RELIABILITY MODELING AND PREDICTION

Modelovanje i predviđanje pouzdanosti

BIBLIOTEKA
DQM MONOGRAFIJE
"KVALITET
I POUZDANOST
U PRAKSI"

THE LIBRARY
DQM MONOGRAPHS
"QUALITY
AND RELIABILITY
IN PRACTICE"

Dr Andrés Carrión García
Dr Ljubiša Papić

RELIABILITY MODELING AND PREDICTION

Modelovanje i predviđanje pouzdanosti

8

Istraživački centar za upravljanje kvalitetom i pouzdanošću
The Research Center of Dependability and Quality Management
DQM, Prijevor, 2015.

Dr Andrés Carrión García
Dr Ljubiša Papić

RELIABILITY MODELING AND PREDICTION

Recenzenti:
Dr Joseph Aronov
Dr Miomir Stanković

Biblioteka:
DQM Monografije "Kvalitet i pouzdanost u praksi", Broj 8

Izdavač:
Istraživački centar DQM
Pošt. fah 132, 32102 Čačak,
E-mail: dqmcenter@mts.rs; Telefoni: (032)883610, (064)1374442

Za izdavača:
Dr Ljubiša Papić

Korektura:
Neda Papić

Priprema za štampu:
Istraživački centar DQM

Štampa:
Štamparija Bajić
Vukašina Ignjatovića 12, 32103 Čačak

Tiraž: 100 primeraka

Godina: 2015.

CIP - Каталогизација у публикацији - Народна библиотека Србије, Београд

621-192
519.873

КАРИЈОН Гарсија, Андрес, 1958-
Reliability Modeling and Prediction = Modelovanje i predviđanje pouzdanosti / Andrés Carrión García, Ljubiša Papić. - Prijevor : Istraživački centar za upravljanje kvalitetom i pouzdanošću = The Research Center of Dependability and Quality Management, 2015 (Čačak : Bajić). - XII, 186 str. : ilustr. ; 24 cm. - (Kvalitet i pouzdanost u praksi : biblioteka DQM monografije = Quality and Reliability in Practice : library DQM monographs ; 8)

Tiraž 100. - About the Authors: str. 185-186. - Bibliografija: str. 172-178.

ISBN 978-86-86355-20-1
1. Папић, Љубиша, 1952- [аутор]
a) Технички системи - Поузданост b) Теорија поузданости
COBISS.SR-ID 220457996

The Depertment of Applied Statistics, Operations Research and Quality, Polytechnic University of Valencia, Valencia, Spain

The Research Center of Dependability and Quality Management – DQM
Prijevor, Serbia

Reliability is, after all, engineering in its most practical form.

James R. Schlesinger
Former United States Secretary of Defense,
from 1973 to 1975 under Presidents Richard Nixon
and Gerald Ford

CONTENTS

PREFACE

Technological revolution contributed to the strong increase of systems complexity, which was in particular distinctively for contemporary aircrafts, motor vehicles, petroleum and chemical facilities, metallurgic systems, nuclear power plants. Contemporary complex systems are characterized by largely branched technological subsystems, a great number and variety of equipment, complexity of algorithms control. That brought to the fact that the reliability assurance issue became the key problem of modern complex systems.

Lawfulness of systems failure occurrence and renewal of its operational capability are being investigated by reliability theory, the impact of external and internal influences on operating processes which are happening within systems are being investigated, calculation methods of systems against reliability and failure prognoses are being developed, modes, methods, means for increasing reliability in system designing and exploiting are being researched and also methods of collecting and recording and statistical data analysis which characterize system reliability are being defined.

Reliability theory is defined as:

"Scientific discipline which investigates and studies methods of providing operational effectiveness in the process of system operation".

Reliability theory studies: reliability criteria and characteristics, methods of reliability analysis, methods of reliability modeling and prediction, methods of reliability increase, methods of system reliability testing, methods of system exploitation and maintenance considering their reliability.

Modern engineers come into touch with complex systems, which requires knowledge about different problems (issues). However, seeking for necessary data and information usually generates significant difficulties because they are scattered in numerous books and journals.

Authors of this book have tried to remove such difficulties and to explain wide enough circles of questions relevant for modeling and prediction of system reliability. In this way, this book could be useful practical source for engineers which try to enter the systems reliability field. Book is suitable as material for university course about system reliability field for students of almost every engineering discipline, on graduate, MSc and PhD studies who are interested in reliability problems. The book contains enough material for single semester subject (course) emphasizing basics and appliance of classical reliability engineering.

This book, as a serious task, represents the result of perennial cooperation in researching and in university teaching between Department of Operational Research, Applied Mathematics and Quality (Polytechnic University of Valencia), Valencia, Spain and Research Center of Dependability and Quality Management, Prijevor, Serbia, during the period of 15 years (2001-2015). Through this monograph authors tried to provide basic knoledge from the field of reliability theory, failure analysis, safety analysis and systems maintenance concept, which could be useful for reliability modeling and prediction during design, testing and exploiting different human made systems for obtaining maximal effectivenes of their operation.

Valencia – Prijevor, 2001-2015. Dr Andrés Carrión García
Dr Ljubiša Papić

Chapter 1

HISTORICAL PERSPECTIVE

1.1 A BRIEF HISTORY OF RELIABILITY

As technological advances have allowed us to develop equipments and infrastructures of increasing complexity, new models and theories have been required to deal with problems of parallel increasing difficulty. The complexity present in design, production, exploitation and maintenance of modern systems, demands the more capable engineering approach to adequately face up systems reliability assurance in an increasingly demanding socio/industrial environment.

Technological development is in connection with the creation of more complex systems, appliances, devices, gauges, tools and equipment, with quality requirements each time more strict and able to play their functions in harder and more demanding conditions. All this facts are un roots of the creation of scientific disciple: reliability engineering [1].

The history of reliability engineering development could be described through four stages [2].

The first stage (up to the 1950's) – defining a research problem and forming a scientific discipline. During World War II, war actions were not only in the military battlefield, but also in the scientific-technical field. Germans were striving to develop new revolutionary weapons, facing new technical challenges that require new methodologies. During the developments of V1 "fling bomb", the mathematician Eric Pieruschka formulated for the first time what we can call today a "reliability model". After the war, systematic researches on durability and reliability of technical systems were developed, and the key indicators for survival and reliability were identified and defined.

The second stage (in the 1960's) – creation of classical reliability theory. Four initiatives were distinctive for this period: the beginning of system durability and reliability study in the stage of designing; the development of calculation method for the system elements on the basis of statistical reliability data; the organization of statistical data collecting and statistical data processing on reliability; and the evaluation of durability, reliability and maintainability indicators.

The third stage (in 1970's) was characterized by system approach to the system reliability analysis on the basis of technical-economical indicators and system development perspective. The durability, reliability and exploitation maintainability management methods based on statistic data analysis about system's item failure, considering cost for their operational capability were developed and have found wide application in engineering in this period.

The fourth stage (contemporary) predicts preparation and introduction of stages' set for reliability assurance of the main elements in designing, production and system use. These stages are prepared on the basis of physical essence analysis results and validity (lawfulness) of the process alteration which happens in elements as well as in the system ensembles in the period of their use.

This progress of system reliability investigation, from statistic description towards physical processes analysis is not accidental. It is explained by the law of transition from quantitative to qualitative changes. First operative stages within the system reliability assurance were in connection with collecting data, their generalization and analysis. Because of complexity of the system technical condition change and absence of engineering methods and tools for recording these processes, investigations were limited on collecting statistical data about failures and items' degradations. In other words, using systems theory terminology, it is noticeable that system reliability investigations were performed on macro level, not considering processes that cause changes of basic elements and items technical conditions. This assured the possibility of quantitative durability assessment without considering (unknowing) "mechanism" of the system reliability decreasing [2].

A significant attribute of our time is more extensive use of fundamental natural sciences achievements solving specific engineering problems, particularly reliability engineering problems. Principled new possibilities for performing experimental researches in solving system reliability assurance problems have been discovered.

Contemporary physics of failure researching methods and experimental equipment, which was built latter years, enables not only recording of changing process of technical condition of system's elements and items, but also assessment of influence of main factors on those processes streaming attributes. In this manner, necessary conditions for performing operational capability analysis of elements and items on system micro level have been created nowadays. That enables more accurate argumentation of reliability assurance stages.

1.2 THE NEED FOR RELIABILITY

In the beginning of 1950's, reliability issues, foremost reliabilities testing and reliability increasing issues of missiles and electronic equipment began to draw in attention of mathematicians – statisticians as well as engineers involved in researching of complex military and industrial systems. Therefore, the emergence of new branch of science - reliability theory, was considered as very natural, and subsequently also biological, economic and other kinds of systems.

The other half of XX century was characterized by occurrence of machines and systems of high design complexity for performing complicated tasks. However, in the process of their operation the amount of quantity of failures began to increase. Failures of complex systems brought to risk for operators, maintenance personnel and environment [3]. Very severe accident on the section II of Three Mile Island (SAD) nuclear power plant in March of 1979, the effusion of toxic gases within Bophal (India) chemical plant in December of 1984, the explosion of multiples Space Shuttle Challenger (in January of 1986) and Columbia (in February of 2003), destruction of the fourth section of Chernobyl nuclear power plant (Ukraine, in April of 1986), explosion of Kursk nuclear submarine (Russia, in August of 2000), series of air crashes and others, demonstrated that reliability issue of complex systems is still far from its solution.

Chapter 2

STATISTICAL BASIS OF RELIABILITY

2.1 RELIABILITY STUDY MOTIVES

The study of the reliability is in good measured a statistical study. This is thus by several motives:

- the models used to represent the life of a system until its failure are statistical models,
- the estimation of the parameters of those models is accomplished through experiment, employing an statistical estimation process,
- the analysis of the behavior of systems formed in base to different systems requires, for the evaluation of the reliability of the system using the information of that of the elements, the use of techniques based on the probabilities calculation.

In consequence, being the methodology used in the analysis of the reliability a statistical methodology, we will proceed below to a short review of those concepts that will be here of interest.

2.2 PROBABILITY CONCEPT

Seeking an intuitive form of defining the probability, we can say that the probability of a result in a certain random experience (affected by the random) is the limit of the relative frequency with which is presented this result in a very large number of repetitions (trials) of the experience [4].

Without be the ideal formulation of the probability concept (for instance, this definition don't considers all those cases in which it is not possible the accomplishment of a "great" number of experiences), it results at least adequate concerning interpretation of the sense that has the probability within field of the reliability [5].

For example, if we consider the probability of obtaining a 5 upon launching a dice, the known rule of Laplace (favorable cases / possible cases) preach that that value will be 1/6, but this only it will be certain the this dice is perfectly balanced, with all their sides having the same probability.

On the other hand, with this definition that we have just exposed, the calculation of the probability would be accomplished repeating many times the launching and obtaining the value limit from the relative frequency. If the dice is correct, that frequency would have to be 1/6, but with this definition would be obtained the correct value from the probability, even with laden dices, in which the results are not equiprobable.

If we wished to calculate the probability that has a system of surpassing a certain duration, with the probability definition that we have seen, the calculation would require the accomplishment of a trial with a great number of elements and the control of the fraction of those which survive. In any case, and independently of what interpretation is granted to the probability of an event, we can define precisely which is the concept and what are its properties from a mathematical point of view.

Consider a random experience in which E is the set of results or sample space, and consider one of the results of that experience, A ($A \in E$). Consider also the class of events, F, that is, those on which it has been defined probability, having this set F a structure of a σ-algebra [6].

We will call probability of the event A to the application defined from the sample space E to the real rectum:

$$E \xrightarrow{p(A)} \Re$$

that it fulfils the following axioms:

A1) The probability of any event is not negative:

$$p(A) \geq 0, \ \forall \ A \in E.$$

A2) The probability of the sure event is one:

$p\ (E) = 1.$

A3) The probability of the union of disjoint events is the sum of its probabilities:

$\forall\ A,B \in \boldsymbol{F}^2\ /\ A\cap B = \varnothing,$
$p(A\cup B) = p(A) + p(B).$

From these axioms, the following properties can be demonstrated:

- Probability of the opposite event:

$\forall A\in \boldsymbol{F},\quad p(\overline{A}) = 1- p(A)$

- Probability of the impossible event:

If $\varnothing$ is the impossible event, then $p\ (\varnothing) = 0$.

If $A\subset B,\ A,B \in \boldsymbol{F}^2$ then

$p(A) \leq p(B)$

- The probability of any event lays between 0 and 1:

$\forall A \in \boldsymbol{F},\quad 0 \leq p(A) \leq 1$

- Probability of the union of two events:

$\forall A,B \in \boldsymbol{F}^2,\quad p(A\cup B) = p(A) + p(B) - p(A\cap B)$

and as a rule, for more than two events:

$$\begin{aligned}
&\forall A_1, A_2,\dots A_n \in \boldsymbol{F}^n,\\
&p(A_1 \cup A_2 \cup\dots A_n) = p(A_1) + p(A_2) + \dots + p(A_n) -\\
&- p(A_1 \cap A_2) - p(A_1 \cap A_2) - \dots\\
&+ p(A_1 \cap A_2 \cap A_3) + p(A_1 \cap A_2 \cap A_4) + \dots\\
&- \dots\\
&+ (-1)^{n-1}\ p(A_1 \cap A_2 \cap \dots \cap A_n)
\end{aligned}$$

2.3 CONDITIONED PROBABILITY. INDEPENDENT EVENTS

Consider an event B of not null probability, and it will be A other event of the same sample space [5]. It is defined as probability of A conditioned to B, and is represented by p (A/B), to the quotient:

$$p(A / B) = \frac{p(A \cap B)}{p(B)}$$

Such expression permits us to obtain the value from the probability of the fact that occur the event A, when we know that it has occurred the event B. It allows us to incorporate the partial knowledge that we may have on which has been the result of a random experience, to obtain the probabilities modified by that information. We will say that two events are independent when the knowledge of the fact that it has been presented one of them do not modify the probability of the other. Making use of the concept and the conditioned probability definition presented, we can write that the necessary and sufficient condition of independence of two events A and B is that is fulfilled anyone of the following expressions (that in reality are equivalent):

$$p(A/B) = P(B),$$
$$p(B/A) = p(A),$$
$$p(A \cap B) = p(A)\ p(B).$$

2.4 THEOREM OF THE TOTAL PROBABILITY. THEOREM OF BAYES

Consider an event B and some events A_i, (i = 1, …, n) that constitute a partition of the sample space E. It can be demonstrated that:

$$\begin{aligned} p(B) &= p(B \cap A_1) + p(B \cap A_2) + \ldots + p(B \cap A_n) = \\ &= p(B/A_1)\ p(A_1) + p(B/A_2)\ p(A_2) + \ldots + p(B/A_n)\ p(A_n) \end{aligned}$$

or well:

$$p(B) = \sum_{i=1}^{n} p(B / A_i)\, p(A_i) \,.$$

This expression is known as the theorem of the partition or theorem of the total probability.

One of the basic theorems, and maybe the most important, of theory of the probability is the Theorem of Bayes. This theorem can be stated is the following.

Consider:

- an event B of non zero probability and
- some events A_i, (I = 1, …, n) that constitute a partition of the sample space E.

It can be demonstrated that:

$$p(A_k/B) = \frac{p(B/A_k)\,p(A_k)}{\sum\limits_i p(B/A_i)\,p(A_i)}.$$

The real interest of this theorem bases in the interpretation that customarily have the A_i and the B, and in the probabilities that permits us to obtain. With much frequency the A_i have the interpretation of causes or origins of B, that turns out to be an effect or consequence of the A_i. So much the notion of cause as that of effect should be taken with a very wide interpretation, and many times only will refer to a temporary precedence in the events sequence (A_i occurs before B).

The theorem of Bayes, since, it will permit us to obtain the probability of the fact that the observed effect B has been caused by A_k, that is to say, the probability of the cause seen the effect. It is a probability which customarily is not obtained in the descriptive analysis of a problem and its calculation, without the theorem Bayes, would be problematic.

2.5 RANDOM VARIABLES. MEAN VALUE

Of a manner little accurate but quite intuitive, we could say that a variable is a random variable when takes values influenced by the random, by contraposition what would be a deterministic variable, in which values are perfectly predictable [1,7].

With more formality we will say than a random variable is an application defined between the sample space E, associated with a certain random experience and the real rectum $\Re$, that fulfils some given conditions. Such application associates to each event A of the sample space an interval in $\Re$, to which at the same time will have associated a probability with value between zero and one, with the one which we call probability of the element A of E, as well as probability of the interval of the real rectum associated with this element (Figure 1).

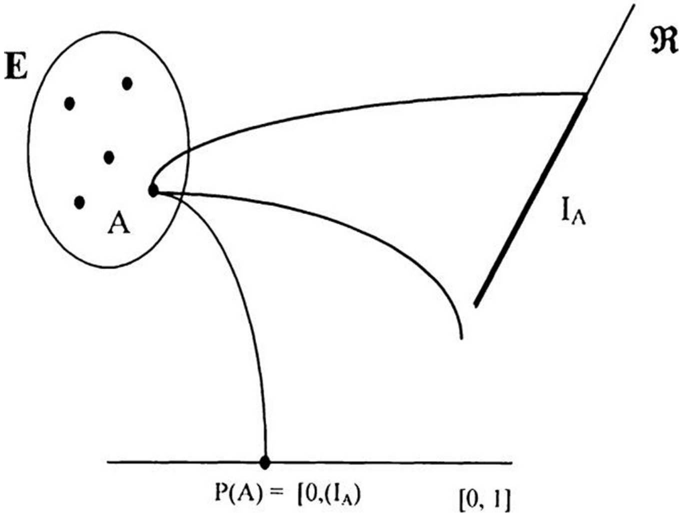


Figure 1. Sample space ***E*** *and the real rectum* $\mathfrak{R}$

The principal two types of random variables that interest us are the discreet and the continuous random variables.

The discreet random variables is characterized when we have a probability function p(x) that gives us the value of the probability in each one of the possible points of the distribution, being fulfilled that the sum of the probabilities will be one and that all will be not negative.

In the case of the continuous variables, the characterization is made through a non negative function f(x), call density function or probability density function, that describes how is distributed the probability between the infinite points (in continuous manner) that configure the existence field of the variable. It is fulfilled that the integral of this function, extended to the existence field of the variable, it is the element.

We will not enter here, because this is not the objective of this publication, in the exact characterization of the random variables.

For the discreet case as well as for the continuous, is defined the distribution function, F(x), as the probability that remains in or to the left of the point x:

$$F(x) = p(X \leq x)$$

where X (capital letter) is the variable and x (tiny) is a point in the existence field of X.

The probability functions, case of random variable discrete, and of density, case of random variable continuous, they are such that we can write:

- random variable discrete: F(x) = $\sum_{\forall x_i \le x} p(x_i)$,
- random variable continuous: F(x) = $\int_{-\infty}^{x} f(x)dx$.

Remark that in the continuous case that the distribution function represents the area located between the density function and the shaft of abcissa, from the abcissa - ∞ until the point considerated x.

Making use of the probability functions and of the density function, we can define the mean value of a variable, E(x), of the following manner:

- random variable discrete: E(x) = $\sum_{i} x_i \, p(x_i)$,
- random variable continuous: E(x) = $\int_{-\infty}^{+\infty} x \, f(x) \, dx$.

and as a rule we will be able to speak also of the value middle of a function g(x) of the random variable:

- random variable discrete: E(g(x)) = $\sum_{i} g(x_i) \, p(x_i)$,
- random variable continuous: E(g(x)) = $\int_{-\infty}^{+\infty} g(x) \, f(x) \, dx$.

Some mean values especially important are:

- the mean m of the variable: m = E(x),
- the variance σ^2 of the variable: σ^2 = E(x-m)^2.

The first one, the average or mean, acts as indicative of the position of the variables, that is to say of the order of magnitude that have the values of the variable.

The variance is interpreted as an indicator of the homogeneity or dispersion of the distribution: as greater is the value σ^2, more dispersed is the distribution.; and as smaller is σ^2, more homogeneous are the values of the variable (in the extreme case, if the existence field of x is reduced to an single value, this coincides with the mean and the variance is zero).The square root of the variance is called the standard deviation of the random variable.

2.6 PROBABILITY DISTRIBUTIONS

A probability distribution is not more than a standard behaviour of a random variable, a behaviour that appears with a frequency in the nature that has arrived to converte it into a model. In this paragraph will be studied some of the probability distributions more used in the field of the reliability: normal, exponential, Weibull, and Pearson (Chi Square) [5,8].

2.6.1 Normal Distribution

The normal probability distribution or gaussian distribution, since of both manners and indistinctively it is known, is a continuous distribution, defined in all the real rectum, and whose Probability density function is:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-m)^2}{2\sigma^2}} \; , \; -\infty \le x \le \infty$$

where m is the average of the variable and σ^2 it is its variance. We will say then that:

$x \equiv N(m,\sigma)$.

Its density function presents a characteristic form known as "bell of Gauss", that it is reflected in the Figure 2.

The density function of the normal don’t has primitive, therefore the probabilities calculation, that are made through the distribution function, requires the numerical integration of the pdf or the use of tables.

$$F(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}\cdot\sigma} \cdot e^{-\frac{(x-\mu)^2}{2\cdot\sigma^2}} dx$$

The distribution function is tabulated for the case of the normal N(0,1), the so called standardised normal. To be able to do use of this table with a normal distribution different to the N(0,1), that is with a general normal with a mean m (not necessarily zero) and a variance σ^2 (not necessarily one), it will have to be accomplished the operation called standardisation, consistent in transforming the variable N(m,σ) into the N(0,1).

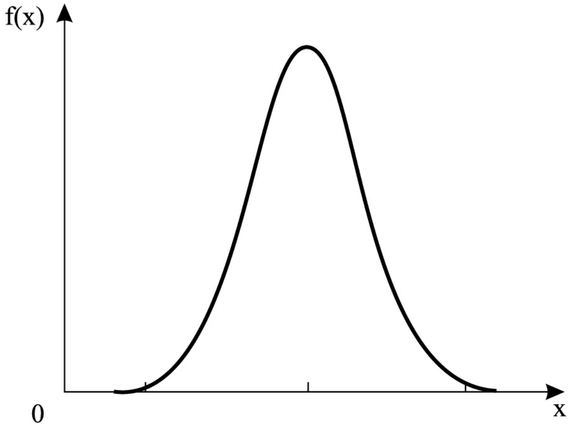


Figure 2. Density function of normal distribution

Consider a normal variable x, with $x \equiv N(m,\sigma)$. The variable z, defined as:

$$z = \frac{x - m}{\sigma}$$

it is a standardised normal. With this operation the calculation of the distribution function (and from this one that of any probability) would be accomplished of the following manner:

$$p(X \le x) = p\left(z \le \frac{x - m}{\sigma}\right) = \Phi\left(\frac{x - m}{\sigma}\right) = \Phi(z)$$

being Φ(z) the value of the distribution function of a standardised normal read in tables.

The Normal distribution is a symmetrical distribution in which the central value is the mean m. One important characteristic of the normal distribution is that it has an area approximately of the 68% in the two central typical deviations (between m- σ and m+ σ), an area of the 95% in the four central typical deviations (between m-2 σ and m+2 σ) and an area of the 99,73% in the six central typical deviations (between m-3σ and m+3σ), easily computable data using the previous table (Figure 3).

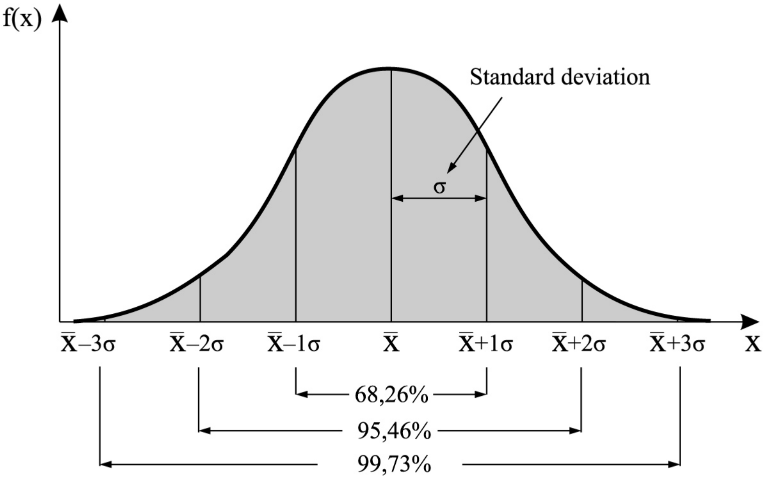


Figure 3. Probability areas of a normal distribution

Observe that in spite of be a variable defined between -∞ and +∞, in practice the values range between those oscillates a normal variable is very limited (between m-4σ and m+4σ we have 99,99% of the population). This fact is of great importance when thinking about the practical applicability of the normal variable.

2.6.2 Exponential Distribution

A continuous random variable is said to have an exponential distribution when it is non negative continues and when its density function has the expression:

$f(t) = \lambda e^{-\lambda t}, t \geq 0$

being λ a non negative constant.

We will say in such a case that $t \equiv \exp(\lambda)$. This random variable frequently represents the life or duration of system elements. The characteristics of this distribution are the following:

- distribution function: $F(t) = 1 - e^{-\lambda t}$,

- mean value: $E(t) = \theta = 1/\lambda$,
- variance: $D^2(t) = 1/\lambda^2$.

As it exists an explicit and simple expression for the distribution function, this variable does not require the use of any type of table, since the calculation of the value of the distribution function and of the probability of any interval is simple.

The aspect that presents its density function is the one which can be seen in the Figure 4. Other peculiarities of the exponential distribution are the following:

- the probability of the fact that the variable surpass its mean value is 36,79%, since it is a clearly asymmetrical distribution (Figure 4),
- it is considered a distribution without memory: the probability of the fact that the variable take values in a certain interval only depends on the length on the interval, not on its initial point:

$$p(t\in[t_1, t_1+T]) = p(t\in[t_2, t_2+T]), \forall (t_1, t_2).$$

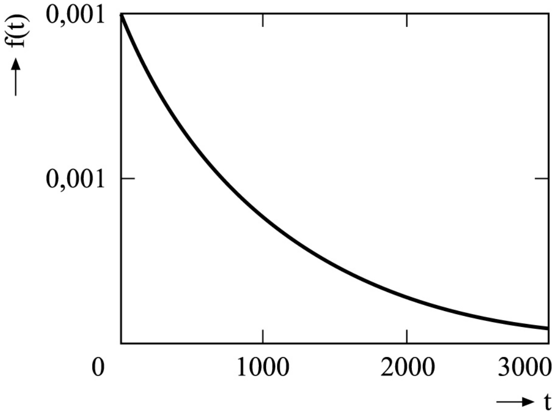


Figure 4. Exponential distribution: density function

2.6.3 Weibull Distribution

As in the exponential case, we consider now a continuous non negative random variable, that customarily we will interpret as the life of a studied element.

We will say that a such variable follows a Weibull distribution if its density function is:

$$f(t) = \beta \frac{(t-\delta)^{\beta-1}}{(\theta-\delta)^{\beta}}\, e^{-\left(\frac{t-\delta}{\theta-\delta}\right)^{\beta}}, t \geq 0$$

expression in which:

δ is the minimal life of the studied elements (δ ≥ 0),

θ is the characteristic life of those elements (θ ≥ δ),

ß is the form parameter or Weibull slope (β > 0).

The minimal life δ is an age that, with surety, will be reached by the studied elements. Frequently, as then it is commented, the minimal life takes the value zero.

The characteristic life θ is an age such that the probability of the fact that it will be surpassed is 36,79%, or, what is equivalent, such that a 63,21% of the elements fail before reaching it. Though the characteristic life is not the average of the Weibull distribution, it can be interpreted as an approximate position indicator (remember that in the exponential distribution the probability of the fact that the mean will be surpassed is precisely 36,79%).

Finally, the form parameter β describes the form of the distribution, and we will see that it is key to understand the behaviour of the life or duration variable of the studied elements.

The distribution function will be:

$$F(t) = 1 - e^{-\left(\frac{t-\delta}{\theta-\delta}\right)^{\beta}}$$

As already it has been commented, frequently the minimal life δ takes the value zero, and in this case the previous expressions would be simplified, resulting the so called "reduced" Weibull distribution, whose density function is:

$$f(t) = \beta \frac{t^{\beta-1}}{\theta^{\beta}} e^{-\left(\frac{t}{\theta}\right)^{\beta}}$$

and the distribution function:

$$F(t) = 1 - e^{-\left(\frac{t}{\theta}\right)^{\beta}} .$$

In this reduced Weibull distribution, the mean value is:

$$E(t) = \theta\left(\Gamma\left(1+\frac{1}{\beta}\right)\right).$$

where Γ is a tabulated function, the Gamma function (or it can be obtained by numerical integration).

The aspect that has the density function of this Weibull variable depends on the value on its parameters. In the Figure 5 is represented the form of the density function for different values of β.

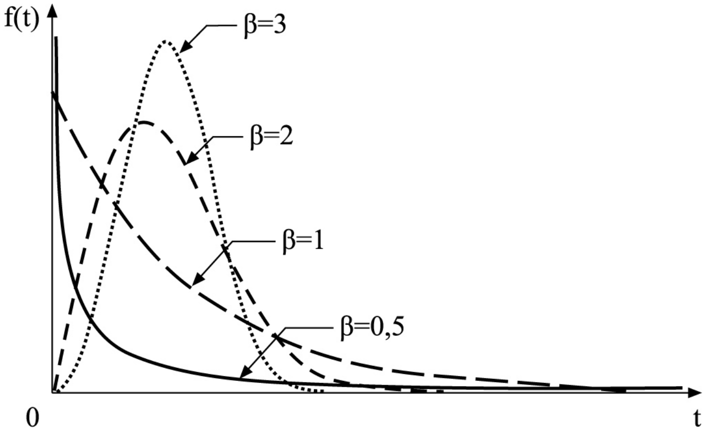


Figure 5. Reduced Weibull distribution: density functions

Observe that for high values of ß the form of the distribution is resembled to the bell of Gauss, that is to say to the normal distribution. In practice, for values of β over 3,2, the Weibull distribution is approximated to the normal.

2.6.4 Pearson or χ^2 (Chi Square) Distribution

The Chi Square distribution is a distribution derived from the normal, such as now we will see, that is employed in a great variety of statistical tests.

Consider a random variable x. We will say that x follows a Chi square distribution with n degrees of freedom (χ_n^2), if is defined as the sum of the squares of n independent normal standardised variable:

$$x \equiv \chi_n^2 = \sum_{i=1}^{n} z_i^2$$ being $z_i = N(0,1)\ \forall i$, independent.

As it is shown in the Figure 6, it is an asymmetrical distribution, in which as the degrees of freedom increases, a convergence to the normal distribution is produced. For degrees of greater freedom of thirty is usual to consider correct this approximation.

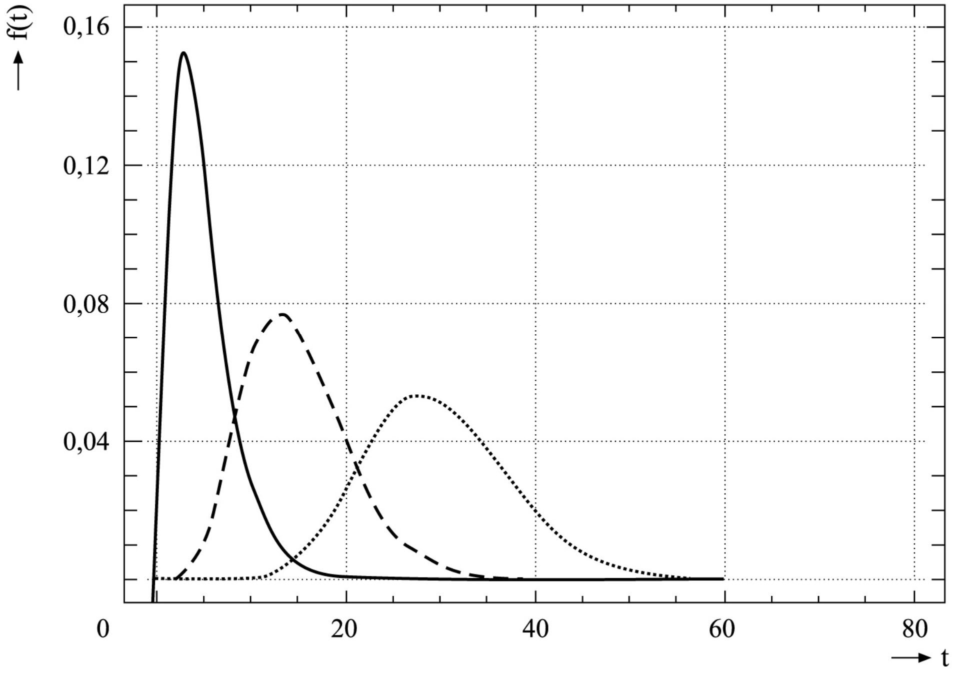


Figure 6. Chi Square distribution: density functions

The distribution function of the variable χ^2 is tabulated. Customarily tables that are handled in reality permit us to obtain the percentage points, that is to say the values from the variable that they are surpassed with a certain probability.

Chapter 3

RELIABILITY: CONCEPT AND BASES

3.1 RELIABILITY DEFINITION

Even though there exists a common reliability notion, which is interpreted as a combination between the duration of a system and its operation safety, here we need a most specific definition of this term, which is the fundamental object of analysis of the following pages.

It is used customarily the following reliability definition [9]:

The reliability of a item is its probability of success in a certain mission that has been assigned to it, when this mission is developed under some given conditions.

The key elements of the previous definition are: item, mission, success (and its opposite, failure), and the conditions under which the mission will be developed. Furthermore, there appear other terms when we deepen in the nature of the previous definition, such as age and date. Lets see what we understand by those concepts.

We call item to each one of the simple elements or compounds that they are object of study. A item can be, according to its degree of complexity, simple or compound:

- the simple items, called elements, are those that can not be decomposed in pieces more elemental, as would be the case of a dock or a power cord.
- the composed items, called systems, are those that are integrated by elements and by smaller order systems, as for example a home appliance or a computer.

Frequently it occurs that items that in reality are systems are, in practice, treated and analysed as elements, applying a principle of "black box" for their analysis: only it interests the global yield in the item and not its detailed behaviour at elements or subsystems level. That would be the case of the electronic ignition system of a car, that even though it is a system, frequently it is treated as element when its reliability is analysed by the cars manufacturer, while for the company supplier of those equipment that is considered clearly as a system, whose structure is of fundamental interest.

Mission is the service or objective that must be fulfilled by the studied elements. Often the mission is formulated in terms of duration, or at least appears that element in its definition. For example, the mission of a television can be to operate of uninterrupted manner during 2000 hours. In this regard it is important to see the commentary that is made more down on the age of the elements.

Failure is any circumstance that prevents that a element complete its mission. The success would be the absence of failure in the development of the mission. It can be possible to distinguish between total failures and partial failures, and in good logic the treatment given to both should be different. However this surpasses the limits of this work, and we will consider the failure as a dichotomic situation, by attempting that the definition of the mission will be sufficiently clear as so that could it can be said without doubt if there is or not success.

Failure can be total and immediate break of system operation or effectiveness decreasing of its operation down to a certain acceptable level [10]. Usually, according to these characteristic, failures can be divided into two kinds:

- immediate failure,
- progressive failure.

This situations are shown in Figure 7.

The **conditions** are the characteristics of the environment in which the mission must be developed. They can include topics such as ambient conditions (pressure, temperature, dampness, etc.), effort level of the element, type of user of the system, etc. These conditions are of extraordinary importance for the evaluation of the reliability. It is very important to insist in that a same system, with a same mission, but accomplished under various conditions, procures different reliabilities.

We will call **age** of a element to any form of measuring its past activity. Frequently that measure is accomplished by the time of use, as in the example of the television, previously commented, but not always it will be thus. For example, in a pneumatic of car the age will be measured better through the kilometres of use than by the time of use; in a spring the age will be measured better with the number of compression-extension cycles that suffers, etc.

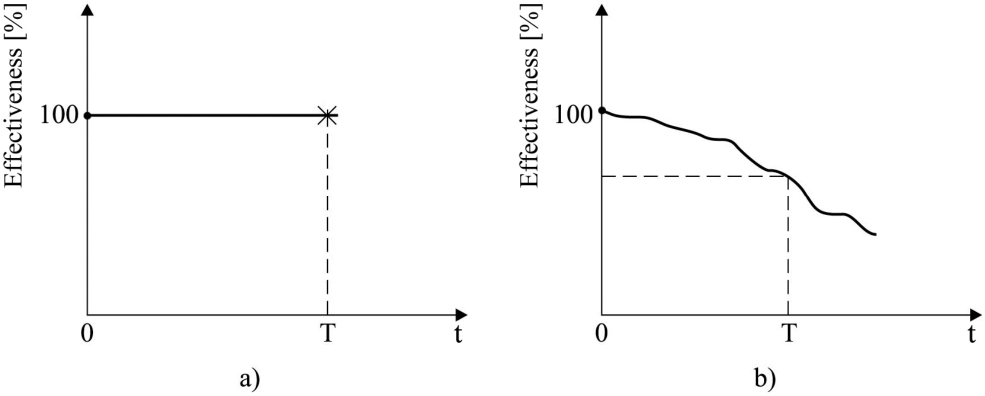


Figure 7. Total and immediate failure (a) and effectiveness decreasing of system operation down to acceptable level (b)

If we call age to any form of measuring the activity developed by the element, **date** will be any point in the age scale.

There is other classification of elements different to the previous one, that distinguishes between continued operation elements and instant operation elements. Between the first can cite a pneumatic of car, that is operating of continuous manner during all its life, and between the second the contact explosion device of a missile, that operates only in the instant in which this makes impact. Evidently in this second case the age concept, such as have seen it, it is not of application and the reliability is not associated to a life (in the sense of duration of the element) but to the probability of success in that instant in which the system must operate.

The following examples show expressions in which appear the previously specified concepts.

- "98% of certain televisions should be capable of operating uninterruptedly during two thousand hours, in a domestic environment". The age is measured here in time, the mission is formulated terms of duration and of operation, is understood that good operation, and the conditions are associated to the environment in which is developed the mission. It is established furthermore a quantified reliability objective, in the form of a required probability of success.

- "A car pneumatic must be able to circulate by highway, at a speed of 90 km./h, without suffering pricked an due to wear or internal failure during 35000 km., with a probability of at least the 99%". Now the age is measured in Km, the mission is expressed in terms of duration and of absence of failure and there are defined also the operation conditions of the system. Also here a numerical reliability objective is fixed.
- "The airbag of a certain car model should not to fail more than a 0,5 for thousand of the times, when an impact of normalised type occurs". Is tried now to an instant operation system, and in consequence the **age**, in the sense of the two previous cases, does not exists. The definition of the mission as well as the accomplishment conditions (impact of normalised type) are presents in the statement. Also appears a quantification of the desired reliability.

3.2 QUANTIFICATION OF THE RELIABILITY

The concepts of element, mission, failure, etc. introduced in the previous paragraph permits us to give a numerical measure of the safety of operation of a system, that is to say, of the capacity that it has to comply with success a given mission [11].

A measure of this capacity is the Reliability function or Survival function,

$$R(t_1,t_2)$$

defined as the probability of the fact that a element comply with success a concrete mission, from the instant t_1 until the instant t_2, under some given service conditions.

Other measure of this capacity is the unreliability, $F(t_1,t_2)$, that is defined as the probability of the fact that the studied element fail during the mission, that is to say,

$$F(t_1,t_2) = 1 - R(t_1,t_2).$$

Supposing t_1=0, the unreliability function will coincide with the distribution function of the life of the element (considered as a random variable), being the probability of the fact that this life not surpass a certain value.

The representation of the number of survivors in function of the time, N(t), with respect to the initial number of elements, $N(t_1)=N_1$, facilitates an intuitive interpretation of the reliability and unreliability concepts [5]. This representation is displayed in Figure 8.

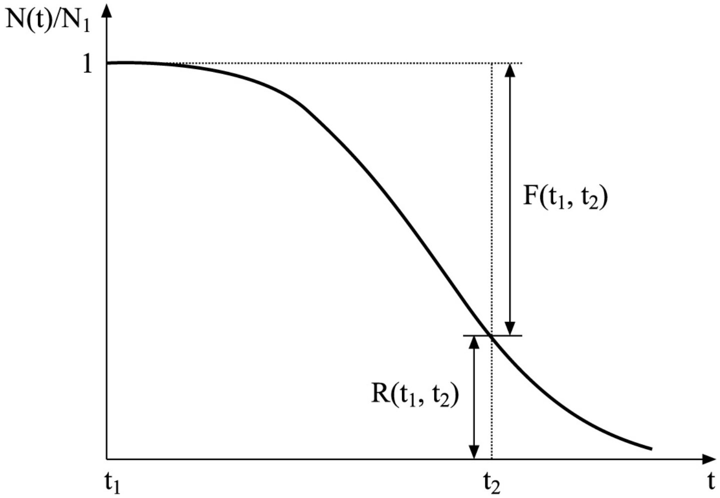


Figure 8. Reliability function or Survival function

Thus since, we can associate the reliability and the unreliability, from t_1 until t_2, to the survival and failure frequencies that are observed when registering the evolution of the survivors fraction to the time, when in the instant t_1 are put simultaneously in operation N_1 elements:

$$R(t_1,t_2)=\frac{N(t_2)}{N(t_1)}=\frac{N(t_2)}{N_1}\quad F(t_1,t_2)=1-\frac{N(t_2)}{N(t_1)}=1-\frac{N(t_2)}{N_1}$$

Observe that the reliability function is a diminishing function with t_2, indicating such decreasing that for missions of growing duration the reliability of success is reduced, tending to zero. On the other hand, we see that $F(t_1,t_2)$ is a growing function with t, being verified that:

$$\lim_{t\to\infty} F(t_1,t_2)=1.$$

If furthermore we call T to the age in the one the element fails, we obtain that

$F(t_1,t_2) = P(T \leq t_2 - t_1)$.

Showing that the unreliability, $F(t_1,t_2)$, is the distribution function of the variable "age of the failure T", or, in other words, the probability of the fact that a element fail before the instant t_2 when the mission has begun in the instant t_1. Graphically we can see the foregoing in the Figure 9.

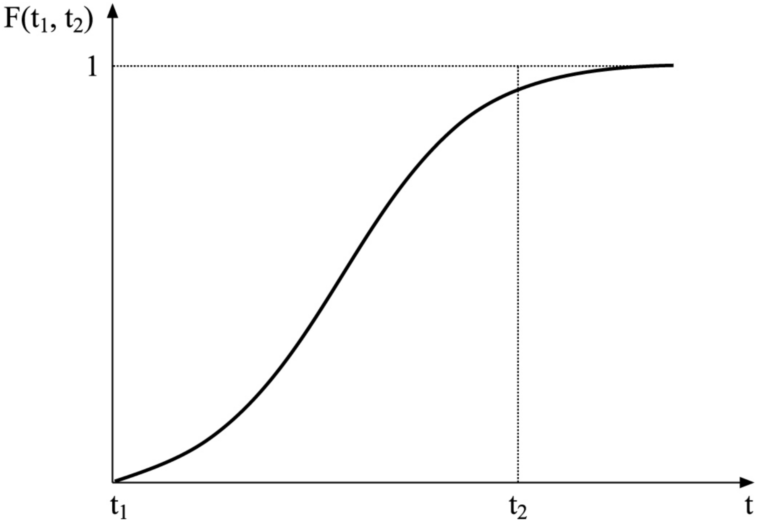


Figure 9. Unreliability function

To simplify the nomenclature, we will call R(t) to the reliability and F(t) to the unreliability of a element, assuming that the beginning of the mission is at t_1=0 and that, therefore, t_2 can be any instant t in the axis T (from zero to infinite).

