TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Phased mission analysis of maintained systems : a study in reliability and risk analysis

Citation for published version (APA):
Terpstra, K. (1984). *Phased mission analysis of maintained systems : a study in reliability and risk analysis*. [Phd Thesis 1 (Research TU/e / Graduation TU/e), Mathematics and Computer Science]. Technische Hogeschool Eindhoven. https://doi.org/10.6100/IR28201

DOI:
10.6100/IR28201

Document status and date:
Published: 01/01/1984

Document Version:
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

Download date: 04. Oct. 2023

PHASED MISSION ANALYSIS OF MAINTAINED SYSTEMS

A Study in Reliability and Risk Analysis

K. TERPSTRA

PHASED MISSION ANALYSIS
OF
MAINTAINED SYSTEMS

A Study in Reliability
and
Risk Analysis

PHASED MISSION ANALYSIS OF MAINTAINED SYSTEMS

A Study in Reliability
and
Risk Analysis

PROEFSCHRIFT

ter verkrijging van de graad van doctor in de technische wetenschappen aan de Technische Hogeschool Eindhoven, op gezag van de rector magnificus, Prof. Dr. S.T.M. Ackermans, voor een commissie aangewezen door het college van dekanen in het openbaar te verdedigen op dinsdag, 4 december 1984, te 16.00 uur.

door

KLAAS TERPSTRA

geboren te Minnertsga

Dit proefschrift is goedgekeurd door de
promotoren: Prof. Dr. Ir. J.W. Cohen
Prof. Dr. J. Wessels

Oan myn frou
Oan Jan en Jinne

Ta de neitins fan
Sjoukje

ACKNOWLEDGEMENTS

I am very grateful to the Netherlands Energy Research Foundation ECN for its support in preparing my doctoral thesis.

I am grateful to:
Mr. H.J. van Grol for his stimulating discussions and continuous support;
Mr. N.H. Dekker for his assistance with the programming;
Mr. E. van der Goot for his help in plotting component behaviour;
Mr. A. Last for suggesting the Heat Removal System as a simple example of a phased mission;
Mr. H. Höcker for preparing the figures; and
Mrs. P.M. Wijns-Kok for typing the various drafts and the final version of the manuscript.

Their help has been highly appreciated by me.

TABLE OF CONTENTS

page

page

page

page

page

page

1. INTRODUCTION

1.1. On the history of reliability theory and risk analysis

The expressions "to be reliable" and "to be available" have been used in daily life for a long time. "To be reliable" as a person may mean, for instance, that *for at least a period* one is considered, based on experience, as someone who does not abuse confidential information supplied. A saying like "you can depend on this person", shows a clear relation with "to be reliable". Something similar holds for "to be available". "To be available" as a person means that a claim is laid on the person in question at *every moment*. For example, domestics must always be available for their employer.
The same reasoning can be applied to man-made equipment. A car, for example, is called "reliable" if it has no defects during a sufficiently long time. The same car is called "available" not only when it is there but if, in addition, one can start it and drive it the moment one wants to use it.
Obviously, "reliability" has something to do with *undisturbed functioning during a certain period*, whereas "availability" tells something about the state at a certain *instant*.
At the beginning of this century the need arose to describe such intuitive notions like reliability and availability in a more precise manner. As technological developments progressed in many fields it became important to predict the behaviour of materials, in particular in order to predict the "lifetime" (the time of undisturbed functioning) of a component. Therefore, the reliability of a component was mathematically defined in terms of a probability, i.e. "the reliability at instant t" was formulated as "the probability that the component does not fail in service during at least a period t". Often the so-called "lifetime distribution" is used instead of the reliability function. The "lifetime distribution" is complementary to the reliability, i.e. it gives the probability that the component fails within a period t. Examples of lifetime distributions are the "Weibull distribution" (suggested by Weibull in the late 1930's) for the life length of materials and the "negative exponential distribution" (in the early 1950's) for electronic components.

During and after the Second World War many technological systems (e.g. military systems and missile systems) have become much more complex. On

the one hand such complex systems lead to higher investments, on the other hand they tend to become less reliable. But, for instance, military equipment, must be highly reliable and accurate on demand as well as during operation to be successful (e.g. intercontinental ballistic missiles with nuclear war heads). But also complex equipment for civil applications has to be very reliable in order to prevent damage to human beings as well as to invested capital (e.g. missile and computer systems for manned space flights and safety systems for nuclear power plants). Because of both factors, viz. higher investment cost and less reliable systems, much attention has been given to the "system reliability" (the probability of undisturbed system operation during a time period) and the "system availability" (the probability that the system is available at an instant), in addition to component reliability and availability. In the early days of system reliability studies, in the late 1950's and early 1960's, system reliability was analysed mainly by means of so-called "reliability block diagrams". Such a reliability block diagram represents the functional working scheme of a system by means of blocks that are connected by lines. Each block represents a subsystem. The reliability of each block (subsystem) is calculated and after that the system reliability is determined on the basis of the reliabilities of the different blocks. But the increasing complexity of the systems made the reliability block diagrams extremely complex too. Because these large and complex block diagrams were no longer manageable new techniques had to be developed to treat system reliability characteristics. One of the techniques that was developed is *fault tree analysis*. It was invented by H.A. Watson (1961) of Bell Telephone Laboratories. He used this technique for the evaluation of the Minuteman Launch Control System. Lateron, employees of the Boeing Company extended the method and made it suitable for computer implementation.

Fault tree analysis (FTA) is a technique directed to the analysis of a specific system failure. The construction of the fault tree for the concerned system failure, called the "TOP-event", proceeds as follows. The TOP-event (system failure) is connected to subsystem failures, which possibly may lead to the system failure, by means of a logical "OR" or "AND". Next, each subsystem failure is connected to failures of the next lower system level, etc. This development stops when component failures (the lowest system level) are reached. The whole structure, starting at the TOP-event and terminating at component level, is called a "fault tree

for the system failure concerned".
Qualitative as well as *quantitative* characteristics for the concerned system failure can be calculated by means of FTA. Qualitative characteristics are, for instance, the possible failure modes which lead to the system failure. These failure modes are called *minimal cut sets*. Each minimal cut set consists of a combination of components, which cause, if they *all* fail, the system failure. Other qualitative characteristics are the so-called *minimal paths*. They are combinations of components that guarantee that the system functions: if *each* component of such a minimal path functions then the system functions. *Quantitative* characteristics are among other things the "system unavailability" and the "lifetime distribution" of the system. These two quantities are complementary to the "system availability" and the "system reliability", respectively. But since in principle FTA is an analysis of a system failure and not of the system functioning, as a rule it are the first mentioned quantities that are calculated. The calculations of the unavailability and the lifetime distribution are based on the minimal cut sets. Therefore, such calculations can only take place after the minimal cut sets have been calculated. Maintenance can also be taken into account but it increases the complexity in calculating the quantitive characteristics considerably. During the last twenty years FTA has proved to be one of the most powerful tools to analyse large and/or complex systems. Although FTA in the early days was only applied to space flight technology, it was rather soon recognized that the technique could be applied to other technological fields. In 1965 at a safety system symposium in Seattle, it was concluded that reliability techniques, among which FTA, could be successfully applied to other areas, such as chemical industry and nuclear engineering. Since then, FTA has become a basic technique for analyzing complex systems within the framework of risk studies for nuclear power plants. Such risk studies have started in the early 1970's.

In every day life risk is a well known phenomenon. In former days the risk of a person to be injured by disease or war operations was much greater than the risk to be injured due to the faulty operation of a technical installation. Nowadays this situation has changed. Several technological systems are considered to give more risk than many once heavily feared diseases. It is a natural requirement that the risk involved in operating such technological systems should be so small that it is acceptable from

the social as well as the economical point of view. For this reason risk assessment has become an important tool in the design of technological systems and scheduling of their operational characteristics.
Risky situations are caused by so-called *hazards*, which may give rise to casualties. For instance, in case of a nuclear power plant the hazard is radiation and release of radioactivity, whereas in case of chemical plants the hazards may be release of toxical material, explosions, etc. For technological systems a hazard occurs in case of an accident within such a system. This accident is often called the *initiating event*. An initiating event in a nuclear power plant is, for example, the rupture of a pipe that transports water to cool the core of the nuclear reactor. As a rule the initiating event does not create the hazard itself, this being due to safety functions of the total system, which are in general available. Therefore, after the initiating event has occurred, the hazardous situation is only created if one or more safety systems fail or have failed. In the case that all safety systems perform their intended functions, the hazard does not occur. In the case that all safety functions fail the hazard occurs completely. Between these extremes a large number of different *consequences*, i.e. nuances concerning the occurrence of the hazard, are possible. Obviously, a consequence depends on which safety systems have failed and which safety systems are functioning. Such a sequence, which starts with the initiating event and is followed by the functioning and/or failure of the different safety systems, is often called an *accident sequence*.
Actually, accident sequences are represented by means of *event trees*.
Such an event tree is a logical scheme that starts with the initiating event. For the first safety system a branch point is introduced, i.e. the first safety system can be in one of two states, viz. the function state or the fail state. The event tree, therefore, consists from this first safety system of two branches. For the second safety system two branch points occur, namely, one for the branch that represents the function state of the first safety system and one for the branch where the first safety system is assumed to be failed. So from the second safety system the event tree consists of four branches, etc. In fact, each of these branches represents an accident sequence, as described before.
For the analysis of a risky (hazardous) situation it is important to assess for a possible accident the amount of release of energy or toxic material. In addition it is necessary to assess the frequency of occurrence of such a release. Therefore, within the framework of risk analysis Henley and Kumamoto [29] formulate the following points which should be considered:

(i) search for possible hazards which cause the dangerous situation;
(ii) if one or more hazards are detected then identify the corresponding initiating events;
(iii) identify the accident sequences which may give rise to the hazards;
(iv) search for each failed system of the accident sequence of step (iii) their respective failure modes (minimal cut sets);
(v) calculate for each accident sequence the probability of occurrence by means of the results of step (iv);
(vi) calculate for each accident sequence its consequence in terms of the identified hazard(s).

In the late 1960's some risk studies concerning nuclear power plants were performed for insurance companies in the USA. These studies were mainly concerned with step (i). The first large-scale risk study has been the Reactor Safety Study (WASH-1400) [16] in the USA; its final report appeared in 1975. The study concentrates on the potential risk for society caused by radioactive release from nuclear power plants. All steps, (i),....,(vi), are fully treated in WASH-1400, its basic techniques being event tree methodology and fault tree analysis. Most of the risk studies which are performed nowadays (for example the Dutch RASIN study [40] (1975) and the German risk study [41] (1980) both concerned with risk from nuclear energy) apply the methodology initiated by the WASH-1400 study.
From step (v) it is seen that for risk analysis often not only the analysis of a single system, but of a number of systems is needed.
In the latter case the systems do not operate at the same time, but one after the other. Furthermore, such systems are often connected by physical (e.g. thermo-hydraulic) processes. This means that these systems are not necessarily mutually independent. One of the dependencies may be a component (e.g. a pump) shared by two or more systems. Because of these dependencies the complexity of the calculations increases considerably.

In modern space flight we also meet dependent systems, for instance, in a missile system. As a rule a missile consists of several stages, i.e. several subsystems. During the flight each of these stages operates during a period of time and then stops working, after which the next stage is initiated. Often a general control system is present for all stages. For such a missile flight (the so-called *mission* of the missile) the most interesting quantity is the probability of a successful flight.

In literature a flight is described by the notion of a *phased mission*. Obviously, a phased mission is a task for a complex system to be performed in parts (phases), one part after the other. Each part (subtask) is carried out by a subsystem of the total system. For the execution of each subtask a certain period of time is needed. The complete task (mission) is successful only if each subtask is successful, i.e. each phase is survived. The mission fails if at least one subtask fails, i.e. when a subsystem failure occurs during the performance of its subtask. The characteristic quantity is the probability of the successful execution of the mission, or its complement, the probability of mission failure. In the first case one might speak of the total *system reliability*. Studies concerning phased mission analysis and based on FTA occur later in literature than risk studies carried out by means of FTA. However, there exists a strong similarity between the models of both problem areas. It is easily seen that the branch of the event tree where each safety system successfully performs its intended function, can be considered as a phased mission. This correspondence has never been invented or discussed in literature. *The present study proceeds by defining each branch of an event tree (accident sequence) as a phased mission.*

The above mentioned Reactor Safety Study has aroused much criticism. This criticism does not concern the methodology applied in the study (step (i),...,(vi)), but is mainly concerned with the quantification of system parameters such as the probability of system failure, the probability of the occurrence of an accident sequence, the failure probability of a vessel and of piping, etc. (see for instance the Lewis report [45]). We shall mention here two objections concerning the probability calculations.

(a) *The uncertainties in the input data (e.g. failure rates).*
In the Reactor Safety Study probability calculations are performed with mean failure rates, mean repairtimes, etc. They are obtained from field data and enter the probability distribution with which the calculations are performed. The inaccuracies in these input parameters may cause large deviations in several probabilities of interest, particularly if events with small probabilities are concerned. Because the field data as used in the Reactor Safety Study are not the outcome of long term measurements the operational value of the calculations based on it are rather questionable.

(b) *The system dependencies that are not correctly taken into account within the accident sequences.*
In the Reactor Safety Study these dependencies are treated by engineering judgement and not by means of exhaustive analytical methods (cf. Barlow et al [32]). This implies that the effect of partial failures of one system cannot be fully taken into account in relation with following systems of the same accident sequence. This may lead to an under-estimation of the probabilities of occurrence of accident sequences and therefore to an under-estimation of the total risk.

The present study is devoted to system reliability and is mainly directed to the quantitative evaluation of accident sequences. Event tree methodology and fault tree analysis are applied as basic techniques. It introduces a new methodology for the calculation of the probability of occurrence of an accident sequence. This new methodology takes correctly into account shared equipment dependencies between the different systems present in an accident sequence. Since large and/or complex systems may contain a large number of minimal cut sets (sometimes millions of it), it is not possible as a rule to obtain the exact analytical solution. Therefore, upper and lowerbounds for the probability of occurrence of an accident sequence are presented. Calculation results show that this probability is under-estimated if system dependencies are not fully taken into account. The new methodology also offers the possibility to get insight into the degree of dependency between systems based on quantitative calculations.
To make the methodology manageable for complex systems, it is implemented in the reliability computer progam PHAMISS. This program is written in FORTRAN-IV for the CDC-Cyber 175. PHAMISS is users friendly and has proven to be a fast and efficient program.

In the sequel of this chapter an elementary treatment of the principles of fault tree analysis, event tree methodology and phased mission analysis is given, together with an outline of the new approach presented in this study.

Finally we review some literature of the different problem areas here.

In the 1960's several books treating reliability theory were produced together with many journals that focussed their attention to the same subject. (For a bibliography see Henley and Kumamoto [29], Historical perspective, references). For the basic concepts of reliability we refer to Barlow and Proschan [17] and [42].

Vesely [21] seems to be the first one who published a systematic study of fault tree analysis. Also several new techniques were introduced to treat the reliability of large and/or complex systems. They are reviewed by Barlow and Proschan [31] and recently by Hwang et al [30].

An introduction to phased mission analysis is given by Esary and Ziehms [8].

For an extensive treatment of the steps (i),...,(vi), to be executed in the framework of a risk study, see Henley and Kumamoto [29], whose book seems to be the first general textbook in this area. They also show the relation between the frequency of occurrence of the amount of release and the consequences by means of the Farmer curve.

For other methods used in risk analysis, like cause-consequence diagrams, decision tables, failure mode and effect analysis (FMEA), etc. the reader is also referred to their book.

An important publication in risk analysis has been the appearance of the Probabilistic Risk Analysis Procedure Guide [38] in April 1982. This guide presents those methods which during the last ten years have turned out to be appropriate in the risk analysis concerning nuclear power plants.

1.2. Basic concepts of fault tree analysis, event tree methodology and phased mission analysis

1.2.1. Fault tree analysis

Fault tree analysis (FTA) is the analysis of a system failure rather than the analysis of system functioning. A system failure is present if the system is not able to perform its intended function. In this situation the system is said to be in the *fail state*. Otherwise the system is in the *function state*. A system consists of components (the smallest units within the system) and their logical relationship. By means of a logical scheme, called the fault tree, a system failure is linked to the various component failures. If for a system failure such a fault tree is present, then by means of FTA several characteristic quantities for such a system failure can be calculated.

FTA consists of two major steps:

(1) the construction of the fault tree ;
(2) the analysis of the fault tree, i.e. the calculation of the different characteristic quantities.

Before treating each of these steps a number of basic assumptions concerning systems and components are summarized. In the present study it is assumed that:

(A1) a number of *components* together with their functional relationship define a *system*;

(A2) a *component* is assumed to be the smallest unit that can occur within a system;

(A3) a component as well as a system behaves *binary*, i.e. the component or the system can be only in one of two states: the *function* state or the *fail* state. If the component (or the system) is in the *function* state, it is *able* to perform its required function; if on the other hand the component (or the system) is in the *fail* state it is *not able* to perform its intended function;

(A4) components behave independently.

Fault tree construction

For a single functional series-parallel system S_1 consisting of the components A, B and C the corresponding functional block diagram (a logical working scheme) is shown in fig. 1.1. and the associated fault tree is depicted in fig. 1.2.
A fault tree always starts with a defined system failure called the *TOP-event*. Such a TOP-event may be caused by a number of other events (e.g. subsystem failures). They form the input for the TOP-event. If one event alone can cause the TOP-event the occurrence in the fault tree is represented by an OR-gate; if all the input events are needed to occur in order to cause the TOP-event then this occurrence is represented by an AND-gate. The same reasoning can be applied for other compound events (subsystem failures) in the fault tree. The construction of the fault tree stops if the input of a gate stems from components only. Because fault tree analysis is the basic technique for the present study we shall not further treat here the possibilities of block diagrams.

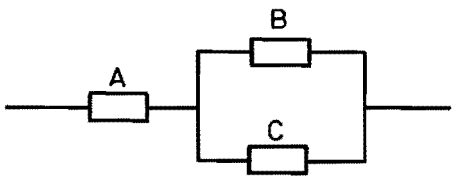


FIG. 1.1. FUNCTIONAL BLOCK DIAGRAM OF SYSTEM S_1.

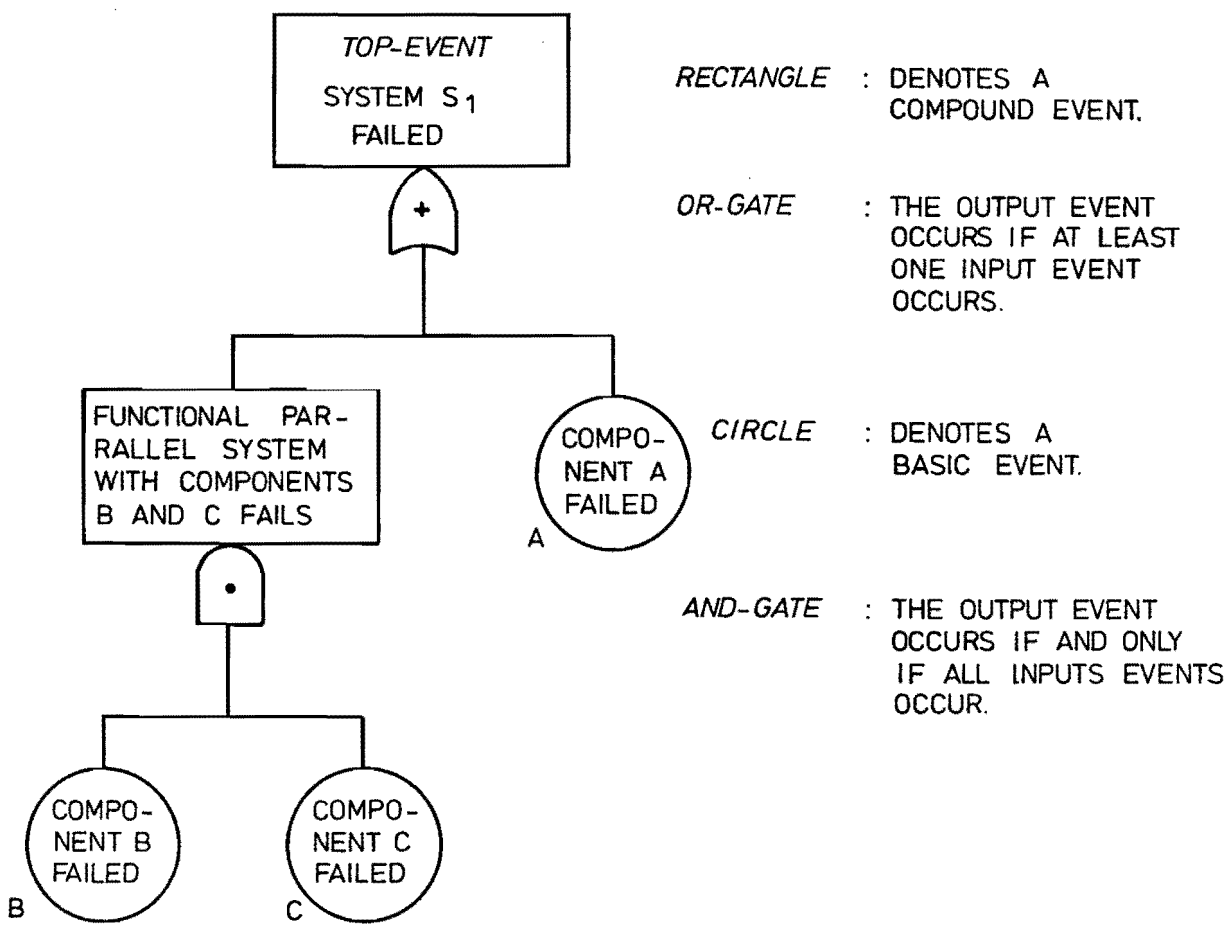


FIG. 1.2. FAULT TREE FOR SYSTEM S_1.

Analysis of the fault tree

Fault tree analysis is a *deductive analysis*, i.e. for a defined system failure called the *TOP-event* of the fault tree all possible *failure modes* for the system failure are searched for in a systematic manner.
A *failure mode* for a system failure consists of one or more components that are in the *fail state* and by their joint fail states they introduce the system failure. Generally we look for the *smallest* groups of components that can introduce the system failure, i.e. the smallest failure modes. Those smallest failure modes are called *minimal cut sets* of the corresponding fault tree. In our example of system S_1 it is easily seen from the fault tree in fig. 1.2. that there are two minimal cut sets, viz. minimal cut set M_1 which consists only of component A and minimal cut set M_2 that contains both the components B and C. We shall denote these two minimal cut sets by:

$$\begin{aligned} M_1 &= \{A\}; \\ M_2 &= \{B,C\}; \end{aligned} \tag{1.1}$$

Obviously, the cut set {A,B,C} is also a failure mode for system S_1 but it is not the smallest one that can be created from the combination of A, B and C. Namely, we can delete A so that {B,C} remains; {B,C} in turn being a failure mode itself. The same is true when we delete component B or component C or both from {A,B,C}. So {A,B,C} is *not* a minimal cut set.
A group of components that assures the *function* state of a system is called a *path set*; a *minimal path set* exists if the deletion of any one of the components of that set implies that system functioning is no longer assured. From the block diagram in fig. 1.1. it is seen that the minimal path sets for system S_1 are given by:

$$\begin{aligned} P_1 &= \{A,B\}; \\ P_2 &= \{A,C\}. \end{aligned} \tag{1.2}$$

Till now we have been concerned with the so-called *qualitative* FTA, i.e. the calculation of the minimal cut sets (and minimal path sets). The qualitative FTA is followed by the *quantitative* FTA, that calculates probabilistic quantities. For this quantitative FTA we need the concepts of *availability* and *reliability*. In the following we shall give their

definitions, some relations between them and discuss some techniques for their evaluation (cf. chapter 5).

Denote by R(t) the *reliability* of a component (or a system) at instant t, by F(t) its *lifetime distribution* or *failure distribution* and by A(t) its *availability*. Then the definitions of R(t), F(t) and A(t) are given by:

R(t) : the probability that the component (or the system) survives the interval [0,t], t≥0; (1.3)

F(t) : the probability that the component (or the system) fails within the interval [0,t], t≥0; (1.4)

A(t) : the probability that the component (or the system) is in the *function* state at instant t, t≥0. (1.5)

Since FTA is directed to the analysis of a system failure, frequently in the present study the components *unavailability* q(t) and the system *unavailability* Q(t) shall be used:

$$q(t) = 1-A(t),\ t\geq 0\ ;\ Q(t) = 1-A(t),\ t\geq 0. \tag{1.6}$$

From (1.3) and (1.4) it is seen that the reliability function and the lifetime distribution of a component or a system are complementary to each other. So the following relation holds:

$$R(t) = 1-F(t),\ t\geq 0. \tag{1.7}$$

As a rule the availability of a component and of a system as well as the reliability of a system are dependent of the maintenance applied to them. If no inspection nor repair is applied to a component or a system the availability and the reliability are identical and simple to calculate (cf. chapter 3):

$$A(t) = R(t) = 1-F(t),\ t\geq 0. \tag{1.8}$$

However, if a component or a system is subjected to maintenance then the calculation of the availability and reliability increases considerably in complexity, especially for large and/or complex systems. Applying FTA, upper- and lowerbounds for the system reliability (or the system lifetime distribution) are calculated if inspection and repair are applied to the

system. By using the theory of Markov chains the lifetime distribution may in fact be calculated exactly. The numerical evaluation, however, is then restricted to rather small systems, i.e. systems with a rather small number of components (see Somma [25]). In the following we shall characterize shortly the calculation of the system's lifetime distribution by means of fault tree analysis; they do not lead to exact calculations but yield upperbounds for F(t).

(B1) For rather small component *unavailabilities* a sharp upperbound for F(t) seems to be the *expected number of system failures* in the time interval [0,t]. But for large time intervals this approximation may give rise to large deviations, it may even become greater than the value one !

(B2) Several systems reach after some time the steady state condition. Lambert [11] introduced for such systems an upperbound for the system's lifetime distribution F(t), the so-called *steady state* upperbound.

(B3) Combination of the methods sub (B1) and (B2) leads to the so-called T*-method: for small t the upperbound is defined by the *expected number of system failures* and for large t by the *steady state* upperbound; here T* is the instant at which the deviation of the expected number of system failures becomes greater than that of the steady state upperbound (cf. Lambert [11]).

(B4) Several authors (cf. Vesely [21], Barlow and Proschan [22], Caldarola [24]) suggest upperbounds for the system's lifetime distribution F(t) by means of fault tree analysis. From these the approach taken by Caldarola [24] is the more attractive one in the author's opinion (cf. chapter 5).

Next we review the calculation of the system availability.
Because a fault tree is a fault oriented graph the system *unavailability* Q(t)=1-A(t) is usually calculated instead of the system availability A(t). Although an exact calculation of Q(t) is in principle possible, mostly upper- and lowerbounds are calculated for Q(t). This because complex systems often contain a large number of minimal cut sets which implies that an exact calculation is very laborious if practically not impossible. We summarize below the basic ideas in deriving the approximations.

(C1) Minimal cut upperbound

Assume that the system (in fact the associated fault tree) has two minimal cut sets M_1 and M_2, respectively. The defined system failure (TOP-event) occurs if at least one of the two minimal cut sets M_1 or M_2 occurs. Denote by A_1 the event "minimal cut set M_1 occurred at instant t" and by A_2 the event "minimal cut set M_2 occurred at instant t". Then the probability Q(t) of system failure at instant t is defined by:

$$Q(t) = Pr\{A_1 \cup A_2\}. \tag{1.9}$$

An upperbound for Q(t) can be derived as follows. First note that for the present case $Pr\{A_1 \cap A_2\} \geq Pr\{A_1\}Pr\{A_2\}$, because both minimal cut sets may share at least one basic event, whereas if they do not A_1 and A_2 are independent. Hence

$$\begin{aligned} Q(t) &= Pr\{A_1\} + Pr\{A_2\} - Pr\{A_1 \cap A_2\} \\ &\leq Pr\{A_1\} + Pr\{A_2\} - Pr\{A_1\}Pr\{A_2\} \\ &= 1 - (1-Pr\{A_2\})(1-Pr\{A_2\}) = Q_u(t), \end{aligned} \tag{1.10}$$

where $Q_u(t)$ is called the *minimal cut upperbound.*
Note that $Q(t)=Q_u(t)$ in the case that the minimal cut sets M_1 and M_2 are mutually independent, i.e. if they do not share components. By means of the minimal path sets a lowerbound for the system unavailability can be obtained.

(C2) The inclusion-exclusion principle

The probability in the right hand side of (1.9) can be developed into:

$$Q(t) = Pr\{A_1\} + Pr\{A_2\} - Pr\{A_1 \cap A_2\}, \tag{1.11}$$

from which it follows that:

$$Q_u(t) = Pr\{A_1\} + Pr\{A_2\} \geq Q(t).$$

If rather small component unavailabilities are used, the upperbound $Q_u(t)$ for the system unavailability Q(t) will in general be a good approximation. In the case that three minimal cut sets M_1, M_2 and

M_3 are present in the system and A_i denotes the event "minimal cut set M_i occurred at instant t" then the system unavailability Q(t) is given by:

$$\begin{aligned} Q(t) &= Pr\{A_1 \cup A_2 \cup A_3\} \\ &= Pr\{A_1\}+Pr\{A_2\}+Pr\{A_3\}-Pr\{A_1 \cap A_2\}-Pr\{A_1 \cap A_3\} \\ &\quad - Pr\{A_2 \cap A_3\}+Pr\{A_1 \cap A_2 \cap A_3\} \end{aligned} \tag{1.12}$$

An upperbound $Q_u(t)$ and a lowerbound $Q_\ell(t)$ for the system unavailability Q(t) are obtained using inequalities that are described in Fréchet [28]:

$$Q_u(t) = Pr\{A_1\}+Pr\{A_2\}+Pr\{A_3\} \geq Q(t)$$

$$Q_\ell(t) = Q_u(t) - Pr\{A_1 \cap A_2\}-Pr\{A_1 \cap A_3\}-Pr\{A_2 \cap A_3\} \leq Q(t)$$

This procedure is called the *inclusion-exclusion principle.*

In the present study this inclusion-exclusion principle is the technique used in deriving upper- and lowerbounds.

1.2.2. Event tree methodology

An event tree is an *inductive* logic diagram. The diagram starts with a given initiating event and shows various sequences of events leading to multiple-outcome states (cf. step (iii) in section 1.1.2.).
With each state is associated a particular consequence (cf. step (vi) in section 1.1.2.).
The event tree methodology is a very useful tool in identifying significant accident sequences, such as for instance those which are associated with nuclear power plant accidents. It also provides the necessary framework for the overall risk assessment by (cf. Lambert [11]):

(i) providing a basis in defining accident scenarios for each initiating event,

(ii) by depicting the relationship of success and failure of safety related systems associated with various accident consequences,

(iii) providing a means defining TOP-events for system fault trees.

A simple event tree for a given initiating event is depicted in fig. 1.3. With respect to the accident sequence two systems S_1 and S_2 are involved such that system S_2 has to become operational after system S_1. If the systems S_1 and S_2 are asked to become operational and to perform their intended functions, they may succeed (S) in performing that function or they may fail (F). The probability that system S_1 fails is denoted by q_1. This implies that the probability that system S_1 succeeds equals $1-q_1$.

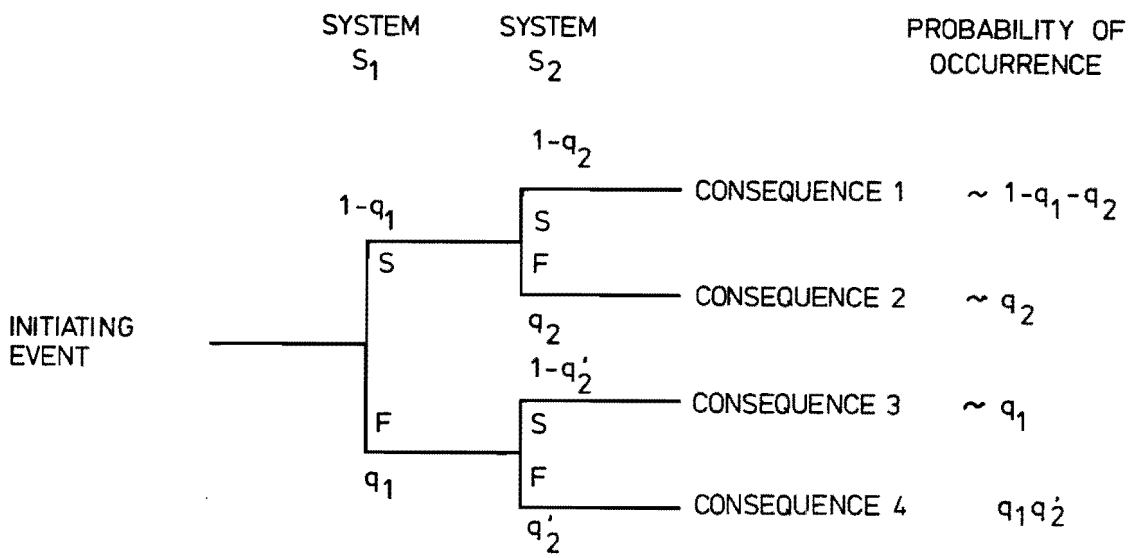


FIG. 1.3. SIMPLE EVENT TREE.

In general a failure of system S_2 is dependent on the state of system S_1 because of system dependencies. If system S_1 does not fail the probability of failure of system S_2 is denoted by q_2, and if system S_1 fails it is given by q_2'. In the case that system S_1 and system S_2 are independent (do not share components) then q_2' equals q_2.

In fig. 1.3. the probability of occurrence is denoted behind each accident sequence. The consequences are not explicitly given but only numbered. The probability of occurrence of each *branch*, i.e. each accident sequence, is simply obtained by multiplying the failure or success probabilities of the systems in that branch. For instance the probability of occurrence of consequence 1 is given by $(1-q_1)(1-q_2) \sim 1-q_1-q_2$, if the probabilities q_1 and q_2 are sufficiently small.

Note that the calculated probabilities in the example of fig. 1.3. are *conditional* probabilities with respect to the initiating event.

For a risk assessment the *absolute* probabilities have to be calculated, i.e. the conditional probability of each branch has to be multiplied with the probability of occurrence of the initiating event (like an explosion, a fire, etc.).
Assume that system S_1 in fig. 1.3. is the system of fig. 1.1. and the system S_2 is given by the functional block diagram of fig. 1.4.
Fig. 1.5. represents the fault tree belonging to the system of fig. 1.4.
Note that system S_1 and S_2 have common components, viz. A and B. It is obvious that system S_2 fails if at least one of the two components A or B fails.

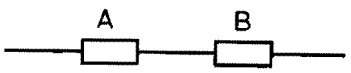


FIG. 1.4. FUNCTIONAL BLOCK-DIAGRAM OF SYSTEM S_2.

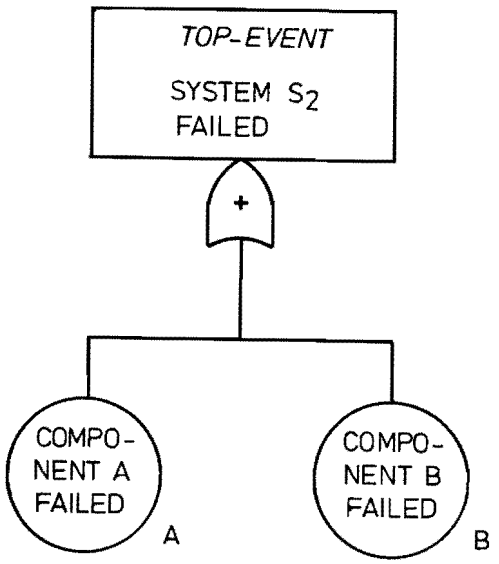


FIG. 1.5. FAULT TREE FOR SYSTEM S_2.

Therefore the minimal cut sets N_1 and N_2 of the fault tree of system S_2 are given by:

$$N_1 = \{A\},$$
$$N_2 = \{B\}. \qquad (1.13)$$

From the minimal cut sets of system S_1 in (1.1) and of system S_2 in (1.13) it is seen that there is a strong dependence between the two systems. For example, if the minimal cut set M_1 of system S_1 occurs, it introduces the occurrence of minimal cut set N_1 of system S_2 because both cut sets

are identical: $M_1=N_1=\{A\}$. The same is true for M_2 with respect to N_2. Here M_2 contains a minimal cut set of system S_2, i.e. $N_2=\{B\}$. So in this special case a failure of system S_1 leads with certainty to a failure of system S_2. *Therefore branch 3 of the event tree in fig. 1.3. can not occur* in this special example. We have just treated the case that a *total system failure* of one system can lead to a *total system failure* of a subsequent system. But also a *partial system failure*, e.g. a failure of a part of the system which does not hamper the system performance, can introduce this phenomenon. In our example of the two systems S_1 and S_2 it is clear from the minimal cut sets M_1 and M_2 that if the components A and C do not fail during the operational time interval of system S_1 but component B does fail then minimal cut set N_2 of system S_2 is introduced which means that system S_2 is failed.
In the past the analysis of total or partial system failure of one system caused by total or partial system failure of another system has been based mainly on engineering judgement. *The methodology developed in the present study analyzes these phenomena exhaustively.*

Up to now only *static* event trees have been developed. This means that within the event tree no instants at which the several systems are demanded for operation, and neither time intervals during which the several systems have to perform their intended functions are incorporated. Only functional sequential arrangement is taken into account. However, the need for *dynamic* event trees, i.e. event trees which contain the mentioned time dependent aspects, is still growing, especially after the incident at Three Miles Island.
The methodology of the present study can treat both types of event trees, i.e. it is able to treat static as well as dynamic event trees.

1.2.3. Phased mission analysis

A first formal mathematical description of the phased mission problem is given by Ziehms [15]. Because that description is clear and contains also some model assumptions we present it here:
"A system consists of several components. The components perform independently of each other, and each of them can be in one of two states, functioning or failed. No component can be repaired or replaced, and each component has a life. The system performs a mission which can be divided

into consecutive time periods, or phases. During each phase it has to accomplish a specified task. From the system configuration (a subset of the components and their functional organization which can be represented, for instance, by a block diagram or a fault tree) changes from phase to phase. As is the case with individual components, only two states of the system are recognized, functioning or failed.
With this situation in mind, the problem itself can be stated as:
Given the survival characteristics of the components, the relevant system configuration in each phase, and the duration of the phases, what is the probability that the system will function throughout the mission, i.e. the mission reliability for the system ?"

Now assume that a system S has to perform a phased mission that consists of two phases, a phase 1 during which subsystem S_1 (a subset of components of system S with their logical relationship) has to perform its intended function and a phase 2 during which subsystem S_2 has to carry out its intended function. Then the time schedule for this phased mission is as depicted in fig. 1.6. The mission starts at instant t=0. The first phase ends at instant T_1 at which the second phase starts. The second phase terminates at instant T_2. So the duration times of phase 1 and phase 2 are T_1 and T_2-T_1, respectively.

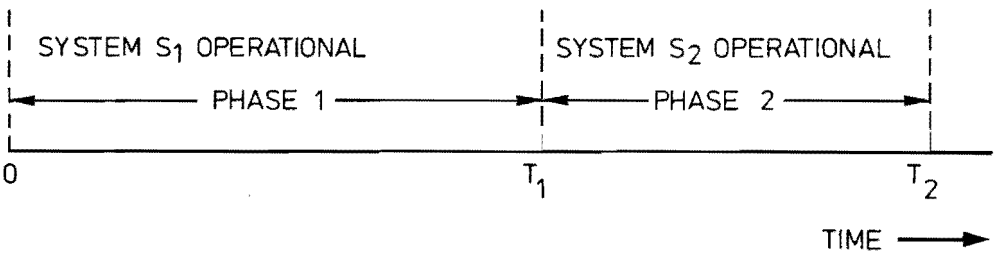


FIG. 1.6. PHASED MISSION TIME SCHEDULE FOR A PHASED MISSION WITH TWO PHASES.

The main characteristic of the methodology provided by Ziehms [15] is that it transforms a multi-phase mission to a single phase mission, i.e. the several subsystems of each phase are transferred into one functional series of systems. Speaking in terms of fault trees it transforms the separate fault trees of the different phases into one fault tree of which the TOP-event is an OR-gate with the TOP-events of the different fault trees as inputs.

To obtain such a transformation from several systems to one system a component transformation has to be accomplished. With the assumption that no repair of a component is allowed, so that its life in phase 2 is dependent on the state of the component at the end of phase 1, such a transformation is realised as follows.
Assume that component c is present in subsystem S_2, that operates during phase 2. Then replace component c in phase 2 by a series system of pseudo-components c_1 and c_2. Pseudo-component c_1 has the original lifetime distribution of component c and pseudo-component c_2 has a lifetime distribution that is conditional to the survival of component c of phase 1, i.e. c_2 possesses the residual lifetime distribution of component c.
Ziehms proves that the thus constructed single phase system has the same reliability as the multi-phase mission. Further he derives an upper- and a lowerbound for the mission reliability by means of this methodology.
In a later paper (cf. Ziehms [14]) he derives new upper- and lowerbounds by means of "cut set cancellation" and the so-called "hazard transform".
Bell [1] is the first one who treats phased missions of maintained systems, although inspection and repair is only permitted during the *operational readiness* phase (OR-phase), which is the time between the installation of the system and the start of the phased mission. For the probability calculations during the phased mission itself he applies the methodology suggested by Ziehms and therefore the only difference with respect to the method of Ziehms is that the probability that a component is in the function state at the start of the mission at instant T_0 (see fig. 1.7.) is not by definition one but may be smaller than one.
On the other hand Bell [1] treats in his study phased missions with *multiple objectives* (see chapter 8).

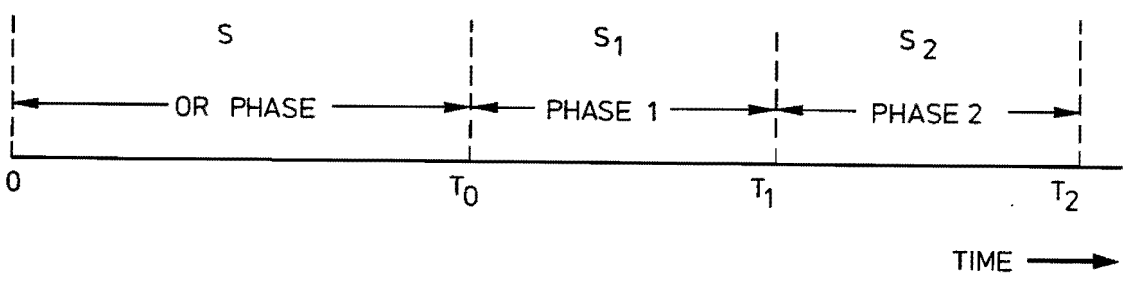


FIG. 1.7. PHASED MISSION TIME SCHEDULE FOR A PHASED MISSION WITH TWO PHASES AND AN OPERATIONAL READINESS PHASE.

Concerning the methodology suggested by Ziehms the following remarks can be made:

(D1) if the correct input data for the components are available then the mission reliability can be calculated by standard methods that are available for single system analysis (see section 1.2.1.);

(D2) the introduction of pseudo-components gives rise to a substantial growth in the number of components, especially in the case of large systems. This large number of created components can lead to practical intractable problems, despite reduction methods such like *cut set cancellation*;

(D3) the method is only applicable for systems that consist during the mission of non-repairable components. We shall demonstrate this by the following argument: assume that a component is repairable during the phased mission. Assume further that the component fails in phase j_1, that the failure of the component is detected and that repair finishes within phase j_2, $j_2 > j_1$. So the component starts a new life somewhere in phase j_2. If the component is also present in the later phase k, $k > j_2 > j_1$, then it should have been replaced in the k^{th} phase by k pseudo-components in case of no repair. But in our situation (repair applied) it has to be replaced by $k-j_2+1$ pseudo-components. This argument shows that the number of pseudo-components for a phase in case of a repair procedure is no longer a fixed number. Therefore, the component transformation as suggested by Ziehms can no longer be easily applied.

Clarotti et al [26] treat phased missions with repairable components by means of the theory of Markov chains as well as by applying fault tree analysis. In their model *on-line* repair is allowed during the OR-phase and during the mission itself. They point out that for their model the analysis by means of Markov chains leads to an exact solution with respect to the probability of mission success, whereas by the application of fault tree analysis an upperbound is obtained for the probability of mission failure. Some aspects of their model give rise to the following remarks.

(D4) By means of fault tree analysis an *upperbound* for the probability of mission failure is obtained, but they do not produce a *lowerbound* for the same quantity. This implies that no insight can be obtained

in the deviation[+] with respect to the exact solution.

(D5) * A number of conditional probabilities are very roughly approximated by one.
* It is assumed that in some cases the mean repairtime is small when compared to the phase duration times. This is not always the case. For instance in case of a LOCA for a BWR (see chapter 2) the first phase lasts half an hour whereas the mean repairtimes are longer.

(D6) From their model description it is not clear which inspection procedures are applied during the phased mission itself.

Fussell [27] treats in his report the *availability*, the *reliability*, the *expected number of failures* and *importance criteria* for a phased mission that contains systems with repairable components. As in the model of Clarotti et al [26] it is assumed that *on-line repair* is possible. Concerning his approach we make the following remarks.

(D7) Only upperbounds are provided for the unavailability during the mission and for the probability of mission failure; therefore no calculation is possible with respect to the deviation[+].

(D8) The methods used for the approximations in (D7) are rather rough and the dependencies between the systems are not fully taken into account.

(D9) The calculation of the *expected number of failures* of the whole system during the mission, which implies probability calculations at epochs at which phases terminate and start, is very laborious. Further, minimal cut sets as well as minimal path sets are required for the calculation.

Other authors that have treated phased mission analysis are Cambell [33] and Montague [34]. Their model assumptions and results are presented in the report of Fussell [27].
Furthermore we mention the papers by Esary [6], Burdick et al [2] and Pedar and Sarma [35].
Finally, we like to make a remark that holds for the models of all the mentioned authors that have discussed phased mission analysis:

[+]deviation means the difference between the upper- and lowerbound for the probability of mission failure (or success).

(D10) The definition of a phased mission as given by Ziehms at the beginning of section 1.2.3. is directed to phased mission reliability. With respect to risk analysis this means that only the probability of the occurrence of the upperbranch of an event tree (see fig. 1.3.) is treated.
The other branches can not be evaluated by the analysis presented by the authors mentioned above.

1.3. The present study

1.3.1. The motivation for the present study

Fussell and Arendt [36] discuss in their paper on system reliability a number of problem areas in engineering methodology. From their paper we cite the following concerning dependencies in event trees, with regard to our example of the event tree in fig. 1.3.:

(E1) *"Usually only one fault tree is developed for a given system failure, but sometimes more than one fault tree is needed. In the example shown in fig. 1.3., if system S_1 succeeds, the fault tree for system S_2 could be different than that for the case when system S_1 fails".*

With respect to repair calculation we quote from the same paper:

(E2) *"... therefore the techniques for treating components with other than constant repair rules are tedious and theoretically unknown".*

A final quotation of their paper concerns phased mission analysis:

(E3) *"Present theoretical methods for analyzing phased missions are limited. The need to be able to treat repairable systems undergoing a phased mission is a problem that needs attention".*

A remark by Vesely and Levine from their paper "Prospects and problems in risk analysis" which is contained in Fussell and Burdick [37] reads:

(E4) *"Reliability analysis is generally concerned with system operability or unavailability. The question of functionability, i.e. whether the system performs its required function when it operates, is generally not treated probabilistically in such analyses. It is possible that,*

in some cases, functional analyses could show the likelihood of functionability failure to be higher than operability failure, thus invalidating a conventionally done reliability analysis. Fortunately, most functionability analyses are done very conservatively so that this is not likely to happen".

These quotations lead to the following remarks.

(F1) There are difficulties in treating the probability of occurrence of every branch of an event tree (cf. (E1)).

(F2) The available models in literature concerning phased mission analysis need to be extended to systems that may be repaired during the mission (cf. (E3)).

(F3) The correspondence between the branch of an event tree where every subsystem successfully performs its required function and a phased mission is not noticed in literature (cf. (E1) and (E3)).

(F4) There is a need for component models with unspecified lifetime and repairtime distributions, i.e. a model not especially based only on negative exponential distributed lifetimes and repairtimes (cf. (E2)).

(F5) There exists a feeling that system reliability calculations in the past have been performed in such a way that the results were nearly in all cases conservative (cf. E4)).

The motivation for the present study stems from the remarks (F1),...,(F5). The present study is mainly concerned with points (F1),...,(F4). By the results so obtained a discussion of point (F5) will be given.

1.3.2. The goals of the present study

The goals of the present study are strongly related to the problems that are treated in the remarks (F1),...,(F4). These goals are formulated as follows:

(G1) develop a general theory that treats the probability of occurrence of each branch of an event tree and that takes correctly into account the dependencies between systems;

(G2) incorporate within the general theory the solution of the problem of phased mission analysis as it has been indicated in section 1.2.3.;

(G3) include in the general model components, that may or may not be repairable, with general lifetime and repairtime distribution, i.e. in the model repairable systems should be taken into account;

(G4) develop a computer program that is based on this general theory, i.e. a computer program that is able to perform fully the probabilistic calculations of a risk analysis and that can handle in a correct way phased mission analysis of repairable systems.

1.3.3. The model and the applied methodology

1.3.3.1. Model assumptions concerning systems and components

Before discussing the methodology we shall first treat a more general definition of a phased mission (cf. chapter 2). To state this general definition we first need the model assumptions concerning systems and components.

The model assumptions for a system are:

(H1) it is assumed that each system is *coherent*, i.e. every component is relevant to the system and a failing component does not lead to a better system performance;

(H2) a system can be in one of two states; i.e. the *fail* state or the *function* state;

(H3) no repair is allowed to a system when it is *operational*, i.e. no *on-line* repair is allowed. If during certain time intervals the system is not operational then repair may be applied.

For components the following model assumptions are introduced:

(H4) the successive lifetimes of a component, which occur in the case that a component is subjected to a repair policy, are assumed to be independent identically distributed variables. The same is valid with respect to the successive repairtimes of the component;

(H5) the lifetimes of the different components of a system are assumed to be mutually independent stochastic variables. The same holds for the repairtimes of the different components. Lifetimes and repairtimes are assumed to be independent;

(H6) each component can be in one of two states, i.e. the *fail* state or the *function* state;

(H7) it is assumed that when repair of a component has been completed the component is as good as new and starts a new life.

1.3.3.2. The extended definition of a phased mission

According to assumption (H2) it is seen in fig. 1.3. that within an event tree both states, i.e. the function state and the fail state, of a system may occur and each of them give rise to another branch. For instance, the function state of system S_2 in fig. 1.3. provides branch 1 and 3 whereas the fail state initiates branch 2 and 4. From fig. 1.3. it is clear that branch 1 occurs if system S_1 as well as system S_2 succeed, whereas branch 2 occurs if system S_1 succeeds and system S_2 fails. If we assign to each system S_j a binary variable u_j such that:

$$\begin{aligned} u_j &= 1, \text{ if system } S_j \text{ succeeds,} \\ &= 0, \text{ if system } S_j \text{ fails,} \end{aligned} \tag{1.14}$$

then each branch of the event tree in fig. 1.3. can be described by means of the two variables u_1 and u_2, e.g. branch 1 is defined by $u_1=1$ and $u_2=1$ and branch 3 by $u_1=0$ and $u_2=1$, which will be denoted in the following by $\{u_1=1,u_2=1\}$ and $\{u_1=0,u_2=1\}$, respectively.
Assume that the initiating event of the event tree in fig. 1.3. occurs at instant T_0 and that in order to handle the consequences of this initial event system S_1 has to function from T_0 to T_1 and system S_2 subsequently from T_1 to T_2. In fact we now have identified branch 1 (system S_1 and system S_2 survive) as a phased mission with the time schedule of fig. 1.7., i.e. the time interval $[0,T_0]$ can be considered as the OR-phase and the time intervals $[T_0,T_1]$ and $[T_1,T_2]$ can be defined to be phase 1 and phase 2. Branch 2 of the event tree in fig. 1.3. is obtained if system S_1 survives the interval $[T_0,T_1]$ and system S_2 is in the fail state at instant T_1

or functions at instant T_1 and fails during the time interval $(T_1,T_2]$. Because there is a strong correspondence between branch 1 and branch 2 it is reasonable *to define branch 2 also as a phased mission.* Since the definition of a phased mission as given in literature (see section 1.2.3.) does not cover this special situation, we have extended it. This extension is mainly concerned with the task of a system, viz. system S_j survives its phase or fails during its phase. The survival of system S_j is indicated by $u_j=1$, whereas its failure is denoted by $u_j=0$. Because each branch of an event tree can be characterized by such a sequence of u_j's as defined by (1.14), the general definition of a phased mission can be formulated as:

> *a sequence of u_j's, $j=1,2,\ldots,K$, K being the number of phases and u_j being a binary variable that indicates whether system S_j survives or fails during its phase, is called a phased mission.* (1.15)

With definition (1.15) every branch of an event tree is now defined to be a phased mission. In our example of the event tree in fig. 1.3. four phased missions can be identified, i.e. $\{u_1=1,u_2=1\}$ (branch 1), $\{u_1=1,u_2=0\}$ (branch 2), $\{u_1=0,u_2=1\}$ (branch 3) and $\{u_1=0,u_2=0\}$ (branch 4).

1.3.3.3. Calculation procedure for the probability of occurrence of a phased mission

Denote by:

$S_j(T_j)$: the event that system S_j survives the time interval $[T_{j-1},T_j]$, i.e. system S_j survives phase j;

$\overline{S_j(T_j)}$: the event that system S_j is failed at instant T_{j-1} or that system S_j functions at instant T_{j-1} and fails during the time interval $(T_{j-1},T_j]$, $j=1,\ldots,K$; K being the number of systems that occur in the phased mission. (1.15)

As an example we take the event tree of fig. 1.3. with system S_1 given by the fault tree of fig. 1.2. and system S_2 by the fault tree of fig. 1.5. The minimal cut sets of the systems S_1 and S_2 are given by (1.1) and (1.13), respectively.

The calculation of the probability of mission success for the phased mission $\{u_1=1,u_2=1\}$, i.e. the probability of occurrence of the upper-branch of the event tree, is identical to the calculation of the probability that system S_1 as well as S_2 survive their respective phases. With (1.15) we get for the probability $M_0(T_0)$ of the occurrence of the upperbranch of the event tree:

$$\begin{aligned} M_0(T_0) &= Pr\{u_1=1,u_2=1\} \\ &= Pr\{S_1(T_1) \cap S_2(T_2)\} \\ &= 1 - Pr\{\overline{S_2(T_1)} \cup \overline{S_2(T_2)}\} \\ &= 1 - [Pr\{\overline{S_1(T_1)}\} + Pr\{\overline{S_2(T_2)}\} - Pr\{\overline{S_1(T_1)} \cap \overline{S_2(T_2)}\}]. \end{aligned} \tag{1.16}$$

The probability $M_0(T_0)$ of mission success in (1.16) is expressed by the probabilities of single system failure and the probability of joint system failure. Because no repair is applied to a system when it is operational (assumption (H3)) the $Pr\{S_1(T_1)\}$ is simply the system availability of system S_1 at instant T_1, and therefore its complement $Pr\{\overline{S_1(T_1)}\}$ is the system unavailability at instant T_1. Also $Pr\{\overline{S_2(T_2)}\}$ is the system unavailability of system S_2 at instant T_2. Denote the occurrence of the fail state of the components A, B and C at instant T_1 by $A(T_1)$, $B(T_1)$ and $C(T_1)$, respectively. The single system unavailability is treated in section 1.2.1. It then follows by the use of (1.1) that:

$$\begin{aligned} Pr\{\overline{S_1(T_1)}\} &= Pr\{A(T_1) \cup (B(T_1) \cap C(T_1))\} \\ &= Pr\{A(T_1)\} + Pr\{B(T_1) \cap C(T_1)\} - Pr\{A(T_1) \cap B(T_1) \cap C(T_1)\} \\ &= Pr\{A(T_1)\} + Pr\{B(T_1)\}Pr\{C(T_1)\} \\ &\quad - Pr\{A(T_1)\}Pr\{B(T_1)\}Pr\{C(T_1)\}\ , \end{aligned} \tag{1.17}$$

the second equality sign based on the mutual independencies of the components. Denote by $q_A(t)$, $q_B(t)$ and $q_C(t)$ the unavailabilities of the components A, B and C at instant t. Then relation (1.17) becomes:

$$Pr\{\overline{S_1(T_1)}\} = q_A(T_1) + q_B(T_1)q_C(T_1) - q_A(T_1)q_B(T_1)q_C(T_1)\ . \tag{1.18}$$

In the same way we get:

$$\Pr\{\overline{S_2(T_2)}\} = q_A(T_2)+q_B(T_2)-q_A(T_2)q_B(T_2) \ . \qquad (1.19)$$

Remains to develop in (1.16) the probability of joint system failure, i.e. $\Pr\{\overline{S_1(T_1)} \cap \overline{S_2(T_2)}\}$. Because of assumption (H3) we obtain with (1.1) and (1.13):

$$\Pr\{\overline{S_1(T_1)} \cap \overline{S_2(T_2)}\} = \Pr\{(M_1 \cup M_2)\cap(N_1 \cup N_2)\},$$

$$= \Pr\{(M_1 \cap N_1)\cup(M_1 \cap N_2)\cup(M_2 \cap N_1)\cup(M_2 \cap N_2)\}, \qquad (1.20)$$

with the occurrence of M_1 and M_2 related to instant T_1 and that of N_1 and N_2 related to instant T_2. The development of (1.20) leads to (cf. (1.10)):

$$\Pr\{\overline{S_1(T_1)}\cap\overline{S_2(T_2)}\} = \Pr\{M_1 \cap N_1\}+\Pr\{M_1 \cap N_2\}+\Pr\{M_2 \cap N_1\}+\Pr\{M_2 \cap N_2\}$$

$$- \ \ldots \ - \Pr\{M_1 \cap M_2 \cap N_1 \cap N_2\} \ , \qquad (1.21)$$

with the terms containing the two-fold and three-fold intersections not explicitly written down because no further information concerning the applied method is gained from them.

Because the minimal cut sets N_1 and N_2 appear in a later phase, i.e. phase 2, than the minimal cut sets M_1 and M_2 which occur in phase 1, the probabilities in (1.21) are conditioned to minimal cut sets that appear in phase 1:

$$\Pr\{\overline{S_1(T_1)}\cap\overline{S_2(T_2)}\} = \Pr\{N_1|M_1\}\Pr\{M_1\}+\Pr\{N_2|M_1\}\Pr\{M_1\}$$

$$+ \Pr\{N_1|M_2\}\Pr\{M_2\}+\Pr\{N_2|M_2\}\Pr\{M_2\}- \ \ldots$$

$$- \Pr\{N_1 \cap N_2|M_1 \cap M_2\}\Pr\{M_1 \cap M_2\} \ . \qquad (1.22)$$

The next step is the replacement of the minimal cut sets in (1.22) by the components which are contained in them. Therefore we get with (1.1) and (1.13):

$$\begin{aligned}\Pr\{\overline{S_1(T_1)}\cap\overline{S_2(T_2)}\} = {} & \Pr\{A(T_2)\,|\,A(T_1)\}\Pr\{A(T_1)\} \\ & + \Pr\{B(T_2)\,|\,A(T_1)\}\Pr\{A(T_1)\} \\ & + \Pr\{A(T_2)\,|\,B(T_1)\cap C(T_1)\}\Pr\{B(T_1)\cap C(T_1)\} \\ & + \Pr\{B(T_2)\,|\,B(T_1)\cap C(T_1)\}\Pr\{B(T_1)\cap C(T_1)\} \\ & - \ldots \\ & - \Pr\{A(T_2)\cap B(T_2)\,|\,A(T_1)\cap B(T_1)\cap C(T_1)\} \\ & \quad . \Pr\{A(T_1)\cap B(T_1)\cap C(T_1)\} \; . \end{aligned} \tag{1.23}$$

Because of the mutual independence of the components and with $q_A(T_1) = \Pr\{A(T_1)\}$, etc. we obtain finally for the probability of the joint failure of system S_1 and system S_2:

$$\begin{aligned}\Pr\{\overline{S_1(T_1)}\cap\overline{S_2(T_2)}\} = {} & \Pr\{A(T_2)\,|\,A(T_1)\}q_A(T_1)+q_A(T_1)q_B(T_2) \\ & + q_A(T_2)q_B(T_1)q_C(T_1) \\ & + \Pr\{B(T_2)\,|\,B(T_1)\}q_B(T_1)q_C(T_1) - \ldots \\ & - \Pr\{A(T_2)\,|\,A(T_1)\}\Pr\{B(T_2)\,|\,B(T_1)\} \\ & \quad . q_A(T_1)q_B(T_1)q_C(T_1) \; , \end{aligned} \tag{1.24}$$

with $\Pr\{A(T_2)\,|\,A(T_1)\}$ being the conditional probability that component A is in the fail state at instant T_2 whenever that component A was in the fail state at instant T_1.

From the relations (1.16), (1.18), (1.19) and (1.24) it is seen that the probability $M_0(T_0)$ has been completely reduced from system unavailabilities to absolute and conditional component unavailabilities. This implies that if the component unavailabilities are calculated the probability $M_0(T_0)$ of mission success for the phased mission $\{u_1=1, u_2=1\}$ is completely determined.

Note that the applied method reduces system dependencies (e.g. at the phase boundaries) to component dependencies. This means that the probability calculations for complex system behaviour are reduced to probability calculations of single component behaviour, although intricate component models are needed to calculate single component behaviour (cf. section 1.3.3.4.).

The probability $M_2(T_0)$ of mission success for the phased mission $\{u_1=1, u_2=0\}$, i.e. the probability of occurrence of the second branch is given by:

$$M_2(T_0) = \Pr\{S_1(T_1) \cap \overline{S_2(T_2)}\}$$

$$= \Pr\{\overline{S_2(T_2)}\} - \Pr\{\overline{S_1(T_1) \cap S_2(T_2)}\} \quad . \tag{1.25}$$

From (1.25) it is seen that $M_2(T_0)$ is obtained by a relation which consists of a number of terms that also occur in (1.16). This implies that if T_1 and T_2 are the same for (1.16) and (1.25) then the probability $M_2(T_0)$ of mission success for branch 2 and $M_1(T_0)$ can be calculated simultaneously.

By the same method as applied to $M_2(T_0)$ we obtain for the probability $M_3(T_0)$ of occurrence of branch 3:

$$M_3(T_0) = \Pr\{\overline{S_1(T_1)}\} - \Pr\{\overline{S_1(T_1) \cap S_2(T_2)}\} \quad , \tag{1.26}$$

whereas $M_4(T_0) = \Pr\{\overline{S_1(T_1) \cap S_2(T_2)}\}$. In practical situations, i.e. for large systems, the technique of calculating the various branch probabilities is too laborious, Therefore upper- and lowerbounds are needed for the probability of mission success. They are obtained by the inclusion-exclusion principle (see section 1.2.1.(C2)).

As a final remark we can state that with the extended definition of a phased mission the probability of mission success for every phased mission as defined in existing literature as well as the probability of occurrence of every branch of an event tree can be obtained by the application of the above mentioned methodology which takes fully into account existing system dependencies.

1.3.3.4. Component behaviour during a phased mission

As it has been shown in section 1.3.3.3. the component unavailabilities are basic for the calculation of the probability of phased mission success. Component models are developed in the present study in order to obtain the component unavailabilities during the mission.

Consider a phased mission that consists of four phases. The mission starts at instant T_0 and the endpoints of the phases 1, 2, 3, and 4, are marked by the instants T_1, T_2, T_3 and T_4.
During each phase a system is operational, i.e. system S_1 is operational during phase 1, etc. Now assume that a component is part of the systems S_1, S_3 and S_4 and does not belong to system S_2. This means that the component has to be *operational* during phase 1, phase 3 and phase 4 and is *dormant* during the OR-phase and phase 2. So the time schedule of the component contains a *first* dormant part (OR-phase), a *first* operational part (phase 1), a *second* dormant part (phase 2) and a *second* operational part (phase 3 and phase 4). This situation is shown in fig. 1.8.

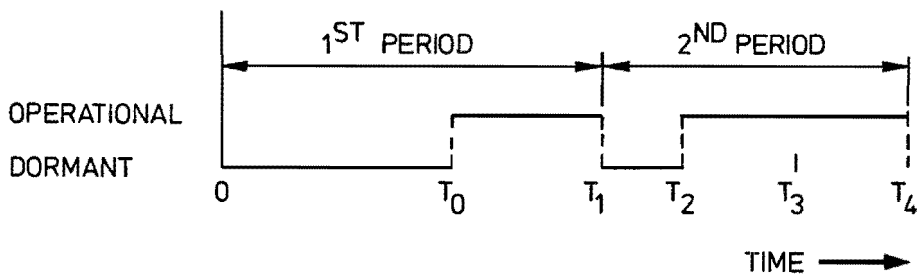


FIG. 1.8. COMPONENT OPERATIONAL DURING THE FIRST, THIRD AND FOURTH PHASE.

Because a dormant part and its subsequent operational part together form a recurrent phenomenon we introduce the notion *a period of a component*, i.e. starting at the instant t=0 the first period consists of the first dormant part together with the following operational part, etc. (see fig. 1.6.). From assumption (H3) it is obvious that during the dormant part of a period of a component that component may be repaired if it is in the fail state, but that during an operational part of a period no repair may be applied to the component.

The notion "period of a component" is basic for the treatment of the component unavailability during a phased mission.
With respect to maintenance procedures to which a component may be subjected the following classes of components are considered in this study:

class 1 : components that are not inspected and therefore they may be considered as *non-repairable*;

class 2 : monitored components, i.e. components that are *continuously* inspected;

class 3 : components that are inspected at *random times*;

class 4 : *periodically* inspected components.

For each of these classes of components formulas have been developed for the component's unavailability for the case of unspecified lifetime and repairtime distributions.
Because the component models for a phased mission are rather complicated they are not further discussed here. For a detailed treatment see chapter 4 of the present study.

1.3.3.5. The reliability computer program PHAMISS

For the general theory as presented in this study the reliability computer program PHAMISS is developed. Single systems as well as phased missions can be treated by PHAMISS.
PHAMISS consists of several program sections, viz.:

- FAULTTREE (minimal cut set determination)
- PROBCAL (availability calculations for a single system as well as for phased missions)
- IMPCAL (importance calculations)
- COMMODE (common cause determination)

The program section FAULTTREE is basic for further calculations by PHAMISS. FAULTTREE generates the minimal cut sets of a single tree or, in case of a phased mission, the minimal cut sets of several trees (up to 10). FAULTTREE is based on bit manipulation, i.e. for each basic event and each gate one bit is needed to represent the event. For each fault tree the basic event failure data (if available) and the minimal cut sets of the fault tree are automatically stored on a permanent device by FAULTTREE.

From this "save" file further qualitative and/or quantitative analyses can be performed. Each of the program sections PROBCAL, IMPCAL and COMMODE can be handled together with FAULTTREE or separately. In the last case a "save" file produced by FAULTTREE must be available. As a speciale feature for each of the program sections the used CP and IO times are printed in the output.
The limiting number of basic events and gates together is 4095; there is no limit on the number or size of the minimal cut sets.

The following classes of components are accepted by PROBCAL:

* non-reparaible;
* monitored;
* randomly inspected;
* periodically inspected *EXSITU* (not accessible during inspection);
* periodically inspected *INSITU* (accessible during inspection);
* constant unavailability;
* constant unavailability during the dormant phase and non-repairable during the operational phase of the mission.

PHAMISS calculates for a single system the time dependent unavailability and for a phased mission an upperbound for the probability of mission success and (optional) the deviation in the upperbound. The input for PHAMISS is *free formatted* and *user friendly*. An exclusive error checking is performed on the input and throughout the whole program.
The program is written in the language FORTRAN-IV for a CDC Cyber-175 computer system. For the program segmented loading is applied. The reliability computer program PHAMISS is developed at ECN (Netherlands Energy Research Foundation).

1.3.3.6. The results of the present study

The main results are:

(I1) the introduction of a general model for the treatment of phased missions as well as for every branch of an event tree and as such the model may have its applications in the following fields:

* risk analysis (probabilistic treatment of event trees);
* space travel (each space vehicle performs a phased mission);

* aircraft industry (each aircraft performs during a flight a phased mission, e.g. with take-off, cruise flight and landing as possible phases);
* comparison studies for alternative technical systems that have to perform complex tasks;
* efficiency and reliability testing of rescue scenarios which in fact are phased missions;
* economic planning;
* warfare (battle strategies can be considered as phased missions).

(I2) an effective analytical technique that allows the calculation of the probability of phased mission success of the model in (I1). The presented approach shows, within the model assumptions (H1),..., (H7), that:

* in principle an exact solution can be obtained for the probability of phased mission success;
* each branch of an event tree can be considered as a phased mission and therefore it can be treated as such;
* *partial system failures*, i.e. failures within the system that do not introduce the TOP-event, are correctly taken into account within the calculation of the probability of mission success;
* if the probability of occurrence of the upperbranch of an event tree (the branch where every system succeeds) is calculated, and if all the phase duration times are the same for every branch, then the probabilities of occurrence of all the other branches can be calculated simultaneously. If an upperbound for the probability of occurrence of the upperbranch is only needed the latter statement is partially true; then the probabilities of occurrence for branches with exactly one failed system are calculated too.

(I3) a reliability computer program called PHAMISS has been developed on the basis of a general model.

1.3.3.7. A survey of the contents

Chapter 1 serves as an introduction to the problem area of phased mission analysis. Starting with a brief review of reliability and risk analysis (the frame work for the present study), the basic concepts of system reliability, fault tree analysis and phased mission analysis are presented in

so far as the present study deals with such notions and concepts.
The last section of this chapter presents an overview of the present study, its results and its fields of application.
Chapter 2 is fully devoted to the description of the phased mission model that is treated in the present study. The motivation for and the description of the model assumptions are treated in detail. The basic notion *a period of a component* is introduced as well as the extended definition of a phased mission. The possibility of several maintenance strategies leads to the introduction of four component classes, i.e. non-repairable components, continuously inspected components, randomly inspected components and periodically inspected components.
Chapter 3 treats the availability of each of the four classes of components during the OR-phase, i.e. during the time between t=0 and the start of the phased mission. The obtained results are general, in so far as the lifetime and repairtime distributions need no specification. A new model is introduced for components subjected to periodical inspection. This model differs from the other models in literature because of its repairtime distribution. In this new model it is assumed that the repairtime is a stochastic variable. In former models it is assumed to be a constant. For a number of specified lifetime and repairtime distributions the component availabilities are explicitly calculated (see table 3.1.). These calculations are described in appendix B.
Chapter 4 is an extension of chapter 3 in so far that it discusses for each of the four classes of components the availability during the phased mission. The results of this chapter are new. Basic for the component's availability calculation is the *period of a component*. General formulas are obtained for the components availability, the most intricate one being that for a continuously inspected component. The unavailability of such a component can be calculated by means of a *recursive relation*.
For the case of a negative exponential distributed lifetime and repairtime a general analytical solution is obtained from this recursive relation. Because in general no analytical solution can be obtained for this recursive expression a procedure is suggested in section 4.3.4.2.2.(c). by which the availability of the component can be calculated for the k^{th} period. This procedure can be applied for a component with an Erlang-2 lifetime distribution and a negative exponential distributed repairtime.
For components that are randomly inspected and also for those that are

periodically inspected some special assumptions are introduced to avoid unrealistic situations. For each of these two classes of components explicit analytical solutions are obtained, in both cases illustrated for a negative exponential distributed lifetime.
Chapter 5 concerns fault tree analysis. It treats the *qualitative* part, i.e. the construction of the fault tree and the determination of *minimal cut sets* and *minimal path sets*, further the *quantitative* part concerning the *system unavailability*, the *lifetime distribution* and several *measures of importance* are considered.
Chapter 6 deals with a general theory of phased missions, the results of this chapter are new. As an introduction to the general theory first a very simple system performing a phased mission is treated. For this example the methodology is completely written out. An exact solution and upperbound with associated deviation are obtained for the probability of mission success (mission failure for the upperbranch of the event tree) of each branch of the constructed event tree. The discussion terminates with a numerical evaluation. The second part of this chapter treats the general methodology for phased mission analysis as suggested by this study.
The methodology is based on fault tree analysis (see chapter 5). The probabilistic treatment of a phased mission (branch of an event tree) is carried out by means of the following steps:

(i) the probability of mission success is reduced to a simple expression that contains all probabilities of single system failures and of all joint system failures;

(ii) the probabilities in step (i) are reduced to the probabilities of occurrence of the minimal cut sets of these single and joint system failures;

(iii) based on the assumptions that the component's state variables are mutually independent random variables the probabilities of the occurrence of one or more minimal cut sets (from one or from more systems) are reduced to the *absolute* and *conditional* component unavailabilities;

(iv) by applying the results of chapter 4, i.e. the calculation of the component unavailabilities, the probability of mission success can be obtained.

The last part of this chapter treats as an example a loss of coolant accident for a Boiling Water Reactor. The example is taken from Burdick et al [2].
In chapter 7 a short description is given of the reliability computer program PHAMISS that has been developed on the basis of the general methodology as described in the present study. For a detailed description of PHAMISS see Terpstra and Dekker [39].
Chapter 8 contains the conclusions of the present study and recommendations for further work in the field of System Reliability with respect to Phased Mission Analysis.
Appendix A treats the renewal function and residual lifetime distribution of a renewal process without repair in the case of the general Erlang-lifetime distribution and Appendix B contains specifications for several lifetime and repairtime distributions of the quantities discussed in chapter 3.

2. THE MODEL

2.1. Introduction

A set of components *together* with a functional organization (relationship) of these components shall be called a *system*, a specific functional organization of these components will be denoted as a *configuration*. This functional organization of the components may be represented by a reliability network diagram or a fault tree, see Lambert [11]. (In this report we shall only use fault trees, see chapter 5).
The system is said to perform a *mission* if during a determined time period the system has to carry out a task. Suppose that the time period can be divided into consecutive time intervals, such that the system has to accomplish a specific task and its configuration does not change during such an interval. Then such an interval will be called a *phase* of the mission; the components and their specific functional organization present during a phase will be referred to as a *subsystem*. Missions of this type are known in literature as *phased missions*.
Actually, Phased Missions are encountered in many fields; the classical example being the voyage of a space vehicle, and recently a theory of Phased Missions has been developed for missions in space travel. The theory may also be used for predicting the behaviour of technical systems which have to perform a complex task. Other important fields are e.g. testing the efficiency and reliability (performance ability) of scenarios for rescue plans to control the effects of disasters such as the outbreak of dangerous epidemics, earthquakes, large fires and water floods, and in particular possible disasters connected with man made systems such as nuclear power plants. Further it may be expected that the theory may have its applications in economic planning, warfare and election campaigns.
It may be expected that the theory of Phased Missions will become an important tool in risk analysis, see e.g. chapter 6. Because the Phased Mission problems are generally of a rather complex nature, we shall first discuss a few examples. The first example considers a technical safety system of a nuclear power plant, it is taken from Fussell [2]. The second example treats a scenario for rescue organization in the case of water floods, whereas the third example stems from analysis of military operations.

Example 1: "Loss of Coolant" accident in a nuclear power plant.

For a Boiling Water Reactor (BWR) of a nuclear power plant a simplified working scheme is sketched in fig. 2.1. Water is pumped via the condensor through pipe B into the pressure vessel. The water flow passing the heat-generating core vaporises

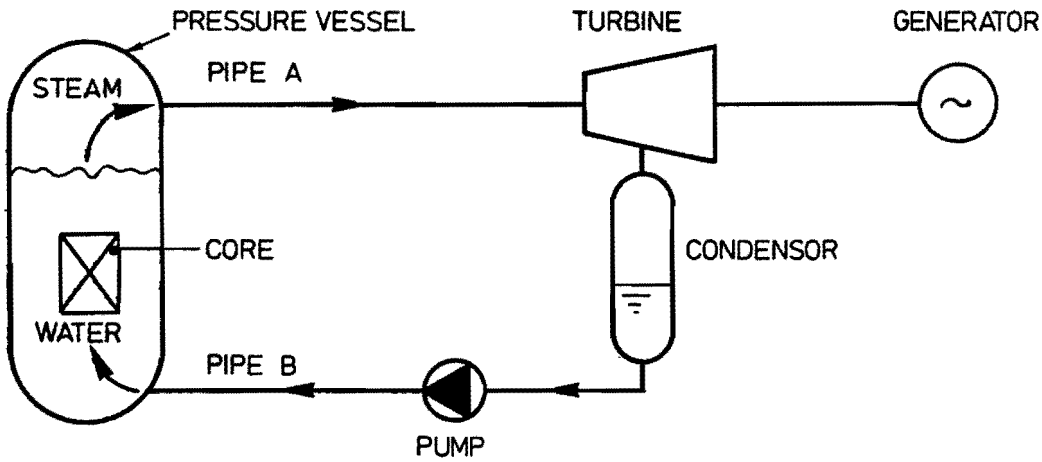


FIG. 2.1. WORKING SCHEME OF A BOILING WATER REACTOR (BWR).

and steam leaving the vessel through pipe A drives the turbine; the generator is powered by the turbine. The steam leaving the turbine is cooled by the condensor (heat exchanger) and pumped back to the pressure vessel.

A so-called "large" Loss of Coolant Accident (LOCA) occurs if suddenly a hole appears in the pressurized system, e.g. due to a heavy pipebreak of pipe B or A. The effect is that the cooling of the core is interrupted, the temperature of the core becomes too high, and it may melt. Such an event leads to very potentially dangerous consequences. A safety system is needed. The mission of the safety system is to prevent overheating of the core and escape of radio active material into the air. Such a system for the BWR is sketched in fig. 2.2. This scheme is oversimplified since we want to illustrate Phased Mission performance and not to discuss a very complex system in detail. The safety system consists of the Emergency Core Cooling System (ECCS), the Suppression Pool Cooling System (SPCS) and the Residual Heat Removal System (RHRS).

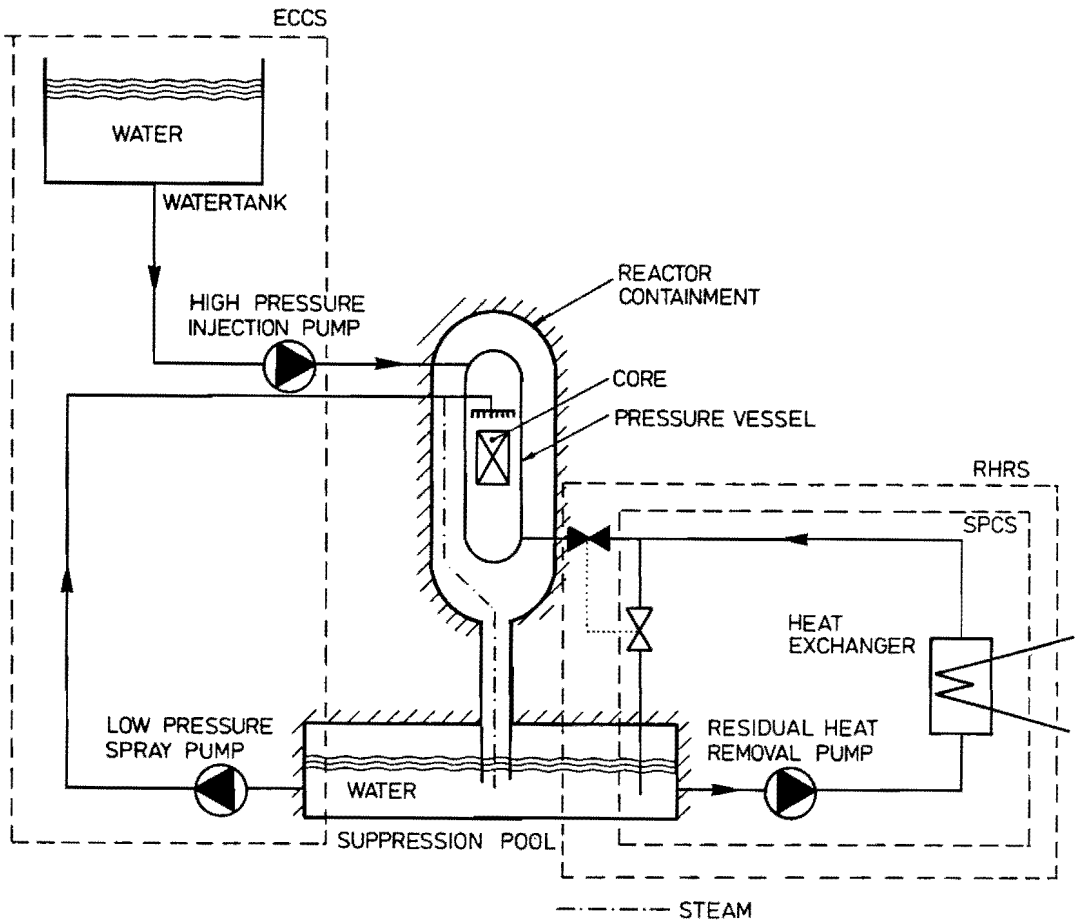


FIG. 2.2. THE SAFETY SYSTEM OF A BWR IN CASE OF A LARGE LOCA.

The first task is to prevent excessive heating of the fuel rods within the reactor vessel immediately after the occurrence of a large LOCA. Therefore the ECCS high and low pressure injection pumps pump water into the vessel. By the very hot core a lot of this water is converted to steam. This steam partially escapes from the reactor vessel. In that case it is led to the suppression pool where it condensates. So the water in the suppression pool is heated by steam. The second task in the mission is now to cool the water in the suppression pool. The SPCS is the designed system to carry out this task. It pumps the water through a heat exchanger and then back to the suppression pool. Because the reactor supplies heat, even when it has stopped generating power, the last task in the mission is to remove this residual heat. It is done by the RHRS, that circulates the water through the core, the suppression pool and the heat exchanger. So each of the mentioned three steps is performed by parts of the total safety system.

So the mission consists of three successive phases:

- Phase 1: Initial core cooling by the ECCS;
- Phase 2: Suppression pool cooling by the SPCS;
- Phase 3: Residual heat removal by the RHRS.

The mission is successful if every phase is successful, i.e. every subsystem survives its appropriate phase. The three subsystems ECCS, SPCS and RHRS are not disjoint. They share a number of components. Because this example is treated extensively in chapter 6 we shall not discuss it further here.

Example 2: Rescue scenario for a waterflood

When a serious flood appears the local population as well as the authorities, the civil servants, the medical service, and so on, have to be alarmed. The first concern is the rescue of lives and evacuation of livestock. This means availability of communication facilities and organization of transport. Also emergency provisions from further damage have to be initiated, and the waterworks for the control of the waterlevel in the area have to be adapted to the emergency situation.
In this example the "disaster plan" i.e. the mission, consists of protecting the lives of people in danger and to restore the inundated area. The system configuration is here the scenario describing the actions to be taken, their timing and the responsibilities and tasks of the various "components" involved, in short the organization of the disaster plan. During the mission we may distinguish roughly the following successive phases:

- Phase 1: Alarming;
- Phase 2: Transport of people and material to the inundated area;
- Phase 3: Evacuation of people in danger and emergency provisions;
- Phase 4: Restoring the inundated area.

For the phases mentioned above a subsystem is needed. Obviously no two subsequent subsystems are identical. For instance, the subsystem functioning during phase 3 does not contain pumps, as it is the case of the subsystem treating phase 4. The mission carried out by the system is considered to be successful if all phases are terminated successfully, which implies that every subsystem survives its phase.

Example 3: Attack of an army group

Consider an army group composed of artillery, cavalry and infantry, each of these sections formed by several smaller army units. The instruction of the army group is to conquer a well defined goal in a fixed time period. To conquer the goal two barriers defended by the enemy have to be taken. The commander of the army group plans the following scheme to succeed:

- First transportation of his army group to a base from which the operation should start;
- Next artillary fire on the first barrier of the enemy during a certain time;
- Then cavalry and infantry should go forward to beat enemy troops and take the first barrier;
- Subsequently artillery and part of the cavalry should open fire on the second barrier;
- After this cannonade the whole infantry and part of the cavalry must storm and beat the enemy resulting in the conquest of the second barrier, the goal is reached.

Obviously the mission is here the conquest of the goal in a planned time period. The components of the system are the commander, the various army units of artillery, cavalry, infantry and the military equipment. The system configuration consists roughly of the military organisation and the strategy. Obviously, the plan described leads to a system with five phases:

- Phase 1: Transportation of the army group to the base from which the attack will start. The whole army group takes part in this action;
- Phase 2: The cannonade by the whole artillery on the first barrier of the enemy;
- Phase 3: The attack of cavalry and infantry on the first barrier. This phase should be split up into more other phases if not the whole of the cavalry and infantry attacks, but combinations of parts of them (e.g. in order to get a continuous strength of the attack);

- Phase 4: Artillery and a part of cavalry together bomb the second barrier of the enemy;
- Phase 5: That part of cavalry that has not fired in the foregoing phase and the whole infantry attack the second barrier to beat the enemy and to occupy the goal.

For each phase the commander of the army group plans a time period so that within the time he got, the operation has succeeded if all phases are successful. Obviously, not every "component" is operational in every phase and the subsystems belonging to each of the phases can now be easily described.

2.2. System and phase modelling

We consider a system S consisting of a number of components $c_i, i=1,\ldots,N$. A subset of this set of components with the relevant components united in a functional relationship so that it can carry out a well defined task, will be called a *subsystem* of system S. The functional relationship between the components of this subsystem will be called the *configuration* of this subsystem.
Henceforth the subsystems will be indicated by $S_j, j=1,\ldots,K$. It should be noted that the sets of components of different subsystems are not necessarily disjoint sets of components. The system S has been designed to perform a task, that consists of K subtasks to be performed in a prescribed order. Each of these subtasks is looked after by a subsysten S_j of S. The time period a subsystem has to operate in order to perform its task is called a *phase*. So phase j is the time interval needed by subsystem S_j to execute part j of the task of system S, $j=1,\ldots,K$. Let system S be installed at time $t=0$, and suppose that S has to start its task at $t=T_0, T_0>0$. T_j shall denote the end of the phase j, $j=0,\ldots,K$. Instead of the word *task* the term *mission* is often used and the time needed to execute the mission is called *mission time*. So a mission is a task performed by system S during a certain time interval. Because of the fact that the time interval needed to perform the mission is split up into a number of phases such a type of mission is called a *phased mission*. Schematically the phased mission is sketched in the next figure.

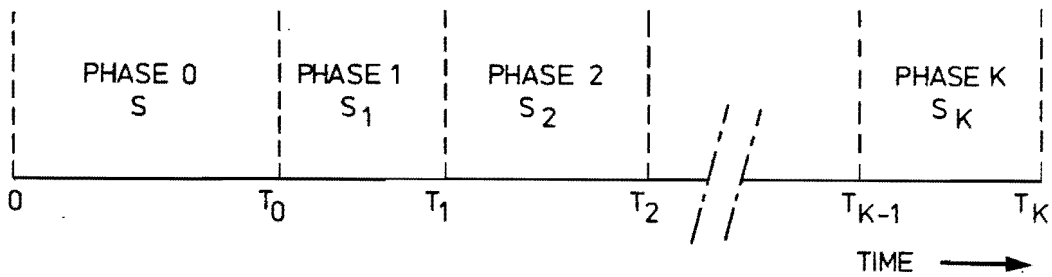


FIG. 2.3. PHASED MISSION CONSISTING OF K PHASES.

During the time interval $(0,T_0)$ the system is in a *dormant* state. This interval is often called the *operational readiness*-phase (OR-phase). In the sequel it will be called phase 0. With this phase we associate by definition the subsystem S_0. (There is no need to specify components and configuration of S_0).

A change from phase j to the next one j+1 is caused by the fact that there is a change in the configuration of system S, i.e. the subsystems S_j and S_{j+1} are not identical. Such a change may be caused by alterations of the hardware and/or of the working mode of one or more components. Changes in the hardware means removing or adding components, whereas changes in the functional relationship of the component means alterations of their working mode. An extreme example for the first case occurs if the subsystems S_j and S_{j+1} have no identical components. A simple example of a change in functional relationship is for instance the situation where subsystem S_j and S_{j+1} differ only by another positioning of a certain switch.

Remark

It is common practice to distinguish components into passive components like vessels, pipes, wiring etc. and active components like pumps, switches etc. The criterion for a component to belong to a subsystem is the following: "failure of the component affects the functioning of the subsystem". No misunderstanding arises for passive components but, possibly, for active components. It is therefore emphasized that for active components the working mode may be *either* passive *or* active, provided of course that the component is relevant.

Phase transition has to be treated carefully in the planning of the phased mission. Therefore we introduce the following definition:

Definition 2.1.

Every change in the hardware configuration and/or components working mode marks the transition from one phase to another phase.

2.3. The period of a component

Consider at time $t, t\in[T_{j-1},T_j)$, component c_i. If component c_i is element of S_j we call component c_i *operational at time t*; if c_i is not element of S_j it is called *dormant at time t*. When component c_i is operational at all time instants of $[t,t+\tau],\tau\geq 0$, it will be said to be operational during that time interval. Also the component is called dormant during a time interval if the component is dormant at every time instant of that interval. From section 2.2. it follows that every component of system S is dormant during the OR-phase (phase 0). Since, by definition, every component is relevant for system S, it is relevant for at least one subsystem of system S, hence the component is operational during at least one phase. So, for every component, the initial dormant time interval is followed by an interval during which the component has to be operational. The first dormant interval together with the subsequent operational interval of component c_i will be called the first *period* of component c_i. The second and following periods are defined similarly if they are present. Obviously *a period consists of a "dormant part" followed by an "operational part"*.

