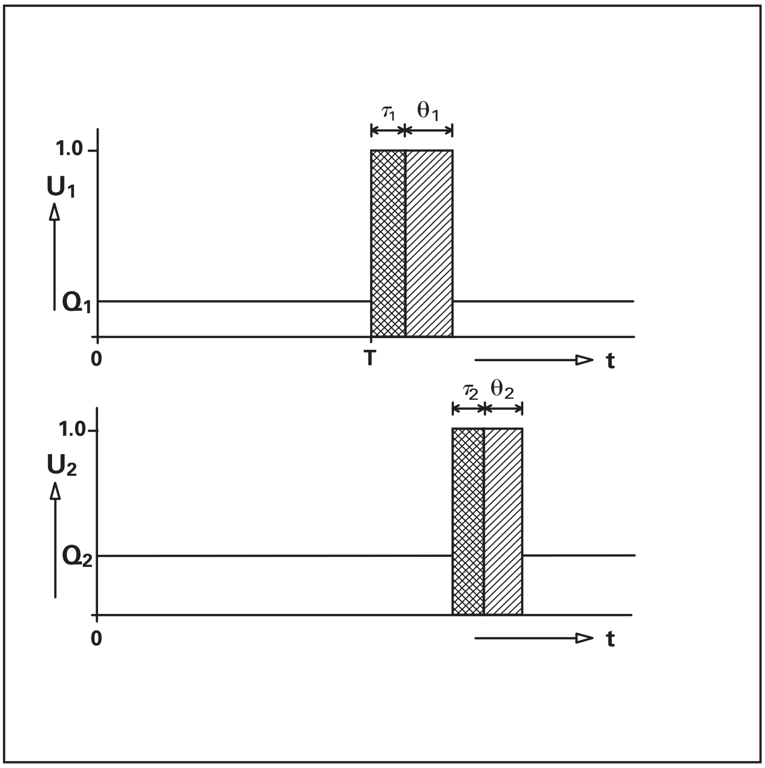
COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
B5 	–	$\frac{\lambda_1 \tau_2^2}{2T}$	$\lambda_1 \theta_1 Q_2$

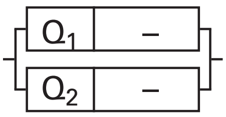
u.f.	= Unrevealed faults.
r.f.	= Revealed faults.

CONTINUATION OF TABLE B: UNAVAILABILITY SECOND-ORDER MINIMAL CUT SETS

FORMULA: B6

Both components have a probability of failure on demand and are tested periodically. First, component one is tested and, if necessary, repaired; next, component two is tested and, if necessary, repaired.



COMPONENT	UNAVAILABILITY		
	FAILURE	TESTING	REPAIR
B6 	Q_1Q_2	$\dfrac{Q_2\tau_1Q_1\tau_2}{T}$	$\dfrac{Q_1\tau_2(\theta_1+\theta_2)}{T}$

u.f. = Unrevealed faults.
r.f. = Revealed faults.

TABLE C: EXPECTED NUMBER OF FAILURES FIRST-ORDER CUT SETS

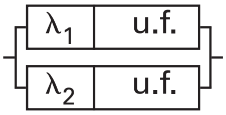
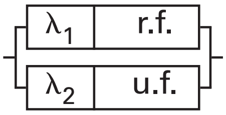
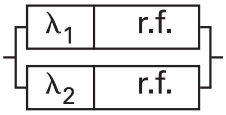
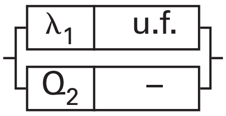
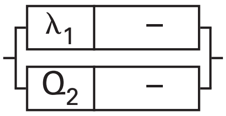
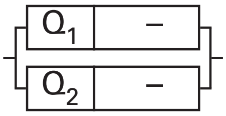
Quantification formulas to calculate the expected number of failure occurrences of first-order minimal cut sets.

COMPONENT	Expected number of failure occurrences in time period (0,T)
	$N(0,T) < 0.1 \rightarrow F(0,T) \approx N(0,T)$
C1 $\boxed{\lambda}\boxed{\text{u.f.}}$	λT
C2 $\boxed{\lambda}\boxed{\text{r.f.}}$	λT
C3 $\boxed{Q}\boxed{-}$	No generally valid formula possible

u.f. = Unrevealed faults.
r.f. = Revealed faults.

TABLE D: EXPECTED NUMBER OF FAILURES SECOND-ORDER CUT SETS

Quantification formulas to calculate the expected number of failure occurrences of second-order minimal cut sets.

COMPONENTS	Expected number of failure occurences in time period (O,T)
	$N(0,T)<.1 - F(0,T) \approx N(0,T)$
D1 	$\lambda_1\lambda_2T^2$
D2 	$\frac{1}{2}\ \lambda_1\lambda_2T^2$
D3 	$\lambda_1\lambda_2(\theta_1+\theta_2)T$
D4 	No generally valid formula possible
D5 	No generally valid formula possible
D6 	No generally valid formula possible

u.f. = Unrevealed failure.
r.f. = Revealed failure.

EVENT TREES

CONTENTS

10.1 INTRODUCTION

Event trees are used to study or model event sequences which can result in different consequences. The first event of the event sequence is called the initiating event. Depending on the occurrence of one or more intermediate events different outcomes can occur. All possible outcomes relevant to the context of the study are included in the event tree.

The objective of an event tree is to provide insight into the possible consequences of one initiating event which can lead to different consequences, while the objective of fault tree analysis is to clarify how one specific top event, can develop from an indefinite number of basis events.

The event trees can be used either for systems in which all components are continuously operating or for systems in which some or all of the components are in a standby mode that involve sequential operational logic and switching. The last type of system is generally associated with safety oriented systems to model accident sequences as the result of a general equipment failure or process upset, the initiating event. For this type of application an event tree analysis is an inductive process where the analyst begins with an initiating event and develops the possible sequences of events that lead to potential accidents.

Although the event tree method is more widely used for safety oriented systems the applications of the technique to both types of systems proceed in a similar manner but with two particular differences between them.

The first is that, with continuously operated systems, the events that can occur, i.e., the components that can fait, can be considered in any arbitrary order. With standby systems, or any system in which the operation of a particular component is dependent on the success or failure of another component, the sequence of events must be considered in the chronological order in which they occur.

The second difference is the starting point of the event tree. In the case of continuously operating systems, the starting point is the system operating normally and the event tree is deduced as a sequence of events involving success and failure of the system components. In the case of standby systems and in particular, safety and mission oriented systems, the event tree is used to identify the various possible outcomes of the system following a given initiating event which is generally an unsatisfactory operating event or situation.

Event trees have found widespread applications in risk analyses for both the nuclear and chemical industries. These type of applications examines the systems in place that would prevent incident-precursors from developing into incidents. The event tree analysis of such a system is often sufficient for the purpose of estimating the safety of the system. Human reliability analysis uses event trees to model all possible outcomes of one or more human failures.

The intention of this chapter is to explain the construction of event trees and to discus the application of event trees in simpte risk analyses. The application of event trees in more comprehensive risk analyses and advanced accident sequence development and quantification will be discussed in chapter 12.

10.2 NOMENCLATURE

A	-	Initiating event
B	-	Heading event
C	-	Heading event
D	-	Heading event
E	-	Heading event
F	-	Heading event
$\bar{B}$	-	Heading event B does not occur
$\bar{C}$	-	Heading event C does not occur
$\bar{D}$	-	Heading event D does not occur
$\bar{E}$	-	Heading event E does not occur
$\bar{F}$	-	Heading event F does not occur
P	-	Probability
P(A)	-	Probability of initiating event A for one year of operation
P(B)	-	Conditional probability of event B
P(C)	-	Conditional probability of event C
P(D)	-	Conditional probability of event D
P(E)	-	Conditional probability of event E
P(F)	-	Conditional probability of event F

Remark:
Conditional: given that the previous events in the accident sequence have occurred

10.3 EVENT TREE ANALYSIS METHODOLOGY

In an event tree there are two types of event to be distinguished, the initiating event and the heading events. An event tree always starts with an initiating event. Other events following that initiating event are called heading or intermediate events.

An initiating event can be recognized from the fact that the various heading events can occur only after occurrences of the initiating event. So the event tree is of interest only if the initiating event has taken place. During the development process of an event tree, conditioned thinking is required. The condition is that at least the initiating event has occurred. The heading events are only of interest after occurrence of the initiating event.

Making an event tree is useful if:

- a specific event can result in more than one outcomes
- one is interested in the probability of occurrence of each of the different outcomes.

More than one outcome implies that several consequences are possible. If this is the case one must always try to make an event tree. For one event and one consequente, a fault tree should be sufficient.

A good event tree offers some very important advantages:

- all possible courses of accidents which can arise from one specific event are arranged in a convenient manner
- an event tree often provides a very good framework for discussions. The point in the tree which is under discussion is clearly defined during discussions. This can then no longer be misinterpreted and the impatient can see whether or not their problem is coming up for discussion (at a different point in the tree)
- as soon as the principle of the event tree is known, everybody can understand why certain events do occur and why other combinations of events do not occur.

In an event tree analysis at least two branches have to be considered for each heading event which plays a role in the accident sequence under consideration.

10.3.1 Construction of an event tree

The construction of an event tree, considering a specific initiating event, starts with the collection of all relevant heading events. The next step is to put the heading events in the right order. For safety applications the heading events are put in chronological order in accordance with the activation of the various safeguarding systems or physical processes which might occur after occurrence of the initiating event. Starting from the initiating even, event sequences are developed by defining branches for each relevant heading event. If the occurrence of a specific heading event does not influence the event sequence under consideration no branch is defined for that specific heading event.

It should be emphasized that one can define more than two branches for a specific heading event if necessary. The only boundary condition is that the enumeration of all branch probabilities must be equal to one.

The event tree construction process described above will be carried out for a simple process which can be understand very easily. Suppose you want to read one specific book for which you need a reading lamp and your reading glasses. For that activity the event tree shown in figure 10.1 can be constructed. In this example the system to be analysed consists of a book, a pair of glasses and a reading lamp. The initiating event is the desire to read a book.

Events A to F are listed at the top of the tree, called the heading of the event tree. An event tree is read by moving along the lines from left to right. Follow the line starting from the far left point. So one assumes that event A (the initiating event) occurs. Soon one reaches the bifurcation under B (a heading event). From there one can follow the line in the ″No″ direction (this means No, the book is not missing) or in the ″Yes″ direction. This means Yes, the book is missing. If the book is missing, it is not relevant whether the lamp works or not and/or the reading glasses are present or not. That is why, if one follows this line, no bifurcations occur from C to F. The consequence is that B occurs and the book cannot be read.

Now follow the fine in the direction ″No″. The book is not missing. One reaches the bifurcation under C. The reading lamp is defective. This time one can also go in the direction ″Yes″, the reading lamp is defective or ″No″ the reading lamp is not defective. If one follows the ″No″ line, one arrives under heading event D (= no spare lamp) but one does not has to consider this because one has light as the reading lamp is not defective.

This is the way an event tree is read. The first event (A = 1 want to read a book) is essentially different from the other events. This first event is called the ″initiating event″. If the initiating event does not occur, the other events are irrelevant. So the initiating event must always be satisfied. The heading events are characterized by the fact that they can occur only if the initiating event occurs.

The advantage of an event tree is that a large number of undesired events are conveniently arranged and only the sensible combinations are entered; see figure 10.2, showing 32 event combinations of which only 8 are sensible (see figure 10.1). The advantage of an arrangement of combinations of events according to consequence can also be linked directly to the event tree. Event combinations for the event tree in figure 10.1 are arranged in table 10.1.

Suppose the probability of occurrence of each event is known and the events are independent of each other. It is then possible to enter the probabilities for the combinations of events in table 10.1. If each column in the table is totalled, the probability of each of the possible consequences is known.

If technical systems are involved, the probabilities of the heading events in an event tree are often determined with fault trees. A heading event is often the top of a fault tree. In general the construction of an event tree is a complicated process.

The biggest and most difficult problem is to arrange the different events in the correct sequence from left to right. If possible the heading events are formulated in a undesired way, failure of a system or failure of a component. One can expect difficulties when working with desired heading events. In the case of desired events, the combination AB would mean that:

- I want to read a book
- the book is there.

In other words, normal reading is possible. This will then apply to all combinations, so the event tree no longer deals with different consequences and therefore loses much of its value.

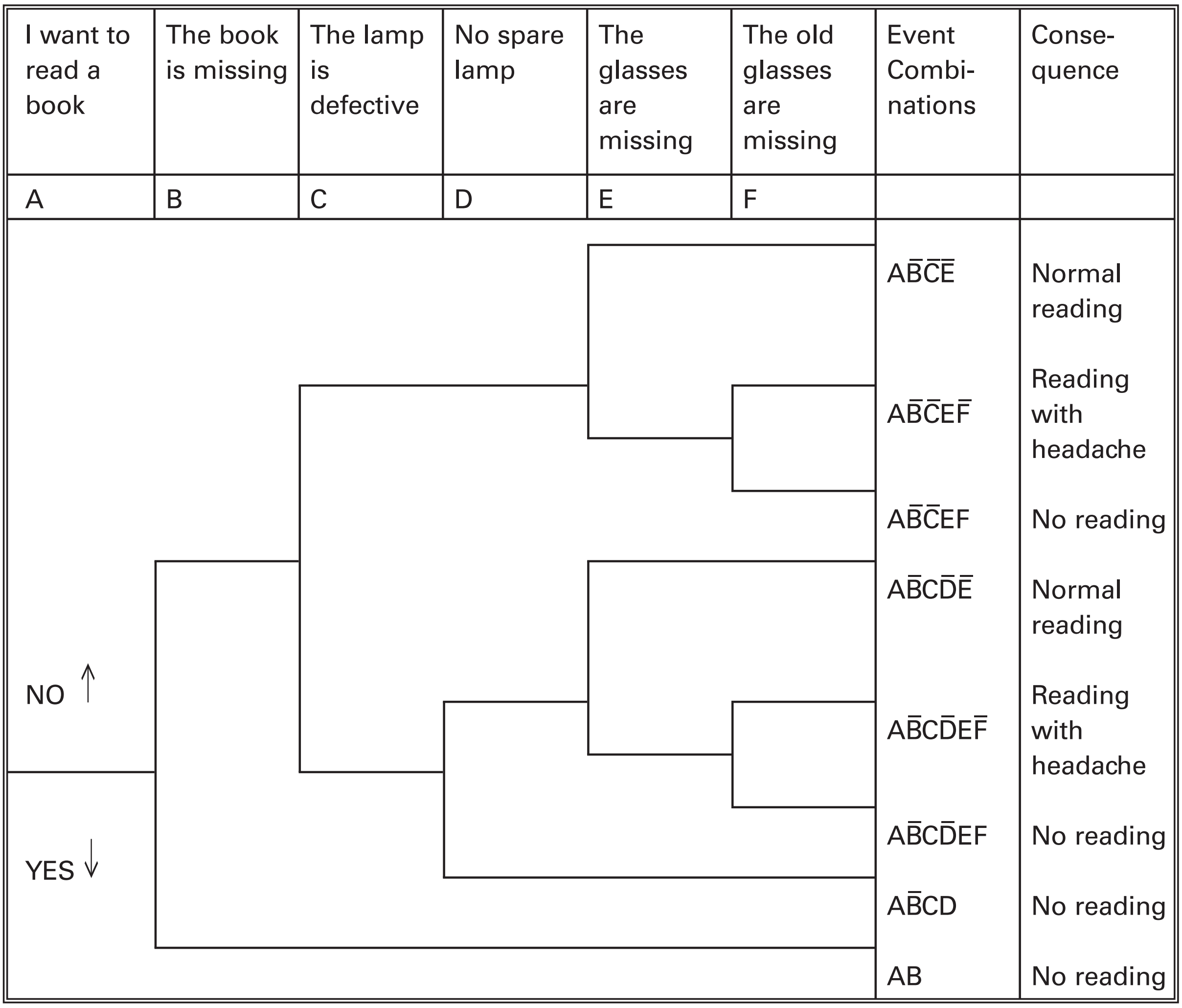
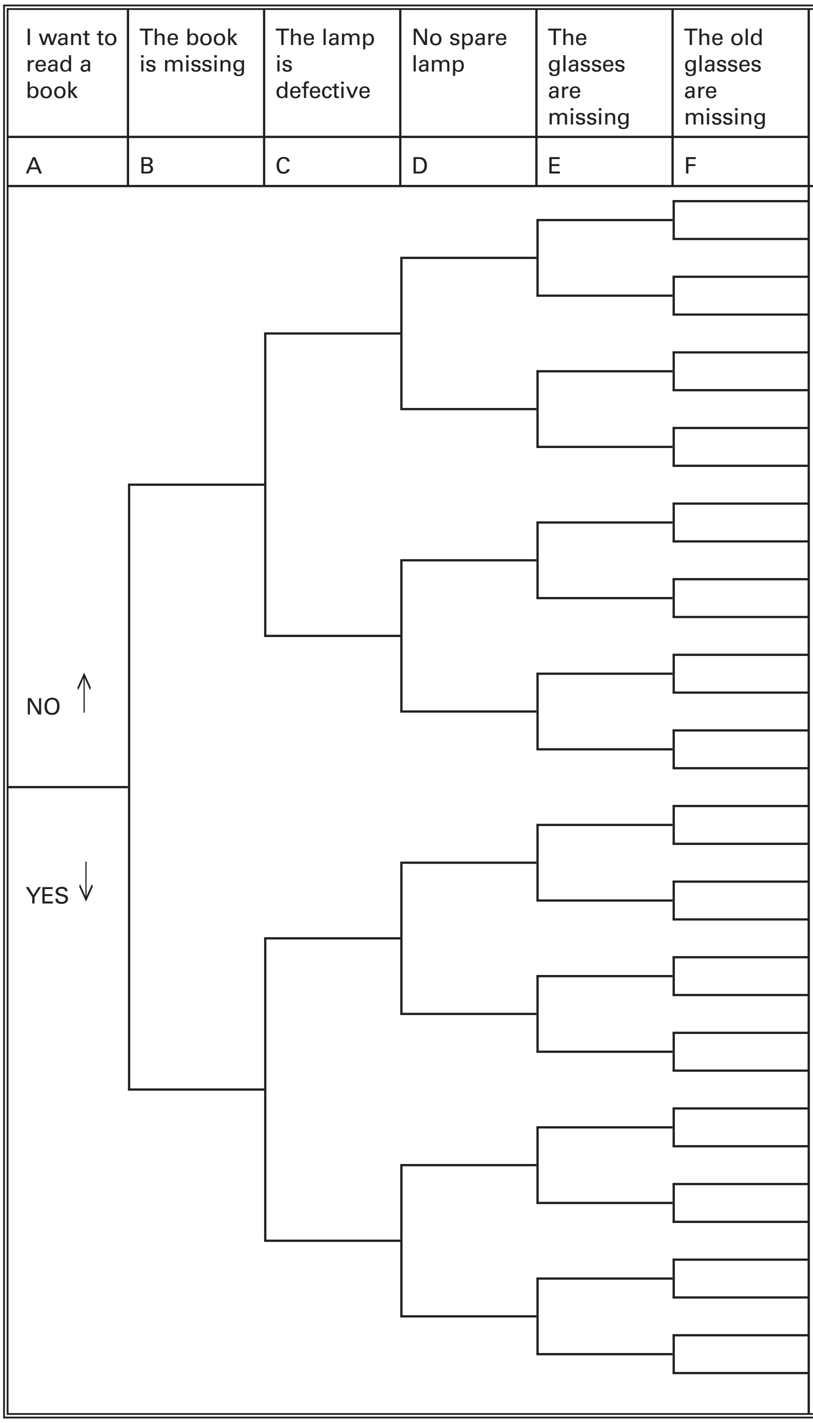


Figure 10.1 : Event tree for reading a book.

Table 10.1: Consequence classes.

Normal reading	**Reading with headache**	**No reading**
$A\bar{B}\bar{C}\bar{E}$	$A\bar{B}\bar{C}E\bar{F}$	$A\bar{B}\bar{C}EF$
$A\bar{B}C\bar{D}\bar{E}$	$A\bar{B}C\bar{D}E\bar{F}$	$A\bar{B}C\bar{D}EF$
		$A\bar{B}CD$
		AB



Event combinations	Consequences
$A\overline{B}\overline{C}\overline{D}\overline{E}\overline{F}$	Normal reading
$A\overline{B}\overline{C}\overline{D}\overline{E}F$	Normal reading
$A\overline{B}\overline{C}\overline{D}E\overline{F}$	Reading with headache
$A\overline{B}\overline{C}\overline{D}EF$	No reading
$A\overline{B}\overline{C}D\overline{E}\overline{F}$	Normal reading
$A\overline{B}\overline{C}D\overline{E}F$	Normal reading
$A\overline{B}\overline{C}DE\overline{F}$	Reading with headache
$A\overline{B}\overline{C}DEF$	No reading
$A\overline{B}C\overline{D}\overline{E}\overline{F}$	Normal reading
$A\overline{B}C\overline{D}\overline{E}F$	Normal reading
$A\overline{B}C\overline{D}E\overline{F}$	Reading with headache
$A\overline{B}C\overline{D}EF$	No reading
$A\overline{B}CD\overline{E}\overline{F}$	No reading
$A\overline{B}CD\overline{E}F$	No reading
$A\overline{B}CDE\overline{F}$	No reading
$A\overline{B}CDEF$	No reading
$AB\overline{C}\overline{D}\overline{E}\overline{F}$	No reading
$AB\overline{C}\overline{D}\overline{E}F$	No reading
$AB\overline{C}\overline{D}E\overline{F}$	No reading
$AB\overline{C}\overline{D}EF$	No reading
$AB\overline{C}D\overline{E}\overline{F}$	No reading
$AB\overline{C}D\overline{E}F$	No reading
$AB\overline{C}DE\overline{F}$	No reading
$AB\overline{C}DEF$	No reading
$ABC\overline{D}\overline{E}\overline{F}$	No reading
$ABC\overline{D}\overline{E}F$	No reading
$ABC\overline{D}E\overline{F}$	No reading
$ABC\overline{D}EF$	No reading
$ABCD\overline{E}\overline{F}$	No reading
$ABCD\overline{E}F$	No reading
$ABCDE\overline{F}$	No reading
$ABCDEF$	No reading

Figure 10.2: Complete event tree (not reduced).

10.3.2 Order of the heading events

It is important to realize that a heading event on the ”left” might affect the next heading event (on its ”right”). This requirement is often satisfied (if possible) by using a chronological sequence. In the event tree in figure 10.1 that means that events E and. F or events C and D must not be interchanged. It would then be impossible to construct this event tree. Interchanging event C with event E and event D with event F so the sequence is ABEFCD gives the event tree in figure 10.3. This does not differ fundamentally from that in figure 10.1 Here too the events can be arranged in three categories. The arrangement is given in table 10.2.

Comparison (per column) between table 10.1 and table 10.2 shows there is some difference. But as soon as the probabilities are entered and each column is totalled, the results per column turn out to be the same after all.

If the heading event B (the book is missing) is piaced at the end of the event tree heading (see figure 10.4), it is still possible to construct a correct event tree. But then ten event combinations are created compared with seven in the previous event trees (figures 10.1 and 10.3). As clarity decreases in proportion as the number of event combinations increases, preference is given to one of the first two event trees.

As already noted, probabilities for the occurrence of events are often determined with fault trees. Sometimes the probabilities can also be taken directly from a file (see Chapter 6, Data Analysis). Whichever method is selected, there is a specific probability for each of the heading events. This probability is indicated by PB for event B, by P_C for event C, and so on. That implies that the probability of B not occurring is equal to $(1-P_B)$ and the probability of C not occurring is equal to $(1-P_C)$. One still assume for the initiating event that it occurs.

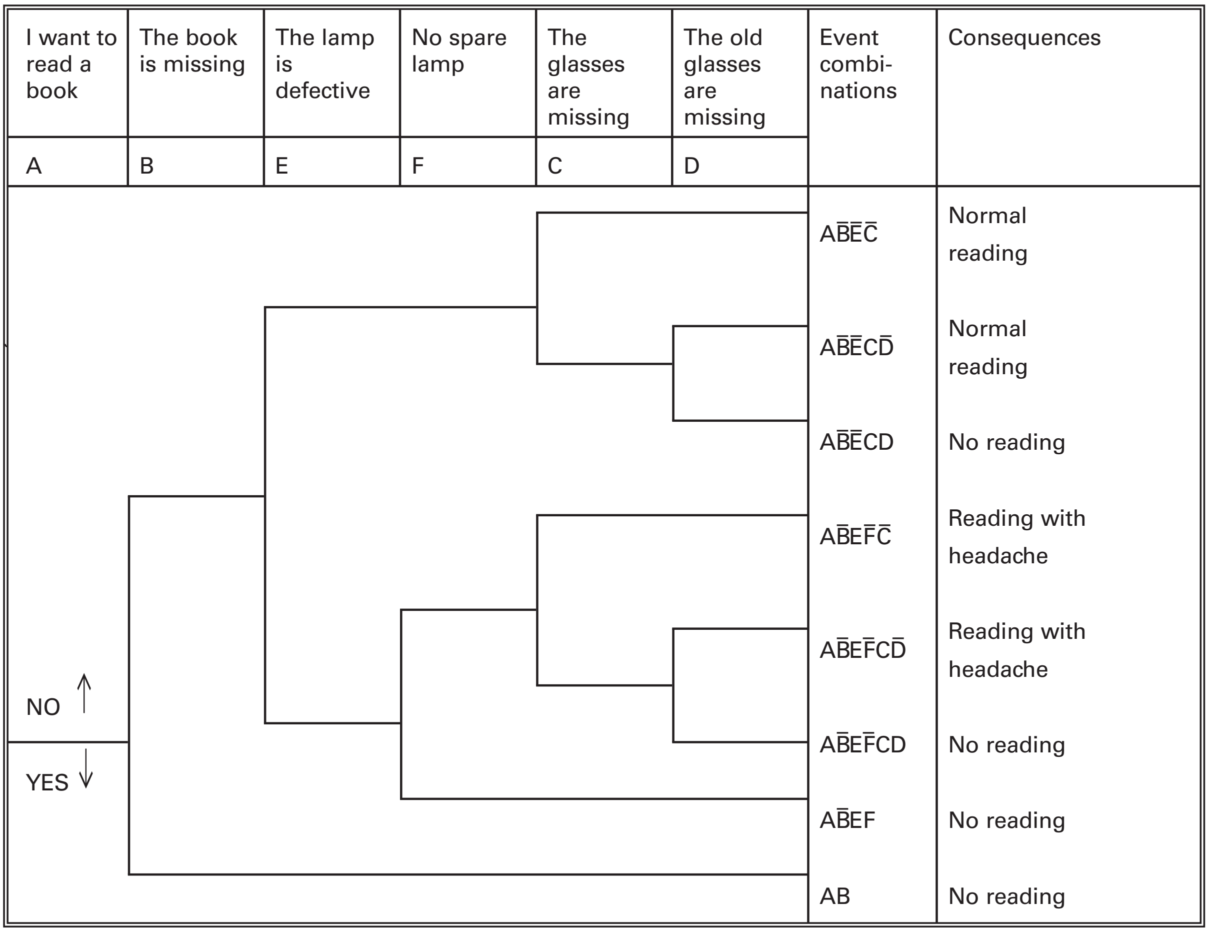
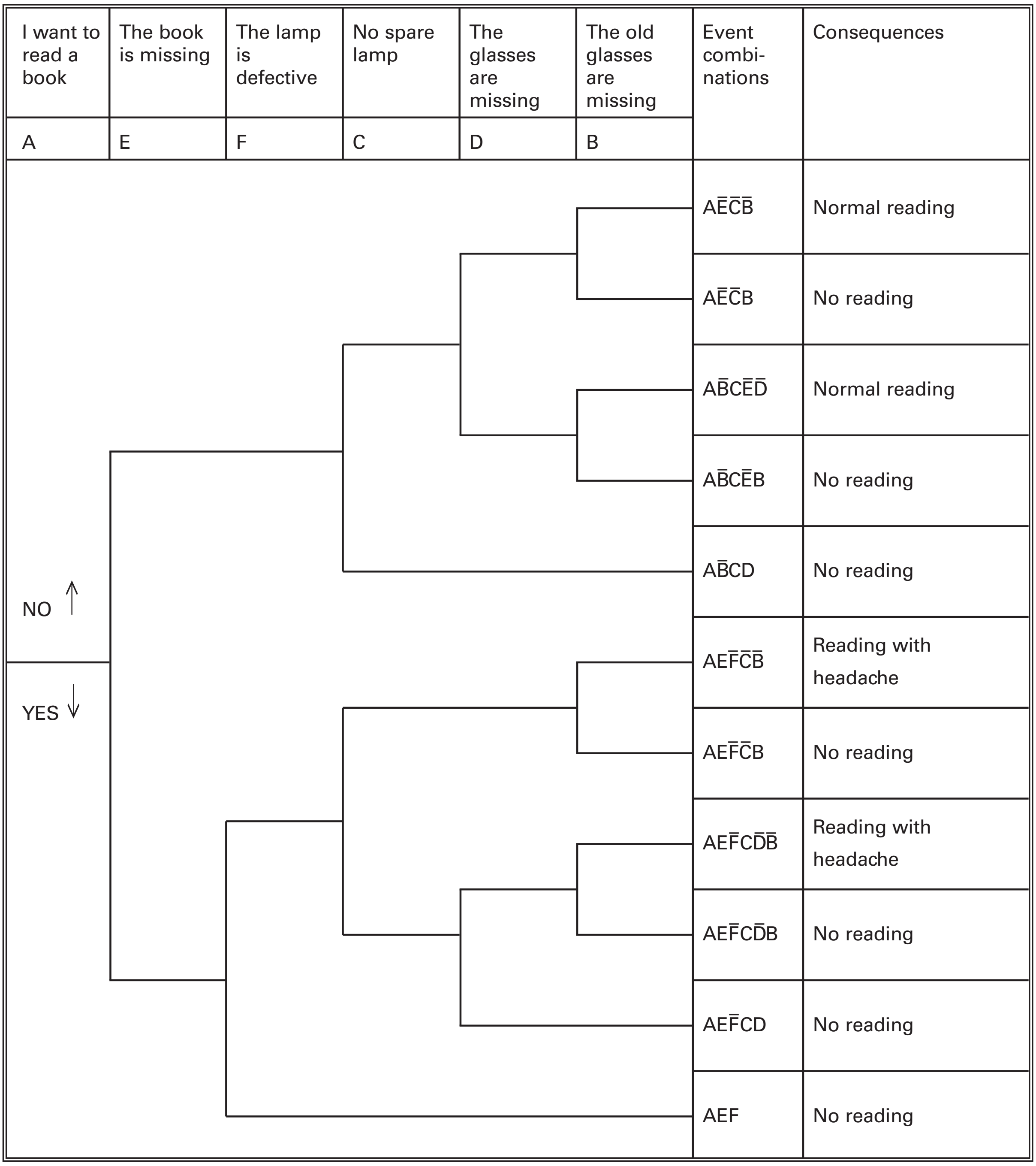


Figure 10.3: Heading events C and D interchanged with heading events E and F.

Table 10.2: Consequence classes after interchanging event combinations (E,F) and (C,D).

Normal reading	**Reading with headache**	**No reading**
$A\overline{B}\overline{C}\overline{E}$	$A\overline{B}\overline{C}E\overline{F}$	$A\overline{B}CD\overline{E}$
$A\overline{B}C\overline{D}\overline{E}$	$A\overline{B}C\overline{D}E\overline{F}$	$A\overline{B}CDE\overline{F}$
		AB
		$A\overline{B}EF$



Event combinations	Consequences
$A\bar{E}\bar{C}\bar{B}$	Normal reading
$A\bar{E}\bar{C}B$	No reading
$A\bar{B}C\bar{E}\bar{D}$	Normal reading
$A\bar{B}C\bar{E}B$	No reading
$A\bar{B}CD$	No reading
$AE\bar{F}\bar{C}\bar{B}$	Reading with headache
$AE\bar{F}\bar{C}B$	No reading
$AE\bar{F}C\bar{D}\bar{B}$	Reading with headache
$AE\bar{F}C\bar{D}B$	No reading
$AE\bar{F}CD$	No reading
AEF	No reading

Figure 10.4: The book is missing as last heading event.

It was noted earlier that, despite a difference in the event trees in figures 10.1 and 10.3 and a difference in tables 10.1 and 10.2, the probabilities of the consequente (totalled per column) in these tables are nonetheless the same. And that would imply that both event trees are correct. Below is the proof is provided for the columns covering:

“No reading”

It follows from the event tree in figure 10.1. that its probability is equal to (see Table 10.1).

$$
\begin{aligned}
&P_{A\bar{B}\bar{C}EF} + P_{A\bar{B}C\bar{D}EF} + P_{A\bar{B}CD} + P_{AB} = \\
&= \quad P_A.(1\text{-}P_B).(1\text{-}P_C).P_E.P_F + P_A.(1\text{-}P_B).P_C.(1\text{-}P_D).P_E.P_F + \\
&\qquad + P_A.(1\text{-}P_B).P_C.P_D + P_A.P_B \qquad (10.1) \\
&= \quad P_AP_EP_F - P_AP_BP_EP_F - P_AP_BP_EP_F + P_AP_BP_CP_EP_F + P_AP_BP_EP_F - P_AP_BP_CP_EP_F - \\
&\qquad - P_AP_CP_DP_EP_F + P_AP_BP_CP_DP_EP_F + P_AP_CP_D - P_AP_BP_CP_D + P_AP_B \\
&= \quad P_AP_B + P_AP_EP_F + P_AP_CP_D - P_AP_BP_EP_F - P_AP_BP_CP_D - P_AP_CP_DP_EP_F + \\
&\qquad + P_AP_BP_CP_DP_EP_F
\end{aligned}
$$

From the event tree in figure 10.3 it follows that its probability is equal to (see table 10.2):

$$
\begin{aligned}
&P_{A\bar{B}CD\bar{E}} + P_{A\bar{B}CDE\bar{F}} + P_{AB} + P_{A\bar{B}EF} \\
&= \quad P_A.(1\text{-}P_B).P_E.P_F + P_A.(1\text{-}P_B).(1\text{-}P_E).P_C.P_D + P_A.P_B + \\
&\qquad + PA.(1\text{-}PB).PE.(1\text{-}PF).PC.PD \\
&= \quad P_AP_EP_F - P_AP_BP_EP_F + P_AP_CP_D - P_AP_BP_CP_D - P_AP_CP_DP_E + P_AP_BP_CP_DP_E + \qquad (10.2) \\
&\qquad + P_AP_B + P_AP_CP_DP_E - P_AP_BP_CP_DP_E - P_AP_CP_DP_EP_F + P_AP_BP_CP_DP_EP_F \\
&= \quad P_AP_B + P_AP_EP_F + P_AP_CP_D - P_AP_BP_EP_F - P_AP_BP_CP_D - P_AP_CP_DP_EP_F + \\
&\qquad + P_AP_BP_CP_DP_EP_F
\end{aligned}
$$

This demonstrates that the two ”No reading” columns result in the same probability. So both event tree are equally correct.

10.4 EVENT TREE QUANTIFICATION

The quantification of an event tree will be explained will an example. The example is a post-incident analysis of a large leakage of pressurized flammable material from an isolated LPG storage tank. An HAZOP analysis indicates that the potential consequences include BLEVE (Boiling Liquid Expanding Vapor Explosion) of the tank if the leak is ignited (either immediately or by flashback). If the leak does not immediately ignite, the cloud can drift away. The cloud can be ignited in that case by several ignition sources and explode UVCE (Unconfined Vapor Cloud Explosion), or produce a flash fire some time later. An event tree is developed to predict possible outcomes from the leakage of LPG. The event tree is depicted in figure 10.5.

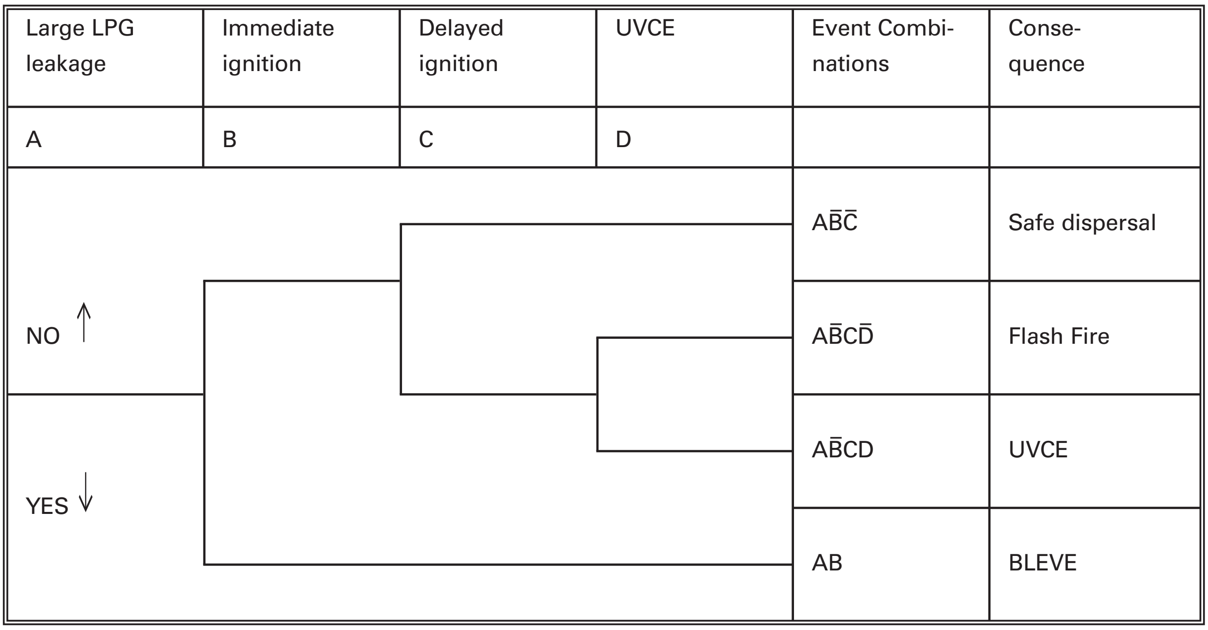


Figure 10.5: Event tree for the LPG leakage initiating event.

The heading events are defined as follows:

A: Large LPG leakage from vessel (Initiating event)
B: Immediate ignition
C: Delayed ignition
D: Unconfined Vapor Cloud Explosion.

A total of four outcomes are identified: a Boiling Liquid Expanding Vapor Explosion, A Unconfined Vapor Cloud Explosion, a Flash Fire or a Safe dispersal.

Assuming independence between the various heading events, the probability of occurrence of the different consequences can be calculated with the following formulas:

P(Safe dispersal) = P(A) * (1 - P(B)) * (1 - P(C)) (10.3)

P(Flash Fire) = P(A) * (1 - P(B)) * P(C) * (1 - P(D)) (10.4)

P(UVCE) = P(A) * (1 - P(B)) * P(C) * P(D) (10.5)

P(BLEVE) = P(A) * P(B) (10.6)

Suppose that the following data is valid for this situation:

P(A) =	5.0E-07	for one year of operation
P(B) =	0.7	-
P(C) =	0.7	-
P(D) =	0.1	-

Subs titution of these values in equations (10.1) up to and inciuding (10.4) gives:

P(Safe dispersal) = 5.0E-07 * (1 - 0.7) * (1 - 0.7)

= 4.5E-08 for one year of operation

P(Flash Fire) = 5.0E-07 * (1 - 0.7) * 0.7 * (1 - 0.1)

= 9.8E-08 for one year of operation

P(UVCE) = 5.0E-07 * (1 - 0.7) * 0.7 * 0.1

= 1.05E-08 for one year of operation

P(BLEVE) = 5.0E-07 * 0.7

= 3.5E-07 for one year of operation

The total frequency of all outcomes is a check to ensure that this equals the initiating event frequency of 5.0E-07 per year.

10.5 EVENT TREE DEVELOPMENT PROCEDURE

The construction of an event tree is sequential, and like fault tree analysis, is top-down (left-right in the usual event tree convention). The construction begins with the initiating event, and the temporal sequences of occurrence of all relevant safety functions or events are entered. Each branch of the event tree represents a separate outcome (event sequence). The process of event tree development can be divided in a number of steps. A concise description of each step will be provided:

Step 1 : *Identification of the initiating event.*

The initiating event, in many quantitative risk assessments, is a failure event corresponding to a release of hazardous material or a plant disturbance which can lead to serious consequences if one or more safety devices fail. This failure event wilt have been identified by one of the methods discussed in chapter 7 "Methods of identification of failure scenario's". The initiating event might correspond to a pipe leak, a vessel rupture, an internal explosion, etc.

Step 2: *Identification of safety function/ Hazard Promoting Factor and Outcome definition.*

A safety function is a device, action, or barrier, that can interrupt the sequence from an initiating event to a hazardous outcome. A hazard promoting factor may change the final outcome (e.g., from a dispersion cloud to a flash fire or to a UVCE).

Step 3: *Construction of event tree.*

The event tree graphically displays the chronological progression of an incident. Starting with the initiating event, the event tree is constructed left to right. At each heading or node two or more alternatives are analysed until a final outcome is obtained for each branch. Only nodes that materially affect the outcome should be shown explicitly in the event tree. Some branches may be more fully developed than others. In pre-incident analysis, the final sequence might correspond to successful termination of some initiating events or a specific failure mode. The listing of the safe recovery and incident conditions is an important output of this analysis. For a post-incident analysis, the final result might correspond to the type of incident outcome.

The event heading should be indicated at the top of the page, over the appropriate branch of the event tree. If possible the heading events should describe the undesired situation. It is usually to have the YES branch downward and the NO branch upward. Starting with the initiating event, each heading event is labelled with a letter identifier. Every final event sequence can then be specified with a unique letter combination. A bar over the letter indicates that the designated event did not occur.

Step 4: *Classify the outcomes.*

The objective in constructing the event tree is to identify important possible outcomes that are important contributors to risk to be quantified. Thus, if an estimated of the risk of offsite fatalities is the goal of the analysis, only outcomes relevant to that outcome need be developed. Branches leading to lesser consequences can be left undeveloped. Many outcomes developed through different branches of the event tree will be similar. The final event tree outcomes can be classified according to type of consequence model that must be employed to complete the analysis.

Step 5: *Estimation of the conditional probability of each branch in the event tree.*

each heading in the event tree (other than the initiating event) corresponds to a conditional probability of some outcome if the preceding event has occurred. Thus, the probabilities associated with each limb must sum to 1.0 for each heading. This is true for either binary or multiple outcomes from a node. The source of conditional probabilities may be historical records, plant and process data, equipment reliability data, human reliability data, expert opinion. It may be necessary to use fault tree techniques to determine some probabilities, especially for complex safety systems in pre-incident analysis.

Step 6: *Quantification of the outcomes.*

The frequency of each outcome may be determined by multiplying the initiating event frequency with the conditional probabilities along the path leading to that outcome. It should be emphasized that this type of quantification is only allowed if the initiating event frequency and the conditional probabilities can be considered all as independent events. If this is not the case the quantification techniques described in chapter 12, "accident Sequence Quantification" have to be used.

Step 7: *Evaluation.*

The results of the event tree analysis should be tested with common sense and against system or process understanding and historical records. Dominant contributors to risk can be identified and recommendations to decrease the risk level can be formulated.

10.6 REFERENCES

[10.1] Reliability Evaluation of Engineering Systems, Concepts and Techniques'
Roy Billington, Ronald N. Allan, Pitman Advanced Publishing Program,
Boston, London, Melbourne, 1985

[10.2] Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples,
Center for chemical process safety of the American Institute of Chemical Engineers,
New York, September 1992.

[10.3] Guidelines for Chemical Process Quantitative Risk Analysis,
Center for chemical process safety of the American Institute of Chemical Engineers,
New York, 1989.

MARKOV PROCESSES

CONTENTS

11.1 INTRODUCTION

The Markov approach can be applied to the random behaviour of systems that vary discretely or continuously with respect to time and space. This discrete or continuous random variation is known as a stochastic process. An example of a stochastic process is a Poisson process. This process describes the random failure of a component, regardless of the physical background that causes this failure. A Markov process is a special form of a stochastic process.

Markov properties:
A stochastic process is called a Markov process if the probability distribution of progress in the process is exclusively determined by the present, whereas the history has no influence on it. This Markov property means that the process has no memory, which implies that if the history until time t is known, progress in the process solely depends on the state of the process at
time t.

As a result of the Markov properties a repaired component is considered to be as good as new and the failure rate of each component is assumed to be independent of the failure sequence of these components. Literature on Markov processes can be found in references [11.1] to [11.5].

Applications in reliability analysis:
Within reliability analysis in general Markov processes with a discrete state-space and a continuous time-space are used. In this chapter binary components are solely discussed, which means components which can be in two states: in operation or failed.

In this chapter only Markov processes with a constant failure and repair rate (transition rates) will be explained. Markov models with constant transition rates between the different system states are called homogeneous. This means that the failure process as welt as the repair process are exponentially distributed. If the transition rates are functions of time, the model is called nonhomogeneous. Given the fact that the repair process is exponentially distributed, the following relation between the repair rate and the mean time to repair can be derived:

$$\mu = \frac{1}{\theta} \tag{11.1}$$

Application:
The Markov approach is very useful in analysing different maintenance strategies. It is very easy to analyse the impact of more repair teams on the unavailability of the system. The Markov approach can also be applied to calculate the probability of failure on demand of a safety system. The Markov approach is very suitable if one is interested in the time-dependent dynamic behaviour of a system.

A particular problem of the Markov approach is that the number of system states is increasing very rapidly with the number of components or units. A possible solution to this problem is to apply a fault tree analysis first and to quantify each minimal cut set with a Markov diagram. This approach is called the Markov cut-set approach. Another solution is not to use the Markov approach but to apply the Fault Tree Technique or Monte Carlo simulation (see chapters 8 and 15). Another disadvantage of the Markov approach is that the interpretations of the results are more difficult than in the case of fault trees.

11.2 NOMENCLATURE

			Dimension
F(0,t)	=	Probability of failure in time interval (0.t)	-
P_i	=	Probability that the system is in state i	-
PFD	=	Probability of failure on demand	-
Q	=	Failure to start probability	-
t	=	Time	hour
β	=	Beta-factor-dependent failure model	-
λ_i	=	Failure rate for component i	-/hour
μ_i	=	Repair rate for component i	-/hour
θ	=	Mean time to repair	hour
Δt	=	Infinitesimal time interval	hour

<u>Subscript</u>

A	=	Component A is up	-
$\underline{A}$	=	Component A is down	-
B	=	Component B is up	-
$\underline{B}$	=	Component B is down	-
C	=	Component C is up	-
$\underline{C}$	=	Component C is down	-

11.3 STATE TRANSITION OR MARKOV DIAGRAM

A Markov analysis makes use of a state transition diagram which is a pictorial representation of all relevant system states in which the system can reside. The state transition diagram models the system behaviour in relation to the proper functioning or failure of the various components of the system with respect to time. The system as a whole can exist in many different states, each being determined by the particular combination of failed (down) and functioning (up) components of the system. This implies that the system jumps from one state to another if one of the components fails. This kind of model is generally called a discrete-state continuous time model.

In principle all relevant states in which the system can reside should be included in a state transition diagram and all known ways in which transitions between states can occur should be inserted. The generation of a state transition diagram is one of the most important parts of the Markov analysis. It translates the analyst's knowledge of the operation of the system into a mathematical model that can be solved by using Markov techniques. It must be emphasized that there are no mathematical models that eliminate the need to exercise engineering judgement and the requirement of a thorough and extensive understanding of the physical and logical operation of the system. The analysts must first translate the system into a state-space diagram recognizing both states of the system, the way these states communicate and the values of the transition rates.

The Markov analysis technique requires that the various states in the state-space diagram be mutually exclusive; only one state at a time can be occupied by the system.

In a state transition diagram each system state is represented by a circle, whereas the number in the circle characterizes the state. The possible transitions are represented by arrows between the different states.

Transition probability:
Figure 11.1 depicts a system that consists of 4 possible states in which it is possible to jump from state 1 to state 3, from state 2 to state 3 and from state 3 to state 4.

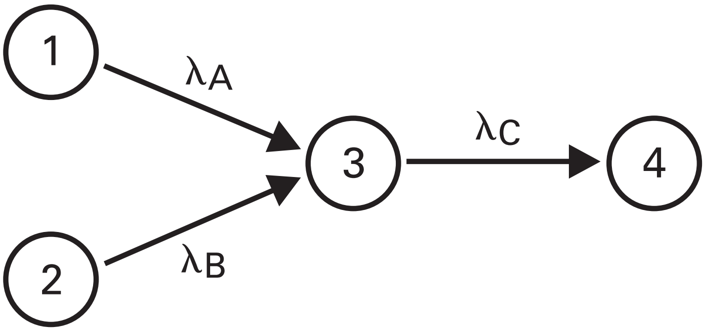


Figure 11.1: Exemple of a state-space diagram.

Given that the system is in state 3 at time t, the Markov constraint implies that the transition probability from state 3 to state 4 in time interval Δt, is given by: λc.Δt.

The probability that the system will jump from state 3 to state 4 in time interval Δt can be calculated with the following formula:

$$P_{3\rightarrow4}(\Delta t)=P_3(t)\ \lambda_C\ \Delta t \qquad (11.2)$$

This formula will be used to derive the differential equations which describe the behaviour in time of an on-line repairable one-unit system.

11.4 ON-LINE REPAIRABLE ONE UNIT SYSTEM

Consider a one-unit system that consists of one on-line repairable component. Repair is started immediately after failure of the system. For the simplest case, the corresponding state transition diagram comprises only two states:

State 1: Component is operating (up)

State 2: Component has failed (down)

The system jumps from state one to state two if the component fails.This is indicated by an arrow from state 1 to state 2. If the component is repaired, the system jumps from state 2 to state 1. Also, this is indicated by an arrow.The state-space diagram for this simple case is shown in figure 11.2.

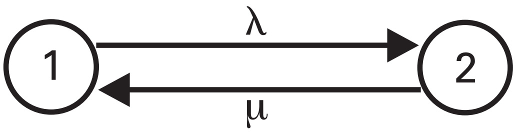


Figure 11.2: State-space diagram for a one-unit system.

The probability that the system is in state 1 is denoted as P1 and the probability that the system is in state 2 is denoted as P2. Since at any time the system can only be in one state, the following boundary condition must apply:

$$P1 + P2 = 1 \qquad (11.3)$$

Within a time period At, one can write the increase or decrease of the probability that the system will be in state 1 or state 2:

$$\begin{aligned} \Delta P1 &= -\lambda\ \Delta t\ P1 + \mu\ \Delta t\ P2 \\ \Delta P2 &= +\lambda\ \Delta t\ P1 - \mu\ \Delta t\ P2 \end{aligned} \tag{11.4}$$

The probability of being in state 1 will be decreased by failure of the component, represented by the term: $-\lambda\ \Delta t\ P1$. On the other hand the probability of being in state 1 will be increased by the possibility of a repair denoted by: $+\mu\ \Delta t\ P2$. Dividing both equations by Δt results in two differential equations:

$$\begin{aligned} \frac{dP1}{dt} &= -\lambda\ P1 + \mu\ P2 \\ \frac{dP2}{dt} &= +\lambda\ P1 - \mu\ P2 \end{aligned} \tag{11.5}$$

Formula (11.5) consists of two coupled ordinary differential equations that must be solved in order to determine P1 and P2. By substitution of formula (11.3) into the second equation of formula (11.5), one differential equation is obtained that describes the probability that the system is in state 2.

$$\frac{dP2}{dt} + (\lambda+\mu)\ P2 = \lambda \tag{11.6}$$

By using the Euler substitution, differential equation (11.6) can be solved. Given the initial condition: $P2(t=0) = 0$, it follows that:

$$P2 = \frac{\lambda}{\lambda + \mu} \quad (1-e^{-(\lambda + \mu)t}) \tag{11.7}$$

The probability P2 as a function of time is depicted in figure 11.3.

From figure 11.3 it can be concluded that after a certain period of time a steady state condition is achieved. This result can also be obtained from equation (11.7) if the value of time t becomes very large ($t \to \infty$).

$$\begin{aligned} t \to \infty \quad : \quad P2 &= \frac{\lambda}{\lambda + \mu} \\ &\approx \lambda + \theta \end{aligned} \tag{11.8}$$

In many practical situations, it turns out that the mean time to repair (MTTR) of a system is very short in comparison with its mean time to failure (MTTF), which implies that $\mu > > \lambda$.

If a system is composed of a number of on-line repairable components, it can be stated that the steady state condition is reached after three times the largest mean repair duration.

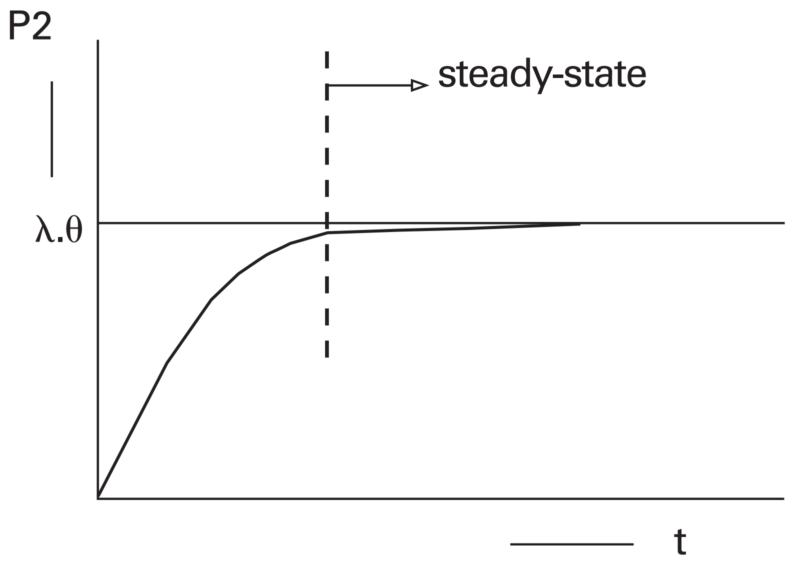


Figure 11.3: Probability of being in state 2 as a function of time.

Steady-state solution:

For a system that is composed of on-line repairable components only, the non-steady-state part is not very interesting from a practical point of view. The steady-state solution can be derived simply by taking the time derivatives of the differential equations describing the Markov process as equal to zero.

$$\left.\begin{array}{l}\dfrac{dP1}{dt} = 0 \\ \\ \dfrac{dP2}{dt} = 0\end{array}\right. \Rrightarrow \begin{array}{l}-\lambda\ P1 + \mu\ P2 = 0 \\ \lambda\ P1 - \mu\ P2 = 0\end{array} \qquad (11.9)$$

This results in a number of algebraical equations which are not independent. However, if one replaces one algebraical equation by the equation that describes the boundary condition, one obtains a correct number of independent algebraical equations which can be solved easily.

$$\begin{array}{r}\lambda\ P1 - \mu\ P2 = 0 \\ P1 + P2 = 1\end{array} \qquad (11.10)$$

Solution:

$$P = \frac{\mu}{\lambda + \mu}$$

$$P2 = \frac{\lambda}{\lambda + \mu} \qquad (11.11)$$

11.5 ONE-OUT-OF-TWO SYSTEM - TWO REPAIR TEAMS

In this paragraph a one-out-of-two system wilt be analysed that consists of two redundant on-line repairable components (see figure 11.4). Two repair teams are available, so each component can be repaired immediately after failure of the component.

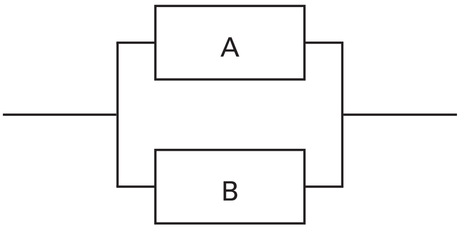


Figure 11.4: One-out-of-two system.

The following system states can be identified:

State 1: Component A is in operation
Component B is in operation

State 2: Component A has failed and is under repair
Component B is in operation

State 3: Component A is in operation
Component B has failed and is under repair

State 4: Component A has failed and is under repair
Component B has failed and is under repair

Considering the identified system states and the possible transitions between those system states, a state-space diagram as depicted in figure 11.5 can be drawn. If dependent failures have to be included in the state transition diagram, an additional arrow between state 1 and state 4 has to be added representing a dependent failure of both units.

Given the state-space diagram, the corresponding differential equations can be easily derived. Row i of the transition matrix represents the decrease or increase in the probability of being in state i.

The elements of the transition matrix can be derived by taking into account the following rules:

Rule 1: The main diagonal element of row i and column i represent the negative sum of the transitions out of state i.

Rule 2: The non-main diagonal elements of row i and column j represent the transition of state i to state j.

One way of checking the transition matrix is to make use of the property of the matrix that the sum of all elements in each column must be zero.

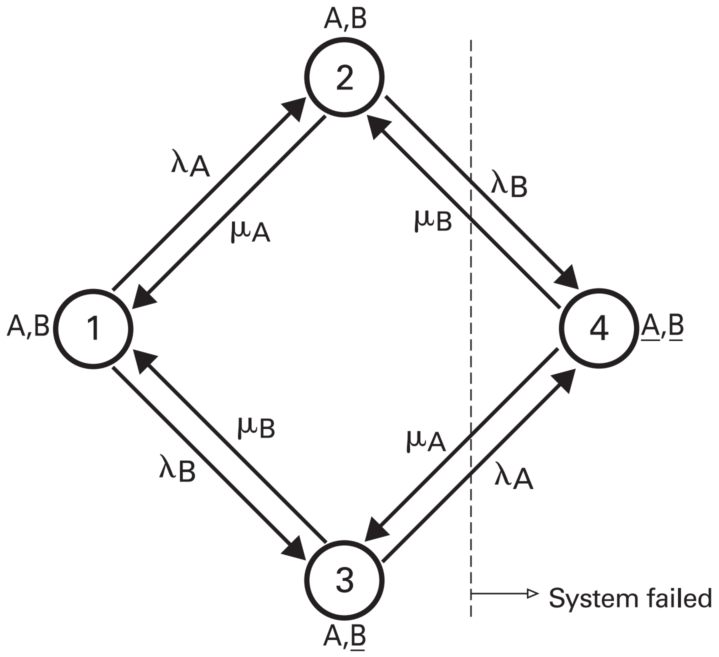


Figure 11.5: State-space diagram one-out-of-two system.

$$\begin{bmatrix} \frac{dP1}{dt} \\ \frac{dP2}{dt} \\ \frac{dP3}{dt} \\ \frac{dP4}{dt} \end{bmatrix} = \begin{bmatrix} -\lambda_A-\lambda_B & \mu_A & \mu_B & 0 \\ \lambda_A & -\lambda_B-\mu_A & 0 & \mu_B \\ \lambda_B & 0 & -\lambda_A-\mu_B & \mu_A \\ 0 & \lambda_B & \lambda_A & -\mu_A-\mu_B \end{bmatrix} \bullet \begin{bmatrix} P1 \\ P2 \\ P3 \\ P4 \end{bmatrix} \qquad (11.12)$$

The steady-state solution can be determined by taking the time derivatives in formula (11.12) as equal to zero and by replacing one of the algebraical equations by the following boundary condition:

$$P1 + P2 + P3 + P4 = 1 \tag{11.13}$$

The state of interest is state 4, because this state represents failure of the complete system. The steady-state solution of state 4 is determined by the solution of a set of four algebraic equations taking into account $\mu> >\lambda$ for all units involved. This assumption generally holds in practice. If the number of algebraic equations is not too high, this set can be resolved by hand.

The final value of the steady-state probability of being in state 4 is equal to the mean unavailability of the two components of the system consisting of two on-line reparable components and is given by:

$$\mu_i » \lambda_j \qquad i = A,B \qquad j = A,B$$

$$P4 \approx \frac{\lambda_A \; \lambda_B}{(\mu_A + \lambda_B) \; (\mu_B + \lambda_B)} \tag{11.14}$$

$$\approx \lambda_A \; \lambda_B \; \theta_A \; \theta_B$$

Using numerical integration techniques, the system of differential equations as given in formula (11.12) can be solved. Figure 11.6 presents an example. From the values of μ_A and μ_B it follows that the maximum mean repair time is equal to 100 hours. It can be seen that after approximately three times this maximum repair time (300 hours) the steady-state solution has nearly been reached.

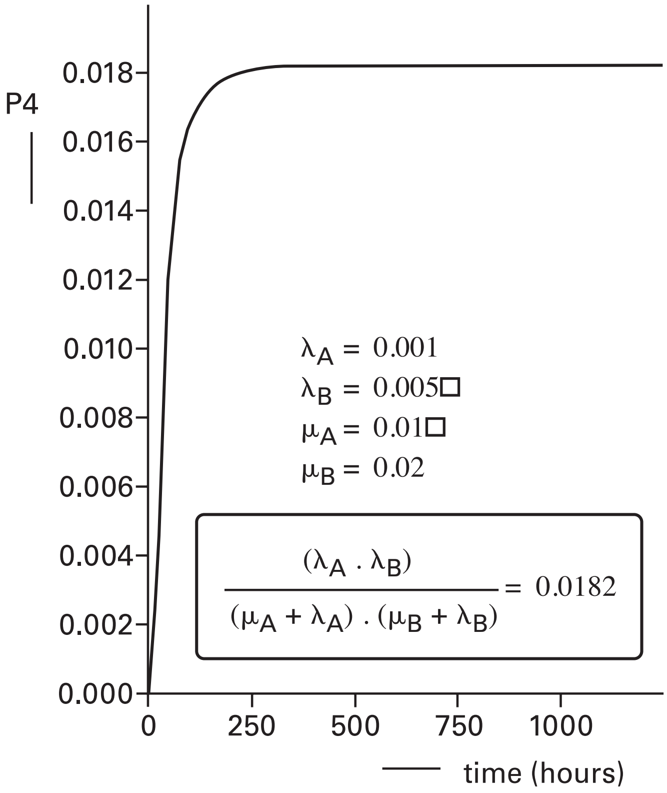


Figure 11.6: Time-dependent solution for state number 4.