3.3 FAILURE RATE

We have seen that the unreliability, F(t), indicates the probability of the fact that a element fail before of the instant t, that is to say,

$F(t) = P(T \leq t)$,

where T is the random variable that indicates the age of the failure, that is to say, the distribution function of the variable life [1,12].

Therefore, if F(t) is the function of failure distribution, deriving it with respect to t we can obtain the density function of life, f(t). Because of this, taking into account to F(0)=0, we can write that:

$$F(t) = P(T \leq t) = \int_0^t f(t) \cdot dt\,,$$

and that:

$$R(t) = 1 - P(T \leq t) = P(T \geq t) = \int_t^\infty f(t) \cdot dt\,.$$

We see that the mean life of the element can be obtained directly from the reliability function. In effect, it is known that:

$$\mu = \int_0^\infty t \cdot f(t) \cdot dt$$

integrating that expression:

$$\mu = \int_0^\infty t \cdot f(t) \cdot dt = [tF(t)]_0^\infty - \int_0^\infty F(t)dt$$

as is given that:

if $t \to \infty$ t F(t) ≈ t (since $F(t) \to 1$)
and
if t = 0 t F(t) = 0

that is to say:

$$[t\,F(t)]_0^\infty \cong [t]_0^\infty$$

and with this:

$$\mu = \int_0^\infty t \cdot f(t) \cdot dt = [t]_0^\infty - \int_0^\infty F(t)dt = \int_0^\infty (1 - F(t))dt = \int_0^\infty R(t) \cdot dt\,.$$

Thus since, the mean life will be:

$$\mu = \int_0^\infty t \cdot f(t) \cdot dt = \int_0^\infty R(t) \cdot dt$$

The Failure Rate, λ(t), is defined as the extinction speed or the relative variation of the number of survivors in the instant t and is related to the number of failures by time element, being by in consequence:

$$\lambda(t) = \lim_{\Delta t \to 0^+} \frac{\left[N(t) - N(t+\Delta t)\right]/N(t)}{\Delta t} = -\frac{N'(t)}{N(t)} = -\frac{R'(t)}{R(t)}$$

that is to say:

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

since:

$$R(t) = \int_t^{\infty} f(t)\,dt = 1 - \int_{-\infty}^{t} f(t)\,dt$$

and consequently:

$$R'(t) = - f(t).$$

When the failure rate is constant: $\lambda(t) = \lambda$.

The reliability in function of the failure rate can be calculated as follows:

$$\lambda(t) = -\frac{dR(t)/dt}{R(t)},$$

$$\lambda(t) \cdot dt = -\frac{dR(t)}{R(t)}$$

integrating both sides of the equality is obtained:

$$\int_0^t \lambda(t) \cdot dt = -\int_0^t \frac{1}{R(t)} \cdot dR(t) = -\ln\left[R(t)\right]$$

and the reliability R(t) is:

$$R(t) = e^{-\int_0^t \lambda(t)dt}.$$

This is so called "basic reliability formula".

3.4 VARIATION OF THE FAILURE RATE

The failure rate λ (t) of almost any type of elements varies in function of the time. Frequently, during the first period of life of the elements the failure rate will be diminishing (early failures period) until is reached a value in the failure rate is maintained sensibly constant (accidental failures period) and that it is the zone called the useful life of the system. Finally, from a given age, the failure rate grows up, generally of a very rapid manner (period of failures by obsolescence or wear out period). In the Figure 10 is shown the curve of the failure rate function.

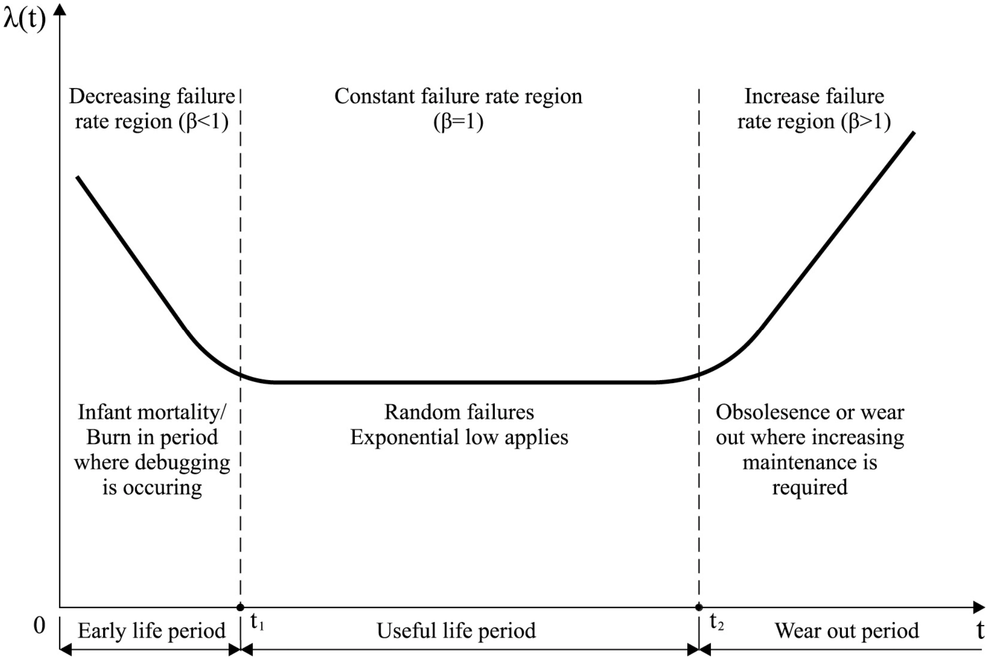


Figure 10. Time dependent failure rate function

The early failures are those which are produced in the initial period of the system operation, generally in the first minutes or hours of operation. They are failures caused by design or manufacture mistakes and once repaired do not occur again in the same element. The early failures can be avoided submitting to the elements to Burn in tests: in occasions is accomplished a test in the 100% of the elements to simulate the operation in this stage and to eliminate this type of failures. The elimination of early failures is necessary to obtain a good reliability, specially in the single mission systems in which a failure can provoke its complete destruction and, in general, by the devastating effect that has the failure of a recently acquired system on the customer.

The useful life period is characterised by having a constant failures rate and by the absolute predominance of the accidental or random failures, caused by many different and unexpected circumstances (not by an improper use neither by manufacture defects). Enter in this category of accidental failures those caused by occasional efforts, mistakes of operation of the user and, in general, to the unpredictable situations not associated with time of use or with the age. The accidental failures can be controlled with a good operation procedure and with an adequate preventive maintenance.

The failures by obsolescence, or wear out failures, are those associated with failure mechanisms due to the use or the age of the element: fatigue of the material, degradation of the elements, insulating, etc., that are originated gradually with the operation of the elements. The failure rate can be reduced with maintenance plans that avoid the depletion of the elements. Consequently, in a system, after the elements have operated correctly during a time b, if the used elements are not replaced by new ones, free of early failures, the service will be made insecure and the reliability will descend to dangerous values. In general, in the obsolescence zone, the growth speed of the failure rate depends on the regime of use of the element in its period of useful life [11].

The total failure rate of the elements can be considered resulting of the sum of the three failure rates originated by early, accidental and obsolescence failures (Figure 11).

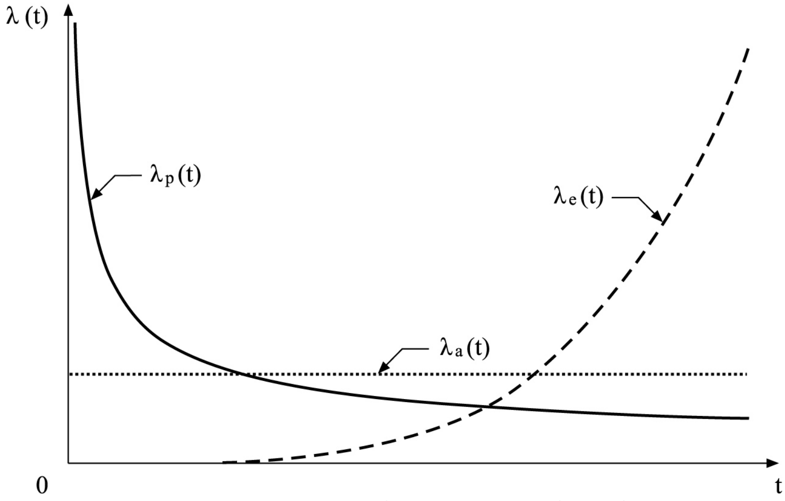


Figure 11. Independence of the causes of the failure rate

Thus since, must:

$\lambda(t)= \lambda_p(t)+ \lambda_a+ \lambda_o(t).$

Therefore, the joint reliability is found as the system of the early, accidental, and obsolescence reliabilities:

$$R(t) = e^{-\int_0^t [\lambda_p(t)+\lambda_a+\lambda_e(t)]\cdot dt} = S_p(t)\cdot S_a(t)\cdot S_e(t)\,.$$

This expression considers that the model followed by the life of the elements is exponential, as it will be studied in other chapter of this book. Also it is considered that the three causes of early, accidental, and by obsolescence failures are mutually independent (if we admitted that the failure rates are additive).

Chapter 4

RELIABILITY MODELS

4.1 STATISTICAL DISTRIBUTIONS

As has been seen previously, in continuous operation elements, the reliability is the probability of survival to a certain mission of duration t, that is to say, the probability of the fact that a element operate more than a time t:

$R(t) = P(T>t)$.

Therefore, to measure or to estimate this probability of correct operation it is necessary to determine the distribution of failure probabilities, that is to say, the distribution of the variable "life of the element" [13]. We will employ for this study the same three statistical distributions that were introduced in the Chapter 2: normal distribution, exponential distribution and Weibull distribution.

4.2 NORMAL MODEL

Lets call t to the variable "life of a element". If we suppose that this variable has a normal distribution with mean m and typical deviation σ, we can obtain that the reliability function is:

$$R(t) = 1 - F(t) = 1-\int_{-\infty}^{t} \frac{1}{\sqrt{2\pi}\cdot\sigma}\cdot e^{-\frac{(t-\mu)^2}{2\cdot\sigma^2}}dt = 1-\phi\left(\frac{t-\mu}{\sigma}\right) = \phi\left(\frac{\mu-t}{\sigma}\right)$$

being f(t) the distribution function of the standardised normal that is found tabulated in corresponding tables. The failure rate for this distribution is:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\frac{1}{\sqrt{2\pi}\cdot\sigma}\cdot e^{-\frac{(t-\mu)^2}{2\cdot\sigma^2}}}{\phi\left(\frac{\mu-t}{\sigma}\right)}$$

which results to be a growing failure rate with t, something which means that it can represent the behaviour of those elements during the wear out period, when the failure rate increases.

The Normal distribution is defined for t ∈ [-∞,∞] but it is evident that the life of a element starts in the instant of its put in operation, and because of this as minimum, if the element is new, it would start in the instant t=0 and, therefore, we can not speak of negative times. Thus since, we only will be able to use this type of distribution as representing the phenomenon of obsolescence, in the case that the mean life is sufficiently far from the origin of ages (t=0) so that the probability bulk left to the zero will be practically zero. It is tended consider that this is thus if μ-3σ>0, that is to say, that $\mu/\sigma>3$, since below this value only remains a 1,3% of population and therefore R(0) ≈1.

4.3 EXPONENTIAL MODEL

As already it was seen, the expression of the density function when the life of the element continues a exponential distribution is:

$f(t) = \lambda\cdot e^{-\lambda t}$, $t\geq0$,

where λ is a positive constant ($\lambda>0$).

As the distribution function, that is to say, its unreliability will be:

$F(t) = 1-e^{-\lambda t}$, $t\geq0$,

the reliability function, probability of survival to a duration t, will be:

$R(t) = 1 - F(t) = e^{-\lambda t}$, $t\geq0$.

An interesting value is the one which is given if t=1/λ, that is to say when the length of the mission coincides with the mean life, in whose case:

$R(1/\lambda) = 0{,}37.$

That is to say, the mean life is reached only by a 37% of the population, as consequence of the asymmetrical character of the distribution (see Chapter 2).

The failure rate is:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda,\ \ t \geq 0.$$

It can be observed that λ(t) does not depend on t or, in other words, the failure rate is constant. Because of this, we will employ the exponential distribution during the useful life period of the system.

It is frequent to represent to the parameter 1/λ by θ, mean life, thus since, the previous formulations would remain as:

$f(t)= \lambda e^{-t/\theta}$, $F(t)=1-e^{-t/\theta}$, $R(T)=e^{-t/\theta}$, $\mu=\theta$, $\sigma=\theta$.

If we look at these expressions of the density, distribution and reliability functions (the one which is here object of study), we observe that it is the relationship between duration of the mission and the mean life, the ratio t/θ, the one which defines the value of the function, and not so much the exclusive value of t or θ.

An important property of the exponential model is that is a model without memory. In effect, it is easy to prove that if once a element has failed accidentally, we repair it and we return it to put on operation until it returns to fail, the duration of the random interval that separates these two consecutive accidental failures continues also a exponential law of parameter θ=1/λ. The exponential distribution is, thus since, a distribution without memory because the probability of the fact that a element fail in a specific period of time depends not on the duration on this and not on the instant in the one the element began the operation:

$$P(t \in [t_1, t_1 + T]) = P(t \in [t_2, t_2 + T]),\ \forall\ t_1, t_2.$$

In effect, they will be t_1, and t_2 such that $t_2 > t_1$.

It is fulfilled that:

$$P(T > t_2 / T > t_1) = \frac{P([T > t_2] \cap [T > t_1])}{P(T > t_1)} = \frac{P(T > t_2)}{P(T > t_1)} =$$

$$= \frac{e^{-\lambda t_2}}{e^{-\lambda t_1}} = e^{-\lambda(t_2 - t_1)} = R(t_2 - t_1)$$

If we call t_1=t, t_2 = $t_{1+\tau}$, it results:

P(T>t+τ/T>t) = R(τ).

That is to say, the reliability depends only on the duration on the mission, t, and not on the age of the element at the beginning of that mission.

Of this is deduced that if τ=1/λ is the mean life, from the beginning of the mission or of the service, until is produced an accidental failure, but furthermore also it can be the mean duration of the time that elapses between two accidental consecutive failures in the same element. For this last cause to θ is called the Mean Time to Failures (MTTF) or Mean Time Between Failures (MTBF), depending if the elements are not repairable elements (MTTF) or repairable with full restitution (MTBF). It is important to remark that we are here supposing that the repair refunds to the element to a similar state to which it has before of the failure. If this is not be true, we would have to enter the definition of others parameters, as for example the Mean Time to First Failure (MTTFF).

4.4 WEIBULL MODEL

If the variable "life of the studied element" is modelled through a complete Weibull distribution, of parameters θ, β and δ, the reliebility function will be:

$$R(t) = e^{-\left(\frac{t-\delta}{\theta-\delta}\right)^{\beta}}$$

Therefore the failure rate is:

$$\lambda(t) = \frac{f(t)}{R(t)} = \beta \cdot \frac{(t-\delta)^{\beta-1}}{(\theta-\delta)^{\beta}}$$

As was commented in the Chapter 2, the parameter δ tends be zero, and in this case we will speak of the reduced Weibull distribution, with the following unreliability, reliability and the failure rate functions with the following expressions:

$$F(t) = 1 - e^{-\left(\frac{t}{\theta}\right)^{\beta}}, \; R(t) = e^{-\left(\frac{t}{\theta}\right)^{\beta}}, \; \lambda(t) = \beta \cdot \frac{t^{\beta-1}}{\theta^{\beta}}.$$

Observe that if t = θ, then F(θ) = 0,63 and R(θ) = 0,37.

As of the equation of the failure rate we can prove that this rate grows or decreases in function of the value of β, that is to say, if β<1 then the failure rate is diminishing, if β>1 is growing, and if β=1, it is constant. Therefore, the Weibull distribution can serve to explain the different situations and periods of the life of a system: if β<1 the Weibull distribution will be able to be used to explain the period of early failures; if β>1 it will serve for the period of failures by obsolescence, and if β=1 we will use it to explain the useful life zone.

In this last case, observe that if in the expressions of the functions of distribution and reliability we make β=1, then the distribution will be that of the exponential model. Therefore, this model results a particular case of the Weibull model, with δ=0 and β=1, remaining the third parameter, θ, identified with the average of the distribution:

exp(1/θ) = W(δ=0, θ, β=1).

A key feature of the Weibull distribution in comparison with the exponential is that now the reliability depends on the age that has the element to the beginning of the mission, and not only of the duration of the same. Or in the same terms that were employing before, they gave Weibull distribution if that it has memory of the past activity of the element. For example, it justifies its use in the period of obsolescence.

Chapter 5

RELIABILITY ESTIMATION AND TESTING

5.1 INTRODUCTION

The statistical models that have been seen in previous chapters are not excessively complex and permit to perform easily forecasts on the behaviour of the studied elements, referred to its reliability. Now then, the use of the involved expressions requires the knowledge of a series of parameters that only is possible to obtain by the way of making experiments and testing. It does not exist any deductive procedure that permit to know the reliability or the life parameters of the studied elements as of their physical, mechanical, electrical, or of any other type of characteristic. Furthermore, upon studying the reliabilities of the elements, we should have very present the work that the element will have during their service and in the periods of standby or of storage, since the reliability of a element is function of the conditions that it must deal with.

Once we have determined these conditions, it is convenient to study separately the "dominant conditions", that is to say, those which have greater influence on the reliability of the element, and the "not dominant" that they are those that can be eliminated or simply improved well by small modifications in the design of the system or with improvements of manufacturing. These last will be tried from eliminating or at least to stabilise as quickly as possible.

The dominant conditions are those which will be submitted to a study as complete as possible, measuring their variation ranges, the accidental overcharges appearance, and even their extreme values. As of here already we can proceed to the design of the tests in order to estimate the failure rates, the means time of service, etc., and as a rule, the parameters necessary for the adjustment to the theoretical models of the samples. The motive that us to consider the use of reliability testing as necessary is the impossibility, already commented, of obtaining by some analytical - deductive method information on the reliability or duration from a system: We react to that impossibility by accomplishing experiences in which it is intended to simulate the behaviour that the system will have when it will be actually used by its user, allowing us to know some characteristics such as its duration, mean life, reliability for certain mission or service, etc.

A reasonable procedure that would seem logical would begin fixing in the nominal value each type of condition (recommended value for normal operation of the element). Taking a random sample of the elements of size n, they are operated under this regime and the times in the one which are produced the failures, as well as the causes that motivate them, are registered. Once accomplished, it is repeated the test with other random sample, but this time changing the operation conditions. In this way, we can obtain the curves from the element for various working conditions.

The previous test method presents large limitations that makes necessary to develop other methods that permit to substitute it in benefit of a greater rapidity. In this paragraph we are going to develop some types of tests and tests attending to different classifications according to the pursued objectives, to the level of the charges applied and to statistical considerations.

5.2 TYPES OF TESTS

In the first place, it must be considered that the objective of the tests in reliability is to know the behaviour that the system will have when it will be actually used. But the real conditions of use can be so assorted and complex that it is difficult to reproduce them all in only one test or in a battery of tests, given the customary time and resources limitation with that usually the companies have. This has moved to develop a series of tests oriented to identify the most important aspects, in each case, of the behaviour of a system. Below it is presented a classification of those tests, in different criteria function [1,5].

5.2.1 By the Objectives

1. Measure tests: Used to know the behaviour of new designs and to analyse the fulfilment of the reliability goals. Prototypes are prepared to obtain the form of the failures distribution, the parameters that determine the distribution and their corresponding confidence intervals. The objective of these tests is to measure the reliability of the element, without questioning the reliability goals previously established. The tests will serve furthermore to give validity to the design of the element.

2. Control tests: The objective of these tests is to maintain the stability of the reliability values in the manufacturing of successive batches, that is to say, tries to assuring the maintenance of a given reliability level in the device.

3. Research tests: They are used to improve the results of reliability by investigating the possible causes of failures in order to study the most appropriate modifications. Tend be guided toward the study of concrete failure modes.

4. Tests in real operation conditions: The objective of this type of test is to know the real behaviour of the production equipment. This tests are routed to know the reliability in real operation conditions.

5.2.2 By its Statistics Nature

1. Estimation tests: Guided to know (to estimate) the value of some of the parameters that reflect the behaviour of the system, concerning its duration. They employ statistical estimation methods, both point estimators or by confidence intervals.

2. Comparison tests: It is intended with them to compare the behaviour of the system concerning its life with a standard previously established. Here we can employ statistical techniques of hypothesis contrast, usually parametrical methods.

5.2.3 By the Charges Applied

1. Tests under constant load: The charges applied to the system tested are constant along of the tests:

- normal tests: they are tested in those which the industrious charges are the same order that those of service,
- accelerated tests: in order to shorten the test time, the industrious charges are superior to those of service.

2. Tests under variable load: The load intensity varies along of the tests:

- tests with linear growth with the load,
- tests with growing load step by step,
- tests with cycles in the load level: the variation takes place according to an anticipated cycle,
- tests with random load.

5.2.4 By the Stopping Criterion of the Test

1. Complete tests: They are those that end when all tested elements have failed. It presents the drawback of the long duration of the test, that causes that is relatively little used.

2. Tests of fixed duration, truncated or limited by time: The length of testing time is preset. These tests tend to correspond to control tests, that is, those whose objective is to assure a minimal reliability level.

3. Tests to a fixed number of failures, censured or limited by failures: The test ends when they have failed a predetermined number of elements. The advantage related with the easy scheduling of testing facilities activity. It is also they employed as control test.

4. Progressive or sequential tests: After each failure, the test controller decides if the test is continued or not. They are also control test.

5. Limited progressive tests: Similar to the previous one, but with a limit in the duration of the test as well as in the number failures. Test is stopped according to results achieved.

The variety of available tests causes that, a priori, there is no possible general recommendation of which to use, The election of the type of test must be adapted to each concrete case and each necessity, acting according to the characteristics of the study. Some factors affecting the decision are the costs of testing, the cost of elements tested, the destructive or non destructives nature of test, the testing facilities availability and the time available for decision making.

5.3 ANALYSIS TEST RESULTS

To achieve optimal results in analyzing failure tests results, a combination of technical and statistical knowledge is need to achieve the best results. Knowing if the failure is due to an accident, to a defect in production or assembling of the element, or is the result of the wear out and the long use is as important as to know which is the best statistical model to apply.

It is also important to control and consider the state of the elements to be tested, as question not directly related with their reliability, as storage conditions causing oxidation, may affect test results. Only elements in a specified condition should be tested, to avoid bias and misinterpretation of results [5].

5.3.1 Reliability Testing for Accidental Failures

Before testing system against accidental failures, it is mandatory to have eliminated early failures. Once it is guaranteed, we have to consider that the statistical model to use for accidental failures is the exponential model. With this model, failures do not depend on the age of the system at the beginning of the mission, but it is recommended to use elements with similar age and past history, as the exponential model is an idealization of what really happens to systems. In any case, this type of tests is more centred in the study of the service length than in the age of the system.

The same caveat referred to the elimination of early failures must be done about wear our failures. We need to be sure that failures are random and not the result of a wear out process. To ensure this, tests must be performed during the useful life of the studied elements. We have to identify the length of this useful life, that is the moment (age) in which wear out problems start to be relevant. Specific testing is required for this purpose.

As commented previously, for random accidental failures modelling, the exponential model is adequate. A exp(λ), in which the failure rate λ is constant will be used. One way of identifying a working value for the useful life limit is based in the fact that random failures are equally distributed over time. If some failure occurs in a high age, not very compatible with an exp(λ) model, we can conclude that this is another type of failure.

Frequently, λ is estimated and a service time b is defined as a time with very low probability of being surpassed (usually $\alpha = 0{,}00135$):

$$R(b) = e^{-\lambda b} = \alpha,$$

$$b = -\frac{1}{\lambda}\ln\alpha = -\theta\ln\alpha .$$

Elements with failure time over b will de discarded for the analysis, as probably they correspond to non random failures, probably wear out failures. We will analyze data from the beginning of the test to age b, except if we have information forcing us to discard some data (as the evidence of a non random failure).

Sample size must be big enough to allow a number of valid failures sufficient for computing good estimates.

5.3.2 Reliability Testing for Wear Out Failures

Again, early failures must be eliminated before testing. The burning process required to do that, makes difficult to start testing with completely new systems. If so, the time of the burning process must be added to the age observed during wear out testing.

The distinction between random and wear out failures also creates a problem. It can be difficult to make this difference, except if we do some "forensic" analysis of failures. Alternative to this, we can use a statistical approach.

For example, if a failure is modeled with a normal $N(\mu,\sigma)$, values under $(\mu\text{-}3\sigma)$ are nor probably caused by wear out, as the their probability is lower than 0,00135. These failures can be discarded for analysis. A similar criterion can be used with the Weibull distribution.

Obviously, to do that we need an initial estimate of μ and σ, parameters that will be re-estimated with test results. Some iteration may be needed to guarantee that test data do not contain values under this revised lower limit.

5.4 ESTIMATION TESTING

All statistical models used in life and reliability modeling require the estimation of some parameters. Frequent goals of testing processes are:

- identify which distribution better fits with data,
- estimate the values of the distribution's parameters,
- test data against some previous hypothesis or requirement affecting parameter's value.

To do that a sample of size n will be taken, formed by an homogeneous set of elements. In following paragraphs different methods of analysis, for different situations, will be presented [14].

5.4.1 Exponential Distribution

As we have seen in previous chapters, the exponential distribution density function is:

$$f(t) = \lambda \cdot e^{-\lambda t}.$$

The corresponding reliability functions is:

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

As can be observed, one single parameter affect the exponential distributions. This parameter is the constant failure rate λ, whose inverse $\theta=1/\lambda$ is the mean life, frequently noted as Mean Time Between Failures (MTBF) for repairable elements or as Mean Time to Failure (MTTF) for non repairable elements.

In consequence, only this parameter, in the form of λ or its inverse θ will be estimated.

5.4.1.1 Parameter Estimation

Point estimation. Point estimation of the mean life (MTBF or MTTF) for any type of test is relatively easy to do, if we are in the useful life (with life following exponential model). In this case:

$$\hat{\theta} = \sum_{i=1}^{n} \frac{t_i}{r} = \frac{T}{r}.$$

That is, the sum of the life of all tested elements (both having failed or not), divided by the number of failures observed in the test. If the test where a complete test, this expression will be the same as the simple mean of elements' life. In the expression, T is the total cumulated test time, and is measure of how much experience has been collected during the test.

Example 5.1: Consider a time limited (truncated) test with ten elements. Test was stopped at 250 hours, with four elements failed during this period (time of failures are 80, 145, 210, 238 [hour]). In this case, our point estimation for the mean life is:

$r = 4.$

$T = 80 + 145 + 210 + 238 + 6 \cdot 250 = 2173$ hours.

Confidence interval estimation. A different way for estimating mean life is using confidence intervals. In this case, the estimation of θ will be different depending on the type of test. In the following expression θ is the confidence level for the intervals.

Complete or censored test (failure limited test).

- Two sided confidence interval

$$\frac{2 \cdot T}{\chi_{2r}^{2(\alpha/2)}} \leq \theta \leq \frac{2 \cdot T}{\chi_{2r}^{2(1-\alpha/2)}}.$$

- One side confidence interval

$$\theta > \frac{2 \cdot T}{\chi_{2r}^{2(\alpha)}}.$$

Truncated test (time limited test).

- Two sided confidence interval

$$\frac{2 \cdot T}{\chi_{2(r+1)}^{2(\alpha/2)}} \leq \theta \leq \frac{2 \cdot T}{\chi_{2(r+1)}^{2(1-\alpha/2)}}.$$

- One side confidence interval

$$\theta \geq \frac{2 \cdot T}{\chi_{2(r+1)}^{2(\alpha)}}.$$

Two sided interval give us an idea of how precise was our point estimation: narrow intervals mean good estimates while wide interval means weak estimates. The second expression, corresponding to one side interval is very interesting for practical purposes. It can be interpreted as the minimum guaranteed (with confidence 1-α) life, according to the result of the test.

Graphic estimation. A graphic estimation method to estimate mean life is also available for the exponential model. Simultaneously, the graphic method tests the goodness of fit of data to the exponential distribution.

To graphically estimate mean life in incomplete reliability test, the method uses is the same for exponential and Weibull distributions, and is presented when discussing Weibull estimation.

The form used (Figure 12) has a x-axis representing age of failure, and in y-axis (with logarithmic scale) are the values of the inverse of the reliability 1/R(t). If failure ages follow an exponential model, points will form approximately a straight line.

To use this method, sample distributions function is computed with

$$F_i(t_i) = \frac{i}{n+1}.$$

Where i is the number of elements failed until age t_i and n in the sample size (total number of elements tested).

If n is great enough, $F(t_i)$ can be calculated as:

$$F_i(t_i) = \frac{i}{n}$$

Thus, using both expressions, the value for reliability estimate is:

$$R_i(t_i) = 1 - \frac{i}{n+1} = \frac{n+1-i}{n+1}$$

or:

$$R_i(t_i) = 1 - \frac{i}{n} = \frac{n-i}{n}$$

depending on the sample size.

Once points are plotted and after checking that they form a straight line, we draw a line based in the points, and the estimate of the mean life θ is obtained as the x value where our line has an ordinate of 2,72, as when R(θ) = 0,37, then 1/R(θ) = e =2,72.

Example 5.2: A test with 37 elements has been performed, assuming that they follow an exponential distribution. The life, in hours, until failure of these elements are recorded in the Table 1.

- Point estimate

Mean life: 221,46 hours

- Confidence intervals estimates:

Two sided interval (α = 5%): [153,73; 286,5]

One sided interval (α = 5%): 160,82

- Graphic estimation (Figure 13). The value obtained, about 230 hours, is similar to the numerical estimation.

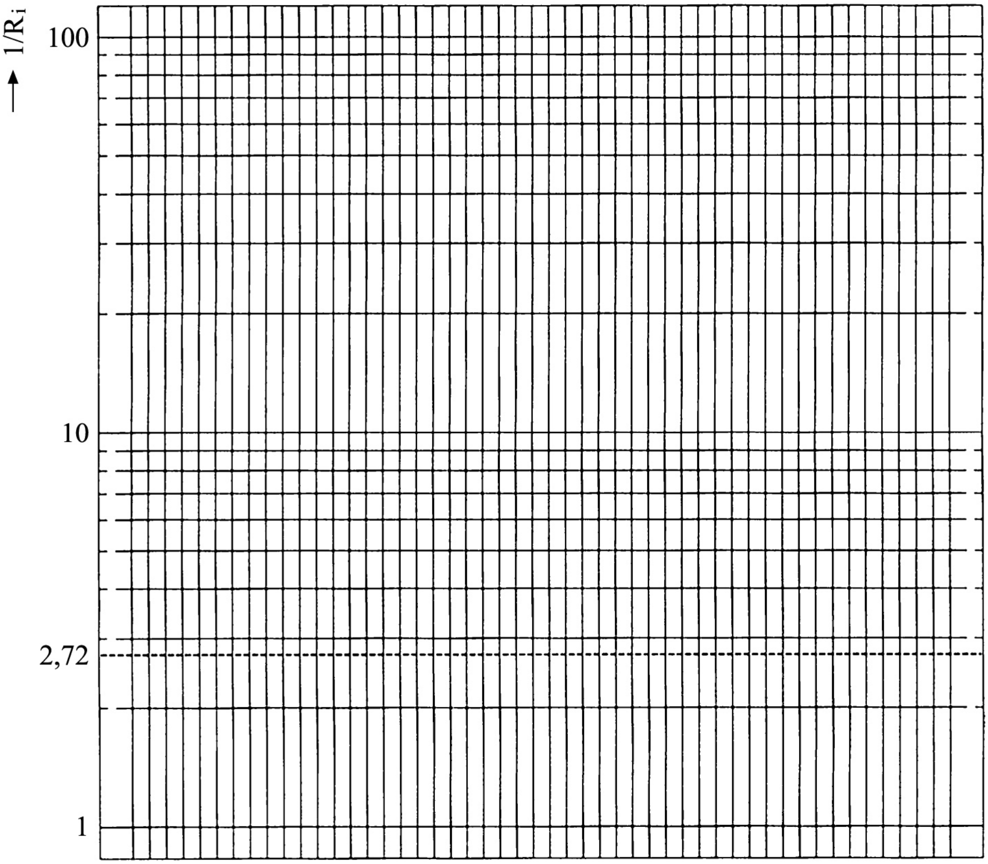


Figure 12 Exponential probabilistic paper

5.4.1.2 Tests Average Duration. Mean Failure Number

In a truncated tests, while the duration of the test is defined from the beginning, the resulting number of failures is unknown. Similarly, in censored tests the number of failures is fixed from the beginning of the test, as is the stopping criterion, but the test duration is unknown. For the exponential model, it is possible to evaluate the average duration of a test limited by the number of failures (censored) and the expected number of failures in time limited test (truncated).

Table 1. The life of element, in hours, until failure occurence

i	t_i[hour]	S_i	$1/S_i$	i	t_i[hour]	S_i	$1/S_i$
1	10	0,974	1,027	21	172	0,447	2,235
2	15	0,947	1,056	22	195	0,421	2,357
3	20	0,921	1,086	23	207	0,395	2,533
4	22	0,895	1,118	24	219	0,368	2,714
5	32	0,868	1,152	25	238	0,342	2,923
6	40	0,842	1,188	26	260	0,316	3,167
7	42	0,816	1,226	27	300	0,289	3,455
8	46	0,789	1,267	28	342	0,263	3,800
9	48	0,763	1,310	29	382	0,237	4,222
10	51	0,737	1,357	30	435	0,211	4,750
11	60	0,710	1,407	31	460	0,184	5,429
12	71	0,684	1,462	32	490	0,158	6,333
13	76	0,658	1,520	33	520	0,132	7,800
14	87	0,631	1,583	34	600	0,105	9,500
15	93	0,605	1,652	35	630	0,079	12,667
16	105	0,579	1,727	36	670	0,053	19,000
17	112	0,553	1,810	37	770	0,026	38,000
18	116	0,526	1,900				
19	127	0,500	2,000				
20	131	0,474	2,111				

Censored tests.

- For non replacement tests, the mean duration will be:

$$E(t) = \theta \cdot \sum_{i=1}^{r} \frac{1}{n - r + i},$$

where n is the sample size, r is the number of failures (stopping criterion) and θ is the mean life.

- For replacement tests, the mean duration will be:

$$E(t) = \frac{r \cdot \theta}{n}$$

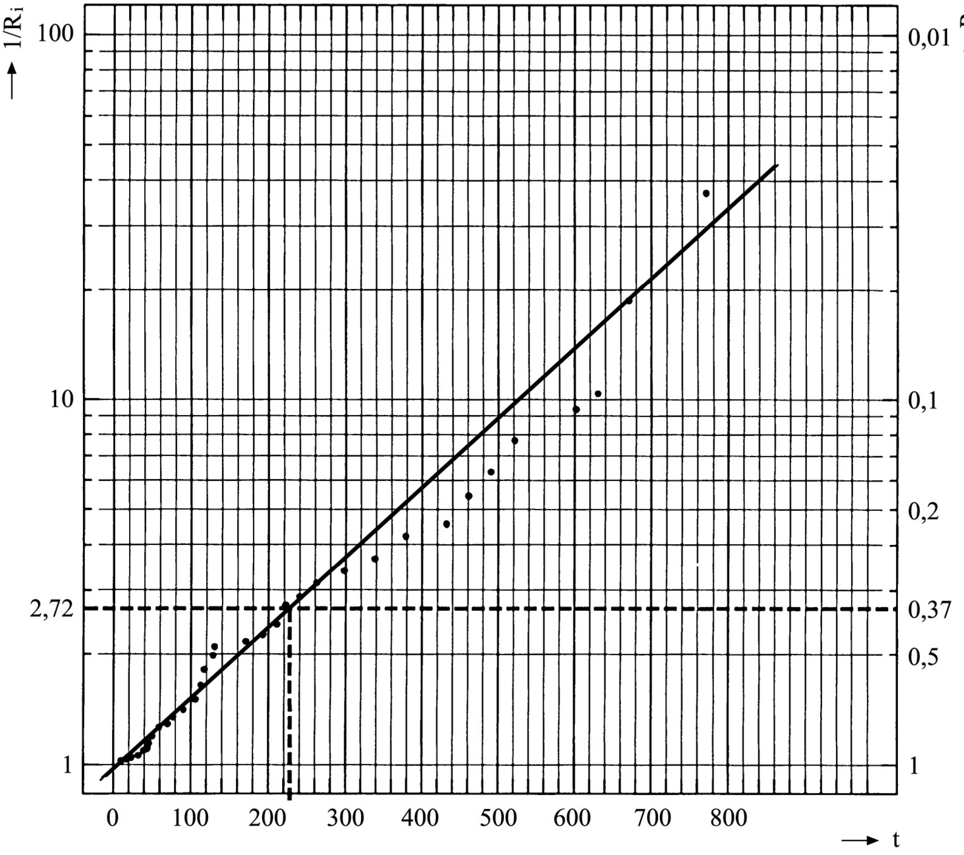


Figure 13. Graphic estimation of exponential distribution parameter

where n is the sample size, r is the number of failures (stopping criterion) and θ is the mean life.

In both cases θ must be known, what in practice requires having historical information or doing a previous test.

Truncated tests.

- For non replacement tests, the mean duration will be:

$E(r)=(1-e^{-T/\theta})\cdot n,$

where n is the sample size, T is the test duration (stopping criterion) and θ is the mean life.

- For replacement tests, the mean duration will be:

$$E(r)=\frac{n\cdot T}{\theta},$$

where n is the sample size, T is the test duration (stopping criterion) and θ is the mean life.

Again, θ must be known, what in practice requires having historical information or doing a previous test.

5.4.2 Normal Distribution

Normal distribution has two parameters, μ and σ, where μ is the mean and σ is the standard deviation. The way of estimating these two parameters depends on the type of test used.

Complete test. Point estimates are obtained with:

$$\hat{\mu} = \bar{t} = \sum_{i=1}^{n} \frac{t_i}{n}, \ \hat{\sigma} = S = \sqrt{\sum_{i=1}^{n} \frac{(t_i - \bar{t})^2}{n-1}}$$

Confidence interval estimates (with confidence level 1-α) are:

$$P\left(\bar{t} - t_{n-1}^{\alpha/2} \cdot \frac{S}{\sqrt{n}} \le \mu \le \bar{t} + t_{n-1}^{\alpha/2} \cdot \frac{S}{\sqrt{n}} \right) = 1 - \alpha$$

$$P\left(\frac{(n-1) \cdot S^2}{\chi^2_{n-1,(\alpha/2)}} \le \sigma^2 \le \frac{(n-1) \cdot S^2}{\chi^2_{n-1,(1-\alpha/2)}} \right) = 1 - \alpha$$

Graphic methods are also available for the normal distribution, using normal probability paper (Figure 14). In this form, x-axis corresponds to element's life, t_i, and y-axis is for the cumulative failure function $F(t_i)$. If data follow a normal distribution, point plotted will lie around a straight line.

After plotting points, a straight line is drawn, and with this line values of μ and σ will be obtained. To do this, we must read the values of t (x-axis) for ordinates 0,16; 0,50; 0,84, values that correspond to m-s, m, and m+s (where m is the estimate for μ and s is the estimate for σ).

Example 5.3: Ten elements have been tested to a failure mode related with wear out. Normal model is then suitable to represent these data. Failure times are: 185, 210, 225, 235, 248, 260, 275, 298, 318, 322 [hour].

Parameter estimation gives the following results:

$$\hat{\mu} = \bar{t} = \sum_{i} \frac{t_i}{10} = 257{,}6 \text{ hours}$$

$$\hat{\sigma} = S = \sqrt{\frac{\sum(t_i - \bar{t})^2}{n-1}} = 45{,}87 \text{ hours}$$

and confidence intervals will be:

- for the mean [224,79; 290,41]
- for the variance [31,57; 83,75]

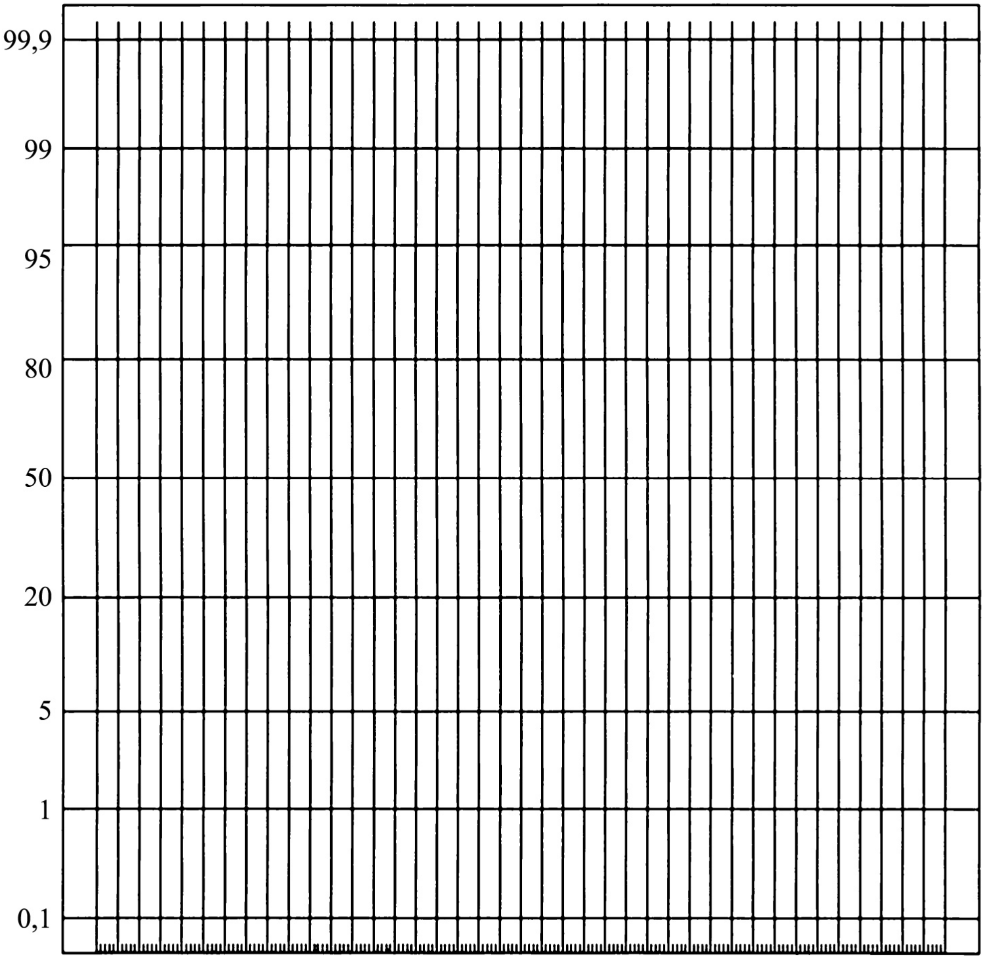


Figure 14. Normal probabilistic paper

5.4.3 Weibull Distribution

Reduced Weibull distribution is characterized by two parameters, β y θ, having the following probability density function:

$$f(t) = \beta \cdot \frac{t^{\beta-1}}{\theta^{\beta}} \cdot e^{-\left(\frac{t}{\theta}\right)^{\beta}}$$

Estimating these parameters by numerical method requires linearize the distribution function and adjusting test results to this model, usually using minimum least squares. Numerical estimation is presented in the following paragraphs. Graphic methods have been traditionally used widely, more frequently that numerical, and are also presented later.