The period of a component is fundamental for the calculation of the availability of the component during the mission, see chapter 4.

For instance, we may have the situation in fig. 2.4. where we see a component with two periods, the component being operational during the first phase and also during the third and fourth phase.

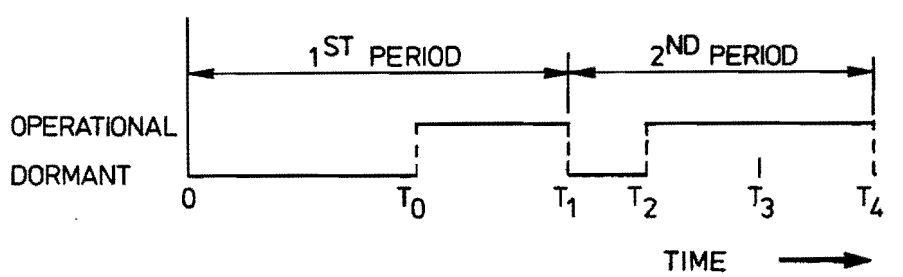


FIG. 2.4. COMPONENT OPERATIONAL DURING THE FIRST, THIRD AND FOURTH PHASE.

2.4. The detailed description of a Phased Mission

Before stating the detailed definition of a phased mission, we shall illustrate the idea behind it by means of an example from risk analysis, although other examples may be given (see for instance example 3 in section 2.1.).

Risk analysis has to deal with two factors, i.e. the probability of occurrence of an accident and the consequences of the accident. When we consider a LOCA (see example 1 in section 2.1.), its immediate consequences may be measured by the amount of radioactive release into the air. To measure the amount of release efficiently, one has to construct an *event tree*; as an example a simple event tree for a large LOCA is sketched in fig. 2.5. The initial accident, i.e. pipe break, is the starting point of the event tree. After the accident has occurred, several subsystems have to operate sequentially in order to control the accident. The state of those subsystems is described in terms of available or not-available, if subsystem operation is required. The sequencing of the subsystems in the event tree depends on their dependency. For instance, if there is no electrical power after pipe break, no other system is able to operate, so electrical power is the first entry in the event tree. In fig. 2.5. the event tree for a LOCA is shown. It consists of a number of branches, for instance, the upper branch describes the situation where after a pipe break electrical power is available and the ECCS is available as soon as electrical power has become available. Similarly, the subsystems taking care of fission product removal and containment integrity are available at the moment they are needed. If electrical power is available but the ECCS fails whereas fission product removal is available, we get that branch of the event tree which ends at *large release*. In the figure all possible branches in the event tree lead to a certain amount of radioactive release. In the last column of the event tree intensities of the radioactive release are qualitatively indicated for every branch of the tree. If all the subsystems function and perform their tasks adequately, the release is very small; in the case that there is no electrical power, the release is very large. From a safety standpoint it is very important to know the probability of occurrence of the various branches, in particular of those which lead to medium, to large and to very large release.

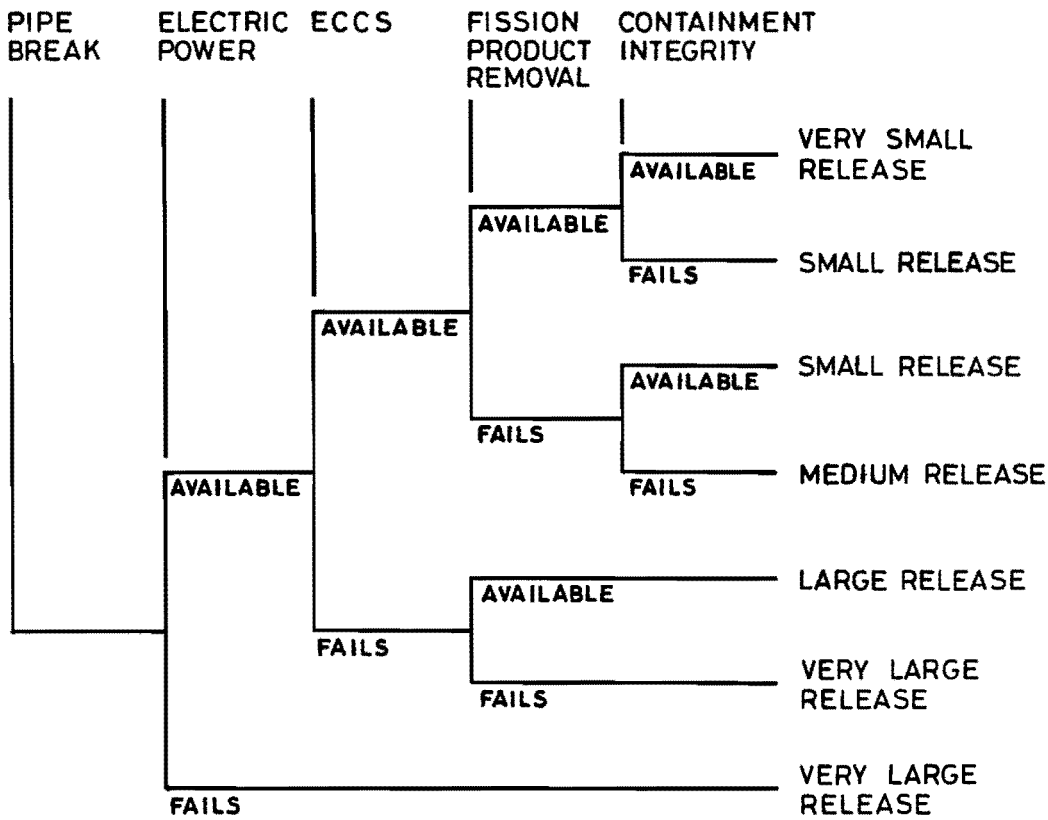


FIG. 2.5 SIMPLIFIED EVEN TREE FOR A LOCA IN A NUCLEAR POWER PLANT

In this example the upper branch of the event tree can actually be described as a phased mission in the sense as mentioned in the preceding section. Actually, this branch consists of four subsystems: electrical power, ECCS, fission product removal and containment integrity. However, we can easily describe any other branch of the event tree as a phased mission. To do this we introduce for every subsystem two tasks, viz.

(i) subsystem accomplishes its intended function, i.e. survives its phase (task 1);

(ii) subsystem fails at the start of its phase or fails during its phase (task 0).

So, for instance, the branch ending at *large release* may be characterized as the three-phase mission for which electrical power fulfills its "first" task, the ECCS its "zero" task and fission product removal its "first" task. For a complete description of the phased mission we need also to specify the duration of the phases.

Next we introduce the binary variables u_j, where $u_j=1$ shall denote that subsystem S_j performs its "first" task and $u_j=0$ that it performs its "zero" task. With every branch of the event tree we can now associate a sequence $u_1,u_2,\ldots$. Each sequence $u_j, j=1,\ldots,$ characterizes a branch of the event tree, and conversely; *the sequence u_j will be called the phased mission for that branch.*

2.5. Component fault detection and repair policies

For the description of the availability of a component it is necessary to have a detailed knowledge of the behaviour of that component. The behaviour of a component is determined by two factors:

(i) the life characteristics of the component, i.e. its failure data and its lifetime distribution;
(ii) the inspection and/or repair policies to which the component is subjected.

First we shall give a detailed description of the concept of the *lifetime* of a component. The epoch between the installation of the component and the time of its first failure will be called the *first lifetime* of the component. It does not matter whether it is an active or a passive component (see remark, § 2.2). If the maintenance policy for this component is such that no repair is incorporated, then this component has only *one* life. If repair is incorporated, then the time between the moment at which the first repair has been completed and the moment the next failure occurs will be called the *second lifetime* of the component, etc. In general a maintained component can be in one of the following states at time t: function state, fail state, repair state or test state. Because we do not know with certainty in which state the component is at time t, the time behaviour of the component has to be described by a stochastic process. To describe this stochastic process we have to know its probabilistic structure. This depends on the maintenance policy to which the component is subjected as well as on the component's structure. We shall first describe the various characteristics of the maintenance policies. Essential for maintenance is fault detection. Concerning detection four possibilities have to be distinguished:

- there is no detection on component failure at all;
- there is a continuous detection on component failure, for instance by means of an alarmlamp as sensor;
- detection is performed at random times. For instance at random moments the system is subjected to a test program. In this category of fault detection of a component we shall also include the fault detection which occurs if a not-active system is demanded to become active. As a rule such a demand is initiated by level crossings of processes within the active systems. Therefore, such demands occur randomly and the components present in the not-active system are considered to be subjected to a random test.
- tests at prescribed times, for instance periodical testing.

Detection of a failed component activates the repair program for the component, but its realisation may be sometimes overruled, see below.
If it is not overruled two cases should be distinguished here, viz. the repair is initiated immediately, as it is the case with continuous detection and at random times, or it is delayed. The latter situation occurs for detection at prescribed times because this detection procedure requires a certain time interval and only at the end of such intervals the required repair can be effectuated.
During a phased mission sometimes the initiating of the repair program can be *overruled*. Such overruling is due to the fact that during the operational part of a period of a component no repair is permitted.
Suppose the repair program is overruled and consider the case of continuous detection: if during the operational part of a period a component failure is detected, then its repair starts immediately at the end of the operational time interval; if a component is in a state of repair at the beginning of its operational time interval, then this repair is interrupted and resumed at the end of its operational time interval.
For components subjected to random testing and components inspected at prescribed times it is always assumed that such tests are not made during the mission. Therefore, no repair is applied to these components during the mission, however, with one exception: if such a component is tested or being repaired at the start of the mission at instant T_0 and its first operational part starts at instant $t_1' > T_0$ then inspection or repair may be continued during $[T_0, t_1')$.

Assumption 2.5.1.: It is assumed that when the repair has been finished the component is as good as new and starts a new life.

On account of the detection and maintenance procedures discussed above four classes of components should be considered.

Class 1: components belonging to this class are not tested; they may be considered as non-repairable components.

Class 2: components which are continuously inspected: if the component is in a dormant part of one of its periods and fails, then repair starts immediately; if it fails during an operational part of a period repair starts immediately after termination of that operational part.

Class 3: components which are inspected at random times. For this class of components the same procedures as stated for class 4 components are valid.

Class 4: components which are inspected at prescribed times. Inspection only takes place during the *OR-phase* (see section 2.2.). Each inspection takes a prescribed time, called *inspection time*. If during the inspection time it turns out that the component is in the fail state, then repair starts immediately after termination of this inspection time.
Inspection nor repair are carried out during the phased mission, i.e. after the start of the mission at instant T_0. However, there is one exception: if the component is inspected or being repaired at instant T_0, and its first operational part starts at instant $t_1' > T_0$, then inspection or repair may be continued during $[T_0, t_1')$.

Above it has been mentioned that the time behaviour of a component should be described by means of a stochastic process. This will be done in chapter 3, but we shall make here some introductory remarks.

Assumption 2.5.2.: The successive lifetimes of a component c_i are assumed to be independent identically distributed variables with distribution $F_i(.)$.

Indicating by $\underline{d}_i$ such a lifetime:

$$F_i(t) = \Pr\{\underline{d}_i < t\}, \quad t \geq 0;$$

$$= 0 \qquad , \quad t < 0.$$

Assumption 2.5.3.: The variables $\underline{d}_i, i=1,\ldots,N$ are assumed to be mutually independent variables.

Subsystem $S_j, j=1,\ldots,K$ and similarly component $c_i, i=1,\ldots,N$ can be available or not available at time t.
Define by $\underline{y}_j(t)$ the state variable of subsystem S_j and by $\underline{x}_i(t)$ the state variable of component c_i at instant t.

$$\begin{aligned} \underline{y}_j(t) &= 1, \text{ if subsystem } S_j \text{ is not available at time t;} \\ &= 0, \text{ if subsystem } S_j \text{ is available at time t.} \end{aligned} \tag{2.1}$$

$$\begin{aligned} \underline{x}_i(t) &= 1, \text{ if component } c_i \text{ is not available at time t;} \\ &= 0, \text{ if component } c_i \text{ is available at time t.} \end{aligned} \tag{2.2}$$

Assumption 2.5.4.: The variables $\underline{x}_i(t), i=1,\ldots,N$ are assumed to be independent variables for every t. (The variables $\underline{y}_j(t), j=1,\ldots,K$ are *not* independent variables, because subsystems may share components).

Assumption 2.5.5.: It is assumed that the subsystems $S_j, j=1,\ldots,K$ are coherent (see chapter 5).

3. RENEWAL THEORY, AVAILABILITY AND RESIDUAL LIFETIME DISTRIBUITON OF A COMPONENT DURING THE OR-PHASE

3.1. Introduction

To describe the stochastic behaviour of the various types of components we need results from renewal theory. For a discussion of the first principles of renewal theory the reader is referred to the literature on stochastic processes, see e.g. Cox and Miller [5] and Feller [9]. Renewal theory is needed here because for the description of the compoment behaviour we need information concerning the availability of a component, concerning the number of replacements and/or repairs during a given time interval and concerning the residual lifetime distribution of a component.

An important quantity in renewal theory is the *renewal function*. This renewal function gives the average number of renewals in an observed time interval. If the behaviour of a component can be described by a renewal process (i.e. a class 2 of class 3 component), then the renewal function is needed to determine the *availability* and the *residual lifetime distribution* of the component at instant t. The availability of a component at instant t is the probability that the component is in the function state at time t. The residual lifetime distribution of a component at time t describes the probability that the component fails within the next time interval τ after t. Both these quantities are necessary in calculating the availability of the component during the phased mission.

Also the availability of a class 4 component is calculated in this chapter. A special feature in this case is that it is assumed that if during the test the component is not in the fail state, after the test the component proceeds with its functioning, i.e. it is then *not* assumed that after the test the component is as good as new.

In section 3.2. the renewal function for a component subjected to immediate replacement is determined, whereas in section 3.3. the renewal function for class 2 and class 3 components is calculated. In section 3.4. the availability of a component is determined and in section 3.5. the residual lifetime distribution is derived. In section 3.6. several results of the theory treated in this chapter are represented, see table 3.1.

3.2. The simple renewal process

Suppose that at time t=0 or earlier a component is installed. The component functions during a certain time $\underline{\ell}_1$ and then it fails. Instantaneously, a new component with the same characteristics is replaced instead of the old one and functions during a time $\underline{\ell}_2$, and so on. Every replacement is called a renewal.

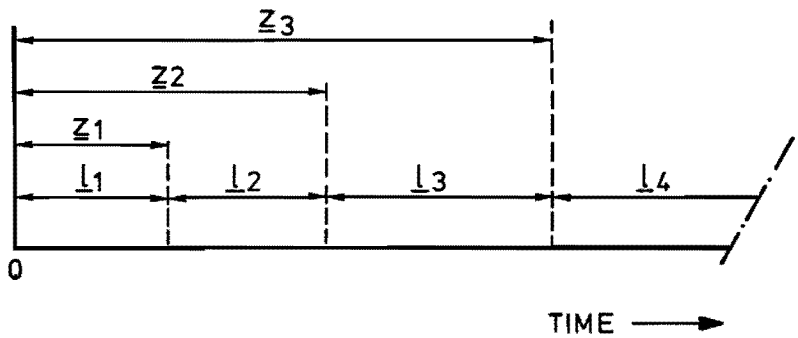


FIG. 3.1. REPLACEMENT PROCESS OF COMPONENTS

Denote by $\underline{\ell}_1, \underline{\ell}_2, \ldots$, a series of independent, non-negative stochastic variables with $\underline{\ell}_2, \underline{\ell}_3, \ldots$, identically distributed. Their distribution functions are denoted by

$$F_1(t) \stackrel{\text{def}}{=} \Pr\{\underline{\ell}_1 < t\}, \quad t>0;$$

$$F(t) \stackrel{\text{def}}{=} \Pr\{\underline{\ell}_i < t\}, \quad t>0, \quad i=2,3,\ldots .$$

The distribution function $F_1(t)$ of the first component may in general differ from that of the following components, since the first component may have been installed previous to t=0. Generally, the distribution of the residual lifetime of a component differs from its lifetime distribution.

It will be assumed that

$$F_1(0+) = 0 \text{ and } F(0+) = 0.$$

Introduce the variables

$$\underline{z}_0 \stackrel{\text{def}}{=} 0, \quad \underline{z}_n \stackrel{\text{def}}{=} \underline{\ell}_1 + \ldots + \underline{\ell}_n, \quad n=1,2,\ldots .$$

So, $\underline{z}_n$ is the sum of the first n renewal times (see fig. 3.1.).

Definition 3.1.

The stochastic process $\{\underline{\nu}(t),\ t\in[0,\infty)\}$ with

$$\underline{\nu}(t) \stackrel{\text{def}}{=} \max\{n:\underline{z}_n<t\},\quad \underline{\nu}(0) \stackrel{\text{def}}{=} 0,$$

will be called a *general renewal process* if $F_1(t)$ and $F(t)$ are not identical; if $F_1(t) \equiv F(t)$ the process is called a *renewal process*. $F(t)$ will be called the *renewal distribution*, and $F_1(t)$ the *distribution of the first renewal time*. As can be seen from its definition, $\underline{\nu}(t)$ is the number of replacements of components in $(0,t)$, i.e. the number of renewals in $(0,t)$. From the definition it follows immediately that for $t>0$,

$$\{\underline{\nu}(t) = 0\} = \{\underline{z}_1 \geq t\}, \tag{3.1}$$

$$\{\underline{\nu}(t) = n\} = \{\underline{z}_n < t,\ \underline{z}_{n+1} \geq t\},\quad n=1,2,\ldots,$$

$$\{\underline{\nu}(t) < n\} = \{\underline{z}_n > t\},\qquad n=1,2,\ldots.$$

The *renewal function* $m(t)$, $t\geq 0$, is defined by

$$m(t) \stackrel{\text{def}}{=} E\{\underline{\nu}(t)\},\quad t\geq 0,$$

and represents the average number of renewals in $(0,t)$.
From (3.1) it follows that

$$m(t) = \sum_{n=1}^{\infty} \Pr\{\underline{\nu}(t)\geq n\} = \sum_{n=0}^{\infty} F_1(t) * F^{(n*)}(t), \tag{3.2}$$

where $F^{(n*)}(t)$ denotes the n-fold convolution of $F(t)$ with itself, $n=1,2,\ldots$; $F^{(0*)}(t)$ is by definition the probability distribution degenerated at $t=0$, i.e.

$$F^{(0*)}(t) = 0,\ t\leq 0,$$
$$= 1,\ t>0.$$

It can be proved easily that $m(t)$ is finite for every finite t, see Feller [9]. From (3.2) it follows that

$$m(t) = F_1(t) + \int_0^t F(t-\tau)\, dm(\tau),\ t \geq 0. \tag{3.3}$$

It may be proved that (3.3) considered as an integral equation for m(t) has a unique solution, which is bounded on finite intervals, and is given by (3.2) [9].

Introducing the Laplace-Stieltjes transforms

$$f_1(\rho) \stackrel{def}{=} \int_0^\infty e^{-\rho t}\, dF_1(t);\ f(\rho) \stackrel{def}{=} \int_0^\infty e^{-\rho t}\, dF(t),\ Re\rho \geq 0,$$

we obtain from (3.3) that

$$h(\rho) \stackrel{def}{=} \int_0^\infty e^{-\rho t}\, dm(t) = \frac{f_1(\rho)}{1-f(\rho)},\ Re\rho > 0. \tag{3.4}$$

Relation (3.4) is a very useful relation for the determination of m(t).

3.3. More complicated renewal processes

In this section we describe some more complicated renewal processes. The processes are generated by the various maintenance disciplines to which components may be subjected. Various characteristics of these processes are needed for the analysis of the influence of component availability on system availability during the mission.
For these processes we first calculate the renewal functions, the availabilities and the distribution of the residual lifetimes.

3.3.1. The renewal function for continuously inspected (class 2) components

Suppose that at time t=0 a component is or was installed and functions. After a certain time it fails. Immediately repair is started. When the component is repaired, it is considered to be new and starts a new life. Denote by $\underline{\ell}_1, \underline{\ell}_2, \ldots$, its successive lifetimes and by $\underline{r}_1, \underline{r}_2, \ldots$, its successive repairtimes. It will be assumed that $\underline{r}_1, \underline{r}_2, \ldots$, are independent non-negative stochastic variables with $\underline{r}_2, \underline{r}_3, \ldots$, identically distributed. Similarly $\underline{\ell}_1, \underline{\ell}_2, \ldots$, are independent non-negative stochastic variables and $\underline{\ell}_2, \underline{\ell}_3, \ldots$, identically distributed; their distribution defined by $F_i(.)$, see assumption 2.5.2.

Denote the repairtime distribution functions of the component, by

$$W_1(t) \stackrel{def}{=} \Pr\{\underline{r}_1 < t\}, \quad t > 0;$$

$$W(t) \stackrel{def}{=} \Pr\{\underline{r}_i < t\}, \quad t > 0, \ i=2,3,\ldots .$$

It will be assumed that

$$W_1(0+) = 0 \text{ and } W(0+) = 0.$$

We have to distinguish two possible situations, viz. the function state and the fail state of the component at t=0. $W_1(t)$ only differs from $W(t)$ if at t=0 the component already is in the fail state.
To incorporate these two initial conditions we introduce the stochastic variables $\underline{g}_n$, n=0,1,... . If the initial state is the function state, then

$$\underline{g}_0 \stackrel{def}{=} 0, \ \underline{g}_1 \stackrel{def}{=} \underline{\ell}_1, \ \underline{g}_n \stackrel{def}{=} \underline{\ell}_n + \underline{r}_{n-1}, \ n=2,3,\ldots .$$

If the initial state is the fail state then

$$\underline{g}_0 \stackrel{def}{=} 0, \ \underline{g}_1 \stackrel{def}{=} \underline{\ell}_1 + \underline{r}_1, \ \underline{g}_n \stackrel{def}{=} \underline{\ell}_n + \underline{r}_n, \ n=2,3,\ldots .$$

Actually the process $\{\ldots,\underline{\ell}_{n-1},\underline{r}_{n-1},\underline{\ell}_n,\underline{r}_n,\ldots\}$ is an alternating process and the process $\underline{g}_n$, n=0,1,..., just defined is an imbedded process of this alternating process, see fig. 3.2.

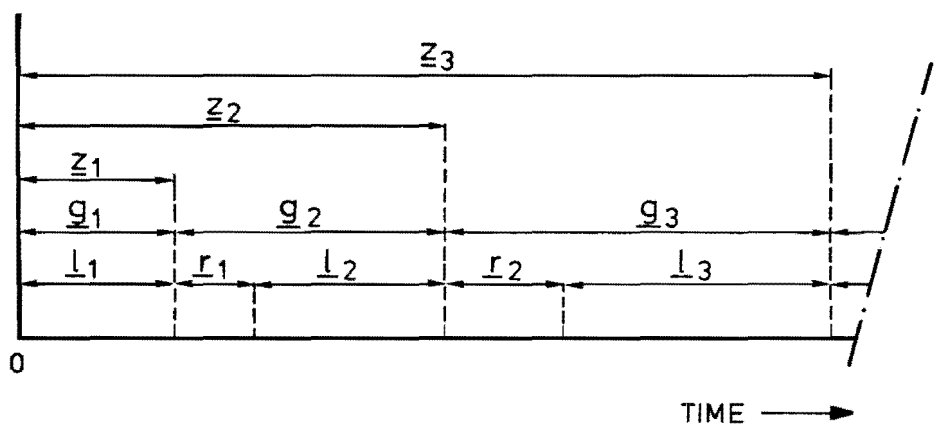


FIG. 3.2. QUANTITIES IN THE ALTERNATING RENEWAL PROCESS OF A COMPONENT.

It is clear that the variables $\underline{g}_n$, n=1,2,..., are independent stochastic variables and $\underline{g}_n$, n=2,3,..., are identically distributed. Define the distribution functions of $\underline{g}_n$, n=1,2,..., by

$$G_1(t) \stackrel{def}{=} Pr\{\underline{\ell}_1<t\} = F_1(t) \quad , \text{if the initial state is the function state,}$$

$$G_1(t) \stackrel{def}{=} Pr\{\underline{\ell}_1+\underline{r}_1<t\} = F(t)*W_1(t), \text{ if the initial state is the fail state,}$$

$$G(t) \stackrel{def}{=} Pr\{\underline{\ell}_n+\underline{r}_{n-1}<t\} = Pr\{\underline{\ell}_n+\underline{r}_n<t\} = F(t)*W(t), \; n=2,3,\ldots , \quad (3.5)$$

assumed that for n=2, $\underline{r}_1$ is a complete repairtime.

Denote by

$$\underline{z}_0 \stackrel{def}{=} 0, \; \underline{z}_n \stackrel{def}{=} \underline{g}_1 + \ldots + \underline{g}_n, \; n=1,2,\ldots . \text{ (see fig. 3.2.)} \quad (3.6)$$

Then, the process $\{\underline{\nu}_1(t), \; t\in[0,\infty)\}$ with

$$\underline{\nu}_1(t) \stackrel{def}{=} \max\{n:\underline{z}_n<t\}, \; \underline{\nu}_1(0) \stackrel{def}{=} 0,$$

is a renewal process.

The Laplace-Stieltjes transforms of $G_1(t)$ and $G(t)$ are denoted by

$$g_1(\rho) = \int_0^\infty e^{-\rho t}\, dG_1(t); \; g(\rho) = \int_0^\infty e^{-\rho t}\, dG(t), \; Re\rho\geq 0.$$

Applying formula (3.4) to the renewal function $m^{(1)}(t)$ of the renewal process $\{\underline{\nu}_1(t), \; t\geq 0\}$ now gives

$$h^{(1)}(\rho) \stackrel{def}{=} \int_0^\infty e^{-\rho t}\, dm^{(1)}(t) = \frac{g_1(\rho)}{1-g(\rho)} = \frac{g_1(\rho)}{1-f(\rho)w(\rho)}, \; Re\rho>0, \quad (3.7)$$

where

$$g_1(\rho) = f_1(\rho) \quad , \text{if the initial state is the function state;}$$

$$= f(\rho)w_1(\rho), \text{ if the initial state is the fail state,}$$

with

$$w_1(\rho) \stackrel{def}{=} \int_0^\infty e^{-\rho t}\, dW_1(t); \; w(\rho) \stackrel{def}{=} \int_0^\infty e^{-\rho t}\, dW(t), \; Re\rho\geq 0.$$

3.3.2. The renewal function for randomly inspected (class 3) components

The process of the behaviour of a component of class 3 may be described by a sequence of stochastic variables $\ldots \underline{\ell}_{n-1}, \underline{w}_{n-1}, \underline{r}_{n-1}, \underline{\ell}_n, \underline{w}_n, \underline{r}_n, \ldots$. Here $\underline{\ell}_n$, n=1,2,... , and similarly $\underline{r}_n$, n=1,2, ..., have the same meaning and the same stochastic properties as in the preceding section, they represent the successive lifetimes and repairtimes.

$\underline{w}_n$ represents the time between the n^{th} failure of the component and the moment of detection of this failure, see fig. 3.3.

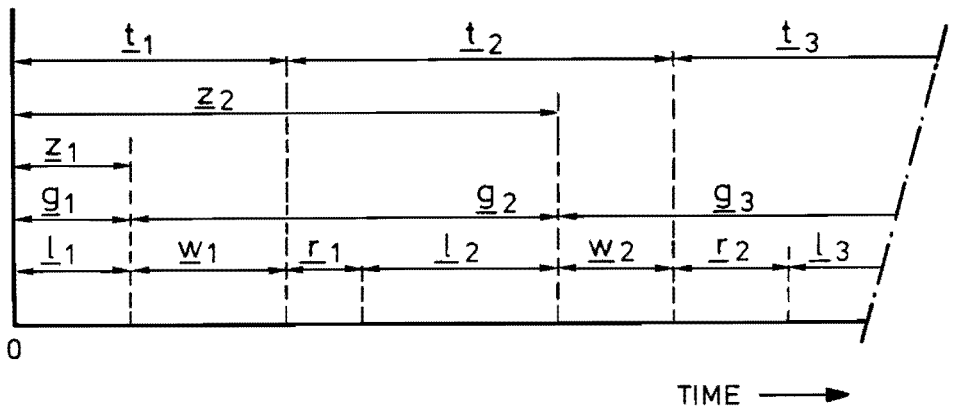


FIG.3.3. REALISATION OF THE RANDOM TEST PROCESS OF A COMPONENT.

The variables $\underline{w}_n$, n=1,2,..., depend on the testprocedure and we shall assume with Caldarola [3] that the moments at which the component is tested form a Poisson process with parameter γ so that

$$\Pr\{k \text{ tests in } (0,t)\} = \frac{(\gamma t)^k}{k!} e^{-\gamma t}, \quad k=0,1,\ldots ; \; t > 0.$$

This implies that the times between the tests are negative exponentially distributed with parameter γ, and are stochastically independent. Denote by $\underline{t}_n$, n=1,2, ... , the time between the $(n-1)^{th}$ and the n^{th} test. Obviously, the distribution of $\underline{t}_n$, n=1,2,..., is

$$H(t) \stackrel{def}{=} \Pr\{\underline{t}_n < t\} = 1 - e^{-\gamma t}, \quad \gamma > 0, \; t > 0, \; n=1,2, \ldots .$$

From the assumption that the testpoints are Poissonian distributed it now follows that the non-negative stochastic variables $\underline{w}_n$, n=1,2,..., are independent identically distributed variables, their distribution being the negative exponential distribution with parameter γ; and further that the families $\{\underline{w}_n, n=1,2,\ldots\}$ and $\{\underline{\ell}_n, \underline{r}_n, n=1,2, \ldots\}$ are independent families.

The assumption that the testmoments can be described by a Poisson process seems to be a reasonable one for practical situations; moreover it simplifies the calculations considerably. It is possible to work with a non-Poissonian testprocess but then the required analysis will be very complicated. Further it should be noted that the random test processes for various components should be independent of each other, otherwise the assumption 2.5.4. might not be valid.
As in the preceding section, we also have to distinguish here the cases whether the initial state is a function or a fail state. If the initial state is the function state then

$$\underline{g}_0 \overset{\text{def}}{=} 0,\ \underline{g}_1 \overset{\text{def}}{=} \underline{\ell}_1,\ \underline{g}_n \overset{\text{def}}{=} \underline{\ell}_n+\underline{w}_{n-1}+\underline{r}_{n-1},\ n=2,3,\ldots .$$

If the initial state is the fail state then

$$\underline{g}_0 \overset{\text{def}}{=} 0,\ \underline{g}_1 \overset{\text{def}}{=} \underline{\ell}_1+\underline{r}_1+\underline{w}_1,\ \underline{g}_n \overset{\text{def}}{=} \underline{\ell}_n+\underline{w}_n+\underline{r}_n,\ n=2,3,\ldots .$$

The variables $\underline{g}_n$, $n=1,2,\ldots$, are again independent, identically distributed variables. The distribution functions of $\underline{g}_n$, $n=1,2,\ldots$, are denoted by

$$\begin{aligned} G_1(t) &\overset{\text{def}}{=} \Pr\{\underline{\ell}_1<t\} && \text{, if the initial state is the function state,} \\ G_1(t) &\overset{\text{def}}{=} \Pr\{\underline{\ell}_1+\underline{r}_1+\underline{w}_1<t\}, && \text{if the initial state is the fail state,} \\ G(t) &\overset{\text{def}}{=} \Pr\{\underline{\ell}_n+\underline{w}_{n-1}+\underline{r}_{n-1}<t\} = \Pr\{\underline{\ell}_n+\underline{w}_n+\underline{r}_n<t\}, && n=2,3,\ldots, \end{aligned} \tag{3.8}$$

assumed that for $n=2$, $\underline{w}_1$ is a complete waiting time.

Define

$$\underline{z}_0 \overset{\text{def}}{=} 0,\ \underline{z}_n \overset{\text{def}}{=} \underline{g}_1 + \ldots + \underline{g}_n,\ n=1,2,\ \ldots\ . \text{ (see fig. 3.3.)} \tag{3.9}$$

The process $\{\underline{\nu}_2(t),\ t\in[0,\infty)\}$ with

$$\underline{\nu}_2(t) \overset{\text{def}}{=} \max\{n:\underline{z}_n<t\},\ \underline{\nu}_2(0) \overset{\text{def}}{=} 0,$$

and $\underline{z}_n$ as defined in (3.9), is a renewal process. Note that again a renewal is defined to occur when the component terminates to function. Applying formula (3.4) to the renewal function $m^{(2)}(t)$ of the above mentioned renewal process, with $g_1(\rho)$ and $g(\rho)$ the Laplace-Stieltjes transforms of the dis-

tribution functions $G_1(t)$ and $G(t)$ in (3.8), the Laplace-Stieltjes transforms of $m^{(2)}(t)$ reads

$$h^{(2)}(\rho) = \int_0^\infty e^{-\rho t}\, dm^{(2)}(t) = \frac{g_1(\rho)}{1-g(\rho)} = \frac{g_1(\rho)}{1-f(\rho)w(\rho)\gamma/(\rho+\gamma)}, \quad \mathrm{Re}\rho>0, \qquad (3.10)$$

where $f(\rho)$ and $w(\rho)$ are defined as in the foregoing sections, and

$$g_1(\rho) = f_1(\rho) \quad \text{, if the initial state is the function state;}$$
$$= f(\rho)w(\rho)\gamma/(\rho+\gamma), \text{ if the initial state is the fail state,}$$

with

$$\int_0^\infty e^{-\rho t}\, d\Pr\{\underline{w}_i<t\} = \frac{\gamma}{\rho+\gamma}, \quad \mathrm{Re}\rho > -\gamma.$$

3.4. The availability of a component

By definition

$$A(t) = \Pr\{\underline{x}(t) = 0\}, \quad t\geq 0,$$

$$A_I(t) = \frac{1}{t}\int_0^t A(\tau)d\tau, \quad t>0,$$

$\underline{x}(t)$ being the state variable of a component as defined by (2.2).
$A(t)$ is called the *point availability* of the component whereas $A_I(t)$ is called its *interval availability*. The point availability $A(t)$ of a component at epoch t is thus the probability that the component is in the function state at instant t whereas the interval availability is defined as the expected fraction of time the component is in the function state during (0,t). In this study we deal only with the point availability $A(t)$ and in the following it will therefore be called "availability". From now on it is assumed that

$$F_1(t) = F(t) \text{ and } W_1(t) = W(t), \qquad (3.10a)$$

unless explicitly stated.
In sections 3.4.1. and 3.4.2. the availability for components of class 2 and 3 will be analysed whereas in section 3.4.3. the availability of components of class 4 is discussed.

3.4.1. The availability of a continuously inspected (class 2) component

The behaviour of a class 2 component has been described in section 3.3.1. If the initial state of the component is the function state then

$$A(t) = \Pr\{\underline{x}(t) = 0\}$$

$$= \Pr\{\underline{\ell}_1 \geq t\} + \sum_{n=1}^{\infty} \Pr\{\underline{z}_n + \underline{r}_n < t,\ \underline{z}_{n+1} \geq t\}$$

$$= \Pr\{\underline{\ell}_1 \geq t\} + \sum_{n=1}^{\infty} \int_{\tau=0}^{t} \Pr\{\underline{\ell}_{n+1} \geq t-\tau\}\, d\Pr\{\underline{z}_n + \underline{r}_n < \tau\}$$

$$= 1 - F(t) + \{1 - F(t)\} * W(t) * m(t),\ t \geq 0.$$

Denote by

$$a(\rho) \stackrel{def}{=} \int_0^{\infty} e^{-\rho t}\, d\, A(t),\ \mathrm{Re}\rho \geq 0,$$

then the Laplace-Stieltjes transforms for the availability of a continuously detected component with $\underline{x}(0) = 0$ is given by

$$a(\rho) = \{1 - f(\rho)\}\{1 + w(\rho)h(\rho)\},\ \mathrm{Re}\rho > 0,$$

with $f(\rho)$, $w(\rho)$ and $h(\rho)$ as defined in section 3.3.1.
From now on the expression for the relevant quantities will be indexed by an "0" or a "1"; the "0" will be used if the initial state of the component is the function state whereas the "1" will be used if it is the fail state.
So the above formulas for the Laplace-Stieltjes transforms of the availability in both cases read

$$a_0(\rho) = \{1 - f(\rho)\}\{1 + w(\rho)h(\rho)\},\ \mathrm{Re}\rho > 0,$$

$$a_1(\rho) = \{1 + f(\rho)\}w(\rho)\{1 + h(\rho)\},\ \mathrm{Re}\rho > 0.$$

Substitution of (3.5) and (3.7) in the above mentioned formulas gives

$$a_0(\rho) = \frac{1-f(\rho)}{1-w(\rho)f(\rho)},\ \mathrm{Re}\rho > 0, \tag{3.11}$$

$$a_1(\rho) = \frac{\{1-w(\rho)\}w(\rho)}{1-w(\rho)f(\rho)},\ \mathrm{Re}\rho > 0. \tag{3.12}$$

Examples of the *unavailability* of continuously inspected (class 2) compoments are shown in the figures 3.4. and 3.6. till 3.9.

3.4.2. The availability of a randomly inspected (class 3) component

The behaviour of a class 3 component has been described in section 3.3.2. Applying the same procedure as given in section 3.4.1. we get

$$a_0(\rho) = \{1 - f(\rho)\}\{1 + \frac{\gamma}{\rho+\gamma} w(\rho)h_0(\rho)\}, \quad Re\rho>0,$$

$$a_1(\rho) = \{1 - f(\rho)\}\ w(\rho)\ \{1 + \frac{\gamma}{\rho+\gamma} h_1(\rho)\}, \quad Re\rho>0,$$

see section 3.3.2. Substitution of (3.8) and (3.10) in the above formulas gives

$$a_0(\rho) = \frac{1-f(\rho)}{1-f(\rho)w(\rho)\gamma/(\rho+\gamma)}, \quad Re\rho>0, \tag{3.13}$$

$$a_1(\rho) = \frac{\{1-f(\rho)\}w(\rho)\gamma/(\rho+\gamma)}{1-f(\rho)w(\rho)\gamma/(\rho+\gamma)}, \quad Re\rho>0. \tag{3.14}$$

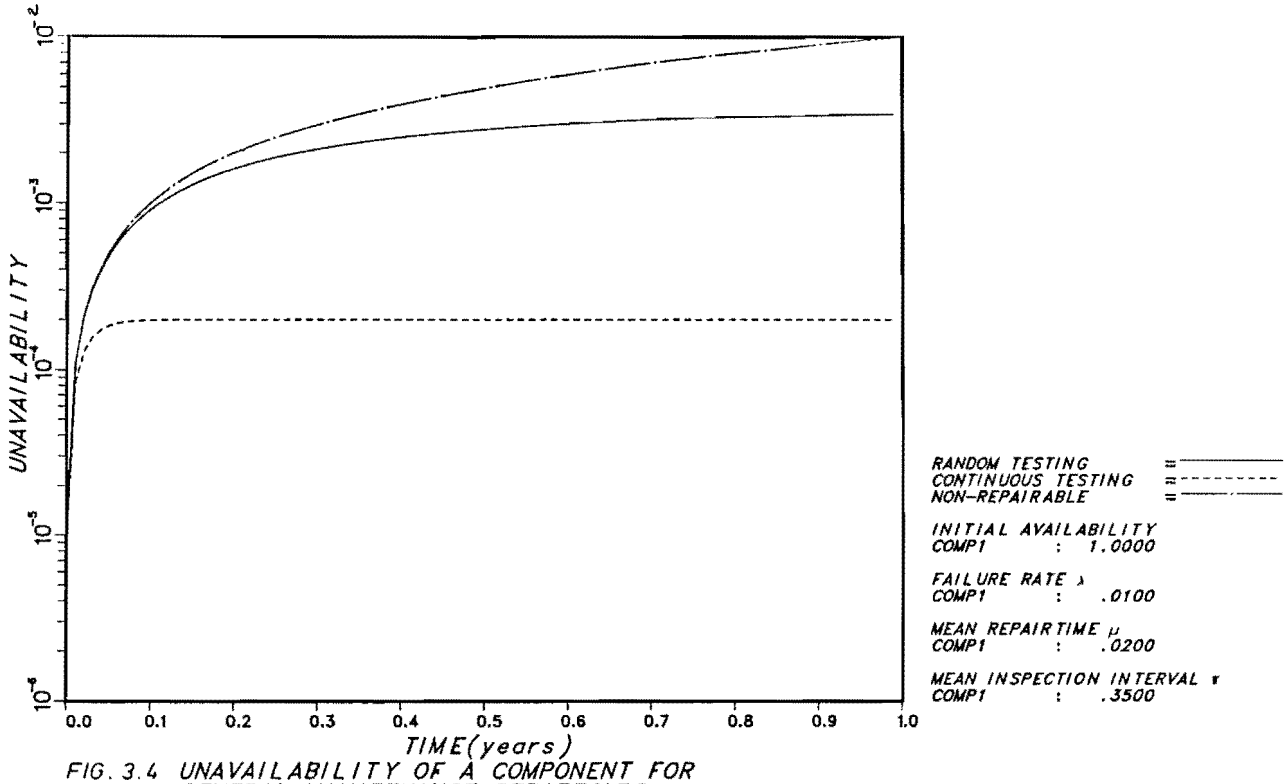


FIG. 3.4 UNAVAILABILITY OF A COMPONENT FOR SEVERAL MAINTENANCE STRATEGIES

LIFETIME DISTRIBUTION : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF CONTINUOUS TESTING : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF RANDOM TESTING : N.E.D.

In fig. 3.4. the *unavailability* of a component subjected to random testing is compared to the unavailability of similar components of which one is non-repairable (class 1) and the other subjected to continuous testing (class 2).

3.4.3. The availability of a periodically inspected (class 4) component

Preliminary we start with the treatment of a rather general inspection procedure, i.e. inspection at prescribed times. After that we turn to periodical inspection.
Suppose that a component is inspected at the times $t_1, t_2, \ldots, t_n, \ldots$, the so-called *inspection times*. If such a component has failed before or at inspection then it will be repaired. Repair starts immediately after termination of the inspection. After the component has been repaired it will be considered as new.

During the time the inspection is performed two strategies are possible, i.e. the inspection can be performed *EXSITU* or *INSITU*. If the component is inspected *EXSITU*, then the installation in which the component is installed has no access to the component during the inspection time; so the component is unavailable during the time the inspection is performed. If the component is inspected *INSITU*, there is no disturbance in the behaviour of the component with respect to its availability, i.e. the component remains accessible for the system.
It is assumed that the time interval needed to inspect the component is a constant, so introduce

$\theta_n \stackrel{def}{=}$ time required to inspect a component at the n^{th} inspection, $n=1,2,\ldots$. (see fig. 3.4.)

It is further assumed that if the component is in the function state after an inspection at $t_n+\theta_n$, $n=1,2,\ldots$, the component life is still going on. This in contradiction with Caldarola [3] and other authors who assume that after inspection without repair the component starts a new life. Another feature here is the assumption that the repairtime of the component is a stochastic variable and not a constant.

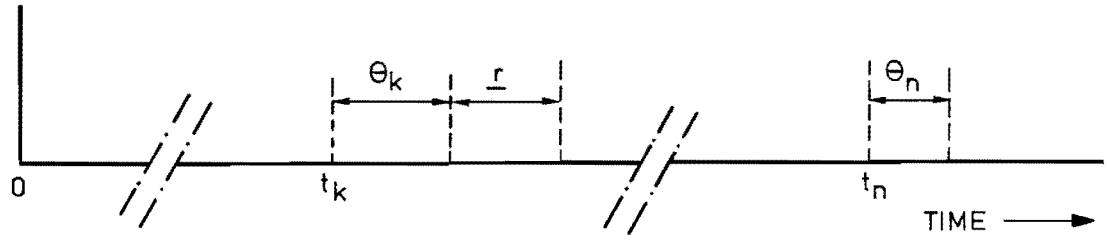


FIG. 3.5. PROCESS OF A COMPONENT SUBJECT TO PERIODICAL INSPECTION.

Suppose that the initial state of the component is the function state and consider the component behaviour during the time interval $t_n \leq t < t_{n+1}$ in case of EXSITU inspection. From the above it may be clear that

$$A_0(t) = 0, \quad t_n \leq t \leq t_n + \theta_n. \tag{3.15}$$

If $t_n + \theta_n < t < t_{n+1}$ it follows that

$$A_0(t) = \Pr\{\underline{x}(t) = 0 \mid \underline{x}(0) = 0\}$$

$$= \Pr\{\underline{x}(t) = 0, \left(\bigcap_{k=1}^{n} (\underline{x}(t_k + \theta_k) = 0)\right) \mid \underline{x}(0) = 0\}$$

$$+ \Pr\{\underline{x}(t)=0, \left(\bigcup_{k=1}^{n} \left(\bigcap_{j=k+1}^{n} (\underline{x}(t_j+\theta_j)=0)\right), \underline{x}(t_k+\theta_k)=1\right)\Big|\underline{x}(0)=0\}.$$

Denote by $\underline{r}$ the repairtime and by $\underline{\ell}$ the lifetime of the component. Since in the present case the testmoments are not random it is natural to assume that if repair is needed at the end of the n^{th} inspection time, then $\underline{r} < t_{n+1} - (t_n + \theta_n)$, $n=1,2,\ldots$, i.e. we assume

$$\Pr\{\underline{r} < \inf_{k=0,1,\ldots} (t_{k+1} - (t_k + \theta_k))\} = 1,$$

where

$$\inf_{k=0,1,\ldots} \{t_{k+1} - (t_k + \theta_k)\} > c, \quad c > 0.$$

Therefore we introduce the *maximum repairtime* R_k for the k^{th} inspection interval with

$$R_k < \inf_{m=0,1,\ldots} \{t_{m+1}-(t_m+\theta_m)\}. \tag{3.16}$$

Denote by $F(t) = \Pr\{\underline{\ell}<t\}$ and $W(t) = \Pr\{\underline{r}<t\}$. From the above it is easily seen that in the *EXSITU* case the availability for the repair interval, i.e. $t\in[t_n+\theta_n, t_n+\theta_n+R_n]$, is given by:

$$A_0(t) = 1-F(t) + \sum_{k=1}^{n-1} \{1-A_0(t_k+\theta_k)\} \int_{\tau=0}^{R_k} \{1-F(t-(t_k+\theta_k+\tau))\}dW(\tau)$$

$$+ \{1-A_0(t_n+\theta_n)\} \int_{\tau=0}^{t-(t_n+\theta_n)} \{1-F(t-(t_n+\theta_n+\tau))\}dW(\tau), \tag{3.17}$$

$$n=1,2,\ldots ;$$

and the availability for the residual interval, i.e. $t\in[t_n+\theta_n+R_n, t_{n+1}]$, is given by:

$$A_0(t) = 1-F(t) + \sum_{k=1}^{n} \{1-A_0(t_k+\theta_k)\} \int_{\tau=0}^{R_k} \{1-F(t-(t_k+\theta_k+\tau))\}dW(\tau), \tag{3.18}$$

$$n=1,2,\ldots .$$

(In (3.17) and (3.18) it is assumed that an empty sum equals zero).
In the case of equidistant testmoments, equal inspection times and equal maximum repairtimes, so that

$$\eta_1 \stackrel{\text{def}}{=} t_1,\ \eta \stackrel{\text{def}}{=} t_{n+1}-t_n,\ \theta \stackrel{\text{def}}{=} \theta_n,\ R \stackrel{\text{def}}{=} R_n,\ n=1,2,\ldots ,$$

we obtain when inspection is *EXSITU* performed from (3.15), (3.17) and (3.18) for the n^{th} inspection interval $[\eta_1+(n-1)\eta, \eta_1+n\eta]$:

$$A_0(t) = 0,\ \eta_1+(n-1)\eta \le t \le \eta_1+(n-1)\eta+\theta; \tag{3.19}$$

$$A_0(t) = 1-F(t) + \sum_{k=1}^{n-1} \{1-A_0(\eta_1+(k-1)\eta+\theta)\} \int_{\tau=0}^{R} \{1-F(t-\eta_1-(k-1)\eta-\theta-\tau)\}dW(\tau)$$

$$+ \{1-A_0(\eta_1+(n-1)\eta+\theta) \int_{\tau=0}^{t-\eta_1-(n-1)\eta-\theta} \{1-F(t-\eta_1-(n-1)\eta-\theta-\tau)\}dW(\tau),$$

$$\eta_1+(n-1)\eta+\theta \le t \le \eta_1+(n-1)\eta+\theta+R; \tag{3.20}$$

$$A_0(t) = 1-F(t)+\sum_{k=1}^{n}\{1-A_0(\eta_1+(k-1)\eta+\theta)\}\int_{\tau=0}^{R}\{1-F(t-\eta_1-(k-1)\eta-\theta-\tau)\}dW(\tau), \tag{3.21}$$

$$\eta_1+(n-1)\eta+\theta+R\le t\le\eta_1+n\eta,\ n=1,2,\ldots\ .$$

Note that in the formulas (3.20) and (3.21) the time η_1 to the first inspection not necessarily equals the time η between two successive testmoments. This offers the possibility of *sequential testing* of two or more components of a system.

If the initial state of the component is the fail state the availability in case of inspection EXSITU can be obtained by the same method:

$$A_1(t) = 0,\ t_n\le t\le t_n+\theta_n; \tag{3.22}$$

$$A_1(t) = \sum_{k=1}^{n-1}\{1-A_1(t_k+\theta_k)\}\int_{\tau=0}^{R_k}\{1-F(t-(t_k+\theta_k-\tau))\}dW(\tau)$$

$$+\{1-A_1(t_n+\theta_n)\}\int_{\tau=0}^{t-(t_n+\theta_n)}\{1-F(t-(t_n+\theta_n+\tau))\}dW(\tau), \tag{3.23}$$

$$t_n+\theta_n\le t\le t_n+\theta_n+R_n,\ n=1,2,\ldots\ ;$$

$$A_1(t) = \sum_{k=1}^{n}\{1-A_1(t_k+\theta_k)\}\int_{\tau=0}^{R_k}\{1-F(t-(t_k+\theta_k+\tau))\}dW(\tau), \tag{3.24}$$

$$t_n+\theta_n+R_n\le t\le t_{n+1},\ n=1,2,\ldots\ .$$

In the case of equidistant testmoments, equal inspection times and equal maximum repairtimes we get from (3.22),..., (3.24),

$$A_1(t) = 0,\ \eta_1+(n-1)\eta\le t\le\eta_1+(n-1)\eta+\theta; \tag{3.25}$$

$$A_1(t) = \sum_{k=1}^{n-1}\{1-A_1(\eta_1+(k-1)\eta+\theta)\}\int_{\tau=0}^{R}\{1-F(t-\eta_1-(k-1)\eta-\theta-\tau)\}dW(\tau)$$

$$+\{1-A_1(\eta_1+(n-1)\eta+\theta)\}\int_{\tau=0}^{t-(\eta_1+(n-1)\eta+\theta)}\{1-F(t-\eta_1-(n-1)\eta-\theta-\tau)\}dW(\tau), \tag{3.26}$$

$$\eta_1+(n-1)\eta+\theta\le t\le\eta_1+(n-1)\eta+\theta+R;$$

$$A_1(t) = \sum_{k=1}^{n} \{1-A_1(\eta_1+(k-1)\eta+\theta)\} \int_{\tau=0}^{R} \{1-F(t-\eta_1-(k-1)\eta-\theta-\tau)\}dW(\tau), \tag{3.27}$$

$$\eta_1+(n-1)\eta+\theta+R \le t \le \eta_1+n\eta, \quad n=1,2,\ldots .$$

A special case is the interval $[0,\eta_1]$. Obviously the availabilities $A_0(t)$ and $A_1(t)$ during this interval are given by:

$$A_0(t) = 1-F(t) \quad \text{and} \quad A_1(t) = 0. \tag{3.28}$$

The unconditional availability of the component at instant t reads

$$A(t) = A_0(t)A(0)+A_1(t)\{1-A(0)\}, \tag{3.29}$$

$A_0(t)$ and $A_1(t)$ as determined above and $A(0) = \Pr\{\underline{x}(0)=0\}$.

Note: In the derivation above the possibility that the component switches to the fail state during the test interval θ_k, k=1,2,..., has not been excluded.

If the inspection is performed INSITU, then the behaviour of the component with respect to its availability during the interval $[t_n+\theta_n,t_{n+1}]$, n=1,2,..., is the same as it is to EXSITU inspection, i.e. in case of INSITU inspection the availabilities $A_0(t)$ and $A_1(t)$ during the interval $[t_n+\theta_n,t_{n+1}]$ are given by (3.17) and (3.18) resp. (3.23) and (3.24). However, the availabilities $A_0(t)$ and $A_1(t)$ during the interval $[t_n,t_n+\theta_n]$, n=1,2,..., in case of INSITU inspection are different from that in case of EXSITU inspection, because if INSITU inspection is performed the component is not by definition unavailable during inspection; the component behaves during such an interval, for instance the interval $[t_n,t_n+\theta_n]$, as it does during the foregoing interval $[t_{n-1}+\theta_{n-1}+R_{n-1},t_n]$. Therefore, the availabilities $A_0(t)$ and $A_1(t)$ of the component during the interval $[t_n,t_n+\theta_n]$ are given by (3.18) resp. (3.24).

In the figures 3.6 till 3.9 an illustration is given of the influence by periodical testing on the *unavailability* of a component.

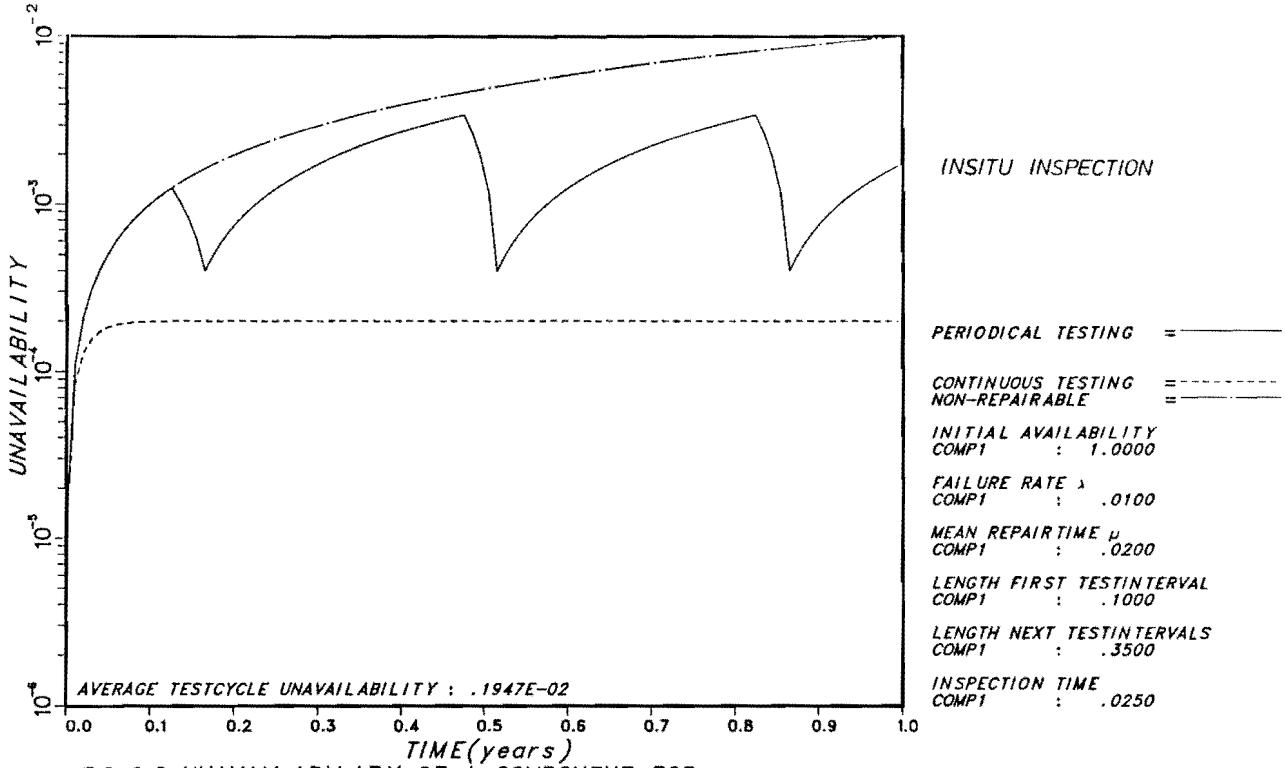


FIG. 3.6 UNAVAILABILITY OF A COMPONENT FOR SEVERAL MAINTENANCE STRATEGIES

LIFETIME DISTRIBUTION : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF CONTINUOUS TESTING : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF PERIODICAL TESTING :
UNIFORM DISTRIBUTION

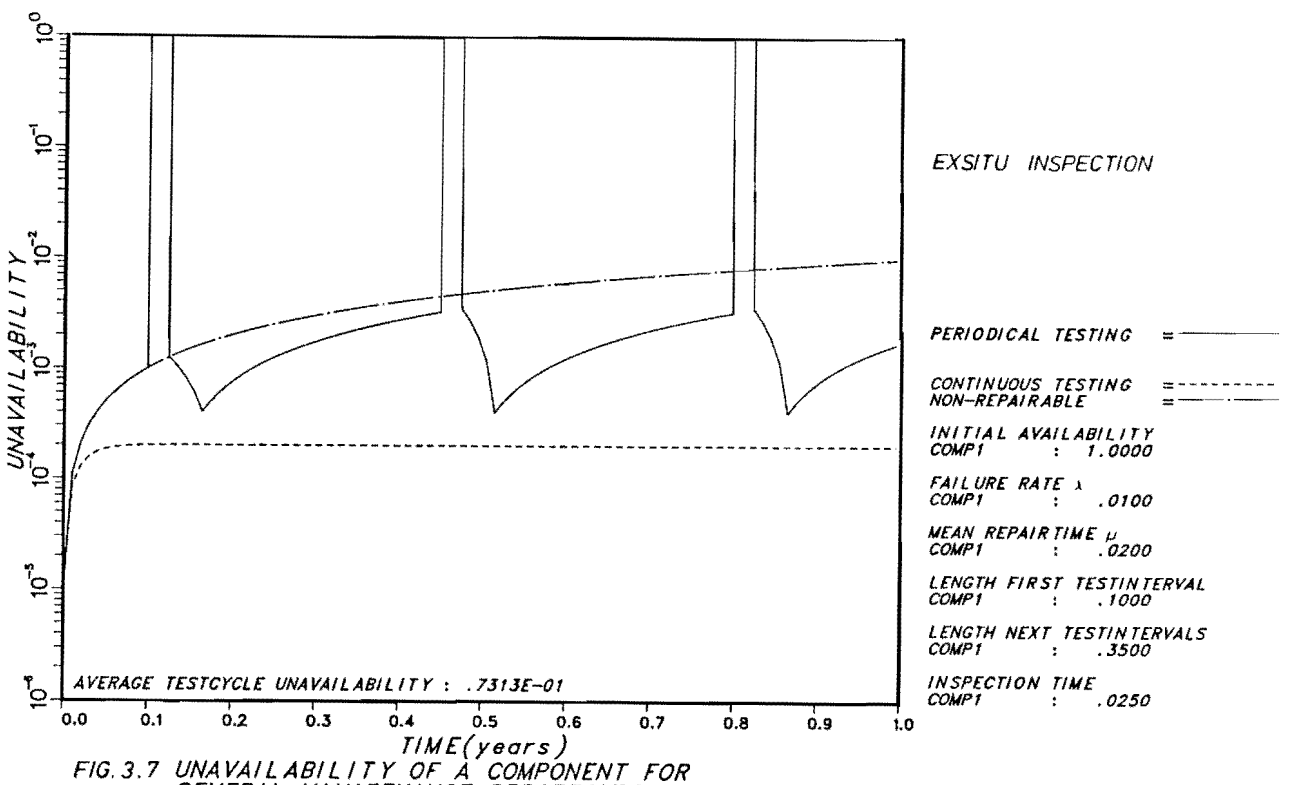


FIG. 3.7 UNAVAILABILITY OF A COMPONENT FOR SEVERAL MAINTENANCE STRATEGIES

LIFETIME DISTRIBUTION : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF CONTINUOUS TESTING : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF PERIODICAL TESTING :
UNIFORM DISTRIBUTION

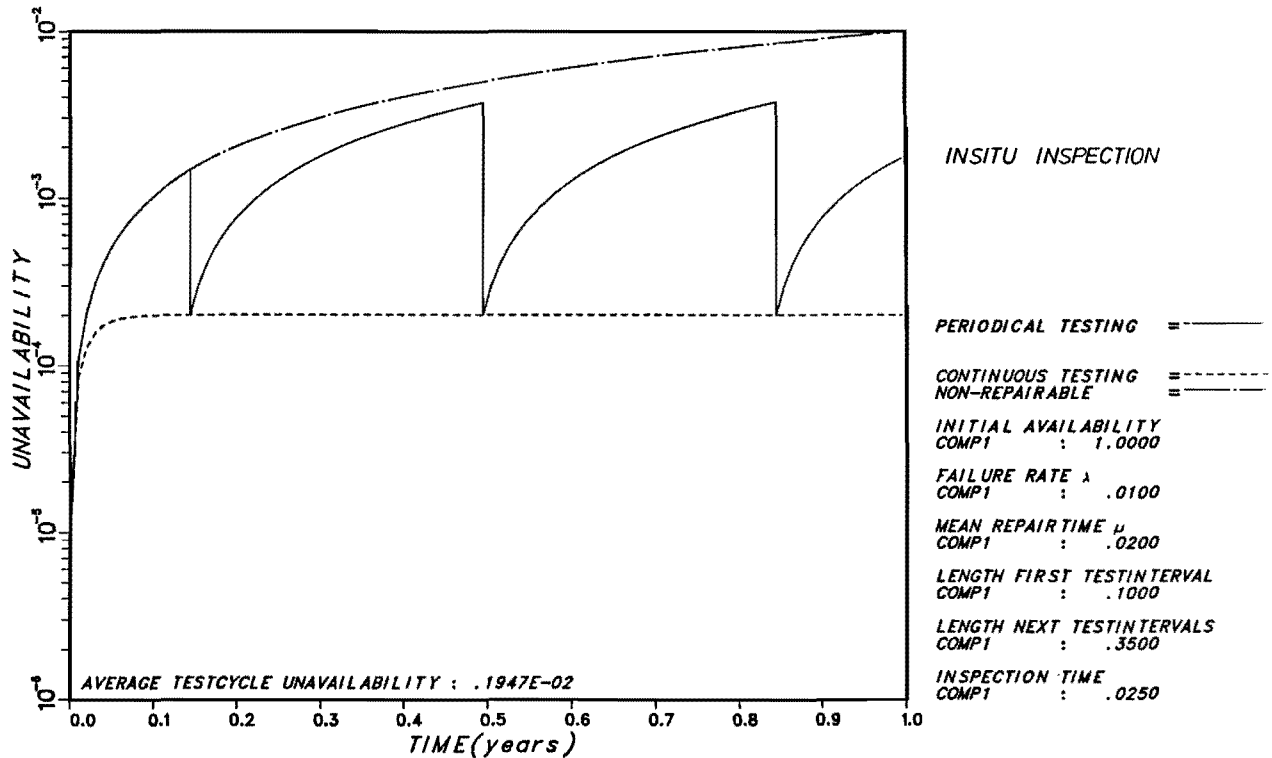


FIG.3.8 UNAVAILABILITY OF A COMPONENT FOR SEVERAL MAINTENANCE STRATEGIES

LIFETIME DISTRIBUTION : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF CONTINUOUS TESTING : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF PERIODICAL TESTING :
STEPFUNCTION (CONSTANT REPAIRTIME)

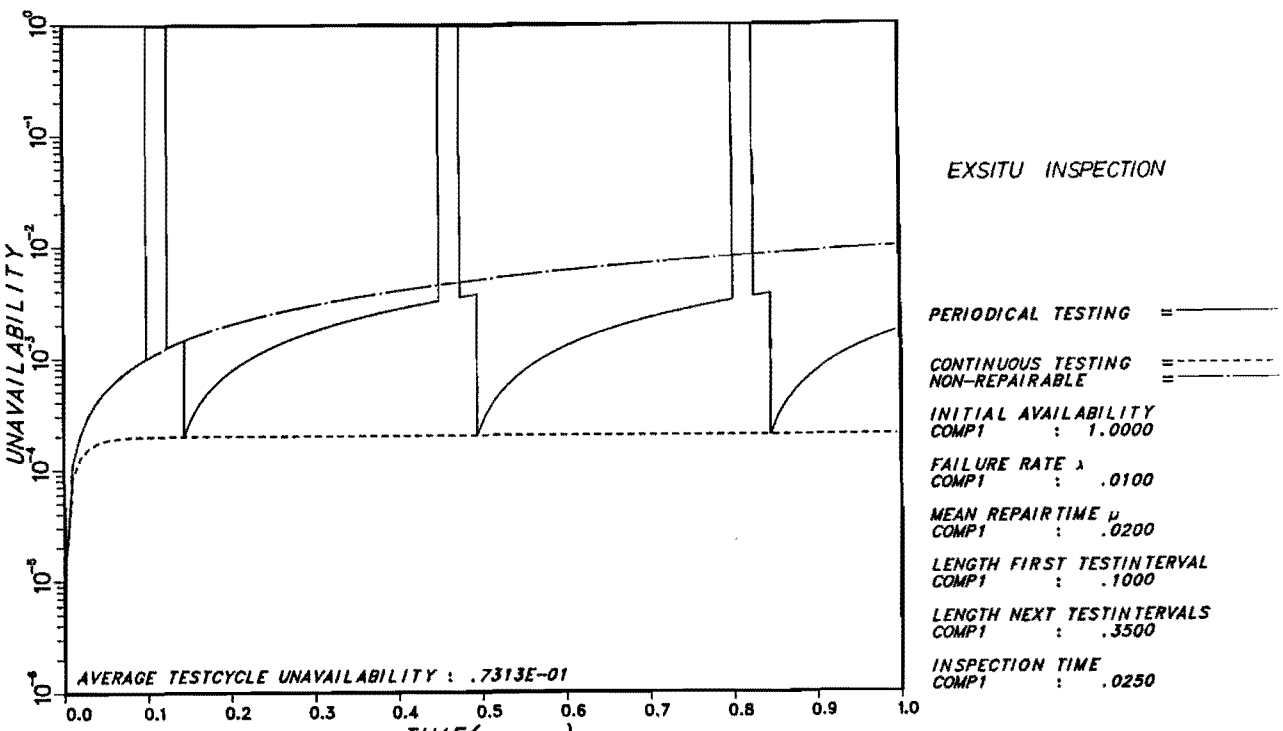


FIG.3.9 UNAVAILABILITY OF A COMPONENT FOR SEVERAL MAINTENANCE STRATEGIES

LIFETIME DISTRIBUTION : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF CONTINUOUS TESTING : N.E.D.
REPAIRTIME DISTRIBUTION IN CASE OF PERIODICAL TESTING :
STEPFUNCTION (CONSTANT REPAIRTIME)

The lifetime distribution of the component is negative exponential and its repairtime is uniformly distributed or is a constant. The INSITU as well as the EXSITU inspection procedures are shown and compared with the unavailability of a similar but non-repairable (class 1) component and with a continuously inspected (class 2) component.

3.5. The functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ of a component

The residual lifetime of a component at instant t is the time interval between t and the next failure of the component (see fig. 3.10). We shall denote by

$$\underline{\zeta}(t) \stackrel{\text{def}}{=} \text{residual lifetime of component at instant } t,\ t\geq 0. \tag{3.30}$$

In the following the functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$,

$$\begin{aligned} G_0(t,\zeta) &\stackrel{\text{def}}{=} \Pr\{\underline{x}(t)=0,\ \underline{\zeta}(t)<\zeta \mid \underline{x}(0)=0\},\ t\geq 0,\ \zeta\geq 0, \\ G_1(t,\zeta) &\stackrel{\text{def}}{=} \Pr\{\underline{x}(t)=0,\ \underline{\zeta}(t)<\zeta \mid \underline{x}(0)=1\},\ t\geq 0,\ \zeta\geq 0, \end{aligned} \tag{3.31}$$

will be derived for several repair policies of a component.

3.5.1. The function $G_0(t,\zeta)$ of a non-repairable component

Suppose a non-repairable (i.e. class 1) component has started life at t=0. Then by (3.31)

$$\begin{aligned} G_0(t,\zeta) &= \Pr\{\underline{x}(t)=0,\ \underline{\zeta}(t)<\zeta \mid \underline{x}(0)=0\} \\ &= \Pr\{t\leq \underline{\ell}<t+\zeta\} = F(t+\zeta) - F(t),\ t\geq 0,\ \zeta\geq 0, \end{aligned} \tag{3.32}$$

where F(t) and $\underline{\ell}$ as defined in section 3.1.

3.5.2. The functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ of a component subjected to a renewal process

When a component is subjected to a renewal process (i.e. the processes described in the sections 3.2. and 3.3.) the residual lifetime based on

its definition (3.30) may be expressed as (see fig. 3.10):

$$\underline{\zeta}(t) \stackrel{\text{def}}{=} \underline{z}_{\underline{\nu}(t)+1} - t, \quad t>0,$$

if $\underline{x}(t) = 0$.

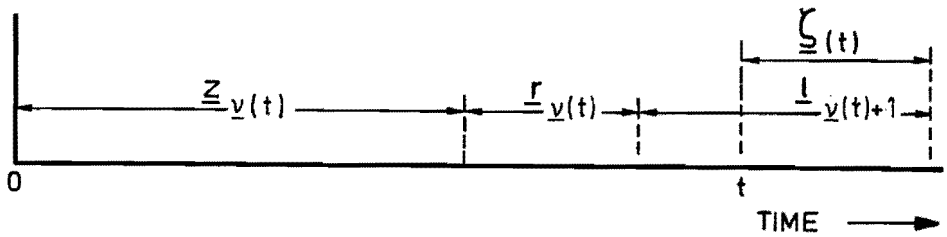


FIG. 3.10. THE RESIDUAL LIFE TIME OF A COMPONENT SUBJECT TO A RENEWAL PROCESS.

Again a renewal is considered to occur at the start of a new repair of the component. The interested quantities are again $G_0(t,\zeta)$ and $G_1(t,\zeta)$ as being defined by (3.31).

3.5.2.1. The function $G_0(t,\zeta)$ of a component subjected to immediate replacement

This renewal process has been described in section 3.2. It is clear from (3.31) that

$$\begin{aligned} G_0(t,\zeta) &= \Pr\{\underline{\zeta}(t)<\zeta,\ \underline{x}(t)=0\} \\ &= \Pr\{t\le\underline{\ell}_1<t+\zeta\} + \sum_{n=1}^{\infty} \Pr\{\underline{z}_n<t,\ t\le\underline{z}_n+\underline{\ell}_{n+1}<t+\zeta\} \\ &= F(t+\zeta) - F(t) + \int_0^t \{F(t+\zeta-\tau) - F(t-\tau)\}dm_0(\tau), \qquad (3.33) \\ &\qquad\qquad t\ge 0,\ \zeta\ge 0, \end{aligned}$$

with $m_0(t)$ being defined by (3.4).

3.5.2.2. The functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ of a continuously inspected component

The model for a continuously inspected (class 2) component is described in section 3.3.1. First we treat the case that the initial state of the component is *functioning*. So from (3.31) it follows that

$$G_0(t,\zeta) = \Pr\{t \le \underline{\ell}_1 < t+\zeta\} + \sum_{n=1}^{\infty} \Pr\{\underline{z}_n + \underline{r}_n < t,\ t \le \underline{z}_{n+1} < t+\zeta\}$$

$$= F(t+\zeta) - F(t) + \int_0^t \{F(t+\zeta-\tau) - F(t+\tau)\}d\{m_0(\tau)*W(\tau)\}, \quad (3.34)$$

$m_0(t)$ defined by (3.7) and $t\ge 0$, $\zeta \ge 0$.

If the initial state of the component is *failed*, then by the same procedure it follows that

$$G_1(t,\zeta) = \int_0^t \{F(t+\zeta-\tau) - F(t-\tau)\}dW(\tau) + \int_0^t \{F(t+\zeta-\tau) - F(t-\tau)\}d\{m_1(\tau)*W(\tau)\}, \quad (3.35)$$

$m_1(t)$ defined by (3.7) and $t\ge 0$, $\zeta \ge 0$.

3.5.2.3. The functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ of a randomly inspected component

The process in case of random inspection is treated in section 3.3.2. By the same procedure as above it follows that if the initial state of the component is the function state, then

$$G_0(t,\zeta) = F(t+\zeta) - F(t) + \int_0^t \{F(t+\zeta-\tau) - F(t-\tau)\}d\{W(\tau)*H(\tau)*m_0(\tau)\}, \quad t\ge 0,\ \zeta \ge 0, \quad (3.36)$$

where $H(t)$ is the distribution function of $\underline{w}_i$, $i=1,2,\ldots$ and $m_0(t)$ is defined by (3.10).

If the initial state of the component is the fail state then

$$G_1(t,\zeta) = \int_0^t \{F(t+\zeta-\tau) - F(t-\tau)\}d\{W(\tau)*H(\tau)\} + \int_0^t \{F(t+\zeta-\tau) - F(t-\tau)\}d\{W(\tau)*H(\tau)*m_1(\tau)\}, \quad t\geq 0,\ \zeta\geq 0, \tag{3.37}$$

where $H(t)$ is the distribution function of $\underline{w}_i$, $i=1,2,\ldots$, and $m_1(t)$ is defined by (3.10).

3.5.3. The functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ for periodically inspected components

The behaviour of a periodically inspected (class 4) component has been described in section 3.4.3. In this case the derivation of the functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ is identical to that of the availability in section 3.4.3. Assume that the instant t belongs to the n^{th} inspection interval, particularly $t\in[t_n+\theta_n+R_n, t_{n+1}]$. Then

$$\begin{aligned}
G_0(t,\zeta) &= \Pr\{\underline{x}(t)=0,\ \underline{\zeta}(t)<\zeta \,|\, \underline{x}(0)=0\} \\
&= \Pr\{\underline{x}(t)=0,\ \underline{\zeta}(t)<\zeta, \left(\bigcap_{k=1}^{n} (\underline{x}(t_k+\theta_k)=0)\right) \,|\, \underline{x}(0)=0\} \\
&\quad + \Pr\{\underline{x}(t)=0, \underline{\zeta}(t)<\zeta, \left(\bigcup_{k=1}^{n} \left(\bigcap_{j=k+1}^{n} (\underline{x}(t_j+\theta_j)=0), \underline{x}(t_k+\theta_k)=1\right)\right) \,|\, \underline{x}(0)=0\} \\
&= \Pr\{t\leq \underline{\ell} \leq t+\zeta \,|\, \underline{x}(0)=0\} \\
&\quad + \sum_{k=1}^{n} \Pr\{\underline{x}(t_k+\theta_k)=1 \,|\, \underline{x}(0)=0\} \Pr\{\underline{x}(t)=0, \underline{\zeta}(t)<\zeta, \\
&\qquad \bigcap_{j=k+1}^{n} (\underline{x}(t_j+\theta_j)=0 \,|\, \underline{x}(t_k+\theta_k)=1,\ \underline{x}(0)=0\} \\
&= \Pr\{t\leq \underline{\ell} \leq t+\zeta\} \\
&\quad + \sum_{k=1}^{n} \{1-A_0(t_k+\theta_k)\} \int_{\tau=0}^{R_k} \Pr\{t-(t_k+\theta_k+\tau)\leq \underline{\ell} \leq t+\zeta-(t_k+\theta_k+\tau)\} dW(\tau)
\end{aligned}$$

$$= F(t+\zeta)-F(t)$$

$$+ \sum_{k=1}^{n} \{1-A_0(t_k+\theta_k)\} \int_{\tau=0}^{R_k} \{F(t+\zeta-(t_k+\theta_k+\tau))-F(t-t_k+\theta_k+\tau))\}dW(\tau)$$

$$= 1-F(t)+ \sum_{k=1}^{n} \{1-A_0(t_k+\theta_k)\} \int_{\tau=0}^{R_k} \{1-F(t-(t_k+\theta_k+\tau))\}dW(\tau) \quad (3.38)$$

$$- [1-F(t+\zeta)+ \sum_{k=1}^{n} \{1-A_0(t_k+\theta_k)\} \int_{\tau=0}^{R_k} \{1-F(t+\zeta-(t_k+\theta_k+\tau))\}dW(\tau)],$$

$$t\in[t_n+\theta_n+R_n, t_{n+1}], \zeta\geq 0.$$

From (3.18) it is seen that $G_0(t,\zeta)$ in (3.38) can be written as the difference of two availabilities, i.e. the availabilities at instant t and at instant $t+\zeta$, where both availabilities are connected to the n^{th} inspection interval. So from (3.38) it follows that

$$G_0(t,\zeta) = A_0(t) - A_0^{(n)}(t+\zeta)^*, \quad t\in[t_n+\theta_n+R_n, t_{n+1}], \zeta\geq 0, \quad (3.39)$$

with $A_0(t)$ as well as $A_0^{(n)}(t+\zeta)$ both being calculated according to the right-hand side of (3.18). Applying the above procedure for all cases occurring during the process for periodically inspected components, it turns out that the functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ can be written as:

$$G_0(t,\zeta) = A_0(t) - A_0^{(n)}(t+\zeta), \quad (3.40)$$

$$G_1(t,\zeta) = A_1(t) - A_1^{(n)}(t+\zeta), \quad (3.41)$$

for $t\in[t_n, t_{n+1}]$, $n=1,2,\ldots;\zeta\geq 0$.

Next we shall describe the functions $A_0^{(n)}(t+\zeta)$ and $A_1^{(n)}(t+\zeta)$ for $t\in[0,t_1]$ and for t belonging to each particular interval contained within $[t_n, t_{n+1}]$, $n=1,2,\ldots$, with $\zeta\geq 0$.
For $t\in[0,t_1]$ it is obvious that $A_0^{(0)}(t+\zeta)=1-F(t+\zeta)$ and $A_1^{(0)}(t+\zeta)=0$.

---

*To $A_0^{(n)}(t+\zeta)$ we have attached the index n to stress the fact that the n is related to t and not to $t+\zeta$, i.e. n is the number of inspection intervals in $[0,t]$.

Therefore, applying (3.40) and (3.41), it follows that:

$$G_0(t,\zeta) = F(t+\zeta)-F(t),\ t\in[0,t_1],\ \zeta\geq 0;$$
$$G_1(t,\zeta) = 0 \qquad ,\ t\in[0,t_1],\ \zeta\geq 0. \tag{3.42}$$

Each interval $[t_n,t_{n+1}]$,n=1,2,..., contains three distinct intervals, i.e. the intervals $[t_n,t_n+\theta_n]$, $[t_n+\theta_n,t_n+\theta_n+R_n]$ and $[t_n+\theta_n+R_n,t_{n+1}]$, respectively. For each of these intervals the functions $A_0^{(n)}(t+\zeta)$ and $A_1^{(n)}(t+\zeta)$ are defined by the same formulas as the functions $A_0(t)$ and $A_d(t)$, respectively, for that particular interval. This means that if $t\in[t_n,t_n+\theta_n]$, by definition $A_0^{(n)}(t+\zeta)=A_1^{(n)}(t+\zeta)=0$ if the inspection is EXSITU performed.
If the inspection is INSITU performed then $A_0^{(n)}(t+\zeta)$ and $A_1^{(n)}(t+\zeta)$ are defined by (3.18) and (3.24) respectively, but not for the n^{th} period but for the $(n-1)^{th}$ period (see section 3.4.3.).
If $t\in[t_n+\theta_n,t_n+\theta_n+R_n]$, then both $A_0(t)$ and $A_0^{(n)}(t+\zeta)$ are defined by (3.17), where $A_0^{(n)}(t+\zeta)$ is obtained by replacing t by $t+\zeta$, except in the upperbound of the integral of the last term in (3.17); this upperbound remains $t-(t_n+\theta_n)$. The same is true for $A_1(t)$ and $A_1^{(n)}(t+\zeta)$ with respect to (3.23). For the last interval, i.e. $t\in[t_n+\theta_n+R_n,t_{n+1}]$, $A_0(t)$ and $A_0^{(n)}(t+\zeta)$ are defined by (3.18), (cf. 3.38), whereas $A_1(t)$ and $A_1^{(n)}(t+\zeta)$ are defined by (3.24).

3.6. Applications

The formulas derived above for the availabilities $A_0(t)$, $A_1(t)$, the renewal functions $m_0(t)$ and $m_1(t)$ and for the functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ have been calculated for several lifetime and repairtime distributions. The explicit expressions thus obtained for these quantities have been listed in appendix B. In table 3.1 a review is given of the contents of appendix B.

TABLE 3.1 Summary of typical calculated variables in relation to several lifetime distributions and repair policies

PROCESS	LIFE TIME DISTRIBUTION	ORDER	REPAIR TIME DISTRIBUTION	$m_0(t)$	$m_1(t)$	$A_0(t)$	$A_1(t)$	$G_0(t,\zeta)$	$G_1(t,\zeta)$
NO REPAIR NO REPLACEMENT	n.e.d.	n.a	-	n.a	n.a	x	irr.	x	irr.
	Erlang	2	-	n.a	n.a	x	irr.	x	irr.
	Erlang	3	-	n.a	n.a	x	irr.	x	irr.
IMMEDIATE REPLACEMENT	n.e.d.	n.a	-	x	irr.		irr.	x	irr.
	Erlang	2	-	x	irr.		irr.	x	irr.
	Erlang	3	-	x	irr.		irr.	x	irr.
ALTERNATING RENEWAL PROCESS	n.e.d.	n.a	n.e.d.	x	x	x	x	x	x
			constant	xx	xx	xx	xx	xx	xx
	Erlang	2	n.e.d.	x	x	x	x	x	x
			constant	xx	xx	xx	xx	xx	xx
RANDOM TEST PROCESS	n.e.d.	n.a	n.e.d.	x	x	x	x	x	x
			constant	xx	xx	xx	xx	xx	xx
	Erlang	2	n.e.d.	xx	xx	xx	xx	xx	xx
			constant	xx	xx	xx	xx	xx	xx
PERIODICAL TESTING	n.e.d.	n.a	uniform	irr.	irr.	x	x	x	x
			constant	irr.	irr.	x	x	x	x

n.e.d : negative exponential distribution
n.a : not applicable
irr. : irrelevant
x : see appendix B
xx : available from the author on request

4. THE AVAILABILITY OF A COMPONENT DURING A PHASED MISSION

4.1. Introduction

In this chapter component behaviour during the mission is discussed. Each class of components is extensively treated, because component behaviour during the mission is *fundamental* for the probability of mission success.

During the mission component behaviour is determined by so-called *dormant parts* and *operational parts*. A *dormant part* for a component is a half-open time interval during which the component is *not* asked to become operational, whereas an *operational part* consists of a half-open time interval during which the component has to be continuously operational. A dormant part as well as an operational part may consist of several phases. Each closed time interval which consists of a *dormant part followed by an operational part* will be called a *period* of the component (see section 2.3.). The *first* period of each component consists of the OR-phase and the first operational part. These periods play an important role for the behaviour of components that are continuously inspected. For randomly tested components and for periodically inspected components only the first period is of interest because components belonging to these classes are not being tested after the mission has been started. Therefore no repair is applied to these components during the mission, however, with one exception: if such a component is tested or being repaired at the start of the mission at instant T_0 and its first operational part starts at instant $t_1' > T_0$ then testing or repair may be continued during $[T_0, t_1')$.

In section 4.2. the availability of non-repairable components is treated. Their availability is identical to the reliability.

In section 4.3. the availability of continuously inspected components during the mission is treated. The behaviour of such a component is rather complicated. Repair is only permitted during the dormant part of a period. So no repair can take place during the operational parts. Therefore, the *original* renewal process which starts at t=0 is disturbed during the first operational part, i.e. the component has to survive that time interval and therefore only one realisation of the renewal process is permitted during that operational part.

To overcome this difficulty a so-called *derived renewal process* is introduced. This derived renewal process starts at the beginning of the second period at instant t_2, see fig. 4.1. It only differs from the original renewal process with respect to the *first renewal time*. The distribution of this first renewal time is dependent on the renewal process of the foregoing period. This procedure can be repeated for the third and following periods if the component has more than two periods. So at the beginning of *each* period a derived renewal process starts. The distribution of the first renewal time of the renewal process for the k^{th} period is completely determined by the derived renewal process of the $(k-1)^{th}$ period. The availability of the component during the k^{th} period is then obtained by applying the k^{th} derived renewal process. Obviously this approach determines the availability of the component during the mission; it will be expressed by means of a recurrence relation. Since, in general, no analytical solution can be obtained from this recurrence relation, a procedure is suggested in section 4.3.4.2.2(c) by which the availability of the component can be calculated for the k^{th} period. As an example this procedure has been applied to a component with an Erlang-2 lifetime distribution and a negative exponentially distributed repairtime.

The availability of randomly tested components during the mission is treated in section 4.4. A randomly tested component is subjected to *random tests* during the OR-phase (the time interval between the instant t=0 and the start of the mission at instant T_0). However, it is assumed that no random tests are performed after the start of the mission. Therefore, no repair is applied to such a component if it is failed during the mission, with one exception: if the component is tested or being repaired at the start of the mission at instant T_0 and the start of the first operational part at instant t_1' for the component is not equal to the start of the mission, i.e. $t_1'>T_0$, then this particular test or repair may be continued. After the start of the first operational part no repair is permitted anymore. An example is discussed for the determination of the availability of a randomly tested component with negative exponentially distributed lifetime and repairtime.

In section 4.5. the availability of a periodically inspected component during the mission is discussed. Such a component is subjected to periodical inspections during the OR-phase. It is assumed that after the start of the mission no inspections are performed and no repair is effectuated,

with the same exception as described for randomly inspected components, i.e. if the component is inspected or being repaired at the start of the mission, then the appropriate action may be continued, but after the start of the first operational part no inspections nor repair is permitted anymore.
The two figures 4.7 and 4.8 show the unavailability of the component during the mission for different situations, viz. the component is being repaired at the start of the mission and the component is not inspected nor being repaired at the start of the mission.
The last section of this chapter, i.e. section 4.6., is devoted to a subject that perhaps should be better treated in chapter 6, which describes phased mission theory. However, to be complete in treating just component behaviour and not system behaviour, the discussion of *conditional* availability of a component during the mission is added to this chapter.
Such a conditional availability arises for a component during the mission when the component is present in more than one system. For instance, suppose that the component belongs to system S_j and system S_ℓ where phase j occurs earlier than phase ℓ. Suppose further that we want to calculate the probability of the event "system S_j failed at instant T_j *and* system S_ℓ failed at instant t , $t>T_j$ and t in phase ℓ. In developing this probability it appears that we have to calculate among others the availability of the component at instant t with respect to its fail state at instant T_j (see chapter 6). For a further detailed description of these conditional availabilities the reader is referred to chapter 6. In section 4.6. of this chapter the conditional availabilities are treated for all classes of components.

4.2. The availability of a non-repairable component during the mission

A class 1 component is assumed to be non-repairable (see section 2.5.). Therefore the event "the component is available at instant t" is equivalent to the event "the component has survived the interval [0,t)". The probability of the latter event is simply the component's reliability at instant t, no matter whether the instant t belongs to the "OR-phase" or to the mission itself. So

$$A_i(t) = 1-F(t),\ t\geq 0. \qquad (4.1)$$

4.3. The availability of continuously inspected components during the mission

In this section the availability of class 2 components during the mission will be discussed. In section 4.3.1. a *derived renewal process* is introduced for each period of the component. This *derived renewal process* arises due to the fact that during the operational part of the first period of the component the original renewal process is interrupted, because no repair is permitted during the operational part of a period.
As an introduction in section 4.3.2. the availability of a component will be calculated for the case that the component is in its first period. Limitation to the first period provides a clear demonstration of the technique used to calculate the availability in general.
In section 4.3.3. the general formula for the availability of a component is derived and after that some applications are treated in section 4.3.4.

4.3.1. The derived renewal process

During the dormant part of the first period (see fig. 4.1) the component is subjected to the alternating renewal process formed by successive lifetimes and repairtimes, i.e. during the dormant time interval this renewal process is not disturbed, but during the following operational part this renewal process is interrupted because no repair is permitted during an operational part of a period.
If there exists a second period for the component, then at the start t_2 of the second period, again a renewal process starts at the beginning of that period. This renewal process lasts till the instant t_2', i.e. the start of the operational part of the second period. At that instant it is interrupted like the renewal process in the first period.
The renewal process starting at the beginning of the second period at t_2 differs from the renewal process of the first period only by its first renewal time. Therefore we shall call it a *derived renewal process*.