11.6 ONE OUT OF TWO SYSTEM - ONE REPAIR TEAM

In this paragraph a one out of two system consisting of two on-line repairable components but with only one repair team available will be analysed (see fgure 11.7). If both components are failed, component A is repaired first. Component A must be regarded as the component with the smallest repair duration.

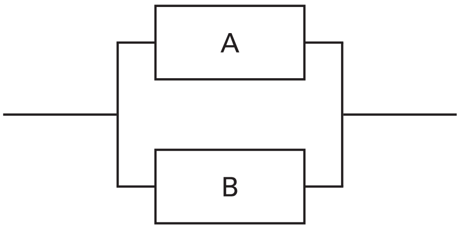


Figure 11.7: One-out-of-two component system.

The following system states can be identified:

State 1: Component A is in operation
Component B is in operation

State 2: Component A has failed and is under repair
Component B is in operation

State 3: Component A is in operation
Component B has failed and is under repair

State 4: Component A has failed and is under repair
Component B has failed but has to wait until completion of repair of component A.

The corresponding state-space diagram is depicted in figure 11.8. One can argue that state four must be split into two different states, 4A and 4B. State 4A represents repair of component A and component B failed. This state corresponds with the situation that component A failed first and component B failed during repair of component A. State 4B represents partial repair of component B and a switch-over of the maintenance crew from component B to component A after failure of component A during repair of component B. Given the Markov property that the process has no memory and that the transition rates are assumed to be constant, both states 4A and 4B can be combined into one state.

From the state-space diagram the differential equations can be obtained. In matrix form they are:

$$\begin{bmatrix} \frac{dP1}{dt} \\ \frac{dP2}{dt} \\ \frac{dP3}{dt} \\ \frac{dP4}{dt} \end{bmatrix} = \begin{bmatrix} -\lambda_A-\lambda_B & \mu_A & \mu_B & 0 \\ \lambda_A & -\lambda_B-\mu_A & 0 & 0 \\ \lambda_B & 0 & -\lambda_A-\mu_B & \mu_A \\ 0 & \lambda_B & \lambda_A & -\mu_A \end{bmatrix} \bullet \begin{bmatrix} P1 \\ P2 \\ P3 \\ P4 \end{bmatrix} \qquad (11.15)$$

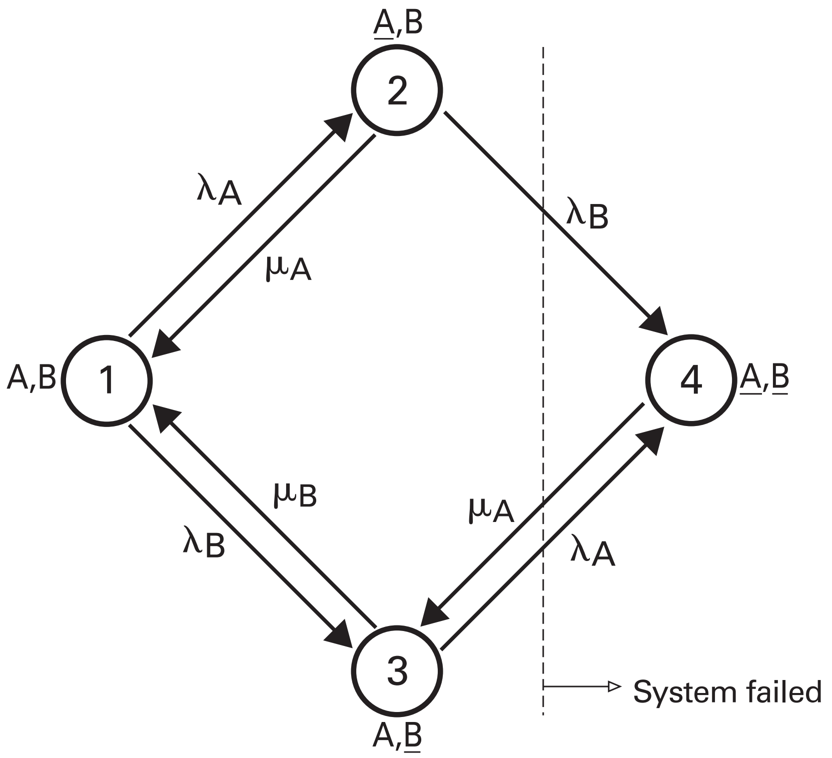


Figure 11.8: State-space diagram one-out-of-two system, one repair team

System state 4 represents total system failure. The steady-state solution for state 4 can be obtained by taking the time derivatives of equation (11.15) as equal to zero. One of the remaining algebraical equations is replaced by the boundary condition (see equation (11.13)) and as the set of four algebraical equations for state 4 is solved. The result is presented as formula (11.16).

Formula (11.16) must be used if only one repair team is available and the component with the smallest repair duration is repaired first in case of a system failure. Formula (11.16) is listed in chapter 9 as formula B-3.

$\mu_i » \lambda_j \qquad i = A,B \qquad j = A,B$

$$P4 = \frac{\lambda_A \ \lambda_B \ (\mu_A + \lambda_B)}{\mu_A{}^2 \ \lambda_B} \qquad (11.16)$$

$$= \lambda_A \ \lambda_B \ \theta_A \ (\theta_A + \theta_B)$$

11.7 THE PROBABILITY OF FAILURE OF A ONE OUT OF TWO SYSTEM

Using the Markov technique it is also possible to determine the probability of failure of a one-out-of-two system consisting of two on-line repairable components. To calculate the probability of failure in time period (0,t), the state-space diagram depicted in figure 11.5 needs to be adjusted. By eliminating the repair possibilities in state 4, probability P4 equals the probability of failure.

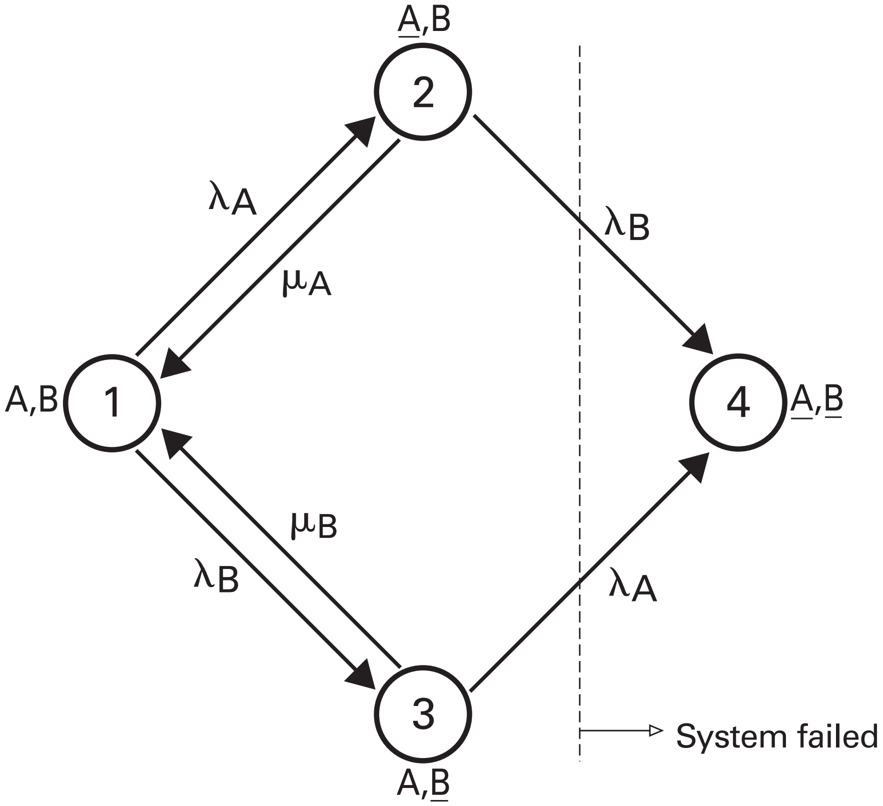


Figure 11.9: State-space diagram probability of failure with one-out-of-two system.

State 4 has now become a so-called absorption state. A state is called an absorption state if no transition to another state is possible after entering this state. Yet a steady-state situation is not possible and probability P4 will increase from zero to eventually one, see figure 11.9. In reference [11.4] the solution of this situation is presented, provided that components A and B are identical.

Identical components:

$$\lambda = \lambda_A = \lambda_B$$
$$\mu = \mu_A = \mu_B \qquad (11.17)$$

Solution:
The differential equation can be solved with Laplace transformation, see reference [11.4]. The probability of failure is given by:

$$F(0,t) = \frac{S1\ (1 - e^{S2\ t}) - S2\ (1 - e^{S1\ t})}{S1 - S2} \qquad (11.18)$$

where:

$$S1 = \frac{3\lambda + \mu + \sqrt{\lambda^2 + 6\lambda\mu + \mu^2}}{2}$$
$$S2 = \frac{3\lambda + \mu - \sqrt{\lambda^2 + 6\lambda\mu + \mu^2}}{2} \qquad (11.19)$$

11.8 STAND-BY SYSTEM

In figure 11.10 the lay-out of an emergency power supply is depicted. In case of normal operation both busbars and the emergency busbar are fed from the grid. If power supply from the grid fails, the main busbar and the emergency busbar are disconnected. The diesel generator starts and is switched onto the emergency busbar.

Such a system can be analysed easily by means of a fault tree. One has to include the failure of power supply from the grid, the control system, the switches and the failure of the diesel generator. One of the minimal cut sets will describe the failure of power supply from the grid in combination with the failure of power supply from the diesel generator. This specific minimal cut set can be quantified excellently with a Markov process.

The following system states can be defined:

State 1: Grid is in operation (Component A)
Diesel generator available (Component B)

State 2: Grid has failed and is under repair
Diesel generator is in operation

State 3: Grid has failed and is under repair
Diesel generator has failed and is under repair

State 4: Grid has been restored
Diesel generator is under repair

The corresponding state space diagram is depicted in figure 11.11. Special attention is called for the failure-to-start probability Q of the emergency diesel generator.

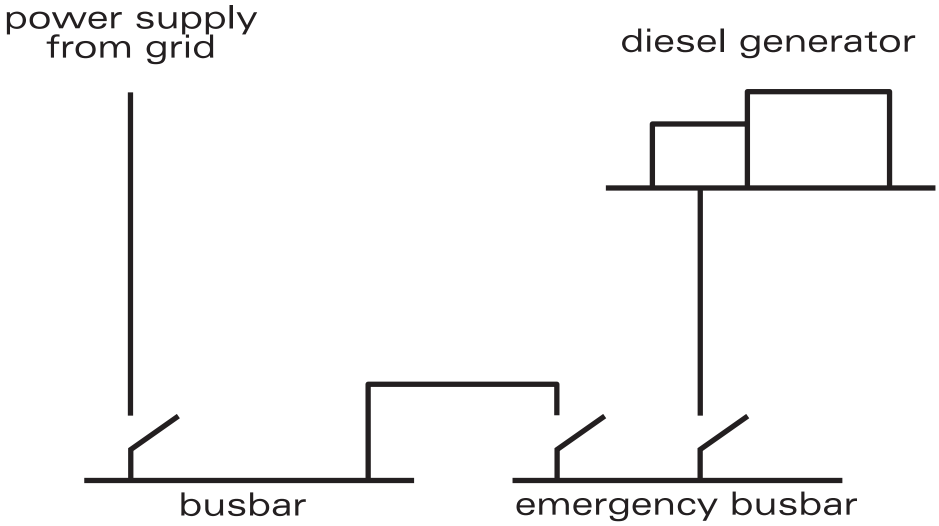


Figure 11.10: System lay-out of emergency power supply.

In state 1 both busbars are fed from the grid. The diesel generator is available but does not run. In state 2 power supply from grid is not available but the diesel generator has started and is in operation. In state 3 power supply from both the grid and the diesel generator is not available. The unavailability of the diesel generator can be a result of either a failure to start or a failure to run after a successful start. The distribution company will repair the power supply and the repair team of the owner of the emergency power supply will try to fix the diesel generator. In state 4 power supply from the grid is restored. However the diesel generator is still under repair.

From the state space diagram the following system of differential equations can be derived:

$$\begin{bmatrix} \frac{dP1}{dt} \\ \frac{dP2}{dt} \\ \frac{dP3}{dt} \\ \frac{dP4}{dt} \end{bmatrix} = \begin{bmatrix} -Q_B-\lambda_A-(1\text{-}Q_B)\lambda_A & \mu_A & 0 & \mu_B \\ (1\text{-}Q_B)\lambda_A & -\lambda_B-\mu_A & \mu_B & 0 \\ Q_B\lambda_A & \lambda_B & -\lambda_A-\mu_B & \lambda_A \\ 0 & 0 & \mu_A & -\mu_B-\mu_A \end{bmatrix} \bullet \begin{bmatrix} P1 \\ P2 \\ P3 \\ P4 \end{bmatrix} \tag{11.20}$$

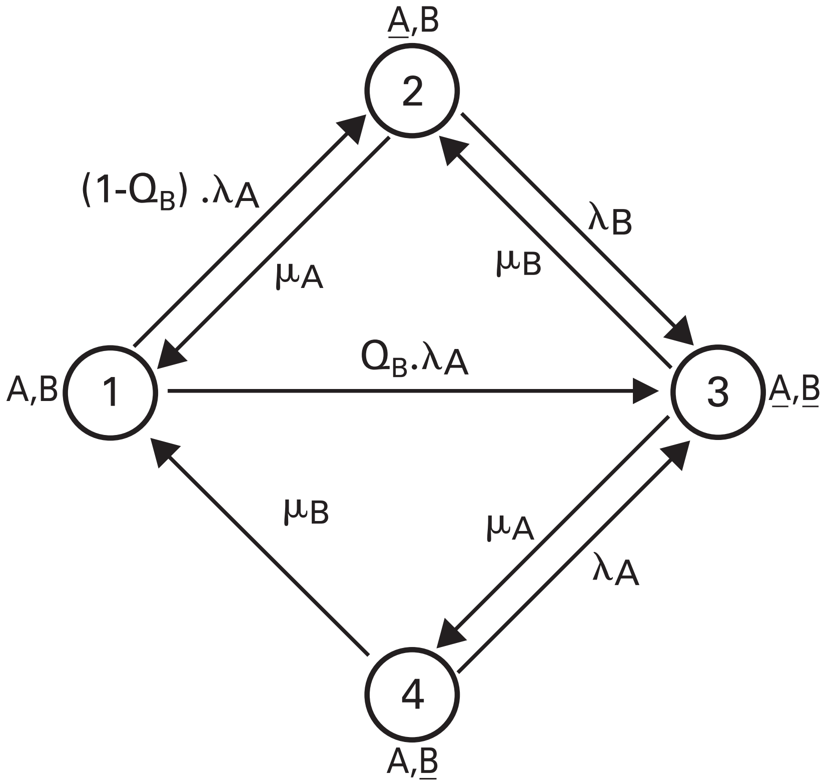


Figure 11.11: State-space diagram of stand-by system

State 3 represents failure of power supply to the emergency busbar. The steady-state solution for state P3 is:

$$P3 \approx \frac{\lambda_A \ \lambda_B + \lambda_A \ Q_B \ \mu_A}{\mu_A \ (\mu_A + \mu_B)}$$

$$\approx (\lambda_A \ \theta_A \ \lambda_B + \lambda_A \ Q_B) \ \frac{(\theta_A \ \theta_B)}{(\theta_A + \theta_B)} \qquad (11.21)$$

If only one repair team is available to restore the grid and repair of the diesel generator is not considered, the transition from state 3 to state 2 (μ_B) has to be removed. The solution now becomes:

$$P3 \approx \quad (\lambda_A \ \theta_A \ \lambda_B + \lambda_A \ Q_B) \ \theta_A \qquad (11.22)$$

11.9 GENERAL APPROACH

Each Markov analysis can be divided into a number of separate steps. A short description of each step will be provided.

Step 1: System familiarization

Before a state-space diagram can be composed, the analyst has to understand exactly how the system operates and which operation, test and maintenance procedures are used. He also has to identify potential dependent and human failures.

Step 2: State-space diagram development

To compose a state-space diagram, all mutually exclusive system states have to be defined. The states of the system at time t = 0 are called the initial states and those representing a final or equilibrium state are called final states. A state is called an absorption state if no transition to another state is possible after entering this state.

Step 3: Composition of transition matrix

After completion of the state-space diagram the transition matrix and the initial conditions have to be determined.

Step 4: Data analysis

In every reliability analysis data analysis is very important to obtain realistic results. If available, possible generic data has to be combined with plant-specific data. All failure and repair rates have to be determined. For stand-by components the test periods used in practice have to be identified.

Step 5: Solution of mathematical model

Depending on the objectives of the study, the steady-state solution or the time-dependent solution must be calculated. For some simple cases solutions in closed form can be applied. Numerical integration techniques can be used in more complex situations.

Step 6: Sensitivity analysis

Sensitivity and importance analysis are useful to identify critical input parameters. It might be necessary to perform additional analysis to reduce the uncertainty in the results.

Step 7: Interpretation of the results

The final step in a Markov analysis is to formulate insights obtained from the analysis.

The approach will be explained with an example of a safety device.

11.10 EXAMPLE OF A HIGH INTEGRITY PRESSURE PROTECTION SYSTEM

In figure 11.12 an example of the lay-out of a high-pressure protection system is provided. The objective of a high-pressure protection system is to protect the low-pressure part of the system against overpressure by closing of at least one of the two shut-off valves. The shut-off valves are spring-return valves and are operated by solenoid valves. The spring will close the shut-off valve after loss of air supply. The complete system is designed fail-safe against loss of power supply or loss of air supply.

The solenoid valves are de-activated by a logic element. Pressure switches are used as input of the one-out-of-two logic element. If a preset pressure level is reached and the pressure switches detect this situation, the solenoid valves are de-activated by the logic. De-activation of the solenoid valves releases air pressure from the shut-off valves, which in turn will be closed by the springs.

For this example a Markov analysis will be performed to calculate the probability of failure on demand, given a high-pressure situation.

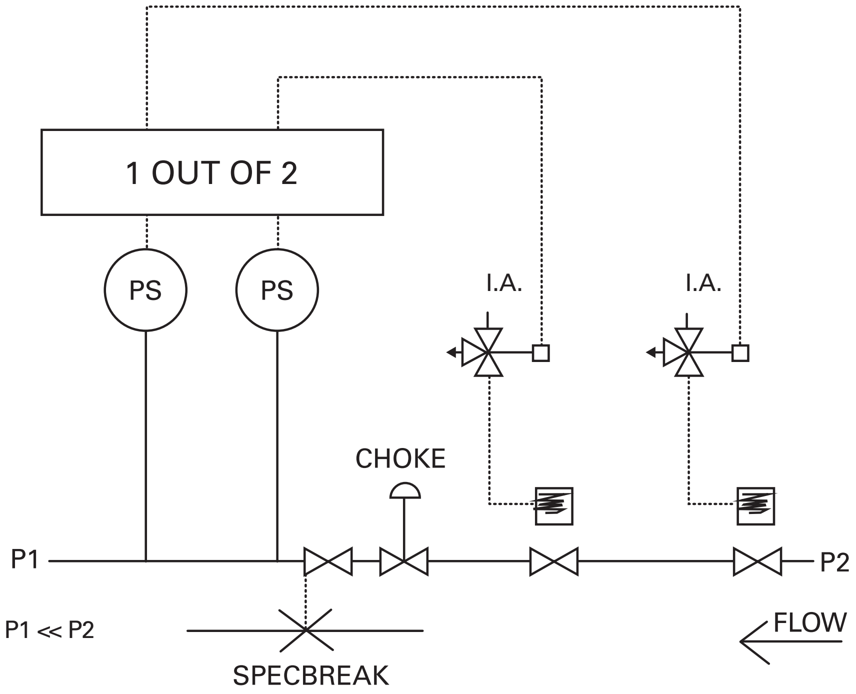


Figure 11.12: Lay-out of high-integrity pressure protection system.

System familiarization:

The system is tested yearly. Testing is performed during annual maintenance. Review of the test procedure showed that a part of the logic is not covered by the test performed annually. This part is only tested once every ten years, during an overhaul performed every ten years. The same procedures are used to calibrate the pressure switches and calibration of the pressure switches is performed by the same maintenance team. Both pressure switches are calibrated on a single day. Also, the solenoid valves and the shut-off valves are maintained in accordance with the same procedures and by the same maintenance team. This implies that the pressure switches as well as the solenoid valves and the shut-off valves are vulnerable to dependent failures. For this reason dependent failures have to be included in the state space diagram.

State space diagram development:

To make the state transition diagram easier to understand and to limit the computations as much as possible, attempts should be made to construct state transition diagrams using as few a number of states as possible. For instance all states that represent system failure and that are covered by the annually performed test can be combined into one system state. Taking into account only the most important failure modes of the system nine system states can be defined. A short description of each system state will be provided.

State 1: All components are up.

State 2: Pressure switch 1 has failed.

State 3: Pressure switch 2 has failed.

State 4: Solenoid valve 1 has failed.

State 5: Solenoid valve 2 has failed.

State 6: Shut-off valve 1 has failed.

State 7: Shut-off valve 2 has failed.

State 8: State eight represents failure of the system that is covered by the annually performed test. The system will be in state eight if:

- Both pressure switches are failed
- Both solenoid valves are failed
- Solenoid valve 1 has failed and failure of solenoid valve 2 or shut off valve 2.
- Solenoid valve 2 has failed and failure of solenoid valve 1 or shut off valve 1.
- Shut off valve 1 has failed and failure of solenoid valve 2 or shut off valve 2.
- Shut off valve 2 has failed and failure of solenoid valve 1 or shut off valve 1.
- Logic 1 has failed or a dependent failure of both shut off valves or both solenoid valves or both pressure switches.

State 9: State nine represents system failure due to failure of that part of the logic that is covered by the test performed during overhaul carried out every ten years.

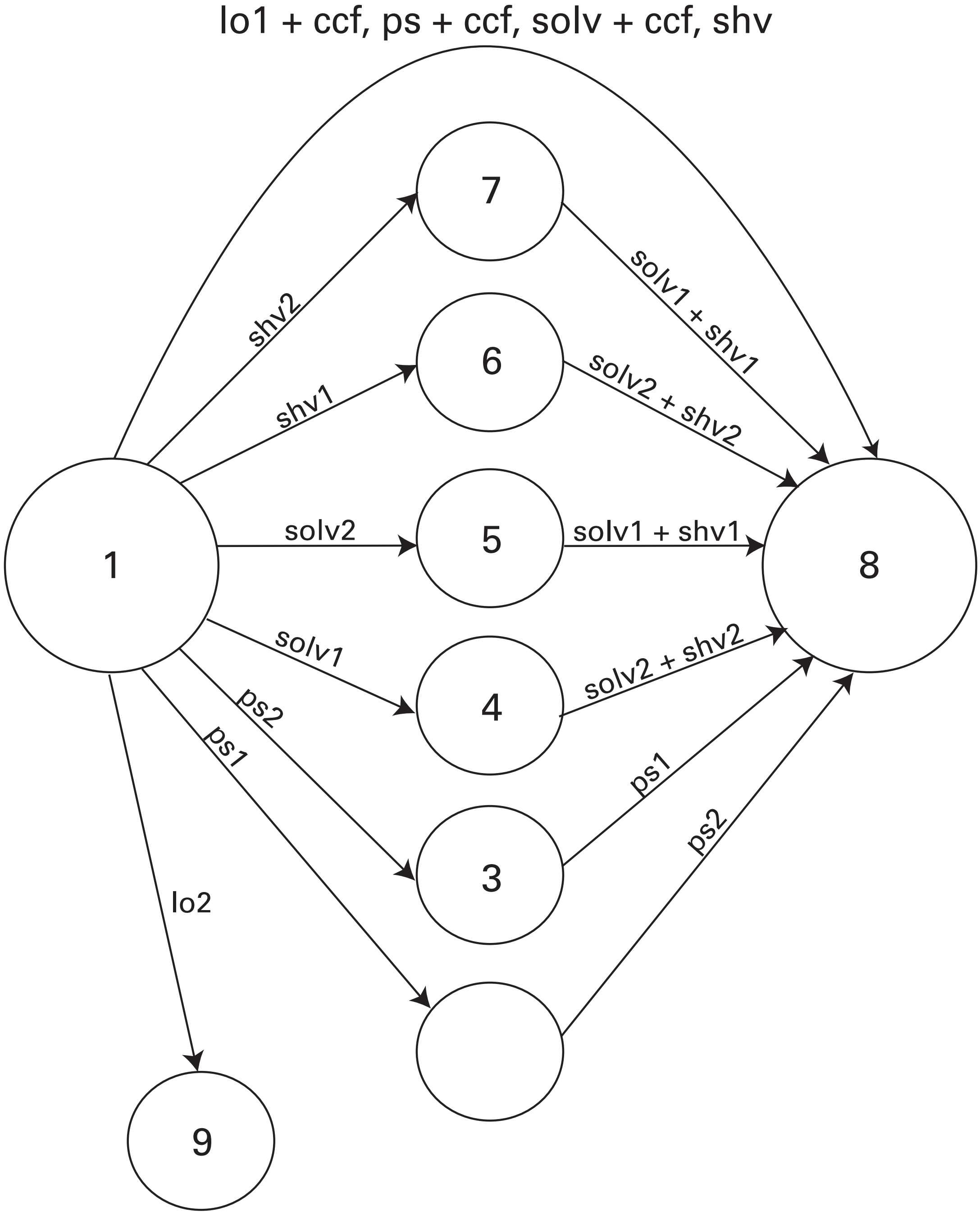


Figure 11.13: State-space diagram of high-integrity pressure protection system.

Composition of transition matrix:

Considering the state-space diagram, the transition rates between the different states can be defined as follows:

$\lambda_{1-2} = \lambda_{ps1}$

$\lambda_{1-3} = \lambda_{ps2}$

$\lambda_{1-4} = \lambda_{solv1}$

$\lambda_{1-5} = \lambda_{solv2}$

$\lambda_{1-6} = \lambda_{shv1}$

$\lambda_{1-7} = \lambda_{shv2}$

$\lambda_{1-8} = \lambda_{lo1} + \lambda_{ccf,shv} + \lambda_{ccf,solv} + \lambda_{ccf,ps}$

$\lambda_{1-9} = \lambda_{lo2}$

$\lambda_{2-8} = \lambda_{ps2}$

$\lambda_{3-8} = \lambda_{ps1}$

$\lambda_{4-8} = \lambda_{solv2} + \lambda_{shv2}$

$\lambda_{5-8} = \lambda_{solv1} + \lambda_{shv1}$

$\lambda_{6-8} = \lambda_{solv2} + \lambda_{shv2}$

$\lambda_{7-8} = \lambda_{solv1} + \lambda_{shv1}$

Nomenclature:

ps	:	pressure switch
shv	:	shut-off valve
sols	:	solenoid valve
ccf,shv	:	dependent failure shut-off valves
ccf,solv	:	dependent failure solenoid valves
ccf,ps	:	dependent failure pressure switches

Data analysis:

A data analysis can be divided into a generic and a plant specific data collection. If a limited amount of plant-specific data is available, a Bayesian update process has to be performed to combine the generic and plant specific data. The results of this data analysis are presented in table 11.1.

To calculate the transition rates representing dependent failure of the two shut-off valves, the two solenoid valves or the two pressure switches, the beta factor model (see chapter 13) has been applied:

$$\lambda_{ccf,v} = \beta \cdot \lambda_{shv}$$

$$\lambda_{ccf.solv} = \beta \cdot \lambda_{sol}$$

$$\lambda_{ccf,ps} = \beta \cdot \lambda_{ps}$$

A beta factor of 0.1 has been used in this example. The transition rates can be calculated with the formulas listed above and the data provided in table 11.1. The results are presented in table 11.2. It should be emphasized that the data presented in this paragraph is for illustrative purposes only and has no practical value.

Table 11.1: Component failure data.

Component	Failure rate (-/hour)	Test period (hour)
Pressure switch	2.01E-06	8760
Shut-off valve	5.0 E-06	8760
Solenoid valve	1.0 E-06	8760
Logic-1	8.0 E-08	8760
Logic-2	2.01E-08	87600
CCF sensors	2.0 E-07	8760
CCF shut-off valves	5.0 E-07	8760
CCF Solenoid valves	1.0 E-07	8760

Table 11.2: Transition rates between different states.	
Transition between	**Failure rate (-lhour)**
1-2	2.00 E-06
1-3	2.00 E-06
1-4	1.00 E-06
1-5	1.00 E-06
1-6	5.00 E-06
1-7	5.00 E-06
1-8	8.80 E-07
2-8	2.00 E-06
3-8	2.00 E-06
4-8	6.00 E-06
5-8	6.00 E-06
6-8	6.00 E-06
7-8	6.00 E-06
1-9	2.00 E-08

Solution of mathematical modek

The nine differential equations are solved by numerical integration. The results are provided in figure 11.14. Series one represents the instantaneous probability of failure on demand. Series two gives the time-average probability of failure on demand in accordance with the following formula:

$$PFD_{\text{time average}} = \frac{1}{T} \int_{t=0}^{T} PFD_{\text{instantaneous}}\, dt \qquad (11.23)$$

The time average value over the test period every ten years can be compared with the time-average value calculated by fault tree analysis. The time-average probability of failure on demand is (t = 87600 hours):

$$PFD_{\text{time average}} = 5.5\ \ 10^{-3} \qquad (11.24)$$

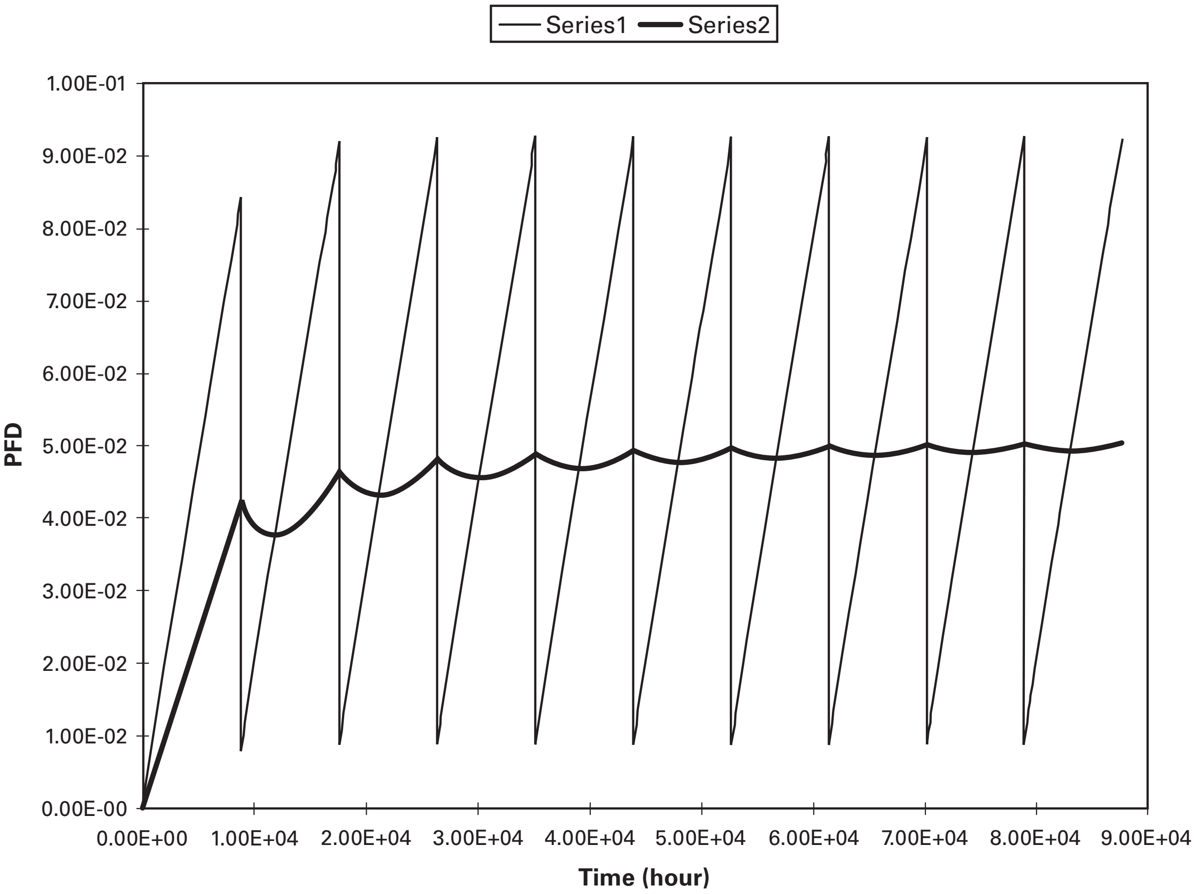


Figure 11.14: Probability of failure on demand as a function of time.

Sensitivity analysis:
To determine the dominant contributors to the probability of failure on demand, the Fussel Vesely importance will be calculated. The Fussel Vesely importance measure of a component X is defined as the fractional contribution to the probability of failure on demand from component X. The Fussel Vesely importance can be expressed as foliows:

$$I_{FV}(X) \quad = \quad \frac{PFD - PFD\ (X = 0)}{PFD} \tag{11.25}$$

PFD : Calculated probability of failure on demand

PFD(X=0) : Calculated probability of failure on demand, given that the failure rate of component X is assumed to be zero.

The results of the importance analysis are presented in table 11.3. From the results it can be concluded that the dominant contributors are: dependent failure of both shut-off valves, the logic that is tested once every ten years, dependent failure of the pressure switches and independent failure of the shut-off valves.

Another interesting subject to investigate in a sensitivity analysis is the test efficiency of the annually performed test. Due to human errors the system might not be tested or the safety device might be left in a failed state. A human error analysis (see chapter 14) has to be performed to calculate the probability of not performing a correct test. If the probability of human error is assumed to be 0.1 for each test performed on a yearly basis, the calculated probability of failure on demand is equal to 6.8 E-03. This is an increase of about 25 percent.

Table 11.3: Fussel Vesely importance

Number	Component type	FV importance
1	CCF shut-off valves	0.38
2	Logic 2	0.16
3	CCF sensors	0.15
4	Shut-off valves	0.14
5	CCF solenoid valves	0.08
6	Solenoid valves	0.04
7	Pressure switches	0.01

Interpretation of results:

The calculated probability of failure on demand of the high-integrity pressure protection system is equal to 5.5 E-03 per demand. The results are dominated by dependent failures and failure of the shut-off valves. Failure to execute the annually performed test can increase the probability of failure on demand considerabiy.

11.11 REFERENCES

[11.1] Dhillon and Singh, Engineering Reliability, John Wiley & Sons, Inc., 1981

[11.2] Henley and Kumamoto, Probabilistic Risk Assessment, New York, IEEE Press, 1992

[11.3] Shooman, Probabilistic Reliability: An Engineering Approach, Mcgraw-Hill Electrical and Electronic Engineering Series, 1968

[11.4] R. Billinton, R.N. Allen, Reliability Evaluation of Engineering Systems,
Pitman Advanced Publishing Programs, Boston - London - Melbourne, 1985.
ISBN 0-273-08484-4

[11.5] IEC 1165, Application of Markov techniques, International standard, First edition, Reference number 1165:1995, 1995-01.

ACCIDENT SEQUENCE DEVELOPMENT AND QUANTIFICATION

CONTENTS

12.1 INTRODUCTION

In a large number of industrial processes hazardous events can occur after occurrences of a process upset or a process disturbance (initiating events) and subsequent failure of one or more safety systems. A safety system will reduce the probability of occurrence of a potential hazardous event or reduce the consequence of such an event.

Depending on the number of protection layers and redundant safety systems, identification and quantification of the risk involved in the operation of a plant is complicated. The methodology described in this chapter is particular useful if more than one protection layer has been applied to reduce the probability or the seriousness of a hazardous event.This methodology is based on the identification of all possible initiating events which can result in a hazardous event and in the development of all possible accident progressions, given an initiating event. For each identified accident progression the consequences have to be identified. This process is called accident sequence development. Event trees can be used to model and calculate the probability of occurrence of the identified hazardous events.

An initiating event is defined as an event that creates a disturbance in the plant and has the potential to lead to a hazardous event, depending on the successful operation of the various mitigating systems in the plant. Initiating events arise from pipe breaks, failure of normal operating systems (e.g. main cooling water pump), support systems like instrument air or power supply etc., or from external events (e.g. seismic events, floods, etc).

The accident sequence development includes all aspects of model building for the plant. The culmination of this task is a model that defines the initiators of potential hazardous events, the response of the plant to these initiators and the spectrum of resulting hazardous events. Specific accident sequences are defined that consist of an initiating event, specific safety system failures and successes, and their timings and human responses. For each accident sequence of events the appropriate system fault trees are combined to find the contributing cut-sets.

The major steps in accident sequence development are:

- Identification of accident sequence initiators (initiating events)
  In general the potential sources of releases of hazardous material to the environment are identified, for the different operational states of the plant.

- Accident progression evaluation
  All safety systems which can be activated given the occurrence of a particular initiating event have to be identified and put in the right chronological order of actuation.

- Accident sequence modeling
  A model is constructed that simulates the initiation of an accident sequence and the response of the plant. This model consists mainly of combinations of event trees that comprise initiating events, system failures and human errors that will lead to a hazardous event.

- Data assessment and parameter estimation
  In this step, all information is collected that is necessary for quantification of the model constructed in the preceding step. The parameters that are estimated can be divided into three major categories: frequencies of initiating events, component unavailabilities, human error probabilities and parameters for the modeling of potential dependencies among various events.

- Accident sequence quantification
  The model constructed in the accident sequences modeling task is quantified using the results of the data assessment and parameter estimation task. The result of this step is the assessment of the probability of occurrence of a hazardous event over a period of one year. Normally this is accompanied by an assessment of the associated uncertainties. Sensitivity studies are made for the important assumptions and the relative importance of the various contributors to the calculated results are indicated.

For more information about accident sequence development and quantification, reference is made to [12.1], [12.2], [12.3], [12.4] and [12.5].

12.2 NOMENCLATURE

λ	=	failure rate	-/h
θ	=	repair duration	h
Q	=	probability of failure on demand	-
T	=	test period	h

12.3 IDENTIFICATION OF INITIATING EVENTS

The identification of initiating events is the initial stage of accident sequence development. Since a risk analysis attempts to address all possible circumstances, this list of initiating events must be as complete as possible. It should be recognized, however, that it is not possible to establish that any such list is complete. A judgement is required that any initiating event not identified would make only a small contribution to the total risk. The scope of a risk analysis could also constrain the initiating events that are to be considered, for instance exclusion of external initiating events like earthquakes, external flooding, air craft impact, etc. A number of Hazard identification techniques which can be used to identify all potential initiating events are described in chapter 7.

There are several approaches to the selection of initiating event each of which has its limitations. Since the aim is to produce a list that is as complete as possible, it is recommended that all of the approaches should be foilowed, although one may be selected as the main approach. The approaches are as follows:

1: **Checklists:**
It is useful to refer to lists of initiating events drawn up for previous risk analyses on similar plants and for the safety analysis report. This may in fact be the starting point.

2: **HAZOP analysis:**
The plant systems (operational and safety) and major components are systematically reviewed to see whether any of the failure modes (e.g. failure to operate, spurious operation, breach, disruption, collapse) could lead directly, or in combination with other failures, to hazardous events. Operational procedures also have to be taken into account in this review process.

3: **Deductive analysis:**
In this approach, the hazardous event is made the top event in a diagram which has the appearance of a fault tree. This top event is successively broken down into all possible categories of events that could cause it to occur. Successful operation of safety systems and other preventive actions are not included. The events at the most fundamental level are then candidates for the list of initiating events for the plant.

4: **Operational experience:**
In this approach, the operational history of the plant in question and of similar plants elsewhere is reviewed for any events that should be added to the list of initiating events. This approach is supplementary and would not be expected to reveal low frequency events. This methodology is comparable with the "Critical Incident Technique" as described in chapter 7, appendix 7-A.3.

Classification of initiating events
Initiating events are generally classified into internal initiating events and external initiating events. Internal initiating events are hardware failures in the plant or faulty operations of plant hardware through human error or computer software deficiencies. External initiating events are events that create extreme environments common to several plant systems. Examples of external initiating events are, for instance: internal flooding, internal fire, missile impact, earthquakes, external floods, high winds, aircraft crashes etc.
For chemical plants, the internat initiating events are divided into the following major categories:

- **Leakages, pipe breaks or vessel rupture:**
  Leakages, pipe breaks or vessel ruptures initiators are all events that directly cause loss of integrity of the primary pressure boundary.

- **Transient initiators:**
  Transient initiators are those that could create the need for a shutdown. Of particular interest are events that can cause a transient and at the same time can cause the total or partial failure of a system needed for mitigating consequences. A special subset of this type of transients is made up of those that are caused by complete or partial failure of support systems (DC and AC power, instrument air, etc.).

Once identified, the initiating events are normally listed in a systematic way, for instance:
- Leakages or break sizes.
- Transients applicable to the plant.
- External initiating events.

A cut-off criterion may be applied to isolate those initiating events which are of very low frequency. The purpose is to avoid undue effort in systems analysis for low frequency initiating events which will not make a significant contribution to the overall risk. Such initiating events should not be discarded but should be recorded and a rough estimate of their contribution should be incorporated into the overall results.

The complete list of initiating events will usually contain many groups of similar events which can be treated in the risk analysis as one event since their impacts on the plant response are identical. The process of combining a number of initiating events, with identical plant response, into one new defined initiating event is called grouping of initiating events (see section 12.4.6).

12.4 EVENT TREE DEVELOPMENT

12.4.1 Introduction

Once accident sequence initiating events have been identified and grouped, it is necessary to determine the response of the plant to each initiating events. This modeling of the responses results in the generation of event sequences. An event sequence model provides sequences of events that, following an initiating event, lead either to a safe state of the plant or to a hazardous event. The outcome of the various accident sequences does not need to result in hazardous events of equal severity. For instance, a pressure safety valve may reduce the probability of occurrence of a reactor vessel rupture, but may cause a smaller release of hazardous material, if it operates to protect the reactor vessel.

Event sequences are expressed in terms of initiating events and successes or failure of mitigating systems. System failures are subsequently represented by another set of models, which are logical combinations of simpler events. In this chapter the event tree technique will be applied to model the accident sequences and the fault tree technique will be used to model safety system failures.

Event trees are graphic models that order and reflect events according to the requirements for mitigation of each group of initiating events. Event tree heading events can be a safety function status, a safety system status, basic events occurring or an operator action. Event trees display some of the functional dependence between event tree heading events; e.g. cases where failure of one system implies that another system cannot perform its function successfully. Such dependence results in omitted branch points.

The event tree headings are normally arranged in either chronological or causal order. Chronological ordering means that events are considered in the chronological order in which they are expected to occur in a hazardous event. Causal ordering means that events are arranged in the tree so that the number of omitted branch points is maximized.

Event tree development includes the execution of the following two steps:
- Accident progression evaluation
- Accident sequence modeling

To perform these steps in a correct way, one must be familiar with the plant response given the occurrence of a specific initiating event. To model the plant response, the following items should be considered; safety functions, success criteria, front line and support systems and dependency matrices. The relation between these items is depicted in figure 12.1.

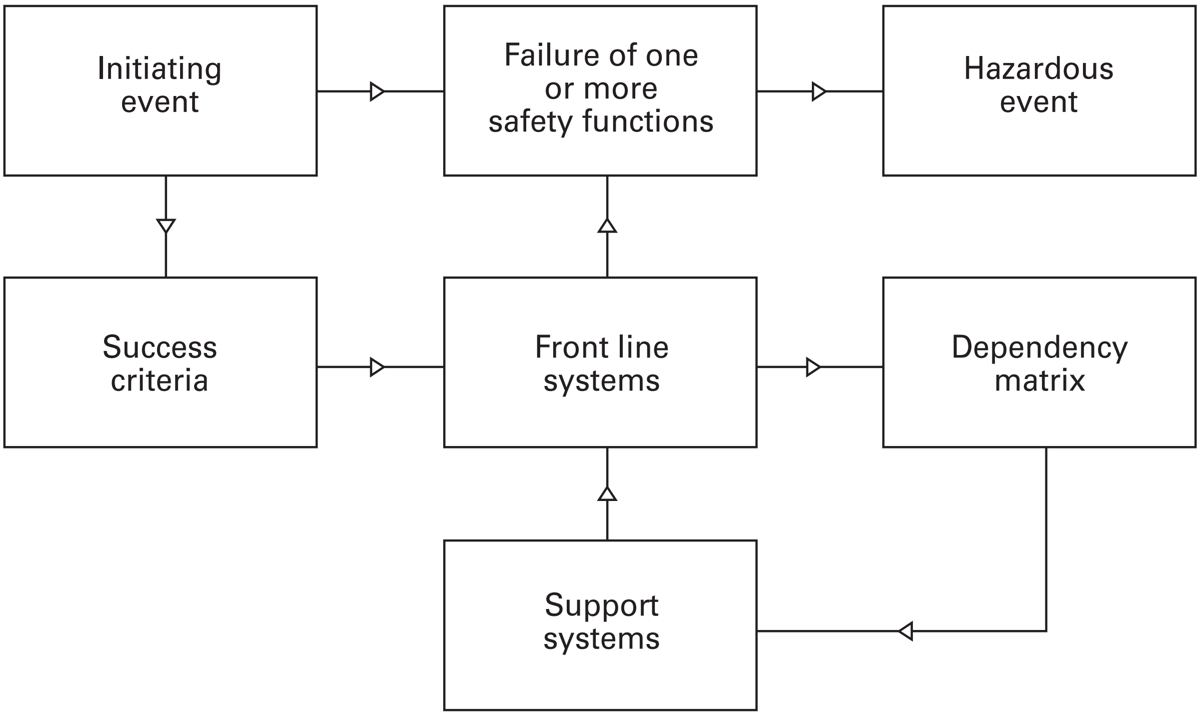


Figure 12.1: Relations between, safety functions, front line systems, success criteria, support systems and dependency matrices.

The safety functions can be considered as the plant defenses against the consequences of the initiating event. Failure of one or more safety functions results in the occurrence of an hazardous event. Safety functions are performed by normal operating systems, safety systems and operator actions. Systems which directly perform a safety function are called front line systems. Some front line systems consist of a number of parallel operating trains. Depending on the initiating event one or more parallel operating trains are required to be able to mitigate the initiating event.These front line system requirements are called success criteria. In general, a front line system cannot operate without one or more support systems like, instrument air, AC and DC power. In a dependency matrix the support systems which are required for proper functioning of the front line system are tabulated. Each of the items introduced above will be described in more detail in one of the following sections.

12.4.2 **Safety functions**

Generally, safety functions are defined by a group of actions that prevent the occurrence of a hazardous event given the occurrence of an initiating event. Such actions can result from the automatic or manual actuation of one or more safety systems, from passive system performance, or from the natural feedback inherent in the design of the plant. An example of a safety function is the pressure control of a reactor by a pressure safety valve. Another example of a safety function is the cooling of a chemical reactor in case of an exothermic reaction.

Definition of the necessary safety functions provides the structure for defining and grouping of safety systems in order to define a complete set of system responses and interactions for each class of initiating events. In the event tree structuring process for every initiating event, the safety functions that need to be performed in order to prevent the occurrence of a hazardous event have to be identified and put in the right chronological order.

One style of constructing event trees is by using the failures of the relevant safety functions as heading events. Relevant means relevant for the mitigation of the initiating event under consideration.This style of composing event trees is called the functional event tree approach. In the systematic event tree approach the failure of relevant normal operating systems, safety systems and operator actions are defined as heading events.

12.4.3 **Front line and support systems**

The systems that directly perform a safety function are termed front line systems, while those systems required for the proper functioning of the front line systems are termed support systems. An emergency cooling water pump to cool a chemical reactor after failure of the main cooling water pump is a front line system because it directly performs the safety function of cooling the reactor.The electrical supply of the emergency cooling water pump does not directly fulfil a safety function, but is required for proper functioning of the emergency cooling water pump. For this reason this electrical supply is called a support system.

For each safety function, all the front line systems that perform this function alone or in combination with other systems, have to be identified.

Dependencies between front line and support systems
To understand the relationships between front line and support systems, a dependence table of front line/support systems can be composed. An example is given in Table 12.1. All systems that are required for the proper functioning of each of these support systems are identified and added to the list of support systems. This process is continued until all systems that somehow affect the functioning of front line systems through this chain of dependencies have been identified.

It is also useful to identify any possible dependencies among support systems in a dependence table of support systems versus support systems. This table is similar to the front line/support system table already mentioned. The dependence table front line/support systems is updated to include the additionally identified support systems and the corresponding dependencies.

Finally, the front line/support systems dependence table would indicate dependencies among front line systems, either because they depend on the same support systems or because they depend on different support systems which themselves depend on a common third system.

In table 12.1 the dependency matrix is given of the example described in section 12.6. An X in column 2-4 indicates that the front line system mentioned in column one is dependent on the support system tabulated in the heading of the dependency matrix.

Table 12.1: Dependency matrix.

Front line system	**Support system**		
	24V DC	**220V AC**	**Instrument Air**
Short stop	X	-	X
Agitator	-	X	-
Emergency Cooling Water	X	X	-
Instrument Safeguarding			
depressurization	X	-	X
Pressure safety valves	-	-	-

12.4.4 **Success criteria**

Depending on the initiating event, the required system performance can be different. Required performance means the minimum system performance that will enable the successful fulfillment of its safety function under the specific conditions created by the initiating event. For instance, one out of two spring-loaded safety valves has to open to prevent the occurrence of an runaway reaction in a specific chemical reactor after failure of the agitator.

The success criteria of front line systems are of particular importance for a risk analysis because they will define the starting point for the subsequent system modeling.

The success criteria for front line systems will undergo an even narrower definition during the evaluation of the plant response, because they may depend not only on the initiator but also on additional system failures or successes in a particular accident sequence.

Success criteria can be unambiguously defined for front line systems, for which a clear success or failure in the performance of a safety function can be recognized. In addition to a performance definition (e.g. flow rate, response time, trip limits), the success criteria must be expressed in hardware terms, such as the number of required emergency cooling water pumps, etc.

Success criteria for support systems cannot be so readily defined because in most cases they serve more than one front line system, and consequently each possible state of the support system (e.g. one diesel generator operating or two diesel generators operating) has a different effect on the front fine systems that perform a certain function. A particular support system state could therefore lead to a safety function success or failure, depending on the particular state of the front line system with which it is combined.

A first step in the assessment of front line success criteria to be derived is to review the relevant design information. However criteria derived from design information might be overly conservative. More realistic success criteria can be obtained by performing a number of best-estimate thermohydraulic or physical calculations.

Where very conservative success criteria are initially derived from design information, it should be recognized that, at some stage in the risk analysis, additional analyses may be necessary to support realistic success criteria for the final risk models. An alternative course of action would be to investigate the effects of relaxing success criteria in a sensitivity analysis. A sensitivity analysis may precede and justify any major additional analysis (e.g. transient analysis) to support more realistic success criteria.

In addition to the success criteria imposed on the front line systems by the initiators, any other special conditions imposed by these initiators must also be assessed and recorded. Such special conditions may be effects on support systems, on symptoms displayed to the operator, on automatic actuation systems or on the potential for inducing dependent failures. These special conditions will be used in grouping the initiators into equivalent classes.

12.4.5 **Top logic**

It is possible that a certain safety function can be fulfilled by more than one front line system. In practice a fault tree will be constructed for each front line system separately. To model the safety function in an event tree heading, these separate fault trees have to be combined. This modeling is normally done by a small fault tree called the top logic. The top logic fault tree represents the correct logic between the safety function and the front line systems which have to perform that particular safety function.

The complete structure of the event tree risk analysis model using, top logic, front line systems and support systems is depicted in figure 12.2. In figure 12.2 safety function 2 represent failure to depressurize either by the instrument safeguarding depressurization system or by the pressure safety relief valve. For operation of the instrument safeguarding depressurization system instrument air is required.

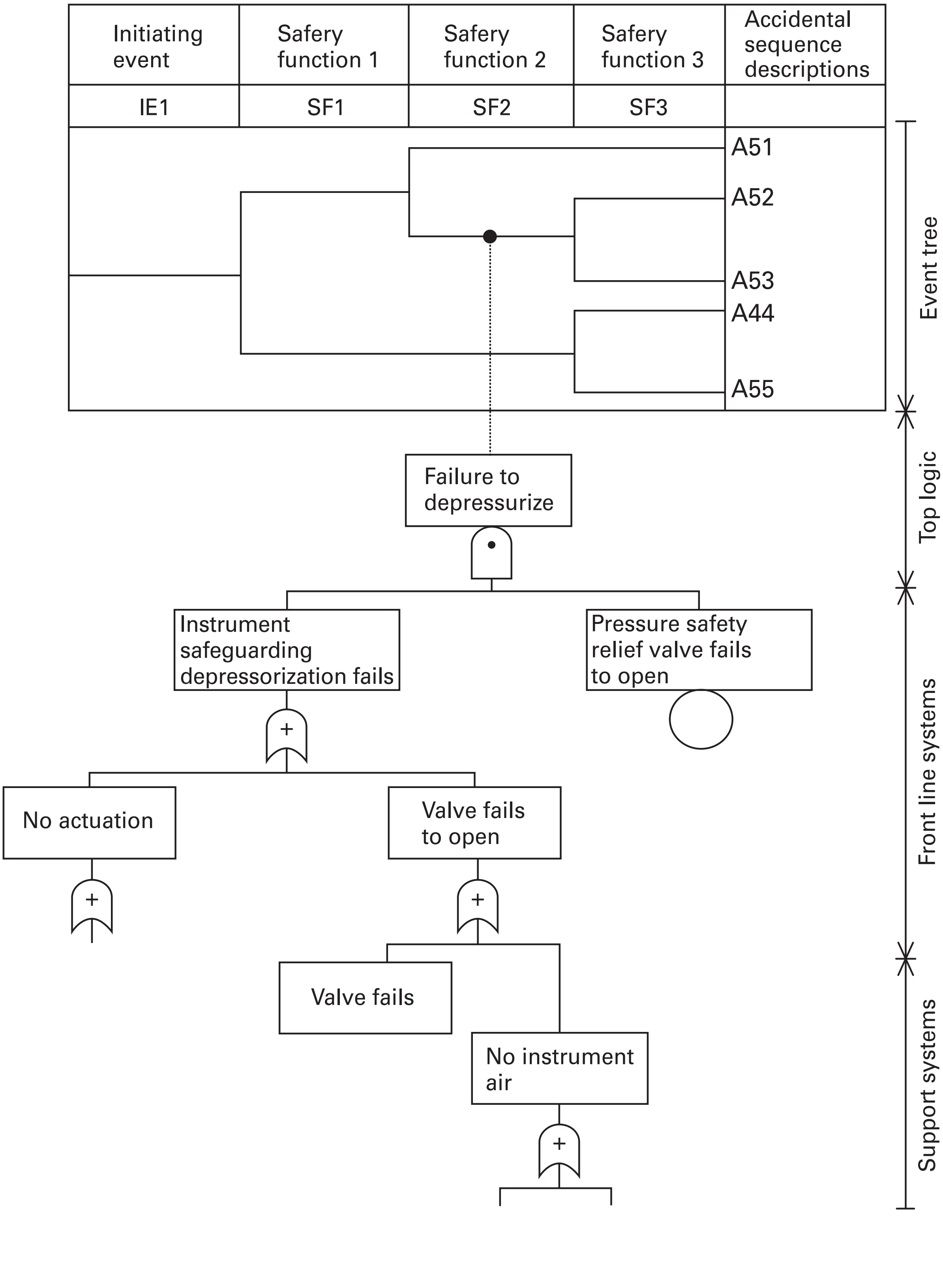


Figure 12.2: Structuring of event tree risk analysis model.

1 2.4.6 Grouping of initiators

Once the task of assessing the requirements of the plant systems has been completed, the initiating events can be grouped in such a way that all events in the same group impose essentially the same success criteria on the front line systems as well as the same special conditions (challenges to the operator, to automatic plant responses, etc.) and thus can be modeled using the same event and fault tree analyses. The purpose of grouping of initiating events is to reduce the effort in performing the risk analysis.

In the grouping process of initiating events one has to consider the following items:

- Safety functions
- System relationships (front line systems and support systems)
- Safety system requirements (success criteria)

This is because initiating events can only be grouped if the demands they make on safety functions, front line systems and support systems are the same.

In the process of grouping, it will become clear that some categories of initiating events need to be subdivided. Dividing breaks by break size (and perhaps location) is a well-known example but other cases should be expected.

The subsequent analysis needed may be reduced by grouping together initiating events that evoke the same type of plant response but for which the front line system success criteria are not identical. The success criteria applied to this group of events should then be the most onerous for any member of the group.

For reasons of traceability, the grouping process has to be documented very carefully.

12.5 QUANTIFICATION OF ACCIDENT SEQUENCES

12.5.1 Introduction

Quantification of accident sequences involves the collection of: initiating events, event trees and fault trees. An important part of the accident sequence quantification is the determination of the initiating event frequencies, the collection of the component failure data and the determination of the probability of the human and dependent failure events. All this numerical data has to be put into a database. The complete structure of the quantification model is depicted in figure 12.3.

The results of quantification of an event tree fault tree model are a number of cut-sets for each accident sequence leading to a hazardous event. Each cut-set of a specific accident sequence contains, as a minimum, the initiating event of that accident sequence.

The following sections describe in more detail the methods and tools used for accident sequence quantification. The method to quantify the sequences depends on the way these sequences are modeled within the entire risk model.

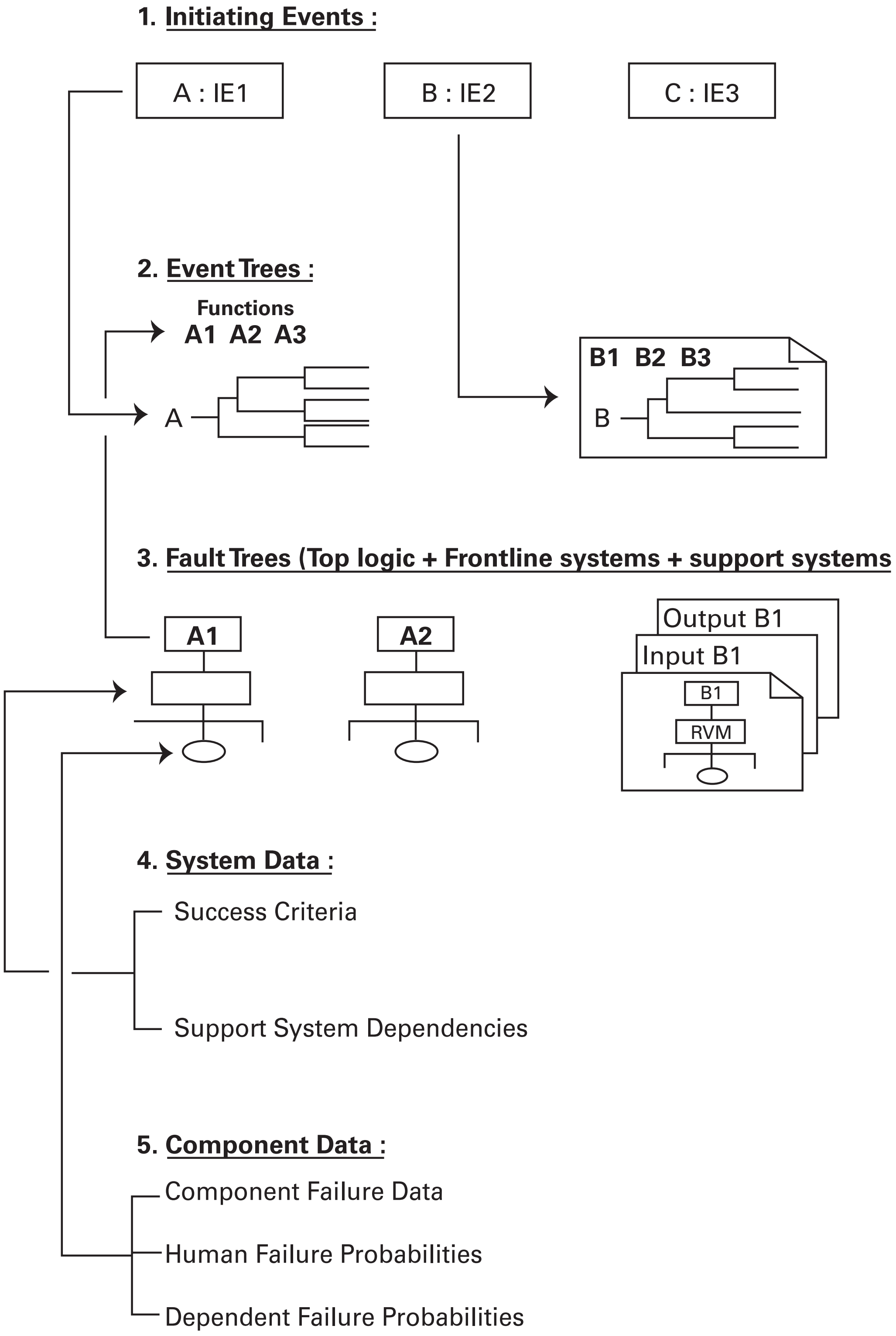


Figure 12.3: Structure of the quantification model.

12.5.2 Small event tree large fault tree approach

In the small event tree large fault tree approach, event trees with safety functions as heading events are first developed and then expanded to event trees with the status of front line systems as headings. The front line system fault tree models are developed down to suitable boundaries with support systems. The support system fault trees may be developed separately and integrated at a later stage into the front line system models. The dependence matrices developed are used here as a first indication of which support systems should be included in the front line system fault trees. This approach generates event trees that are concise and that allow for a synthesized view of an accident sequence. In the small event tree approach, dependence and the corresponding importance of support systems are not explicitly apparent.