5.4.3.1 Numerical Method

In Weibull model reliability function is (for life t):

$$R(t) = e^{-\left(\frac{t}{\theta}\right)^{\beta}} ,$$

and from this we can obtain:

$$\ln R(t) = -\left(\frac{t}{\theta}\right)^{\beta} , \; \ln\left(\frac{1}{R(t)}\right) = \left(\frac{t}{\theta}\right)^{\beta}$$

$$\ln\left(\ln\left(\frac{1}{R(t)}\right)\right) = \beta \ln t - \beta \ln \theta$$

and this expression is linear in ln(t).

If we consider that:

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

we have the estimates for β and θ, adjusting a minimum least squares regression line to the values x_i and y_i:

$$x_i = \ln t_i$$

$$y_i = \ln\left(\ln\left(\frac{1}{1-F(t_i)}\right)\right)$$

and if we write the adjusted line as y = a + mx, the estimates for our parameters are:

$$\hat{\beta} = m$$

$$\hat{\theta} = e^{\frac{a}{\beta}}$$

5.4.3.2 Graphical Method I. Complete Tests

For complete tests, the form used has a logarithmic scale in x-axis and a double logarithmic scale in y-axis. The first one corresponds to life ti and ordinates to the reliability function R(t_i) or the unreliability function F(t_i) (Figure 15).

Sample distribution function is simply the cumulative failure frequency, but with a slight correction. Values of reliability and unreliability (distribution function) are calculated with:

$$F_i(t_i) = \frac{i - 0'3}{n + 0'4}$$

$$R_i(t_i) = \frac{n + i + 0'1}{n + 0'4}$$

where i is the number of elements failed until age t_i and n is the sample size (total number of elements tested).

Points defined by (t_i, F(t_i)) are plotted in Weibull paper. We have to check if points form a straight line. If not, Weibull model is not an adequate option. If an proximate straight line is accepted, the proceed an follows:

- draw a straight line over the points plotted,
- Weibull slope, β, is obtained in the graduated arch in the top left of the Weibull paper, by drawing a parallel to the line passing by the reference point (center of the arch),
- the characteristic life, θ, is obtained as the time (x-axis) corresponding to an ordinate of 0,63 in the line drawn.

With the values of these two parameters, mean adn variance of the distribution can be calculated with:

$$\hat{\mu} = \theta \cdot \Gamma\left(1 + \tfrac{1}{\beta}\right); \;\; \hat{\sigma}^2 = \theta^2 \cdot \left[\Gamma\left(1 + \tfrac{2}{\beta}\right) - \Gamma^2\left(1 + \tfrac{1}{\beta}\right)\right] \; .$$

where Γ(.) is the Gamma function.

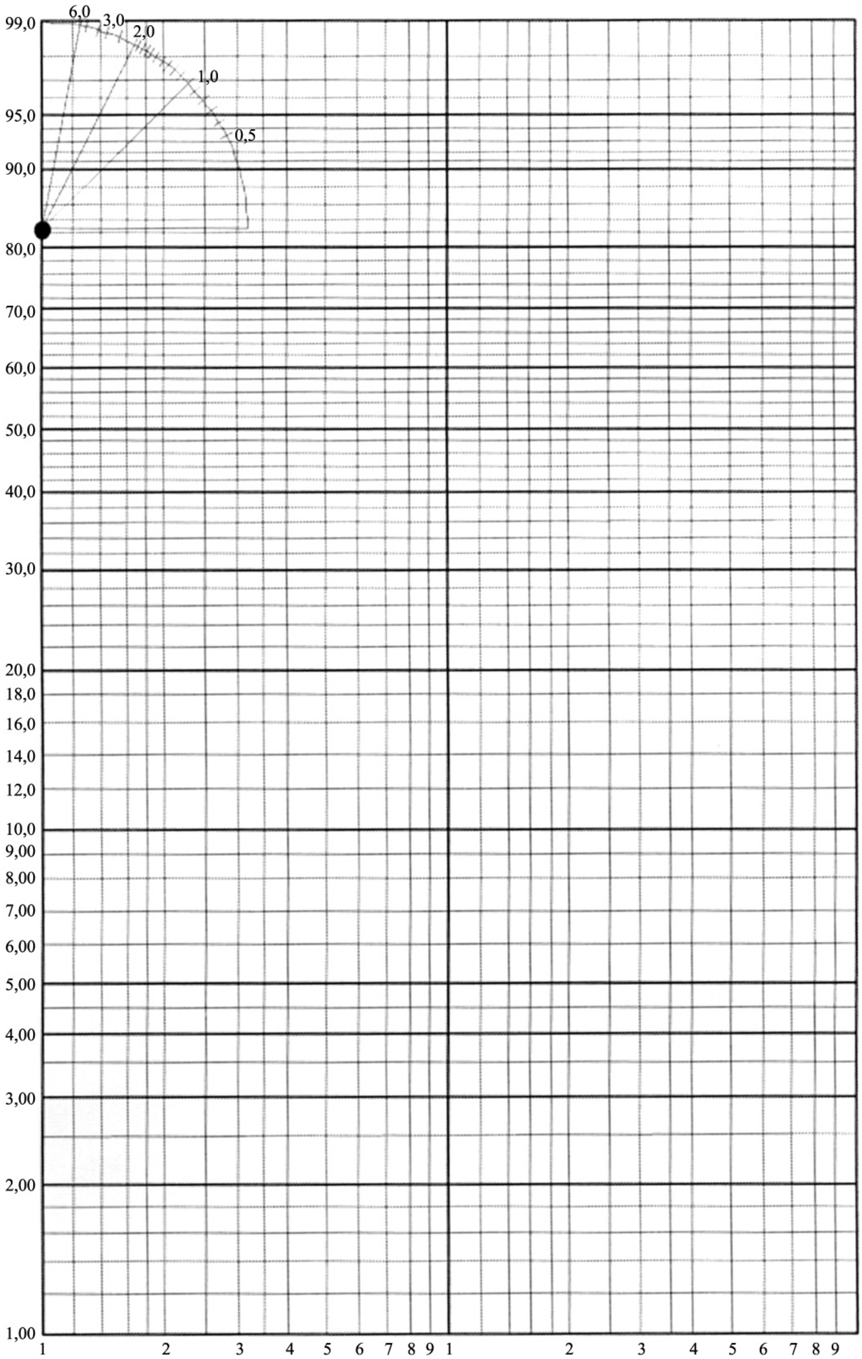


Figure 15. Weibull probabilistic paper for complete tests

Example 5.4: Twelve steel springs have been tested until failure. Number of work cycles have been recorded.

With the values obtained we compute the values of the estimated distribution function for each the failure times in Table 2.

Table 2. Values of the estimated distribution function for each the failure times

T_i	F_i	T_i	F_i
116800	5,6	171500	54,0
138500	13,7	191300	62,1
155500	21,8	220800	70,2
157700	29,8	229000	78,2
158000	37,9	245900	86,3
171000	46,0	262300	94,4

Using Weibull probabilistic paper, the corresponding points are plotted (Figure 16), and values for parameters estimetes can be obtaied:

$\beta = 4{,}5$, $\theta = 195000$ work cycles.

5.4.3.3 Graphical Method II. Incomplete Tests

For incomplete tests, we have to record failure times t_i, where r of the total K tested elements have failed. The procedure is valid for both censored and truncated test, that is for test limited by time or bay failures.

Weibull paper used for this second case is different to that used in the previous paragraph. Values in x-axis is again for the failure age of the failed elements, while ordinates correspond the cumulative hazard function (Figure 17).

Hazard function is computed as:

$$h_t = \frac{100}{K - m_t}.$$

where K is the number of elements tested and m_t is the number of elements with life under t (both failed and surviving elements).

Hazard function is computed only for elements failed at their corresponding failure times (so we have r values for h_t).

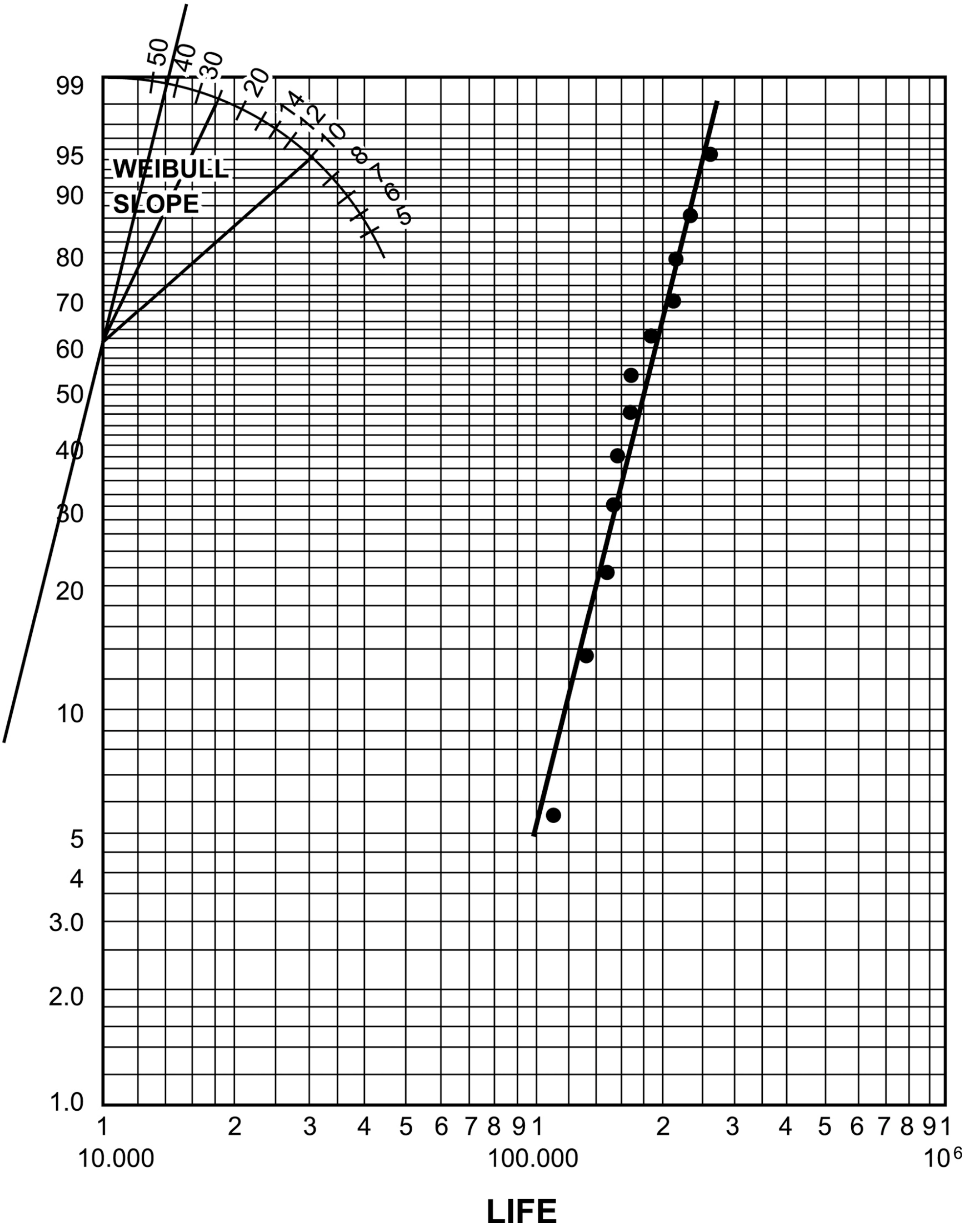


Figure 16. Graphical estimation of Weibull distribution parameters for complete tests

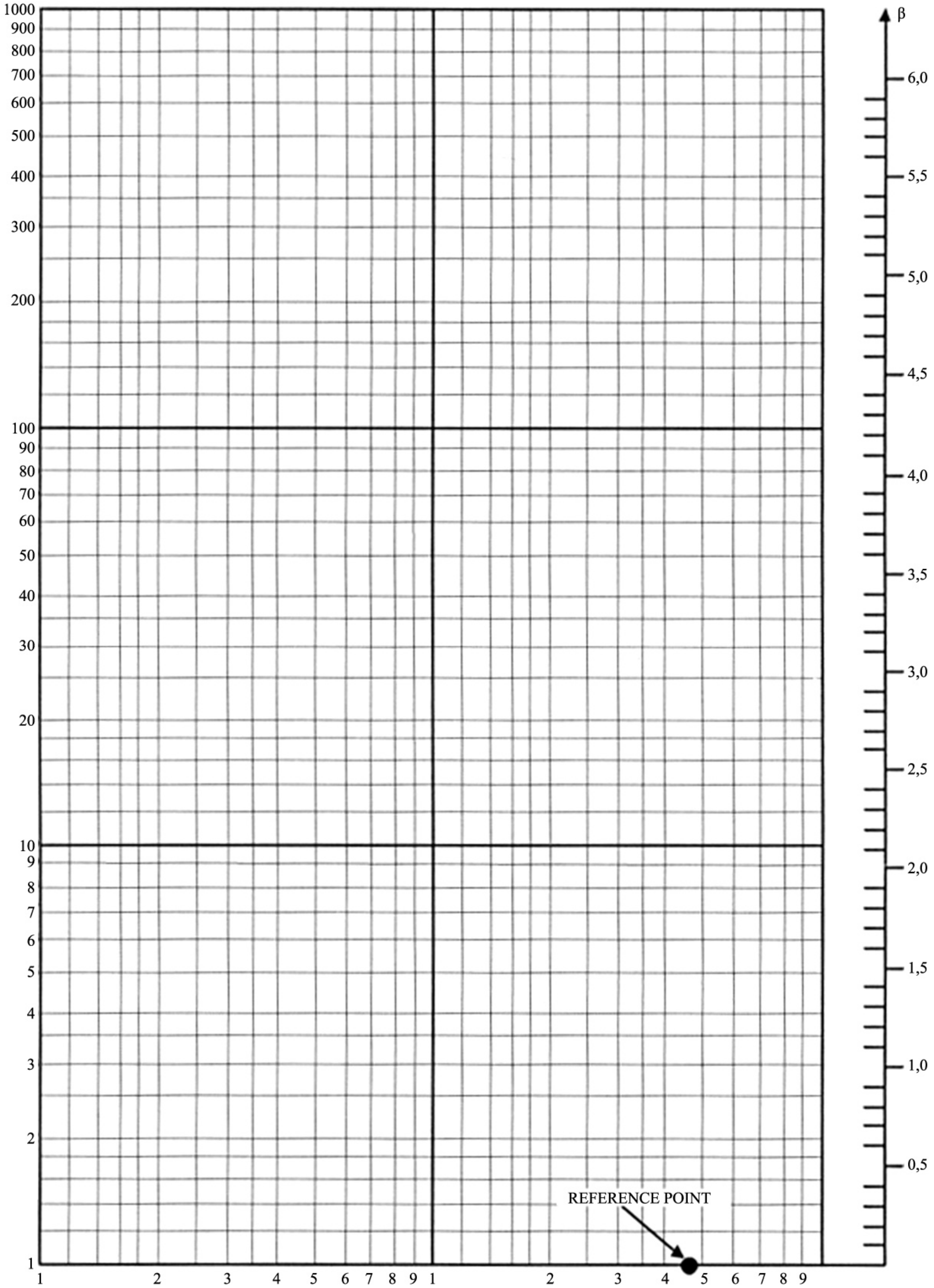


Figure 17. Weibull probabilistic paper for incomplete tests

Then we calculate the cumulative hazard function H_t, and points (t, H_t) for failure times will be plotted. To estimate Weibull parameters we proceed as follows:

- check if point form approximately an straight line. Trace a straight line over the points plotted.
- draw a parallel to this line by the reference point. Weibull slope β can be read where this parallel cuts the corresponding scale.

The characteristic life, θ, is obtained as the time (x-axis) corresponding to a cumulative hazard value of 100.

Example 5.5: A sample of twenty roller bearings is tested against fatigue failure. Test was limmited to 250 hours, and nine elements have failed.

Failure times: 128, 145, 162, 170, 191, 210, 223, 235, 246 [hour].

In two other elements the test was stopped by reasons different to element failure, in time 155 hours and 220 hours. Table 3 presents data and hazard function calculations.

Table 3. Data and hazard function calculations

t_i	n_i	h_t	H_t
128	20	5,00	5,00
145	19	5,26	10,26
155**	18		
162	17	5,88	16,15
170	16	6,25	22,40
191	15	6,67	29,06
210	14	7,14	36,21
220**	13		
223	12	8,33	44,54
235	11	9,09	53,63
246	10	10,00	63,63
250**	9-1		

Using the graphical method presented, we obtain Figure 18, obtaining the following estimates:

β = 4, θ = 290 hours.

Weibull slope value is read in the righ hand side scale, while characteristica life is obtained as the time for cumulative hazard equals 100.

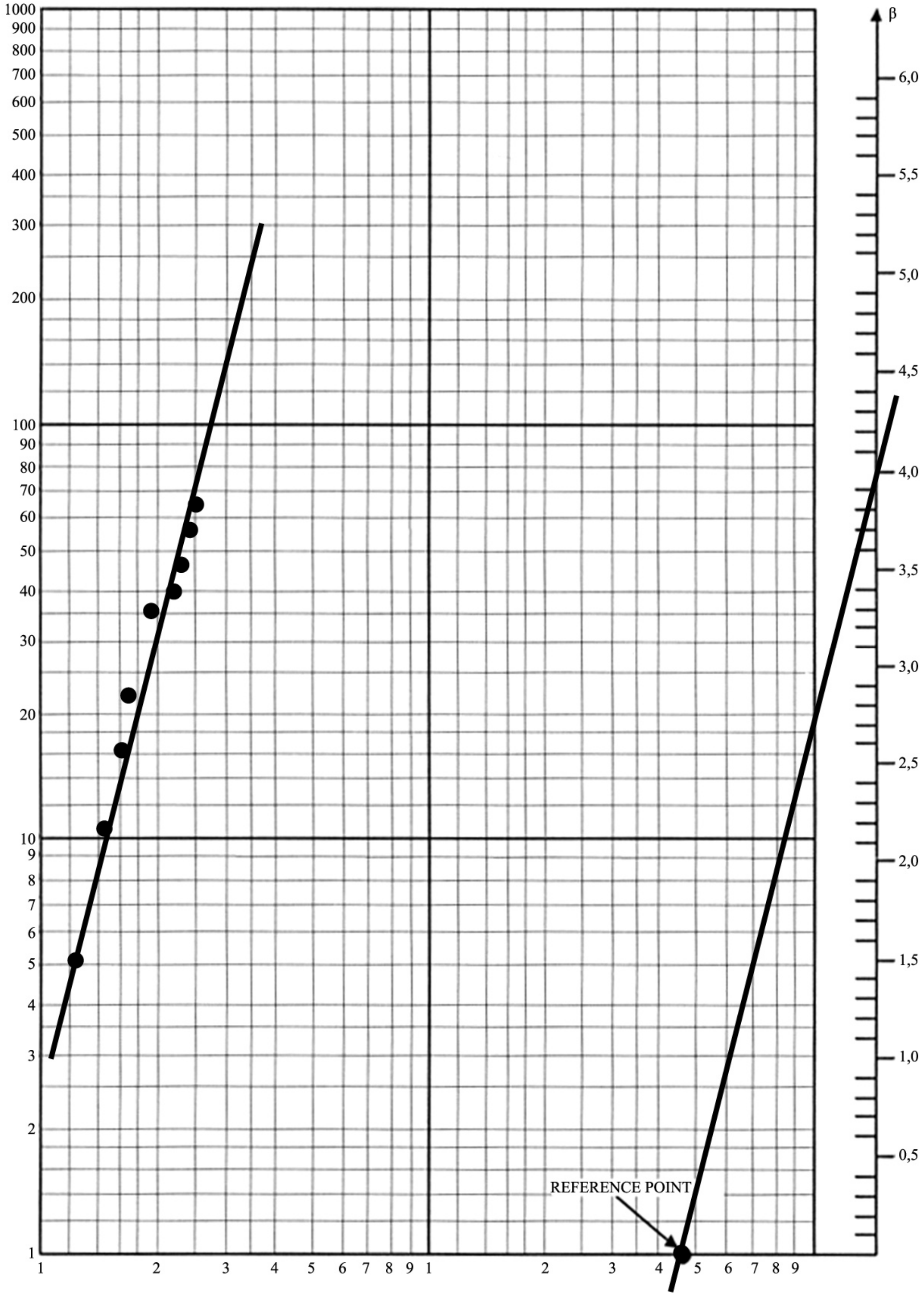


Figure 18. Graphical estimation of Weibull distribution parameters for incomplete tests

5.5 COMPARISON TESTING

The goal of this type of tests is not to estimate the values of the distribution parameters, but to check if a previously stated hypothesis or requirement is achieved, usually referred to the distribution mean life.

Formally, these tests are hypothesis tests, where the null hipothesis (H_0) is that the mean life has some specified value, and the alternative hypothesis (H_1) is that the mean value is different (or frequently lower than) the specified value. For example, we can test $H_0(\theta \geq \theta_0)$ vs $H_1(\theta < \theta_0)$, to check of our systems mean life is equal to θ_0 or is lower to this value.

In practice, this test compares the estimated mean life with a critical value, accepting the null hypothesis if estimated mean is over the critical value and rejecting in other case. As in any other statistical test, we have to consider a level of uncertainty in our decisions, and we have to decide the confidence level of the test.

Usually incomplete testing is used. In the following the methods for censored and truncated tests are presented. It is important to say that we are assuming exponential model.

Censored tests. The hypothesis to test are $H_0(\theta \geq \theta_0)$ vs. $H_1(\theta < \theta_0)$.

Considering that r is the number of failures observed (stopping criterion), then:

$$\sum_{i=1}^{r} \frac{2 \cdot t_i}{\theta} = \frac{2 \cdot T}{\theta} \equiv \chi^2_{2r}$$

where t_i are the failure times corresponding to r observed failures. Its distribution is a Chi Square with 2r degrees of freedom.

With this information, the rule for deciding is the same as for $H_0(\theta = \theta_0)$ vs. $H_1(\theta < \theta_0)$, and the zone for rejecting the null hypothesis is:

$$R = \{\vec{t} \,/\, \hat{\theta} < a\} \ .$$

and as the estimate of θ is T/r, we have:

$$R = \{\vec{t} \,/\, T < r \cdot a\} .$$

If the confidence level is fixed at 1-α, the interval for accepting H_0 is:

$$1\text{-}\ \alpha = P(T \geq r \cdot a \,/\, \theta = \theta_0) = P\left(\frac{2 \cdot T}{\theta} \geq \frac{2 \cdot r \cdot a}{\theta} \,/\, \theta = \theta_0\right) = P\left(\chi^2_{2r} \geq \frac{2 \cdot r \cdot a}{\theta_0}\right)$$

and:

$$\frac{2\cdot r\cdot a}{\theta_0}=\chi_{2r}^{2(\alpha)} \text{ and } a=\frac{\theta_0}{2\cdot r}\chi_{2r}^{2(\alpha)}.$$

Then, H_0 will be rejected when

$$R=\left\{\vec{t}\,/\,T<\frac{\theta_0}{2}\chi_{2r}^{2(\alpha)}\right\}.$$

Test efficiency, as its operating characteristic curve, can be checked. The probability of accepting H_0, depending on the value of θ is:

$$P_a=P\left(T\geq\frac{\theta_0}{2}\chi_{2r}^{2\,(\alpha)}\right)=P\left(\frac{2\cdot T}{\theta}\geq\frac{\theta_0}{\theta}\chi_{2r}^{2\,(\alpha)}\right)=P\left(\chi_{2r}^{2\,(\alpha)}\geq\frac{\theta_0}{\theta}\chi_{2r}^{2\,(\alpha)}\right)=1-F_{\chi^2_{2r}}\left(\frac{\theta_0}{\theta}\chi_{2r}^{2\,(\alpha)}\right)$$

where F is the distribution function of a Chi Square with 2r degrees of freedom.

Example 5.6: Some type of relays are been installed in an industrial equipment, and the requirement asks for 100000 commutations as minimum value for the mean life. To check if the goal is achieved, and to accept or reject a relays shipment, a test censored to 20000 commutations is prepared. The results are:

- number of failures: 4,
- failure times: 8000, 12500, 16000, 18800 [?].

To accept or reject shipment, with α=5%, the acceptance zone is:

$$A=\left\{\vec{t}\,/\,T\geq\frac{\theta_0}{2}\chi_{2r}^{2(\alpha)}\right\}$$

where: θ_0 = 20000, r = 4, $\chi_8^{2(0.05)}=$15,51, resulting:

$$A=\left\{\vec{t}\,/\,T\geq 155100\right\}$$

and as in this test T = 275,300, relays must be accepted.

Truncated test. The hypothesis to test are usually:

$H0(\theta\geq\theta_0)$ vs $H1(\theta<\theta_0)$.

In this case, test is limited by time. To do this, a sample of size n is taken and, depending on the number of failures observed (until time T_0, the stopping criterion) null hypothesis will be accepted or not.

Table 4 shows the minimum sample size to use, depending on the number of failures allowed to accept the null hypothesis. Sample size also depends on the ratio T_0/θ_0 where T_0 is the test duration and θ_0 is the meal life value to test. Confidence level for the table is 90%, and exponential distribution is assumed.

Table 4. Sample size for truncated tests (confidence level 90%)

Acceptance number	Ratio T_0/θ_0												
	1,0	0,5	0,2	0,1	0,05	0,02	0,01	0,005	0,002	0,001	0,0005	0,0002	0,0001
0	3	5	12	24	47	116	231	461	1.152	2.303	4.606	11.513	23.026
1	5	9	20	40	79	195	390	778	1.946	3.891	7.780	19.450	38.838
2	7	12	28	55	109	266	533	1.065	2.662	5.323	10.645	26.612	53.223
3	9	15	35	69	137	333	668	1.337	3.341	6.681	13.362	33.404	66.808
4	11	19	42	83	164	398	798	1.599	3.997	7.994	15.988	39.968	79.936
5	13	22	49	97	190	462	927	1.855	4.638	9.275	18.549	46.374	92.747
6	15	25	56	110	217	528	1.054	2.107	5.267	10.533	21.064	52.661	105.322
7	16	28	63	123	243	589	1.178	2.355	5.886	11.771	23.542	58.855	117.710
8	18	31	70	136	269	648	1.300	2.599	6.498	12.995	25.990	64.974	129.948
9	20	34	76	149	294	709	1.421	2.842	7.103	14.206	28.412	71.030	142.060
10	22	37	83	161	319	770	1.541	3.082	7.704	15.407	30.814	77.034	154.068
11	22	40	89	174	344	830	1.660	3.320	8.300	16.598	33.197	82.991	165.982
12	25	42	95	187	369	888	1.779	3.557	8.891	17.782	35.564	88.908	177.816
13	27	45	102	199	393	947	1.896	3.792	9.479	18.958	37.916	94.790	189.580
14	29	48	108	212	417	1.007	2.013	4.026	10.064	20.128	40.256	100.640	201.280

Example 5.7: A shipment from a supplier is been checked in a truncated test od 100 hours, allowing only one failure during the testing time. Requiered mean life is 1000 hours. If α=10%, how many elements need to be tested?

$T_0 = 100$,

$\theta_0 = 1000$ hours.

And the ratio is:

$T_0/\theta_0 = 0{,}1$.

As the acceptance number is 1, using Table 4, we obtain that:

$n \geq 40$.

From the observation of the real life, it is deduced that elements theoretically equal have different behaviours upon submitting them to the same operation conditions. These variations compel to a statistic treatment for the estimation of the reliability, but all statistical process is based on measured real and observed facts and, therefore, it will be necessary to obtain the real data for the determination of this reliability.

Chapter 6

RELIABILITY TESTING PLANS

6.1 ADVANCED CONCEPTS OF RELIABILITY ACCELERATED TESTINGS

One of the basic problem of the quality of service rising of modern systems is assurance of their high level reliability, what is in direct connection with decreasing the life cycle cost. It's enough to say, for example, that at the computer systems the hardware failures and software errors make worthless all previous work, solving of problems must be repeated, and it stops work of the complex automation systems which operate in "real time" regime. This, of course, causes considerable rise in the life cycle cost.

One possible concept of the life cycle engineering, which also comprises a phase of the system testings, has been developed at University of Exeter, The Centre for Management of Industrial Reliability and Cost Effectiveness, Exeter, UK, [15], as it is shown in Figure 19.

Requests for high reliability, during the system testings for reliability assessment, result in enormous consumption of time, material and cost. According to the estimations described in [16], in the World, the testing cost for reliability control is even 50-70% of development system cost. Testing cost for reliability assessment, in Russia, for example, is 20.000 to 150.000 dollars, depending on the strength and complexity of the company itself [17]. This shows modern tendency to get more information for reliability analysis. However, the testing cost rise brings down the competittiveness of a company at trade.

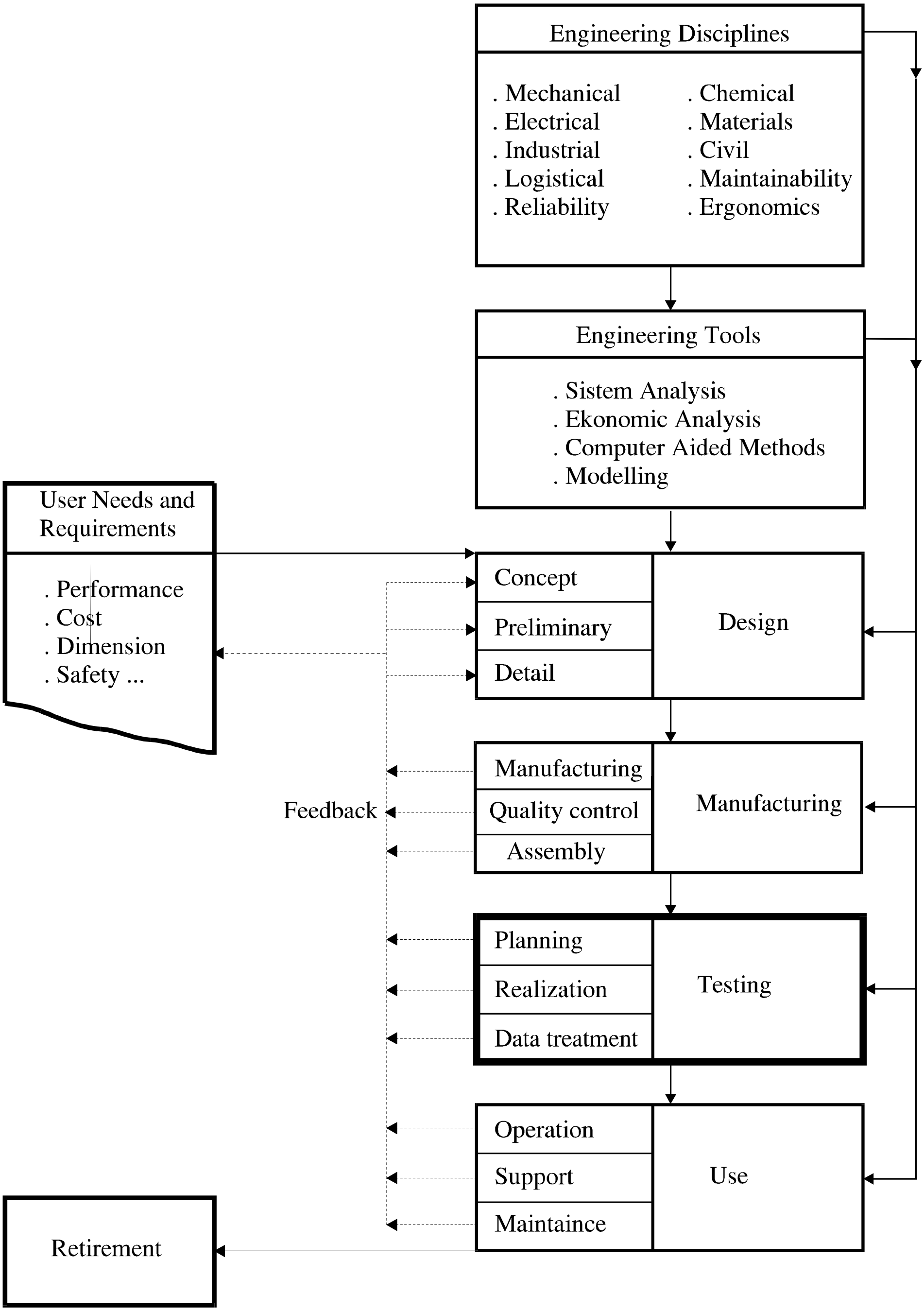


Figure 19. Concept of the life cycle engineering

That is why different procedures of accelerated testings are being intensively investigated and why they are getting practical use relating to the testings of long duration, so-called "exploitation watching", in other to obtain, at the end, the decrease of the life cycle cost [18].

6.2 ACCELERATED TESTINGS

It is not necessary, either rational, to subject all system's elements to testings during system accelerated testings for reliability assessment. It is enough to subject, according to the priority, to the accelerated testings only those elements or elements which restrict the quantity or quality of the system reliability parameters [19]. For all that, one should keep in mind the logical principle, shown in Figure 20, that the system reliability assessment of its each element (which mean time between failures, depending on kind of the system, can take hundred thousands hours of use), requires inadmissable much time and cost. This can be illustrated with some real examples [20].

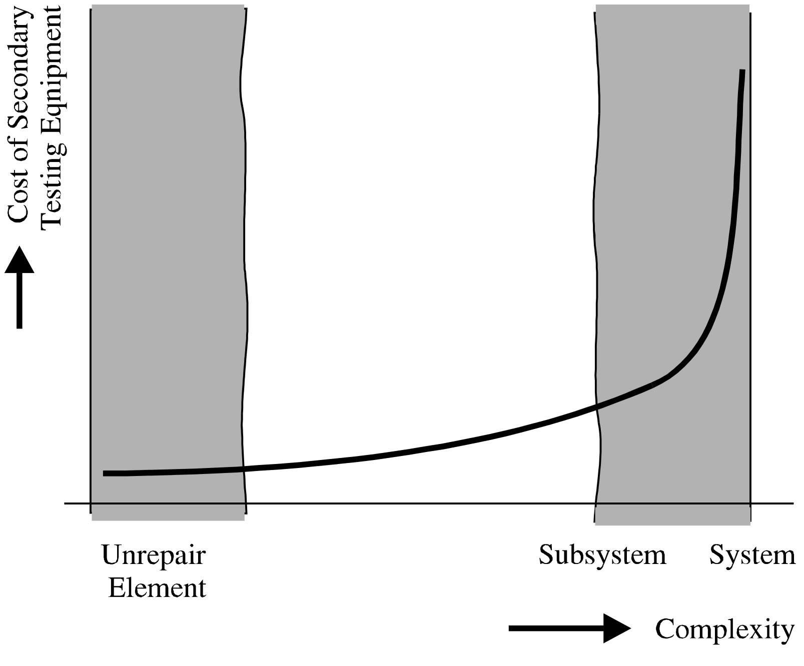


Figure 20. Dependence of cost of secondary testing equipment cost according to system complexity

The accelerated testings for strength assessment of 10 tractor motor crankshafts costed 2 % of testing cost during use of the tractors. As well, the accelerated testings of the tractor gearings were 27 times cheaper and they lasted 18 times shorter than the testings in use. Finaly, there is data that the accelerated testings of a tractor booth (cabin) costed 9 times cheaper and lasted 20 shorter than if they were done during use.

6.3 BASIC APPROACH

As distinguished from the accelerated, that is, forced testings (which base on intensifyng of the process or operating regime), this chapter examinates the accelerated testings without intense the processes which often result in additional failures or damages what brings, in the end, to distortion of the real picture of the system behaviour and reliability in state of use. The demonstrative testings represent one of the possible approaches to problem solving according the accelerated testings [16]. For example, in accordance with the current regulations of International Civil Aviation Organization (ICAO), it is permissible to demonstrate possibility of successful flight of the civil planes with shortened testings in restricted number of flights. It can be explained with the fact that it is impossible to provide, for such complex systems as the planes are, the secondary equipment for reliability performances assessment of each individual element that will operate in the completely controlled conditions, as it is shown in Figure 20. Modern interpretation of the demonstrative testings takes additional information from the shortened testings which are being carried out in different phases of the life cycle system. By realization of an approach, the basic volume of testings is transferred from the use phase of the system to the modeling and testings with simulation in early phases of design (concept and preliminary design), as it is shown in Figure 19. Such an approach is based on the potential failure modes, causes, effects and criticality analysis in design and development of the systems [19].

6.4 RELIABILITY SHORTENED TESTING PLAN

All testings of systems for reliability assessment can be devided into three phases [21]:

1. planning,
2. performing testings,

3. processing results to determine expected parameters or make decisions.

Each phase requires correspondent problems solution according to its metodology. The most complex and the most important problem while planning testings is to determine testings scope (sample size n), testing results credibility and precision depend on it.

The following important factors, taken into consideration for forming knowledge-based plans of shortened testings for systems reliability assessment, are given:

1. testing one or more systems (1 or N),
2. continuous control, periodical control or control only before start or at the end of testing,
3. testing with or without maintenance (replacement) of failure systems,
4. simultaneous testings or testings in various periods of all systems,
5. testings up to failure of all systems or to in advance fixed failure quantity or up to the end of in advance fixed UP TIME.

Combining given factors a number of varous plans of shortened testings for systems reliability assessment be formed, they have following marks:

1. [NUN], [NUr], [NUT], [NU(r,T)];
2. [NRr], [NRT], [NR(r,T)];
3. [NMr], [NMT], [NM(r,T)].

Testing plans classification ([NU...], [NR...], [NM...]) for system reliability assessment according to criterion - testing interruption factor (r, T, r or T) is given in Table 5.

Table 5. Shorted testings plans classification according to testing interruption criterion and system maintainability

Criterion of testing break	Plan of shortened testings for reliability assessment		
	Object are not replaced: U	Object are replaced: R	Object are maintained: M
r	[NUr]	[NRr]	[NMr]
t	[NUT]	[NRT]	[NMT]
r or T	[NU(r,T)]	[NR(r,T)]	[NM(r,T)]

Realization of testing plan is performed according to the following model [22]. A quantity of failures occurred up to the moment t is marked by d(t). Function d(t) cannot decrease, and it takes values 0, 1, 2, ..., successively in the course of testing. Growth function points d(t) correspond to random moments t_i. Real function d(t) obtained by testing is called testing process trajectory or failure number distribution. When failure number distribution d(t) enters G planes region (Figure 21) testings are interrupted.

Plane G is a semi-plane t>T with plans [NUT] and [NRT]. According to these plans testings are interrupted at the moment T when the trajectory d(t) enters the region G = {d(t):t≥T} (Figure 21.a). In the case of plans [NUR] and [NRr] testings are interrupted at the moment t_r when the trajectory d(t) enters the region G = {d(t):d≥r} (Figure 21.b). At the end with plans [NU(r,T)] and [NR(r,T)] testings are interrupted at the moment when the trajectory d(t) enters the region G = {d(t): or t≥T or d≥r} (Figure 21.c).

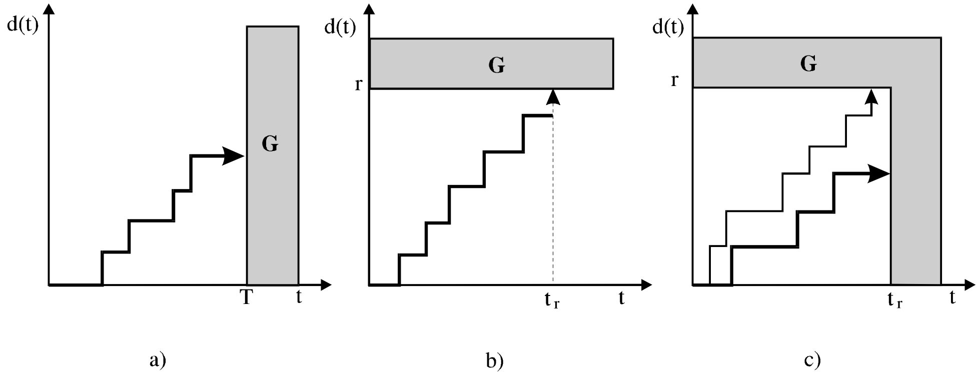


Figure 21. Testing process trajectories with different plans for reliability assessment testing

To test hard metal (HM) plates durability, the optimum plan of shortened testing for reliability assessment, type [NRr], is the most convenient (limitation: maximum testing time, expected reliability parameter: mean UP TIME). It is treated in the following way. N HM plates of the same type is constantly tested. HM plates failed at testing are replaced by new ones. Testing is interrupted when a number of HM plates is r.

On the basis of the initial algorithm [21], testing plan is defined quantitatively [NR50] (Table 6). According to this plan, a parameter, that is, a quantity of failed HM plates when testing is interrupted, is r = 50.

Table 6. Quantitative defining shortened testings plan [NR50]: Proposed values for determining failure number r

δ	Failure numbers r at γ equals			
	0,80	0,90	0,95	0,99
0,05	315	650	1000	2500
0,10	80	200	315	650
0,15	50	100	150	315
0,20	25	50	100	200

Adopted values: δ = 0,20; γ = 0,90
Quantitative testing plan definition: [NR50]

It is enough to say that failures make worthless the entire preliminary work at many systems, for example, at the computer systems, then they bring to nacessary repeatings of the problem solutions and to the stoppages in work of the complex automatized systems. Naturally, all these cause significant increases of the systems life cycle cost. The claims for high reliability, which are set to the modern systems, take much time and money and ask for great material consumption during reliability testings. However, the cost increases of the reliability testings lower the competitiveness of the companies. For that reason the different procedures of accelerated testings are being intensively researched and applied in practice in order to reduce systems life cycle cost and to replace the long-term testings. In this paper the advanced accelerated testings concepts of reliability are based on: making smaller the volume of the system sample, the reducing of testing time and precision increase of the parameter measurings, what enable getting of information on the system reliability without accuracy loss of the analysis and with the reduced cost.

Chapter 7

RELIABILITY BLOCK DIAGRAM

7.1 INTRODUCTION

It is important to clarify the difference between elements reliability and systems reliability. In the first one we are only concerned by the overall operation of the element in terms of its life while accomplishing a certain mission. In the second one we will consider that, in complex items (called systems), their structure and elements are determinant for their survival or failure in the assigned mission. It is then an essential object of interest the role that plays this internal structure in the success or fail of the mission [14].

Sometimes, in systems we can find elements that don't have influence in the development of a certain mission, although they can have in others. Since these elements don't influence the operation, they will neither influence the reliability, and, in consequence, we will ignore them for the corresponding calculations.

To determine the reliability of a system, we should find the reliabilities of each one of the influential elements. We will construct a certain type of functional chart, that is to say, a graphic representation of the connections among the influential elements, in order to verify what happens with the system when each one of them fails. The reliability block diagram will include an entrance to and an exit from the system, and each one of the elements will be united by connector lines, so that, if all the possible "routes" that unite entry with exit fail, then the system will fail [5,11].

From this chart we will be able to find what we will call "calculated reliability", since it is determined in base to the probability theory and not by means of tests. The reliability value obtained from life tests would be the "observed reliability". Evidently, the observed reliability should coincide with the calculated reliability, because other result only means that we have made some mistake in the analysis process, or that the mission has been developed in different conditions to those that were used to calculate the elements reliabilities.

Is important to emphasise that the functional reliability chart, does not necessarily corresponds with the physical system structure. It is more a functional representation of the behaviour of the system against the failure. In the following sections we will study some typical systems models and the way to perform their reliability analysis.

7. 2 SERIES SYSTEMS

7.2.1 Definition

A system is called to be a series system when the full system works if and only if all of its elements are functioning. It is equivalent to say that the system fails if at least one of its elements fails. From this definition we can construct the graph of Figure 22.