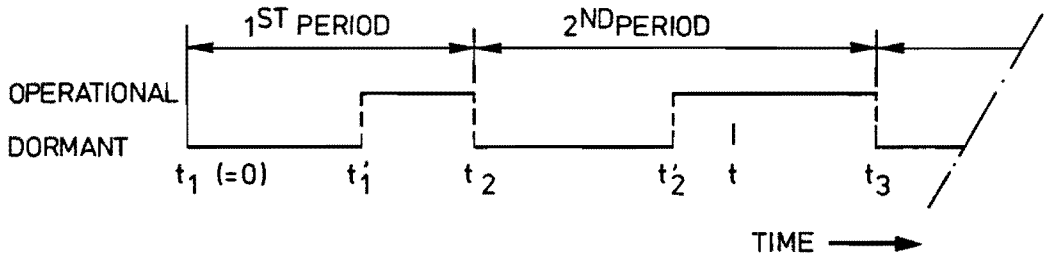


FIG.4.1. SECOND PERIOD OF A COMPONENT.

Three different realizations are possible for the first renewal time of this derived renewal process for the second period:

(i) the component survives the operational part of the first period. The first renewal time of the derived renewal process is the residual lifetime of the component at the start of the second period at t_2;

(ii) the component fails before t_1' (the start of the operational part of the first period) and repair is not yet finished at t_1'. The first renewal time of the derived renewal process is the sum of the residual repairtime of the component at t_1' and the following lifetime;

(iii) the component fails during the operational part of the first period which starts at t_1', so no repair has been taken place at the end of the operational part at t_2.
Therefore the first renewal time is the sum of a complete repair-time and the following lifetime.

The residual lifetime and repairtime, mentioned in (i) and (ii), are dependent of the renewal process of the first period. The same reasoning can be applied in the case that a component possesses more than two periods. Then the component's behaviour during the dormant part of each of these periods is subjected to a *derived renewal process. The several renewal processes only differ by their first renewal times.* The first renewal time of the derived renewal process starting at the beginning of the k^{th} period is only dependent of the derived renewal process starting at the beginning of the $(k-1)^{th}$ period.

4.3.2. The availability of a continuously inspected component during its first period

A period of component c is characterized by three time points, i.e. the time at which the period starts, the time at which the operational part of the period starts and the time at which that period ends. In general the last mentioned time is the starting time for the next component's period except for its last period. It is therefore that the following variables are introduced:

$$t_k \stackrel{def}{=} \text{starting time of period k of component c ,} \tag{4.2}$$

$$t'_k \stackrel{def}{=} \text{starting time of the operational part of period k of component c ,} \tag{4.3}$$

$$k=1,2,\ldots ,$$

where $t_1 \stackrel{def}{=} 0$.

The assumed behaviour of the component is shown in fig. 4.2., see also fig. 4.3. The component has to be dormant from t=0 up to $t=t'_1$, when the component has to become operational.

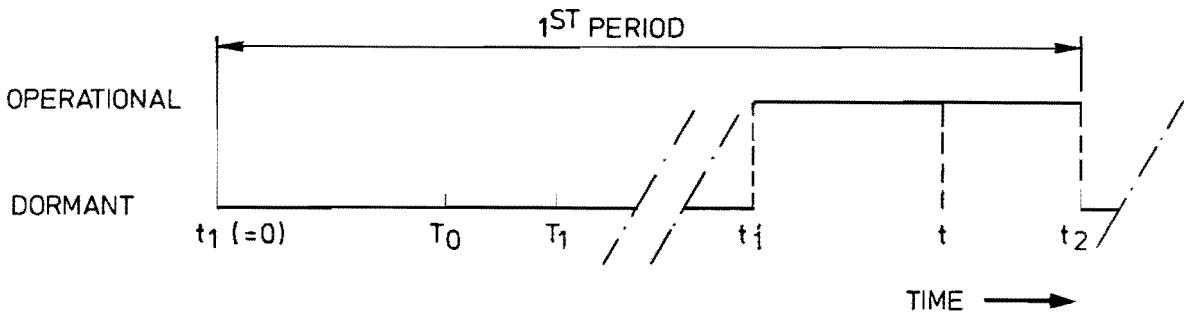


FIG. 4.2. THE FIRST PERIOD OF A COMPONENT.

Denote by

$$A(t) \stackrel{def}{=} \text{availability of component c at time t, } t\geq 0. \tag{4.5}$$

So

$$A(t) = Pr\{\underline{x}(t)=0\}, \tag{4.6}$$

$\underline{x}(t)$ defined by (2.2).

During the dormant part of the first period (the OR-phase) the component's behaviour is determined by the original renewal process that has started at $t=t_1$ with the initial state the function state or the fail state.
So for $t\in[t_1,t_1')$ the availability A(t) becomes

$$\begin{aligned} A(t) &= \Pr\{\underline{x}(t)=0\} \\ &= \Pr\{\underline{x}(t)=0,\ \underline{x}(t_1)=0\} + \Pr\{\underline{x}(t)=0,\ \underline{x}(t_1)=1\} \\ &= \Pr\{\underline{x}(t)=0 \mid \underline{x}(t_1)=0\}\ \Pr\{\underline{x}(t_1)=0\} \\ &\quad + \Pr\{\underline{x}(t)=0 \mid \underline{x}(t_1)=1\}\ \Pr\{\underline{x}(t_1)=1\}, \qquad t\in[t_1,t_1'). \end{aligned} \tag{4.7}$$

Define:

$$A_{0,k}(t) = \Pr\{\underline{x}(t)=0 \mid \text{given at instant } t_k \text{ component c is in the function state}\}; \tag{4.8}$$

$$A_{1,k}(t) = \Pr\{\underline{x}(t)=0 \mid \text{given at instant } t_k \text{ component c is in the fail state}\}, \tag{4.9}$$

$$k=1,2,\ldots .$$

From the above definitions the availability in (4.7) can be written as

$$\begin{aligned} A(t) &= A_{0,1}(t)A_{0,1}(t_1) + A_{1,1}(t)A_{1,1}(t_1) \\ &= A_{0,1}(t)A_{0,1}(t_1) + A_{1,1}(t)\{1-A_{0,1}(t_1)\}, \qquad t\in[t_1,t_1'), \end{aligned} \tag{4.10}$$

with $A_{0,1}(t_1)$ as the initial condition, i.e. $A_{0,1}(t_1) \stackrel{\text{def}}{=} A_{0,1}(0)$ is the probability that component c is in the function state at the start of the first renewal process.
In calculating the availability of the continuously inspected component at instant t in the operational part of the period, i.e. $t\in[t_1',t_2)$, two conditions have to be fulfilled:

- the component has to be available at instant t_1';
- the component has to survive the time interval $t-t_1'$.

So the availability at instant t depends on the availability at instant t_1', which in turn depends on the state of the component at the start of its renewal process. Since no repair is permitted during the operational part of a period of component c (see section 2.5.), obviously the component is in the fail state at instant t, $t\in[t_1',t_2)$, if it is in the fail

state at instant t_1', i.e. $\Pr\{\underline{x}(t)=0, \underline{x}(t_1')=1\}=0$. So the next result is obtained:

$$\begin{aligned} A(t) &= \Pr\{\underline{x}(t)=0, \underline{x}(t_1')=0\} \\ &= \Pr\{\underline{x}(t)=0, \underline{x}(t_1')=0, \underline{x}(t_1)=0\} + \Pr\{\underline{x}(t)=0, \underline{x}(t_1')=0, \underline{x}(t_1)=1\} \\ &= \Pr\{\underline{x}(t)=0, \underline{x}(t_1')=0 \mid \underline{x}(t_1)=0\} \Pr\{\underline{x}(t_1)=0\} \\ &\quad + \Pr\{\underline{x}(t)=0, \underline{x}(t_1')=0 \mid \underline{x}(t_1)=1\} [1-\Pr\{\underline{x}(t_1)=0\}], \\ &\qquad\qquad t\in[t_1', t_2). \end{aligned} \tag{4.11}$$

Define the functions

$H_{0,k}(t,t_k';t_k)$ = the probability that component c is available during the whole interval $[t_k',t]$, given at instant t_k the component is in the function state, $t\geq t_k'>t_k$; (4.12)

$H_{1,k}(t,t_k';t_k)$ = the probability that component c is available during the whole interval $[t_k',t]$, given at instant t_k the component is in the fail state, $t\geq t_k'>t_k$, (4.13)

t_k and t_k' defined by (4.2) and (4.3), respectively.
Applying the definitions (4.6), (4.12) and (4.13) to (4.11) we get for the availability

$$A(t) = H_{0,1}(t,t_1';t_1)\, A_{0,1}(t_1) + H_{1,1}(t,t_1';t_1)\{1-A_{0,1}(t_1)\}, \qquad t\in[t_1',t_2). \tag{4.14}$$

The next step concerns the derivation of expressions for the functions $H_{0,1}(t,t_1';t_1)$ and $H_{1,1}(t,t_1';t_1)$. By definition (4.12)

$$H_{0,1}(t,t_1';t_1) = \Pr\{\underline{x}(t)=0, \underline{x}(t_1')=0 \mid \underline{x}(t_1)=0\}. \tag{4.15}$$

Because no repair is permitted during the operational part of a period the event "$\underline{x}(t)=0$, $\underline{x}(t_1')=0$" is equal to the event "the residual lifetime of component c at t_1' exceeds $t-t_1'$, $\underline{x}(t_1')=0$". So define:

$\underline{\zeta}(t)$ = residual lifetime of component c at instant t; (4.16)

$G_{0,k}(t,\tau)$ = $\Pr\{\underline{\zeta}(t)<\tau,\ \underline{x}(t)=0 \mid$ given at instant t_k component c is in the function state$\}$; (4.17)

$G_{1,k}(t,\tau)$ = $\Pr\{\underline{\zeta}(t)<\tau,\ \underline{x}(t)=0 \mid$ given at instant t_k component c is in the fail state$\}$. (4.18)

Applying (4.16) and (4.17) to (4.15) we get

$$H_{0,1}(t,t_1';t_1) = \Pr\{\underline{\zeta}(t_1')>t-t_1',\ \underline{x}(t_1')=0|\underline{x}(t_1)=0\}$$
$$= \Pr\{\underline{x}(t_1')=0|\underline{x}(t_1)=0\} - \Pr\{\underline{\zeta}(t_1')<t-t_1',\ \underline{x}(t_1'=0|\underline{x}(t_1)=0\}$$
$$= A_{0,1}(t_1'-t_1)-G_{0,1}(t_1'-t_1,t-t_1'), \quad t\in[t_1',t_2). \quad (4.19)$$

By the same procedure the function $H_{1,1}(t,t_1';t_1)$ reads

$$H_{1,1}(t,t_1';t_1) = A_{1,1}(t_1'-t_1)-G_{1,1}(t_1'-t_1,t-t_1'), \quad t\in[t_1',t_2). \quad (4.20)$$

The functions $G_{i,.}(.,.)$ and the availabilities $A_{.,.}(.)$ of the component are extensively treated in chapter 3.
If the initial conditions, i.e. $A_{.,1}(t_1)$, are known, then by (4.10), (4.14), (4.19) and (4.20) the availability of the component at time t during the first period is completely determined.

4.3.3. The availability of a continuously inspected component during its k^{th} period

This general case is sketched in fig. 4.3.

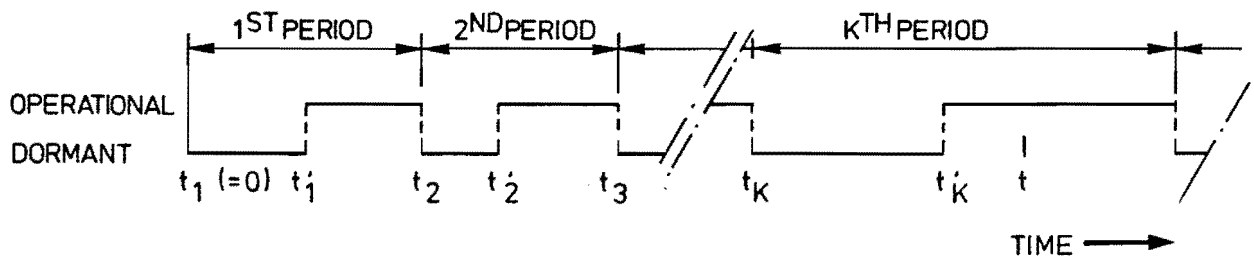


FIG.4.3. K^{TH} PERIOD OF A COMPONENT.

Denote by

$$P_k(t) \stackrel{def}{=} \text{availability of component c at instant t, t belonging to period k;} \tag{4.21}$$

$$P_0(t_1) \stackrel{def}{=} A_{0,1}(t_1). \tag{4.22}$$

From (4.21) it follows for the availability $P_k(t)$ of the component at instant t during the k^{th} period that

$$\begin{aligned} P_k(t) &= \Pr\{\underline{x}(t)=0\}, \\ &= \Pr\{\underline{x}(t)=0,\ \underline{x}(t_k)=0 \cup \underline{x}(t_k)=1\} \\ &= \Pr\{\underline{x}(t)=0 \mid \underline{x}(t_k)=0\}\ \Pr\{\underline{x}(t_k)=0\} \\ &\quad + \Pr\{\underline{x}(t)=0 \mid \underline{x}(t_k)=1\}\ [1-\Pr\{\underline{x}(t_k)=0\}], \qquad t\in[t_k,t_{k+1}). \end{aligned}$$

Applying (4.21) to the right-hand side of the above mentioned expression, we get the recurrence relation

$$\begin{aligned} P_k(t) &= \Pr\{\underline{x}(t)=0 \mid \underline{x}(t_k)=0\}\ P_{k-1}(t_k) \\ &\quad + \Pr\{\underline{x}(t)=0 \mid \underline{x}(t_k)=1\}\ [1-P_{k-1}(t_k)], \qquad t\in[t_k,t_{k+1}). \end{aligned} \tag{4.23}$$

We know from section 4.3.1., that a derived renewal process starts at $t=t_k$, the beginning of the k^{th} period. The first probability in the right-hand side of (4.23) is conditioned with respect to the event "$\underline{x}(t_k)=0$", so the initial state of the derived renewal process is the function state, whereas the probability in the second term is conditioned to the event "$\underline{x}(t_k)=1$", i.e. the initial state of the derived renewal process is the fail state. The availability of component c at time t during the *dormant* part of the k^{th} period follows directly from (4.23):

$$P_k(t) = A_{0,k}(t)P_{k-1}(t_k) + A_{1,k}(t)\ \{1-P_{k-1}(t_k)\}, \qquad t\in[t_k,t_k'), \tag{4.24}$$

where the availabilities $A_{\cdot,k}(.)$ are determined by the derived renewal process starting at t_k.
The availability of component c at time t during the *operational* part depends on the availability at time t_k'. So we get from (4.23)

$$P_k(t) = \Pr\{\underline{x}(t)=0,\ \underline{x}(t_k')=0 \,|\, \underline{x}(t_k)=0\}\ P_{k-1}(t_k) + \\ + \Pr\{\underline{x}(t)=0,\ \underline{x}(t_k')=0 \,|\, \underline{x}(t_k)=1\}\ [1-P_{k-1}(t_k)], \qquad (4.25)$$
$$t\in[t_k', t_{k+1}).$$

Along the same lines as in section 4.3.2. we get for (4.25) with (4.12) and (4.13):

$$P_k(t) = H_{0,k}(t,t_k';t_k)P_{k-1}(t_k) + H_{1,k}(t,t_k';t_k)[1-P_{k-1}(t_k)], \qquad (4.26)$$
$$t\in[t_k', t_{k+1}),$$

with

$$H_{0,k}(t,t_k';t_k) = A_{0,k}(t_k')-G_{0,k}(t_k',t-t_k'),$$
$$H_{1,k}(t,t_k';t_k) = A_{1,k}(t_k')-G_{1,k}(t_k',t-t_k'), \qquad t\in[t_k', t_{k+1}), \qquad (4.27)$$

where the availabilities $A_{.,k}(.)$ and the functions $G_{.,k}(.,.)$ are determined by the derived renewal process starting at t_k.
The availabilities $P_k(t)$ in the relations (4.23) and (4.26) both depend on the availabilities at each endpoint of the foregoing periods and on the initial condition $P_0(t_1)=A_{0,1}(t_1)$. Therefore, we shall first solve relation (4.26) for $t=t_{k+1}$ in order to determine $P_k(t_{k+1})$, k=0,1,... . So define

$$p_k = P_k(t_{k+1}),$$
$$a_k = H_{0,k}(t_{k+1},t_k';t_k), \qquad (4.28)$$
$$b_k = H_{1,k}(t_{k+1},t_k';t_k).$$

Substitution of (4.28) into (4.26) for $t=t_{k+1}$ gives

$$p_k = a_k p_{k-1} + b_k(1-p_{k-1})$$
$$= (a_k-b_k)p_{k-1} + b_k, \quad k=1,2,\ldots . \qquad (4.29)$$

with the initial condition

$$p_0 = A_{0,1}(t_1).$$

The solution of the recurrence relation (4.29) reads

$$p_k = \prod_{j=1}^{k} (a_j - b_j) p_0 + \sum_{j=1}^{k} \{ \prod_{\ell=j+1}^{k} (a_\ell - b_\ell) \} b_j, \quad k=1,2,\ldots . \tag{4.30}$$

Applying (4.28) to (4.30), it follows that

$$P_k(t_{k+1}) = \prod_{j=1}^{k} \{H_{0,j}(t_{j+1},t_j';t_j) - H_{1,j}(t_{j+1},t_j';t_j)\} P_0(t_1)$$

$$+ \sum_{j=1}^{k} [\prod_{\ell=j+1}^{k} \{H_{0,\ell}(t_{\ell+1},t_\ell';t_\ell) - H_{1,\ell}(t_{\ell+1},t_\ell';t_\ell)\}] \tag{4.31}$$

$$\cdot H_{1,j}(t_{j+1},t_j';t_j), \quad k=1,2, \ldots .$$

It is seen from (4.24), (4.26) and (4.31) that if the functions $A_{.,k}(.)$ and $H_{.,k}(.,.;.)$ are determined and the initial condition $P_0(t_1)$ is known, then the availability $P_k(t)$ is completely determined for the dormant part as well as for the operational part of the k^{th} period.

4.3.4. Some applications for continuously inspected components

In this section two examples shall be treated for the determination of the availability of a class 2 component during the mission. The first example treats the case that both the lifetime and the repairtime of the component are negative exponentially distributed. The second example treats the situation where the component has a negative exponentially distributed repairtime and an Erlang-2 distributed lifetime. In both cases exact analytical solutions are obtained.

4.3.4.1. The availability of a continuously inspected component during its k^{th} period with negative exponential lifetime and repairtime distribution

Because the negative exponential distribution is memoryless, the residual lifetime and repairtime, mentioned in section 4.3.2., have the same distribution as the original lifetime and repairtime, respectively. Therefore, all the derived renewal processes are identical to the renewal process that starts at the beginning of the first period.

The lifetime distribution F(t) and the repairtime distribution W(t) of component c are defined by

$$F(t) = 1-e^{-\lambda t},\ \lambda>0, t\geq 0;$$
$$W(t) = 1-e^{-\mu t},\ \mu>0, t\geq 0. \tag{4.32}$$

From the definitions (4.8) and (4.9) and from appendix B, where $A_{0,1}(t)$, $A_{1,1}(t)$, $G_{0,1}(t,\zeta)$ and $G_{1,1}(t,\zeta)$ have been calculated (cf. (B32),...,(B35)), it follows for k=1,2,..., that for $t_k \leq t < t_k'$,

$$A_{0,k}(t) = 1 - \frac{\lambda}{\lambda+\mu}\{1-e^{-(\lambda+\mu)(t-t_k)}\}, \tag{4.33}$$

$$A_{1,k}(t) = \frac{\mu}{\lambda+\mu}\{1-e^{-(\lambda+\mu)(t-t_k)}\}, \tag{4.34}$$

$$G_{0,k}(t,\zeta) = (1-e^{-\lambda\zeta})\, A_{0,k}(t), \tag{4.35}$$

$$G_{1,k}(t,\zeta) = (1-e^{-\lambda\zeta})\, A_{1,k}(t). \tag{4.36}$$

Because the residual lifetime is independent of the history of the renewal process it follows from (4.27) that

$$H_{.,k}(t,t_k';t_k) = A_{.,k}(t_k') - G_{.,k}(t_k', t-t_k')$$
$$= e^{-\lambda(t-t_k')} A_{.,k}(t_k'), \qquad t\in[t_k', t_{k+1}). \tag{4.37}$$

Substitution of (4.33) and (4.34) into (4.37), and then by substituting the result into (4.31) gives

$$P_k(t_{k+1}) = \exp\{-\lambda(t_{k+1}-t_1) - \mu \sum_{j=1}^{k}(t_j'-t_j)\}P_0(t_1)$$
$$+ \frac{\mu}{\lambda+\mu}\sum_{j=1}^{k}\exp\{-\lambda(t_{k+1}-t_j') - \mu\sum_{\ell=j+1}^{k}(t_\ell'-t_\ell)\} \tag{4.38}$$
$$\cdot\,[1-\exp\{-(\lambda+\mu)(t_j'-t_j)\}],$$

$P_0(t_1)$ being the initial condition.

Applying (4.33) and (4.34) to (4.24) results in the availability of component c at instant t during the *dormant* part of the k^{th} period:

$$P_k(t) = e^{-(\lambda+\mu)(t-t_k)} P_{k-1}(t_k) + \frac{\mu}{\lambda+\mu}\{1-e^{-(\lambda+\mu)(t-t_k)}\}, \qquad t\in[t_k,t_k'), \tag{4.39}$$

with $P_{k-1}(t_k)$ given by (4.38).
Using (4.33), (4.34) and (4.37) we get from (4.26) the availability of component c at instant t during the *operational* part of the k^{th} period:

$$P_k(t) = \left[e^{-(\lambda+\mu)(t_k'-t_k)} P_{k-1}(t_k) + \frac{\mu}{\lambda+\mu}\{1-e^{-(\lambda+\mu)(t_k'-t_k)}\}\right] e^{-\lambda(t-t_k')}, \qquad t\in[t_k',t_{k+1}). \tag{4.40}$$

In fig. 4.4. an illustration is given for the *unavailability* of a continuously inspected component during the mission as described in this section with the initial availability $P_0(t_1)=1$. We have taken the *unavailability* instead of the *availability*, since the latter function is in practical situations, i.e. for reliable components, near to the value one, and therefore difficult to represent as a curve.

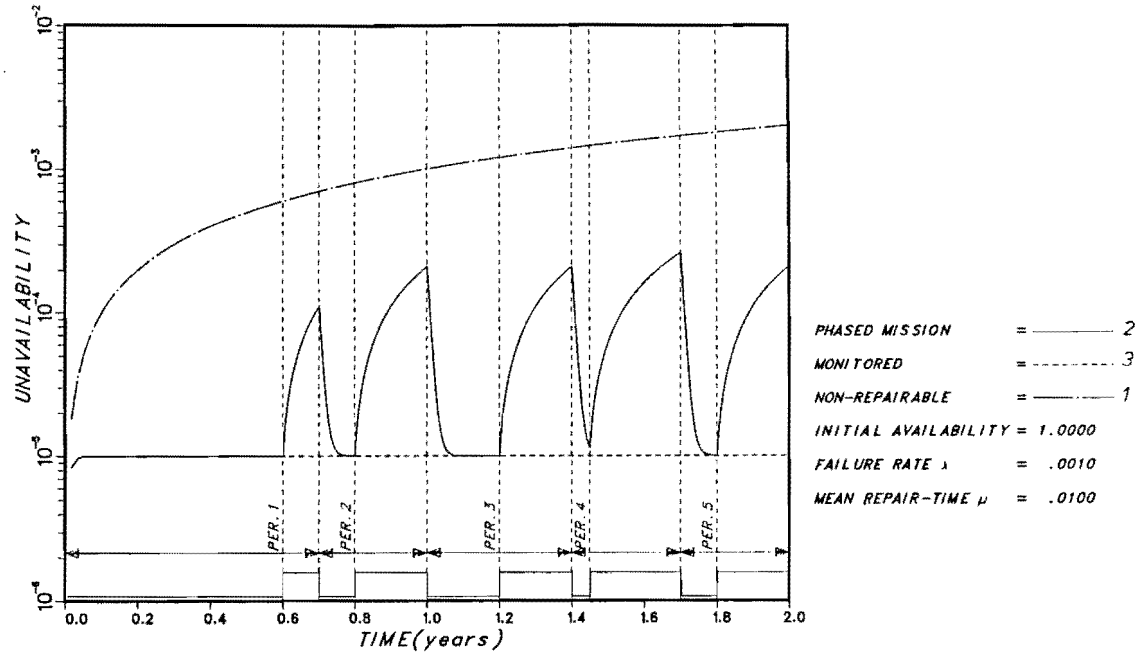


FIG.4.4 UNAVAILABILITY FOR A CONTINUOUSLY INSPECTED COMPONENT DURING A PHASED MISSION
N.E.D. LIFETIME DISTRIBUTION
N.E.D. REPAIRTIME DISTRIBUTION

Three curves are shown, i.e.

(i) curve 1: the component is non-repairable (class 1 component);
(ii) curve 2: the component is continuously inspected (class 2 component) and fulfills a mission;
(iii) curve 3: The component is continuously inspected (class 2 component) and does not fulfill a mission. (So the unavailability is continuously governed by the original renewal process and therefore not disturbed).

The determination of the figure has been realized as follows. To calculate the curve 2 we start with an initial availability $P_0(t_1)=1$.
For given t first k is determined. Then $P_{k-1}(t_k)$ is calculated by means of (4.38). After that the availability $P_k(t)$ is determined by (4.39) or (4.40) depending on whether the instant t belongs to the dormant part of the period or to the operational part. The determination of the curve 1 is effectuated by (4.1) and (4.32), whereas the curve 3 is determined by (4.39) with k=1 and $P_0(t_1)=1$.

In fig. 4.4. component c has five periods in case of the mission (curve 2). The failure rate is 10^{-3}/hr and its mean repairtime is 10^{-2} hr. (These figures are fictitious and possess no practical meaning). It is seen that during the OR-phase curve 2 and curve 3 are identical, which could be expected. After that curve 2 is between curve 1 and curve 3, as it should be; because curve 1 shows the unavailability of component c_i in the case that the component is not inspected, so no repair is possible at all, while curve 3 shows the unavailability in the case of the most optimal detection and repair policy (continuous inspection).

4.3.4.2. The availability of a continuously inspected component during its k^{th} period with Erlang-2 lifetime distribution and a negative exponential repairtime distribution

The Erlang-2 lifetime distribution F(t) and the negative exponential repairtime distribution W(t) are defined by:

$$F(t) = 1-(1+\lambda t)e^{-\lambda t},\ \lambda>0, t\geq 0;$$
$$W(t) = 1-e^{-\mu t},\ \mu>0,\ t\geq 0. \qquad (4.41)$$

If a continuously inspected component has an Erlang-2 lifetime distribution and a negative exponentially distributed repairtime, then the derived renewal processes with initial state the *fail state* are identical to the original renewal process that starts at $t=t_1$ with initial state the fail state. *However, the derived renewal processes starting with initial state the function state are not identical.* This because the Erlang-2 distribution has a memory. Therefore these derived renewal processes differ with respect to their first renewal time distribution (see section 4.3.2.(i)). Because the availability during the first period has been discussed in section 3.4.1. concerning the dormant part and in section 3.5.2.2. with respect to the operational part of this period, we shall start here with deriving the first renewal time distribution for the second period of the component with initial state the function state. Subsequently the availability of the component during the dormant part as well as during the operational part shall be calculated for this period.
The advantage in calculating the relevant functions for the second period is to demonstrate the method and to get insight into the formulas obtained, since the formulas for the k^{th} period are more complicated.
The last section will be devoted to the derivation of the characteristics for the k^{th} period.

4.3.4.2.1. The availability of a continuously inspected component during its second period

4.3.4.2.1(a) The distribution of the first renewal time of the derived renewal process in the second period with initial state the function state

The first renewal time distribution $F_2^{(1)}(t)$ of the derived renewal process for the second period of component c with initial state the function state is defined by:

$$F_2^{(1)}(t) = \Pr\{\underline{\ell}_2^{(1)} < t \mid \underline{x}(t_2)=0\},\ t>0, \tag{4.42}$$

with

$\underline{\ell}_2^{(1)} \stackrel{def}{=}$ the first lifetime of component c during the derived renewal process in the second period.

The distribution function $F_2^{(1)}(t)$ is in fact the residual lifetime distribution of the renewal process of the first period of the component at instant t_2, conditioned to the event that the residual lifetime has survived the time interval $[0,t_2-t_1']$. So in (4.42) the event "$\underline{x}(t_2)=0$" is similar to the event "$\underline{x}(t_1')=0,\underline{\zeta}(t_1')\geq t_2-t_1'$" , $\underline{\zeta}(t_1')$ being the residual lifetime of component c at t_1' as defined by (4.16).

Therefore (4.42) becomes:

$$
\begin{aligned}
F_2^{(1)}(t) &= \Pr\{\underline{\ell}_2^{(1)}<t \mid \underline{x}(t_1')=0,\ \underline{\zeta}(t_1')\geq t_2-t_1'\} \\
&= \Pr\{\underline{\ell}_2^{(1)}<t,\ \underline{x}(t_1)=0 \mid \underline{x}(t_1')=0,\ \underline{\zeta}(t_1')\geq t_2-t_1'\} \\
&\quad + \Pr\{\underline{\ell}_2^{(1)}<t,\ \underline{x}(t_1)=1 \mid \underline{x}(t_1')=0,\ \underline{\zeta}(t_1')\geq t_2-t_1'\} \\
&= \frac{\Pr\{\underline{\ell}_2^{(1)}<t,\ \underline{x}(t_1')=0,\ \underline{\zeta}(t_1')\geq t_2-t_1' \mid \underline{x}(t_1)=0\}}{\Pr\{\underline{x}(t_1')=0,\ \underline{\zeta}(t_1')\geq t_2-t_1' \mid \underline{x}(t_1)=0\}} \Pr\{\underline{x}(t_1)=0\} \\
&\quad + \frac{\Pr\{\underline{\ell}_2^{(1)}<t,\ \underline{x}(t_1')=0,\ \underline{\zeta}(t_1')\geq t_2-t_1' \mid \underline{x}(t_1)=1\}}{\Pr\{\underline{x}(t_1')=0,\ \underline{\zeta}(t_1')\geq t_2-t_1' \mid \underline{x}(t_1)=1\}} [1-\Pr\{\underline{x}(t_1)=0\}],
\end{aligned}
\tag{4.43}
$$

where t_1' is the length of the *dormant part* and t_2-t_1' the length of the *operational part* of the first period.
In (4.43) the event "$\underline{\ell}_2^{(1)}<t,\ \underline{\zeta}(t_1')\geq t_2-t_1'$" is similar to the event "$t_2-t_1'\leq\underline{\zeta}(t_1')<t+t_2-t_1'$". So

$$
\begin{aligned}
F_2^{(1)}(t) &= \frac{\Pr\{t_2-t_1'\leq\underline{\zeta}(t_1')<t+t_2-t_1',\ \underline{x}(t_1')=0 \mid \underline{x}(t_1)=0\}\ \Pr\{\underline{x}(t_1)=0\}}{\Pr\{\underline{x}(t_1')=0 \mid \underline{x}(t_1)=0\}-\Pr\{\underline{\zeta}(t_1')<t_2-t_1',\ \underline{x}(t_1')=0 \mid \underline{x}(t_1)=0\}} \\
&\quad + \frac{\Pr\{t_2-t_1'\leq\underline{\zeta}(t_1')<t+t_2-t_1',\underline{x}(t_1')=0|\underline{x}(t_1)=1\}[1-\Pr\{\underline{x}(t_1)=0\}]}{\Pr\{\underline{x}(t_1')=0|\underline{x}(t_1)=1\}-\Pr\{\underline{\zeta}(t_1')<t_2-t_1',\underline{x}(t_1')=0|\underline{x}(t_1)=1\}} \\
&\qquad\qquad 0\leq t\leq t_3-t_2.
\end{aligned}
\tag{4.44}
$$

Applying (4.8), (4.9), (4.17), (4.18) and (4.22) to (4.44) we get:

$$
\begin{aligned}
F_2^{(1)}(t) &= \frac{G_{0,1}(t_1',t+t_2-t_1')-G_{0,1}(t_1',t_2-t_1')}{A_{0,1}(t_1') - G_{0,1}(t_1',t_2-t_1')} P_0(t_1) \\
&\quad + \frac{G_{1,1}(t_1',t+t_2-t_1')-G_{1,1}(t_1',t_2-t_1')}{A_{1,1}(t_1') - G_{1,1}(t_1',t_2-t_1')} \{1-P_0(t_1)\}, \\
&\qquad\qquad 0\leq t\leq t_3-t_2.
\end{aligned}
\tag{4.45}
$$

From appendix B, (cf. (B38), (B39) and (B40)), three distinct cases can be considered with respect to the functions $A_{.,1}(.)$ and $G_{.,1}(.,.)$. This distinction depends on the values of the parameters λ and μ, viz.

(i) $\mu > 4\lambda$,

(ii) $\mu = 4\lambda$,

(iii) $\mu < 4\lambda$.

For each of these different situations the functions $A_{.,1}(.)$ and $G_{.,1}(.,.)$ are calculated in section B3.2. of appendix B. Here we shall only treat case (i), i.e. $\mu>4\lambda$, because this assumption is the most practical one. The reason for this is that $\mu>4\lambda$ implies $1/\mu < 1/4\lambda$, i.e. the mean repairtime is smaller than a quarter of the mean lifetime, which is mostly the case for components used in technical installations.
So from appendix B, formulas (B45), (B46), (B49) and (B51), it follows that the availabilities $A_{.,1}(.)$ and the functions $G_{.,1}(.,.)$ of the first period are given by:

$$A_{0,1}(t) = 1 - \frac{1}{\mu}\left[\nu_{1,1}+\nu_{2,1}e^{\rho_1 t}-\nu_{3,1}e^{\rho_2 t}\right], \qquad t\in[t_1,t_1'), \tag{4.46}$$

$$\rho_{1,2} = -\frac{1}{2}(\mu+2\lambda) \pm \frac{1}{2}\sqrt{\mu^2-4\lambda\mu}, \qquad \mu>4\lambda, \tag{4.47}$$

$$\nu_{1,1} = \frac{\mu\lambda^2}{\rho_1\rho_2}, \quad \nu_{2,1} = \frac{\mu\lambda^2}{\rho_1(\rho_1-\rho_2)}, \quad \nu_{3,1} = \frac{\mu\lambda^2}{\rho_2(\rho_1-\rho_2)}; \tag{4.48}$$

$$A_{1,1}(t) = 1 - \frac{\lambda}{\lambda+2\mu} + \frac{\mu}{\rho_1-\rho_2}\left\{\frac{\rho_1+2\lambda}{\rho_1}e^{\rho_1 t} - \frac{\rho_2+2\lambda}{\rho_2}e^{\rho_2 t}\right\}, \qquad t\in[t_1,t_1'); \tag{4.49}$$

$$G_{0,1}(t_1',\zeta) = g_{0,1}(t_1')\{1-(1+\lambda\zeta)e^{-\lambda\zeta}\}+h_{0,1}(t_1')\lambda(1-e^{-\lambda\zeta}), \qquad 0\le\zeta\le t_2-t_1', \tag{4.50}$$

$$g_{0,1}(t_1') = \frac{\mu}{\lambda+2\mu} + \frac{\lambda^2\mu}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1(t_1'-t_1)}}{\rho_1(\rho_1+\lambda)} - \frac{e^{\rho_2(t_1'-t_1)}}{\rho_2(\rho_2+\lambda)}\right\}, \tag{4.51}$$

$$h_{0,1}(t_1') = \frac{\mu}{\lambda(\lambda+2\mu)} + \frac{\lambda^2\mu}{\rho_1-\rho_2}\{\frac{e^{\rho_1(t_1'-t_1)}}{\rho_1(\rho_1+\lambda)^2} - \frac{e^{\rho_2(t_1'-t_1)}}{\rho_2(\rho_2+\lambda)^2}\}; \quad (4.52)$$

$$G_{1,1}(t_1',\zeta) = g_{1,1}(t_1')\{1-(1+\lambda\zeta)e^{-\lambda\zeta}\}+h_{1,1}(t_1')\lambda(1-e^{-\lambda\zeta}),$$

$$0\le\zeta\le t_2-t_1', \quad (4.53)$$

$$g_{1,1}(t_1') = \frac{\mu}{\lambda+2\mu} + \frac{\lambda\mu^2}{\rho_1-\rho_2}\{\frac{e^{\rho_1(t_1'-t_1)}}{\rho_1(\rho_1+\mu)(\rho_1+\lambda)} - \frac{e^{\rho_2(t_1'-t_1)}}{\rho_2(\rho_2+\mu)(\rho_2+\lambda)}\}, \quad (4.54)$$

$$h_{1,1}(t_1') = \frac{\mu}{\lambda+2\mu} + \frac{\lambda\mu^2}{\rho_1-\rho_2}\{\frac{e^{\rho_1(t_1'-t_1)}}{\rho_1(\rho_1+\mu)(\rho_1+\lambda)^2} - \frac{e^{\rho_2(t_1'-t_1)}}{\rho_2(\rho_2+\mu)(\rho_2+\lambda)^2}\}, \quad (4.55)$$

with ρ_1 and ρ_2 in (4.48),...,(4.55) as defined by (4.47).

Next define:

$$v_{0,1}(t,\tau) \stackrel{\text{def}}{=} \frac{P_0(t_1)}{A_{0,1}(t)-G_{0,1}(t,\tau)}, \qquad t>0,\tau>0; \quad (4.56)$$

$$v_{1,1}(t,\tau) \stackrel{\text{def}}{=} \frac{1-P_0(t_1)}{A_{1,1}(t)-G_{1,1}(t,\tau)}, \qquad t>0,\tau>0, \quad (4.57)$$

$P_0(t_1)$ defined by (4.22) and $A_{0,1}(t)$, $A_{1,1}(t)$, $G_{0,1}(t,\tau)$ and $G_{1,1}(t,\tau)$ by (4.46), (4.49), (4.50) and (4.53), respectively.

Substitution of (4.50), (4.53), (4.56) and (4.57) into (4.45) gives after some elementary calculations;

$$F_2^{(1)}(t) = (\psi_{1,1}v_{0,1}+\varphi_{1,1}v_{1,1})[1-(1+\frac{\psi_{1,1}\psi_{2,1}v_{0,1}+\varphi_{1,1}\varphi_{2,1}v_{1,1}}{\psi_{1,1}v_{0,1}+\varphi_{1,1}v_{1,1}}\lambda t)e^{-\lambda t}],$$

$$0\le t\le t_3-t_2, \quad (4.58)$$

with $v_{0,1}$ and $v_{1,1}$ as defined by (4.56) and (4.57), respectively, and

$$\psi_{1,1} = g_{0,1}(t_1')\{1+\lambda(t_2-t_1')\} + \lambda h_{0,1}(t_1'); \tag{4.59}$$

$$\psi_{2,1} = g_{0,1}(t_1')/\psi_{1,1}; \tag{4.60}$$

$$\varphi_{1,1} = g_{1,1}(t_1')\{1+\lambda(t_2-t_1')\} + \lambda h_{1,1}(t_1'); \tag{4.61}$$

$$\varphi_{2,1} = g_{1,1}(t_1')/\varphi_{1,1}; \tag{4.62}$$

$g_{0,1}(t)$ and $h_{0,1}(t)$ defined by (4.51) and (4.52), respectively, and $g_{1,1}(t)$ and $h_{1,1}(t)$ by (4.54) and (4.55), respectively.
If we define

$$\begin{aligned} \beta_2 &= \psi_{1,1}v_{0,1} + \varphi_{1,1}v_{1,1}, \\ \alpha_2 &= \psi_{1,1}\psi_{2,1}v_{0,1} + \varphi_{1,1}\varphi_{2,1}v_{1,1}, \end{aligned} \tag{4.63}$$

then it follows from (4.58) that

$$F_2^{(1)}(t) = \beta_2\{1-(1 + \frac{\alpha_2}{\beta_2}\lambda t)e^{-\lambda t}\}, \quad t\geq 0. \tag{4.64}$$

Taking the limit $\zeta\to\infty$ in (4.50) and (4.53) we get:

$$\begin{aligned} A_{0,1}(t) &= \lim_{\zeta\to\infty} G_{0,1}(t,\zeta), \\ A_{1,1}(t) &= \lim_{\zeta\to\infty} G_{1,1}(t,\zeta). \end{aligned} \tag{4.65}$$

Applying (4.65) to (4.45) we obtain the limiting function $F_2^{(1)}$:

$$F_2^{(1)} \stackrel{\text{def}}{=} \lim_{\zeta\to\infty} F_2^{(1)}(t) = 1. \tag{4.66}$$

From (4.64) and (4.66) it is obvious that $\beta_2=1$. Therefore, the first renewal time distribution in the second period of component c when the initial state is the function state has the form:

$$F_2^{(1)}(t) = 1 - (1+\alpha_2\lambda t)e^{-\lambda t}, \quad t\geq 0, \lambda>0, \tag{4.67}$$

α_2 being defined by (4.63).

4.3.4.2.1(b) The availability and the function $G_{0,2}(t,\zeta)$ of the derived renewal process during the second period with initial state the function state

The derived renewal process considered is a renewal process with $F_2^{(1)}(t)$ as the distribution function of the first renewal time, F(t) as the lifetime distribution and W(t) as repairtime distribution, $F_2^{(1)}(t)$, F(t) and W(t) being defined by (4.67) and (4.41), respectively. The Laplace-Stieltjes transforms of these functions are:

$$f_2^{(1)}(\rho) \stackrel{\text{def}}{=} \int_0^\infty e^{-\rho t}\, dF_2^{(1)}(t) = \frac{\lambda\{(1-\alpha_2)\rho+\lambda\}}{(\rho+\lambda)^2}, \quad \mathrm{Re}(\rho)>0; \tag{4.68}$$

$$f(\rho) \stackrel{\text{def}}{=} \int_0^\infty e^{-\rho t}\, dF(t) = \frac{\lambda^2}{(\rho+\lambda)^2}, \quad \mathrm{Re}(\rho)>0; \tag{4.69}$$

$$w(\rho) \stackrel{\text{def}}{=} \int_0^\infty e^{-\rho t}\, dW(t) = \frac{\mu}{\rho+\mu}, \quad \mathrm{Re}(\rho)>0. \tag{4.70}$$

From section 3.3.1. it follows that the Laplace-Stieltjes transform $a_{0,2}(\rho)$ of the availability of this renewal process is expressed by:

$$\begin{aligned} a_{0,2}(\rho) &\stackrel{\text{def}}{=} \int_0^\infty e^{-\rho t}\, dA_{0,2}(t) \\ &= 1 - f_2^{(1)}(\rho) + \frac{\{1-f(\rho)\}f_2^{(1)}(\rho)w(\rho)}{1-f(\rho)w(\rho)} \\ &= 1 - \frac{\{1-w(\rho)\}f_2^{(1)}(\rho)}{1-f(\rho)w(\rho)}, \quad \mathrm{Re}(\rho)>0. \end{aligned} \tag{4.71}$$

Substitution of (4.68), (4.69) and (4.70) into (4.71) gives

$$a_{0,2}(\rho) = 1 - \frac{\lambda\{\lambda+(1-\alpha_2)\rho\}}{(\rho-\rho_1)(\rho-\rho_2)}, \quad \mathrm{Re}(\rho)>0, \tag{4.72}$$

ρ_1 and ρ_2 being defined by (4.47) and α_2 by (4.63). By inversion of (4.72), and taking into account that the start of the renewal process is shifted over a time t_2, we get for the availability $A_{0,2}(t)$:

$$A_{0,2}(t) = 1 - \frac{1}{\mu}\,[\nu_{1,2}+\nu_{2,2}e^{\rho_1(t-t_2)}-\nu_{3,2}e^{\rho_2(t-t_2)}],$$

$$t_2 \le t < t_2', \tag{4.73}$$

$$\nu_{1,2} = \frac{\lambda^2\mu}{\rho_1\rho_2}\ ;$$

$$\nu_{2,2} = \frac{\lambda\mu\{\lambda+(1-\alpha_2)\rho_1\}}{\rho_1(\rho_1-\rho_2)}\ ; \tag{4.74}$$

$$\nu_{3,2} = \frac{\lambda\mu\{\lambda+(1-\alpha_2)\rho_2\}}{\rho_2(\rho_1-\rho_2)}\ .$$

To determine the function $G_{0,2}(t,\zeta)$ as defined by (3.25) note that

$$\frac{d}{dt}\{m_2(t)*W(t)\} = \nu_{1,2}+\nu_{2,2}e^{\rho_1 t}-\nu_{3,2}e^{\rho_2 t},\ t\ge 0, \tag{4.75}$$

ρ_1 and ρ_2 being defined by (4.47) and $\nu_{1,2}$, $\nu_{2,2}$, $\nu_{3,2}$ by (4.74). From the definition of $G_{0,2}(t,\zeta)$, cf. (3.25), and from (4.75) it follows that

$$\begin{aligned} G_{0,2}(t_2',\zeta) = {} & \{1-(1+\alpha_2\lambda\zeta)e^{-\lambda\zeta}\}e^{-\lambda(t_2'-t_2)} \\ & + \{\delta_{1,2}+(-\delta_{1,2}-\delta_{2,2}+\delta_{3,2})e^{-\lambda(t_2'-t_2)}+\delta_{2,2}e^{\rho_1(t_2'-t_2)} \\ & -\delta_{3,2}e^{\rho_2(t_2'-t_2)}\}\{1-(1+\lambda\zeta)e^{-\lambda\zeta}\} \\ & + \{\gamma_{1,2}+(\alpha_2-\delta_{1,2}-\delta_{2,2}+\delta_{3,2})(t_2'-t_2)e^{-\lambda(t_2'-t_2)} \\ & +\gamma_{2,2}e^{\rho_1(t_2'-t_2)}-\gamma_{3,2}e^{\rho_2(t_2'-t_2)}\}\lambda(1-e^{-\lambda(t_2'-t_2)}), \\ & 0\le\zeta\le t_3-t_2', \end{aligned} \tag{4.76}$$

with

$$\delta_{1,2} = \frac{\nu_{1,2}}{\lambda} \quad , \quad \gamma_{1,2} = \frac{\nu_{1,2}}{\lambda^2} \quad ;$$

$$\delta_{2,2} = \frac{\nu_{2,2}}{\rho_1+\lambda} \quad , \quad \gamma_{2,2} = \frac{\nu_{2,2}}{(\rho_1+\lambda)^2} \quad ; \qquad (4.77)$$

$$\delta_{3,2} = \frac{\nu_{3,2}}{\rho_2+\lambda} \quad , \quad \gamma_{3,2} = \frac{\nu_{3,2}}{(\rho_2+\lambda)^2} \quad ,$$

$\nu_{1,2}$, $\nu_{2,2}$ and $\nu_{3,2}$ being defined by (4.74).

4.3.4.2.1(c) The availability of the component during the second period

Because the repairtime distribution is negative exponential and therefore memoryless, it is obvious that the availability $A_{1,2}(t)$ and the function $G_{1,2}(t)$ for the renewal process of the second period of the component are identical to those of the first period, so

$$A_{1,2}(t) = A_{1,1}(t-t_2), \qquad t_2 \leq t < t_2',$$

and (4.78)

$$G_{1,2}(t_2',\zeta) = G_{1,1}(t_2'-t_2,\zeta), \qquad 0 \leq \zeta \leq t_3-t_2'.$$

Using (4.73), (4.76) and (4.78) it is clear that the function $H_{0,2}(t,t_2';t_2)$ and $H_{1,2}(t,t_2';t_2)$ given by (4.27) are completely determined, and therefore the availability $P_2(t)$ given by (4.26) can be calculated during the dormant part of the second period as well as during the operational part.

4.3.4.2.2. The availability of a continuously inspected component during its k^{th} period

4.3.4.2.2(a) The availability $A_{0,k}(t)$ and the function $G_{0,k}(t,\zeta)$ of the derived renewal process during the k^{th} period with initial state the function state

With the first renewal time distribution $F_k^{(1)}(t)$ of the derived renewal process during the k^{th} period and the lifetime and repairtime distributions F(t) and W(t) being defined by (4.41) and applying the same methodology as used in section 4.3.4.2.1(b) it is seen that $A_{0,k}(.)$ and $G_{0,k}(.,.)$ are given by (4.79) and (4.80), respectively:

$$A_{0,k}(t) = 1 + \frac{1}{\mu}\{\nu_{1,k}+\nu_{2,k}e^{\rho_1(t-t_k)}-\nu_{3,k}e^{\rho_2(t-t_k)}\}, \qquad (4.79)$$

$$t_k \le t < t'_k,$$

$$\begin{aligned} G_{0,k}(t'_k,\zeta) = {} & e^{-\lambda(t'_k-t_k)}\{1-(1+\alpha_k\lambda\zeta)e^{-\lambda\zeta}\} \\ & + \{\delta_{1,k}+(-\delta_{1,k}-\delta_{2,k}+\delta_{3,k})e^{-\lambda(t'_k-t_k)}+\delta_{2,k}e^{\rho_1(t'_k-t_k)} \\ & -\delta_{3,k}e^{\rho_2(t'_k-t_k)}\}\{1-(1+\lambda\zeta)e^{-\lambda\zeta}\} \\ & + \{\gamma_{1,k}+(\alpha_k-\delta_{1,k}-\delta_{2,k}+\delta_{3,k})(t'_k-t_k)e^{-\lambda(t'_k-t_k)} \\ & +\gamma_{2,k}e^{\rho_1(t'_k-t_k)}-\gamma_{3,k}e^{\rho_2(t'_k-t_k)}\}\lambda(1-e^{-\lambda\zeta}), \end{aligned} \qquad (4.80)$$

$$0 \le \zeta \le t_{k+1}-t'_k.$$

It remains to determine the quantities α_k, $\delta_{1,k}$, $\delta_{2,k}$, $\delta_{3,k}$, $\gamma_{1,k}$, $\gamma_{2,k}$, $\gamma_{3,k}$, $\nu_{1,k}$, $\nu_{2,k}$ and $\nu_{3,k}$. The expressions for these quantities are obtained by the same methodology as used for the case of k=2, cf. section 4.3.4.2.1(b). We present in the next section the relations for general k.

4.3.4.2.2(b) The distribution of the first renewal time of the derived renewal process in the k^{th} period with initial state the function state

The first renewal time distribution $F_k^{(1)}(t)$ of the derived renewal process for the k^{th} period if the initial state is the function state is derived completely similarly of that for the second period in section 4.3.4.2.1(a):

$$\begin{aligned} F_k^{(1)}(t) = {} & \frac{G_{0,k-1}(t'_{k-1},t+t_k-t'_{k-1})-G_{0,k-1}(t'_{k-1},t_k-t'_{k-1})}{A_{0,k-1}(t'_{k-1})-G_{0,k-1}(t'_{k-1},t_k-t'_{k-1})}P_{k-1}(0) \\ & + \frac{G_{1,k-1}(t'_{k-1},t+t_k-t'_{k-1})-G_{1,k-1}(t'_{k-1},t_k-t'_{k-1})}{A_{1,k-1}(t'_{k-1})-G_{0,k-1}(t'_{k-1},t_k-t'_{k-1})} \\ & .\{1-P_{k-1}(0)\}, \end{aligned} \qquad (4.81)$$

with $A_{0,k-1}(.)$, $A_{1,k-1}(.)$, $G_{0,k-1}(.,.)$ and $G_{1,k-1}(.,.)$ and $P_{k-1}(.)$ being defined by (4.8), (4.9), (4.17), (4.18) and (4.26), respectively.

From (4.46) and (4.73) it is clear that the function $A_{0,2}(t)$ is identical to the function $A_{0,1}(t)$. Also the function $G_{0,2}(t,\zeta)$ is similar to the function $G_{0,1}(t,\zeta)$, i.e. each of these two functions is a sum of products where each product consists of two terms, one term being a function of t and the other term being a function of ζ.

Because of this property and because $F_3^{(1)}(t)$ only depends on the characteristics of the second period, it may be expected that $F_3^{(1)}(t)$ has the same form as $F_2^{(1)}(t)$. By induction it can be shown that

$$F_k^{(1)}(t) = 1 - (1+\alpha_k\lambda t)e^{-\lambda t}, \qquad \lambda>0, t\geq 0, k=1,2,\ldots , \tag{4.82}$$

with

$$\left.\begin{aligned} \alpha_1 &\stackrel{\text{def}}{=} 1, \\ \alpha_k &\stackrel{\text{def}}{=} \psi_{1,k-1}\psi_{2,k-1}v_{0,k-1} + \varphi_{1,k-1}\varphi_{2,k-1}v_{1,k-1}, \quad k=2,3,\ldots ; \end{aligned}\right\} \tag{4.83}$$

$$\left.\begin{aligned} \psi_{1,k-1} &= \chi_{1,k-1}+\chi_{3,k-1}, \\ \psi_{2,k-1} &= (\chi_{1,k-1}\chi_{2,k-1}+\chi_{3,k-1}\chi_{4,k-1})/\psi_{1,k-1}; \end{aligned}\right\} \tag{4.84}$$

$$\left.\begin{aligned} \chi_{1,k-1} &= \{1+\alpha_{k-1}\lambda(t_k-t'_{k-1})\}e^{-\lambda(t_k-t_{k-1})}, \\ \chi_{2,k-1} &= \alpha_{k-1}/\{1+\alpha_{k-1}\lambda(t_k-t'_{k-1})\}, \\ \chi_{3,k-1} &= [\{1+\lambda(t_k-t'_{k-1})\}g_{0,k-1}+\lambda h_{0,k-1}]e^{-\lambda(t_k-t'_{k-1})}, \\ \chi_{4,k-1} &= g_{0,k-1}/[\{1+\lambda(t_k-t'_{k-1})\}g_{0,k-1}+\lambda h_{0,k-1}]; \end{aligned}\right\} \tag{4.85}$$

$$\left.\begin{aligned} \varphi_{1,k-1} &= [\{1+\lambda(t_k-t_{k-1})\}g_{1,k-1}+\lambda h_{1,k-1}]e^{-\lambda(t_k-t'_{k-1})}, \\ \varphi_{2,k-1} &= g_{1,k-1}/[\{1+\lambda(t_k-t'_{k-1})\}g_{1,k-1}+\lambda h_{1,k-1}]; \end{aligned}\right\} \tag{4.86}$$

$$
\begin{aligned}
v_{0,k-1} &= \frac{P_{k-2}(t_{k-1})}{A_{0,k-1}(t'_{k-1}-t_{k-1})-G_{0,k-1}(t'_{k-1}-t_{k-1},t_k-t'_{k-1})}\,, \\
v_{1,k-1} &= \frac{1-P_{k-2}(t_{k-1})}{A_{1,k-1}(t'_{k-1}-t_{k-1})-G_{1,k-1}(t'_{k-1}-t_{k-1},t_k-t'_{k-1})}\,,
\end{aligned}
\tag{4.87}
$$

with $A_{\cdot,k-1}(.)$ being defined by (4.79) and (4.49) and $G_{\cdot,k-1}(.,.)$ being defined by (4.80) and (4.53). In (4.83),...,(4.87) the argument t'_{k-1} for the different functions is dropped in order to make the formulas more transparent.

The functions $g_{0,k-1}$ and $h_{0,k-1}$ in (4.85) and (4.86) are given by:

$$
\begin{aligned}
g_{0,k-1} = {} & \delta_{1,k-1}+(-\delta_{1,k-1}-\delta_{2,k-1}+\delta_{3,k-1})e^{-\lambda(t'_{k-1}-t_{k-1})}+ \\
& \delta_{2,k-1}e^{\rho_1(t'_{k-1}-t_{k-1})}-\delta_{3,k-1}e^{\rho_2(t'_{k-1}-t_{k-1})}\,,
\end{aligned}
\tag{4.88}
$$

$$
\begin{aligned}
h_{0,k-1} = {} & \gamma_{1,k-1}+(\alpha_{k-1}-\delta_{1,k-1}-\delta_{2,k-1}+\delta_{3,k-1})e^{-\lambda(t'_{k-1}-t_{k-1})}+ \\
& \gamma_{2,k-1}e^{\rho_1(t'_{k-1}-t_{k-1})}-\gamma_{3,k-1}e^{\rho_2(t'_{k-1}-t_{k-1})}\,,
\end{aligned}
\tag{4.89}
$$

with

$$
\begin{aligned}
\delta_{1,k-1} &= \frac{\nu_{1,k-1}}{\lambda}\,, \quad \delta_{2,k-1} = \frac{\nu_{2,k-1}}{\rho_1+\lambda}\,, \quad \delta_{3,k-1} = \frac{\nu_{3,k-1}}{\rho_2+\lambda} \\
\gamma_{1,k-1} &= \frac{\nu_{1,k-1}}{\lambda^2}\,, \quad \gamma_{2,k-1} = \frac{\nu_{2,k-1}}{(\rho_1+\lambda)^2}\,, \quad \gamma_{3,k-1} = \frac{\nu_{3,k-1}}{(\rho_2+\lambda)^2}\,;
\end{aligned}
\tag{4.90}
$$

$\nu_{1,k}$, $\nu_{2,k}$ and $\nu_{3,k}$ in (4.90) being defined as:

$$
\begin{aligned}
\nu_{1,k-1} &= \frac{\lambda^2\mu}{\rho_1\rho_2}\,, \\
\nu_{2,k-1} &= \frac{\lambda\mu\{\lambda+(1-\alpha_{k-1})\rho_1\}}{\rho_1(\rho_1-\rho_2)}\,, \\
\nu_{3,k-1} &= \frac{\lambda\mu\{\lambda+(1-\alpha_{k-1})\rho_2\}}{\rho_2(\rho_1-\rho_2)}\,,
\end{aligned}
\tag{4.91}
$$

ρ_1 and ρ_2 being defined by (4.47) and α_{k-1} being defined by (4.83).
The functions $g_{1,k-1}$ and $h_{1,k-1}$ are given by (4.54) and (4.55) with t_1' and t_1 replaced by t_{k-1}' and t_{k-1}, respectively.
From (4.83) it is seen that α_k is only dependent of characteristics of the foregoing $(k-1)^{th}$ period and therefore $F_k^{(1)}(t)$ in (4.82) is completely determined if the characteristics of the foregoing period are calculated.

4.3.4.2.2(c) The availability of the component during the k^{th} period

As it has already been mentioned in section 4.3.4.2.1(c), we recall that the derived renewal processes starting with initial state the fail state and with a negative exponentially distributed repairtime are identical to the original renewal process that starts at t_1 with initial state the fail state.
So

$$A_{1,k}(t) = A_{1,1}(t-t_k) \quad , \quad t\in[t_k,t_k'),k=1,2,\ldots ; \tag{4.92}$$

$$G_{1,k}(t_k',\zeta) = G_{1,1}(t_k'-t_k,\zeta), \quad 0\le\zeta\le t_{k+1}-t_k',k=1,2,\ldots . \tag{4.93}$$

With (4.79), (4.80), (4.92) and (4.93) all functions characterizing the availability of the component during the renewal process of the k^{th} period are completely determined. Therefore the functions $H_{0,k}(t,t_k';t_k)$ and $H_{1,k}(t,t_k';t_k)$ being defined by (4.27) can be calculated. So the availability $P_k(t)$ as given by (4.24) and (4.26) is completely determined.
They will be calculated by a recursive scheme, i.e. by the following procedure:

(i) calculate the numerical values for the functions

α_j, j=1,2,...,k;

$H_{.,j}(t_{j+1},t_j';t_j)$, j=1,2,...,k-1,

α_j being defined by (4.81) and $H_{.,j}(.,.;.)$ by (4.27);

(ii) calculate recursively the functions

$P_j(t_{j+1})$, j=1,2,...,k-1,

$P_j(.)$ being defined by (4.31), using the functions calculated in step (i);

(iii) with the results of the foregoing steps (i) and (ii) calculate

$$P_k(t),\ t_k \leq t < t_{k+1},$$

as defined by (4.24), (availability during the *dormant* part of the k^{th} period) and (4.26), (availability during the *operational* part of the k^{th} period).

In fig. 4.5. an example is shown of a phased mission for a class 2 component with Erlang-2 lifetime distribution and negative exponential repair-time distribution, and with the same input numbers and the same mission as shown in the example of section 4.3.4.1.2.

Three curves are shown:

(i) curve 1: the component is non-repairable (class 1 component);

(ii) curve 2: the component is continuously inspected (class 2 component), and fulfills a mission;

(iii) curve 3: the component is repairable (class 2 component) and does not fulfill a mission. (So the unavailability is continuously governed by the original renewal process and therefore not disturbed).

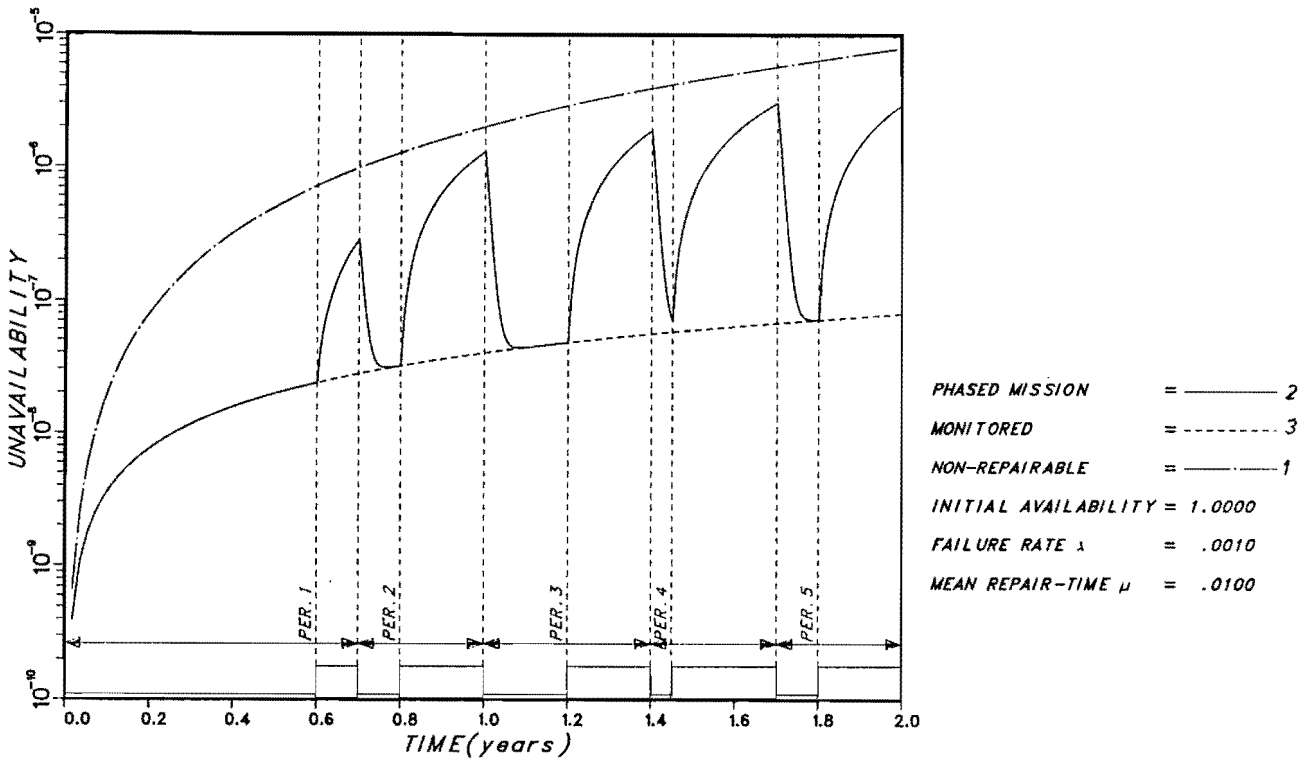


FIG.4.5 UNAVAILABILITY FOR A CONTINUOUSLY INSPECTED COMPONENT DURING A PHASED MISSION
ERLANG-2 LIFETIME DISTRIBUTION
N.E.D. REPAIRTIME DISTRIBUTION

Comparison of fig. 4.4. and fig. 4.5. shows that in case of an Erlang-2 lifetime distribution the unavailability is considerably decreased.

4.4. The availability of a randomly inspected component during the mission

A randomly inspected component is subjected to *random* testing during the *OR-phase*, however, random testing is stopped at the moment that the mission starts, i.e. at $t=T_0$. So if the component is in the fail state during the mission, *this fail state is not detected* and therefore no repair can be applied to the component during the phased mission.
However, there is one exception to this rule: If the component is being repaired at the start of the mission at $t=T_0$, and the first operational phase of the component starts at $t_1'>T_0$, then repair may be continued. Therefore, there exists the possibility that repair has been finished before the instant t_1', i.e. the component is in the *function* state at the start of its first operational phase whereas it was in the *fail* state at the start of the mission.
So, three distinct intervals can be considered for the behaviour of a randomly inspected component performing a mission:

- the OR-phase,
- the interval $[T_0,t_1')$, i.e. the interval between the start of the mission and the start of the first operational part of the component,
- the interval $[t_1',T_K]$, i.e. the interval between the start of the first operational part for the component and the end of the mission.

In the next sections the availability of a randomly inspected component during each of the mentioned intervals will be treated. As an application, explicit formulas will be derived in the case of negative exponentially distributed lifetime and repairtime.

4.4.1. The availability of a randomly inspected component during the OR-phase

During the OR-phase the component is subjected to the original renewal process that starts at $t=t_1$, and therefore the availability $P_1(t)$ is defined by:

$$P_1(t) = A_{0,1}(t)P_0(t_1) + A_{1,1}(t)\{1-P_0(t_1)\}, \quad 0\le t<T_0. \tag{4.94}$$

with $A_{0,1}(t)$ and $A_{1,1}(t)$ defined by (4.8) and (4.9) and $P_0(t_1) \stackrel{def}{=} A(0)$, $t_1 \stackrel{def}{=} 0$. The availabilities $A_{0,1}(t)$ and $A_{1,1}(t)$ are determined by (3.13) and (3.14).

4.4.2. The availability of a randomly inspected component during the interval $[T_0,t_1']$

The availability $P_1(t)$ of the component during the interval $[T_0,t_1']$, T_0 being the start of the mission and t_1' being the start of the first operational part, is determined by:

$$
\begin{aligned}
P_1(t) &= \Pr\{\underline{x}(t)=0\} \\
&= \Pr\{\underline{x}(t)=0|\underline{x}(t_1)=0\}\Pr\{\underline{x}(t_1)=0\}+\Pr\{\underline{x}(t)=0|\underline{x}(t_1)=1\}\Pr\{\underline{x}(t_1)=1\} \\
&= [\Pr\{\underline{x}(t)=0,\underline{x}(T_0)=0|\underline{x}(t_1)=0\}+\Pr\{\underline{x}(t)=0,\underline{x}(T_0)=1|\underline{x}(t_1)=0\}] \\
&\quad . \Pr\{\underline{x}(t_1)=0\} \\
&\quad +[\Pr\{\underline{x}(t)=0,\underline{x}(T_0)=0|\underline{x}(t_1)=1\}+\Pr\{\underline{x}(t)=0,\underline{x}(T_0)=1|\underline{x}(t_1)=1\}] \\
&\quad . \Pr\{\underline{x}(t_1)=1\} \\
&= [H_{0,1}(t,T_0;t_1)+\Pr\{\underline{x}(t)=0,\underline{x}(T_0)=1|\underline{x}(t_1)=0\}]P_0(t_1) \\
&\quad +[H_{1,1}(t,T_0;t_1)+\Pr\{\underline{x}(t)=0,\underline{x}(T_0)=1|\underline{x}(t_1)=1\}]\{1-P_0(t_1)\}, \\
&\qquad\qquad t\in[T_0,t_1'), \qquad (4.95)
\end{aligned}
$$

$H_{.,1}(.,.;.)$ defined by (4.19) and (4.20), and $P_0(t_1)$ being the initial condition, i.e. $P_0(t_1) = A(0)$.

In order to calculate $P_1(t)$ in (4.95) we have to develop the expressions for the probabilities of the events "$\underline{x}(t)=0,\underline{x}(T_0)=1|\underline{x}(t_1)=$.", i.e. the events "the component is in the fail state at instant T_0 and in the function state at instant $t>T_0|\underline{x}(t_1)=$.".

If the component is in the fail state at instant T_0, two distinct situations are possible:

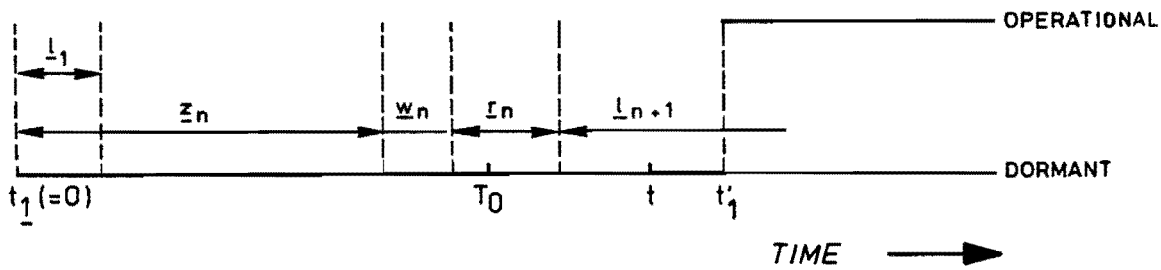
- the component is in the fail state at instant T_0 and the fail state has not yet been detected; so no test has been performed till T_0 after the state transition of the component form the function state to the fail state;
- the component is in the fail state at instant T_0 and is being repaired.

In the first situation the fail state of the component is not detected at instant T_0. Since no test is performed after the instant T_0, the fail state of the component will not be detected at all. Therefore, it is obvious that the probability of the event "$\underline{x}(t)=0,\underline{x}(T_0)=1\,|\,\underline{x}(t_1)=$. and the fail state of the component not yet detected at T_0" equals zero.

In the other situation, i.e. the event "the component is in the fail state at instant T_0 and is being repaired", there exists a non-zero probability of the occurrence of this event. Therefore define

$$\begin{aligned} X_0(t,T_0) &= \Pr\{\underline{x}(t)=0,\underline{x}(T_0)=1, \text{ component c being under repair} \\ &\qquad \text{at instant } T_0\,|\,\underline{x}(t_1)=0\}, \quad t\in[T_0,t_1'); \\ X_1(t,T_0) &= \Pr\{\underline{x}(t)=0,\underline{x}(T_0)=1, \text{ component c being under repair} \\ &\qquad \text{at instant } T_0\,|\,\underline{x}(t_1)=1\}, \quad t\in[T_0,t_1'). \end{aligned} \tag{4.96}$$

In the next figure a realisation is shown for the event "$\underline{x}(t)=0,\underline{x}(T_0)=1$, component c is under repair at instant $T_0\,|\,\underline{x}(t_1)=0$".



(For an explanation of the variables $\underline{\ell}$, $\underline{z}$, $\underline{w}$ and $\underline{r}$ see section 3.3.2.) .

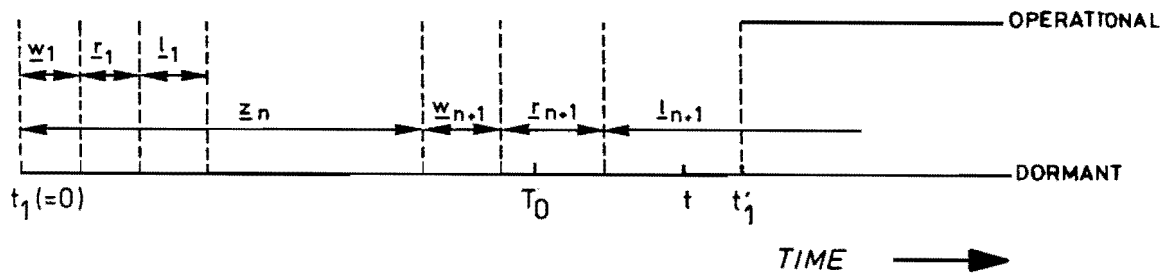
It follows that

$$X_0(t,T_0) = \sum_{n=1}^{\infty} \Pr\{\underline{z}_n+\underline{w}_n<T_0, T_0\le \underline{z}_n+\underline{w}_n+\underline{r}_n<t, \underline{z}_{n+1}\ge t\,|\,\underline{x}(t_1)=0\}$$

$$= \sum_{n=1}^{\infty} \int_{u=0}^{T_0} \int_{v=T_0-u}^{t-u} \Pr\{\underline{\ell}_{n+1}\ge t-u-v\}\,d_u \Pr\{\underline{z}_n+\underline{w}_n<u\}\,d_v \Pr\{\underline{r}_n<v\}$$

$$= \int_{u=0}^{T_0} \int_{v=T_0-u}^{t-u} \{1-F(t-u-v)\} d_u m_0(u) * H(u) d_v W(v), \quad t \in [T_0, t_1'), \quad (4.97)$$

with F(.), W(.), H(.) the lifetime, the repairtime and the interinspection time distribution of the component, respectively, and $m_0(.)$ its renewal function with initial state the function state (see section 3.3.2.).
In the next figure a realisation is sketched in the case that the initial state of the renewal process is the *fail* state.



Obviously

$$X_1(t,T_0) = \sum_{n=0}^{\infty} \Pr\{\underline{z}_n + \underline{w}_{n+1} < T_0, T_0 \leq \underline{z}_n + \underline{w}_{n+1} + \underline{r}_{n+1} < t, \underline{z}_{n+1} \geq t \mid \underline{x}(t_1)=1\}$$

$$= \int_{u=0}^{T_0} \int_{v=T_0-u}^{t-u} \{1-F(t-u-v)\} d_u H(u) d_v W(v) \quad (4.98)$$

$$+ \int_{u=0}^{T_0} \int_{v=T_0-u}^{t-u} \{1-F(t-u-v)\} d_u m_1(u) * H(u) d_v W(v), \quad t \in [T_0, t_1'),$$

with F(.), W(.) and H(.) as being defined in (4.97) and $m_1(t)$ the renewal function with initial state the fail state.
To summarize the obtained results of this section, it follows that the availability $P_1(t)$ in (4.95) of the component during the interval $[T_0, t_1')$ can be expressed by

$$P_1(t) = \{H_{0,1}(t,T_0;t_1) + X_0(t,T_0)\}\, P_0(t_1) + \{H_{1,1}(t,T_0;t_1) + X_1(t,T_0)\}\{1-P_0(t_1)\}, \quad T_0 \le t < t_1', \tag{4.99}$$

$H_{.,1}(.,.;.)$ being defined by (4.19) and (4.20), $X_0(.)$ and $X_1(.)$ being defined by (4.97) and (4.98) and $P_0(t_1)$ being the initial availability.

4.4.3. The availability of a randomly inspected component during the interval $[t_1', T_K]$

The expression for the availability $P_1(t)$ during the interval $[t_1', T_K]$ differs from the expression for the availability during the interval $[T_0, t_1')$ because of the repair policy.

For the availability calculation at instant t during the interval $[T_0, t_1')$, repair was permitted during the whole interval $[T_0, t_1']$. However, during the interval $[t_1', T_K]$ *no repair is permitted*. So, from (4.97) and (4.98), it follows that for $t > t_1'$ the functions $X_0(t,T_0)$ and $X_1(t,T_0)$ are given by:

$$X_0(t,T_0) = \int_{u=0}^{T_0} \int_{v=T_0-u}^{t_1'-u} \{1-F(t-u-v)\}\, d_u m_0(u) * H(u)\, d_v W(v), \qquad t \in [t_1', T_K], \tag{4.100}$$

$$X_1(t,T_0) = \int_{u=0}^{T_0} \int_{v=T_0-u}^{t_1'-u} \{1-F(t-u-v)\}\, d_u H(u)\, d_v W(v) + \int_{u=0}^{T_0} \int_{v=T_0-u}^{t_1'-u} \{1-F(t-u-v)\}\, d_u m_1(u) * H(u)\, d_v W(v), \qquad t \in [t_1', T_K], \tag{4.101}$$

the functions $F(.)$, $W(.)$, $H(.)$, $m_0(.)$ and $m_1(.)$ being defined by (4.97) and (4.98). Note that functioning at $t > t_1'$ implies that the repair is completed before t_1'.

The availability $P_1(t)$ of the component during $[t_1', T_K]$ is given by (4.99), but in this case the functions $X_0(t,T_0)$ and $X_1(t,T_0)$ are defined by (4.100) and (4.101), respectively.

4.4.4. An application: the availability of a randomly inspected component with negative exponentially distributed lifetime and repairtime

In this application we shall derive explicit expressions for the availability of a randomly inspected component for each of the three intervals which may occur during a phased mission of such a component.
The lifetime distribution F(t) and the repairtime distribution W(t) are negative exponentially distributed and defined by (4.32):

$$F(t) = 1-e^{-\lambda t}, \quad \lambda>0, t\geq 0,$$
$$W(t) = 1-e^{-\mu t}, \quad \mu>0, t\geq 0. \tag{4.32}$$

The interinspection time distribution H(t) is also negative exponential (see section 3.3.2.).

$$H(t) = 1-e^{-\gamma t}, \quad \gamma>0, t\geq 0. \tag{4.102}$$

From appendix B, chapter B4 it follows that three distinct cases for the calculation of the component's availability $P_1(t)$ have to be distinguished, they depend on the values of the parameters λ, μ and γ, viz:

$$\begin{array}{lll} (\text{i}) & 0<\gamma<\lambda+\mu-2\sqrt{\lambda\mu} \quad \text{and} & \gamma>\lambda+\mu+2\sqrt{\lambda\mu}, \\ (\text{ii}) & \gamma=\lambda+\mu-2\sqrt{\lambda\mu} \quad \text{and} & \gamma=\lambda+\mu+2\sqrt{\lambda\mu}, \\ (\text{iii}) & \lambda+\mu-2\sqrt{\lambda\mu}<\gamma<\lambda+\mu+2\sqrt{\lambda\mu}. & \end{array} \tag{4.103}$$

The most usual situation in practice is the one where the inspection rate γ is far larger than the sum of the failure rate λ and the repair rate μ, because then a *random* inspection procedure may be acceptable. In case of a low test frequency a *random* test procedure is of little use. Therefore, the most practical situation for *random* testing is given in case (i) by $\gamma>\lambda+\mu+2\sqrt{\lambda\mu}$.
Because all three cases can be treated similarly by using the relevant formulas from appendix B, see chapter B4, only case (i) shall be discussed in this section.

4.4.4.1. The availability during the OR-phase

The availability $P_1(t)$ is given by (4.94):

$$P_1(t) = A_{0,1}(t)P_0(t_1) + A_{1,1}(t)\{1-P_0(t_1)\},\quad t\geq 0,$$

$P_0(t_1)$ being the initial availability.
For this interval it follows from appendix B, formulas (B67) and (B68) for $t_1 \stackrel{def}{=} 0$, that:

$$A_{0,1}(t) = \frac{\mu\gamma}{\lambda\mu+\lambda\gamma+\mu\gamma} + \frac{(\rho_1+\mu)(\rho_1+\gamma)}{\rho_1(\rho_1-\rho_2)}e^{\rho_1 t} - \frac{(\rho_2+\mu)(\rho_2+\gamma)}{\rho_2(\rho_1-\rho_2)}e^{\rho_2 t},$$

$$t\in[0,T_0), \qquad (4.104)$$

with

$$\rho_{1,2} = -\frac{1}{2}(\lambda+\mu+\gamma) \pm \frac{1}{2}\sqrt{(\lambda+\mu+\gamma)^2 - 4(\lambda\mu+\lambda\gamma+\mu\gamma)}; \qquad (4.105)$$

and

$$A_{1,1}(t) = \frac{\mu\gamma}{\lambda\mu+\lambda\gamma+\mu\gamma} + \frac{\mu\gamma}{\rho_1(\rho_1-\rho_2)}e^{\rho_1 t} - \frac{\mu\gamma}{\rho_2(\rho_1-\rho_2)}e^{\rho_2 t},$$

$$t\in[0,T_0), \qquad (4.106)$$

with ρ_1 and ρ_2 being defined by (4.105).
With (4.104) and (4.106) and the initial availability $P_0(t_1)$ the availability $P_1(t)$ during the interval $[0,T_0]$ is completely determined. Note that (4.103)(i) implies that $(\lambda+\mu+\gamma)^2-4(\lambda\mu+\lambda\gamma+\mu\gamma)>0$.

4.4.4.2. The availability during the interval $[T_0,t_1')$

During the interval $[T_0,t_1')$ the availability $P_1(t)$ is described by (4.99):

$$\begin{aligned} P_1(t) = {} & \{H_{0,1}(t,T_0;t_1) + X_0(t,T_0)\}P_0(t_1) \\ & + \{H_{1,1}(t,T_0;t_1) + X_1(t,T_0)\}\{1-P_0(t_1)\}, \quad t\in[T_0,t_1'), \end{aligned} \qquad (4.99)$$

$H_{\cdot,1}(\cdot,\cdot;\cdot)$ being defined by (4.19) and (4.20), $X_0(\cdot,\cdot)$ and $X_1(\cdot,\cdot)$ being defined by (4.97) and (4.98), respectively.

From appendix B, expressions (B71) and (B75), it follows that

$$G_{0,1}(T_0,t-T_0) = \left[\frac{\mu\gamma}{\rho_1\rho_2} + \frac{\lambda\mu\gamma}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 T_0}}{\rho_1(\rho_1+\lambda)} - \frac{e^{\rho_2 T_0}}{\rho_2(\rho_2+\lambda)}\right\}\right]\{1-e^{-\lambda(t-T_0)}\}, \quad (4.107)$$

$$G_{1,1}(T_0,t-T_0) = \left[\frac{\mu\gamma}{\rho_1\rho_2} + \frac{\lambda(\mu\gamma)^2}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 T_0}}{\rho_1(\rho_1+\lambda)(\rho_1+\mu)(\rho_1+\gamma)}\right.\right.$$

$$\left.\left. - \frac{e^{\rho_2 T_0}}{\rho_2(\rho_2+\lambda)(\rho_2+\mu)(\rho_2+\gamma)}\right\}\right]\{1-e^{-\lambda(t-T_0)}\}, \quad (4.108)$$

ρ_1 and ρ_2 being defined by (4.105).
From its definition

$$H_{.,1}(t,T_0;0) = A_{.,1}(T_0) - G_{.,1}(T_0,t-T_0), \qquad t\in[T_0,t_1').$$

From (4.104) and (4.107) it is seen that $H_{0,1}(t,T_0;0)$ is completely determined. The same holds for $H_{1,1}(t,T_0;0)$ by applying (4.106) and (4.108).

The Laplace-Stieltjes transforms $z(\rho)$ and $h_0(\rho)$ of the functions $H(t)$ and $m_0(t)$, respectively, are defined by the expressions (B54) and (B61) from appendix B:

$$z(\rho) = \frac{\gamma}{\rho+\gamma}, \qquad \mathrm{Re}(\rho)>-\gamma, \quad (4.109)$$

$$h_0(\ ) = \frac{\lambda(\rho+\mu)(\rho+\gamma)}{\rho(\rho-\rho_1)(\rho-\rho_2)}, \qquad \mathrm{Re}(\rho)>0, \quad (4.110)$$

ρ_1 and ρ_2 being defined by (4.105). Denoting by LS{.} the Laplace-Stieltjes operator, it follows from (4.109) and (4.110) that

$$LS\{\frac{d}{dt}(m_0(t)*H(t))\} = \frac{\lambda\gamma(\rho+\mu)}{(\rho-\rho_1)(\rho-\rho_2)}, \qquad \mathrm{Re}(\rho)>0.$$

Applying the inverse Laplace transform yields:

$$\frac{d}{dt}\{m_0(t)*H(t)\} = \frac{\lambda\mu\gamma}{\rho_1\rho_2} + \frac{\lambda\gamma}{\rho_1-\rho_2}\left\{\frac{\rho_1+\mu}{\rho_1}e^{\rho_1 t} - \frac{\rho_2+\mu}{\rho_2}e^{\rho_2 t}\right\}, \qquad t\geq 0. \quad (4.111)$$

Substitution of (4.32) and (4.111) into (4.97) gives after integration for the function $X_0(t,T_0)$:

$$X_0(t,T_0) = \frac{\lambda\mu\gamma}{\lambda-\mu}\left\{e^{-\mu(t-T_0)} - e^{-\lambda(t-T_0)}\right\} \cdot \left[\frac{1}{\rho_1\rho_2} + \frac{1}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 T_0}}{\rho_1} - \frac{e^{\rho_2 T_0}}{\rho_2}\right\}\right], \quad t\in[T_0,t_1'), \tag{4.112}$$

ρ_1 and ρ_2 being defined by (4.105).
Using the same technique we obtain for the function $X_1(t,T_0)$ as given by (4.98):

$$X_1(t,T_0) = \frac{\lambda\mu\gamma}{\lambda-\mu}\left\{e^{-\mu(t-T_0)} - e^{-\lambda(t-T_0)}\right\} \cdot \left[\frac{1}{\rho_1\rho_2} + \frac{\lambda\mu\gamma^2}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 T_0}}{\rho_1(\rho_1+\mu)(\rho_1+\gamma)} - \frac{e^{\rho_2 T_0}}{\rho_2(\rho_2+\mu)(\rho_2+\gamma)}\right\}\right], \quad t\in[T_0,t_1'), \tag{4.113}$$

ρ_1 and ρ_2 being defined by (4.105).

Since the functions $H_{\cdot,1}(t,T_0;0)$ and $X_{\cdot}(t,T_0)$ can be calculated by (4.104), (4.106), (4.107) and (4.108) and by (4.112) and (4.113) respectively, the availability $P_1(t)$ of the component as defined by (4.99) is completely determined for the interval $[T_0,t_1')$.

4.4.4.3. The availability during the interval $[t_1',T_K]$

In this section we shall present the explicit expressions for the functions $X_0(t,T_0)$ and $X_1(t,T_0)$ in the interval $[t_1',T_K]$, without derivation, since the results are obtained by the same technique as applied in the foregoing section.
During this interval the availability $P_1(t)$ is given by (4.99) and the functions $H_{\cdot,1}(t,T_0;0)$ are determined by (4.104), (4.106),...,(4.108).
The expressions for the functions $X_{\cdot}(t,T_0)$ during the interval $[t_1',T_K]$ read:

$$X_0(t,T_0) = \frac{\lambda\mu\gamma}{\lambda-\mu}\left\{e^{-\lambda(t-t_1')-\mu(t_1'-T_0)} - e^{-\lambda(t-T_0)}\right\}$$

$$\cdot\left[\frac{1}{\rho_1\rho_2} + \frac{1}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 T_0}}{\rho_1} - \frac{e^{\rho_2 T_0}}{\rho_2}\right\}\right], \qquad (4.114)$$

$$t\in[t_1',T_K],$$

$$X_1(t,T_0) = \frac{\lambda\mu\gamma}{\lambda-\mu}\left\{e^{-\lambda(t-t_1')-\mu(t_1'-T_0)} - e^{-\lambda(t-T_0)}\right\} \qquad (4.115)$$

$$\cdot\left[\frac{1}{\rho_1\rho_2} + \frac{\lambda\mu\gamma^2}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 T_0}}{\rho_1(\rho_1+\mu)(\rho_1+\gamma)} - \frac{e^{\rho_2 T_0}}{\rho_2(\rho_2+\mu)(\rho_2+\gamma)}\right\}\right],$$

$$t\in[t_1',T_K],$$

ρ_1 and ρ_2 being defined by (4.105).

In fig. 4.6. an example is shown for the unavailability of a randomly inspected component with negative exponentially distributed lifetime and repairtime during the mission.

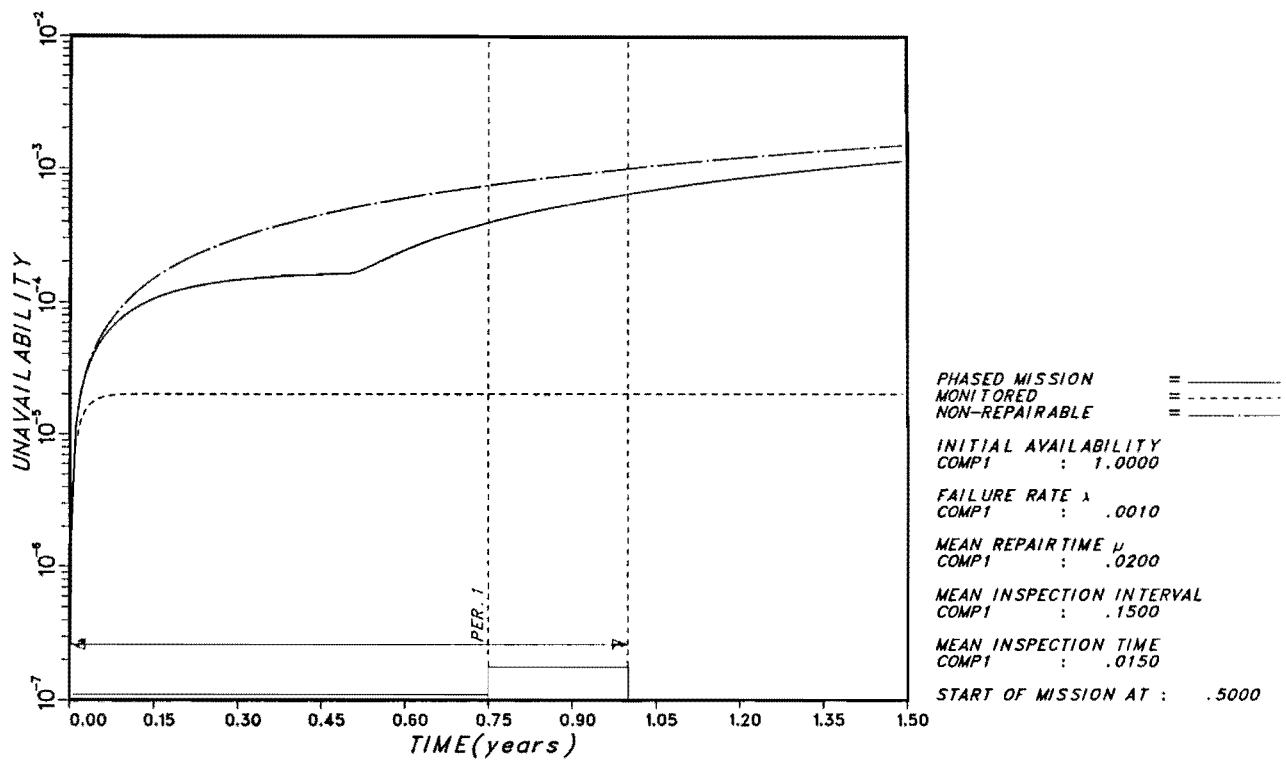


FIG.4.6 UNAVAILABILITY FOR A RANDOM INSPECTED COMPONENT DURING A PHASED MISSION
N.E.D. LIFETIME DISTRIBUTION
N.E.D. REPAIRTIME DISTRIBUTION

Three curves are shown in fig. 4.6.:

(i) curve 1: the component is non-repairable (class 1 component);
(ii) curve 2: the component is randomly inspected (class 3 component) and fulfills a mission;
(iii) curve 3: the component is continuously inspected (class 2 component) and does not fulfill a mission.