Another name often used for the small event tree - large fault tree approach is ”the fault tree linking approach”. This points at a basic issue of this approach, namely the fact that front-line systems are modeled using large fault trees, comprising dependencies on support systems. The support systems may be modeled by fault trees to be integrated, i.e. linked, in a later stage. The small event trees are used to describe the functional dependencies of the front-line systems to the initiating events. These event trees are then used to link all fault trees in order to establish a fault tree for each of the hazardous event sequences. A typical example of the small event tree large fault tree approach is depicted in figure 12.2, see section 12.4.5.

In this chapter the Fault Tree Linking approach will be explained. The main characteristics of the small event tree large fault tree approach are:

- The event tree describes a functional response to selected and grouped initiators. The concise event tree provides a synthesized view of the possible accident sequences.

- The event trees are converted into fault trees by means of ”accident sequences logic” and ”top logic”. System fault trees are established to model the unavailability of the systems addressed in the top logic fault trees, i.e. systems performing the safety function as given in the event tree headings. Unavailability of support systems is modeled in separated fault trees to be linked to the safety systems fault trees to model the dependencies.

- The constructed model, after linking or inclusion of all fault trees, is a very large fault tree for each of the accident sequences. It is not possible to get a clear overview of this entire model. Dependencies and the corresponding importance of support systems are not explicitly apparent.

- This model is not ”final” as the success paths in the accident sequences are not taken into account. This will be accounted for after the calculations of the cut-sets, see section 12.5.5.2.

- The fault trees must be evaluated to find the cut-sets for all accident sequences and for all event tree headings.

- Three cut-set file manipulations must be performed:
  - The cut-sets of the hazardous event sequences which contain a cut-set that is in the cut-set file of the success path for that sequences must be deleted.
  - The cut-sets containing two events which cannot occur together must be deleted, e.g. maintenance of both redundant components, which cannot occur in practice.
  - Non-recovery events must be added to the cut-sets where proceduralized or routine operator actions can eliminate one of the faults in the cut-set and thereby prevent the hazardous event.

- The correctness of the model, after incorporation of all changes described above, can only be assessed by review of the cut-sets.

- There is a large number of fault tree evaluation tools available. When buying one of these, one must consider that handling of the large fault trees requires special codes and a great deal of computer capacity.

- The logic fault tree model provides the possibility to analyze the criticality of events by setting events to ”success” or ”failed”. This feature is incorporated in most fault tree evaluation tools.

- Computer codes which support the small event tree large fault tree approach are: CAFTA, NUPRA and RISK SPECTRUM, references [12.7], [12.8] and [12.9].

12.5.3 Large event tree small fault tree approach

In the large event tree approach, all support system states appear explicitly in the event trees. The top events on the fault trees have associated boundary conditions; these boundary conditions include the assumption that the support system is in the particular state appropriate to the event sequence being evaluated. Separate fault trees must be used for a given system for each set of boundary conditions. These separate fault trees can be produced from a single fault tree that includes the support systems and that, before being associated with a particular sequence, is ’conditioned’ on the support system state associated with this sequence.

This approach generates large event trees that explicitly represent the existing dependence. However, the complexity of the event trees increases rapidly with the number of support systems and the number of support system states that are explicitly depicted in the tree. An additional consideration is that the large event tree approach, does not explicitly identify what specific combinations of support system failures lead to front line system failures.

The most important characteristics of the large event tree small fault tree approach are:

- The event tree linking method is more scenario-orientated, more descriptive. Each of the initiating events initiates a chain of events which branches into many paths, representing different scenarios leading to various hazardous event stages.

- Not only the front-line safety systems are modeled in the event tree in response to an initiator, the support system unavailabilities are modeled explicitly in the even trees as well.

- All event tree heading events are modeled by small fault trees. These fault trees are completely independent in that two fault trees do not contain the same event. These fault trees are calculated for the various plant stages (depending on the branch in the event tree).

- For one event tree heading, more than one failure probability might be calculated (by means of a fault tree) to account for the plant configuration or other system failures occurring ”earlier” in the scenario. These are called the split fractions.

- This makes it possible to evaluate plant response with each systems configuration and for maintenance activity. The identification and quantification process tracks the effects of configuration and on-going activities.

- Because of the fact that only event trees with independent headings are to be quantified, the conditional probabilities of the split fractions can simply be multiplied. It is then straightforward to implement a truncation (see section 12.5.5.1) of the model quantification by simply cutting off the multiplication ”while going through the event tree” when the truncation limit is reached. In this process, the number of truncated branches can be recorded.

- Where there is a large number of fault tree evaluation tools available, there are not so many tools to support this linked event tree approach. One specialized tool is RISKMAN, see reference [12.6].

The structure of the large event tree small fault tree approach is depicted is depicted in figure 12.4.

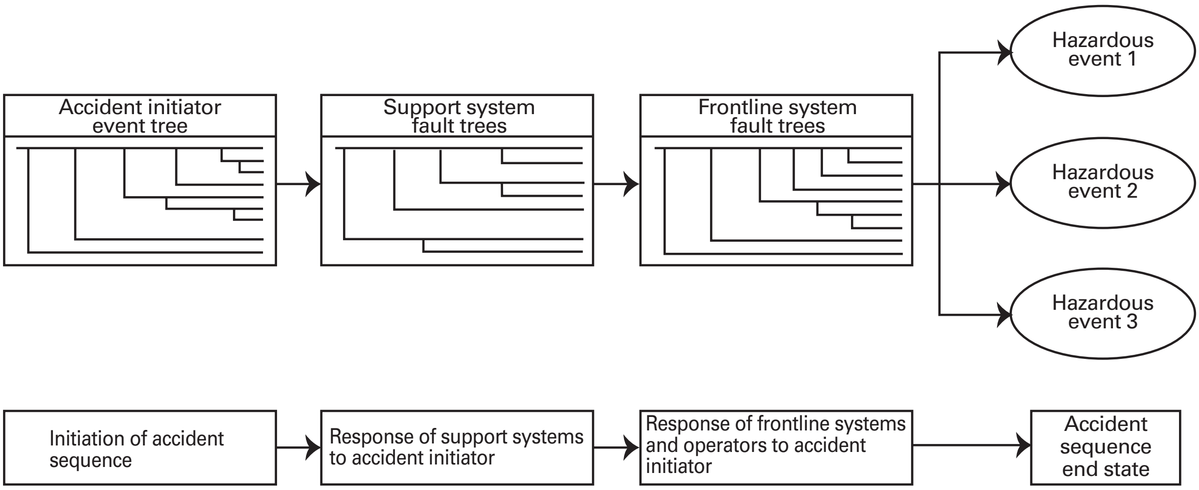

Accident initiator event tree
Support system fault trees
Frontline system fault trees
Hazardous event 1
Hazardous event 2
Hazardous event 3
Initiation of accident sequence
Response of support systems to accident initiator
Response of frontline systems and operators to accident initiator
Accident sequence end state

Figure 12.4: Structure large event tree small fault tree approach.

12.5.4 Determination and quantification of accident sequence cut-sets

In manipulating event trees and fault trees in the small event tree approach, the fault trees are combined with the event trees to produce a large fault tree for each accident sequence, which can be evaluated to find the minimal cut-sets for each accident sequence. In figure 12.5 the accident sequence fault tree to calculate the cut sets for accident sequence AS3 from figure 12.2 (see section 12.4.5) has been depicted.

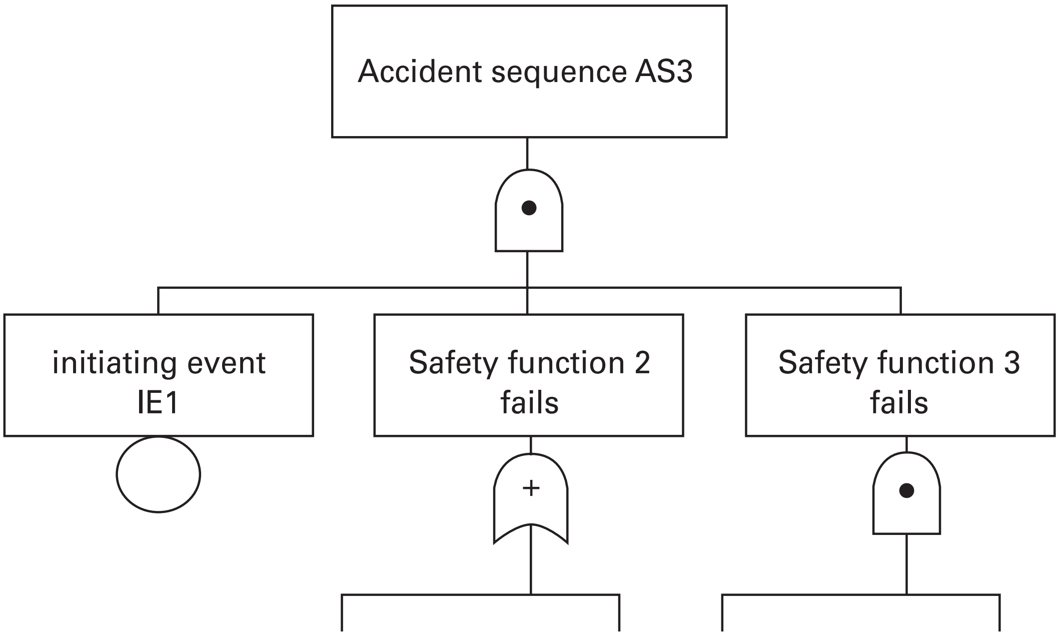


Figure 12.5: Accident sequence fault tree.

The accident sequence minimal cut-sets contain the initiating event and a combination of basic events that result in the accident sequence given this initiator.

In order to establish this, the total set of fault trees (accident sequence fault tree, system fault trees, top logic fault trees and, if necessary, fault trees to calculate the initiating event frequency) must be linked to compile the complete risk model.This compilation will result in one large fault tree for each of the accident sequences.The file containing these fault trees is often called the ”Master”.The following steps are performed to create the Master:
- Load the fault tree describing sequence logic
- Include top logic into this fault tree
- Include system fault trees into this fault tree

Most fault tree software tools provide the option of importing other fault trees. This is a straightforward task, provided that the naming of the gates in the original fault trees matches the naming of the tops of the imported fault tree.

12.5.5.1 CUT-OFF FREQUENCY

In order to make the sequence quantification practical, it is generally necessary to truncate the analysis; that is, to consider only those cut-sets whose probability is above some cut-off value. Practice has shown that it is generally adequate to consider a truncation value that is smaller by a factor of 1000 than a dominant value that is obtained or a criterion value that is considered. Thus, if a criterion value of 10^{-5} is to be demonstrated, a truncation value of 10^{-8} is generally adequate. As another example, if a cut-set of 10^{-4} has been obtained, then a truncation value of 10^{-7} is generally adequate.

12.5.5.2 DELETION OF SUCCESS PATHS

The deletion of success paths refers to the case where the success of a system is included in the sequences of events that define an accident sequence. It is important to consider explicitly the success of this system in the Boolean reduction of the accident sequence to avoid an overestimation of its frequency. Such situations typically arise when the system models (fault trees) for front-line systems include the support systems (Small Event Tree - Large Fault Tree approach!). In such a situation the success of a front line system implies the success of its support systems, which cannot then be considered as contributing to the failure of a different front line system in the same accident sequence.

The exact treatment of this problem requires the use of success models. In the linked fault tree approach, this can result in very large fault trees for the accident sequences, which cannot be evaluated with the common computer tools available. One way around this problem is the cut-set matching technique, where two lists of cut-sets are generated:

- The first list contains the accident sequence cut-sets, corresponding to the linked fault trees of the failed systems.

- The second list contains the cut-sets of the fault trees of each system whose success is part of the accident sequence.

These two lists are then compared and the cut-sets of the first list that contain a cut-set that appears in the second list are eliminated. This is not an exact treatment but the error that is introduced is in most cases insignificant.

12.5.5.3 DELETION OF MUTUALLY EXCLUSIVE EVENTS

Deleting of mutually exclusive events from the calculated cut-sets is important in the small event tree approach. If a cut-set arises in which for example two maintenance actions are included which are not allowed to be executed simultaneously, this cut-set must be deleted from the cut-set file. This can be done by comparing the accident sequence cut-sets with a file containing a list of combinations of events that cannot occur simultaneously. This can be performed automatically and the files with mutually exclusive events has to be established only once.

12.5.5.4 INCLUSION OF NON-RECOVERY EVENTS

A recovery action can be defined as one or more operator actions to restore a failed safety system. In general this restoration is done by activating an alternative system which can be put into service to take over the function of the failed safety system.

To identify a potential recovery action, the circumstances under which such an action has to be performed must be known. This information can be derived from the accident sequence minimal cut-sets. Each accident sequence minimal cut-set represents one possible way in which the sequence may occur. The information available to the operator and the recovery action to be taken generally depend on the combination of events that have occurred and hence on the particular minimal cut-set.

Therefore recovery actions are generally considered at the minimal cut-set level rather than at the accident sequence level. Since there may be a large number of minimal cut-sets for an accident sequence, it may be necessary to consider recovery for the most significant minimal cut-sets only.

A probability of non-recovery is estimated for each minimal cut-set which is recoverable by some operator recovery action. The frequency of the minimal cut-set is then multiplied by its probability of non-recovery to estimate the final minimal cut-set frequency with recovery. The final estimated frequency of an accident sequence is computed using these minimal cut-set frequencies with recovery.

The primary events of a particular accident sequence minimal cut-set may or may not be recoverable by routine recovery actions. Extraordinary recovery actions are not considered, but routine recovery actions are. For example, the overhaul of a pump is not considered, but the manual realignment of a valve, whether by a hand switch in the control room or local turning, is. If a primary event can be recovered by a routine recovery action, the location of the recovery action is determined.

12.5.6 **Review of accident sequence cut-sets**

An important task is the review of cut-sets generated by the Boolean reduction process and the subsequent cut-set manipulations. An important task is validation of the risk model by examination of the cut-sets generated. To perform this examination, one must be familiar with details of the plant as well as with the risk model. If cut-sets are found which are not in accordance with the expectations of the reviewer, the risk model has to be reviewed and if necessary modified.

12.6 **EXAMPLE OF THE SAFEGUARDING SYSTEM OF A BATCH REACTOR**

This example concerns the analysis of the effectiveness of a simplified safeguarding system of a batch polymerization reactor, see figure 12.6. The process is the polymerization of vinyl chloride monomer. Vinyl chloride monomer is a flammable and has toxic combustion products and is known as a carcinogen.

12.6.1 Normal operating procedures

In reference 12.1 the operational steps for this process are defined as follows:

Step 1: Demineralized water charging
Operation starts by filling the reactor with a controlled charge of demineralized water.
An undercharge might lead to quality problems and a potential runaway reaction.

Step 2: Vinyl Chloride Monomer charging
An accurate charge of vinyl chloride monomer is added to the reactor.

Step 3: Reactor heat-up
To initiate the reaction process, an initiator is added from the charge pot to the batch. Steam supply is connected to the cooling water circulating through the reactor jacket until the batch reaches a temperature at which the reaction will proceed.

Step 4: Reaction
The steam supply is shut off and cooling water is circulating through the reactor jacket to control temperature by removing the heat of polymerization. To achieve a uniform temperature in the batch, the agitator operates during the polymerization process.

Step 5: Termination
The polymerization process is completed when the reactor pressure starts to decrease. The batch will be dumped to a downstream holding facility.

12.6.2 Hazard identification and safeguarding system

The HAZOP analysis shows that a runaway reaction can be initiated by a number of failure events (see reference [12.1]), among which:
- Loss of normal cooling water supply
- Agitator motor drive failure
- Temperature control failure.

The runaway reaction will rupture the reactor vessel, releasing the vinyl chloride monomer with major damage potential. To prevent a runaway reaction, the following safeguarding features are present:

- Two emergency cooling water pumps. One emergency cooling water pump is sufficient to prevent a runaway reaction.

- A short-stop chemical, which can stop the polymerization very rapidly after addition. This has to be initiated by the operator. The operator will be alerted by a high temperature or high pressure alarm. The short-stop is effective only if the agitator remains in operation.

  If the agitator fails, the short-stop must be added within two minutes, to allow mixing before the liquid swirl in the reactor dissipates. As a back-up, the reactor contents must be mixed by ”burping” the reactor, dropping pressure to generate rising bubbles within the bulk liquid mass. Burping is carried out by manually opening of the emergency vent valves.

- An automatic depressurization system that will be activated automatically by the safeguarding system after reaching the high-high pressure or temperature set point. In the event of an uncontrolled reaction, the reaction can be safely limited by depressurizing the reactor to the vent system.The heat of vaporization of the boiling reaction mass safely removes heat from the reactor.

- Two pressure safety valves are present which form an independent protection layer. If the pressure in the reactor has been increased to a preset value, the pressure safety valves will open. Although the runaway reaction will be stopped, opening of the pressure safety valves will lead to a release of hazardous material.

12.6.3 Safety functions identification

The safety functions of the PVC batch reactor are:
- Control of the reaction
- Remove heat of polymerization
- Maintain integrity primary pressure boundary.

The front line safety systems which are able to fulfil these safety functions are listed in table 12.2.

Table 12.2 Safety functions and corresponding front line systems.

Safety function	Front line system
Control reaction	- Short-stop and agitator
Remove heat of polymerization	- Normal cooling water system - Emergency cooling water system - Instrument depressurization system - Pressure safety valves
Maintain integrity of pressure boundary (pressure control)	- Instrument depressurization system - Pressure safety valves

12.6.4 Initiating event and event tree development

This example will be limited to the analysis of one initiating event: loss of normal cooling water supply. Normal cooling water supply can be lost due to loss of off-site power, control failure or cooling water pump failure. Loss of off-site power will also cause the agitator to fail. Depending on the type of control failure, it might be that this failure will also cause the emergency cooling water supply to fail. As a consequence, these three different causes for normal cooling water supply failure cannot be grouped into one initiating event.

In this example only normal cooling water supply failure due to failure of the cooling water pump and due to control failure, which does not affect the emergency cooling water supply, will be analyzed. The corresponding initiating event is indicated by ICW1.

Review of the safeguarding systems shows that the following sequence of events will occur as a response to the selected initiating event:

- By a low cooling water flow signal the emergency cooling water pumps will be activated and the operator will be alerted by an alarm.

- If cooling water supply is not restored by the emergency cooling water pumps, the operator will be alerted by a high temperature or high pressure alarm. The operator has to add short stop in about 15 minutes.

- If temperature and pressure continue to increase, the emergency vent will be activated by the high-high temperature or high-high pressure sensors.

- If pressure and temperature increase further, the pressure safety valves will open and hazardous material will be released into the environment.

An event tree has been developed to describe all possible accident sequences given the occurrence of initiating event ICW 1, see figure 12.7.

After occurrence of the initiating event ICW 1, the emergency cooling water supply will be activated first. Successful restoration of the cooling water supply implies that the operator can take the plant out of operation according to normal operating procedures.

If restoration of the cooling water supply fails, the operator has to add short stop. This action can be performed from the control room. The available time to perform this action, after a high temperature alarm, is about fifteen minutes.

Failure to add short stop will increase the reactor pressure and temperature. At a high-high reactor pressure or high-high reactor temperature the emergency depressurization vent valves will be opened automatically. Due to the depressurization of the reactor the heat of polymerization is safely removed from the reactor by vaporization of the boiling reaction mass.

If the automatic depressurization fails, the last line of defense will be the pressure safety valves.

Adding short stop is only effective as long as the agitator continues to operate. Although the probability of agitator failure will be small, after adding short stop, an additional branch is added for reason of completeness. Failure of the agitator requires depressurization, either by the automatic depressurization system or by the pressure safety valves. The corresponding sequences are incorporated into the event tree.

12.6.5 Description of the safety systems

Emergency cooling water supply:
The emergency cooling water supply safety system consists of one low flow sensor, control logic and two emergency cooling water pumps.

Short stop:
Short stop is added by opening of two air-operated valves. Each air-operated valve is activated by a solenoid valve (24V DC). Pressurized nitrogen will force the short stop agent into the batch. Agitation is necessary for good distribution of the short stop to rapidly terminate the polymerization process. If the agitator fails, the reactor contents can be mixed by dropping pressure to generate rising bubbles within the bulk liquid mass; this action is called ”burping the reactor”. Proper functioning of the 24V DC support system is required to open the air-operated valve.

Agitator:
To drive the agitator, a direct drive configuration has been selected. 220V AC power supply is required to operate the agitator.

Automatic depressurization system:
One-out-of-two air-operated valves has to open to effectively depressurize the reactor. Each air-operated valve is activated by a solenoid valve. The fait-safe principle has been applied with respect with the instrument air supply but not with respect to the 24V DC actuation power supply.

Pressure safety valves:
As an independent safety layer, two redundant spring-loaded safety valves are used to depressurize the reactor. If the reactor pressure exceeds the set point of the pressure safety valves, the valves will pop open.

12.6.6 Accident sequence and top logic fault trees

In the event tree diagram (see figure 12.7) the heading events are indicated as follows:

ICW	: Initiating event, Loss of normal cooling water supply
ECWF	: Failure of emergency cooling water supply
SSF	: Operator fails to add short stop
AGF	: Agitator fails before the reaction has been stopped
ISDEPF	: Instrument safeguarding depressurization fails
PSVF	: Pressure safety valve fails to open

All identified event tree heading events can be linked directly to one safeguarding system. This implies that top logic is not required for this example. The accident sequence fault trees for accident sequences SEQ4, SEQ5, SEQ7 and SEQ8 are depicted in figures 12.8, 12.9, 12.10, 12.11 and 12.12.

12.6.7 Success criteria

The required system performance or success criteria to mitigate the consequences for the selected initiating event ”loss of normal cooling water supply” are listed in table 12.3.

Table 12.3: Success criteria initiating event ICW 1.

Initiating event	Systems
Loss of normal cooling water supply	- One-out-of-two emergency cooling water pumps
	- Short stop and agitator
	- One-out-of-two instrument safeguarding depressurization valves
	- One-out-of-two pressure safety valves

12.6.8 System fault trees

The unavailability of the safety systems is modeled in detail in the system fault trees. The tops of these fault trees will be connected to the event tree via the accident sequence fault trees in a later stage. In many cases it is useful to model the unavailability of the support systems, e.g. electrical power, cooling or air supply, initially as separate fault trees. The top events of these support system fault trees must be named in the same way as the basic events in the front-line system fault trees referring to these support systems. This makes it possible to link the fault trees together.

In this example this is not done and the support systems are directly modeled into the safety system fault trees. Simplified system fault trees are plotted in figures 12.13, 12.14, 12.15, 12.16 and 12.17. The corresponding component identification is given in appendix 12-A.

To avoid unnecessary complexity in this example, the system failures are represented as basic events (circles) and the support systems on which they depend, e.g. the electrical power supply, are modeled as basic events as well. Note that the event tree heading events are not independent, due to the fact that three systems rely on 24V DC, two systems on 220V AC and two systems on instrument air (see also the dependency matrix in table 12.2).

Because of the fact that the instrument safeguarding depressurization system is designed as fail safe, failure of the instrument air system is not included in the fault tree. Failure of this support system will cause the instrument safeguarding depressurization valves to open and for this reason failure of the instrument air system cannot contribute to the top event and the instrument safeguarding depressurization valves fail to open.

The system fault trees are the constituents of the risk model and can be constructed using any fault tree code.

1 2.6.9 Quantification of accident sequence cut-sets

The algebraic solution (boolean reduction) of the accident sequence fault trees and the associated quantification must be established both for the accident sequence fault trees and the top logic fault trees (if present), with the systems fault trees and if necessary the support system fault trees linked to them. This will result in a number of the cut-sets for each accident sequence.

To determine the minimal cut-sets, screening values might be used for various events, e.g. for the human failures identified in the event trees and fault trees. Human failures which contribute significantly to the hazardous event frequency (”dominant failures”) are then studied further as part of the human performance task; errors which do not contribute significantly are not considered to warrant further study.

The component database used in the quantification process is listed in appendix 12-B. It should be emphasized that the data listed in appendix 12-B is for illustrative purposes only.

12.6.10 Quantification results

All non-success sequences have been quantified. The cut-sets of sequence 8 are listed in appendix 12-C. The probability of occurrence over a period of one year are tabulated in table 12.4 for each sequence quantified. As could be expected (see section 12.6.4), the probability of occurrence of sequences SEQ3, SEQ4 and SEQ5 is very low. This is due to the low probability of failure of the agitator over a period of one hour.

From appendix 12-C it is clear that the dominant contribution for a runaway reaction is:

- A failure to close of check valve 1 of the cooling water system
  During normal plant operation pump P1 is in operation. After failure of pump P1 both emergency cooling water pumps are demanded to operate. If check valve CV1 does not close after activation of both emergency cooling water pumps, backflow through pump P1 occurs and cooling of the reactor fails.

- An independent failure of one of the two air-operated valves in the input line of the short stop system

- Independent failure of both instrument safeguarding air-operated depressurization valves

- Dependent failure of both pressure safety valves.

Table 12.4: Probability of occurrence sequences

Sequence	Description	Frequency per year
SEQ2	Reaction stopped by short stop	1.1E-01
SEQ3	Burping	2.3E-06
SEQ4	Releases to environment	3.6E-07
SEQ5	Runaway reaction	4.1E-09
SEQ6	Reaction stopped by depressurization	7.9E-02
SEQ7	Releases to environment	1.5E-02
SEQ8	Runaway reaction	1.8E-04

12.7 COMPUTER CODES

To support event tree analyses special computer codes have been developed which are mostly used in combination with a fault tree code. If one does not have the intention to combine event trees with fault trees only a general purpose spreadsheet computer code like EXCEL or LOTUS are sufficient to quantify an event tree.

A large assortment of computer codes exist to perform event tree fault tree analyses. One of the most advanced code developed in Europe is RISK SPECTRUM (reference [12.9]). Well-known codes developed in the United States of America are the NUPRA code (reference [12.8]) and the CAFTA code (reference [12.7]). All three codes support as well fault tree analysis as event tree analysis and have plotting capabilities and support importance and uncertainty analyses.

12.8 REFERENCES

[12.1] Guidelines for Safe Automation of Chemical Processes, Center for chemical process safety of the American Institute of Chemical Engineers, 345 East 47 Street, New York, NY 10017, ISBN 0-8169-0554-1.

[12.2] Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples, Center for chemical process safety of the American Institute of Chemical Engineers, 345 East 47 Street, New York, NY 10017, ISBN 0-8169-0491-X.

[12.3] Guidelines for Chemical Process Quantitative Risk Analysis, Center for chemical process safety of the American Institute of Chemical Engineers, 345 East 47 Street, New York, NY 10017, ISBN 0-8169-0402-2.

[12.4] Procedures for Conducting Probabilistic Safety Assessment of Nuclear Power Plants (Level 1), Safety Series No 50-P-4, IAEA, Vienna 1992, ISBN 92-0-1-2392-8.

[12.5] NUREG/CR-2300, PRA procedure guide, A guide to the performance of probabilistic risk assessments for nuclear power plants,U.S. Nuclear regulatory commission, January 1983.

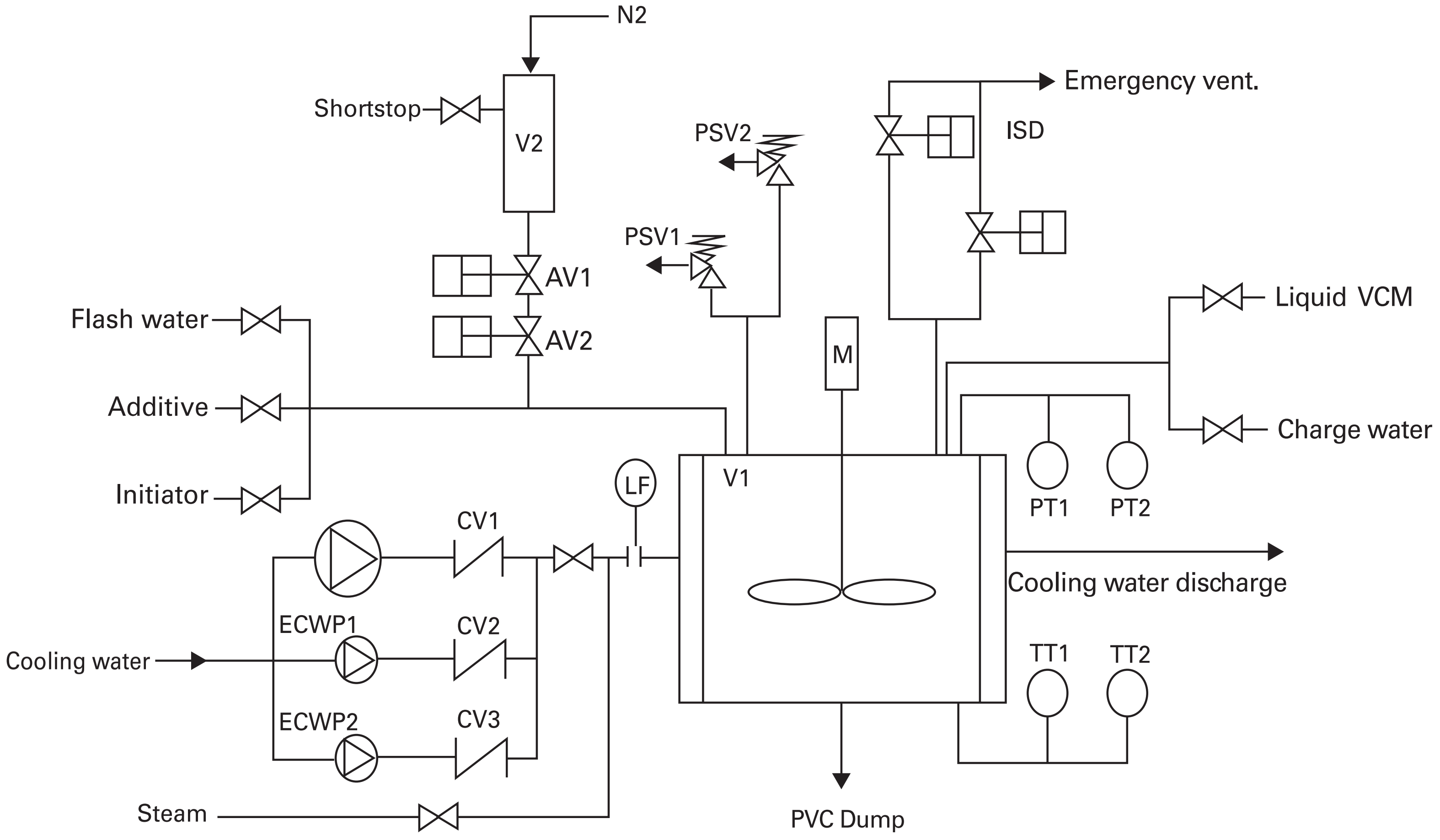
[12.6] RISKMAN User's manual, PLG. Inc., 4590 MacArthur Boulevard, Suite 400, Newport Beach, California, CA 92660-2027, USA.

[12.7] CAFTA User's manual,Science Applications International Corporation, 4920 El Camino Real, Los Altos, California 94022, USA.

[12.8] NUPRA User's manual,Halliburton NUS Corporation, 910 Clopper Road, P.O. Box 6032, Gaithersburg, MD 20877-0962, USA.

[12.9] RISK SPECTRUM, Professional Risk & Reliability Software, RELCON AB, P.O. Box 1288, S-17225 Sundbyberg, Sweden.

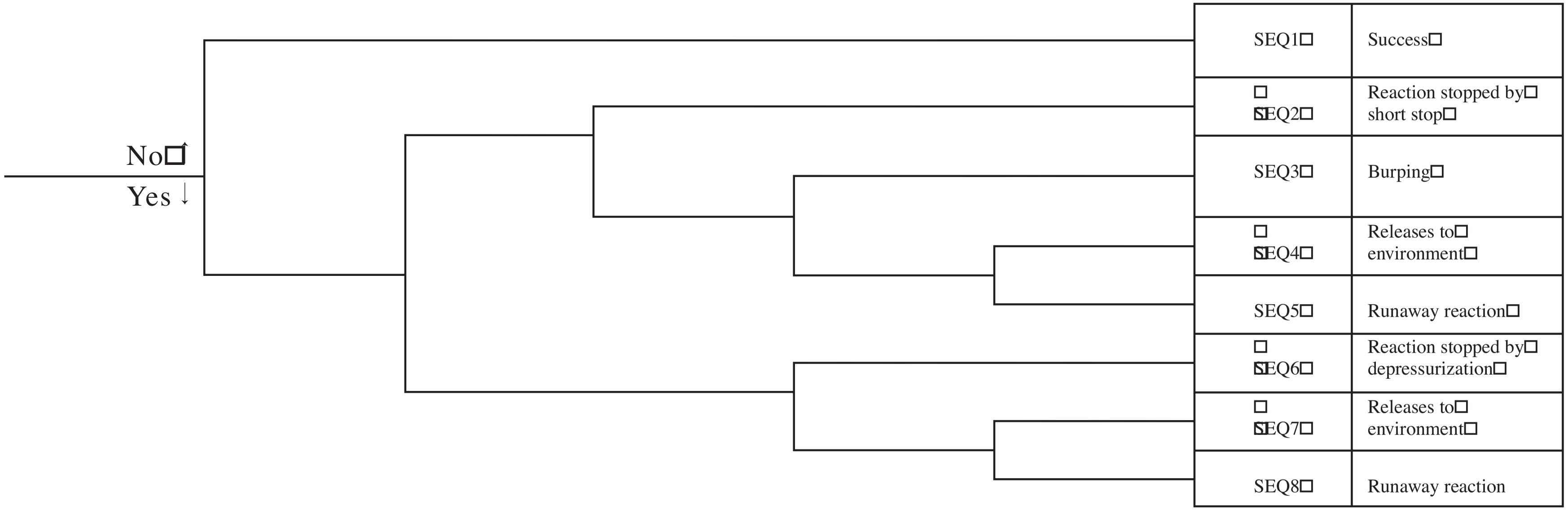
Figure 12.6: Lay-out PVC reactor.



V1 : Reactor
V2 : Shortstop
ISD : Instrument Safeguarding Depressarization

Figure 12.7: Loss of normal cooling water supply event tree.

Loss of normal□ cooling water supply□	Failure of emergency□ cooling water supply□	Operator fails to□ add short stop□	Agitator fails before□ the reaction has been□ stopped□	Instrument□ safegurading□ depressurization fails□	Pressure safety□ valves fail to open□	Sequence□ identification	Description of□ consequence
ICW1	**ECWF**	**SSF**	**AGF**	**ISDEPF**	**PSVF**		



SEQ1□	Success□
□ SEQ2□	Reaction stopped by□ short stop□
SEQ3□	Burping□
□ SEQ4□	Releases to□ environment□
SEQ5□	Runaway reaction□
□ SEQ6□	Reaction stopped by□ depressurization□
□ SEQ7□	Releases to□ environment□
SEQ8□	Runaway reaction

Figure 12.8: Accident sequence fault tree SEQ4.

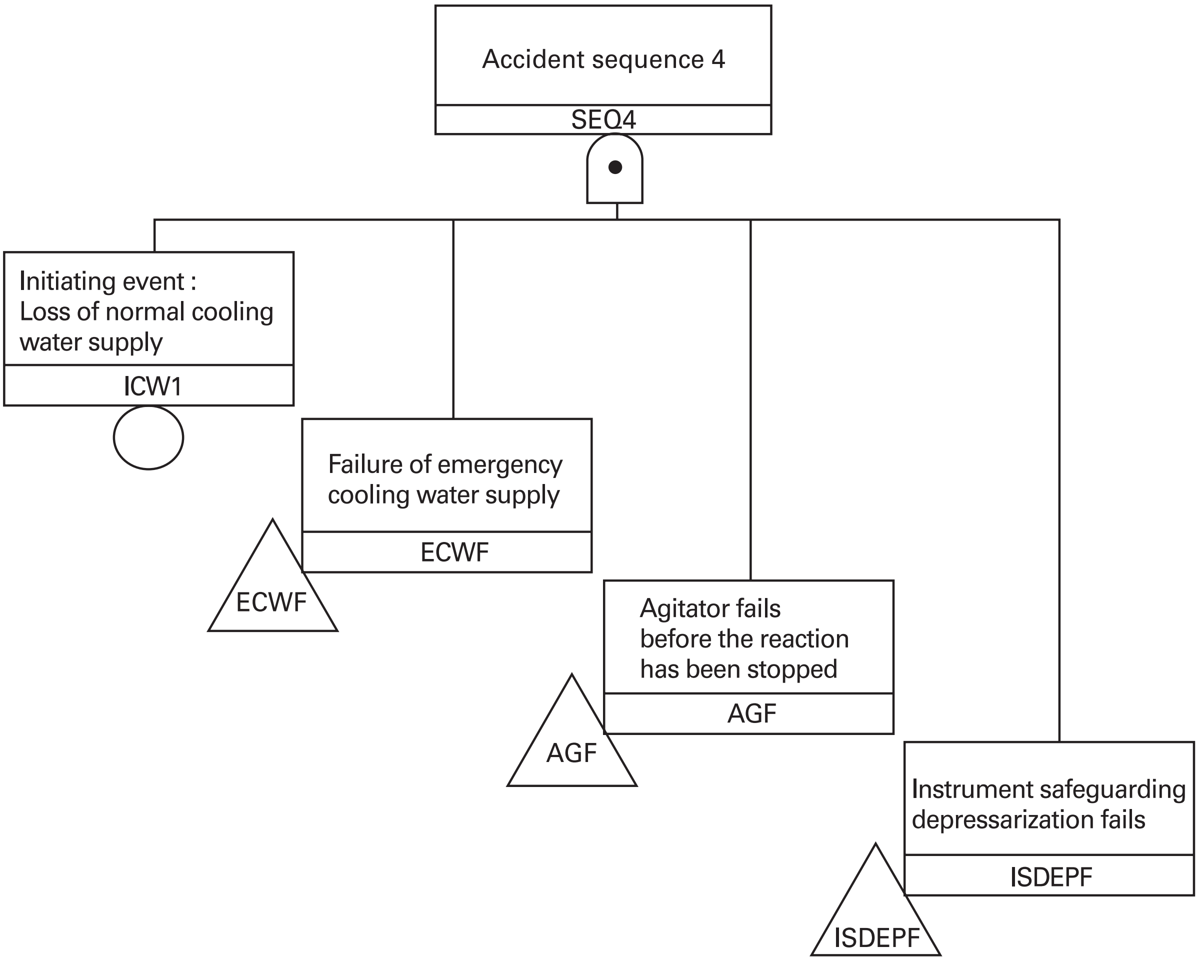

Accident sequence 4
SEQ4
Initiating event :
Loss of normal cooling water supply
ICW1
Failure of emergency cooling water supply
ECWF
ECWF
Agitator fails before the reaction has been stopped
AGF
AGF
Instrument safeguarding depressarization fails
ISDEPF
ISDEPF

Figure 12.9: Accident sequence fault tree SEQ5. Accident sequence 5

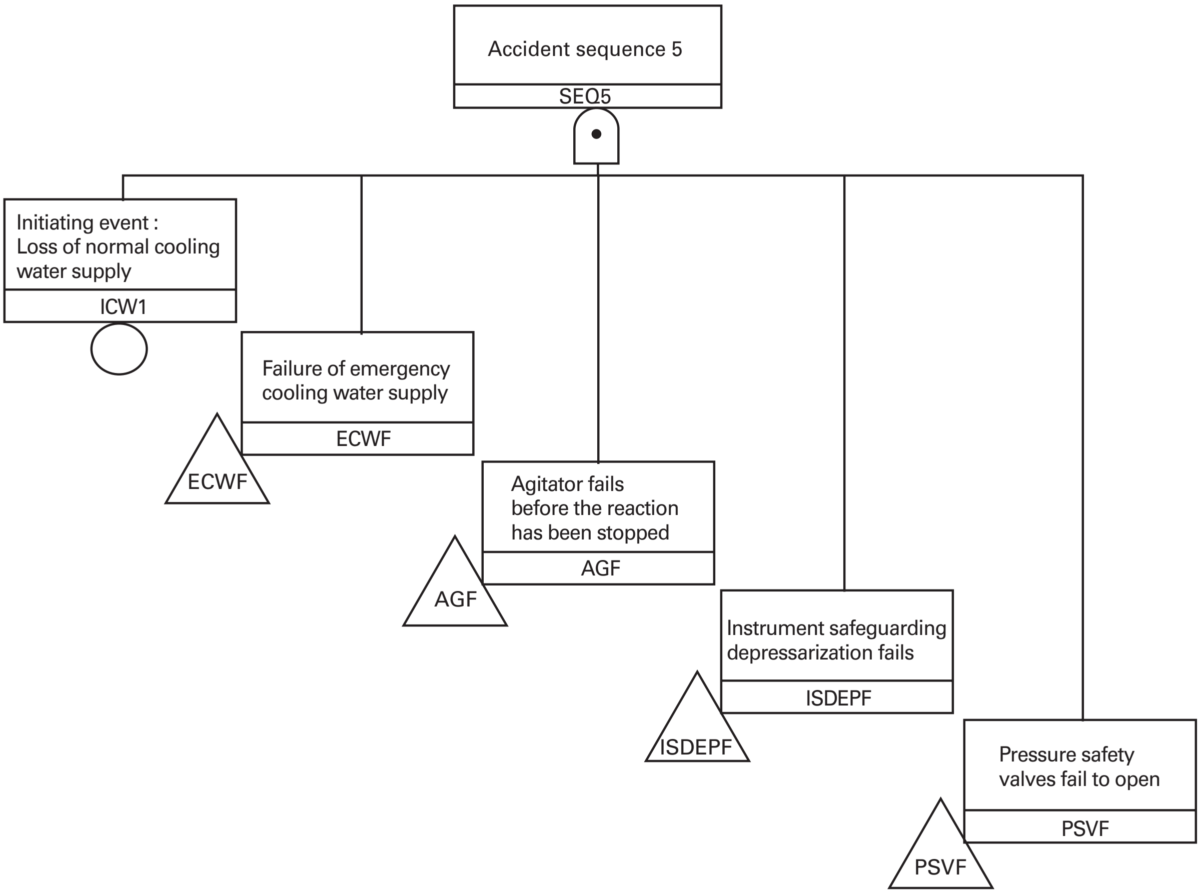


Figure 12.10: Accident sequence fault tree SEQ6. Accident sequence 6

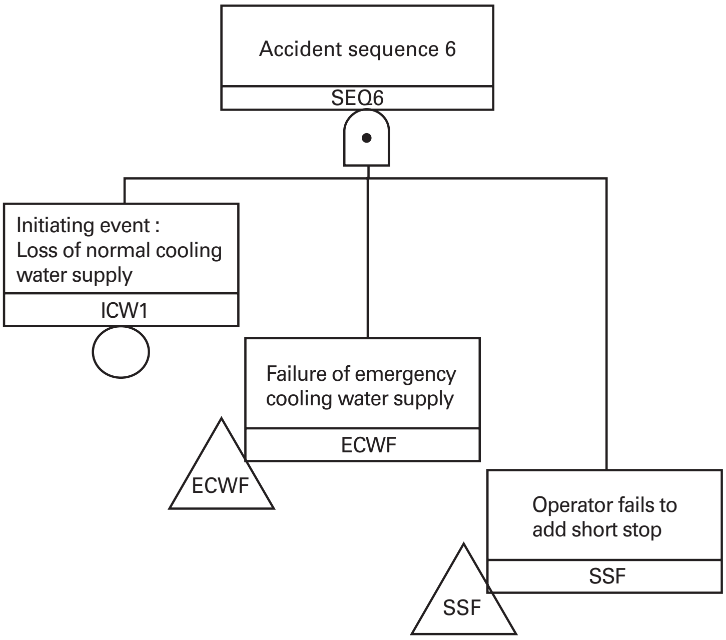

Accident sequence 6
SEQ6
Initiating event :
Loss of normal cooling water supply
ICW1
Failure of emergency cooling water supply
ECWF
ECWF
Operator fails to add short stop
SSF
SSF

Figure 12.11: Accident sequence fault tree SEQ7. Accident sequence 7

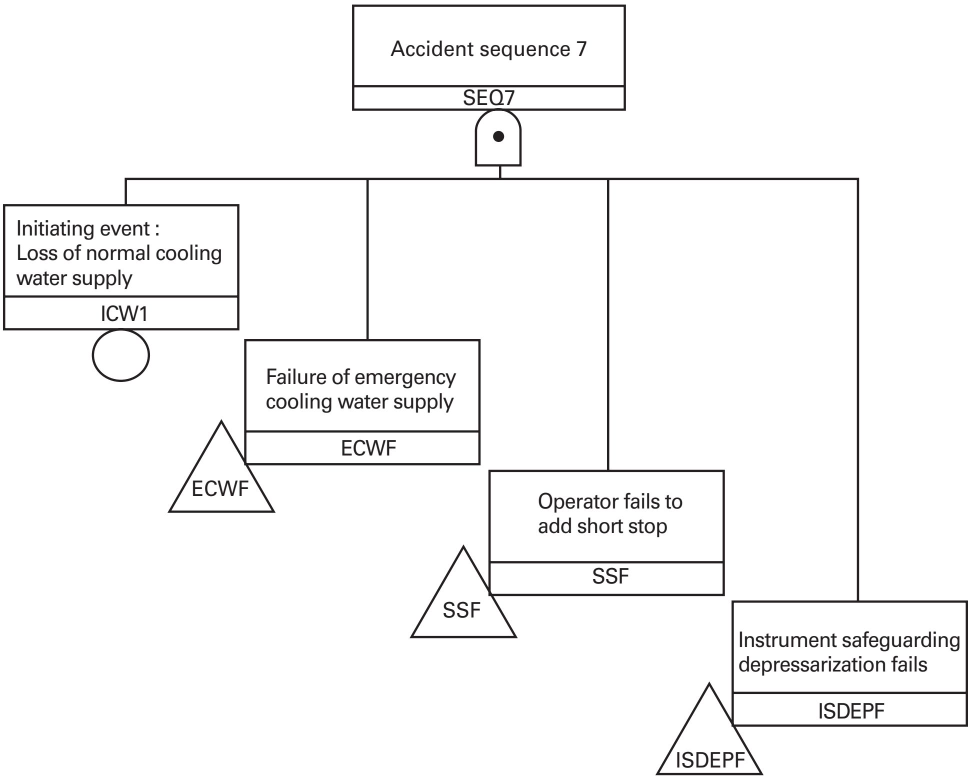

Accident sequence 7
SEQ7
Initiating event :
Loss of normal cooling water supply
ICW1
Failure of emergency cooling water supply
ECWF
ECWF
Operator fails to add short stop
SSF
SSF
Instrument safeguarding depressarization fails
ISDEPF
ISDEPF

Figure 12.12: Accident sequence fault tree SEQ8. Accident sequence 8

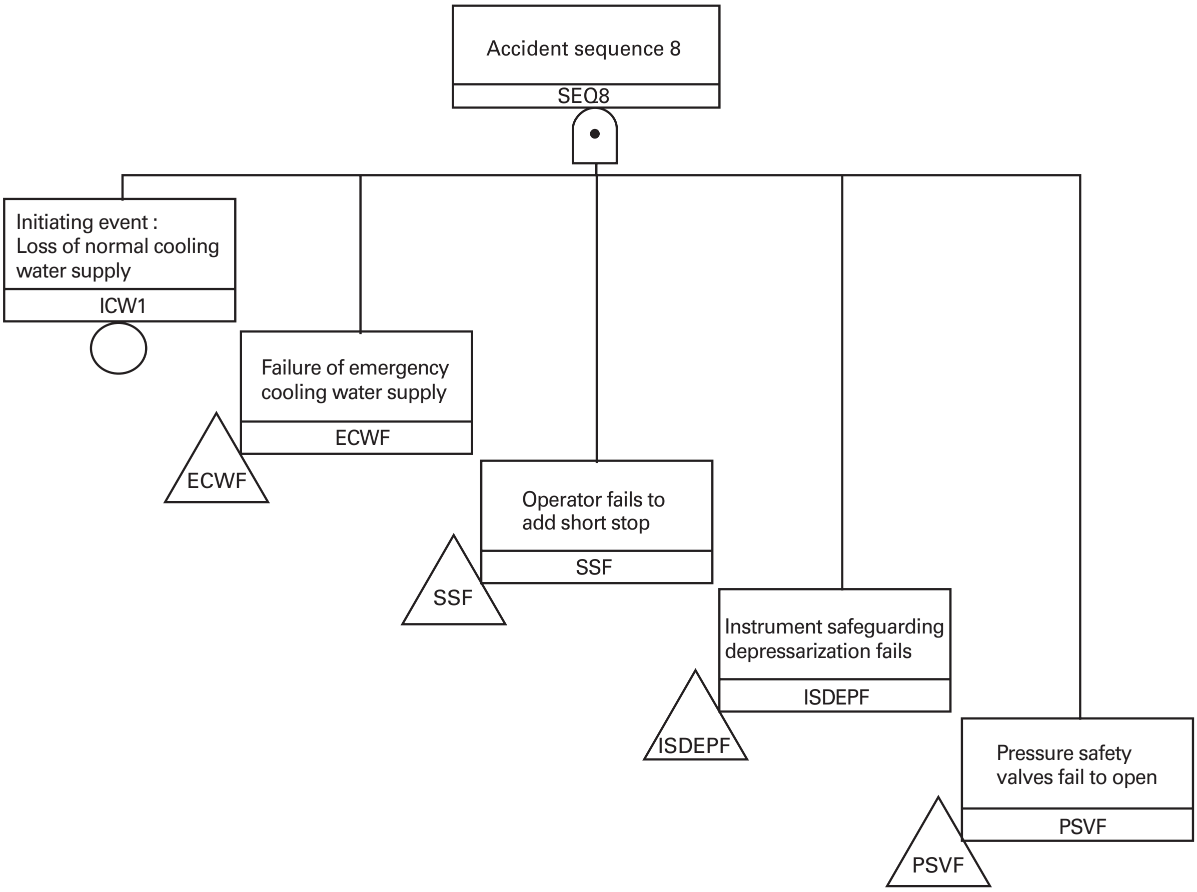


Figure 12.13: Fault tree emergency cool water system (ECWF).

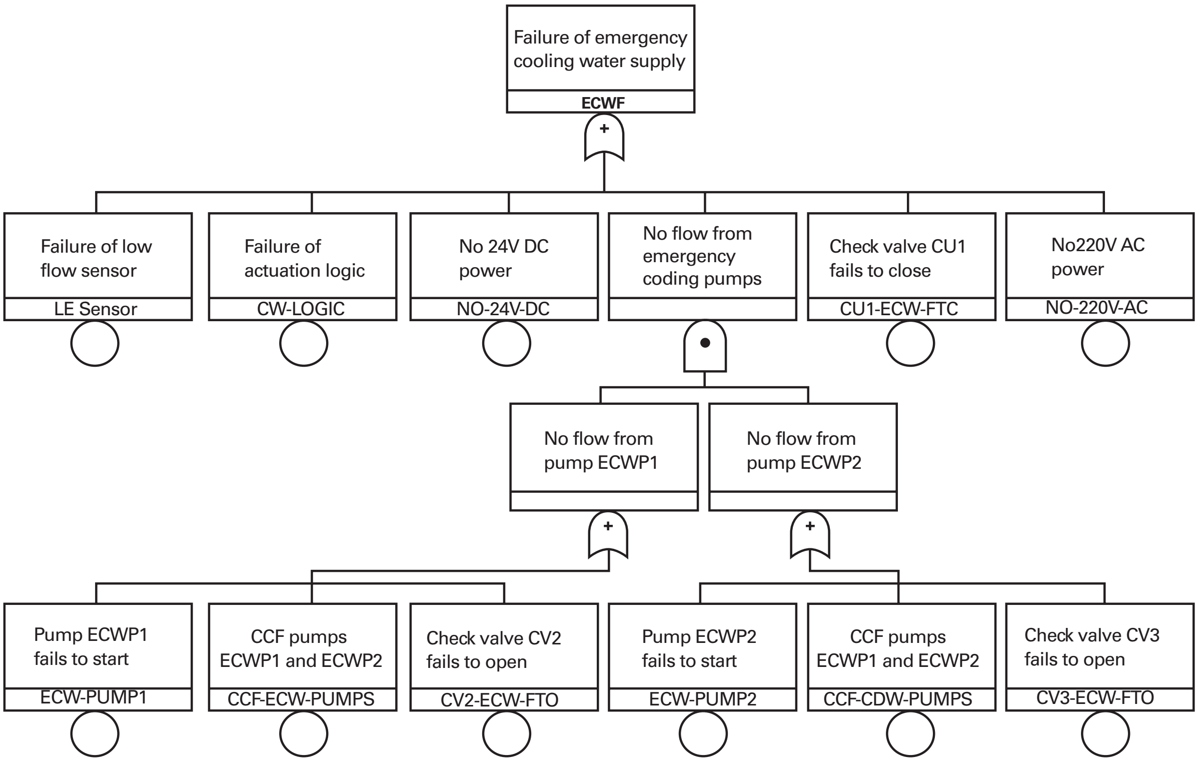

Failure of emergency cooling water supply
ECWF
+
Failure of low flow sensor
LE Sensor
Failure of actuation logic
CW-LOGIC
No 24V DC power
NO-24V-DC
No flow from emergency coding pumps
Check valve CU1 fails to close
CU1-ECW-FTC
No220V AC power
NO-220V-AC
No flow from pump ECWP1
No flow from pump ECWP2
+
+
Pump ECWP1 fails to start
ECW-PUMP1
CCF pumps ECWP1 and ECWP2
CCF-ECW-PUMPS
Check valve CV2 fails to open
CV2-ECW-FTO
Pump ECWP2 fails to start
ECW-PUMP2
CCF pumps ECWP1 and ECWP2
CCF-CDW-PUMPS
Check valve CV3 fails to open
CV3-ECW-FTO

Figure 12.14: Fault tree failure to add short stop (SSF).

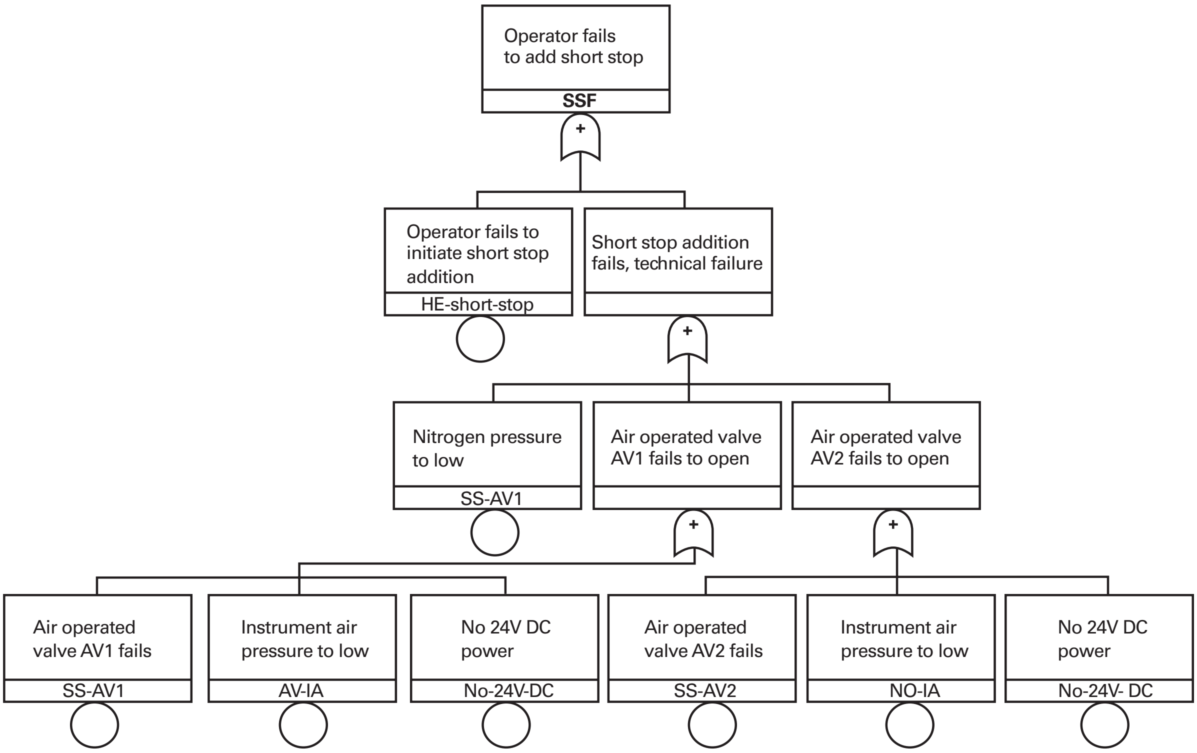

Operator fails to add short stop
SSF
+
Operator fails to initiate short stop addition
HE-short-stop
Short stop addition fails, technical failure
+
Nitrogen pressure to low
SS-AV1
Air operated valve AV1 fails to open
+
Air operated valve AV2 fails to open
+
Air operated valve AV1 fails
SS-AV1
Instrument air pressure to low
AV-IA
No 24V DC power
No-24V-DC
Air operated valve AV2 fails
SS-AV2
Instrument air pressure to low
NO-IA
No 24V DC power
No-24V- DC

Figure 12.15: Fault tree agitator failure (AGF)

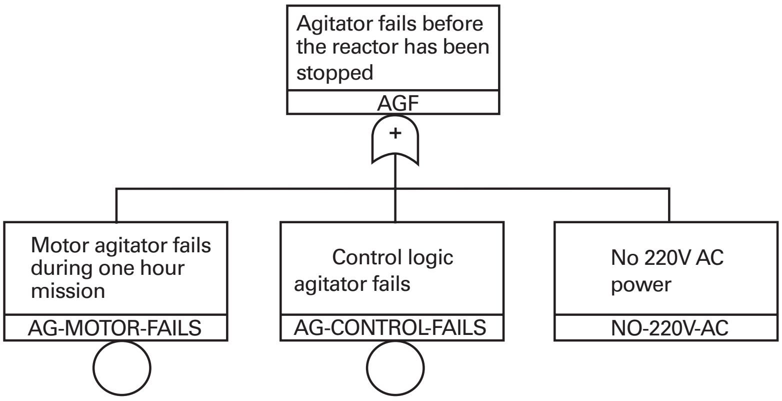
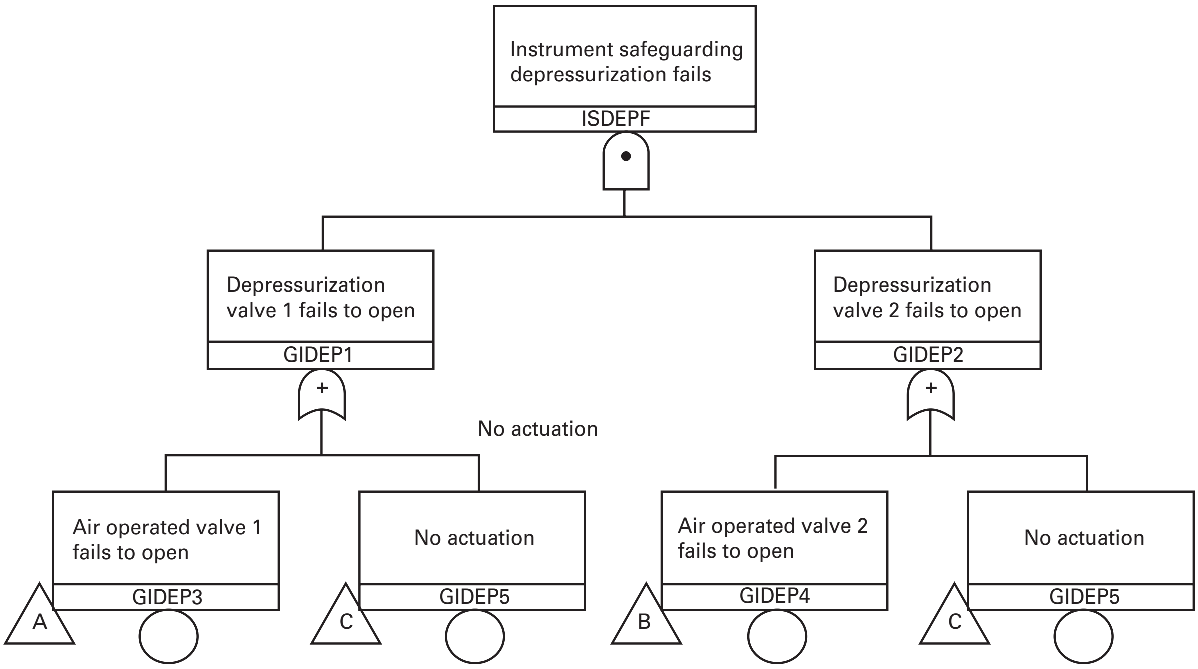
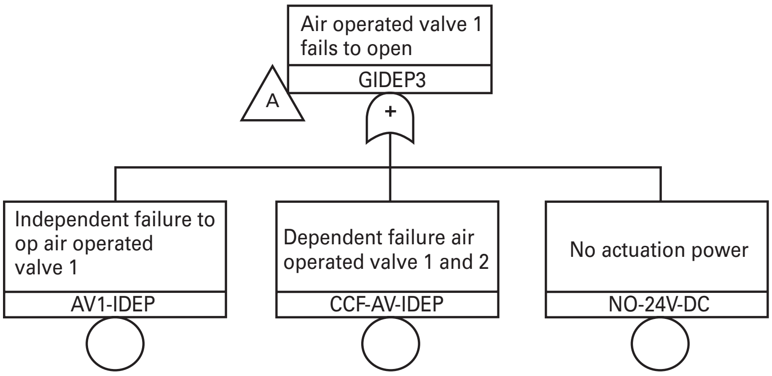

Agitator fails before the reactor has been stopped
AGF
+
Motor agitator fails during one hour mission
AG-MOTOR-FAILS
Control logic agitator fails
AG-CONTROL-FAILS
No 220V AC power
NO-220V-AC

Figure 12.16a Fault tree instrument safeguarding depressurization (ISDEPF).