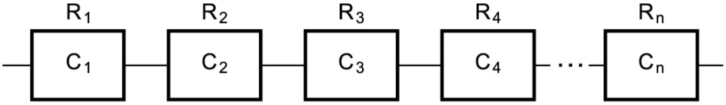


Figure 22. Series system

If we call R_i to each of the elements C_i reliabilities and R_s to the system reliability, and we assume the independence between elements, the system reliability will be:

$$R_s = P(T_s>t) =$$
$$= P[(T_1>t)\cap(T_2>t)\cap...\cap(T_n>t)]=P(T_1>t)\cdot P(T_2>t)\cdot\ ...\ \cdot P(T_n>t)$$

$$R_s = R_1\cdot R_2\cdot ...\cdot R_n\ ,$$

where T_s is the life of the system, T_i is each elements C_i, life and n is the number of elements of the series system.

Thus, **the system reliability is the product of the elements reliabilities**. The survival of the system requires the survival of all the elements.

Example 7.1: In Figure 23 we show a sample series system with five elements.

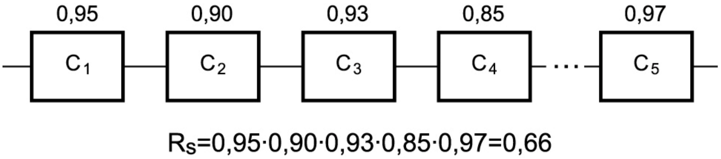


Figure 23. Example of series systems reliability calculation

As the system reliability is the product of the elements reliabilities, and all these probabilities are lower than 1, if the number of multiplying reliabilities (the number of elements of the system) is high, the system reliability value can be very small, even if each of the individual elements have a good realibility value. For instance, if we connect in a series system 150 elements, each with reliability 0,99, the system reliability will be:

$$R_s = 0{,}99^{150} = 0{,}22.$$

7.2.2 Exponential Series Systems

In the central part of a element's life, the exponential life model is the most frequently used. For such a element the pdf for the random variable "life of the element" is:

$$f_i(t) = \lambda_i \cdot e^{-\lambda_i \cdot t}, \ t\geq 0,$$

and the reliability function is:

$$R_i(t) = e^{-\lambda_i \cdot t}, \ t\geq 0.$$

For the case of a series system composed only of exponential elements, the reliability calculation will be:

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = \prod_{i=1}^{n} e^{-\lambda_i \cdot t} = e^{-t\cdot\sum_{i=1}^{n}\lambda_i}.$$

If we call $\lambda_s = \Sigma\lambda_i$, then:

$$R_s(t) = e^{-\lambda_s \cdot t},$$

that is, the system life is also a exponentially distribution random variable, with a failure rate that is the sum of the failure rates of the system elements.

Following with this case, the system mean life will be the inverse of the sum of the inverses of the elements mean lives:

$$\theta_s = \frac{1}{\lambda_s} = \frac{1}{\sum_{i=1}^{n} \lambda_i} = \frac{1}{\sum_{i=1}^{n} \frac{1}{\theta_i}},$$

and, if all the elements forming the system are identical, the system mean life will be:

$$\theta_s = \frac{\theta_i}{n}.$$

Figure 24 shows the reliability change with respect to life time, for various n values, when all elements are identical and the life model, for all elements, is exponential.

7.3 PARALLEL REDUNDANT SYSTEMS

7.3.1 Definition

A system is called to be a parallel redundant system if verifies the following conditions:

- The system fails only if all its elements fail. It is equivalent to say that the system survives if at least one of the elements survive.
- Each element is capable, by itself, to accomplish the mission.
- All not failed elements are operating all the mission time (all the elements are simultaneously **under charge**).
- The elements are mutually independent, that is: the state of fail or not fail of each element don't modifies the reliability of the rest of the elements.

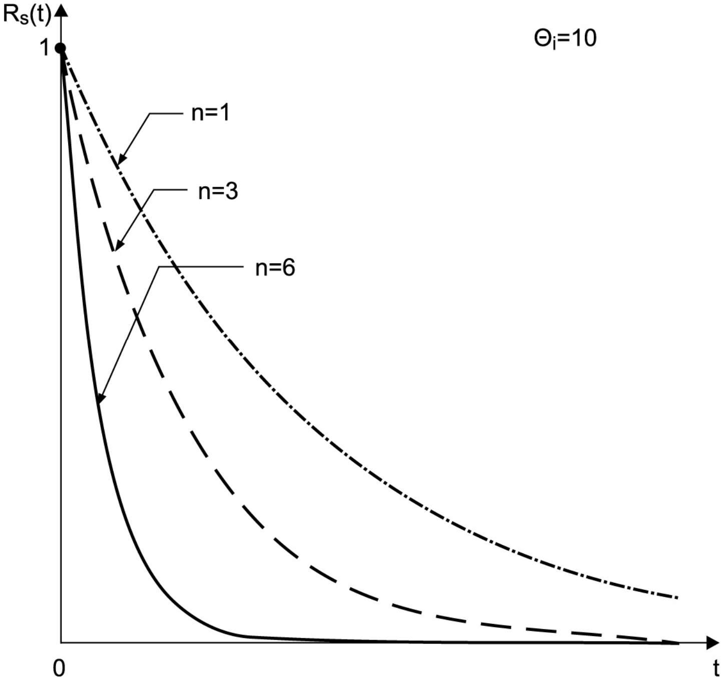


Figure 24. Series system reliability with identical elements

From the first condition we can deduce the reliability block diagram of Figure 25.

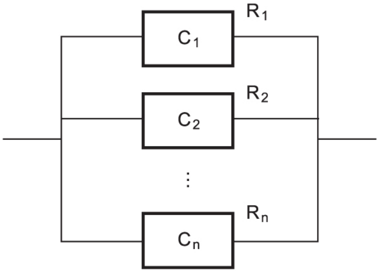


Figure 25. Parallel system

The system reliability can be calculated as:

$P(T_s<t) = P\ [\ (T_1<t) \cap (T_2<t) \cap \ldots(T_n<t)\ ] = P(T_1<t)\ P(T_2<t)\ \ldots\ P(T_n<t)$ and as $P(T<t) = 1 – R(t)$, it results:

$$P(T_s<t) = 1 - R_s = (1-R_1) \cdot (1-R_2) \cdot\ldots\cdot (1-R_n),$$
$$R_s = 1 - (1-R_1) \cdot (1-R_2) \cdot\ldots\cdot (1-R_n).$$

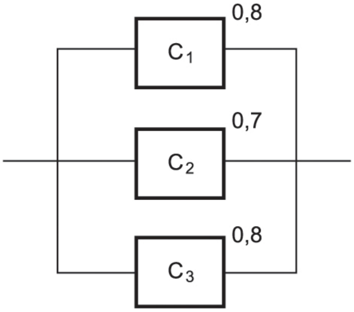
where T_s is the system life, T_i is each elements C_i, life and n is the number of in parallel elements.

Observe that the effect of such system structure in the reliability ios just the opposite of the series structure: in a parallel redundant system the system reliability is the product of the elements reliabilities.

Example 7.2: Figure 26 shows a simple three elements redundant parallel system. System reliability is 0,988, much greater than any of the elements reliabilities.

In this type of systems, as the number of parallel elements increases, system reliability will also increase, even starting with low reliability elements. For example, if we consider a 20 parallel elements system, each one of them with reliability 0,2, the system reliability will be:

$$R_s = 1 - (1-0,2)^{20} = 0,988.$$



$R_S=1-(1-0,8)\cdot(1-0,7)\cdot(1-0,8)=0,988$

Figure 26. Example of parallel system reliability calculation

7.3.2 Exponential Redundant Parallel Systems

If we consider a parallel system integrated by exponential elements, each of them with life probability density function:

$$f_i(t) = \lambda_i \cdot e^{-\lambda_i \cdot t}, t\geq 0,$$

and reliability function:

$$R_i(t) = e^{-\lambda_i \cdot t}, t\geq 0,$$

we obtain for the entire system the reliability function:

$$R_s(t) = 1 - \prod_{i=1}^{n} \left[1 - R_i(t)\right] = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda_i \cdot t}),$$

which do not corresponds to a exponential model reliability function: a redundant parallel system integrated by exponential elements does not has a exponential distribution.

If all the elements were identical, we can obtain that:

$$R_s(t) = 1 - \left(1 - e^{-\lambda_i \cdot t}\right)^n,$$

and the system mean life:

$$\theta_s = \theta_i \cdot \left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right).$$

Figure 27 shows the effect in system reliability of the use of the redundant parallel structure.

7.4 SERIES-PARALLEL SYSTEMS

In many cases, complex systems can be fully decomposed in such subsystems that all of them are series or parallel systems. Making the analysis of this "mixed" systems is easy if we apply the previous calculation principles for each series or parallel subsystem, substituting each subsystem by a "virtual element" with its same reliability, and repeat again the process in a reiterative simplification process. The problem is that the analysis can be boring and the error becomes easy. We show some examples illustrating this calculation procedure.

Figure 28.a shows a RBD with a series system of two parallel subsystems. Figure 28.b shows a RBD with a parallel system of two series subsystems.

In figure 27.b reliability can be calculated as:

$$R_S = P(\ [(T_1>t)\cup(T_2>t)]\cap[(T_3>t)\cup(T_4>t)\cup(T_5>t)]\ ) =$$

$$= P[(T_1>t)\cup(T_2>t)]\cdot P[(T_3>t)\cup(T_4>t)\cup(T_5>t)].$$

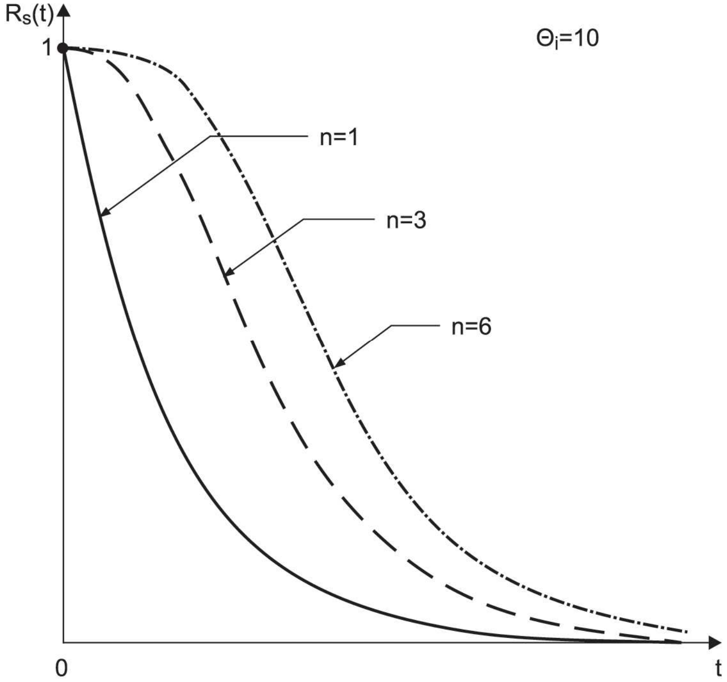


Figure 27. Identical element redundant parallel system reliability

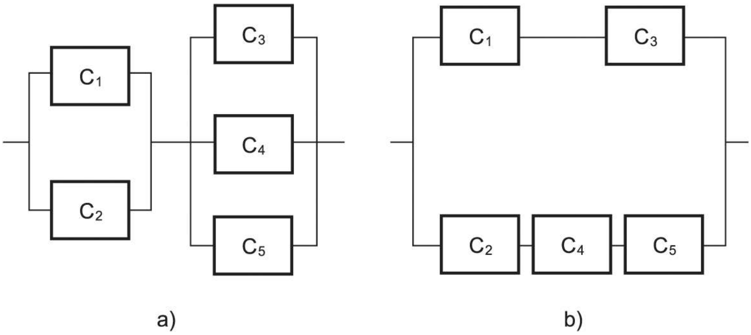


Figure 28. Series-parallel systems

That is, the product of the two parallel subsystems reliabilities, corresponding to the general series structure:

$$R_s = [1-(1-R_1)(1-R_2)]\cdot[1-(1-R_3)\cdot(1-R_4)\cdot(1-R_5)].$$

In figure 28.b:

$$R_s = P(\ [(T_1>t)\cap(T_3>t)]\cup[(T_2>t)\ \cap(T_4>t)\cap(T_5>t)]\ ) =$$
$$= [1-R_1R_3]\cdot[1-R_2R_4R_5],$$

$$1 - R_s = [1-R_1R_3]\cdot[1-R_2R_4R_5],$$

that is: system unreliability is the product of the two series subsystems reliabilities, as corresponds to the overall parallel structure.

7.5 NON SERIES-PARALLEL SYSTEMS

7.5.1 Delta-Star Transformation

Not all the systems can be fully decomposed in only series or parallel subsystems. This fact requires the use of different analysis techniques such as those presented in this chapter. But previously to the review of these methods, we will comment a useful transformation for some structures.

Systems with logic diagrams that have "delta" configurations may be transformed to logic diagrams containing "star" or "Y" configurations. Often it results in a simpler configuration that can be transformed in series/parallel structures.

To derive the equations for transforming a logical "delta" into a logical "star", we take a terminal or final perspective of the two diagrams, as indicated in Figure 29, so that the reliability between any two terminals of the delta configuration must be equal to the reliability between these same two terminals of the star configuration. Application of this principle leads to the equivalencies shown in Figure 30.

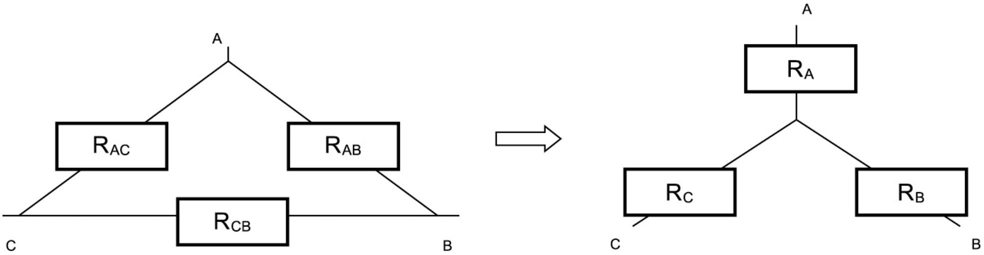


Figure 29. Delta-star transformation

Equating the reliabilities of each pair of diagrams in Figure 29 results in three equations that can then be solved for R_A, R_B, and R_C. The result is:

$$R_A = \sqrt{\frac{\left[1-(1-R_{AC})(1-R_{CB}R_{AB})\right]\left[1-(1-R_{CB})(1-R_{AC}R_{AB})\right]}{\left[1-(1-R_{AB})(1-R_{AC}R_{CB})\right]}}\,,$$

$$R_B = \sqrt{\frac{\left[1-(1-R_{AB})(1-R_{AC}R_{CB})\right]\left[1-(1-R_{CB})(1-R_{AC}R_{AB})\right]}{\left[1-(1-R_{AC})(1-R_{CB}R_{AB})\right]}}\,,$$

$$R_C = \sqrt{\frac{\left[1-(1-R_{AC})(1-R_{CB}R_{AB})\right]\left[1-(1-R_{AB})(1-R_{AC}R_{CB})\right]}{\left[1-(1-R_{CB})(1-R_{AC}R_{AB})\right]}}\,.$$

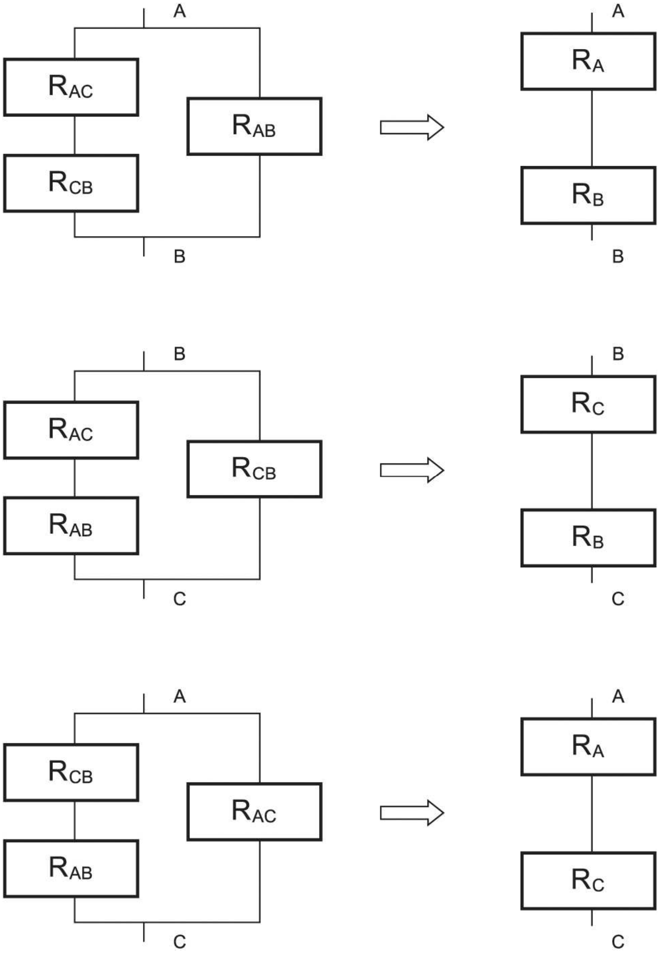


Figure 30. Delta-star equivalencies

7.5.2 General Systems

A general system is a system that can not be analysed with the previous methods. Figure 31 shows one of such systems.

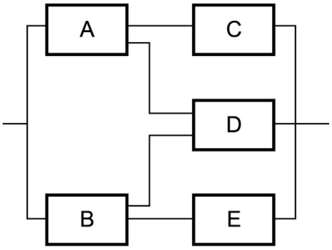


Figure 31. General system

For the analysis of general systems we have different methods or procedures that can allow us to deal with this, in general, complex structures. Again, as in the case of series/parallel systems, the problem is that all procedures are reiterative and boring, making in practice very easy the appearance of errors when manual analysis is performed. The use of software tools is highly recommended if exact reliability calculations are needed.

7.5.2.1 Decomposition

The decomposition approach is also called the conditional probability approach and the factoring algorithm. In this approach, we reduce the logic diagram sequentially into sub-structures that are connected in series/parallel and then recombine these substructures using conditional probability. We can apply this method to the diagram of Figure 32.

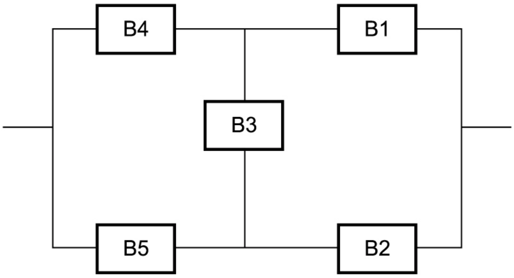


Figure 32. Example for decomposition method

The reliability block diagram of Figure 32 is frequently called bridge diagram and, as can be noted, can not be transformed is in series or parallel subsystems. The basic idea stems from the recognition that:

$$P(A) = P(A \cap B) + P(A \cap \overline{B}) = P(B)P(A \mid B) + P(\overline{B})P(A \mid \overline{B}).$$

Or, in terms of Figure 11:

$$P(S_S) = P(S_S \cap S_{B3}) + P(S_S \cap F_{B3}) = P(S_{B3})P(S_S \mid S_{B3}) + P(F_{B3})P(S_S \mid F_{B3}).$$

Where S_S is the system success, S_i is the i-element success and F_i the i-element failure. Denoting, as usual, R_S as the probability that the system works, we can write this as

$$R_S = R_S(\text{given B3 works})R_{B3} + R_S(\text{given B3 fails})F_{B3.}$$

The reliabilities of the system, given that B3 works, and given that B3 fails, can be observed from inspecting Figure 32, so that the system reliability is:

$$R_S = \{(1\text{-}F_{B4}F_{B5})(1\text{-}F_{B1}F_{B2})\}R_{B3}+\{1\text{-}(1\text{-}R_{B4}R_{B1})(1\text{-}R_{B5}R_{B2})\}F_{B3.}$$

7.5.2.2 Tieset Method

Tieset method consists in identifying the subsets of elements that guarantee the succes of the system itself if the elements of the subset succeed. A tieset is a set of elements that fullfil this requierement [1].

The nomenclature used refers a element by its name (i.e.: A or b…). More precisely, what we represent by A is the succes event for this element. A tieset is identified by the list of its elements names (i.e.: ACD), meaning that all the elements of the tieset succed in the mission. In the system of Figure 31, we have that ABC is a tieset, and also AC, ACD, BCD, and some others. The probability that a tieset succeeds is the product of its elements reliabilities:

$$P(ACD) = P(A)\cdot P(B)\cdot P(D) = R_A\cdot R_B\cdot R_{D.}$$

Assuming that the life of each element is independent form the others.

A special type of tieset is this where there is no extra element in the set (meaning that the set no longer causes a success if any one of the elements fails). These are called minimal tieset. In the system of Figure 31, the minimal tiesets are AC, AD, BE and BD.

When two tie sets are intersected the result is a new tieset that includes all the elements of the original tiesets. The intesection of AD and BD is therefore ABD. The probability of the new tieset can be computed as previously explained. In this example:

AD ∩ BD = ABD, P(AD ∩ BD) = P(ABD).

To calculate the system reliability, we have to calculate the probability of the union of all the minimal tiesets: the system will succeed if at least one of the minimal tiesets os open. If we call P_i to each of the minimal tiesets, we have:

$$R_s = P(P_1 \cup P_2 \cup \cdots \cup P_n) = \sum_{i=1}^{n} P(P_i) - \sum_{i \neq j}^{n} P\left(P_i \cap P_j\right) + \cdots +$$

$$+(-1)^{r+1} \sum_{i \neq j \neq \cdots \neq k} P\left(P_i \cap P_j \cap \cdot\cdot (r) \cdot\cdot \cap P_k\right) + \ldots + (-1)^{n-1} P(P_1 \cap P_2 \cap \ldots \cap P_n).$$

Applying this expression to the system of figure 10, we have that:

R_S = P(AC)+P(AD)+P(BD)+P(BE)-
-P(AC∩AD)-P(AC∩BD)-P(AC∩BE)-P(AD∩BD)-
-P(AD∩BE)-P(BD∩BE)+P(AC∩AD∩BD)+
+P(AC∩AD∩BE)+P(AD∩BD∩BE)+P(AC∩BD∩BE)-
-P(AC∩AD∩BD∩BE) =
= P(AC)+P(AD)+P(BD)+P(BE)-P(ACD)-P(ABCD)-P(ABCE)-
- P(ABD)-P(ABDE)-P(BDE)+P(ABCD)+P(ABCDE)+P(ABDE)
+P(ABCDE)-P(ABCDE) =
= P(AC)+P(AD)+P(BD)+P(BE)-P(ACD)-P(ABCE)-
-P(ABD)-P(BDE)+P(ABCDE).

And subtituting the probabilities by its expresión in function of the elements reliabilities:

$R_S = R_A \cdot (R_C + R_D) + R_B \cdot (R_D + R_E) - R_A \cdot R_C \cdot R_D - R_A \cdot R_B \cdot R_C \cdot R_E - R_A \cdot R_B \cdot R_D -$
$- R_B \cdot R_D \cdot R_E - R_A \cdot R_B \cdot R_C \cdot R_D \cdot R_{E.}$

Obviously, the use of this procedure can leads to a long, boring and easy to mistake process, if the system is only a little more complex than our example.

7.5.2.3 Cutset Method

This method is very similar to the tieset method, but instead of working with sets of elements that guarantee the success of the system, we identify and analyze here sets of elements that guarantee the failure of the entire system [1].

The nomenclature is also similar: We refer a element by its name (i.e.: A or b…). More precisely, what we represent by A is the failure event for this element. A cutset is identified by the list of its elements names (i.e.: ACD), meaning that all the elements of the cutset fail in the mission. In the system of figure 10, we have that AB is a cutset, and also CDE, ADE, ABCD, and some others. The probability that a cutset fails is the product of its elements unreliabilities:

$$P(ACD) = P(A)\cdot P(B)\cdot P(D) = (1-R_A)\cdot(1-R_B)\cdot(1-R_D).$$

Assuming that the life of each element is independent form the others.

We can define here a special type of cutest called minimal cutest: A minimal cutset C is a cutset where the set remaining after the removal of any of its elements is no longer a cutset. This definition means that all elements of a minimal cutset must be failed to cause system failure. In the system of Figure 31, the minimal cutsets are AB, ADE, BCD and CDE.

When two cutsets are intersected the result is a new cutset that includes all the elements of the original cutsets. The intesection of AB and BCD is therefore ABCD. The probability of the new cutset can be computed as previously explained. In this example:

$$AB \cap BCD = ABCD, P(AB \cap BCD) = P(ABCD).$$

To calculate the system unreliability, we have to calculate the probability of the union of all the minimal cutsets: the system will fail if at least one of the minimal cutsets appears. If we call C_i to each of the minimal cutsets, we have:

$$1-R_s = P(C_1 \cup C_2 \cup \cdots \cup C_n) = \sum_{i=1}^{n} P(C_i) - \sum_{i\neq j}^{n} P\left(C_i \cap C_j\right) + \cdots +$$

$$+ (-1)^{r+1} \sum_{i\neq j\neq \cdots \neq k} P\left(C_i \cap C_j \cap \cdot\cdot (r) \cdot\cdot \cap C_k\right) + \ldots + (-1)^{n-1} P(C_1 \cap C_2 \cap \ldots \cap C_n).$$

This expression can be developed in a similar manner that we did in the tieset method:

$$\begin{aligned}
R_S = {} & 1\text{-}P(AB)\text{-}P(CDE)\text{-}P(ADE)\text{-}P(BCD)+P(AB\cap CDE)+ \\
& + P(AB\cap ADE)+P(AB\cap BCD)+P(CDE\cap ADE)+P(CDE\cap BCD)+ \\
& + P(ADE\cap BCD)\text{-}P(AB\cap CDE\cap ADE)\text{-}P(AB\cap CDE\cap BCD)\text{-} \\
& \text{-}\ P(AB\cap ADE\cap BCD)\text{-}P(CDE\cap ADE\cap BCD)+ \\
& + P(AB\cap CDE\cap ADE\cap BCD) = \\
& = 1\text{-}P(AB)\text{-}P(CDE)\text{-}P(ADE)\text{-}P(BCD)+P(ABCDE)+P(ABDE)+ \\
& + P(ABCD)+P(ACDE)+P(BCDE)+P(ABCDE)\text{-}P(ABCDE)\text{-} \\
& \text{-}\ P(ABCDE)\text{-}P(ABCDE)\text{-}P(ABCDE)+P(ABCDE) = \\
& = 1\text{-}P(AB)\text{-}P(CDE)\text{-}P(ADE)\text{-}P(BCD)+P(ABDE)+P(ABCD)+ \\
& + P(ACDE)+P(BCDE)\text{-}P(ABCDE).
\end{aligned}$$

Than can be expressed using unreliabilities ($F_i = 1\text{-}R_i$) as:

$$\begin{aligned}
R_S = {} & 1\text{-}F_AF_B\text{-}F_CF_DF_E\text{-}F_AF_DF_E\text{-}F_BF_CF_D+F_AF_BF_DF_E+F_AF_BF_CF_D+ \\
& +F_AF_CF_DF_E+F_BF_CF_DF_E\text{-}F_AF_BF_CF_DF_E.
\end{aligned}$$

7.5.2.4 Partition Method

It consist in using a event tree analysis [23] approach to evaluate if each of the branches of the tree causes system success or failure.

The first step is to develop a tree with the different situation of the different elements of the system, in what refers to its success or failure. We should then identify which branches lead to the system success and which ones to the system failure. Some considerations should be kept in mind:

- at each node of the tree, two options have to be considered: the next element's success or failure.
- a branch of the tree is truncated if the events present in the branch imply the system failure or success.
- the order in which elements are considered is important only in the sense that it can simplify the tree, but the final result will be the same.

The second step is to associate to each segment of the tree the probability of its corresponding event. This probability will be equal to the element reliability (if the segment leads to a elements success) or the element unreliability (if the element fails).

Finally, the probability of each branch is computed multiplying the probabilities of all the segments of the branch, and then the system reliability is calculated as the sum of the probabilities of the branches leading to system success.

For the example system of Figure 31, two alternative trees have been developed (Figures 33 and 34).

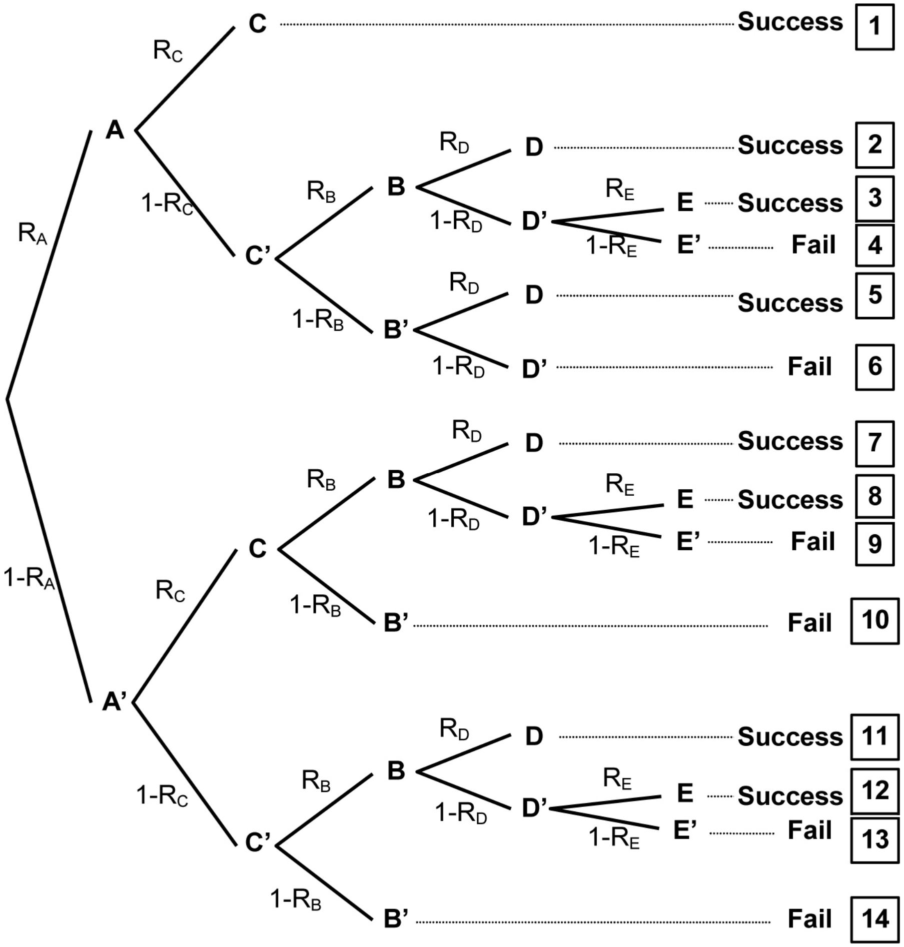


Figure 33. Partition method tree (a)

Using these trees, system reliability can be calculated as the sum of the probabilities of branches 1, 2, 3, 5, 7, 8, 11 and 12, resulting in:

$$\begin{aligned}R_s = {} & R_A \cdot R_C + R_A \cdot (1-R_C) \cdot R_B \cdot R_D + R_A \cdot (1-R_C) \cdot R_B \cdot (1-R_D) \cdot R_E + \\ & + R_A \cdot (1-R_C) \cdot (1-R_B) \cdot R_D + (1-R_A) \cdot R_C \cdot R_B \cdot R_D + \\ & + (1-R_A) \cdot R_C \cdot R_B \cdot (1-R_D) \cdot R_E + 1-R_A) \cdot (1-R_C) \cdot R_B \cdot R_D + \\ & + (1-R_A) \cdot (1-R_C) \cdot R_B \cdot (1-R_D) \cdot R_{E,}\end{aligned}$$

that can be simplified:

$$\begin{aligned}R_s = {} & R_A \cdot R_C + R_A \cdot (1-R_C) \cdot [R_D + R_B \cdot (1-R_D) \cdot R_E] + \\ & + (1-R_A) \cdot R_B \cdot [R_D + (1-R_D) \cdot R_E].\end{aligned}$$

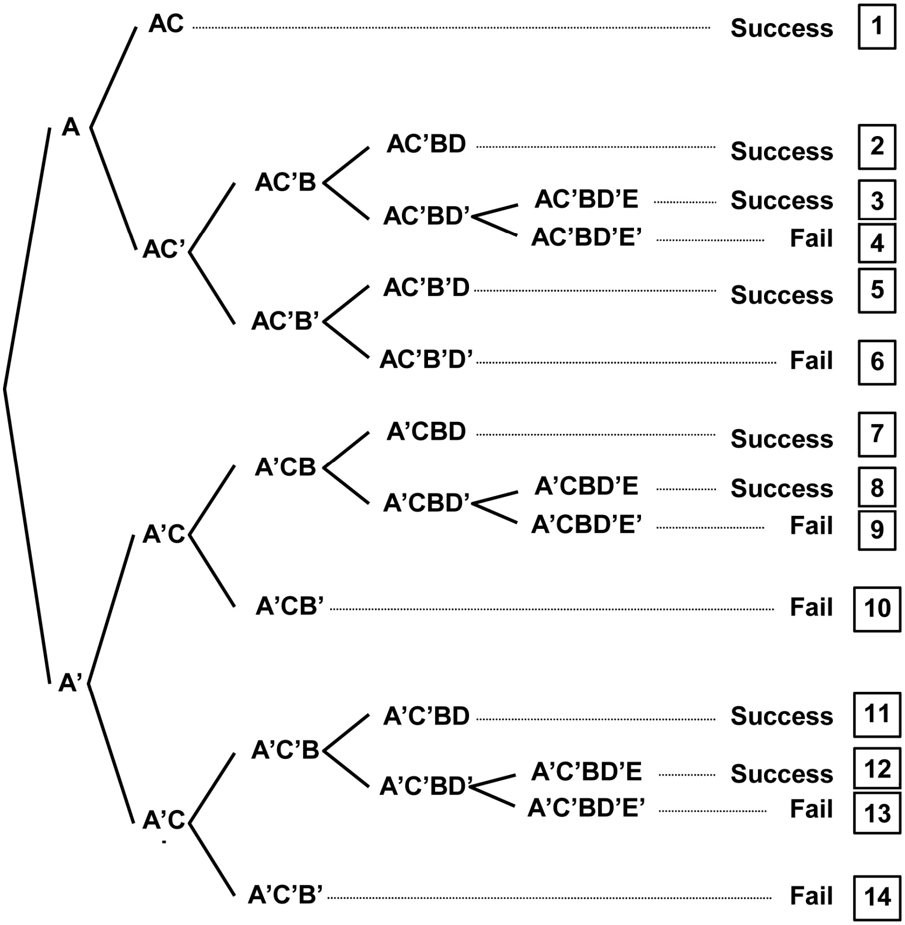


Figure 34. Partition method tree (b)

Alternatively, the unreliability can be calculated as the sum of the probabilities of of branches 4, 6, 9, 10, 13 and 14:

$$\begin{aligned}1-R_s = {} & R_A\cdot(1-R_C)\cdot R_B\cdot(1-R_D)\cdot(1-R_E)+R_A\cdot(1-R_C)\cdot(1-R_B)(1-R_D)+\\ & + (1-R_A)\cdot R_C\cdot R_B\cdot(1-R_D)\cdot(1-R_E)+(1-R_A)\cdot R_C\cdot(1-R_B)+\\ & + (1-R_A)\cdot(1-R_C)\cdot R_B\cdot(1-R_D)\cdot(1-R_E)+\\ & + (1-R_A)\cdot(1-R_C)\cdot(1-R_B),\end{aligned}$$

that can be also simplified:

$$1-R_s = R_A\cdot(1-R_C)\cdot(1-R_D)\cdot[1-R_B\cdot R_E]+(1-R_A)\cdot[1-R_B\cdot R_E- R_B\cdot R_D\cdot(1-R_E)].$$

Reliability block diagram shows graphical logical connection of elements that build a certain system. The basic schemes of logical elements' connection are series and parallel. More complex structural schemes of systems could be created from them, such as series-parallel and non series-parallel ones. While designing some Reliability block diagram should be known that series or parallel physical structure does not automatically means the same logical connection in relation to reliability. Reliability block diagram is very good basic method for reliability system analysis. This chapter shows the method for calculation of system reliability on basis of the Reliability block diagram.

Chapter 8

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS

8.1 INTRODUCTION

Manufacturing management today is surrounded by a number of concepts, which it is argued will enable managers to carry out more effectively and efficiently the function of controlling the manufacturing operation. This in turn will lead to higher profits for the organisation as a whole. As the pressure from foreign and domestic competitors increases, these individual manufacturing concepts have had to be integrated. One of these concepts is called Total Quality Management (TQM). One of the tools within TQM system is the so called Failure Mode and Effects Analysis (FMEA) [24]. This is one of the tools that can be used to reduce the costs of quality (Table 17).

The FMEA technique evaluates the potential failure of a system or process and its effects, identifies what actions could be taken to eliminate or minimise the failure from occurring and documents the whole procedure. It is used from the initial planning stages of designing and processing a system through to the end of its life.

The reason for undertaking an FMEA is to continually improve systems, processes, reliability and to reduce warranty thereby increasing customer satisfaction. FMEA along with other quality tools support the practice and philosophy of problem prevention and continuous improvement which are key elements of Total Quality Management.

Table 7. Quality cost structure

QUALITY COST			
Cost of quality assurance		Cost of defects	
Cost of prevention defects	Cost of control	Internal cost	External cost
. Planning of quality assurance	. Input control	. Defect	. Service
. Planning of control	. Control process	. Additional work	. Negative reputation on account of defective system
. Development of control strategy	. Acceptance control	. Over time work	. Drop of price
. Education of staff for quality assurance	. Control equipment	. Additional control	. Responsibility for system

The FMEA technique was first reported in the 1920′s [26] but its use has only been significantly documented since the early 1960′s. It was developed in the United States of America in the 1960′s [27] by North American Space Agency (NASA) as a means of addressing a way to improve the reliability of military equipment. During that decade the technique was used in the aerospace, nuclear and electronic industries. It has been used in the automotive industry since the early 1970′s. Its use was accelerated in the 1990′s to address the major reliability and quality challenge presented by the Japanese car manufacturers whose increasing penetration and rising reputation had led to their present market share of 10,7% in Europe and 12% in North America [28].

To illustrate the efficiency of such a preventive FMEA approach, the so-called **ten times system cost increase** rule is cited. This rule states that the cost of removing a defect from a system phase is equivalent to ten times the cost of actually preventing it from occurring (Figure 34). This fact was ascertained in the 1960′s, during the reliability assurance system drive by the USA military. In reference [28] emphasised that the cost of removing of unreliable equipment being used were ten times those foreseen for the reliability assurance during project planning.

The simple **ten times system cost increase** rule points to the efficiency of early discovery (and hence avoidence) of potential defects and failures. In this situation, it is very important to have available methods which can make possible identification of potential defects (failures) of systems, and to be able to resolve these failures (Table 8) [29]. The FMEA is a methodology which is now commonly used to tackle the stated problem.

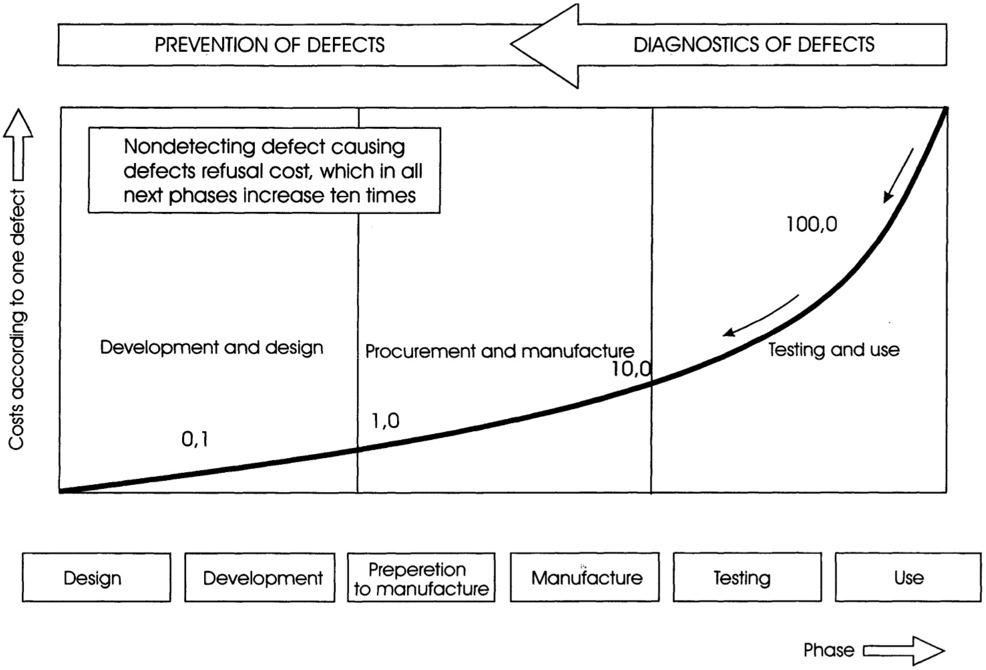


Figure 34. Principle ten times system cost increase

According to IEV [30] the failure criticality represents a group of characteristic which characterise the failure effects. Classification of failures according to their critical degrees should help in separating the failures (and in removing their reasons), which could seriously effect life, health and environment of people. These failures are called catastrophic ones and they must be found out during project planning and removed according to priority. This criticality issue has evolved its own terminology, Failure Modes, Effects and Criticality Analysis (FMECA), and is now considered to be the parent of FMEA.

Table 8. Statistical methods of quality management in development process of new system

PHASE	Phase of development				Phase of production	
	Planning		Basic project	Prototype. Typical project	Production and marketing	Production and sale
BASIC METHOD	Quality function deployment (QFD)	Planning of quality deployment (affinity diagrams)	QFD for subsystems	QFD for elements	Control chart analysis Capability studies	Control program Technological chart Manual of exploitation and maintenance Sample statistical control
	Reliability management	Demands and reliabilty prognosis of structure elements Testings for reliability estimation / simulation FMEA / FMECA FTA Development of systems: maintenance, overhauling and diagnosis				Reliability analysis on the basis of distributions: Weibull, Gumbel, Gauss, etc. Censored sample analysis
	Quality technology	Regression analysis of experimental data	Parameters plannig and experiment planning (Taguchi)		ANOVA (multifactoral)	
		Loss function	Tolerance planning (Taguchi)		Regression analysis	
	Statistical analysis Classical methods (hard computing)	Multifactoral regression. Sensitivity analysis			Simulation modelling	
		Seven simple methods of statistical quality control: Check sheets, Pareto diagrams, Ishikawa diagrams, histograms, scatter diagrams, stratification data, control charts				
		Seven new methods of quality management: Affinity diagrams, interrelationship diagraphs, tree diagrams, matrix diagrams, matrix data analysis, process decision program charts, PERT system.				

8.2 IMPLEMENTING THE FMECA METHOD

There are six key stages to implementing the FMECA methodology. However, the six key stages assume that the soft issues of implementation (such as management commitments, communication, training, availability of resources, knowledge of FMECA methodology) are already in place.

With this assumption in mind, the six key stages of FMECA can now be stated, as below:

- formulation and analysis of the structure functional block diagram system,
- analysis for exploitation of the system conditions,
- reciprocal effects analysis of the system parts (units of equipment),
- analysis of failure mechanism parts, failure criterions and failure modes,
- classification of potential failure effects,
- analysis of potential methods (ways) for failure prevention.

As mentioned earlier, and according to the International Standards IEC series 812, FMECA covers two procedures [31]:

a) FMEA,

b) Failure Criticality Analysis (estimation) (CA).