4.5. The availability of a periodically inspected component during the mission

The availability of a periodically inspected component during the OR-phase is described in section 3.4.3. Furthermore, it is assumed that after the start of the mission at instant T_0 neither inspections nor repair are applied to the component. However, if *at the start of the mission* the component is being inspected or being repaired, it is assumed that this inspection or repair may be continued. Whether this inspection or repair can be finished before the start of the first operational part of the component at instant t_1' depends on the length of the time interval $[T_0,t_1')$.
Because of this exception (the same as made for randomly inspected components, see section 4.4.), the availability of a periodically inspected component at an instant t during the mission depends on whether the start of the mission at instant T_0 and the start of the first operational part at instant t_1' belong to the same inspection interval or not.
Suppose that the start of the mission at instant T_0 belongs to the n^{th} inspection interval, n=1,2,..., i.e. $T_0 \in [\tau_n,\tau_{n+1}]$, τ_n being the start of the n^{th} inspection. Then two distinct situations are possible:

$$\begin{aligned} &(i) \quad t_1' \in [\tau_n,\tau_{n+1}], \\ &(ii) \quad t_1' > \tau_{n+1}, \end{aligned} \tag{4.116}$$

this separation motivated by the assumption that after the start of the mission at instant T_0 no new inspection is initiated. For calculating the availability at instant t for case (i) of (4.116) we should distinguish the interval $[0,t_1')$ during which inspection and repair are performed and the interval $[t_1',T_K]$ during which neither inspection nor repair are allowed. The availability during the interval $[0,t_1')$ is treated in section 3.4.3.,

whereas the availability $P_1(t)$, $t\in[t_1',T_K]$ is defined by:

$$\begin{aligned} P_1(t) &= \Pr\{\underline{x}(t)=0\} \\ &= \Pr\{\underline{x}(t)=0,\underline{x}(t_1')=0\} \\ &= \Pr\{\underline{x}(t_1')=0,\underline{\zeta}(t_1')>t-t_1'\}, \qquad t\in[t_1',T_K], \end{aligned} \tag{4.117}$$

$\underline{\zeta}(t_1')$ being the residual lifetime of the component at instant t_1'. Treating the availability at instant t for the second situation (ii) of (4.116), it is clear that there are also two different intervals that have to be considered, viz. the interval $[0,\tau_{n+1})$ during which inspection and repair is performed and the interval $[\tau_{n+1},T_K]$ during which neither inspection nor repair is allowed. The availability during the interval $[0,\tau_{n+1})$ is treated in section 3.4.3. The availability $P_1(t)$ for case (ii) during the interval $[\tau_{n+1},T_K]$ is obtained by:

$$\begin{aligned} P_1(t) &= \Pr\{\underline{x}(t)=0\} \\ &= \Pr\{\underline{x}(t)=0,\underline{x}(\tau_{n+1})=0\} \\ &= \Pr\{\underline{x}(\tau_{n+1}=0,\underline{\zeta}(\tau_{n+1})>t-\tau_{n+1}\}, \qquad t\in[\tau_{n+1},T_K], \end{aligned} \tag{4.118}$$

$\underline{\zeta}(\tau_{n+1})$ being the residual lifetime of the component at instant τ_{n+1}. From (4.117) and (4.118) it is seen that the availabilities $P_1(t)$ during the interval $[t_1',T_K]$ in case (i) and during the interval $[\tau_{n+1},T_K]$ in case (ii) only differ with respect to the instants at which these intervals start. So these availabilities can be treated in a similar way.

Therefore we introduce the instant t' such that

$$\begin{aligned} t' &= t_1' \quad , \text{ if } T_0,t_1'\in[\tau_n,\tau_{n+1}], \\ &= \tau_{n+1}, \text{ if } T_0\in[\tau_n,\tau_{n+1}] \text{ and } t_1'>\tau_{n+1}, n=1,2,\ldots . \end{aligned} \tag{4.119}$$

The availabilities $P_1(t)$ as defined by (4.117) and (4.118) are now obtained by the following derivation:

$$P_1(t) = Pr\{\underline{x}(t')=0, \underline{\zeta}(t')>t-t'\},$$

$\underline{\zeta}(t')$ being the residual lifetime of the component at instant t'. It follows that

$$\begin{aligned} P_1(t) &= Pr\{\underline{x}(t')=0, \underline{\zeta}(t')>t-t' \,|\, \underline{x}(0)=0\} Pr\{\underline{x}(0)=0\} \\ &\quad + Pr\{\underline{x}(t')=0, \underline{\zeta}(t')>t-t' \,|\, \underline{x}(0)=1\}[1-Pr\{\underline{x}(0)=0\}] \\ &= [Pr\{\underline{x}(t')=0 \,|\, \underline{x}(0)=0\} - Pr\{\underline{x}(t')=0, \underline{\zeta}(t')<t-t' \,|\, \underline{x}(0)=0\}] Pr\{\underline{x}(0)=0\} \\ &\quad + [Pr\{\underline{x}(t')=0 \,|\, \underline{x}(0)=1\} - Pr\{\underline{x}(t')=0, \underline{\zeta}(t')<t-t' \,|\, \underline{x}(0)=1\}] \\ &\quad \cdot [1-Pr\{\underline{x}(0)=1\}] \\ &= \{A_{0,1}(t') - G_{0,1}(t', t-t')\} A(0) \\ &\quad + \{A_{1,1}(t') - G_{1,1}(t', t-t')\}\{1-A(0)\}, \qquad t\in[t', T_K], \end{aligned} \tag{4.120}$$

with $A_{0,1}(.)$ and $A_{1.1}(.)$ being defined by (3.18),...,(3.20) and (3.24),..., (3.26) respectively; for $G_{0,1}(.,.)$ see (3.38) and for $G_{1,1}(.,.)$ see (3.39). Applying (3.38) and (3.39) to (4.120) we obtain:

$$\begin{aligned} P_1(t) &= [A_{0,1}(t') - \{A_{0,1}(t') - A^{(n)}_{0,1}(t'+t-t')\}]A(0) \\ &\quad + [A_{1,1}(t') - \{A_{1,1}(t') - A^{(n)}_{1,1}(t'+t-t')\}]\{1-A(0)\} \\ &= A^{(n)}_{0,1}(t)A(0) + A^{(n)}_{1,1}(t)\,\{1-A(0)\}, \qquad t\in[t', T_K], \end{aligned} \tag{4.121}$$

with $A^{(n)}_{0,1}(.)$ and $A^{(n)}_{1,1}(.)$ related to the interval [0,t'] for the component's periodical inspection process (see section 3.5.3.), and with t' defined by (4.119).

In the figures 4.7. and 4.8. examples are shown for the unavailability of a periodically inspected component during a phased mission (drawn line). In fig. 4.7. the start of the mission is contained in the inspection interval and the start of the first operational part in the repair interval, whereas in fig. 4.8. the start of the first operational part lies outside the repair interval.

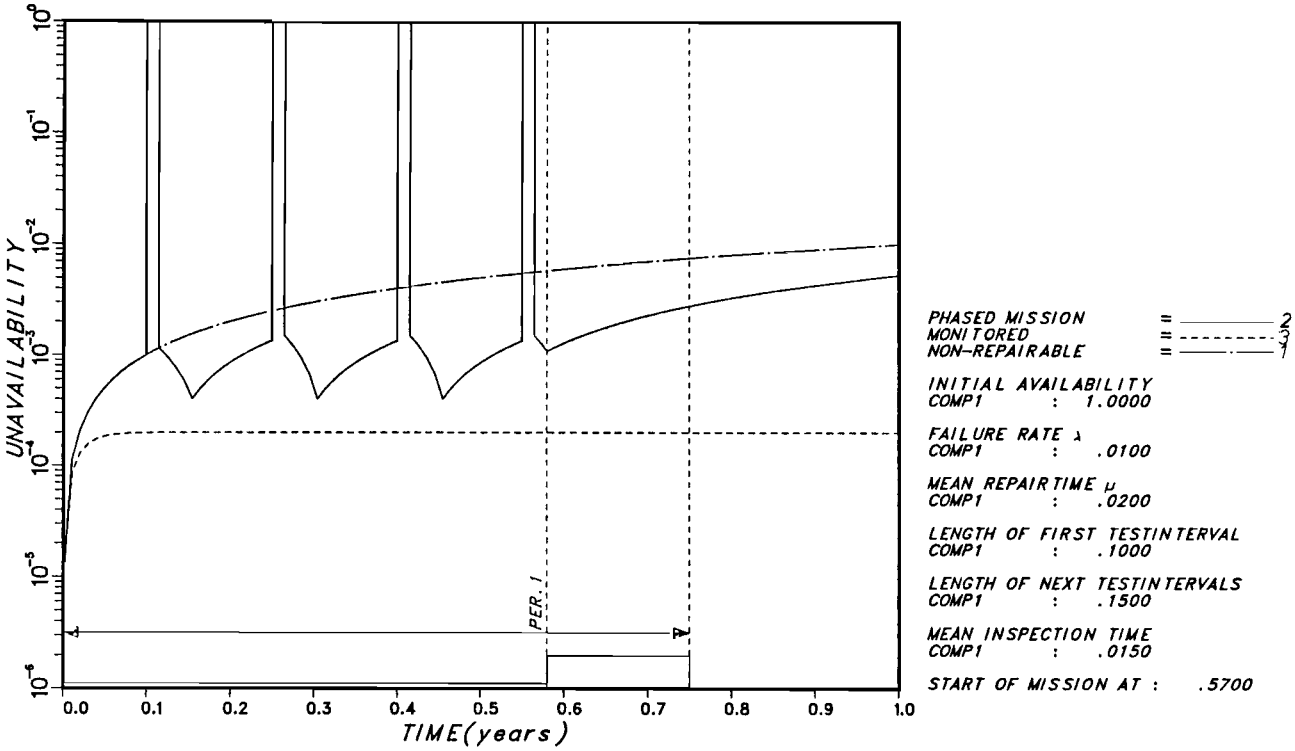


FIG.4.7 UNAVAILABILITY FOR A PERIODICALLY INSPECTED COMPONENT DURING A PHASED MISSION
N.E.D. LIFETIME DISTRIBUTION
UNIFORM REPAIRTIME DISTRIBUTION

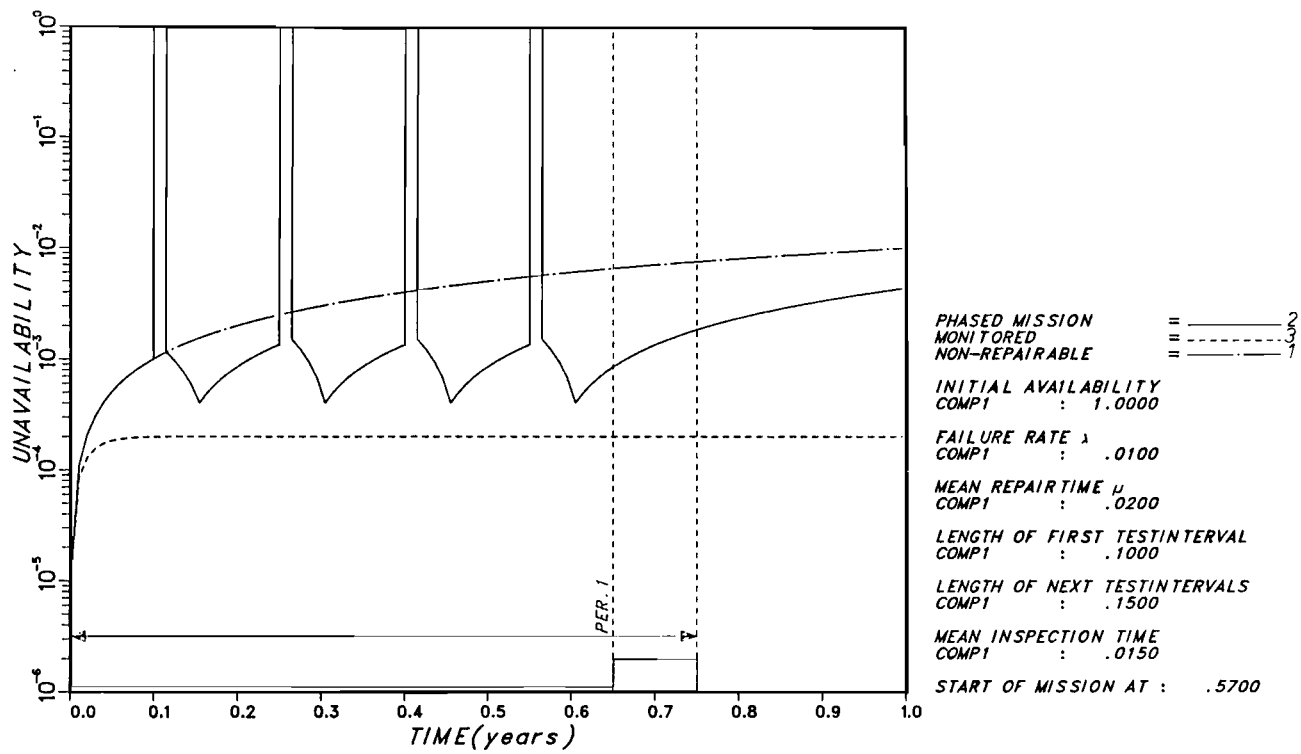


FIG.4.8 UNAVAILABILITY FOR A PERIODICALLY INSPECTED COMPONENT DURING A PHASED MISSION
N.E.D. LIFETIME DISTRIBUTION
UNIFORM REPAIRTIME DISTRIBUTION

In each figure three curves are shown:

(i) curve 1: the component is non-repairable (class 1 component);

(ii) curve 2: the component is periodically inspected (class 4 component) and fulfills a mission, its repairtime is uniformly distributed;

(iii) curve 3: the component is continuously inspected (class 2 component) and does not fulfill a mission. Its repairtime is n.e.d.

4.6. The conditional availability of a component during the mission

In calculating phased mission success often the availability of a component has to be calculated at instant t with respect to (conditioned to) the fail state of the component at an earlier instant $T_j<t$. Therefore we introduce the conditional availability $A(t|T_j)$ of a component:

$$A(t|T_j) = \Pr\{\underline{x}(t)=0|\underline{x}(T_j)=1\},\ t>T_j, \tag{4.122}$$

T_j being the end of an *operational* phase of the component (see chapter 6). The reason why and in what manner these conditional probabilities arise in phased mission analysis is fully treated in chapter 6.

4.6.1. The conditional availability of non-repairable, randomly inspected and periodically inspected components during the mission

If a non-repairable, randomly inspected or periodically inspected component has become operational, then it is supposed (see chapter 2) that for such a component no repair is permitted during the continuation of the mission. Therefore, if such a component is in the fail state at the start of its first operational part or switches during the mission to the fail state, then it remains in the fail state till the end of the mission. So for these classes of components, the conditional availability $A(t|T_j)$ is obviously given by:

$$A(t|T_j)=0,\ t>T_j>T_0\geq 0. \tag{4.123}$$

4.6.2. The conditional availability of a continuously inspected component during the mission

During a phased mission repair is permitted for a continuously inspected component during the time intervals the component needs not to be operational, i.e. repair is permitted during the dormant part of the periods of that component. No repair is permitted during the operational part of the periods of the component. So two distinct situations can be distinguished, viz. (i) the instants t and T_j, $t>T_j$, belong to the same period or (ii) the instants t and T_j do *not* belong to the same period of the component. In case (i) the instants t and T_j belong to the same operational part of a period of the component, so if the component is in the fail state at instant T_j it is in the fail state at instant t with certainty. Therefore

$$A(t|T_j)=0, \text{ if t and } T_j,\ t>T_j, \text{ belong to the same operational part of a continuously detected component.} \qquad (4.124)$$

If instant t and instant T_j do not belong to the same period (case (ii)) then they belong to different periods, say instant T_j belongs to period k_1 and instant t belongs to period k_2, $k_2>k_1$, of the component. (Note that T_j is the end of an operational phase in period k_1). The end of period k_1 is marked by the instant t_{k_1}. From the above it is clear that if the component is in the fail state at instant T_j, it is in the fail state at instant t_{k_1} (T_j and t_{k_1} belong to the same operational part). At instant t_{k_1} a derived renewal process starts with the initial state the fail state in this case (see section 4.3.2.). If we call the dormant part of the $(k_1+1)^{th}$ period the OR-phase, then the calculation of the conditional availability $A(t|T_j)$ is reduced to the calculation of the absolute availability $P_{k_2-k_1}(t-t_{k_1+1})$ with initial condition $P_0(0)=0$.

So the conditional availability of a continuously inspected component for the original mission has changed into the calculation of an absolute availability of this component for another mission with initial state the fail state. Suppose the original mission for the component is characterized by the instants:

$$t_1, t_1', t_2, t_2', \ldots, t_{k_1}, t_{k_1}', \ldots, t_{k_2}, t_{k_2}', t_{k_2+1}, \ldots, \tag{4.125}$$

with t_k and t_k', k=1,2,..., as defined by (4.2) and (4.3), respectively, being the start of the k^{th} period and the k^{th} operational part. To be able to calculate the conditional availability $A(t|T_j)$, we consider a new mission characterized by the instants:

$$0, t_{k_1+1}' - t_{k_1+1}, t_{k_1+2} - t_{k_1+1}, \ldots, t_{k_2} - t_{k_1+1}, t_{k_2}' - t_{k_1+1}, t_{k_2+1} - t_{k_1+1}, \ldots . \tag{4.126}$$

The renewal process that starts at instant t=0 in the new mission is the derived renewal process that starts in the mission of (4.125) at instant t_{k_1+1} with initial state the fail state. During the other periods of the mission of (4.126) we have to deal with the derived renewal processes described by the original mission of (4.125). So the derived renewal processes starting during the mission of (4.126) at instants $t_{k_1+n} - t_{k_1+1}$, n=1,2,..., are identical to those starting during the original mission of (4.121) at the instants t_{k_1+n}, n=1,2,... .
Summarizing the above mentioned, we obtain for the conditional availability $A(t|T_j)$ of a continuously inspected (class 2) component during the mission with t and T_j not belonging to the same period:

$$A(t|T_j) = P_{k_2-k_1}(t-t_{k_1+1}), \quad t \in [t_{k_2}, t_{k_2+1}], \quad T_j \in [t_{k_1}', t_{k_1+1}), \quad k_2 > k_1, \tag{4.127}$$

with $P_k(t)$ defined by (4.24) if $t \in [t_k, t_k')$ and by (4.26) if $t \in [t_k', t_{k+1})$. The mission within the time interval $[0, t-t_{k_1+1}]$ is described by (4.126) and derived from the original mission as described by (4.125).

5. FAULT TREE ANALYSIS

5.1. Introduction

In the past decade *fault tree analysis* has become an important tool in system reliability. Fault tree analysis is a formalized deductive technique that provides a systematic approach to investigate the possible modes of occurrence of a defined system state, in particular undesired states. Fault tree analysis was first conceived by H.A. Watson of Bell Telephone Laboratories in connection with an Air Force contract to study the Minuteman missile launch-control system.

Boeing Company analysts have extended the technique and developed computer programs for both qualitative and quantitative analysis. In 1965 at a system safety symposium in Seattle, Washington, it was recognized that aerospace technology could be successfully extended to nuclear reactor safety technology and to various other civil systems.

In 1967 Garrick et al recommended implementation of aerospace techniques in quantifying system reliability and safety, and in establishing the relative importance of various components to system operation. In the mid 60's Farmer from the United Kingdom Atomic Energy Agency analysed a spectrum of reactor accidents in order to estimate the overall risk from nuclear power plant operation. Risk in this case was defined to be the product of two factors namely the probability of occurrence of the accident and its consequences. Based on these considerations an elaborate risk assessment of nuclear power plant operation was completed in 1974 by the United States Atomic Energy Commission, known as the RASMUSSEN study. Also in Germany a risk study directed to the impact of nuclear power plants on society has been performed. It started in 1976 and its first phase was finished in 1979.

In the early 1970's system safety and reliability techniques were also applied in the chemical industry. So far for a brief review of the origin of fault tree analysis. For further details the reader is referred to Lambert [11].

The technique of fault tree analysis will be used in the present study of Phased Missions. It is therefore, that we give in this chapter a brief description of fault tree analysis. For an extensive treatment of its principles and its use the reader is again referred to Lambert [11].

The objectives of Fault Tree Analysis are:

- to find systematically all possible failure modes of the occurrence of the "top" event (i.e. the considered undesirable system failure);
- to give a clear and graphical representation of all possible modes of operation of the system;
- to have a foundation to judge alternatives of design, maintenance and inspection.

Fault Tree Analysis consists of two important phases:

- the construction of the fault tree;
- the evaluation of the fault tree.

In section 5.2. the construction of the fault tree and the determination of all failure modes leading to the top event will be treated (qualitative fault tree analysis). In section 5.3. the evaluation of the fault tree will be discussed; it is based on a probabilistic approach (quantitative fault tree analysis).

5.2. Qualitative Fault Tree Analysis

5.2.1. Basic elements of the fault tree

For the evaluation of system performance it is necessary to have an insight in the possibilities of the occurrences of "undesired" states or events (so-called "top" events). Once a top event (in generally a highly undesired event) has been defined, its possibility (and probability) of occurrence has to be analysed. *Fault tree analysis is a technique for a systematic investigation of the possible failure modes resulting in the top event.* Obviously, for such an analysis a highly detailed description of the top event is required. For the analysis of the top event a number of concepts are needed. These concepts and their "symbol" representations will be now firstly discussed.

- A *primary event* (failure) or a *basic event* is an event that will not be described by more detailed events: such a description not being possible at all, or because of a lack of data, or not being relevant for the analysis.

- A *compound event* is an event which can be described by the *conjunction* and/or *disjunction* of primary events. The conjunction and disjunction operations will be represented by "AND" and "OR" gates.

- An *undeveloped event* is a compound event of which the performance evaluation is not possible. Therefore, it is not further investigated.

- A *normal event* is an event that does occur with probability zero or one.

- An *"OR" gate* is a logical relation between the input events and the output event: *the output event occurs if at least one of the input events occurs.*

- An *"AND" gate* is a logical relation between the input events and the output event: *the output event occurs if and only if all input events occur.*

For the events introduced above a symbolic notation is used in the graphical representation of fault trees. In fig. 5.1. the symbolic notation is illustrated.

Large fault trees often contain compound events which appear at several places in the fault tree. It is convenient to describe such branches once. To indicate where such a branch occurs in the tree and which branch is meant, special *transfer labels* are used. At each place where a *branch* is inserted in the tree it is represented by a *"transfer-in"* label, whereas that branch itself is represented by a *"transfer-out"* label, each of the labels carrying the same name. In fig. 5.2. the symbol representation of these labels is shown.

Concerning the behaviour of the basic elements of a fault tree it is once and for all assumed that every event has only two possible outcomes:

(i) the event occurs,
(ii) the event does not occur.

If the *event occurs*, this means that the element under consideration (for instance a component like a switch, a valve, wiring or a relay or a human element like an operator or a driver) is in the fail state; on the other hand if the *event does not occur*, the element is in the *function state*.

An element is in the function state if it performs its prescribed behaviour, otherwise it is in the fail state.

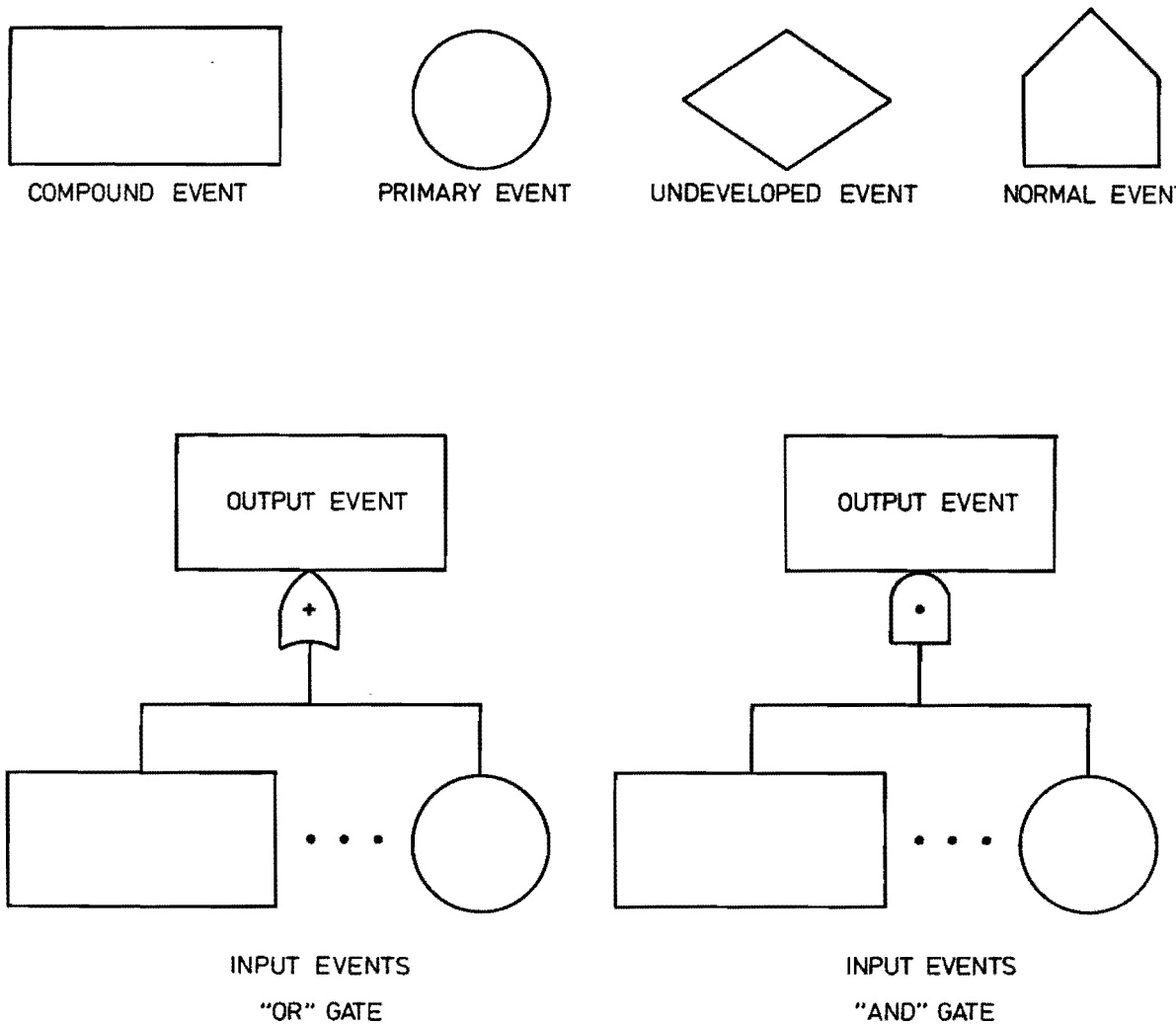


FIG. 5.1. SYMBOLS USED IN FAULT TREE ANALYSIS.

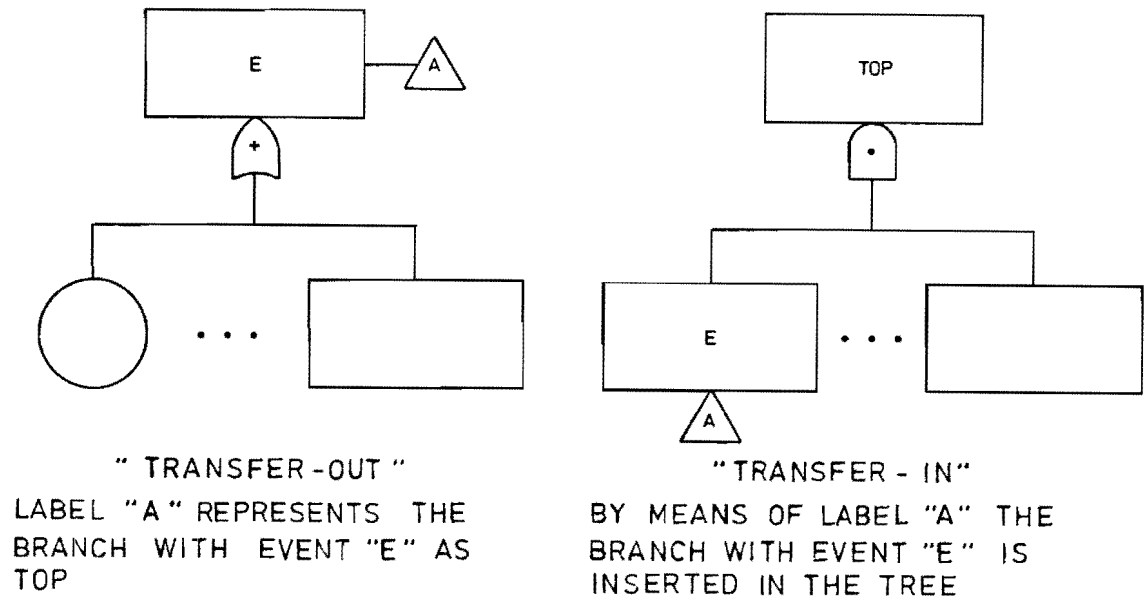


FIG. 5.2. TRANSFER LABELS IN A FAULT TREE

5.2.2. Some examples concerning the description of the "fail" state and the "function" state

In practice it is often not so obvious how to define for a component the fail state and the function state, since most components do not behave binarily, as it has been assumed in the foregoing. On the basis of some examples definition of fail state and function state will be illustrated.

Example 1: a wire

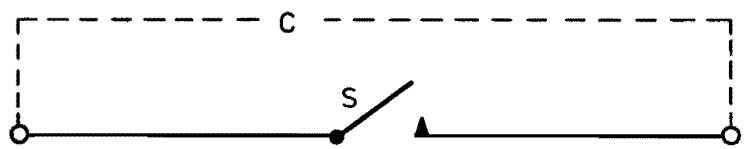
As a first example we take a wire that connects two points A and B galvanically. The basic event in this case is: "defect of the wire in circuit AB". When we are only interested in current or no current through the wire it behaves as a binary component. The fail state is defined by "no current through the wire from A to B"; if there exists a voltage between A and B, the function state is defined by "current through the wire from A to B". If we are not only interested in current or no current, but also in partial current, the fail state and the function state have to be defined more carefully, i.e. when the current is less than I the wire is in the fail state and when the current is greater than I the wire is in the function state.

Example 2: a valve

In hydraulic and pneumatic systems usually the components have more than two states. For example, a valve in a pipe has infinitely many positions. The event "the valve is closed" formally means: no flow is possible through the pipe. But sometimes in practical situations the effect of the closure of 90 percent of the pipe flow area is the same as that of a 100 percent closure. This means that in this case the event "valve is closed" can be described by "the valve is closed for more than 90 percent of the pipe flow area". If the valve is commanded to open but stays closed, then the fail state is characterized by "the valve does not open more than 10 percent of the pipe flow area" (basic event) and the function state by "the valve opens for more than 10 percent of the pipe flow area".

Example 3: a two-position switch

The switch can be in two positions, i.e. "open" and "closed". But there are four possible states for the switch.



- switch is open ; when commanded to close, it closes,
- switch is open ; when commanded to close, it fails to close,
- switch is closed; when commanded to open, it opens,
- switch is closed; when commanded to open, it fails to open.

If in a fault tree the event "circuit C fails" occurs, we must know what the intended function of circuit C is. In the case that circuit C has to be closed, then it means that the occurrence of the event "circuit C fails" includes that switch S fails to close. It is obvious that the fail state of switch S now is "switch S fails to close", which is a basic event, and that the function state is "switch S is in the position "open" and functions". If on the other hand the circuit has to be opened, the occurrence of the event "circuit C fails" means that switch S "fails to open"

(basic event) and the function state is that "switch S is in the position "closed" and functions". It is clear that the fail states "switch S fails to open" and "switch S fails to close" exclude each other at the same epoch. In constructing the fault tree one has to take care of this phenomenon.

5.2.3. Classification of events

Two main groups of events can be distinguished in constructing fault trees:

(a) events that can be predicted with certainty (normal events),
(b) events that cannot be predicted with certainty.

Ad (a):
As a matter of fact these are planned events, for example:
- removal of a battery for maintenance during system operation;
- control rods are inserted when an operator pushes a scram bar.
  This is an example from operation of a nuclear reactor. In such a reactor fission of Uranium takes place. This fission is caused by neutrons and at each fission new neutrons are created. Reactor power is proportional to the fission rate, which in turn depends on the neutron flux density in the reactor core. So, to control reactor power, the neutron flux has to be controlled. This is done by the so-called "control rods", which contain neutron absorbing materials such as Cadmium. By slowly moving the control rods into and out of the core the neutron flux is controlled. However, to stop the reactor all control rods have to be inserted at once. This last action is called a *"scram"*.

Ad (b):
Such events can be divided into two classes:
Class 1: a system element fails to perform an "intended" function, for instance,
- pump fails to start when switch is closed.

Class 2: a system element performs an "inadvertent" function such as
- spurious scram of a reactor during operation.
  This means that the reactor is stopped by insertion of the control rods for no reason. (For "scram" see ad (a)).

5.2.4. Classification of system failures

If a system failure occurs, the question is always whether the failure is caused by a *subsystem* or by a *component*. In the first case the event has to be developed further. In the second case there are three failure mechanisms that may cause the component to be in the fail state:

- a primary failure : that is a failure due to the internal characteristics of the component; such a failure is corrected by repairing the component or by replacing the component by a new one;
- a secondary failure : that is a failure due to excessive environmental or operational stress placed on the component;
- a command fault : here the component functions in a proper way, but it is activated by a command that should not have been occurred.

5.2.5. The construction of the fault tree

The construction of a fault tree will be demonstrated on the basis of the passive electrical network in fig. 5.3.

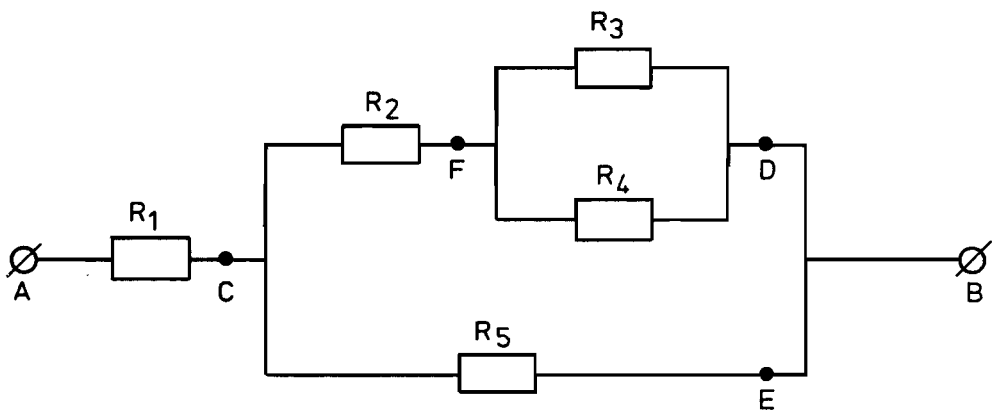


FIG. 5.3. PASSIVE ELECTRICAL NETWORK.

As a possible TOP event we take in this case the event "no current through the network" or "no current through A-B". For this top event (G1) we shall construct the fault tree (see fig. 5.4.). The top event may be caused by the event "no current through A-C" (event G2) *or* by the event "no current through C-B" (event G3), or by both of them.

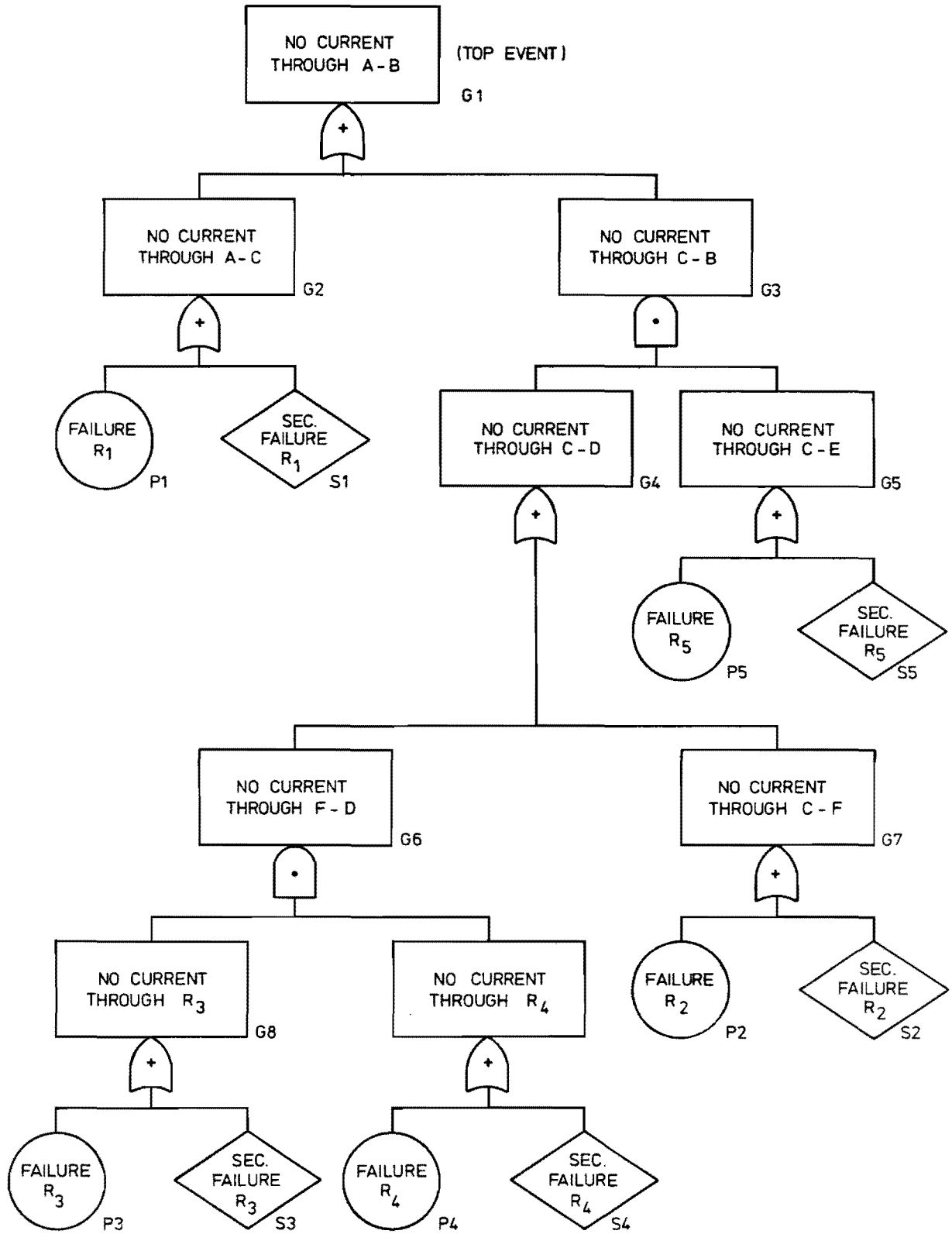


FIG. 5.4. FAULT TREE OF THE PASSIVE ELECTRICAL NETWORK.

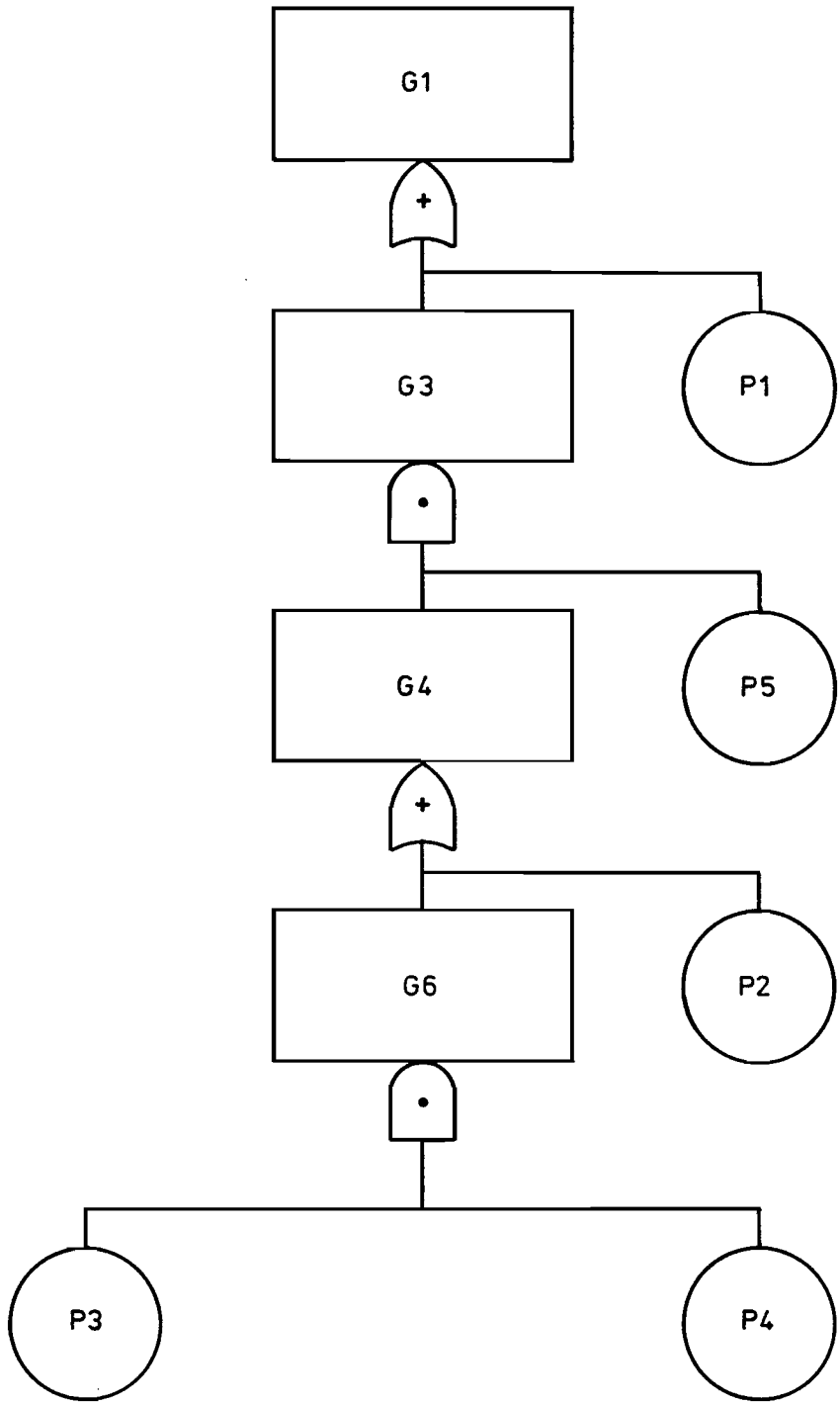


FIG. 5.5. REDUCED FAULT TREE OF THE ELECTRICAL NETWORK.

So in fig. 5.4. the output event G1 is obtained by means of an OR gate from the input events G2 and G3. The event G2 "no current through A-B" is caused by a failure of component R_1 (if we neglect wiring), i.e. a primary failure (P1) or a secondary failure (S1). Since gate event G2 has been developed to basic elements, the development of the fault tree for this branch stops. Event G3 is caused by the events G4, "no current through C-D", *and* G5, "no current through C-E". So the output event G3 is represented by an AND gate. Going on in this way the whole fault tree of the system in fig. 5.3. is constructed and depicted in fig. 5.4. If we remove all secondary failures of this fault tree, we get the so-called *"reduced"* fault tree of fig. 5.5.
Secondary failures are incorporated in the fault tree for reasons of completeness. Often they will not be considered because they are difficult to specify and, if so, they have a very small probability of occurrence, when compared to failure probabilities of other basic events.

5.2.6. Minimal cut sets and minimal path sets

The identification of those components or those groups of components that can cause system failure is necessary for the system reliability analysis. For this purpose the following concepts are introduced: *cut set*, *minimal cut set*, *path set* and *minimal path set*.

Cut set

A cut set is any specific combination of basic events whose combined occurrence causes the top event to occur.

Minimal cut set

A minimal cut set is a cut set that does not remain a cut set if it is reduced.

Path set

A path set is any specific combination of basic events whose combined non-occurrence assures the non-occurrence of the top event.

Minimal path set

A minimal path set is a path set that does not remain a path set if it is reduced.

Cut sets and path sets are *dual* concepts. Changing OR gates into AND gates and vice versa and complementing every event of the original fault tree we get the *dual* fault tree. The cut sets of the original fault tree are the path sets of the dual fault tree and vice versa.
Cut sets or path sets may be used in principle to obtain quantitative system characteristics. Very often they are used to obtain bounds on the system unreliability or unavailability, see Barlow and Proschan [15].

In table 5.1. the minimal cut sets and minimal path sets, obtained from the reduced fault tree in fig. 5.5. of the system in fig. 5.3., are tabulated. Complex systems contain many minimal cut sets, sometimes hundreds of thousands. Therefore, its analysis can only be realized by making use of a computer. Nowadays many computer programs are available to obtain the minimal cut sets, see Henley and Kumamoto [29]. In treating complex systems, even today with big and fast computers, it takes a lot of time and money to determine all the minimal cut sets.

TABLE 5.1.

MINIMAL CUT SETS OF THE ELECTRICAL NETWORK

Nr.	Order*	Minimal cut sets
K_1	1	{P1}
K_2	2	{P2,P5}
K_3	3	{P3,P4,P5}

MINIMAL PATH SETS OF THE ELECTRICAL NETWORK

Nr.	Order*	Minimal path sets
Q_1	2	{P1,P5}
Q_2	3	{P1,P2,P3}
Q_3	3	{P1,P2,P4}

*"Order" means the number of basic events contained in a minimal cut set or a minimal path set.

5.3. Quantitative fault tree analysis

Quantitative fault tree analysis can be divided into the following steps:

- construction of the structure function of the system;
- applying probability theory to the system.

5.3.1. Construction of the structure function of the system

Characterize the state of the system (top event) at time t by the binary stochastic variable

$$\underline{y}(t) \overset{\text{def}}{=} \text{state of the system at time t;} \tag{5.1}$$

$\underline{y}(t) = 0$, the system is available at time t,

$= 1$, the system is not available at time t,

and further the state of a component c_i, i=1,...,N, as defined in (2.2) by

$\underline{x}_i(t)$ = state of component c_i, i=1,...,N, at time t,

$\underline{x}_i(t) = 1$, if component c_i is not available at time t;

$= 0$, if component c_i is available at time t,

N being the number of components in the system. The state of the system is dependent on the state of the components, i.e.

$$\underline{y}(t) \overset{\text{def}}{=} y(\underline{x}_1(t), \underline{x}_2(t), \ldots, \underline{x}_N(t)). \tag{5.2}$$

Now suppose that the fault tree has a *coherent structure*; this means that:

i) every component of the system is relevant to the system, this includes that every component has an influence on $\underline{y}(t)$,

and that

ii) the function $\underline{y}(t)$ is non-decreasing in each of its arguments, i.e. that the occurrence of a basic event cannot transfer the system from $\underline{y}(t)=1$ to $\underline{y}(t)=0$.

Define

$$\vec{\underline{x}}(t) = (\underline{x}_1(t), \underline{x}_2(t), \ldots, \underline{x}_N(t)) \tag{5.3}$$

and denote by

$$\begin{aligned} \underline{y}(1_i,\vec{\underline{x}}(t)) &\stackrel{\text{def}}{=} \text{state of the system at time t with component } c_i \\ &\quad \text{in the fail state; } i=1,\ldots,N;\ t\geq 0; \\ \underline{y}(0_i,\vec{\underline{x}}(t)) &\stackrel{\text{def}}{=} \text{state of the system at time t with component } c_i \\ &\quad \text{in the function state; } i=1,\ldots,N;\ t\geq 0. \end{aligned} \tag{5.4}$$

Now consider

$$\Delta\underline{y}_i(t) \stackrel{\text{def}}{=} \underline{y}(1_i,\vec{\underline{x}}(t)) - \underline{y}(0_i,\vec{\underline{x}}(t)), \qquad i=1,\ldots,N;\ t\geq 0. \tag{5.5}$$

If $\Delta\underline{y}_i(t)=1$, then component c_i is called *critical* for the system at time t, because $\Delta\underline{y}_i(t)=1$ implies that $\underline{y}(1_i,\vec{\underline{x}}(t))=1$ and $\underline{y}(0_i,\vec{\underline{x}}(t))=0$. Hence from (5.5) it is seen that

$$\Delta\underline{y}_i(t)=1$$

implies that the system fails if component c_i fails and the system functions if component c_i functions.

Next we introduce (cf. section 5.2.6.)

$$\begin{aligned} N_c &\stackrel{\text{def}}{=} \text{number of minimal cut sets of the system;} \\ N_p &\stackrel{\text{def}}{=} \text{number of minimal path sets of the system.} \end{aligned} \tag{5.6}$$

Since a minimal cut set occurs if *every* basic event of the cut set occurs, and the top event occurs if *at least* one minimal cut set occurs, the structure function for the fault tree (system) reads

$$\underline{y}(\vec{\underline{x}}(t)) = \coprod_{\ell=1}^{N_c} \prod_{i\in M_\ell} \underline{x}_i(t), \tag{5.7}$$

where i passes through all basic events of minimal cut set M_ℓ and

$$\coprod_{\ell=1}^{h} z_\ell \stackrel{\text{def}}{=} 1 - \prod_{\ell=1}^{h} (1-z_\ell). \tag{5.8}$$

It is also possible to give the structure function of the system in terms of minimal path sets. Since the occurrence of a minimal path set is caused by *at least* one occurrence of the basic events contained in it and the top event occurs if *all* minimal path sets occur, the structure function now reads

$$\underline{y}(\vec{\underline{x}}(t)) = \prod_{r=1}^{N_p} \coprod_{i\in P_r} \underline{x}_i(t), \tag{5.9}$$

where i passes through all basic events of minimal path set P_r.

5.3.2. System unavailability (the probability of the top event)

Denoting by $F_i(t)$ the lifetime distribution of component c_i, i=1,...,N, and by $A_i(t)$ its availability (see chapter 3), then the unavailability $q_i(t) \overset{def}{=} Pr\{\underline{x}_i(t)=1\}$ at time t is given by

$$\begin{aligned} q_i(t) &= F_i(t) \quad , \text{ if component } c_i \text{ is non-repairable,} \\ &= 1-A_i(t) \quad , \text{ if component } c_i \text{ is repairable, } t\geq 0, i=1,\ldots,N. \end{aligned} \tag{5.10}$$

The unavailability of the system is denoted by

$$\begin{aligned} g(\vec{q}(t)) &\overset{def}{=} Pr\{y(\vec{\underline{x}}(t))=1\}, \\ \vec{q}(t) &= \{q_1(t),\ldots,q_N(t)\}. \end{aligned} \tag{5.11}$$

Because complex systems may contain a very large number of minimal cut sets it is often not possible to calculate the probability of the top event exactly, this due to the fact that the calculation is too lengthy, i.e. too much computer time is needed. Therefore the system unavailability has to be approximated. Two methods may be used here, i.e. (i) the method of the minimal cut upperbound and minimal path lowerbound for $g(\vec{q}(t))$ and (ii) the procedure of inclusion and exclusion. The first method provides a quick calculation whereas the second method is slower but more accurate.

5.3.2.1. The minimal cut upperbound and the minimal path lowerbound

Since

$$g(\vec{q}(t)) = E\{y(\vec{x}(t))\},$$

and because (5.9) and (5.7) imply

$$E\{\underline{y}(t)\} = E\left\{\prod_{r=1}^{N_p} \coprod_{i\in P_r} \underline{x}_i(t)\right\} \geq \prod_{r=1}^{N_p} \coprod_{i\in P_r} E\{\underline{x}_i(t)\},$$

$$E\{\underline{y}(t)\} = E\left\{\prod_{\ell=1}^{N_c} \coprod_{i\in M_\ell} \underline{x}_i(t)\right\} \leq \prod_{\ell=1}^{N_c} \coprod_{i\in M_\ell} E\{\underline{x}_i(t)\},$$

it follows that

$$\prod_{r=1}^{N_p} \coprod_{i\in P_r} q_i(t) \leq g(\vec{q}(t)) \leq \coprod_{\ell=1}^{N_c} \prod_{i\in M_\ell} q_i(t). \tag{5.12}$$

(For a proof of (5.12) see Barlow and Proschan [17]).

Obviously, the lowerbound in (5.12) is obtained by considering the minimal paths for the top event, whereas the upperbound stems from the minimal cuts for the same top event.
For so-called "reliable systems", that are systems with a rather long mean time between failures (MTBF), the unavailability $g(\vec{q}(t))$ of the system appears to be rather close to its upperbound; a result which stems from experience with models for which $g(\vec{q}(t))$ in (5.12) can be calculated exactly (cf. Lambert [11]).

5.3.2.2. The inclusion-exclusion principle

Denote by

$\underline{\psi}_j(t)$ the state variable of minimal cut set M_j of the system at time t, $t\geq 0$; $j=1,\ldots,N_c$; N_c is the number of minimal cut sets of the system, (5.13)

i.e.

$\underline{\psi}_j(t) = 1$, if the minimal cut set M_j occurs at time t,
$= 0$, otherwise.

The probability of the top event is defined by

$$g(t) = \Pr\{\underline{y}(t)=1\} = \Pr\{\bigcup_{j=1}^{N_c} (\underline{\psi}_j(t)=1)\}. \tag{5.14}$$

From (5.14) it follows that

$$g(t) = \sum_{j=1}^{N_c} \Pr\{\underline{\psi}_j(t)=1\} - \sum_{j_1=1}^{N_c-1} \sum_{j_2=j_1+1}^{N_c} \Pr\{\underline{\psi}_{j_1}(t)=1, \underline{\psi}_{j_2}(t)=1\} + \ldots . \tag{5.15}$$

Introduce the variables S_k, $k=1,\ldots,N_c$, by

$$S_k \stackrel{\text{def}}{=} \sum_{j_1=1}^{N_c-k+1} \sum_{j_2=j_1+1}^{N_c-k+2} \cdots \sum_{j_k=j_{k-1}+1}^{N_c} \Pr\{\underline{\psi}_{j_1}(t)=1, \underline{\psi}_{j_2}(t)=1, \ldots, \underline{\psi}_{j_k}(t)=1\}, \quad k=1,\ldots,N_c. \tag{5.16}$$

Substitution of (5.16) into (5.15) gives

$$g(t) = S_1 - S_2 + S_3 - \ldots . \tag{5.17}$$

As

$$S_1 \geq S_2 \geq S_3 \geq \ldots \geq S_k \geq \ldots \geq S_{N_c},$$

it follows for the probability of the top event that

$g(t) \leq S_1$, often called the "rare event" approximation,

$$g(t) \geq S_1 - S_2, \tag{5.18}$$

$g(t) \leq S_1 - S_2 + S_3$, etc.

When S_1 is used as an approximation for g(t) it is usually called the "rare event approximation".
So, by the above procedure, the system unavailability can be bounded from above and from below as accurate as desired. In this study the inclusion-exclusion principle as described above will be applied.

5.3.3. The lifetime distribution of a system (system unreliability)

For complex systems it is in general very difficult to determine the exact lifetime distribution. In principle it is possible, but even in simple cases the numerical evaluation is hardly possible. Even if the stochastic behaviour of the system can be modelled by a Markov process with discrete state space, for instance if all lifetime and repairtime distributions are negative exponential, it is hardly possible to calculate the system lifetime distribution. To get some insight in the lifetime distribution of the system we therefore have to use approximations. In the next subsections we shall discuss some of these approximation techniques.
For some special cases it is possible to determine the exact system lifetime distribution by using fault tree analysis, viz. for systems with only non-repairable components and also for systems for which all minimal cut sets are mutually independent. For a system consisting of only non-repairable components the unavailability at time t is equal to the probability that the lifetime of a system is less than t, so that the lifetime distribution can be determined by (5.17). In the case of mutual independent minimal cut sets (with or without repairable components) the lifetime distribution $F_S(t)$ of the system at time t is fully determined by the lifetime (time to occurrence) distributions $D_j(t)$, $j=1,\ldots,N_c$, of the minimal cut sets of the system. Because (cf. (5.15))

$$
\begin{aligned}
1-F_S(t) &= \Pr\{\text{system lifetime is greater than } t\} \\
&= \Pr\{\bigcap_{j=1}^{N_c} (\text{the lifetime of minimal cut set } M_j \text{ is greater than } t)\} \\
&= \prod_{j=1}^{N_c} \Pr\{\text{the lifetime of minimal cut set } M_j \text{ is greater than } t\},
\end{aligned}
$$

the last equality sign being based on the assumed mutual independence of all minimal cut sets. So

$$1-F_S(t) = \prod_{j=1}^{N_c} \{1-D_j(t)\}. \qquad (5.19)$$

Because in practical situations the total number of components in a minimal cut set is usually rather limited, it is possible to calculate $D_j(t)$ with reasonable computer time.
In general, when repairable components are allowed and minimal cut sets are not necessarily independent, fault tree analysis is not able to produce an exact solution for the system lifetime distribution (see Clarotti [18] and Parry [19]).

Finally, it is noted that at present attempts are made to calculate the system lifetime distribution by applying the theory of Markov processes. If all lifetime and repairtime distributions of the component are negative exponential, then the stochastic behaviour of the system can be described by a discrete state space, continuous time parameter Markov process. The lifetime distribution is now actually an entrance distribution for this Markov process and it can be calculated in principle. The construction of feasible computer programs for this entrance distribution is actually the crucial point, see Somma [25].

5.3.3.1. The expected number of system failures in [0,t]

In this section we discuss the expected number of system failures in [0,t] because this function occurs in the approximations for the system lifetime distribution, to be discussed in the next sections. The expected number of system failures in [0,t] will be indicated by $m_S(t)$.
Since the state variables $\underline{x}_i(t)$,i=1,...,N, are binary variables, the structure function $\underline{y}(t) = y(\vec{\underline{x}}(t))$ is linear in all its arguments. From $g(\vec{q}(t))=E\{\underline{y}(t)\}$ and $q_i(t)=E\{\underline{x}_i(t)\}$ it is now readily seen that $g(\vec{q}(t))$ is also linear in all its arguments, because it has been assumed that all $\underline{x}_i(t)$'s are independent (see assumption 2.5.4.). From this property and from (5.4) and (5.5) we get the probability that component c_i is critical at time t

$$\Pr\{\Delta \underline{y}_i(t)=1\} = E\{\Delta \underline{y}_i(t)\} = E\{y(1_i,\vec{\underline{x}}(t))\} - E\{y(0_i,\vec{\underline{x}}(t))\}$$

$$= g(1_i,\vec{q}(t)) - g(0_i,\vec{q}(t))$$

$$= \frac{\partial g(\vec{q}(t))}{\partial q_i(t)}, \qquad i=1,\ldots,N;t\geq 0, \tag{5.20}$$

with

$$g(1_i,\vec{q}(t)) = \Pr\{y(1_i,\vec{\underline{x}}(t))=1\}, g(0_i,\vec{q}(t)) = \Pr\{y(0_i,\vec{\underline{x}}(t))=1\}.$$

So for a system consisting of repairable and/or non-repairable components and for dt very small, the event

"system failure in (t,t+dt)"

$$= \bigcup_{i=1}^{N} \text{"component } c_i \text{ causes system failure in } (t,t+dt)\text{"}$$

$$= \bigcup_{i=1}^{N} \text{"component } c_i \text{ critical at time t and component } c_i \text{ fails in } (t,t+dt)\text{"}. \tag{5.21}$$

With respect to the calculation of Pr{system failure in (t,t+dt)} from (5.21), it is first noted that the event "component c_i critical at time t" is independent from the event "component c_i fails in (t,t+dt)" because the function $y(\vec{\underline{x}}(t))$ is linear in all its arguments so that the right hand side of (5.5) does not contain $\underline{x}_i(t)$. Secondly, it will be assumed that the probability that two components will fail simultaneously is negligibly small. Note that this assumption requires that components do not fail by common causes.

Taking the probability of both sides of (5.21) it follows that

$$\Pr\{\text{system failure in } (t,t+dt)\}$$

$$= \sum_{i=1}^{N} \Pr\{\text{component } c_i \text{ critical at time t}\} \cdot \Pr\{\text{component } c_i \text{ fails in } (t,t+dt)\}. \tag{5.22}$$

Since it has been assumed that the probability of more than one component failure in (t,t+dt) is negligible, we have for the density $dm_S(t)$ of the expected number of system failures in [0,t]

$$dm_S(t) = 0.\Pr\{\text{no system failure in } (t,t+dt)\}$$
$$+ 1.\Pr\{\text{system failure in } (t,t+dt)\}$$
$$= \Pr\{\text{system failure in } (t,t+dt)\}. \qquad (5.23)$$

On the basis of (5.23), (5.22) and (5.20) we obtain for the density of the expected number of system failures in [0,t]

$$dm_S(t) = \sum_{i=1}^{N} \frac{\partial g(\vec{q}(t))}{\partial q_i(t)}\, dm_i(t),\ t\geq 0, \qquad (5.24)$$

$m_i(t)$ being the renewal function of component c_i as defined in chapter 3. From (5.24) the expected number of system failures in [0,t] is simply calculated by integration.

5.3.3.2. Upper and lowerbound for the system lifetime distribution according to Murchland

The time dependent behaviour of a system composed of repairable and non-repairable components is binary, i.e. the system can be in the function state or in the fail state. Assume that the system is in the function state at instant t=0. Denote by $F_S(t)$ its first lifetime distribution and by $g(\vec{q}(t))$ its unavailability. Then it is easily seen that the system availability at instant t is given by

$$1-g(\vec{q}(t)) = \Pr\{\text{no system failure in } [0,t]\}$$
$$+ \sum_{k=1}^{\infty} \Pr\{k \text{ system failures in } [0,t], \text{ the system functions at instant } t\};\ t\geq 0. \qquad (5.25)$$

From (5.25) it is easily seen that

$$1-g(\vec{q}(t)) \geq \Pr\{\text{no system failure in } [0,t]\} = 1-F_S(t),$$

or

$$g(\vec{q}(t)) \leq F_S(t),\ t\geq 0. \qquad (5.26)$$

For the expected number of system failures in [0,t], denoted by $m_S(t)$, the following identity can be written down:

$$m_S(t) = \sum_{k=1}^{\infty} k \Pr\{k \text{ system failures in } [0,t]\}$$

$$\geq \sum_{k=1}^{\infty} \Pr\{k \text{ system failures in } [0,t]\} = F_S(t), t\geq 0. \qquad (5.27)$$

On the basis of (5.26) and (5.27) the lower and upperbound for the system lifetime distribution, introduced by Murchland [20], are obtained; i.e.

$$g(\vec{q}(t)) \leq F_S(t) \leq m_S(t), \quad t\geq 0. \qquad (5.28)$$

The upperbound in (5.28) for F(t) appears to be an excellent approximation for small values of t. For large values of t, however, $m_S(t)$ behaves as a linear function whereas $F_S(t)$ ultimately reaches the value one.

5.3.3.3. The steady state upperbound for the system lifetime distribution suggested by Lambert

Assume that *all* components have a constant failure rate and a constant repair rate, and assume that the system is in steady state at instant t=0, i.e. (cf. (5.10)) $q_i(t) = \mu_i/(\mu_i+\lambda_i)$, $i=1,\ldots,N$; λ_i the failure rate and μ_i the repair rate of component c_i. Based on these assumptions Lambert [11] derives an upperbound for the system lifetime distribution in the steady state, along the following lines.
The expected number of system failures $m_{S,i}(0,\tau)$ in the time interval $[0,\tau]$ caused by component c_i is

$$m_{S,i}(0,\tau) = \int_0^{\tau} \frac{\partial g(\vec{q}(v))}{\partial q_i(v)}\, dm_i(v), \qquad \tau\geq 0. \qquad (5.29)$$

(For the derivation of relation (5.29) see section 5.3.3.1.).
From (5.29) it follows that

$$m_{S,i}(0,\tau+t) - m_{S,i}(0,\tau) = \int_{\tau}^{\tau+t} \frac{\partial g(\vec{q}(v))}{\partial q_i(v)}\, dm_i(v), \qquad \tau\geq 0, t\geq 0. \qquad (5.30)$$

Introduce

$$\Delta g_i \stackrel{\text{def}}{=} \lim_{t\to\infty} \frac{\partial g(\vec{q}(t))}{\partial q_i(t)} = \frac{\partial g(\vec{q})}{\partial q_i} \tag{5.31}$$

with

$$\vec{q} \stackrel{\text{def}}{=} (q_1,\ldots,q_N),\ q_i \stackrel{\text{def}}{=} \lim_{\tau\to\infty} q_i(\tau) = \frac{\mu_i}{\lambda_i+\mu_i},\ i=1,\ldots,N, \tag{5.32}$$

then

$$\int_\tau^{\tau+t} \frac{\partial g(\vec{q}(v))}{\partial q_i(v)}\, dm_i(v) = \int_\tau^{\tau+t} \{\frac{\partial g(\vec{q}(v))}{\partial q_i(v)} - \Delta g_i\}\, dm_i(v)$$

$$+ \Delta g_i\, \{m_i(\tau+t) - m_i(\tau)\}.$$

From (5.31) it follows that for every $\varepsilon>0$ there exists a number $v(\varepsilon)>0$ such that if $v>v(\varepsilon)$

$$|\frac{\partial g(\vec{q}(v))}{\partial q_i(v)} - \Delta g_i| < \varepsilon,$$

with $v(\varepsilon) \to \infty$ if $\varepsilon\to 0$.

Therefore, for $\tau>\tau(\varepsilon)$

$$|\int_\tau^{\tau+t} \{\frac{\partial g(\vec{q}(v))}{\partial q_i(v)} - \Delta g_i\}\, dm_i(v)| \le \int_\tau^{\tau+t} |\frac{\partial g(\vec{q}(v))}{\partial q_i(v)} - \Delta g_i|\,|dm_i(v)| < \varepsilon_m,$$

with

$$\tau(\varepsilon) \to \infty \text{ if } \varepsilon_m \to 0,$$

$$\varepsilon_m = \varepsilon\{m_i(\tau+t) - m_i(\tau)\} > 0.$$

So taking the limit $\tau\to\infty$ of both sides of (5.30) and introducing

$$m_{S,i}(t) \stackrel{\text{def}}{=} \lim_{\tau\to\infty} [m_{S,i}(0,\tau+t) - m_{S,i}(0,\tau)],$$

relation (5.30) becomes

$$m_{S,i}(t) = \Delta g_i \lim_{\tau\to\infty} [m_i(\tau+t) - m_i(\tau)], \qquad t\geq 0, \tag{5.33}$$

with

$$m_i(t) = \frac{\lambda_i\mu_i}{\lambda_i+\mu_i}\, t + \frac{\lambda_i^2}{\lambda_i+\mu_i}\,(1-e^{-(\lambda_i+\mu_i)t}), \qquad t\geq 0, \tag{5.34}$$

as defined by relation (B28) of appendix B, supposed that component c_i is in the function state at t=0.
Substitution of (5.34) into (5.33) and taking the limit shows the following result

$$m_{S,i}(t) = \Delta g_i \cdot \frac{\lambda_i\mu_i}{\lambda_i+\mu_i}\, t\,, \qquad t\geq 0,\ i=1,\ldots,N, \tag{5.35}$$

Δg_i being the expected number of system failures caused by component c_i in the time interval $[0,1/\lambda_i + 1/\mu_i]$.
If we denote by $F_{S,i}(t)$ the lifetime distribution of the system exclusively in connection with component c_i, i.e. $F_{S,i}(t)$ is the probability that component c_i causes exactly one system failure in [0,t], then from (5.28) obviously

$$m_{S,i}(t) \geq F_{S,i}(t)\,, \qquad t\geq 0. \tag{5.36}$$

From (5.36) it follows that the probability that component c_i does not cause system failure in [0,t] is bounded from below by

$$1 - m_{S,i}(t)$$

or, by substitution of (5.35)

$$1 - \Delta g_i \frac{\lambda_i\mu_i}{\lambda_i+\mu_i}\, t\,, \qquad t\geq 0. \tag{5.37}$$

The result obtained in (5.37) is essentially a result applying for steady state conditions, i.e. it is assumed that at time t=0 the steady state is prevalent.
If we consider the special time interval $[0,1/\lambda_i+1/\mu_i]$ we get from (5.37) the next lowerbound for $1-F_{S,i}(t)$

$$1 - F_{S,i}(t) \geq 1 - \Delta g_i \frac{\lambda_i\mu_i}{\lambda_i+\mu_i} t \geq (1-\Delta g_i)^{\frac{\lambda_i\mu_i}{\lambda_i+\mu_i} t},$$

$$0 \leq t \leq 1/\lambda_i + 1/\mu_i, \qquad (5.38)$$

since $\Delta g_i \leq 1$.

Now assume that the event "component c_i, i=1,...,N, causes system failure" is independent from the events "component c_k causes system failure", k=1,...,N, k≠i. Then the probability of no system failure in (0,t) is

$$1 - F_S(t) = \prod_{i=1}^{N} \{1-F_{S,i}(t)\} \geq \prod_{i=1}^{N} (1-\Delta g_i)^{\frac{\lambda_i\mu_i}{\lambda_i+\mu_i} t}$$

or

$$F_S(t) \leq 1 - \prod_{i=1}^{N} (1-\Delta g_i)^{\frac{\lambda_i\mu_i}{\lambda_i+\mu_i} t}, \qquad 0 \leq t \leq 1/\lambda_i + 1/\mu_i. \qquad (5.39)$$

The upperbound in (5.39) is now suggested by Lambert [11] to be the steady state upperbound $\hat{F}_S(t)$ for the system lifetime distribution $F_S(t)$,

$$\hat{F}_S(t) = 1 - \prod_{i=1}^{N} (1-\Delta g_i)^{\frac{\lambda_i\mu_i}{\lambda_i+\mu_i} t}, \qquad 0 \leq t \leq 1/\lambda_i + 1/\mu_i. \qquad (5.40)$$

Remark 5.3.1.

We have restricted ourselves here to the time interval $[0,1/\lambda_i+1/\mu_i]$. For reliable systems the mean lifetime of a component is as a rule greater than 10 years while the mean repairtime is less than about a month, i.e. $\lambda < 10^{-1}$/year and $1/\mu < 0{,}1$ year. Therefore, the time interval under consideration is in general sufficiently long for practical purposes.

Remark 5.3.2.

The assumption that the failures of the components are stochastically

independent is in general not true. However, if the basic event state variables $\underline{x}_i(t)$ are "associated", the bound in (5.39) will still hold. The random variables $\underline{x}_1(t),\ldots,\underline{x}_N(t)$ are "associated" if $\mathrm{cov}[f_1(\vec{\underline{x}}(t)), f_2(\vec{\underline{x}}(t))]\geq 0$ for all pairs of increasing binary functions f_1, f_2. It can be proved (cf. Barlow and Proschan [17]) that independent stochastic variables are associated.

5.3.3.4. Approximation of the system lifetime distribution by the T*-method

The expected number of system failures $m_S(t)$ appears to be a good approximation for the system lifetime distribution $F_S(t)$ for small values of t, as discussed in section 5.3.3.2. The steady state upperbound $\hat{F}_S(t)$ for $F_S(t)$, derived in the foregoing section is typically suited for large values of t. Obviously there exists an instant T* such that for $t<T^*$, $m_S(t)$ gives a better approximation for $F_S(t)$ than $\hat{F}_S(t)$ does, whereas for $t>T^*$, $\hat{F}_S(t)$ gives the better approximation of the two quantities. So the approximation of the system lifetime distribution by the T*-method becomes

$$\begin{aligned} F_S(t) &\leq m_S(t) \quad , \quad t\leq T^*, \\ F_S(t) &\leq \hat{F}_S(t) \quad , \quad t>T^*, \end{aligned} \tag{5.41}$$

$m_S(t)$ determined by (5.24) and $\hat{F}_S(t)$ by (5.40).
The determination of the moment T* is a rather complicated matter, it is discussed in Lambert [11].

5.3.3.5. An approximation for the system lifetime distribution as suggested by Vesely

Another approach is based on Vesely [21]. He defines a system failure rate analogous to the failure rate of a component, the latter being defined as

$$\lambda_i(t)dt \stackrel{\text{def}}{=} \Pr\{\underline{\ell}_i<t+dt \,|\, \underline{\ell}_i\geq t\} = \frac{dF_i(t)}{1-F_i(t)} \quad , \quad t\geq 0; i=1,\ldots,N; \tag{5.42}$$

$F_i(t)$ the distribution function of the lifetime $\underline{\ell}_i$ of component c_i.

He introduces as the system failure rate $\tilde{\Lambda}(t)$ the expression

$$\tilde{\Lambda}(t) \stackrel{def}{=} \frac{\frac{dm_S(t)}{dt}}{1-g(\vec{q}(t))}, \qquad t\geq 0, \tag{5.43}$$

and then proposes to take for the system lifetime distribution $\tilde{F}_S(t)$:

$$\tilde{F}_S(t) = 1 - \exp\{-\int_0^t \tilde{\Lambda}(\tau)d\tau\}, \qquad t\geq 0. \tag{5.44}$$

Because $m_S(t)$ and $g(\vec{q}(t))$ can be calculated for the system, the distribution $\tilde{F}_S(t)$ can be found.
In fact $\tilde{\Lambda}(t)$ is not exact the system failure rate because $\tilde{\Lambda}(t)dt$ means "the probability of a failure in $(t,t+dt)$ conditioned to no failure *at time t*", while for the correct system failure rate $\Lambda(t)$ the condition has to be *"no failure in the interval* $[0,t]$".
It is not possible to determine whether $\tilde{\Lambda}(t)$ is an upperbound for the real system failure rate $\Lambda(t)$ or not. Namely from (5.27) it follows that for every t, $dm_S(t) \geq dF_S(t)$ and from (5.26) that $1-g(\vec{q}(t))\geq 1-F_S(t)$. This includes that the numerator as well as the denumerator of $\tilde{\Lambda}(t)$ are always greater than the corresponding values of $\Lambda(t)$. However, for reliable systems (cf. section 5.3.2.1.), it has been shown that $\tilde{F}_S(t)$ gives a good approximation for the system lifetime distribution (see Lambert [11]).

5.3.3.6. The Barlow-Proschan upperbound for the system lifetime distribution

We consider the following system. It is composed of two types of compoments,

- non-repairable (class 1) components (cf. section 2.5.) having non-decreasing failure rate lifetime distributions,
- continuously detected (class 2) components, having negative exponential lifetime distributions.

Concerning the repairtime distributions of continuously detected components it is assumed that they have non-increasing repair rates. Further it is assumed that at time zero all components are in the function state.

For such a system the first lifetime distribution is of the NBU type. (A distribution F(.) is NBU or New Better than Used if and only if $1-F(\tau+t) \leq \{1-F(\tau)\}\{1-F(t)\}$). For a proof of this statement see Barlow and Proschan [22].
Obviously the first lifetime distribution $F_S(t)$ of a system composed of components with negative exponential lifetime and repairtime distributions, is NBU.
Define μ_S as the mean of the first system lifetime, and E_u as the mean lifetime of the system in the steady state. Then it can be proved (cf. Barlow and Proschan [22]) that for the system S introduced above

$$\mu_S \geq E_u, \tag{5.45}$$

when it is assumed that the system S possesses a steady state. (Note that a system S in series with a non-repairable component does not possess a steady state). For $F_S(t)$ of type NBU and with mean μ_S, the next bound is obtained (cf. Marshall and Proschan [23]):

$$F_S(t) \leq t/\mu_S, \qquad t \leq \mu_S. \tag{5.46}$$

From (5.45) and (5.46) it follows that

$$F_S(t) \leq t/E_u, \qquad t \leq \mu_S. \tag{5.47}$$

Since μ_S is unknown, $F_S(t)$ can be bounded from above by means of E_u, which quantity can be calculated as will be shown in the following.
From (5.35) if follows that the expected number of system failures $m_{S,i}$ caused by a continuously detected component c_i in the steady state per unit of time equals

$$m_{S,i} = \frac{\lambda_i \mu_i}{\lambda_i + \mu_i} \Delta g_i, \tag{5.48}$$

supposing that the repairtime of component c_i is negative exponentially distributed. Barlow and Proschan [22] show that (5.48) also holds for repairtime distributions with non-increasing repair rates.
The average number of system failures m_S per unit of time in the steady state becomes with (5.48)

$$m_S \overset{def}{=} \lim_{t\to\infty} \frac{m_S(t)}{t} = \sum_{i=1}^{N} \frac{\lambda_i\mu_i}{\lambda_i+\mu_i} \Delta g_i, \tag{5.49}$$

N being the number of components in the system.
On the other hand (cf. Barlow and Proschan [22]),

$$m_S = \lim_{t\to\infty} \frac{m_S(t)}{t} = \frac{1}{E_u+E_d}, \tag{5.50}$$

$E_d \overset{def}{=}$ the mean repairtime of the system in the steady state.

Since the limiting system unavailability $g(\vec{q})$, (cf. (5.32)), equals

$$\frac{E_d}{E_u+E_d}, \tag{5.51}$$

it follows from (5.49), (5.50) and (5.51) that

$$E_u = \{1-g(\vec{q})\} / \sum_{i=1}^{N} \frac{\lambda_i\mu_i}{\lambda_i+\mu_i} \Delta g_i. \tag{5.52}$$

Substitution of (5.52) into (5.47) results in the Barlow-Proschan upperbound for the first system lifetime distribution $F_S(t)$

$$F_S(t) \leq \frac{t}{1-g(\vec{q})} \sum_{i=1}^{N} \frac{\lambda_i\mu_i}{\lambda_i+\mu_i} \Delta g_i, \qquad t \leq \mu_S. \tag{5.53}$$

5.3.3.7. An upperbound for the system lifetime distribution suggested by Caldarola

Caldarola [24] suggests an upperbound for the first system lifetime distribution $F_S(t)$ based on the lifetime distribution of the minimal cut sets of system S. So denote by $\underline{b}_j$ the first lifetime of minimal cut set M_j, $j=1,\ldots,N_c$, N_c being the number of minimal cut sets in the system.
Let $D_j(t)$ be the distribution function of $\underline{b}_j$, $j=1,\ldots,N_c$.
The system survives the time interval $[0,t]$ if each minimal cut set survives this interval. Therefore the following relation holds

$$1-F_S(t) = \Pr\{\underline{b}_1>t,\ \underline{b}_2>t,\ldots,\ \underline{b}_{N_c}>t\}$$

$$= \Pr\{\underline{b}_1>t\} \prod_{j=2}^{N_c} \Pr\{\underline{b}_j>t \mid \underline{b}_1>t,\ldots,\underline{b}_{j-1}>t\}$$

$$\geq \prod_{j=1}^{N_c} \Pr\{\underline{b}_j>t\} = \prod_{j=1}^{N_c} [1-D_j(t)], \qquad t\geq 0. \tag{5.54}$$

The inequality sign in (5.54) is correct because the probability of survival of $[0,t]$ by minimal cut set M_j is the product of the survival probabilities of each of the components contained in M_j; if M_j shares components with $M_1,\ldots,M_{j-1}$, then we know that these components survive $[0,t]$ with certainty. So the conditional probabilities in (5.54) are greater or equal to the marginal probabilities.
Relation (5.54) can be written as

$$F_S(t) \leq 1 - \prod_{j=1}^{N_c} [1-D_j(t)], \qquad t\geq 0. \tag{5.55}$$

From (5.55) we see that the system lifetime distribution is bounded from above, and that the upperbound is completely determined by the lifetime distribution $D_j(t), j=1,\ldots,N_c$, of the minimal cut set M_j of the system. By Caldarola [24] a method is introduced to calculate the distribution function $D_j(t)$ of minimal cut set M_j. His method exists in solving a set of integral equations for the density functions $d_j(t)$ of $D_j(t)$,

$$d_j(t) = \frac{dD_j(t)}{dt}, \qquad t\geq 0, j=1,\ldots,N. \tag{5.56}$$

In the following we shall outline his idea for the calculation of $d_j(t)$, from which by integration $D_j(t)$ is determined.
Consider minimal cut set M_j (which may be considered as a parallel working system) with structure function $\underline{\psi}_j$ (cf. (5.2)) and first lifetime distribution $D_j(t)$. Suppose that all components of M_j are in the function state at $t=0$, however, this assumption is not essesntial but it simplifies the analysis.
We can write for the unavailability of M_j at time t

$$\Pr\{\underline{\psi}_j(t)=1\} = \int_0^t \Pr\{\underline{\psi}_j(t)=1, \tau \leq \underline{b}_j < \tau+d\tau\}$$

or

$$\Pr\{\underline{\psi}_j(t)=1\} = \int_0^t \Pr\{\underline{\psi}_j(t)=1 \,|\, \underline{b}_j=\tau\} d_j(\tau)d\tau \ , \qquad t\geq 0, \tag{5.57}$$

$\underline{b}_j$ the first lifetime of minimal cut set M_j.
Suppose system S, and therefore every minimal cut set of the system, consists of class 1 components (cf. section 2.5.), class 2 components with negative exponential repairtime distributions and/or components that are characterized by an arbitrary lifetime distribution and that are inspected at regular intervals; also it is assumed that these components are renewed at the moment of inspection. If the above mentioned types of components are present in M_j, then Caldarola [24] proves

$$\Pr\{\underline{\psi}_j(t)=1 \,|\, \underline{b}_j=\tau\} = \Pr\{\underline{\psi}_j(t)=1 \,|\, \underline{\psi}_j(\tau)=1\} \ , \qquad t>\tau\geq 0. \tag{5.58}$$

Note that if relation (5.58) is fulfilled, the system behaviour at time t is *only* dependent on the state of the system *at* time $\tau<t$ and *not* dependent on the *history before* instant τ, i.e. not dependent on the interval $[0,\tau]$. Therefore the unavailability $v_j(t)$ of minimal cut set M_j at time t in (5.57) becomes with (5.58)

$$v_j(t) = \int_0^t v_{1,j}(\tau,t) d_j(\tau)d\tau \ , \qquad t\geq 0, \tag{5.59}$$

$$v_j(t) \stackrel{\text{def}}{=} \Pr\{\underline{\psi}_j(t)=1\} \ , \qquad t\geq 0, \tag{5.60}$$

$$v_{1,j}(\tau,t) \stackrel{\text{def}}{=} \Pr\{\underline{\psi}_j(t)=1 \,|\, \underline{\psi}_j(\tau)=1\} \ , \qquad t>\tau\geq 0. \tag{5.61}$$

Caldarola [24] now calculates $v_j(t)$ and $v_{1,j}(\tau,t)$ and then solves the integral equation (5.59) with respect to $d_j(t)$. After that $D_j(t)$ is determined from $d_j(t)$ by integration. So, for every minimal cut set M_j of the system, its first lifetime distribution $D_j(t)$ is calculated, and the upperbound for the system lifetime distribution $F_S(t)$ in (5.55) is calculated.

5.3.4. Measures of importance of primary events and minimal cut sets

The total system unavailability is composed of the unavailabilities of the components or of that of groups of components. From the design as well as from the operational point of view it is important to know which component or groups of components make the larger contribution to the system unavailability. It is this question which will be discussed in the present section. The influence of a component or of a group of components will be indicated by a so-called "measure of importance". There are various definitions possible for this measure, and the more important ones will be discussed below. Usually such a measure of importance of a component is based on the component's unavailability and on the component's function in the total system behaviour. The knowledge of the measure of importance is of great value in the design phase of the system as well as for the maintenance of the system. Namely, knowledge of these measures may give clues for improving the system design e.g. by eliminating components or groups of components with a too high unavailability or by rearranging them into a structure with a better measure of importance.
Maintenance schedules for systems can be optimized by constructing repair checklists based on the measure of importance of components and/or subsystems.

Another application of the measure of importance arises in the field of fault location. By means of the measure of importance for a component those components can be detected whose locations are appropriate for applying a passive sensor, which accelerates fault detection if a system failure occurs, see Lambert [11].

Birnbaum (1969) seems to be the first investigator who introduced the concept of measure of importance. After him Vesely (1971) defined another concept of measure of importance, later also described by Fussell (1975). In all these definitions the system is considered at one time moment, its history is not explicitly incorporated. The first definition of a measure of importance incorporating the behaviour of components which fail sequentially in time is due to Barlow and Proschan (1974); also Lambert (1975) developed such a definition. The ranking of components by means of their measures of importance is from large values to small values, i.e. a component which contributes more to system failure (has higher measure of importance) is placed before a component that has a

lower contribution to system failure (has smaller measure of importance). In section 5.3.4.1. the measures of importance for components are discussed, whereas in section 5.3.4.2. a description is given of the measures of importance for minimal cut sets. It is important to mention that both measures of importance can be divided into two groups, i.e. (i) each measure gives information about a component or minimal cut set at an instant of time, which implies that these measures do not contain information about the foregoing history of the system, and secondly (ii) each measure contains also information about the way system failure occurs sequentially in time. In section 5.3.4.3. applications and use of measures of importance are discussed, and suggestions are given about the use of the appropriate measure of importance. Finally all measures of importance treated are summarized in table 5.3. at the end of this chapter.
During the discussion of the measures of importance some applications are shown in connection with the electrical system of fig. 5.3, a system with continuously inspected components (see section 2.5.). The failure rates and repair rates of the components of this system are tabulated in the subjoined table 5.2. All these values are fictitious and no practical meaning should be given to them. They are chosen in this way for the sake of demonstration.

TABLE 5.2. Failure rates and repair rates of the components of the electrical system in fig. 5.3.

Component	Failure rate (λ/year)	Repair rate (μ/year)
R_1	0.1	1.0
R_2	0.111	1.5
R_3	0.125	1.2
R_4	0.143	2.0
R_5	0.167	1.33

5.3.4.1. Measures of importance for components

5.3.4.1.1. Birnbaum's measure of importance

Birnbaum (1969) seems to be the first investigator who introduced the concept of "measure of importance". As such he defined the "reliability importance" $B_i(t)$ of component c_i. For $B_i(t)$ he took

$$B_i(t) \stackrel{\text{def}}{=} \frac{\partial g(\vec{q}(t))}{\partial q_i(t)} = g(1_i,\vec{q}(t)) - g(0_i,\vec{q}(t)),$$

$$t\geq 0,\ i=1,\ldots,N, \qquad (5.62)$$

with $q_i(t)$ defined by (5.10) and the right hand side of (5.62) defined by (5.20).