Instrument safeguarding depressurization fails
ISDEPF
Depressurization valve 1 fails to open
GIDEP1
Depressurization valve 2 fails to open
GIDEP2
No actuation
Air operated valve 1 fails to open
GIDEP3
A
No actuation
GIDEP5
C
Air operated valve 2 fails to open
GIDEP4
B
No actuation
GIDEP5
C

12.16b: Fault tree instrument safeguarding depressurization (ISDEPF).


Air operated valve 1 fails to open
GIDEP3
A
+
Independent failure to op air operated valve 1
AV1-IDEP
Dependent failure air operated valve 1 and 2
CCF-AV-IDEP
No actuation power
NO-24V-DC

12.16c: Fault tree instrument safeguarding depressurization (ISDEPF).

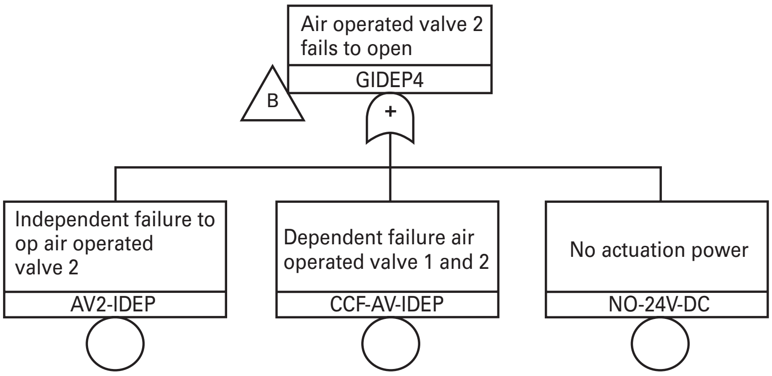
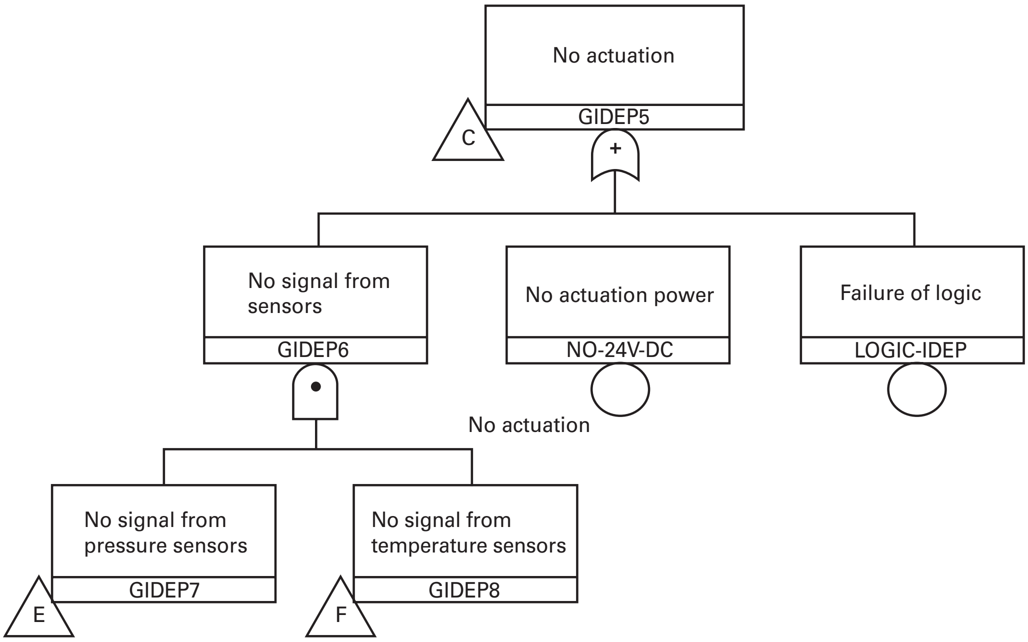
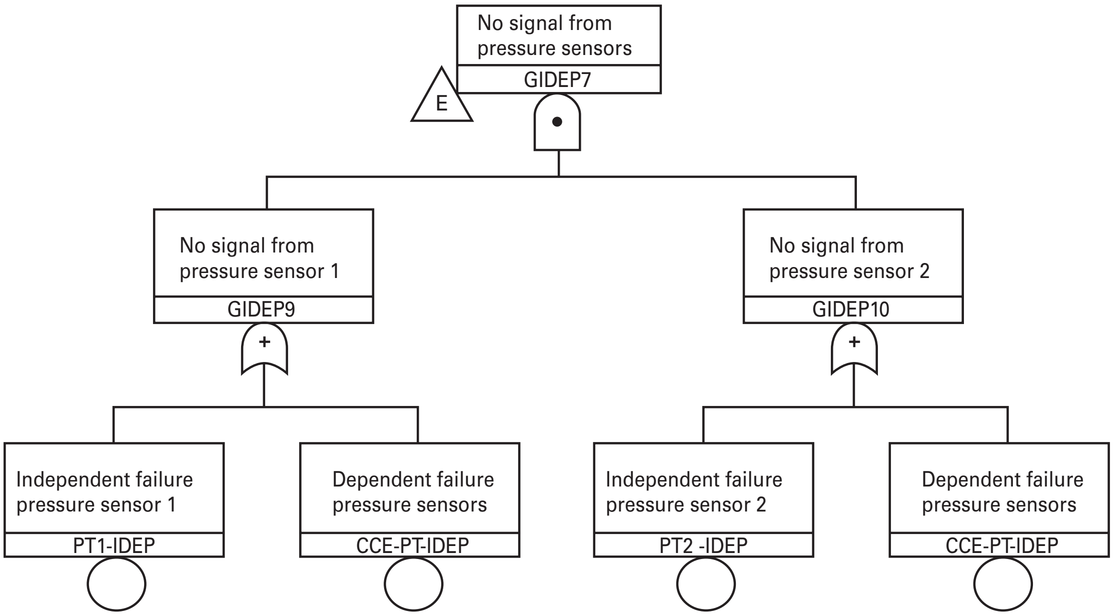

Air operated valve 2 fails to open
GIDEP4
B
+
Independent failure to op air operated valve 2
AV2-IDEP
Dependent failure air operated valve 1 and 2
CCF-AV-IDEP
No actuation power
NO-24V-DC

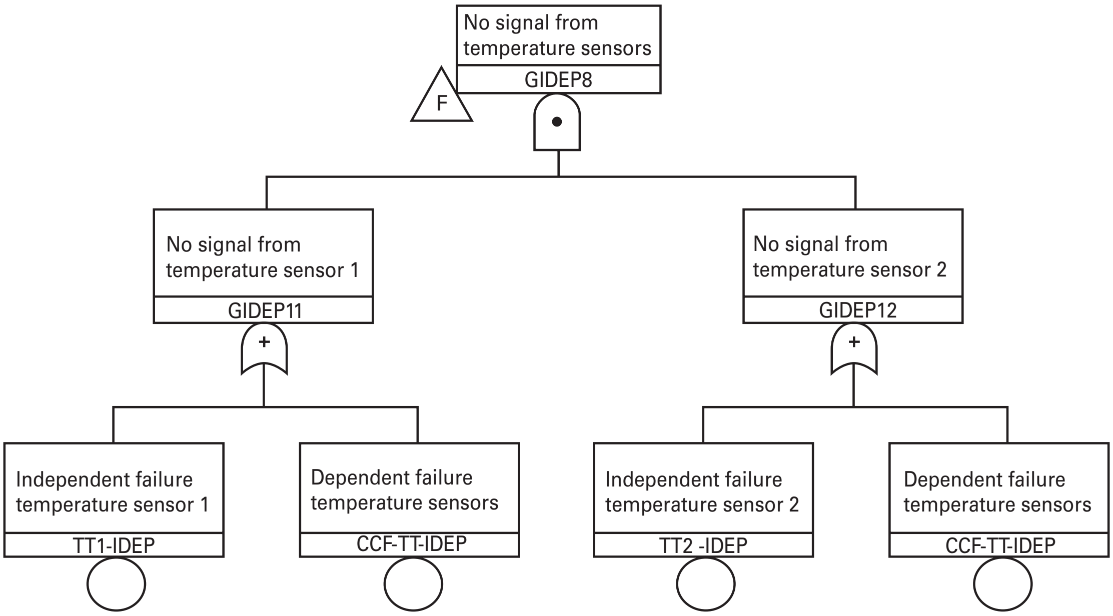
Figure 12.16d: Fault tree instrument safeguarding depressurization (ISDEPF). No actuation



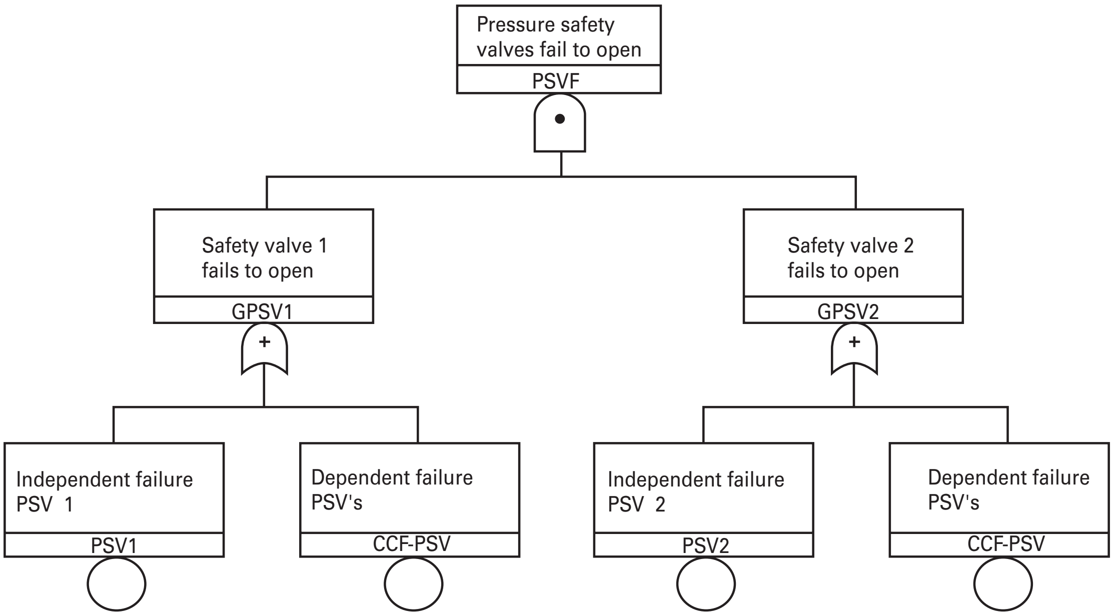
12.16e: Fault tree instrument safeguarding depressurization (ISDEPF).


No signal from pressure sensors
GIDEP7
E
No signal from pressure sensor 1
GIDEP9
No signal from pressure sensor 2
GIDEP10
Independent failure pressure sensor 1
PT1-IDEP
Dependent failure pressure sensors
CCE-PT-IDEP
Independent failure pressure sensor 2
PT2 -IDEP
Dependent failure pressure sensors
CCE-PT-IDEP

12.16f: Fault tree instrument safeguarding depressurization (ISDEPF).


No signal from temperature sensors
GIDEP8
F
No signal from temperature sensor 1
GIDEP11
No signal from temperature sensor 2
GIDEP12
Independent failure temperature sensor 1
TT1-IDEP
Dependent failure temperature sensors
CCF-TT-IDEP
Independent failure temperature sensor 2
TT2 -IDEP
Dependent failure temperature sensors
CCF-TT-IDEP

12.17: Fault tree pressure safety valves (PSVF).


Pressure safety valves fail to open
PSVF
Safety valve 1 fails to open
GPSV1
Safety valve 2 fails to open
GPSV2
+
+
Independent failure PSV 1
PSV1
Dependent failure PSV's
CCF-PSV
Independent failure PSV 2
PSV2
Dependent failure PSV's
CCF-PSV

Appendix 12-A: Component identification.

Basic Event	Description
AG_CONTROL_FAILS	Control logic agitator fails during one-hour mission
AG_MOTOR_FAILS	Motor agitator fails during one-hour mission
AV1_IDEP	Air-operated valve 1 instrument depressurization fails to open
AV2_IDEP	Air-operated valve 2 instrument depressurization fails to open
CCF_AV_IDEP	Dependent failure air-operated valves instrument depressurization
CCF_ECW_PUMPS	Dependent failure emergency feedwater pumps
CCF_PSV	Dependent failure pressure safety valves
CCF_PT_IDEP	Dependent failure pressure transmitters
CCF_TT_IDEP	Dependent failure temperature transmitters
CV1_ECW-FTC	Check valve 1 cooling water system fails to close
CV2_ECW_FTO	Check valve 2 cooling water system fails to open
CV3_ECW_FTO	Check valve 3 cooling water system fails to open
CW_LOGIC	Logic cooling water system fails to respond
ECW_PUMP1	Emergency cooling water pump 1 fails to start
ECW_PUMP2	Emergency cooling water pump 2 fails to start
HE_SHORT_STOP	Operator fails to activate short stop addition
ICW1	Initiating event, loss of normal cooling water supply
LF_SENSOR	Failure of low flow sensor cooling water system
LOGIC_IDEP	Logic instrument depressurization fails to respond
N2_FAILURE	Nitrogen pressure too low to add short stop
NO_24V_DC	24V DC power supply failure
NO_220V_AC	220V AC power supply fails during mission of one hour
NO_IA	Instrument air supply failure
PSV1	Pressure safety valve 1 fails to open
PSV2	Pressure safety valve 2 fails to open
PT1_IDEP	Pressure transmitter 1 fails to respond
PT2_IDEP	Pressure transmitter 2 fails to respond
SS_AV1	Air-operated valve 1 short stop fails to open
SS_AV2	Air-operated valve 2 short stop fails to open
TT1_IDEP	Temperature transmitter 1 fails to respond
TT2_IDEP	Temperature transmitter 2 fails to respond

Appendix 12-B: Component database

Basic Event	Type	Lambda, Q	T	Theta
AG_CONTROL_FAILS	4	1.00E-07	1	0
AG_MOTOR_FAILS	4	2.00E-05	1	0
AV1_IDEP	1	5.00E-05	8760	0
AV2_IDEP	1	5.00E-05	8760	0
CCF_AV_IDEP	1	1.00E-05	8760	0
CCF_ECW_PUMPS	1	5.00E-06	8760	0
CCF_PSV	1	1.00E-06	8760	0
CCF_PT_IDEP	1	3.00E-07	8760	0
CCF_TT_IDEP	1	5.00E-07	8760	0
CV1_ECW_FTC	1	1.00E-04	8760	0
CV2_ECW_FTO	1	1.00E-06	8760	0
CV3_ECW_FTO	1	1.00E-06	8760	0
CW_LOGIC	1	1.00E-07	8760	0
ECW_PUMP1	1	5.00E-05	8760	0
ECW_PUMP2	1	5.00E-05	8760	0
HE_SHORT_STOP	3	5.00E-02	8760	0
ICW1	3	2.00E-01	8760	0
LF_SENSOR	1	8.00E-06	8760	0
LOGIC_IDEP	1	1.00E-07	8760	0
N2_FAILURE	1	1.00E-05	8760	0
NO_24V_DC	2	5.00E-06	0	4.00
NO_220V_AC	4	3.00E-05	1	0
NO_IA	2	1.00E-05	0	4.00
PSV1	1	1.00E-05	8760	0
PSV2	1	1.00E-05	8760	0
PT1_IDEP	1	3.00E-06	8760	0
PT2_IDEP	1	3.00E-06	8760	0
SS_AV1	1	5.00E-05	8760	0
SS_AV2	1	5.00E-05	8760	0
TT1_IDEP	1	5.00E-06	8760	0
TT2_IDEP	1	5.00E-06	8760	0

```
Remarks:

1:      Lambda      per hour
        Q           per demand
        T           hour (test period)
        Theta       hour (repair duration)
        ICW1        per year

2: Type:
   1     :Time-related component model in stand-by mode of operation
   2     :Time-related component model in continuous mode of operation
   3     :bemand-related model component
   4     :Time-related model with required mission time of operation.
```

Appendix 12-C: Cut-set list sequence 8.

```
Total contributions: 1.8E-04

    Cut set             Contribution   Per cent  Formula   Recovery

1   ICW1                2.15E-05       12.22     400
    AV1_IDEP
    AV2_IDEP
    CCF_PSV
    CV1_ECW-FTC
    SS_AV1

2   ICW1                2.15E-05       12.22     400
    AV1_IDEP
    AV2_IDEP
    CCF_PSV
    CV1_ECW_FTC
    SS_AV2

3   ICW1                1.61E-05       9.18      400
    AV1_IDEP
    AV2_IDEP
    PSV1
    PSV2
    CV1_ECW_FTC
    SS_AV1

4   ICW1                1.61E-05       9.18      400
    AV1_IDEP
    AV2_IDEP
    PSV1
    PSV2
    CV1_ECW_FTC
    SS_AV2

5   ICW1                1.18E-05       6.70      400
    CCF_PSV
    CCF_AV_IDEP
    CV1_ECW_FTC
    SS_AV1

6   ICW1                1.18E-05       6.70      400
    CCF_PSV
    CCF_AV_IDEP
    CV1_ECW_FTC
    SS_AV2

7   ICW1                8.60E-06       4.89      400
    PSVI
    PSV2
    CCF_AV_IDEP
    CV1_ECW_FTC
    SS_AV1

8   ICW1                8.60E-06       4.89      400
    PSV1
    PSV2
    CCF_AV_IDEP
    CV1_ECW_FTC
    SS_AV2

9   ICW1                4.30E-06       2.44      400
    AV1_IDEP
    AV2_IDEP
    CCF_PSV
    CV1_ECW_FTC
    N2_FAILURE
```

```
10  ICW1                  4.03E-06       2.29      400
    AV1_IDEP
    AV2_IDEP
    CCF_PSV
    ECW_PUMP1
    ECW_PUMP2
    SS_AV1

11  ICW1                  4.03E-06       2.29      400
    AV1_IDEP
    AV2_IDEP
    CCF_PSV
    ECW_PUMP1
    ECW_PUMP2
    SS_AV2

12  ICW1                  3.23E-06       1.84      400
    AV1_IDEP
    AV2_IDEP
    PSV1
    PSV2
    CV1_ECW_FTC
    N2_FAILURE

13  ICW1                  2.94E-06       1.67      400
    AV1_IDEP
    AV2_IDEP
    CCF_PSV
    CV1_ECW_FTC
    HE_SHORT_STOP

14  ICW1                  2.36E-06       1.34      400
    CCF_PSV
    CCF_AV_IDEP
    CV1_ECW_FTC
    N2_FAILURE

15  ICW1                  2.15E-06       1.22      400
    CCF_PSV
    ECW_PUMP1
    ECW_PUMP2
    CCF_AV_IDEP
    SS_AV1

16  ICW1                  2.15E-06       1.22      400
    CCF_PSV
    ECW_PUMP1
    ECW_PUMP2
    CCF_AV_IDEP
    SS_AV2
```

```
17  ICW1                  2.15E-06       1.22      400
    AV1_IDEP
    AV2_IDEP
    PSVI
    PSV2
    CV1_ECW_FTC
    HE_SHORT_STOP

18  ICW1                  1.72E-06       0.98      400
    PSV1
    PSV2
    CCF_AV_IDEP
    CV1_ECW_FTC
    N2_FAILURE

19  ICW1                  1.72E-06       0.98      400
    AV1_IDEP
    AV2_IDEP
    CCF_PSV
    LF_SENSOR
    SS_AV1

20  ICW1                  1.72E-06       0.98      400
    AV1_IDEP
    AV2_IDEP
    CCF_PSV
    LF_SENSOR
    SS_AV2
```

DEPENDENT FAILURE ANALYSIS

CONTENTS

13.1 INTRODUCTION

An independent failure event is defined as an event in which a component failure occurs, causally unrelated to any other component failure. On the other hand, two or more failure events causally related are called dependent failure events.

In probabilistic safety assessments, treatment of dependencies is very important because dependent failures can be dominant contributors to system unavailabilities.The following types of dependencies can be distinguished:

1: Shared equipment dependencies, where one system is a support system for others or a component is shared by several systems/subsystems. Failure of the support system leads directly to complete or partial failure of all the supported systems.

2: Functional dependencies, where the operation or non-operation of a system affects the ability of another system to be operated (e.g. where a low pressure injection system cannot be used unless the reactor is depressurized first).

3: Common cause initiators, where the failure of a support system causes an initiating event and also impacts the availability of mitigating systems.

4: Human interaction dependencies, where an operator error affects the operation of one or more than one system or component.

5: Physical interaction failures, where the environmental effects caused by a failure (e.g. after a pipe rupture) cause other systems to fail.

6: Common cause failures where two or more identical or similar components fail at the same time because of some common cause not covered by explicit modelling of the types of dependencies given above. Common cause failures may, for example, be due to design errors or deficiencies, lack of quality control in manufacturing or installation, procedural errors during operation or maintenance, or environmental effects such as excessive temperature.

7: One special type of common cause failure that has to be considered is that class that might impact on multiple human failure events in a given scenario.

8: Major energetic external events which have the capability of causing damage to a wide range of equipment, cutting across system boundaries.

Some dependent failure events can be clearly understood at the time of system modelling and are therefore explicitly modelled in the event or fault trees. An example of such an event is a multiple component failure caused by failure of a common support system, like failure due to loss of the instrument air supply system.The first five types of dependencies belong to this category.

In a probabilistic risk assessment, that group of dependent events whose failure mechanisms are not modelled explicitly in the system logic model and whose cause does not involve failure or unavailability of another component are known as common cause events. Their causes are typically unforeseen events, conditions or phenomena. For example they can arise from problems of design, external environment, extreme meteorological conditions, manufacturing faults, human errors, etc. Common cause failures are inevitable, although they can be reduced with appropriate defences or suitable countermeasures.

The sixth type is most important when analysing redundant systems in which each channel or train has identical components. Common cause failures can lead to loss of more than one channel or train. Common cause failure (CCF) can also form a dependence in which identical or similar components fail due to the same cause in different systems causing failure of both systems. They are addressed by adding common cause failure events to the logic model. In standard probabilistic safety assessment practice, common cause failure events are generally only modelled within a redundant system.

The seventh type is handled during the quantification of event sequence frequencies and requires specific HRA input. The Human Reliability Analysis section explains how to handle these type of dependencies.

The external events are usually addressed by performing specialized studies using an already existing internal events model.

In order to understand the methodology presented in this document, it is strongly recommended to read all the definitions concerning dependent failures very carefully.

13.1.1 **Dependent events and their mechanisms**

To understand and model dependent events, it is necessary to answer three questions:
- Why do components fail or why are they unavailable?
- What is it that can lead to multiple failures?
- Are there any measures taken to prevent the occurrence of multiple failures.

These questions lead to the consideration of three concepts:
- Root cause
- Linking or coupling mechanism
- Defences strategy against dependent failures.

A root cause is the basic reason or reasons why a component fails, any of which, if corrected would prevent the occurrence of the component failure. For failures to become multiple failures from the same cause, the conditions have to affect all the components simultaneously. This is called the coupling mechanism. Dependent failures can be prevented by a variety of defences. A defence can operate to prevent the occurrence of failure (root cause) or to decouple the failures by decreasing the similarity of components and their environment (coupling mechanism).

In literature the terms conditioning event and trigger event are sometimes used. A conditioning event is an event which predisposes a component to failure, or increases its susceptibility to failure, but does not itself cause failure. In the case of a pump failure due to high humidity, the conditioning event could have been failure of maintenance personnel to properly seal the pump control cabinet following maintenance. The effect of the conditioning event is latent, but the conditioning event is in this case a necessary contribution to the failure mechanism.

A trigger event is defined as an event which activates a failure, or initiates the transition to the failed state, whether or not the failure is revealed at the time the trigger event occurs. An event which has led to high humidity in a room would be such a trigger event. A trigger event is therefore a dynamic feature of the failure mechanism. A trigger event, particularly in the case of common cause events, is usually an event external to the components in question.

Root cause:
A root cause is the basic reason or reasons why a component fails. There are four general types of root causes.

a: Hardware
Isolated random equipment failures due to causes inherent in the affected component.

b: Human Errors
during plant operations (dynamic interaction with the plant), errors during equipment testing or maintenance, and errors during design, manufacturing and construction.

c: Environmental
Events that are external to the equipment but internat to the plant that result in environmental stresses being applied to the equipment.

d: External
Events that initiate externally to the plant and that result in abnormal environmental stresses being applied to the equipment.

A number of generic causes of dependent failures are listed appendix 13-A, tables 13-A-1 and 13-A-2.

Coupling mechanism:
Given the existence of the root cause, the second concept of importance is that of a linking or coupling mechanism, which is what leads to multiple equipment failure. The coupling mechanism explains why a particular cause impacts on several components. Obviously, each component fails because of its susceptibility to the conditions created by the root cause, and the role of the coupling mechanism or link is in making those conditions common to several components. The three broad categories of coupling mechanisms are functional, spatial, and human.

a: Functional Couplings

- **Connected equipment**
  Encompasses plant design involving shared equipment, common input, and loop dependencies plus situations in which the same equipment provides multiple functions.

- **Nonconnected equipment**
  Encompasses interrelated success criteria, such as the relationship between a standby system and the system it is supporting. More subtle forms of nonconnected equipment couplings are environmental conductors, such as heating, ventilation, and air conditioning systems.

b: Spatial Couplings

- **Spatial proximity**
  Refers to equipment found within a common room, fire barriers, flood barriers, or missile barriers.

- **Linked equipment**
  Equipment in different locations that, although not functionally related, is similarly affected by an extreme environmental condition possibly due to the breach of a barrier.

c: Human Couplings
Refers to activities, such as design, manufacturing, construction, installation, quality control, plant management, station operating procedures, emergency procedures, maintenance, testing and inspection procedures, and implementation, etc.

For example, suppose that two components are susceptible to fire and that they are located in the same room. A dependent failure event could occur as a result of an event at the plant, which results in a fire in this room. Fire is the root cause of failure of both components. One immediately recognizable coupling mechanism is the fact that both components are located in the same room. For some examples of coupling mechanisms see appendix 13-A, table 13-A-3.

Defence strategy:
The third concept is the concept of engineered or operational defences against unanticipated equipment. Typical tactics applied in a defensive scheme include design control, segregation of equipment, well designed test and inspection procedures, maintenance procedures, review of procedures, training of personnel, manufacturing and construction quality control, and installation and commissioning quality control.The different tactics may be particularly effective in mitigating specific types of dependent or common cause failures.

As an example of a defensive strategy, physical separation of redundant equipment reduces the probability of simultaneous failure of the equipment due to certain environmental effects. In this case the defence operates to remove the coupling mechanism.

13.1.2 Classification of dependent failures

Dependent failures can be classified according to the characteristics of the event and the time at which it is introduced into the system. This will be particularly relevant when considering the defences against dependent failures. Normally dependent failures are classified in four groups.

- *Design errors*
  Common characteristics in the design phase can result in errors. If these errors are not revealed and corrected prior to the operations stage they will persist as an actual or a potential dependent failure until revealed by some operations procedure, or by a system failure at a time when a demand is made on the system to operate. Functional deficiencies in the design specification stage or realization faults result in a system not having the capability to perform the necessary function.

- *Construction errors*
  Actual or potential dependent failure can be introduced into a system during the Construction stages when the design is converted into an operational system in its operational environment. They will have similar effects on the system, if they are not revealed and corrected, by persisting until revealed by some operations procedure or by a system failure at the time when a demand is made on the system to operate.

- *Operator errors*
  Dependencies can be introduced into a system by activities which are associated with the interfaces between the system and the various types of operations staff involved. It not only includes the activities themselves, but the written procedures and supervision which control them.

- *Energetic events*
  Extremes of normal environmental conditions within the design limits or even more adverse conditions, either continuous or transient, perhaps due to some circumstances that were not anticipated in the design stage, can induce a dependent failure into a redundant system. Such conditions can cause increased component failure rates, which might be interpreted as a dependent failure, or can cause sudden complete failure, which is much more likely to be identified as a dependent failure.

13.1.3 **Defences against dependent failures**

Dependent failures can be prevented by a variety of defences. A defence can operate to prevent the occurrence of failures or to decouple failures. An example to prevent the occurrence of failures is to ensure that control cabinets are adequately protected against humidity by a quality control of the seals. This is equivalent to ensuring the hardening of the components, and is a defence against potential conditioning events. Another example of a defence that attempts to prevent the occurrence of failures is the training of maintenance staff to ensure correct interpretation of procedures. The coupling factors are not directly affected by these two defences.

A defence against dependent failures by decoupling can be achieved by effectively decreasing the similarity of components and their environment in some way that prevents a particular type of failure cause from affecting all components simultaneously and allows more opportunities for detecting failures before they appear in all components of the group.

The key to successful mitigation and prevention of dependent failures is to understand how the primary defences might fail. A general set of defence tactics described below. This set is to be regarded as general tactics implemented to decrease the likelihood of component or system unavailability.

- *Separation*
  Separation by barriers to confine or restrict any physical phenomena to prevent a potentially damaging condition to all components.

- *Diversity*
  The use of totally different approaches to achieve the same result (functional diversity) or the use of different types of equipment (equipment diversity) to perform the same function.

- *Fail-safe design*
  In certain cases, application of the fait-safe principle affords added protection against dependent failures. Where possible, safeguard systems are designed such that faults in the system or failure of a support system (e.g. power supply) trigger actions that restore the plant to a safe condition.

- *Staggered testing and maintenance*
  In case of staggered testing, the interval between tests of two similar components is shortened. Severe failure of a whole higher redundant system can already be detected by only two subsequent tests, the results of which will reveal a common cause failure condition, if present. Staggered testing results in reducing the potential system downtime to only a small fraction of the system's test interval. An example is a common cause failure that appears after a certain number of pump operating hours, i.e. is fatigue-related. If all the redundant pumps are switched regularly so that they all have approximately the same history of operating time, then it is more likely that such a root cause will propagate into failure of all pumps at about the same time (high potential for common cause). Therefore, a preventive measure could be to keep at least one pump with a much smaller history of operating time and to perform preventive maintenance in a staggered way.

- *Functional and Proof testing*
  Commissioning with proof testing is considered as an intensive debugging phase, in which unexpected failure behaviour can at least be detected for components which are installed in large quantities. On the system level, latent initial design or construction errors can be identified and eliminated by demands under increasingly realistic conditions.

- *Quality Control*
  A program to ensure that the product is in conformance with the documented design, and that its operation and maintenance take place according to approved procedures, standards and regulatory requirements.

13.2 NOMENCLATURE

EF	=	error factor	-
m	=	number of components in the common-cause component group	-
n_k	=	number of historical events involving k components in a failed state	-
T	=	test period	hour
Q_k	=	failure rate or probability of failure on demand of a basic event involving k specific components	-/hour or -
Q_t	=	total failure rate (independent and dependent) or total probability of failure on demand	-/hour or -
Qi	=	independent failure frequency for each component.	-/hour
p	=	conditional probability of failure of each component, given a non-lethal shock.	
α_k	=	fraction of the total frequency of failure events occurring in the system and involving of k out of m components due to common cause	-
μ	=	frequency of occurrence of non-lethal shocks	-/hour
ω	=	frequency of occurrence of lethal shocks	-/hour

13.3 FRAMEWORK TO PERFORM A COMMON CAUSE FAILURE ANALYSIS

To analyse dependent failures, a framework has been developed which consists of four stages (see reference [13.1]). Each stage is divided into a number of steps to be executed by the dependent failure analyst. In this section the procedural framework will be described.

Stage 1: System Logic Model Development

The basic system failure logic is modelled in terms of basic events that represent component status.

Steps:
1.1 System Familiarization
1.2 Problem Definition
1.3 Logic Model Development

Stage 2: Identification of Common Cause Component & Groups

The principal object is to identify, the groups of components that are felt to have significant potential for common cause failures using qualitative and quantitative screening.

Steps:
2.1 Qualitative Analysis
2.2 Quantitative Screening

Stage 3: Common Cause Modelling and Data analysis

Common cause basic events are defined for inclusion in the logic model to represent the residual dependent failures, and probability models are constructed for each new basic event. At this stage, the logic model is extended from a component- state basis to a component-group-impact basis. Historical data on multiple events are analysed and the parameters of the probability models for common cause basic events estimated.

Steps:
3.1 Definition of Common Cause Basic Events
3.2 Selection of Probability Models for Common Cause Basic Events
3.3 Data Classification and Screening
3.4 Parameter Estimation

Stage 4: System Quantification and Interpretation of Results

The results are integrated into the system and sequence analyses and the results are analysed.

Steps:
4.1 Quantification
4.2 Results Evaluation and Sensitivity Analysis
4.3 Reporting

Each of the stages will be described in detail in the following paragraphs.

13.4 STAGE 1: SYSTEM LOGIC MODEL DEVELOPMENT

The objective of this stage is to construct a logic model that identifies the contributions of component states that lead to failure of the system. This stage involves steps that are familiar to systems analysts. The three basic steps of this stage are:

Step 1.1: System Familiarization

Step 1.2: Problem Definition

Step 1.3: Logic Model Development

Although the above steps are the essential elements of any systems analysis, the emphasis of the following discussion will be on those aspects that are more directly relevant to the treatment of common cause events. Consequently, some of the details about those elements of analysis that are routinely considered in system analysis work are not presented. Similarly, the available systems modelling techniques (fault trees) are not discussed.

13.4.1 Step 1.1 - System Familiarization

This is an essential element of any system analysis. To be able to model a system, the analyst must understand what the intended function of the system is, what components it is composed of, and what procedures govern its operation, testing and maintenance. In addition, the analyst needs to know the relation of the system being analysed to other systems, as well as to its physical environment in the broader picture of a plant model.

Particular attention needs to be paid to identifying those elements of design, operation, and maintenance and test procedures that could influence the probability of multiple component failures. The information collected in this step is essential in the identification of potential sources of dependence and grouping of components in the screening phases of the analysis (Steps 2.1 and 2.2).

13.4.2 Step 1.2 - Problem Definition

In this step, the analysis boundary conditions, such as the physical and functional system boundaries of the system, functional dependencies on other systems (support systems), functional interfaces with other systems, and, finally, system success criteria, need to be defined. This determines what equipment should be modelled, how it should operate for the system to perform its intended function (which failure modes to consider), what are the success criteria, and what are the applicable mission time and possible initial system alignments. In this process, potential operator actions, the impact of test and maintenance requirements, and other assumptions and ground rules imposed on the analysis in the context of the overall plant model should be identified.

From the point of view of dependent failures, those root causes of dependency that are to be explicitly modelled are identified, for instance support system dependencies or functional dependencies. Similarly, certain categories of human errors, such as calibration errors and errors in returning equipment and system to their original configuration after testing and maintenance, are typically modelled by explicitly using human reliability analysis techniques. In table 13.1 a checklist of potential root causes is listed.

The following step is to define the scope of the residual common cause failure analysis. The residual common causes are those root causes of multiple failures that are not modelled explicitly, but could contribute to system unavailability. This process then defines the scope of the residual common cause failure analysis. It cannot be emphasized enough that extra care is needed in the application of parametric common cause models to avoid double counting of causes explicitly modelled. It is these residual common cause events that are treated using the parametric common cause models discussed later.

Table 13.1: Checklist of common cause categories.

Normal environment:
- Dust
- Humidity
- Temperature
- Vibrations

Internally generated abnormal environmental conditions:
- Temperature
- Pressure
- Radiation
- Chemical corrosion
- Pipe whip
- Missiles
- Jet impingement
- Internal flooding
- Explosions
- Fires

Externally generated abnormal environmental conditions:
- Aircraft crash
- Explosions in vicinity of site
- Fire in vicinity of site

Extreme natural environment:
- Extreme weather conditions
- Floods
- Earthquakes

Effects of design errors:
- System or component unfit for mission
- Systems with potential CCF
- Systems difficult to maintain

Effects of manufacturing errors

Effects of assembly errors

Effects of human errors:
- During operation
- During testing and maintenance

13.4.3 Step 1.3 - Logic Model Development

The first step in any system analysis is the development of a logic model that relates a system state, such as 'system unavailable', to lower-component-level states. By convention, the lowest level of input to the logic model represents single-component-unavailable events. This will be called a component-level logic model and can be used to generate minimal cut sets. It is when this logic model is used to construct a probability model that the question of independence of events arises. The remaining stages are concerned with the assessment of the significance of this dependence on the evaluation of probabilistic measures of system performance, such as reliability or unavailability.

The key step in any systems analysis is the development of a logic model that relates a system state, such as 'system unavailable', to a combination of more elementary events, such as component states. There are a number of techniques for logical representation of a system. The most commonly used logic model is the fault tree.

13.5 STAGE 2: IDENTIFICATION OF COMMON-CAUSE COMPONENT GROUPS

The principal object is to identify, using qualitative and quantitative screening, the groups of components that are feit to have significant potential for common-cause failures.

Step 2.1 : Qualitative Analysis

Step 2.2: Quantitative Screening

The objectives of this screening stage include:

- Identifying the groups of system components to be included in or eliminated from the CCF analysis.
- Prioritizing the groups of system components identified for further analysis so that time and resources can be best allocated during the CCF analysis.
- Providing engineering arguments to aid in the data analysis step (Step 3.3).
- Providing engineering insights for later formulation of defence alternatives and stipulation of recommendations in Stage 4 (Quantification and Interpretation of Results) of the CCF analysis.

These objectives are accomplished through the qualitative analysis and quantitative screening steps. These two steps are presented separately, but they can be performed interactively.

Much of the information collected in Step 1.1 and the analysis boundary conditions defined in Step 1.2 are directly relevant to the process of identifying common-cause component groups, which involves an engineering evaluation of failure causes, coupling mechanisms and existing defences against common-cause failure in the system being analysed.

The end result of the screening is a list of CCF groups of which the analyst feels confident, in light of the wide range of postulated causes of CCF events and the carefully selected screening arguments, that they adequately bound the common-cause event possibilities that will be subjected to further study.

13.5.1 **Step 2.1 - Qualitative Analysis**

In this step, a search is made for common attributes of components and mechanisms of failure that can lead to common-cause events. Past experience and understanding of the engineering environment are used to identify signs of potential dependence among redundant components. Also, experience is used to identify the effectiveness of defences that may exist to preclude or reduce the probability of the occurrence of certain CCF events. This search identifies initial groups of system components to be included in the analysis.

An important part of this step is to identify the groups of system components to be included in the common-cause failure analysis. A common-cause failure group is a set of identical or similar components that have a significant likelihood of experiencing a common-cause event. It is then assumed that common-cause events are confined within these predefined groups. Since many combinations of components can be postulated, it is desirable to focus upon those common-cause failure groups that have a significant likelihood of dependence that contributes to overall system unreliability or unavailability.

The first step in defining common-cause failure groups is to identify groups of components that have similar attributes. In appendix 13-A, table 13-A-4, an extensive list is provided to identify the most common attributes for consideration:

Table 13-A-4 in appendix 13-A is simply a tooi to help account for factors affecting component interdependence and to readily identify the presence of identical redundant components. It provides a method of documenting the qualitative analysis required to support the selection of common-cause groups.

Much work is needed to determine the relation between various root causes, coupling mechanisms and defensive tactics, while valuable insight can be gained by considering, in a qualitative fashion, the effectiveness of some broad categories of defences for various general groups of causes. Such an analysis can be useful in the evaluation of common-cause event data for plant-specific applications. As an example, physical separation of redundant equipment may reduce the chance of simultaneous failure of the equipment due to some environmental effects. In this case, the defence operates to weaken the coupling mechanism. Other tactics may be effective in reducing the likelihood of root causes resulting in independent failures as well as common-cause failures.

Guidelines:
Based on nuclear experience in performing these evaluations and in analysing operating nuclear experience data, additional guidance can be provided in the assignment of component groups.

The most important guidelines are the following:

- To identify important root causes, the following types of root causes and component group combinations are to be considered:
    - root causes that affect similar kinds of equipment.
    - same installation procedures
    - same maintenance procedures
    - operating or testing procedures
    - common design and manufacturing processes.
    - root causes that affect any equipment in the same location.
    - Harsh environments caused by energetic events (fires, floods, earthquakes, explosions, missiles, etc.)
    - Harsh environments caused by nonenergetic events or extremes of normal environmental conditions (contamination, vibration, moisture, corrosion, high temperature, etc.)

- When identical, functionally non-diverse, and active components are used to provide redundancy, these components should always be assigned to a common-cause group, one group for each group of identical redundant components.

- When diverse redundant components have piece parts that are identically redundant, the components should not be assumed to be fully independent. One approach in this case is to break down the component boundaries and identify the common piece parts as a common-cause component group. For example, pumps can be identical except for their drivers.

- In systems reliability analysis, it is frequently assumed that certain passive components can be omitted, based on arguments that active components dominate. In applying this principle to common cause analysis, care must be taken not to exclude such important events as debris blockage of redundant pump strainers, etc.

- Some potential common-cause groups can be eliminated based on operating experience data. For example, there is no data to support the concept of intersystem common-cause failure events, so that it is generally not necessary to define common-cause groups that mix equipment from various systems. However, a plant-specific analysis should be performed to identify any special intersystem dependency.

Susceptibility of a group of components to common-cause failures not only depends on their degree of similarity, but also on the existence or lack of defensive measures against common causes and the degree of their effectiveness. It is clear that engineering judgement is needed to define common-cause failure groups. Based on nuclear experience the component types listed in table 13.2 should be considered in a dependent failure analysis.

Table 13.2: Component types to be considered in a CCF analysis (based on nuclear experience).

- Pumps - Diesel generators - Gas turbines - Compressors	- Logic channels - Sensors - Strainers (blockage)
- Motor-operated valves - Air-operated valves - Hydraulically operated valves - Check valves - Pressure relief valves	- Transmission lines - Breakers - Busbars - Batteries

Qualitative screening criteria:
The following is a description of some additional criteria that can be used to identify common-cause scenarios involving errors in the installation, maintenance, testing or operation of components and scenarios involving harsh environments.

- Except in scenario's involving harsh environment, the assumption of independence among diverse components is a good one and is supported by operating experience data.

- In the screening of installation, maintenance, testing, and operating error scenarios, determine if there are any plausible errors either in performing the task or in the procedures defining the task that could result in component unavailability. If there are none, the scenario may be discarded. For example, if a procedure does not call for removing a component from service, there is little chance that the component will be left in a disabled state at the end of the task.

- In general, it is only necessary to consider minimal cut sets whose basic events are all affected by the same procedure within one testing interval. Common-cause scenarios associated with plant testing and maintenance schedules should be examined to determine whether the scenario is credible. For example, consider a minimal cut set involving three pumps. A common preventive maintenance task is to be performed at one month intervals on each of the three pumps.The plant maintenance schedule calls for this maintenance to be staggered among the three pumps; for instance, pump 2 is to be serviced one month after pump 1, and pump 3 is to be serviced two months after pump 1. A functional test of the pumps is also to be performed monthly, and it too is to be staggered. Each pump is to be tested one month after its preventive maintenance.Therefore, an error that occurs during the maintenance of pump 1 will probably be discovered and corrected before the same error can cause pump 3 to fail and, possibly, even pump 2. Thus, the minimal cut set will probably never occur due to errors in this maintenance task and the scenario may be eliminated from the analysis.

- Situations in which different personnel perform a task on multiple components in a minimal cut set may be screened out. The systematic repetition of task-related errors is highly dependent on the interpretation of the working procedure and on the effects of stress, fatigue, and personnel abilities. These factors can vary considerably among individuals.

- Another observation from history is that spurious failure modes do not experience common cause failures, e.g., there is no recorded instance where multiple motor-operated valves have transferred closed (i.e. failed to remain open) due to common cause.

- A plant visit can be performed for making a detailed survey to determine the spatial relationships of components, sources of harsh environments, barriers to harsh environments of interest and any other pertinent factors. The plant visit may determine that some scenarios are incredible in light of these details. For example, an analyst may discover several penetrations with unsealed conduits connecting equipment in different locations. Moisture in one location (e.g. at an upper floor) could propagate through the conduits and cause the components connected to these conduits in the other locations (e.g., at a lower floor) to fail. Since operating experience indicates several component failures due to moisture propagating through conduits, moisture could cause a dependent failure of components in these locations. A detailed analysis of the locations, however, may reveal that the unsealed conduits do not connect equipment in the same minimal cut set to a common source of moisture. Thus, the scenario can be screened out.

13.5.2 **Step 2.2 - Quantitative Screening**

After the qualitative screening of Step 2.1 has been completed, the analyst has identified groups of components that, by virtue of similarity, environment, etc., have been judged to be susceptible to common-cause failures. One can further reduce the list of important common- cause candidate groups by performing quantitative screening. In this quantitative screening process, a conservative value is assigned to the probability of each dependent failure event. System unavailability is evaluated using conservative values, and the dominant contributors to system unavailability are identified. These dominant contributors will be emphasized in Stages 3 and 4.

In performing quantitative screening for common cause failure candidates, one is actually performing a complete quantitative common-cause analysis, except for the fact that a conservative and very simple quantification model is used. The procedure is as follows:

Task 1:
In this task the fault trees are modified to explicitly include a single common-cause failure event for each component in a common-cause group that causes all members of the group to fail. Implementation in the fault tree can be achieved by adding an OR gate for each basic event in the common-cause group.

Task 2:
The modified fault trees are solved, by using a fault tree reduction code to obtain the minimal cut sets for the system. The significance of this process is that, in large systems or accident sequences, some truncation of cut sets on failure probability
must usually be performed to obtain any solution at all, and the product of independent failures is often lost in the truncation process due to its small value, while the (numerically larger) common-cause term will survive.

Task 3:
Numerical values for the CCF basic events can be estimated using the simple beta factor model (see section 13.623, formula 13.3). The beta factor model provides a conservative approximation of the common-cause event frequency regardless of the number of redundant components in the common-cause basic event being considered. For screening purposes, the analyst may use $\beta = 0.1$.

Task 4:
In task four the modified fault tree is quantified. From the quantitative result it will be clear if a common-cause failure can be neglected or not. For those common-cause failures which cannot be neglected, a more detailed common-cause failure analysis is required.

13.6 STAGE 3: COMMON-CAUSE MODELLING AND DATA ANALYSIS

At the completion of Stage 2, the analyst has developed a component level logic model of the system and has defined the scope of the common cause analysis in terms of component groups. The purpose of this third stage is to modify the logic model to incorporate common cause events, and to analyse the data for quantifying the parameters of this model.

Common-cause basic events are defined for inclusion in the logic model to represent the residual common-cause failures, and probability models are constructed for each new basic event. At this stage, the logic model is extended from a component-state basis to a component-group impact basis. Historical data on multiple events are analysed and the parameters of the probability models for common-cause basic events estimated.

Step 3.1: Definition of Common Cause Basic Events

Step 3.2: Selection of Probability Models for Common-Cause Basic Events

Step 3.3: Data Classification and Screening

Step 3.4: Parameter Estimation

13.6.1 Step 3.1 - Definition of Common-Cause Basic Events

To model common-cause failures, it is convenient to define common-cause basic events; that is, basic events that represent multiple failures of components from shared root causes. This step also leads to a redefinition of the single-component basic events. Definition of new basic events leads to a redefinition of the structure of the logic model to include the new events.

This step will be explained an example. The example concerns the steam supply of a chemical reactor, see figure 13.1. The chemical reactor is heated by two coils. When the temperature is high the steam supply to both coils has to be shut off. To achieve a high level of safety, two shut-off valves are mounted in each coil. In case of a high temperature one valve in each line must close whereas all four valves should close given the design. All four valves are identical and are maintained and tested according to the same procedures. For this reason dependent failures have to be considered.

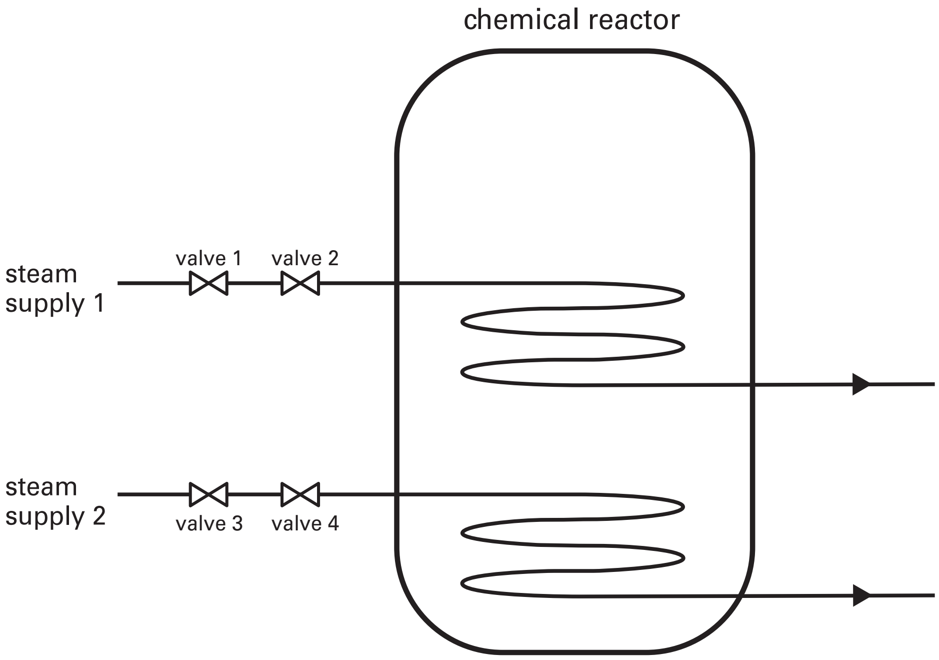


Figure 13.1: Four-valve example system

Shut-off of the steam supply to the reactor fails if the two valves in one of the two steam supply lines fail to close. If only independent failures are considered, two second order minimal cut sets describe this failure event:

IFvalve1.IFvalve2
IFvalve3.IFvalve4

The four identical valves have to be identified as one common-cause group. The following common-cause events can be defined:

Affecting two components:
- Common cause of valves 1 and 2 (CCF12)
- Common cause of valves 1 and 3 (CCF13)
- Common cause of valves 1 and 4 (CCF14)
- Common cause of valves 2 and 3 (CCF23)
- Common cause of valves 2 and 4 (CCF24)
- Common cause of valves 3 and 4 (CCF34)

Affecting three components:
- Common cause of valves 1, 2 and 3 (CM 23)
- Common cause of valves 1, 2 and 4 (CM 24)
- Common cause of valves 1, 3 and 4 (CCF134)
- Common cause of valves 2, 3 and 4 (CCF234)

Affecting four components:
- Common cause of valves 1, 2, 3 and 4 (CCF1234)

The next step is to redefine the basic events in order to incorporate component failure due to common cause. This is done by expanding the independent basic events by a number of basic events which represent the common-cause basic events. Care has to be taken that all possible combinations of common-cause failures are incorporated. The branch of the fault tree that represents failure of valve 1 is depicted in figure 13.2.

Basic event valve 1: IFvalve1 + CCF12 + CCF13 + CCF14 +
CCF123 + CCF124 + CCF134 + CCF1234

Basic event valve 2: IFvalve2 + CCF12 + CCF23 + CCF24 +
CCF123 + CCF124 + CCF234 + CCF1234

Basic event valve 3: IFvalve3 + CCF13 + CCF23 + CCF34 +
CCF123 + CCF134 + CCF234 + CCF1234

Basic event valve 4: IFvalve4 + CCF14 + CCF24 + CCF34 +
CCF124 + CCF134 + CCF234 + CCF1234

Replacing the basic events in the fault tree by the newly defined basic events and solving the fault tree results in the following minimal cut sets (see appendix 13-C):

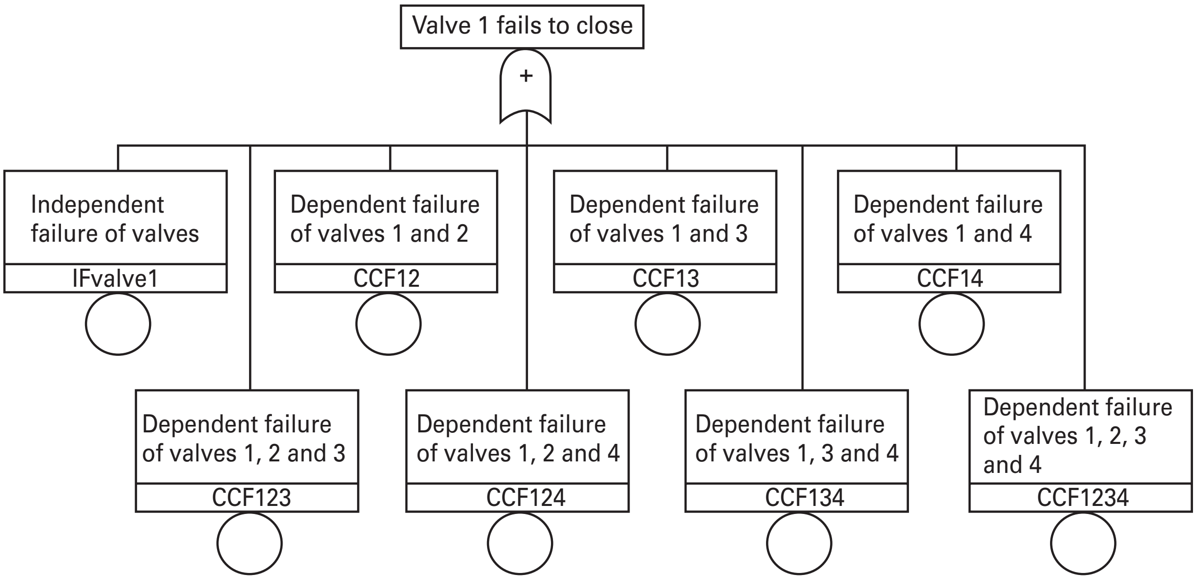

Valve 1 fails to close
+
Independent failure of valves
IFvalve1
Dependent failure of valves 1 and 2
CCF12
Dependent failure of valves 1 and 3
CCF13
Dependent failure of valves 1 and 4
CCF14
Dependent failure of valves 1, 2 and 3
CCF123
Dependent failure of valves 1, 2 and 4
CCF124
Dependent failure of valves 1, 3 and 4
CCF134
Dependent failure of valves 1, 2, 3 and 4
CCF1234

Figure 13.2: Fault tree branch representing failure of valve1.

First-order cut sets:

CCF12
CCF123
CCF1234
CCF124
CCF134
CCF234
CCF34

Second-order cut sets:

CCF13.CCF14
CCF13.CCF23
CCF13.CCF24
CCF14.CCF23
CCF14.CCF24
CCF24.CCF23
IFvalve1.IFvalve2
IFvalve4.IFvalve3
IFvalve1.CCF23
IFvalve1.CCF24
IFvalve2.CCF13
IFvalve2.CCF14
IFvalve3.CCF14
IFvalve3.CCF24
IFvalve4.CCF13
IFvalve4.CCF23

A remark has to be made about the cut sets of the type CCFxy.CCFxz. The most convenient approach to handle these type of cut sets is to define the common-cause events related to a particular basic event as mutually exclusive. Such a definition implies that the cut sets of the type CCFxy.CCFxz are identically zero (see reference [13.2]). In practice cut sets like CCFxy.CCFxz require little attention because the contribution of these cut sets is considerably smaller than the contribution of cut sets like CCFxyz.

13.6.2 Step 3.2 - Selection of Probability Models for Common Cause Basic Events

The objective of this step is to provide a transition from the logic model in Step 3.1 to a model that can be quantified.This is done by associating a probability model, such as the constant failure rate model or the constant probability of failure with demand model, with each basic event (dependent and independent failures). Each model has one or more parameters and estimators for these parameters that, in terms of measurements of numbers of failure events and number of components failed, are based on specific assumptions.

Symmetry assumption:
The symmetry assumption postulates that the common-cause failure probability of any k components in a group size of m, only depends on the number k, and not on which k components are the failed ones. In other words, the common-cause failure probability of k components, within a certain group of m similar components, is the same, regardless of which k components have failed.

For example, consider the four-valve example system the group of 4 similar components valvel, valve2, valve3 and valve4. The symmetry assumption implies that the common-cause failure probability of components valvel and valve2 (CCF12) is equal to the common-cause failure probability of components:

- Valve1 and valve3:	CCF13
- Valve1 and valve4:	CCF14
- Valve2 and valve3:	CCF23
- Valve2 and valve4:	CCF24
- Valve3 and valve4:	CCF34.

In other words:

CCF 12 = CCF 13 = CCF 14 = CCF23 = CCF24 = CCF34

The value of the common-cause failure of two components is only a function of the number k = 2, within the same group.

Parametric models

Parametric modelling is the most widely used method for implicit modelling. There are several of these models, and they are categorized based on the number of parameters, their assumption regarding the cause, coupling mechanism, and impact of common-cause failures. The most popular methods are: basic parameter model, beta factor model, multiple Greek letter model, alpha factor model and binomial failure rate model. All these models are described in detail in reference [13.1], only the basic parameter, the beta, the alpha factor and the binomial failure rate model will be described in this paragraph.

The Basic Parameter Model is explained because this models forms the basis for all other parametric models. The Beta model is the most widely used model and for this reason the Beta model cannot be neglected. Given the dependent failure data normally available, the Alpha model is developed. Application of the Alpha model requires recording of multiple failures. In practice this data is only available in the nuclear industry. To overcome the lack of dependent failure data the Binomial Failure Rate model can be used, which requires only three parameters. These three parameters are usually based on nuclear experience.

Basic parameter model

The most general of the commonly used parametric models is the Basic Parameter Model. In this model, a set of parameters Q_k ($1 \leq k \leq m$) is defined as follows:

Q_k = probability of a basic event involving k specific components, where $1 \leq k \leq m$.

The factor m represents the number of components in the common cause component group. The model is based on the symmetry assumption. Depending on the system modelling requirements, Q_k can be defined as a probability of failure per demand or as a failure rate.

The total probability of failure Q_t of a specific component can be defined in terms of the basic specific parameters (Q_k's) as follows:

$$Q = \sum_{k=1}^{m} \frac{(m - 1)!}{(m-k)!\,(k-1)!} Q_k \qquad (13.1)$$

The binomial term in formula (13.1) represents the number of different ways in which a specific component can fail with (k-1) other components in a group of m similar components.

Application of formula (13.1) to component groups of m = 2, 3 and 4 results in:

$$m = 2: Q_t = Q_1 + Q_2$$

$$m = 3: Q_t = Q_1 + 2Q_2 + Q_3 \qquad (13.2)$$

$$m = 4: Q_t = Q_1 + 3Q_2 + 3Q_3 + Q_4$$

The model that uses Q_k's as defined above to calculate system failure probabilities is called the basic parameter model. Unfortunately, the data required to estimate the Q_k's directly is generally unavailable. It is for this reason that other models have been developed, which require additional assumptions, but in return they simplify the parameter estimation from historical data.

Beta factor model

The most widely used single parameter model is known as the beta factor model. According to this model a fraction (β) of the component failure rate can be associated with common-cause events shared by the other component in that group. Whenever a common-cause event occurs, all components within the common-cause component group are assumed to fail. Therefore, based on this model, for a group of m components all Q_k's are zero except Q_1 and Q_m. The expressions to calculate the Q_k's are written as:

$$Q_1 = (1 - \beta)\, Q_t$$

$$Q_k = 0 \quad (k > 1, k < m) \qquad (13.3)$$

$$Q_m = \beta\, Q_t$$

This implies that the beta factor is defined as:

$$\beta = \frac{Q_m}{Q_1 + Q_m} \qquad (13.4)$$

m = The number of components in the common-cause component group.

Q_t = Total failure frequency of each component due to all independent and common-cause events.

Q_k = Probability of a basic event involving k specific components $1 \leq k \leq m$.

Alpha factor model

The alpha factor model defines common-cause failure probabilities from a set of failure frequency ratios and the total component failure probability Q_t. The alpha parameters are defined as follows:

α_k = Fraction of the total frequency of failure events occurring in the system and involving the failure of k out of m components due to common cause.

$$\sum_{k=1}^{m} \alpha_k = 1 \qquad (13.5)$$

An important advantage of the alpha factor model is that the alpha factor parameters are directly related to the observable number of events in failure records.

The formulas to calculate the Q_k's of the alpha factor model are:

$$\alpha_t = \sum_{k=1}^{m} k\ \alpha_k$$

Non-staggered testing:

$$Q_k = m \frac{\alpha_k}{\binom{m}{k}\alpha_t} Q_t \qquad (13.6)$$

Staggered testing:

$$Q_k = \frac{m}{k} \frac{\alpha_k}{\binom{m}{k}\alpha_t} Q_t$$

m = Number of components in the component group.

Q_t = Total failure frequency of each component due to all independent and common cause events.

Q_k = Probability of a basic event involving k specific components $1 \leq k \leq m$.

It is noticed that in order to calculate Q_k, not only α_k is needed, but all alphas, from k = 1 to m, in accordance with the definition of α_t.

The formula presented for staggered testing is only valid in case all components of the common-cause group are tested after detection of a failure in one of the components of the common-cause group. For the sake of convenience, the formulas for the Q_k's in case of non-staggered testing are presented in appendix 13-B.

Binomial failure rate model

The binomial failure rate model considers two types of failures. The first represents independent component failures and the second type is caused by shocks that can result in failure of any number of components in the system. According to this model there are two types of shocks: lethal and non-lethal. When a non-lethal shock occurs, each component within the common cause component group is assumed to have a constant and independent probability of failure. To describe the failure of components due to a non-lethal shock, the binomial distribution is used. When a lethal shock occurs, all components are assumed to fail with a conditional probability of unity. Application of the binomial failure rate model with lethal shocks requires the use of the following set of parameters:

Q_t = independent failure frequency for each component.

μ = frequency of occurrence of non-lethal shocks.

p = conditional probability of failure of each component, given a non-lethal shock.

ω = frequency of occurrence of lethal shocks.

m = number of components in common-cause group.

The frequency of basic events involving k specific components is given as:

$$
\begin{aligned}
Q_1 &= Q_l + \mu p\ (1 - p)^{m-1} && k = 1 \\
Q_k &= \mu (p)^k\ (1 - p)^{m-k} && 2 \leq k < m \\
Q_m &= \mu p^m + \omega && k = m
\end{aligned}
\tag{13.7}
$$

Independent of the number of components in a common-cause component group, the total failure frequency of each component due to all independent and common-cause events is given by:

$$Q_t = Q_l + \mu p + \omega \tag{13.8}$$

For a number of components values for p, μ and ω can be found in reference [13.5].