Each of these two procedures will be discussed in the following sections.

8.3 THE FMEA METHOD

The FMEA method can be used for system, product or process analysis. In each case, the FMEA help select optimum system alternatives and establishes whether reliability targets can be supported. It identifies systematic interactions within the concept and is the basis for developing diagnostics procedures, fault management techniques and determines changes required to overcome the potential failures.

The matrix form is the most convenient for implementing the FMEA method into effect, as suggested in [32]. An example of the matrix FMEA form is shown in Tables 9 and 10, and Figures 35 and 36. This example shows the application of the FMEA method to an flexible manufacturing line (FML) process buffer stocks. Figure 35 shows the structural block diagram of a buffer stock system module (inter-operational stocks) which consists of five sub-modules (1441, 1442, 1443, 1444 and 1445). Two of these sub-modules have corresponding sub-modules (in this case equipment) which directly impact it. Thus sub-module 1441 (charging of buffer stock) consists of the following parts: 14411, 1412, 14413 and 14414. This is also the case for sub-module 1444.

Table 9. FMEA table form of FML buffer stock

FMEA OF SYSTEM					Module: FML BUFFER STOCK	Code: 144	
Item	Code of item	Part	Code of part	Quan-tity	Failure mode	Code of failure mode	End effect
Charging of buffer stock	1441	Hydraulic cylinder	14411	1	. Wear of working surface of cylinder . Wear of plunger . Wear of piston ring and plunger axle . Jamming plunger in cylinder	FM1 FM2 FM3 FM4	E3 E3 E3 E2
		Limit switch	14412	2	. Loosening of cable connection . Burn of contacts . Wear of driving parts . Loosening fixing parts . Jamming or fracture of spring	FM5 FM6 FM7 FM8 FM9	E3 E3 E3 E3 E2
		Holddown of product	14413	1	. Loosening of connection of accepting surface . Jamming of torsion springs	FM10 FM11	E3 E2
		Guide	14414	2	. Jamming of guide	FM12	E2
Buffer stock of FML	144	Limit switch for addition of storingshed	1442	1	. Loosening of cable connection . Burn of contacts . Wear of driving parts . Loosening fixing parts . Jamming or fracture of spring	FM5 FM6 FM7 FM8 FM9	E3 E3 E3 E3 E2
		Storingshed	1443	1	. Loosening of adjustable frame of storing-shed	FM13	E3
Product refter to inclined plane	1444	Hydraulic cylinder	14441	1	. Wear of working surface of cylind. . Wear of plunger . Wear of piston ring and plunger axle . Jamming plunger in cylinder	FM1 FM2 FM3 FM4	E3 E3 E3 E3
		Multi-grouser shoe	14442	1	. Loosening of connection of shoe	FM14	E3
		Fixed shoe	14443	1	. Loosening of connection of shoe	FM14	E3
		Axle	14444	1	. Warping of axle	FM15	E3
Bufer stock of FML	1444	Inclined plane	1445	1	. Loosening of fixed and adjustable frame	FM16	E3

Table 10. End effects of FML failure modes

Description of effect	Mark
Possibility for imperial safety of operator	E1
Momentary breakdown of system	E2
Breakdown of system after some time	E3
Product out of tolerance without possibility additionaly work	E4
Product out of tolerance with possibility additionaly work	E5
Crossing operating time	E6
Loss possibility functional control of system	E7
Loss possibility dimensional control of product	E8
Dificult control of system	E9

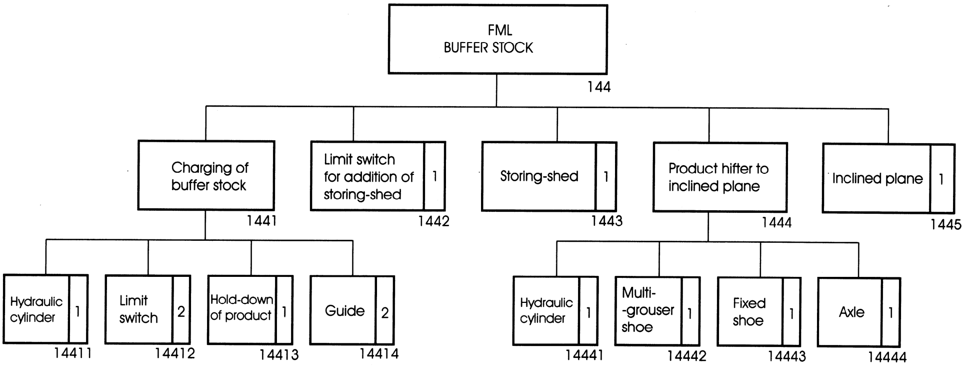


Figure 35. Structural block diagram of FML buffer stock

The FMEA method is applied through an inductive procedure. Thus the failure modes of sub-module 1441 are to be identified through the corresponding failures of its own sub-mo-dules 14411 to 14414. The details of this analysis are shown in Tables 9 and 10. Figure 36 shows the combined analysis for both the sub-modules 1441 and 1444 at the first level of FMEA, leading onto the second level of FMEA for module 1444.

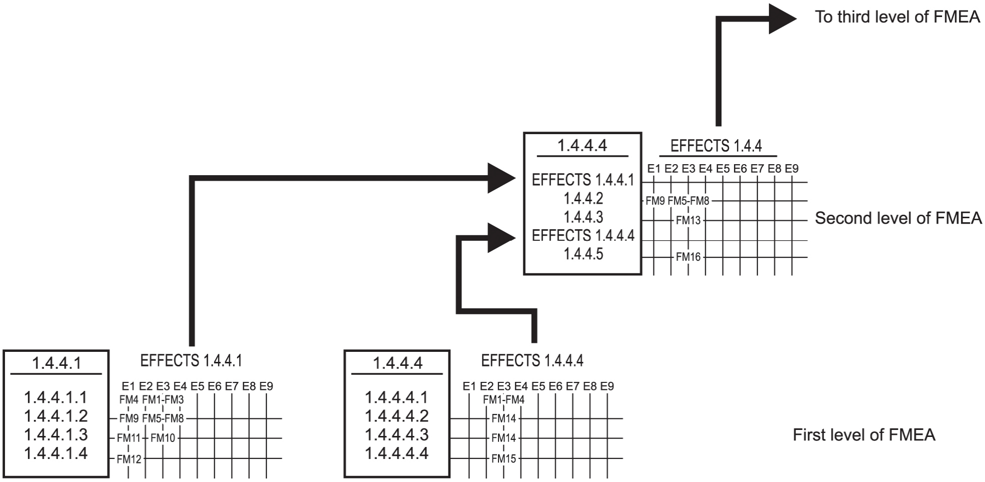


Figure 36. FMEA matrix form of FML buffer stock

The parts failure effects are classified, in accordance with their effects to higher structural level units, as follows:

- Local failures: These do not result in failures at higher level modules,
- Intermediate failures: These will result in failures at higher level modules,
- Final failures: These will cause the complete system failure (irrespective of which level they occur at).

A further classification of these failures can be determined, based on their final effects (rather than the effects to higher structural level):

- Category I - Catastrophic failure
- Category II - Important failure (but does not cause difficulty in carrying out the system function).
- Category III - Intermediate failure (a marginal failure which inflicts some economic losses).
- Category IV - Insignificant failure (excluded from the three categories above).

The Matrix FMEA form enables visualisation of the whole analysis process. The complete procedure needs to be fully documented and kept for later analysis and action (and possible future quality audits).

It is also recommended to complement the FMEA method with a frequency analysis, which considers, in aqualitative form, the potential frequency (probability) of failure occurrence. Table 11 illustrates BS 5760 recommended matrix estimation frequency classification and importance of a failure according to the categories from I to IV [33]. Failure causes which belong to A group must be removed absolutely, so that construction of the project must be changed in designing process, increasing appropriate reserves of strength, stability, softening exploitation conditions of the system. Failure causes from groups B and C should be further analysed, that is, the failure mechanisms, degrading processes characters and other factors important for fuller description of failures, should be determined. The following decisions could be reached: to modernise the system, to change maintenance and repair policies, to increase frequency and depth, do diagnosis and do other corrections. Failures for groups B and C are added in the special data base to be further analysed and tested. Additional analysis for failure causes from D group is unnecessary.

Table 11. Failure criticality matrix

Expected Frequency of failure appearance	Weight (importance) of failure, category			
	I	II	III	IV
Often	A	A	A	C
Probably	A	A	B	C
Seldom	A	B	B	D
Very seldom	A	B	B	D
Improbably	B	C	C	D

In work [34] some quantitative evaluations of failure appearing frequency are recommended (first of all, for the motor parts), and they are shown in Table 12. It is evident that this classification requires more precise analysis for other dangerous systems.

Table 12. Levels of failures appearance probability

Expected frequency of failure appearance	Probability of failure appearance P
Often	P > 0,2
Probably	0,1 < P < 0,2
Seldom	0,01 < P < 0,1
Very seldom	0,001 < P < 0,01
Improbably	P < 0,001

8.4 FAILURE CRITICALITY ANALYSIS METHOD

For the second phase of analysis, a quantitative estimation of failure criticality is needed. Lately, several basic methods have been recommended for criticality estimation. They are established in accordance with suitable national standards, for example, in the Automobile Association of Germany Standards VDA [35], in USA Military Standards MIL-STD-1629A [27] and in British Standards BS 5750: Part 5 [33].

The purpose of the construction FMECA type is to separate the most important potential failures in relation to their frequencies of appearances, defining of possible procedures to prevent their appearing in implementation and defining difficulties of the failure effects [36]. Separation of the most important failures is carried out with comparison of criticality ith failure C_i with some maximal value C_{cr}. If $C_i>C_{er}$, then the ith failure will be considered important (critical) one and must be eliminated. If $C_o<C_i<C_{er}$, then corrections are necessary in order to minimise criticality, for example, change of the maintenance and repair policies. These failures are to be added in an appropriate database to be further analysed and tested. Failures with $C_i<C_o$ are null and void and development of additional measures is unnecesary. It should be emphasised that the criticality evaluation procedure (given below) makes it possible for a plan of corrective measures to be worked out, around the scheme contained on Figure 37. This criticality evaluation (C) procedure is:

$$C = B_1 \cdot B_2 \cdot B_3 \qquad (1)$$

where,

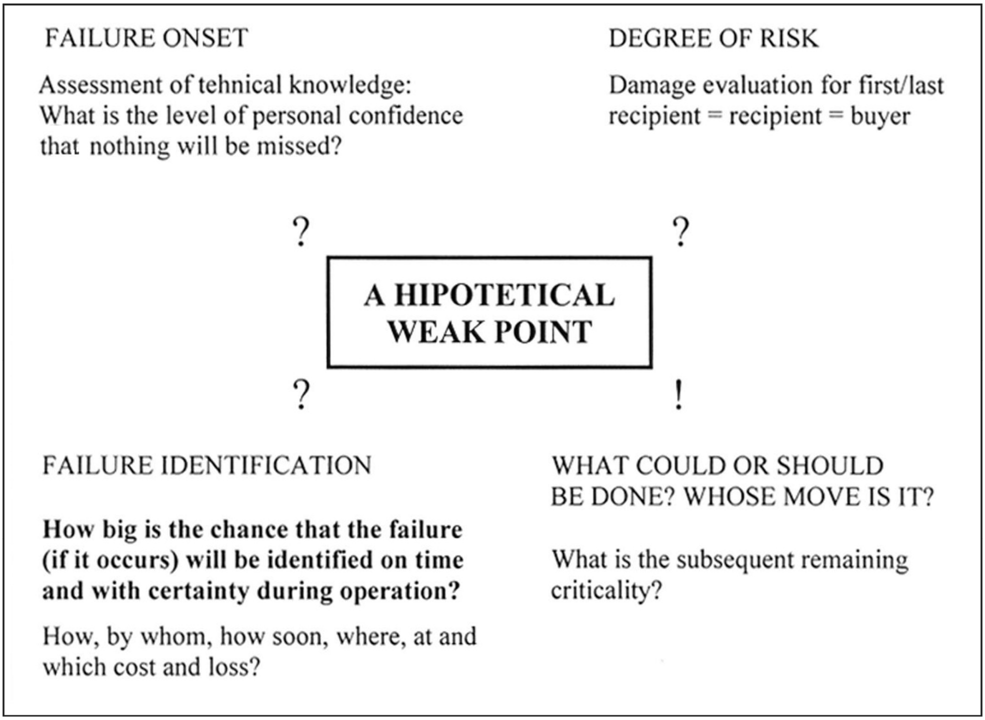
B_1 is the estimation of frequency

B_2 is the estimation of failure discovering probability (prior to implementation).

B_3 is the estimation of difficulty of the failure effects.

The B_i (i=1,2,3) factor estimation, which directly effects criticality, directs the project engineer to ascertain appropriate corrections in order to reduce the criticality. In a number of studies on FMECA methods [37,38,39], it is accepted that $1<B_i<10$ (i=1,2,3) and that a recommended value of $C_{cr}=125$ be taken.

The purpose of the process FMECA is to separate those technological process - operations which have the greatest effect on the system reliability. The principle of importance estimation for the process FMECA is as the same for the construction FMECA. The process FMECA procedure has been described detail in [40]. Likewise, the purpose of the system FMECA is to separate these subsystems, modules or parts of the manufacturing system which have the most effect if a critical failure was to occur. Real examples of systems FMECA applications are cited in reference [411].



FAILURE ONSET

Assessment of tehnical knowledge: What is the level of personal confidence that nothing will be missed?

DEGREE OF RISK

Damage evaluation for first/last recipient = recipient = buyer

FAILURE IDENTIFICATION

How big is the chance that the failure (if it occurs) will be identified on time and with certainty during operation?

How, by whom, how soon, where, at and which cost and loss?

WHAT COULD OR SHOULD BE DONE? WHOSE MOVE IS IT?

What is the subsequent remaining criticality?

Figure 37. Aspects of criticality degree estimamtion

In USA militar standard MIL-STD-1629a [27], it is recommended that the estimation of criticality of ith failure mode of ith part (for pth category) be given by the following:

$$C_{ijp} = \alpha_{ij} \cdot \beta_{ijp} \cdot \lambda_i t_i \qquad (2)$$

where,

α_{ijp} - relative difficulty of the jth failure mode of the ith part,

β_{ijp} - conditional probability that the jth failure mode of the ith part will provoke the pth category of effects (p = I, II, III, IV),

λ_i - failure rate of the ith part,

t_i - operating time of the ith part,

n - quantity failure mode of the part.

In addition, the total criticality of the ith part, according to the pth category of effects is equal to:

$$C_{ip} = \sum_{j=1}^{h} C_{ijp} = \sum_{j=1}^{h} \alpha_{ij} \beta_{ijp} \lambda_i t_i \qquad (3)$$

The values of β_{ijp} are to be calculated or determined from appropriate tables given in standard handbooks.

When a typical FMECA procedure is carried out, it is not possible to carry out a complete analysis on every possible failure mode. Only the failure modes with critical (severe) effects are to be analysed and resolved. To illustrate this point, it has been established that on a manufactured motor vehicle there are approximately 12000 different failure modes. For a motor vehicle engine there are approximately 5000 and for a simple switch there are approximately 250 modes [35].

8.5 FMECA TEAM

The FMECA procedure is usually carried out as part of the TQM system. It is now well established that most TQM implementations need to be team based and certainly the FMECA procedure is no different in this context. A special FMEA team needs to be formed consisting of multi-skilled and multi-functional team members. The task of the team is to raise the efficiency of the project and speed the transition of the FMECA to actual manufacturing of the test samples. Such an FMECA team would correspond to Demings [42] ideas about removing the inter-determental barriers amongst the organisation′s functions resulting in the achievement of high quality and reliability.

The FMECA procedure directly influences quality and reliability by removing potential failures of high-degree criticality factors. It is also shown that the FMECA procedure is a simple methodology which allows specialists to participate in a multi-disciplined team to analyse the problem in hand. This team based approach allows the FMECA procedure to be extremely effective in resolving failure mode problems. This is most noticeable for catastrophic failures. The results of the proper application of FMECA procedures is avoidance of poor (negative) quality, which in itself leads to reduced costs (internally) and satisfied customers (externally).

Chapter 9

FAULT TREE ANALYSIS

9.1 INTRODUCTION

Fault Tree Analysis (FTA) was developed in Bell Telephone Laboratories in 1961 as a method for assessment of safety system for launching intercontinental rocket Minuteman. The method was improved and suitable software was developed in the company Boeing. Recently, fault tree analysis has been most often use method for estimation of safety and reliability. Fault tree is a logic diagram which shows connection between a potential unwanted event (critical failure mode, accident) on the system level and the cause of that event. These causes might be: equipment failure, environment conditions and human error. Depending on the aims of analysis there are two possible approaches to the fault tree analysis: qualitative and quantitative. Possible result of the qualitative analysis is a list of combinations: environment factors, human errors, and element failure, which may be caused by unwanted events in the system. Suitable quantitative analysis enables possible estimation of probability of unwanted event which might occur during certain period of time while the system is on/in operation.

Use of Failures Modes and Effects Analysis (FMEA) [24] in safety engineering of systems, although it may be time and cost demanding, does not include other possible problems apart from equipment failure, such as human errors. Element failure with many systems may cause interruption of system operation but not the disturbance of safety.

In some situations it is necessary to have the method of analysis which is focused on possible occurrence of one event which shows the complex relation of the cause of that event which includes all influential factors, but does not take into account outside measures. Due to these reasons, Bell Telephone Laboratories according to the request of U.S. Air Force has developed Fault Tree Analysis (FTA) [43].

In U.S. Air Force wanted to know the possibilities and probability of thoughtless and unauthorized launching of the rocket Minuteman and thoughtless and unauthorized handling of nuclear plant.

Although the fault tree analysis was developed to determine relativity quantitatively, it is much more used in a qualitative way because different factors can be presented in a systematic way which may be researched in any situation. Quantitative analysis and results are favorable in many changes, but to apply quantitative analysis, you need to do qualitative analysis first. However, many analytics of reliability think that obtaining quantitative results is not worth additional efforts.

9.2 DEDUCTIVE APPROACH

There are two approaches which can be used in analysis of casual connections between element failure and system failure. These are inductive and deductive analyses. Inductive analysis starts with the set of states in the Down Time of elements, and the procedure is carried out by identification (determining) of possible consequences, that is by the approach "what will happen if". Fault tree analysis presents an example of deductive analysis [44] (Figure 38), i.e. approach "what may cause this". This analysis is used for identification of casual connections which lead to certain types of system failure modes (Figure 39).

Fault tree presents a method which is used to express a concrete type of system failure over some types of element failure and operator's acting. The type of system failure which is considered is called "top event", while the fault tree which is still developing presents events which have caused it. Thus, the events presented (described) in the tree are defined down to the lowest/bottom events. This tree development procedure is over when we come to the types of element failures, marked as basic events. Fault tree analysis includes collecting data about basic events occurrence possibility.

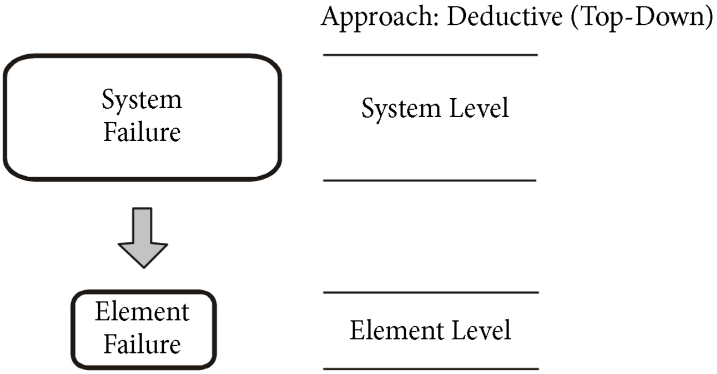


Figure 38. Deductive approach in the failure analysis

Top event is event whose possibility (or probability) of occurrence is to be determined. The choice of top event is the first step in this procedure. It is important that top event and system boundaries have been chose taking into account that analysis should not be too complicated or too poor for providing requested results.

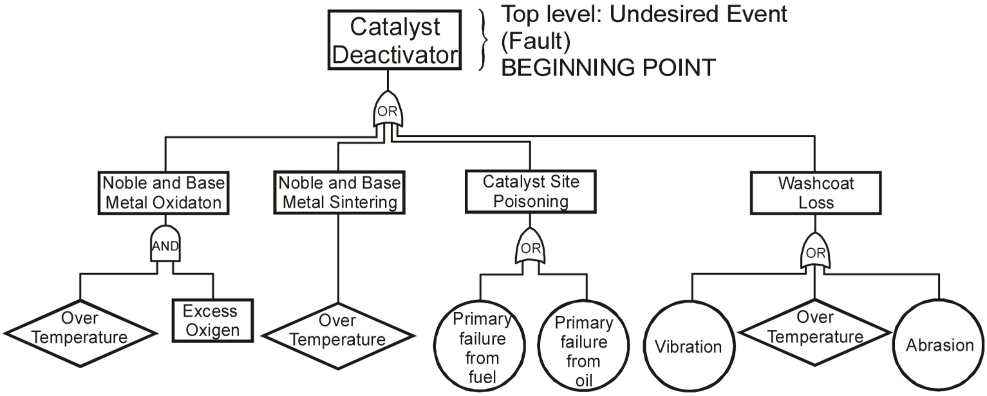


Figure 39. Fault tree example: Beginning point

Each fault tree considers one of many possible types of system failures, which means that during estimation/assessment of any system more than one fault tree may be constructed. For example, when the safety of system protection is evaluated, top event mostly refers to system protection failure when there is a request for carrying out demanded task. This top event leads to fault tree development up to the modeling of the cause of this situation. It is possible to take different levels of redundancy and changes of shape of safety protection system so that probability of their failure in the required moment is very little.

9.3 FMECA AND FTA

Failure Modes, Effects and Criticality Analysis is in connection with Fault Tree Analysis. The first method began popular with reliability engineers [45]. Both these methods are logically very similar although, generaly speaking, they look very different. Some reliability analysts debate weather is it better to performe analysis from the top or from the bottom (Figure 40). In practice it is the most appropriate to use the both ways simultaniously, which means that FTA and FMECA are logically equivalent methods [46].

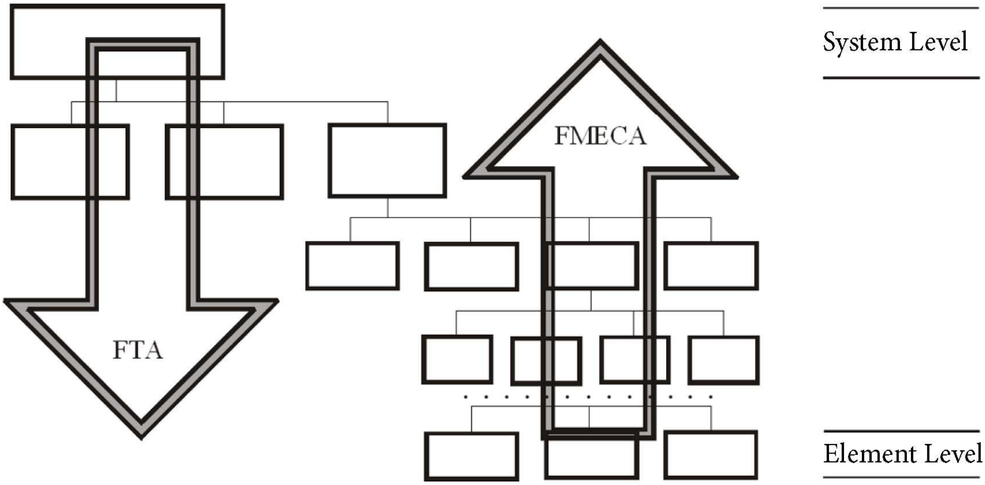


Figure 40. Top-Down and Bottom-Up approaches (ways) in the failure analysis

Fault Tree Analysis is not universal method for all types of system, even not for systems such as simple house hold machines. The development and application of fault tree demands days, and sometimes even weeks. For more complex systems, such as aircrafts, the fault tree generating demands years, which does not exclude the possibility of error occurrence.

9.4 FAULT TREE CONSTRUCTION

9.4.1 Fault Tree Methodology

Fault tree analysis uses deductive approach to show strengths and weaknesses of designing. That is "Top-Down" approach, contrary to "Bottom-Up" approach at Failure, Modes, Effects and Critically Analysis. Accordingly, it is started from the top event and it goes from top to bottom determining different paths where modes of fault may cause occurrence of real top event.

Standard procedure of fault tree analysis includes the following steps [47,48]:

1. System defining, its aim functions, base and rules and all suppositions for usage in real analysis.

2. Development of dimple block diagrams (hierarchical and functional block diagrams, reliability block diagrams) of the system, which shows inputs, outputs, links.

3. Defining a problem and condition boundaries (description of a problem, i.e. unwanted top event and defining positions of system boundaries).

4. Defining of real influential top event (system failure mode, as a final effect of element failure mode).

5. Construction of fault tree for the top event, up to the highest degree of giving details? , by using the rules of logic.

6. Qualitative analysis application (determining of minimal cut sets).

7. Collecting of basic data, such as failure rate, mean time between failure or possibility of element failure modes.

8. Quantitative analysis application (determining of probability of occurrence of top event).

9. Control of completed fault tree.

10. Giving recommendations for all actions in the phase of using and maintenance or change in the phase of system design.

11. Proving documents of the real fault tree analysis and obtained results.

9.4.2 Fault Tree Symbols

The notion of fault tree became in connection with analysis of system reliability. The aim of forming the fault tree is a symbolic presentation of the sequence of condition appearing which cause failure mode, critical (unwanted) event for the functioning of the system as a whole. Fault Tree Methodology is very closely connected with more general Event Tree Analysis (ETA) [49], where failure system modes are not only intermediary and final. To apply fault tree and event tree methodology it is important to know functional connections/links of system wholes in the way of logic scheme, taking into account interconnection of element and whole failure modes. Methodological base for these approaches is provided by theory of graphs, mathematical logic and theory of relativity.

The scheme of the fault tree includes two basic types of symbols, gates and events. Gates either allow or prevent passing of logic failure mode towards the tree and show the link between the ‘real’ events needed for occurrence of top event. On the top of fault tree there is a top event – a complete failure system [44,48].

The following example shows how to use real symbols [48]. A simple fault tree of light installation is shown in the Figure 41. In this case "passing" of any kind of failure mode through OR gate will cause the occurrence of top event.

Basic events shown in the shape of a circle, present the end of real fault tree analysis. If we want to do the quantitative analysis of these events, data are needed. Thus, there is no need to develop fault tree branches so far from the place of event as the data are not available.

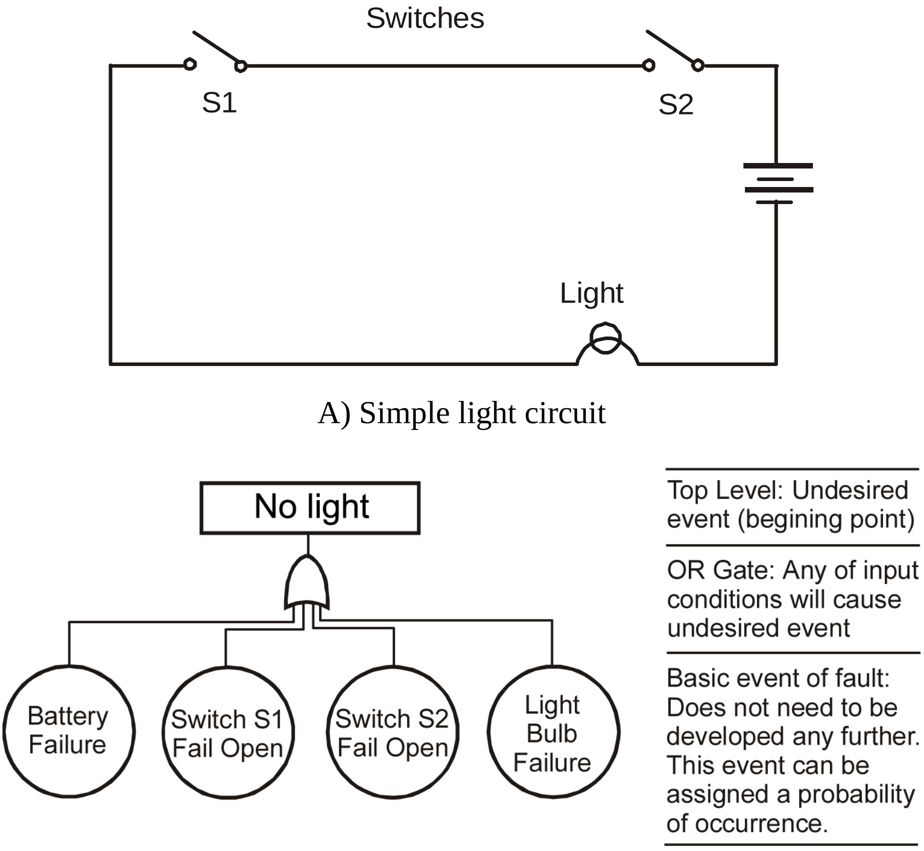
Symbols which are used for description of casual connections are gates and events are shown in the Figure 42.

9.4.3 Defining a Problem and Position of System Boundaries

Starting activities in the fault tree analysis relate to clearly identify the following two sub steps:

1. description of a problem, i.e. unwanted top event and
2. defining of system boundaries position.

Real unwanted (critical) event which is going to be analyzed is usually called top event. It is very important to define clearly the top event. It is not the case; the real analysis will be of limited value. For example, description of a real event "Fire in a factory" is too general and undefined. Correct description of a top event should always give the answers to the questions; WHAT, WHERE and WHEN [47]:


Switches
S1
S2
Light
No light
Battery Failure
Switch S1 Fail Open
Switch S2 Fail Open
Light Bulb Failure
Top Level: Undesired event (begining point)
OR Gate: Any of input conditions will cause undesired event
Basic event of fault: Does not need to be developed any further. This event can be assigned a probability of occurrence.

A) Simple light circuit

B) Fault tree of a simple light circuit

Figure 41. Simple Fault tree example

WHAT: Describes which type of unwanted event occurs (for example: fire);

WHERE: Describes where the unwanted event occurs (for example: during the process of oxidation in a reactor);

WHEN: Describes when the unwanted event occurs (for example: during normal/usual work).

Accordingly, more precise description of a top event is: "Fire in the process of oxidation during usual work".

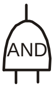
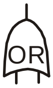
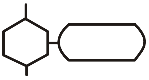
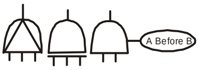
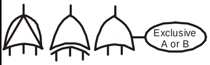
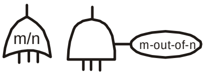
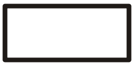
Symbol	Name	Description
Two common logic symbols		
	AND gate	Provides an output event only if all the input events occur
	OR gate	Provides an output event if one or more of the input events are present
Other logic symbols		
	Inhibit gate	This is used with a conditional event. Input produces output directly only when the conditional input is satisfied
	Priority (ordered) AND gate	This requires that the input events follow a specific "order of occurrence" in order for the output event to occur
	Exclusive OR gate	In order for the output event to occur, only one of the input events would have to occur. The output event will not occur if more than one input event occurs
	Sampling gate	This requires thath at least m of the n possible input events occur (where m≤n-1) for the output event to occur
Event symbols		
	Rectangle	An event or a fault that results from the combination of more basic faults and that can be developed further

Figure 42. Symbols used in Fault tree analysis

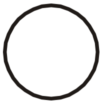
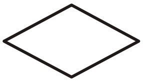
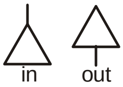
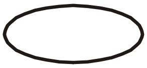
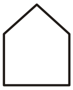
Symbol	Name	Description
Event symbols		
	Circle	A basic event of a fault that does not need to be developed any further. This type of event is independent of other events and indicates termination at that point. This event can be assigned a probability of occurence
	Diamond	An undeveloped event or fault; an event that is not developed further either because further development is of insufficient censequence of because the necessary information is unavailable
	Triangle	Used as a transfer symbol to move or connect information from one part or page of the fault tree to another when constructing a lengthly or complex fault tree
	Oval	A conditional event. This usually functions in combination with a logic gate, generally an Inhibit gate
	House	Input events that are not themselves faults that are expected to cause the output event to occur

Figure 42. Symbols used in Fault tree analysis (continuation)

Determination of system boundaries is important for the success of analysis [44]. Many systems have the outside supply of electricity and, maybe, water supply. It seems that it is not efficient to include all possible cases of failure in the electricity supply, backwards through the systems of production and distribution. It also seems that with these additional details do not provide any useful information regarding system estimation.

Position of the outside boundaries will be partly chosen taking into consideration the system function/operation. In case when the phone bell is not loud enough to attract the attention in all parts of a house, then the outside boundaries will be placed closer the phone. If the problem includes the noise on the line when the phone is in function, outside boundaries will be much farther so that they can include lines in the house, and even the local telephone central.

The second most important thing when the outside boundaries are in question refers to the field. For example, the condition of the plant at the start and finish of work may produce different dangers for its normal functioning, which may lead inevitably to its failure.

The end of solving a problem for which the analysis is developed should also be defined. For example, is it necessary to expand the analysis up to the level of a sub system or even further – to the element level? The choice of outside boundaries is made taking into account the scope of analysis, end of analysis and how detailed the analysis is.

Reliability analyst must provide that certain boundaries are possible and undisputable, taking care of the analysis aims. In order to come to the reliable conclusions about the system, the inclusion of wider part of the system may be needed within the outside boundaries. However, this may ask for expensive and long term analyses. If the recourses for such analyses are not available, real boundaries must be limited, which means that expected amount of information as a result of the analysis must be reduced.

9.4.4 Basic Rules for Fault Tree Construction

When for a certain system a failure mode is chosen as a top event, the concrete fault tree is developed by determining of direct, necessary and sufficient causes for its occurrence. It is important to point out that these are not causes of the top event at element level but its close causes. This is called a concept of "close causes" [44].

Direct, necessary and sufficient causes of a top event are then considered sub top events, and then the procedure itself determines their direct, necessary and sufficient causes. Thus, the concrete tree is continually developing becoming closer to the final analysis, when a complete tree has been developed.

There is no set of established rules whose application provides construction of the exact fault tree in all cases. However, there certain rules which may help to develop a tree in accordance with methodology [44]. These are the following rules.

Rule 1:

Write the statements so that the whole symbol of the failure mode is filled in.

Note down WHAT is a failure mode, WHERE and WHEN it occurs.

Examples of statements of failure modes:

1 "The front door bell does not ring when you press the button".

2 "A car cannot be started when the key is turned in".

Rule 2:

If a concrete failure mode in a symbol for an event can be caused by the same element failure mode, that event is classified as a mode failure caused by "element state". If a concrete failure mode is not caused by element failure mode, then the event is classified as a failure caused by "system state".

If the event is a failure mode classified as "element state", then the event can be developed as:

- primary failure mode,
- secondary failure mode,
- force failure mode.

If the event is a failure mode classified as a "system state", then the concrete event is developed according to direct, necessary and sufficient causes.

Primary failure mode is defined as any element failure mode which occurs in the conditions for which the element is designed to work or it happens due to natural aging.

Secondary failure mode is defined as any element failure mode which occurs as a result of element position under the conditions it is not designed for, either in past or in present, or may be it is caused by failure mode of other system elements.

Force failure mode is defined when the element is in the state of fault due to either the wrong operation (work, surveillance) of signals or noise.

Rule 3:

All inputs into a concrete gate should be completely described (defined) before developing any of them.

Rule 4:

Inputs into a gate should accurately describe events of failure mode, using rectangular symbols, while gates should not be directly connected to other gates.

9.5 FAULT TREE AND RELIABILITY BLOCK DIAGRAM

9.5.1 Reliability Calculation Models

Forming of a fault tree for a complex system supposes precise knowledge of functional element links causes of their failure modes as well as effects of these failure modes. The former is obtained by forming hierarchic-functional system schemes and reliability block schemes. A more detailed structural approach takes into account both primary and secondary failure modes; these are basic failures, etc. After forming a fault tree, its qualitative and quantitative estimation is carried out and probability is calculated of a complete resulting system failure on the basis of familiar information of element reliability, that is, on the basis of information of probabilities and rates of their failure modes, of availability, etc.

Two graphic models of reliability calculation can be suggested for the system, one of which is a reliability block diagram, and the other a typical tree.

In practice it is possible to choose a model of system structure with the help of fault tree or with the reliability block diagram. When the fault tree is limited only to OR gates and AND gates, both models give the same result, that is why it is possible to turn a concrete fault tree into a concrete reliability block diagram and vice versa [47].

I reliability block diagram, "link" with the help of a block means that element shown in the form of a block is functioning. This shows that certain failure mode or certain set of failure modes of a concrete element do not occur. In the concrete fault tree, as a basic event, the same failure mode or certain set of failure modes of a particular element may happen. When the top event in a fault tree presents "system failure mode", while basic events are determined in the sense it has already been stated, it can easily be seen, for example, that reliability series connection (Figure 43) is equivalent to fault tree where all basic events are connected by one OR gate. A particular top even occurs if element 1 or element 2 or element 3 or element n … fails.

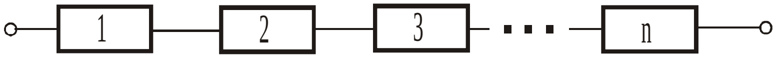


Figure 43. Reliability block diagram of series system

In the same way a concrete reliability parallel connection (Figure 44) can be presented as a fault tree where all the basic events are connected by one AND gate. A particular top event occurs, that is, the reliability parallel connection fails if element 1 and element 2 and element 3 and …element n fail.

The examples which show how a reliability block diagrams transfer into fault tree diagrams are given [47].

If mark with C_i a logical variable which corresponds to the state of functioning of i's element, and with S – the state of system functioning, then the trees shown in Figure 45 converted to system fault trees. A line above the logical variable marks its negation, that is, opposite event.

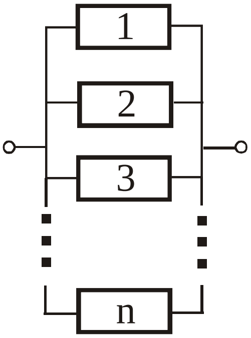


Figure 44. Reliability block diagram of parallel system

As a more complex example we consider the system fault tree of the heavy plane chassis [50] where its physical model and its reliability block diagram are shown (Figure 46). The system has 18 wheels, two of them form the front wheel N (nosewheel), 8 wheels form two trolley W1 and W2, placed under the central body of the aircraft, and another 8 form two more trolley R1 and R2, placed closer to the tail. In the aim of simplifying, the analysis is focused on faults connected with the loss of wheel work ability. System failure occurs in case of failure of one of the subsystems – front trolley, at least one of central trolley, or both trolley closer to the tail. The concrete reliability block diagram of an aircraft is also shown in the Figure 46.

Carrying trolley, two central trolley, and a couple trolley closer to the tail make a reliability series connection. Wheels of all wheels make a parallel connection. Rear wheels also make a parallel connection, supposing that in case of wheel failure of one trolley the load can be taken over by the wheels of other trolley.