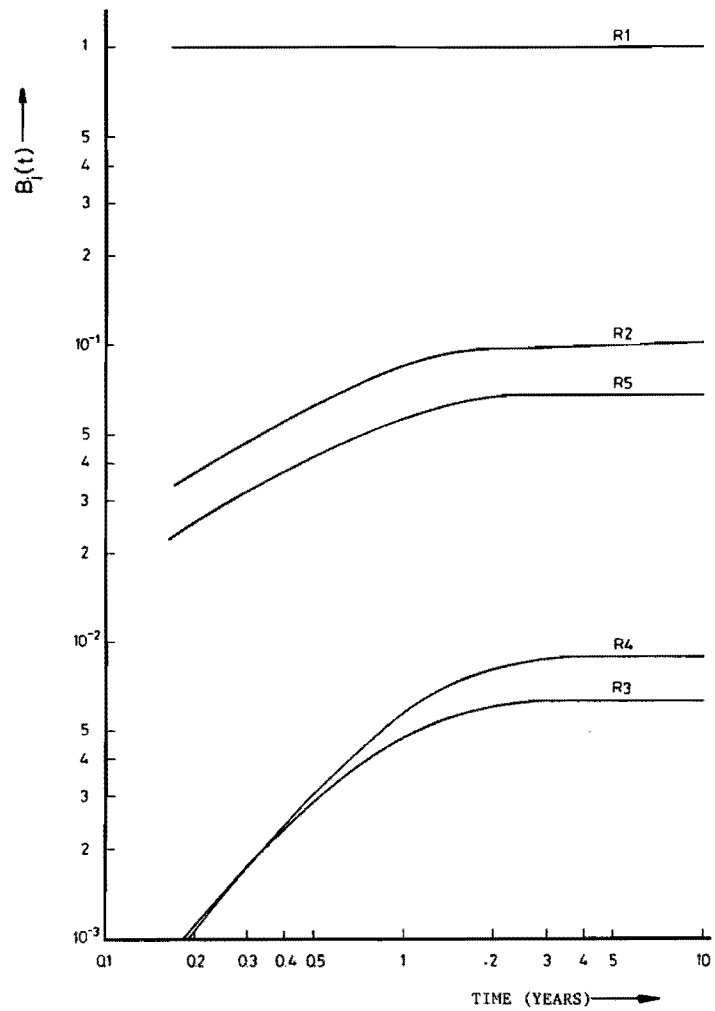


FIG. 5.6 BIRNBAUM 's MEASURE OF IMPORTANCE $B_i(t)$ FOR COMPONENTS

From this definition it is seen that Birnbaum's reliability importance is the ratio of the change in system reliability versus the component reliability, i.e. it is the probability that component c_i is critical at instant t.
Applying table 5.2. (see section 5.3.4.) Birnbaum's measure of importance for the components $R_1,\ldots,R_5$ of the system of fig. 5.3. are presented in fig. 5.6. From this figure it is seen that component R_1 is the most critical one in connection with system failure. This agrees with the intuitive feeling that a single component in series with the rest of the system must be an important component. Therefore this component deserves special attention. The measure of importance for the components R_2 and R_5 are about the same and are about a decade smaller than that of R_1.
Components R_3 and R_4 are the least important ones.
Their measures of importance are about two decades smaller than that of R_1.

5.3.4.1.2. Vesely-Fussell's measure of importance

Denote by $y_i(\vec{\underline{x}}(t))$ the structure function (see (5.7)) of the union of all minimal cut sets of the system containing component c_i. This means that $y_i(\vec{\underline{x}}(t))=1$ if and only if $\underline{x}_i(t)=1$ ($\underline{x}_i(t)$ being the state variable of component c_i at instant t), i.e. the union of all minimal cut sets containing component c_i occurs if and only if component c_i is in the fail state at epoch t. The probability that component c_i contributes to system failure is

$$g_i(\vec{q}(t)) \stackrel{def}{=} \Pr\{y_i(\vec{\underline{x}}(t))=1\}\ , \quad t\geq 0. \tag{5.63}$$

The contribution of component c_i to system failure, given that the system is in the fail state at instant t, the so-called "Vesely-Fussell measure of importance" $V_i(t)$ for component c_i, is defined by

$$\begin{aligned} V_i(t) &\stackrel{def}{=} \Pr\{\text{component } c_i \text{ contributes to system failure at instant } t \mid \text{the system is in the fail state at instant } t\} \\ &= \Pr\{y_i(\vec{\underline{x}}(t))=1 \mid y(\vec{\underline{x}}(t))=1\} \\ &= \frac{\Pr\{y_i(\vec{\underline{x}}(t))=1\}}{\Pr\{y(\vec{\underline{x}}(t))=1\}} = \frac{g_i(\vec{q}(t))}{g(\vec{q}(t))} \quad , \quad t\geq 0,\ i=1,\ldots,N \end{aligned} \tag{5.64}$$

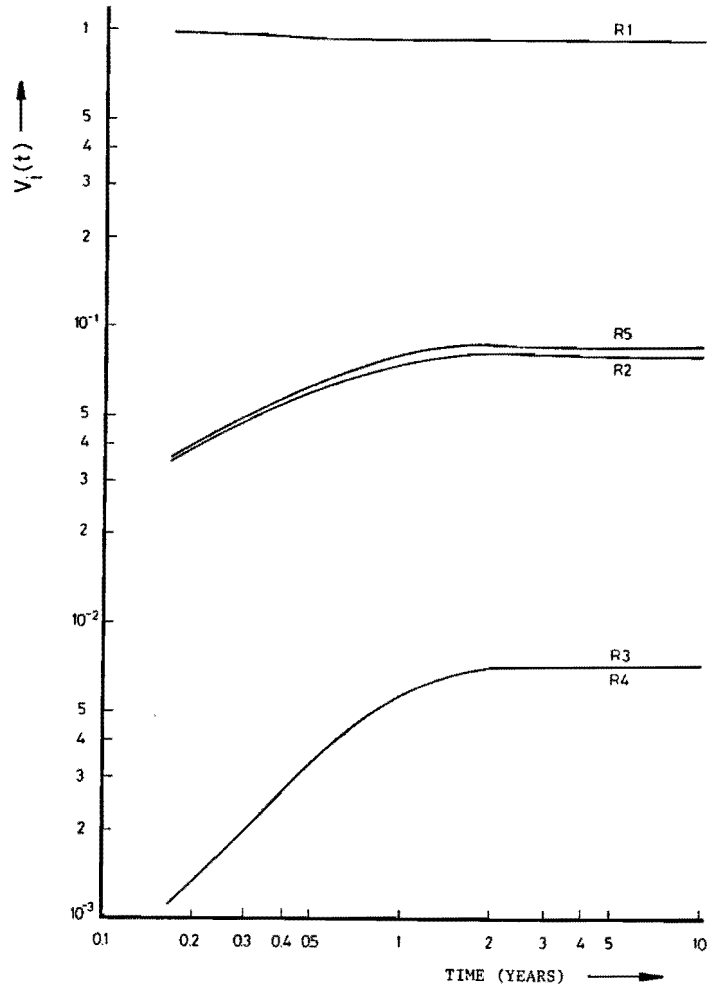


FIG. 5.7. VESELY-FUSSELL 's MEASURE OF IMPORTANCE $V_i(t)$ FOR COMPONENTS

In fig. 5.7. the Vesely-Fussell's measures of importance for the components $R_1,\ldots,R_5$ of the system in fig. 5.3. are shown; the numerical input is taken from table 5.2. (see section 5.3.4.).

5.3.4.1.3. Criticality importance

From Birnbaum's measure of importance it is possible to derive another measure of importance, called "criticality importance". In fact criticality importance for component c_i is the conditional probability that component c_i causes system failure at instant t, given that the system has failed at epoch t, i.e. component c_i is critical at instant t *and* component c_i has failed by time t given system failure at instant t.

Denote by $K_i(t)$ the criticality importance for component c_i, then it follows that

$$K_i(t) \stackrel{def}{=} \Pr\{\text{component } c_i \text{ critical at instant } t, \text{ component } c_i \text{ failed by instant } t \mid \text{system failed at instant } t\}.$$

Because the event "component c_i critical at instant t, component c_i failed by time t" implies the event "system failed by time t", the above expression becomes

$$K_i(t) = \frac{\Pr\{\text{component } c_i \text{ critical at instant } t, \text{ component } c_i \text{ failed by time } t\}}{\Pr\{\text{system failed at instant } t\}}$$

$$= \frac{\{g(1_i,\vec{q}(t)) - g(0_i,\vec{q}(t))\}\, q_i(t)}{g(\vec{q}(t))}, \quad t\geq 0, i=1,\ldots,N, \qquad (5.65)$$

the numerator being the product of the probabilities of the events "component c_i critical at instant t" and "component c_i failed by instant t" (see section 5.3.3.1.).

In the case that component c_i is element of every minimal cut set of the system $K_i(t) = V_i(t)$, since in this case

$$g(0_i,\vec{q}(t)) = g_i(0_i,\vec{q}(t)) = 0,$$

$$g(1_i,\vec{q}(t)) = g_i(1_i,\vec{q}(t))\, q_i(t) = g_i(\vec{q}(t)),$$

the Vesely-Fussell measure of importance

$$V_i(t) = \frac{g_i(\vec{q}(t))}{g(\vec{q}(t))},$$

is obtained.

In fig. 5.8. the criticality importance for the components $R_1,\ldots,R_5$, of the system in fig. 5.3. are shown. The numerical input is taken from table 5.2. (see section 5.3.4.).

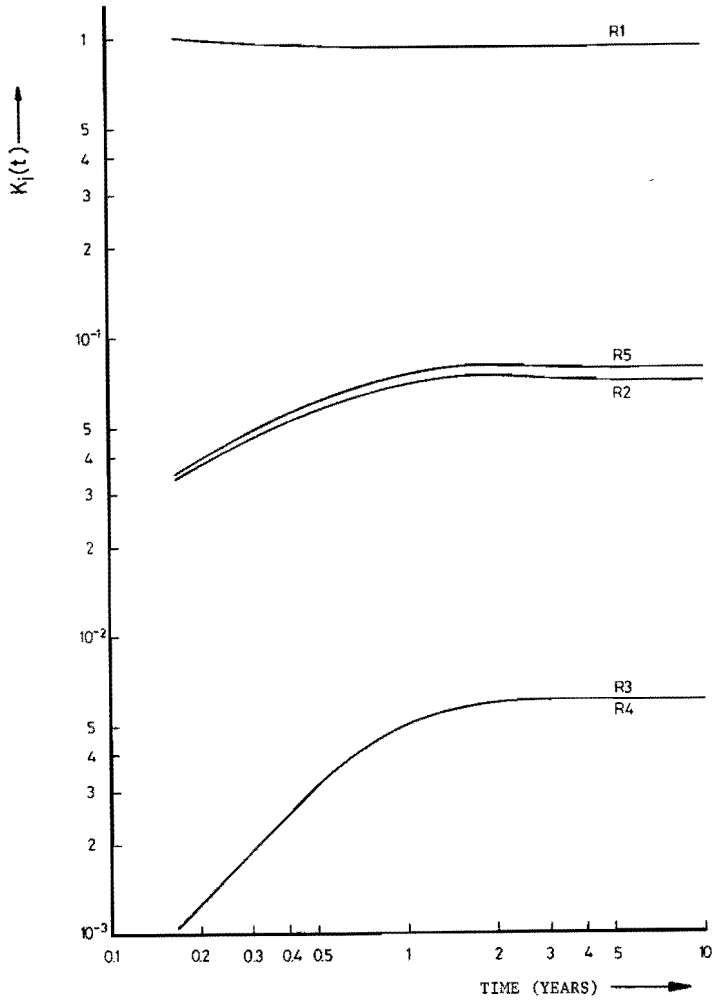


FIG. 5.8. CRITICALITY IMPORTANCE K_i (t) FOR COMPONENTS

5.3.4.1.4. Barlow-Proschan's measure of importance

The foregoing measures of importance have been calculated at the instant t without using any information about system performance before t in so far this information can not be deducted from the fail state at instant t. The present section and the following section treat measures of importance for components such that component behaviour sequentially in time is incorporated, i.e. we consider the measure of importance for component c_i at instant t by taking into account the behaviour of this component during [0,t].

The probability that component c_i causes system failure in the small interval (t,t+dt) is equal to the product of the probabilities that component c_i is critical at instant t and that it fails in (t,t+dt):

$$\{g(1_i,\vec{q}(t)) - g(0_i,\vec{q}(t))\}\, dm_i^+(t) \quad , \quad t\geq 0, i=1,\ldots,N, \tag{5.66}$$

g(.) being the system unavailability and

$$m_i^+(t) \stackrel{def}{=} \begin{cases} (\text{i}) & \text{the lifetime distribution for non-repairable components;} \\ (\text{ii}) & \text{the renewal function (see chapter 3) for continuously inspected and randomly inspected components;} \\ (\text{iii}) & \text{the residual lifetime distribution (see chapter 3) for periodically inspected components.} \end{cases} \tag{5.67}$$

In fact (5.66) expresses the average number of system failures in (t,t+dt) caused by component c_i (see section 5.3.3.1.). The average number of system failures in [0,t] caused by component c_i then reads:

$$\int_{\tau=0}^{t} \{g(1_i,\vec{q}(\tau))-g(0_i,\vec{q}(\tau))\}dm_i^+(\tau) \quad , \quad t\geq 0, i=1,\ldots,N. \tag{5.68}$$

Because the expression in (5.68) may become greater than one, it is normed to one by division through the average number of system failures (not only caused by component c_i) in [0,t], $m_S(t)$ (see section 5.3.3.1.).
The result $P_i(t)$ is called the "Barlow-Proschan measure of importance" for component c_i:

$$P_i(t) = \frac{\int_{\tau=0}^{t} \{g(1_i,\vec{q}(\tau))-g(0_i,\vec{q}(\tau))\}dm_i^+(\tau)}{m_S(t)} \quad , \quad t\geq 0;\ i=1,\ldots,N. \tag{5.69}$$

Remark: If the system S contains only non-repairable components, then $P_i(t)$ represents the probability that component c_i causes system failure in [0,t] given system failure at instant t.

In fig. 5.9. Barlow-Proschan's measures of importance for the components of the system in fig. 5.3. with input data from table 5.2. (see section 5.3.4.) are represented.

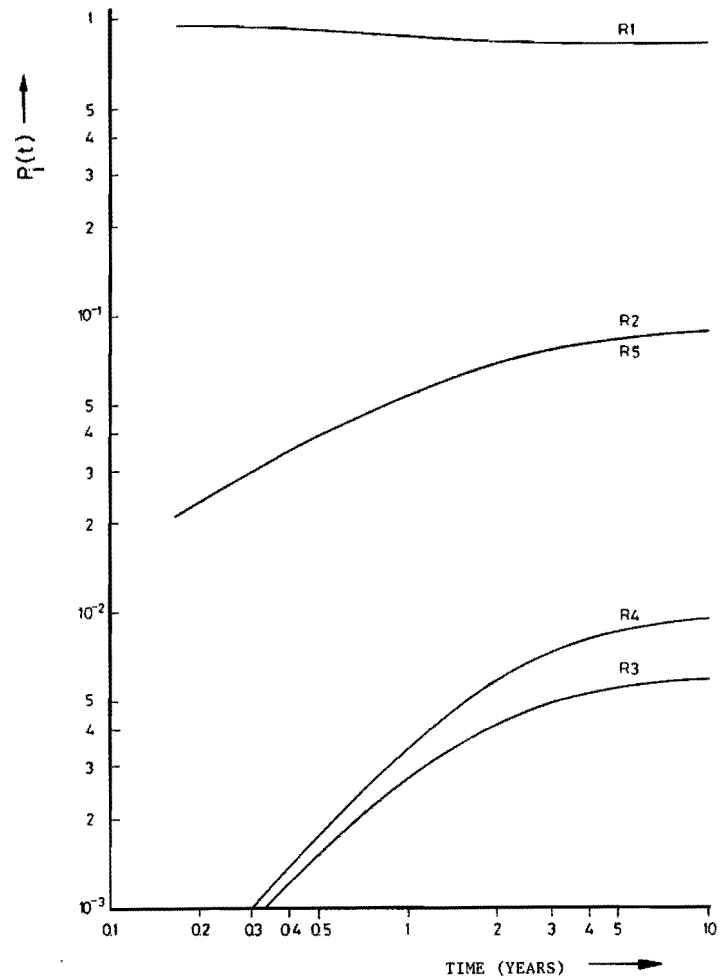


FIG. 5.9 BARLOW-PROSCHAN 's MEASURE OF IMPORTANCE P_i (t) FOR COMPONENTS

5.3.4.1.5. Sequential contributory measure of importance

Passive sensors are sometimes introduced to detect the failure of a component, say component c_i, also if failure of c_i not necessarily implies system failure. Of course, when there is need for such a passive sensor at instant t, it means that failure of c_i brings system failure very close. It is therefore of interest to consider the contribution of component c_i to system failure actually caused by component c_j. In this section a measure for such a contribution is described.

The contribution of component c_i to the average number of system failures in (t,t+dt), when component c_i is in the fail state and component c_j causes system failure reads:

$$\{g(1_i,1_j,\vec{q}(t)) - g(1_i,0_j,\vec{q}(t))\}\, q_i(t)\, dm_j^+(t) \quad , \quad t\geq 0,$$

where $m_j^+(t)$ is defined by (5.67). The contribution of component c_i to the average number of system failures in [0,t], when system failure is caused by component c_j, then becomes:

$$\int_{\tau=0}^{t} \{g(1_i,1_j,\vec{q}(\tau)) - g(1_i,0_j,\vec{q}(\tau))\}\, q_i(\tau)\, dm_j^+(\tau) \quad , \quad t\geq 0.$$

The contribution of component c_i to the average number of system failures in [0,t], when system failure is not caused by component c_i, is:

$$\sum_{\substack{j\in H_i \\ j\neq i}} \int_{\tau=0}^{t} \{g(1_i,1_j,\vec{q}(\tau))-g(1_i,0_j,\vec{q}(\tau))\}\, q_i(\tau)\, dm_j^+(\tau) \quad , \quad t\geq 0, \quad (5.70)$$

here H_i is the set of all components appearing at least once in a minimal cut set containing component c_i.
Dividing the expression in (5.70) by the average number of system failures $m_S(t)$ in [0,t] we get the so-called sequential contributory measure of importance $Q_i(t)$ for component c_i:

$$Q_i(t) \overset{\text{def}}{=} \sum_{\substack{j\in H \\ j\neq i}} \frac{\int_{\tau=0}^{t} \{g(1_i,1_j,\vec{q}(\tau))-g(1_i,0_j,\vec{q}(\tau))\}q_i(\tau)dm_j^+(\tau)}{m_S(t)} \quad , \quad (5.71)$$

$$t\geq 0;\ i=1,\ldots,N.$$

Remark: If the system contains only non-repairable components, then $Q_i(t)$ represents the probability that component c_i is contributing to system failure when another component causes the system to fail, given that the system is failed at instant t.

5.3.4.1.6. Barlow-Proschan's steady state measure of importance

Suppose that the system is composed of only continuously detected components. The stochastic process describing the reliability behaviour of such a component may be in the long run, i.e. for large values of t, very well approximated by a stationary process. It will be assumed that the

reliability behaviour of all components and also for the total system may be described by a stationary stochastic process. For this assumption the unavailability for each component c_i is then a constant, i.e. $q_i=\lambda_i/(\lambda_i+\mu_i)$ (cf. (5.32)).
For this steady state situation it is possible to construct a time invariant "measure of importance" for components. The average number of system failures in $(t,t+\Delta t)$ caused by component c_i is (analogous to section 5.3.4.1.4.):

$$m_{S,i}(0,t+\Delta t)-m_{S,i}(0,t) = \int_{\tau=t}^{t+\Delta t} \{g(1_i,\vec{q}(\tau))-g(0_i,\vec{q}(\tau))\}dm_i(\tau), \quad t\geq 0,\tau\geq 0, \tag{5.72}$$

$m_{S,i}(0,t)$ being defined in section 5.3.3.3. and $m_i(t)$ being defined in section 3.3.1. Because of the steady state assumption $q_i(t)$ is independent of t and $dm_i(t) = \lambda_i\, dt/(\lambda_i+\mu_i)$ so that relation (5.72) becomes

$$m_{S,i}(\Delta t) = \{g(1_i,\vec{q})-g(0_i,\vec{q})\}\,\frac{\lambda_i\mu_i}{\lambda_i+\mu_i}\,\Delta t,\ \Delta t\geq 0,\ i=1,\ldots,N, \tag{5.73}$$

$\vec{q}$ being defined by (5.32).
The average number of system failures $m_S(t,t+\Delta t)$ in the time interval $(t,t+\Delta t)$ is obtained by taking the sum over all components contained in the system and hence

$$m_S(\Delta t) \overset{\text{def}}{=} \lim_{t\to\infty} m_S(t,t+\Delta t)$$

$$= \sum_{j=1}^{N} \{g(1_j,\vec{q})-g(0_j,\vec{q})\}\,\frac{\lambda_j\mu_j}{\lambda_j+\mu_j}\,\Delta t,\ \Delta t\geq 0. \tag{5.74}$$

The ratio R_i of the average number of system failures caused by component c_i (cf. (5.73)) and the average number of system failures (cf. (5.74)), is called the "steady state Barlow-Proschan measure of importance" for component c_i:

$$R_i = \frac{\{g(1_i,\vec{q})-g(0_i,\vec{q})\}/(1/\lambda_i+1/\mu_i)}{\sum_{j=1}^{N} \{g(1_j,\vec{q})-g(0_j,\vec{q})\}/(1/\lambda_j+1/\mu_j)},\ i=1,\ldots,N. \tag{5.75}$$

5.3.4.1.7. Lambert's measure of importance

For the calculation of each of the foregoing measures of importance for components the "absolute" values of the failure rates of the components are needed. These values are not always available, and if available only known within a certain confidence interval. Lambert [11] has developed a measure of importance which for its application does not need the "absolute" values of the failure rate but their ratio's. Frequently these ratio's are easier to obtain. Lambert claims that this measure of importance is more sensitive than the above mentioned measures of importance. The method has a restriction viz. it can be applied only to systems that are composed of non-repairable components with lifetime distributions belonging to a certain class; the latter requirement implies that component failure rates are proportional to each other (see below).
The requirement concerning the lifetime distribution means that for every component c_i its lifetime distribution can be written as

$$F_i(t) = 1 - e^{-R(t)\xi_i}, \quad i=1,\ldots,N, \tag{5.76}$$

with ξ_i independent of t, $t \geq 0$.
From (5.76) it is seen that

$$\xi_i = \int_{\tau=0}^{t} \lambda_i(\tau)d\tau/R(t), \tag{5.77}$$

with $\lambda_i(t)$ the failure rate of $F_i(t)$, i.e.

$$\lambda_i(t) = \frac{\frac{d}{dt}F_i(t)}{1-F_i(t)} . \tag{5.78}$$

We now take some component, say j, as the reference component, and note that it follows from (5.76):

$$e^{-R(t)} = \{1-F_j(t)\}^{1/\xi_j}, \quad j=1,\ldots,N. \tag{5.79}$$

It is seen because the ξ_i are time independent that

$$\frac{\xi_i}{\xi_j} = \frac{\int_{\tau=0}^{t} \lambda_i(\tau)d\tau/R(t)}{\int_{\tau=0}^{t} \lambda_j(\tau)d\tau/R(t)}$$

$$= \frac{\ln\{1-F_i(t)\}}{\ln\{1-F_j(t)\}} . \qquad (5.80)$$

This ratio will be denoted by χ_i, i.e.

$$\chi_i = \frac{\xi_i}{\xi_j} , \quad i=1,2,\ldots,N. \qquad (5.81)$$

Hence we may write, see (5.80)

$$F_i(t) = 1-\{1-F_j(t)\}^{\chi_i} , \quad i=1,2,\ldots,N, \qquad (5.82)$$

χ_i being the so-called *proportional hazard*.
Note that the proportional hazard for component c_j (the referent component) equals one, i.e. $\chi_j=1$.

Obviously the class of distribution functions as introduced by Lambert is fully specified by the failure distribution of the reference component and the proportional hazards $\chi_1,\ldots,\chi_N$.
Hence it follows that the system unavailability $g(\vec{F}(t))$ can be written as a function of the variables $F_j(t)$ and $\chi_1,\ldots,\chi_N$:

$$g(\vec{F}(t)) = g(F_j(t),\vec{\chi}), \qquad (5.83)$$

$$\vec{\chi} \stackrel{\text{def}}{=} (\chi_1,\ldots,\chi_N) . \qquad (5.84)$$

Lambert's measure of importance $S_i(t)$, in Lambert [11] called the *upgrading function*, is now defined by

$$S_i(t) = \frac{\partial g(F_j(t),\vec{\chi})}{g(F_j(t),\vec{\chi})} \Bigg/ \frac{\partial \chi_i}{\chi_i}$$

$$= \frac{\chi_i}{g(F_j(t),\vec{\chi})} \frac{\partial g(F_j(t),\vec{\chi})}{\partial \chi_i} \quad , \quad i=1,2,\ldots,N; \quad t\geq 0. \qquad (5.85)$$

It obviously measures the change in the probability of the top event relative to the change in the proportional hazard.

5.3.4.2. Measures of importance for minimal cut sets

5.3.4.2.1. Barlow-Proschan's measure of importance

A minimal cut set occurs at instant t if all but one component have been failed before instant t and the component, that has not been failed by instant t, fails in the small interval (t,t+dt).
Suppose that minimal cut set K_j of the system occurs at instant t and suppose that component $c_i \in K_j$ is the last component that fails. Then the elementary probability of occurrence $p_j^{(i)}(t)$ of minimal cut set K_j at instant t reads:

$$p_j^{(i)}(t) = \left[\prod_{\substack{\ell \in K_j \\ \ell \neq i}} q_\ell(t) \right] dm_i^+(t) \quad , \quad t\geq 0, \qquad (5.86)$$

$m_i^+(t)$ defined by (5.67).

The probability $\Delta k_j^{(i)}(t)$ that minimal cut set K_j is critical at instant t with respect to component c_i, i.e. component c_i fails as the last component of minimal cut set K_j, is defined analogous to that of a component (cf. (5.5)):

$$\Delta k_j^{(i)}(t) = g(1^{K_j}, \vec{q}(t)) - g(0_i, 1^{K_j-\{i\}}, \vec{q}(t)) \quad , \quad t\geq 0. \qquad (5.87)$$

In (5.87) 1^{K_j} means that all components of minimal cut set K_j are in the fail state at instant t, whereas $1^{K_j-\{i\}}$ indicates that all components except component c_i of minimal cut set K_j are in the fail state at instant t.

Obviously

$$g(1^{K_j}, \vec{q}(t)) = 1, \tag{5.88}$$

because minimal cut set K_j occurs and by definition then the top event occurs with certainty.
The average number of system failures caused by minimal cut set K_j in (t,t+dt) is the product of the probabilities of the events "minimal cut set K_j is critical at instant t" and "minimal cut set K_j occurs in the small time interval (t,t+dt)" (cf. (5.22) in the case of a single component).
Therefore we obtain for the average number of system failures in (t,t+dt) caused by minimal cut set K_j, applying (5.86) and (5.87):

$$\sum_{i \in K_j} \Delta k_j^{(i)}(t)\, p_j^{(i)}(t) \quad , \quad t \geq 0. \tag{5.89}$$

It follows from (5.89) that the average number of system failures in [0,t], caused by minimal cut set K_j, equals

$$\sum_{i \in K_j} \int_{\tau=0}^{t} \Delta k_j^{(i)}(\tau)\, p_j^{(i)}(\tau) \quad , \quad t \geq 0. \tag{5.90}$$

Normalizing the expression in (5.90) by the average number of system failures $m_S(t)$ in (0,t), i.e. dividing it by $m_S(t)$, and substituting (5.86), (5.87) and (5.88) into (5.90), we get Barlow-Proschan's measure of cut set importance $BP_j(t)$ for minimal cut set K_j:

$$BP_j(t) = \frac{\sum_{i \in K_j} \int_{\tau=0}^{t} \{1 - g(0_i, 1^{K_j - \{i\}}, \vec{q}(\tau))\} \prod_{\substack{\ell \in K_j \\ \ell \neq i}} q_\ell(\tau)\, dm_i^+(\tau)}{m_S(t)} \quad , \tag{5.91}$$

$$j = 1, \ldots, N_c; \quad t \geq 0,$$

N_c (cf. (5.6)) being the number of minimal cut sets of the system.
In fig. 5.10., $BP_j(t)$ is represented for the minimal cut sets K_1, K_2 and K_3 (cf. table 5.1.) of the electrical network of fig. 5.3.; the input data for the components are taken from table 5.2. (see section 5.3.4.).

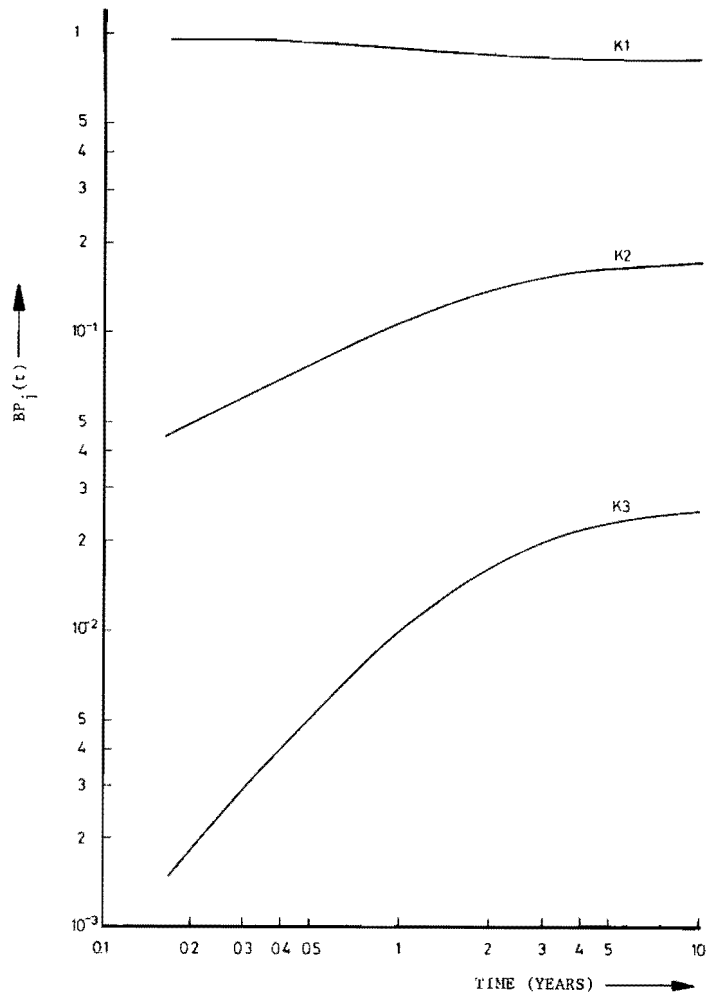


FIG. 5.10 BARLOW-PROSCHAN 's MEASURE OF IMPORTANCE BP_j (t) FOR MINIMAL CUT SETS

It is seen from fig. 5.10. that there is a great difference in importance between the minimal cut sets K_1, K_2 and K_3. Obviously K_1 is the most important one between them. The second one in importance is minimal cut set K_2. The least important one is minimal cut set K_3. The reason for these differences is the different order of the cut set. Minimal cut set K_1 is identical to component R_1, i.e. K_1 is a cut set of order one. Therefore if component R_1 fails then the system fails. Minimal cut set K_2 is composed of two components, i.e. component R_2 and component R_5, and is therefore a cut set of order two. System failure caused by minimal cut set K_2 means that both components R_2 and R_5 have to be failed.

Intuitively it is felt that the minimal cut set K_1 is more dangerous to the system than minimal cut set K_2. From fig. 5.10. it is seen that the measure of importance confirms this feeling.
The same reasoning can be applied with respect to minimal cut set K_3.

5.3.4.2.2. Vesely-Fussell's measure of importance

Taking the ratio $VF_j(t)$ of the probability of occurrence of minimal cut set K_j at instant t and the system unavailability at instant t, we get the so-called Vesely-Fussell measure of importance for minimal cut set K_j:

$$VF_j(t) = \frac{\prod_{i \in K_j} q_i(t)}{g(\vec{q}(t))}, \quad t>0;\ j=1,\ldots,N_c. \tag{5.92}$$

Note that $g(\vec{q}(t))>0$ for $t>0$.

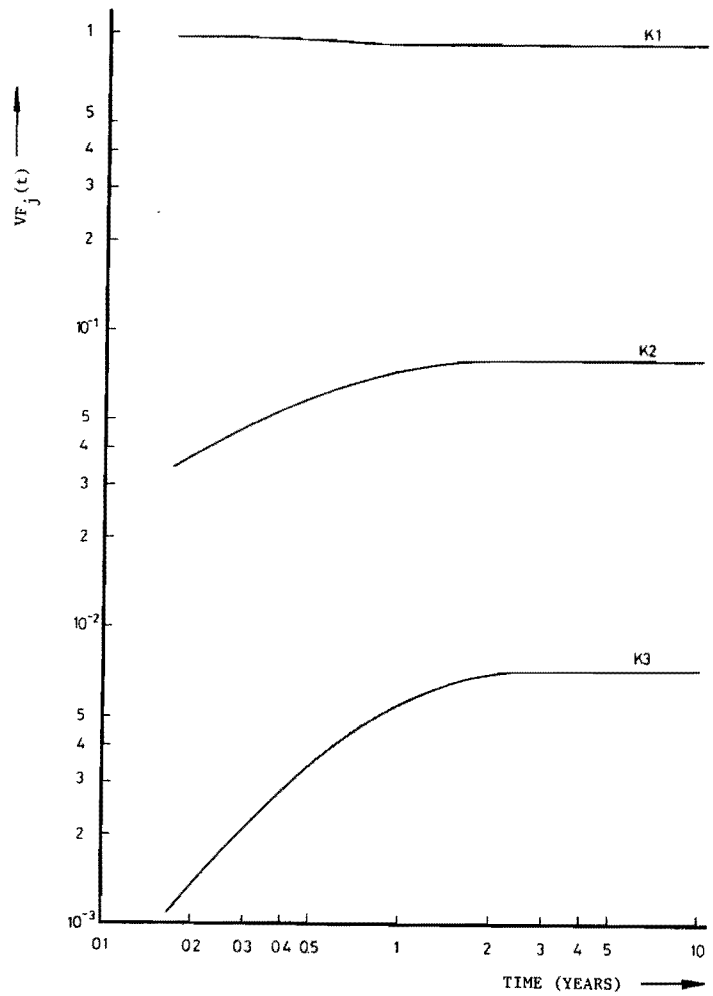


FIG. 5.11 VESELY-FUSSELL's MEASURE OF IMPORTANCE $VF_j(t)$ FOR MINIMAL CUT SETS

The Vesely-Fussell measures of importance for the minimal cut sets K_1, K_2 and K_3 of the electrical network in fig. 5.3. are shown in fig. 5.11; the component input data is taken from table 5.3. (see section 5.3.4.).

5.3.4.3. The application and the use of measures of importance

The use of measures of importance is two-fold, viz.
- to trace the weak points in a system (design),
- to obtain indications for system (design) upgrading.

The use of measures of importance, as well for components as for minimal cut sets, is in general not always simple. In each specific case it has to be clear for which purpose the measure of importance should be applied. In most cases the result will be the same irrespective of which measure of importance is used.It is very difficult to point out according to logical considerations which measure should be used for a particular situation; therefore in most cases the choice is rather intuitive. Nevertheless we shall discuss in the following a few particular situations and we shall try to give some suggestions for the use of the appropriate measure of importance.

5.3.4.3.1. Dormant systems

When a system is dormant during a time interval (cf. section 2.3.), then the measures, which are based on sequentially failing of the components in time, are not appropriate. The measures based on an instant have to be applied. The reason for this is that if a component fails (or a minimal cut set occurs) and the system is dormant at that instant, this failure will not be noticed. It will be noticed some instant later, i.e. the instant at which the system has to change from the dormant situation to the operating situation. So in this case we are not able to track the failures of components in time and therefore it is appropriate to use for dormant systems:

(i) for components
- Birnbaum's measure of importance (section 5.3.4.1.1.);
- Vesely-Fussell's measure of importance (section 5.3.4.1.2.);
- Criticality importance (section 5.3.4.1.3.);

(ii) for minimal cut sets
- Vesely-Fussell's measure of importance (section 5.3.4.2.2.).

5.3.4.3.2. Operating systems

For an operating system (cf. section 2.3.) it is possible to detect system failure immediately, because this failure terminates the functioning of the system. System failure occurs, assuming no common cause failures, if a minimal cut set occurs. The last event is caused ultimately by the failure of a component. Obviously the way the system fails in time does play a role. Therefore the sequential measures in time are the more appropriate ones to be used in this case, i.e. Barlow-Proschan's measure of importance, as well for components (section 5.3.4.1.4.) as for minimal cut sets (section 5.3.4.2.1.).

5.3.4.3.3. System design stage

During the phase that a system is in its design stage, changes in the system configuration are easily carried out. Because the system is not yet operational the measures of importance treated in section 5.3.4.3.1. can be applied. But during the design stage of a system often the characteristics of the components are not precisely known. On the other hand during the design as a rule no account is taken of repair. So Lambert's measure of component importance (section 5.3.4.1.7.) is appropriate for this situation. Lambert [11] claims that this measure is more sensitive than the other ones.

5.3.4.3.4. System in steady state conditions

If a system can be considered to be in the steady state, i.e. each component of the system is a continuously inspected component, then Barlow-Proschan's steady state measure of importance (section 5.3.4.1.6.) is recommended.

5.3.4.3.5. Optimal location of passive sensors

As described in section 5.3.4.1.5. it is possible to determine which components should be watched by a passive sensor. The ranking of the components for this option is done by the sequential contributory measure of importance (section 5.3.4.1.5.) for components. Note that this type of sensors can only be applied to systems during their operational time intervals.

5.3.4.3.6. Other applications

So far we have treated applications of measures of importance for system upgrading and location of passive sensors. Other applications can be found in:

(i) generation of repair checklists, and
(ii) simulation of system failure, by means of fault tree analysis.

The last two applications will not be treated here. For a discussion of these methods, see Lambert [11].

TABLE 5.3.

MEASURES OF IMPORTANCE OF COMPONENTS

Measures of importance of components

1. Birnbaum

$$\frac{\partial g(\vec{q}\ (t))}{\partial q_i(t)} = g\ (1_i,\vec{q}(t))-g\ (0_i,\vec{q}(t))$$

2. Criticality

$$\frac{\{g\ (1_i,\vec{q}(t))-g\ (0_i,\vec{q}(t))\}q_i(t)}{g\ (\vec{q}(t))}$$

3. Lambert

$$\frac{\chi_i}{g(F_j(t),\vec{\chi})} \cdot \frac{\partial g(F_j(t),\vec{\chi})}{\partial \chi_i}$$

4. Vesely-Fussell

$$\frac{g_i(\vec{q}(t))}{g\ (\vec{q}(t))}$$

5. Barlow-Proschan

$$\frac{\int_0^t \{g\ (1_i,\vec{q}(\tau))-g\ (0_i,\vec{q}(\tau))\}dm_i^+(\tau)}{m_S(t)}$$

6. Barlow-Proschan steady state

$$\frac{\{g\ (1_i,\vec{q})-g\ (0_i,\vec{q})\}/(1/\lambda_i+1/\mu_i)}{\sum_{j=1}^{n} \{g\ (1_j,\vec{q})-g\ (0_j,\vec{q})\}/(1/\lambda_j+1/\mu_j)}$$

7. Sequential contributory

$$\sum_{\substack{j\in H_i \\ j\neq i}} \frac{\int_0^t \{g(1_i,1_j,\vec{q}(\tau))-g(1_i,0_j,\vec{q}(\tau))\}q_i(\tau)dm_j^+(\tau)}{m_S(t)}$$

Measures of importance of minimal cut sets

1. Barlow-Proschan

$$\frac{\sum_{i\in K_j} \int_0^t \{1-g\ (0_i,1^{K_j-\{i\}},\vec{q}(\tau))\} \prod_{\substack{\ell\in K_j \\ \ell\neq i}} q_\ell(\tau)dm_i^+(\tau)}{m_S(t)}$$

2. Vesely-Fussell

$$\frac{\prod_{i\in K_j} q_i(t)}{g\ (\vec{q}(t))}$$

6. PHASED MISSION ANALYSIS

6.1. Introduction

In this chapter we shall treat phased mission analysis of maintained systems, i.e. we shall calculate the probability of mission success. The underlying methodology is fault tree analysis (cf. chapter 5). The difficulty in treating a phased mission in contrast with a single system mission is the possibility that two or more systems are dependent of each other, i.e. they share components (cf. chapter 2). In this study the dependencies between systems are fully taken into account and an exact calculation of the probability of mission success is possible, but in practical situations hampered. This is due to the large number of minimal cut sets that are contained in large and/or complex systems, which imply for the exact calculation of the probability of mission success (i) the need for an extremely large computer memory and (ii) very time consuming calculations. However, it is possible to obtain upper- and lowerbounds for the probability of mission success, with an accuracy which is sufficient for most of the practical situations encountered.
The procedure to calculate the probability of mission success is the following:

(S1) for each phase the fault tree of the associated subsystem is constructed and its minimal cut sets are determined;

(S2) the absolute and conditional component unavailabilities are evaluated;

(S3) the probability of mission success is calculated.

As stated before, upper- and lowerbounds for the probability of mission success are needed in practical situations. In this chapter, therefore, we shall present an upperbound and a lowerbound (or the difference between both bounds) for the probability of mission success.

The present model differs from the models that exist in literature. In order to be able to discuss the various approaches to the problem of phased mission analysis we summarize our model assumptions (cf. chapter 2):

(A1) it is assumed that each system is *coherent*, so that every component is relevant to the system (cf. chapter 5);

(A2) each system behaves *binary*, i.e. a system can be in one of two states: the *fail* state or the *function* state;

(A3) no repair is allowed to a system when it is *operational*, i.e. no *on-line* repair is allowed. If during certain time intervals the system is not operational, then repair may be applied;

(A4) the successive lifetimes of a component, for the case that a component is subjected to a repair policy, are assumed to be independent identically distributed variables. The same assumption is made for the successive repairtimes of a component;

(A5) the lifetimes of the various components of a system are assumed to be mutually independent stochastic variables; the same holds for the repairtimes of the various components;

(A6) each component can be in one of two states; i.e. the *fail* state or the *function* state;

(A7) it is assumed that when repair has been finished for a component the component is as good as new and starts a new life.

Note that assumption (A5) with respect to the different repairtimes of the components implies that it is assumed that *multiple repair* is applied to the components, i.e. if a component fails or is detected to be failed then repair starts immediately for that component, despite the fact that perhaps other components are also under repair.

In literature phased mission analysis models have been treated by Ziehms [15] (and Esary), Bell [1], Clarotti et al [26] and Fussell [27]. We shall now discuss these models concerning the assumptions made, the mutual differences and the capability of the models.

(B1) All the authors apply (implicitly or explicitly mentioned) the assumptions (A1),...,(A7). With respect to the repair policies, viz. assumption (A3), the authors treat mutually different models:
Ziehms assumes that all components are class 1 (non-repairable) components.
Bell treats class 1 (non-repairable) and class 2 (continuously inspected) components during the OR-phase and assumes that during the mission itself all components are non-repairable.
Clarotti applies component models during the OR-phase as well as during

the mission itself which are not clearly specified, i.e. class 1 (non-repairable) components and repairable components are mentioned, but the nature of fault detection is not specified.
He assumes that repair is applied during the dormant time interval of a component as well as during the operational part, i.e. *on-line* repair.
Fussell, finally, treats class 1 (non-repairable) and class 2 (continuously inspected) components during the OR-phase as well as during the mission itself, i.e. he also applies *on-line* repair. He also introduces another class of components, viz. components that can be instantaneously inspected and repaired at the phase-boundaries, i.e. at the epochs $T_j, j=1,\ldots,K-1$, (K being the number of phases) at which the phase of subsystem S_j terminates and that of subsystem S_{j+1} starts.

(B2) The present study as well as the other models assume fixed phase duration times, i.e. the times $T_j-T_{j-1}, j=1,\ldots,K$, are *deterministic* variables and not *stochastic* variables.
(For a discussion of this subject see chapter 8).

(B3) The present study as well as that of Ziehms present results, for general lifetime (and repairtime) distributions. Bell, Clarotti and Fussell use in their formulations negative exponentially distributed lifetimes and repairtimes.

(B4) In contrast with the present study all the other models are fully directed to the phased mission where every subsystem has to survive its appropriate phase. In the case of an event tree this means that their models can only treat the upperbranch of an event tree, whereas the present model can treat every branch of an event tree and as such can be applied for risk analysis.

(B5) The present study as well as the other models calculate the probability of mission success. It is noted that Fussell also introduces the *expected number of system failures* as well as *measures of importance* for components and minimal cut sets during the phased mission.
Ziehms as well as Bell (who applies the theory developed by Ziehms) obtain an exact solution for the probability of mission success for the case that all components are non-repairable. They also derive upper- and lowerbounds for this probability. Clarotti and Fussell only derive an upperbound for the probability of mission success

within their respective models in which on-line repair is applied. The present study leads also to an exact solution. For practical situations, however, as it has been pointed out at the beginning of this section, upperbounds and lowerbounds are derived for the probability of mission success.

(B6) A noticeable difference between the present and that of the other approaches is that the methodology developed within this study does not meet any problem with probability calculations at the phase-boundary instants $T_j, j=1,\ldots,K-1$; the other models need here intricate reasoning to overcome the system dependendies that arise at such phase-boundaries. Despite those intricate operations to be carried out when applying the other models, the partial system failures are not fully and correctly taken into account (with the exception of Ziehms). The present study takes *all dependencies* between systems, also partial failures, correctly into account without cumbersome operations at the phase-boundary instants.

(B7) Bell is the only one who treats phased missions with multiple objectives. However, the present study is also able to treat such problems (see for a discussion chapter 8).

For more information about the models of Ziehms [15], Bell [1], Clarotti et al [26] and Fussell [27], see section 1.2.3. of chapter 1.

In commenting the statements about the applicability of the models mentioned it seems here to be appropriate to state explicitly that *the methodology of the present study is a very general approach* because of its capability:

* to treat every branch of an event tree;
* to take correctly into account all partial system failures;
* to work with general lifetime- and repairtime distributions for the components;
* to take into account repair of a component when it is not operational during the mission itself;
* to provide upper- and lowerbounds for the probability of mission success (in principle the exact values can be obtained if computational effort is not limited).

As an introduction into the methodology that will be developed in this chapter a very simple example is extensively treated in section 6.2. Exact solutions, upperbounds and lowerbounds are presented for the probability of system failure and mission success. A discussion concerning the results concludes this section.
The general phased mission theory shall be developed in section 6.3. Here exact solutions for the probabilities of mission success for the several branches of an event tree with their respective upperbounds and lowerbounds shall be presented and discussed afterwards.
Section 6.4. is devoted to an application, the example of a phased mission of a BWR in case of a large LOCA (cf. example 1 of section 2.1.) is discussed here.

It is explicitly noted that the ratio between the numerical value of the upperbound and its deviation (difference between upper- and lowerbound) needs special attention. For a discussion of this subject see section 6.3.6. (v).

6.2. Demonstration of the algorithm for a simple case

The aim of this section is to give insight into the procedure for calculating the probability of mission success (failure) for a system performing a phased mission. The procedure is based on fault tree analysis and consists in general of the following steps:

- a detailed system description;
- description of the several phases;
- discussion of the relevant phased missions (event tree);
- description of the failure mode of each component;
- construction of the fault tree for each phase;
- determination of the minimal cut sets for each phase;
- classification of the components, i.e. whether it is a non-repairable, continuously detected, randomly detected or periodically inspected component;
- calculation of the probability of mission success or mission failure.

To demonstrate this procedure a very simplified system performing a phased mission consisting of four phases shall be treated in detail, in particular with respect to the probability calculations. In connection with this special

attention will be given to the mutual dependencies between subsystems of distinct phases.

6.2.1. System description

The system concerned is a hydraulic heat removal system (HRS); it is schematically depicted in fig. 6.1.

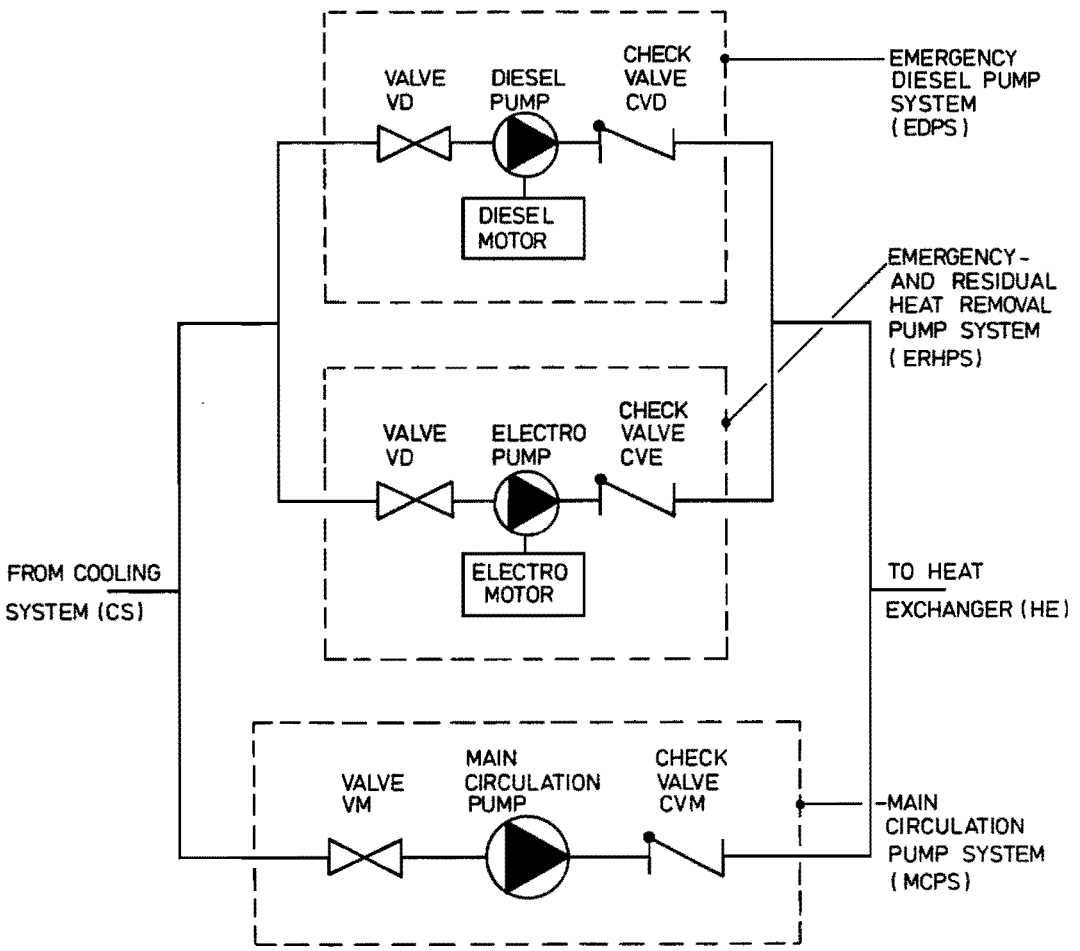


FIG. 6.1. HEAT REMOVAL SYSTEM (HRS).

In practice the system is somewhat more complicated but for the sake of illustration the system in fig. 6.1. is a simplified version.
The heat removal system (HRS) has to remove the heat from a heat exchanger (HE). The HRS performs its task by transporting (pumping) water from a source (used for cooling) of a relatively low temperature to the heat exchanger (HE) where the water is heated up. The heated water is pumped back to the cooling system (CS), for instance a channel, a river or a lake.

In fact the HRS consists of three pumping systems, i.e. the main circulation pumpsystem (MCPS), the emergency- and residual heat removal pumpsystem (ERHPS) and an emergency diesel pumpsystem (EDPS). Each of these systems in the scheme of fig. 6.1. consists of a pump, a hand operated valve upstream the pump, a checkvalve downstream the pump and piping. The main circulation pump (MCP) is driven by off-site power, the electro pump (EP) is driven by an emergency power supply and the diesel driven pump (DP) is powered by a diesel motor.
The HRS has to perform its task during a certain fixed time period, say 24 days. During this period the MCPS has to function and the other two pumpsystems are standby. After 24 days the main circulation pump (MCP) is stopped and the ERHPS and EDPS have to take over the pumping function to take care of the residual heat removal subject to the condition that one of the two systems alone is sufficient to perform this task.
The procedure is now that both systems (ERHPS and EDPS) are initiated at the moment that the MCP is stopped. But if after 20 seconds it appears that the ERHPS functions then the diesel pump (DP) is stopped by means of a signal that is produced by measurement armature on checkvalve CVE in the ERHPS, the signal being based on the flow through checkvalve CVE.
If during the period of 24 days the functioning of pump MCP is stopped by loss of off-site power or by a failure that occurs within the MCP then the other two pumpsystems are immediately started to take over the pumping function as described above. In the case of loss of off-site power the emergency heat removal system has to function for half an hour after which the MCPS is restored and takes over the cooling function. If the emergency heat removal system is started after a failure of the MCPS, it has to function during two hours and it is used to remove the residual heat, because the main system is stopped after a failure of the MCPS. The same holds for the regular MCPS-stop after 24 days.
The structure of the heat removal system as described in this section is applied in "big heat capacity" systems.

6.2.2. Description and definition of the phases during a phased mission for the heat removal system (HRS)

As described in the foregoing section the HRS has to function during fixed periods, in our case periods of 24 days. After such a period the residual heat removal system has to function for 2 hours.

To demonstrate the algorithm for calculating the probability of phased mission success, we shall describe in this section a number of assumptions concerning the modelling of system performance. These assumptions deviate from the real system performance as described in section 6.2.1. These deviations are introduced to allow a simple calculation, because calculation of the probability of mission success in case of real system performance is much more complicated. Since the aim of our phased mission example concerning the Heat Removal System is to demonstrate the algorithm rather than real system operation, we therefore allow ourselves some, perhaps irrational, restrictions to and assumptions on real system performance.

To construct a phased mission for the HRS the following model assumptions are introduced:

(i) suppose that the HRS, i.e. the MCPS, starts to function at instant T_0;

(ii) it is assumed that in the cycle of 24 days at the 10th day, i.e. at instant T_0 + 240 hrs, a loss of off-site power appears. Such an interruption lasts as a rule from some seconds to some minutes with a certain frequency in daily life;

(iii) at the moment that a *loss of off-site* power occurs the MCPS is stopped (a secondary failure) and the emergency pumping system (ERHPS or EDPS) has to take over the pumping function for half an hour;

(iv) it is assumed that in case of a loss of off-site power restoration of the MCPS lasts half an hour. After that time interval the MCPS is assumed to be able to perform again its intended function;

(v) after 24 days from the start of the mission, i.e. at instant T_0 + 576 hrs, the MCPS is stopped and the residual heat removal system (ERHPS or EDPS) is started and has to function for two hours;

(vi) it is assumed that in case of a failure of the MCPS (a primary failure) the emergency cooling system is not started. This assumption is not real but it is introduced to simplify the analysis;

(vii) if the HRS fails to cool for longer than half an hour it is assumed that this interruption is catastrophic for the whole system, incl. heat exchangers, vessels, etc.

From the model assumptions (i),...,(vii) it follows that we can distinguish four phases for the mission that starts at instant T_0. In table 6.1. these phases together with their respective systems are listed.

Table 6.1. Phases for the HRS with their respective systems

PHASE	PHASE INTERVAL (HRS)	SYSTEM
OR-phase	$[0,T_0]$	MCPS ERHPS EDPS
phase 1	$[T_0, T_0 + 240]$	MCPS
phase 2	$[T_0 + 240, T_0 + 240{,}5]$	ERHPS EDPS
phase 3	$[T_0 + 240{,}5, T_0 + 576]$	MCPS
phase 4	$[T_0 + 576, T_0 + 578]$	ERHPS EDPS

T_0 : instant at which the mission starts
OR-phase: Operational Readiness phase

For modelling assumptions concerning component behaviour see section 6.2.4.

6.2.3. Discussion of the several phased missions that can be constructed

In section 2.4. a detailed description is given of a phased mission. From that description it is obvious that theoretically the total number of phased missions that can be constructed with respect to the four phases that are described in section 6.2.2. equals sixteen, i.e. 2^4.
But practically speaking the number of phases is less than sixteen, because not all of them can occur.
For the event tree that can be constructed for the HRS it is obvious that:

(i) if the first subsystem, i.e. the MCPS, fails during the first phase no continuation of the succeeding branches is possible because of severe damage (see assumption 6.2.2. (vii)). Therefore only one branch remains from the original eight branches. The phased mission for that branch consists only of one phase, i.e. phase 1;

(ii) the same reasoning for the branches where the MCPS fails during phase 3 can be applied as it is done in (i). Then only the first three phases are necessary for the calculations of the several phased missions that remain;

(iii) if there is no heat removal during at most half an hour, it is assumed that the damage to the whole system is repairable. Therefore the branches where the subsystem of phase 2 has to perform task "zero", i.e. the subsystem has to fail during its phase, can be continued.

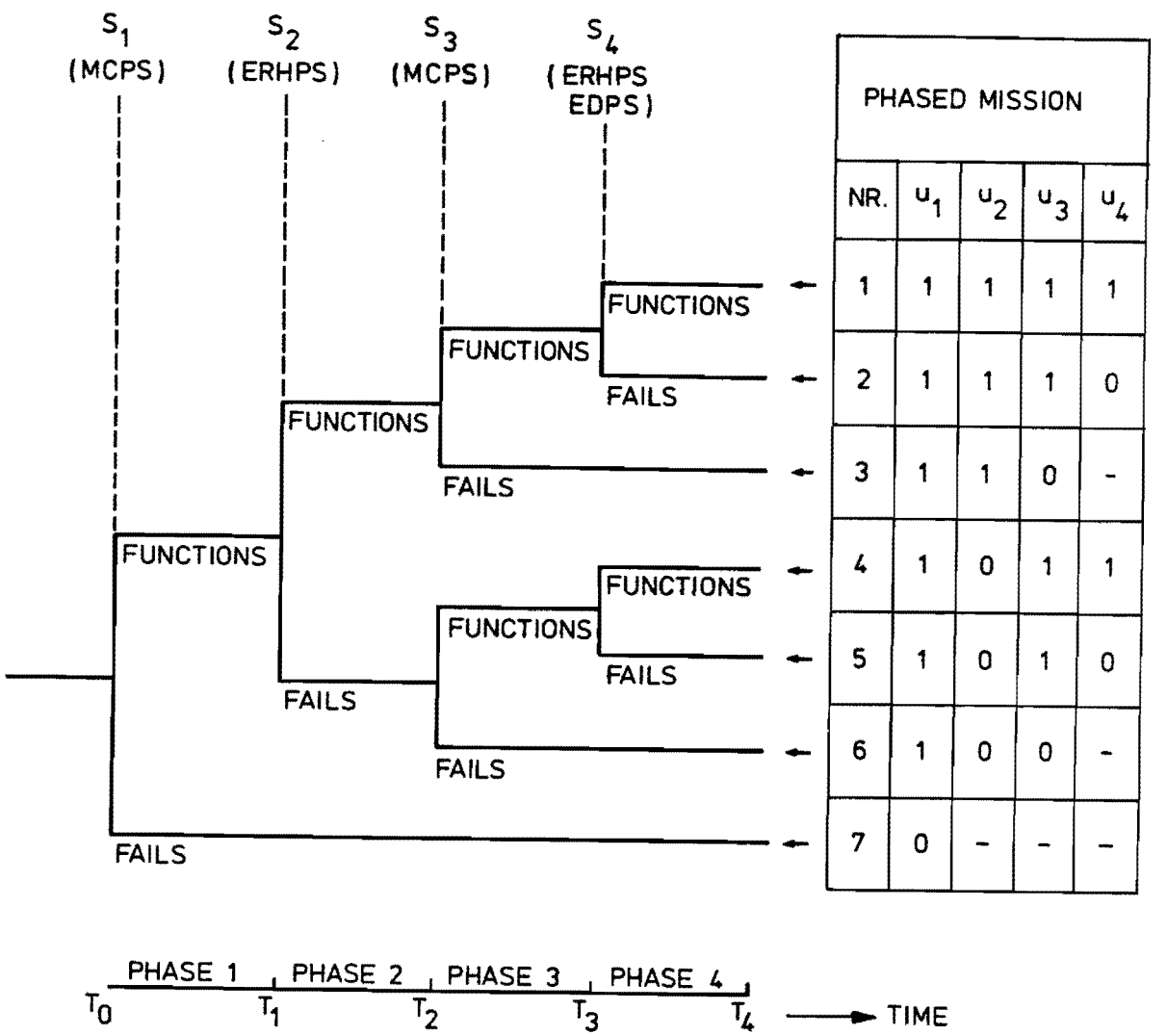


FIG. 6.2. THE EVENT TREE AND THE ASSOCIATED PHASED MISSIONS FOR THE HRS.

Based on these considerations the event tree of fig. 6.2. is constructed. Each branch of the event tree represents a phased mission. From the theoretically sixteen possible missions only seven remain. Every phased mission in fig. 6.2. is coded in a table by means of the task that each subsystem has to fulfill during that specific mission. This task is defined by a binary variable u (see section 2.4.), i.e.

$u_j = 1$, subsystem S_j survives its phase,

$= 0$, subsystem S_j fails during its phase.

6.2.4. Description of the failure mode of the components

In this study it is supposed that each component behaves binary, i.e. the component is in the fail state or in the function state.
Therefore it is necessary to define for each component what is meant by the fail state and the function state.

Concerning the component behaviour it is assumed that:

(i) the hand operated valves VD, VE and VM are definitely in open position and do not fail during the mission;

(ii) the piping does not fail during the mission;

(iii) the diesel pump DP and the diesel motor DM are considered as one component with two states, i.e. the function state and the fail state;

(iv) the electro pump EP and the electro motor EM are also considered as one component with only two states.

So the system of fig. 6.1. can be further simplified to the system of fig. 6.3. in which only six components are left.

We shall denote the components in fig. 6.3. by c_i, i=1,...,6, with

c_1 : MCP , main circulation pump;
c_2 : CVM , checkvalve CVM;
c_3 : EPM , component (subsystem) consisting of the electro driven pump and the electro motor (emergency power);
c_4 : CVE , checkvalve CVE;

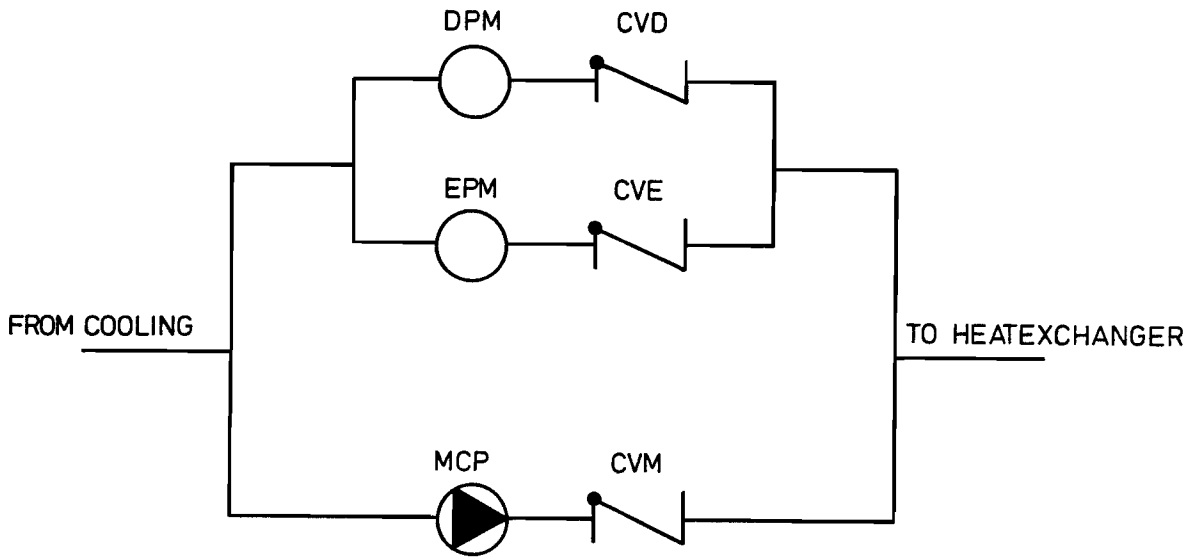


FIG.6.3. OVERSIMPLIFIED HEAT REMOVAL SYSTEM.

Table 6.2. Failure modes of the components in the HRS

COMP. No.	COMP. IDENT.	COMPONENT FAILURE MODE
c_1	MCP	the MCP is in the fail state if it does not transport any water when needed
c_2	CVM	checkvalve CVM is in the fail state if it is closed when it has to be open
c_3	EPM	the EPM system is in the fail state when it does not transport any water when needed. This may be due to the electro motor or to the electro driven pump or to both
c_4	CVE	checkvalve CVE is in the fail state if it is closed and remains closed when it has to open
c_5	DPM	the DPM system is in the fail state if it does not transport any water when needed. This may be due to the diesel motor, to the diesel driven pump or to both
c_6	CVD	checkvalve CVD is in the fail state if it is closed and remains closed when it has to open

c_5 : DPM , component (subsystem) consisting of diesel driven pump and diesel motor;

c_6 : CVD , checkvalve CVD.

For each of the mentioned components their respective failure modes are given in table 6.2.

6.2.5. The fault tree and minimal cut sets for each phase of the HRS

In the figures 6.4. and 6.5. the fault trees for the several phases of the phased mission performed by the HRS are shown. Because the system configurations in phase 1 and phase 3 are identical (see table 6.1.) as well as the system configurations during the phases 2 and 4, each figure shows the fault tree of two phases, i.e. fig. 6.4. represents the fault tree for phase 1 and phase 3, whereas fig. 6.5. consists of the fault tree for the phases 2 and 4.
Denote by $M_k^{(j)}, j,k=1,\ldots,4$, the k^{th} minimal cut set of subsystem S_j. Then it follows easily from the fault trees in figs. 6.4. and 6.5. that the minimal cut sets for the several phases are defined by

$$\begin{aligned} \text{phase 1} : \quad & M_1^{(1)} = \{c_1\}, \\ & M_2^{(1)} = \{c_2\}; \end{aligned} \tag{6.1}$$

$$\begin{aligned} \text{phase 2} : \quad & M_1^{(2)} = \{c_3, c_5\}, \\ & M_2^{(2)} = \{c_3, c_6\}, \\ & M_3^{(2)} = \{c_4, c_5\}, \\ & M_4^{(2)} = \{c_4, c_6\}; \end{aligned} \tag{6.2}$$

$$\begin{aligned} \text{phase 3} : \quad & M_1^{(3)} = \{c_1\}, \\ & M_2^{(3)} = \{c_2\}; \end{aligned} \tag{6.3}$$

$$\begin{aligned} \text{phase 4} : \quad & M_1^{(4)} = \{c_3, c_5\}, \\ & M_2^{(4)} = \{c_3, c_6\}, \\ & M_3^{(4)} = \{c_4, c_5\}, \\ & M_4^{(4)} = \{c_4, c_6\}. \end{aligned} \tag{6.4}$$

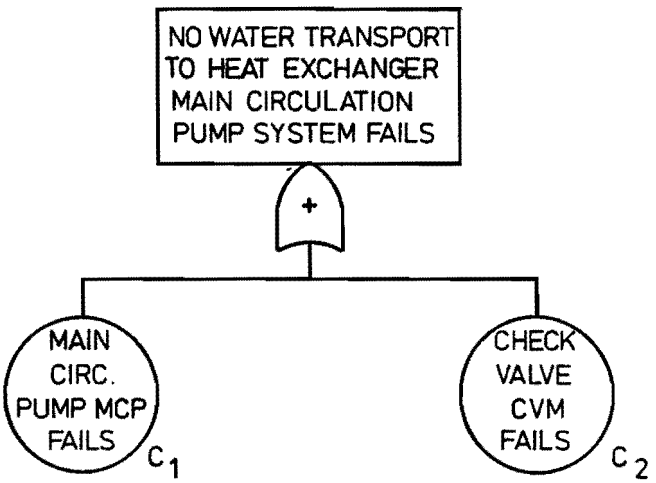


FIG. 6.4. FAULT TREE FOR PHASE 1 AND PHASE 3 OF THE PHASED MISSION PERFORMED BY THE HRS.

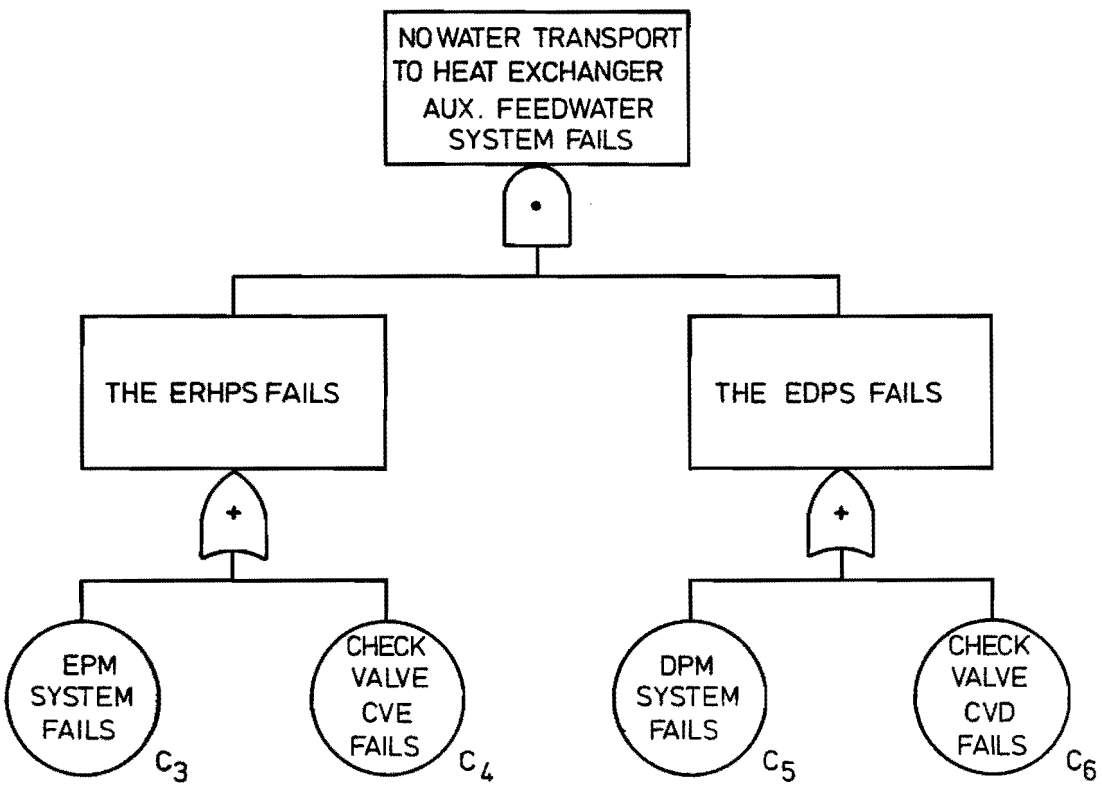


FIG. 6.5. FAULT TREE FOR PHASE 2 AND 4 OF THE PHASED MISSION PERFORMED BY THE HRS.

6.2.6. The probability of mission success for the upperbranch of the event tree for the Heat Removal System (HRS)

The upperbranch of the event tree in fig. 6.2. for the HRS occurs if each of the subsystems S_j, $j=1,\ldots,4$, survives its appropriate phase, i.e. the mission with tasks $u_1=u_2=u_3=u_4=1$ is performed. The mission starts at instant T_0 and phase j terminates at instant T_j, $j=1,\ldots,4$. From table 6.1. (see section 6.2.2.) it is obvious that for our example:

$$\begin{aligned} T_1 &= T_0 + 240, \\ T_2 &= T_0 + 240{,}5, \\ T_3 &= T_0 + 576, \\ T_4 &= T_0 + 578. \end{aligned} \tag{6.5}$$

Since no repair is permitted to a system when it is in an operational state, the system has survived its phase with certainty if it is in the function state at the end of its phase, i.e. subsystem S_j has survived phase j if $\underline{y}_j(T_j)=0$, $\underline{y}_j(\cdot)$ being the state variable for subsystem S_j (see section 2.5.). Therefore the probability of mission success $M_1(T_0)$ for the phased mission $\{u_1=1,\ldots,u_4=1\}$ of the HRS, that starts at instant T_0, can be defined by:

$$M_1(T_0) = \Pr\{\underline{y}_1(T_1)=0,\underline{y}_2(T_2)=0,\underline{y}_3(T_3)=0,\underline{y}_4(T_4)=0\} \quad , T_0 \geq 0. \tag{6.6}$$

In (6.6) every system state is the function state. In order to apply fault tree analysis we have to turn to the fail state for every system. Therefore it follows from (6.6) if we take the complementary probability of the right hand side:

$$M_1(T_0) = 1 - \Pr\{\overline{\underline{y}_1(T_1)=0},\overline{\underline{y}_2(T_2)=0},\overline{\underline{y}_3(T_3)=0},\overline{\underline{y}_4(T_4)=0}\} \ ,$$

where the upperbar indicates complementation. It follows that:

$$\begin{aligned} M_1(T_0) &= 1 - \Pr\{(\overline{\underline{y}_1(T_1)=0}) \cup (\overline{\underline{y}_2(T_2)=0}) \cup (\overline{\underline{y}_3(T_3)=0}) \cup (\overline{\underline{y}_4(T_4)=0})\} \\ &= 1 - \Pr\{\underline{y}_1(T_1)=1) \cup (\underline{y}_2(T_2)=1) \cup (\underline{y}_3(T_3)=1) \cup (\underline{y}_4(T_4)=1)\} \end{aligned}$$

$$
\begin{aligned}
&= 1 - \\
&\quad [+ \Pr\{\underline{y}_1(T_1)=1\} \\
&\quad + \Pr\{\underline{y}_2(T_2)=1\} \\
&\quad + \Pr\{\underline{y}_3(T_3)=1\} \\
&\quad + \Pr\{\underline{y}_4(T_4)=1\} \\
&\quad - \Pr\{\underline{y}_1(T_1)=1,\underline{y}_2(T_2)=1\} \\
&\quad - \Pr\{\underline{y}_1(T_1)=1,\underline{y}_3(T_3)=1\} \\
&\quad - \Pr\{\underline{y}_1(T_1)=1,\underline{y}_4(T_4)=1\} \\
&\quad - \Pr\{\underline{y}_2(T_2)=1,\underline{y}_3(T_3)=1\} \qquad (6.7) \\
&\quad - \Pr\{\underline{y}_2(T_2)=1,\underline{y}_4(T_4)=1\} \\
&\quad - \Pr\{\underline{y}_3(T_3)=1,\underline{y}_4(T_4)=1\} \\
&\quad + \Pr\{\underline{y}_1(T_1)=1,\underline{y}_2(T_2)=1,\underline{y}_3(T_3)=1\} \\
&\quad + \Pr\{\underline{y}_1(T_1)=1,\underline{y}_2(T_2)=1,\underline{y}_4(T_4)=1\} \\
&\quad + \Pr\{\underline{y}_1(T_1)=1,\underline{y}_3(T_3)=1,\underline{y}_4(T_4)=1\} \\
&\quad - \Pr\{\underline{y}_1(T_1)=1,\underline{y}_2(T_2)=1,\underline{y}_3(T_3)=1,\underline{y}_4(T_4)=1\}], \; T_0 \geq 0.
\end{aligned}
$$

From the fault trees in the figures 6.4. and 6.5. it can be concluded that subsystem S_1 shares no components with subsystem S_2 nor subsystem S_4. Therefore, subsystem S_1 behaves independent of the subsystems S_2 and S_4. Hence the variables $\underline{y}_1(t)$ and $\underline{y}_2(t)$ as well as $\underline{y}_1(t)$ and $\underline{y}_4(t)$ are stochastically independent. The same is true for $\underline{y}_3(t)$ with respect to $\underline{y}_2(t)$ and $\underline{y}_4(t)$. Denote by:

$$
\begin{aligned}
&Q_j(t) = \Pr\{\underline{y}_j(t)=1\} \;, \; j=1,\ldots,4; \\
&Q_{j_1,j_2}(t_1,t_2) = \Pr\{\underline{y}_{j_1}(t_{j_1})=1,\underline{y}_{j_2}(t_{j_2})=1\} \;, \qquad (6.8) \\
&\qquad\qquad j_1=1,\ldots,3; \; j_2=j_1+1,\ldots,4; \; t_1,t_2 \geq 0.
\end{aligned}
$$

Making use of the above mentioned independencies and applying (6.8) to (6.7) it follows that the probability $M_1(T_0)$ of mission success can be written as:

$$\begin{aligned} M_1(T_0) = 1 - [&Q_1(T_1)+Q_2(T_2)+Q_3(T_3)+Q_4(T_4) \\ &- \{Q_1(T_1)Q_2(T_2)+Q_{1,3}(T_1,T_3)+Q_1(T_1)Q_4(T_4) \\ &\quad + Q_2(T_2)Q_3(T_3)+Q_{2,4}(T_2,T_4)+Q_3(T_3)Q_4(T_4)\} \\ &+ \{Q_{1,3}(T_1,T_3)Q_2(T_2)+Q_1(T_1)Q_{2,4}(T_2,T_4) \\ &\quad +Q_{1,3}(T_1,T_3)Q_4(T_4)+Q_{2,4}(T_2,T_4)Q_3(T_3)\} \\ &- Q_{1,3}(T_1,T_3)Q_{2,4}(T_2,T_4)]. \end{aligned} \tag{6.9}$$

From (6.9) it is seen that for the calculation of mission success in this particular case only the unavailabilities $Q_1(T_1)$, $Q_2(T_2)$, $Q_3(T_3)$, $Q_4(T_4)$, $Q_{1,3}(T_1,T_3)$ and $Q_{2,4}(T_2,T_4)$ have to be developed.
Denote by

$\underline{\psi}_k^{(j)}(t)$ = the state variable of minimal cut set $M_k^{(j)}$ at instant t (see definition (5.13)).

From section 5.3.1. it is clear that a system is in the fail state if at least one minimal cut set of that system occurs. So from (6.1) it follows that (cf. (5.15)):

$$\begin{aligned} Q_1(T_1) &= \Pr\{(\underline{\psi}_1^{(1)}(T_1)=1) \cup (\underline{\psi}_2^{(1)}(T_1)=1)\} \\ &= \Pr\{\underline{\psi}_1^{(1)}(T_1)=1\}+\Pr\{\underline{\psi}_2^{(1)}(T_1)=1\}-\Pr\{\underline{\psi}_1^{(1)}(T_1)=1,\underline{\psi}_2^{(1)}(T_1)=1\} \\ &= \Pr\{\underline{x}_1(T_1)=1\}+\Pr\{\underline{x}_2(T_1)=1\}-\Pr\{\underline{x}_1(T_1)=1,\underline{x}_2(T_1)=1\}, \end{aligned}$$

$\underline{x}_i(.)$ being the state variable of component c_i (see definition (2.2)). It is assumed (cf. section 2.5.) that the state variables of different components are mutually independent stochastic variables. Therefore it follows that:

$$Q_1(T_1) = \Pr\{\underline{x}_1(T_1)=1\}+\Pr\{\underline{x}_2(T_1)=1\}-\Pr\{\underline{x}_1(T_1)=1\}\ \Pr\{\underline{x}_2(T_1)=1\}. \tag{6.10}$$

Denote by:

$$q_i(t) = \Pr\{\underline{x}_i(t) = 1\} \ , \tag{6.11}$$

then it follows from (6.10) and (6.11) that:

$$Q_1(T_1) = q_1(T_1)+q_2(T_1)-q_1(T_1)q_2(T_1). \tag{6.12}$$

Applying the same procedure to the probabilities $Q_2(T_2)$, $Q_3(T_3)$ and $Q_4(T_4)$ the result reads:

$$\begin{aligned} Q_2(T_2) &= \Pr\{(\underline{\psi}_1^{(2)}(T_2)=1)\cup(\underline{\psi}_2^{(2)}(T_2)=1)\cup(\underline{\psi}_3^{(2)}(T_2)=1)\cup(\underline{\psi}_4^{(2)}(T_2)=1)\} \\ &= q_3(T_2)q_5(T_2)+q_3(T_2)q_6(T_2)+q_4(T_2)q_5(T_2)+q_4(T_2)q_6(T_2) \\ &\quad - \{q_3(T_2)q_5(T_2)q_6(T_2)+q_3(T_2)q_4(T_2)q_5(T_2) \\ &\qquad + 2q_3(T_2)q_4(T_2)q_5(T_2)q_6(T_2)+q_3(T_2)q_4(T_2)q_6(T_2) \\ &\qquad + q_4(T_2)q_5(T_2)q_6(T_2)\} \\ &\quad + 4q_3(T_2)q_4(T_2)q_5(T_2)q_6(T_2) \\ &= \{q_3(T_2)+q_4(T_2)\}\{q_5(T_2)+q_6(T_2)-q_5(T_2)q_6(T_2)\} \\ &\quad - q_3(T_2)q_4(T_2)q_5(T_2)\ \{1-q_6(T_2)\}; \end{aligned} \tag{6.13}$$

$$Q_3(T_3) = Q_1(T_3); \tag{6.14}$$

$$Q_4(T_4) = Q_2(T_4), \tag{6.15}$$

where (6.14) and (6.15) are identities because phase 1 and phase 3 on the one hand and phase 2 and phase 4 on the other hand are represented by the same system configuration, respectively (see section 6.2.2.). Next we shall calculate the probabilities $Q_{1,3}(T_1,T_3)$ and $Q_{2,4}(T_2,T_4)$. These probabilities refer to dependent systems, for instance $Q_{1,3}(T_1,T_3)$ is the probability that subsystem S_1 has failed at instant T_1 and sub-

system S_3 has failed at instant $T_3 > T_1$, where both subsystems S_1 and S_3 are identical in this particular case. So from (6.8) it follows that for $T_3 > T_1 \geq 0$:

$$Q_{1,3}(T_1,T_3) = \Pr\{\underline{y}_1(T_1)=1, \underline{y}_3(T_3)=1\}. \tag{6.16}$$

In the following, (6.16) will be developed into absolute and conditional probabilities. *The condition in the latter probabilities is a system failure mode, i.e. a minimal cut set, and not a system state.* Therefore we get from (6.16) applying (6.1) and (6.3):

$$\begin{aligned}
Q_{1,3}(T_1,T_3) &= \Pr\{(\underline{\psi}_1^{(1)}(T_1)=1) \cup (\underline{\psi}_2^{(1)}(T_1)=1), (\underline{\psi}_1^{(3)}(T_3)=1) \cup (\underline{\psi}_2^{(3)}(T_3)=1)\} \\
&= \Pr\{\underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_1^{(3)}(T_3)=1\} \\
&\quad + \Pr\{\underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(3)}(T_3)=1\} \\
&\quad + \Pr\{\underline{\psi}_2^{(1)}(T_1)=1, \underline{\psi}_1^{(3)}(T_3)=1\} \\
&\quad + \Pr\{\underline{\psi}_2^{(1)}(T_1)=1, \underline{\psi}_2^{(3)}(T_3)=1\} \\
&\quad - \Pr\{\underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(1)}(T_1)=1, \underline{\psi}_1^{(3)}(T_3)=1\} \\
&\quad - \Pr\{\underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(1)}(T_1)=1, \underline{\psi}_2^{(3)}(T_3)=1\} \\
&\quad - \Pr\{\underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_1^{(3)}(T_3)=1, \underline{\psi}_2^{(3)}(T_3)=1\} \\
&\quad - \Pr\{\underline{\psi}_2^{(1)}(T_1)=1, \underline{\psi}_1^{(3)}(T_3)=1, \underline{\psi}_2^{(3)}(T_3)=1\} \\
&\quad + \Pr\{\underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(1)}(T_1)=1, \underline{\psi}_1^{(3)}(T_3)=1, \underline{\psi}_2^{(3)}(T_3)=1\} \\
&= \Pr\{\underline{\psi}_1^{(3)}(T_3)=1 \,|\, \underline{\psi}_1^{(1)}(T_1)=1\} \Pr\{\underline{\psi}_1^{(1)}(T_1)=1\} \\
&\quad + \Pr\{\underline{\psi}_2^{(3)}(T_3)=1 \,|\, \underline{\psi}_1^{(1)}(T_1)=1\} \Pr\{\underline{\psi}_1^{(1)}(T_1)=1\} \\
&\quad + \Pr\{\underline{\psi}_1^{(3)}(T_3)=1 \,|\, \underline{\psi}_2^{(1)}(T_1)=1\} \Pr\{\underline{\psi}_2^{(1)}(T_1)=1\}
\end{aligned}$$

$$
\begin{aligned}
&+ \Pr\{\underline{\psi}_2^{(3)}(T_3)=1 \,|\, \underline{\psi}_2^{(1)}(T_1)=1\}\Pr\{\underline{\psi}_2^{(1)}(T_1)=1\} \\
&- \Pr\{\underline{\psi}_1^{(3)}(T_3)=1 \,|\, \underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(1)}(T_1)=1\} \\
&\quad \cdot \Pr\{\underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(1)}(T_1)=1\} \\
&- \Pr\{\underline{\psi}_2^{(3)}(T_3)=1 \,|\, \underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(1)}(T_1)=1\} \\
&\quad \cdot \Pr\{\underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(1)}(T_1)=1\} \\
&- \Pr\{\underline{\psi}_1^{(3)}(T_3)=1, \underline{\psi}_2^{(3)}(T_3)=1 \,|\, \underline{\psi}_1^{(1)}(T_1)=1\}\Pr\{\underline{\psi}_1^{(1)}(T_1)=1\} \\
&- \Pr\{\underline{\psi}_1^{(3)}(T_3)=1, \underline{\psi}_2^{(3)}(T_3)=1 \,|\, \underline{\psi}_2^{(1)}(T_1)=1\}\Pr\{\underline{\psi}_2^{(1)}(T_1)=1\} \\
&+ \Pr\{\underline{\psi}_1^{(3)}(T_3)=1, \underline{\psi}_2^{(3)}(T_3)=1 \,|\, \underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(1)}(T_1)=1\} \\
&\quad \cdot \Pr\{\underline{\psi}_1^{(1)}(T_1)=1, \underline{\psi}_2^{(1)}(T_1)=1\} \\
= &\Pr\{\underline{x}_1(T_3)=1 \,|\, \underline{x}_1(T_1=1\}\Pr\{\underline{x}_1(T_1)=1\} \\
&+ \Pr\{\underline{x}_2(T_3)=1 \,|\, \underline{x}_1(T_1)=1\}\Pr\{\underline{x}_1(T_1)=1\} \\
&+ \Pr\{\underline{x}_1(T_3)=1 \,|\, \underline{x}_2(T_1)=1\}\Pr\{\underline{x}_2(T_1)=1\} \\
&+ \Pr\{\underline{x}_2(T_3)=1 \,|\, \underline{x}_2(T_1)=1\}\Pr\{\underline{x}_2(T_1)=1\} \\
&- \Pr\{\underline{x}_1(T_3)=1 \,|\, \underline{x}_1(T_1)=1, \underline{x}_2(T_1)=1\}\Pr\{\underline{x}_1(T_1)=1, \underline{x}_2(T_1)=1\} \\
&- \Pr\{\underline{x}_2(T_3)=1 \,|\, \underline{x}_1(T_1)=1, \underline{x}_2(T_1)=1\}\Pr\{\underline{x}_1(T_1)=1, \underline{x}_2(T_1)=1\} \\
&- \Pr\{\underline{x}_1(T_3)=1, \underline{x}_2(T_3)=1 \,|\, \underline{x}_1(T_1)=1\}\Pr\{\underline{x}_1(T_1)=1\} \\
&- \Pr\{\underline{x}_1(T_3)=1, \underline{x}_2(T_3)=1 \,|\, \underline{x}_2(T_1)=1\}\Pr\{\underline{x}_2(T_1)=1\} \\
&+ \Pr\{\underline{x}_1(T_3)=1, \underline{x}_2(T_3)=1 \,|\, \underline{x}_1(T_1)=1, \underline{x}_2(T_1)=1\} \\
&\quad \cdot \Pr\{\underline{x}_1(T_1)=1, \underline{x}_2(T_1)=1\}
\end{aligned}
$$

Because the component state variables $\underline{x}_i(.), i=1,\ldots,6$, are mutually independent stochastic variables it follows that:

$$\begin{aligned} Q_{1,3}(T_1,T_3) = {} & [\Pr\{\underline{x}_1(T_3)=1 \,|\, \underline{x}_1(T_1)=1\}+q_2(T_3)]q_1(T_1) \\ & + [q_1(T_3)+\Pr\{\underline{x}_2(T_3)=1 \,|\, \underline{x}_2(T_1)=1\}]q_2(T_1) \\ & - [\Pr\{\underline{x}_1(T_3)=1 \,|\, \underline{x}_1(T_1)=1\}+\Pr\{\underline{x}_2(T_3)=1 \,|\, \underline{x}_2(T_1)=1\}] \\ & \quad \cdot q_1(T_1)q_2(T_1) \\ & - \Pr\{\underline{x}_1(T_3)=1 \,|\, \underline{x}_1(T_1)=1\}q_1(T_1)q_2(T_3) \\ & - \Pr\{\underline{x}_2(T_3)=1 \,|\, \underline{x}_2(T_1)=1\}q_1(T_3)q_2(T_1) \\ & + \Pr\{\underline{x}_1(T_3)=1 \,|\, \underline{x}_1(T_1)=1\}\Pr\{\underline{x}_2(T_3)=1 \,|\, \underline{x}_2(T_1)=1\} \\ & \quad \cdot q_1(T_1)q_2(T_1), \quad T_3>T_1>0, \end{aligned} \tag{6.17}$$

$q_i(.)$ being defined by (6.11).
Define:

$$\begin{aligned} v_i &= \Pr\{\underline{x}_i(T_3)=1 \,|\, \underline{x}_i(T_1)=1\} \ , \ i=1,2; \\ &= \Pr\{\underline{x}_i(T_4)=1 \,|\, \underline{x}_i(T_2)=1\} \ , \ i=3,\ldots,6. \end{aligned} \tag{6.18}$$

Applying (6.18) to (6.17) the result reads:

$$\begin{aligned} Q_{1,3}(T_1,T_3) = {} & \{v_1+q_2(T_3)\}q_1(T_1) \\ & + \{q_1(T_3)+v_2\}q_2(T_1) \\ & - \{v_1+v_2\}q_1(T_1)q_2(T_1) \\ & - v_1q_1(T_1)q_2(T_3) \\ & - v_2q_1(T_3)q_2(T_1) \\ & + v_1v_2q_1(T_1)q_2(T_1), \quad T_3>T_1>0. \end{aligned} \tag{6.19}$$

Denote by:

$$w_j = \Pr\{\underline{\psi}_j^{(2)}(T_2)\}\ ,\ j=1,\ldots,4;$$
$$w_{jk} = \Pr\{\underline{\psi}_j^{(2)}(T_2)=1, \underline{\psi}_k^{(2)}(T_2)=1\}\ ,\ j=1,2,3;\ k=j+1,\ldots,4. \tag{6.20}$$

From (6.2) and (6.11) we get for w_j and w_{jk} in (6.20):

$$\begin{aligned}
w_1 &= q_3(T_2)q_5(T_2),\\
w_2 &= q_3(T_2)q_6(T_2),\\
w_3 &= q_4(T_2)q_5(T_2),\\
w_4 &= q_4(T_2)q_6(T_2),\\
w_{12} &= q_3(T_2)q_5(T_2)q_6(T_2),\\
w_{13} &= q_3(T_2)q_4(T_2)q_5(T_2),\\
w_{14} &= q_3(T_2)q_4(T_2)q_5(T_2)q_6(T_2),\\
w_{23} &= w_{14},\\
w_{24} &= q_3(T_2)q_4(T_2)q_6(T_2),\\
w_{34} &= q_4(T_2)q_5(T_2)q_6(T_2).
\end{aligned} \tag{6.21}$$

The probability of the simultaneous occurrence of more than two minimal cut sets equals w_{14}.