13.6.3 Step 3.3 - Data Classification and Screening

This step will be executed only in a plant specific common cause analysis. The purpose of this step is to evaluate and classify event reports to provide input for parameter estimation. It is necessary to take care to distinguish between events whose causes are explicitly modelled and those that are to be included in the residual common cause event models. The sources of data available to an analyst are event reports on both single and multiple equipment failures. Since plant-specific data on multiple equipment failures are rare, it is necessary to extend the search to other plants. However, since other plants may be designed or operated differently, events that occurred at one plant may not be possible at another. Thus, the data should not be used blindly, but should be carefully reviewed for applicability. This review concentrates on root causes, coupling mechanisms, and defensive strategies in place at the plant of interest. Since the event reports are generally not as detailed as an analyst would like, analysis of these reports requires a great deal of judgement, while a systematic approach to this screening is essential for scrutability and reproducibility of the analysis. One such approach is the impact vector method which is described in reference [13.1].

13.6.4 Step 3.4 - Parameter Estimation

The objective of this task is to provide data estimates for the parameters of the model selected to quantify the common-cause basic events. A distinction has to be made between the application of generically derived values for the various parameters and a plant specific analysis of the relevant parameters.

Generically derived values:
If classified event reports are not available or if the event screening process is not within the scope of the project, one has to use 'generic beta factors'. These generic beta factors are mainly based on nuclear experience and have been derived for a number of components (see table 13.3). It is the responsibility of the analyst to defend any conclusion derived from generic beta factors. The generic beta factors include both failures to start on demand and failure to run for all components except breakers and valves. Hence, they represent an average of these modes weighed by their relative frequency of occurrence.

Table 13.3: Generic beta factors (based on nuclear experience).

Component	Generic beta factor
Diesel generators	.05
Motor-operated valves	.08
Check valves	.06
Service water pumps	.03
Auxiliary feedwater pumps	.03
Containment spry pumps	.05
Residual heat removal pumps	.11
Safety injection pumps	.17
Safety/Relief valves PWR	.07
Safety/Relief valves BWR	.22
Chillers	.11
Fans	.13
Reactor trip breakers	.19
Remaining components	.10

Plant-specific analysis
The purpose of this step is to use the information obtained in Step 3.3 concerning the number of applicable events of single and multiple failures and the number of failed components to estimate the parameters of the common-cause probability models. There are several sources of uncertainty, including the interpretation of the data to elicit causal mechanisms, the assessment of their impact at the plant being modelled, and uncertainty about how the data was obtained. Consequently, it is essential not only to provide a point estimate but also to characterize this uncertainty numerically.

Beta factor model

The beta factor model was originally developed for a system of two redundant components and the estimators that are often presented in the literature also assume that the data are collected from two unit systems. However, in reference [13.2] a generalized beta factor estimator is provided for a system of m redundant components. This generalized beta factor is defined as follows:

$$\beta \;=\; \frac{\sum_{k=2}^{m} k \,.\, n_k}{\sum_{k=1}^{m} k \,.\, n_k} \tag{13.9}$$

m = the number of components in the common-cause group

n_k = the number of historical events involving k components in a failed state.

For a two-unit system (m= 2), the estimator of the beta factor reduces to the familiar estimator mostly presented in the literature:

$$\beta \;=\; \frac{2\ n_2}{n_1 = 2\ n_2} \tag{13.10}$$

Alpha factor model:

An estimator for each of the alpha factor parameters (α_k) can be based on its definition as the fraction of total failure events that involve k component failures due to common cause:

$$\alpha_k = \frac{n_k}{\sum_{k=1}^{m} n_k} \tag{13.11}$$

where:

m = the number of components in the common cause group

n_k = the number of historical events involving k components in a failed state.

At this point, the advantage of the alpha factor method is readily noticed: there is no need to estimate the number of demands. All the parameters are obtained by dividing the number of events involving k failures by the total number of events from any data source. It is also possible to use probabilities from one source of data, and independently a total failure rate from another source. For example, plant specific data may be used to estimate a total failure probability Q_t and a more general source involving several plants to estimate the alpha factors.

The number of demands on the system is not directly required. However, it should be noted that the assumptions underlying the estimation of the number of demands are embedded in the formulation of the alpha factor method (see appendix 2 of reference [13.2]). One of these assumptions is that in each test or actual demand, the entire common cause component group is challenged, which is equivalent to a non-staggered testing scheme.

13.7 STAGE 4: SYSTEM QUANTIFICATION AND INTERPRETATION OF RESULTS

The results are integrated into the system and sequence analyses and the results are analysed.

Step 4.1: Quantification

Step 4.2: Evaluation of Results and Sensitivity Analysis

Step 4.3: Reporting

The purpose of this stage is to use the output of the previous stages to perform a quantification, the performance of a sensitivity analyses, and the interpretation of results.

13.7.1 Step 4.1: Quantification

The event probabilities obtained for the common cause events as a result of Stage 3 of the analysis are incorporated into the solution for the unavailability of the systems or into event-sequence frequencies in the usual way of cut sets quantification. The results of this step include the numerical results and the identification of key contributors.

13.7.2 Step 4.2: Evaluation of Results and sensitivity and uncertainty analysis

The final step in system analysis prior to documentation is the interpretation of the quantification results. In addition to the overall top event frequency or unavailability and its uncertainty estimate, the results should also summarize the relative contributions of independent hardware failures, failures involving tests or maintenance, and common cause failures.

It will be clear that there is considerable uncertainty in the estimation of common-cause failure probabilities. Although an uncertainty analysis can express the significance of this in an integral sense, it is also useful to see how significant such uncertainties can be by using sensitivity analyses to illustrate the direct relationship between input values for the common-cause basic events and the top overall system results.

Uncertainty analysis:
In order to analyse the errors in the common-cause factor estimates, it is necessary to begin with the identification of the different sources of uncertainty:

- Classification of data due to ambiguity in the event reports and in the event interpretation for plant-specific use.

- Possible deficiencies in the source database, e.g. under-reporting of independent events.

- Uncertainty about sizes of systems in the database.

- Statistical uncertainty due to limited size of the data sample.

A detailed uncertainty analysis of the common cause factors requires a lot of effort. In this case only a coarse uncertainty estimation will be presented.

It is noted that each final common-cause failure rate is given by the product of a common cause factor times the total failure rate. If it is assumed that the common cause factor and the total failure rate are both lognormally distributed, then it can be shown that the product is also a lognormal distribution. The mean value and the error factor can be calculated with the following formulas:

$$\text{Mean} \quad = \quad \text{Mean1 Mean2}$$

$$\text{EF} \quad = \quad \exp[1.645 \sqrt{(\frac{\text{lnEF1}}{1.645})^2 \; + (\frac{\text{lnEF2}}{1.645})^2]} \qquad (13.12)$$

EF1 and EF2 are the error factors of the common-cause factor and the total failure rate, respectively.

13.7.3 Step 4.3: Reporting

The final step is the reporting of the analysis. It is particularly important to be clear in specifying what assumptions have been used and to identify the consequences of using these assumptions. In particular, the argumentation of why some potential common-cause failures are screened out should be well documented.

13.8 EXAMPLE

This example considers the design of a continuously stirred tank reactor (CSTR) that uses a highly exothermic reaction to produce a chemical compound. To identify potential Hazards, a HAZOP analysis shows that a runaway exothermic reaction is possible in the CSTR. The protection against this undesirable event is provided by two CSTR dump valves (V1 and V2) that should open and quench the reaction mixture in a water filled sump (see figure 13.3). The dump valves will be opened if the temperature inside the CSTR rises above a preset limit.

13.8.1 Stage 1: System logic model development:

Step 1.1 - System familiarization

The dump valve actuators are pneumatically operated and are controlled by a voting logic unit (VLU). The VLU commands the valves to open when at least two out of three temperature channels indicate a high/high condition. Each temperature channel has its own temperature sensor (TO). The temperature sensors are all set to trip at the same temperature. For proper functioning of the dump valves the instrument air system is required. The VDU is powered by an electrical supply of 24 Volt DC. Failure of the power supply of the VDU results in a spurious actuation signal to open both dump valves.

Both dump valves are identical, also the three temperature sensors are identical. The dump valves as well as the three temperature sensors are tested by the same maintenance crew during the annual maintenance. Testing of the temperature sensors also includes testing of the voting logic.

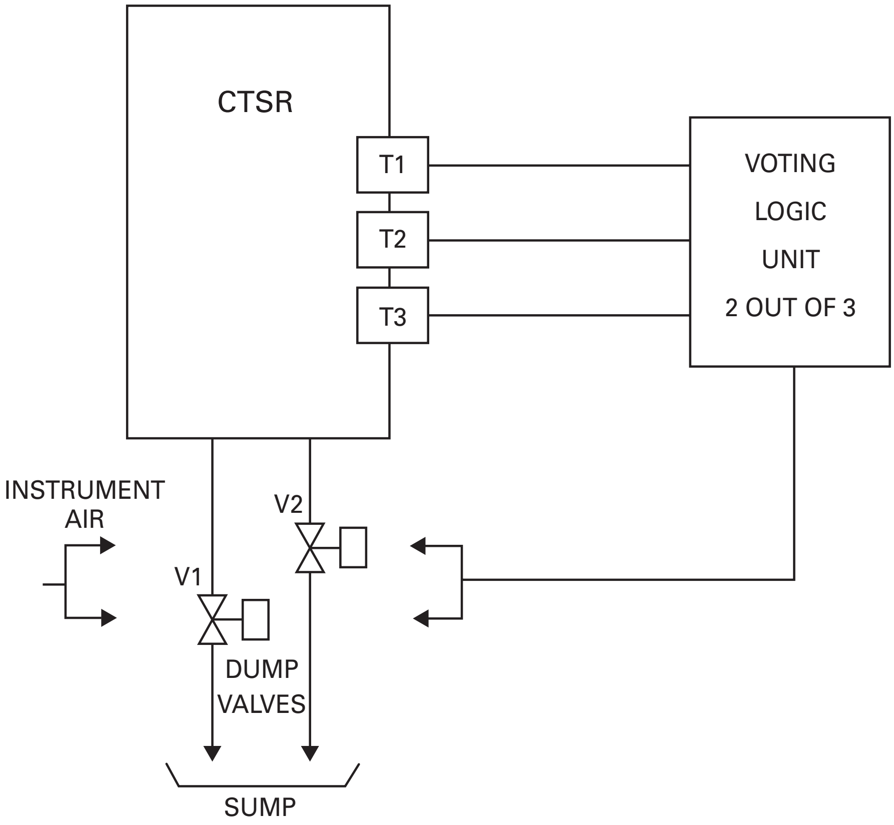


Figure 13.3: Instrument safeguarding CSTR

Step 1.2 - Problem definition
The top event of interest can be defined as follows:

> "CSTR fails to dump following a high-temperature upset"

Successful operation of the instrument safeguarding system requires operation of at least two out of three temperature sensors, the VDU and at least one of the two dump valves.

Step 1.3 - Logic model development
A fault tree has been composed to determine the minimal cut sets. One dependency, viz. the common support system of the dump valves (instrument air) can be modelled directly in the fault tree.

The fault tree structure is given by:

```
Gate                 Type

TOP                  AND GATE1                GATE2
GATE1                OR DVALVE_1              INSTR_AIR            NO_SIGNAL_VLU
GATE2                OR DVALVE_2              INSTR_AIR            NO_SIGNAL_VLU
NO_SIGNAL_VLU        OR VLU_FAILS             NO_SIGNAL_SENS
NO_SIGNAL_SENS       AND NO_SIGNAL_S1_S2      NO_SIGNAL_S1_S3      NO_SIGNAL_S2_S3
NO_SIGNAL_S1_S2      OR TS_1                  TS_2
NO_SIGNAL_S1_S3      OR TS_1                  TS_3
NO_SIGNAL_S2_S3      OR TS_2                  TS—3
```

Solving the fault tree results in the following first and second order cut sets:

```
   VLU_FAILS
   INSTR_AIR

 DVALVE_1   .  DVALVE_2
     TS_2   .  TS_3
     TS_1   .  TS_2
     TS_1   .  TS_3
```

From the cut sets it can be concluded that redundancy is present in relation to the dump valves and the temperature sensors.

13.8.2 Stage 2: Identification of common-cause component groups

Step 2.1 - Qualitative analysis

The purpose of this step is to determine which common-cause events are important for the system and should therefore be included in the subsequent steps of the analysis. At this stage of the analysis, the analyst must decide which groups of components are vulnerable to a common-cause event affecting two or more components within that group.

For the CSTR safeguard system there are two candidate common-cause component groups: the two identical dump valves and the three identical temperature sensors.The composition of the two common-cause groups is as follows:

Group 1: Dump valve group
DVALVE_1
DVALVE_2

Group 2: Temperature sensor group
TS_1
TS_2
TS–3

The objective of the remainder of this section is to identify which candidate common cause component groups should be retained for analysis of the subsequent steps.

The root cause and coupling mechanism analysis is performed by first identifying an initial set of root causes of interest for the equipment in the CSTR safeguard system and by also identifying the group of components affected by each root cause. Then each root cause and component group combination is analysed, based mostly on engineering arguments to assess how they could impact the CSTR safeguard system. Some combinations may be 'not applicable' to the CSTR safeguard system. Other combinations may be easily detectable and easily repairable. In both cases, the combinations are unimportant. Other combinations may be judged applicable to the CSTR safeguard system.

Three types of root cause and component group combinations must be addressed:

type 1: root causes that primarily affect similar equipment.

type 2: root causes that affect equipment operated according to the same procedures.

type 3: root causes that affect equipment in the same location.

The initial root cause analysis of failure for the equipment of interest consists of a detailed review of all failure reports, other system reliability analyses (e.g. FMEA) and previous studies on similar systems. This review must be exhaustive to ensure that all fault categories are adequately considered. The material that follows, however, was developed for illustrative purposes and is not based on a data review. Table 13.4 summarizes the root-cause and component-group combinations defined for the CSTR safeguard system.

Table 13.4: Root cause and component group combinations initially defined for the CSTR safeguard system.

Combination number	Root cause of interest	Affected equipment	Type of root cause
1	Anything but procedure and environmentally related causes	Dump valves	1
2	Anything but procedure and environmentally related causes	Temperature sensors	1
3	Calibration errors	Temperature sensors	2
4	Errors committed during maintenance	Dump valves	2
5	Harsh environment in the vicinity of the CSTR	All field equipment, dump valves and temperature sensors	3

Each root-cause and component group combination summarized in table 13.4 has to be analysed in detail. Engineering arguments must be formulated to justify why a common cause group can be discarded from further analysis. The analyst who is performing this analysis must be familiar with the operating experience of the equipment under consideration. Engineering judgement is mostly required at this stage of the common cause failure analysis.

Combination 1: Anything but procedure and environmentally related causes (dump valves):
A large number of multiple failure events involving air-operated valves have resulted from design deficiencies, manufacturing defects and installation errors. Moreover, review of the failure data records showed that about seventy per cent of all failures of valves used in this type of service involved blockage of flow caused by process material plugging the valve inlet or valve internals. For these two reasons, this root cause and component group is judged to be very important.

Combination 2: Anything but procedure and environmentally related causes (sensors):
The temperature sensors of this type are in service for many years. It is expected that design or manufacturing deficiencies are very unlikely for this type of temperature sensors. For this reason the contribution of this root cause and component group combination to system unavailability is judged to be low. Thus, root-cause and component-group combination 2 is discarded from further analysis.

Combination 3: Calibration errors (sensors):
Operating experience shows that the majority of failures involving temperature sensors are associated with calibration activities. All temperature sensors are calibrated by the same maintenance crew on the same day and in accordance with the same procedures. Therefore, this root cause and component-group combination is judge to be important in this analysis.

Combination 4: Errors committed during maintenance (dump valves):
Maintenance on the dump valves is performed once per year. After maintenance both valves are subjected to a test. For this reason it is expected that this root-cause component-group combination is not an important contributor to the unavailability of the safeguard system. Root-cause and component group number 4 is discarded from further analysis.

Combination 5: Harsh environment in the vicinity of the CSTR:
A plant walk down showed that no harsh environmental conditions can occur close enough to the plant under consideration to disable the instrument safeguarding system. This root cause component group does not need to be analysed further.

Step 2.2 - Quantitative screening
This step is important if the number of potential common cause events is too large to perform a detailed common-cause analysis for every common-cause basic event. If this is the case, prioritization of the common-cause events is necessary. This prioritization is done by performing a quantitative screening analysis. Mostly the beta factor method is used to perform a quantitative screening analysis (see paragraph 5.2.3). The logic of the fault tree is modified to incorporate a common-cause basic event for each identified common-cause group.

Modified fault tree input logic:

```
Gate                 Type

TOP                  OR   GATE0           CCF_DVALVES
GATE0                AND  GATE1           GATE2
GATE1                OR   DVALVE_1        INSTR_AIR          NO_SIGNAL_VLU
GATE2                OR   DVALVE_2        INSTR_AIR          NO_SIGNAL_VLU
NO_SIGNAL_VLU        OR   VLU_FAILS       NO_SIGNAL_SENS     CCF_SENSORS
NO_SIGNAL_SENS       AND  NO_SIGNAL_S1_S2 NO_SIGNAL_S1_S3    NO_SIGNAL_S2_S3
NO_SIGNAL_S1_S2      OR   TS_1            TS_2
NO_SIGNAL_S1_S3      OR   TS_1            TS_3
NO_SIGNAL_S2_S3      OR   TS_2            TS_3
```

In table 13.5 all relevant component failure data, component types and test periods are provided. It should be emphasized that all data provided in this chapter are for illustrative purposes only.

Table 13.5: Component data.

Name	Component code	Component type	Lambda	Test period	Repair duration
Dump valves	DVALVE_1, DVALVE_2	Tested stand by	2.0E-06	8760	
Temp. sensors	TS_1, TS_2, TS_3	Tested stand by	4.0E-06	8760	
Voting Logic	VLU_FAILS	Tested stand by	2.0E-07	8760	
Instrument air	INSTR_AIR	On line repairable	1.01E-05	-	8

For screening purposes the beta factor is taken equal to 0.1. The failure rate of the common-cause basic events can be calculated as follows:

CCF_DVALVES	=	beta * lambda_valves
	=	0.1 * 2.0E-06
	=	2.0E-07

CCF_SENSORS	=	beta lambda_sensors
	=	0.1 * 4.0E-06
	=	4.0E-07

The minimal cut sets can be quantified with the formulas provided in the chapter ”Quantification of minimal cut sets” or with a fault tree computer code.

The calculated results for cut set unavailabilities are:

```
     Cut set                   Contribution    Per cent       Formula

1    CCF_SENSORS                 1.75E-03        35.63          A-1
2    CCF_DVALVES                 8.76E-04        17.83          A-1
3    VLU_FAILS                   8.76E-04        17.83          A-1
4    TS_2 . TS_3                 4.09E-04         8.33          B-1
5    TS_1 . TS—2                 4.09E-04         8.33          B-1
6    TS_1 . TS_3                 4.09E-04         8.33          B-1
7    DVALVE_1 . DVALVE_2         1.02E-04         2.08          B-1
8    INSTR_AIR                   8.00E-05         1.63          B-1
```

Contributions:

First order	:	3.6E-03
Second order	:	1.3E-03
Total unavailability	:	4.9E-03

From the results it can be concluded that both common cause events are important potential contributors to the unavailability of the CSTR safeguard system.

13.8.3 Stage 3: Common-cause modelling and data analysis

Step 3.1 - Definition of common cause basic events

Common cause events need to be defined for two common cause groups, viz. the two air-operated dump valves and the three temperature sensors. The definition of common-cause basic events is done by defining all possible common-cause events as represented by formula (13.1). For the CSTR safeguard system this includes:

DVALVE_1 : IFDVALVE1 or CCF_DVALVES

DVALVE_2 : IFDVALVE2 or CCF_DVALVES

TS1_FAILS : IFTS1 or CCF_TS1TS2 or CCF_TS1TS3 or CCF_TS1TS2TS3

TS2_FAILS : IFTS2 or CCF_TS1TS2 or CCF_TS2TS3 or CCF_TS1TS2TS3

TS3_FAILS : IFTS3 or CCF_TS1TS3 or CCF_TS2TS3 or CCF_TS1TS2TS3

Independent as well as common-cause basic events have been defined. The independent and common-cause basic events are incorporated into the fault tree, based on the methodology of section 5.1. The modified fault tree structure is given by:

Fault tree structure:

```
Gate               Type

TOP                AND   GATE1               GATE2
GATE1              OR    DVALVE1_FAILS       INSTR_AIR           NO_SIGNAL_VLU
GATE2              OR    DVALVE2_FAILS       INSTR_AIR           NO_SIGNAL_VLU
NO_SIGNAL_VLU      OR    VLU_FAILS           NO_SIGNAL_SENS
NO_SIGNAL_SENS     AND   NO_SIGNAL_S1_S2     NO_SIGNAL_S1_S3     NO_SIGNAL_S2_S3
NO_SIGNAL_S1_S2    OR    TS1_FAILS           TS2_FAILS
NO_SIGNAL_S1_S3    OR    TS1_FAILS           TS3_FAILS
NO_SIGNAL_S2_S3    OR    TS2_FAILS           TS3_FAILS
DVALVE1_FAILS      OR    IFDVALVE1           CCF_DVALVES
DVALVE2_FAILS      OR    IFDVALVE2           CCF_DVALVES
TS1_FAILS          OR    IFTS1               CCF_TS1TS2          CCF_TS1TS3
                         CCF_TS1TS2TS3
TS2_FAILS          OR    IFTS2               CCF_TS1TS2          CCF_TS2TS3
                         CCF_TSITS2TS3
TS3_FAILS          OR    IFTS3               CCF_TS1TS3          CCF_TS2TS3
                         CCF_TSITS2TS3
```

By solving the modified fault tree, the following minimal cut sets are generated:

```
     CCFDVALVES
     CCFTS1TS2TS3
     VLU_FAILS
     CCFTSITS2
     CCFTSITS3
     CCFTS2TS3
     INSTR_AIR

    IFTS2  .  IFTS3
    IFTS1  .  IFTS2
    IFTS1  .  IFTS3
IFDVALVE1  .  IFDVALVE2
```

Step 3.2 - Selection of probability models for common cause basic events

The easiest model to apply is the beta factor model, because only one parameter needs to be determined. For illustrative purposes, not the beta factor but the more complicated alpha model is selected for this example.

Step 3.3 - Data classification and screening

To calculate the various alpha factors, the numbers of single, double and triple failure events have to be known for the dump valves and the temperature sensors. To determine the number of failures, the analyst should review previous occurrences of failures and postulate how they could have occurred in the system of interest. This review involves identifying events whose causes are explicitly modeled in the fault tree. For example, a failure report may describe a loss of two valves because of loss of instrument air, but this event is already modeled in the fault tree and should not be considered in evaluating common-cause failures of the valves. Another aspect that should be investigated is whether there are conditions that would make the failures that occurred at other plants more or less likely to occur at the plant being studied. If this is the case, the generic data must be adjusted to accommodate those differences. After a careful review of the maintenance records of similar plants, the following single, double and triple failure events could be identified:

Dump valves:

Number of single failure events	:	300
Number of double failure events	:	21

Temperature sensors:

Number of single failure events	:	200
Number of double failure events	:	8
Number of triple failure events	:	4

Step 3.4 - Parameter estimation

To calculate the various alphas formula (13.11) has to be applied:

Dump valves:

$$\alpha_1 = \frac{n_1}{n_1 + n_2}$$

$$= \frac{300}{300 + 21} \qquad (13.13)$$

$$= 0.935$$

$$\alpha_2 = \frac{n_1}{n_1 + n_2}$$

$$\frac{21}{300 + 21} \qquad (13.14)$$

$$= 0.065$$

$$\alpha_t = \alpha_1 + 2\alpha_2$$

$$= 1.065 \qquad (13.15)$$

For illustrative purposes the beta factor will be calculated with formula (13.10):

$$\beta = \frac{2\ n_2}{n_1 + 2\ n_2}$$

$$= \frac{2\ 21}{300 + 2\ 21} \tag{13.16}$$

$$= 0.123$$

Temperature sensors:

$$\alpha_1 = \frac{n_1}{n_1 + n_2 + n_3}$$

$$= \frac{200}{200 + 8 + 4} \tag{13.17}$$

$$= 0.943$$

$$\alpha_2 = \frac{n_2}{n_1 + n_2 + n_3}$$

$$= \frac{8}{200 + 8 + 4} \tag{13.18}$$

$$= 0.038$$

$$\alpha_3 = \frac{n_3}{n_1 + n_2 + n_3}$$

$$= \frac{4}{200 + 8 + 4} \tag{13.19}$$

$$= 0.019$$

$$= \alpha_t\ \ \alpha_1 + 2\alpha_2 + 3\alpha_3$$

$$= 1.075 \tag{13.20}$$

For illustrative purposes the beta factor will be calculated with formula (13.9):

$$\begin{aligned}\beta &= \frac{2\ n_2 + 3\ n_3}{n_1 + 2n_2 + 3n_3} \\ &= \frac{2 * 8 + 3 * 4}{200 + 2 * 8 + 3 * 4} \qquad (13.21) \\ &= 0.123\end{aligned}$$

13.8.4 Stage 4: System quantification and interpretation

Step 4.1 - Quantification

The quantification of the common cause basic events is done by application of formula (13.6): Dump valves:

$$\begin{aligned}Q_1 &= \frac{\alpha_1}{\alpha_t}\ Q_t \qquad (13.22) \\ &= \frac{0.935}{1.065} * 2\ 0E\text{-}06 \\ &= 1.75E\text{-}06\end{aligned}$$

$$\begin{aligned}Q_2 &= \frac{\alpha_2}{\alpha_t}\ Q_t \\ &= \frac{2 * 0.065}{1.065} * 2\ 0E\text{-}06 \\ &= 2.46E\text{-}07\end{aligned}$$

The basic event failure rates for the redundant dump valves can be adapted as follows:

IFDVALVE1	= Q_1
IFDVALVE2	= Q_1
CCF_DVALVES	= Q_2

Temperature sensors:

$$Q_1 = \frac{\alpha_1}{\alpha_t} Q_t$$

$$= \frac{0.943}{1.075} * 4.0E\text{-}06 \qquad (13.24)$$

$$= 3.51E\text{-}06$$

$$Q_2 = \frac{\alpha_2}{\alpha_t} Q_t$$

$$= \frac{0.038}{1.075} * 4.0E\text{-}06 \qquad (13.25)$$

$$= 1.40E\text{-}07$$

$$Q_3 = 3 \frac{\alpha_3}{\alpha_t} Q_t$$

$$= \frac{3 * 0.019}{1.075} * 4.0E\text{-}06 \qquad (13.26)$$

$$= 2.11\ E\text{-}07$$

The basic event failure rates of the redundant temperature sensors have to be adapted as follows:

IFTS1	= Q_1
IFTS2	= Q_1
IFTS3	= Q_1
CCF_TS1TS2	= Q_2
CCF_TS1TS3	= Q_2
CCF_TS2TS3	= Q_2
CCF_TS1TS2TS3	= Q_3

The next step in the analysis is the quantification of the modified fault tree. The recommended approach to quantification is to first perform a point estimate using the mean values. The results can be used to identify significant contributors and to reduce the amount of effort and computation to propagate the uncertainty distributions in the final result.

Component database:
The modified database is as follows:

```
Basic Event           Type     Lambda         T           Theta

CCF_DVALVES           TS       2.46E-07       8760        0
CCF_TS1TS2            TS       1.40E-07       8760        0
CCF_TSITS2TS3         TS       2.11E-07       8760        0
CCF_TS1TS3            TS       1.40E-07       8760        0
CCF_TS2TS3            TS       1.40E-07       8760        0
IFDVALVEI             TS       1.75E-06       8760        0
IFDVALVE2             TS       1.75E-06       8760        0
IFTS1                 TS       3.51E-06       8760        0
IFTS2                 TS       3.51E-06       8760        0
IFTS3                 TS       3.51E-06       8760        0
INSTR_AIR             OR       1.02E-05       0           8.00
VLU_FAILS             TS       2.00E-07       8760        0
```

TS : Tested stand-by component
OR : On line repairable component
T : Test period
Theta : Repair duration.

The calculated point estimate of the unavailability of the safeguard system of the CSTR is given by:

Unavailability.

```
    Cut set                  Contribution       Per cent    Formula

1   CCFDVALVES                 1.08E-03           18.50        A-1
2   CCFTSITS2TS3               9.24E-04           15.87        A-1
3   VLU_FAILS                  8.76E-04           15.04        A-1
4   CCFTS1TS2                  6.13E-04           10.53        A-1
5   CCFTSITS3                  6.13E-04           10.53        A-1
6   CCFTS2TS3                  6.13E-04           10.53        A-1
7   IFTS2 . IFTS3              3.15E-04            5.41        B-1
8   IFTS1 . IFTS2              3.15E-04            5.41        B-1
9   IFTS1 . IFTS3              3.15E-04            5.41        B-1
10  INSTR_AIR                  8.16E-05            1.40        A-2
11  IFDVALVE1 . IFDVALVE2      7.83E-05            1.35        B-1
```

Contributions:

First order	:	4.8E-03
Second order	:	1.0E-03
Total unavailability	:	5.8E-03

Step 4.2 - Evaluation of Results and sensitivity analysis

From the results it can be concluded that common-cause failures are the dominant contributors to the unavailability of the instrument safeguard system of the CSTR. The uncertainty in unavailability due to uncertainty in the numerical values used for the common-cause model parameters can be obtained using one of the available techniques for uncertainty propagation. An uncertainty analysis using the Monte Carlo sampling technique for the results obtained with the alpha model is presented in the chapter "Importance Sensitivity and Uncertainty Analysis".

13.9 REFERENCES

[13.1] Procedures for Treating Common Cause Failures in Safety and Reliability Studies, Procedural Framework and Examples.
U.S. Nuclear Regulatory Commission. NUREG/CR-4780, Volume 1, January 1988.

[13.2] Procedures for Treating Common Cause Failures in Safety and Reliability Studies, Analytical Background and Techniques.
U.S. Nuclear Regulatory Commission.
NUREG/CR-4780, Volume 2, January 1989.

[13.3] Defenses against common-mode failures in redundancy systems
United Kingdom atomic energy authority.
A guide for management designers and operators.
A.J. Bourne, G.T. Edwards, D.M. Hunns, D.R. Poulter, I.A. Watson
SRD R 196, January 1981.

[13.4] A Database of Common-Cause Events for Risk and Reliability Applications, Pickard, Lowe and Garrick, Inc., June 1992.
EPRI TR-100382,

[13.5] Atwood.C.L, Distributions for Binomial failure rate parameters, Nuclear Technology, Volume 79, October 1987.

APPENDIX 13-A: TABLES

Table 13-A-1: Generic causes of a dependent failure of a mechanical, thermal or environmental nature.

Generic Cause	Example of Source
Impact	Pipe whip Water hammer Missiles Earthquakes Structuralfailure
Vibration	Machinery in motion Earthquakes
Pressure	Explosion Out-of-tolerance system changes (Pump overspeed, flow blockage
Grit	Air dust Metal fragments generated by moving parts with inadequate tolerances Crystallized boric acid from control system
Moisture	Condensation Pipe rupture Rainwater
Stress	Thermal stress at weids of dissimilar metals
Temperature	Fire Lightning Welding equipment Cooling system faults Electrical short-circuit
Freezing	Water freezing
Corrosion (Acid)	Boric acid from chemical control system Acid used in maintenance for rust removal and cleaning
Corrosion	In water medium or around high-temperature metals (e.g. filaments)

Table 13-A-2: Generic causes of dependent failures of an electrical or radiation nature.

Generic Cause	Example of Source
Electromagnetic interference	Welding equipment Rotating electrical machinery Lightning Power supplies Transmission lines
Radiation damage	Neutron sources Charged particles radiation
Conducting medium	Moisture Conductive gases
Out-of-tolerance voltage	Power surge
Out-of-tolerance current	Short-circuit

Table 13-A-3: Examples of coupling mechanisms.

Common Link	Example situations that can result in system failure when all basic events in a minimal cut set share the special condition
Energy Source	Common drive shaft Same power supply
Calibration	Misprinted calibration instructions
Manufacturer	Repeated manufactoring error, such as neglect to properly coat relay contacts
Installation contractor	Same subcontractor or crew
Maintenance	Incorrect procedure Inadequately trained personnel
Operator or operation	Operator disabled or overstressed Faulty operating procedures
Proximity	Location of components in one cabinet or one room
Test procedure	Fault test procedure that may affect all components normally tested together
Energy flow paths	Location in same hydraulic loop Location in same electrical circuit
Similar parts	Important in the case of minimal cut sets which contain only pumps, only valves, etc.

Table13-A-4: Examples to identify components that have similar attributes.

Type of common attribute	Examples
Component type including any special design or construction characteristics	- motor operated valve - swing check valve - component size - material.
Component use	- system isolation - flow modulation - parameter sensing - motive force.
Component manufacturer	
Component-internal conditions	- absolute or differential pressure range - temperature range - normal flow rate - chemistry parameter ranges - power requirements.
Component-external environmental conditions	- temperature range - humidity range - barometric pressure range - atmospheric particulate content and concentration.
Component location name and/or location code	- fire - flooding - turbine missiles.
Component initial conditions and operating characteristics	- normally closed - normally open - energized or de-energized - normally running - standby.
Component testing procedures and characteristics	- testinterval - test configuration or line-up - effect of test on system operation.
Component maintenance procedures and characteristics	- planned - preventive maintenance frequency - maintenance configuration or line-up - effect of maintenance on system operation.

APPENDIX 13-13: FORMULAS ALPHA MODEL

Group size equals 2:

$$\alpha_t = \alpha_1 + 2\,\alpha_2$$

$$\begin{aligned} Q_1 &= \frac{\alpha_1}{\alpha_t}\,Q_t \\ Q_2 &= \frac{\alpha_2}{\alpha_t}\,Q_t \end{aligned} \tag{13.27}$$

Group size equals 3:

$$\begin{aligned} \alpha_t &= \alpha_1 + 2\,\alpha_2 + 3\,\alpha_3 \\ Q_1 &= \frac{\alpha_1}{\alpha_t}\,Q_t \\ Q_2 &= \frac{\alpha_2}{\alpha_t}\,Q_t \\ Q_3 &= 3\,\frac{\alpha_3}{\alpha_t}\,Q_t \end{aligned} \tag{13.28}$$

Group size equals 4:

$$\begin{aligned} \alpha_t &= \alpha_1 + 2\,\alpha_2 + 3\,\alpha_3 + 4\,\alpha_4 \\ Q_1 &= \frac{\alpha_1}{\alpha_t}\,Q_t \\ Q_2 &= \frac{2}{3}\,\frac{\alpha_2}{\alpha_t}\,Q_t \\ Q_3 &= \frac{\alpha_3}{\alpha_t}\,Q_t \\ Q_4 &= 4\,\frac{\alpha_4}{\alpha_t}\,Q_t \end{aligned} \tag{13.29}$$

APPENDIX 13-C: MINIMAL CUT SETS DETERMINATION FOUR-VALVE EXAMPLE

Input fault tree:

```
Top       OR    Gate1     Gate2
Gate1     AND   Gate3     Gate5
Gate2     AND   Gate7     Gate9
Gate3     OR    Gate4     IFvalve1  CCF12     CCF13     CCF14
Gate4     OR    CCF123    CCF124    CCF134    CCF1234
Gate5     OR    Gate6     IFvalve2  CCF12     CCF23     CCF24
Gate6     OR    CCF123    CCF124    CCF234    CCF1234
Gate7     OR    Gate8     IFvalve3  CCF13     CCF23     CCF34
Gate8     OR    CCF123    CCF134    CCF234    CCF1234
Gate9     OR    Gate10    IFvalve4  CCF14     CCF24     CCF34
Gate10    OR    CCF124    CCF134    CCF234    CCF1234
```

Fault tree analysis:

Number of ’and’ gates	= 2
Number of ’or’ gates	= 9
Total number of gates	= 11
Total number of basic events	= 15

Basic events in fault tree:

```
CCF12     CCF124    CCF14     CCF24       IFvalve2
CCF123    CCF13     CCF23     CCF34       IFVALVE3
CCF1234   CCF134    CCF234    IFvalve1    IFvalve4
```

First-order cut sets:

```
  CCF12
  CCF123
  CCF1234
  CCF124
  CCF134
  CCF234
  CCF34
```

Second-order cut sets:

```
  CCF13 . CCF14
  CCF13 . CCF23
  CCF13 . CCF24
  CCF14 . CCF23
  CCF14 . CCF24
  CCF24 . CCF23
  Ifvalve1 . CCF23
  IFvalve1 . CCF24
  IFvalve2 . CCF14
  IFvalve2 . CCF13
  IFvalve3 . CCF14
  IFvalve3 . CCF24
  IFvalve4 . CCF13
  IFvalve4 . CCF23

IFvalve1 . IFvalve2
IFvalve4 . IFvalve3
```

HUMAN FAILURES

CONTENTS

14.1 INTRODUCTION

A review of accident analyses shows that human failures play an important role in the occurrence of accidents. For this reason it is important to identify potential human errors and to decrease the probability of occurrence of human failures. In general, this should be the main goal of a human reliability analysis.

The causes and consequences of human failure events are not as simple as with hardware failures. The cause behind a human failure event may sometimes be referred to as human error. This is a misleading term, since many so called errors are not caused by the human being under consideration but by circumstances beyond his or her control. One important issue is the need to consider the organizational factors that create the preconditions for human failures, as well as their immediate causes. The plant and corporate management levels determine conditions at the operational level that either support effective performance or give rise to failures. The safety beliefs and priorities of the organization will influence the extent to which resources are made available for safety as opposed to production objectives.

Human errors and human failures are so common that it is easy to assume that human failures occur stochastically, i.e. anywhere at and any time with a certain probability. Human reliability analysis techniques can model and quantify only some types of failures. Any other event that is not covered by a human reliability analysis can be quantified using subjective judgement.

Human failures can occur during any life cycle or mode of operation of the plant. In this respect human failures can be divided into the following categories:

- Human failures during design, construction and modification of the plant.
- Human failures during operation or maintenance.
- Human failures due to errors of management and administration.

Human failures during design, construction and modification are part of the dependent failure analysis and will not be dealt with in this chapter. The main focus of this chapter will be to analyse human failures during operation and during maintenance. A short overview will be presented concerning organizational and management influence factors.

This chapter is intended as a guideline on how to perform a human reliability analysis, given some generally accepted methodologies and general failure data. The goal of a human failure analysis should not only be a quantification of human error probability. The goal of a human failure analysis also should be to identify all possible human errors and to identify improvements that contribute to eliminating or decreasing the probability of human errors. In writing this chapter, a number of papers have been reviewed and the most promising and internationally accepted methods have been selected (see section 14.10).

First of all, this overview of the general framework on how to perform a human reliability analysis will be given. The framework consists of a number of phases and steps. Each phase will be described and the appropriate techniques to perform each step will be mentioned. Performing a human reliability analysis in accordance with this framework makes it possible to identify the dominant human errors and to generate measures to improve human performance and to reduce the human failure probability.

It should be emphasized that human behaviour is a complex matter that cannot be adequately represented by simple models such as those used for component and system reliability. This makes the analysis of human reliability more dependent on the judgement of the analyst.

The human failure analyst must be familiar with the identification and quantification of errors by operators and maintenance personnel. He must be able to understand the operational procedures in relation to the behaviour of the plant in accident conditions. Further more the HRA specialist must be able to judge about the circumstances under which the operator has to do his duty.

The human error quantification task is part of the basic event probability quantification of a fault tree. Together with the initiating event frequency, the component failure probability and the dependent failure probability the human error probability has to be put into a database which is used to quantify the fault tree, see chapters 8 and 12.

14.2 NOMENCLATURE AND ABBREVIATIONS

A,B	=	calibration constants	-
f	=	error factor	hours or minutes
HEP	=	human error probability	-
FLI	=	failure likelihood index	-
m	=	median response time	minutes
t	=	available time	hours or minutes
S_i	=	numerical rating or degree-of-difficulty score for performance shaping factor i	-
w_i	=	relative importance of performance shaping factor I	-
σ	=	logarithmic standard deviation	-

Subscripts:

r	=	randomness factor
u	=	uncertainty factor

ABBREVIATIONS

APJ	Absolute Probability Judgement
CR	Control Room
EF	Error Factor
EOP	Emergency Operating Procedures
ERS	Error Reduction Strategies
HCR	Human Cognitive Reliability
HEA	Human Error Analysis
HEART	Human Error and Assessment and Reduction Technique
HEI	Human Error Identification
HEP	Human Error Probability
HRA	Human Reliability Analysis
HTA	Hierarchical Task Analysis
OAET	Operator Action Event Tree
OAT	Operator Action Tree
PIF	Performance Influence Factors
PRA	Probabilistic Risk Assessment
PSF	Performance Shaping Factors
QRA	Quantítative Risk Assessment
SLI	Success Likelihood Index
SLIM	Success Likelihood Index Method
SOP	Standard Operating Procedures
TA	Task Analysis
TESEO	Tecnica Empire Stima Errori Operatori
TRC	Time Reliability Correlation
THERP	Technique for Human Error Rate Prediction
VDU	Visual Display Unit

14.3 PROCEDURAL FRAMEWORK

To perform a human reliability analysis or to perform a human error reduction analysis one has to perform a number of tasks. To put these tasks in the right order a procedural framework has been developed. This section is a brief description of the procedural framework to perform such an analysis. There are four phases, each of which contains a number of steps. They are summarized in table 14.1.

Table 14.1: Procedural framework.

1:	Familiarization
-	Collection of information
-	Plant visit
-	Review of written procedures.
2:	Qualitative analysis
-	Task analysis
-	Identification of potential human errors
-	Classification of human errors
-	Modelling of human errors in risk analysis.
3:	Quantification of human failures
-	Calculation of human error probabilities
-	Human error consequence analysis
-	Recovery analysis.
4:	Evaluation
-	Sensitivity and uncertainty analysis
-	Recommendations
-	Reporting.

14.3.1 Familiarization

If a human reliability analysis is part of a more extensive risk assessment, the human reliability analyst has to review all relevant documents generated by the systems analyst. Especially he has to focus on the human interaction with the system. For instance, he should find out which human action events have been identified by the systems analyst. Which procedures are available to carry out these actions and what are the plant conditions when these actions are to be carried out.

A plant visit is essential in the performance of a plant-specific human reliability analysis. The purpose of such a visit is to allow the analyst to familiarize himself with the operator-relevant characteristics of the plant. The intention of a plant visit is to identify the aspects of the control room, the general plant layout, and the plant’s administrative control system that affects human performance.

During the systems analysis the analyst identifies human actions that directly affect the system-critical components he has previously identified. In the light of the information obtained from the plant visit, the human reliability analyst must review these actions in the context of their actual performance to determine whether any factors exist that influence behaviour with regard to these system-critical actions and that may have been overlooked by the system analyst.

14.3.2 Qualitative analysis

A qualitative human failure analysis is one of the reducing the human failure contribution to risk. following techniques:

- A task analysis
- A human failure identification analysis
- A performance shaping- or influence analysis
- A human failure consequence analysis
- A human failure reduction analysis.

A task analysis is required to perform an accurate human failure identification analysis and an analysis of performance shaping factors. Both issues play an essential role in the contribution to risk due to human failures.

14.3.3 Quantitative analysis

A large number of techniques exist to quantify the probability of human failures. However a small number of these techniques have actually been applied in practical risk assessment. Important in the quantification process are the type of human failures and the performance shaping factors. Important shaping factors are: plant interface and indication of conditions, unambiguousness of actions, task complexity, procedural guidance, training and experience, adequacy of time to accomplish action and stress.

The purpose of the consequente analysis is to evaluate the relevant consequences to the system of the human errors identified. The consequente analysis is limited to the human reliability analysis, but impacts the overall risk or reliability analysis of the system.

After occurrence of a failure, a recovery action might be possible that will achieve a less undesirable plant state. It is usually convenient to postpone consideration of the effect of recovery actions in the sequence of activities in the human reliability analysis until the total system success and failure probabilities have been determined. At this stage of the analysis the circumstances are known under which the recovery action has to be performed. It might also be the case that a possible recovery action does not need to be quantified because of the low probability of occurrence of the accident sequence in consideration.

14.3.4 Evaluation

Sensitivity and uncertainty analysis:
It should be clear that there is considerable uncertainty in the estimation of human failure probabilities. An uncertainty analysis is useful to integrate the individual parameter uncertainty into the calculated human failure probability. It is also useful to see how significant such

uncertainties can be by using sensitivity analyses to determine the direct relationship between the input values for human error probabilities and the overall system results.

Recommendations:
Given the quantitative results and the sensitivity and uncertainty analysis, one has to formulate recommendations on how to decrease the probability of human errors.

Reporting:
The final step is the reporting of the analysis. It is particularly important to specify clearly what assumptions have been used and to identify the consequences of using these and other assumptions.

14.4 QUALITATIVE ANALYSIS

14.4.1 Task analysis

The purpose of a task analysis is to collect information on a human activity in such a way that this information can be used in a human error reduction program or a human reliability analysis. A detailed task analysis is required for most of the human error identification techniques and human reliability analysis techniques.

Task analysis describes the demands made on the operator in the tasks he or she has to perform, and examines the resources required and available to enable the operator to meet those demands. A demand is a requirement for the operator to meet some goal which is a partial requirement for achieving a higher goal. Resources refer not only to the equipment the operator uses (displays, controls, tools, procedures, etc.) but also to human resources of memory, information processing, attention, learning, physical skills, adaptation, etc. In theory, by comparing demands to resources, potential errors and sources of errors can be identified. However, the situation is complicated by the fact that operators may make errors when there is no task demand, i.e. so called extraneous acts.

Different task analysis techniques may help the analyst to:
- Provide a clear description of what is involved in the task
- Collect data about the task
- Generate ideas about error sources
- Generate ideas concerning solutions to problems.

Many task analysis techniques are currently available in ergonomics and other risk analysis which deal with the description and analysis of human involvement in systems, such as:
- Charting and network techniques
- Decomposition methods
- Hierarchical task analysis
- Link analysis
- Operational sequence diagrams
- Time line analysis.

For a description of the available methods, see reference [14.7]. Only the decomposition technique will be described in this chapter because, this technique is very suitable to analyse operator actions during execution of a procedure.

Decomposition technique:
Task decomposition is a structured way of expanding the information from a task description into a series of more detailed statements about particular issues which are of interest to the human failure analyst. It starts from a set of task descriptions which describe how each element within a particular task is undertaken. For each of these task elements, the analyst then systematically collects further information about specific aspects of the talk. This information is presented in a table for each task element using an appropriate set of sub-headings. The result is that the total information for each step is decomposed into a series of statements about this task. The format of this table is not specified, but the table must contain all the information necessary to perform the other parts of the analysis.

By defining a proper heading, one has to consider three types of decomposition categories:

Descriptive categories:
The task features have to be described in detail. The level of detail necessary in a task analysis and the amount of information recorded should reflect the level of detail of the risk analysis and are determined judge mentally. The guiding rule for this determination is that the tabulated information must be sufficient to recapitulate the rationale for a human error probability estimation or for a human error reduction analysis, if required.

Organization-specific categories:
These categories cover task information that is very specific to the organization for which the task analysis is being carried out. They involve assessing whether some criterion that is of particular importance to that organization is being met. For instance, it may be necessary to assess whether any task elements violate a checklist item, which will allow the analyst to focus upon aspects of the task which do not meet some important criteria. These categories can also be used to indicate where further input data are necessary from other staff members involved in the system development.

Modelling categories:
If the information generated in the task analysis is to be used in other parts of the human failure analysis, the information presented in the task analysis must be able to support the other part of the human failure analysis.

In most cases, the necessary information will consist of items such as:
- The piece of equipment on which an action is performed
- The action required of the operator
- The limits of his performance
- The location of the controls and displays
- Explanatory notes.

To support the analyst with the selection of descriptive decomposition categories, a taxonomy of such categories is presented in table 14.2.

14.4.2 **Identification of potential human errors**

Once the breakdown of task steps has been done (see section 14.4.1), errors likely to be made must be identified for each step. The determination whether for any given step an error of omission should be considered, or one of the types of errors of commission that are likely for that step, must be made based on the relevant performance shaping factors and on the task analysis proper. It is recommended to list the steps chronologically. Based on the characteristics of the actual performance situation, the human reliability analyst must determine and record which types of errors the operator is likely to make and which not. For example, if an operator is directed by a set of written procedures to manipulate a valve and that valve is fairly well isolated on the panel, has a different shape than other valves on the same panel, and has been very well labelled, the analyst may determine that errors of selection are not to be considered in this case. He should also have determined that an error of omission made in following the written procedures might be made. Extreme care should be exercised in deciding which errors, if any, are to be completely discounted in an analysis.

Table 14.2: Taxonomy example.

Description of task Description Type of activity/behaviour Task/action verb Function/purpose Sequence of activity	**Performance of the task** Performance Time taken/starting time Required speed Required accuracy Criterion of response adequacy
Requirements for undertaking the task Initiating cue/event Information Skills/training requirement Personnel requirements/staffing	**Other activities** Subtasks Communications Co-ordination requirements Concurrent tasks
Hardware features Location Controls used Displays used Critical values Job aids required	**Output from task** Output Feedback
Nature of the task Actions required Decisions required Response required Complexity Task difficulty Task criticality Degree of attention required	**Consequences/problems** Likely/typical errors Errors made /problems Error consequences Adverse conditions/hazards

Human error identification is a critical part of human error assessment; if an important potential human error is not identified, the risk assessment cannot be regarded as complete. The human error identification process has to fulfil the following three criteria (Kirwan):

- It must ensure comprehensiveness of error identification and thus the accuracy of the risk assessment modelling

- It should provide useful and accurate understanding of potential human errors in case error reduction is required
- It should ensure that the assessment provides and remains a useful database during the lifetime of the plant.

To identify potential human errors, a number of human error techniques can be applied, for instance:
- Technique for human error rate prediction (THERP)
- Hazard and operability study (HAZOP)
- Systematic human error reduction and prediction approach (SHERPA)
- Generic error modelling system (GEMMS).

The THERP technique is described in section 14.5.2. Because the HAZOP technique can be learned rather quickly and is very well known, only the HAZOP technique to identify potential human errors will be described in this section. The HAZOP technique is not only used to identify potential human errors but also to identify hardware failure which can lead to hazardous events. The HAZOP technique offers significant potential for identifying and reducing human errors because:
- a HAZOP is carried out by a group of experts among which members with operational experience
- a task analysis showing the sequence of operations and staff involvement is available
- an extended guide word list is available.

A HAZOP is a well established technique in process design auditing and engineering risk assessment. It is typically applied in the early design stages but can also be applied to existing systems or during system modification. It utilizes the experience of the HAZOP chairman and the system design and operational personnel in a powerful analysis of a new or existing plant. It is primarily applied to process and instrumentation diagrams. Small sections of plant process equipment and piping lines on the diagram are selected and a set of guide words is applied to each section to detect design deviations. For instance guide words such as ”no flow” or ”reverse flow” can be applied to a piece of piping feeding into a pump. “What if” questions can be asked to identify deviations from normal system operations. The HAZOP team might consider, for example, this question: ”what if reverse flow occurred through the valve”. To perform a HAZOP for human error identification, it is useful to interchange the traditional HAZOP guide words by those defined by Whalley (see reference H 4.9]), see table 14.3.

Table 14.3: Human error HAZOP key words.

- not done	- later than
- repeated	- as well as
- less than	- misordered
- sooner than	- other than
- more than	- part of

In addition to the HAZOP guide words, the error classification as presented in table 14.4 can be used. The results of a HAZOP are reported in tables. An example of such a table is given in table 14.5. The advantages of HAZOP are that it occurs at an early design stage, and errors are identified by a team of experts. This means that errors can be identified early and rectified at minimal cost. In terms of the three basic criteria, the HAZOP technique can be fairly comprehensive. During the documentation phase it must be taken into account to document the reasoníng behind the errors identified.

Table 14.4: Error classification.

Action Errors:
- Action omitted
- Action too early
- Action too late
- Action too little
- Action too much
- Action too short
- Action too long
- Action in wrong direction
- Right action on wrong object
- Wrong action on right object
- Misalignment error

Checking Errors:
- Checking omitted
- Check incomplete
- Right check on wrong object
- Wrong check on right object
- Check mistimed
- Wrong check on wrong object

Retrieval Errors:

Information not obtained
- Wrong information obtained
- Information retrieval incomplete

Transmission Errors:
- Information not transmitted
- Wrong information transmitted
- Information transmission incomplete

Selection Errors:
- Selection omitted
- Wrong selection made

Plan Errors:
- Plan preconditions ignored
- Incorrect plan executed

Table 14.5: Example table HAZOP.

No.	Deviation	Indication	Causes	Consequences	Actions recommendations
1					
2					
n					

14.4.3 Classification of human errors

The classical human factors engineering approach to human failure was based on a black box model of human behaviour that focused primarily on information input data and control action output. Nowadays approaches based on cognitive psychology are used. The key difference in comparison with the human failure engineering approach is that the cognitive approach emphasizes the role of intentions, goals, and meanings as an aspect, of human behaviour. The term cognitive is based on the Latin "cognoscere", which means to know. Instead of conceptualizing the human being as a passive system element, to be treated in the same way as a pump or a valve, the cognitive approach emphasizes the fact that people impose their opinion on the information they receive, and their actions are always directed to achieving some explicit or implicit goal.

A major advantage of the cognitive perspective is that it provides a basis for the prediction and classification of human errors. An effective classification system for errors is essential from several points of view. To collect data on human errors from industrial experience for the purpose of discerning trends, identification of recurrent types of errors, or for developing a quantitative data base of error probabilities, one needs a basis for grouping together errors of similar type.

Classification systems of human errors are used in three ways:
- Analysis of incidents, to identify what happened and prevent recurrence, and to derive data from such incidents
- Human error identification, to identify errors which may have an impact upon system goals and risk levels
- Human error quantification, to match existing data to identified human errors to quantify the likelihood of occurrence.

In the past a number of human error classifications have been presented. The most important ones will be described in this section.

Swain and Guttmann:
Swain and Guttmann have defined two major categories of human error:
- Errors of omission
  A person fails to perform the task or part of the task
- Errors of commission
  - A person performs the task or step incorrectly
  - A person introduces some subtask or step that should not have been performed
  - A person performs some subtasks or steps out of sequence
  - A person fails to perform the task or step within the allocated time, either too early or too late.

From a system point of view, any one of the above actions is considered an error only when it reduces or has the potential of reducing system reliability, system safety, or the likelihood that some other system success criterion will not be met.

Rasmussen's skill-rule-knowledge framework:
Rasmussen defined the notions of skili-based, rule-based, and knowledge-based actions. Skill-based actions are those actions which are routinely performed, while rule-based are those for which the operator needs the support of procedures and rules; knowledge-based actions are those that rely on the operator's knowledge of the plant and for which no rules have been formulated.

- **Skill-based:**
  In skill-based behaviour, there is a very close coupling between the sensor input and the response action. Skill-based behaviour does not directly depend on the complexity of the task, but rather on the level training and the degree of practice in performing the task. Different factors may influence the specific behaviour of a particular individual; however, a group of highly trained operators would be expected to perform skill-based tasks expeditiously or even mechanistically with a minimum of mistakes. For rule- and knowledge-based behaviour the connection between sensory inputs and output actions is not as direct as for skill-based behaviour. At the skill-based level, human performance is governed by stored patterns of preprogrammed instructions represented as analog structures in a time-space domain. Errors at this level are related to the intrinsic variability of force, space or time coordination.

- **Rule-based:**
  Rule-based actions are governed by a set of rules or associations that are known and followed. A major difference between rule-based and skill-based behaviour depends on the degree of practice. If the rules are not well practised, the human being has to recall consciously or check each rule to be followed. Under these conditions the human response is expected to be less timely and more prone to mistakes, since additional cognitive processes must be called upon. The potential for error results from problems with memory, the lack of willingness to check each step in a procedure or failure to perform each and every step in the procedure in the proper sequence. The rule-based level is applicable to tackling familiar, problems in which solutions are governed by stored rules of the type ”if (state) then (diagnosis)” or ”if (state) then (remedial action)”. Here, errors are typically associated with the misclassification of situations leading to the application of the wrong rule or with the incorrect recall of procedures.

- **Knowledge-based:**
  When symptoms are ambiguous or complex, when the state of the plant is complicated by multiple failures or unusual events, or when the instruments give only an indirect reading of the state of the plant, the operator has to rely on his knowledge and his behaviour is determined by more complex cognitive processes. Rasmussen calls this knowledge-based behaviour. The performance of a human being with this type of behaviour depends on his knowledge of the plant and his ability to use that knowledge. This type of behaviour is expected to increase the probabilities of occurrence of mistakes or misjudgements and to increase the time interval until appropriate action is taken. The knowledge-based level is applicable in new situations for which actions must be planned on-line, using conscious analytical processes and stored knowledge. Errors at this level arise from resource limitations and incomplete or incorrect knowledge.

Reason:

Slips and mistakes
Slips are defined as errors in which the intention is correct, but a failure occurs when the activity is carried out. Mistakes arise from an incorrect intention, which leads to an incorrect action sequence, although this may be quite consistent with the wrong intention. Incorrect intentions may arise from lack of knowledge or inappropriate diagnosis.

Violations
An error that occurs when an action is taken that contravenes known operational rules, restrictions, and or procedures.The definition of violation excludes actions taken to intentionally harm the system. The classification of human errors, adapted from Reason, is given in figure 14.1.

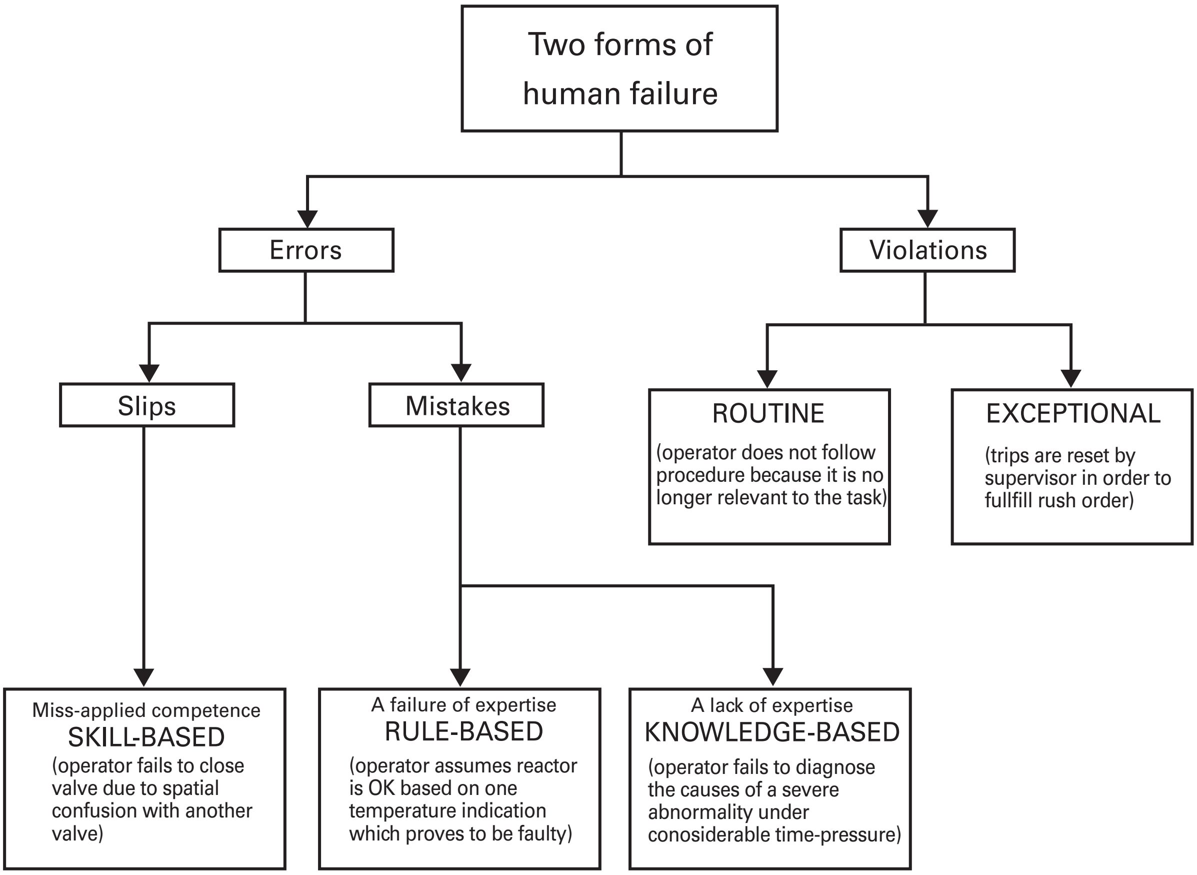

Two forms of human failure
Errors
Violations
Slips
Mistakes
ROUTINE
(operator does not follow procedure because it is no longer relevant to the task)
EXCEPTIONAL
(trips are reset by supervisor in order to fullfill rush order)
Miss-applied competence
SKILL-BASED
(operator fails to close valve due to spatial confusion with another valve)
A failure of expertise
RULE-BASED
(operator assumes reactor is OK based on one temperature indication which proves to be faulty)
A lack of expertise
KNOWLEDGE-BASED
(operator fails to diagnose the causes of a severe abnormality under conosiderable time-pressure)

Figure 14.1: Reason, Classification of human errors.