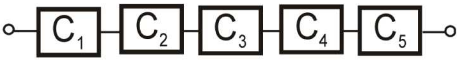
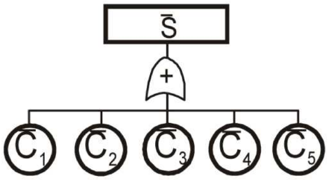
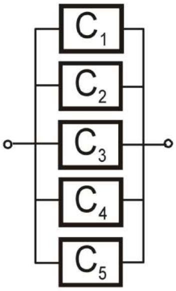
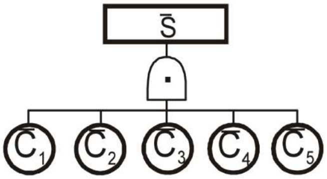
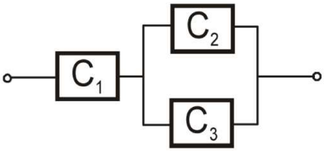
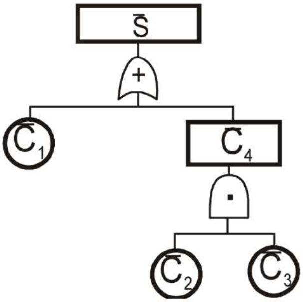
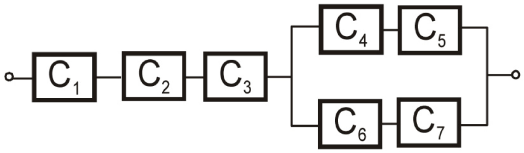
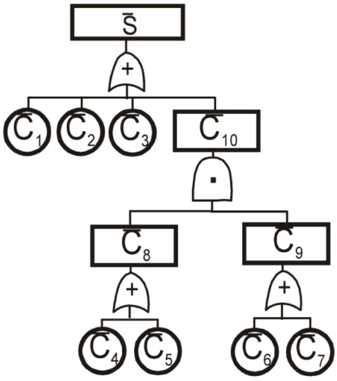
Reliability Block Diagram (S)	Fault Tree ($\bar{S}$)
	 $\bar{S}$ + $\bar{C}_1$ $\bar{C}_2$ $\bar{C}_3$ $\bar{C}_4$ $\bar{C}_5$
	 $\bar{S}$ · $\bar{C}_1$ $\bar{C}_2$ $\bar{C}_3$ $\bar{C}_4$ $\bar{C}_5$
	 $\bar{S}$ + $\bar{C}_1$ $\bar{C}_4$ · $\bar{C}_2$ $\bar{C}_3$
	 $\bar{S}$ + $\bar{C}_1$ $\bar{C}_2$ $\bar{C}_3$ $\bar{C}_{10}$ · $\bar{C}_8$ $\bar{C}_9$ + + $\bar{C}_4$ $\bar{C}_5$ $\bar{C}_6$ $\bar{C}_7$

Figure 45. Reliability block diagram conversion to a Fault tree

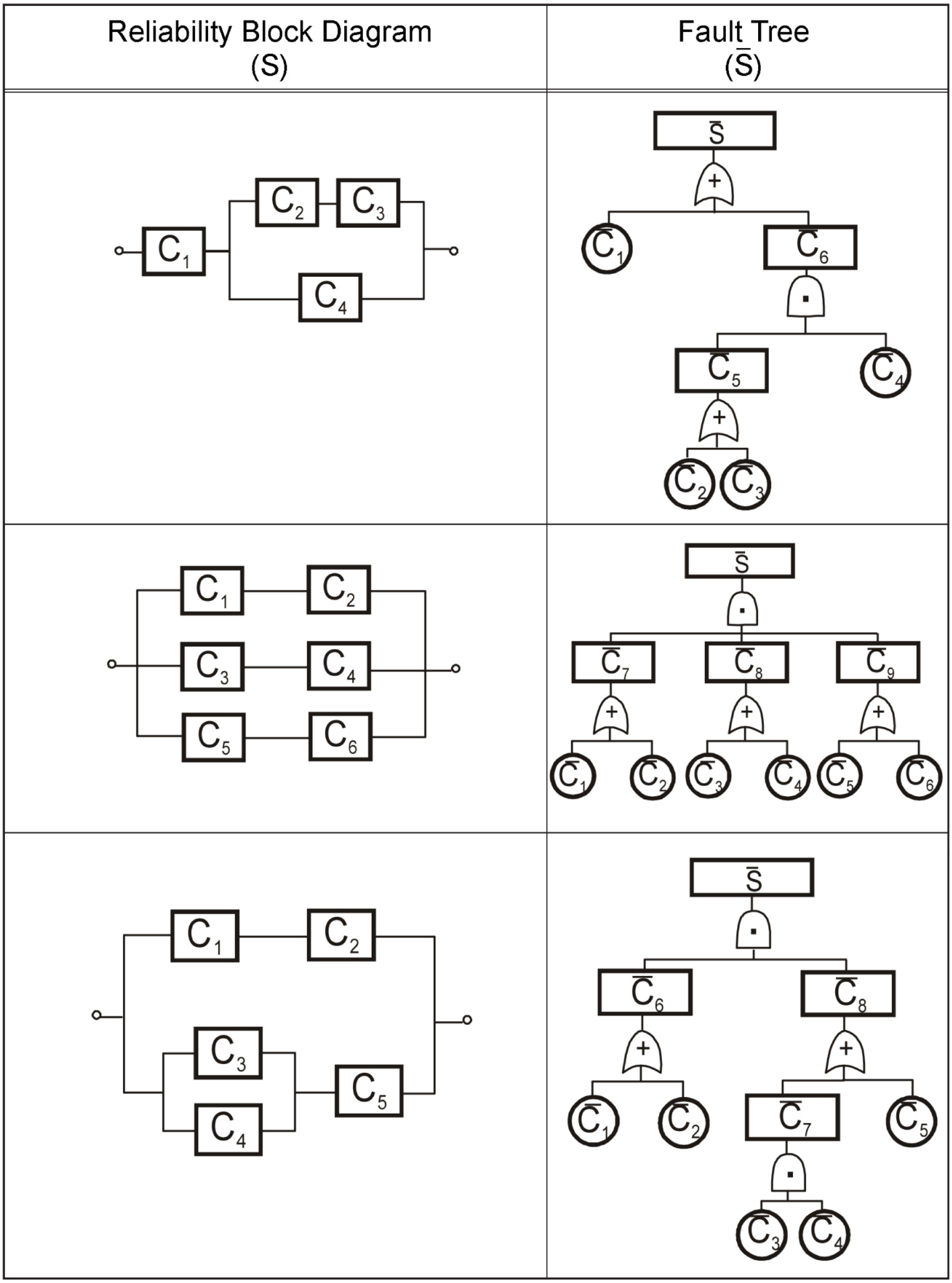


Figure 45. Reliability block diagram conversion to a Fault tree (continuation)

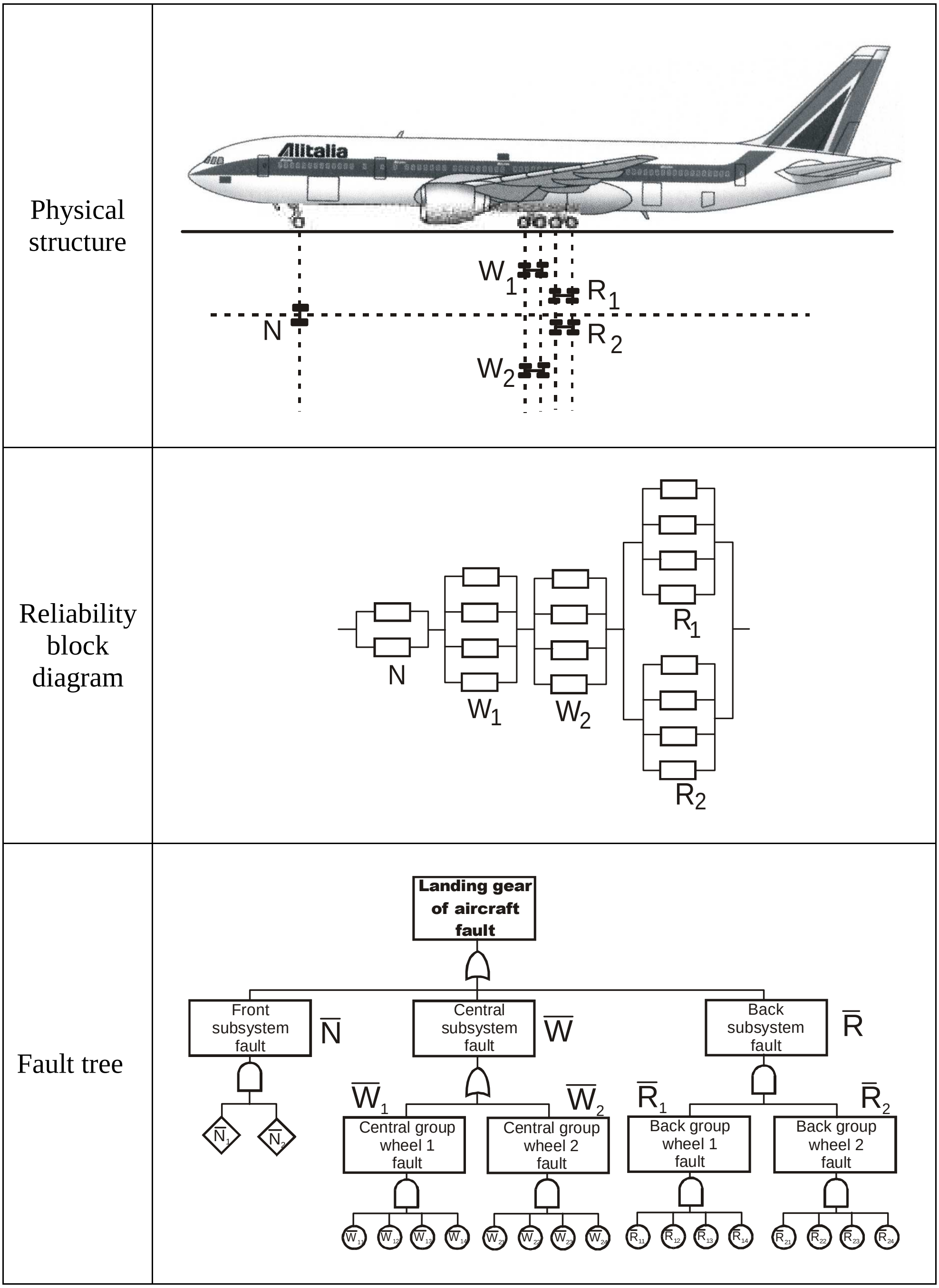

Physical structure
Alitalia
W_1
R_1
N
R_2
W_2
Reliability block diagram
N
W_1
W_2
R_1
R_2
Fault tree
Landing gear of aircraft fault
Front subsystem fault
$\overline{N}$
Central subsystem fault
$\overline{W}$
Back subsystem fault
$\overline{R}$
$\overline{N}_1$
$\overline{N}_2$
$\overline{W}_1$
$\overline{W}_2$
$\overline{R}_1$
$\overline{R}_2$
Central group wheel 1 fault
Central group wheel 2 fault
Back group wheel 1 fault
Back group wheel 2 fault
$\overline{W}_{11}$ $\overline{W}_{12}$ $\overline{W}_{13}$ $\overline{W}_{14}$
$\overline{W}_{21}$ $\overline{W}_{22}$ $\overline{W}_{23}$ $\overline{W}_{24}$
$\overline{R}_{11}$ $\overline{R}_{12}$ $\overline{R}_{13}$ $\overline{R}_{14}$
$\overline{R}_{21}$ $\overline{R}_{22}$ $\overline{R}_{23}$ $\overline{R}_{24}$

Figure 46. System Aircraft: Physical structure, Reliability block diagram and Fault tree

9.6 QUALITATIVE ASSESSMENT

9.6.1 Cut Sets and Path Sets

For a concrete fault tree, failure system modes are clearly determined by cut sets which represent the group of basic events. If all basic events occur, top event will occur definitely. Accordingly, a certain cut set is defined as any basic event or combination of basic events whose (simultaneous) occurrence will cause occurrence tope events (Figure 47) [48,49].

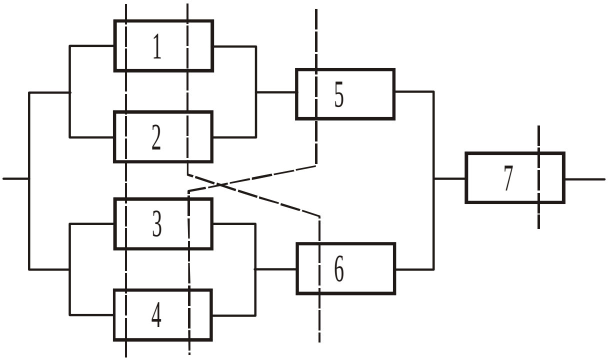


Figure 47. Cut sets

On the other hand, path sets represent dual concept of cut sets. That is a group of basic events, so that if none of the events happen, then top event will not occur. Accordingly the path set is defined as a particular event or a combination of events whose not occurring provide not occurring of a top event (Figure 48) [48,49]. When a certain system has only one top event, then not occurring of certain basic events (failure mode) in the path set provide a successful system operation. When it is established/found out that there are more then one top events, this non occurrence does not mean/guarantee that system operation will be successful. In such cases, a concrete path sets provide only non occurrence of individual top event.

There are two simple rules for determining of cut sets [48]:

1. Certain OR gate always increases the number (quantity) of cut sets (for every input in the OR gate there will be a special group of cut sets),

2. Certain AND gate always increases the size of a cut set (there will be one cut set for a particular AND gate, and every input will increase the size of a particular cut sets).

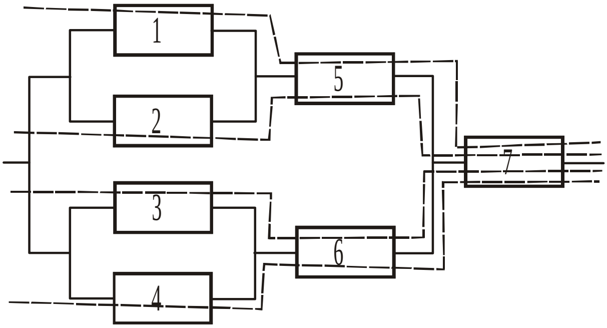


Figure. 48. Path sets

Illustrative example for determination of cut sets of a fault tree (qualitative assessment), for the failure mode "Motor overheats" shown in the Figure 49, includes two ways [48].

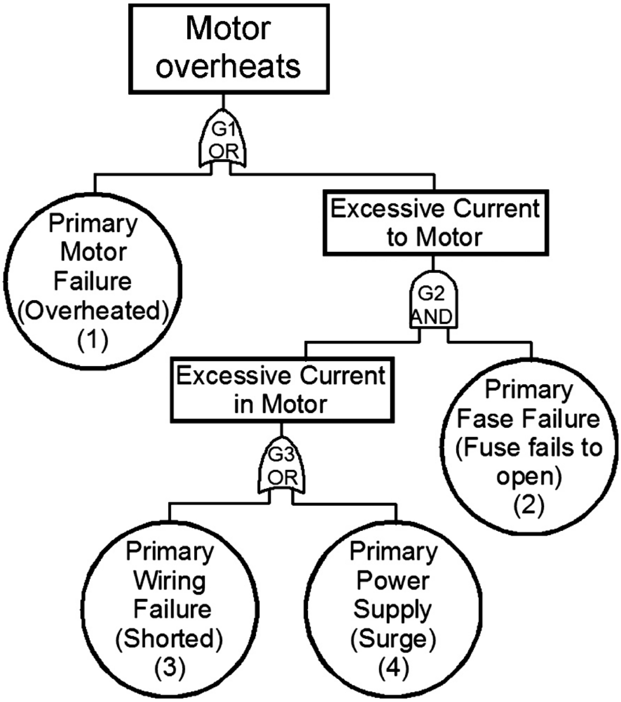

Motor overheats
G1 OR
Primary Motor Failure (Overheated) (1)
Excessive Current to Motor
G2 AND
Excessive Current in Motor
Primary Fase Failure (Fuse fails to open) (2)
G3 OR
Primary Wiring Failure (Shorted) (3)
Primary Power Supply (Surge) (4)

Figure 49. Fault tree for failure mode "Motor overheats"

1st Way – Determination of the cut set by visual check up, directly for the concrete fault tree:

Remark:

It should be taken into account that every input in the certain OR gate generates (produces) a special cut sets and that every AND gate generates (produces) only one cut set. Every input in certain AND gate just increases the size of a particular cut set.

Concrete cut sets for a concrete fault tree:

(1) Primary motor failure mode (Motor overheats)

OR

(2) Primary electric switch failure mode (Switch failed in the open position) **AND (3)** Primary failure mode of electric installation (Short cut).

OR

(2) Primary failure mode of an electric switch (Switch failed in the open position) **AND (4)** Primary failure mode of electric current supply (Top loading).

2nd Way – Determination of cut sets by using algorithms:

Application of algorithm:

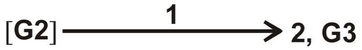
Step 1: Numbering each gate and event in a concrete fault tree.

Step 2: Start from the highest gate in a concrete fault tree and substitute that gate with appropriate events at input. A concrete highest gate, marked with G1 for gate 1, is OR gate with two inputs which determine two cut sets:

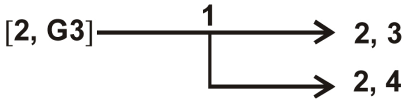
1
G2

Each cut set is written in a separate row. Each row which has a gate must be widen by replacing certain gate with some of its inputs.

Step 3: Gate 2 (G2) has two inputs. As this gate is actually AND gate, both appropriate inputs will be shown in the same row:



Step 4: By using this same approach, the gate 3 (G3) is replaced by its inputs. The gate 3 is OR with two inputs. This tells us that gate 3 must be replaced with two separate rows – each input has its row:



Step 5: Now all gates are replaced with their inputs, and the complete list of cut sets for the failure mode "Motor overheats" is developed. These cut sets are:

1
2,3
2,4.

Remark:

This procedure can be used for determination of cut sets for any size of a fault tree. For large fault trees it is possible to save the time by using software program which is based on equations of Boolean logic algebra for a fault tree when determining the concrete cut set.

9.6.2 Method for Obtaining CUt Sets

9.6.2.1 What is MOCUS?

Method for Obtaining CUt Sets (MOCUS) is an algorithm that can be used to find the minimal cut sets in a fault tree. Consider the fault tree in Figure 50 where the gates are numbered from G0 to G6. The example of fault tree is copied from [51].

9.6.2.2 The MOCUS Algorithm Application

The idea:

The MOCUS algorithm start at the G0 gate directly under TOP EVENT. If this is an OR gate, each input to the gate is written in separate rows. The inputs may be new gates. Similary, if the G0 gate is an AND gate, the inputs to the gate are written in separate columns. The idea is to successively replace each gate with its inputs (basic events and new gates) until one has gone through the whole fault tree and is left with just the basic events. When this procedure is completed, the rows in the established matrix represent the cut sets in the fault tree.

Step 1:

Since G0 is an OR gate:
1
G1
2

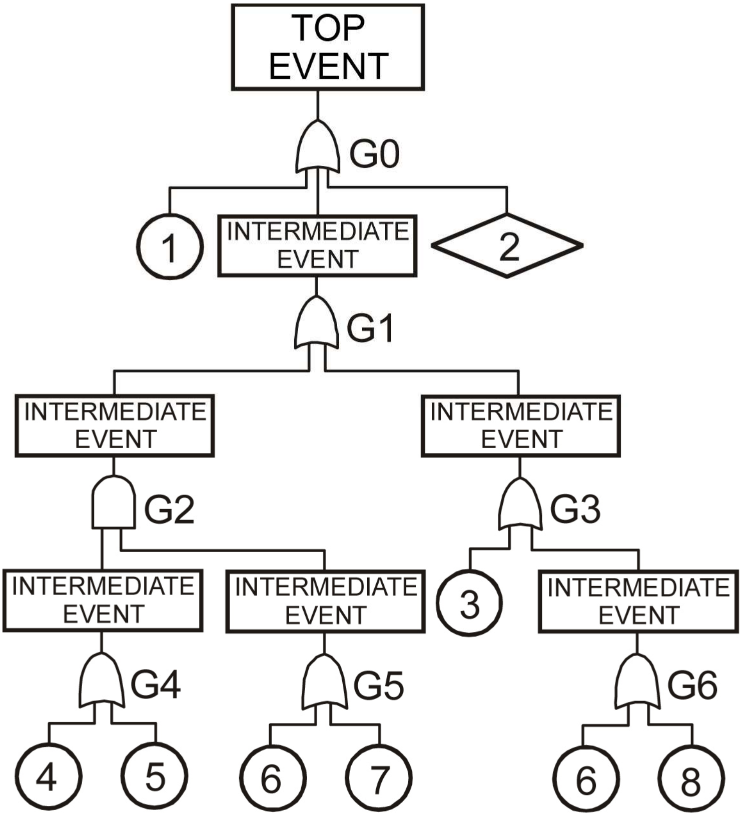


Figure 50. Example of a fault tree for explain the MOCUS algorithm

Step 2:
Since G1 is an OR gate:
1
G2
G3
2

Step 3:
Since G2 is an AND gate:
1
G4, G5
G3
2

Step 4:

Since G3 is an OR gate:

1
G4, G5
3
G6
2

Step 5:

Since G4 is an OR gate:

1
4, G5
5, G5
3
G6
2

Step 6:

Since G5 is an OR gate:

1
4, 6
4, 7
5, 6
5, 7
3
G6
2

Step 7:

Since G6 is an OR gate:

1
4, 6
4, 7
5, 6
5, 7
3
6
8
2

From the fault tree obtained the following 9 cut sets:

[1]
[2]
[3]
[6]
[8]
[4, 6]
[4, 7]
[5, 6]
[5, 7]

9.6.2.3 Comments

Comment 1:

Since [6] is a cut set, [4, 6] and [5, 6] are not minimal, we are left with the following list of minimal cut sets:

[1], [2], [3], [6], [8], [4, 7], [5, 7].

In orther words, five minimal cut sets are of order 1 and two minimal cut sets of order 2.

Comment 2:

The reason that the MOCUS algorithm in this case leads to nonminimal cut sets is that basic event 6 occurs several places in the fault tree.

Comment 3:

After the minimal cut sets are determined, some idea of failure importance can be obtained by ordering the minimal cut sets according to thier size. Single-element minimal cut sets are listed first, then dobuble-element cut sets, then triple-element cut sets, and so on.

9.6.2.4 Reduced Fault Tree

If the same input is present at more than one place in the fault tree, it is possible to develop an equivalent "reduced" fault tree form the minimal cut sets. This reduced fault tree in Figure 51 will not contain the duplicated inputs and can be used as the model for quantitative evaluation.

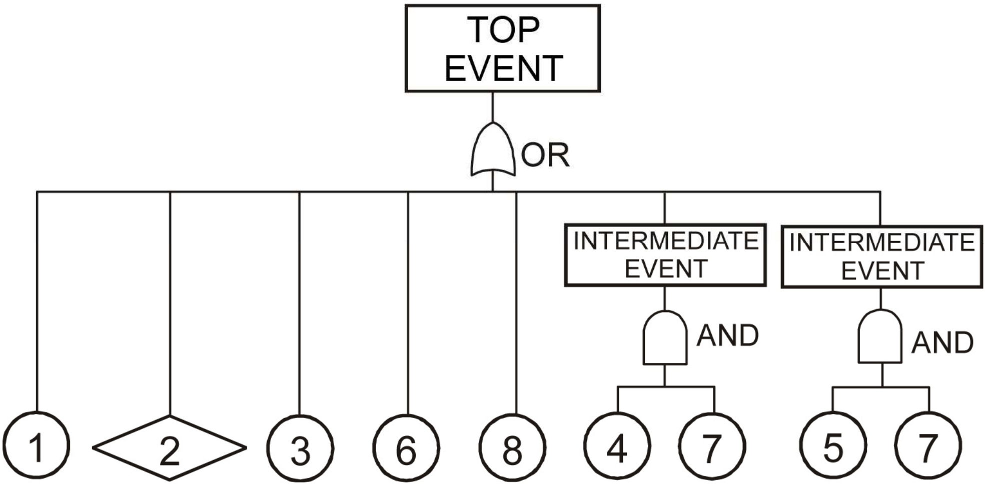


Figure 51. Reduced Fault tree

9.6.3 The Criticality of a Cut Set (Qualitative Evaluation of the Fault Tree)

A qualitative evaluation of the fault tree may be carried out on the basis of the minimal cut sets. The criticality of a cut set (i.e., the order of the cut set) depends obviously on the number of basic events in the cut set. A cut set of order one is usually more critical than a cut set of order two, or more. When we have a cut set of order one, the Top Event will occur as soon as the corresponding basic event occurs. When a cut set has two basic events, both of these have to occur simultaneously to cause the Top Event to occur.

Another important factor is the type of basic events of a minimal cut set. We may rank the criticality of the various cut sets according to the following ranking of basic events:

1. human error,
2. active equipment failure,
3. passive equipment failure.

This ranking is based on the assumption that human errors occur more frequently than active equipment failures and that active equipment is more prone to failure than passive equipment (e.g., an active or running pump is more exposed to failures than a passive standby pump). Based on this ranking, we get the ranking of the criticality of minimal cut sets of order two. See Table 13: rank 1 is the most critical.

Table 13. Criticality ranking of minimal cut sets of order two

Rank	Basic event 1 (type)	Basic event 2 (type)
1	Human error	Human error
2	Human error	Active equipment failure
3	Human error	Passive equipment failure
4	Active equipment failure	Active equipment failure
5	Active equipment failure	Passive equipment failure
6	Passive equipment failure	Passive equipment failure

9.7 QUANTITATIVE ASSESSMENT

9.7.1 Probability of a Top Event in Case of Fault Tree Without Events Repetition

In case that fault tree contains independent basic events as top events which repeat only once within a tree, then the probability of a top event can be determined by probability of basic events' acting**,** bottom-up through the concrete tree. During this procedure the probability of intermediate events are calculated beginning from the foot of the concrete tree and moving upwards until the probability of the top event is not determined.

For example, the fault tree for the top event "Potential failure mode of an engine" is considered, Figure 52, which contains three non repetitive basic events (1), (2), and (3) which occur independently of any other, with corresponding probabilities shown in the Table 14 [48].

This approach is suitable and regular/right, but unfortunately it can be applied at simple fault trees which do not have repetitive events. If we could analyze trees with repetitive events, this approach would not be appropriate, as the occurrence of the intermediate event would not be independent any more.

Probability equation for "Potential failure mode of an engine":

$$P(\text{Potential failure mode of an engine}) = [P(1)+P(2)-P(1)\cdot P(2)]\cdot P(3)=$$
$$= (0{,}001 + 0{,}002 - 0{,}001 \cdot 0{,}002) \cdot 0{,}01 = 0{,}0003.$$

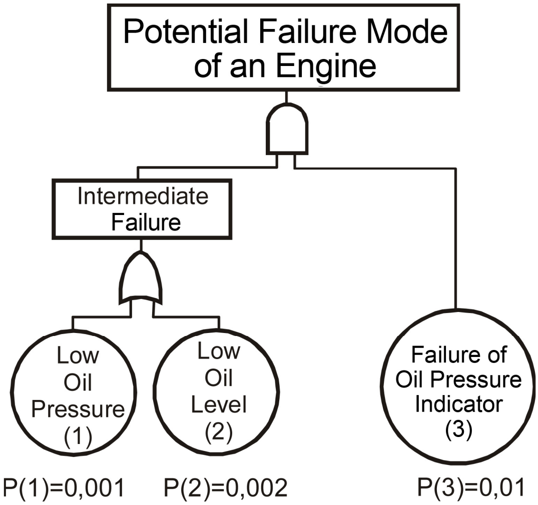


Figure 52. Fault tree for the top event "Potential failure mode of an engine"

Table 14. Probabilities for of the lowest-level of the fault tree for failure mode at the top level "Potential failure mode of an engine"

Event	Failure mode	Probability of failure mode occurrence P_F	Probability of operation (Reliability) $R = 1 - P_F = P_O$
1	Low oil pressure	0,001	0,999
2	Low oil lewel	0,002	0,998
3	Failure of oil pressure indicator	0,01	0,99

Corresponding reliability block diagram shown on Figure 53.

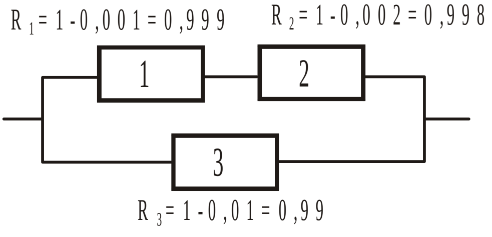


Figure 53. Reliability block diagram for fault tree for the top event "Potential failure mode of an engine"

Reliability equation for the engine:

$$R_E = P(\text{Engine operation}) = 1 - [(1 - R_1 \cdot R_2) \cdot (1 - R_3)] =$$
$$=1 - [(1 - 0{,}999 \cdot 0{,}998) \cdot (1 - 0{,}990)] = 0{,}9997.$$

9.8 ADVANTAGES AND DISADVANTAGES OF FAULT TREE ANALYSIS

Fault tree analysis is effective and multipurpose method which points out the importance of failure aspect as early as system designing. The results of analysis are shown in an easy and understandable way. Fault tree analysis can be carried out in any phase of designing. The concrete fault tree can be constructed up to any degree of details, depending on information and time availability, as well as on financial circumstances.

Fault tree analysis is top-down method for determining factors and causes which cause unwanted, critical failure modes with catastrophic consequences. Starting from the unwanted event, causes or failure modes are determined at the next lower functional level, which is gradually repeating downwards until the wanted level is not reached. Methods like cut sets and Boole's algebra can be applied for reliability assessment and safety on the basis of formed fault tree together with appropriate values of failure rate, probability of failure, etc., for basic events in the tree. Benefits of this method are possibility of parallel, redundant and reserve paths which can satisfy several cross-connected systems. This method is very useful when one or two problems should be analyzed. Drawbacks of this method are: very often large, complex trees are needed for an accurate description of a situation and the method demands a special tree for each unwanted event.

Top event should be a central part of the whole analysis. Mainly fault trees are applied in critical situations in the aim of safety, such as nuclear production in the plants, aircrafts and communication networks. Top, unwanted event is defined as the beginning or the existence of danger or subsystem failure within a system.

Fault tree analysis is more universal method than Analysis of modes, effects and critical failures for the reliability and safety analysis, as it can take into account multipurpose/complex failures, including human errors or wrong actions.

Chapter 10

STATISTICAL SAFETY ANALYSIS

10.1 BASIC PRINCIPLES OF STATISTICAL SAFETY ANALYSIS

Basic problems when carrying out statistical safety analysis involve selecting the most hazardous scenarios which have the biggest impact on risk assessment. Statistical safety analysis is carried out by a team of experts which, as a rule, consists of: designers, process engineers, mechanics and experts for engineering statistics and statistical safety analysis. Their role is working out certain calculations which enable establishing possible scenarios for development of accidents, as well as assessment of the system accident effects. Any kind of accident condition results in damaging personnel health and life and great economic losses resulting from the cost of reengineering and restarting up of the system.

When carrying out statistical safety analysis in an earlier stage as possible its results are more effective as system safety assurance will involve lower cost. This is explained by the rule of ten times increase of costs for removing/elimination of defects (nonconformities) when transition to the next system life cycle phase [14]. This simple rule of ten times cost increase shows the importance of the early detection potential problems in the field of safety.

The base of statistical safety analysis is event tree construction, i.e. carrying out system analysis of what occurs after initial event.

The procedure of carrying out of statistical safety analysis includes the following stages:

- choice and classification of initial events, as well as assessment of their frequency,
- using real data about systems' items reliability in studied scenarios of what occurs after initial event,
- analysis of the sequence of accident occurrence,
- probabilities calculation of realization of accident occurrence sequence,
- classification of final stages and risk calculation.

It should be pointed out that carrying out statistical safety analysis presents a very complex and difficult problem whose solution often demands for engagement other experts except for the ones mentioned above. As statistical safety analysis is carried out in the phase of designing and maintenance, when some data and pieces of information about certain processes and phenomena may be missing or incomplete, risk calculation is followed by high degree of uncertainty [52]. As a rule, possible uncertainties in risk calculations do not influence solutions to other problems of statistical safety analysis, as it is supposed that they equally influence calculation risk values, for example when comparing different variants of system design.

In many cases, carrying out statistical safety analysis fully can be more difficult. Therefore only qualitative and quantitative analysis of system reliability is carried out [53].

In order to increase safety analysis objectivity verified (approved) databases should be used which contain knowledge about reliability indicators of similar items and regimes and their work conditions, as well as specialized databases about personnel reliability.

Results of statistical safety analysis are formed in reports and submit to the archive for later checking and expert opinions. These results are to be inspected by detailed engineering analysis so that suitable corrective actions can be taken. A very important demand when carrying out statistical safety analysis is simplicity of their results interpretation as in the opposite case it may happen that it is not understood by engineering personnel. Furthermore, basic stages of carrying out statistical safety analysis are considered step by step.

10.2 INITIAL EVENTS ANALYSIS

At this stage a list of possible events potentially hazardous from the aspect of damage occurrence which exceeds allowed level is made and a selection from the list is made of initial events group which is later used for modeling by means of event tree construction. Carrying out of this stage is necessary in order to reduce selected scenarios of possible accidents.

When making the whole list of initial events internal and external initial events should be separated. Internal initial events are caused by system items failures, operator's incorrect activities or maintainer's errors, while external are caused by – influences connected with natural phenomena or human activities in the territory (region) where the system is located (earthquakes, winds, floods, terrorist attacks) [53]. Classification of initial events is shown in Figure 54.

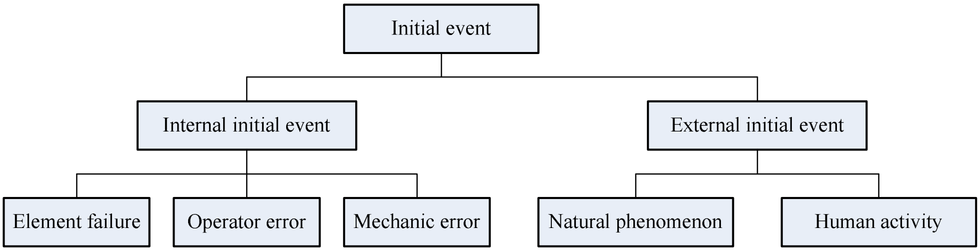


Figure 54. Classification of initial events

As the starting data for carrying out this stage, accident analysis of similar systems is used. The importance of work in this stage is conditioned by the need for safety assurance not only in the period of normal exploitation, but when initial event occurs [54].

Short consideration of some kinds of initial events is given.

Earthquakes are oscillations of earth's crust due to sudden movements and fractures in the earth's crust. Movement of the ground during an earthquake has a wave character.

Classification of earthquakes according to the dimension and strength is done in according to the dimensionless scale of magnitude M which characterized total energy of elastic oscillations, caused by an earthquake. The scale M is in the interval between 0 and 9. Rate of an earthquake on the ground surface is assessed according to the international scale UNESCO MSK -1964. Earthquakes classification according to the magnitudes, degrees and average frequency is shown in Table 15.

Winds are atmosphere whirlwinds (whirlpools). Winds of great dimensions (surfaces) speed of up to 120 km/h are hurricanes. Annual hurricanes quantity ν possible to describe via Poisson's law with density function:

$$f(\nu) = \mu\nu \exp(-\mu)/\nu! \qquad (1)$$

where:

μ - mean annual hurricane frequency (for hurricanes of Atlantic Ocean coast in U.S.A., μ = 2).

Table 15. Classification of earthquakes

Earthquake characteristic	Magnitude M	Degree J	Average frequency of earthquake (during the year)
World proportion			1-2
Strong, regional significance	7-8	9-10	15-20
Strong, local significance	6-7	7-8	100-150
Mean	5-6	6-7	750-1000
Weak, local	4-5	5-6	5000-7000

Floods are sinking of regions (grounds) due to rising of water level in a river, lake or sea. Between different natural catastrophes, according to frequency and material losses, in many countries floods are on first place.

System items failures have the main role in accidents occurrence. Thus in the last ten years in the coal mines of Serbian Electric-Power Industry, the causes of excavator items accidents can be grouped in the way as it is given in Table 16.

In other potentially hazardous systems this accident share is changeable, but even in these cases system items failures have the main role in accidents occurrence.

As a rule, failure frequency or failure rate of system items are determined according to the results obtained from specially organized testing of these items for reliability assessment or when testing within the system structure. However the most accurate assessment of failure rate is obtained by data processing about failures from the exploitation of the similar systems. As a result a database about items reliability is formed and it can be used for initial events analysis. By taking out information about items reliability from corresponding database, frequency assessment of initial events can be done for the factor of "system items failure".

Table 16. Causes of excavator items accidents

Cause of accident	Accident share [%]
Difficult exploitation conditions	27
Error in manufacture and assembly	22
Operator's error	18
Mechanic's error	13
Fatigue of materials, wear of equipment and corrosion processes	8
Inadequacy design	7
Other miscellaneous factors	5

Personnel errors (operator, mechanic) also play an essential role in accident occurrence which is proved by the data from Table 16. Analysis of these data show that human (personnel) errors in more than 30% cases present causes of initial events of accidents with bucket wheel excavators. Here, error is meant a human (personnel) failure mode, which is not connected with a strike or sabotage. According to previous research data [55], incorrect, or wrong activities of personnel when operating complex systems caused up to 40% of unwanted results when rocket testing, up to 30% radio electronics equipment failures.

For initial events analysis connected with personnel errors, it is important to have data about human reliability. Today, this information about human errors is found in special databases which are formed according to the results of special laboratory experiments or according to results of exploitation of one system type. Detailed information about personnel reliability analysis is given in the literature [56].

Taking into account of human factor in risk analysis presents significant value of statistical safety analysis.

Screening presents a procedure of excluding those initial events from the starting list whose frequency (rate) value is very low and whose consequences (on the basis of results of analysis of similar systems accidents) are worthless (minimal) in comparison with other initial events. In that way screening enables shortening of the list of initial events up to a reasonable level. As a result, a final list of initial events with suitable frequency values of their occurrences is formed, which further enables carrying out quantitative risk calculation [57]. The procedure of screening can be carried out by applying Pareto diagram method [58] or method of Failure Modes, Effects and Criticality Analysis [25].

10.3 ANALYSIS OF ACCIDENTS OCCURRENCE SCENARIOS

As it is previously explained, system safety is defined by order of events, for example by personnel errors, external events and others, which cannot be treated as failures. Furthermore, analysis of great number of accidents of different kinds of systems show that they usually result (cumulate) from an order of events, whose order (and connections) is suitable to present as an event tree [53]. Event tree presents continuous non periodical graph where an initial event and intermediate event are distinguished, caused by occurrence of initial and final states. Initial and intermediate events which come later really describe possible paths of unwanted event flow (accident).

The most important and bright sides of the methodology of event tree construction for risk calculation are: analysis simplicity, visualization of risk calculation and possibility of taking into account of operator (mechanic) by means of including real elements into the event tree which characterize the work of operator (mechanic) or by means of studying initial events of accidents which are connected with personnel errors. Event trees are oriented towards taking into account cause-effect dependence among system items condition in certain instants of time among which critical conditions may be found.

Event tree is constructed with an aim of effects analysis of some initial event I_0 (item failure, personnel error, or external event), which is drawn at the foot of a tree base. This initial event may (or may not) lead to later events, directly caused by initial event which are called events of the first level: I_{11}, I_{12}, ..., I_{1k}. Each event of the first level may (or may not) cause later events which are directly connected with it. Putting it in another way, event tree by itself presents a logical diagram which defines (shows) a set of system final states, out of which each represents realization of certain intermediate events combination, which can influence accident development process in initial event.

The following events can be used as intermediate:

- successful or unsuccessful activation of system items, including insurance and blockade,
- correct or incorrect activity of personnel (operator, mechanic).

Development of a event tree is carried out by a certain schedule:

Step 1. Choice of a certain initial event from the final list of initial events and its description.

Step 2. Determination of functions, which should be carried out by certain system items when certain initial event chosen from the list occurs.

Step 3. Modeling event tree (construction of accident development scenario).

Step 4. Classification of final states set.

The first step is clear and is not necessary to be explained. As a result of carrying out the first step it is possible to construct a event tree base.

System for lifting of bucket wheel excavator SRs 1200x24/4x0(400kW)+VR rotor's arrow which consists of two driving item parallel connected (in reliability block diagram) whose task is lifting and lowering rotor's arrow during the digging process in the coal mines is shown in Figure 55.

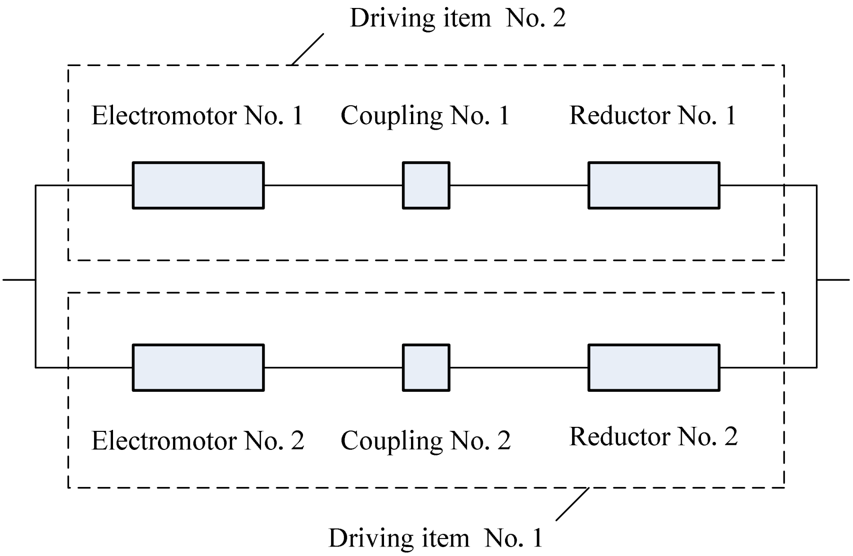
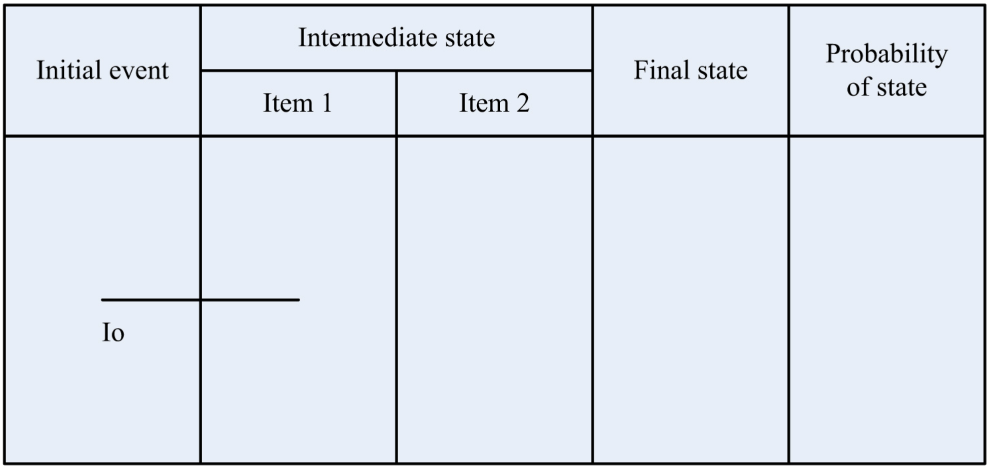


Figure 55. System for lifting of bucket wheel excavator SRs 1200x24/4x0(400kW)+VR rotor's arrow (fragment)

From the final list of initial events, which have been considered in the previous step, the event I_0 is chosen – mechanical defect of small gear on outgoing spindle of driving item No.1. After carrying out the first step, columns of Figure 56 are filled and the event tree base is constructed. In Figure 56 the following marks are introduced:

- Items 1 and 2 respectively – driving item No. 1 and driving item No. 2,
- I_0 – initial event (mechanical defect of small gear on outgoing spindle of driving item No. 1).



Initial event	Intermediate state		Final state	Probability of state
	Item 1	Item 2		
Io				

Figure 56. Example of event tree construction table fill out after first step of the analysis

It is useful to give additional clarifications which should completely explain modeling of event tree. Modeling the event tree enables, as it has already been said, taking into account personnel role assessment after occurrence of initial event if its participation is predicted. This can be achieved by introducing of fictions item in second column of Figure 56 and corresponding showing of the point of branching which show the acting of personnel: "stair" up – correct reaction of the operator and "stair" down – incorrect work of the operator.

10.4 RISK CALCULATION

If for a particular initial event I_0 we can select n scenarios of accidents occurrence which are marked as: E_1, E_2, ..., E_n, in this case accident may occur before realization of n non simultaneous (random) scenarios of accident occurrence. Thus, accident is an event (in statistical sense) which represents a collection of non simultaneous (random) events E_1, E_2, ..., E_n. So, accident probability (conditional) is shown with the formula:

$$Q(I_0) = \sum_{i=1}^{n} Q_i(E_i / I_0),\ i = 1, 2, ..., n \qquad (2)$$

where:

Q_i (E_i / I_0) - probability of realization of the scenario of accident occurrence for particular initial event.

For calculating total probability $R(I_0)$ of accident occurrence (unconditional) it is necessary to take into account probability $P(I_0)$ of initial event occurrence. In that case, according to the total probability formula, accident probability $R(I_0)$ can be calculated when initial event I_0 occurs:

$$R(I_0) = P(I_0) \cdot \sum_{i=1}^{n} Q_i(E_i / I_0) = \sum_{i=1}^{n} P(I_0) \cdot Q_i(E_i / I_0), \qquad (3)$$

where:

$P(I_0)$ - probability of initial event occurrence I_0 for a certain period of time T, e.g. for one year. This probability is determined by using results of initial events analysis.

The last expression presents total probability formula which characterizes unconditional (full) accident occurrence probability, i.e. accident risk R [55].

In practice, as initial events are very rare, for probability distribution of their occurrence for the time T a Poisson's distribution can be taken:

$$P(\nu = m) = \lambda^m \cdot e^{-\lambda} / m!,\ m = 0, 1, 2, ..., \lambda,\ \lambda > 0 \qquad (4)$$

which characterizes occurrence probability of exact m initial events in a time item. Here λ is intensity of initial event occurrence which is measured by their number in a item time.

Supposing that m = 1, a $\lambda \cdot T \approx 0$ (which is justified for high reliable potential dangerous systems) it is obvious that:

$$P(\nu = 1) = P(I_0) \approx \lambda.$$

Thus, in formula (3) for calculating risk instead of initial event occurrence probability it is useful to change the rate (frequency) of its occurrence:

$$R(I_0) = \lambda \sum_{i=1}^{n} Q_i (E_i / I_0) . \qquad (5)$$

This substitution is connected with simpler risk defining as accident frequency in a time item. Majority of quantitative safety analysis includes risk assessment exactly in this form. Apart from this, very often analysis of initial events relies on the information about frequency and not on probability of their occurrence.

On the other hand, values $Q_i(E_i/I_0)$, i = 1, 2, ..., n is calculated according to the formula of simultaneous occurrence of independent events probability (in a set) which form particular scenario of accident occurrence E_i. In other words, if E_i is a scenario of accident occurrence caused by k_i independent, in a set events (items failures, personnel errors, items operation without failures) whose probabilities are equal to π_{ij} then:

$$Q_i (E_i / I_0) = \prod_{j=1}^{k_i} \pi_{ij}. \qquad (6)$$

where:

$j = 1, 2, ..., k_i$

$\pi_{ij} = p_{ij}$ - probability of operation without failures or $\pi_{ij} = q_{ij}$ - failure probability.

It should be emphasized that assumption of independence within a group of events, which enter in accident occurrence scenario, is rather disputable. However, taking into account dependence of events can make the calculation of probability $Q_i(E_i/I_0)$ much more difficult that is why it is not considered here.

Calculated values $Q_i(E_i/I_0)$ are entered in the fifth column of Figure 57. Apart from that, sometimes, it is useful to enter values of all events scenarios realization probability in this column. As an example, in Figure 57 probability values of all possible scenarios previously classified in appropriate groups are given.