Applying the same method as used for the derivation of $Q_{1,3}(T_1,T_3)$ in (6.19), we get as a result for $Q_{2,4}(T_2,T_4)$:

$$\begin{aligned}
Q_{2,4}(T_2,T_4) = {} & [v_3v_5\{1-q_4(T_4)\}\{1-q_6(T_4)\}+v_3q_6(T_4)\{1-q_4(T_4)\}\\
& + v_5q_4(T_4)\{1-q_6(T_4)\}+q_4(T_4)q_6(T_4)]w_1\\
& + [v_3v_6\{1-q_4(T_4)\}\{1-q_5(T_4)\}+v_3q_5(T_4)\{1-q_4(T_4)\}\\
& + v_6q_4(T_4)\{1-q_5(T_4)\}+q_4(T_4)q_5(T_4)]w_2\\
& + [v_4v_5\{1-q_3(T_4)\}\{1-q_6(T_4)\}+v_4q_6(T_4)\{1-q_3(T_4)\}\\
& + v_5q_3(T_4)\{1-q_6(T_4)\}+q_3(T_4)q_6(T_4)]w_3
\end{aligned}$$

$$
\begin{aligned}
&+ [v_4v_6\{1-q_3(T_4)\}\{1-q_5(T_4)\}+v_4q_5(T_4)\{1-q_3(T_4)\} \\
&\quad + v_6q_3(T_4)\{1-q_5(T_4)\}+q_3(T_4)q_5(T_4)]w_4 \\
&- [(v_3v_5+v_3v_6-v_3v_5v_6)\{1-q_4(T_4)\} \\
&\quad + q_4(T_4)\{v_6+v_5(1-v_6)\}]w_{12} \\
&- [(v_3v_5+v_4v_5-v_3v_4v_5)\{1-q_6(T_4)\} \\
&\quad + q_6(T_4)\{v_4+v_3(1-v_4)\}]w_{13} \qquad (6.22) \\
&- [(v_3v_6+v_4v_6-v_3v_4v_6)\{1-q_5(T_4)\} \\
&\quad + q_5(T_4)\{v_3+v_4(1-v_3)\}]w_{24} \\
&- [(v_4v_5+v_4v_6-v_4v_5v_6)\{1-q_3(T_4)\} \\
&\quad + q_3(T_4)\{v_5+v_6(1-v_5)\}]w_{34} \\
&+ [(v_3v_5+v_4v_5-v_3v_4v_5)(1-v_6) \\
&\quad + v_6(v_3+v_4-v_3v_4)]w_{14},
\end{aligned}
$$

$q_i(.)$, v_i, w_j and w_{jk} being defined by (6.11), (6.18) and (6.21), respectively.

With the component unavailabilities $q_i(.)$ and v_i, i=1,...,6, given, the variables w_j and w_{jk}, as defined by (6.21), can be calculated and therefore the functions $Q_j(.)$, j=1,...,4 are completely determined by (6.12) through (6.15) and $Q_{1,3}(T_1,T_3)$ and $Q_{2,4}(T_2,T_4)$ by (6.19) and (6.22), respectively. *So the probability $M_1(T_0)$ of mission success for the upperbranch of the event tree of fig. 6.2. and given by (6.9) is completely determined.*

6.2.7. Calculation of the probability of occurrence of the other branches of the event tree

From the event tree of fig. 6.2. it is seen that there are another six branches. Each of these branches can be defined as a phased mission. However, in each of these branches one or more subsystems have failed. In the following we shall show that by means of the results of the foregoing section the probability $M_k(T_0)$, k=2,...,7, of branch k (cf. fig. 6.2.)

can be calculated. Actually, this is an illustration of a general rule that will be explained in section 6.3.6.

6.2.7.1. The occurrence probability $M_2(T_0)$ for branch 2, i.e. the phased mission $\{u_1=1, u_2=1, u_3=1, u_4=0\}$

The second branch in the event tree of fig. 6.2. is characterized by the phased mission $\{u_1=1,u_2=1,u_3=1,u_4=0\}$, i.e. the subsystems S_1, S_2 and S_3 have to survive their respective phases and subsystem S_4 has to fail during its phase. So (cf. (6.6)),

$$M_2(T_0) = \Pr\{\underline{y}_1(T_1)=0,\underline{y}_2(T_2)=0,\underline{y}_3(T_3)=0,\underline{y}_4(T_4)=1\} \quad , T_0\geq 0, \qquad (6.23)$$

with $\underline{y}_j(.)$ being the state variable for subsystem S_j (cf. section 2.5.). Applying simple probabilistic analysis we obtain from (6.23):

$$\begin{aligned}
M_2(T_0) &= \Pr\{\underline{y}_4(T_4)=1\}-\Pr\{\overline{(\underline{y}_1(T_1)=0,\underline{y}_2(T_2)=0,\underline{y}_3(T_3)=0)},\underline{y}_4(T_4)=1\} \\
&= \Pr\{\underline{y}_4(T_4)=1\}-\Pr\{(\underline{y}_1(T_1)=1 \cup \underline{y}_2(T_2)=1 \cup \underline{y}_3(T_3)=1),\underline{y}_4(T_4)=1\} \\
&= \Pr\{\underline{y}_4(T_4)=1\}-[\Pr\{\underline{y}_1(T_1)=1,\underline{y}_4(T_4)=1\}+\Pr\{\underline{y}_2(T_2)=1,\underline{y}_4(T_4)=1\} \\
&\qquad + \Pr\{\underline{y}_3(T_3)=1,\underline{y}_4(T_4)=1\} \\
&\qquad - \Pr\{\underline{y}_1(T_1)=1,\underline{y}_2(T_2)=1,\underline{y}_4(T_4)=1\} \\
&\qquad - \Pr\{\underline{y}_1(T_1)=1,\underline{y}_3(T_3)=1,\underline{y}_4(T_4)=1\} \qquad (6.24) \\
&\qquad - \Pr\{\underline{y}_2(T_2)=1,\underline{y}_3(T_3)=1,\underline{y}_4(T_4)=1\} \\
&\qquad + \Pr\{\underline{y}_1(T_1)=1,\underline{y}_2(T_2)=1,\underline{y}_3(T_3)=1,\underline{y}_4(T_4)=1\}] \\
&= Q_4(T_4) - [Q_1(T_1)Q_4(T_4)+Q_{2,4}(T_2,T_4)+Q_3(T_3)Q_4(T_4) \\
&\qquad - Q_1(T_1)Q_{2,4}(T_2,T_4)-Q_{1,3}(T_1,T_3)Q_4(T_4) \\
&\qquad - Q_{2,4}(T_2,T_4)Q_3(T_3)+Q_{1,3}(T_1,T_3)Q_{2,4}(T_2,T_4)], \; T_0\geq 0,
\end{aligned}$$

where the independencies between the subsystems has been taken into account and $Q_j(.)$, $j=1,\ldots,4$ is given by (6.12) through (6.15), respectively, and $Q_{1,3}(T_1,T_3)$ and $Q_{2,4}(T_2,T_4)$ by (6.19) and (6.22), respectively.

6.2.7.2. The occurrence probability $M_3(T_0)$ for branch 3, i.e. the phased mission $\{u_1=1,u_2=1,u_3=0\}$

Treating branch 3 in the same way as we have treated branch 2 in section 6.2.7.1., we get for the occurrence probability $M_3(T_0)$:

$$\begin{aligned} M_3(T_0) &= \Pr\{\underline{y}_1(T_1)=0,\underline{y}_2(T_2)=0,\underline{y}_3(T_3)=1\} \\ &= \Pr\{\underline{y}_3(T_3)=1\}-\Pr\{(\overline{\underline{y}_1(T_1)=0,\underline{y}_2(T_2)=0}),\underline{y}_3(T_3)=1\} \\ &= \Pr\{\underline{y}_3(T_3)=1\}-\Pr\{(\underline{y}_1(T_1)=1 \cup \underline{y}_2(T_2)=1),\underline{y}_3(T_3)=1\} \\ &= \Pr\{\underline{y}_3(T_3)=1\}-[\Pr\{\underline{y}_1(T_1)=1,\underline{y}_3(T_3)=1\}+\Pr\{\underline{y}_2(T_2)=1,\underline{y}_3(T_3)=1\} \\ &\qquad - \Pr\{\underline{y}_1(T_1)=1,\underline{y}_2(T_2)=1,\underline{y}_3(T_3)=1\}] \qquad (6.25) \\ &= Q_3(T_3)-[Q_{1,3}(T_1,T_3)+Q_2(T_2)Q_3(T_3)-Q_{1,3}(T_1,T_3)Q_2(T_2)],\ T_0\geq 0, \end{aligned}$$

$Q_j(.)$, j=1,2, being given by (6.13) and (6.14), respectively, and $Q_{1,3}(T_1,T_3)$ by (6.19).

6.2.7.3. The occurrence probability $M_4(T_0)$ for branch 4, i.e. the phased mission $\{u_1=1,u_2=0,u_3=1,u_4=1\}$

The treatment of this branch is identical to that of branch 2 (cf. section 6.2.7.1.). The occurrence probability $M_4(T_0)$ for branch 4 is given by:

$$\begin{aligned} M_4(T_0) = Q_2(T_2)-[&Q_1(T_1)Q_2(T_2)+Q_2(T_2)Q_3(T_3)+Q_{2,4}(T_2,T_4) \\ &- Q_{1,3}(T_1,T_3)Q_2(T_2)-Q_1(T_1)Q_{2,4}(T_2,T_4) \\ &- Q_3(T_3)Q_{2,4}(T_2,T_4) \\ &+ Q_{1,3}(T_1,T_3)Q_{2,4}(T_2,T_4)]\ ,\quad T_0\geq 0, \qquad (6.26) \end{aligned}$$

$Q_j(.)$, j=1,2,3, being given by (6.12), (6.13) and (6.14), respectively, and $Q_{1,3}(T_1,T_3)$ and $Q_{2,4}(T_2,T_4)$ being given by (6.19) and (6.22) respectively.

6.2.7.4. The occurrence probability $M_5(T_0)$ for branch 5, i.e. the phased mission $\{u_1=1, u_2=0, u_3=1, u_4=0\}$

In branch 5 two subsystems have to fail during their respective phases. Therefore, the probability $M_5(T_0)$ of mission success, i.e. the probability of the occurrence of branch 5, is defined by:

$$\begin{aligned}
M_5(T_0) &= \Pr\{\underline{y}_1(T_1)=0, \underline{y}_2(T_2)=1, \underline{y}_3(T_3)=0, \underline{y}_4(T_4)=1\} \\
&= \Pr\{\underline{y}_2(T_2)=1, \underline{y}_4(T_4)=1\} \\
&\quad - \Pr\{\overline{(\underline{y}_1(T_1)=0, \underline{y}_3(T_3)=0)}, \underline{y}_2(T_2)=1, \underline{y}_4(T_4)=1\} \\
&= \Pr\{\underline{y}_2(T_2)=1, \underline{y}_4(T_4)=1\} \\
&\quad - [\Pr\{\underline{y}_1(T_1)=1, \underline{y}_2(T_2)=1, \underline{y}_4(T_4)=1\} \\
&\qquad + \Pr\{\underline{y}_2(T_2)=1, \underline{y}_3(T_3)=1, \underline{y}_4(T_4)=1\} \\
&\qquad - \Pr\{\underline{y}_1(T_1)=1, \underline{y}_2(T_2)=1, \underline{y}_3(T_3)=1, \underline{y}_4(T_4)=1\}] \\
&= Q_{2,4}(T_2,T_4) - [Q_1(T_1)Q_{2,4}(T_2,T_4) + Q_3(T_3)Q_{2,4}(T_2,T_4) \\
&\qquad\qquad - Q_{1,3}(T_1,T_3)Q_{2,4}(T_2,T_4)] \\
&= \{1-Q_1(T_1)-Q_3(T_3)+Q_{1,3}(T_1,T_3)\}Q_{2,4}(T_2,T_4), \quad T_0 \geq 0, \qquad (6.27)
\end{aligned}$$

$Q_1(T_1)$ and $Q_3(T_3)$ being given by (6.12) and (6.14), respectively, and $Q_{1,3}(T_1,T_3)$ and $Q_{2,4}(T_2,T_4)$ by (6.19) and (6.22), respectively.

6.2.7.5. The occurrence probability $M_6(T_0)$ for branch 6, i.e. the phased mission $\{u_1=1, u_2=0, u_3=0\}$

The occurrence $M_6(T_0)$ for branch 6 is given by:

$$\begin{aligned}
M_6(T_0) &= \Pr\{\underline{y}_1(T_1)=0, \underline{y}_2(T_2)=1, \underline{y}_3(T_3)=1\} \\
&= \Pr\{\underline{y}_2(T_2)=1, \underline{y}_3(T_3)=1\} - \Pr\{\underline{y}_1(T_1)=1, \underline{y}_2(T_2)=1, \underline{y}_3(T_3)=1\} \\
&= Q_2(T_2)Q_3(T_3) - Q_{1,3}(T_1,T_3)Q_2(T_2), \quad T_0 \geq 0, \qquad (6.28)
\end{aligned}$$

$Q_2(T_2)$ and $Q_3(T_3)$ being given by (6.13) and (6.14), respectively, and $Q_{1,3}(T_1,T_3)$ by (6.19).

6.2.7.6. The occurrence probability $M_7(T_0)$ for branch 7, i.e. the phased mission $\{u_1=0\}$

The probability $M_7(T_0)$ of occurrence of branch 7 is a very simple one, i.e.

$$M_7(T_0) = Pr\{\underline{y}_1(T_1)=1\}=Q_1(T_1), \quad T_0 \geq 0, \tag{6.29}$$

$Q_1(T_1)$ being defined by (6.12).

6.2.8. A numerical application for the Heat Removal System (HRS)

In this section a numerical application for the HRS shall be given for three different maintenance strategies, i.e.

(i) the case in which every component is a class 1 component, e.g. every component of the HRS is non-repairable (cf. input table 6.3);

(ii) the components are maintained in different ways. Some are not inspected (non-repairable) while others are inspected periodically (cf. input table 6.4);

(iii) all components are inspected continuously (cf. input table 6.5).

The input data for the strategies (i), (ii) and (iii) are presented in tables 6.3., 6.4., and 6.5., respectively. The input numbers are fictitious and do not relate to practical situations. They are only used for the sake of demonstration of the proposed technique for treating phased missions.

In this application all components have a negative exponentially distributed lifetime. The repairtime distribution for class 2 components (continuously detected) is negative exponential, whereas in case of class 4 components (periodically inspected) the repairtime is uniformly distributed.

For the three strategies (i), (ii) and (iii), respectively, calculations have been performed for two different cases, viz. in the first case the mission starts at instant 200 (T_0 = 200 hrs) and in the other case the mission starts at instant 1000 (T_0 = 1000 hrs). These different calculations offer the possibility to get insight into the behaviour of the probabilities $M_k(T_0)$ of mission success as a function of the instant T_0 at which the mission starts.

Because the approach to phased mission analysis in this study is different from the methods applied up till now we like to compare present results with outcomes obtained by former methods. Therefore a calculation based on a former method (see (R1) and (R2) below) has been carried out for the mission that starts at T_0 = 1000 hrs. Note that the probability calculations performed in the past have never correctly taken into account the dependencies between subsystems that are a part of a phased mission.

As a former method we shall take here the special calculation method which assumes no dependencies between subsystems. It is defined by the following rules (R1) and (R2).

(R1) Calculate for each subsystem S_j, $j=1,\ldots,K$, the probability $Q_j(T_j)$ of system failure. The probability that the upperbranch of the event tree does not occur is then bounded by $P_0(T_0)$:

$$P_0(T_0) = \sum_{j=1}^{K} Q_j(T_j).$$

(R2) Assume that branch j of the event tree is characterized by: k subsystems, i.e. $S_{j_1},\ldots,S_{j_k}$, have to fail during their respective phases and the other (K-k) subsystems have to survive their phases. For this branch the probabilities $Q_{j_\ell}(T_{j_\ell})$, $\ell=1,\ldots,k$, of system failure are calculated and the probability of mission success (the probability of occurrence of branch j) is bounded from above by $P_j(T_0)$:

$$P_j(T_0) = \prod_{\ell=1}^{K} Q_{j_\ell}(T_{j_\ell}).$$

For the calculation of the probabilities $Q_j(T_j)$ performed in the steps (R1) and (R2) the component models of chapter 3 are used. So the extended component models for phased mission analysis of chapter 4 are not applied.

The results of the several calculations are presented in the following tables:

Table 6.6. - in this table the probabilities $M_k(T_0)$, k=1,...,7, of mission success for each branch are shown for the three mentioned maintenance strategies; the mission starts at T_0 = 200 hrs. Two solutions are given, i.e. an exact solution and an approximate solution (upperbound and the difference between upper- and lowerbound). For the approximations see section 6.3.

Table 6.7. - this table shows for T_0 = 1000 hrs (i.e. the mission starts at instant 1000) the probabilities $M_k(T_0)$, k=1,...,7 of mission success; the nomenclature is the same as table 6.6.

Table 6.8. - for each strategy this table presents the probabilities of mission success obtained by:
* the exact solution;
* the upperbound calculated by the present study;
* the upperbound calculated by the former approach (heading "Former Method").

The probability of mission success is obtained after several calculation steps as it has been shown in this section 6.2.:

* first the calculation of the *absolute* and *conditional* component unavailabilities, $q_j(.)$ and v_j, respectively;
* after that the calculation of the occurrence probabilities w_j and w_{jk} of the minimal cut sets;
* then the calculation of the system unavailabilities $Q_j(.)$ and $Q_{j,k}(.,.)$;
* and finally the probabilities $M_k(T_0)$ of mission success.

For the missions that start at T_0 = 1000 hrs the following tables present the results of the calculations for the several mentioned steps (except for the probabilities $M_k(T_0)$ which are presented in table 6.7.).

Table 6.9. - this table shows the *conditional* component unavailabilities v_i, i=1,...,6, for each class of applied components;

Table 6.10. - this table shows the *absolute* component unavailabilities $q_i(.)$ at the instants T_1, T_2, T_3 and T_4 (the endpoints of phase 1, phase 2, phase 3 and phase 4, respectively) for

each applied class of components;

Table 6.11. - a table showing the occurrence probabilities w_j and w_{jk} for the minimal cut sets of each phase at the instants T_1, T_2, T_3 and T_4 for the three strategies mentioned in (i), (ii) and (iii) of this section;

Table 6.12. - this table contains the probabilities $Q_j(.)$ of single system failure and $Q_{1,3}(T_1,T_3)$ and $Q_{2,4}(T_2,T_4)$ for joint system failure for the three mentioned maintenance strategies. The results of two calculations are presented for these probabilities, viz.

* those according to the exact solution, and
* those according to the approximated solution, i.e. an upperbound and the difference between upper- and lowerbound.

For the approximate solution see section 6.3.

In order to show the influence of the specially developed component behaviour models for phased mission analysis a last table is added. This table 6.13. presents the upperbounds of the probabilities of the top events for the four subsystems S_1, S_2, S_3 and S_4. The present study applies the specially developed component models of chapter 4, whereas the approach as at present used in practice applies the component models of chapter 3. Table 6.13. is described by:

Table 6.13. - the content of the table consists of upperbounds for the probabilities $Q_j(.)$ of system failure for the subsystems S_1, S_2, S_3 and S_4, respectively, for all strategies; the missions start at T_0 = 1000 hrs.
The upperbound beneath the heading "Present Study" is obtained by the use of component models of chapter 4, whereas the upperbound beneath the heading "Former Method" is obtained using component models of chapter 3.

Table 6.3. COMPONENT INPUT DATA FOR STRATEGY (i), i.e. INPUT DATA IN CASE THAT ALL COMPONENTS ARE NON-REPAIRABLE (CLASS 1 COMPONENTS)

COMPONENT		INITIAL AVAILABILITY	FAILURE RATE / hr	MEAN REPAIR TIME (hrs)	TIME TO FIRST INSPECTION (hrs)	INSPECTION INTERVAL (hrs)	INSPECTION DURATION (hrs)
Nr.	CLASS	a_0	λ	μ	η_1	η	θ
c_1	1	1.	$5 * 10^{-5}$	-	-	-	-
c_2	1	1.	10^{-6}	-	-	-	-
c_3	1	1.	$5 * 10^{-5}$	-	-	-	-
c_4	1	1.	10^{-6}	-	-	-	-
c_5	1	0.98	$3 * 10^{-4}$	-	-	-	-
c_6	1	1.	10^{-6}	-	-	-	-

Table 6.4. COMPONENT INPUT DATA FOR STRATEGY (ii), i.e. INPUT DATA IN CASE OF CLASS 1 (NON-REPAIRABLE) COMPONENTS AND CLASS 4 (PERIODICALLY INSPECTED) COMPONENTS

COMPONENT		INITIAL AVAILABILITY	FAILURE RATE / hr	MEAN REPAIR TIME (hrs)	TIME TO FIRST INSPECTION (hrs)	INSPECTION INTERVAL (hrs)	INSPECTION DURATION (hrs)
Nr.	CLASS	a_0	λ	μ	η_1	η	θ
c_1	4	1.	$5 * 10^{-5}$	24.	168	168	1.
c_2	1	1.	10^{-6}	-	-	-	-
c_3	4	1.	$5 * 10^{-5}$	24.	192	168	1.
c_4	1	1.	10^{-6}	-	-	-	-
c_5	4	.98	$3 * 10^{-4}$	24.	216	168	1.
c_6	1	1.	10^{-6}	-	-	-	-

Table 6.5. COMPONENTS INPUT DATA FOR STRATEGY (iii), i.e. INPUT DATA IN CASE THAT ALL COMPONENTS ARE CONTINUOUSLY INSPECTED (CLASS 2 COMPONENTS)

COMPONENT		INITIAL AVAILABILITY	FAILURE RATE / hr	MEAN REPAIR TIME (hrs)	TIME TO FIRST INSPECTION (hrs)	INSPECTION INTERVAL (hrs)	INSPECTION DURATION (hrs)
Nr.	CLASS	a_0	λ	μ	η_1	η	θ
c_1	2	1.	$5 * 10^{-5}$	24.	-	-	-
c_2	2	1.	10^{-6}	2.	-	-	-
c_3	2	1.	$5 * 10^{-5}$	24.	-	-	-
c_4	2	1.	10^{-6}	2.	-	-	-
c_5	2	.98	$3 * 10^{-4}$	24.	-	-	-
c_6	2	1.	10^{-6}	2.	-	-	-

Table 6.6. PROBABILITIES OF MISSION SUCCESS (T_0 = 200 hrs)

MISSION					PROBABILITY OF MISSION SUCCESS								
					STRATEGY (i)			STRATEGY (ii)			STRATEGY (iii)		
					ALL COMPONENTS NON-REPAIRABLE (CLASS 1)			COMP. c_1, c_3 AND c_5 ARE PERIODICALLY INSPECTED (CLASS 4) COMP. c_2,c_4 AND c_6 ARE NON-REPAIRABLE (CLASS 1)			ALL COMPONENTS CONTINUOUSLY INSPECTED (CLASS 2)		
No.	CODE				EXACT SOLUTION	FIRST ORDER APPROXIMATION		EXACT SOLUTION	FIRST ORDER APPROXIMATION		EXACT SOLUTION	FIRST ORDER APPROXIMATION	
i	u_1	u_2	u_3	u_4		UPPERBOUND	DEVIATION++)		UPPERBOUND	DEVIATION++)		UPPERBOUND	DEVIATION++)
1	1	1	1	1	$4.73 * 10^{-2}$+)	$7.30 * 10^{-2}$	$2.62 * 10^{-2}$	$4.00 * 10^{-2}$	$5.89 * 10^{-2}$	$1.91 * 10^{-2}$	$3.01 * 10^{-2}$	$4.32 * 10^{-2}$	$1.31 * 10^{-2}$
2	1	1	1	0	$5.93 * 10^{-3}$	$8.76 * 10^{-3}$	$3.70 * 10^{-3}$	$4.68 * 10^{-3}$	$6.65 * 10^{-3}$	$2.15 * 10^{-3}$	$9.79 * 10^{-6}$	$1.01 * 10^{-5}$	$4.36 * 10^{-7}$
3	1	1	0	-	$1.66 * 10^{-2}$	$3.89 * 10^{-2}$	$2.24 * 10^{-2}$	$1.67 * 10^{-2}$	$3.36 * 10^{-2}$	$1.70 * 10^{-2}$	$1.68 * 10^{-2}$	$2.98 * 10^{-2}$	$1.31 * 10^{-2}$
4	1	0	1	1	0	$3.15 * 10^{-3}$	$3.35 * 10^{-3}$	0	$1.80 * 10^{-3}$	$1.90 * 10^{-3}$	$8.66 * 10^{-6}$	$8.93 * 10^{-6}$	$3.85 * 10^{-7}$
5	1	0	1	0	$3.02 * 10^{-3}$	$3.16 * 10^{-3}$	$2.08 * 10^{-4}$	$1.74 * 10^{-3}$	$1.81 * 10^{-3}$	$1.00 * 10^{-4}$	$8.75 * 10^{-11}$	$9.03 * 10^{-11}$	$3.90 * 10^{-12}$
6	1	0	0	-	$5.22 * 10^{-5}$	$1.22 * 10^{-4}$	$7.03 * 10^{-5}$	$3.01 * 10^{-5}$	$6.05 * 10^{-5}$	$3.05 * 10^{-5}$	$1.50 * 10^{-7}$	$2.66 * 10^{-7}$	$1.17 * 10^{-7}$
7	0	-	-	-	$2.22 * 10^{-2}$	$2.22 * 10^{-2}$	$9.59 * 10^{-6}$	$1.68 * 10^{-2}$	$1.68 * 10^{-2}$	$7.22 * 10^{-6}$	$1.33 * 10^{-2}$	$1.33 * 10^{-2}$	$3.17 * 10^{-6}$

+) For mission no. 1 (u_1=u_2=u_3=u_4=1) the probability of mission failure is presented

u_j = 1, subsystem S_j survives phase j;

= 0, subsystem S_j fails during phase j, j=1,2,3,4.

++) Deviation: difference between upper- and lowerbound.

Table 6.7. PROBABILITIES OF MISSION SUCCESS (T_0 = 1000 hrs)

MISSION					PROBABILITY OF MISSION SUCCESS								
					STRATEGY (i)			STRATEGY (ii)			STRATEGY (iii)		
					ALL COMPONENTS NON-REPAIRABLE (CLASS 1)			COMP. c_1, c_3 AND c_5 ARE PERIODICALLY INSPECTED (CLASS 4) COMP. c_2, c_4 AND c_6 ARE NON-REPAIRABLE (CLASS 1)			ALL COMPONENTS CONTINUOUSLY INSPECTED (CLASS 2)		
No.	CODE				EXACT SOLUTION	FIRST ORDER APPROXIMATION		EXACT SOLUTION	FIRST ORDER APPROXIMATION		EXACT SOLUTION	FIRST ORDER APPROXIMATION	
i	u_1	u_2	u_3	u_4		UPPERBOUND	DEVIATION[++]		UPPERBOUND	DEVIATION[++]		UPPERBOUND	DEVIATION[++]
1	1	1	1	1	$1.05 * 10^{-1}$[+]	$1.89 * 10^{-1}$	$8.90 * 10^{-2}$	$4.42 * 10^{-2}$	$6.75 * 10^{-2}$	$2.37 * 10^{-2}$	$3.01 * 10^{-2}$	$4.32 * 10^{-2}$	$1.31 * 10^{-2}$
2	1	1	1	0	$9.49 * 10^{-3}$	$3.03 * 10^{-2}$	$2.44 * 10^{-2}$	$4.66 * 10^{-3}$	$6.86 * 10^{-3}$	$2.44 * 10^{-3}$	$9.79 * 10^{-6}$	$1.01 * 10^{-5}$	$4.36 * 10^{-7}$
3	1	1	0	-	$1.57 * 10^{-2}$	$7.74 * 10^{-2}$	$6.32 * 10^{-2}$	$1.67 * 10^{-2}$	$3.77 * 10^{-2}$	$2.11 * 10^{-2}$	$1.68 * 10^{-2}$	$2.98 * 10^{-2}$	$1.31 * 10^{-2}$
4	1	0	1	1	0	$2.00 * 10^{-2}$	$2.30 * 10^{-2}$	0	$2.00 * 10^{-3}$	$2.14 * 10^{-3}$	$8.66 * 10^{-6}$	$8.93 * 10^{-6}$	$3.85 * 10^{-7}$
5	1	0	1	0	$1.84 * 10^{-2}$	$2.01 * 10^{-2}$	$3.02 * 10^{-3}$	$1.92 * 10^{-3}$	$2.02 * 10^{-3}$	$1.43 * 10^{-4}$	$8.75 * 10^{-11}$	$9.03 * 10^{-11}$	$3.90 * 10^{-12}$
6	1	0	0	-	$3.19 * 10^{-4}$	$1.55 * 10^{-3}$	$1.24 * 10^{-3}$	$3.34 * 10^{-5}$	$7.55 * 10^{-5}$	$4.24 * 10^{-5}$	$1.50 * 10^{-7}$	$2.66 * 10^{-7}$	$1.17 * 10^{-7}$
7	0	-	-	-	$6.13 * 10^{-2}$	$6.13 * 10^{-2}$	$7.45 * 10^{-5}$	$2.09 * 10^{-2}$	$2.09 * 10^{-2}$	$2.44 * 10^{-5}$	$1.33 * 10^{-2}$	$1.33 * 10^{-2}$	$3.17 * 10^{-6}$

+) For mission no. 1 ($u_1=u_2=u_3=u_4=1$) the probability of mission failure is presented

u_j = 1, subsystem S_j survives phase j;

= 0, subsystem S_j fails during phase j, j=1,2,3,4.

++) Deviation: difference between upper- and lowerbound.

Table 6.8. PROBABILITIES OF MISSION SUCCESS FOR THE HRS
THE EXACT SOLUTION AND UPPERBOUNDS OBTAINED BY THE PRESENT STUDY AND A FORMER APPROACH
(T_0 = 1000 hrs)

MISSION					PROBABILITY OF MISSION SUCCESS								
					STRATEGY (i)			STRATEGY (ii)			STRATEGY (iii)		
					ALL COMPONENTS NON-REPAIRABLE (CLASS 1)			COMP. c_1, c_3 AND c_5 ARE PERIODICALLY INSPECTED (CLASS 4) COMP. c_2, c_4 AND c_6 ARE NON-REPAIRABLE (CLASS 1)			ALL COMPONENTS CONTINUOUSLY INSPECTED (CLASS 2)		
No.	CODE				EXACT SOLUTION	FIRST ORDER APPROXIMATION (UPPERBOUND)		EXACT SOLUTION	FIRST ORDER APPROXIMATION (UPPERBOUND)		EXACT SOLUTION	FIRST ORDER APPROXIMATION (UPPERBOUND)	
i	u_1	u_2	u_3	u_4		PRESENT STUDY	FORMER METHOD		PRESENT STUDY	FORMER METHOD		PRESENT STUDY	FORMER METHOD
1	1	1	1	1	$1.05 * 10^{-1}$ +)	$1.89 * 10^{-1}$	$2.36 * 10^{-1}$	$4.42 * 10^{-2}$	$6.75 * 10^{-2}$	$9.45 * 10^{-3}$	$3.01 * 10^{-2}$	$4.32 * 10^{-2}$	$2.42 * 10^{-3}$
2	1	1	1	0	$9.49 * 10^{-3}$	$3.03 * 10^{-2}$	$3.03 * 10^{-2}$	$4.66 * 10^{-3}$	$6.86 * 10^{-3}$	$1.84 * 10^{-4}$	$9.79 * 10^{-6}$	$1.01 * 10^{-5}$	$8.59 * 10^{-6}$
3	1	1	0	-	$1.57 * 10^{-2}$	$7.74 * 10^{-2}$	$7.74 * 10^{-2}$	$1.67 * 10^{-2}$	$3.77 * 10^{-2}$	$4.71 * 10^{-3}$	$1.68 * 10^{-2}$	$2.98 * 10^{-2}$	$1.20 * 10^{-3}$
4	1	0	1	1	0	$2.00 * 10^{-2}$	$2.00 * 10^{-2}$	0	$2.00 * 10^{-3}$	$1.81 * 10^{-4}$	$8.66 * 10^{-6}$	$8.93 * 10^{-6}$	$8.59 * 10^{-6}$
5	1	0	1	0	$1.84 * 10^{-2}$	$2.01 * 10^{-2}$	$6.06 * 10^{-4}$	$1.92 * 10^{-3}$	$2.02 * 10^{-3}$	$3.33 * 10^{-8}$	$8.75 * 10^{-11}$	$9.03 * 10^{-11}$	$7.38 * 10^{-11}$
6	1	0	0	-	$3.19 * 10^{-4}$	$1.55 * 10^{-3}$	$1.55 * 10^{-3}$	$3.34 * 10^{-5}$	$7.55 * 10^{-5}$	$8.53 * 10^{-7}$	$1.50 * 10^{-7}$	$2.66 * 10^{-7}$	$1.03 * 10^{-8}$
7	0	-	-	-	$6.13 * 10^{-2}$	$6.13 * 10^{-2}$	$6.14 * 10^{-2}$	$2.09 * 10^{-2}$	$2.09 * 10^{-2}$	$4.37 * 10^{-3}$	$1.33 * 10^{-2}$	$1.33 * 10^{-2}$	$1.20 * 10^{-3}$

+) For mission no. 1 (u_1=u_2=u_3=u_4=1) the probability of mission failure is presented

u_j = 1, subsystem S_j survives phase j;
= 0, subsystem S_j fails during phase j, j=1,2,3,4.

Table 6.9. CONDITIONAL COMPONENT UNAVAILABILITIES

(T_0 = 1000 hrs)

COMPONENT		NON-REPAIRABLE (CLASS 1)	CONTINUOUS INSPECTION (CLASS 2)	PERIODICAL INSPECTION (CLASS 4)
c_i	v_i	CALCULATED BY (4.123)	CALCULATED BY (4.127)	CALCULATED BY (4.123)
c_1	v_1	1.	$9.80 * 10^{-1}$	1.
c_2	v_2	1.	$7.78 * 10^{-1}$	1.
c_3	v_3	1.	$1.30 * 10^{-3}$	1.
c_4	v_4	1.	$4.00 * 10^{-6}$	1.
c_5	v_5	1.	$7.75 * 10^{-6}$	1.
c_6	v_6	1.	$4.00 * 10^{-6}$	1.

Table 6.10. ABSOLUTE COMPONENT UNAVAILABILITIES

(T_0 = 1000 hrs)

COMPONENT		NON-REPAIRABLE (CLASS 1) CALCULATED BY (4.1)				CONTINUOUS INSPECTION (CLASS 2) CALCULATED BY (4.39) AND (4.40)				PERIODICAL INSPECTION (CLASS 4) CALCULATED BY (4.121)			
c_i	$q_i(.)$	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4
c_1	q_1	$6.01*10^{-2}$	$6.01*10^{-2}$	$7.58*10^{-2}$	$7.59*10^{-2}$	$1.31*10^{-2}$	$1.29*10^{-2}$	$2.93*10^{-2}$	$2.70*10^{-2}$	$1.97*10^{-2}$	$1.98*10^{-2}$	$3.61*10^{-2}$	$3.62*10^{-2}$
c_2	q_2	$1.24*10^{-3}$	$1.24*10^{-3}$	$1.58*10^{-3}$	$1.58*10^{-3}$	$2.42*10^{-4}$	$1.89*10^{-4}$	$5.24*10^{-4}$	$1.94*10^{-4}$	-[1]	-	-	-
c_3	q_3	$6.01*10^{-2}$	$6.01*10^{-2}$	$7.58*10^{-2}$	$7.59*10^{-2}$	$1.20*10^{-3}$	$1.22*10^{-3}$	$1.20*10^{-3}$	$1.30*10^{-3}$	$1.86*10^{-2}$	$1.86*10^{-2}$	$3.49*10^{-2}$	$3.50*10^{-2}$
c_4	q_4	$1.24*10^{-3}$	$1.24*10^{-3}$	$1.58*10^{-3}$	$1.58*10^{-3}$	$2.00*10^{-6}$	$2.50*10^{-6}$	$2.00*10^{-6}$	$4.00*10^{-6}$	-	-	-	-
c_5	q_5	$3.24*10^{-1}$	$3.25*10^{-1}$	$3.89*10^{-1}$	$3.90*10^{-1}$	$7.15*10^{-3}$	$7.30*10^{-3}$	$7.15*10^{-3}$	$7.74*10^{-3}$	$9.96*10^{-2}$	$9.98*10^{-2}$	$1.86*10^{-1}$	$1.86*10^{-1}$
c_6	q_6	$1.24*10^{-3}$	$1.24*10^{-3}$	$1.58*10^{-3}$	$1.58*10^{-3}$	$2.00*10^{-6}$	$2.50*10^{-6}$	$2.00*10^{-6}$	$4.00*10^{-6}$	-	-	-	-

[1] not computed

T_1 = 1240 hrs

T_2 = 1240.5 hrs

T_3 = 1576 hrs

T_4 = 1578 hrs

Table 6.11. OCCURRENCE PROBABILITIES OF THE MINIMAL CUT SETS (T_0 = 1000 hrs)

MINIMAL CUT SET	STRATEGY (i): ALL COMPONENTS NON-REPAIRABLE (CLASS 1)		STRATEGY (ii): COMPONENTS c_1, c_3 AND c_5 ARE PERIODICALLY INSPECTED (CLASS 4); COMPONENTS c_2, c_4 AND c_6 ARE NON-REPAIRABLE (CLASS 1)		STRATEGY (iii): ALL COMPONENTS CONTINUOUSLY INSPECTED (CLASS 2)	
OCCURRENCE PROBABILITIES OF THE MINIMAL CUT SETS OF THE SUBSYSTEMS S_1 AND S_3						
$M_i^{(j)*}$	T_1	T_3	T_1	T_3	T_1	T_3
M_1	$6.01 * 10^{-2}$	$7.58 * 10^{-2}$	$1.97 * 10^{-2}$	$3.61 * 10^{-2}$	$1.31 * 10^{-2}$	$2.93 * 10^{-2}$
M_2	$1.24 * 10^{-3}$	$1.58 * 10^{-3}$	$1.24 * 10^{-3}$	$1.58 * 10^{-3}$	$2.42 * 10^{-4}$	$5.24 * 10^{-4}$
M_1M_2	$7.45 * 10^{-5}$	$1.20 * 10^{-4}$	$2.44 * 10^{-5}$	$5.70 * 10^{-5}$	$3.17 * 10^{-6}$	$1.54 * 10^{-5}$
OCCURRENCE PROBABILITIES OF THE MINIMAL CUT SETS OF THE SUBSYSTEMS S_2 AND S_4						
$M_i^{(j)**}$	T_2	T_4	T_2	T_4	T_2	T_4
M_1	$1.95 * 10^{-2}$	$2.96 * 10^{-2}$	$1.86 * 10^{-3}$	$6.51 * 10^{-3}$	$8.91 * 10^{-6}$	$1.01 * 10^{-5}$
M_2	$7.45 * 10^{-5}$	$1.20 * 10^{-4}$	$2.31 * 10^{-5}$	$5.53 * 10^{-5}$	$3.05 * 10^{-9}$	$5.20 * 10^{-9}$
M_3	$4.03 * 10^{-4}$	$6.16 * 10^{-4}$	$1.24 * 10^{-4}$	$2.94 * 10^{-4}$	$1.83 * 10^{-8}$	$3.10 * 10^{-8}$
M_4	$1.54 * 10^{-6}$	$2.50 * 10^{-6}$	$1.54 * 10^{-6}$	$2.50 * 10^{-6}$	$6.25 * 10^{-12}$	$1.60 * 10^{-11}$
M_1M_2	$2.42 * 10^{-5}$	$4.68 * 10^{-5}$	$2.30 * 10^{-6}$	$1.03 * 10^{-5}$	$2.23 * 10^{-11}$	$4.02 * 10^{-11}$
M_1M_3	$2.42 * 10^{-5}$	$4.68 * 10^{-5}$	$2.30 * 10^{-6}$	$1.03 * 10^{-5}$	$2.23 * 10^{-11}$	$4.01 * 10^{-11}$
M_1M_4	$3.00 * 10^{-8}$	$7.39 * 10^{-8}$	$2.85 * 10^{-9}$	$1.63 * 10^{-8}$	$5.57 * 10^{-17}$	$1.61 * 10^{-16}$
M_2M_3	$3.00 * 10^{-8}$	$7.39 * 10^{-8}$	$2.85 * 10^{-9}$	$1.63 * 10^{-8}$	$5.57 * 10^{-17}$	$1.61 * 10^{-16}$
M_2M_4	$9.24 * 10^{-8}$	$1.89 * 10^{-7}$	$2.86 * 10^{-8}$	$8.74 * 10^{-8}$	$7.63 * 10^{-15}$	$2.08 * 10^{-14}$
M_3M_4	$5.00 * 10^{-7}$	$9.74 * 10^{-7}$	$1.53 * 10^{-7}$	$4.64 * 10^{-7}$	$4.56 * 10^{-14}$	$1.24 * 10^{-13}$
$M_1M_2M_3$ +)	$3.00 * 10^{-8}$	$7.39 * 10^{-8}$	$2.85 * 10^{-9}$	$1.63 * 10^{-8}$	$5.57 * 10^{-17}$	$1.61 * 10^{-16}$

* $M_i^{(1)} \equiv M_i^{(3)}$

** $M_i^{(2)} \equiv M_i^{(4)}$

+) All threefold intersections are identical to $M_1M_2M_3$; cf. (6.21)

T_1 = 1240 hrs

T_2 = 1240.5 hrs

T_3 = 1576 hrs

T_4 = 1578 hrs

Table 6.12. PROBABILITY OF SYSTEM FAILURE
(T_0 = 1000 hrs)

	PROBABILITY OF SYSTEM FAILURE								
	STRATEGY (i)			STRATEGY (ii)			STRATEGY (iii)		
	ALL COMPONENTS NON-REPAIRABLE (CLASS 1)			COMP. c_1, c_3 AND c_5 ARE PERIODICALLY INSPECTED (CLASS 4) COMP. c_2, c_4 AND c_6 ARE NON-REPAIRABLE (CLASS 1)			ALL COMPONENTS CONTINUOUSLY INSPECTED (CLASS 2)		
	EXACT	FIRST ORDER APPROXIMATION		EXACT	FIRST ORDER APPROXIMATION		EXACT	FIRST ORDER APPROXIMATION	
PROBABILITY	SOLUTION	UPPERBOUND	DEVIATION++)	SOLUTION	UPPERBOUND	DEVIATION++)	SOLUTION	UPPERBOUND	DEVIATION++)
$Q_1(T_1)$	$6.13 * 10^{-2}$	$6.13 * 10^{-2}$	$7.45 * 10^{-5}$	$2.09 * 10^{-2}$	$2.09 * 10^{-2}$	$2.44 * 10^{-5}$	$1.33 * 10^{-2}$	$1.33 * 10^{-2}$	$3.17 * 10^{-6}$
$Q_2(T_2)$	$2.00 * 10^{-2}$	$2.00 * 10^{-2}$	$4.91 * 10^{-5}$	$2.00 * 10^{-3}$	$2.00 * 10^{-3}$	$4.79 * 10^{-6}$	$8.93 * 10^{-6}$	$8.93 * 10^{-6}$	$4.46 * 10^{-11}$
$Q_3(T_3)$	$7.73 * 10^{-2}$	$7.74 * 10^{-2}$	$1.20 * 10^{-4}$	$3.76 * 10^{-2}$	$3.77 * 10^{-2}$	$5.70 * 10^{-5}$	$2.98 * 10^{-2}$	$2.98 * 10^{-2}$	$1.54 * 10^{-5}$
$Q_4(T_4)$	$3.02 * 10^{-2}$	$3.03 * 10^{-2}$	$9.49 * 10^{-5}$	$6.84 * 10^{-3}$	$9.86 * 10^{-3}$	$2.12 * 10^{-5}$	$1.01 * 10^{-5}$	$1.01 * 10^{-5}$	$8.06 * 10^{-11}$
$Q_{1,3}(T_1,T_3)$	$6.13 * 10^{-2}$	$6.15 * 10^{-2}$	$3.38 * 10^{-4}$	$2.09 * 10^{-2}$	$2.10 * 10^{-2}$	$1.25 * 10^{-4}$	$1.30 * 10^{-2}$	$1.30 * 10^{-2}$	$1.78 * 10^{-3}$
$Q_{2,4}(T_2,T_4)$	$2.00 * 10^{-2}$	$2.01 * 10^{-2}$	$2.22 * 10^{-4}$	$2.00 * 10^{-3}$	$2.02 * 10^{-3}$	$2.48 * 10^{-5}$	$9.03 * 10^{-11}$	$9.03 * 10^{-11}$	$1.17 * 10^{-15}$

++) Deviation: difference between the upper- and lowerbound.

Table 6.13. PROBABILITY OF SINGLE SYSTEM FAILURE FOR THE HRS

PROBABILITIES OF SINGLE SYSTEM FAILURE OBTAINED BY THE PRESENT STUDY AND THE FORMER APPROACH (T_0 = 1000 hrs)

	PROBABILITY OF SYSTEM FAILURE											
	STRATEGY (i)				STRATEGY (ii)				STRATEGY (iii)			
	ALL COMPONENTS NON-REPAIRABLE (CLASS 1)				COMP. c_1, c_3 AND c_5 ARE PERIODICALLY INSPECTED (CLASS 4) COMP. c_2, c_4 AND c_6 ARE NON-REPAIRABLE (CLASS 1)				ALL COMPONENTS ARE CONTINUOUSLY INSPECTED (CLASS 2)			
	PRESENT STUDY		FORMER METHOD		PRESENT STUDY		FORMER METHOD		PRESENT STUDY		FORMER METHOD	
PROBABILITY	UPPERBOUND	DEVIATION+)	UPPERBOUND	DEVIATION+)	UPPERBOUND	DEVIATION+)	UPPERBOUND	DEVIATION+)	UPPERBOUND	DEVIATION+)	UPPERBOUND	DEVIATION+)
$Q_1(T_1)$	$6.13*10^{-2}$	$7.45*10^{-5}$	$6.14*10^{-2}$	$7.45*10^{-5}$	$2.09*10^{-2}$	$2.44*10^{-5}$	$4.37*10^{-3}$	$3.89*10^{-6}$	$1.33*10^{-2}$	$3.17*10^{-6}$	$1.20*10^{-3}$	$2.40*10^{-9}$
$Q_2(T_2)$	$2.00*10^{-2}$	$4.91*10^{-5}$	$2.00*10^{-2}$	$4.90*10^{-5}$	$2.00*10^{-3}$	$4.79*10^{-6}$	$1.81*10^{-4}$	$3.84*10^{-7}$	$8.93*10^{-6}$	$4.46*10^{-11}$	$8.59*10^{-6}$	$3.43*10^{-11}$
$Q_3(T_3)$	$7.74*10^{-2}$	$1.20*10^{-4}$	$7.74*10^{-2}$	$1.19*10^{-4}$	$3.77*10^{-2}$	$5.70*10^{-5}$	$4.71*10^{-3}$	$4.94*10^{-6}$	$2.98*10^{-2}$	$1.54*10^{-5}$	$1.20*10^{-3}$	$2.40*10^{-9}$
$Q_4(T_4)$	$3.03*10^{-2}$	$9.49*10^{-5}$	$3.03*10^{-2}$	$9.45*10^{-5}$	$6.86*10^{-3}$	$2.12*10^{-5}$	$1.84*10^{-4}$	$4.73*10^{-7}$	$1.01*10^{-5}$	$8.06*10^{-11}$	$8.59*10^{-6}$	$3.43*10^{-11}$

+) Deviation: difference between upper- and lowerbound

6.2.9. Some remarks concerning the outcome of the numerical calculations

In this section we shall give some comments on the results of the numerical calculations. These comments will be divided into two parts, viz. (i) those on the exact results and (ii) those on the approximate results.

6.2.9.1. Remarks concerning the exact probabilities for mission success

(1) Difference between the three strategies

(a) With respect to the upperbranch of the event tree of fig. 6.2. (mission no. 1) it appears from table 6.6. and table 6.7. that strategy (iii) shows a lower probability for mission failure than strategy (ii), which in turn shows a lower probability for mission failure than strategy (i). Therefore strategy (iii) is the best one with respect to the probability of occurrence of the upperbranch. By applying strategy (iii) the highest probability of mission success for mission no. 1 is obtained.
This conclusion could be expected, because the procedure of continuous testing (applied for all components for strategy (iii)) is the optimal test procedure with respect to component behaviour.

(b) For mission no. 3 ($u_1=u_2=1, u_3=0$) strategy (i) shows the lowest probability of mission success, followed by strategy (ii). Strategy (iii) shows the highest probability (see table 6.6. and table 6.7.).
The explanation for this is the following: the probability that the subsystems S_1 and S_2 survive their respective phases is for strategy (i) (all components non-repairable) smaller than it is for the other two strategies where tests and repair are performed during the OR-phase. However, the probability that subsystem S_3 fails during its phase is for strategy (i) greater than for the other two strategies. These two factors lead to a higher probability when strategy (i) is applied instead of strategy (ii) or strategy (iii). The same argument explains the difference between strategy (i) and strategy (iii). Here the fact that repair is possible during the mission with strategy (iii) plays also a role.

(c) During the mission no repair is allowed in the case of strategy (i) and in the case of strategy (ii). This implies that a subsystem that fails during the mission, remains failed for the residual mission time.

In our example subsystem S_2 and subsystem S_4 are identical. In mission no. 4 ($u_1=1, u_2=0, u_3=u_4=1$) subsystem S_2 has to fail and subsystem S_4 has to survive. This is physically impossible in case of the strategies (i) and (ii). Therefore the probability of the occurrence of this branch is zero for the first two strategies (see the tables 6.6. and 6.7.).

However, this conclusion is not true for strategy (iii). Here repair for subsystem S_2 is allowed during phase 3, and therefore the probability of mission success for mission no. 4 is positive.

(2) Comparison of the probabilities of mission success at different instants depending on the starting time of the mission

Table 6.6. contains for all strategies the probabilities of mission success for all missions that start at T_0 = 200 hrs, whereas table 6.7. shows the same probabilities for all missions that start at T_0 = 1000 hrs.
Comparing the corresponding probabilities for strategy (i) it is noticed that the probabilities for T_0 = 1000 hrs are greater than those for T_0 = 200 hrs. The same is true for the corresponding probabilities for strategy (ii), although less significant, due to testing and repair during the OR-phase.
Comparing the corresponding probabilities in the tables 6.6. and 6.7. for strategy (iii), it is seen that there is no difference between them. This is caused by the fact that all components for strategy (iii) are continuously inspected during the OR-phase, and therefore the component unavailability approaches a constant value. It is then said that the component has reached its *steady state*.
So, if all components are in the steady state at instant T_0 = 200 hrs they are also in the steady state at instant T_0 = 1000 hrs, i.e. both missions start with the same initial conditions concerning the components unavailabilities. Therefore the corresponding probabilities of mission success in the tables 6.6. and 6.7. do not differ for strategy (iii).

6.2.9.2. Remarks concerning the upperbound approximation for the probability of mission success

(a) Comparison of the corresponding upperbound approximations for the probabilities of mission success in the case of the strategies (i) and (ii) for T_0 = 200 hrs and T_0 = 1000 hrs (see tables 6.6. and 6.7.) shows that the approximation becomes less accurate when T_0 increases. In fact this is caused by the increasing component unavailabilities of class 1 components (non-repairable components). No differences appear in the corresponding probabilities in the case of strategy (iii). The explanation for this phenomenon is given in 6.2.9.1.(2).

(b) If the probability of occurrence of a branch from an event tree is calculated by the assumption that all systems are mutually independent, i.e. they have no components in common, then the approximation (see the rules (R1) and (R2)) in section 6.2.8. yields often an *under*-estimation of the exact probability of mission success.

In the case of the HRS this type of *under*-estimation occurs for (see table 6.8.):

strategy (i): mission no. 5;
strategy (ii): mission no. 1, 2, 3, 5, 6, 7;
strategy (iii): all missions.

The difference between the true value of the probability of mission success and the under-estimated value increases accordingly as the system dependencies increase (as an example see section 6.4., table 6.19. with respect to the phased mission of a BWR).
It may therefore be concluded that application of the rules (R1) and (R2) (see section 6.2.8.) in the case of a risk analysis may lead to an under-estimation of the total calculated risk.
Obviously, the approach proposed in the present study indeed creates upperbounds for the probabilities of mission success. Therefore, an under-estimation of the total risk in the case of a risk analysis can not occur.

(c) The probability of mission success for mission no. 4 in case of the strategies (i) and (ii) equals zero (see that table 6.6. and 6.7.). However, the upperbound approximation produces a probability of

mission success that is greater than zero with a maximal deviation that is greater than the calculated upperbound. For such situations where the upperbound for the probability of mission success is smaller than the deviation it can sometimes be deduced that the exact probability of mission success equals zero, assuming that the concerned probabilities are rather small. On conditions this statement is proved in section 6.3.6. The cases for which the probability of mission success equals zero by definition are also treated in section 6.3.6.
In our example concerning mission no. 4 of the HRS it is obvious that if subsystem S_2 has to fail during its phase, subsystem S_4 (which is identical to subsystem S_2) can not survive its phase in case of the strategies (i) and (ii), because no repair during the mission is allowed.

6.3. Phased mission analysis

On the basis of a very simple system the methodology in treating a phased mission has been illustrated in the foregoing section. In this section we shall develop the general approach. It ultimately leads to an exact solution. Another advantage of the method presented here is the treatment of phased missions during which one or more subsystems have to be failed during the mission, i.e. the introduction of task 1 and task 0 for a subsystem (cf. section 2.4.). This means that in treating an event tree it is not necessary to introduce special gates (like a NOT-gate).
Because complex systems contain a large number of minimal cut sets (sometimes millions), it is in practical situations preferable to calculate an upperbound for the probability of mission success. From the exact solution for the probability, as given in this study, it is possible to derive such an upperbound together with a lowerbound.
Therefore we shall present in the next sections for the probability of mission success:

- an upperbound for mission success;
- the difference between the upper- and lowerbound. In the sequel we shall call this difference the *deviation*.

For the calculation of the upperbounds we shall often apply the inequalities of Bonferroni (cf. Fréchet [28]). Therefore we shall first give a brief description of these inequalities.

Assume that $A_1, A_2, \ldots, A_n$ are events and denote by:

$$V_1 = \sum_{i_1=1}^{n} \Pr\{A_{i_1}\},$$

$$V_2 = \sum_{i_1=1}^{n-1} \sum_{i_2=i_1+1}^{n} \Pr\{A_{i_1} A_{i_2}\}.$$

Then with

$$P \stackrel{def}{=} \Pr\{\bigcup_{i=1}^{n} A_i\}$$

the following upper- and lowerbound for the probability P can be deduced (cf. Frechet [28]):

$$V_1 - V_2 \leq P \leq V_1. \tag{6.30}$$

6.3.1. The phased mission where system S has to survive every phase

The phased mission treated in this section can be characterized by "system S survives every phase". This event is equivalent to the event "subsystem S_j survives phase j, j=1,...,K", where K denotes the number of phases. In fact we treat the upperbranch of an event tree (see for example fig. 2.5.). This means that the mission can be described by the sequence

$$\{u_1 = 1, u_2 = 1, \ldots, u_K = 1\}, \tag{6.31}$$

where u_j, j=1,...,K, is described in section 2.4. Denote by $M_0(T_0)$ the probability that the mission defined by expression (6.31) and starting at instant T_0 is successful so that:

$$M_0(T_0) = \Pr\{\text{subsystem } S_j \text{ survives phase } j, j=1,\ldots,K\}, \quad T_0 \geq 0. \tag{6.32}$$

Because no repair is permitted to subsystem S_j during phase j, it is clear that the event "subsystem S_j survives phase j" is equivalent to the event "subsystem S_j is available at instant T_j", where T_j is the instant at which phase j terminates (see section 2.2.).

So relation (6.32) becomes

$$M_0(T_0) = \Pr\{\underline{y}_1(T_1)=0, \underline{y}_2(T_2)=0, \ldots, \underline{y}_K(T_K)=0\} \ , \tag{6.33}$$

where $\underline{y}_j(t)$, $j=1,\ldots,K$ is the state variable of subsystem S_j at instant t as defined by (2.1).
For reliable systems the probability $M_0(T_0)$ is as a rule near to the value one and in practice it is more usual to deal with the complementary probability $J_0(T_0)=1-M_0(T_0)$ of mission failure.
So in the following we shall deal with $J_0(T_0)$.
From (6.33) it follows that:

$$J_0(T_0) = \Pr\{\overline{(\underline{y}_1(T_1)=0, \underline{y}_2(T_2)=0, \ldots, \underline{y}_K(T_K)=0)}\}$$

$$= \Pr\{\bigcup_{j=1}^{K} (\underline{y}_j(T_j)=1)\} \ . \tag{6.34}$$

From (6.30) it follows that an upperbound for $J_0(T_0)$ is obtained by the sum of the probabilities of single subsystem failure. The failure probability Q_j of each subsystem S_j is bounded from above by Q_j', being the sum of the occurrence probabilities of its minimal cut sets (cf. section 5.3.2.2.). Therefore, the upperbound $J_0'(T_0)$ of the probability $J_0(T_0)$ of mission failure, is given by

$$J_0'(T_0) = \sum_{j=1}^{K} Q_j' \geq J_0(T_0) \tag{6.35}$$

Next we will derive the deviation in the upperbound $J_0'(T_0)$. From (6.30) it is seen that a lowerbound for $J_0(T_0)$ in (6.34) is given by the difference of two terms, viz. the first term being the sum of the probabilities of single system failure and the second term being the sum of the probabilities of joint failure of two subsystems. So

$$J_0(T_0) \geq \sum_{j=1}^{K} \Pr\{\underline{y}_j(T_j)=1\}$$

$$- \sum_{j_1=1}^{K-1} \sum_{j_2=j_1+1}^{K} \Pr\{\underline{y}_{j_1}(T_{j_1})=1, \underline{y}_{j_2}(T_{j_2})=1\}. \tag{6.36}$$

If we denote by L'_j the sum of the occurrence probabilities of the two-fold intersections of the minimal cut sets of subsystem S_j at instant T_j, and by Q'_{j_1,j_2} the "rare event" approximation (cf. section 5.3.2.2.) of the probability of a joint failure of the subsystems S_{j_1} (at instant T_{j_1}) and S_{j_2} (at instant T_{j_2}), then it is easily deduced from (6.36) that

$$J_0(T_0) \geq J'_0(T_0) - (L'_j + \sum_{j_1=1}^{K-1} \sum_{j_2=j_1+1}^{K} Q'_{j_1,j_2}) , \tag{6.37}$$

$J'_0(T_0)$ being given by (6.35).
From (6.35) and (6.37) it is obvious that the deviation in $J'_0(T_0)$ is bounded from above by

$$E'_0(T_0) = L'_j + \sum_{j_1=1}^{K-1} \sum_{j_2=j_1+1}^{K} Q'_{j_1,j_2} . \tag{6.38}$$

6.3.2. The phased mission where exactly one subsystem has to fail during the mission

The phased mission described in this section is characterized by the following sequence of u's:

$$\{u_1=1,\ldots,u_{j-1}=1,u_j=0,u_{j+1}=1,\ldots,u_K=1\} , \tag{6.39}$$

i.e. the event "every subsystem survives its phase, except subsystem S_j which fails during its phase".
The probability $M_j(T_0)$ of mission success for the mission in (6.39) is given by the following identity:

$$M_j(T_0) = \Pr\{(\bigcap_{\substack{k=1 \\ k\neq j}}^{K} \underline{y}_k(T_k)=0),\underline{y}_j(T_j)=1\} , \quad j=1,\ldots,K. \tag{6.40}$$

$\underline{y}_j(T_j)$ being the state variable of subsystem S_j. From (6.40) we obtain

$$M_j(T_0) = \Pr\{y_j(T_j)=1\} - \Pr\{\bigcup_{\substack{k=1\\k\neq j}}^{K} (y_k(T_k)=1, y_j(T_j)=1)\} ,$$
$$j=1,\ldots,K . \qquad (6.41)$$

An upperbound for $M_j(T_0)$ is obtained by the failure probability of subsystem S_j at instant T_j, which in turn is bounded from above by Q_j', being the sum of the occurrence probabilities of its minimal cut sets. So, the upperbound $M_j'(T_0)$ for $M_j(T_0)$ is given by:

$$M_j'(T_0) = Q_j' , \quad j=1,\ldots,K . \qquad (6.42)$$

Applying the "inclusion-exclusion" principle (cf. section 5.3.2.2.) and (6.30) to the probabilities in the right hand side of (6.41), it is easily seen that the deviation in the upperbound $M_j'(T_0)$ for the probability of mission success $M_j(T_0)$ is bounded from above by:

$$E_j'(T_0) = L_j' + \sum_{\substack{k=1\\k\neq j}}^{K} Q'_{k,j} , \quad j=1,\ldots,K. \qquad (6.43)$$

L_j' being the sum of the occurrence probabilities of the two-fold intersections of the minimal cut sets of subsystem S_j and $Q'_{k,j}$ being the "rare event" approximation for the probability of a joint failure of the subsystems S_k (at instant T_k) and S_j (at instant T_j).

6.3.3. The phased mission where exactly two subsystems have to fail during the mission

The phased mission discussed in this section is characterized by

$$\{u_1=1,\ldots,u_{j_1-1}=1,u_{j_1}=0,u_{j_1+1}=1,\ldots,$$
$$u_{j_2-1}=1,u_{j_2}=0,u_{j_2+1}=1,\ldots,u_K=1\} ,$$

i.e. all subsystems survive their respective phases except the subsystems S_{j_1} and S_{j_2} that fail during phase j_1 and phase j_2, respectively. Therefore, the probability $M_{j_1,j_2}(T_0)$ of mission success reads:

$$M_{j_1,j_2}(T_0) = \Pr\{\bigcap_{\substack{j=1 \\ j\neq j_1,j_2}}^{K} (\underline{y}_j(T_j)=0), \underline{y}_{j_1}(T_{j_1})=1, \underline{y}_{j_2}(T_{j_2})=1\}$$

$$= \Pr\{\underline{y}_{j_1}(T_{j_1})=1, \underline{y}_{j_2}(T_{j_2})=1\}$$

$$- \Pr\{\bigcup_{\substack{j=1 \\ j\neq j_1,j_2}}^{K} (\underline{y}_j(T_j)=1), \underline{y}_{j_1}(T_{j_1})=1, \underline{y}_{j_2}(T_{j_2})=1\} ,$$

$$j_1,j_2=1,\ldots,K;$$

$$j_1\neq j_2 . \qquad (6.44)$$

Applying the same method as in the foregoing sections we obtain from (6.44) for the upperbound $M'_{j_1,j_2}(T_0)$ of the probability of mission success $M_{j_1,j_2}(T_0)$ the following relation:

$$M'_{j_1,j_2}(T_0) = Q'_{j_1,j_2} , \quad j_1,j_2=1,\ldots,K;\ j_1\neq j_2 , \qquad (6.45)$$

Q'_{j_1,j_2} being the "rare event" approximation of the probability of a joint failure of the subsystems S_{j_1} and S_{j_2}.
The deviation $E'_{j_1,j_2}(T_0)$ in $M'_{j_1,j_2}(T_0)$ is given by:

$$E'_{j_1,j_2}(T_0) = L'_{j_1,j_2} + \sum_{\substack{j=1 \\ j\neq j_1,j_2}}^{K} Q'_{j_1,j_2,j} , \quad j_1,j_2=1,\ldots,K;\ j_1\neq j_2 , \qquad (6.46)$$

L'_{j_1,j_2} being the from above bounded deviation in Q'_{j_1,j_2} and $Q'_{j_1,j_2,j}$ being the "rare event" approximation of the probability of a joint failure of the three subsystems S_{j_1} (at instant T_{j_1}), S_{j_2} (at instant T_{j_2}) and S_j (at instant T_j).

6.3.4. The phased mission where exactly k subsystems have to fail during the mission

In this section the general phased mission will be discussed. This general phased mission can be characterized by a sequence of u's denoting the tasks for the several subsystems, i.e. $u_j=0$ means subsystem S_j has to fail during the j^{th} phase whereas $u_j=1$ means that subsystem S_j has to survive phase j. Therefore the phased mission where exactly k subsystems have to fail during their appropriate phases can be characterized by:

$$\{u_j=1, j=1,\ldots,K \text{ with } j\neq j_1,\ldots,j_k; u_{j_1}=u_{j_2}=\ldots=u_{j_k}=0\} .$$

So the probability $M_{j_1,\ldots,j_k}(T_0)$ of mission success reads:

$$\begin{aligned} M_{j_1,\ldots,j_k}(T_0) &= \Pr\{\text{subsystem } S_j \text{ has to survive phase } j, \\ &\qquad j=1,\ldots,K; j\neq j_1,\ldots,j_k; \text{ and subsystem } S_\ell \\ &\qquad \text{has to fail during phase } \ell,\ \ell=j_1,\ldots,j_k\} \\ &= \Pr\{\Big(\bigcap_{\substack{j=1 \\ j\neq j_1,\ldots,j_k}}^{K} (\underline{y}_j(T_j)=0)\Big), \underline{y}_{j_1}(T_{j_1})=1,\ldots,\underline{y}_{j_k}(T_{j_k})=1\} \\ &= \Pr\{\underline{y}_{j_1}(T_{j_1})=1,\ldots,\underline{y}_{j_k}(T_{j_k})=1\} \qquad (6.47) \\ &\quad - \Pr\{\bigcup_{\substack{j=1 \\ j\neq j_1,\ldots,j_k}}^{K} (\underline{y}_{j_1}(T_{j_1})=1,\ldots,\underline{y}_{j_k}(T_{j_k})=1, \\ &\qquad\qquad \underline{y}_j(T_j)=1\} . \end{aligned}$$

From (6.47) it can easily be deduced, by applying the "rare event" approximation and the inequalities (6.30), that the upperbound $M'_{j_1,\ldots,j_k}(T_0)$ for the probability of mission success and the deviation $E'_{j_1,\ldots,j_k}(T_0)$ are given by the following relations:

$$M'_{j_1,\ldots,j_k}(T_0) = Q'_{j_1,\ldots,j_k} , \qquad (6.48)$$

Table 6.14. UPPERBOUNDS AND DEVIATIONS TOGETHER WITH THEIR ASSOCIATED VARIABLES FOR THE PROBABILITIES OF MISSION SUCCESS

NUMBER OF SYSTEMS TO BE FAILED DURING THE MISSION ℓ	UPPERBOUND FOR THE PROBABILITY OF MISSION SUCCESS $M'_{j_1,\ldots,j_\ell}(T_0)$	DEVIATION IN UPPERBOUND $E'_{j_1,\ldots,j_\ell}(T_0)$	ASSOCIATED VARIABLES $Q'_{j_1,\ldots,j_\ell}$ $L'_{j_1,\ldots,j_\ell}$
0	(*) $\sum_{j=1}^{K} Q'_j$	$\sum_{j=1}^{K} L'_j + \sum_{j_1=1}^{K-1} \sum_{j_2=j_1+1}^{K} Q'_{j_1,j_2}$	(***) $Q'_j = \sum_{\ell=1}^{N_j} \Pr\{\underline{\psi}_\ell^{(j)}(T_j)=1\}$ $Q'_{j_1,j_2} = \sum_{\ell_1=1}^{N_{j_1}} \sum_{\ell_2=1}^{N_{j_2}} \Pr\{\underline{\psi}_{\ell_1}^{(j_1)}(T_{j_1})=1, \underline{\psi}_{\ell_2}^{(j_2)}(T_{j_2})=1\}$ $L'_j = \sum_{n_1=1}^{N_j-1} \sum_{n_2=n_1+1}^{N_j} \Pr\{\underline{\psi}_{n_1}^{(j)}(T_j)=1, \underline{\psi}_{n_2}^{(j)}(T_j)=1\}$
1	Q'_j	$L'_j + \sum_{\substack{k=1 \\ k\neq j}}^{K} Q'_{j,k}$	
2	Q'_{j_1,j_2}	$L'_{j_1,j_2} + \sum_{\substack{j=1 \\ j\neq j_1,j_2}}^{K} Q'_{j_1,j_2,j}$	$Q'_{j_1,j_2,j} = \sum_{\ell_1=1}^{N_{j_1}} \sum_{\ell_2=1}^{N_{j_2}} \sum_{\ell_3=1}^{N_j} \Pr\{\underline{\psi}_{\ell_1}^{(j_1)}(T_{j_1})=1, \underline{\psi}_{\ell_2}^{(j_2)}(T_{j_2})=1, \underline{\psi}_{\ell_3}^{(j_3)}(T_{j_3})=1\}$ L'_{j_1,j_2} not explicitly given (**)
k (k=3,...,K)	$Q'_{j_1,\ldots,j_k}$	$L'_{j_1,\ldots,j_k} + \sum_{\substack{j=1 \\ j\neq j_1,\ldots,j_k}}^{K} Q'_{j_1,\ldots,j_k,j}$	$Q'_{j_1,\ldots,j_k} = \sum_{n_1=1}^{N_{j_1}} \sum_{n_2=1}^{N_{j_2}} \cdots \sum_{n_k=1}^{N_{j_k}} \Pr\{\underline{\psi}_{n_1}^{(j_1)}(T_{j_1})=1, \underline{\psi}_{n_2}^{(j_2)}(T_{j_2})=1, \ldots, \underline{\psi}_{n_k}^{(j_k)}(T_{j_k})=1\}$ $L'_{j_1,\ldots,j_k}$ not further developed

(*) Probability $J_0(T_0)$ of mission failure

(**) Inserted in the reliability computer program PHAMISS

(***) $\underline{\psi}_\ell^{(j)}(t)$: state variable for minimal cut set M_ℓ of subsystem S_j, considered at instant t

N_j: number of minimal cut sets of subsystem S_j

$$E'_{j_1,\ldots,j_k}(T_0) = L'_{j_1,\ldots,j_k} + \sum_{\substack{j=1 \\ j\neq j_1,\ldots,j_k}}^{K} Q'_{j_1,\ldots,j_k,j} \quad , \qquad (6.49)$$

with $Q'_{j_1,\ldots,j_k}$ being the "rare event" approximation of the probability of a joint failure of the subsystems $S_{j_1},\ldots,S_{j_k}$, $L'_{j_1,\ldots,j_k}$ being the deviation in $Q'_{j_1,\ldots,j_k}$ and $Q'_{j_1,\ldots,j_k,j}$ being the "rare event" approximation of the probability of a joint failure of the subsystems $S_{j_1},\ldots,S_{j_k}$ and S_j.

In table 6.14. the results of the sections 6.3.1.,...,6.3.4. are summarized, i.e. table 6.14. contains the upperbounds and deviations made in the upperbound calculation for mission failure in case that every subsystem has to survive its appropriate phase and for mission success for all the other phased missions.

6.3.5. Calculation of the probability $Z^{(j_1,\ldots,j_k)}_{n_1,\ldots,n_k}$

To calculate the probability of mission success $M_{j_1,\ldots,j_k}(T_0)$ (or mission failure $J_0(T_0)$) it is necessary to know the basic probabilities $Z^{(j_1,\ldots,j_k)}_{n_1,\ldots,n_k}$ defined by:

$$Z^{(j_1,\ldots,j_k)}_{n_1,\ldots,n_k} = \Pr\{\underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1,\ldots,\underline{\psi}^{(j_k)}_{n_k}(T_{j_k})=1\} \quad , \quad k=1,\ldots,K, \qquad (6.50)$$

with $\underline{\psi}^{(j)}_{n}(T_j)$ being the state variable of minimal cut set M_n of subsystem S_j at instant T_j. Each minimal cut set $\underline{\psi}^{(j)}_{n}(T_j)$ consists of one or more components that are in the fail state. The state variables $\underline{x}_i(t)$ of the components are considered to be mutually independent, i.e.

$$\Pr\{\bigcap_{i=1}^{N}(\underline{x}_i(t)=1)\} = \prod_{i=1}^{N}\Pr\{\underline{x}_i(t)=1\} \quad ,$$

N being the number of components in the system.

In the next sections we shall discuss the scheme for the calculation of $Z^{(j_1,\ldots,j_k)}_{n_1,\ldots,n_k}$. As an introduction $Z^{(j)}_{n}$ shall be treated first.

Next a sketch is given of the systematic calculation of $Z_{n_1,n_2}^{(j_1,j_2)}$. The last section of this paragraph will be devoted to the general case, i.e. $Z_{n_1,\ldots,n_k}^{(j_1,\ldots,j_k)}$ for general k.

6.3.5.1. Calculation of the probability $Z_n^{(j)}$

As it has already been mentioned, a minimal cut set may consist of several components, each component being in the fail state. Suppose that minimal cut set M_n of subsystem S_j consists of m components, i.e. the components $c_{i_1}, c_{i_2},\ldots,c_{i_m}$. It then follows that:

$$Z_n^{(j)} = \Pr\{\underline{\psi}_n^{(j)}(T_j)=1\}$$

$$= \Pr\{\underline{x}_{i_1}(T_j)=1,\underline{x}_{i_2}(T_j)=1,\ldots,\underline{x}_{i_m}(T_j)=1\}$$

$$= \prod_{\ell=1}^{m} \Pr\{\underline{x}_{i_\ell}(T_j)=1\}$$

$$= \prod_{\ell=1}^{m} q_{i_\ell}(T_j) \quad , \tag{6.51}$$

$\underline{x}_{i_\ell}(T_j)$, $\ell=1,\ldots,m$, being the state variable of component c_{i_ℓ} at instant T_j, and $q_{i_\ell}(T_j)$ being the unavailability of component c_i at instant T_j with

$$q_{i_\ell}(T_j) = 1 - A_{i_\ell}(T_j) \quad , \tag{6.52}$$

$A_{i_\ell}(T_j)$ being the component's availability.

The calculation of the component's availability $A_{i_\ell}(.)$ has been performed in chapter 4. Four different cases have to be considered.

(i) component c_i is a class 1 component, i.e. a non-repairable component. The calculation of $A_i(T_j)$ is performed according to (4.1);

(ii) component c_i is a class 2 component (continuously inspected). Then $A_i(T_j)$ is calculated by either (4.24) or (4.26) depending on the instant T_j, i.e. whether instant T_j belongs to the dormant part or

to the operational part of the period to which instant T_j belongs;

(iii) component c_i is a class 3 component (randomly inspected). Its availability has to be calculated by (4.49);

(iv) component c_i is a class 4 component (periodically inspected). The component's availability is given by (4.121).

6.3.5.2. Calculation of the probability $Z^{(j_1,j_2)}_{n_1,n_2}$ -

Suppose that $T_{j_1} < T_{j_2}$, then

$$Z^{(j_1,j_2)}_{n_1,n_2} = \Pr\{\underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1, \underline{\psi}^{(j_2)}_{n_2}(T_{j_2})=1\}$$

$$= \Pr\{\underline{\psi}^{(j_2)}_{n_2}(T_{j_2})=1 \,|\, \underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1\} \Pr\{\underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1\} \; . \qquad (6.53)$$

The last factor on the right hand side of relation (6.53) is the probability of the occurrence of cut set M_{n_1} of subsystem S_{j_1} at instant T_{j_1} as treated in section 6.3.5.1. The conditional probability in relation (6.53) it not simply the probability of the occurrence of cut set M_{n_2} of subsystem S_{j_2} at time T_{j_2}. This is only the case if cut set M_{n_1} and cut set M_{n_2} don't have components in common. Suppose this is not true, and that for example cut set M_{n_2} contains the components c_{i_1}, c_{i_2}, c_{i_3} while cut set M_{n_1} contains the components c_{i_1}, c_{i_2} and c_{i_4}. Then it follows for the conditional probability in relation (6.53) that

$$\Pr\{\underline{\psi}^{(j_2)}_{n_2}(T_{j_2})=1 \,|\, \underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1\}$$

$$= \Pr\{\underline{x}_{i_1}(T_{j_2})=1, \underline{x}_{i_2}(T_{j_2})=1, \underline{x}_{i_3}(T_{j_2})=1 \,| \qquad (6.54)$$

$$\underline{x}_{i_1}(T_{j_1})=1, \underline{x}_{i_2}(T_{j_1})=1, \underline{x}_{i_4}(T_{j_1})=1\},$$

where $\underline{x}_i(t)$ is the state variable of component c_i at time t. Because the families $\{\underline{x}_i(t), t\geq 0\}, i=1,\ldots,N$ are assumed to be independent families

(see assumption 2.5.4.) (6.54) becomes

$$\Pr\{\underline{\psi}_{n_2}^{(j_2)}(T_{j_2})=1 \,|\, \underline{\psi}_{n_2}^{(j_1)}(T_{j_1})=1\}$$

$$= \Pr\{\underline{x}_{i_1}(T_{j_2})=1 \,|\, \underline{x}_{i_1}(T_{j_1})=1\}\Pr\{\underline{x}_{i_2}(T_{j_2})=1 \,|\, \underline{x}_{i_2}(T_{j_1})=1\}$$

$$\cdot \Pr\{\underline{x}_{i_3}(T_{j_2})=1\} \,. \qquad (6.55)$$

Dependent on the maintenance policy applied to a component we have to distinguish two cases, i.e. the component is non-repairable during the mission or the component is a class 2 component (continuously inspected and repairable during the dormant part of a period). Therefore we shall assume in our eaxmple that component c_{i_1} is non-repairable during the mission and that component c_{i_2} is a continuously inspected (class 2) component. The first conditional probability in the right hand side of relation (6.55) becomes

$$\Pr\{\underline{x}_{i_1}(T_{j_2})=1 \,|\, \underline{x}_{i_1}(T_{j_1})=1\} = 1, \qquad (6.56)$$

because component c_{i_1} is non-repairable during the mission. So if it is in the fail state at instant T_{j_1} it will certainly be in the fail state at instant T_{j_2}, since both instants belong to the same mission.
The second conditional probability in (6.55) is more complicated to evaluate. The result reads

$$\Pr\{\underline{x}_{i_2}(T_{j_2})=1 \,|\, \underline{x}_{i_2}(T_{j_1})=1\}=1 \quad \text{, if } T_{j_2} \text{ and } T_{j_1} \text{ belong to the same operational part of a period of component } c_{i_2};$$

$$=1-P_{k^*}(T_{j_2}-T^*), \text{ otherwise.} \qquad (6.57)$$

In (6.57) k* denotes the number of periods of component c_{i_2} between T_{j_1} and T_{j_2}, however, not included the period containing instant T_{j_1}. The instant T* is the beginning of the next period of component c_{i_2} after T_{j_1}. If T_{j_1} and T_{j_2} belong to the same operational part of a period

of component c_{i_2}, the component remains failed at T_{j_2} if it was unavailable at $T_{j_1} < T_{j_2}$, because no repair is permitted during an operational part of the component. If T_{j_2} and T_{j_1} don't belong to the same operational part the unavailability of the component can be calculated by means of formula (4.24) or (4.26), its renewal process starting at T* and the initial state of the component being the *fail state*, (cf. section 4.6.2.). The $\Pr\{\underline{x}_{i_3}(T_{j_2})=1\}$ is simply the unavailability of component c_{i_3} at instant T_{j_2}, see (6.52).

6.3.5.3. Calculation of the probability $Z^{(j_1,\ldots,j_k)}_{n_1,\ldots,n_k}$ -

Assume that $T_{j_1} < T_{j_2} < \ldots < T_{j_k}$, then

$$Z^{(j_1,\ldots,j_k)}_{n_1,\ldots,n_k} = \Pr\{\underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1,\ldots,\underline{\psi}^{(j_k)}_{n_k}(T_{j_k})=1\}$$

$$= \Pr\{\underline{\psi}^{(j_k)}_{n_k}(T_{j_k})=1 \,|\, \underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1,\ldots,\underline{\psi}^{(j_{k-1})}_{n_{k-1}}(T_{j_{k-1}})=1\}$$

$$\cdot \Pr\{\underline{\psi}^{(j_{k-1})}_{n_{k-1}}(T_{j_{k-1}})=1 \,|$$

$$\underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1,\ldots,\underline{\psi}^{(j_{k-2})}_{n_{k-2}}(T_{j_{k-2}})=1\}$$

$$\cdot \ldots$$

$$\cdot \Pr\{\underline{\psi}^{(j_2)}_{n_2}(T_{j_2})=1 \,|\, \underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1\}$$

$$\cdot \Pr\{\underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1\}. \qquad (6.58)$$

If k=1 or k=2 we get the cases that are treated in sections 6.3.5.1. and 6.3.5.2., respectively. So suppose k > 2.
The conditional probabilities in (6.58) can be treated in a similar way as it is done for the conditional probability of (6.54).

As a first example assume that component c_i only belongs to the minimal cut sets M_{n_r} and M_{n_k} of the subsystems S_{j_r} and S_{j_k}, respectively, with $r < k$. We want to calculate the first conditional probability arising in (6.58). This conditional probability is the product of the probabilities that every component belonging to minimal cut set M_{n_k} is in the fail state at instant T_{j_k}. So one factor of this product is:

$$\Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{\psi}_{n_1}^{(j_1)}(T_{j_1})=1,\ldots,\underline{\psi}_{n_{k-1}}^{(j_{k-1})}(T_{j_{k-1}})=1\}$$

$$= \Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{x}_i(T_{j_r})=1\} \quad , \tag{6.59}$$

because component c_i only belongs to the systems S_{j_k} and S_{j_r}.
From (6.57) and section 4.6.2. it follows for the conditional unavailability in (6.59) that:

$$\Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{x}_i(T_{j_r})=1\}=1 \quad \text{, if } T_{j_r} \text{ and } T_{j_k} \text{ belong to the same operational part;}$$

$$=1-P_{k^*}(T_{j_k}-T^*), \text{ otherwise.} \tag{6.60}$$

In (6.60) k^* is the number of periods between T_{j_k} and T_{j_r}, not included the period to which T_{j_r} belongs. T^* is the start of the next period after T_{j_r}.
As a second example we assume that component c_i belongs only to the minimal cut sets $M_{n_{r_1}}$, $M_{n_{r_2}}$ and M_{n_k} of the subsystems $S_{j_{r_1}}$, $S_{j_{r_2}}$ and S_{j_k}, respectively, with $r_1 < r_2 < k$. It now follows for the same conditional probability as treated before that we get:

$$\Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{\psi}_{n_1}^{(j_1)}(T_{j_1})=1,\ldots,\underline{\psi}_{n_{k-1}}^{(j_{k-1})}(T_{j_{k-1}})=1\}$$

$$= \Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{x}_i(T_{j_{r_1}})=1,\underline{x}_i(T_{j_{r_2}})=1\} \; . \tag{6.61}$$

In (6.61) the event "$\underline{x}_i(T_{j_k})=1$" is conditioned by two events, viz.

"$\underline{x}_i(T_{j_{r_1}})=1$" and $\underline{x}_i(T_{j_{r_2}})=1$". We first consider the case that lifetimes and repairtimes are negative exponentially distributed. Then the conditional probability in (6.61) changes to:

$$\Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{x}_i(T_{j_{r_1}})=1, \underline{x}_i(T_{j_{r_2}})=1\} = \Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{x}_i(T_{j_{r_2}})=1\}, \quad (6.62)$$

which probability has been treated in (6.60).
If in general component c_i belongs to the minimal cut sets

$$M_{j_{r_1}}, M_{j_{r_2}}, \ldots, M_{j_{r_s}}, M_{j_k},$$

of the subsystems $S_{j_{r_1}}, S_{j_{r_2}}, \ldots, S_{j_{r_s}}$, respectively, with

$$r_1, r_2, \ldots, r_s < k,$$

and $T \stackrel{\text{def}}{=} \max(T_{j_{r_1}}, T_{j_{r_2}}, \ldots, T_{j_{r_s}})$, then

$$\begin{aligned}
\Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{\psi}_{n_1}^{(j_1)}(T_{j_1})=1, \ldots, \underline{\psi}_{n_{k-1}}^{(j_{k-1})}(T_{j_{k-1}})=1\} \\
= \Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{x}_i(T_{j_{r_1}})=1, \ldots, \underline{x}_i(T_{j_{r_s}})=1\} \\
= \Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{x}_i(T)=1\}, \quad (6.63)
\end{aligned}$$

the latter probability treated in (6.60).

Next we consider the case that lifetimes and repairtimes have general distribution functions. This means that the properties of the negative exponential distribution as used in (6.62) and (6.63) are not valid anymore. No problem arises for the calculation of the unavailability of non-repairable, randomly inspected and periodically inspected components because they are assumed to be non-repairable during the mission itself (see chapter 2). But for continuously inspected (class 2) components the conditional probability

$$\Pr\{\underline{x}_i(T_{j_k})=1 \,|\, \underline{x}_i(T_{j_{r_1}})=1,\ldots,\underline{x}_i(T_{j_{r_s}})=1\}$$

has to be calculated by means of the methodology of the *derived renewal processes* as described in section 4.3.
Those calculations are very complicated. Further it is seen from the given examples (see fig. 4.4. and fig. 4.5.) that the unavailability in the case of a negative exponentially distributed lifetime is an upperbound for the unavailability in the case that the lifetime has an Erlang-2 distribution. Therefore it seems reasonable to apply the negative exponential distribution because of two reasons, viz. (i) possibly it provides an upperbound for the unavailability in the case of lifetime distributions with an increasing failure rate and (ii) it saves a lot of complicated calculations.

Each conditional probability in (6.58) is treated in the way as described in the foregoing. So the probability $Z^{(j_1,\ldots,j_k)}_{n_1,\ldots,n_k}$ is calculated for $j_1<j_2<\ldots<j_k$ by the following steps:

(i) break the probability $Z^{(j_1,\ldots,j_k)}_{n_1,\ldots,n_k}$ into the product of k-1 conditional probabilities of which the general form is given by:

$$\Pr\{\underline{\psi}^{(j_\ell)}_{n_\ell}(T_{j_\ell})=1 \,|\, \underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1,\ldots,\underline{\psi}^{(j_{\ell-1})}_{n_{\ell-1}}(T_{j_{\ell-1}})=1\},\ \ell=2,\ldots,k,$$

and the probability

$$\Pr\{\underline{\psi}^{(j_1)}_{n_1}(T_{j_1})=1\};$$

(ii) search for those components in minimal cut set M_{j_ℓ} (with state variable $\underline{\psi}^{(j_\ell)}_{n_\ell}(T_{j_\ell})$) which are not present in any minimal cut set contained in the condition. We shall mention this group of components *group 1*. The remaining components of minimal cut set M_{j_ℓ} shall be called *group 2*;

(iii) calculate the *absolute* unavailabilities for the components belonging to *group 1* (cf. section 6.3.5.1.);

(iv) calculate the *conditional* unavailabilities for the components belonging to *group 2*, as it has been shown in this section;

(v) the conditional probability in step (i) is now obtained by taking the product of all calculated component unavailabilities that are calculated in step (iii) and step (iv);

(vi) calculate $Pr\{\underline{\psi}_{n_1}^{(j_1)}(T_{j_1})\}$, (cf. section 6.3.5.1.);

(vii) the probability $Z_{n_1,\ldots,n_k}^{(j_1,\ldots,j_k)}$ is obtained by the multiplication of the obtained conditional probabilities calculated in step (v) and $Pr\{\underline{\psi}_{n_1}^{(j_1)}(T_{j_1})=1\}$ calculated in step (vi)

6.3.6. Remarks concerning the proposed method and its possibilities

(i) The present method shows that an exact solution for the probability of a phased mission is possible in principle

In this section, i.e. section 6.3., it is demonstrated that for the phased mission model as described in chapter 2 the exact solution for the probability of mission success in principle can be obtained by means of fault tree analysis.
Because complex systems contain in general a large number of minimal cut sets, upperbound approximations for the probability of mission success have to be applied for practical applications.
Within this study upperbounds for the probability of mission success together with their associated deviations are obtained.