Accident sequence risk analysis-based classification:

If a risk analysis is performed by using the accident sequence approach (initiating events, event trees and fault trees), a classification scheme can be used which is in accordance with this approach. In this approach an initiating event is defined as an event that creates a disturbance in the plant and has the potential to lead to undesired consequences, depending on the successful operation of the various safety systems. The following types of failures can be defined:

Pre-initiator failures: (Latent error)
Testing and maintenance actions prior to an initiating event

Human-induced initiators:
Actions which might cause initiating events

Post-initiator failures: (Dynamic operator action failure)
Emergency-procedure-driven actions taken to deal with and mitigate the consequences of accident sequences and actions which aggravate accident sequences

Recovery actions:
Actions to restore failed equipment by repair or by alternative equipment.

14.4.4 Analysis of performance shaping (influence) factors

The terms performance shaping factor or performance influence factor cover the same item and are used to refer anything that could increase or decrease performance, and thus to the error probability, for a particular type of task. In this chapter only the term performance shaping factor will be used. Performance shaping factors are hypothetical, since one does not know for certain that they will have a particular effect in a specific situation. Experimental work generally does not give the kind of data needed about performance shaping factors that is useful in human reliability quantification. Two kinds of performance shaping factors are normally considered; the external performance shaping factors, and the internal performance shaping factors.

The external performance shaping factors include:

- The organizational preconditions corresponding to the organizational structure (hierarchies, form of payment, opportunity to continued education), and the educational dynamics (working time, tool engineering, structure of working)
- The technical preconditions corresponding to the difficulty of the task connected with the machine, task design, the system's technical realization, and the situation factors such as layout, anthropometric considerations, and the design of the environment.

The internal performance shaping factors include:

- The capacity of performance, which corresponds to the individual factors such as physiological capacity (constitution, age) and psychological capacity (mental aptitude, level of education, training)
- The physiological fitness including the individual's disposition and conditioning (practice, training)
- The psychological willingness, including intrinsic motivation (interest, inclination, social integration, mood level of pretension, prestress) and extrinsic motivation (opportunity of promotion, work conditions, working climate, wage level).

An extensive list and explanation of performance shaping factors is given in the CCPS Guidelines. The most important groups of performance shaping factors are:

- Operating environment
  - Physical work environment
  - Work pattern

- Task characteristics
  - Equipment design
  - Control panel design
  - Job aids and procedures
  - Training

- Operator characteristics
  - Experience
  - Personality factors
  - Physical condition and age

- Organizational and social factors
  - Team work and communications
  - Management policies

14.4.5 Modelling of human errors in risk analysis

For this paragraph it is assumed that the risk model has been constructed by application of event trees and fault trees. The risk analysts usually try to keep the event trees as economical as possible. If the short-event-tree/long-fault-tree approach has been adopted, the human failure events are not usually incorporated as top events into an event tree, although they could be. Post-initiator events are mostly modelled near the top of the fault tree. The human-induced initiators are part of the initiator events analysis. As such, each will be given a specific initiator designator, and some may have an associated fault tree to help quantify the initiator frequency. Figure 14.2 indicates where the human failure events are most effectively incorporated into the risk assessment model. The linking of event trees and fault trees is explained in chapter 12.

Pre-initiator failures:
Pre-initiator failures occur before the occurrence of an initiating event. Often they leave the stand-by equipment in an unavailable situation. These events have no dependency on a sequence, since they precede the assumed initiator and can therefore be modelled as an independent event anywhere in the event tree or fault tree. The great majority of pre-initiators occur as failures during testing or maintenance. Three methods are available to the system modeler for incorporating pre-initiator events:

1: Model a pre initiator event for any component that is maintained or otherwise manipulated during normal operation.

2: Model a pre initiator event for each procedure, placing an identically named event with each component, or segment modelled for equipment manipulated during the procedure.

3: Model a pre initiator event for each train of the system, or other logical grouping of equipment, and account for different procedures and equipment manipulations at this model level.

The first method easily merges with the popular component-oriented system modelling techniques. However, this method produces dependent basic human failure events.

The best method of incorporating pre-initiator human failure events is according to actual activities in the plant, e.g. the maintenance procedures. All the procedures are gathered and the manipulated equipment is identified. Then each component, or group of components, is given a pre-initiator human failure event at the model's desired level. The associated procedure that manipulates this component or group of components is then modelled using task analytical human reliability analysis methods. This method can be very time consuming.

The recommended method of incorporating pre-initiator human failure events is method 3, in combination with a screening analysis. Making use of a screening analysis allows train-grouped human failure events to be initially quantified. Events surviving the screening, which are typically few, are then modelled similarly to method 2 if necessary.

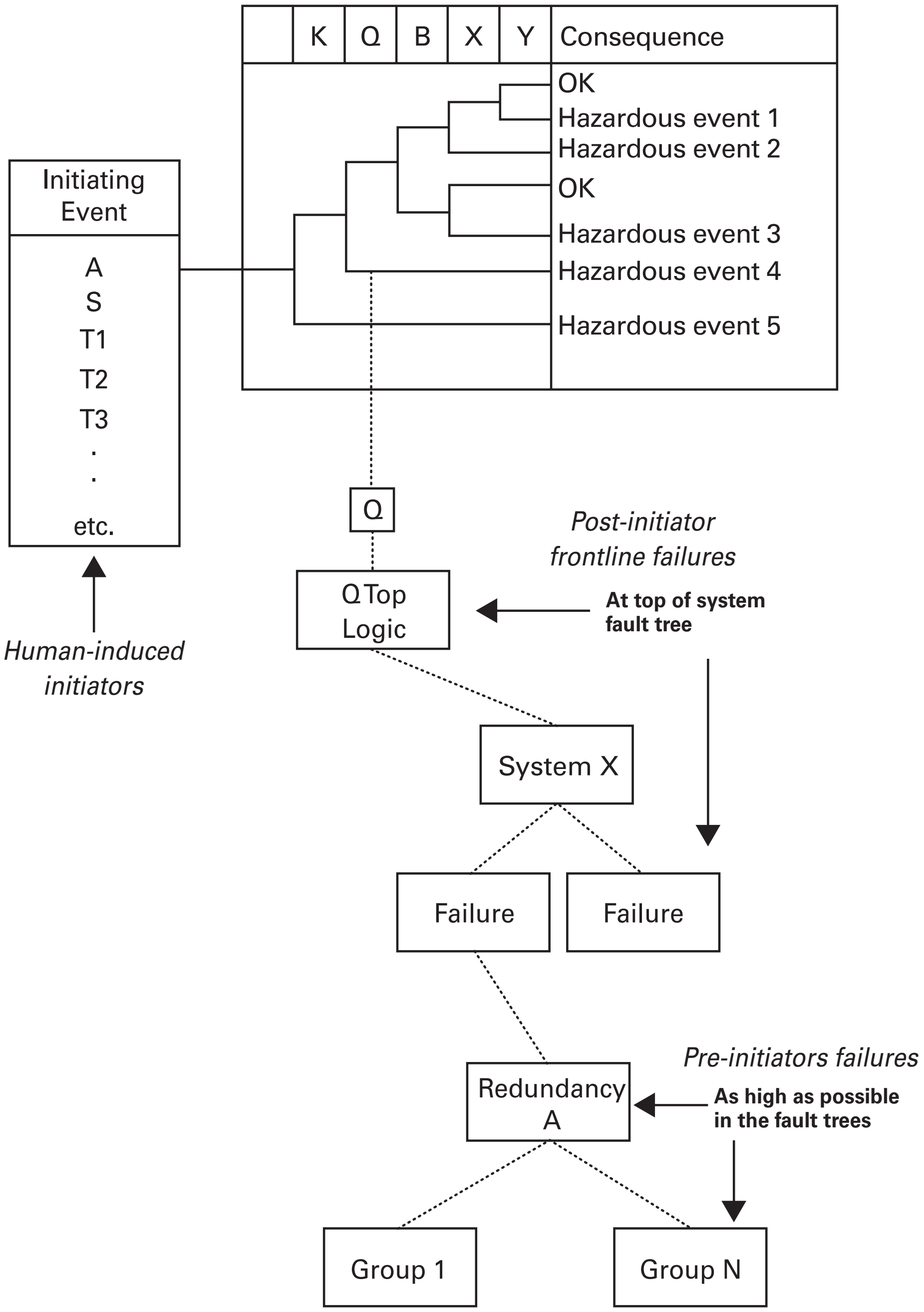


Figure 14.2: Recommended incorporation of human failure events.

Human-induced initiators:
Human-induced initiators are initiating events that are identified to have predominantly human failure causes. Standard risk assessment lists do not distinguish the root cause of an initiator and this type of events is often not modelled separately in a risk analysis. If the risk assessment requires the definition of a specific human-induced initiator, the plant incident database must be able to support quantification of this specific human-induced initiating event. Otherwise, the human induced initiator is a random human failure event and can only be quantified using subjective judgement.

Post-initiator human failure events:
Following an initiator, operators must start response activities to mitigate the effects of the initiator and establish a safe shutdown of the plant. These activities can correspond to the symptom-based emergency procedure systems. All post-initiator human failures are highly dependent on the sequence in which they are postulated to occur. As a result, incorporating and screening such events at an occurrence probability of less than unity is potentially non-conservative until cut set details are specified. Also, since a sequence can be considered as an AND gate, there is always the possibility of cut sets that contain more than one post-initiator human failure event, again creating the significant possibility of erroneously eliminating sequences from further consideration based on non-conservative, joint human failure probabilities.

To avoid these pitfalls and to avoid unnecessary early efforts, the following strategy is recommended for identifying post-initiator human failures. Basically, the strategy is to model post-initiator events as little as possible before the sequence cut sets are known, in particular to:

1 : Model post-initiator human failures only in safety systems.
Some non safety systems require manual actuation, but modelling of these systems can be deferred until the sequences are developed through the safety systems.

2: Do not initially model recoveries that are of the backup variety
A backup action is the verification that an automatically actuated system did not actuate plus the attempt to actuate it manually. The failure of such of a recovery action clearly should be directly associated in a model with the originating failure of the automatic system in an and gate. These backup failures can be identified easily at the cut set level and therefore do not need to be modelled in the event tree/fault tree model.

3: Do not model third or lower priority systems in initial risk assessment models
The purpose of this guideline is also to separate the recovery model from the failure model as much as possible. All symptom-based emergency procedures list multiple systems in an implied priority for the contingency when safety-related equipment faits. These systems represent third or lower priorities in a list of possible systems. It is recommended that these systems will not be modelled until sequences are determined. At that time, human and hardware events may need to be modelled.

14.5 QUANTIFICATION OF HUMAN ERROR EVENTS

All human reliability quantification techniques quantify the human error probability (HEP). The human error probability is defined as:

$$\text{HEP} = \frac{\text{Number of errors occurred}}{\text{Number of opportunities for error}} \tag{14.1}$$

In quantifying human failure events, the type of failure must be specified in advance. Human failure events have a probability of failure per demand. The human failure event is quantified as the conditional probability of the failure, given the demand. This is even the case for human events that are time-dependent, such as those that occur after the initiating event.

Data problem:
In reality there are very few recorded data of human error events. The most important reason for not having such data are:
- Difficulties in estimating the number of opportunities for error in realistically complex tasks
- Confidentiality and unwillingness to collect and publish human failures.

It is clear that there is a data problem which cannot be solved easily. Not only the lack of data is a problem, the generalizability of available data is difficult as well. How to apply, for example, data collected in chemical plants to a nuclear power plant? Given the lack of data situation, a number of non-data-dependent approaches have been developed. This is not necessarily a bad thing, expert opinion has been used successfully in other areas. Take notice that not all human failure events have to be quantified accurately. The most efficient approach is to apply a screening value first. After screening it will be clear if a more detailed human reliability analysis is required or not.

14.5.1 Screening of human failure events

The human reliability screening task activities start by checking the validity of the human failure events that are defined in the model at the time of the screening and removing those that are not valid. The remaining events are assigned conservative probability values, which are less than unity, whenever possible. This process is called quantitative screening. The probabilities used to screen the human failure events arise from conservative estimates from appropriate human reliability analysis techniques. Table 14.6 shows probability screening values that should be used for categories of valid events.

Table 14.6: Generic Human Error Probabilities screening values.

Type of human error event	**Screening value**
Latent (pre-initiator) human failure events:	
- miscalibration	0.03
- failures in the restoration following maintenance	0.03
- dependent failures in redundant trains	0.003
Human-induced initiators	Not screened
Dynamic (post-initiator) human failure events:	
- failure to actuate manually initiated systems	0.4
- failure to backup automatic systems	0.4
- failure to recover the function of failed systems	1.0

14.5.2 Calculation of human error probabilities

A large number of quantification techniques are available and a lot of bench mark analyses have been executed. Given this overwhelming amount of information, a selection has to be made. In this chapter the following techniques will be described:
- Absolute probability judgement
- Technique for human error rate prediction (THERP)
- Time Reliability Correlation (TRC)
- Modified SLIM-based approach

The selection criteria applied are: state of the art, well accepted, accurate, the number of studies in which the technique has been used.

Absolute probability judgement:
Absolute probability judgement is the use of experts to generate human error probabilities directly. It may occur in various forms, from the single expert assessor to the use of a large group of individuals who may work together, or whose estimates may be mathematically aggregated. Absolute probability judgement requires experts with in depth knowledge of the area they are being asked to assess. It is preferable, if experts are meeting and sharing their expertise and discussing their arguments in a group, to utilize a facilitator. The facilitator's role is to try to prevent biases due to personality variables in the group, and biases in making expert judgments, from occurring and distorting the results.

Technique for human error rate prediction (THERP):
The THERP technique is developed by the well-known human reliability specialists Swain and Guttmann. The THERP technique is one of the most accepted human reliability techniques in the international risk analysis community.

The THERP technique consists of the following elements:
- A database of human error probabilities
- Performance shaping factors such as stress which affect human performance and can be used to alter the basic human error probabilities in the database
- An event tree modelling approach
- A dependency model.

The THERP technique is often classified as a decomposition approach. This means that its description of human operator tasks has a higher resolution than many other techniques. One of the advantages of the THERP technique is that it is a logical approach with a larger degree of emphasis on error recovery than most other methods. Besides, benchmark exercises show that the THERP technique is one of the most accurate techniques.

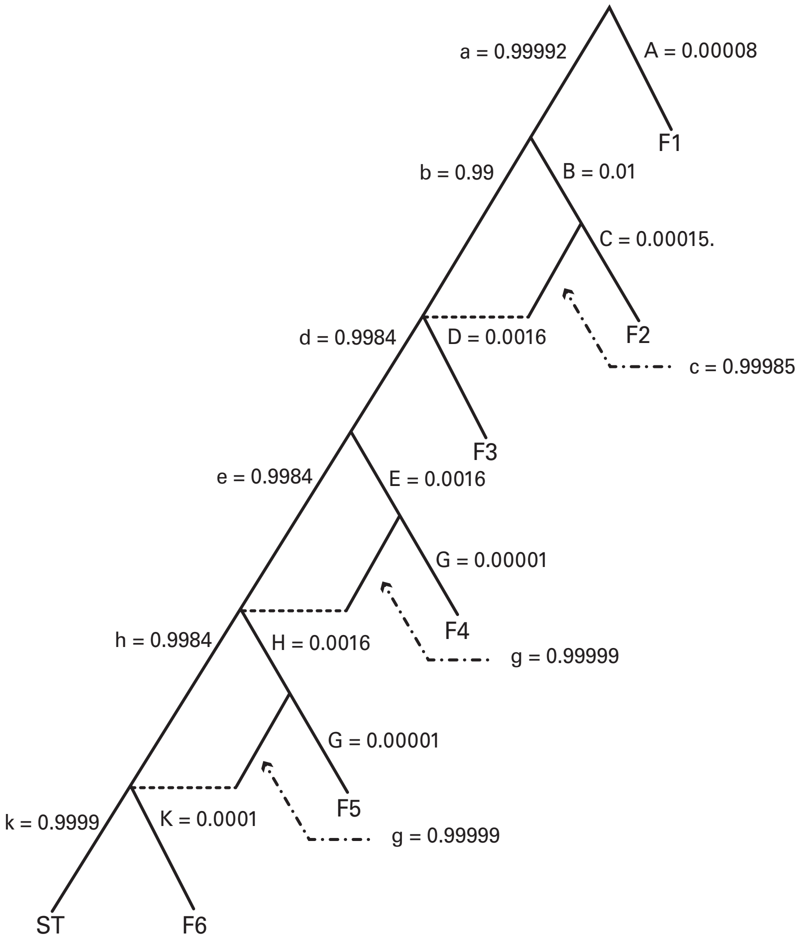
A THERP analysis can be divided into a number of tasks:

Task 1: Problem definition
Problem definition is achieved through plant visits and review of the documents generated by the system analysts. In most cases the systems analyst has defined a number of tasks to be performed by the operator or the maintenance crew. Each task has to be reviewed by the human reliability analyst. As a result of this task, it must be clear to the human reliability analyst under which conditions these tasks have to be performed and that all relevant tasks have been taken into account.

Task 2: Qualitative error prediction
The second task is to perform a detailed task analysis. THERP is usually applied at the level of specific tasks and the steps within these tasks. The form of task analysis used therefore focuses on the operations which would be the lowest level in a hierarchical task structure. The next step is to identify potential human error events. The main types of error considered in a THERP analysis are:
- Errors of omission
- Errors of commission
- Selection error
    - Selects wrong control
    - Mispositions control
    - Issues wrong command
- Sequence error (action carried out in wrong order) - Time error (too early or too late)
- Quantitative error (too little or too much).

An important part of this task is to identify the various performance shaping factors for each task that has to be quantified. The analyst also needs to record opportunities to recover errors at this stage of the analysis.

Task 3: Event tree development
After identification of the errors that could occur in the execution of each task, event trees have to be constructed to represent the errors identified. Complex tasks can generate very elaborate event trees. Error recovery can be incorporated by a dotted line (see example in figure 14.3).



Event	Description	HEP
A :	Fail to initiate action to annunciator	0.00008
B :	Misdiagnosis	0.01
C :	Fail to initiate action to annunciator	0.00015
D :	Omit step 2.4	0.0016
E :	Omit step 2.5	0.0016
G :	Fail to initiate action to annunciator	0,00001
H :	Omit step 2.6	0.0016
K :	Fail to initiate emergency cooling system	0.0001

Figure 14.3: Example of a THERP event tree.

Task 4: Quantification
Quantification in a THERP analysis is carried out as follows:

- Identify the errors in the event tree for which human failure data is required

- Select appropriate data tables in the THERP handbook (see reference [14.13]). The handbook contains a large number of tables giving error probabilities for operations commonly found in control rooms or plants. It must borne in mind that the handbook was originally written for the nuclear industry, as the data reflects the types of operations found in that industry and the values given are applicable to operators with equivalent education and training

- Modify the basic data according to guidelines provided in the handbook, to reflect differences in the assumed "nominal" conditions and the specific conditions for the task being evaluated. An important factor to be taken into account is the level of stress perceived by the operator when performing the task

- Modify the value obtained from the previous stage to reflect possible dependencies among error probabilities assigned to individual steps in the task analysed. A dependence model (see paragraph 4.5) is provided which allows for levels of dependence from complete dependence to independence to be modelled. Dependence could occur if one error affects the probability of subsequent errors

- Combine the modified probabilities to give the overall error probability for the task.

Task 5: Development of an error reduction strategy
If human error probability reduction is required, the human reliability analyst has to reexamine the event trees to determine whether any performance shaping factors can be modified or task structures or procedures changed to reduce the error probability.

Time reliability correlation:
The time reliability correlation has many variants since its first development. Essentially is that the time reliability correlation model assumes that in diagnostic tasks the probability of non response in an emergency situation is greatly influenced by the time available for diagnosis. Recent variants of the time reliability correlation have allowed other performance shaping factors to have some effects on the human error probabilities. The time reliability correlation has the advantage that it can be integrated easily with other engineering based assessments of transient behaviour and modelling. In figure 14.4 an example is presented of a time reliability curve. Three lines are plotted; the 5th percentile lower bound, the mean value and the 95th percentile upper bound. In reference [14.16] the formulas to describe the three plotted lines are derived, these formulas are:

Mean value:

$$\mathrm{HEP}(t) = \Phi\left[\frac{-\ln\left(\frac{t}{m}\right)}{\sqrt{\sigma_r^2 = \sigma_u^2}}\right] \qquad (14.2)$$

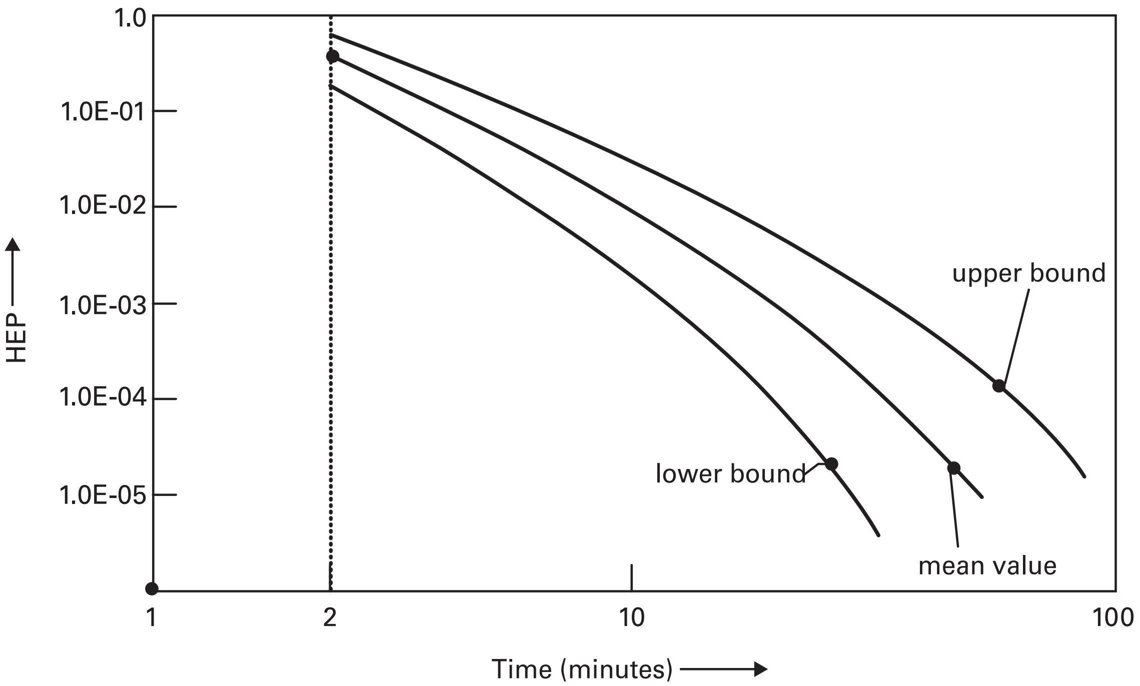


Figure 14.4: Typical example of a time reliability correlation.

Lower bound:

$$HEP(t)_{0.05} = \Phi\left[\frac{-\ln\left(\frac{t}{m}\right) - 1.645\ \sigma_u}{\sigma_r}\right] \tag{14.3}$$

Upper bound:

$$HEP(t)_{0.95} = \Phi\left[\frac{-\ln\left(\frac{t}{m}\right) - 1.645\ \sigma_u}{\sigma_r}\right] \tag{14.4}$$

where:

HEP(t) = mean human failure event probability within period t
Φ = the standard normal cumulative distribution
t = available response time
m = median response time
f_r = randomness error factor

(14.5)

σ_r = logarithmic standard deviation for randomness $= \dfrac{\ln(f_r)}{1.645}$
f_u = uncertainty error factor
σ_u = logarithmic standard deviation for uncertainty = $\dfrac{\ln(f_u)}{1.645}$

To calibrate the time reliability correlation three parameters have to be estimated; the median response time (m), the randomness error factor (fr) and the uncertainty factor (f_u). Calibration of the time reliability correlation has to be done by calibration of the formula against human failure data based on simulator training of operators or based on generic data. In reference [14.16] chapter 10 details are provided to perform such calibration.

Modified SLIM-based approach:
In this chapter an adaptation of the SLIM method will be described. The original SLIM method (see reference [14.17] is based on the following assumptions:

- The probability of operator error in a particular situation depends on the combined effects of a set of performance shaping factors that influence the operator's ability to accomplish the action successfully
- Analysts have to address each of these performance shaping factors independently so that the overall evaluation can be expressed as the sum of the results of each PSF to form a numerical success likelihood index
- The actual quantitative error rate is related to the numerical success likelihood index by a logarithmic relationship
- The logarithmic relationship is calibrated, on a situational basis, by using appropriately selected calibration tasks having generally accepted error rates.

The original SLIM method has been modified so that the analysts scale the degree of difficulty, rather than the potential for success, when they score the action. This change in orientation produces a failure likelihood index (FLI) rather than a success likelihood index (SLI). This approach has the advantage of quantitatively highlighting the causes of operator difficulty. A high score combined with a high weight produces a large FLI compared to other ratings. This permits efficient analysis of the potential problem areas and trends.

The performance shaping factors mostly selected in the modified SLIM approach are:

- plant interface and indications of conditions
- ignificant preceding and concurrent actions
- task complexity
- procedural guidance
- training and experience
- adequacy of time to accomplish action
- stress.

All performance shaping factors are rated against two criteria:

- A **score** related to the degree to which the conditions of performance shaping factors help or hinder the operator performing the action
- A **weight** related to the relative influence of each PSF on the probability of the success of the action.

The failure likelihood index (FLI) is calculated based on the relative importance and numerical rating of each performance shaping factor.

The quantification process is done in a series of stages. First, a normalized weight for each PSF is obtained by dividing the weight assigned by the evaluation team by the total of all of the weights for that particular action. The FLI is calculated by multiplying the normalized weight of the PSF by its score and adding that result to similar results for the other performance shaping factors:

$$\mathrm{FLI} = \sum w_i \, . \, S_i \tag{14.6}$$

where

i = PSF that has an influence on the error rate of the action.
HEP = human error probability
FLI = failure likelihood index
w_i = relative importance of performance shaping factor i, ($\sum w_i = 1$)
S_i = numerical rating or degree-of-difficulty score for performance shaping factor i
A,B = calibration constants

The human error probability (HEP) is related to the failure likelihood index (FLI) according to the following formula:

$$\mathrm{Log}\,(\mathrm{HEP}) = A + B \, . \, (\mathrm{FLI}) \tag{14.7}$$

The coefficients A and B of the correlation can be obtained from a least-squares fit of the FLI of a selected set of calibration actions with known human error probabilities.

For the calibration process well defined actions have to be used, obtained from evaluations for other risk analyses and other statistical or analytical evidence of failure probabilities for these actions. The calibration procedure should ensure that the numerical error probability estimates are realistic and consistent with available data, observed human behaviour and results from comparable expert evaluations of similar activities.

The evaluation of dynamic human errors with the modified SLIM-based approach has to be made consistent by the development of a set of forms and instructions to explain the rating procedures for the performance shaping factors. During development of these instructions one has to be sure that the independente of the performance shaping factors is maintained.

It is important to recognize that the quantification of human error rates is only a small portion of the information obtained from the modified SLIM approach. The trends of weights and scores provide much valuable information regarding the evaluator’s judgment with respect to the focus of safety-related actions and the difficulties involved in accomplishing them.

Recommendation of quantification technique:
In table 14.7 the recommended human error quantification techniques have been given for each type of human failure.

Table 14.7: Recommended quantification technique.

Type of human failure	**Quantification technique**
Pre-initiator human errors	THERP
Human-induced initiators	Plant specific
Dynamic operator actions	Modified SLIM or TRC
Recovery actions	Modified SLIM or TRC

14.5.3 **Human error consequence analysis**

The objective of consequence analysis is to evaluate the safety consequence to the system of any human errors that may occur. In order to address this issue, it is necessary to consider the nature of the consequente of human failures in detail. At least three types of consequences are possible after occurrence of a human failure:

- The overall objective of the task is not achieved
- In addition to the task not achieving its intended objective, some other undesired consequences might occur due to misdiagnosis
- The intended objective is achieved but some other undesired consequence occurs, which may even be associated with another system, unrelated to the primary task.

Risk assessment has focused mostly on the first type of failure, but a comprehensive consequence analysis has to consider other types of consequences as well, because all possible outcomes could be sources of risk to the plant.

14.5.4 **Recovery analysis**

Each accident sequence minimal cut set represents one possible way in which the sequence may occur. The information available to the operator and the recovery action to be taken generally depends on the combination of events that have occurred and hence on the particular minimal cut set.

Therefore, recovery actions are generally considered at the minimal cut set level rather than at the accident sequence level. Since there may be a large number of minimal cut sets for an accident sequence, it may be necessary to consider recovery actions for only the most significant minimal cut sets.

A probability of non-recovery is estimated for each minimal cut set that is recoverable by some operator recovery action. The probability of occurrence of the minimal cut set is then multiplied by its probability of non-recovery to estimate the final minimal cut set probability of occurrence with recovery. The final estimated probability of occurrence for an accident sequence is computed using these minimal cut set probabilities of occurrences with recovery.

The primary events of a particular accident sequence minimal cut set may or may not be recoverable by routine recovery actions. Extraordinary recovery actions are not considered, but routine recovery actions are. For example, the overhaul of a pump is not considered, but the manual realignment of a valve, whether by a hand switch in the control room or by local turning, is. If a primary event can be recovered by a routine recovery action, the location of the recovery action is determined.

In general, recovery actions can be separated into those that can be accomplished from the control room and those that can only be performed locally. If recovery can only be performed locally and the local site is inaccessible, the primary event is considered non-recoverable.

Once a primary event is deemed recoverable and the location of the recovery action is determined, a critical time for the recovery action is estimated. Two types of critical times are considered when determining the critical time for a recovery action. The primary event itself can have a critical recovery period which is independent of the accident sequence or of the state of the process in an accident sequence. An example of this type of primary event critical time is that associated with the lubricating oil cooling for a pump. If the primary event is the loss of such cooling, there is a definite time interval during which the pump can operate without the cooling, and this time interval defines the critical time for the recovery of the primary event.

For the second case, the time in which a mitigatory action can be carried out is considered. In general, the accident sequences can be combined into groups, with each group having its own set of critical times.

When both types of critical times are applicable for a particular recovery action, the shortest critical time is used.

After the critical times and locations of the possible recovery actions are established, the probability of recovery is estimated for each recovery action. The probability of non-recovery is one minus the probability of recovery. If a primary event is not recoverable, its probability of recovery is zero and its probability of non-recovery is one.

Table 14.8 is an example of a simple generic recovery model for which the probability of recovery and non-recovery is a function of the critical time and location of the recovery action. Suppose that the available time to perform a recovery action after failure of a component or a system is 18 minutes (critical time for recovery). If this recovery action can be performed in the control room, the probability of non-recovery in accordance with table 14.8 is 0.1. If recovery is also possible outside the control room, the probability of non-recovery is 0.25, see table 14.8 last column. If recovery is possible both in and out the control room, the probability of non-recovery used in the analysis should be the smaller one, viz. 0.1 in this example.

Table 14.8: Probabilities of recovery and non-recovery (IAEA PSA Guide).

Critical time for recovery action		Recovery probability	Non-recovery probability
In control room	Locally		
(min)	(min)		
< 5	< 15	0.00	1.00
5-10	15-20	0.75	0.25
10 - 20	20 - 30	0.90	0.10
20 - 30	30 - 40	0.95	0.05
30 - 60	40 - 70	0.97	0.03
< 60	> 70	0.99	0.01

Table 14.8 was developed from a simplified human reliability model that accounted for two important factors in estimating recovery and non-recovery probabilities:

- Time available to perform a recovery action
- Location in which the recovery action takes place.

More recent models of human actions include other factors; for example, the modified SLIM method (see section 14.5.2) includes as variables the conditions of the work under which the action must be accomplished, the requirements of the task itself and the psychological and cognitive condition of the operators.

For most minimal cut sets, recovery of a single primary event of the minimal cut set will restore the sequence to success (no core damage). For these minimal cut sets, the frequency of the minimal cut set is multiplied by the probability of non-recovery to estimate the final frequency of the minimal cut set with recovery. Recovery of more than one primary event in a cut set should be avoided.

If the non-recovery probability due to human error is very small, one has to consider the probability of non-recovery due to hardware failures.

14.5.5 Assessment of dependencies

It is important to realize that in case of multiple human error events, all events except the first one represent conditional events of success and failure. Dependence between events directly affects the probability of occurrence of the conditional probabilities. Some cases of dependence will be spotted during discussions with the plant personnel. During plant visits special attention has to be given to equipment similarities that contribute to the level of dependence between actions performed on similar equipment.

Dependencies can occur between two performances with respect to errors of omission, errors of commission, or both. If a dependence is assessed due to the fact that two actions are called for in the same procedural step, dependence is likely to affect human error probability for errors of omission. If components are to be manipulated at different times in a given procedure, the dependence may affect the human error probability for errors of commission, especially for selection errors.

To incorporate the effect of dependence in the calculation of a sequence of human errors one can apply the dependency model of Swain and Goodmann. Consider a sequence of two human errors:

Sequence of human errors: HE1 * HE2

The human failure probability of the first human error is equal to P1. The independent human failure probability of the second human error is equal to P2. The equations for the conditional human failure probability for the second human error, given the occurrence of the first human failure, are as follows:

Zero dependence: $(P2)_{\text{Conditional}} = P2$

Low dependence: $(P2)_{\text{Conditional}} = (\ 1.0 + 19.0 * P2\ ) / 20.0$

Moderate dependence: $(P2)_{\text{Conditional}} = (\ 1.0 + 6.0 * P2\ ) / 7.0$

High dependence: $(P2)_{\text{Conditional}} = (\ 1.0 + P2\ ) / 2.0$

Complete dependence: $(P2)_{\text{Conditional}} = 1.0$

These equations reflect dependencies among tasks by one person performing operations on more than one component.

14.6 ORGANIZATIONAL AND MANAGEMENT INFLUENCE FACTORS

A lot of research is going on to evaluate human failure probability as a function of the complex network of organizational influences that impact upon these probabilities. One of the analysis techniques to determine the organizational influence is the influence diagram approach. The purpose of an influence diagram is to represent the effects of not only the direct influences of factors such as procedures, training, and equipment design on error probability, but also of the organizational influences and policy variables affecting these direct factors.

The development of an influence diagram starts with the identification of the interactions between indirect and direct performance shaping factors that determine human failure probabilities. The influence diagram is then constructed in accordance with the identified interactions. Once the influence diagram has been developed, the current status of the lowest level factors (for instance, project management and feedback from operational experience) has to be assessed. The assessment made is the probability that the factor being considered is positive or negative in its contribution to error. This evaluation is performed on all the bottom-level influences in the influence diagram. Once these individual factors have been evaluated, the next stage is to evaluate the combined effects of the lowest-level influences on higher-level influences, as specified by the structure of the influence diagram. This process is repeated for combinations of these variables on the factors that directly impact on the probability of success or failure for the scenario being evaluated. These numerical assessments are combined to give weights which are then used to modify the unconditional human failure probabilities that the failure wilt occur, given the various positive or negative combinations of the influences assessed earlier. The unconditional human failure probability has to be determined using another technique, as described in section 14.5.2.

Important direct performance shaping factors are:
- Quality of training
- Availability of effective operating instructions
- Time pressure.

Important indirect performance shaping factors are:
- Feedback from operational experience
- Use of task analysis
- Policy for generating instructions
- Staffing levels
- Task complexity
- Assignment of job roles
- Project management.

For more details, see the CCPS Guidelines, reference [14.20] and [14.26].

For incorporating organizational factors into a traditional quantitative risk analysis approach, event trees and fault trees, see Davoudian. The approach presented here has to be considered as a first step to incorporating organizational factors into a quantitative risk analysis.

14.6.1 **INPO Human performance enhancement system**

The human performance enhancement system (HPES) is a technique used to determine the root causes of events or incidents that occur at an installation. The result of personnel performance is portrayed in the events or incidents that occur at an installation. The root cause of technical and non-technical events always leads back to people. The management of an installation is required to set up an organization with suitable personnel, comprehensive instructions and procedures in order to prevent events or incidents occurring at an installation. An assumption of the method is that all personnel attempt to complete their tasks as well as they can under the circumstances. The HPES method does not place the blame for events or incidents on the employee, but on the management. If deviant behaviour does occur, management should have ensured that the problem was identified before the person caused the event or incident. The term ”human error” is also avoided as it is too negative, and the term ”inappropriate action” is used instead.

The HPES considers all causal factors at an installation that are within the control of management. By addressing the human performance problems at an installation, the number of events or incidents should decrease. Recurring problems should decrease due to corrective measures addressing true causes of inappropriate performance instead of treating symptoms.

For technical problems the HPES method has defined appropriate causal factors, that should have been in place to prevent the occurrence of the event. There is one category for influences outside the control of management.

The causal factors considered by the HPES method for human performance problems are as follows:

- Verbal communication
- Written communication
- Interface design or equipment condition
- Environmental conditions
- Work schedule
- Work practices
- Work organization and planning
- Supervisory methods
- Training and qualification
- Change management
- Resource management
- Managerial methods.

The causal factors considered by the HPES method for technical problems are as follows

- Design configuration and analysis
- Equipment specification, manufacture and construction
- Maintenance and testing
- Plant and system operation
- External influences.

The objective of an HPES is to improve plant performance by reducing the number of failure events. This also applies to the reduction of human failure events.

In the HPES technique the smalt, unimportant events and near misses are investigated as well. The fact that a near miss occurs requires investigation because the event may occur again in less favorable conditions and cause a serious incident. The causal factors resulting in serious incidents are also present in the near misses.

14.7 HUMAN ERROR REDUCTION ANALYSIS TECHNIQUES

The first step in a human error reduction analysis is to identify the dominant contributors to the calculated human error probabilities. This is mostly done by performing a sensitivity analysis. After identification of the dominant contributors, the following error reduction approaches can be used:

Reduction of operator involvement:
The involvement of the operator can be reduced by automation of the process or by additional safeguarding equipment.

Error pathway blocking:
The system can be re-designed in such a way that the error can no longer occur. In general this will include some hardware or software changes. Error pathway blocking usually requires functional reorganization and can even lead to alteration of the process at a fundamental level. Such changes require an investigation that does not simply lead to new maintenance or operational errors.

Performance shaping factor error reduction:
In most important quantification techniques performance shaping factors are used to calculate the human error probability. These performance shaping factors can be reviewed to identify which performance shaping factor appear most important in the quantification process. Once identified, the analyst has to propose a modification in such a way that the performance shaping factor can be reduced.

Increasing predictability:
Increasing the ability of the operator to anticipate problems is a useful additional recovery mechanism and may involve the implementation of predictor display, early alarms, trend displays, etc.

Enhancing detectability:
Detectability of situations can be increased in two main ways:
- Enhancing detection of an abnormality.
- Enhancing diagnosis of what the abnormality is. This can be achieved by hazard identification training prior to processing of information.

Both methods allow the operator to effectively detect the event earlier.

Increasing controllability:
Increasing the power which operators have to recover systems, e.g. avoidance of system dynamics designs where failure is sudden and catastrophic and essentially non-recoverable. The use of buffers in the process cycle to render systems less tightly coupled etc. makes systems more controllable.

Increasing competence:
Increasing the competente and confidence of operators to react to and control process deviations can be achieved by training, in particular simulator training.

Identification of error reduction measures is not enough to reduce the probability of human errors. Implementing and maintaining these error reduction measures might be difficult. Implementation can be difficult for the following reasons:
- New training is required
- It is possible that responsibilities and perceived autonomy will shift, possibly in a direction they do not desire
- Lack of consultation of the personnel affected may involve feelings of distrust and resentment etc.

A solution to this problem can be to follow a systems approach. A systems approach simply converts any error reduction mechanism into an error reduction strategy, which affects other human performance areas as well as the one which is the focus of the mechanism. For example, changing of a display as an error reduction measure must also affect training and procedures systems.

The easiest way to achieve this systems approach to error reduction is to involve operators from the start, even to the eitent of their involvement in the human reliability analysis itself.

14.8 JOB AIDS AND PROCEDURES

To improve operator performance, job aids can be considered. Job aids can consist of flowcharts, checklists, decision tables, standard operating instructions and emergency procedures. Providing job aids will not automatically improve operator performance. Common problems with job aids are:

- Procedures do not correspond to the way the job is actually done
- The information contained in procedures is correct, but is not put in a form usable by the individual at his or her workplace
- The distinction between procedures as regulatory standards and as instructions to perform a task is not adequately made
- Rules and procedures are not considered as applicable to the individuals or the situation in question
- The user of the procedures does not understand the underlying reasoning behind them and therefore carries out alternative actions that appear to achieve the same purpose but are easier to perform.

Criteria for selecting job aids are:

Flowcharts:
Flowchart and decision tables offer a concise organization of the information and job criteria required to perform fault diagnosis and planning tasks

Checklists:
Checklists can be used for tasks which involve remembering sequences of steps

Procedures:
Procedures provide step-by-step directions on how and when to perform various tasks involving stringent memory requirements, calculations, accuracy and difficult decisions.

Operating instructions:
Standard operating instructions are usually provided for critical tasks involving changes in the plant operating conditions such as plant start-up or shutdown.

Emergency procedures:
Emergency procedures are provided for tasks involving diagnosing plant or instrumentation failures and stabilizing and recovering abnormal plant conditions.

To select the most appropriate method to support the process worker, one needs to consider the characteristics of the task and the type of support to be provided. In general job aids and procedures are useful for tasks:

- which are performed rarely
- which require complex logic
- which involve following long and complex action sequences and for which reference to printed instructions is not disruptive.

Training should be performed for tasks which are:

- performed frequently
- require complex manual skills
- involve unforeseen plant conditions

Clarity of instructions:
Clarity of instructions is very important. Four ways of improving the comprehensibility of technical instructions are:
- Avoid the use of more than one action in each step of the procedure
- Use language that is concise but comprehensive to the users
- Use the active voice (Motate switch” instead of the ”switch should be rotated”)
- Avoid complex sentences containing more than one negative.

14.9 EXAMPLE

14.9.1 Familiarization

In figure 14.5 the lay-out of a electrical distribution system is given. The main bus-bars A1 and A2 are fed by the grid. The emergency bus-bar B1 is fed by main bus-bar A1 and emergency bus-bar B2 is fed by main bus-bar A2. If the power supply of a main bus-bar to an emergency bus-bar fails, the power supply to the emergency bus-bar is restored by a diesel generator. Each emergency bus-bar (B1 and B2) has a separate diesel generator. If a grid failure occurs, both bus-bars A1 and A2 are out of service and both emergency bus-bars B1 and B2 have to be fed by the diesel generators DG1 and DG2.

After recovery of the grid the feed of the main bus-bars to the emergency bus-bars has to be restored. This is done by an synchronization device that has to be activated by the operator. The operator has to activate the synchronization device of bus-bar B1 first by pressing a button. After activation of synchronization of bus-bar B1 he has to wait until the position indicator of breaker S1 indicates a closed position and the position indicator of breaker S2 an open position. After successful completion of the restoration of bus-bar B1 the operator continuous with the restoration of bus-bar B2 by activation of the synchronization device of bus-bar B2. If the restoration of bus-bar B1 is not successful the operator has the stop the restoration process and has to ask for assistance from the maintenance department. Failure of the synchronization device implies that the power supply to the emergency bus-bar is stopped.

A written procedure is available to perform an automatic synchronization of both bus-bars. However, in practice this procedure is not used because it is normally a simple step-by-step task that is performed from memory.

The question of interest is the probability of failure of the power supply to both emergency bus-bars.

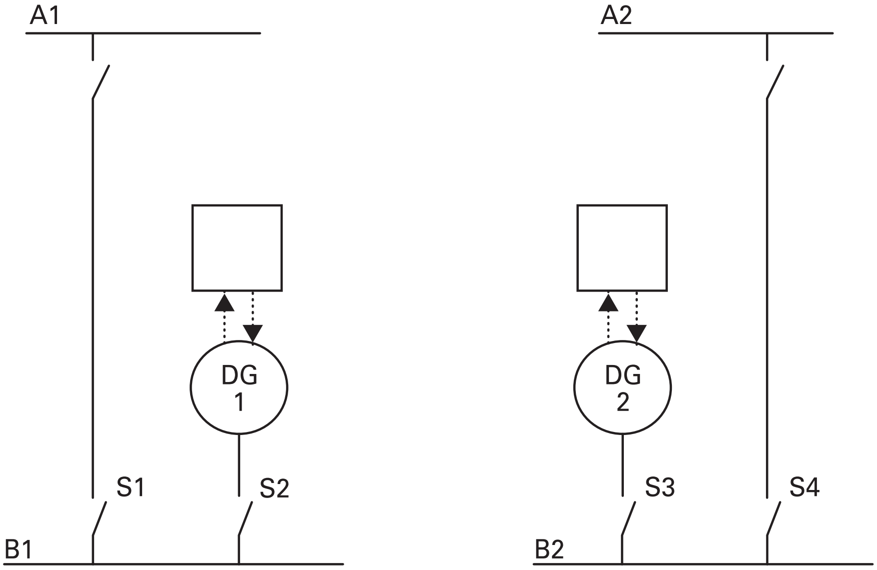


Figure 14.5: Lay-out of the power supply to two emergency bus-bars

14.9.2 **Qualitative analysis**

Task analysis:

The first step of the analysis is to identify the human actions and equipment failures that can lead to the failure of the power supply to both bus-bars. After review of the procedures and the performance of a plant visit, the following tasks could be identified:

Step 1:
Start automatic synchronization of bus-bar B1 by activating the synchronization device of bus-bar B1.

Step 2:
The operator has to wait until the synchronization process of bus-bar B1 is completed.

Step 3:
After completion of the synchronization of bus-bar B1 the operator has to check the positions of the breakers S1 and S2. Breaker S1 must be in the closed position and breaker S2 must be in the open position.

Step 4:
If the synchronization process is not successfully completed the operator has to stop the synchronization procedure and to ask for assistance of the maintenance department.

Step 5:
After successful completion of the synchronization process of bus-bar B1 the operator has to start the automatic synchronization device of bus-bar B2.

Step 6:
The operator has to wait until the synchronization of bus-bar B2 is completed and has to check whether the synchronization was successful or not.

Identification and classification of potential human errors:
Only error of omission are considered in this example.The following potential errors of omission are identified:

A: No execution of the synchronization process.

B: The operator does not wait until the synchronization of bus-bar B1 is completed.

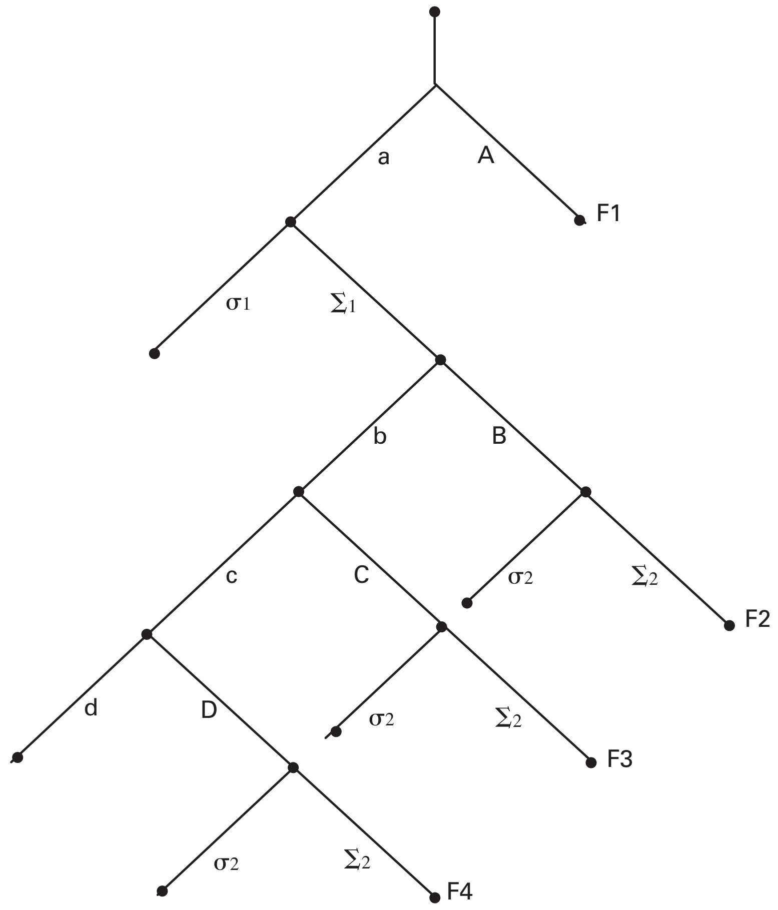
C: The operator does not check the position of the breakers S1 and S2 after completion of the synchronization process of bus-bar B1.

D: The operator does not stop the synchronization process after failure of the synchronization of bus-bar B1.

Other potential errors of omission can be identified but are not important in relation to failure of both bus-bars B1 and B2.

Human error event tree:
Taking into account all potential errors identified a human error event tree for improper restoration of both bus-bars can be constructed. (see figure 14.6). All potential human errors are represented by capital letters. Technical failure of the synchronization device is represented by capital Greek letters.

Inspection of the HRA event tree shows that three failure sequences (F2, F3 and F4) can lead to unavailability of both emergency bus-bars.



A : No execution of procedure.
B : Operator does not wait.
C : Operator does not perform the check.
D : Operator does not stop.
∑1 : Technical failure synchronization bus-bar B1.
∑2 : Technical failure synchronization bus-bar B2.

Figure 14.6: HRA Event Tree for improper synchronization of both emergency bus-bars.

14.9.3 **Quantification**

To generate a quantitative result the analyst must estimate the probability of each failure or error included in the HRA event tree. Data for all the human failures and errors are available in tables in the handbook, Swain and Guttman (1983). The analyst must modify these data as necessary to account for specific characteristics of the work situation, such as stress levels, equipment design features.

Expierence shows that the failure probability of the automatic synchronization device is equal to 0.1 per demand. This figure is applicable for failures which lead to loss of the power supply to the bus-bar in consideration.

Table 14.9 summarizes the data used in this problem. From table 20-11 (8) (see reference [14.13]) it can be concluded that misinterpretation of the status lamp indicators is negligible.

Table 14.9: Events included in the HRA event tree.

Failure symbol	Failure description	Estimated HEP	Data source
A	No execution of procedure	0.001	Table 20-8 (1)
$\sum_1$	Failure of synchronization device bus-bar B1	0.1	Field data
B	Operator does not wait	0.05	Table 20-7 (5)
$\sum_2$	Failure of synchronization device bus-bar B1	0.1	Field data
C	Operator does not perform the check	0.05	Table 20-7 (5)
D	Operator does not stop	0.05	Table 20-7 (5)

After completion of table 14.9 the analyst can calculate the total probability of failure of both bus-bars given a demand for synchronization. The probabilities of a specific path is calculated by multiplying the probabilities of each success and failure limb in that path. Table 14.10 summarizes the calculations of the HRA results, which are normally rounded to one significant digit after the intermediate calculations are completed.

Table 14.10: Human reliability analysis results.

Sequence	Probability of failure given a demand
F2 = a $\sum_1$ B $\sum_2$	0.0005
F2 = a $\sum_1$ b C $\sum_2$	0.00047
F2 = a $\sum_1$ b c D $\sum_2$	0.00045
Ftotal = F2 + F3 + F4	0.001

The probability of failure of both emergency bus-bars, given a demand for synchronization is equal to 0.001. Improvements can be achieved by training of the operators to use the written procedures.

14.10 REFERENCES

General:

[14.1] Human reliability assessment, A two day course,
Organized by IBC Technical Services Ltd.
The London Press Centre- London, 9th/10th September 1986.

[14.2] CCPS Guidelines, Guidelines for preventing human errors in process safety, Center for Chemical Process Safety of the American Institute of Chemical Engineers. New York.

[14.3] Reason, J, Human error,Cambridge University Press, 1990

[14.4] Heslinga, G, Technique for Human Error Sequence Identification and Signification, Thesis University of Delft, December 1988.

Procedural framework:

[14.5] Bell, B.J., Swain, A.D, A procedure for conducting a human reliability analysis for nuclear power plants, Final report, NUREG/CR-2254, SAND81-1655 RX,AN

Task analysis:

[14.6] Kirwan, B, 1992, and Ainsworth, L.K, A Guide to Task Analysis,
Taylor & Francis Inc., 1992.

Identification of potential human errors:

[14.7] Kirwan, B, 1992, Human error identification in human reliability assessment. Part 1: Overview of approaches. Applied Ergonomics 1992, 23(5), 299-318.

[14.8] Kirwan, B, 1992, Human error identification in human reliability assessment. Part 2: Detailed comparison of techniques. Applied Ergonomics 1992, 23(6), 371-381.

[14.9] Whalley, S.P, Minimizing the cause of human error, 10th Advances in Reliability Technology Symposium Elsevier (1988).

[14.10] Embry, D.E, SHERPA: a systematic human error reduction and prediction approach, Paper presented at the international topical meeting on advances in human factors in nuclear power systems, Knoxville, Tennessee, April 1986.

[14.11] Macwan, A, Mosleh, A, A methodology for modeling operator errors of commission in probabilistic risk assessment, Reliability Engineering and System Safety 45 (1994), pages 139-157.

Quantification of human failures:

[14.12] SRD, Human reliability assessors guide, RTS 88/95Q,
P. Humphreys, October 1988.

[14.13] Swain, A.D, 19834 Guttmann, H.E, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Washington,D.C: US Nuclear Regulatory Commission, 1983.

[14.14] IAEA PSA Guide, Procedures for conducting probabilistic safety assessments of nuclear power plants (Level 1), Safety series No. 50-P-4, International atomic energy agency, Vienna, 1992, ISBN 92-0-102392-8.

[14.15] IAEA PSA Guide, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Safety series No. 50-P-10, International atomic energy agency, Vienna, 1992, ISBN 92-0-103395-8.

[14.16] E.M. Dougherty, Jr. and J.R. Fragola, Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications, Wiley Interscience, 1988, ISBN 0 471-60614-6.

[14.17] P.C. Cacciabue, Evaluation of human factors and man-machnie problems in the safety of nuclear power plants, Nuclear Engineering and Design 109 (1988) 417-431, North-Holland, Amsterdam.

[14.18] Williams, J.C, HEART - A Proposed Method for Assessing and Reducing Human Error. In procedings of the 9th Advances in Reliability Technology Symposium, University of Bradford, 4 April 1986, Published by NCSR, UKAEA, Culcheth, Cheshire.

Human reliability data collection:

[14.19] Kletz,T.A, and Whitaker, G.D, 1973, Human Error and Plant Operation, Note EDN 4099, Petrochemicals Div., ICI Ltd.

Organizational and management influence factors:

[14.20] Safety Management Systems in the Process industry, Institute for system engineering and informatics, Proceedings CEC Seminar on 7/8 October, 1993, Ravella (SA), Italy, Joint Research Centre European Commission, Report EUR 15743 EN, ISBN 92-826-8223-4.

[14.21] The influence of organization and management on the safety of NPPS and other complex industrial systems, International institute for applied System Analysis, WP-91-28, July 1991, Laxenburg, Austria

[14.22] Root cause analysis, Institute of Nuclear Plant Operators, INPO-90-004

[14.23] Phillips, L.D, Embrey, D.E, Humphreys, P,& Selby, D.L,
A sociotechnical approach to assessing human reliability. In R.M. Oliver & J.A. Smith (Eds.), Influence diagrams, Belief Nets and Decision Making: their Influence on Safety and Reliability, New York, Wiley.

[14.24] Davoudian, K, Wu, Jya-Syin, Apostolakis, G, Incorporating organizational factors into risk assessment through the analysis of work processes, Reliability Engineeering and System Safety 45 (1994), pp 85-105

[14.25] United Kingdom Atomic Authority (1991), Long Guide to Reducing Human Error in Process Operations, Warrington, UK: AEA Technology Ltd.

[14.26] Auditing and Safety Management for Safe Operation and Land Use Planning: A cross-national comparison and validation exercise, A Report for the Commission of the European Comminities, Contract EV5V-CT92-0068 Environmental Programme, 20 December 1995.

APPENDIX 14-A: HUMAN RELIABILITY PROBABILITY DATA COLLECTION

Table 14-A-1: HEART unreliability values (reference [14.18])

Task	Description of task	Proposed HEP	Bounds (5th - 95th)
A	Totally unfamiliar, performed at speed with no real idea of likely consequences.	0.55	0.35-0.97
B	Shift or restore system to a new original state on a single attempt without supervision or procedure.	0.26	0.14-0.42
C	Complex task requiring high level of comprehension and skill.	0.16	0.12-0.28
D	Fairly simple task performed rapidly or given scant attention.	0.09	0.06-0.13
E	Routine, highly-practiced, rapid task involving relatively low level of skill.	0.02	0.007 - 0.045
F	Restore or shift a system to original or new state following procedures, with some checking.	0.003	0.0008 - 0.007
G	Completely familiar, well designed, highly practiced, routine task occurring several times per hour, performed to highest possible standards by highly motivated, highly trained and experienced person, totally aware of implications of failure, with time to correct potential error, but without the benefit of significant job aids.	0.0004	0.00008 - 0.009
H	Response correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state.	0.00002	0.000006-0.0009
M	Miscellaneous task for which no description can be found.	0.03	0.008-0.11

Table 14-A-2: Operator error estimates (Kletz)

No.	Description	HEP
1	Omission or incorrect execution of step in a familiar startup routine	0.001
2	Failure to respond to audible alarm in quiet control room by pressing single button	0.001
3	Failure to respond to auditable alarm in quiet control room by some more complex action such as going outside and selecting correct valve among many	0.01
4	Failure to respond to audible alarm in busy control room within 10 minutes	0.1
5	Failure to carry out rapid and complex actions to avoid serious incident such as an explosion	0.5

Table 14-A-3: THERP Estimated HEP's related to failure of administrative control.

No	Description	HEP	EF
1	Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals.	0.01	5
2	Initiate a scheduled shiftly checking or inspection function.	0.001	3
3	Use written operations procedures under normal operating conditions.	0.01	3
4	Use written operations procedures under abnormal operating conditions.	0.005	10
5	Use a valve change list or restoration list.	0.01	3
6	Use written test or calibration procedure.	0.05	5
7	Use written maintenance procedures.	0.3	5
8	Use a checklist properly.	0.5	5

UNCERTAINTY, IMPORTANCE AND SENSITIVITY ANALYSIS OF INPUT PARAMETERS FOR FAULT TREES

CONTENTS:

15.1 INTRODUCTION

Any probabilistic risk assessment or probabilistic reliability assessment established to gain insight in the risk or reliability associated with a particular plant consists of a variety of assumptions, simplifications, idealizations and conservatisms which can not be avoided. This means that the risk or reliability model is a model of reality but that any result of a risk or reliability model will, of course, be uncertain. This seems to be a trivial statement but it is an important issue to consider. People understanding this basic feature of a risk or reliability model might ask: "What is the impact of this uncertainty on the usefulness of the safety analysis?".

The objective of an uncertainty, importance and sensitivity analysis is to address the following type of questions:

- Which factors or parameters are the largest contributions to the overall risk?
- How sensitive is the resulting undesired event probability to for example an estimated human error probability?
- What is the effect of parameter uncertainty on the overall risk result?

The objective of an importance analysis is to determine the importance of contributors to the calculated risk, accident sequence frequency or system unavailability. The objective of a sensitivity analysis is to determine the sensitivity of the risk analysis results to input assumptions, models and failure data. In analyzing both importance and sensitivity, particular for basic events, it should be recognized that the two are related. Basic events which have a high calculated importance initially wilt also display a high sensitivity.

The objective of an uncertainty analysis is to provide qualitative discussion and quantitative measures of the uncertainties in the results of a risk or reliability analysis. Sources of uncertainties present in a risk or reliability analysis are traditionally categorized in three groups:

1. Completeness.
2. System Modeling adequacy.
3. Input Parameter Uncertainty.

Uncertainty due to completeness is difficult to assess or quantify. Completeness depends on a structured approach towards fault tree construction, a correct definition of objective, scope, system boundaries, failure scenario identification etc.

Uncertainty due to system modeling adequacy can be partly assessed by closer assessment of those cut sets that contribute most to the top event. Additional numerical calculations or more detailed analyses can be performed. The modeling adequacy introduced by the selected maximum cut set order can be assessed by recalculating the fault tree model for a higher cut set order, as far as the capacity of computer and codes allows this. The modeling uncertainty associated with the conceptual models used often cannot be avoided and can generally not be quantified as such.

The third source of uncertainty, input parameter uncertainty is the main focus of this document.

The theory presented in this chapter relates to fault tree analyses. But the same type of techniques can be made available for Markov processes and event tree analyses.

15.2 NOMENCLATURE

			Dimension
λ	-	failure rate	-/hour
τ	-	test duration	hour
θ	-	repair duration	hour
a,b	-	constants	-
E	-	basic event	-
Q	-	probability of failure per demand	-
P	-	probability	-
U	-	time average unavailability	-
T	-	test period	hour
EF	-	Error Factor	-
RAW	-	Risk Achievement Worth	-
RRW	-	Risk Reduction Worth	-
MTTF	-	mean time to failure	hour
MDT	-	mean down time	hour

<u>Subscript</u>

top	-	top event
FV	-	Fussel Vesely
B	-	Birnbaum

15.3 UNCERTAINTY ANALYSIS

15.3.1 Introduction

Uncertainty analysis is an important task of a risk analysis. it should be emphasized that the uncertainties associated with the ways in which undesired consequence might occur pertain regardless of whether or not a risk analysis is performed for the plant. It is one of the main advantages of a risk analysis that it can identify a number of sources of this uncertainty and quantify and describe a substantial part of it.

Since the risk and reliability models attempt to simulate reality, it is inevitable that there will be simplifying assumptions and idealizations of rather complex processes and phenomena. These simplifications and idealizations will generate uncertainties. One can distinguish three major catego-ries of sources of uncertainties in these models.

1: *Completeness.*
The main thrust of the risk or reliability model is to assess the possible scenarios (sequences of events) that can lead to undesirable consequences. However, there is no guarantee that this process can ever be complete and that all possible scenarios have been identified and properly assessed. This lack of completeness introduces an uncertainty in the results and conclusions of the analysis that is difficult to assess or quantify.