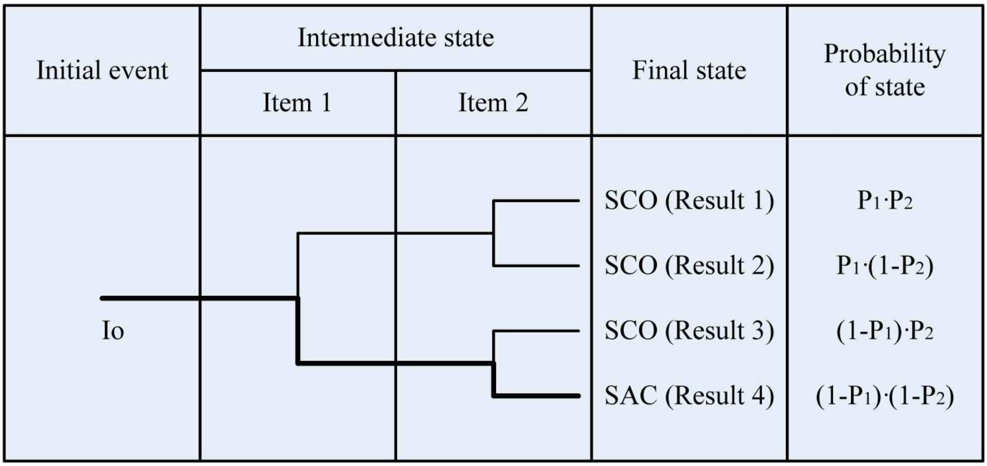
Analysis of the fourth column in Figure 57 shows that the number of accident scenarios equals item (i = 1). In that case:

$$Q (I_0) = Q_1 (E_1 / I_0). \qquad (7)$$

On the other hand, conditional probability $Q_1(E_1/I_0)$ of accident scenario realization (failure probability of both items) is determined as:

$$Q_1 (E_1 / I_0) = (1 - P_1) \cdot (1 - P_2). \qquad (8)$$

Here, when calculating value Q factor of time is not taken into account (determined operation time) which has an important role when calculating probability operation without failure. It is obvious that if a set of final states matches with the full set of elementary events (within the limits of elementary probability theory), in that case the sum of all final states probability equals to item.



Legend:
SCO - state of capability to operate
SAC - state of accident

Figure 57. Example Event tree with presentation final states probabilities

The risk accident value is calculated according to the formula (8) taking into account conditions (7):

$$R (I_0) = P (I_o) \cdot Q (E_1 / I_0) = P (I_0) \cdot (1 - P_1) \cdot (1 - P_2). \qquad (9)$$

In complex cases the event tree can be extended, thus the analysis of risk calculation results becomes complicated accordingly.

10.5 ANALYSIS OF CALCULATION RISK RESULTS

As the initial events in the event tree analysis, besides functional failure modes in the mechanism for the hoist of rotor's arrow, observed modes are of personnel errors (operators and maintainers). Based on data from the bucket wheel excavator SRs 1200x24/4x0 (400kW)+VR failure map [59] founds out the list of modes of operator error, modes of maintainer error and failure modes of Mechanism for the hoist of rotor's arrow.

1. List of modes of operator errors, n=1,2:

- The operator often turns on mechanism for the hoist of rotor's arrow,
- The operator often turns on mechanism for the hoist of rotor's arrow when the excavator is on ground level.

2. List of modes of maintainer error, m=1,2,3:

- Maintainer has not properly performed assembly of the coupling at the small group generator,
- Maintainer has not made centering of electric motors precisely,
- Maintainer has not adjusted arrester for car interlocking.

3. List of failure modes of mechanism for the hoist of rotor's arrow, k=1,2,3:

- Breaking at the back gearbox shaft (front-end) for the hoist of rotor's arrow,
- Outage of electric-hydraulic lifter (releaser) at operating brake,
- Mechanical defect of ropes for the hoist of rotor's arrow.

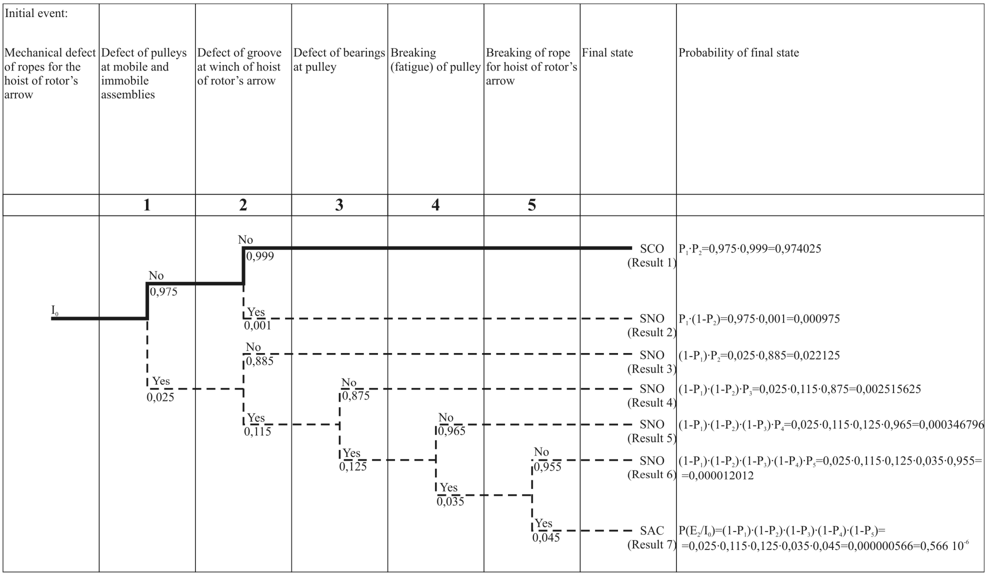
Event tree for the initial event - failure mode of mechanism for the hoist of rotor's arrow, k=3: Mechanical defect of ropes for the hoist of rotor's arrow, is shown in Figure 58.

The probability of occurence of a state of accident scenario realization is:

$$P(E_2/I_0) = (1 - P_i) \cdot (1 - P_2) \cdot (1 - P_3) \cdot (1 - P_4) \cdot (1 – P_5) =$$
$$= 0{,}025 \cdot 0{,}115 \cdot 0{,}125 \cdot 0{,}035 \cdot 0{,}045 = 0{,}566 \cdot 10^{-6}.$$

This result analysis presents final stage of statistical safety analysis. Its content depends (to a great extent) on overall aims of statistical safety analysis. For example, risk calculation results enable solving problems:

- comparison of several system variants (in the safety section),
- showing of principal realization of required safety,
- choice of effective maintenance management process or system.


Initial event:
Mechanical defect of ropes for the hoist of rotor's arrow
Defect of pulleys at mobile and immobile assemblies
Defect of groove at winch of hoist of rotor's arrow
Defect of bearings at pulley
Breaking (fatigue) of pulley
Breaking of rope for hoist of rotor's arrow
Final state
Probability of final state
1
2
3
4
5
I_0
No
0,975
Yes
0,025
No
0,999
Yes
0,001
No
0,885
Yes
0,115
No
0,875
Yes
0,125
No
0,965
Yes
0,035
No
0,955
Yes
0,045
SCO (Result 1)
SNO (Result 2)
SNO (Result 3)
SNO (Result 4)
SNO (Result 5)
SNO (Result 6)
SAC (Result 7)
$P_1 \cdot P_2 = 0{,}975 \cdot 0{,}999 = 0{,}974025$
$P_1 \cdot (1-P_2) = 0{,}975 \cdot 0{,}001 = 0{,}000975$
$(1-P_1) \cdot P_2 = 0{,}025 \cdot 0{,}885 = 0{,}022125$
$(1-P_1) \cdot (1-P_2) \cdot P_3 = 0{,}025 \cdot 0{,}115 \cdot 0{,}875 = 0{,}002515625$
$(1-P_1) \cdot (1-P_2) \cdot (1-P_3) \cdot P_4 = 0{,}025 \cdot 0{,}115 \cdot 0{,}125 \cdot 0{,}965 = 0{,}000346796$
$(1-P_1) \cdot (1-P_2) \cdot (1-P_3) \cdot (1-P_4) \cdot P_5 = 0{,}025 \cdot 0{,}115 \cdot 0{,}125 \cdot 0{,}035 \cdot 0{,}955 = 0{,}000012012$
$P(E_2/I_0) = (1-P_1) \cdot (1-P_2) \cdot (1-P_3) \cdot (1-P_4) \cdot (1-P_5) = 0{,}025 \cdot 0{,}115 \cdot 0{,}125 \cdot 0{,}035 \cdot 0{,}045 = 0{,}000000566 = 0{,}566\ 10^{-6}$

Legend:
No – Without unwanted event
Yes – unwanted event happened
SCO - state of capability to operate
SNO - state of noncapability to operate
SAC - state of accident.

Figure 58. Event tree for initial event Mechanical defect of ropes for the hoist of rotor's arrow

For solving this problem it is necessary to compare risk values R(I_0), calculated for several system variants and choose the one where the risk value is minimal. Solving of the second problem is connected with comparison of calculated risk value R(I_0) with criterion risk value. For solving the third problem of special importance is that with inadequate operation maintenance safety must not be endangered, which causing accidents states of excavator items. Any state of accident results in endangered health and life of personnel and great economic losses expressed through cost of reengineering and repeated starting of the bucket wheel excavator.

Chapter 11

MAINTENANCE CONCEPTS

11.1 BALANCED APPROACH TO MAINTENANCE

Defining the maintenance concept of the systems is a central place in the maintenance system. Terms of system utilization indicate that the maintenance activity is organized by service which, above all, must be flexible, i.e. ready to adjust its plans and processes daily according to emerged circumstances. It has to be able to make preparations and achieve maximal involvement in the performance of maintenance tasks in short period of time [11,60]. Flexibility of maintenance service is particularly reflected in its ability to perform its job of preventive maintenance during the technological systems breakdown. Therefore, maintenance service has to subordinate its work to primary goal, as to achievement of maximal systems effectiveness along with lower maintenance cost, Figure 59.

Today there is necessity for balanced approach to maintenance using a combination of appropriate corrective, preventive, predictive and proactive maintenance concepts, Figure 60. Thereat these concepts should not be independent, but integrated into singular maintenance concept. Effective maintenance concept of the system could be reached through their appropriate combination, starting from certain advantages and disadvantages of different maintenance concepts.

Regards to each new maintenance concept provides new opportunities for further development and creating conditions for better functioning of the system, it is necessary to analyze each specific maintenance concept, with a comprehensive analysis of possible applications of modern concepts, based on existing experiences and research results. Application of any maintenance concept is very important for users of systems which must operate with a high effectiveness and safety degree.

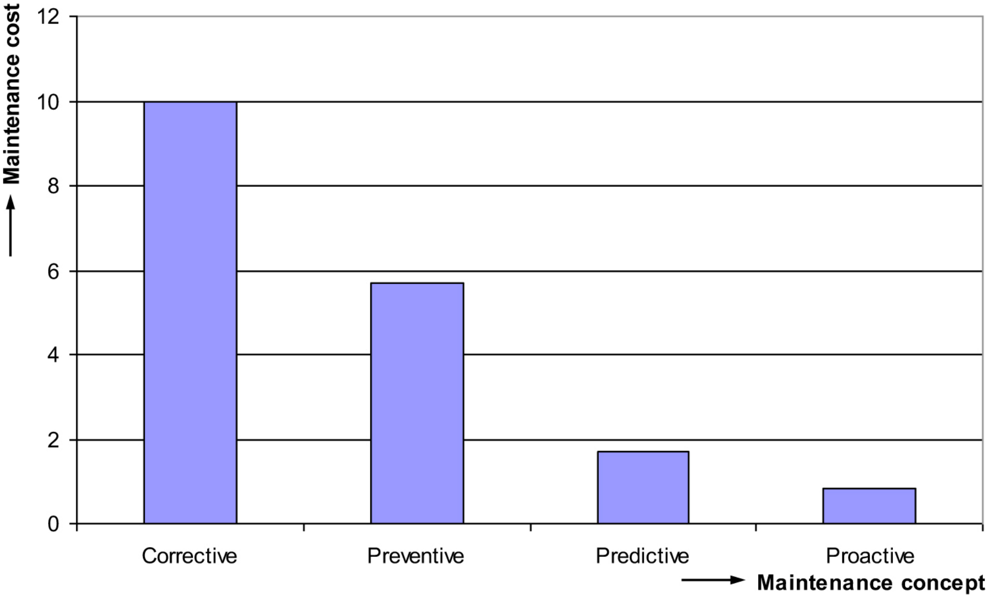


Figure 59. Maintenance concepts and relative maintenance cost

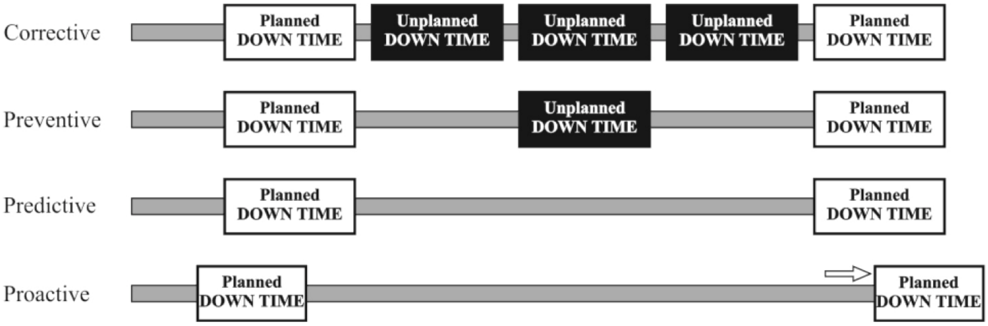


Figure 60. Maintenance concept comparison

11.2 CORRECTIVE MAINTENANCE

Corrective maintenance concept has dominated long period of time, whereas its costs are relatively high due to unplanned breakdowns, system damages and overtime work. In this maintenance concept, management and maintenance service only anticipate the real condition of the system. Therefore, it is practically impossible to plan the needs of maintenance, nor predict the availability of the system. Operation to failure concept, as the other name of this concept is, should be only a small part of modern maintenance programs, because in some situations, however, it makes sense to apply this concept. As an example we can use a plant where a large number of similar machines work, whose repair or replacement is not expensive. When a machine fails, other is starting, and plant is not in the long breakdown.

11.3 PERIODIC PREVENTIVE MAINTENANCE

Periodic preventive maintenance concept is the progress in relation to the operation to failure concept. This concept is sometimes called the maintenance based on the history. This means that history (the previous behavior) of each system is analyzed, periodic maintenance is planned to prevent the appearance of the statistically expected problems. It is well known from the reliability analysis that most groups of similar machines would evince the failure rate (obtained on the basis of behavior monitoring in a long time), whence appearance of adverse events could be predicted. Examples for this are machines exposed to wear depending on durability (e.g. breakers), as well as machines exposed to corrosion (e.g. machines working in aggressive environments). Periodic preventive maintenance includes activities such as lubricants and filters replacement, periodic cleaning and inspection, etc. This concept activities can be planned on the basis of: the calendar time (the so-called calendar based maintenance), machines working hours, the number of manufactured parts, amount of excavated overburden or coal, etc.

11.4 PREDICTIVE MAINTENANCE

Transition to predictive maintenance concept it was next maintenance concept improvement. The concept is based on determination of machine state during its operation. This concept was called maintenance on the base determined condition, so that is:

PREDICTIVE MAINTENANCE = CONDITION BASED MAINTENANCE.

Predictive maintenance concept is based on the fact that the majority of machine parts or assemblies will evince a kind of warning (symptoms) before failure. Reading these symptoms, which warn machine operator or mechanic, requires several types of nondestructive testing, such as: oil analysis, wear, particle analysis, vibration analysis, shock pulse analysis, temperature measurement, etc. The application of these tastings for determining the state of machine results in significantly more successful maintenance in relation to possibilities of previous maintenance concepts. Predictive maintenance allows management to control excavator items, and other technological equipment and the maintenance program in open pit mine fields. The company which uses predictive maintenance, excavator item operative state is known at any time. This allows much more precise maintenance scheduling. This excavator item maintenance concept uses different techniques, whereof the most important are: periodic vibration analysis, stress state analysis, analysis of temperature and torque analysis.

In machines that are subject to continuous vibration monitoring, the alarm announces as soon as the vibrations increase over pre-determined level. In this way, the spread of failure is prevented. It is proven in a number of papers that in comparison to other techniques of nondestructive testing, vibrations data analysis provides the most information about the system parts and assemblies state [61]. Analysis of oil and particles caused by wear are important elements of modern planning programs, especially in critical or very expensive technological equipment. Thermography is the measurement of surface temperature by infrared detection and of great use in the problems detection in electrical installation (switches), as well as in other parts with difficult access. Motor circuit curve analysis is a very useful technique for detection of cracked or broken rotor bars, and during the motor working. Also, electric motor stator testing by electric strokes can be used for initial phase of isolation failure detection.

The basic advantage of predictive maintenance of mechanical and electrical equipment is the higher availability and reliability, thanks to longer Up Time and shorter Down Time, as shown in the Figure 61. Time trend of failure development in the machines can be carefully monitored and maintenance tasks can be planned on that basis. This can be achieved by dynamic and process parameters monitoring and data exchange with programmable logical controllers (PLC). That contributes to technological equipment maintenance cost reduction.

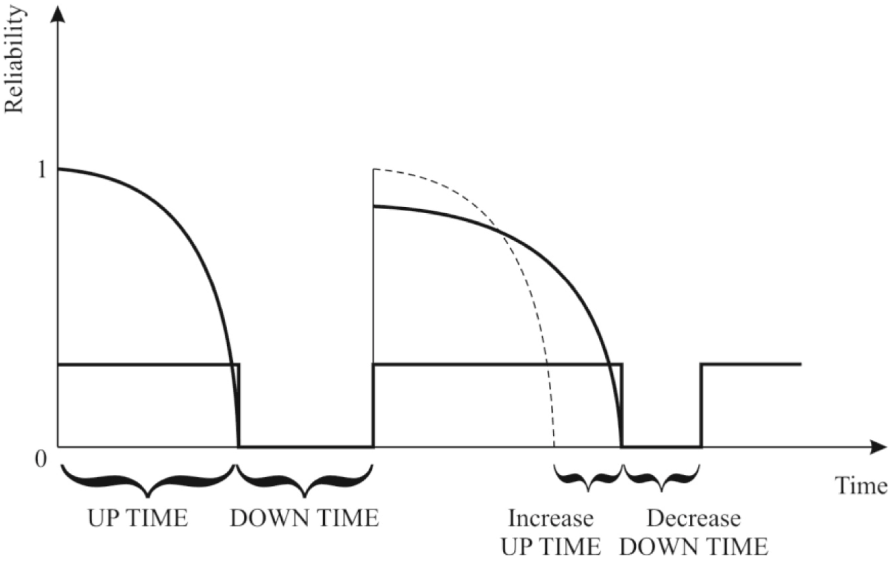


Figure 61. With systems predictive maintenance advantage defining

Numerous projects reports from different industrial branches state the equipment productivity increase for 2-10% based on the predictive maintenance application [62]. Next predictive maintenance benefit is of the spare parts and labor cost reduction. Repair of machine which failed during the operation can be up to ten times more expensive than planned repair of the same machine. A large number of new machines fail soon after commissioning because of the failures that occur in trial operation period or incorrect installation or improper inspection. Predictive maintenance techniques can be used in order to provide a valid machine commissioning. Many plants condition new installed equipment take-over on the basis of confirmation from vibrations measurement. Predictive maintenance reduces machines accident occurrence probability what improves occupational health.

11.5 PROACTIVE MAINTENANCE

The so-called proactive maintenance, which includes various methods and technologies for maximal reducing of corrective maintenance in practice, is innovation in relation to predictive maintenance concept [62]. Basic part of proactive maintenance concept is the mechanisms of failure causes analysis, based on the Failure Modes, Effects And Criticality

Analysis (FMECA) method. Applying this method, the main machines failure causes can be eliminated, so that is:

PROACTIVE MAINTENANCE = PREDICTIVE MAINTENANCE + FMECA.

Successful proactive maintenance over time due to corrective measures, primarily through project-engineering activities and system reengineering, allows removal of the adverse events causes, which result with UP TIME or states of accident. One of the most important properties of this maintenance concept is that its techniques can easily be added to the existing maintenance concepts.

11.6 LEAN MAINTENANCE

The base of scientific approach of the Toyota Company consists of asking question "Why" 5 times when discovering a problem, which is marked as "5 Why?". If you get answer five times to the question "Why?", then the root cause of the problem and the way of solving it will be clear [63]. Analysis of root causes of maintenance problem based on five times repetition of the question "Why?" is implemented in the maintenance system of the Toyota Company as well [64]. Method "5 Why?" is devoted to detailed problem and culture research, which lead to root causes of all these problems. Method "5 Why?" is usually used in Toyota for tracing source of maintenance problems.

11.7 SAFETY BASED MAINTENANCE

Technical system safety is a characteristic of a system to prevent appearance of the risk, that is, the appearance of the undesirable events (critical failures) with catastrophic effects to human health and life, the environment and economic activities [65]. Safety of the technical systems, in essence, represents their abilities to avoid failures which could harm the population and/or the environment or to do considerable economic damage. Excessive loads and effects, mistakes of personnel, intentional actions of men can be also the sources of the increased risks. Safety techniques, increases and safety prognosis are much analogous to the adequate methods - techniques relations to the reliability of the technical systems [62]. However, there are three specific characteristics which require special approach to the safety problem. First, the degree of ability to avoid failures must be high so that the failures and another deficiencies, which disturb safety should be very rare. Second, many catastrophic failures come as the effects of the natural or the anthropological origine, like earthquakes, floods, hurricanes, storms. These events are rare and practically unpredictable and information about their reappearances (frequencies) and intensities and other parameters are extremely indefinite or unreachable in principle. Third, many critical failures (the ones which cause damages, but damages-catastrophes) do not appear because of imperfection of the system but owing to the human factor. This statement is confirmed by analysis done as at the big catastrophes, so also at statistics of small but critical failures.

There is no absolute safety (as well as the absolute ability to avoid failures - reliability). It is always present the probability, different of the null, that the failure with serious effects will happen in the observed final time interval, for example, during the determined utilization. That probability is named - the risk.

Moving to the risk characteristic, as the probability of some extremely undesirable events there are [65]:

- risk when the catastrophic failure of the technical system can occur (ruin risk of the building or the object, melting of the active phase of the nuclear reactor, breaking of the main gas line or oil pipeline, etc.),
- risk to which each individual person is exposed (risk for the builders, miners, operators at the nuclear power plant, pilots etc.).

The first group risk is conditionally called - the structural risk, and the risk from the second group is called the individual risk. Then, the general risk depends on number of people exposed to some definite risk, and the fatal risk, which means - death of people.

This classification includes also the ecological and business risks [65]. The ecological risk estimates the damage degrees, - the direct and the indirect ones. The business risk represents the damage risk which could be done to the environment, to the natural and historical conditions, as well as to the business activities.

A long time, the main scientific and practical discussions were oriented towards achievement of the most important characteristics of improvement (effectiveness, capacity and speed increase, new materials and technology development), without taking into account system accidents and disasters occurrence risk. This led to the fact that practically all industrially developed countries were showed unprepared for the difficult social, economic and environmental consequences of accidents and disasters, increasing by number and consequences severity [54,65]. At the same time, the human made systems which are doubtless hazard to people and the environment, in most cases are created using traditional design principles (sequential design) and simplified engineering methods of tests planning (sequential engineering) [66].

This required, in the last decade of the twentieth century, establishment of new principles and concepts of system safety assurance based on concurreng engineering approach [14,67], as shown in the Figure 62. At the same time, undoubtedly, the basic requirement of safety assurance concept, consist of accidents elimination, is generally accepted. In fact, the large system accidents cause maximum injury. On the other hand, the total accidents and disaster injury depends a lot on system item's failure mode. Therefore, it proved to be useful the inclusion of adequate maintenance concept principles in system safety assurance concept.

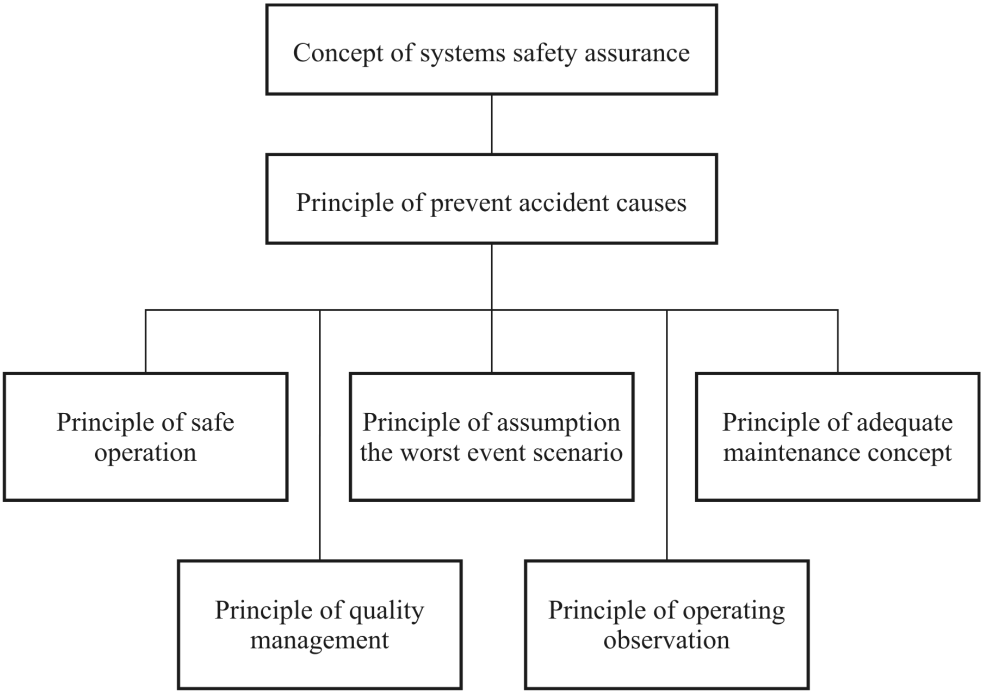

Concept of systems safety assurance
Principle of prevent accident causes
Principle of safe operation
Principle of assumption the worst event scenario
Principle of adequate maintenance concept
Principle of quality management
Principle of operating observation

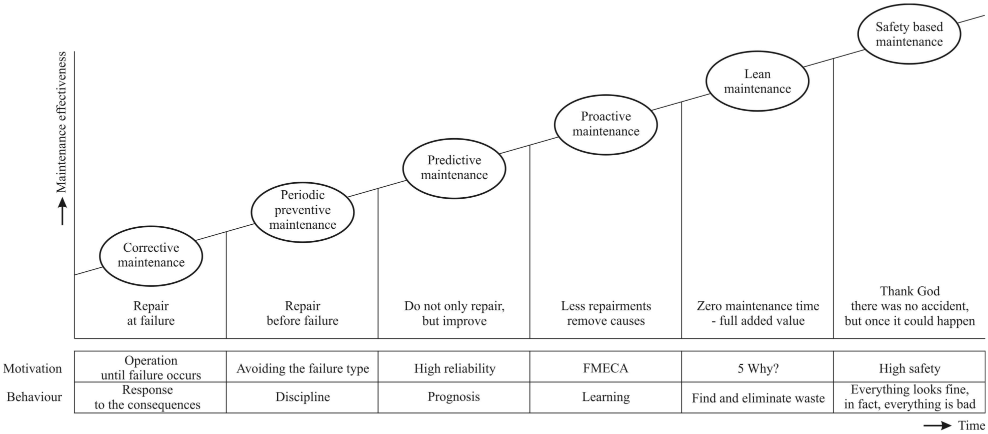
Figure 62. Systems safety assurance concept

Safety based maintenance concept consider, primarily, risk degree, i.e. possible injuries caused by failure modes during system operation. Methods of safety analysis and risk evaluation aim to identify and quantify areas with a potentially possible appearance of system accident state Well-conducted risk evaluation is a prerequisite for the selection of an adequate system maintenance concept.

11.8 EFFECTIVE MAINTENANCE CONCEPT

Systems maintenance successfulness is highly dependable on maintenance concept used. In order to increase maintenance effectiveness, some appropriate maintenance concept cannot be applied as such, it has to be created and adopted according to actual situation on site. Some authors of the significant projects on the matter [59] consider it to be wrong to bind maintenance concept with only one term (corrective, preventive, periodical, predictive, proactive) and identify it as such. More important is what is actually going on in specific maintenance task, what are the procedures used, resources, personnel (competence, education, equipment, organization, motivation). Possible number of applied maintenance concept variants is very large, and therefore it is necessary to choose the most appropriate one.

According to previously stated it can be concluded that once chosen maintenance concept is not to be used for ever, it is rather to be changed and adapted according to most up to date scientific and technological knowledge, changes in operational and near surrounding and results of adopted maintenance concept results, according to general recommendations shown in Figure 63.



	Repair at failure	Repair before failure	Do not only repair, but improve	Less repairments remove causes	Zero maintenance time - full added value	Thank God there was no accident, but once it could happen
Motivation	Operation until failure occurs	Avoiding the failure type	High reliability	FMECA	5 Why?	High safety
Behaviour	Response to the consequences	Discipline	Prognosis	Learning	Find and eliminate waste	Everything looks fine, in fact, everything is bad

Figure 63. Maintenance concept development phases

Effective maintenance concept of the system has been developed and proposed on the basis of universal possible usages analysis of corrective, periodically preventive, predictive, proactive, lean and safety based maintenance concepts in modern conditions. Starting from certain advantages and disadvantages of each concept, effective maintenance concept of the system was reached by balanced approach, i.e. their appropriate combination [68]. However, it has been indicated that traditionally used systems reliability characteristics are not sufficient for complete description of their effectiveness. It was established as a reason that reliability characteristics do not indicate function disturbance level during system operation. It is suggested on new safety assess indicators adoption in system operation stage based on disturbance sequence modeling. It is very important that inappropriate maintenance concept must not put under question safety, i.e. cause system accident condition. Any accident condition would result with staff health and life threats and great economical losses through reengineering and system launch costs. Because of that safety based maintenance concept was consided in this work.

Chapter 12

RELIABILITY TERMINOLOGY

12.1 RELIABILITY TERMS AND DEFINITIONS

Many definitions are taken or paraphased from the following documents:

[69] Tracy Philip Omdahl, editor: Reliability, Availability and Maintainability (RAM) Dictionary, Quality Council of Indiana, West Terre Haute, 1988, 360 p.

[70] Robert Dovich, Bill Wortman: CRE Primer, Council of Indiana, West Terre Haute, 2002, 748 p.

Availability: A measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at an unknown (random) time.

Bathtub Curve: Description for the appearance of the classic and often oversimplified graph which ploth time or cycles against the life-cycle failure rate and/or hazard rate, which dependent on time or cycles. Accounts for the change in failure rates and hazard functions over the system life cycle, from high at first, to lower, then to high at the end of life.

Burn-in: The operation of an item under stress to stabilize its characteristica.

Calibration: A comparison of a measuring device with a known standard.

Checkout: Tests or observations of an item to determine its condition or status.

Element: Functional part of a system or equipment that is essential to operational completeness of the subsystem or equipment. It may consist of a combination of:

- accessories,
- assemblies,
- attachments,
- parts.

Corrective action: A documented design, process, procedure or materials change implemented and validated to correct the cause of failure or design deficiency.

Criticality: A relative measure of the consequence of a failure mode and its frequency of occurences.

Data Collection: Creating a history of relevant events, conditions, parameters, values and other details necessary to adequately measure an aspect of system effectiveness in laboratory and/or field testing. Includes:

- failure analysis records,
- failure reports,
- reliability group test record,
- test records,
- element repair tags.

De-Bugging: A process to detect and remedy inadequacies. Not to be confused with term such Burn-in, Fault Isolation or Screening.

Degradation: A gradual impairment in the ability to perform a specified task or mission. Gradual deterioration in performance as a function of time and/or stress. Decreasing mechanical or electrical strength.

Dependability: A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during specified mission profile, given item availability at the start of the mission.

Diagnosis: The functions performed and the techniques used in determining and/or isolating the cause of malfunctions. Identifying and defining a condition by evaluating its symptoms.

Diagnostic: A software function to detect, discover and futrher isolate an equipment malfunction or a processing error. Pertaining to detection and isolation of a malfunction or mistake. A message generated by a computer program indicating possible faults in another system element, for example, a syntax fault flagged by a compailer. Pertaining to the detection and isolation of faults or failures.

Disassemble: Opening an item and removing a number of parts or subassemblies to make the item that is to be replaced accessible to removal. This does not include the actual removal of the item to be replaced.

Downing Event: The event which causes an item to become unavailable to initiate its mission (the transition from Up-Time to Down-Time).

Durability: A measure of useful life (a special case of reliability).

Element: Constituent part of anything. Includes:

- assembly,
- part,
- set,
- subassembly,
- element.

Dynamic Reliability Model: A model in which reliability is time or usage dependent. Contrast with Static Reliability Model. Examples include:

- parallel,
- series,
- shared load parallel,
- standby redundant.

Environment: The aggregate of all external and internal conditions (such as temperature, humidity, radiation, magnetic and electric fields, shock vibration, etc.) either natural or man made or self-induced, that influences the form, performance, reliability or survival of an item.

Early Life Period: Period of equipment life starting just after final assembly, when initial equipment failures occur at a higher than normal rate due to presence of defective parts, poor workmanship and abnormal operating procedures. A system's performance for a break-in usage period after delivery and during which failures are expected and more tolerablethan later. The period of an item's life cycle including the Installation Period. Contrast with Useful Life and Wearout Life. Also called Burn-in Period.

Error: Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition, for example, the difference between a multilated message and the original message. Mild term for mistake. Human action that results in a fault. Includes in a design specification:

- incorrect translation of a requirement,
- misinterpretation of user requirements,
- omission of a requirement.

Error Human: Categories include:

- contributing error,
- design error,
- fabrication error,
- handling error,
- human boredom,
- inspection error,
- maintenance error,
- operator error.

Event Tree: A decision theory technique that lists all possible actions one might take in a situation and their consequences. This is useful to help chose between various courses of action. This subdivides the system into elements and evaluates consequences of failure. Event trees give a forward looking logic by describing hypothetical causes of potential accidents.

Event Tree Analysis is contemporary Bottom-Up method of logical modeling for operation and failure because of response (reaction) investigation starting from initial event, and presentation of subsequent events and consequences temporal (chronological) courses. This analysis method is being exploited for probabilities appraisal and system operation or failure consequences that emerge because certain initial event occurred.

Failure: The event or inoperable state, in which any item or part of an item does not perform as previously specified.

Failure Activating Cause: Stress or forces, such as shock or vibration, which induce or activate a failure mode.

Failure Analysis: Subsequent to a failure, the logical systematic examination of an item, its construction, application and documentation to identify the failure and determine the failure mechanism and its basic course.

Failure Catastrophic: A failure that can cause item loss.

Failure Critical: A failure or combination of failures, that prevents an item from performing a specified mission.

Failure Dependent: A failure which is caused by the failure of an associated item. Not independent.

Failure Effect: The consequence(s) a failure mode has on the operation, function or status of an item. Failure efforts are classified as local effects, next higher levels, and end effects.

Failure Independent: Failure which occurs without being caused by the failure of any other item. Not dependent.

Failure Mechanism: A physical, chemical, electrical, thermal, or other, process which results in failure.

Failure Mode: The consequence of the mechanism through which the failure occurs, i.e., short, open, fracture, excessive wear.

Failure Mode and Effects Analysis (FMEA): A procedure by which each potential failure mode in a system is analyzed to determine the results or effects of those failure modes on the system and to classify each potential failure mode according to its severity. The procedure has three main steps:

- document all probable failures, create functional and reliability block diagrams, define system missions and environments;
- determine the effect of each failure on system operation, documenting compensating methods for each failure mode, failure detection methods;
- identify single-point failures, documenting and identifying emaining problems, corrective action effect, corrective design.

Failure Mode, Effects and Criticality Analysis (FMECA): A procedure including Failure Mode and Effects Analysis, but subsequent to it, to clasify each potential failure effect according to its severity. This includes documenting Catastrophic and Critical failures.

Failure Probability: Probability of failure in a given time or usage period. Unreliability.

Failure Random: A failure whose occurrence is predicable only in a probabilistic or statistical sense. His applies to all distributions.

Failure Rate: The total number of failures within an item population, divided by the total number of life elements expended by that population, during a particular measurement interval under stated conditions. The number of failures of an item within the population per element measure of life in terms such as cycles, time, transactions, computer runs or some other stressful usage. During the useful life period, failure rate is often considered constant for an exponential element. The rate at which failures occur in the interval between two times.This is the ration of the probability that failure occurs in the interval between the two times, given that is has not occurred prior to the beginning time, divided by the interval length. In reliability modeling, the ratio of the number of failures of a given category or severity to a given period of time. For example, failures per hour of execution time or month.

Failure Reporting Analysis and Corrective Action System (FRACAS): A closed loop system of data collection, analysis and dissemination to identify and correct failures of a system or process. A formal management economic information system including at least five distinct and basic sequential and iterative functions:

- recording data about individual failure incidents at first, often manually later, oftn automatically on a formal failurereport from or data structure,
- reporting data to an analysis group of engineers members who are responsible to do something about each failure,
- analysis of individual failures or series of related failures to discover the causes of failures to recommend or initiate corrective action,
- forwarding engineering oriented correction plans once the cause of failure is known to functional groups responsible for taking corrective action,
- checking on corrective action adequacy to see if further action is required close the loop on the initial failures revise and repeat corrective action if necessary.

Failure Symptom: Any circumstance, event or condition perceived at any level of observation as a result of a failure and which indicates its existence or occurrence, but which is not the root cause. Often Failure effect.

Fault: Immediate cause of failure (e.g., maladjustment, misalignment, defect, etc.). An accidental condition that causes a previously functional element to fail to perform its required function. A manifestation of an error in software. Sometimes called Bug. The hypothesized or identified cause of an error or of a failure. Often classified based on duration, extent, value and whether the cause was physical or human. A degradation in performance due to:

- hardware: defect, detuning, failure of parts, maladjustment, misalignment;
- software statement: incorrect, missing, unnecessary.

Fault Isolation: The process of determining the location of a fault to the extent necessary to effect repair.

Fault Localisation: The process of determining the approximate location of a fault.

Fault Tolerance: System characteristic which maintains prescribed functions or services to End users and Intermediate users, despite the existemce of a fault or faults. Fault avoidance technology, the other category of High reliability technology, is not included in this definition. In a very strict sense, complete tolerance of a system to a fault or faults. The designed-in capability of a system to continue correctly executing in the presence of a limited number of hardwarenor software faults. Survival attribute of a system that allows it to deliver its expected service after faults have manifested themselves within in. For software, making programs that have errors be able to continue to function despite the errors by confinig, detecting and recovering tchniques similar to hardware and also Dual programming. Using redundancy to provide alternate signal or information to negate the failure effect.This is done by providing extra retry/execute time or extra elements. Extra elements implies all hardware necessary to supply the extra signal or information to guard against the effect of failures. Extra time may imply resources or required actions to:

- confine,
- detect,
- diagnose,
- mask,
- reconfigure,
- recover,
- reintegrat,
- repair,
- restart,
- retry.

Fault Tree: A graphical representation showing the logical relationships among fault events. It is a consise and orderly description of the various combinations of possible fault events within a system which could result in some predefinrd or undesirable safety event for the system. This graphic form allows ready identification and mathematical evaluation of the impact of these fault events to measure system safety.Constructed using the binary logical downward development of the Top event into its contributing fault events. Each fault event results in a branch containing more basic events. The tree is complete when all events are developed down to the level of primary failures.

Fault Tree Analysis (FTA): A top-down approach to failure analysis starting with an undesirable event called a Top event, such as a failure or malfunction and then detemining all the ways it can happen. Contrasts with a Failure Mode and Effects Analysis which is a bottom-up approach. FTA is often called a "backwards" FMEA, in that the logic proceeds fom failure effects of interest to discover possible causes, rather than from all ccauses of possible failure to discower possible effects. An analytical tool to:

- identify and properly relate all reasonably probable events which could result in substantial damage to a system, loss of a system, safety critical condition;
- assess the effect on system safety of design or environmental changes,
- use symbols representing conditions which may cause system failure,
- math model probability of occurrence of an undesirable Top event,
- identify potential safety hazarda,
- communicate and support trade-of, system design adequacy decisions,
- recommend corresponding corrections.

Fault Tree Sumbols: Two kinds of symbols used in a Fault Tree, logic symbols and event representation symbols:

- bollean logic symbols: AND, OR, priority AND, exclusive OR, delay and inhibit gates,
- event representations:

- circle (primary failure event whose probability is derived empirically),
- diamond (event whose possible causes are intentionally not developed due to insignificance of, or lack of empirical data),
- double diamond (a simplified fault tree event resulting from identified but not displayed version of the fault tree),
- elipse (a conditional event indicating any gate condition or restriction),
- house (event that is expected to occur during normal operation),
- inverted triangle (a transferred event is identical in function but includes one or more different events in the second location),
- rectangle (a fault event resulting from fault or failure events combining through a logic gate),

- triangles (a transfer in, when from above, or transfer out, when from the side),
- upright triangle (an event transferred to another part of the fault tree is the same event in both locations).

Human Factor Engineering: Engineering treatment of a complex equipment design a a unified man-machine system in order to minimiye errors. It considers the quantitative influence of the operator, maintenace specialist and training for both, on the system performance, reliability and maintainability. Also called Human engineering.

Human Failure: The inability of the user or operator of an item to initiate a correct, required or specified action or response needed to allow the continuous or correct function of the item.

Human Failure Modes: Failure modes of human performance which result in system failure effects. Includes:

- failure to perform the task:
- at all,
- completely,
- correctly,
- partly,
- within the alloted time.;
- performing some task out of sequence which should not be performed.

Human Reliability: The probability that a human crew or operator will complete a task successfully or commit no errors that would cause item failure under given conditions and in a specified minimum period.

Inherent Reliability: The potential reliability of an item or potential in its design under realistic and/or stated conditions of use and operation.

Installation Period: A specific period at the beginning of Early Life during which arrival quality, installation quality and system performance requirements may be measured during a specified period after customer acceptance.

Item: A non-specific term used to denote any product, including systems, materials, parts, subassemblies, sets, accessories, etc. Element of material or software at any level of assembly. A term that is intentionally not specific and may denote any system. Include:

- accessory,
- element,
- set,

- software,
- subassembly,
- subsystem,
- system.

Life Elements: A measure of the duration of use applicable to the item. Examples include:

- attempts to operate,
- cycles,
- distance,
- operating hours.

Logistic Support: Methods by which support materials are supplied to the service and support effort. Related items considered include:

- geographic considerations,
- inventory,
- personnel,
- service parts,
- test equipment,
- transportation.

Maintainability: A System Effectiveness concept that measure of the ability of an item to be retained in or restored to operating condition in a specified interval of Down Time. The probability that an item of hardware or software will be retained in, or restored to, specific condition within a given period of time, when maintenance is initiated and performed in accordance with prescribed procedures and resources by personnel having specified skill levels, using prescribed procedures and resources. It is a characteristic of:

- adequacy of maintenance procedures test equipment,
- environment under which maintenance is performed,
- equipment design and installation,
- personnel available in the required skill levels.

Maintenance: All actions necessary for retaining an item in or restoring it to a specified condition. Making an already produced item conform with its original specification. Overoming deterioration of systems caused by experiences in life, environment and performance, in order to increase System effectiveness. The ongoing function of keeping hardware and software functional elements, items or equipment in, or restoring them to, serviceable condition. It includes combinations of any Corrective and Preventice actions.