(ii) The general approach offers the possibility of treating every branch of a time dependent event tree, i.e. the proposed method is very suitable for probabilistic risk analysis (PRA)

In chapter 2 the definition of a phased mission is given. This definition is actually an extension of the present one used in present day literature. The last mentioned definition only covers phased missions that occur as upperbranches of event trees, i.e. phased missions where each system has to survive its phase. The definition of chapter 2 defines *every* branch of the event tree as a phased mission. For each branch of an event tree the probability

of mission success can be obtained by the methodology as developed in this study (as a rule upperbounds for the probability of mission success will be calculated). Therefore the proposed method is very suitable for probabilistic risk analysis (PRA).

(iii) If the probability of the occurrence of the upperbranch of an event tree is calculated, then the probabilities of occurrence of all the other branches become also available

To calculate the probability of occurrence of the upperbranch of an event tree all single system failure probabilities and all joint (two by two, three by three, etc.) system failure probabilities have to be calculated.
The probability of occurrence of each other branch is composed of a number of the mentioned single and joint system failure probabilities.
In the case that an upperbound for the probability of occurrence of the upperbranch is calculated together with its deviation, then upperbounds for the probabilities of occurrence of the following branches also become available:

* for each branch where exactly one subsystem has to fail; in this case the associated deviation is calculated too;
* for each branch where exactly two subsystems have to fail.

Concerning the above mentioned it is assumed that the lengths of the phases, i.e. $T_{j+1}-T_j$, $j=1,\ldots,K$, for each branch are the same as they are for the upperbranch.
In the case that the length of a phase is shortened because system failure during that phase is defined to occur within a smaller time interval, a separate calculation has to be carried out for that particular branch.

(iv) The method takes partial system failures correctly into account

A *partial system failure* exists for a system if a number of components, but not all, of a minimal cut set of that system are in the *fail* state. So a *partial system failure* does not imply a *total system failure*.

If such a *partial system failure* exists for subsystem S_j and this partial failure mode contains a minimal cut set of the subsequent subsystem S_{j+1}, then subsystem S_{j+1} is in the fail state at the moment that it has to become operational. Therefore *partial system failures* of subsystem S_j are important for the behaviour of the subsystems that have to operate after subsystem S_j within a phased mission. It may be strongly conjectured that *partial system failures* are hardly taken into account correctly in probabilistic calculations. The approach presented in this study does take these *partial system failures* correctly into account.

(v) Detection of phased missions that are impossible to occur

Assume that:

(C1) subsystem S_{j_1} has to become operational before subsystem S_{j_2} during a phased mission with K phases;

(C2) subsystem S_{j_1} has to fail during its phase ($u_{j_1}=0$) and subsystem S_{j_2} has to survive its phase ($u_{j_2}=1$);

(C3) both subsystems consist of non-repairable components during the phased mission;

(C4) a system failure of subsystem S_{j_1} implies a system failure of subsystem S_{j_2}, i.e. each minimal cut set of S_{j_1} introduces at least one minimal cut set of S_{j_2};

(C5) the probabilities of single system failure and joint system failure are rather small.

From the assumptions (C1),...,(C4) it is directly seen that the probability of mission success for a branch with $\{...,u_{j_1}=0,...,u_{j_2}=1,...\}$ equals zero. This because subsystem S_{j_1} has to fail during its phase and subsystem S_{j_2} has to survive its phase. But no repair is applied to both subsystems. With assumption (C4) the mission is therefore impossible.

As a rule for complex systems this situation can not be seen beforehand. At the same time it is practically impossible to realize an exact calculation because of the large number of minimal cut sets

of the subsystems. Therefore upperbound approximations have to be carried out.

In the following we shall show that by means of the upperbound approximation for the probability of mission success and its associated deviation sometimes it is possible to detect that the phased mission can not occur.

For the sake of simplicity we assume that all subsystems have to survive their phases, except subsystem S_{j_1}.

An upperbound for the probability of mission success for the mission $\{u_1=1,\ldots,u_{j_1}=0,\ldots,u_{j_2}=1,\ldots,u_K=1\}$ is (cf. (6.42)):

$$M'_{j_1}(T_0) = Q'_{j_1} \quad , \tag{6.64}$$

Q'_{j_1} being an upperbound for the unavailability of subsystem S_{j_1}.

The deviation $E'_{j_1}(T_0)$ in the upperbound $M'_{j_1}(T_0)$ is (cf. (6.43)):

$$E'_{j_1}(T_0) = L'_{j_1} + \sum_{\substack{k=1 \\ k\neq j_1}}^{K} Q'_{j_1,k} \quad ,$$

L'_{j_1} and $Q'_{j_1,k}$ being described in section 6.3.2. From the assumptions (C3) and (C4) it is deduced that:

$$Q'_{j_1,j_2} = Q'_{j_1} \quad .$$

Therefore the deviation $E'_{j_1}(T_0)$ becomes

$$E'_{j_1}(T_0) = L'_{j_1} + Q'_{j_1} + \sum_{\substack{k=1 \\ k\neq j_1,j_2}}^{K} Q'_{j_1,k} \tag{6.65}$$

From (6.64) and (6.65) it is obvious that the following relation holds:

$$E'_{j_1}(T_0) \geq M'_{j_1}(T_0) \quad . \tag{6.66}$$

The inequality (6.66) is also true in case of large values for the component unavailabilities, for instance values near to one. Therefore, we assume that component unavailabilities are rather small, which implies that system unavailabilities are rather small (assumption (C5)). In that case the inequality (6.66) does not occur if the assumptions (C1),...,(C4) are not fulfilled.
We have proved that if the assumptions (C1),...,(C4) are fulfilled, then relation (6.66) holds. We can not prove the opposite case, but if a calculation of upperbound and deviation shows relation (6.66), we might have an indication.

Therefore, if assumption (C5) is true and the calculated deviation is greater than or equal to the calculated upperbound for the probability of mission success, it can sometimes be concluded that this particular mission can not occur, i.e. the probability of mission success equals zero.

6.4. An application: A phased mission within a Boiling Water Reactor

The example treated in this section is a phased mission that arises within a Boiling Water Reactor (BWR, cf. chapter 2) when a large *Loss of Coolant Accident* (LOCA) has occurred. The example is taken from Burdick et al [2] and we shall follow mainly their system description. Our description will be slightly different because we have incorporated some pipelines and valves to the system. We need these incorporations to give a consistent description of system behaviour through all phases. Fault trees and calculation results, however, are not affected by these alterations.
In chapter 2 a simplified description is given of the working state of a BWR and the function of the related safety systems in the case of a LOCA.

6.4.1. System and phase description

The following nomenclature is used in the example of this chapter:

BWR boiling water reactor;
ECCS emergency core cooling system;
LOCA loss of coolant accident;
HPCS high pressure core spray system;

LPCS low pressure core spray system;
LPCI low pressure core injection system;
ADS automatic depressurization system;
HX heat exchanger.

The ECCS used in this example consists of eight components (see for instance fig. 6.6.): HPCS, LPCS, LPCI-A, LPCI-B, LPCI-C, ADS, HX-A and HX-B. The name of the system is also used to denote the event of its failure. As seen in fig. 6.6., HX-A and HX-B are in two of the three LPCI loops. The difference between our ECCS and that of Burdick [2] is the incorporation of the pipeline which includes valve V4 and that of valve V5 (see fig. 6.6. until 6.8.).
Similar symmetric incorporations have been made in the right hand side circuit, they are not shown in the relevant figures.
We consider the accident initiated by a break of the main feedwater pipeline at point A, see fig. 6.6.
One mission of the ECCS is to prevent excessive heating of the fuel rods within the reactor vessel as soon as possible after a large LOCA and then to keep water circulating to and from the reactor vessel until the rods are cool (cf. chapter 2).
After a LOCA has occurred the phased mission of the ECCS consists for the case under consideration of the following three phases:

phase 1 - initial core cooling;
phase 2 - suppression pool cooling;
phase 3 - residual heat removal.

Each phase will now be discussed briefly:

For phase 1 (initial core cooling) either the HPCS alone, or the ADS and one of the LPCI's, or the ADS and the LPCS are needed, i.e. if all these three functions fail the mission of phase 1 fails. The purpose of phase 1 is to reflood the core and cool the fuel rods as soon as possible after the break. The valves V1 and V5 are open whereas the valves V2, V3 and V4 are closed. Phase 1 is assumed to last 0.5 hours.
For phase 2 (suppression pool cooling), the ADS is required to limit pressure build-up in the reactor vessel. One HX and the corresponding LPCI are needed to cool the water within the suppression pool. Also, one of the two remaining LPCI's, or the LPCS, or the HPCS is needed to circulate the

water from the suppression pool to the reactor vessel.
In phase 2, the valves V3 and V5 are open and the other valves are closed (see fig. 6.8.). The length of phase 2 is 36 hours.
In the description of the present phased mission it will be assumed that the system operates normally, i.e. the break has been repaired or is isolated, at the start of phase 3. (If this assumption is not introduced we have to consider a more complicated phased mission).
For phase 3 (residual heat removal) one of the HX and the corresponding LPCI are needed. At the start of phase 3 it is supposed that the valves V2 and V4 will be open and the valves V1, V3 and V5 will be closed (see fig. 6.9. The complete flow loop is not shown). Phase 3 is assumed to last 84 hours.

Note that in the case the component LPCI is used in fact the pump in the LPCI loop is meant. As already mentioned the detailed ECCS is not shown in the figures 6.6. until 6.9. It is assumed that all components, except the eight components that are mentioned at the beginning of this section, perform their required functions with certainty. In the figures 6.7.,..., 6.9. the heavy drawn parts indicate the most relevant part of the system for the concerned phase.

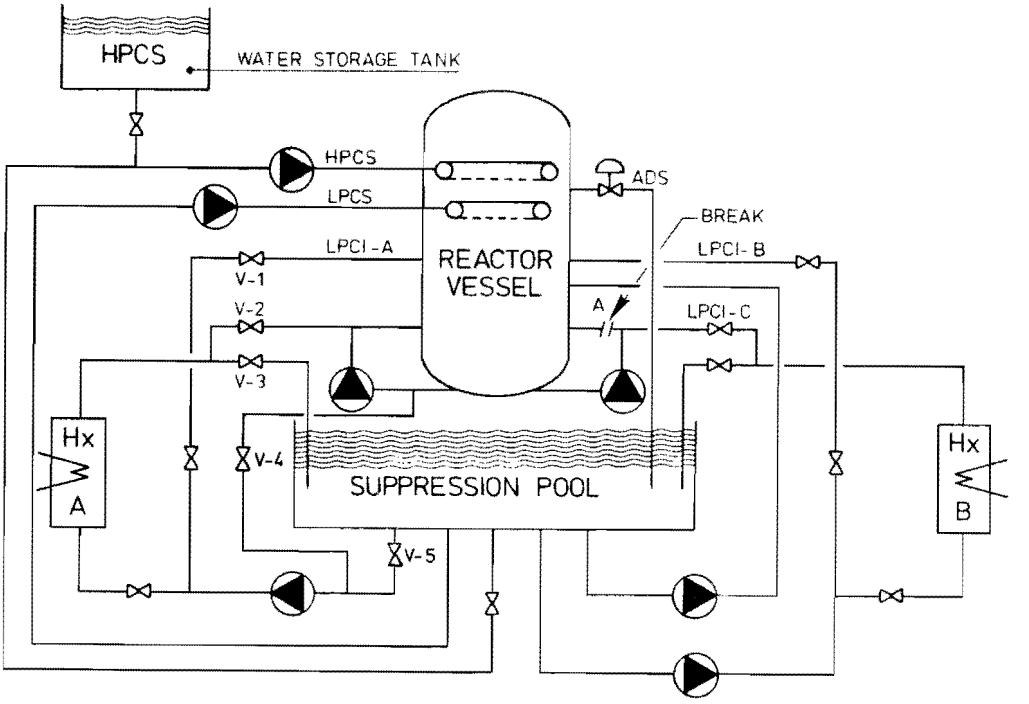


FIG. 6.6. THE SIMPLIFIED ECCS OF A BWR.

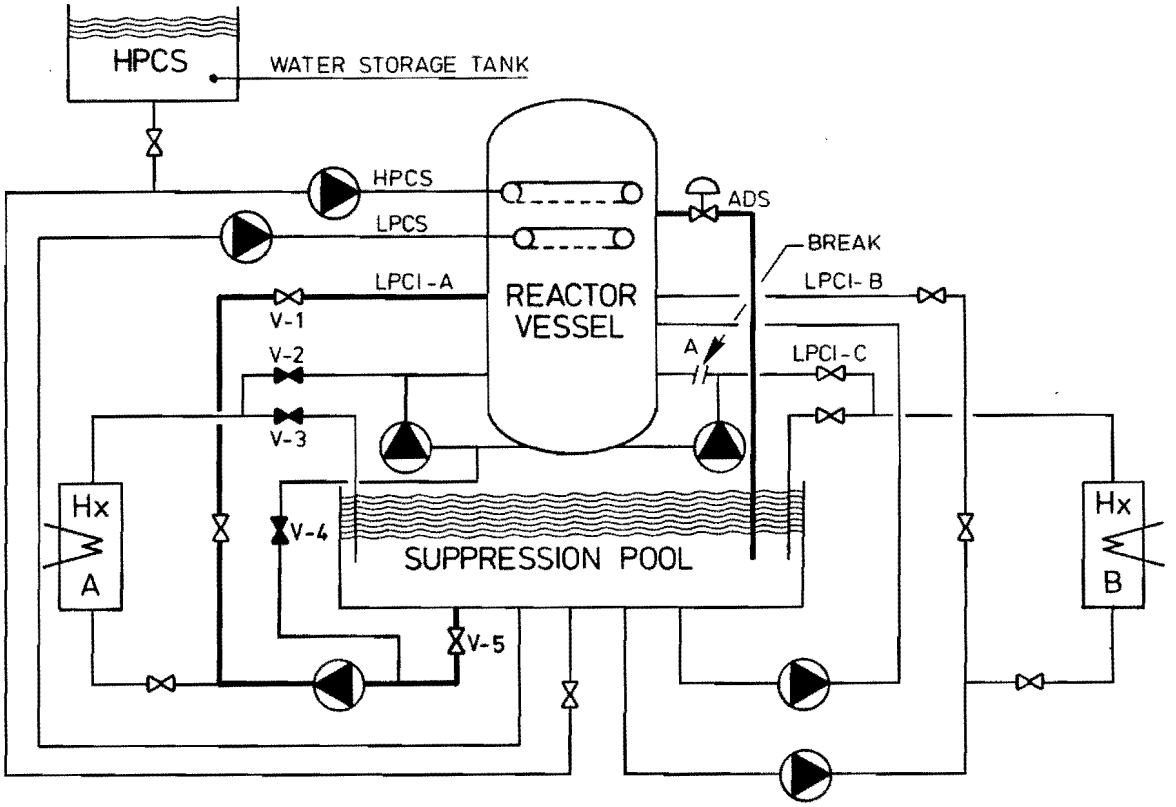


FIG. 6.7. THE ECCS DURING THE FIRST PHASE.

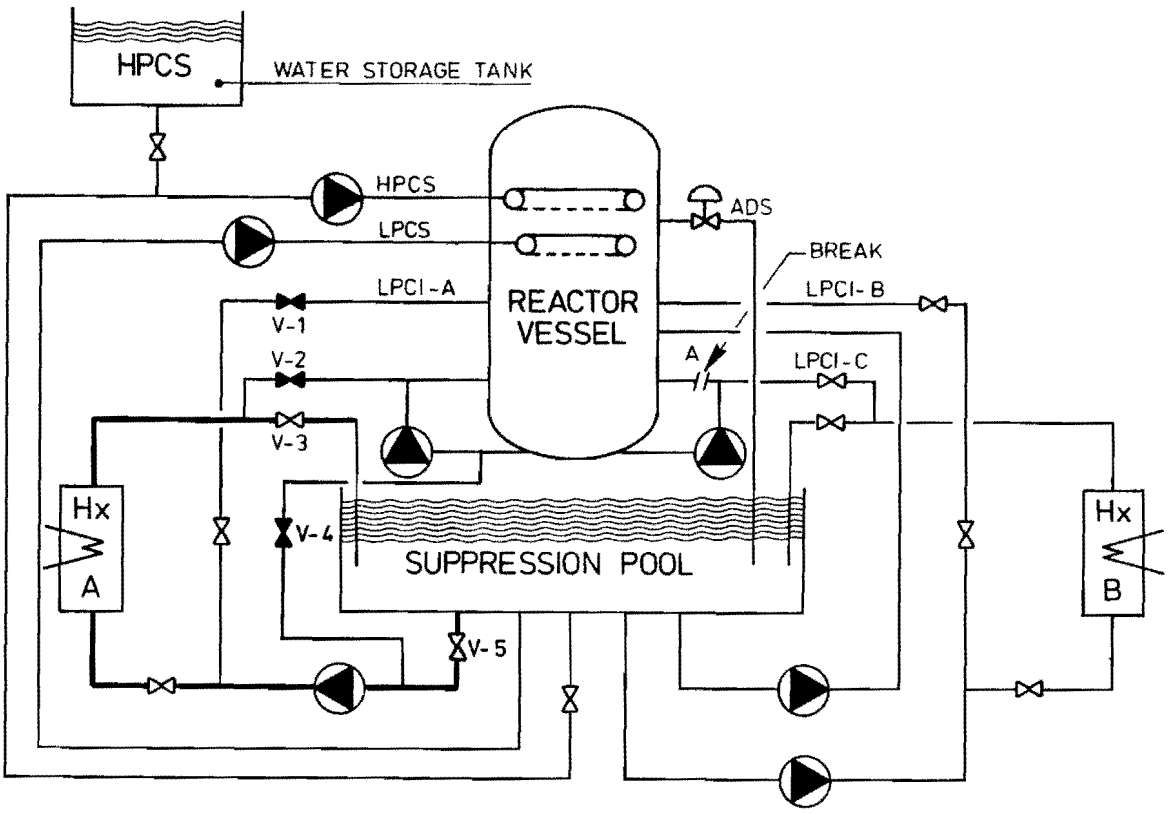


FIG. 6.8. THE ECCS DURING THE SECOND PHASE.

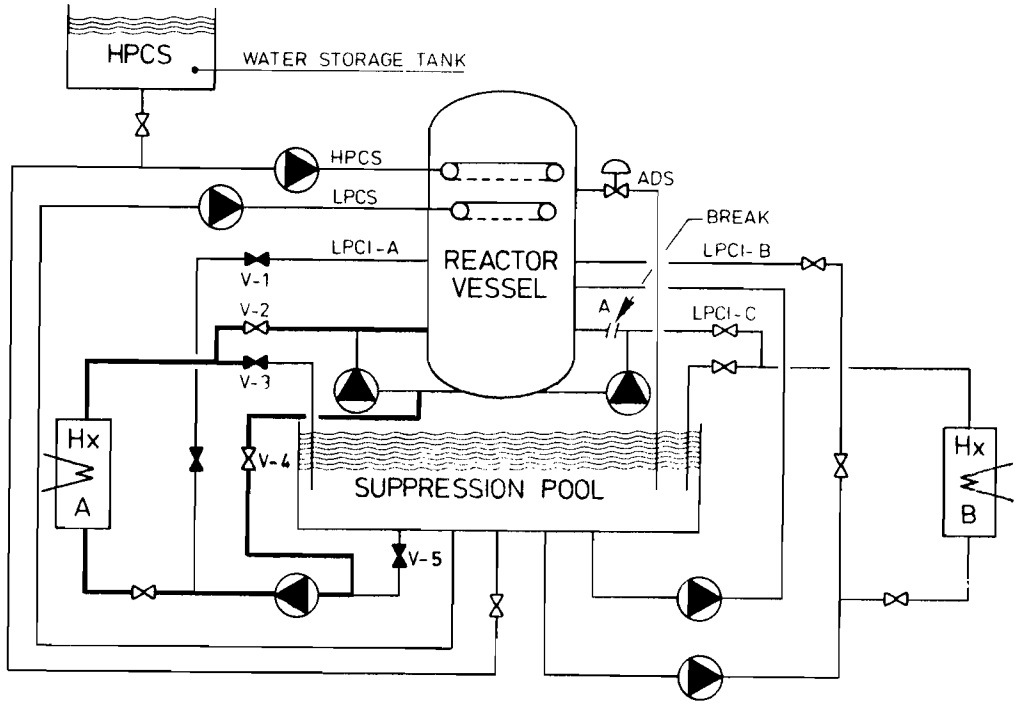


FIG. 6.9. THE ECCS DURING THE THIRD PHASE.

6.4.2. Phased mission description for the ECCS of the BWR and the fault trees for each phase

From the system description of the foregoing section we know that three phases are present for the ECCS. During phase j, j=1,2,3, the subsystem S_j of the ECCS has to perform its task. The several subsystems are composed of the following components:

$$\begin{aligned} S_1 &: \{\text{HPCS,LPCS,ADS,LPCI-A,LPCI-B,LPCI-C}\}; \\ S_2 &: \{\text{HPCS, LPCS,ADS,LPCI-A,LPCI-B,LPCI-C,HX-A,HX-B}\}; \\ S_3 &: \{\text{LPCI-A,LPCI-B,HX-A,HX-B}\}. \end{aligned} \tag{6.67}$$

Suppose that the phased mission for the ECCS starts at instant T_0, then the time schedule is given in table 6.15.

In the case that an event tree is constructed for the phased mission of the ECCS which consists of three phases, 2^3 different branches are possible. In practical situations a number of these branches do not occur so that less than eight remain. In our example, however, we shall study each of the theoretically possible eight branches. This because of the dependencies between the three subsystems.
In practical cases (see for example WASH-1400 [16]) event trees often occur with branches that contain two or three failed systems.

Table 6.15 Phases for the ECCS with their respective components

PHASE	PHASE INTERVAL (hrs)	SYSTEM
OR-phase	$[0,T_0^*)$	HPCS,LPCS,ADS,LPCI-A, LPCI-B,LPCI-C,HX-A,HX-B
phase 1	$[T_0,T_0+0.5)$	HPCS,LPCS,ADS,LPCI-A, LPCI-B,LPCI-C
phase 2	$[T_0+0.5,T_0+36.5)$	HPCS,LPCS,ADS,LPCI-A, LPCI-B,LPCI-C,HX-A,HX-B
phase 3	$[T_0+36.5,T_0+120.5]$	LPCI-A,LPCI-B,HX-A,HX-B

*T_0 : instant at which the mission starts.

Our approach shows that if partial or full system failures are not correctly taken into account it may give rise to an under-estimation of the probability of occurrence of these branches of two or more failed systems. As a rule such an under-estimation increases accordingly as the dependencies between the involved systems increase.
In fig. 6.10. the event tree is depicted for the ECCS. Each branch is defined as a phased mission by means of the tasks of each subsystem. The fault trees for the subsystems S_1, S_2 and S_3 are shown in the figures 6.11., 6.12. and 6.13., respectively.
Denote by $M_k^{(j)}$,j=1,2,3, the k^{th} minimal cut set of subsystem S_j. From their respective fault trees the minimal cut sets of the systems are easily deduced and given by:

for subsystem S_1 (phase 1):

$$M_1^{(1)} = \{ADS,HPCS\};$$
$$M_2^{(1)} = \{HPCS,LPCS,LPCI\text{-}A,LPCI\text{-}B,LPCI\text{-}C\}; \qquad (6.68)$$

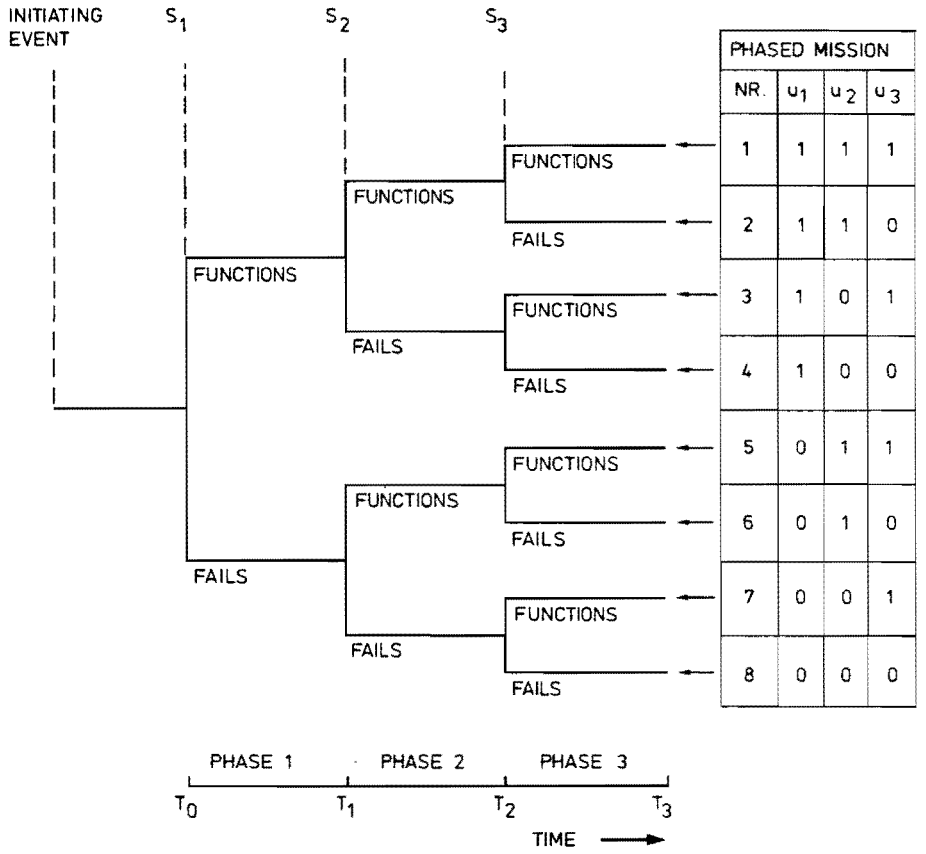


FIG. 6.10. THE EVENT TREE AND THE ASSOCIATED PHASED MISSIONS FOR THE ECCS IN CASE OF A LARGE LOCA.

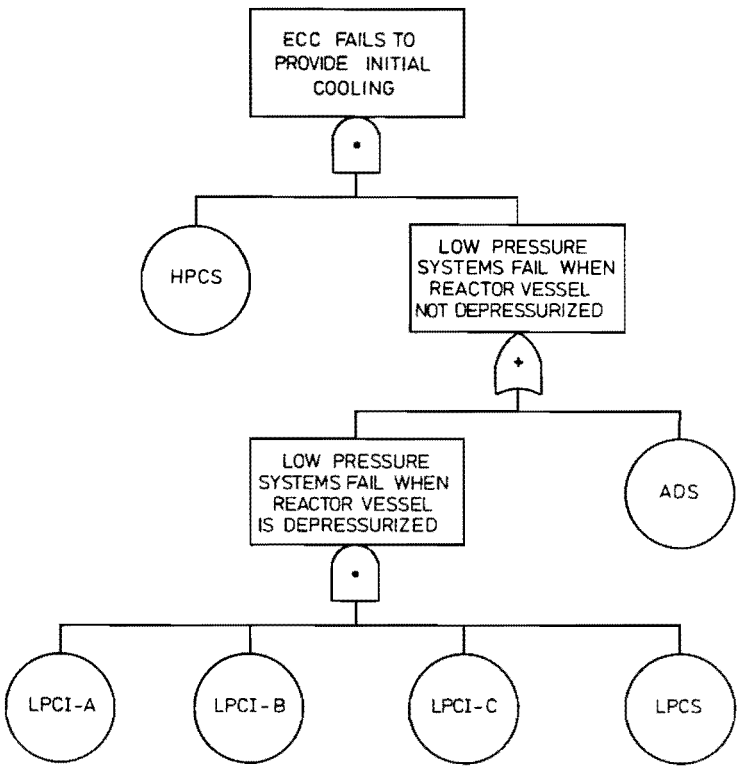


FIG. 6.11. THE FAULT TREE FOR PHASE 1 OF THE ECCS AFTER A LARGE LOCA.

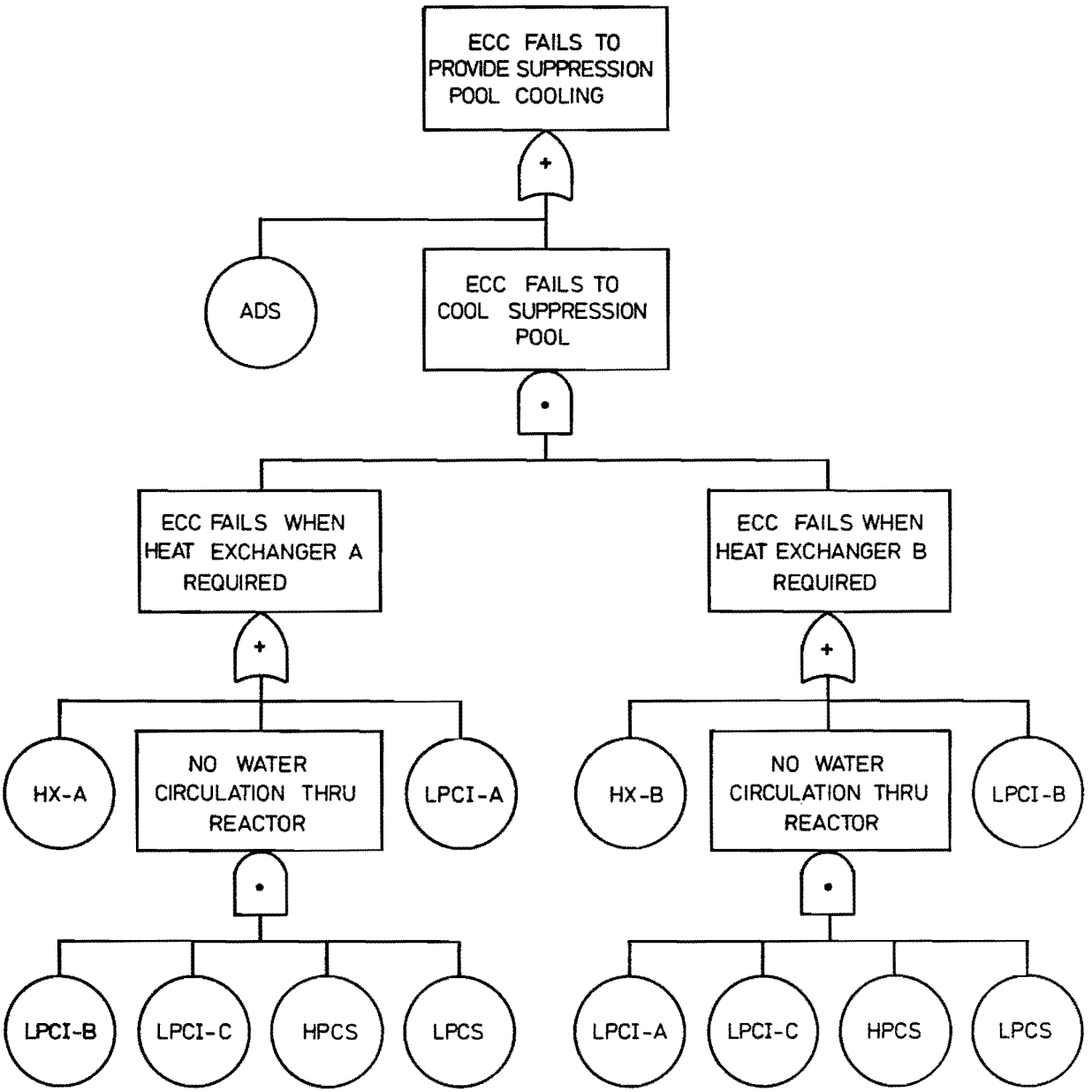


FIG. 6.12. THE FAULT TREE FOR PHASE 2 OF THE ECCS AFTER A LARGE LOCA.

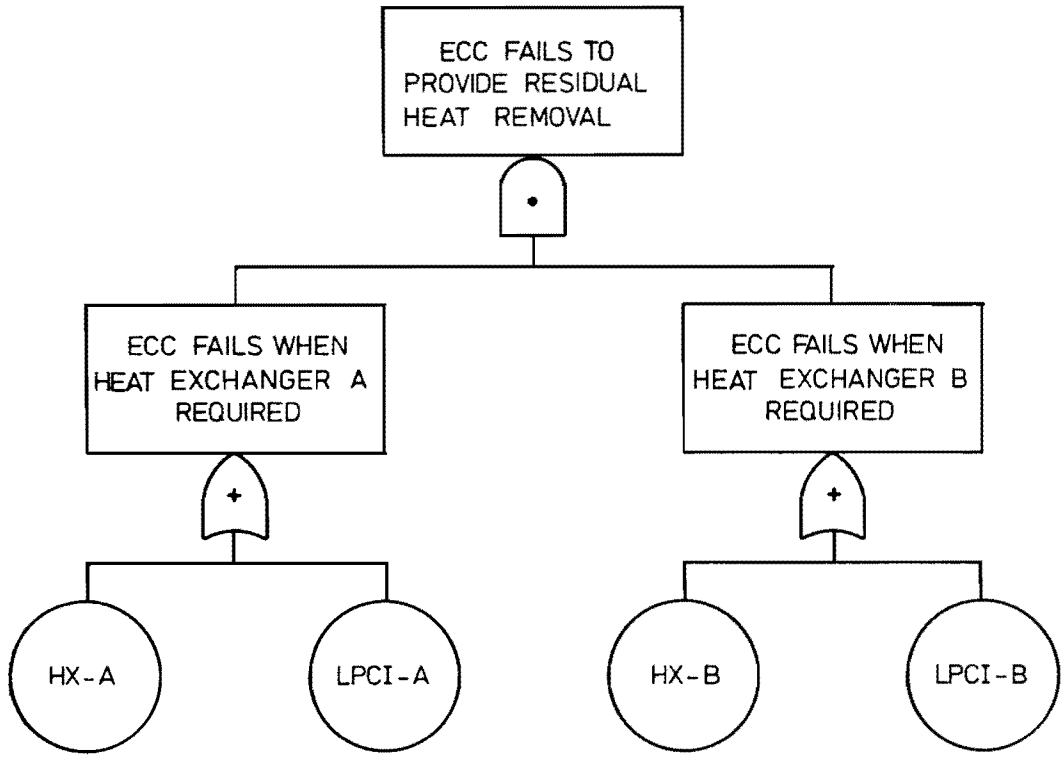


FIG. 6.13. THE FAULT TREE FOR PHASE 3 OF THE ECCS AFTER A LARGE LOCA.

Table 6.16. Component input data for the strategies (i) and (ii) in the case of the phased mission of the ECCS

COMPONENT	INITIAL AVAILABILITY a_0	FAILURE RATE/hr λ	MEAN REPAIR TIME (hrs) μ
HPCS	1.	$2.7 * 10^{-4}$	2.5
ADS	1.	$1.4 * 10^{-5}$	1.0
LPCI-A	1.	$2.5 * 10^{-5}$	2.5
LPCI-B	1.	$2.5 * 10^{-5}$	2.5
LPCI-C	1.	$2.5 * 10^{-5}$	2.5
LPCS	1.	$2.6 * 10^{-6}$	3.0
HX-A	1.	$2.8 * 10^{-6}$	24
HX-B	1.	$2.8 * 10^{-6}$	24

for subsystem S_2 (phase 2):

$$
\begin{aligned}
M_1^{(2)} &= \{\text{ADS}\};\\
M_2^{(2)} &= \{\text{LPCI-A,LPCI-B}\};\\
M_3^{(2)} &= \{\text{LPCI-A,HX-B}\};\\
M_4^{(2)} &= \{\text{LPCI-B,HX-A}\};\\
M_5^{(2)} &= \{\text{HX-A,HX-B}\};\\
M_6^{(2)} &= \{\text{HPCS,LPCI-C,LPCI-A,LPCS}\};\\
M_7^{(2)} &= \{\text{HPCS,LPCI-C,LPCI-B,LPCS}\};
\end{aligned}
\tag{6.69}
$$

for subsystem S_3 (phase 3):

$$
\begin{aligned}
M_1^{(3)} &= \{\text{LPCI-A,LPCI-B}\};\\
M_2^{(3)} &= \{\text{LPCI-A,HX-B}\};\\
M_3^{(3)} &= \{\text{LPCI-B,HX-A}\};\\
M_4^{(3)} &= \{\text{HX-A,HX-B}\}.
\end{aligned}
\tag{6.70}
$$

6.4.3. Numerical results

In this section we shall present the numerical results for the phased mission of the ECCS as depicted in the event tree of fig. 6.10.
Two strategies with respect to the inspection policy of the components are considered, viz.

strategy (i): all components are class 1 (non-repairable) components;
strategy (ii): all components are class 2 (continuously inspected) components.

The calculations are performed for two different values of the instant T_0 at which the phased mission starts, i.e. for T_0 = 0 year and T_0 = 1 year. The component input data for this numerical evaluation are shown in table 6.16.

The failure rates are taken from Burdick [2] whereas the mean repairtimes have been assessed by the author. The calculation results of the numerical evaluation are presented in the tables 6.17.,...,6.20.

Table 6.17. - This table shows for the probability $M_k(T_0)$ of mission success for T_0=0 the exact value, an upperbound and its associated deviation calculated by the method presented in this study both for the strategies (i) and (ii).

Table 6.18. - Figures of the corresponding variables from table 6.17. are presented for the case that the mission starts at T_0=1 year.

Table 6.19. - For strategy (i) and (ii) the table shows for the probability $M_k(T_0)$ of mission success for T_0=0 year the exact value and an upperbound calculated by the method presented in this study; also are shown the results obtained by the method based on the rules (R1) and (R2) (cf. section 6.2.8.). This latter type of method has been used in applications.

Table 6.20. - This table contains the corresponding figures of table 6.19. but for the case that each mission starts at instant T_0=1 year.

Finally the probability $J_0(T_0)$ of mission failure of the upperbranch of the event tree of fig. 6.10. for strategy (i) is graphically shown in fig. 6.14., whereas in fig. 6.15., for the same strategy (i) the system unreliability during the mission is depicted for T_0=0, .25, 1 and 5 years, respectively.
The figures 6.14. and 6.15. present the ultimate results of our analysis for the upperbranch of the event tree. In fig. 6.14. the probability of mission failure of the ECCS is shown as a function of the starting instant T_0 of the mission. (The broken line of the graph has been obtained by interpolation between its exact calculated endpoints. Detailed calculation of it is costly and unnecessary). Fig. 6.15. shows for the same strategy the system unreliability during the mission. The four graphs shown correspond with four different starting instants of the mission. The endpoints of these graphs correspond with the same points in fig. 6.14. This fig. 6.15. therefore shows how these ultimate probabilities are approached during the development of the mission.

6.4.4. Discussion of the numerical results

In this section we shall make some remarks concerning the numerical results.

(D1) From table 6.17. it is seen that in the case that the mission starts at instant T_0=0 no differences in the exact values for the probabilities of mission success exist between strategy (i) and (ii). This because there exists no OR-phase so that repair is not very effective in the case of strategy (ii). If the mission starts at instant T_0=1 year, i.e. there exists an OR-phase of 1 year, then inspection and repair play an important role (see the exact values for the strategies (i) and (ii) in table 6.18.).

(D2) From the tables 6.17. and 6.18. it is seen that there is a strong increase of the probability of mission failure for mission no. 1 (the upperbranch of the event tree) if T_0 changes from 0 to 1 year in the case of strategy (i). Because the probability of mission failure for the upperbranch equals the sum of the probabilities of mission success for the remaining branches, these probabilities increase too.
In the case of strategy (ii) (all components continuously detected) only a minor difference is noted with respect to the results of table 6.17. and 6.18. This is due to the optimal inspection and repair procedure for each of the components.

Comparison of the results for T_0=0 and T_0=1 shows that not only the exact values but also the relevant upperbounds and their associated deviations increase for strategy (i). In other words, the upperbound and the associated deviation both increase according as the mission starts later.
For strategy (ii), however, the exact values as well as the associated upperbound and deviation hardly change with T_0. This shows clearly the quality improvement by applying strategy (ii) instead of (i).

(D3) The phased missions no. 5 (u_1=0,u_2=u_3=1) and no. 6 (u_1=0,u_2=1,u_3=0) are physically not possible. This can be concluded from the tables 6.17. and 6.18. because it is seen that for those branches the deviation is greater than or equal to the upperbound for the probability of mission success (cf. section 6.3.6.).

It is affirmed by checking the minimal cut sets of the subsystems. For the missions no. 2 (u_1=1,u_2=1,u_3=0) and no. 3 (u_1=1,u_2=0,u_3=1), which start after 1 year (see table 6.18.), the deviation is also greater than the upperbound, but nevertheless these missions are possible. For these missions assumption (C5) in section 6.3.6.(v) is not fulfilled, i.e. the probability of occurrence of the minimal cut sets are rather large. Therefore the first order approximation of the system unavailability (upperbound) is not very accurate.

(D4) From the tables 6.19. and 6.20. it is seen that the approximation performed by the method based on the rules (R1) and (R2), (cf. section 6.2.8.) is no longer an upperbound for the probability of mission success in the case that two or more systems have to be failed, i.e. for the missions no. 4 (u_1=1,u_2=u_3=0), no. 7 (u_1=u_2=0, u_3=1) and no. 8 (u_1=u_2=u_3=0). In some cases the under-estimation of the probability of mission success may be considerable and may lead to dangerous conclusions. In particular when the results for the exact calculation show that the relevant probabilities of the involved branches are relatively large and the contribution to the overall risk is considerable.

(D5) From fig. 6.14. for the strategy (i) it is seen that the probability of mission failure for the upperbranch of the event tree in fig. 6.10. strongly increases with T_0. If the mission starts after half a year then it fails with a probability of at least 0.1.
From fig. 6.15. it is clear that the largest contribution to mission failure comes from system S_2. This is due to the component ADS which appears to be a minimal cut set for system S_2 with a large failure rate, e.g. $\lambda_{ADS}=1.4*10^{-5}$/hrs (cf. table 6.16.). If no repair is applied to the component its contribution to the failure probability after one year (8760 hrs) is roughly: $1-\exp(-1.4*10^{-5}*8760)=1.15*10^{-1}$.

Table 6.17. PROBABILITIES OF MISSION SUCCESS FOR THE ECCS IN THE CASE OF A LARGE LOCA (T_0 = 0 hrs)

MISSION				PROBABILITY OF MISSION SUCCESS					
				STRATEGY (i)			STRATEGY (ii)		
				ALL COMPONENTS NON-REPAIRABLE (CLASS 1)			ALL COMPONENTS CONTINUOUSLY INSPECTED (CLASS 2)		
No.	CODE			EXACT SOLUTION	FIRST ORDER APPROX.		EXACT SOLUTION	FIRST ORDER APPROX.	
i	u_1	u_2	u_3		UPPERBOUND	DEVIATION++)		UPPERBOUND	DEVIATION++)
1	1	1	1	$5.22 * 10^{-4}$+)	$5.23 * 10^{-4}$	$1.04 * 10^{-6}$	$5.22 * 10^{-4}$	$5.23 * 10^{-4}$	$1.04 * 10^{-6}$
2	1	1	0	$1.02 * 10^{-5}$	$1.12 * 10^{-5}$	$1.04 * 10^{-6}$	$1.02 * 10^{-5}$	$1.12 * 10^{-5}$	$1.04 * 10^{-6}$
3	1	0	1	$5.11 * 10^{-4}$	$5.12 * 10^{-4}$	$1.04 * 10^{-6}$	$5.11 * 10^{-4}$	$5.12 * 10^{-4}$	$1.04 * 10^{-6}$
4	1	0	0	$1.03 * 10^{-6}$	$1.04 * 10^{-6}$	$2.54 * 10^{-9}$	$1.03 * 10^{-6}$	$1.04 * 10^{-6}$	$2.54 * 10^{-9}$
5	0	1	1	0	$9.45 * 10^{-10}$	$9.45 * 10^{-10}$	0	$9.45 * 10^{-10}$	$9.45 * 10^{-10}$
6	0	1	0	0	$1.06 * 10^{-14}$	$1.16 * 10^{-14}$	0	$1.06 * 10^{-14}$	$1.16 * 10^{-14}$
7	0	0	1	$9.45 * 10^{-10}$	$9.45 * 10^{-10}$	$1.25 * 10^{-14}$	$9.45 * 10^{-10}$	$9.45 * 10^{-10}$	$1.25 * 10^{-14}$
8	0	0	0	$1.06 * 10^{-14}$	$1.16 * 10^{-14}$	-1)	$1.06 * 10^{-14}$	$1.16 * 10^{-14}$	-1)

1) The program PHAMISS (see chapter 7) does not allow the evaluation of these values.

+) For mission no. 1 (u_1=u_2=u_3=1) the probability of mission failure is presented.

++) Deviation: difference between upper- and lowerbound.

Table 6.18. PROBABILITIES OF MISSION SUCCESS FOR THE ECCS IN THE CASE OF A LARGE LOCA (T_0 = 8760 hrs)

MISSION				PROBABILITY OF MISSION SUCCESS					
				STRATEGY (i)			STRATEGY (ii)		
				ALL COMPONENTS NON-REPAIRABLE (CLASS 1)			ALL COMPONENTS CONTINUOUSLY INSPECTED (CLASS 2)		
No.	CODE			EXACT SOLUTION	FIRST ORDER APPROX.		EXACT SOLUTION	FIRST ORDER APPROX.	
i	u_1	u_2	u_3		UPPERBOUND	DEVIATION++)		UPPERBOUND	DEVIATION++)
1	1	1	1	$1.59 * 10^{-1}$+)	$3.21 * 10^{-1}$	$1.86 * 10^{-1}$	$5.37 * 10^{-4}$	$5.38 * 10^{-4}$	$1.34 * 10^{-6}$
2	1	1	0	$7.01 * 10^{-4}$	$4.79 * 10^{-2}$	$6.51 * 10^{-2}$	$1.07 * 10^{-5}$	$1.21 * 10^{-5}$	$1.31 * 10^{-6}$
3	1	0	1	$1.19 * 10^{-2}$	$1.59 * 10^{-1}$	$1.70 * 10^{-1}$	$5.25 * 10^{-4}$	$5.26 * 10^{-4}$	$1.33 * 10^{-6}$
4	1	0	0	$4.20 * 10^{-2}$	$5.97 * 10^{-2}$	$3.47 * 10^{-2}$	$1.31 * 10^{-6}$	$1.31 * 10^{-6}$	$4.27 * 10^{-9}$
5	0	1	1	0	$1.05 * 10^{-1}$	$1.16 * 10^{-1}$	0	$1.70 * 10^{-8}$	$1.70 * 10^{-8}$
6	0	1	0	0	$5.39 * 10^{-3}$	$1.17 * 10^{-2}$	0	$2.05 * 10^{-13}$	$2.27 * 10^{-13}$
7	0	0	1	$9.96 * 10^{-2}$	$1.10 * 10^{-1}$	$1.79 * 10^{-2}$	$1.70 * 10^{-8}$	$1.70 * 10^{-8}$	$2.50 * 10^{-13}$
8	0	0	0	$5.14 * 10^{-3}$	$1.14 * 10^{-2}$	-	$2.05 * 10^{-13}$	$2.27 * 10^{-13}$	-

+) For mission no. 1 ($u_1=u_2=u_3=1$) the probability of mission failure is presented.

++) Deviation: difference between upper- and lowerbound.

Table 6.19. PROBABILITIES OF MISSION SUCCESS FOR THE ECCS IN THE CASE OF A LARGE LOCA THE EXACT SOLUTION AND UPPERBOUNDS OBTAINED BY THE PRESENT STUDY AND A FORMER APPROACH (T_0 = 0 hrs)

MISSION				PROBABILITY OF MISSION SUCCESS					
				STRATEGY (i)			STRATEGY (ii)		
				ALL COMPONENTS NON-REPAIRABLE (CLASS 1)			ALL COMPONENTS CONTINUOUSLY INSPECTED (CLASS 2)		
No.	CODE			EXACT SOLUTION	FIRST ORDER APPROX. (upperbound)		EXACT SOLUTION	FIRST ORDER APPROX. (upperbound)	
i	u_1	u_2	u_3		PRESENT STUDY	FORMER METHOD		PRESENT STUDY	FORMER METHOD
1	1	1	1	$5.22 * 10^{-4}$ +)	$5.23 * 10^{-4}$	$5.23 * 10^{-4}$	$5.22 * 10^{-3}$	$5.23 * 10^{-4}$	$1.40 * 10^{-5}$
2	1	1	0	$1.02 * 10^{-5}$	$1.12 * 10^{-5}$	$1.12 * 10^{-5}$	$1.02 * 10^{-5}$	$1.12 * 10^{-5}$	$1.67 * 10^{-8}$
3	1	0	1	$5.11 * 10^{-4}$	$5.12 * 10^{-4}$	$5.12 * 10^{-4}$	$5.11 * 10^{-4}$	$5.12 * 10^{-4}$	$1.40 * 10^{-5}$
4	1	0	0	$1.03 * 10^{-6}$	$1.04 * 10^{-6}$	$5.73 * 10^{-9}$	$1.03 * 10^{-6}$	$1.04 * 10^{-6}$	$2.34 * 10^{-13}$
5	0	1	1	0	$9.45 * 10^{-10}$	$9.45 * 10^{-10}$	0	$9.45 * 10^{-10}$	$6.74 * 10^{-10}$
6	0	1	0	0	$1.06 * 10^{-14}$	$1.06 * 10^{-14}$	0	$1.06 * 10^{-14}$	$1.13 * 10^{-17}$
7	0	0	1	$9.45 * 10^{-10}$	$9.45 * 10^{-10}$	$4.84 * 10^{-13}$	$9.45 * 10^{-10}$	$9.45 * 10^{-10}$	$9.44 * 10^{-15}$
8	0	0	0	$1.06 * 10^{-14}$	$1.16 * 10^{-14}$	$5.42 * 10^{-18}$	$1.06 * 10^{-14}$	$1.16 * 10^{-14}$	$1.58 * 10^{-22}$

+) For mission no. 1 ($u_1=u_2=u_3=1$) the probability of mission failure is presented.

Table 6.20. PROBABILITIES OF MISSION SUCCESS FOR THE ECCS IN THE CASE OF A LARGE LOCA THE EXACT SOLUTION AND UPPERBOUNDS OBTAINED BY THE PRESENT STUDY AND A FORMER APPROACH (T_0 = 8760 hrs)

MISSION				PROBABILITY OF MISSION SUCCESS					
				STRATEGY (i)			STRATEGY (ii)		
				ALL COMPONENTS NON-REPAIRABLE (CLASS 1)			ALL COMPONENTS CONTINUOUSLY INSPECTED (CLASS 2)		
No.	CODE			EXACT SOLUTION	FIRST ORDER APPROX. (upperbound)		EXACT SOLUTION	FIRST ORDER APPROX. (upperbound)	
i	u_1	u_2	u_3		PRESENT STUDY	FORMER MERHOD		PRESENT STUDY	FORMER METHOD
1	1	1	1	$1.59 * 10^{-1}$ +)	$3.21 * 10^{-1}$	$3.22 * 10^{-1}$	$5.37 * 10^{-4}$	$5.38 * 10^{-4}$	$1.40 * 10^{-5}$
2	1	1	0	$7.01 * 10^{-4}$	$4.79 * 10^{-2}$	$5.00 * 10^{-2}$	$1.07 * 10^{-5}$	$1.21 * 10^{-5}$	$1.68 * 10^{-8}$
3	1	0	1	$1.19 * 10^{-2}$	$1.59 * 10^{-1}$	$1.67 * 10^{-1}$	$5.25 * 10^{-4}$	$5.26 * 10^{-4}$	$1.40 * 10^{-5}$
4	1	0	0	$4.20 * 10^{-2}$	$5.97 * 10^{-2}$	$8.35 * 10^{-3}$	$1.31 * 10^{-6}$	$1.31 * 10^{-6}$	$2.35 * 10^{-13}$
5	0	1	1	0	$1.05 * 10^{-1}$	$1.05 * 10^{-1}$	0	$1.70 * 10^{-8}$	$9.44 * 10^{-9}$
6	0	1	0	0	$5.39 * 10^{-3}$	$5.25 * 10^{-3}$	0	$2.05 * 10^{-13}$	$1.59 * 10^{-16}$
7	0	0	1	$9.96 * 10^{-2}$	$1.10 * 10^{-1}$	$1.75 * 10^{-2}$	$1.70 * 10^{-8}$	$1.70 * 10^{-8}$	$1.32 * 10^{-13}$
8	0	0	0	$5.14 * 10^{-3}$	$1.14 * 10^{-2}$	$8.77 * 10^{-4}$	$2.05 * 10^{-13}$	$2.27 * 10^{-13}$	$2.22 * 10^{-21}$

+) For mission no. 1 ($u_1=u_2=u_3=1$) the probability of mission failure is presented.

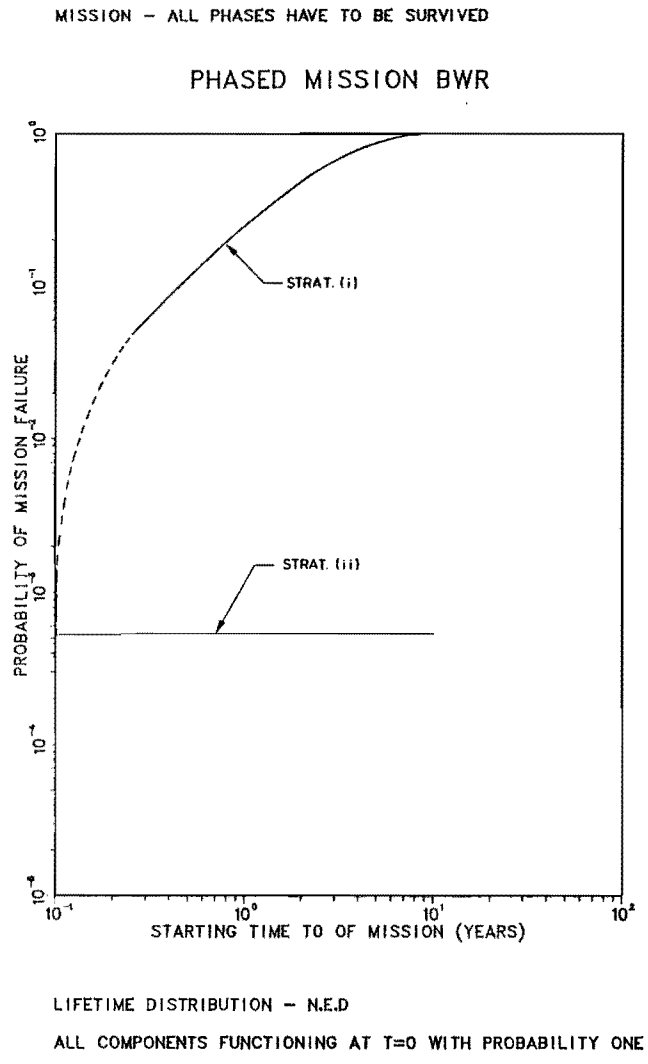


FIG. 6.14. THE PROBABILITY OF MISSION FAILURE FOR THE UPPERBRANCH OF THE EVENTTREE OF THE ECCS AS A FUNCTION OF THE STARTING INSTANT T_0 OF THE MISSION

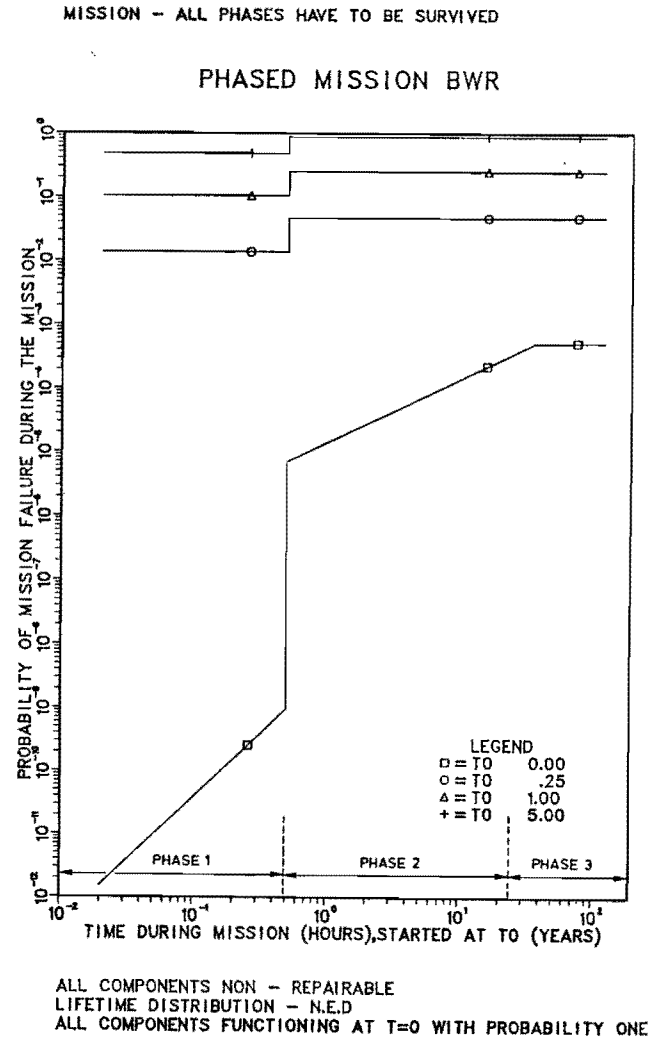


FIG. 6.15. THE PROBABILITY OF MISSION FAILURE DURING THE MISSION FOR THE UPPERBRANCH OF THE EVENTTREE OF THE ECCS

7. THE RELIABILITY COMPUTER PROGRAM PHAMISS

7.1. Introduction

For large systems it is very laborious to obtain the probability of mission success for a phased mission or even to calculate the system unavailability of a single system. Therefore a new "reliability computer program" called PHAMISS is developed to treat the problems of single system reliability and unavailability as well as those of phased mission analysis.
The set-up of the program PHAMISS is based on the approach of phased mission analysis as described in chapter 6. This has given rise to some special difficulties in the organization of the program.
These difficulties concern two aspects, viz. (i) computer memory requirements and (ii) computer running time. In the following we shall briefly discuss these aspects.

(i) Computer memory requirements

The methodology that has been developed in chapter 6 to obtain the the probability of mission success is based on fault tree analysis. As it has been pointed out in chapter 5, large fault trees may contain a large number of minimal cut sets. In fact it is often impossible to obtain all minimal cut sets of a single fault tree due to a limited computer memory. For phased mission analysis we not only need the minimal cut sets of a single system but of several systems at the same time.

(ii) Computer running time

In many cases it requires much computer time to obtain the minimal cut sets of large fault trees. In the case of a phased mission where more than one fault tree has to be treated, the required computer time then accumulates strongly.

To cope with the problems just mentioned the program PHAMISS has been developed.

The reliability computer code PHAMISS is a fully dynamically written program with segmented loading. The language is FORTRAN-IV and the program

is operational at a CDC Cyber-175. Its source consists of about 10000 FORTRAN statements.
In the sequel of this chapter we shall briefly discuss the set-up and capabilities of the program PHAMISS. For a detailed description of PHAMISS see Terpstra and Dekker [39].
In section 7.2. the program philosophy is discussed, whereas in section 7.3. the program sections FAULTTREE, PROBCAL, IMPCAL and COMMODE are treated. In section 7.4. the set-up of the input deck for PHAMISS is shown and its output is discussed.

7.2. The program philosophy

The reliability computer program PHAMISS consists of one main program and several subroutines. After the main program PHAMISS the next level consists of the following four program sections:

- FAULTTREE (minimal cut set determination);
- PROBCAL (availability calculations for a single system as well as for phased missions);
- IMPCAL (importance calculations);
- COMMODE (determination of common cause failure modes).

Each of these four program sections can be applied separately from each other or combined. However, the program section FAULTTREE is basic for further calculations by PROBCAL, IMPCAL or COMMODE, because each of these three program sections needs as input minimal cut sets (generated by FAULTTREE).
The program section FAULTTREE stores on a permanent device, called a "save file", for each fault tree the component input data and the obtained minimal cut sets of that fault tree. If such a "save file" already exists for that fault tree, then the program section FAULTTREE destroys the *old* "save file" and creates a *new* one. This "save file" option makes it possible to perform so-called *restart calculations*. Such calculations can be performed by each of the program sections PROBCAL, IMPCAL and COMMODE without the use of the program section FAULTTREE. A restart calculation is only possible if a "save file" exists for each fault tree and no changes are made in that fault tree. The restart calculation procedure is schematically depicted in the following diagram of fig. 7.1.

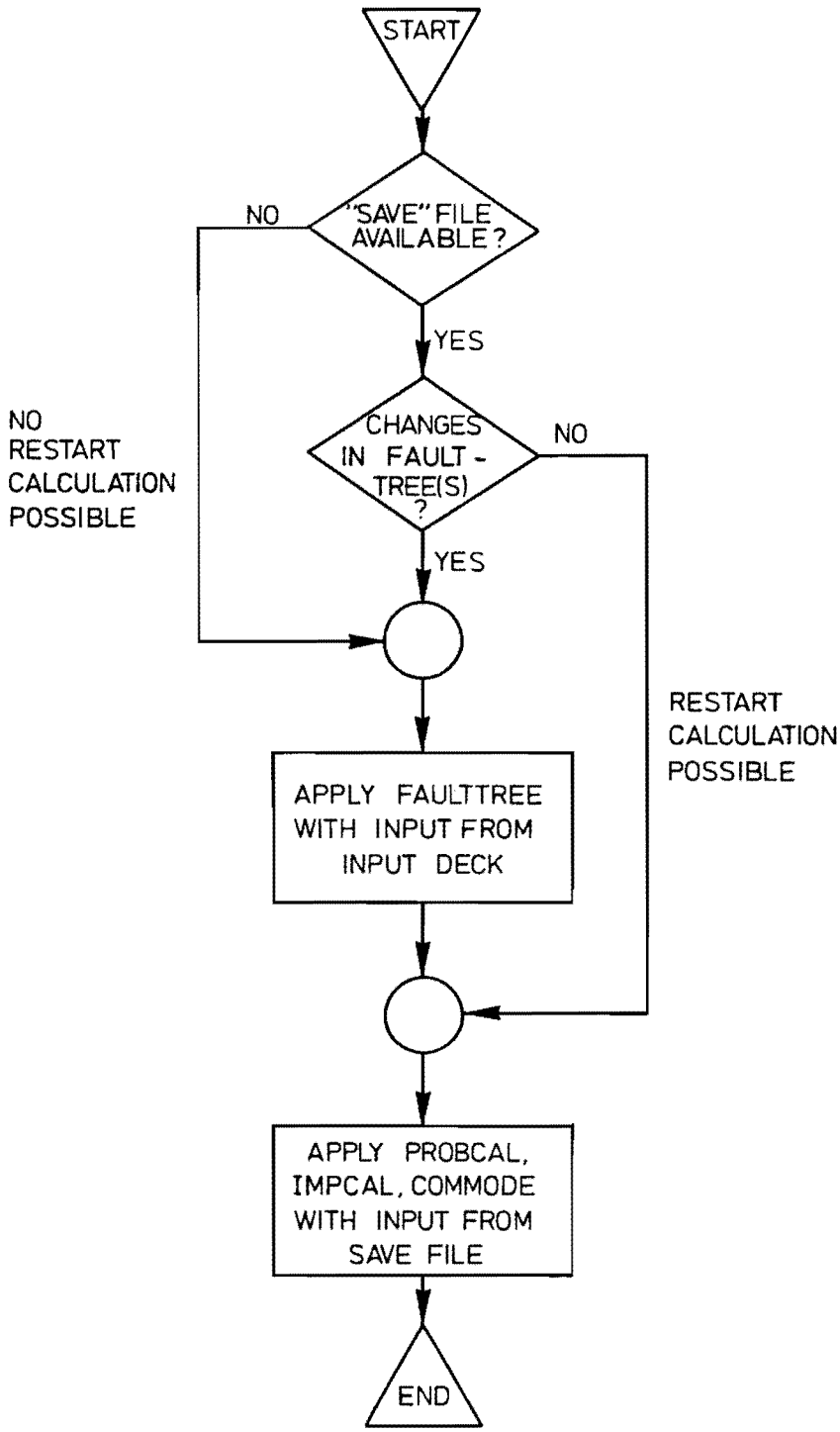


FIG. 7.1. POSSIBLE OPTIONS TO APPLY PHAMISS WITH RESPECT TO FAULTTREE (RESTART OPTION).

The input of the program PHAMISS is *free-formatted* and easy to understand (see section 7.4.). An extensive error checking on the input and throughout the whole program with clearly printed messages is available. Therefore the program PHAMISS is *users-friendly*.

7.3. The program sections FAULTTREE, PROBCAL, IMPCAL and COMMODE

In this section we shall briefly discuss the special features of each of the four program sections FAULTTREE, PROBCAL, IMPCAL and COMMODE. It is not our intention to give here a detailed discussion of each calculation procedure. For a more detailed discussion see Terpstra and Dekker [39].

7.3.1. The program section FAULTTREE

The program section FAULTTREE generates the minimal cut sets and/or path sets of a single fault tree or in the case of a phased mission the minimal cut sets of several trees (up to 10).
The input for the program section FAULTTREE consists of:
* the component identification and (optionally) its failure data;
* the description of one or more fault trees.

The program section FAULTTREE consists of three parts:

(A1) the input treatment of the fault tree;
(A2) the generation of the minimal cut sets of the fault tree;
(A3) the output representation.

In the following we shall make some remarks concerning the procedures applied by FAULTTREE for each of the steps (A1), (A2) and (A3) pointwise. For a description of the input data and output for FAULTTREE see section 7.4.

(A1) The input treatment of the fault tree

(A1.1) The minimal cut set generation by FAULTTREE is based on *bit manipulation*. Each component and each gate are represented by one single bit position instead of one computer word (one computer word on the CDC Cyber-175 contains 60 bits) or one byte.
For the minimal cut set generation this means that if there are N_c components and N_g gates in the fault tree a cut set needs $[(N_c+N_g+W-1)/W]+1$ computer words (or bytes) if W is the number of

bits of a computer word (or a byte), whereas a minimal cut set is stored in $[N_c+W-1/W]+1$ computer words.
If all minimal cut sets have to be determined, this procedure is very profitable with respect to memory requirements, because the order of a minimal cut set does not play any role with regard to the maximal number of computer words needed to contain the largest minimal cut sets.

(A1.2) We shall give here some definitions that are needed for the sequel.

(B1) A *basic event* (BE) is a primary event (see section 5.2.1.).

(B2) The *domain* of a gate-event is the set of BE's contained in the subtree with that gate as TOP-event.

(B3) A *super event* (SE) is a gate event whose domain consists of BE's that have only one successor.

(B4) A *logical combined event* (LCE) is an artificial gate whose predecessors are a uniquely determined group of BE's and/or SE's. Each BE or each SE that belongs to the LCE only occurs in the fault tree in conjunction with all the other members of the group.

(B5) An *independent branch* (IB) of the fault tree is a gate-event whose domain has no intersection with the domain of the rest of the tree.

(A1.3) In order to make the minimal cut set procedure faster and to reduce the number of minimal cut sets, the following sequence of actions is taken during the input treatment by the program section FAULTTREE before it starts its calculation:

(i) the determination of the SE's;

(ii) the determination of the largest IB's;

(iii) all *cascades* are removed from the fault tree. A *cascade* exists if two or more OR-gates (and AND-gates) are descendants. This anti-cascade procedure may lead to a large number of predecessors for some remaining gates in the fault tree;

(iv) all LCE's are determined;

(v) the gate-events are *arranged* by special criteria. The arrangement of the gates determines the sequence of development of the distinct gates. For the minimal cut set determination SE's and LCE's are considered as BE's.

(A.2) The generation of the minimal cut sets of the fault tree

(A2.1) The minimal cut set generation procedure is from the *top to the bottom*, i.e. the TOP-event is replaced by its predecessors etc., until all events in a cut set are BE's, SE's and/or LCE's. The difficulties in generating minimal cut sets arise from the AND-gates because in many cases such type of gates do increase the number of minimal cut sets significantly. Therefore a special procedure is implemented for those AND-gates with a large number of cut sets (more than 10000). This special procedure determines firstly the minimal cut sets of each predecessor of such an AND-gate and secondly by combination of the minimal cut sets of its predecessors the minimal cut sets of the AND-gate are formed. After that the minimal cut sets of the AND-gate are correctly inserted into the minimal cut sets of the TOP-event. So the special procedure of the determination of the minimal cut sets of such an AND-gate is a *bottom to top* procedure. We found that this procedure accelerated the calculation procedure significantly.

(A2.2) The calculation procedure for the determination of the minimal cut sets is:

* the minimal cut sets of the TOP-event are expressed by basic events (BE), super events (SE), logical combined events (LCE) and independent branches (IB);
* each IB is considered as a TOP-event. Its minimal cut sets are expressed in BE's, SE's and LCE's;
* subsequently the minimal cut sets of the IB's are inserted into the minimal cut sets of the TOP-event of the fault tree. The remaining elements of the minimal cut sets of the fault tree are BE's, SE's and LCE's.

The "save-file" that is made by FAULTTREE contains the minimal cut sets of the fault tree expressed in BE's, SE's and LCE's. The reduction of the number of minimal cut sets when expressed in BE's, SE's and LCE's with regard to the number of minimal cut sets expressed in BE's is enormous for a great number of fault trees.

(A.3) The output representation

The output for the program section FAULTTREE is briefly described in section 7.4. We already mention here a special feature of the program: after each program (section) step the needed CP and IO times for that step are printed in the output.

7.3.2. The program section PROBCAL

The program section PROBCAL performs probability calculations concerning:

(C1) the single system unavailability;
(C2) the probability of mission success in the case of a phased mission.

The input of the program section PROBCAL consists of:
* the component failure date;
* the minimal cut sets of one or more trees (see section 7.4.);
* data that describes the mission.

In the input for PROBCAL one has to specify whether it concerns a single system or a phased mission (see section 7.4.).

(C1) The single system unavailability

The system unavailability is calculated by PROBCAL by means of:
* the minimal cut set upperbound (cf. (5.12)), or
* the upperbound obtained by the inclusion-exclusion principle (cf. (5.18)).

The method to be chosen can be specified in the input. For the calculation of the system unavailability the component models of chapter 3 are used.
If the system unavailability is calculated for more than one instant it is possible to represent the system unavailability graphically by a plot produced by PROBCAL.

(C2) The probability of mission success in the case of a phased mission

The probability of mission success for a phased mission is obtained by the approximations as shown in table 6.14. These calculations imply:
* an upperbound and a lowerbound for the probability of mission success; The lowerbound calculation is optionally, because it may be very time consuming.

For a phased mission the probability calculations are performed at the end points of the phases, i.e. at the instants T_j,j=1,2,...,K, if the mission consists of K phases. However, for a phased mission where every system has to survive its phase also calculations can be performed at the starting points of each phase, i.e. at the instants T_j,j=0,1,...,K-1. Therefore the possibility exists that for such a phased mission optionally a plot can be produced of the system unreliability during the mission by PROBCAL.

Presently PROBCAL accepts seven classes of components:
- class 1: components that are not inspected (non-repairable);
- class 2: components that are monitored (continuously inspected);
- class 3: components that are randomly inspected;
- class 4: components that are periodically EXSITU inspected;
- class 5: components that are periodically INSITU inspected;
- class 6: components with a constant unavailability (a failure probability per demand or per cycle);
- class 7: components with a constant unavailability during the dormant phase and a non-repairable behaviour during the operational phase.

The present version of the program contains these seven component classes with a negative exponentially distributed lifetime and repairtime for the component, except for the classes 4 and 5. Here the repairtime distribution is the uniform distribution or the repairtime is a constant, which should be specified in the input. It is not difficult to extend the program with Erlang-2 distributed lifetimes for the components.
The maximal number of phases that can be treated by PROBCAL is presently 10, and the maximal number of systems that have to be failed during the mission is restricted to 3. Lowerbound calculations in the case of a phased mission can be performed for missions that consist of less than 3 failed systems. With the present state of affairs these restrictions do not seem to be a serious barrier for practical applications. But PROBCAL can be extended in this respect.

7.3.3. The program section IMPCAL

The program section IMPCAL calculates measures of importance (cf. section 5.3.4.) for components as well as for minimal cut sets. Presently the program calculates Vesely-Fussell's measure of importance for components by (5.64) and for minimal cut sets by (5.92).
IMPCAL calculates these measures for at most 5 distinct instants. For the measure of importance of minimal cut sets a cut-off value α, $0 < \alpha < 1$, is used to reduce the number of minimal cut sets in the list. If the value of the minimal cut set(s) with the largest measure of importance equals β then all minimal cut sets with a measure of importance smaller than $\alpha\beta$ are not taken into consideration.
The input of the program section IMPCAL consists of:
* the component failure date;
* the minimal cut sets of the fault tree

7.3.4. The program section COMMODE

The program section COMMODE performs qualitative calculations. It searches for those minimal cut sets of a fault tree that can occur by a common cause, such as a fire, too high pressure, too high humidity, etc. In fact such a cause for the occurrence of a minimal cut set is a common secondary failure for all components contained in the concerned cut set (cf. section 5.2.4.). To identify such minimal cut sets, that are sensitive for a common cause failure of the components, for each component its secondary failures are denoted by a *label*. Such a label may be for instance a "P" (for pressure), a "T" (for temperature), etc. A *label* may also indicate the physical position of the component such as "R1" (for room R1), etc.
If all components of a minimal cut set share at least one label they have something in common that may lead to system failure. The input for the program section COMMODE consists of:
* the labels for each component;
* the minimal cut sets of the system.

7.4. The input philosophy for PHAMISS and its output

7.4.1. The general structure of the input deck for PHAMISS

In fig. 7.2. the general set up of the input deck for PHAMISS is depicted. Such an input deck consists of:

(D1) the *initial* input unit;
(D2) input units for the program sections that are applied.

The *initial* input unit contains general information, such as
* the problem description heading;
* the names of the program sections that will be used;
* the number of fault trees in the case of a phased mission, etc.

The cards containing such kind of information are called *program control cards*. Alphanumeric names (keywords) on a program control card are put between asterisks.
The initial unit as well as the program section input units contain a number of such program control cards, that control the *actions* and the *print out* of the program. In the initial unit as well as in the program section input units program control cards are always kept together within one section called the *program control section* of the unit. This program control section always precedes the data input section of a unit.
It starts with the general problem heading card in the case of the initial unit and with the program section name in the case of a program section input unit. Each program control section is terminated with the program control card: *GOON*. No fixed sequence exists concerning the program control cards within a program control section, except that for the initial input unit the problem heading card is the first one, the *TREES* card (optional) must be the second card and for each other input unit the program section name must be the first one.
In the case of a phased mission a *FAULTTREE* program section input unit has to be constructed for each fault tree that exists for the mission. Furthermore there exists no fixed sequence for the input units within the general input deck for PHAMISS, except that the initial input unit has to be the first one and if more than one *FAULTTREE* input unit exists, then these input units should be kept together.
From what has been said it is clear that the initial input unit is fully a program control section.
For a complete description of all existing program control cards, see Terpstra and Dekker [39].

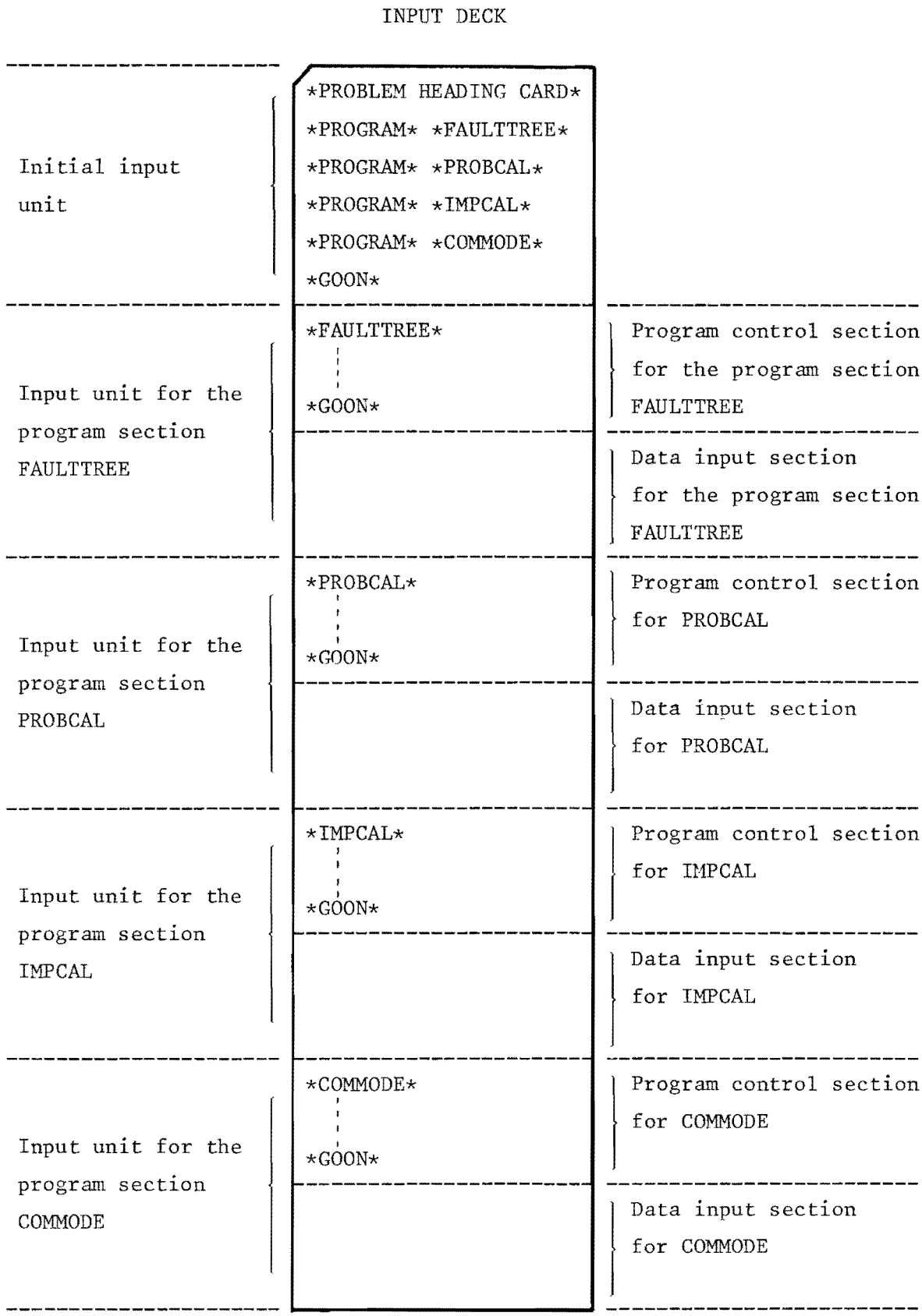


Fig. 7.2. General structure of the input deck for the program PHAMISS

7.4.2. The structure of each of the program section input units

The general set-up of a program section input unit is:
* firstly a program control section;
* secondly a data input section.

The program control sections are treated in section 7.4.1. Therefore we shall now describe the set-up of the *data input sections*.
A *data input section* may consist of several *parts*. Each *part* starts with a *keyword* for that special *part* and ends with in the last record of such a part the name: END. Each keyword is placed between asterisks.
The several distinct program section input units are shown in the figures 7.3.,...,7.6.
The *keywords* for the several *parts* are listed in table 7.1.

7.4.3. The output of the program PHAMISS

The output of the program PHAMISS may consist of:
* printed output;
* plotted output.

If the plot option is used (by means of the program control card *PLOT*) a plot can be produced for:
* the time dependent unavailability of a single system;
* the unreliability during the phased mission where every system has to survive its phase.

The printed output always consists of:
* the representation of the input (program control cards included);
* for each program step the used CP and IO times.

The printout of the different program units is listed below.

Table 7.1. Keywords for the several *parts* of the program section data input units.

PROGRAM SECTION	KEYWORD (PART)	NOTES
FAULTTREE	*COMPONENTS*	identifies the component input that consists for each component of: * component name * component failure data (optional) * component description (optional)
	GATES	identifies the input part for the fault tree. It describes for each gate its type and its predecessors.
PROBCAL	*COMPONENTS*	see under *FAULTTREE*. Applicable in the case that no component failure data was added to the input unit *FAULTTREE* or in the case of changes in the component failure data.
	SYSUNAV	marks the time dependent unavailability of a single system. The input consists of: * the instants at which the considered time interval begins and ends, * the number of extra instants for the calculation.
	MISSION	identifies a phased mission calculation. The input consists of: * the instant at which the mission starts and the endpoints of each phase; * the task that each system has to carry out.
IMPCAL	*COMPONENTS*	see *PROBCAL*
	IMPORTANCE	identifies importance calculations. The input consists of: * the number of instants at which the calculation has to be performed; * the cut off value (optional).
COMMODE	*COMPONENTS*	identifies common cause analysis. The input consists of: * for each component its name and the attached labels.
	LABELS	identifies the list of labels. The input consists of: * the name of the label and its description.

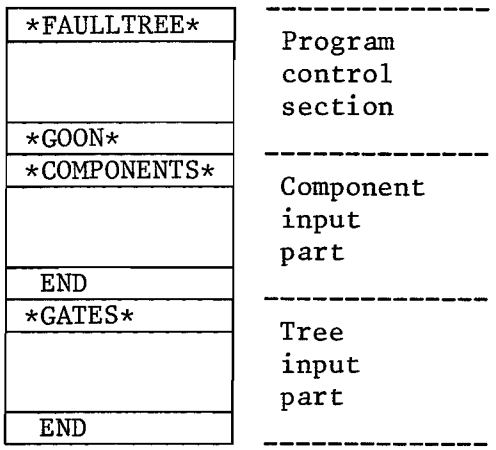


Fig. 7.3. Structure of the FAULTTREE input unit

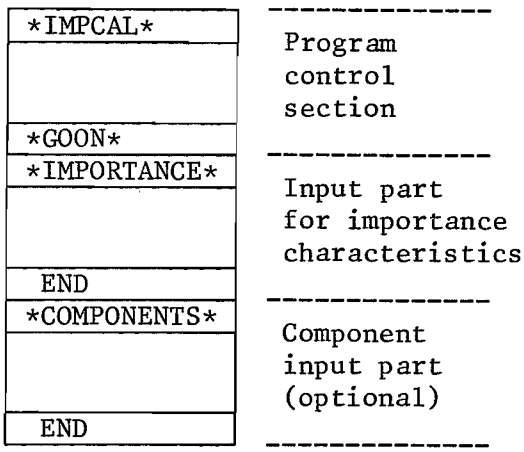


Fig. 7.4. Structure of the IMPCAL input unit

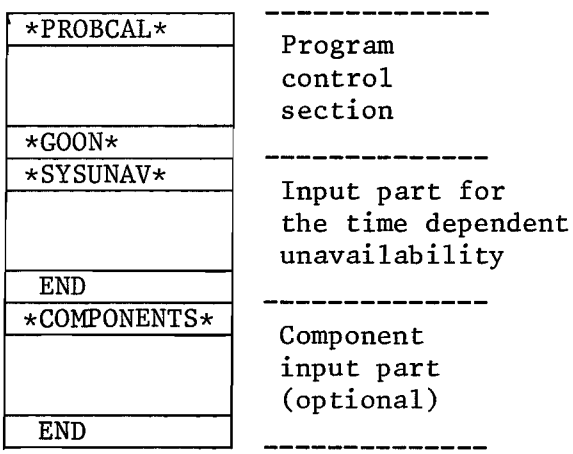


Fig. 7.5.a. Structure of the PROBCAL input unit in the case of a single system

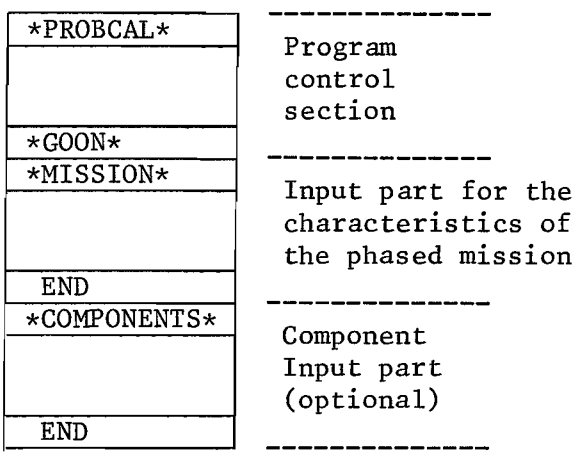


Fig. 7.5b. Structure of the PROBCAL input unit in the case of a phased mission

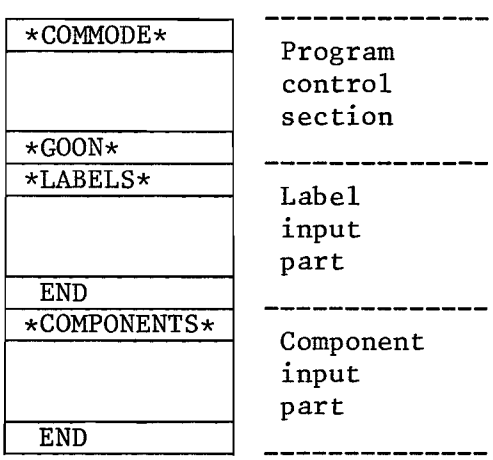


Fig. 7.6. Structure of the COMMODE input unit

PROGRAM SECTION	PRINTED OUTPUT
FAULTTREE	* system characteristics such as the number of basic events, gates, super events etc. of the fault tree; * the minimal cut sets (optional); * a list with the number of minimal cut sets of each order.
PROBCAL	In the case of a single system: * the unavailability at each desired instant; the maximal and minimal unavailability at the considered time interval; * the interval unavailability. In the case of a phased mission: * an upperbound and (optionally) a lowerbound for the probability of mission success.
IMPCAL	* a list of component with their calculated measures of importance, ranked from the high to the low; * a list of minimal cut sets with the same characteristics as the components.
COMMODE	* a list of minimal cut sets where the components of each cut set share at least one *label* that is printed too.

In Appendix C the input deck for PHAMISS and its output is given for the example of a phased mission of the ECCS of the BWR as described in section 6.4. All components are considered to be non-repairable (class 1). The task for each system during the phased mission is to survive, i.e. $u_1=u_2=u_3=1$.
Finally the program characteristics of PHAMISS are put together and shown in table 7.2.

Table 7.2. Characteristics of the reliability computer program PHAMISS

CODE	INPUT	QUANTITATIVE CALCULATIONS	IMPORTANCE CALCULATIONS	UNCERTAINTY ANALYSIS	OTHER FEATURES	TYPE OF COMPUTER LANGUAGE AND AVAILABILITY
PHAMISS	Control information; Basic event names; Optional: basic event description; Basic event failure data; For a single system analysis: - the fault tree description For a phased mission analysis: - the fault tree for each phase - the phase boundary times - the phased mission description For common cause analysis: - basic event labels The input is users friendly. An extensive error checking is performed on the input and throughout the whole program package. The input is free formatted.	For a single system: - time dependent system unavailability For a phased mission: - calculation of the upperbound of the occurrence probability of every branch of a time dependent event tree - calculation of the maximal error in the upperbound of the occurrence probability of a phased mission The code accepts the following classes of components: * non-repairable * monitored * random inspected * periodical inspected EXSITU * periodical inspected INSITU * constant unavailability * constant unavailability during the dormant phase and non-repairable during the operational phase of the mission	Yes, performed by the program section IMPCAL	No	Much attention has been spent to the program section FAULTTREE that generates minimal cut sets: - cut set generation is based on bit manipulation - the used method is from top to bottom, but for special intermediate gates from bottom to top - the limiting number of basic events and gates is 4095 - there is no limit on the number or size of the cut sets - from each intermediate gate the cut sets can be generated - AND, OR and K-of-N gates are implemented - fault tree truncation can be applied by cut set order - the sets of each fault tree are automatically saved on a permanent file, the "save" file for further qualitative and quantitative analysis A plot option is available for - the time dependent unavailability of a single system - the probability of mission failure of the upperbranch of an event tree (the phased mission where every system has to survive its phase)	CDC Cyber-175, FORTRAN IV, segmented loading, available from ECN, Holland

8. CONCLUSIONS AND RECOMMENDATIONS FOR FURTHER WORK

8.1. Introduction

The motivation for the present study is formulated as follows (cf. section 1.3.1.).:

> the need for a general methodology that analyses phased missions and all branches of an event tree with the possibility to take into account repair of the system during its mission and the effects of component models with general distributed lifetimes and repairtimes.

In the chapters 2, 4 and 6 a methodology has been developed which meets the requirements just described. A central point in the development of this methodology is the introduction of the concept of *period of a component* (cf. section 2.3.). The introduction of this concept makes it possible to separate the analysis of the system behaviour from that of the component behaviour. As a result the calculation of the probability of mission success appears to be very simple (cf. table 6.14.). However, that of the component unavailability becomes rather intricate, particularly if no negative exponentially distributed lifetimes and repairtimes are applied (cf. section 4.3.4.2.).
The results of the present study, its advantages and the possibilities offered by the methodology presented here, are discussed in section 8.2. In section 8.3. some recommendations for further work in the field of phased mission analysis are given.