2: *System Modelling adequacy.*
Even for those scenarios that have been identified, the event sequence and system logic models do not precisely represent reality. There are uncertainties introduced by the relative inadequacy of the conceptual models, the mathematical models, the numerical approxima-tions, the coding errors and the computational limits. These uncertainties are discussed as part of the uncertainty analysis in the risk analysis, and sensitivity studies are usually performed to assess their relative importance.

3: *Input parameter uncertainties.*
The parameters of the various models used in the risk analysis are not exactly known because of scarcity or lack of data, variability within the populations of plants and/or components, and assumptions made by experts. Input parameter uncertainties are the uncertainties that are at present most readily quantifiable.

The third source of uncertainty is the main focus of this chapter. In the succeeding sections, the importance and sensitivity analyses are described. These analyses concentrate on the hypothetical deviation of a single parameter, analysing the effect on the calculated overall undesired event frequency. There is no correlation made with possible deviations of other parameters at the same time. Moreover, no statement is made on the probability of such deviations towards higher or lower values.

An uncertainty analysis is carried out by assessing the possible ranges of the estimated parameters in the risk analysis. For each of these uncertain parameters, a distribution is established describing which values are most likely and which values are less likely. The overall undesired event frequency is then expressed as a function of the uncertainty distributions of the parameters, resulting in an uncertainty distribution for the overall undesired event frequency.

The quantification of the third category of uncertainties, input parameter uncertainties, is usually done by considering a risk analysis result (e.g. undesired event frequency) as the output of a model which has as inputs parameters that are characterized as random variables.The probability distribution function assumed for each parameter then quantifies the uncertainty that is due either to lack of knowledge about the exact value of this parameter or to actual variations in the value of the parameter among the members of a certain population.

The most widely used technique for propagating uncertainties is Monte Carlo simulation. In general, a Monte Carlo simulation consists of generating a random sample of the inputs of the model and determining the risk analysis output from each set of input parameters. All samples together form a probability density function of the undesired event frequency. First the Monte Carlo simulation method will be explained in more detail.

15.3.2 Description of Monte Carlo simulation

The basic idea of the Monte Carlo simulation technique, is to set up an analogous stochastic process which behaves as much like the actual model as possible.The model process is then observed, and the results are tabulated and treated as if they were experimental data representing the actual problem.

For those fault tree applications, where a basic event is better described by a probability distribution than by a single value, it is sometimes desirable to obtain theTop Event probability distribution.This will be difficult or impossible to do analytically.The Monte Carlo technique applies random values for the basic event probability in order to determine the Top Event probability. By repeating this process many times, the probability distribution of the Top Event can be studied simultaneously. However, this may require a large amount of computer time. The Monte Carlo method can be applied to other problems, including uncertainty analysis.

Since Monte Carlo simulation involves no complex mathematical analysis, it is an attractive alternative approach. It is a relatively easy way to model complex systems, and the input algorithms are easy to understand.There are no constraints regarding the nature of input assumptions on parameters such as failure and repair rates, so non-constant values can be used. It is also easy to model aspects such as queuing rules for repairs, repair priorities and 'cannibalization' (the use of serviceable spare parts from unserviceable systems).

One problem with Monte Carlo analysis is its expensive use of computer time. Since every event (failure, repair, movement, etc.) must be sampled for every unit of time, using the input distributions, a simulation of a moderately large system over a reasonable period of time can require hours of computer run-time. Also, since the simulation of probabilistic events generates variable results, in effect simulating the variability of real life, it is usually necessary to perform a number of runs in order to obtain estimates of means and variances of the output parameters of interest, such as availability, number of repairs arising and repair facility utilization. On the other hand, the effects of variations can be assessed.

The various Monte Carlo techniques can be distinguished on the basis of the random sampling method as follows:

1 : *Simple random sampling (SRS).*
Simple random sampling is the simplest of the sampling methods. In this method, every value of the sample is randomly sampled from its distributions. The advantages of simple random sampling are simplicity of generation, availability of well known methods of estimation and statistical analysis, robustness and aggregation. With regard to aggregation, simple random samples obtained using the same models and parameter distributions can be combined to make larger samples. There is one main disadvantage of simple random sampling: it may require many simulations which for complex time consuming models might impose excessive computer time requirements.

2: *Latin hypercube sampling (LHS).*
Latin hypercube sampling is one method of sampling a large number of input variables that yields estimators of model response more efficiently than simple random sampling. The name of the sampling method derives from its similarity to certain fractional factorial sampling plans. Latin hypercube sampling partitions a parameter range into discrete intervals. A parameter value within each interval is sampled using simple random sampling. This approach reduces the sample size (relative to simple random sampling) required to obtain estimates of a specified precision. The beneficial characteristics of latin hypercube sampling include its unbiased and efficient estimators. The efficiency of latin hypercube sampling versus the simple random sampling has been demonstrated for cases in which the output is a monotonic function of the input variables, as is the case for risk models when the rare event approximation is used. (In the rare event approximation, the undesired event frequency is expressed as a closed, monotonic function of the various input parameters, i.e. sums of products). If, however, non-events (e.g. successes) are included in the model, then the model ceases to be monotonic and there is no theoretical basis for assuming that latin hypercube sampling performs better than simple random sampling.

The key features in a Monte Carlo simulation are generation of a series of values of one or more random variables with specified probability densities, examination of the way the system behaves for paired values of these random values, and tabulation of the result as if it were the outcome of an experiment. To apply the Monte Carlo technique the following is required:

- *A uniform random number generator:*
  Monte Carlo simulation includes the chance variation inherent in most real-life problems. The device used to create this variation when the models are run on a digital computer is the random number generator. This generator usually is a subprogram that returns values from a uniform distribution (see chapter 4) of the intervals 0.0 to 1.0.

- *Generators from distributions:*
  Algorithms are available to generate random variables from distributions by making transformations on one or several values generated from the uniform random generator.

This will be explained with an example:

Consider the exponential cumulative distribution function (see chapter 4):

$$R(t) = e^{\frac{-1}{MTTF} \cdot t} \tag{15.1}$$

The inverse cumulative distribution function is given by:

$$t = -MTTF \ . \ \ln\{R(t)\} \tag{15.2}$$

To generate an exponentially distributed, positive, random deviate of the mean value MTTF, using RAN(NSEED) as the source of uniform deviates the following algorithm can be used:

$$EXPDEV = -MTTF \ . \ ALOG\ (RAN\ (NSEED)) \tag{15.3}$$

- *Computer code that defines the problem to be solved:*
  In a Monte Carlo model the digital simulation model moves from one distinct state to another. The state of the model at any point in time is represented by a set of variables. An event in a simulation model causes the model to change its state, so whenever an event occurs one or more of the variables representing the model are changed. Most simulation models are programmed so that simulated time moves directly from one event to the next. Most of the programming effort in developing difficult models is in keeping the events in proper chronological order and moving the model correctly from one event to the next. For more details see reference [15.1]. A well known general purpose computer code to perform simulation runs is AMIR, see reference 15.4.

15.3.3 Uncertainty propagation with Monte Carlo simulation

The system characteristics as computed in chapter 9 ”Quantification of minimal cut sets” are referred to as point values because fixed values were used for the failure rates and other data parameters. In a probabilistic approach, because of the variations and uncertainties in the failure rates and data parameters, these quantities are treated as random variables. Since the Hazard frequency or the system characteristics is a function of these random variables, it is itself then a random variable.The process of determining the undesired event frequency or system characteristic distribution as a function of the individual parameter distributions is called uncertainty propagation.

A variety of uncertainty propagation analysis methods can be used. For the random variable approach, the method most adaptable to a fault tree evaluation is the Monte Carlo simulation technique.The Monte Carlo method can accommodate general distributions, general sizes of the errors, and dependencies.

In the Monte Carlo method, the fault tree evaluations are repeated a number of times (each repetition is called a ”trial”) using different data values (e.g., failure rates and repair durations) for each calcula-tion. The variation in the data values is ”simulated” by randomly sampling from probability distribution functions which describe the variability in the data.

The probability distributions can be distributions representing the imprecision in the parameter estimates or can be distributions representing plant-to-plant variation in the failure rates and other data.

Each trial calculation will give one value for the result of interest such as the undesired event frequency, system unavailability or failure occurrence rate. The whole set of repeated calculations will give a set of system results from which an error spread is determined (e.g., picking the 5 per cent largest value and 95 per cent largest value to represent the 90 per cent range for the result).

The above method is completely analogous to repeating an experiment many times to determine the error in the experimental value. The final error spread on the result is the estimate of the result variability arising from the variability in the failure rates and other data treated as random variables.

If the cut sets are established for the fault tree to be analysed, and if for every basic event an uncertainty distribution is provided, than the calculation of the top event uncertainty can be made.

A Monte Carlo simulation program performs a series of trials on the basic event in a cut set equation. In each trial, values of the parameters with defined distributions are chosen randomly from the uncertainty distribution. The chosen values are substituted into the cut set equation, and the out-come value of the top event probability is determined. The results of many hundreds of trials are then ordered by the probability outcome values. This result can be plotted as a histogram, representing the uncertainty distribution for the top event probability. It is then possible to find an estimate for the mean value of the top event probability and the 5 per cent and 95 per cent percentiles of its uncertainty distribution.

This process results in a random sample of the Hazard frequency. Quantitative measures of the uncertainty associated with the output are then derived from this random sample.

Another approach that has been used for uncertainty propagation is that of discretization. According to this technique, all input variables and parameters are discretized; that is, their range is divided into a finite number of regions. A single value, such as the midpoint, represents the whole region and the value is assigned the probability corresponding to that region. All combinations of the discrete values of the input variables are then taken, with each combination having the probability of occurrence specified by the joint probability of the discrete input variables.

15.3.4 **Representation of input parameter uncertainty**

The parameters of the various reliability models used in a faut tree, can not be exactly known because of several reasons. It is important to classify these sources of uncertainty in two categories:

- *Imprecision in the parameter estimate*
  e.g. due to the random nature of the event, or due to the scarcity or lack of data, or because of the imprecision of the method to asses for example human error probabilities.
- *System-to-system variability*
  e.g. due to the use of generic data from similar systems or the use of data from other fields of application with possibly other operational conditions.

The first class is concerned with those cases where the estimate itself will provide a reasonable assessment of the unknown parameter but the confidence might be not very strong. This type of uncertainty applies to basic events (partly) quantified with plant specific data. It concerns statistical confidence, or lack of confidence, because of the use of poor or an inadequate amount of data.

The concept of system-to-system variability, second class, applies to those basic events which have been quantified using generic data, and accounts for the fact that the components in the specific plant analysed, may not be well represented by the generic mean values found in databases that can be established based on other applications. This system-to-system variability will generally be higher when generic data is used from other fields of application. This is because for other fields is it very well possible that other components requirements apply and that the component is exposed to other pressures, fluids, temperature, weather conditions etc.

Although there are conceptual differences between these two types of uncertainty, the methods commonly used for dealing with these uncertainties in the fault tree model are the same. All input parameters are characterized as random variables. The probability distribution assumed for each parameter then quantifies the uncertainty that is due either to lack of knowledge about the exact value of this parameter or to actual variations in the value of the parameter among the members of a certain population.

For each basic event in the fault tree model, the analyst must:

- select an appropriate distribution type to describe the uncertainty and
- estimate the parameters of this distribution to describe the estimate and the uncertainty about the probability of this basic event.

From the available information a best estimate (mean) is established for all parameters in the risk analysis model and an interval in which the parameter values lies with 90 per cent certainty. This 90 per cent uncertainty interval is bounded by the 5 per cent and 95 per cent percentiles, where the 95 per cent percentile represents a 95 per cent confidence that the real value is less than or equal to that value.

A distribution type often used to model the uncertainty is the so called Lognormal distribution (see chapter 4). This is a typically skew distribution which often suits good for this purpose. This distribution is characterized by two parameters: a mean and an error factor (EF):

$$EF = \sqrt{\frac{p_{95\%}}{p_{5\%}}} \qquad (15.4)$$

This error factor indicates the spread, i.e. the measure of confidence, about the parameter.

In the following a brief overview is provide of the possible distribution types, their application and the parameters to be assessed.

Normal distribution (see chapter 4 "Statistics"):
For parameter values which are not too small, a normal distribution can be applied to describe the parameter uncertainty. Due to the fact that the normal distribution is not restricted to positive values, it is advisory not to use the normal distribution for parameters with an order of magnitude smaller than 10^{-2}. For parameter that are smaller, a lognormal distribution (see chapter 4) should be used.

The parameters to be quantified for the normal distribution are:

- Mean : Most likely value of the parameter

- Range factor : Quotient of 95 per cent bound of the uncertainty interval and the median value (RF = $p_{95\%}$ / median)

The uncertainty interval is bounded by the 5 per cent and 95 per cent percentiles. The 95 per cent percentile ($p_{95\%}$) represents a 95 per cent probability that the real value is less than or equal to that value and similarly with a probability 0.05, the real value is below the 5 per cent percentile. This means that with 90 per cent probability the real value is in the 90 per cent uncertainty interval [$p_{5\%}$, $p_{95\%}$].

Lognormal distribution (see chapter 4):
A distribution type suitable to model the uncertainty in small parameters is the lognormal distribution (A parameter X is lognormally distributed if the parameter log(X) is normally distributed). This distribution is only defined for positive values of the parameter whereas using the normai distribution negative values are possible, which is in general not correct for reliability applications.

The lognormal distribution is a typically skew distribution which often suits good for the uncertainty quantification of fault trees. This distribution is characterized by the following two parameters

- Median : Most likely value of the parameter or 50 per cent percentile of the uncertainty distribution.

- Error factor : The error factor indicates the spread, i.e. a measure of confidence, about the parameter. { EF = SQRT($p_{95\%}/p_{5\%}$) }

From the available information a best estimate (median) is established for the parameter in the fault tree model and an interval in which the parameter values lies with 90 per cent certainty.

Loguniform distribution (see chapter 4):
Another distribution sometimes used in modelling parameter uncertainty is the loguniform distribution. On a logarithmic scale this distribution is flat between given upper and lower bounds. As in reliability applications, the parameter ranges can vary in orders of magnitude this logarithmic scale provides a reasonable representation. The loguniform can therefore be regarded as a distribution in which very little information is provided. The parameter values to be assessed are:

- Median : Best estimate of the parameter value; the centre of the uncertainty interval on a logarithmic scale.

- Range Factor : Ratio between upper bound of the possible parameter range and the median value (upper/median)

Estimation of error or range factors:
If no or insufficient specific failure data is available, generic sources or expert judgement should be used. Some generic databases provide a confidence interval for the component failure data. This can be used in the uncertainty assessment. There is a difference between statistical confidence intervals and the described interpretation of uncertainty intervals. However, as this is often the only information available, the statistical confidence interval can be used as a probabilistic uncertainty interval.

If in addition to this generic data, some plant specific failure data of the components is available, then the generic data can be updated to reflect this specific information as well. The method for this updating is called Bayesian Inference but will not be treated here. In chapter 6 "Data Analysis" more information of this method can be found.

In the case that sufficient test data is available for the component, this can be used to establish the confidence interval by applying statistical estimation techniques. These techniques are addressed in chapter 6 "Data Analysis".

Typical error factors often used are:

EF = 3 Relatively little uncertainty, for example: common cause failure parameters of the β-factor or α-factor model.

EF = 15 Very uncertain estimates, for example: human failure probabilities established using generic quantification models.

An error factor lower than three indicates large confidence in the estimate. The error factor 15 indicates low confidence; it states that the only confidence to be put in the estimate is that the actual value is expected (with 95 per cent certainty) to be not higher than 15 times the estimate. In general the error factors used will be between these two values.

15.3.5 Specific issues in propagating uncertainties

If one intends to perform an uncertainty analysis special attention has to be paid to the following issues:

1 : *Treatment of similar components.*
If two or more primary events have the same parameter (e.g. failure rates and failure mode), then in the uncertainty analysis these parameters should be totally correlated. Thus in the random sample they should be represented by the same random variable.

If this would not be done and the uncertainty would be placed on every basic event independently, then this would mean that the uncertainties are uncorrelated. Then, at every calculation in the Monte Carlo simulation, a sample is taken for each of the basic events, resulting in narrow confidence bounds. Using the uncertainty per component type or group, increases spread in the outcome as the correlated uncertainty is accounted for. This difference arises because multiple sampling from what is in effect the same distribution tends to produce a weighting toward the mean of that distribution.

2: *Inclusion of non-events.*
The uncertainty propagation is usually based on the rare event approximation, as in the case when the point calculations are carried out. However, for certain events, particularly human errors modelled at the event tree level, it might be important to include non-events to avoid an overestimation of the final result. Events with mean values of around 0.10 or greater can take values close to unity during the generation of the random sample. If this is the case, accident sequences that assume the success of these events should be multiplied by the complementary probabilities.

3: *Probability density functions for input variables.*
Probability density functions are used to characterize the uncertainties and hence the random variable distributors. The inputs to be characterized by appropriate probability density functions include the frequenties of the initiating events, the component failure rates and the human error probabilities. If a plant specific assessment of these parameters is performed, then the plant specific posterior probability density functions are to be used. If a generic database is used, then the appropriate probability density functions defined in the database should be used.

4: *Results.*
The results should include the mean and the median values, together with sufficient information about the distribution to allow the user to estimate the probability associated with any interval.

15.4 IMPORTANCE ANALYSIS

The purpose of an importance evaluation is to identify the important basic events with regard to the occurrence of the undesired event.The types of importance which are determinable from a fault tree can be grouped in two classes:

- Qualitative importances.
- Quantitative importances.

The qualitative importances are importances that are derived from the logic structure of the fault tree model.This means for example that single point failures, (cut sets with only one basic event), require special attention.

The quantitative importances are the importances of the top event contributors and of changes, that are derived from the quantitative results. Although quantitative importance can provide more detailed information than the qualitative importances, e.g. ranking of basic events according to their unavailability contribution, they are also subject to the greater uncertainty associated with the quantification.

15.4.1 Qualitative importance measures

The minimum cut sets are the keys towards quantifying the fault tree. However, the minimum cut sets also provide qualitative, structural information which can be used to identify important component failures and important situations that can lead to undesirable consequences.

For the single component minimum cut sets of a system it is clear that these are the single point failures that result in system failure.

On the basis of reliability considerations, it is known that components that have a common failure susceptibility are subject to failure from one common cause which can fait all the components (see also Chapter 13 ″Dependent failure analysis″). So higher order minimum cut sets can be reviewed to identify these common failure susceptibilities.

These common susceptibilities are significant only if the susceptible components are in the same minimum cut set. The minimum cut set information from risk or reliability studies can thus be evaluated to identify the minimum cut sets in which all the components have a common susceptibility. The common susceptibilities in a minimum cut set that can be specifically focused upon include are:

1: All components of the same generic type (such as all pumps) in a minimum cut set (critical group) indicative of potentially common, critical vulnerabilities

2: All components in a minimum cut set in the same location

3: All components in a minimum cut set under the same maintenance or testing procedure

4: All human errors in a minimum cut set that implies that human errors alone can fait critical subsystems, systems or functions

5: All components in a minimum cut set that can be exposed to a common harsh or degrading environment

6: All components in a minimum cut set not testable in routine surveillance testing, thereby giving a critical undetectable failure mode

7: All components in a minimum cut set tested under a common pre-operational or start procedure: if the procedure is inadequate, a critical failure mode can be untested or undetected.

These common cause failure susceptibilities can be further evaluated quantitatively using the approaches presented in Chapter 13 ″Dependent failure analysis″

15.4.2 Quantitative importance measures

Where the qualitative importance analysis concentrates on the minimum cut sets, the quantitative importance measures analyse the importance of individual basic events.

In order to understand which factors control the overall risk results, several importance measures for the various events in the final cut sets can be calculated. Based on these measures a ranking can be established to find the most critical events in the risk or reliability model. These measures are defined as follows for a basic event E. The measures are named according to their application in risk analysis but can equivalently be used in reliability and availability studies.

The following notation is used:

$$\begin{aligned} \mathrm{E} &= \text{the basic event under consideration} \\ \mathrm{P}(E) &= \text{probability that event E has occurred} \\ \mathrm{P}_{\mathrm{top}} &= \text{overall top event probability} \\ \mathrm{P}_{\mathrm{top}}(x) &= \text{top event probability given P(E) = x} \\ \mathrm{P}_{\mathrm{i}}(E) &= \text{probability of the ith cut set containing basic event E} \end{aligned} \tag{15.5}$$

Fussell-Vesely /mportance (I_{FV}):
The Fussell-Vesely importance measure is expressed in relative terms. It indicates the risk associated with a given basic event E. That is, how much this component or event is contributing to system failure.

$$\begin{aligned} \mathrm{I}_{\mathrm{FV}}(\mathrm{E}) &= \frac{\text{Sum of cutset contributions containing basic event E}}{\mathrm{P}_{\mathrm{top}}} \\ &= \frac{\sum_{i} \mathrm{Cutset}_{\mathrm{i}}\ (E)}{\mathrm{P}_{\mathrm{top}}} = \frac{\mathrm{P}_{\mathrm{top}} - \mathrm{P}_{\mathrm{top}}(\mathrm{O})}{\mathrm{P}_{\mathrm{top}}} \end{aligned} \tag{15.6}$$

Birnbaum Importance (I_B):
The Birnbaum importance measure of basic event E is defined as the rate of change of the top event probability (derivative) with respect to a change in the probability of occurrence of basic event E. This can, because of the linearity of the fault tree equation.

$$\mathrm{I}_{\mathrm{B}}(\mathrm{E}) = \frac{\mathrm{d}\ (\mathrm{P}_{\mathrm{top}})}{\mathrm{d}\ \mathrm{P}(\mathrm{E})} \tag{15.7}$$

$$\mathrm{I}_{\mathrm{B}}(\mathrm{E}) = \mathrm{P}_{\mathrm{top}}(1)\text{-}\mathrm{P}_{\mathrm{top}}(\mathrm{O}) \tag{15.8}$$

The Birnbaum importance measures the difference in top event probability when basic event E occurs and when basic event E does not occur. The Birnbaum importance gives the increase in contribution associated with the occurrence of basic event E.

Risk Achievement Worth (RA W):

The Risk Achievement Worth measure is expressed as a ratio giving the factor by which the top event probability increases due to a component not being available, i.e. the event occurs with certainty. It is the change of the outcome in a worst case scenario. This is an interesting measure to assess which elements are the most crucial in maintaining the current level of reliability or availability.

$$\mathrm{RAW(E)} \quad = \quad \frac{P_{top}(1)}{P_{top}} \tag{15.9}$$

Risk Reduction Worth (RRW):

The Risk Reduction Worth is a measure of the risk reduction that would be achieved when the unavailability of a component is reduced to zero, i.e. the event certainly does not occur. This measure aids in setting design improvement priorities.

$$\mathrm{RRW(E)} \quad = \quad \frac{P_{top}}{P_{top}(O)} \tag{15.10}$$

Each of the importance measures provides a different view on the importance of basic events. The choice will depend on the use of the ranking established by the importance measures. In general a ranking made based on the Fussell-Vesely importance is similar to one based on the Risk Reduction Worth, whereas the rankings based on Risk Achievement Worth and Birnbaum are comparable as well. The Fussell-Vesely and the Birnbaum importance are most often used as a measure of contribution associated to a component.

It should be emphasized that, in general, the importante measures are calculated by only changing the basic event probability of one basic event. Given this method of calculation no information can be extracted from the importance lists if one is interested in the resulting effect if two or more probabilities of basic events are changed.

Practical application shows that an importance analysis is only useful if the dominant contributors have to be determined out of a large number of cut sets.

15.5 SENSITIVITY ANALYSIS

The objective of a sensitivity analysis is to vary the failure probability of various basic events and observe the change in top event probability. In general the sensitivity analysis is carried out by making changes in the input parameters and performing a requantification of the model.

15.5.1 Introduction

Sensitivity studies are performed to assess the impact of variations or changes to the component data or to the fault tree model. It is particularly convenient to assess effects of component data variations using the formulas presented in chapter 9 ”Quantification of minimal cut-sets” because they explicitly contain component failure rates, test intervals, and repair times as variables. In sensitivity analyses different values may be assigned these variables to determine the differences in any result. For example, if T is a periodic testing interval, then the effects on system unavailability with regard to different testing intervals can be studied by varying the T’s for the components. This can entail as simple a calculation as redoing the computations with different T’s or as complex as employing dynamic programming. Likewise, failure rates can be changed to determine the effects of upgrading or downgrading component reliabilities.

As a type of sensitivity evaluation, formal error analyses can be performed to determine the error spread in any final result due to possible data uncertainties or variabilities. The error spread obtained for the results gives the uncertainty or variability associated with the result. The error analyses employ statistical or probabilistic techniques, which are independent of the fault tree evaluation techniques. This type of sensitivity estimation will be explained in section 15.5 ”Uncertainty Analysis”.

The purpose of a sensitivity analysis is twofold:

1: To address those modelling assumptions suspected of having a potentially significant impact on the results. These assumptions are generally in areas where information is lacking and heavy reliance must be placed on the analyst’s judgement.

2: To determine the sensitivity of the calculated value for the reliability characteristic to possible dependencies among component failures and among human errors

Sensitivity analysis can be performed by substituting alternative assumptions and evaluating their individual impacts on the results. Sensitivity analyses of possible dependencies among component failures and among human error are further discussed in the following subsections.

15.5.2 Component failure rate sensitivity analysis

A wide spectrum of sensitivity analyses can be performed, depending on the needs of the engineer. As a type of sensitivity study, scoping-type evaluations can also be performed by using a high failure rate and a low failure rate for a particular event on the tree. If the system reliability characteristic does not change significantly, then the event is not important and no more attention need to be paid. If the system reliability characteristic does change significantly, then more precise data must be obtained or the event must be further developed to more basic causes.

In judging the significante of an effect, it is important that the analyst takes the precision of his data into account. For example, although a factor of 2 variation in the system unavailability might be very significant when failure rates are known to 3 significant figures, the same factor of 2 variation would probably not be significant when failure rates are known only to an order of magnitude.

Single failures in any of the systems can be tabulated and discussed separately. The discussion can give the defences or conditions that reduce the contributions of these events to system unreliability or unavailability.

15.5.3 Component failure dependence analyses

The sensitivity prescribed here is intended to explore, among other things, whether a detailed common cause failure analysis is warranted for a particular group of components. As a first step, a search is conducted for areas that are sensitive to coupling between hardware failures. Searches for sensitivity to dependence can be carried out on a system basis or on an accident sequence basis. The following assessment can be performed to further quantify common cause and dependence potentials.

1: The minimal cut sets can be searched for dependence suspect minimal cut sets. Dependence suspect minimal cut sets are minimal cut sets containing failures of components, of which two or more have a common property that renders them susceptible to dependent failures. These susceptibilities, together with the way of determining dependence suspect minimal cut sets, were described in Chapter 13 ”Dependent failure analysis”. (Note that for more refined analyses not all components in the cut set have to have the common property, but only two or more.)

2: Each dependence suspect minimal cut set can be requantified as follows:
   a: Identify the highest failure probability among the potentially coupled events having a common cause failure susceptibility
   b: Set the product of the remaining coupled failure probabilities equal to 0.1.

3: For each type of coupling, the pertinent dependence suspect minimal cut sets can be presented, together with their respective new and old quantifications; the ratio change in system unavailability can also be presented.

4: Whenever the effect of a given coupling on a given system is substantial (e.g. greater than a factor of two in system unavailability), the corresponding change in the frequenties of the affected core damage sequences can be presented, together with a discussion of precautions, actions or conditions existing in the subject plant that serve to reduce the potential dependence.

15.5.4 Human error dependence analyses

The human error dependence sensitivity analyses should be performed similarly to the component dependence sensitivity analyses. The dependence suspect minimal cut sets that can be identified are those containing multiple human errors of any type. The minimal cut set can also contain compo-nent failures; it is the fact that it contains multiple human errors that renders it suspect. Rather than being requantified, these dependence suspect minimal cut sets can be analysed and a description given of the precautions, management control or conditions that serve to eliminate significant dependencies among the human errors in the cut sets. These discussions can be prepared in a tabular format, with the dependence suspect minimal cut sets ordered according to the number of human errors involved.

15.6 EXAMPLE

15.6.1 Introduction

The example presented in chapter 13: ”Dependent failure analysis” will be used to perform an importance, sensitivity and uncertainty analysis. This example considers the design of a continuously stirred tank reactor (CSTR) that uses a highly exothermic reaction to produce a chemical compound. To identify potential Hazards, a HAZOP analysis shows that a runaway exothermic reaction is possible in the CSTR. The protection against this undesirable event is provided by two CSTR dump valves (V1 and V2) that should open and quench the reaction mixture in a water filled sump (see figure 15.1). The dump valves will be opened if the temperature inside the CSTR rises above a preset limit.

The dump valve actuators are pneumatically operated and are controlled by a voting logic unit (VLU). The VLU commands the valves to open when at least two out of three temperature channels indicate a high/high condition. Each temperature channel has its own temperature sensor (TS). The temperature sensors are all set to trip at the same temperature. For proper functioning of the dump valves the instrument air system is required. The VLU is powered by an electrical supply of 24 Volt DC. Failure of the power supply of the VLU results in a spurious actuation signal to open both dump valves.

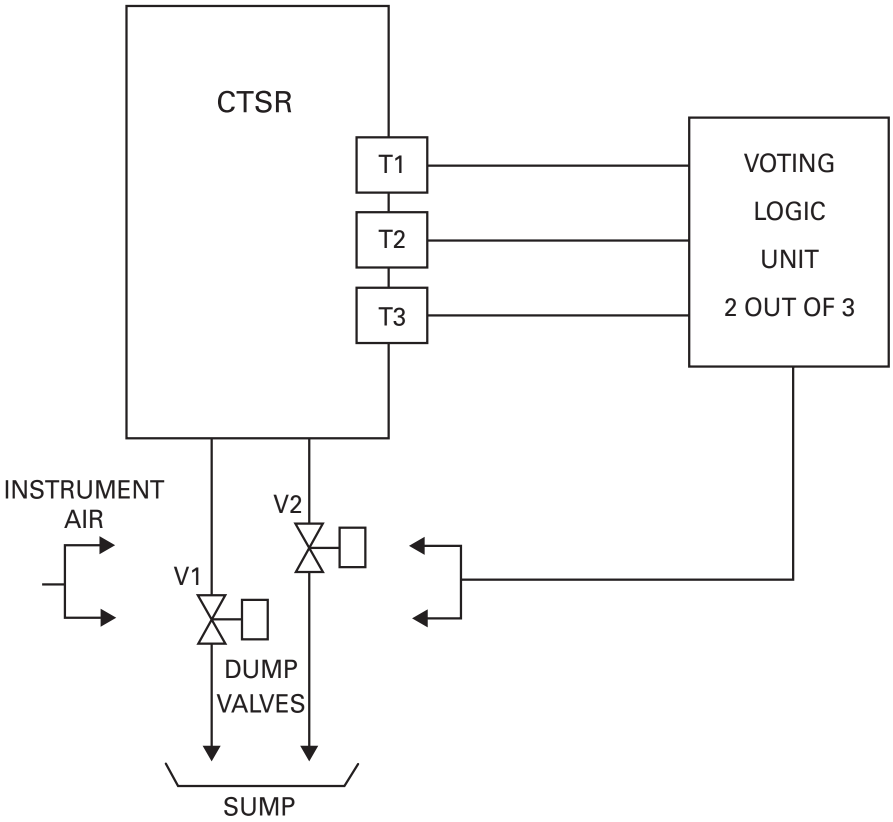


Figure 15.1: Instrument safeguarding CSTR.

Both dump valves are identical, also the three temperature sensors are identical. The dump valves as well as the three temperature sensors are tested by the same maintenance crew during the annual maintenance. Testing of the temperature sensors also includes testing of the voting logic. The top event of interest is defined as follows:

> ”CSTR fails to dump following a high-temperature upset”

Successful operation of the instrument safeguarding system requires operation of at least two out of three temperature sensors, the VLU and at least one of the two dump valves.

For the CSTR safeguard system two common-cause component groups have been identified: the two identical dump valves and the three identical temperature sensors. The composition of the two common-cause groups is as follows:

Group 1:	Dump valve group
	IFDVALVE1
	IFDVALVE2
Group 2:	Temperature sensor group
	IFTS1
	IFTS2
	IFTS3

15.6.2 Fault tree analysis

In comparison to the example presented in chapter 13, ”Dependent failure analysis” the fault tree structure is modified to perform the importance, sensitivity and uncertainty analysis. The purpose of this modification is to calculate explicitly the importance, sensitivity and uncertainty of the alpha factors. The modified fault tree structure is as follows:

Modified fault tree structure:

Gate	Type	Descendant	Descendant	Descendant	Descendant
TOP	AND	GATE1	GATE2		
GATE1	OR	DVALVEI_FAILS	INSTR_AIR	NO_SIGNAL_VLU	
GATE2	OR	DVALVE2_FAILS	INSTR_AIR	NO_SIGNAL_VLU	
NO_SIGNAL_VLU	OR	VLU_FAILS	NO_SIGNAL_SENS		
NO_SIGNAL_SENS	AND	NO_SIGNAL_S1_S2	NO_SIGNAL_S1_S3	NO_SIGNAL_S2_S3	
NO_SIGNAL_S1_S2	OR	TS1_FAILS	TS2_FAILS		
NO_SIGNAL_S1_S3	OR	TS1_FAILS	TS3_FAILS		
NO_SIGNAL_S2_S3	OR	TS2_FAILS	TS3_FAILS		
DVALVEI_FAILS	OR	IFDVALVEI	CCFDVALVES		
DVALVE2_FAILS	OR	IFDVALVE2	CCFDVALVES		
TS1_FAILS	OR	IFTS1	CCFTSITS2	CCFTSITS3	CCFTSITS2TS3
TS2_FAILS	OR	IFTS2	CCFTSITS2	CCFTS2TS3	CCFTSITS2TS3
TS3_FAILS	OR	IFTS3	CCFTSITS3	CCFTS2TS3	CCFTS1TS2TS3
CCFDVALVES	AND	ALPHA2_VALVES	IFDVALVE		
CCFTSITS2	AND	ALPHA2_SENSORS	TS12_FAILS		
CCFTSITS3	AND	ALPHA2_SENSORS	TS13_FAILS		
CCFTS2TS3	AND	ALPHA2_SENSORS	TS23_FAILS		
CCFTSITS2TS3	AND	ALPHA3_SENSORS	TS123_FAILS		

The cut sets can be solved by a general purpose fault tree analysis code (see reference 15.5), The results are two first order minimal cut sets and nine second order minimal cut sets:

Minimal cut sets:

```
First order Minimal Cut Sets:


   INSTR_AIR
   VLU_FAILS

Second Order Minimal Cut Sets:
      IFVALVEI  .  IFVALVE2
         IFTS2  .  IFTS3
         IFTS1  .  IFTS2
         IFTS1  .  IFTS3
  ALPHA2_VALVES  .  IFVALVE
ALPHA3_SENSORS  .  TS123_FAILS
ALPHA2_SENSORS  .  TS12_FAILS
ALPHA2_SENSORS  .  TS13_FAILS
ALPHA2_SENSORS  .  TS23_FAILS
```

15.6.3 **Quantification of fault tree.**

In table 15.1 all relevant component failure data, component types and test periods are provided. It should be emphasized that all data provided in this chapter are for illustrative purposes only.

Table 15.1: Component data.

Name	Component code	Component type	Lambda	Test period	Repair duration
Dump valves	IFVALVE_1, - IFVALVE_2	Tested stand by	2.0E-06	8760	
Temp. sensors	IFTS1, IFTS2, IFTS3	Tested stand by	4.0E-06	8760	
Voting Logic	VLU_FAILS	Tested stand by	2.0E-07	8760	
Instrument air	INSTR_AIR	On line re airable	1.0E-05	-	8

To perform the importance, sensitivity and uncertainty analysis the alpha factors are incorporated in the fault tree as multiplication factors for the total failure rates. To calculate these multiplication factors the information provided in chapter 13: "Dependent Failure Analysis" has been used.

The resulting values are:

Alpha Valves	:	0.122
Alpha Two Sensors	:	0.0353
Alpha Three Sensors	:	0.0530

All values used are tabulated in the component database:

Component database:

```
Basic Event          Type       Lambda, Q     T           Theta

ALPHA2_SENSORS         DM        1.76E-02      0            0
ALPHA2_VALVES          DM        1.22E-01      0            0
ALPHA3_SENSORS         DM        5.30E-02      0            0
IFVALVE                TS        2.00E-06      8760         0
IFVALVE_1              TS        2.00E-06      8760         0
IFVALVE_2              TS        2.00E-06      8760         0
IFTS1                  TS        4.00E-06      8760         0
IFTS2                  TS        4.00E-06      8760         0
IFTS3                  TS        4.00E-06      8760         0
INSTR_AIR              OR        1.02E-05      0            8.00
TS12_FAILS             TS        4.00E-06      8760         0
TS123_FAILS            TS        4.00E-06      8760         0
TS13_FAILS             TS        4.00E-06      8760         0
TS23_FAILS             TS        4.00E-06      8760         0
VLU_FAILS              TS        2.00E-07      8760         0
```

DM	=	Demand model	
TS	=	Tested stand-by component	
OR	=	On line repairable component	
Lambda	=	Failure rate	-/hour
Q	=	Probability of failure on demand	-
T	=	Test period	hour
Theta	=	Repair duration	hour

Quantification of the cut sets gives the following results:

Unavailability.

Contribution first order minimal cut sets	9.57E-04	15.59	per cent
Contribution second order minimal cut sets	5.18E-03	84.41	per cent
Contribution higher order minimal cut sets	0	0.0	per cent
Total unavailability	6.14E-03		

```
Cut set                       Contribution       Per cent    Formula

1    IFVALVE                  1.07E-03           17.41       B4
     ALPHA2_VALVES
2    TS123_FAILS              9.29E-04           15.12       B4
     ALPHA3_SENSORS
3    VLU_FAILS                8.76E-04           14.26       A1
4    TS12_FAILS               6.18E-04           10.07       B4
     ALPHA2_SENSORS
5    TS13_FAILS               6.18E-04           10.07       B4
     ALPHA2_SENSORS
6    TS23_FAILS               6.18E-04           10.07       B4
     ALPHA2_SENSORS
7    IFTS2                    4.09E-04           6.67        B1
     IFTS3
8    IFTS1                    4.09E-04           6.67        B1
     IFTS2
9    IFTS1                    4.09E-04           6.67        B1
     IFTS3
10   IFVALVE1                 1.02E-04           1.67        B1
     IFVALVE2
11   INSTR_AIR                8.16E-05           1.33        A2
```

From the results it can be concluded that common-cause failures are the dominant contributors to the unavailability of the instrument safeguard system of the CSTR.

15.6.4 Importance analysis

The importance analysis is carried out by running a general purpose fault tree analysis computer code, see reference 15.5. No additional input is required to run the importance module. The results can be presented as follows:

Results Importance Analysis:

```
     Basic Event             Fussel-Vesely      RRW                 Criticality

1    ALPHA2_SENSORS            3.02E-01         1.43                3.02E-01
2    ALPHA2_VALVES             1.74E-01         1.21                1.74E-01
3    IFDVALVE                  1.74E-01         1.21                1.74E-01
4    ALPHA3_SENSORS            1.51E-01         1.18                1.51E-01
5    TS123_FAILS               1.51E-01         1.18                1.51E-01
6    VLU_FAILS                 1.43E-01         1.17                1.42E-01
7    IFTS1                     1.33E-01         1.15                1.33E-01
8    IFTS2                     1.33E-01         1.15                1.33E-01
9    IFTS3                     1.33E-01         1.15                1.33E-01
10   TS12_FAILS                1.01E-01         1.11                1.01E-01
11   TS13_FAILS                1.01E-01         1.11                1.01E-01
12   TS23_FAILS                1.01E-01         1.11                1.01E-01
13   IFDVALVEI                 1.67E-02         1.02                1.67E-02
14   IFDVALVE2                 1.67E-02         1.02                1.67E-02
15   INSTR_AIR                 1.33E-02         1.01                1.32E-02
```

```
     Basic Event             RAW            Birnbaum

1    VLU_FAILS               1.63E+02         0.99
2    INSTR_AIR               1.63E+02         0.99
3    IFDVALVE                2.07E+01         0.12
4    TS123_FAILS             9.48E+00         0.05
5    ALPHA2_SENSORS          9.26E+00         0.05
6    IFTSI                   8.48E+00         0.05
7    IFTS2                   8.48E+00         0.05
8    IFTS3                   8.48E+00         0.05
9    TS12_FAILS              6.65E+00         0.04
10   TS13_FAILS              6.65E+00         0.04
11   TS23_FAILS              6.65E+00         0.04
12   ALPHA3_SENSORS          3.70E+00         0.02
13   IFDVALVEI               2.89E+00         0.01
14   IFDVALVE2               2.89E+00         0.01
15   ALPHA2_VALVES           2.25E+00         0.01
```

Considering the limited number of cut sets the results of the importance analysis are not surprising. From the importance lists it can be concluded that the value of the alpha factor describing a common cause failure of two sensors is important for the overall unavailability. From a maintenance perspective the first order minimal cut sets
VLU-FAILS and INSTR_AIR are important to maintain the current value for unavailability.

15.6.5 **Sensitivity analysis**

The concept of a sensitivity analysis is to vary the failure probability of a selected number of basic events and to observe the change in the reliability characteristic of interest. In general only one component failure probability is changed at a time.

For this example it is decided to vary the total failure rate of the dump valves, the total failure rate of the sensors and the alpha factors for both components. The variation of the failure rate of the dump valves has been done by a simultaneous variation of the basic events IFVALVE, IFVALVE_1 and IFVALVE_2. Also the variation of the failure rates of the basic events of the sensors (IFTS1, IFTS1, IFTS3, TS12_FAILS, TS13_FAILS, TS23_FAILS and TS123_FAILS) is done simultaneously. In table 15.2 the results of the variation of the total failure rates of the dump valves and the sensors is listed.

Table 15.2: Results sensitivity analysis failure rates dump valves and failure rate sensors.

Multiplication factor failure rate	Resulting unavailability due to a variation of the failure rate of the dump valves	Resulting unavailability due to a variation of the failure rate of the sensors
0.0625	0.0050	0.0023
0.125	0.0051	0.0025
0.25	0.0052	0.0029
0.5	0.0055	0.0038
1.0	0.0061	0.0061
2.0	0.0075	0.0126
4.0	0.0109	0.0329
8.0	0.0201	0.103
16.0	0.0483	0.361

To investigate the influence of the common cause failures a sensitivity analysis has been performed by variation of the alpha factors. Reviewing different databases shows that the average alpha factor describing dependent failure of two components is about 0.05. The alpha factor (see chapter 13) for the two dump valves 0.12 is rather high. Considering this information it is decided to vary the alpha factors between (0.25 * alpha) and (4.0 * alpha). The results are presented in table 15.3.

From the results of the sensitivity analysis it can be concluded that the total failure rate of the sensors gives the largest variation in the calculated unavailability of the safety system. The variation in the unavailability due to variation of the alpha factors is relatively small.

Table 15.3: Results sensitivity analysis alpha factors.

Multiplication factor	Sensitivity variation alpha factor valves	Sensitivity variation alpha2 factor sensors	Sensitivity variation alpha3 factor sensors
	Resulting unavailability	Resulting unavailability	Resulting unavailability
0.25	0.0053	0.0047	0.0054
0.5	0.0056	0.0052	0.0057
1.0	0.0061	0.0061	0.0061
2.0	0.0072	0.0079	0.0071
4.0	0.0928	0.0116	0.0089

The results are often plotted against eachother in one diagram called *spider plots.*
These spider plots are typically presented on a log-log scale (double logarithmic) and have a characteristic convex shape, see figures 15.2 and 15.3.

These plots are especially useful for events that are quantified with a large degree of uncertainty, for example human failure events and common cause failure events.

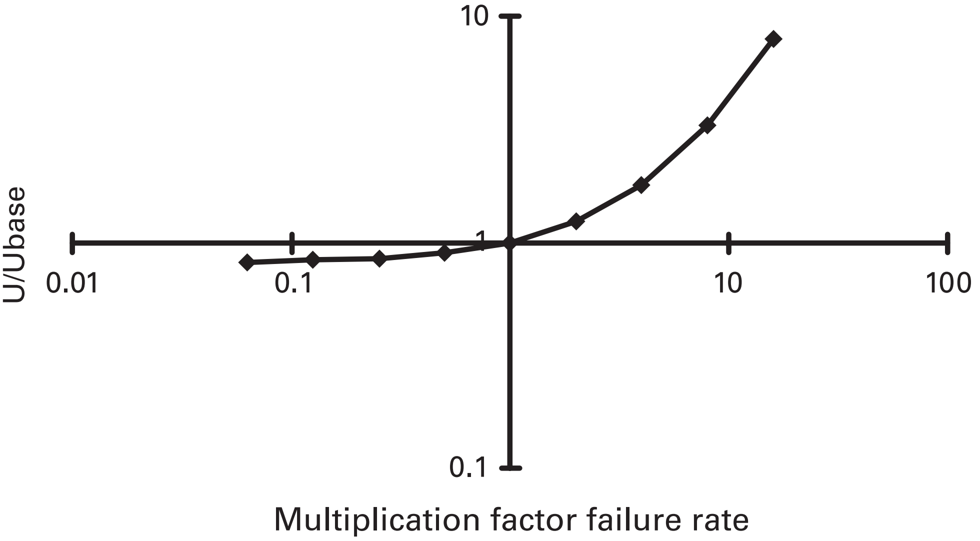


Figure 15.2: Spider plot sensitivity analysis failure rate dump valves.

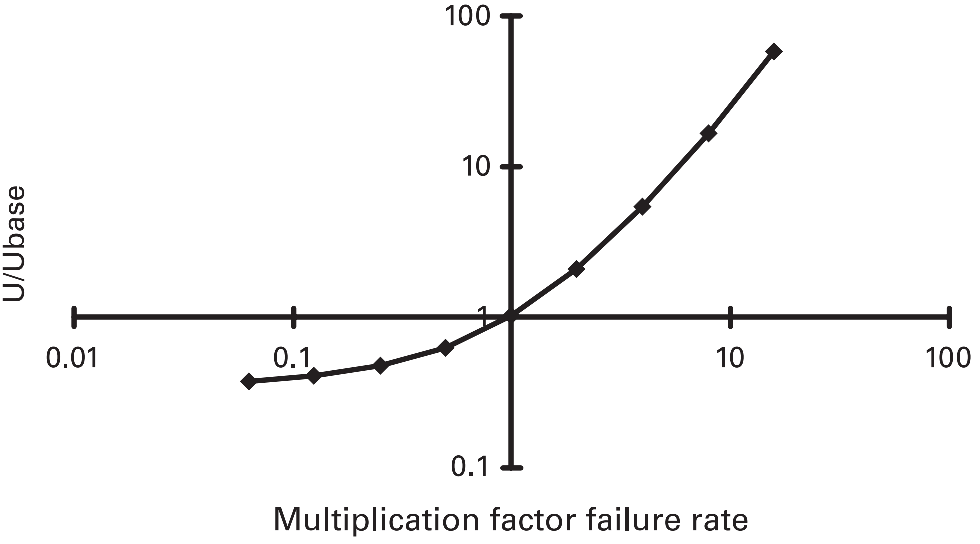


Figure 15.3: Spider plot sensitivity analysis failure rate sensors.

15.6.6 Uncertainty analysis

The Monte Carlo approach has been applied to calculate the uncertainty propagation due to the uncertainty in the input parameters, failure rates, repair duration and alpha factors.

For all basic events of the example, a best estimate and an error factor has been established. To bound the values for the alpha factors between a lower and an upper limit a log-uniform has been selected to model the uncertainty of the alpha factors. In general low and high values of the failure rates are not excluded from the uncertainty analysis. For this reason the log-normal distribution (see chapter 4) has been selected to model the uncertainty of the failure rates.

It is not advisable to use the log-normal distribution to model the uncertainty of the repair duration of the instrument air system because very short or very large repair duration is not expected the for instrument air system. For this reason the repair duration of the instrument air system is modelled by a log-uniform distribution (see chapter 4).

The uncertainty for components of the same type (dump valves and sensors) is not in the first place due to variations between the components but inherent to the estimate of the component failure data. As a consequence the uncertainty of both dump valves are completely correlated. The same holds for the sensors. This implies that only one uncertainty distribution has to be used to model the uncertainty propagation of the dump valves through the model. This has been achieved by definition of a group of identical components in the database for the dump valves as well as for the sensors.

The error or range factors have to be based on the uncertainty provided in generic databases or on expert judgement. Some typical values have been used in this example. The resulting database used to perform the uncertainty analysis is given below:

Database uncertainty analysis:

Basic Event	**Parameter**	**Distribution**	**Error Factor**	**Group**
ALPHA2_SENSORS	alpha factor	Log-uniform	3.0	—
ALPHA2_VALVES	alpha factor	Log-uniform	3.0	—
ALPHA3_SENSORS	alpha factor	Log-unifprm	3.0	—
IFDVALVE	failure rate	Log-normal	3.0	VALVES
IFDVALVE1	failure rate	Log-normal	3.0	VALVES
IFDVALVE2	failure rate	Log-normal	3.0	VALVES
IFTS1	failure rate	Log-normal	6.0	SENSORS
IFTS2	failure rate	Log-normal	6.0	SENSORS
IFTS3	failure rate	Log-normal	6.0	SENSORS
TS12_FAILS	failure rate	Log-normal	6.0	SENSORS
TS123_FAILS	failure rate	Log-normal	6.0	SENSORS
TS13_FAILS	failure rate	Log-normal	6.0	SENSORS
TS23_FAILS	failure rate	Log-normal	6.0	SENSORS
VLU_FAILS_FAILS	failure rate	Log-normal	9.0	—
INSTR_AIR	failure rate	Log-normal	6.0	—
INSTR_AIR	repair duration	Log-uniform	3.0	—

Uncertainty analysis:

The Monte Carlo simulation has been performed by using a general purpose Fault Tree Analysis code (see reference 15.5). Thirty two thousand trials have been made in the Monte Carlo simulation. This means that thirty-two-thousand times values are selected from each parameter distribution and with these values the top event unavailability is recalculated by substituting in the cut sets formulas. The non-smoothness of the curve due to this sampling is presented in figure 15.4. The numerical results are tabulated in table 15.4.

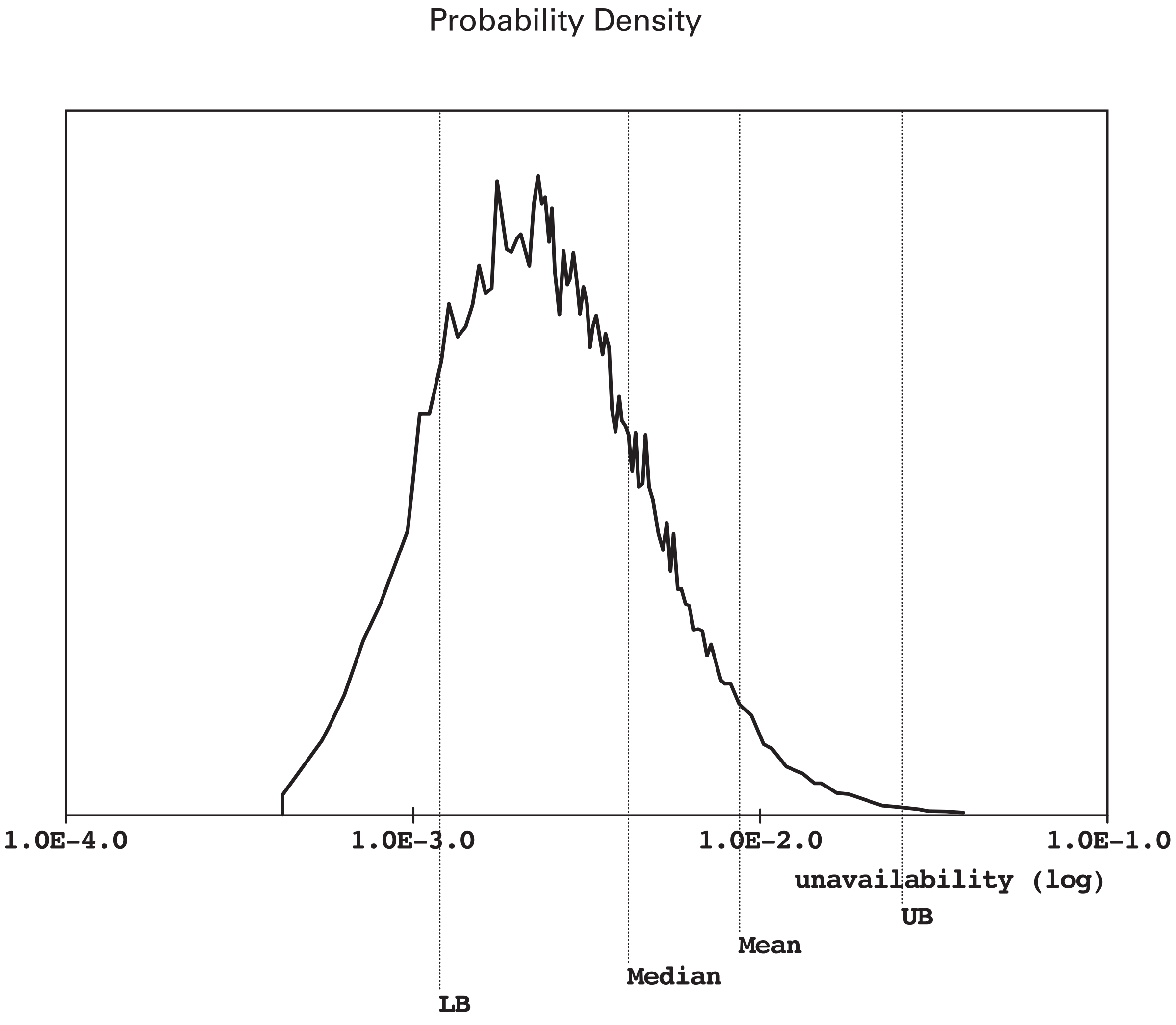


Figure 15.4: Uncertainty distribution unavailability safety system.

Table 15.4: Results uncertainty analysis (Grouped).

Distribution parameter	Value
Median	4.22E-03
Mean	8.79E-03
Standard Deviation	2.60E-02
Lower Bound (5%)	1.20E-03
Upper Bound (95%)	2.64E-02
Error Factor	4.7
Sample Size	32000

Reviewing table 15.4 shows that the calculated mean value in the uncertainty analysis is higher than the calculated mean in section 15.6.4. This is because the failure rates of both dump valves and the failure rates of the sensors are correlated completely.

If no correlation has been applied the results as tabulated in table 15.5 would have been generated. In this case the calculated mean is exactly equal to the calculated mean that is calculated in section 15.6.4. Also the error factor is much less than the error factor in the correlated case.

Table 15.5 gives the results if the variability of the failure rates between the different components in the system have to be taken into account. In general this is not done because of a lack of information about such a variability.

The number of trials (32000) is sufficient to calculate the upper bound, lower bound and mean value due to uncertainty propagation. This number of trials would have not been sufficient if a full scope Monte Carlo simulation has been performed to calculate the unavailability of the safety system. For such an analysis the number of trials has to be much higher due to the relative low failure rate of the components.

Table 15.5: Results uncertainty analysis (Ungrouped).

Distribution parameter	**Value**
Median	5.09E-03
Mean	6.14E-03
Standard Deviation	4.22E-03
Lower Bound (5%)	2.12E-03
Upper Bound (95%)	1.35E-02
Error Factor	2.5
Sample Size	32000

15.7 REFERENCES

[15.1] E.J. Henley, H. Kumamoto
Probabilistic Risk Assessmeny; Reliability Engineering, design and Analysis,
IEEE Press, New York, 1992.

[15.2] Fault Tree Handbook
U.S. Nuclear Regulatory Commission NUREG-0492

[15.3] PRA Procedures Guide
A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants.
U.S. Nuclear Regulatory Commission, NUREG/CR-2300
Final Report, January 1983.

[15.4] AMIR computer code, System Engineering Monte-Carlo based advanced software,
Malchi Science Ltd., Professor A. Dubi, P.O. Box 1194, Beer-Sheva, Israel.

[15.5] J.C.H. Schi uier, Manual Fault Tree Analysis code FTA,
KEMA Nuclear, 40721-NUC-94-4582, 11 januari 1995,
P.O. Box 9035, 6800 ET Arnhem.

RAM SPECIFICATION

CONTENTS

16.1 INTRODUCTION

A Reliability Availability Maintainability (RAM) specification is a tooi to optimize life cycle costs of equipment that will be acquired. In literature instead of RAM the acronym ARM and the word Dependability can be found. Reliability, availability and maintainability are properties of a component or system just like efficiency or capacity. As a lack of for instance efficiency will influence life cycle costs negatively, the same is true for a lack of RAM. RAM should therefore be treated as any other property that can be acquired, and RAM targets can be agreed upon. RAM guarantees can be negotiated depending on commercial factors.

RAM targets could be:

- a mean forced unavailability of 5%, with an additional requirement concerning for example the mean failure frequency and maximum repair time;
- a mean planned unavailability of 7% related to preventive maintenance;

The acquisition of any item, be it a single piece of equipment or an entire plant, is a phased process. This phased process is illustrated, in simplified form in table 16.1. RAM procurement should be an integral part of the total procurement program.

Acquiring RAM will generally not come free in terms of effort, man hours, and budgets, but asking for it will help in getting a piece of equipment with (low) life-cycle costs. Furthermore, it can assist in: 1) balancing the investment costs (system lay-out, redundant equipment, choice of material) against the costs of unavailability; and 2) reducing maintenance costs by taking maintenance into account during the design phase.

All necessary steps to attain the RAM goals set must be laid down in a document: the RAM specification. This RAM specification is part of the purchase contract.

In the following paragraphs the meaning, contents and application of RAM specifications are presented.

16.2 NOMENCLATURE

FU	=	Forced unavailability	-
MTTR	=	Mean time to repair	hour
λ	=	failure rate	-/hour

16.3 RAM MANAGEMENT

The process of acquisition consists of four phases, which are shown below in short. In every phase RAM tasks have to be performed and managed by the purchaser as well as the supplier to secure the RAM requirements to be met.

The four phases are:

Specification: This phase should include activities such as feasibility studies and evaluations of preliminary designs to accomplish the project goals. The activities are carried out mainly by the purchaser: what do you want and make clear what you want;

Tender: During this phase the tenderer's responses are evaluated and deviations are identified, resulting (via an iterative process) in an agreement of requirements and placing of the contract;

Construction: Procurement -purchasing of all equipment- and commissioning -evaluation and if necessary modification to ensure that RAM goals are met- take place in this phase of the process; and

Operation: In this phase RAM performance has to be compared with the RAM goals;

Table 16.1: Project acquisition phases and RAM activities.

PHASE		ACTIVITY
1	Specification	- Specification of requirements - Communication of requirements
2	Tender	- Evaluation of tenderer's responses - feedback and agreement of requirements
3	Construction	- placement of contract - monitoring progress
4	Operation	- comparison of RAM performance with goals

The complexity, duration and importance of each activity will vary with the complexity of the equipment and the goals set. In the following sections the contents of every phase will be discussed as welt as the actions to be taken.

16.4 SPECIFICATION PHASE

16.4.1 Specification of requirements

To specify the RAM requirement, it is necessary to know which of the RAM properties is important. Degending on process and function either a high reliability or a high availability can be the determining factor.
At this stage general requirements can be defined, while more detailed requirements can be placed later in the contract stage. The level of detail of the requirements is of course also dependent on the design stage of the object in question. A preliminary analysis can be very helpful in this stage.

As stated before, acquiring RAM will generally not come free. While RAM activities may reduce the costs of redesigning and result in less improvisation etc, RAM activities will require a budget and man-hours. Especially if the RAM analyst and manufacturer are uncertain, a high price tag may be presented. The costs of lacking of RAM and benefits of gaining RAM should therefore be known. Ideally, the RAM targets should be selected to optimize the life-cycle costs, conditional upon safety and environmental requirements being met. The targets may have to be adjusted, for example if it becomes clear that no commercial system will show the RAM required.

The costs of lacking of RAM can also be used to specify guarantee clauses. The subject of guarantees will be discussed in section 16.4.4.

The first step in specifying the requirements is acquiring a frame of reference from previous experience. Previous experience is invaluable. Lack of experience makes it much more difficult to establish realistic targets. Table 16.2 gives an example of historical data (experience).

Table 16.2: example of basic RAM information for generator transformers

year	operating hours	number of failures	total failure duration
1973	418200	9	3669
1974	332848	3	28
1975	360962	2	213
1976	356377	2	9
1977	336964	4	209
1978	308641	5	687
1979	311370	1	1
1980	273363	5	420
1981	266457	1	7
1982	224399	3	4700
1983	201036	2	827
1984	209043	3	9674
1985	193087	0	0
total	3842747	40	20444

REMARK: it should be emphasized that the data presented in this table are for illustrative purposes only and cannot be regarded as valid data.

The data from table 16.2 can be used to generate RAM goals. For instance, the average failure rate (λ), the mean time to repair (MTTR) and the average forced unavailability (FU):

$$\lambda = \frac{40}{3842747} = 1.10^{-5} \qquad (16.1)$$

$$MTTR = \frac{20444}{40} = 511 \qquad (16.2)$$

$$FU = \frac{20444}{3842747 + 20444} * 100 = 0.53\% \qquad (16.3)$$

An example of RAM goals for a heat recovery boiler is given below:

HEAT RECOVERY BOILER
The system shall comply to the following quantitative requirements. Compliance shall be demonstrated by the analysis techniques agreed upon.

Planned Unavailability (planned outage)
Overhaul scheme:
1 week in year 1, 2, 3, 5, 6, 7
4 weeks in year 4, 8

Forced Unavailability (forced outage)
80 hours a year based on 8000 operating hours a year

If no historical data are present on the system as a whole, RAM behaviour can be predicted from data or estimates of its constituents. Reliability block diagrams (see reference [16.8]), fault trees and event trees are the standard prediction techniques used. In simple cases the prediction of system RAM behaviour can be estimated by simple addition of the RAM parameters of its components.