Maintenance Action: An element of a maintenance event. Any task necessary to retain an itam in, or restore it to, a specified condition. May consist one or more tasks (i.e., fault localisation, fault isolation, servicing and inspection) necessary to retain in or restore an item to a specified condition.

Maintenance Condition Based: Preventive maintenance of an item that is prompted by a knowledge of its condition as determined from routine or continuous testing.

Maintenance Corrective: All actions performed as a result of failure, to restore an item to a specified condition. Corrective maintenance can include any or all of the following steps: localization, isolation, disassembly, interchange, re-assembly, alignment and checkout.

Maintenance Event: One or more maintenance actions required to effect corrective and preventive maintenance due to any type of failure or malfunction, false alarm or scheduled maintenance plan.

Maintenance Plan: A document that identifies the managementn and technical approach that will be used to maintain a system. Typically describes:

- facilities,
- resources,
- schedules,
- tools.

Maintenance Preventive: All actions performed in an attempt to retain an item in specified condition by providing systematic inspection, detection and prevention of incipient failures. All actions performed on a specific, periodic and planned schedule to retain an item in specified working condition through checking and reconditioning. Also called Perodic maintenance and Scheduled maintenance. Contrast with Corrective Maintenance.

Maintenance Ratio: A measure of the total maintenance manpower burden required to maintain an item. It is expressed as the cumulative number of man-hours of maintenance expended in direct labor during a given period of the life elements divided by the cumulative number of end item life elements during the same period.

Maintenance Scheduled: Preventive maintenance performed at prescribed points in the item's life.

Maintenance Specialist: The individual who performs Preventive maintenance and also responds to a user's service call to a repair facility and performs Corrective maintenance on a device or system. Interchangeable terms referring to the same person or function are:

- customer engineer,
- field engineer,
- maintenance person,
- mechanic,
- repair person,
- service person,
- technician.

Maintenance Task: The maintenance effort necessary to retain an item in, change it to, or restore it to a specified condition.

Maintenance Time: An element of Down Time which excludes modification and delay time. Ptreventive and corrective time required for hardware and/or software maintenance which takes the equipment out of service.

Maintenance Unscheduled: Corrective maintenace required by item conditions.

Mean Time Between Failure (MTBF): A basic measure of reliability for repairable items: The mean number of life elements during which all parts of the item perform within their specified limits, during a particular measurement interval under stated conditions.

Mean Time Between Maintenance (MTBM): A measure of the reliability taking into account maintenance policy. The total number of life elements expended by a given time, divided by the total number of maintenance events (scheduled and unscheduled) due to that item.

Mean Time Between Removals (MTBR): A measure of the system reliability parameter related to demand for logistic support: The total number of system life elements divided by the total number of items removed from that system during a stated period of time.

Mean Time To Failure: A basic measure of reliability for non-repairable items: The total number of life elements of an item divided by the total number of failures within that population, during a particular measurement interval under stated conditions.

Mean Time To Repair (MTTR): A basic measure of maintainability: The sum of corrective maintenance times at any specific level of repair, divided by the total number of item failures during a particular interval under stated conditions.

Mean Time To Restore System (MTTRS): A measure of the system maintainability parameter, related to availability and readiness: The total corrective maintenance time, divided by the total number of events, during a stated period of time (Excludes time for off-system maintenance and repair of detached elements).

Mechanism of Failure: The original defect which initiated the item failure. The physical process by which a degradation proceeds to the point of failure. Identifies:

- electrical weakness,
- internal defects,
- nature of external stresses leading to failure,
- quality defects,
- structural defects.

Minimal Cut Sets: In a Fault Tree Analysis, a set of primary failure events, inhibitory conditions and/or undeveloped faults that must all occur in order for the Top Event to occur. Most fault trees will have many different cut sets. Each minimal cut set represents a mode by which the Top Event can occur.

Minimal Path Set: In a Fault Tree Analysis, a Path Set which cannot by any furter reduced yet still remain a path set.This set is determined from the Dual Event Tree using the Minimal Cut Set agorithm to find its minimal cuts.

Mission Profile: A time-phased description of the events and environments an item experiences from initiation to completion of a specified mission, to include the criteria of mission success or critical failures. Chronological description, from start to finish, of all usage and operation cycles which a system must perform throughout the life cycle for which its reliability is to be specifie. Includes all:

- criteria to judge success or failure,
- modes of an item's tasks or missions,
- operation requirements,
- significantly different system environments,
- tas lengths.

Model: An approximate mathematical representation that simulates the behavior of a process, item or concept such as failure rate, in order to increase understanding of, and control over, the system.

M-of-N Systems Model: A generalization of the Parallel rule of unreliability which requires a minimum number "m" of the "n' total original identical parallel modules to function correctly in order for the system to function correctly. It will function as long as "n" minus the number of failures is less than "m". Also called R-out-of-N redundancy and K-out-of-m element system.

Not Operating: Condition of a device that has none of the electrical or mechanical stresses inherent in the active state of that device for which it is designed. It may, however, have stresses from the environment in which it is installed, transported, handled or stored. The state wherein an item is able to function but is not required to function. Not to be confused with Down Time.

Operable: The state of being able to perform the intended function.

Parallel System: A system in which only failure of all items in parallel will cause system failure. Contrast with Series system.

Predicted Reliability: That reliability which is expected at some future date, postulated on analysis of the design and the predicted Mean Time Between Failure or the probability of survival. The estimateg reliability of finaly developed and operable equipment. This value may exclude infant mortality and maximize reliability by assuming that equipment will be operated within design limitations and before wearout.

Probability of Failure: Unreliability. Probability that equipment will fail. The numerical conpliment of Reliability.

Probability of Success: Reliability.

Probability Paper: Paper with special grids intended to facilitate plotting probability distributions. Papers especially useful in reliability include those for distributions such as:

- beta,
- binomial,
- normal,
- Weibull.

Random Failure: Any failure whose cause and/or mechanism make its exact time of occurrence unpredictable, for all practical purposes, but which may be anticipated in a probabilistic or statistical sense. The statistical nature of the randomises should be proven in order for the failure to be classified as random. A failure conforming to the exponential failure law. Occasional failures during Useful life, after Early life when final efforts have been made to eliminate design deficiencies and remove unsound elements and after early manufacturer, serviceperson and user learning but before wearout becomes a factor or Wearout life.

Random Sample: A selection of observations of a phenomenon sampled in such a way that each chosen observation has the same probability of selection as every other observation of the phenomenon.

Random Variable: A quantity whose outcome depends on a probability distribution.

Redundancy: The existence of more than one means for accomplishing a given function. Each means of accomplishing the function need not necessarily be identical. In an item, existence of twoo or more, but not necessairly identical, ways to perform its function. Provision of more than one element to share a load in order to improve performance, even though any element alone would work but at a lesser performance.Only if correct design considerations are made, when other elements fail, can the duplicated and unfailed element or elements take over. In a database, the storage of the same data item or groups of items in two or more files in case a failure makes one inaccessible.

Redundancy Active: That redundancy wherein all redundant items are operating simultaneously.

Redundancy Standby: That redundancy wherein the alternative means of performing the function is not operating until it is activated upon failure of the primary means of performing the function.

Reliability: The probability that an item can perform its required or intended functions for a specified period of time under stated conditions. Often considered to be a subset of Quality. The probability of a mechanical part strength being greater than the stress for all likely values of the stress. The probability of successful performance. Probability of survival beyond a given time or usage. Ability to perform adequately.

Reliability Assessment: The process of determining the achieved level of reliability of an existing system or system element. An estimate of the achieved reliability calculated using data gathered during tests and performance measurement.

Reliability Assurance: The management and technical integration of the reliability activities essential in maintaing reliability achievements including design, production and system assurance. Deliberate positive measures to provide confidence that a specified reliability will be achieved.

Reliability Block Diagram: A static form of reliability analysis using a functional black box diagram to portray and analyze the reliability relationship of elements in a system. Each element of a system is a box block that is in some way interconnected with or through the other boxes of the system at a desired level of assembly. The basic relationships between elements are depicted as lines that may be:

- dotted, for conditional probabilities,
- parallel, if no redundant element failure causes system failure,
- serial, if single failure results in entire assembly or system failure.

Reliability Growth: The improvement in a reliability parameter caused by the successful learning or correction of faults or deficiencies in item design, manufacture, sales, use or service.

Reliability Growth Management: The discipline of predicting and controlling the rate of change of failure rate due to Learning factors in such a way that the required failure rate is achieved at or before customer delivery. The systematic planning for reliability achievement as a function of time and other resources and controlling the ongoing rate of achievement by reallocation of resources based on comparisons between planned and assessed reliability values.

Reliability Engineering: The science of including those factors in the basic design which will assure the required degree of reliability, availability and maintainability.

Reliability Mission: The ability of an item to perform its required functions for the duration of a specified "mission profile".

Reliability Model: A model to predict, estimate or assess reliability.

Eliability Tests: Tests and analysis which are to measure both the level of reliability of an item and also the dependability or stability of this level with time and use under various environmental conditions.A test to statistically prove that specified System Effectiveness is achieved with specified confidence.

Removal: Regardless of its condition, extracting a:

- element,
- line of code,
- piece of equipment,
- structure.

Renewal: A failure and repair cycle.

Repairable Item: An item which can be restored to perform all of its required functions by corrective maintenance.

Screening: A process for inspecting items to remove those that are unsatisfactory or those likely to exshibit early failure. Inspection includes visual examination, physical dimension measurement and functional performance measurement under specified environmental conditions.

Servicing: The performance of any act needed to keep an item in operating condition (i.e. lubricating, fueling, oiling, cleaning, etc.), but not including preventive maintenance of parts or corrective maintenance tasks.

Series System: System in which failure of any item will constitute a failure of the system and whose reliability is the joint probability of all items in the system not failing, based Lusser's System Law. Contrast with Parallel system.

Severity: The consequences of a failure mode. Severity considers the worst potential consequence of a failure, determined by the degree of injury, property damage or system damage that could ultimately occur. Often used interchangeably with Criticality.

Software: Programs, procedures, rules and associated documentation as opposed to psysical equipment.

Software Failure: Corruption or absence of an expected associated software element. Corruption or absence of an expected soft parameter as a result of eitherdata corruption in memory or data corruption on a peripheraldevice.

Software Fault Detection: Automatic or manual isolation of software faults.

Software Life Cycle: Often represented and managed in a chronological sequence of five phases:

- requirements specifications (systm analysia, preliminary design review),
- design (critical design review, about 60% of all errors are caused here),
- implementation (peer code reviews, about 40% of all errors are caused here),
- checkout (acceptance test, les than half of all errors are usually caught here),
- maintenance or system operation and modification (more than half of all errors are usually caught here).

Software Maintainabiliy: A property of being maintainable that is specified to be present in software to a desired degree. For software to be maintainable these characteristics must be present to some measurable degree:

- modifiable (augmentable, structured),

- testable (accessible, communicative, its usage can be measured, structured),
- understandable (consise, consistent, legible, self-descriptive).

Software Maintenance: Modification of software after delivery to the user. The task of keeping software updated and working properly. This accounts for improvements and changes that are always being made in software. Bugs occur even in long-established programs. May be classified as:

- adaptive; to adapt the system software product to a changed environment,
- corrective; to substitute correct code for errors,
- perfective; to improve performance.

Software Quality: The totality of features and characteristics of a software product that determine its ability to satisfy given needs or conform to specifications. The degree to which software possesses a desired combination of attributes. The degree to which a customer or user perceives that software or software characteristics in use meets his/her composite expectations.

Software Reliability: The probability that software will not cause the failure of a system for a specified time under specified conditions. This is a function of both the inputs to, and use of, the system, as well as the existence of faults in the software. The inputs to the system determine whether existing faults, is any, are encountered. The ability of a program to perform a required function under stated conditions for a stated period of time. The extent to which software can be expected to perform its intended functions in a satisfactory manner. A property of being reliable that is specified to be present in software to a degree. Degree to which a software system both satisfies its requirements and delivers usable services. Software is measurably reliable when it is:

- accurate,
- complete,
- externally consistent,
- operating correctly in all but a tolerably small number of situations,
- robust enough to operating even when its specifications are violated,
- self-contained, with its own:

- diagnostics,
- initialization,
- input checks.

Software Reliability Data: Information necessary to assess the reliability of software at selected points in the software life cycle. Examples include:

- error data and time data for reliability models,
- program attributes such as complexity,
- programming characteristics such as: development techniques used programmer experience.

Software Testing: Testing to determine if a program meets its requirements. May be divided into three categories:

- assurance,
- functional,
- performance.

Spares: Replacement items for failed, broken or otherwise nonfunctional elements of equipment. Those support items tha are an integral part of an end item or system which is considered repairable.

Static Reliability Model: A model using a constant reliability level, or levels, from a preliminary reliability analysis in which a fixed time period is chosen. Black box reliability block diagrams are examples of such models. It is used to determine the possible design configurations and to determine the necessary reliability levels for subsystems and elements. Contrast with Dmanic Reliability Model.

Statistics: The art and science of making sense out of, and quantifying, uncertainty.

Subsystem: A combination of sets, groups and lower level assemblies which both performs an operational function within a system and is a major subdivision of the system. A major secondary or subordinate system or subdivision, usually capable of operating independently of, or asynchronously with, a controlling system and that performs a specified function in the overall operation of a system.

Symptom: Failure effect perceived at a maintenance boundary. The initial indication which causes an item to be considered failed.

System: A composite of equipment, skils and techniques capable of performing or supporting an operational role. A complete system includes all equipmnt, related facilities, material, software, services and personnel required for its operation and support to the degree that it can be considered self-sufficient in its intended operational environment. Generally, an organized, interconnected and unided collection that is self-sufficient in its intended customer operational environment and capable of either performing or supporting an operational function, or both. A complete system may require any or all of the following for its operation and support:

- accessories,
- assemblies,
- complete operating equipment,
- elements,
- equipment,
- material,
- personnel,
- procedures,
- related facilities,
- services,
- skills,
- software,
- techniques.

System Effectiveness: Probability that a system can successfully meet an operational demand within a given time period and when operated under specified conditions. System measures should be carefully tailored to, and agreed upon for, a particular application and cannot be applied indiscriminately.

System Life Cycle: Life Cycle of a particular system. This is a chronological sequence of orderly and interrelated life cycle stages and activities that lead from conception to successful installation, operation and ultimately, to the removal of the system item from further useful service.

System Reliability: The probability that a system, including all its hardware and software subsystems, will perform a required task or mission for a specified time in a specified environment.

System Safety: The optimum safety level attained when engineering and system safety management principles are applied throughout a system life cycle.

Test: A comparison of specifications or expectations to what is actually present. To ascertain the state or condition of an element, device or system. A measurement procedure providing enough information to allow determination that a set of tested elements functions properly. To compare a standard response to an item's response when appropriate stress or energy is applied. To establish or increase confidence that an item performs as specified by exercising it and comparing the results to the required results.Contrast with Debug.

Test Acceptance: A test conducted under specified conditions by or on behalf of a customer using delivered or deliverable items, in order to determine the item's compliance with specified requirements. Formal test to determine whether an item satisfies its Acceptance Criteria and to enable an actual or hypothetical customer to determine whether to accept the item. Testing that users require as a condition before they accept the tested item, or other items represented by tested item. A test to determine system conformance to design specifications, as a condition of acceptance within a manufacturer in a subsequent phase of the system life cycle.

Test Plan: A document prescribing the approach to be taken for intended testing activities.

Time: The universal measure of duration. The general word "time' will be modified by an additional term when used in reference to operating time, mission time, test time, etc. In general expressions such as "Mean Time Between Failure (MTBF)", time stands for "life elements" which must be more specificially defined. A element of duration or usage that is used in all measures of System Effectiveness.

Time Active: That time during which an item is in an operational inventory. A time element useful to quantify System Effectivness equal to the time during which an item is being used or attempts are being made to use it.

Time Administrative: That element of delay time, not included in the supply delay time. A form Delay Time used to help quantify System Effectiveness equal to that portion of system or equipment Down Time included under neither Logistic Time nor Active Repair Time. This is equal to overhead time spent directing or managing the tasks required by an assigned maintenance activity. Also called Administrative Down Time. Activities include:

- answering mail,
- filing reports,
- library maintenance,
- preparing repair orders,
- waiting for maintenance specialists.

Time Alert: That element of Up Time during which an item is assumed to be in specified operating condition and is awaiting a command to perform its intended mission. Up Time during which an item is assumed to be operable and awaiting instructions to start its intended mission.

Time Checkout: That element of Maintenance Time during which performance of an item is verified to be a specified condition.

Time Delay: Time to recognize a problem or start a corrective action. That element of Down Time during which no maintenance is being accomplished on the item because of either supply or administrative delay.

Time Down (Down Time): That element of active time during which an item is not in condition to perform its required function. Elapsed time measured from when a defect has been reported for maintenance until the time the equipment is returned to the user operating properly. The interval during which the hardware system is in a failed state. It can not be operated without some repair activity on the system or else requires operator intervention. Time that equipment is not available to the user for useful work. Down Time reduces Availability and Dependability.

Time Inactive: That time during which an item is in reserve. A time category used to quantify System Effectiveness equal to the time during which an item is either in reserve or in inactive inventory.

Time Mission: That element of Up Time required to perform a stated Mission Profile. Operating Time.

Time Not Operating: That element of Up Time during which the item is not required to operate. A dormant Up Time state in which an item is able to function but is not required to function. Not to be confused with Down Time.

Time Up (Up Time): That element of Active Time during which an item is in condition to perform its required functions (increases Availability and Dependability). An Active Time category needed to quantify System Effectiveness equal to the time during which the system is in an acceptable operating condition or can perform its intended or required functions. This time interval is measured from the completion of a repair or recovery action until the next failure. Contrast with Down Time, when no productive work can be accomplished.

Top Event: In a Fault Tree Analysis, the undesirable system condition for which a Fault Tree is to be drawn. For any given system there may be many possibilities of top events and selecting top events to develop in an analysis is done with care, in order to avoid developing irelevant ones.

System boundary conditions depend on the top event. Top events are often established from hazard analysis or certification criteria.

Unreliability: The probability that a system, subsystem or element will fail to perform a required or intended function under stated conditions for a specified period of time.The probability of unsuccessful performance.The probability of not meetingspecification requirements. The complement of Reliability.

Useful Life: The number of Life Elements, such as cycles or time, from manufacture to when the item has an unrepairable failure or unacceptable failure rate. The total operating time between final manufacturing Debugging and Wearout for an item. Contrast with Early Life. Inappropriate situations, this period is considered to have an exponential failure distribution with a constant failure rate. This is than called the Random Failure Period

User: Anyone who requires the services of an item. A user may be, in turn, classified as either an End User or an Intermediate User.

Wearout: The process which results in an increase of the failure rate or probability of failure with inreasing number of life elements.

Weibull Distribution: A versatile distribution valuable in reliability applications. The family of distributions derived from it assume a variety of useful forms when the values of its there parameters called scale (alpha), slope (beta) and location (gama) are chosen in an intentional manner. It is used for a rapid and graphical approximate estimation procedure that becomes little biased for large sample sizes.The Weibull distribution is unable to attain certain skewness and kurtosis attainable by the more appropriate distributions which it mimics.

Weibull Paper: A type of Probability Paper used with the Weibull graphical estimation technique to show Unreliability and to estimate the Weibull Slope.

REFERENCES

[1] Carrion Garcia A., Carot Sanches T.: Fiabilidad, mantenibilidad y analisis de seguridad, Universidad Politecnica de Valencia, Valencia, 2000, 143 p.

[2] Zorin V. A.: Nadezhnost' mekhanicheskikh sistem, Infra-M, Moskva, 2015, 384 s.

[3] Choi S. K., Grandhi R. V., Canfield R. A.: Reliability-Based Structural Design, Springer-Verlag, London, 2007, 316 p.

[4] Ming Hu J., Kaminskiy M., Ushakov I. A.: Statistical Inference Concepts, In: Product Reliability, Maintainability and Supportability, Handbook, Pecht M., ed., CRC Press, Boca Raton, 2009, pp. 31-56.

[5] O'Connor P. D. T., Kleyner A.: Practical Reliability Engineering, John Wiley and Sons, Chichester, 2012, 512 p.

[6] Carrion Garcia A., Carot Sanches T.: Conceptos basos de estadistica, Universidad Politecnica de Valencia, Valencia, 1999, 112 p.

[7] Ramakumar R.: Engineering Reliability: Fundamentals and Applications, Prentice-Hall International, New Yersey, 1993, 494 p.

[8] Das D., Pecht M.: Practical Probability Distributions for Product Reliability Analysis, In: In: Product Reliability, Maintainability and Supportability, Handbook, Pecht M., ed., CRC Press, Boca Raton, 2009, pp. 57-81.

[9] Hoyland A., Rausand M.: System Reliability Theory, Models and Statistical Methods, Yohn Wiley and Sons, New York, 1994, 533 p.

[10] Ushakov I. A.: Kurs teorii nadezhnosti sistem, Drofa, Moskva, 2008, 240 s.

[11] Nachlas J. A.: Reliability Engineering, Probabilistic Models and Maintenance Methods, Taylor and Francis, Boca Raton, 2005, 395 p.

[12] Das D., Pecht M.: Reliability Concepts, In: In: Product Reliability, Maintainability and Supportability, Handbook, Pecht M., ed., CRC Press, Boca Raton, 2009, pp. 19-29.

[13] Wolstenholme L. C.: Reliability Modelling, A Statistical Approach, Chapman and Hall/CRC, Boca Raton, 1999, 272 p.

[14] Yang G.: Life Cycle Reliability Engineering, John Wiley and Sons, New Yersey, 2007, 531 p.

[15] ... (1995) Msc: Reliability and Maintainability, The Centre for Management of Industrial Reliability, Cost and Effectiveness, School of Engineering, University of Exter, Exeter, 36 p.

[16] Aronov I., Papic L.: Certification of Manufacturing in Yugoslavia According to Reliability Criterion (In Serbian), Kvalitet i standardizacija, Vol. 1-2, 1992, pp. 43-46.

[17] Aronov I., Ovchinnikov M. V.: Nekotoryxe osobennosti ispol'zovaniya sistemy sbora i obrabotki informatsii o nadyozhnosti izdeliy mashinostroenya, Ekspress-Standart, Vol. 40, 1976.

[18] Papic L.: Methods of Increasing Testing Efficiency for Technological Systems Reliability Estimation (In Serbian with English Summary), OMO, Belgrade, 1993, 236 p.

[19] Knezevic J., Papic L., Aronov J.: Advanced Approaches to Reliability and Safety Assurance of Complex Systems on the Basis FMEA Method, Proceedings of 6th International MIRCE Symposium, Logistics: Engineering, Economics, Environment and Management, Exeter, 1996, pp. 58-75.

[20] Kugel' R.V.: Ispitaniya na nadyozhnost' mashin i ikh elementov, Mashinostrenie, Moscow, 1982, 181 p.

[21] Papic L., Aronov J.: Knowledge-Based Analysis and Optimization of Reliability shortened Testing Plan Choice for Manufacturing Systems, Proceedings of the 3rd Internantional Conference Computer Integraterd Manufacturing - ICCIM '95, Vol. 2, Singapore, 1995, pp. 1271-1280.

[22] Gnedenko B., Belyaev Yu., Solov'yev A.: Matematicheskite metody u teorii nadyozhnosti, Nauka, Moscow, 1965, 524 p.

[23] Zio E.: An Introduction to the Basis of Reliability and Risk Analysis, World Scientific, New Yersey, 2007, 234 p.

[24] Stamatis D. H.: Failure Mode Effect Analysis: FMEA from Theory to Execution, Second Edition, American Society for Quality, Milwaukee, 2003, 487 p.

[25] Anleitner M. A.: The Power of Deduction, Failure Modes and Effects Analysis for Design, ASQ Quality Press, Milwukee, 2011, 208 p.

[26] Bell D., McBride P., Wilson G.: Managing Quality, Butterworth Heinemann, 1994.

[27] ... MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, Department of Defence, Washington, DC, USA, 1980, 53 p.

[28] Clabro S. R.: Reliability Principles and Practices, McGraw-Hill Book Company, Inc, New York, 1962, 367 p.

[29] Papic L.: Statistical Methods of Quality Management in Development Process of New Product, Lecture at Chapter Meeting, Society of Logistics Engineers, Research Centre MIRCE, School of Engineering, University of Exeter, UK, 28 March, 1996.

[30] … IEV 50(191), International Electrotechnical Vocabulary (IEV), Chapter 191, Dependability and Quality and Service, International Electrotechnical Commission, Geneve, 1988, 135 p.

[31] … IEC Standard, Publication 812, Procedures for Failure Mode and Effects Analysis (FMEA), Bureau Central de la Commission Electrotechnique International, Geneve, Suisse, 1985, 39 p.

[32] Barbour G. L.: Failure Modes and Effects Analysis by Matrix Method, Proceedings of Annual Reliability and Maintainability Symposium, 1977, pp, 144-119.

[33] … BS5750: Part 5, Reliability of Systems, Equipment and Components, Part 5, Guide to Failure Modes, Effects and Criticality Analysis (FMEA and FME-CA), British Standard Institute, UK, 1991, 43 p.

[34] Stamenkovic B., Holovac S.: Failure Modes, Effects and Criticality Analysis: The Basic Concepts and Applications, In: Logistics Engineering, IIS-IBK, Dubrovnik, 1987, pp. 113-134.

[35] … Quality Assurance, Analysis of Appearing Possibilities and Defect Effects (FMEA), TUV Rheinland Holding AG, Germany, 1993, 35 p.

[36] Zermen Z, ed.: AMDEC, Analysis of Failure Modes and Their Effect and Criticality, Metholodogy, EGTM, France, 1995, 24 p.

[37] Akinfiev L. L., Aronov I. Z., et all: Reliability of Mechanical Products, Practical Guide to Standardization, Certification and Assurance (In Russian), Russian Standard Institute, Moscow, 1990, 328 p.

[38] Kachalov V. A., Agaev A. V.: AMDEC: Method of Failure Modes, Effects and Criticality Analysis, Quality Management (In Russian), Bulletin, Vol. 10, No. 1, CNIIatominform, Moscow, 1996.

[39] Kubarev A. I.: Analiz kharaktera potentsial'nykh defektov i prichin ikh vyzyvayushchikh, Nadezhnost' i kontrol' kachestva. 20(1988)12, s. 43-46.

[40] Popovic B.: Quality Assurance (In Serbian), Science, Belgrade, 1992, 284 p.

[41] Papic L., Holovac S., eds.: Failure Modes, Effects and Criticality Analysis (FMECA), Theoretical and Applied Aspects (In Serbian), DQM, Cacak, 1994, 233 p.

[42] Deming W. E.: Out of the Crisis, Cambridge, MIT Center for Advanced Engineering Satudy, 1986, 498 p.

[43] Hammer W.: Product Safety Management and Engineering, by Willie Hammer, 1993, 317 p.

[44] Andrews J. D., Moss T. R.: Reliability and Risk Assessment, Longman Scientific and Technical, Harlow, 1993, 387 p.

[45] Papic L., Khan M.: Quality Assurance on the Basis of Failure Modes, Effects and Criticality Analysis: A Review, Communications in Dependability and Quality Management, Volume 1, Number 1, 1998, pp. 101-113.

[46] Blanchard B. S.: Logistics Engineering and Management, Fifth Edition, Prentice-Hall International, Inc., Upper Saddle River, 1998, 544 p.

[47] Hoyland A., Rausand M.: System Reliability Theory, Models and Statistical Methods, John Wiley and Sons, Inc., New York, 1994, 533 p.

[48] Grant Ireson W., Coombs C. F. Jr., Moss R. Y.: Handbook of Reliability Engineering and Management, Second Edition, McGraw-Hill, New York, 1996, 812 p.

[49] Kumamoto H., Henley E. J.: Probabilistic Risk Assessment and Management for Engineers and Scientists, Second Edition, Institute of Electrical and Electronics Engineers, Inc, New York, 1996, 615 p.

[50] Klyuev V. V., Gusenkov A. P., eds: Mechanical Engineering, Reliability (In Russian) Mashinostroenie, Moscow, 1998, 592 p.

[51] Barlow R. E., Lambert H. E.: Introduction to Fault Tree Analysis, In: Reliability and Fault Tree Analysis, Theoretical and Applied Aspects of System Reliability and Safety Assessment (Dedicated to Professor Z. W. Birnbaum), Barlow R. E., Fussell J. B., Singpurwalla N. D., editors, Society for Industrial and Applied Mathematics, Philadelphia, 1975, pp. 7-35.

[52] Knezevic J., Papic L., Vasic B.: Sources of Fuzziness in Vehicle Maintenance Management, Journal of Quality in Maintenance Engineering, Vol. 3, No. 4, 1997, pp. 281-284.

[53] Papic L., Pantelic M., Aronov J., Verma A. K.: Statistical Safety Analysis of Maintenance Management Process of Excavator Units, International Journal of Automation and Computing, 7(2), May 2010, pp. 146-152.

[54] Kletz T.: Learning from Accidents, Butterworth-Heinemann Ltd., Oxford, 1994, 279 p.

[55] Aronov J.: Methodology of Operational Safety Management On the Base Disturbances Statistical Analysis During Systems Operation and Assessment Methods Standardization, PhD Thesis (In Russian), VNIIS, Moscow, 1998, 254 p.

[56] Kletz T.: An Engineer's View of Human Errors, Institution of Chemical Engineers, Rugby, 1991, 209 p.

[57] Zio E.: Computational Methods for Reliability and Risk Analysis, World Scientific Publishing Co. Pte. Ltd., Singapore, 2007, 362 p.

[58] Dale B.G.: Managing Quality, Blackwell Publishing, Oxford, 1999, 495 p.

[59] Papic L., Pantelic M.: Implementation Methodology for Risk Minimization into Maintenance Process of Production System at Coal Mines, Report of Contract No. 4617 (In Serbian), DQM Research Center - Kolubara Metal, Prijevor - Vreoci, 2009, 468 p.

[60] Knezevic J.: Systems Maintainability, Analysis, Engineering and Management, Chapman and Hall, London, 1997, 400 p.

[61] Nikolic B., Spasojevic R., Sekularac B.: Technoeconomical Analysis of Appliance Vibrodiagnostics in Preventive Maintenance in Open Pit Mine Kolubara, Proceedings 12th International conference Dependability and Quality Management, ICDQM-2009, Belgrade, 2009, pp. 412-417.

[62] Bertrand M.: Proactive Maintenance, Reactive, Preventive, and Predictive Maintenance Practices Within a Proactive Approach, SKF Reliability Systems, San Diego, 2003, 8 p.

[63] T. Ohno: Toyota Production System, Beyond Large-Scale Production, Diamond, Inc., Tokyo 1978, 207 p.

[64] B. Weigand, R. Langmaack, and T. Baumgarten: Lean Maintenance System, Zero Maintenance Time – Full Added Value, Lean Management Institut, Aachen, 2005, 165 p.

[65] Kletz T.: Lessons from Disaster, How Organizations Have No Memory and Accidents Recur, Institution of Chemical Engineers, Rugby, 1993, 184 p.

[66] Blanchard B.S., Fabrucky W.J.: Systems Engineering and Analysis, Prentice Hall, Upper Saddle River, 1997, 750 p.

[67] Syan C.S., Menon U.: Concurrent Engineering, Concepts, Implementation and Practice, Chapman and Hall, London, 1994, 254 p.

[68] Papic L., Aronov J., Pantelic M.: Safety Based Maintenance Concept, International Journal of Reliability, Quality and Safety Engineering, Vol. 16, No. 6, 2009, pp. 533-549.

[69] Tracy Philip Omdahl, editor: "Reliability, Availability and Maintainability (RAM) Dictionary, Quality Council of Indiana, West Terre Haute, 1988, 360 p.

[70] Robert Dovich, Bill Wortman: CRE Primer, Council of Indiana, West Terre Haute, 2002, 748 p.

SUMMARY

The "Reliability Modeling Prediction" monograph considers issues of reliability analysis, safety analysis, failure analysis and systems maintenance concepts. Under systems the authors allude to different kinds of technical objects (equipment, gears, instruments and mechanisms) which different branches of industry design, produce, exploiting and maintenance. This monograph describes in detail: probability concept of reliability, reliability quantification, probability distributions for reliability analysis, types of reliability tests and reliability testing plans, reliability block diagram method, failure modes, effects and criticality analysis, fault tree analysis, event tree analysis and systems maintenance concepts.

Chapter 1: Historical Perspective. This chapter presents a brief history of reliability theory. The chapter describes why need for reliability engineering.

Chapter 2: Statistical Basis of Reliability. This chapter presents reliability study motives and probability concept. The focus is on condition probability, independent events, theorem of the total probability, theorem of Bayes, random variable, mean values and probability distributions.

Chapter 3: Reliability: Concept and Bases. This chapter introduces reliability definition. The chapter discusses quantification of the reliability, failure rate, including variation of the failure rate.

Chapter 4: Reliability Models. In this chapter, basic types of continuous probability distributions are introduced. Three continuous distributions (normal, exponential, and Weibull) commonly used in reliability modeling and failure rate assessments are presents.

Chapter 5: Reliability Estimation and Testing. This chapter presents the concept of reliability test method and provides an oveview types of reliability tests. Also, this chapter presents test results analysis and different methods of estimation testing analysis. Finally, this chapter presents checking previously stated hypothesis referred to the distribution mean life.

Chapter 6: Reliability Testing Plans. Advanced concepts of reliability accelerated testings are used as a means for reliability assessment. This chapter examinate the accelerated testings without intense the processes which often result in additional failures or damages what brings, in the end, to distortion of the real picture of the system behaviour and reliability in state of use. This chapter describes reliability shortened testing plan phases and testing process trajectories.

Chapter 7: Reliability Block Diagram. This chapter describes how to combine reliability of elements and items to calculation system reliability. Reliability block diagram method are used as a means to represent the logical system structure and develop reliability models for a series systems, parallel systems, series/parallel systems and non series/parallel systems.

Chapter 8: Failure Modes, Effects and Criticality Analysis. Knowledge of failure modes that cause system failure is essential for reliable systems design practice. This chapter presents a methodologies Failure modes and effects analysis (FMEA) and Failure criticality analysis (FMECA). The knowledge about both of this methodologies FMEA and FMECA helps in effective systems design, manufacturing and maintenance.

Chapter 9: Fault Tree Analysis. This chapter presents Fault tree analysis (FTA) for system reliability modeling. Deductive approach in the failure analysis is introduced. The chapter provides fault tree construction methodology. This chapter shows how reliability block diagram can be converted to system fault tree. Finally, this chapter describes fault tree qualitative and quantitative assessment methodologies.

Chapter 10: Statistical Safety Analysis. Basic principles of statistical safety analysis can be applied for development possible scenarious of accidents occurence from the initial event. This chapter discusses initial event analysis and presents risk calculation including Event tree analysis (ETA).

Chapter 11: Maintenance Concepts. Balanced approach to maintenance into maintenance system describes in this chapter. This chapter provides a definitions of different maintenance concepts: corrective maintenance, periodic preventive maintenance, predictive maintenance, proactive maintenance, lean maintenance and safety based maintenance. On the base previous concepts, this chapter presents effective maintenance concept.

Chapter 12: Reliability Terminology. This chapter presents reliability terms and definitions. Definitions of the terms took from a two cited references published by Council of Indiana.

REZIME

U monografiji "Reliability Modeling and Prediction" su razmotrena pitanja anlize pouzdanosti, analize sigurnosti, analize otkaza i koncepcija održavanja sistema. Pod sistemima, autori podrazumevaju različite vrste tehničkih objekata (opremu, uređaje, aparate, mehanizme), koji se projektuju, prozvode, koriste i održavaju u različitim granama industrije. U ovoj monografiji detaljno su opisani: verovatnosna koncepcija pouzdanosti, kvantifikovanje pouzdanosti, raspodele verovatnoća za analizu pouzdanosti, vrste ispitivanja i planova ispitivanja za ocenu pouzdanosti, metoda blok dijagram u smislu pouzdanosti, analiza vrsta, posledica i kritičnosti otkaza, analiza stabla otkaza, analiza stabla događaja i koncepcije održavanja sistema.

Poglavlje 1: Istorijska perspektiva. Ovo poglavlje prikazuje kratku istoriju teorije pouzdanosti. Poglavlje opisuje zašto je potrebno inženjerstvo pouzdanosti.

Poglavlje 2: Statistička osnova pouzdanosti. Ovo poglavlje prikazuje razloge za proučavanje pouzdanosti i verovatnosnu koncepciju. Pažnja je usredsrešena na uslovnu verovatnoću, nezavisne događaje, teoremu potpune verovatnoće, Bayesovu teoremu, slučajnu promenljivu, srednje vrednosti i raspodele verovatnoća.

Poglavlje 3: Pouzdanost: koncepcija i osnove. Ovo poglavlje uvodi definiciju pouzdanosti. U poglavlju se raspravlja o kvantifikovanju pouzdanosti i intenziteta otkaza, uključujući promenu intenziteta otkaza.

Poglavlje 4: Modeli pouzdanosti. U ovom poglavlju se uvode osnovne vrste kontinualnih raspodela verovatnoća. Prikazane su tri kontinualne raspodele (normalna, eksponencijalna i Weibullova) koje su obično korišćene u modelovanju pouzdanosti i ocenama intenziteta otkaza.

Poglavlje 5: Ispitivanje i ocena pouzdanosti. Ovo poglavlje prikazuje koncepciju metoda ispitivanja za ocenu pouzdanosti i pruža pregled vrsta ispitivanja za ocenu pouzdanosti. Takođe, ovo poglavlje prikazuje način analize rezultata i različite metode ocene analize ispitivanja. Najzad, ovo poglavlje prikazuje proveru prethodno fomulisanih hipoteza koje se odnose na srednje vreme rada.

Poglavlje 6: Planovi ispitivanja za ocenu pouzdanosti. Savremene koncepcije ubrzanih ispitivanja za ocenu pouzdanosti su korišćene kao sredstvo za određivanje pouzdanosti. Ovo poglavlje razmatra ubrzana ispitivanja bez pojačavanja određenih procesa koji često imaju za posledicu dodatne otkaze ili oštećenja koji imaju za posledicu, u krajnjoj linini, iskrivljivanje realne slike o ponašanju sistema i pouzdanosti tokom njegovog korišćenja. Ovo poglavlje opisuje faze planova skraćenih ispitivanja za ocenu pouzdanosti i trajektorije ispitivanja.

Poglavlje 7: Blok dijagram u smislu pouzdanosti. Ovo poglavlje opisuje kako se povezuju pouzdanosti elemenata i celina pri proračunu pouzdanosti sistema. Metoda Blok dijagram u smislu pouzdanosti je korišćena kao sredstvo za opisivanje logičke strukture sistema i razradu modela pouzdanosti za sisteme sa rednom, paralelnom, redno-paralelnom i drugim vezama.

Poglavlje 8: Analiza vrsta, posledica i kritičnosti otkaza. Poznavanje vrsta otkaza koje prouzrokuju otkaz sistema je važan element u praksi projektovanja pouzdanosti sistema. Ovo poglavlje prikazuje metodologije Analize vrsta i posledica otkaza (FMEA) i Analize kritičnosti otkaza (FMECA). Poznavanje ove dve metodologije, FMEA i FMECA, pomaže pri efektivnom projektovanju, proizvodnji i održavanju suistema.

Poglavlje 9: Analiza stabla otkaza. Ovo poglavlje prikazuje Analizu stabla otkaza (FTA) u modelovanju pouzdanosti sistema. Predstavljen je deduktivni prilaz u konkretnoj analizi otkaza. Poglavlje definiše metodologiju konstrukcije stabla otkaza. Ovo poglavlje pokazuje kako se blok dijagram u smislu pouzdanosti može pretvoriti u stablo otkaza sistema. Najzad, ovo poglavlje opisuje metodologiju kvalitativne i kvantitativne ocene stabla otkaza.

Poglvalje 10: Statistička analiza sigurnosti. Osnovna načela statističke analize sigurnosti se mogu primeniti u razvoju mogućih scenarija nastanka havarija od početnog događaja. Ovo poglavlje razmatra analizu početnog događaja i prikazuje proračun rizika uključujući Analizu stabla događaja (ETA).

Poglavlje 11: Koncepcije održavanja. U ovom poglavlju se opisuje uravnoteženi prilaz održavanju, u okviru sistema održavanja. Ovo poglavlje pruža definicije različitih koncepcija održavanja: korektivnog održavanja, periodičnog preventivnog održavanja, prediktivnog održavanja, proaktivnog održavanja, ekonomičnog održavanja i održavanja zasnovanog na sigurnosti. Na osnovu prethodnih koncepcija, ovo poglavlje prikazuje efketivnu koncepciju održavanja.

Poglavlje 12: Terminologija pouzdanosti. Ovo poglavlje prikazuje pojmove i definicije u oblasti pouzdanosti. Definicije datih pojmova su uzete iz dva literaturna naslova koje je objavio Council of Indiana.

ABOUT THE AUTHORS

Andrés Carrión García is PhD in Industrial Engineering, and associate professor at the Department of Applied Statistics, Operations Research and Quality in the Universidad Politécnica de Valencia (UPV, Spain). He has been head of this Department since 2001 to 2010. At present he is Director of the research Centre for Quality and Change Management and director of the Master Degree in Data Analysis Engineering, both in the UPV. His research has been oriented basically in two lines. The first one corresponds to the use of statistical tools in different fields of knowledge, as health studies, industrial processes, reliability of civil infrastructures, education and quality control. The second one is related with quality management, and especially in what refers to quality and management in HEI. He has been cooperating with industries since 1984, mainly in the automotive sector. He has a long experience of teaching and consulting in Latin America, where he has participated in postgraduate and doctoral programs in different countries and universities. He has participated as international consultant in projects with the Andean Pact and Mercosur, in the fields of statistics and quality. He is author or co-author of different publications in national and international journals, as well as in conferences in Europe, Asia and Latin America. He is member of the editorial board and reviewer of international journals. He has directed eleven PhD Thesis in his research fields and a number of Master Degree Thesis in the same areas. He is senior member of the American Society for Quality (ASQ), and member of the Spanish Association for Quality (AEC).

Ljubisa Papic is a Professor and Head of the Department of Industrial and Systems Engineering in the Faculty of Technical Sciences Cacak at the University of Kragujevac, Serbia. He received the PhD degree in Reliability Engineering from University of Novi Sad, Serbia. He is a

Member of Russian Quality Problems Academy and Corresponding Member of Serbian Engineering Sciences Academy. His research topics are: reliability testing, failure analiysis, safety analysis, concurrent engineering. He has published more than 400 journal and conference papers and technical publications in the areas. Professor Papic is director and founder the *Research Center of Dependability and Quality Management (DQM Research Center), Prijevor, Serbia* and he is serving as Editor-in-Chief of *Communications in Dependability and Quality Management, An Int. J.*, Serbia. Also he is serving as an Editorial Board Member of *Metody menedzhmenta kachestva* (Methods of Quality Management) international journal in Moscow, Editorial Board Member of *International Journal of Systems Assurance Engineering and Management* (Springer) and as Deputy Editor-in-Chief of *Problemy Mashinostroeniya i Avtomatizatsii* (Problems of Mechanical Engineering and Automatization), International Journal of Russian Academy of Sciences in Moscow, Russia. He was a Visiting Professor at Ben-Gurion University of the Negev, Israel, at Valencia Polytechnic University, Spain and at Samara State Aerospace University, Russia. He is a Member of the *IEEE Reliability Society* and Senior member of the *ASQ*. Professor Papic is a recipient of *Education and Research Leadership Award* and *Award for Pioneering International Education and Research in Industrial Quality and Reliability Management* by *Society for Reliability Engineering, Quality and Operations Management*.