Experience is very helpful in deciding for which pieces of equipment RAM requirements should be set. For new systems a FME(C)A is a valuable tooi to focus on RAM. Setting RAM goals will only pay off for those components which dominate the system’s RAM performance.

16.4.2 Communication of requirements

The main issue in the communication of requirements is: **speaking** the same language and being specific. This is of course not an exclusive RAM-related problem. However, the engineering units such as power (kW) or frequency (Hz) are well known and their use in for instance an enquiry specification will not pose any problem as long as the targets are quantitative. Asking for ”a diesel engine with a high enough power rating” is not normal practice and will result in disappointment. The same can be said for RAM requirements; asking for a ”reliable plant” is pointless. RAM requirements have to be quantitative as well. Whether the requirements are stated numerically in the early phases of the specification depends on the following items:

- if RAM requirements are exceptional, numerical values should be presented as soon as possible to emphasize to the tenderer that something special is wanted
- if RAM requirements are of an average nature it can be worthwhile to see what a tenderer is prepared to offer, by only stating that RAM will be an (important) item in the decision process. In the contract the numerical values negotiated for targets and guarantees are included.

In asking for quantitative RAM requirements, two problems can arise:

- the units of measurement are misunderstood;
- the ways to demonstrate the achievement is complicated by mathematical or statistical techniques;

It is the purchaser’s responsibility to state clearly and simply what is wanted and to check whether what he asks for is understood by the tenderer.

The RAM target values should be thoroughly prepared and never unrealistic. Unrealistic values will result in either:

- a very expensive piece of equipment;
- shortfall of the target values

or both.

On the other hand, conservative target values will provide no incentive to the supplier to strive for improvement of RAM values and adding RAM requirements to the contract will prove to be useless.

In communicating what is required, not only the targets and the means to demonstrate their achievement have to be stated but also the operating, maintenance and inspection strategies and the operating modes of the equipment. Especially in the case of RAM guarantees it should be expected that the tenderer will state the need of a minimum set of spares or a maintenance contract. Other important information to supply to the tenderers is:

- the evaluation criteria and methods; for instance LCC-models;
- the importance of the RAM parameters;
- the system boundaries within which RAM is applicable;
- time frame;
- definitions: e.g. what is forced, what is a failure, what is normal preventive maintenance?
- which RAM related tasks are expected from the suppliers?

Having stated what is required is one thing. Getting it is another matter. The RAM parameters are measures of equipment behaviour. These parameters will only be measured on the equipment after it has been procured. Because most of the parameters can only be evaluated meaningfully after a relatively long period, as opposed to thermal efficiency, power rating etc., a difference in measurement results. There are two approaches which can be used separately or combined, in order to get what is required. The first approach is the RAM assurance program and the second is the use of contracted RAM guarantee clauses.

16.4.3 RAM assurance program

The RAM assurance program contains those agreements made between purchaser and supplier to assure the delivery of equipment with the qualities asked for. It states among other things the methods that are used to predict RAM, how to realize it (design!) and how it will be proved and which methods the purchaser will apply for audit purposes.

The program must be matched to the supplier's capability. Therefore, it should be drawn up in close consultation with the supplier.

The following items are essential to the program:

- an organization diagram of the supplier, showing the position of the RAM coordinator responsible for RAM management and coordination. The RAM coordinator should have experience in the field of RAM. In case of lack of experience an external consultant is worthwhile; however, the drive for RAM should come from the purchaser;
- a description of the methods and procedures to model and predict RAM behaviour. Those tools are the same as the tools used to decide what is required, only now the supplier's viewpoint on RAM behaviour is added, after screening, as a new element;
- procedures to implement the results of RAM activities into the design process, for instance by design reviews;
- procedures to follow and control RAM activities during the process. Table 16.3 gives a rough overview of the tasks to be performed in realizing the RAM requirements.

Implementation of the RAM assurance program has to be a joint activity between purchaser and supplier. However, since the supplier should be able to influence RAM from the very start (design, construction, etc.) and should have largest population of (identical) systems to gather RAM information from, it is logical to have the RAM program carried out by the supplier. In practice it often appears that buyers and users have more RAM information than suppliers. In that case information will have to be transferred to the supplier. Checks on progress and contents are made by the purchaser. When dealing with tenderers who are unable or unwilling to cooperate in RAM without an alternative supplier being available, the purchaser has to manage the program ”in-house” or use an external consultant.

Table 16.3: RAM tasks to be performed by purchaser and supplier

Phase, see table 16.1	Task	
	Purchaser	Supplier
1 Specification	- establish RAM goals - evaluate potential suppliers - evaluate RAM methodology - prepare clearly recognizable RAM section of inquiry document.	- provision of historical data - appoint RAM coordinator - prepare RAM response
2 Tender	- Agree RAM content of document, including RAM assurance program	
3 Construction	- monitor progress of RAM tasks - provide response to changes - identify RAM test format	- carry out agreed RAM tasks - supply RAM assessment of equipment to deliver
4 Operation	- perform RAM test - monitor RAM behaviour - feedback of RAM behaviour to supplier	- respond to RAM shortfalls

16.4.4 RAM guarantees clauses

Target values
RAM guarantees may be introduced in the same way as for instance efficiency guarantees. The difference between for instance availability and efficiency is that the former requires much more operating time to arrive at a situation in which the statistical uncertainty is low enough to draw conclusions. The main reason is that failure frequencies are generally low, ranging from 0.1 to 10 per year per system and that the width of the statistical uncertainty is a function of the observed number of failures. This is illustrated in figure 16.1 using the data of table 16.2. In this figure the failure frequency over the observed period and its 5% lower and 95% upper bound are given. The result is based on 13 calendar years with approximately 50 transformers per year. Collecting the same experience with one new transformer would mean an evaluation period of 13 * 50 = 650 years. Measurement over a shorter period, as is illustrated for the years 1980 and 1981, may result in different outcomes.

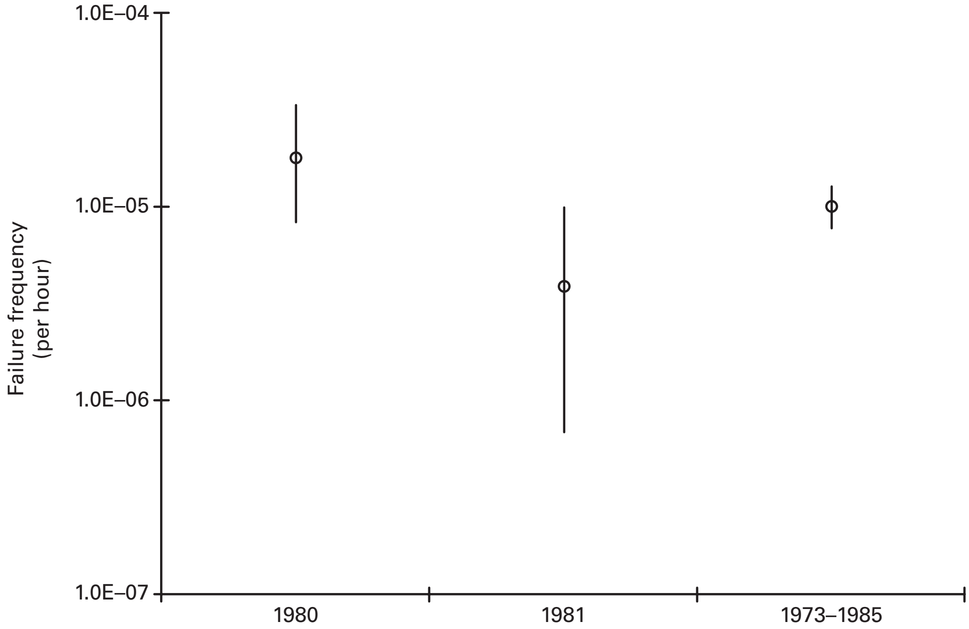


Figure 16.1: Failure frequency and confidence bounds for a generator transformer

REMARK: The data are represented for illustration purposes only and cannot be regarded as valid

Given these statistical aspects of measuring RAM, guarantee values should be not be identical to the RAM targets based on median values of a large population, as the probability of falling short of this value is 50%, but **related** to them. The guarantee value has to be based on:

- the expected number of realizations (e.g. number of failures) in the measuring period;
- the uncertainty in the expected target value;
- the measuring period, and;
- the confidence level applied to the guarantee value (e.g. the 90% upper bound of the target value).

Classical statistical hypothesis testing can be used to evaluate the results during and after the guarantee measurement period. Guarantee values can be constructed, for instance with Monte Carlo simulation.

In figure 16.2 this process is illustrated for a fictitious gas turbine having a mean failure frequency of 10 failures a year and a mean time to repair of 60 hours. The cumulative probability curves are calculated using Monte Carlo simulation.

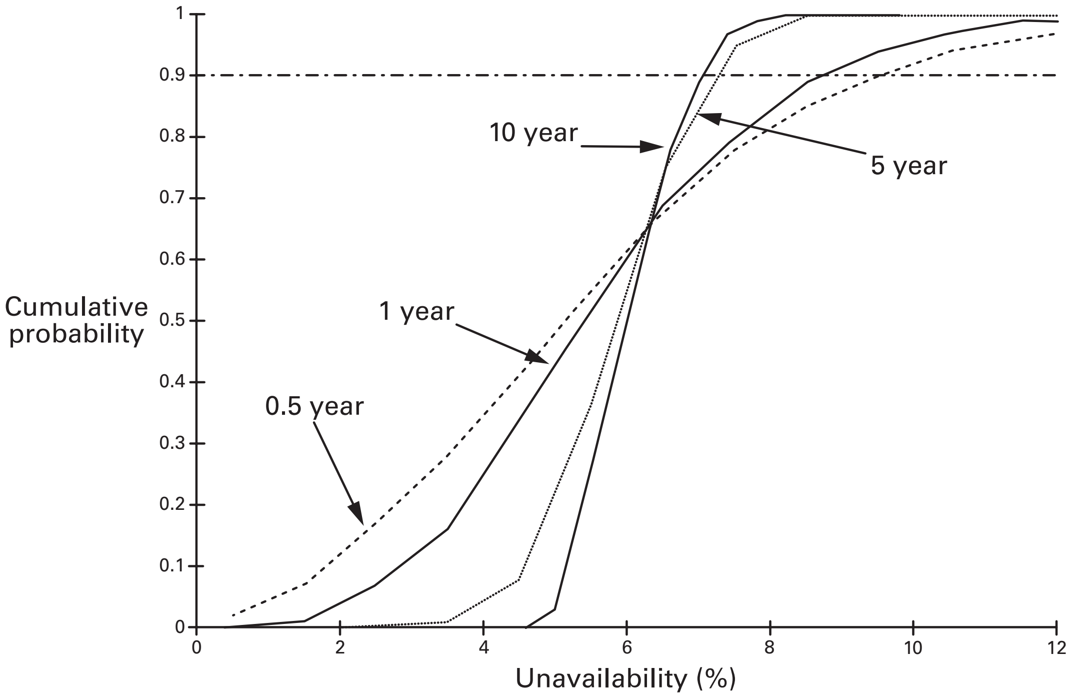


Figure 16.2: Cumulative probability curves of unavailability of a fictitious gas turbine, measurement periods of 0.5, 1, 5, and 10 year

The results illustrate the fact that the guarantee value for the unavailability with a confidence bound of for instance 90% differs widely as a function of the agreed guarantee period. For a half-year period the value is approximately 9.5% and for a 5-year period only 7%, the mean value being 6.3%. The figure shows that in this case a guarantee period in the order of 5 years is necessary before the effects of stochastics dampen to an acceptable level.

Penalties

In using RAM guarantees and penalties it is of the utmost importance that the parameter under consideration is defined very carefully in terms of its function -"what is a failure-, the boundaries within which it is applicable -"is the failure caused by external events or not?"-, and the applicable and excluded process conditions.

The consequences of any shortfall should be clearly stated:

- actions to be taken to repair shortfall;
- effect on guarantee end date, e.g. prolonged measurement period;
- the size of the penalties;
- enforcement of the penalties

When during the measuring period the RAM guarantee value is reached, there should be no discussion about the validity of the data. Therefore, the quality of data collection and analysis has to be assured, for instance by means of a quality system like ISO 9000. The data format, the type of information to be collected and the analysis procedures have to agreed upon before the start of the measurement period.

16.5 TENDER PHASE

16.5.1 Evaluation of the response of the tenderers

The similarity and dissimilarity between the enquiry specification and the tenders is a measure of how effectively the requirements were communicated and an indication of the ability of the tenderers to provide their tenders.

The evaluation of the tenders should include:

- a review of historical data supplied;
- a review of predictive techniques used;
- assessments of
  - the tenderer's RAM capabilities (staff, commitment);
  - cost impact of perceived RAM shortfall;
  - needs for penalty clauses in combination with guarantees;
- review of spare part policy, repair and maintenance requirements and strategy;

This evaluation should leave the purchaser in a position to:

- rank the tender(er)s;
- have a coarse measure of the tenderer's potential in relation to RAM
- draft the RAM documentation for every supplier

16.5.2 Feedback and agreement of requirements

During the feedback stage the discrepancies between what is wanted and what is offered have to be ironed out. The tenderer has to be informed about:

- what is believed to have been offered;
- whether their tenders are acceptable;
- what shortfall exists and what should consequently be altered;

Generally this process will be iterative. Finally it should be clear to the purchaser as welf as to the tenderers what is to be supplied, what is not to be supplied and what actions will be taken in case of shortfall/non-delivery of contracted items.

Interestingly, the discussions held between purchaser and tenderer will in itself have improved the RAM performance. Another spin-off is that it will be clear which tenderers are disinterested in RAM or not familiar with the RAM of their products. However, an interest in RAM will not automatically result in a satisfactory product. This requires further efforts, the burden of which should be shared between purchaser and supplier.

16.6 CONSTRUCTION PHASE

16.6.1 Placement of contract

Depending on the complexity of the item to be purchased, the design is already fixed at this stage or design work has still to be done. In most cases attention will now be focused on maintainability. However, in the latter case refinement of the reliability aspect is also possible.

The contract should clearly state the RAM parameters, the RAM Assurance program and the RAM penalty clauses.

Having asked for RAM-Assurance, the purchaser must now show his commitment to it.

16.6.2 Monitoring progress

Progress monitoring is straightforward in case of a fixed design and a product already on the market, and is restricted to delivery and commissioning. In case of a complex and not fully finalized design, the RAM assurance program should incorporate the evaluation of the effects of changes on the overall RAM targets.

In the construction phase, maintenance requirements should be confirmed, including spares, resources, manuals, Reliability Centred Maintenance schemes (see chapter 17), etc.

It should be clear that this phase is the last opportunity to prevent serious shortcomings in RAM.

16.7 OPERATIONAL PHASE

In this phase the comparison of RAM performance is made with the goals set. RAM parameter data are collected and statistically evaluated. The results are compared with the guarantee values and clauses. A data acquisition and collection scheme is needed to provide the data and information to perform this kind of analysis. If no such scheme exists, its development should be part of the RAM tasks.

With the operating experience the spares and maintenance strategies should be evaluated and reviewed. The data acquisition and collection scheme will serve here as a valuable tool for the next generation of systems.

16.8 REFERENCES

[16.1] ISO 9000-4: Quality Management and Quality Assurance Standards, Part 4 - Guide to Dependability Programme Management

[16.2] IEC 300-1: Dependability Management, Part 1 - Dependability Programme Management

[16.3] IEC 300-2: Dependability Management, Part 2 - Dependability Programme Elements and Tasks

[16.4] IEC 300-3: Dependability Management, Part 3 - Applications Guide

[16.5] BS 5760: Britisch Standard Institute , Reliability of Constructed or Manufactured Products, Systems, Equipments, and Components
Part 1 - Guide to Reliability and Maintainability Management
Part 2 - Guide to the Assessment of Reliability
Part 3 - Guide to Reliability Practices: Examples
Part 4 - Guide to Specification Clauses Relating to the Achievement and Development of Reliability in New and Exsting Items

[16.6] UNIPEDE: Draft Guideline on Dependability Management for the Power Industry, Part 1 - Procurement of Equipment, ref: 01006Ren9507, May 1995

[16.7] Reliability Program for Systems and Equipment Development and Production; Military Standard 785B, MIL-STD-785B, august 1988, DoD Washington

[16.8] AMIR/SPAR, System Engineering Monte-Carlo based advanced software, Malchi Science Ltd., Professor A. Dubi, P.0. Box 1194, Beer-Sheva, Israel.

STRUCTURING OF MAINTENANCE

CONTENTS

17.1 INTRODUCTION

Structuring of maintenance is an activity intended to focus maintenance resources on those components that dominate the overall performance of a plant in terms of production loss, maintenance costs, maintenance activities, (un)planned outages etc. Structuring of maintenance involves the analysis of functional failures of technical systems, with the intention to establish the measures and actions needed to prevent or reduce the likelihood of such failures and their consequences. A system is considered to have failed functionally if it ceases to work as required within the given operating conditions. The measures and actions as suggested by the analysis may be preventive maintenance, modification (design changes), or staff instruction.

In structuring of maintenance activities, two separate phases can be distinguished:

- qualitative phase;
- quantitative phase;

The qualitative phase, commonly named Reliability-centred Maintenance RCM [17.1] results in a list of maintenance activities, recommended modifications and staff instructions, including a priority list for all three of them. The next step is to examine the recommendations from the list on their technical and practical feasibility. Subsequently, the feasible options are subjected to financial scrutiny. The financial viability of certain items is assessed as part of the quantitative analysis procedure [17.3].

The result of both phases is a so-called maintenance plan/concept, being a set of maintenance rules stating how, what, and when maintenance activities have to take place. ”How” is condition-based, use-based, or corrective (breakdown) maintenance. ”What” describes the precise work to be done and includes work instructions, etc, white ”when” states the interval.

A maintenance concept can be made on every level of detail, from a single component up to a complete plant.

Structuring of maintenance is a dynamic, ongoing process. Functional requirements and operating conditions are subject to change, knowledge is constantly being acquired. Maintenance activities have to take this into account. Accordingly the maintenance plan has to be modified regularly. By encouraging a healthy critical attitude at all levels and proper co-operation between the production department, the technical service department and the process engineers, maintenance structuring leads to the rationalization of production and maintenance systems.

In the next few paragraphs the qualitative and quantitative phases of maintenance structuring will be discussed.

17.2 NOMENCLATURE

α	=	slope of simplified bathtub curve	-
μ(TF)	=	mean time to failure of a component	hour
τ	=	test duration	hour
CC	=	corrective (maintenance) costs	NLG
CC_{pr}	=	consequence costs of the process, given a failure	NLG
Cdt_{pr}	=	down time costs of a process	NLG
C_i	=	costs of inspection	NLG
C_{cons}	=	conservation costs	NLG
Cpt_{cons}	=	conservation costs for a given conservation interval t_{cons}	NLG
C_{test}	=	costs per functional testing	NLG
$C_{test,n}$	=	costs of n functional tests	NLG
D	=	number of demands on a standby component	-/hour
E(TC)	=	total expected costs of a component	NLG
E(tr)	=	expected life, given a maintenance interval	hour
FME(C)A	=	Failure Modes Effect (Criticality) Analysis	-
n	=	number of tests	-
P{F | t}	=	failure probability over a period t	-
PC	=	preventive maintenance costs	NLG
R(t)	=	reliability over a period t	-
RCM	=	Reliability-centred Maintenance	-
t	=	test interval, time	hour
T_0	=	random failure period	hour
T_c	=	duration of the corrective maintenance action	hour
t_i	=	inspection interval	hour
T_i	=	optimal inspection interval	hour
t_{cons}	=	conservation interval	hour
T_{cons}	=	optimal conservation interval	hour
t_r	=	maintenance interval	hour
T_r	=	optimal maintenance interval	hour
T_{rev}	=	duration of the preventive maintenance action	hour
Uf	=	mean hidden unavailability of a standby component	-
Z(t)	=	failure frequency at t	-/hour
Z_0	=	random failure frequency	-/hour

17.3 QUALITATIVE ANALYSIS (Reliability-centred Maintenance)

17.3.1 General approach

Maintenance is generally defined as: ”ensuring that physical assets continue to fulfil their intended functions”. It will be clear that for this to be possible the equipment must be capable of fulfilling its intended function to start with. Maintenance - the process of ensuring continuation - can only deliver its designated capacity and can never increase it. The word ”intended” in intended function is essential in maintenance. There are two elements in the intended function: in the first place the operating context and secondly the specific expected performance.
In case the asset is incapable of meeting the desired performance, redesign has to be considered or the performance goals have to be lowered.

In view of the foregoing, Reliability-centred Maintenance is defined as: ”A process used to determine what must be done to ensure that any physical asset continues to fulfill its intended functions in its present operating context” [17.1]. RCM is called Reliability-centred because it focuses on ensuring that a piece of equipment continues to achieve its designated capability or inherent reliability.

In other words, Reliability-centred Maintenance (RCM) is an analysis methodology to assess qualitatively what and when maintenance actions to which component are necessary so that the component or the system will continue to operate as it is intended, and what priority those actions have.

The first stage of RCM is to draw up a list of the systems or components for which structured maintenance is required. Thereafter, the process entails for each of these components that seven standard questions will be asked, as follows:

1: What are the functions and associated performance standards of the asset?
As maintenance means ensuring that assets continue to fulfill their intended functions, maintenance objectives can only be established when these functions are known in combination with the desired performance level. The latter need to be quantified;

2: In what way does it fail to fulfil its functions? An asset fails functionally when it is unable to meet a desired standard of performance.

3: What causes each failure? The modes which cause loss of function enable one to identify mechanisms and to understand which causes are sought to prevent

4: What happens when each failure occurs?
The effect of failure modes cover such issues as downtime, effect on product quality and quantity, and environmental and safety-related problems; This step is important in deciding how much a failure matters and what level and kind of maintenance is needed;

5: In what way does each failure matter?
The consequences, including criticality (how much does is matter in combination with how often does it happen) of each effect is assessed. To structure the analysis, the consequences can be classified into four groups:
- hidden failure consequences:
  the functional failure in itself has no consequences, but in combination with another failure the consequences may be large. Hidden failures are often associated with safety devices. They are given a high priority;
- safety and environmental consequences
- operational consequences:
  A failure has operational consequences if it affects production (quantity, quality, etc.). The amount of money they cost, suggests how much may be or needs to be spend on preventing them;
- non-operational consequences:
  associated costs are only direct costs of repair;

By this structured review of consequences RCM integrates the operational, environmental and safety objectives into the maintenance scheme. It brings safety and environment to the attention of (maintenance) management.
It focuses attention on those activities with the highest impact on performance and at the same time lists those activities which have little or no effect on performance. Essentially, RCM establishes whether each failure has significant consequences. If it does, the question is if preventive steps are possible and what kind of preventive steps can be taken. If not, usually no preventive maintenance is necessary;

6: What can be done to prevent each failure? Is condition or use-based maintenance possible;

7: If prevention of failure is not possible, what else can be done?;
- Depending on the consequences, several options are possible:
- hidden failures: periodic functional testing, redesign
- safety and environment: in principle, redesign or process changes
- operational: corrective maintenance, redesign or process changes
- non-operational: corrective maintenance, redesign or process changes

The whole procedure is comparable with traditional failure mode and effects analysis (FME(C)A, [17.2], see Chapter 7). From the answers to questions 1 to 5 a list of priorities is drawn up and the technical feasibility of preventive maintenance is considered (question 6), for instance using a decision diagram (see figure 17.1). Where preventive maintenance does not appear to offer an adequate solution, the possibility of system modification or staff instruction can be explored (question 7).

Although various decision diagrams are in use, they vary only in their depth and detail. The choice of diagram matters less than ensuring that it is used intelligently; whatever diagram one opts for, activities are selected purely on the basis of their technical feasibility. Financial viability is considered at a later stage.

17.3.2 Who knows what?

It is virtually impossible for maintenance engineers/personnel to answer all seven of the standard questions for every component. Especially the questions 1, 4 and 5 are much better answered by production staff or by operators. One or more project groups - depending on the scope of the project - are therefore set up, in which representatives from the production department as well as the maintenance departments go through the maintenance structuring process together. Ideally, each group contains a facilitator, a representative (supervisor) from the maintenance department, a representative from the production department, an operator and a maintenance engineer, if necessary supported by a technical specialist or process engineer. Ideally, all group members should be trained in RCM or at least have knowledge of the process.

The facilitator's task is to ensure that:
- RCM is applied correctly;
- that each group member understands the questions and that differences in interpretation are prevented;
- reasonable consensus is reached;
- the documentation is completed;

Provided that the company has enough facilitators, several project groups can operate in parallel. The project groups' maintenance proposals and other recommendations can be assessed by middle managers, before being passed on to the maintenance and production managers for approval. The various alternatives are first examined to see whether they are technically feasible; the feasible options are then subjected to financial scrutiny. Financial assessment takes place in the second phase of the analysis.

17.3.3 Standards and indicators

In general it is important to find out how much better the new approach is than the old one. At every level of the organization, people want to know whether they are going about things the right way, or whether they can improve. The answers can often be obtained by reference to standards. When setting standards, it is very often helpful to know what has been achieved in the past; it is then possible to see how one is doing relative to last year or the year before.

Historical and technical data from the production company's database management system are vitally important, since it forms the basis for determining the most appropriate courses of action. The question is, however, what indicators should be used to compare actual performance against the standard. The usual indicators are failure frequency, scheduled unavailability, unscheduled unavailability, cost and attributable man-hours. By regularly quantifying these indicators, it is possible to assess performance and make trend analyses. For proper control of maintenance activities, the relevant data has to be available at all system levels. Plant-level indicators are intended primarily to support strategic decision-making by the plant manager and technical service manager. The production manager and the technical service sector manager will use the indicators mainly to determine their budgetary and manpower requirements. For maintenance engineers and others, system-level and subsystem-level performance indicators will be more useful.

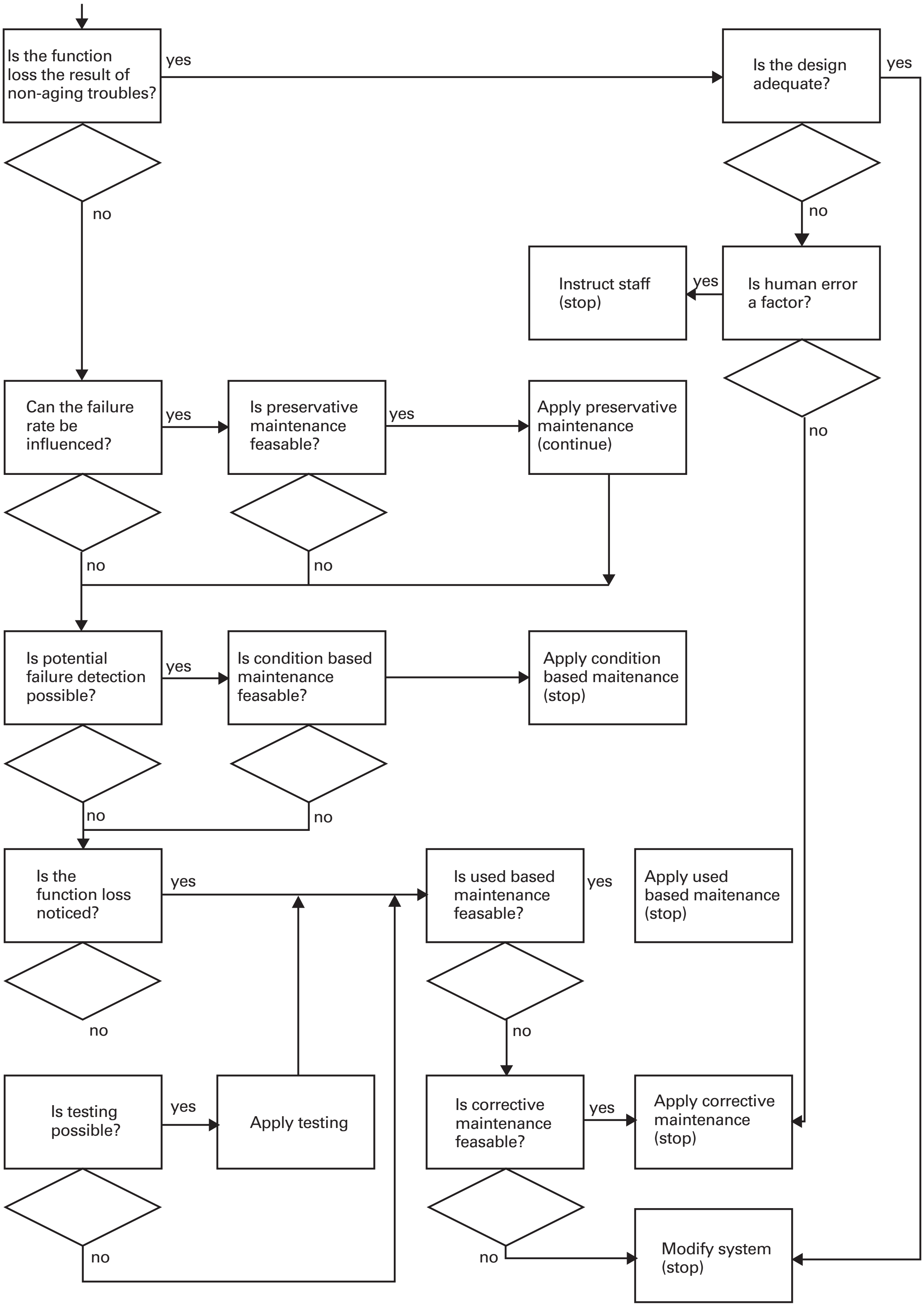

Is the function loss the result of non-aging troubles?
yes
no
Is the design adequate?
yes
no
Instruct staff (stop)
yes
Is human error a factor?
no
Can the failure rate be influenced?
yes
no
Is preservative maintenance feasable?
yes
no
Apply preservative maintenance (continue)
Is potential failure detection possible?
yes
no
Is condition based maintenance feasable?
no
Apply condition based maitenance (stop)
Is the function loss noticed?
yes
no
Is used based maintenance feasable?
yes
no
Apply used based maitenance (stop)
Is testing possible?
yes
no
Apply testing
Is corrective maintenance feasable?
yes
no
Apply corrective maintenance (stop)
Modify system (stop)

Figure 17.1: Typical decision diagram.

To work out failure frequencies and unavailability levels, operating hours have to be logged in the database management system. What this comes down to in practice is recording the dates and times of failures affecting the unit in question. Similarly, the dates and times of the unit's release for maintenance and subsequent release for service have to be noted.

Furthermore, RCM is not simply a matter for the technical service department. Cooperation between the production department and the technical service department is necessary for the improvement of operational efficiency. For this reason, it is important to weigh the cost of maintenance activities against the productivity of the company, in other words the relation between reliability, availability and maintainability should not be forgotten. In section 17.3.2 this relation is discussed.

17.3.4 **Advantages of RCM**

The outcomes of an RCM analysis are fourfold. It greatly enhances the understanding of how the system works, together with the understanding of what it can and cannot achieve. It creates a good insight into the ways a component and system can fait and, maybe even more important, it unearths the root causes of faílures. This makes it possible to allocate resources to the right problems. Furthermore, it produces a list of proposed tasks including maintenance schedules, revised operating procedures and redesign. Last but not least, it promotes team-building.

The advantages of Reliability-Centred Maintenance are not restricted to the area of maintenance; RCM affects the whole plant. it helps the maintenance department in:

- structuring and allocating their resources more adequately by focusing attention on those activities that have the greatest impact on plant performance. Consequently, it reduces the amount of routine work most of the times.
- building a comprehensive maintenance database of all in-house experience, listing all maintenance requirements of the significant equipment used and the skills required. It also provides insight into the spares requirement;

On the company level, it results in:
greater safety and environmental protection, as the safety and environmental implications of every failure mode are taken into account, **before** their effect on operation;

- increased operational security (reliability and availability), resulting from selection of only the most effective maintenance activities;
- extended technical service life for expensive systems, achieved through the use of condition-dependent maintenance;
- greater cooperation between the production department and the technical service department, resulting from the creation of discussion opportunities in multidisciplinary project groups;

Table 17.1: Example of an RCM information sheet.			
UNIT: BLOCK A		**Date:** 11-11-1970	**Sheet:** 1 of 3
Component: Coal pulverizer I	**Component N$_o$:** A-305-I		
Function	functional failure	failure cause	failure effect
1 pulverize coal	A no pulverizing		primary effect: trip of pulverizer; possible decrease in power output of block, depending on redundancy level of pulverizers
			downtime to replace: 1 day
		1 bearing failure	downtime to repair: 2 months
		2 drive failure	see raw coal bunker (A-235-1/4)
		6 no coal	higher amount of unburned fuel, efficiency reduction; downtime to repair: 12 hours
	B particle size distribution	1 classifier failure §	efficiency reduction; downtime to replace: 6 hours
	C to high power consumption	1 roller wear	efficiency reduction; downtime to replace: 10 hours
		2 table wear	reduction in power output and efficiency; no maintenance action possible
			--
			pulverizer outage; time to replace: 4 hours
D	reduction in capacity	1 coal quality	pulverizer outage; time to repair: 2 hours
-------------------------------	-------------------------------------	----------------------------------	--
2 retain coal in system	A No retention	1 seal failure	
		2 wear of skin casing	
-------------------------------	-------------------------------------	----------------------------------	
3			

Remark: Redundancy level of pulverizers is a function of the amount of coal needed and the number of available pulverizers. The amount of coal is a function of coal quality and power rating of the unit.

17.3.5 A Coal Pulverizer

One of the fuels used in generating electrical energy is coal. Before the coat can be burned in a conventional coal-fired unit, the raw coal has to be pulverized. This grinding is done in coal pulverizers.

The first step in an RCM analysis is to define the function of a pulverizer: pulverize raw coal. The associated performance standards are related to grinding quality (particle size and distribution), capacity (ton/hour) and power consumption. Particle size requirements depend on burner type, coal quality (carbon content) etc, but the most common requirement is that 70% of the particles should be smaller than 74 micron. Capacity is of course dependent on pulverizer type. Typical capacities are between 1 and 100 ton per hour, with a power consumption of approximately 10 kWh per ton coal.

The next step is to identify functional failures. Examples are: no pulverizing, insufficient pulverizing (partical size), less pulverizing (capacity drop). Having identified all functional failures, the associated failure modes (causes) are listed. In table 17.1 an example of an RCM information sheet is given. Having collected this information, the next step is to establish the appropriate maintenance action, using a selection diagram as shown in figure 17.1. Table 17.2 illustrates the results of this step.

Table 17.2: Example of RCM worksheet.

Reference from RCM information sheet: no. XXX			Maintenance action	Maintenance interval
function	functional failure	failure cause		
1	A	1	A lubrication and check on clearance, correct if necessary	weekly
			B replace	six months
1	A	2		
1	A	5	....	
1	B	1	check particle size	weekly
1	C	1	monitor power consumption, inspect table and rollers if consumption exceeds Y MW	not applicable

As an example, the first functional failure - failure cause combination (no pulverizing as a result of a bearing failure) will be analysed. The seizure of a bearing is an age-dependent process, so the answer to the first question of figure 17.1 is no: the function loss is a result of ageing. The next question is: can the failure rate be influenced? The answer is yes, by regular lubrication and checking the bearing on clearance and adjusting if necessary. Preserving actions are indeed possible, so the first maintenance action on the bearing is preservation. The interval can be based on experience, for instance once a week. Another possibility of establishing the preservation interval will be shown in section 17.4. Continuing the diagram raises the next question: is condition-based maintenance possible? In principle the answer is yes, bearing vibration can be monitored and analysed, but this technique is not feasible in this case. Furthermore, visual inspection without taking apart the bearing assembly is not possible either. Condition-based maintenance is therefore no option. As the function loss is not hidden, use- based maintenance is an option. Again the interval can be based on experience, but as a coal pulverizer system has redundancy most of the times, corrective maintenance is also a feasible option. The decision in favour of use-based maintenance or corrective maintenance should be based on weighing the costs of the preventive tasks against the cost of repair and the additional costs (for instance, costs of operational and environmental consequences). In the next chapter a method of dealing with this problem as well as the choice of the maintenance interval will be discussed.

The table can be completed by adding for every maintenance action information about personnel, equipment, labour hours and spares required.

17.4 QUANTITATIVE ANALYSIS

17.4.1 Introduction

In the qualitative phase of the maintenance analysis a priority list of technically feasible maintenance activities is drawn up. However, the economical side of the maintenance action has not been taken into account. Although inspection or even condition monitoring of a component can be technically feasible from a economical point of view, the best maintenance action can be corrective maintenance. Parameters influencing the choice for a certain type of maintenance action are, for instance:

- duration of a planned maintenance action;
- spares needed;
- duration of an unplanned maintenance action;
- influence of (un)availability of spares
- additional costs of a failure
  - production loss;
  - additional damage to other equipment;
  - environment;
  - safety;
- (time-dependent) probability of an unplanned maintenance action;

Except the latter, all parameters are costs or can be translated into costs. Consequently, a quantative model with the aim of answering the question which type of maintenance should be applied and how often it should be done, will have to take into account only costs and probability. This answer can be found by solving an optimization problem.

17.4.2 The optimization problem; the relation between reliability, availability and maintenance

Overhauling or replacing a component on a regular basis will shorten its mean life, as of most components the whole life will not be used. Decreasing the maintenance interval will therefore increase the reliability of a component, but at the same time decrease its availability. It should be noted that in case the overhaul interval is reduced too drastically, reliability can start to decrease after a certain interval as a result of possible infant mortality. Associated with this increase and decrease are costs in terms of time (production loss), costs of spares, residual value, man-hours etc. Most of these costs are independent of interval length and as such simply a function of the number of overhauls. But some, the residual value for instance, are time dependent. On the other hand, increasing the interval will reduce reliability and availability as result of a failure, but increases the availability as a result of a reduction of planned maintenance.

The optimization problem is born: finding the minimum of the costs caused by unavailability, resulting from corrective and preventive maintenance costs, residual value, spares etc.

17.4.3 Optimization models

Several models have been developed to solve the maintenance optimization problem. The models are based on a reliability concept and are applicable to all kinds of technical systems. The reliability concept in the models is the use of the failure behaviour of the component as a function of time in the search for a balance of costs between preventive maintenance and corrective maintenance.

Three basic models can be distinguished, based on differences in failure behaviour (hidden failures, revealed failures) and the possibility of condition monitoring by inspection.
The first model optimizes the maintenance intervals of on-line repairable components (components that fail revealed). The second model is applicable to components which fail unrevealed (hidden failures). The third model optimizes inspection intervals.
The fourth model concerns the conservation of technical systems, irrespective of the above-mentioned differences.

17.4.4 Model I: On-line repairable systems

The on-line repairable (= revealed) failure model is a use-based maintenance model which optimizes the maintenance intervals of a production component. The property of a production component is that the component fails revealed (noticeable). The maintenance action is (or is equivalent to) replacement so the component is as good as new after the maintenance action (the renewal process). The model needs cost and failure behaviour information in respect of a given maintenance interval, t:

- Corrective (maintenance) costs, CC
- Preventive (maintenance) costs, PC
- Failure probability, P{F|t}

Corrective costs are the total costs incurred after the occurrence of a failure. It includes replacement costs, downtime costs and consequence costs (damage). If no failure occurs, a preventive maintenance action will take place. These costs include replacement costs and downtime costs, whereby the downtime costs of a preventive maintenance action will be smaller than or equal to the downtime cost of a corrective maintenance action.

Finding the failure probability, for instance in the form of a bathtub curve is often the most difficult part of maintenance optimization. Most of the time there is no failure versus time relation readily available. Still, one needs to know the failure probability to optimize maintenance.

To build a mathematical model for the failure behaviour, different sources of information and levels of detail can be used, for instance:

- a ”simplified” bathtub curve
- a (Weibull) distribution, which has been fitted to (plant-specific) data
- a (remnant) life model describing failure probability as a function of process and equipment parameters and time.

The simplified bathtub curve is a solution to the problem of modelling failure behaviour when no or practically no data are available. The bathtub curve is constructed using Expert Opinion (see chapter 4 for (im)possibilities and problems). To make a simplified bathtub curve, one needs an estimation of the mean time to failure of a component μ(TF), the random failure period T_0 and the number of random failures per time period Z_0. These three parameters determine the simplified bathtub curve, which is based on a negative exponential distribution function in the random failure period and is based on a Weibull distribution function with shape parameter $\beta = 2$ in the period after T_0. Figure 17.2 shows a simplified bathtub curve. During the random failure period from $t = 0$ to $t = T_0$, the failure frequency (Z_0) is independent of time. After $t = T_0$ the failure frequency increases lineally with time. The slope of the curve (o) is determined by the three parameters.

In formula:

For $t <= T_0$:

the failure rate is constant:

$$Z(t) = Z_0$$

and the failure distribution function is:

$$P[F \mid t] = 1 - e^{-Z_0 t} \tag{17.1}$$

For $t >= T_0$:

the failure rate becomes:

$$Z(t) = Z_0 + \alpha(t - T_0) \text{ and } \alpha > 0$$

The failure distribution function is:

$$P[F \mid t] = 1 - e^{-Z_0\ t - \frac{1}{2}\ \alpha(t\ -\ T_0^2)} \qquad (17.2)$$

Introducing Reliability R(t) = 1 - P{F|t}, a can be calcuiated by solving numerically:

$$\mu(\mathrm{TF}\ ) = \int_0^\infty \mathrm{R}\ (\mathrm{t}\ )\ \mathrm{dt} \qquad (17.3)$$

The total expected costs of a component E(TC) is defined as the sum of corrective costs CC times failure probability P{F|t} and preventive costs PC times reliability R(t). These expected costs are made in a cycle, E(t) (the mean lifetime given the maintenance period tr. In formula:

$$\mathrm{E(TC|tr)} = \mathrm{CC}\ .\ \mathrm{P\{F|tr\}} + \mathrm{PC}\ .\ (1\text{-}\mathrm{P\{F|tr\}})$$

$$\mathrm{E\ (tr)} = \int_0^{\mathrm{tr}} \mathrm{R}\ (\mathrm{t}\ )\ \mathrm{dt} \qquad (17.4)$$

Minimizing the expected costs per cycle gives an optimal maintenance intervalTr. See fig 17.2.

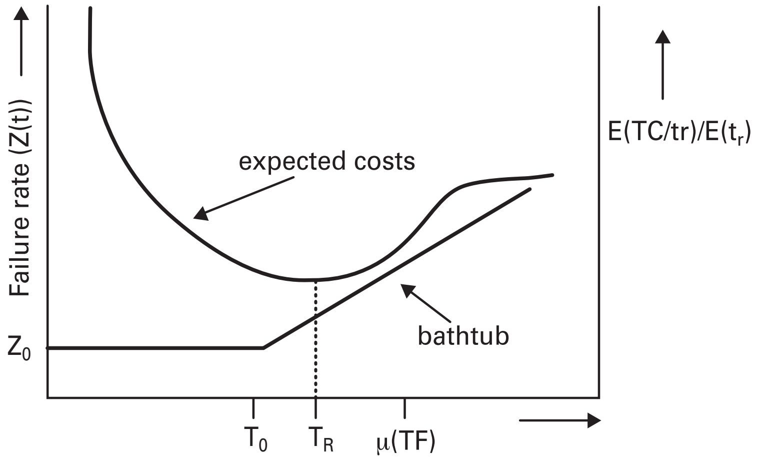


Figure 17.2: Simplified bathtub curve and expected cost curve as function of maintenance interval.

17.4.5 MODEL II, periodically tested systems

This model is applicable for components with hidden failures, for instance safety devices. The model takes into account the possible unavailability of a standby component at the unpredictable moment of a process demand. If the component is not available due to a hidden failure, testing or maintenance, high consequence costs are made (explosion, very long downtime of the process).

The main difference between models I and II is that an optimal maintenance interval in case of hidden failures wilt be achieved only if the test interval is optimal. Because of the fact that an optimal test interval is dependent on the maintenance interval, finding the optimal maintenance interval is an iterative process. This is illustrated in figure 17.3. In this figure two expected costs curves are shown, belonging to two different test intervals. Each curve has its own optimum maintenance interval. However, the expected costs differ in this optimum. As the costs in the case of curve 1 are lower than those of curve 2, the test and maintenance interval belonging to curve 1 is an optimum.

The total expected costs of a model II component are divided into two parts:
- the standby part
- the process part.

The standby part
The standby part of the total expected costs, $E(TC_{stb} \mid tr,t)$, is equal to the total expected costs of model I. Only the test costs, $C_{test,\ n}$, if there are any, have to be added:

$$C_{test,\ n} = n \ . \ C_{test}$$

where
- n is the mean number of tests per cycle
- C_{test} is the costs of one test.

This results in the following formula for the total expected costs of the standby component:

$$E(TC_{stb}|t_r,t) = CC \ . \ P\{F|t_r\} + PC \ . \ (1 - P\{F|t_r\}) + n \ . \ C_{test}$$

The process part
The costs or risks of the process part are associated with and determined by three situations of the stand-by component:
- it failed hidden
- it is tested
- it is maintained

In the last two situations one has to differentiate between the possibility of stopping or continuing operation during testing and maintenance. Stopping or not stopping is not applicable in case of the hidden failure situation.

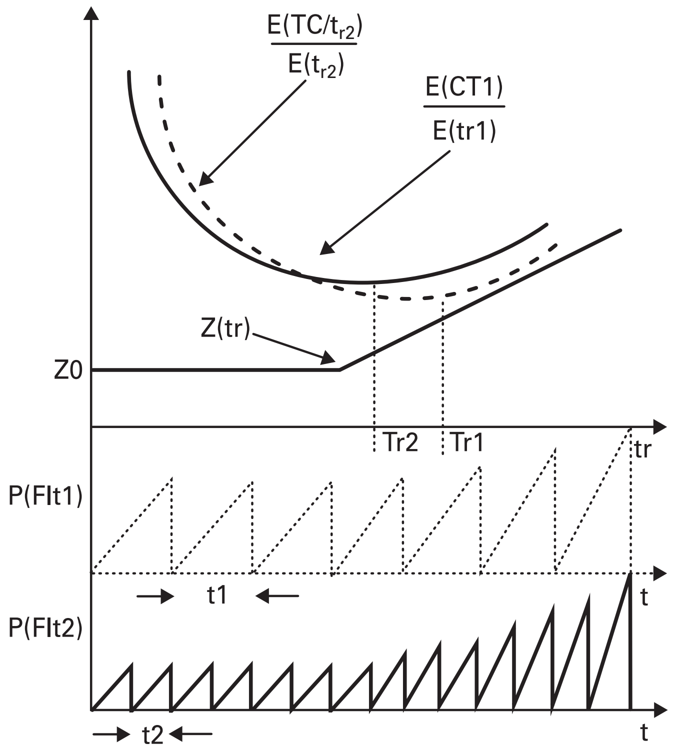


Figure 17.3: Two different combinations of test and maintenance intervals.

Hidden failure:

The risk due to a hidden failure of the standby component is given by:

$$\mathrm{Uf}\ .\ \mathrm{D}\ .\ \mathrm{CC}_{pr}$$

where:

$$\mathrm{Uf} = \sum_{i=1}^{n} \int_{t_{i-1}}^{t_i} \mathrm{P}\ [F_i\,|\tau]\ d\tau \text{ and } t_i = t_{i-1} + t \qquad (17.5)$$

D = number of demands per unit of time of the process on the standby component;
CC_{pr} = consequence costs of failed process

Testing:

If the process is stopped during a test, the contribution to the total risk due to testing will be:

$$n\ .\ \mathrm{T}\ .\ Cdt_{pr}$$

where
n = the mean number of tests per cycle
T = the test duration and
Cdt_{pr} = the downtime process costs per time period.

If the process is not stopped, the downtime process costs Cdt_{pr} become a risk, equal to the risk resulting from hidden failures: D . CC_{pr}

Maintenance:

If the process is stopped during maintenance, the contribution to the total expected costs because of maintenance will be

$$[P\{F|tr\}\ .\ Tc\ +\ (1 - P\{F|t_r\})\ .\ T_{rev}]\ .\ Cdt_{pr}$$

where
T_c = the duration of the corrective maintenance action on the standby component
T_{rev} = the duration of the preventive maintenance action (revision) on the standby component

Again, if the process is not stopped, the downtime costs Cdt_{pr}, become a risk D * $CC_{pr.}$

Total expected costs of maintenance, testing and hidden failure:
As Uf and n are functions of the test interval t, the total risk is a function of tr as well as t. In formula:

$$E(TC|t_r,\ t) = E(TC_{st}|t_r,t) + E(TC_{pr}|t_r,t)$$

where:

$$\begin{aligned} E(TC_{pr}|t_r,t) = {} & Uf\ .\ D\ .\ CC_{pr}\ + \\ & [n\ .\ \mathrm{T} + P\{F|t_r\}.T_c + (1\text{-}P\{F|t_r\})\ .T_{rev}]\ .\quad [X\ .\ D\ .\ CC_p + (1\ \text{-}\ X)\ .\ Cdtt_{pr}] \end{aligned}$$

where :
X = 0 if the process is stopped
X = 1 if the process is not stopped

$$P\ [F_i|\mathrm{T}]\ =\ 1\ -\ e^{\int_{t_{i-1}}^{t_i} Z\ (s)\ ds} \tag{17.6}$$

As in model I, the total expected costs have been made in a cycle $E(t_r)$. Minimizing the total expected cost per cycle gives an optimal maintenance interval T_r given a test interval t. By varying the test interval t the optimal combination of t and T_r can be found in an iterative way.

17.4.6 MODEL III, Inspection

Model III is a condition-based maintenance model which optimizes the inspection intervals of a component and predicts when a replacement action has to be taken, given the mean residual lifetime.

The model again needs costs and failure behaviour information in respect of a given lifetime T:

1: Corrective (maintenance) costs, CC
2: Preventive (maintenance) costs, PC
3: Inspection costs, C;
4: Failure probability, $P(F\ t_r,T)$

Corrective and preventive costs are defined in the same way as in model I. The inspection costs are incurred every time the component is inspected. The failure probability concerns the probability that the failure prediction property reaches a limit during the next inspection period, given the present lifetime of the component. So condition-based maintenance is only applicable if such a failure prediction property exists. Furthermore, neither the preventive costs nor the difference between corrective and preventive costs are allowed to be higher than the inspection costs.

The inspection risk of a component IR is defined as the sum of the difference between corrective and preventive costs CC-PC times the failure probability and the inspection costs C; times the reliability:

$$E(IR|t_i) = (CC - PC) \ . \ P\{F|t_r\} + C_i \ . \ (1 - P\{F|t_r\})$$

This risk is incurred in a cycle $E(t|t_i,T)$, the mean lifetime given the inspection period t_i and the present lifetime T. Minimizing the risk per cycle gives an optimal inspection interval T_i. A replacement action has to be taken when the inspection risk becomes too high or when the inspection interval becomes too small.

17.4.7 MODEL IV, conservation

Model IV optimizes the conservation interval of a component and predicts when a replacement action has to be taken, given the conservation frequency.

The model needs cost and failure behaviour information:

1: Corrective replacement costs, CC
2: Preventive replacement costs, PC
3: Conservation costs per time unit, given a conservation interval t_{cons}: Cpt_{cons}
4: Failure probability, $P(F|t,t_{cons})$

Corrective and preventive costs are defined in the same way as in model I. The conservation costs are incurred every time a conservation action takes place. Generally the conservation costs are not constant, but they are a function of the conservation frequency. The failure probability concerns the probability that the component will fail given a certain conservation frequency. So the failure probability is also a function of the conservation frequency. The impact of conservation on the shape of the simplified bathtub curve is shown in figure 17.4. The impact of different conservation intervals on the parameter T_0 is shown in figure 17.5, and the possible relationship between C_{cons} and t_{cons} is given in figure 17.6.

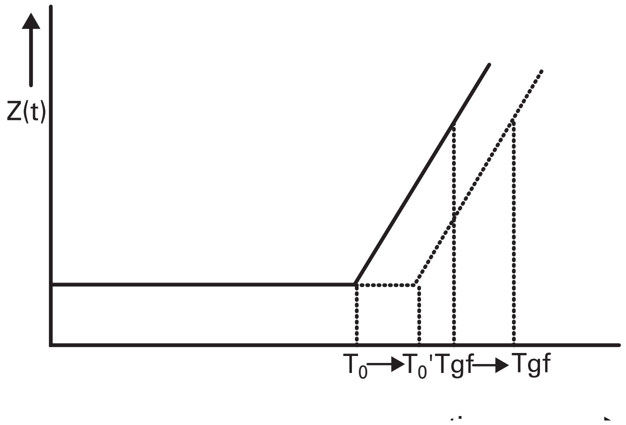


Figure 17.4: Impact of conservation on the simplified bathtub curve.

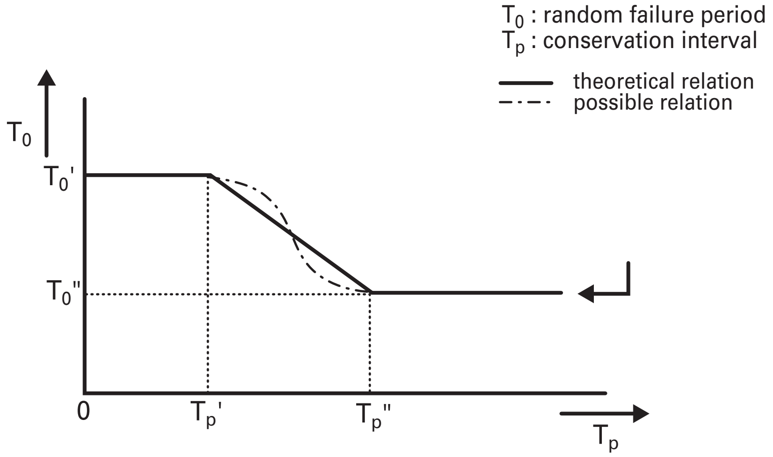


Figure 17.5: Impact of the conservation T_p on the random failure period characterized by the location of T_0.

Again the total expected costs of a component are defined as the sum of corrective costs times failure probability and preventive costs times the reliability. These total expected costs are made in a cycle E(t|t_c, t_{cons}) (the mean lifetime given the maintenance period t, and the conservation interval t_{cons}). Minimizing the expected costs per cycle plus the conservation costs per time unit Cpt_{cons} gives an optimal maintenance interval T, given the conservation interval Cpt_{cons}.
Comparing the minimum total expected costs per cycle for every conservation interval ton, gives the optimal conservation interval T_{cons} and the optimal replacement interval T_r.

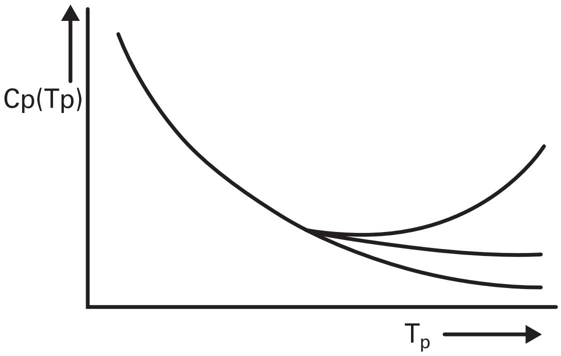


Figure 17.6: Possible relations between conservation interval (Tp) and conservation costs (Cp(Tp)).

17.4.8 A coal pulverizer

The RCM analysis of the coat pulverizer resulted in condition-based maintenance for the rollers. It is impossible to establish the condition of the roller bearings, monitoring the power consumption. These bearings are normally maintained on use-based level. Plant X uses a two-year interval, coupled to the normai overhaul/main inspection schedule of the boiler. The second reason for the two-year interval is the fact that no redundancy in pulverizing capacity is available. Failure of one of the six pulverizers results in an approximately proportional reduction in MWe output.

The question can be raised, however, if the two-year interval used is the optimal interval. With model 1 this question can be answered.

The model needs information concerning the life expectancy of the components and costs.
A pulverizer has three rollers and two bearings per roller. Replacement costs of the bearings are six times NLG 2000 plus NLG 1000 labour costs. The down time in case of a planned replacement is 8 hours and in case of a bearing failure 12 hours, due to an extra 4 hours, logistics time. The additional costs of unplanned unavailability are approximately 1660 per hour, resulting in NLG 20,000 per failure.

From interviews with maintenance personnel and information from maintenance records, the following conclusions could be drawn concerning the life expectancy of the bearings. The random failure rate is practically zero. The random failure period is 1.5 years and the mean life time 2 years.

Input and results are given in table 17.3. The optimum maintenance interval under the conditions stated above is 24.35 months (the shaded column 4 of table 17.3). So it can be concluded that the interval used at the moment is indeed the optimum interval and that no changes have to be made. In figure 17.7 the total expected costs per unit of time are given. The curve (no. 3) has a minimum at approximately 24 months. Curve 1 shows the expected costs of corrective maintenance and curve 2 those of preventive maintenance.

Table 17.3: Input and results of Model I; optimum maintenance interval for bearings of coal pulverizer rollers

INPUT

```
 Component                : roller bearing
 Dimension                : month
 Distribution type        : Simplified bathtub curve
 T0                       : 18      months
 Z(t=0)                   : 1e-6    per month
 Tgf                      : 36      months

 Replacement costs                      : 13000      Nlg
 Repair time in case of failure         : 12    hour
 Planned revision time                  : 8     hour
 Additional costs in case of failure    : 20000      Nlg

RESULTS
 Kg          [Nlg]  :       0.00   10000.00   20000.00   30000.00   40000.00   50000.00
 Tr       [months]  : Corrective      29.44      24.35      22.42      21.40      20.77
 Ztr   [per month]  :      0.028     0.0096     0.0039     0.0021     0.0013    0.00089
 Ktr   [Nlg/month]  :     360.95     554.46     615.17     643.41     659.80     670.51
```

As the additional costs, being mainly the costs associated with replacement power are the only parameter that can change significantly, a sensitivity analysis is carried out on this parameter. The first column of table 17.3 shows the result in case these costs are zero. This situation applies for instance in case of redundancy in pulverizing capacity. The optimum strategy in this case is corrective maintenance. In case the power replacement costs are NLG 50,000 the optimum maintenance interval is still approximately 21 months (20.77, see table 17.3), which indicates that the optimum interval is not very sensitive to changes in replacement power costs.

However, as 21 months does not tie in with the normal overhaul scheme of the boiler, the best option is 24 months. As this is not the optimum, the associated risk will be higher. This risk is represented by the total expected costs per time unit (Ktr): NLG 670.51. The extra risk as a result of not using the optimum interval can be determined from graphs like the one given in figure 17.7. This increase in risk has to be weighed against the extra costs of a planned stop at 21 months in this case.

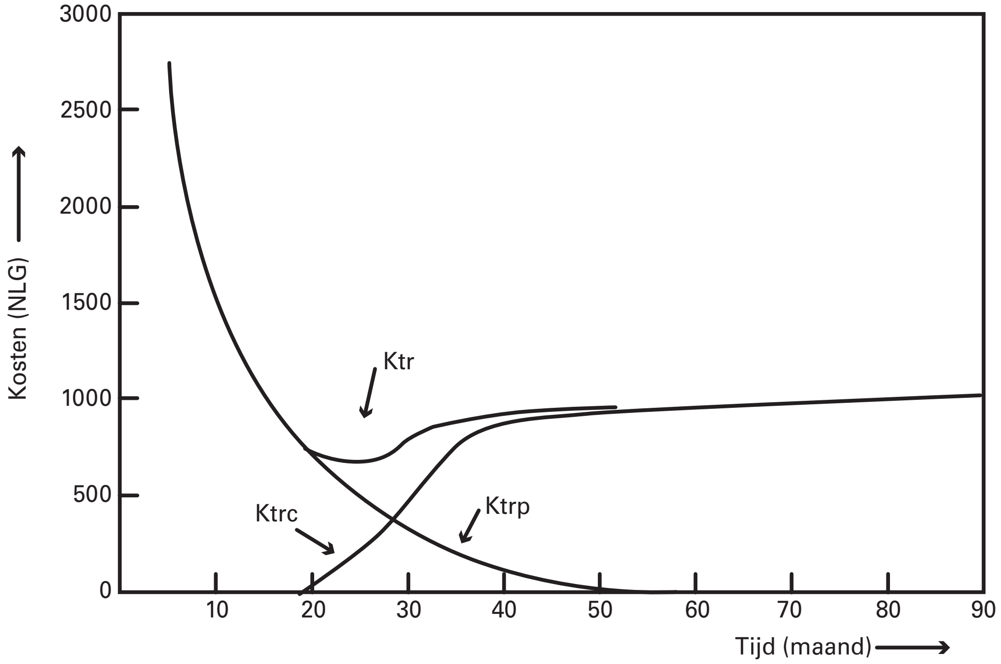


Figure 17.7: Expected preventive maintenance costs (curve Ktrp), expected corrective maintenance costs (curveKtrc) and total expected costs (curve Ktr) as function of maintenance interval.

17.5 REFERENCES

[17.1] Moubray, J.M., (1991), Reliability Centred Maintenance, Butterworth Heinemann Ltd, Oxford, ISBN 0 7506 02309.

[17.2] Hazard and Operability Study Why? When? How?, Report of the Directorate-General of Labour, First Edition 1982, Publication of the Directorate-General of Labour of the Ministry of Social Affairs and Employment, P.O. Box 69, 2270 MA Voorburg, the Netherlands,
(ISBN 0166-8935 AIR 3E/8207).

[17.3] Industrieel Onderhoud [Industrial maintenance], Van Gestel, PJ, KEMA report no. 21548-MAP-1, KEMA 1992; P.J. van Gestel, P.O. Box 9035, 6800 ET Arnhem, The Netherlands.

[17.4] KMOSS handleiding, KEMA 1994; P.J. van Gestel, P.O. Box 9035, 6800 ET Arnhem, The Netherlands.

[17.5] Smith, A.M., (1993), Reliability Centered Maintenance, McGraw-Hill, Inc,
ISBN 0-07-05p9046-X.