8.2. Results, advantages and possibilities of the present approach

8.2.1. Results

The results of the present study are in fact two-fold:

(A1) A general methodology that
- * can treat phased missions as well as every branch of an event tree because each branch of an event tree can be defined as a phased mission (cf. section 2.4.);
- * takes correctly into account the system dependencies that occur if systems have components in common;

* is applicable to a variety of problem areas of practical interest, such as:
  - risk analysis;
  - complex system behaviour as occurring in, e.g. space travel, safety systems of nuclear power plants, off-shore activities;
  - efficiency and reliability testing of scenarios considered as phased missions, e.g. rescue scenarios, tactical and strategic battle scenarios in warfare.

(A2) A reliability computer program called PHAMISS that evaluates numerically our approach when applied to real systems. It handles single system behaviour as well as sequential system behaviour (phased mission).

8.2.2. Advantages

The advantages of the present approach when compared with the present approach in literature are:

(B1) general lifetime and repairtime distributions for the components can be taken into account;

(B2) a separate treatment of system behaviour and component behaviour during the phased mission by the introduction of the notion *period of a component* (cf. section 2.3.);

(B3) a variety of strategies for maintenance of components can be incorporated in the analysis;

(B4) if the exact values can not be calculated due to a too large computer effort,with reasonable computer effort upperbounds and lowerbounds can be obtained;

(B5) *partial* system failures are correctly taken into account;

(B6) for each phase within an event tree only one fault tree has to be constructed in order to treat every branch of the event tree. Others like Fussell and Arendt [36] think of different trees dependent whether a foregoing system succeeds or fails.

8.2.3. Possibilities

The methodology presented here is able to treat several problem areas within the field of reliability theory. In the following we shall give a brief survey of its possibilities.

(C1) The present approach can analyse phased missions with one objective as it has been shown in chapter 6.

(C2) In some cases the present methodology can treat phased missions with more than one objective as it will be illustrated below for a problem as discussed by Bell [1].
In fig. 8.1. a situation is shown for a system S that has to perform a phased mission with three objectives O_1, O_2 and O_3. The objectives O_1 and O_2 have to be carried out by the subsystems $S_{1,1}$ and $S_{1,2}$, respectively; they do not have components in common. Each of the two subsystems $S_{1,1}$ and $S_{1,2}$ is also independent of the rest of the whole system S. At instant T_1 subsystem $S_{1,1}$ starts its own phased mission separately from the rest of the system. The same occurs for subsystem $S_{1,2}$ at instant T_3. The phased mission for $S_{1,1}$ possesses two phases and that of $S_{1,2}$ three phases.

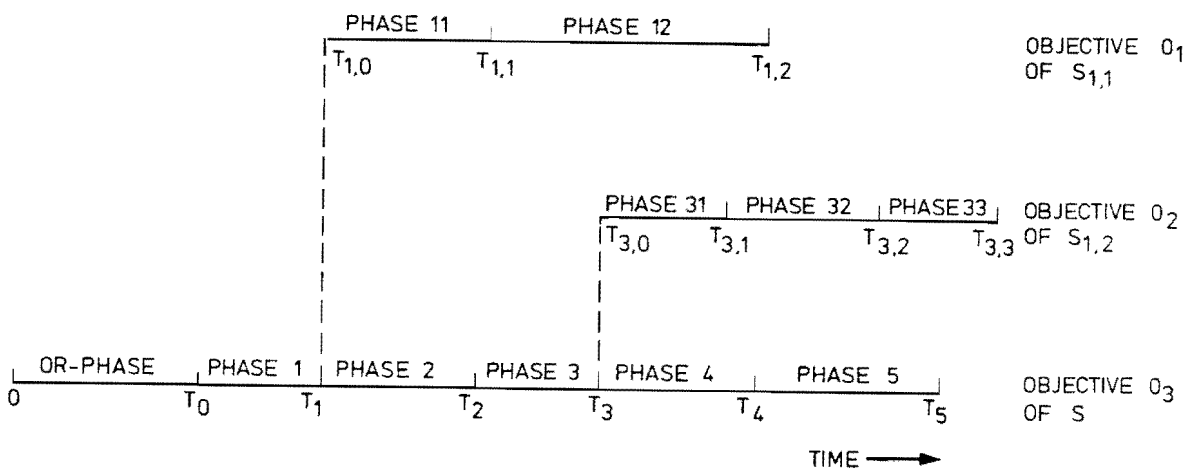


FIG. 8.1. TIME SCHEDULE FOR A MULTIPLE OBJECTIVE PHASED MISSION.

By the present approach it is possible to calculate the probability of mission success for each of the three objectives by defining for each objective a distinct phased mission:

(i) objective O_1: the phased mission consists of the OR-phase, and the phases 1, 11 and 12;

(ii) objective O_2: the phased mission consists of the OR-phase, and the phases 1, 2, 3, 31, 32 and 33;

(iii) objective O_3: the phased mission consists of the OR-phase, and the phases 1, 2, 3, 4 and 5.

For all phased missions each subsystem has to survive its phase. (Other combinations of the tasks of the subsystems are also possible).

(C3) Some maintenance procedures give rise to a phased mission of a single system, for instance the safety system of a nuclear power plant. Often such a safety system contains two chains and it is initiated if *both* chains ask for its function.
Such safety chains are periodically inspected, the one after the other. If one of these chains is inspected its function is "shortened", so that if the other chain asks for its function the safety system is initiated.
During such an inspection the system configuration is changed, i.e. one chain is no longer present in the system. Such a situation may be considered as a phased mission and can be analysed by the present approach.

8.3. Recommendations for further work

We shall briefly indicate some topics within the problem area of phased mission analysis that are of interest for further investigation. They concern:

(D1) phased missions with multistate components;
(D2) confidence intervals for the probability of mission success;
(D3) phased missions with multiple objectives;
(D4) phased missions with stochastic phase duration times.

Ad (1): Single systems with multistate components have been studied by Caldarola [43] and Barlow and Wu [44].

REFERENCES

[1] Bell, G.B. (1975), *Multi-Phase-Mission Reliability of Maintained Standby Systems*, Report NPS-55-Ey-75121, Naval Postgraduate School, Monterey, California.

[2] Burdick, G.R., Fussell, J.B., Rasmuson, D.M. and Wilson, J.R. (1977), Phased Mission Analysis: A Review of New Developments and an Application, *IEEE Transactions on Reliability*, Vol. R-26, No. 1, pp. 43-49.

[3] Caldarola, L. (1977), Unavailability and Failure Intensity of Components, *Nuclear Engineering and Design*, 44, pp. 147-162, North-Holland Publishing Company.

[4] Cohen, J.W. (1969), *The single Server Queue*, North-Holland Publishing Company, Amsterdam.

[5] Cox, D.R. and Miller, H.D. (1970), *Renewal Processes*, Methuen, London.

[6] Esary, J.D. (1977), *The Effect of Modelling Depth on Reliability Prediction for Systems subject to a Phased Mission Profile*, Report NPS-55-77-32, Naval Postgraduate School, Monterey, California.

[7] Esary, J.D., Proschan, F. and Walkup, D.W. (1967), Association of Random Variables, with Applications, *Annals of Mathematical Statistics*, 38, pp. 1466-1474.

[8] Esary, J.D. and Ziehms, H. (1975), Reliability Analysis of Phased Missions, *Reliability and Faulttree Analysis*, SIAM, Philadelphia, pp. 213-236.

[9] Feller, W. (1971), *An introduction to Probability Theory and its Applications*, Vol. II, John Wiley and Sons, New York.

[10] Fussell, J.B., Henry, E.D. and Marshall, N.H. (1974), *MOCUS - A Computer Program to obtain Minimal Cut Sets from Faulttrees*, Report ANCR-1156, Aerojet Nuclear Company, Idaho Falls, Idaho.

[11] Lambert, H.E. (1975), *Faulttrees for Decision Making in Systems Analysis*, Report UCRL-51829, Lawrence Livermore Laboratory.

[12] Rubin, J.C. (1964), The Reliability of Complex Networks, *Proceedings of the Annual Aerospace Reliability and Maintainability Conference*, 3rd, Washington D.C., pp. 262-264.

[13] Weisberg, S.A. and Schmidt, J.H. (1966), Computer Technique for Estimating System Reliability, *Proceedings of the 1966 Annual Symposium on Reliability*, San Francisco, California, pp. 87-97.

[14] Ziehms, H. (1978), Approximations to the Reliability of Phased Missions, *Naval Research Logistic Quarterly*, V25, N2, pp. 229-242.

[15] Ziehms, H. (1974), *Reliability Analysis of Phased Missions*, Report AD/A-003781, Naval Postgraduate School, Monterey, California.

[16] Reactor Safety Study (1975), *An Assessment of Accident Risks in U.S. in Commerical Nuclear Power Plants*, Report NUREG-75/104, U.S. Nulear Regulatory Commission, Washington.

[17] Barlow, R.E. and Proschan, F. (1975), *Statistical Theory of Reliability and Life Testing*, Holt, Rhinehart and Winston, Inc., New York.

[18] Clarotti, C.A. (1981), Limitations of Minimal Cut Set Approach in Evaluating the Reliability of Systems with Repairable Components, *IEEE Transactions on Reliability*, Vol. R-30, pp. 335-338.

[19] Parry, G.W. (1979), *Regeneration Diagrams*, UKAEA report, SRD-R143.

[20] Murchland, J. (1976), Fundamental Probability Relations for Repairable Items, *Proceedings of the NATO Advanced Study Institute on Generic Techniques in Systems Reliability Assessment*, Liverpool, pp. 293-294.

[21] Vesely, W.E. (1970), A Time Dependent Methodology for Faulttree Evaluation, *Nuclear Engineering and Design*, 13, pp. 337-360.

[22] Barlow, R.E. and Proschan, F. (1976), Theory of Maintained Systems: Distribution of Time to First Failure, *Mathematics of Operations Research*, Vol. 1, no. 1, pp. 32-42.

[23] Marshall, A.W. and Proschan, F. (1970), Classes of Distributions applicable in Replacement, with Renewal Theory Implications, *Proceedings of the 6th Berkeley Symposium on Mathematical Statistics and Probability*, Vol. 1, edited by L. le Cam, J. Neyman and E.L. Scott, pp. 395-415, University of California, Berkeley Press.

[24] Caldarola, L. (1976), A Method for the Calculation of the Cumulative Failure Probability Distribution of Complex Repairable Systems, *Nuclear Engineering and Design*, 36, pp. 109-122.

[25] Somma, R. (1980), Markov Approach to System Reliability and its Implementation on Computer, *Reliability Methods based on State Analysis*, C.E.C., Joint Research Center, Ispra, Italy.

[26] Clarotti, C.A., Contini, S., Somma, R. (1980), Repairable Multiphase Systems, Markov and Faulttree Approaches for Reliability Evaluation, *Synthesis and Analysis Methods for Safety and Reliability Studies*, edited by G. Apostolakis, S. Garriba and G. Volta, Plenum Press, New York and London.

[27] Fussell, J.B. (1981), *Phased Mission System Reliability Analysis*, Vol. 1: Methodology, Vol. 2: Computer Code, Report EPRI NP-1945, Palo Alto, California.

[28] Fréchet, M. (1940), *Les Probabilités associées a un système d'événements compatibles et dépendants*, Première partie, Hermann & Cie, Editeurs, Paris.

[29] Henley, E.J. and Kumamoto, H. (1981), *Reliability Engineering and Risk Assessment*, Prentice Hall, Inc., Englewood Cliffs, N.J.

[30] Hwang, C.L., Tillman, F.A., Lee, M.H. (1981), System Reliability Evaluation Techniques for Complex/Large Systems - A Review, *IEEE Transactions on Reliability*, Vol. R-30, No. 5, pp. 416-423.

[31] Barlow, R.E. and Proschan, F. (1976), Some Current Academic Research in System Reliability Theory, *IEEE Transactions on Reliability*, Vol. R-25, No. 3, pp. 198-202.

[32] —— (1975), *Reliability and Fault Tree Analysis*, edited by R.E. Barlow, J.B. Fussell and N.D. Singpurwalla, SIAM, Philadelphia.

[33] Cambell, D.J. (1978), *A Procedure for Determining the Importance of Basis Events to Systems Undergoing a Phased Mission*, Report NERS-78-07, University of Tennessee, Knoxville.

[34] Montague, D.F. (1979), *A Procedure for Determining the Expected Number of Failures of a Phased Mission* , Report NERS-79-03, University of Tennessee, Knoxville.

[35] Pedar, A. and Sarma, V.V.S. (1981), Phased Mission Analysis for Evaluating the Effectiveness of Aerospace Computing Systems, *IEEE Transactions on Reliability*, Vol. R-30, no. 5, pp. 429-437.

[36] Fussell, J.B. and Arendt, J.S. (1979), System Reliability Engineering Methodology: A Discussion of the State of the Art, *Nuclear Safety*, Vol. 20, no. 5, pp. 541-550.

[37] —— (1977), *Nuclear Systems Reliability Engineering and Risk Assessment*, edited by J.B. Fussell and G.R. Burdick, SIAM, Philadelphia.

[38] —— (1982), *PRA Procedures Guide*, A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants, Report NUREG/CR-2300, Review Draft, Vol. 1 and Vol. 2, U.S. Nuclear Regulatory Commission, Washington.

[39] Terpstra, K. and Dekker, N.H. (1984), *PHAMISS - A Reliability Computer Program for Phased Mission Analysis and Risk Analysis*, Users-Manual, ECN, Petten (to be issued).

[40] —— (1975), *Risico-analyse van de splijtstofcyclus in Nederland*, N.V. Samenwerkende Electriciteits-Productiebedrijven, Arnhem.

[41] —— (1979), *Deutsche Risikostudie Kernkraftwerke*, Verlag TUV Rheinland GmbH, Köln.

[42] Barlow, R.E. and Proschan, F.H. (1965), *Mathematical Theory of Reliability*, John Wiley and Sons, Inc., New York.

[43] Caldarola, L. (1980), *Generalized Faulttree Analysis Combined with State Analysis*, Report KfK 2530, Kernforschungszentrum Karlsruhe.

[44] Barlow, R.E. and Wu, A.S. (1978), Coherent Systems with Multistate Components, *Mathematics of Operations Research*, Vol. 3, no. 4, pp. 275-281.

[45] Lewis, H.W. et al (1978), *Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission*, Report NUREG/CR-0400, U.S. Nuclear Regulatory Commission, Washington.

LIST OF ABBREVIATIONS

ADS	Automatic Depressurization System
BWR	Boiling Water Reactor
CS	Cooling System
CVD	Checkvalve (near diesel pump)
CVE	Checkvalve (near electro pump)
CVM	Checkvalve (near main circulation pump)
DM	Diesel Motor
DP	Diesel Pump
DPM	Component (subsystem) consisting of the diesel driven pump DP and the diesel motor DM
ECCS	Emergency Core Cooling System
EDPS	Emergency Diesel Pump System
EM	Electro Motor
EP	Electro Pump
EPM	Component (subsystem) consisting of the electro driven pump EP and the electro motor EM
ERHPS	Emergency and Residual Heat Removal Pumping System
FTA	Fault Tree Analysis
HE	Heat Exchanger
HPCS	High Pressure Core Spray system
HRS	Heat Removal System
LOCA	Loss of Coolant Accident
LPCI	Low Pressure Core Injection system
LPCS	Low Pressure Core Spray system
MCP	Main Circulation Pump
MCPS	Main Circulation Pump System
MTBF	Mean Time Between Failures
NBU	New Better than Used
OR-phase	Operational Readiness phase
SPCS	Suppression Pool Cooling System
VD	Hand operated valve (near diesel pump)
VE	Hand operated valve (near electro pump)
VM	Hand operated valve (near main circulation pump)

APPENDIX A

THE RENEWAL FUNCTION AND THE FUNCTION $G_0(t,\zeta)$ OF A RENEWAL PROCESS WITHOUT REPAIR IN THE CASE OF THE ERLANG LIFETIME DISTRIBUTION

Consider a renewal process where the time between two successive renewals is defined by the Erlang distribution

$$F(t) = 1-e^{-\lambda t} \sum_{i=0}^{k-1} \frac{(\lambda t)^i}{i!} , \quad t\geq 0, \ \lambda>0. \tag{A1}$$

A realisation of the above mentioned renewal process is the process of an installed component starting its life at t=0, and immediately replaced by an identical component when it fails, etc., with the Erlang distribution as lifetime distribution.
The Laplace-Stieltjes transform of F(t) is

$$f(\rho) = \frac{1}{(1+\rho/\lambda)^k} , \quad \mathrm{Re}\rho > -\lambda. \tag{A2}$$

From (3.4) (Chapter 3) it follows that the Laplace-Stieltjes transform of the renewal function $m_0(t)$ reads

$$h(\rho) = \frac{f(\rho)}{1-f(\rho)} = \frac{1}{(1+\rho/\lambda)^k-1}$$

$$= \sum_{j=0}^{k-1} \frac{a_j}{(1+\rho/\lambda)-\theta^j}$$

$$= \sum_{j=1}^{k-1} \frac{a_j}{1-\theta^j} \frac{\lambda(1-\theta^j)}{\rho+\lambda(1-\theta^j)} ,$$

where

$$\theta \stackrel{\mathrm{def}}{=} e^{\frac{2\pi i}{k}} . \tag{A3}$$

The constants a_j, j=0,1,...,k-1 are determined by

$$a_j = \lim_{s\to\theta^j} \frac{s-\theta^j}{s^k-1} = \lim_{s\to\theta^j} \frac{1}{ks^{k-1}} = \frac{1}{k\theta^{j(k-1)}} = \frac{\theta^j}{k}, \quad j=0,1,\ldots,k-1.$$

So $h(\rho)$ reads

$$h(\rho) = \frac{\lambda}{k\rho} + \frac{1}{k} \sum_{j=1}^{k-1} \frac{\theta^j}{1-\theta^j} \frac{\lambda(1-\theta^j)}{\rho+\lambda(1-\theta^j)}, \quad \mathrm{Re}\rho>0.$$

By inverse transformation it follows for $m_0(t)$ that

$$m_0(t) = \frac{\lambda t}{k} + \frac{1}{k} \sum_{j=1}^{k-1} \frac{\theta^j}{1-\theta^j} \{1-e^{-\lambda t(1-\theta^j)}\}, \quad t\geq 0, \ \lambda>0, \tag{A4}$$

and θ as defined by (A3).

From (3.22) and because of (3.37) the function $G_0(t,\zeta)$ for this process reads

$$G_0(t,\zeta) = F(t+\zeta) - F(t) + \int_{\tau=0}^{t} \{F(t+\zeta-\tau) - F(t-\tau)\} dm_0(\tau), \quad t\geq 0, \ \zeta\geq 0,$$

and by substituting (A1) and (A4) it follows that

$$\begin{aligned} G_0(t,\zeta) &= e^{-\lambda t} \sum_{i=0}^{k-1} \left[\frac{(\lambda t)^i}{i!} - \frac{\{\lambda(t+\zeta)\}^i}{i!} e^{-\lambda\zeta}\right] \\ &\quad + \int_0^t \left[\sum_{i=0}^{k-1} \left\{\frac{\{\lambda(t-\tau)\}^i}{i!} - \frac{\{\lambda(t+\zeta-\tau)\}^i}{i!} e^{-\lambda\zeta}\right\} e^{-\lambda(t-\tau)}\right] \\ &\quad \cdot \frac{\lambda}{k}\left[1+\sum_{j=1}^{k-1} \theta^j e^{-\lambda\tau(1-\theta^j)}\right] d\tau \\ &= e^{-\lambda t} \sum_{i=0}^{k} \left[\frac{(\lambda t)^i}{i!} - \frac{\{\lambda(t+\zeta)\}^i}{i!} e^{-\lambda\zeta}\right] \\ &\quad + \frac{\lambda}{k} e^{-\lambda t} \sum_{i=0}^{k-1} \frac{\lambda^i}{i!}\left[e^{\lambda t} \int_{v=0}^{t} v^i e^{-\lambda v} dv - e^{\lambda t} \int_{v=\zeta}^{t+\zeta} v^i e^{-\lambda v} dv\right. \\ &\quad \left. + \sum_{j=1}^{k-1} \theta^j \left\{e^{\lambda\theta^j t} \int_{v=0}^{t} v^i e^{-\lambda\theta^j v} dv \right.\right. \\ &\quad \left.\left. - e^{\lambda\theta^j(t+\zeta)} e^{-\lambda\zeta} \int_{v=\zeta}^{t+\zeta} v^i e^{-\lambda\theta^j v} dv\right\}\right]. \end{aligned}$$

With

$$\int_{\alpha}^{\beta} v^i e^{-\lambda v}\, dv = e^{-\lambda\alpha} \sum_{k=0}^{i} \frac{i!}{k!} \frac{\alpha^k}{\lambda^{i-k+1}} - e^{-\lambda\beta} \sum_{k=0}^{i} \frac{i!}{k!} \frac{\beta^k}{\lambda^{i-k+1}}\ ,\ \beta>\alpha,$$

and some reorganisation, the function $G_0(t,\zeta)$ reads

$$G_0(t,\zeta) = e^{-\lambda t} \sum_{i=0}^{k} \left[\frac{(\lambda t)^i}{i!} - \frac{\{\lambda(t+\zeta)\}^i}{i!} e^{-\lambda\zeta}\right] +$$

$$+ \frac{1}{k} \sum_{i=0}^{k-1} \left[1 - \sum_{n=0}^{i} \left\{\frac{(\lambda t)^n}{n!} e^{-\lambda t} + \frac{(\lambda\zeta)^n}{n!} e^{-\lambda\zeta} - \frac{\{\lambda(t+\zeta)\}^n}{n!} e^{-\lambda(t+\zeta)}\right\}\right.$$

$$\left. + e^{-\lambda t} \sum_{j=1}^{k-1} \left\{\frac{e^{\lambda\theta^j t}}{\theta^{ji}} - \sum_{n=0}^{i} \frac{1}{\theta^{j(i-n)}} \left\{\frac{(\lambda t)^n}{n!} + \frac{(\lambda\zeta)^n}{n!} e^{\lambda\theta^j t - \lambda\zeta}\right.\right.\right.$$

$$\left.\left.\left. - \frac{\{\lambda(t+\zeta)\}^n}{n!} e^{-\lambda(t+\zeta)}\right\}\right\}\right], \qquad \text{(A5)}$$

$$\theta = e^{\frac{2\pi i}{k}};\ t\geq 0,\ \zeta\geq 0,\ \lambda>0,\ k=1,2,\ldots,$$

From (A5) it is immediately clear that

$$G_0(0,\zeta) = \lim_{t\to 0} G_0(t,\zeta) = 1 - e^{-\lambda\zeta} \sum_{i=0}^{k-1} \frac{(\lambda\zeta)^i}{i!}\ ,\ \zeta\geq 0,\ \lambda>0,$$

which means that at the start of the renewal process the function $G_0(0,\zeta)$ is simply the Erlang distribution itself, which is evident.
As an illustration we shall present the explicit expressions of the renewal function and the function $G_0(t,\zeta)$ for the cases that k=2 and k=3. With some elementary calculations it is deduced from (A4) and (A5) that

<u>k=2</u>

$$m_0(t) = \frac{\lambda t}{2} - \frac{1-e^{-2\lambda t}}{4}\ ,\ t\geq 0,\ \lambda>0; \qquad \text{(A6)}$$

$$G_0(t,\zeta) = 1-e^{-\lambda\zeta} - \frac{1}{2}\lambda\zeta e^{-\lambda\zeta}\,(1+e^{-2\lambda t}),\ t\geq 0,\ \zeta\geq 0,\ \lambda>0\ . \qquad \text{(A7)}$$

<u>k=3</u>

$$m_0(t) = \frac{\lambda t-1}{3} + \frac{1}{9}\{3\cos(\tfrac{1}{2}\sqrt{3}\,\lambda t) - \sqrt{3}\sin(\tfrac{1}{2}\sqrt{3}\,\lambda t)\}e^{-\frac{3}{2}\lambda t}, \quad t\geq 0,\ \lambda>0; \qquad \text{(A8)}$$

$$G_0(t,\zeta) = 1 - \{1 + \frac{2}{3}\lambda\zeta + \frac{1}{6}(\lambda\zeta)^2\}\,e^{-\lambda\zeta} + \frac{1}{2}(\lambda t)^2\,e^{-\lambda t}$$

$$- \frac{1}{3}[\{\lambda\zeta + (\lambda\zeta)^2\}\cos(\tfrac{1}{2}\sqrt{3}\,\lambda t) + \sqrt{3}\sin(\tfrac{1}{2}\sqrt{3}\,\lambda t)], \qquad \text{(A9)}$$

$$t\geq 0,\ \zeta\geq 0,\ \lambda>0.$$

APPENDIX B

SPECIFICATIONS FOR SEVERAL LIFETIME AND REPAIRTIME DISTRIBUTIONS OF THE QUANTITIES DISCUSSED IN CHAPTER 3

In this section explicit formulas for the quantities $A_0(t)$, $A_1(t)$, $m_0(t)$, $m_1(t)$, $G_0(t,\zeta)$ and $G_1(t,\zeta)$ will be presented for special lifetime- and repairtime distributions.
Its contents consists of:

page

B1 Components without repair and without replacement

The general expressions for the availability and the function $G_0(t,\zeta)$ are:

$$A_0(t) = 1 - F(t), \quad t \geq 0; \tag{B1}$$

$$G_0(t,\zeta) = F(t+\zeta) - F(t), \quad t \geq 0, \ \zeta \geq 0. \tag{B2}$$

B1.1 Lifetime distribution: negative exponential distribution

$$F(t) = 1 - e^{-\lambda t}, \quad t \geq 0, \ \lambda > 0; \tag{B3}$$

$$A_0(t) = e^{-\lambda t}, \quad t \geq 0, \ \lambda > 0; \tag{B4}$$

$$G_0(t,\zeta) = 1 - e^{-\lambda \zeta}, \quad t \geq 0, \ \zeta \geq 0, \ \lambda > 0. \tag{B5}$$

B1.2 Lifetime distribution: Erlang distribution

$$F(t) = 1 - e^{-\lambda t}\{1 + \lambda t + \ldots + \frac{(\lambda t)^{k-1}}{(k-1)!}\}, \quad t \geq 0, \ \lambda > 0, \ k = 1,2,\ldots . \tag{B6}$$

Because of practical considerations only the cases where k=2 and k=3 are treated.

k=2

For $t \geq 0$, $\zeta \geq 0$ and $\lambda > 0$ it follows that:

$$F(t) = 1 - e^{-\lambda t}(1 + \lambda t); \tag{B7}$$

$$A_0(t) = (1 + \lambda t)e^{-\lambda t}; \tag{B8}$$

$$G_0(t,\zeta) = 1 - e^{-\lambda(t+\zeta)} - \lambda(t+\zeta)e^{-\lambda(t+\zeta)} - \{1 - e^{-\lambda t}(1 + \lambda t)\}$$

$$= \{1 - (1 + \frac{\lambda\zeta}{1+\lambda t})\, e^{-\lambda\zeta}\}(1+\lambda t)e^{-\lambda t}. \tag{B9}$$

k=3

Fot $t \geq 0$, $\zeta \geq 0$ and $\lambda > 0$ it follows that:

$$F(t) = 1 - e^{-\lambda t}\{1 + \lambda t + \tfrac{1}{2}(\lambda t)^2\}; \tag{B10}$$

$$A_0(t) = e^{-\lambda t}\{1 + \lambda t + (\tfrac{1}{2}\lambda t)^2\}; \tag{B11}$$

$$G_0(t,\zeta) = 1 - e^{-\lambda(t+\zeta)}\{1 + \lambda(t+\zeta) + \tfrac{1}{2}\lambda^2(t+\zeta)^2\} -$$

$$[1 - e^{-\lambda t}\{1 + \lambda t + \tfrac{1}{2}(\lambda t)^2\}]$$

$$= [1 - \frac{1 + \lambda(t+\zeta) + \tfrac{1}{2}\lambda^2(t+\zeta)^2}{1 + \lambda t + \tfrac{1}{2}(\lambda t)^2}\, e^{-\lambda\zeta}]\{1 + \lambda t + \tfrac{1}{2}(\lambda t)^2\}\, e^{-\lambda t}. \tag{B12}$$

The parameter λ can be obtained from the relation:

$$E\{\underline{\ell}\} = k/\lambda, \quad k=1,2,\ldots, \tag{B13}$$

so that in the cases of k=2 and k=3, respectively,

$$\lambda = 2/E\{\underline{\ell}\} \text{ and } \lambda = 3/E\{\underline{\ell}\}.$$

B2 Components which are immediately replaced

Here we have to discuss components subject to the renewal process described in section 3.2. It is supposed here that the distribution of the lifetime of the first component is equal to the other lifetime distributions, i.e. $F_1(t) = F(t)$. So from section 3.4. it follows that for every distribution of the lifetime:

$$a_0(\rho) = \{1 - f(\rho)\}\{1 + h_0(\rho)\} = \{1 - f(\rho)\}\{1 + \frac{f(\rho)}{1-f(\rho)}\} = 1,$$

so, for this process it is obvious that

$$A_0(t) = 1, \quad t \geq 0. \tag{B14}$$

B2.1 Lifetime distribution: negative exponential distribution

$$F(t) = 1 - e^{-\lambda t}, \quad t \geq 0, \ \lambda > 0;$$

$$A_0(t) = 1, \quad t \geq 0 \text{ (see (B14))}.$$

From section 3.4 it follows that for $f(\rho) = \lambda/(\rho+\lambda)$:

$$h_0(\rho) = \frac{f(\rho)}{1-f(\rho)} = \frac{\lambda/(\rho+\lambda)}{1-\lambda/(\rho+\lambda)} = \frac{\lambda}{\rho}, \quad \mathrm{Re}(\rho) > 0,$$

so that the average number of renewals in [0,t] reads

$$m_0(t) = \lambda t, \quad t \geq 0, \ \lambda > 0. \tag{B15}$$

The renewal process appears to be the Poisson process.
From (3.33), (B15) the function $G_0(t,\zeta)$ is obtained by:

$$G_0(t,\zeta) = 1 - e^{-\lambda(t+\zeta)} - 1 + e^{-\lambda t} + \int_0^t \{1 - e^{-\lambda(t+\zeta-\tau)} - 1 + e^{-\lambda(t-\tau)}\} d(\lambda\tau)$$

$$= 1 - e^{-\lambda\zeta}, \quad t \geq 0, \ \zeta \geq 0, \ \lambda > 0. \tag{B16}$$

B2.2 Lifetime distribution: Erlang distribution with k=2 and k=3

k=2

$$F(t) = 1 - e^{-\lambda t}(1 + \lambda t), \quad t \geq 0, \ \lambda > 0;$$

$$f(\rho) = \frac{1}{(1+\rho/\lambda)^2}, \quad \mathrm{Re}(\rho) > -\lambda; \tag{B17}$$

$$A_0(t) = 1.$$

From the expressions (A6) and (A7) in appendix A it follows for the renewal function and the function $G_0(t,\zeta)$:

$$m_0(t) = \tfrac{1}{2}\lambda t - \frac{1 - e^{-2\lambda t}}{4}, \quad t\geq 0, \ \lambda>0; \tag{B18}$$

$$G_0(t,\zeta) = 1 - e^{-\lambda\zeta} - \tfrac{1}{2}\lambda\zeta e^{-\lambda\zeta}(1 + e^{-2\lambda t}), \quad t\geq 0, \ \zeta\geq 0, \ \lambda>0. \tag{B19}$$

k=3

$$F(t) = 1 - e^{-\lambda t}\{1 + \lambda t + \tfrac{1}{2}(\lambda t)^2\};$$

$$f(\rho) = \frac{1}{(1+\rho/\lambda)^3}, \quad \mathrm{Re}(\rho) > -\lambda; \tag{B20}$$

$$A_0(t) = 1, \quad t\geq 0.$$

From the expressions (A8) and (A9) in appendix A it follows for $m_0(t)$ and $G_0(t,\zeta)$ that:

$$m_0(t) = \frac{\lambda t-1}{3} + \frac{1}{9}\{3\cos(\tfrac{1}{2}\sqrt{3}\lambda t) - \sqrt{3}\sin(\tfrac{1}{2}\sqrt{3}\lambda t)\} e^{-3\lambda t/2}, \quad t\geq 0, \ \lambda>0; \tag{B21}$$

$$G_0(t,\zeta) = 1 - \{1 + \frac{2}{3}\lambda\zeta + \frac{1}{6}(\lambda\zeta)^2\} e^{-\lambda\zeta} + \tfrac{1}{2}(\lambda t)^2 e^{-\lambda t} - \frac{1}{3}[\{\lambda\zeta + (\lambda\zeta)^2\}\cos(\tfrac{1}{2}\sqrt{3}\lambda t) + \sqrt{3}\sin(\tfrac{1}{2}\sqrt{3}\lambda t)], \quad t\geq 0, \ \zeta\geq 0, \ \lambda>0. \tag{B22}$$

B3 Components subjected to the alternating renewal process

The alternating renewal process is described in section 3.3.1.

B3.1 Negative exponential lifetime distribution and negative exponential repairtime distribution

$$F(t) = 1 - e^{-\lambda t}, \quad t\geq 0, \ \lambda>0;$$

$$W(t) = 1 - e^{-\mu t}, \quad t \geq 0, \ \mu > 0; \tag{B23}$$

$$f(\rho) = \frac{\lambda}{\rho+\lambda}, \quad \mathrm{Re}(\rho) > -\lambda; \tag{B24}$$

$$w(\rho) = \frac{\mu}{\rho+\mu}, \quad \mathrm{Re}(\rho) > -\mu. \tag{B25}$$

From (3.7), (B24) and (B25):

$$h_0(\rho) = \frac{f(\rho)}{1-w(\rho)f(\rho)} = \frac{\lambda(\rho+\mu)}{\rho(\rho+\lambda+\mu)}, \quad \mathrm{Re}(\rho) > 0; \tag{B26}$$

$$h_1(\rho) = \frac{f(\rho)w(\rho)}{1-f(\rho)w(\rho)} = \frac{\lambda\mu}{\rho(\rho+\lambda+\mu)}, \quad \mathrm{Re}(\rho) > 0. \tag{B27}$$

By inverse Laplace transformation it follows from (B26) and (B27) that the renewal functions $m_0(t)$ and $m_1(t)$ are given by:

$$m_0(t) = \frac{\lambda\mu}{\lambda+\mu} t + \frac{\lambda^2}{\lambda+\mu} \{1 + e^{-(\lambda+\mu)t}\}, \quad t \geq 0, \ \lambda > 0, \ \mu > 0; \tag{B28}$$

$$m_1(t) = \frac{\lambda\mu}{\lambda+\mu} \left[t - \frac{1}{\lambda+\mu} \{1 - e^{-(\lambda+\mu)t}\}\right], \quad t \geq 0, \ \lambda > 0, \ \mu > 0. \tag{B29}$$

From (3.11), (3.12), (B24) and (B25), $a_0(\rho)$ and $a_1(\rho)$ are given by:

$$a_0(\rho) = \frac{\rho+\mu}{\rho+\lambda+\mu}, \quad \mathrm{Re}(\rho) > -(\lambda+\mu); \tag{B30}$$

$$a_1(\rho) = \frac{\mu}{\rho+\lambda+\mu}, \quad \mathrm{Re}(\rho) > -(\lambda+\mu). \tag{B31}$$

By inverse transformation we obtain from (B30) and (B31):

$$A_0(t) = 1 - \frac{\lambda}{\lambda+\mu} \{1 - e^{-(\lambda+\mu)t}\}, \quad t \geq 0, \ \lambda > 0, \ \mu > 0; \tag{B32}$$

$$A_1(t) = \frac{\mu}{\lambda+\mu} \{1 - e^{-(\lambda+\mu)t}\}, \quad t \geq 0, \ \lambda > 0, \ \mu > 0. \tag{B33}$$

From (3.34), (3.35), (B28), (B29), (B32) and (B33) the functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ are derived:

$$G_0(t,\zeta) = (1 - e^{-\lambda\zeta})\, A_0(t), \quad t\geq 0, \ \zeta\geq 0, \ \lambda>0; \tag{B34}$$

$$G_1(t,\zeta) = (1 - e^{-\lambda\zeta})\, A_1(t,\zeta), \quad t\geq 0, \ \zeta\geq 0, \ \lambda>0. \tag{B35}$$

This result can also be obtained by remembering that the negative exponential distribution is *memoryless*.

B3.2 Erlang-2 lifetime distribution and negative exponential repair-time distribution

$$F(t) = 1 - e^{-\lambda t}(1 + \lambda t), \quad t\geq 0, \ \lambda>0;$$

$$W(t) = 1 - e^{-\mu t}, \quad t\geq 0, \ \mu>0;$$

$$f(\rho) = \frac{\lambda^2}{(\rho+\lambda)^2}, \quad \mathrm{Re}(\rho) > -\lambda;$$

$$w(\rho) = \frac{\mu}{\rho+\mu}, \quad \mathrm{Re}(\rho) > -\mu.$$

The Laplace-Stieltjes transforms of $m_0(t)$, $m_1(t)$, $A_0(t)$ and $A_1(t)$ all have the same denominator (see (3.7), (3.11) and (3.12)), i.e.

$$1 - f(\rho)w(\rho) = 1 - \frac{\lambda^2\mu}{(\rho+\lambda)^2(\rho+\mu)}$$

$$= \frac{\rho\{\rho^2+(\mu+2\lambda)\rho+\lambda^2+2\lambda\mu\}}{(\rho+\lambda)^2(\rho+\mu)}.$$

The zero's of the expression above are:

$$\rho_{1,2} = -\tfrac{1}{2}(\mu+2\lambda) \pm \tfrac{1}{2}\sqrt{\mu^2-4\lambda\mu}, \ \rho_3=0. \tag{B36}$$

There are three cases for which the zero's are different, i.e. $\mu^2-4\lambda\mu>0$, $\mu^2-4\lambda\mu=0$ and $\mu^2-4\lambda\mu<0$. Define:

$$\alpha = -\tfrac{1}{2}(\mu+2\lambda),\ \beta = \tfrac{1}{2}\sqrt{\mu^2-4\lambda\mu},\ \sigma = \sqrt{4\lambda\mu-\mu^2}. \tag{B37}$$

Three cases are now:

$$\text{case 1: } \rho_{1,2} = \alpha\pm\beta\ ,\ \rho_3=0; \tag{B38}$$

$$\text{case 2: } \rho_{1,2} = \alpha\ \ \ ,\ \rho_3=0; \tag{B39}$$

$$\text{case 3: } \rho_{1,2} = \alpha\pm i\sigma,\ \rho_3=0, \tag{B40}$$

where $i^2 = -1$.
Because all the three cases can be treated in a similar way only case 1 is discussed here.

Case 1: $\rho_{1,2} = \alpha\pm\beta,\ \rho_3=0$.

From (3.7) and the above mentioned it follows that:

$$h_0(\rho) = \frac{f(\rho)}{1-f(\rho)w(\rho)} = \frac{\lambda^2(\rho+\mu)}{\rho(\rho-\rho_1)(\rho-\rho_2)}\ ,\ \mathrm{Re}(\rho) > 0.$$

$\Rightarrow$

$$m_0(t) = \alpha_1 + \alpha_2 t + \alpha_3 e^{\rho_1 t} + \alpha_4 e^{\rho_2 t},\ t\geq 0, \tag{B41}$$

$$\left.\begin{aligned} \alpha_1 &= \frac{2\alpha\lambda^2\mu + \lambda^2(\alpha^2-\beta^2)}{(\alpha^2-\beta^2)^2},\ \alpha_2 = \frac{\lambda^2\mu}{\alpha^2-\beta^2}\ , \\ \alpha_3 &= \frac{(\rho_1+\mu)\lambda^2}{2\beta\rho_1^2}\ ,\ \alpha_4 = -\frac{(\rho_2+\mu)\lambda^2}{2\beta\rho_2^2}\ . \end{aligned}\right\} \tag{B42}$$

Also from (3.7) it follows that:

$$h_1(\rho) = \frac{f(\rho)w(\rho)}{1-f(\rho)w(\rho)} = \frac{\lambda^2\mu}{\rho(\rho-\rho_1)(\rho-\rho_2)}\ ,\ \mathrm{Re}(\rho) > 0.$$

$\Rightarrow$

$$m_1(t) = \alpha_1 + \alpha_2 t + \alpha_3 e^{\rho_1 t} + \alpha_4 e^{\rho_2 t}, \quad t \geq 0, \tag{B43}$$

$$\left.\begin{aligned} \alpha_1 &= \frac{2\alpha\lambda^2\mu}{(\alpha^2-\beta^2)^2} \quad , \quad \alpha_2 = -\frac{\lambda^2\mu}{\alpha^2-\beta^2} \, , \\ \alpha_3 &= \frac{\lambda^2\mu}{2\beta\rho_1^2} \quad , \quad \alpha_4 = -\frac{\lambda^2\mu}{2\beta\rho_2^2} \, . \end{aligned}\right\} \tag{B44}$$

From (3.11) we get for $a_0(\rho)$:

$$a_0(\rho) = \frac{1-f(\rho)}{1-f(\rho)w(\rho)} = 1 - \frac{\lambda^2}{(\rho-\rho_1)(\rho-\rho_2)} \, , \quad \mathrm{Re}(\rho) > 0.$$

$\Rightarrow$

$$A_0(t) = 1 - \frac{\lambda^2}{\alpha^2-\beta^2} - \frac{\lambda^2}{2\beta}\left\{\frac{e^{\rho_1 t}}{\rho_1} - \frac{e^{\rho_2 t}}{\rho_2}\right\}, \quad t \geq 0. \tag{B45}$$

From (3.12) it follows for $a_1(\rho)$ that:

$$a_1(\rho) = \frac{\{1-f(\rho)\}w(\rho)}{1-f(\rho)w(\rho)} = \frac{\mu(\rho+2\lambda)}{\rho(\rho-\rho_1)(\rho-\rho_2)} \, , \quad \mathrm{Re}(\rho) > 0.$$

$\Rightarrow$

$$A_1(t) = \frac{2\lambda\mu}{\alpha^2-\beta^2} + \frac{\mu}{2\beta}\left\{\frac{(\rho_1+2\lambda)e^{\rho_1 t}}{\rho_1} - \frac{(\rho_2+2\lambda)e^{\rho_2 t}}{\rho_2}\right\} \, , \quad t \geq 0. \tag{B46}$$

From (B41) and W(t) as defined above it follows that:

$$\frac{d}{dt}\{m_0(t) * W(t)\} = \beta_1 + \beta_3 e^{\rho_1 t} + \beta_4 e^{\rho_2 t} \, , \quad t \geq 0, \tag{B47}$$

$$\beta_1 = -\alpha_2, \quad \beta_3 = \frac{\mu\alpha_3\rho_1}{\rho_1+\mu} \, , \quad \beta_4 = \frac{\mu\alpha_4\rho_2}{\rho_2+\mu} \, , \tag{B48}$$

with α_2, α_3 and α_4 as defined by (B42).

From (3.34) and (B47) the function $G_0(t,\zeta)$ is given by:

$$G_0(t,\zeta) = v_0(t)\ \{1-(1+\lambda\zeta)e^{-\lambda\zeta}\} + w_0(t)\lambda(1-e^{-\lambda\zeta}),\ t\geq 0,\ \zeta\geq 0, \quad \text{(B49)}$$

$$\left.\begin{aligned} v_0(t) &= \frac{\mu}{\lambda+2\mu} + \frac{\lambda^2\mu}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 t}}{\rho_1(\rho_1+\lambda)} - \frac{e^{\rho_2 t}}{\rho_2(\rho_2+\lambda)}\right\}, \\ w_0(t) &= \frac{\mu}{\lambda(\lambda+2\mu)} + \frac{\lambda^2\mu}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 t}}{\rho_1(\rho_1+\lambda)^2} - \frac{e^{\rho_2 t}}{\rho_2(\rho_2+\lambda)^2}\right\}. \end{aligned}\right\} \quad \text{(B50)}$$

Using the same procedure as for $G_0(t,\zeta)$ we get from (3.35) for $G_1(t,\zeta)$:

$$G_1(t,\zeta) = v_1(t)\ \{1-(1+\lambda\zeta)e^{-\lambda\zeta}\} + w_1(t)\lambda(1-e^{-\lambda\zeta}),\ t\geq 0,\ \zeta\geq 0, \quad \text{(B51)}$$

$$\left.\begin{aligned} v_1(t) &= \frac{\mu}{\lambda+2\mu} + \frac{\lambda\mu^2}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 t}}{\rho_1(\rho_1+\mu)(\rho_1+\lambda)} - \frac{e^{\rho_2 t}}{\rho_2(\rho_2+\mu)(\rho_2+\lambda)}\right\}, \\ w_1(t) &= \frac{\mu}{\lambda+2\mu} + \frac{\lambda\mu^2}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 t}}{\rho_1(\rho_1+\mu)(\rho_1+\lambda)^2} - \frac{e^{\rho_2 t}}{\rho_2(\rho_2+\mu)(\rho_2+\lambda)^2}\right\}. \end{aligned}\right\} \quad \text{(B52)}$$

B4 Components subjected to the random test process

In this section the random test process as described in chapter 3 will be treated. The lifetime and the repairtime are assumed to be negative exponentially distributed, i.e.

$$F(t) = 1 - e^{-\lambda t},\ t\geq 0,\ \lambda>0;$$

$$W(t) = 1 - e^{-\mu t},\ t\geq 0,\ \mu>0.$$

The time between two demands (tests) is also negative exponentially distributed with parameter γ:

$$H(t) = \Pr\{\underline{t}_n<t\} = 1 - e^{-\gamma t},\ t\geq 0,\ \gamma>0,\ n=1,2,\ \ldots\ . \quad \text{(B53)}$$

The Laplace-Stieltjes transforms of F(t), W(t) and H(t) are given by $f(\rho)$, $w(\rho)$ and $z(\rho)$, respectively:

$$f(\rho) = \frac{\lambda}{\rho+\lambda} \quad , \ \mathrm{Re}(\rho) > -\lambda;$$

$$w(\rho) = \frac{\mu}{\rho+\mu} \quad , \ \mathrm{Re}(\rho) > -\mu;$$

$$z(\rho) = \frac{\gamma}{\rho+\gamma} \quad , \ \mathrm{Re}(\rho) > -\gamma. \tag{B54}$$

From (3.10), (3.13) and (3.14) it is clear that $h_0(\rho)$, $h_1(\rho)$, $a_0(\rho)$ and $a_1(\rho)$ all possess the same nominator.

$$\eta(\rho) \overset{\text{def}}{=} 1 - f(\rho)w(\rho)z(\rho), \ \mathrm{Re}(\rho) > 0. \tag{B55}$$

Substitution of $f(\rho)$, $w(\rho)$ and $z(\rho)$ in (B55) gives for $\eta(\rho)$:

$$\eta(\rho) = 1 - \frac{\lambda}{\rho+\lambda} * \frac{\mu}{\rho+\mu} * \frac{\gamma}{\rho+\gamma}$$

$$= \frac{\rho\{\rho^2 + (\lambda+\mu+\gamma)\rho + \lambda\mu + \lambda\gamma + \mu\gamma\}}{(\rho+\lambda)(\rho+\mu)(\rho+\gamma)} \quad , \ \mathrm{Re}(\rho) > 0.$$

The zero's of $\eta(\rho)$ in the above expression are given by:

$$\begin{aligned} \rho_{1,2} &= -\tfrac{1}{2}(\lambda+\mu+\rho) \pm \tfrac{1}{2}\sqrt{(\lambda+\mu+\gamma)^2 - 4(\lambda\mu+\lambda\gamma+\mu\gamma)}, \\ \rho_3 &= 0. \end{aligned} \tag{B56}$$

Define:

$$\begin{aligned} &\alpha = -\tfrac{1}{2}(\lambda+\mu+\gamma), \ \beta = \tfrac{1}{2}\sqrt{(\lambda+\mu+\gamma)^2 - 4(\lambda\mu+\lambda\gamma+\mu\gamma)}, \\ &\sigma = \tfrac{1}{2}\sqrt{4(\lambda\mu+\lambda\gamma+\mu\gamma) - (\lambda+\mu+\gamma)^2}. \end{aligned} \tag{B57}$$

There are three cases for which the zero's are different, i.e.

$$\text{case 1: } \rho_{1,2} = \alpha \pm \beta \ , \ \rho_3 = 0; \tag{B58}$$

$$\text{case 2: } \rho_{1,2} = \alpha \quad , \ \rho_3 = 0; \tag{B59}$$

$$\text{case 3: } \rho_{1,2} = \alpha \pm i\sigma, \ \rho_3 = 0. \tag{B60}$$

where $i^2 = -1$.

Because all the three cases can be treated in a similar way only case 1 is discussed here.

Case 1: $\rho_{1,2} = \alpha \pm \beta$, $\rho_3 = 0$

From (3.10) and the above mentioned it follows that:

$$h_0(\rho) = \frac{f(\rho)}{1-f(\rho)w(\rho)z(\rho)} = \frac{\lambda(\rho+\mu)(\rho+\gamma)}{\rho(\rho-\rho_1)(\rho-\rho_2)} \quad , \ \mathrm{Re}(\rho) > 0. \tag{B61}$$

$\Rightarrow$

$$m_0(t) = \alpha_1 + \alpha_2 t + \alpha_3 e^{\rho_1 t} + \alpha_4 e^{\rho_2 t}, \ t \geq 0, \tag{B62}$$

$$\left.\begin{aligned} \alpha_1 &= \frac{\lambda(\mu+\gamma)\rho_1\rho_2 + \lambda\mu\gamma(\rho_1+\rho_2)}{\rho_1^2\rho_2^2}, \ \alpha_2 = \frac{\lambda\mu\gamma}{\rho_1\rho_2}, \\ \alpha_3 &= \frac{\lambda\rho_1^2 + \lambda(\mu+\gamma)\rho_1 + \lambda\mu\gamma}{\rho_1^2(\rho_1-\rho_2)} \quad , \ \alpha_4 = \frac{\lambda\rho_2^2 + \lambda(\mu+\gamma)\rho_2 + \lambda\mu\gamma}{\rho_2^2(\rho_2-\rho_1)} \end{aligned}\right| \tag{B63}$$

For $h_1(\rho)$ we get from (3.10):

$$h_1(\rho) = \frac{f(\rho)w(\rho)z(\rho)}{1-f(\rho)w(\rho)z(\rho)} = \frac{\lambda\mu\gamma}{\rho(\rho-\rho_1)(\rho-\rho_2)} \quad , \ \mathrm{Re}(\rho) > 0. \tag{B64}$$

$\Rightarrow$

$$m_1(t) = \alpha_1 + \alpha_2 t + \alpha_3 e^{\rho_1 t} + \alpha_4 e^{\rho_2 t}, \ t \geq 0, \tag{B65}$$

$$\left.\begin{aligned} \alpha_1 &= \frac{\lambda\mu\gamma(\rho_1+\rho_2)}{\rho_1^2\rho_2^2} \quad , \ \alpha_2 = \frac{\lambda\mu\gamma}{\rho_1\rho_2}, \\ \alpha_3 &= \frac{\lambda\mu\gamma}{\rho_1^2(\rho_1-\rho_2)} \quad , \ \alpha_4 = \frac{\lambda\mu\gamma}{\rho_2^2(\rho_2-\rho_1)}. \end{aligned}\right| \tag{B66}$$

From (3.13) we get for $a_0(\rho)$:

$$a_0(\rho) = \frac{1-f(\rho)}{1-f(\rho)w(\rho)z(\rho)} = \frac{\rho^2 + (\mu+\gamma)\rho + \mu\gamma}{(\rho-\rho_1)(\rho-\rho_2)}.$$

$\Rightarrow$

$$A_0(t) = \frac{\mu\gamma}{\lambda\mu+\lambda\gamma+\mu\gamma} + \frac{(\rho_1+\mu)(\rho_1+\gamma)}{\rho_1(\rho_1-\rho_2)} e^{\rho_1 t} - \frac{(\rho_2+\mu)(\rho_2+\gamma)}{\rho_2(\rho_1-\rho_2)} e^{\rho_2 t}, \quad t\geq 0. \tag{B67}$$

From (3.14) it follows for $a_1(\rho)$ that:

$$a_1(\rho) = \frac{\{1-f(\rho)\}w(\rho)z(\rho)}{1-f(\rho)w(\rho)z(\rho)} = \frac{\mu\gamma}{(\rho-\rho_1)(\rho-\rho_2)}, \quad \mathrm{Re}(\rho) > 0.$$

$\Rightarrow$

$$A_1(t) = \frac{\mu\gamma}{\lambda\mu+\lambda\gamma+\mu\gamma} + \frac{\mu\gamma}{\rho_1(\rho_1-\rho_2)} e^{\rho_1 t} - \frac{\mu\gamma}{\rho_2(\rho_1-\rho_2)} e^{\rho_2 t}, \quad t\geq 0. \tag{B68}$$

From (B61) and the Laplace-Stieltjes transforms of W(t) and H(t) it follows that:

$$\mathrm{LS}\left\{\frac{d}{dt} m_0(t)*W(t)*H(t)\right\} = \frac{\rho\lambda(\rho+\mu)(\rho+\gamma)}{\rho(\rho-\rho_1)(\rho-\rho_2)} * \frac{\mu}{\rho+\mu} * \frac{\gamma}{\rho+\gamma}$$

$$= \frac{\lambda\mu\gamma}{(\rho-\rho_1)(\rho-\rho_2)}, \quad \mathrm{Re}(\rho) > 0. \tag{B69}$$

$\Rightarrow$

$$\frac{d}{dt} m_0(t)*H(t)*W(t) = \frac{\lambda\mu\gamma}{\rho_1\rho_2} + \frac{\lambda\mu\gamma}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 t}}{\rho_1} - \frac{e^{\rho_2 t}}{\rho_2}\right\}, \quad t\geq 0. \tag{B70}$$

From (3.36) and (B70) we get for $t\geq 0$ and $\zeta\geq 0$:

$$G_0(t,\zeta) = \left[\frac{\mu\gamma}{\rho_1\rho_2} + \frac{\lambda\mu\gamma}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 t}}{\rho_1(\rho_1+\lambda)} - \frac{e^{\rho_2 t}}{\rho_2(\rho_2+\lambda)}\right\}\right](1-e^{-\lambda\zeta}). \tag{B71}$$

From (B64) and the Laplace-Stieltjes transforms of W(t) and H(t) it follows that:

$$\mathrm{LS}\left\{\frac{d}{dt} m_1(t)*W(t)*H(t)\right\} = \frac{\lambda(\mu\gamma)^2}{(\rho-\rho_1)(\rho-\rho_2)(\rho+\mu)(\rho+\gamma)}, \quad \mathrm{Re}(\rho) > 0. \tag{B72}$$

$\Rightarrow$

$$\frac{d}{dt} m_1(t)*W(t)*H(t) = \beta_0 + \beta_1 e^{\rho_1 t} + \beta_2 e^{\rho_2 t} + \beta_3 e^{-\mu t} + \beta_4 e^{-\gamma t}, \quad t\geq 0, \tag{B73}$$

$$\left.\begin{aligned}
&\beta_0 = \frac{\lambda\mu\gamma}{\rho_1\rho_2} \quad , \quad \beta_1 = \frac{\lambda(\mu\gamma)^2}{\rho_1(\rho_1-\rho_2)(\rho_1+\mu)(\rho_1+\gamma)} \quad , \\
&\beta_2 = \frac{\lambda(\mu\gamma)^2}{\rho_2(\rho_2-\rho_1)(\rho_2+\mu)(\rho_2+\gamma)} \ , \ \beta_3 = \frac{\lambda(\mu\gamma)^2}{\mu(\rho_1+\mu)(\rho_2+\mu)(\mu-\gamma)} \ , \\
&\beta_4 = \frac{\lambda(\mu\gamma)^2}{\gamma(\rho_1+\gamma)(\rho_2+\gamma)(\gamma-\mu)} \ .
\end{aligned}\right\} \qquad (B74)$$

From (3.37), (B73) and

$$\frac{d}{dt} W(t)*H(t) = \frac{\mu\gamma}{\mu-\gamma} (e^{-\gamma t} - e^{-\mu t}),$$

we get for $t\geq 0$ and $\zeta\geq 0$:

$$G_1(t,\zeta) = \left[\frac{\mu\gamma}{\rho_1\rho_2} + \frac{\lambda(\mu\gamma)^2}{\rho_1-\rho_2}\left\{\frac{e^{\rho_1 t}}{\rho_1(\rho_1+\lambda)(\rho_1+\mu)(\rho_1+\gamma)}\right.\right.$$

$$\left.\left. - \frac{e^{\rho_2 t}}{\rho_2(\rho_2+\lambda)(\rho_2+\mu)(\rho_2+\gamma)}\right\}\right](1-e^{-\lambda\zeta}). \qquad (B75)$$

B5 Components subjected to periodical inspection

The model assumptions for components subjected to periodical inspection are described in § 3.4.3. In this section we shall derive explicit results for the availabilities $A_0(t)$ and $A_1(t)$ and the functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$ in the case of *EXSITU* inspection of a class 4 component. Its lifetime distribution is assumed to be negative exponential, i.e.

$$F(t) = 1 - e^{-\lambda t} \ , \ t\geq 0, \ \lambda>0. \qquad (B76)$$

Two different repairtime distributions are considered, viz:

(i) the repairtime is uniformly distributed, i.e.

$$\begin{aligned} W(t) &= \frac{t}{\mu} \ , \ 0\leq t\leq\mu; \\ &= 1 \ , \ t>\mu \ ; \end{aligned} \qquad (B77)$$

(ii) the repairtime is a constant, i.e.

$$\begin{aligned} W(t) &= 0 \ , \ 0\leq t\leq\mu; \\ &= 1 \ , \ t>\mu \ . \end{aligned} \qquad (B78)$$

Periodical inspection means (cf. § 3.4.3): equidistant test moments, equal inspection times and equal maximal repairtimes. We recall here the different parameters that describe such a process:

η_1 : time to the first inspection;
η : time between two successive inspections;
θ : time needed to inspect the component.

For the process of the periodical inspection the time interval $[0,\eta_1]$ till the first inspection is a special interval. The availabilities $A_0(t)$ and $A_1(t)$ during $[0,\eta_1]$ are given by:

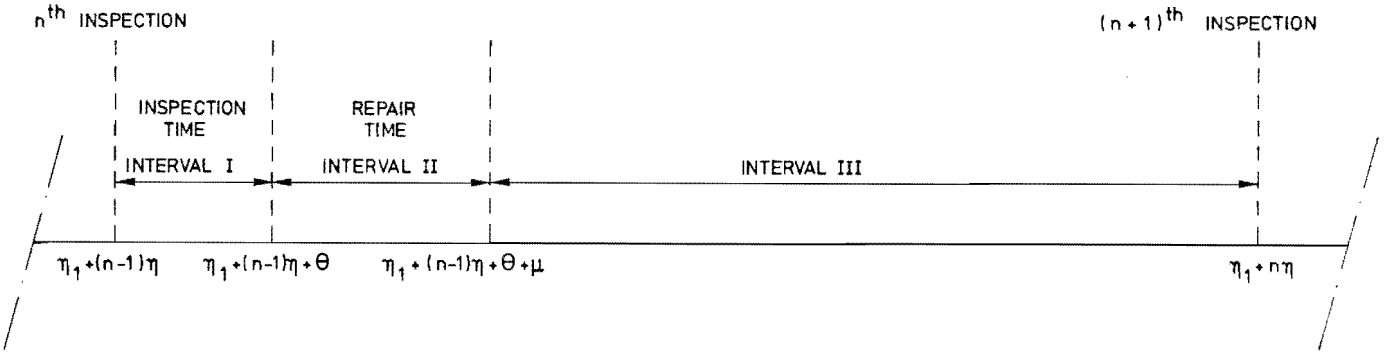
$$\begin{aligned} A_0(t) &= 1 - F(t) = e^{-\lambda t}, \quad 0 \le t \le \eta_1; \\ A_1(t) &= 0 \qquad\qquad\quad , \quad 0 \le t \le \eta_1. \end{aligned} \tag{B79}$$

Each of the other intervals between two successive inspections contain three different intervals with respect to the calculation procedure of the availabilities. These three different intervals for the n^{th} inspection interval (i.e. the inspection interval that starts at the instant at which the n^{th} inspection is performed) are (see fig. below) for n=1,2,... :

interval I (the inspection interval):
$[\eta_1+(n-1)\eta,\ \eta_1+(n-1)\eta+\theta]$;

interval II (the repair interval):
$[\eta_1+(n-1)\eta+\theta,\ \eta_1+(n-1)\eta+\theta+\mu]$,
μ being the maximal length of the repairtime;

interval III (the interval where no inspection nor repair is applied to the component):
$[\eta_1+(n-1)\eta+\theta+r,\ \eta_1+n\eta]$.



Below explicit formulas shall be derived for the availability of the component in each of the intervals I, II and III.

B5.1 Negative exponential lifetime distribution and a uniform distributed repairtime

B5.1.1. The availability in the case of the timedependent process

In this section the lifetime distribution of the component is defined by (B76) and its repairtime distribution by (B77).

(a1) Interval I: $[\eta_1+(n-1)\eta, \eta_1+(n-1)\eta+\theta]$

Because the component is EXSITU inspected the availabilities $A_0(t)$ and $A_1(t)$ during this interval are by definition given by:

$$A_0(t) = 0; \qquad A_1(t) = 0. \tag{B80}$$

(a2) Interval II: $[\eta_1+(n-1)\eta+\theta, \eta_1+(n-1)\eta+\theta+\mu]$

Substitution of (B76) and (B77) into (3.20) and (3.26) gives for the availabilities $A_0(t)$ and $A_1(t)$:

$$A_0(t) = e^{-\lambda t}\Big[1+c_1 \sum_{k=1}^{n-1}\{1-A_0(\eta_1+(k-1)\eta+\theta)\}e^{\lambda(\eta_1+(k-1)\eta+\theta)}\Big] + c_0\{1-A_0(\eta_1+(n-1)\eta+\theta)\}\{1-e^{-\lambda(t-\eta_1-(n-1)\eta-\theta)}\}; \tag{B81}$$

$$A_1(t) = c_1 e^{-\lambda t} \sum_{k=1}^{n-1}\{1-A_1(\eta_1+(k-1)\eta+\theta)\}e^{\lambda(\eta_1+(k-1)\eta+\theta)} + c_0\{1-A_1(\eta_1+(n-1)\eta+\theta)\}\{1-e^{-\lambda(t-\eta_1-(n-1)\eta-\theta)}\}, \tag{B82}$$

with c_0 and c_1 in (B81) as well as in (B82) being defined by

$$c_0 = \frac{1}{\lambda\mu} \quad , \quad c_1 = c_0(e^{\lambda\mu}-1). \tag{B83}$$

(B81) and (B82) are implicit expressions for the availabilities $A_0(t)$ and $A_1(t)$, respectively. To get the explicit solution we shall determine first the explicit expression for $A_0(t)$ in the case that t is the starting instant of the repair interval, i.e. $t=\eta_1+n\eta+\theta$. So define

$$t = \eta_1+n\eta+\theta; \text{ and} \tag{B84}$$

$$a_n = A_0(\eta_1+(n-1)\eta+\theta)e^{\lambda(\eta_1+(n-1)\eta+\theta)}, \quad n=1,2,\ldots . \tag{B85}$$

Substitution of (B84) and (B85) into (B81) gives:

$$a_{n+1} = 1+c_1\left\{\sum_{k=1}^{n} e^{\lambda(\eta_1+(k-1)\eta+\theta)} - \sum_{k=1}^{n} a_k\right\}$$

$$= 1+c_1\left\{f_n - \sum_{k=1}^{n} a_k\right\}, \quad n=1,2,\ldots , \tag{B86}$$

c_1 being defined by (B83) and f_n given by

$$f_n = e^{\lambda(\eta_1+\theta)} \frac{(1-e^{\lambda n\eta})}{1-e^{\lambda\eta}} . \tag{B87}$$

From (B86) it follows that:

$$a_{n+1} - a_n = c_1(f_n-f_{n-1}) - c_1a_n$$

$\Rightarrow$

$$a_{n+1} = c_1(f_n-f_{n-1}) + (1-c_1)a_n, \quad n=1,2,\ldots . \tag{B88}$$

From (B85) it is obvious that for n=1 we get

$$a_1 = A_0(\eta_1+\theta)e^{\lambda(\eta_1+\theta)} = e^{-\lambda(\eta_1+\theta)}e^{\lambda(\eta_1+\theta)}$$

$$= 1. \tag{B89}$$

The solution of the recursive relation (B88) with initial condition (B89) reads:

$$a_n = (1-c_1)^{n-1} + c_1 \sum_{k=1}^{n-1} (f_k - f_{k-1})(1-c_1)^{n-1-k}, \quad n=1,2,\ldots . \tag{B90}$$

Substitution of f_k (see (B87)) into (B90) gives:

$$a_n = (1-c_1)^{n-1} + c_1 e^{\lambda(\eta_1+\theta)} \frac{\{(1-c_1)^{n-1} - e^{\lambda(n-1)\eta}\}}{1-c_1-e^{\lambda\eta}}, \quad n=1,2,\ldots . \tag{B91}$$

From (B81), (B87) and (B91) we get for the availability $A_0(t)$:

$$\begin{aligned} A_0(t) = {} & e^{\lambda t}\{1+c_1(f_{n-1}-g_{n-1})\} \\ & + c_0\{1-a_n e^{-\lambda(\eta_1+(n-1)\eta+\theta)}\}\{1-e^{-\lambda(t-\eta_1-(n-1)\eta-\theta)}\}, \end{aligned} \tag{B92}$$

with c_0 and c_1 being defined by (B83), a_n by (B91) and g_n given by:

$$g_n = \sum_{k=1}^{n} a_k = \frac{1-(1-c_1)^n}{c_1} + \frac{c_1 e^{\lambda(\eta_1+\theta)}}{1-c_1-e^{\lambda\eta}} \left\{ \frac{1-(1-c_1)^n}{c_1} - \frac{1-e^{\lambda n\eta}}{1-e^{\lambda\eta}} \right\}, \quad n=1,2,\ldots . \tag{B93}$$

Using the same solution method we get for $A_1(t)$:

$$\begin{aligned} A_1(t) = {} & c_1 e^{-\lambda t}\{f_{n-1}-h_{n-1}\} \\ & + c_0\{1-b_n e^{-\lambda(\eta_1+(n-1)\eta+\theta)}\}\{1-e^{-\lambda(t-\eta_1-(n-1)\eta-\theta)}\}, \end{aligned} \tag{B94}$$

c_0 and c_1 being defined by (B83) and b_n and h_n being given by:

$$b_n = a_n - (1-c_1)^{n-1} ; \tag{B95}$$

$$h_n = g_n - \frac{1-(1-c_1)^n}{c_1}, \tag{B96}$$

with a_n and g_n being defined by (B91) and (B92), respectively.

(a3) Interval III: $[\eta_1+(n-1)\eta+\theta+\mu,\ \eta_1+n\eta]$

By the same method as used for the calculation of $A_0(t)$ and $A_1(t)$ for interval II we get for the availabilities in interval III:

$$A_0(t) = e^{-\lambda t}\{1 + c_1(f_n-g_n)\}, \tag{B97}$$

c_1, f_n and g_n being defined by (B83), (B87) and (B93), respectively.

$$A_1(t) = c_1 e^{-\lambda t}(f_n-h_n), \tag{B98}$$

c_1, f_n and h_n being defined by (B83), (B87) and (B96), respectively.

B5.1.2 The availability in the case of the stationary process

The availabilities $A_0(t)$ and $A_1(t)$ tend to a stationary behaviour after a large number of inspections, i.e. there exists nearly a difference between the values $A_0(t)$ and $A_0(t+\eta)$ for $t\to\infty$. In order to obtain this stationary behaviour, define

$$A(\tau) = \lim_{n\to\infty} A_0(\eta_1+(n-1)\eta+\tau),\ 0\le\tau\le\eta. \tag{B99}$$

Note that instead of $A_0(\eta_1+(n-1)\eta+\tau)$ we can also take $A_1(\eta_1+(n-1)\eta+\tau)$. Calculating $A_0(\eta_1+(n-1)\eta+\tau)$ for (B92) and (B97) and taking the limit for $n\to\infty$ we get for the different intervals:

Interval I : $A(\tau) = 0,\ 0\le\tau\le\theta$ (by definition); (B100)

Interval II : $$A(\tau) = \frac{1-v_1 e^{-\lambda(\tau-\theta)}}{\lambda\mu+1-v_1},\ \theta\le\tau\le\theta+\mu, \tag{B101}$$

with

$$v_1 = \frac{1-e^{-\lambda(\eta-\mu)}}{1-e^{-\lambda\eta}}; \tag{B102}$$

Interval III: $$A(\tau) = v_2 e^{-\lambda(\tau-\theta-\mu)},\ \theta+\mu\le\tau\le\eta, \tag{B103}$$

with

$$v_2 = \frac{1-e^{-\lambda\mu}}{\lambda\mu(1-e^{-\lambda\eta}) + (e^{-\lambda\mu}-1)e^{-\lambda\eta}}. \tag{B104}$$

B5.2 Negative exponential lifetime distribution and a constant repairtime

In this section the lifetime distribution of the component is given by (B76) and its repairtime distribution by (B78).
We shall summarize the results for the time dependent process as well as for the stationary situation because the derivation of the concerned availabilities is done by the same method as for the case of the uniformly distributed repairtime.

B5.2.1. The availability in the case of the time dependent process

(b1) The interval I: $[\eta_1+(n-1)\eta, \eta_1+(n-1)\eta+\theta]$

$$A_0(t) = 0;$$

$$A_1(t) = 0. \tag{B105}$$

(b2) The interval II: $[\eta_1+(n-1)\eta+\theta, \eta_1+(n-1)\eta+\theta+\mu]$

$$A_0(t) = e^{-\lambda t}\{1+c_3(f_{n-1}-g_{n-1})\}, \tag{B106}$$

with f_{n-1} and g_{n-1} as given by (B87) and (B93), respectively, with c_1 replaced by c_3; c_3 is defined by

$$c_3 = e^{\lambda\mu}. \tag{B107}$$

$$A_1(t) = c_3 e^{-\lambda t}(f_{n-1}-h_{n-1}), \tag{B108}$$

c_3 being defined by (B107) and f_{n-1} and h_{n-1} as given by (B87) and (B96) with c_1 replaced by c_3.

(b3) The interval III: $[\eta_1+(n-1)\eta+\theta+\mu, \eta_1+n\eta]$

$$A_0(t) = e^{-\lambda t}\{1+c_3(f_n-g_n)\}, \tag{B109}$$

$$A_1(t) = c_3 e^{-\lambda t}(f_n-h_n), \tag{B110}$$

c_3 in (B109) and (B110) being defined by (B107); f_n, g_n and h_n are given by (B87), (B93) and (B96) with c_1 replaced by c_3.

B5.2.2 The availability in the case of the stationary process

For the definition of $A(\tau)$, see (B99).

Interval I : $A(\tau) = 0$, $0 \leq \tau \leq \theta$ (by definition) (B111)

Interval II : $A(\tau) = w_1 e^{-\lambda(\tau-\theta)}$, $\theta \leq \tau \leq \theta+\mu$, (B112)

with

$$w_1 = \frac{1}{1+(e^{\lambda\eta}-1)e^{-\lambda\mu}} \tag{B113}$$

Interval III: $A(\tau) = w_2 e^{-\lambda(t-\theta-\mu)}$, (B114)

with

$$w_2 = \frac{1}{1+(e^{\lambda\mu}-1)e^{-\lambda\eta}} . \tag{B115}$$

B5.3 The functions $G_0(t,\zeta)$ and $G_1(t,\zeta)$

Because the lifetime distribution is negative exponential it is easy understood that for $t \geq 0$ and $\zeta \geq 0$:

$$G_0(t,\zeta) = A_0(t)(1-e^{-\lambda\zeta}); \tag{B116}$$

$$G_1(t,\zeta) = A_1(t)(1-e^{-\lambda\zeta}). \tag{B117}$$

APPENDIX C

A PHASED MISSION CALCULATION PERFORMED BY PHAMISS FOR THE ECCS OF A BWR AS DESCRIBED IN CHAPTER 6

C1 Description of the input deck and the output

This appendix shows an input deck for PHAMISS and the associated output as it is given by the computer program.
The example is taken from § 6.4. i.e. a phased mission for the Emergency Core Cooling System (ECCS) of a Boiling Water Reactor (BWR). The mission that is chosen is that one where every subsystem has to survive its phase.

The input deck

The input deck is shown in section C2. It consists of the following "INPUT UNITS":

(i) an "INITIAL INPUT UNIT"; followed by
(ii) three "FAULTTREE INPUT UNITS", viz.
"FAULTTREE INPUT UNIT 1"
"FAULTTREE INPUT UNIT 2", and
"FAULTTREE INPUT UNIT 3"; and closed by
(iii) a "PROBCAL INPUT UNIT".

(i) The "INITIAL INPUT UNIT"

The "INITIAL INPUT UNIT" starts with the *problem title* card, followed by the *TREES* card. The *TREES* card indicates the number of "FAULTTREE INPUT UNITS" that are present in the PHAMISS input deck (in the present example this number is 3).
The next two program control cards indicate that the program sections FAULTTREE (minimal cut set calculation) and PROBCAL (probability calculations) are needed.
The "INITIAL INPUT UNIT" is closed by the *GOON* card.

(ii) The "FAULTTREE INPUT UNITS"

After the "INITIAL INPUT UNIT" the three "FAULTTREE INPUT UNITS" are inserted to the PHAMISS input deck. Each of them consists of a "PROGRAM CONTROL SECTION" and a "DATA INPUT SECTION".

The "PROGRAM CONTROL SECTION"

Each "PROGRAM CONTROL SECTION" starts with the "FAULTTREE INPUT UNIT HEADER NAME" *FAULTTREE* and contains the following program control cards:

(a) the *HEADING* card for a special unit title which description is given on the next card. For instance, each output page for "FAULTTREE INPUT UNIT 1" starts with the title "initial core cooling - phase 1";

(b) the *PFNAME* card that defines the "SAVE-file" for that particular input unit, e.g. the "SAVE-file" for the "FAULTTREE INPUT UNIT 1" has the PF-name "BWRMCS1" with "ID=N3KT";

(c) the *SPLITUP* card which means that the minimal cut sets are presented in *basic events*;

(d) the *PRINT* card in order to print the minimal cut sets (default they are not printed).

Each of these "PROGRAM CONTROL SECTIONS" is closed by the *GOON* card.

The "DATA INPUT SECTION"

The "DATA INPUT SECTION" of "FAULTTREE INPUT UNIT 1" consists of two parts, viz.

- a "COMPONENT INPUT PART"; followed by
- a "TREE INPUT PART".

The other two "FAULTTREE INPUT UNITS" only possess a "TREE INPUT PART". This because the "COMPONENT INPUT PART" of the first "FAULTTREE INPUT UNIT" must contain all components which are present in the union of the three subsystems.
The "COMPONENT INPUT PART" starts with the keyname *COMPONENTS* and is closed by the "END" card. It contains "COMPONENT NAME CARDS". For a description of such a card we take as an example the first "COMPONENT NAME CARD" that is present in the "COMPONENT INPUT PART" of "FAULTTREE INPUT UNIT 1". The parameters on the card are (in sequence):

- the name of the component (HPCS);
- the component's class (1, i.e. non-repairable);
- its lifetime distribution (0, i.e. negative exponential);
- its repairtime distribution (0, i.e. negative exponential);
- its failure rate ($2.7 * 10^{-4}$/hr);
- its mean repairtime (2.5 hrs). In the case of a class 1 component this repairtime is neglected by PHAMISS;
- the number of omitted parameters (0(5)). This last parameter is necessary because the input is *free-formatted*.

Each "TREE INPUT PART" starts with the keyname *GATES* and is closed by the "END" card. Each *tree card* contained in it describes a gate of the faulttree. Such a tree card starts with the name of the considered gate followed by its type (AND or OR) and its predecessors (inputs).

(iii) The "PROBCAL INPUT UNIT"

The "PROBCAL INPUT UNIT" consists of a "PROGRAM CONTROL SECTION" followed by a "DATA INPUT SECTION".

The "PROGRAM CONTROL SECTION"

The "PROGRAM CONTROL SECTION" starts with the "PROBCAL INPUT UNIT HEADER NAME" *PROBCAL*, is closed by the *GOON* card and contains the following program control cards:

(a) the *PHASED MISSION* card which means that the system unreliability during the phased mission is not only calculate for each phase at the terminating instant of that phase but also at the starting instant, i.e. at the instants T_0 and T_1 for phase 1, T_1 and T_2 for phase 2 and T_2 and T_3 for phase 3, respectively.

(b) the *PFNAME* cards for each of the three phases. Because a PROBCAL calculation always starts from the "SAVE-file(s)", the identification of the concerned "SAVE-file(s)" has to be present in the "PROGRAM CONTROL SECTION" of PROBCAL. In the case of a phased mission calculation the sequence of the "SAVE-files" has to be the appropriate sequence of the concerned phases.

Therefore, in our example, the first "SAVE-file" has to be "BWRMCS1" (for phase 1), the second one "BWRMCS2" (for phase 2) and the third one "BWRMCS3" (for phase 3).

(c) the *ERROR* card that indicates that an error calculation is performed . (See for the definition of the error in the probability of mission failure (success) table 6.14 of chapter 6).

The "DATA INPUT SECTION"

For this example the "DATA INPUT SECTION" of the "PROBCAL INPUT UNIT" consists of only one "INPUT PART", namely the "MISSION INPUT PART".
The "MISSION INPUT PART" starts with the keyname *MISSION* and is closed by the "END" card. Furthermore it contains two data cards. The values on the *first* data card determine the time schedule of the mission, i.e. the start of the "OR-phase" (at t=0), the start of the mission (at t=0), the start of the second phase (at t=0.5), the start of the third phase (at t=36.5) and the end of the mission (at t=120.5).
The numbers on the *second* data card express the task of each subsystem during its appropriate phase. In the present example all subsystems have to survive their respective phases, i.e. $u_1=1$, $u_2=1$ and $u_3=1$ (see § 2.4. for the definition of a phased mission).

The output

The output of PHAMISS is self explaining. However, we shall make some remarks concerning the present example.

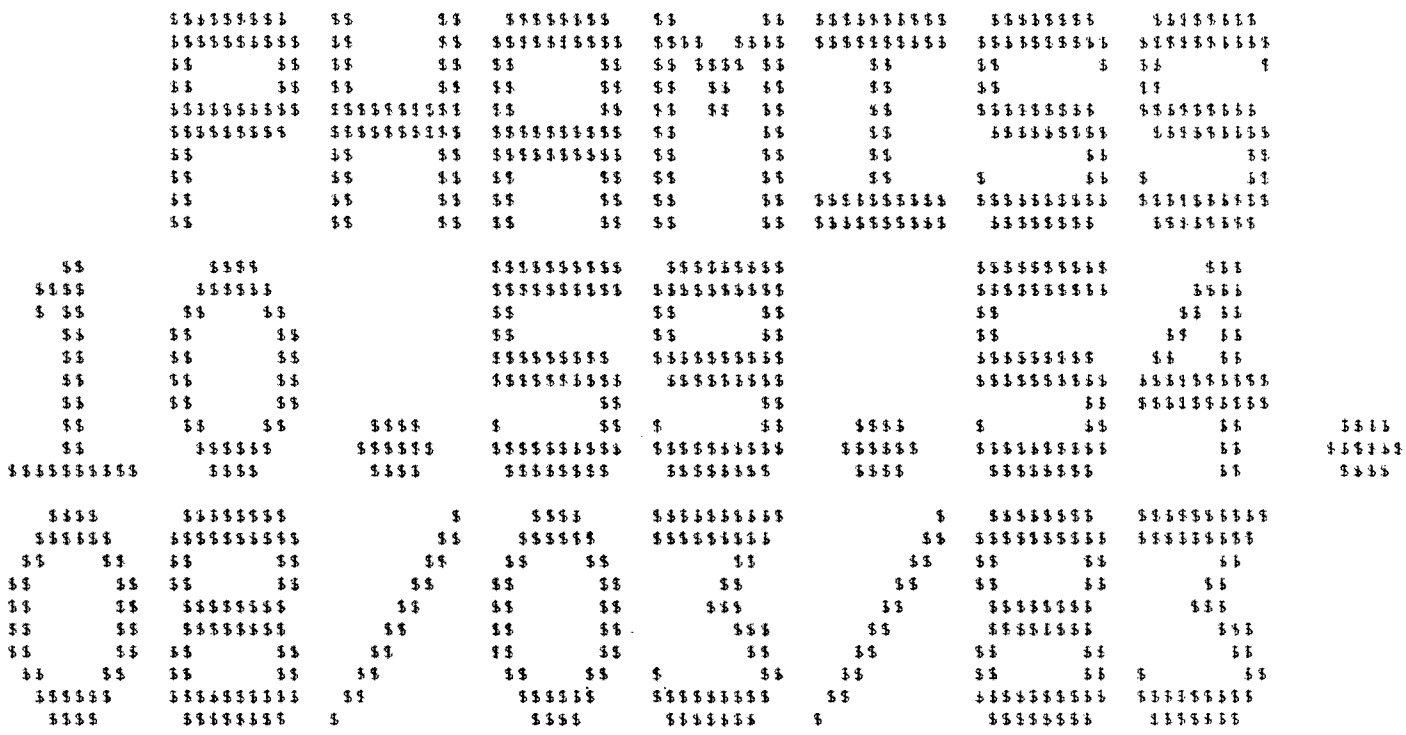
(1) For each program control card present in the PHAMISS input deck a message is printed in the output. This facilitates the user in checking his calculations.

(2) In the case that the failure probability of the phased mission where every subsystem has to survive its phase (indicated by $u_1=u_2=u_3=1$) is calculated, the probability of mission success for a number of other phased missions is easily calculated too (see § 6.3.6. (iii)). The probabilities of mission success for these phased missions are presented in the table with the heading "OTHER MISSIONS" in the PROBCAL output section.

(3) The last table of the PROBCAL output section shows the time dependent behaviour of the system during the phased mission where every subsystem has to survive its phase. The heading of this table is "-PHASED MISSION-".

C2 The input deck for PHAMISS

```
*PHASED MISSION EXAMPLE  (BWR - 1977)*
*TREES*  3
*PROGRAM*  *FAULTTREE*  *CUTS*
*PROGRAM*  *PROBCAL*
*GOON*
*FAULTTREE*
*HEADING*
 PHASE 1 - INITIAL CORE COOLING
*PFNAME*  *BWRMCS1*  *N3KT*
*SPLITUP*
*PRINT*
*GOON*
*COMPONENTS*
 HPCS   1  0  0  0.  2.7E-04  2.5  0(5)
 ADS    1  0  0  0.  1.4E-05  1.0  0(5)
 LPCIC  1  0  0  0.  2.5E-05  2.5  0(5)
 LPCIA  1  0  0  0.  2.5E-05  2.5  0(5)
 LPCIB  1  0  0  0.  2.5E-05  2.5  0(5)
 LPCS   1  0  0  0.  2.6E-06  3.0  0(5)
 HX-A   1  0  0  0.  2.8E-06  24.  0(5)
 HX-B   1  0  0  0.  2.8E-06  24.  0(5)
 END
*GATES*
 G1     AND,HPCS,G2
 G2     OR,ADS,G3
 G3     AND,LPCIA,LPCIB,LPCIC,LPCS
 END
*FAULTTREE*
*HEADING*
 PHASE 2 - SUPPRESSION POOL COOLING
*PFNAME*  *BWRMCS2*  *N3KT*
*SPLITUP*
*PRINT*
*GOON*
*GATES*
 G1     OR,ADS,G2
 G2     AND,G3,G4
 G3     OR,HX-A,LPCIA,G5
 G5     AND,LPCIB,LPCIC,HPCS,LPCS
 G4     OR,HX-B,LPCIB,G6
 G6     AND,LPCIA,LPCIC,HPCS,LPCS
 END
*FAULTTREE*
*HEADING*
 PHASE 3 - RESIDUAL HEAT REMOVAL
*PFNAME*  *BWRMCS3*  *N3KT*
*SPLITUP*
*PRINT*
*GOON*
*GATES*
 G1     AND,G2,G3
 G2     OR,HX-A,LPCIA
 G3     OR,HX-B,LPCIB
 END
*PROBCAL*
*PHASED MISSION*
*PFNAME*  *BWRMCS1*  *N3KT*
*PFNAME*  *BWRMCS2*  *N3KT*
*PFNAME*  *BWRMCS3*  *N3KT*
*ERROR*
*GOON*
*MISSION*
 0.  0.  0.5  36.5  120.5
 1  1  1
 END
```



```
+++++++++++ NOTES ++++++++++++++++++++++++++++++++++++++++
+          =======                                        +
+    IN CASE OF DIFFICULTIES PLEASE CONTACT               +
+    N.H.DEKKER - ENERGIE ONDERZOEK CENTRUM NEDERLAND     +
+                                                         +
+    MIN.FIELDLENGTH ON JOBCARD : 150000 OCTAL.           +
+                                                         +
+    TO GET INFORMATION ABOUT THE INPUT, JUST RUN         +
+    THE PROGRAM WITH ONLY THE CARD :                     +
+    *INPUT*                                              +
+    IN THE INPUT RECORD.                                 +
+                                                         +
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

****
PHASED MISSION EXAMPLE (BWR - 1977)
****

PHASE 1 - INITIAL CORE COOLING

PROGRAM : FAULTTREE CUTS ORDER : ALL

SAVE-FILE WILL BE DEVELOPED.

PF-NAME
****
SAVEFILE 1 : BWRMCS1 ID = N3KT

EXTRA OUTPUT PRINTED.

PHASED MISSION EXAMPLE (BWR - 1977)

COMPONENTS
****

NR.	COMPO. NAME	TYPE	LIFE TIME DISTR.	REP. TIME DISTR.	INIT.UNAV./ CONST.UNAV.	FAILURE RATE.	MEAN REP.TIME	FIRST TEST INTERVAL	NEXT TEST INTERVAL	TESTING TIME	MAINTE NANCE CYCLE	MAINTE NANCE TIME
1	HPCS	1	0	0	0.	2.700E-04	2.500E+00	0.	0.	0.	0	0.
2	ADS	1	0	0	0.	1.400E-05	1.000E+00	0.	0.	0.	0	0.
3	LPCIC	1	0	0	0.	2.500E-05	2.500E+00	0.	0.	0.	0	0.
4	LPCIA	1	0	0	0.	2.500E-05	2.500E+00	0.	0.	0.	0	0.
5	LPCIB	1	0	0	0.	2.500E-05	2.500E+00	0.	0.	0.	0	0.
6	LPCS	1	0	0	0.	2.600E-06	3.000E+00	0.	0.	0.	0	0.
7	HX-A	1	0	0	0.	2.800E-06	2.400E+01	0.	0.	0.	0	0.
8	HX-B	1	0	0	0.	2.800E-06	2.400E+01	0.	0.	0.	0	0.

GATES
****

GATE	TYPE	PREDECESSORS.			
G1	AND	HPCS	G2		
G2	OR	ADS	G3		
G3	AND	LPCIA	LPCIB	LPCIC	LPCS

NR.	GATE NAME	TYPE	PREDECESSORS
1	G3	AND	-LPCIC -LPCIA -LPCIB - LPCS
2	G2	OR	- ADS + G3
4	G1	AND	+@0001
3	@0001	AND	- HPCS + G2

NUMBER OF COMPONENTS : 8
NUMBER OF GATES : 4
NUMBER OF SUPEREVENTS: 3
INDEPENDENT BRANCHES : 0
MAX.ORDER OF TOPEVENT: 5
TOP EVENT : G1

GATES MARKED WITH * ARE SUPER EVENTS WITH MORE THEN ONE PATH TO THE TOP.
GATES MARKED WITH + ARE SUPER EVENTS WITH" ONE PATH TO THE TOP.
COMPONENTS MARKED WITH - ARE COMPONENTS WITH ONE PATH TO THE TOP.
GATE-NAMES STARTING WITH @ OR @@ ARE INSERTED BY THE PROGRAM
GATE-NAMES STARTING WITH ONE @ ARE JOINT EVENTS. (JE)
GATE-NAMES STARTING WITH @@ ARE LOGICAL COMBINED EVENTS. (LCE)

MAX.NUMBER OF CUTSETS : 2

PHASE 1 - INITIAL CORE COOLING

END INPUT .449(CP.SEC) TOT.CP.TIME : .449(SEC)
.239(IO.SEC) TOT.IO.TIME : .239(SEC)

NUMBER OF MIN.CUTSETS(WITH LOG.COMB.EVENTS.): 1

END MIN.CUTSETS .011(CP.SEC) TOT.CP.TIME : .460(SEC)
.028(IO.SEC) TOT.IO.TIME : .267(SEC)

INFORMATION SAVED. PF=BWRMCS1 ID=N3KT

PHASE 1 - INITIAL CORE COOLING

NR.	ORDER	CUTSET
1	2	ADS HPCS
2	5	LPCS LPCIB LPCIA LPCIC HPCS

NUMBER OF MIN.CUTSETS OF ORDER	1	0
NUMBER OF MIN.CUTSETS OF ORDER	2	1
NUMBER OF MIN.CUTSETS OF ORDER	3	0
NUMBER OF MIN.CUTSETS OF ORDER	4	0
NUMBER OF MIN.CUTSETS OF ORDER	5	1
TOT.NUMBER OF MIN.CUTSETS		2

END OUTPUT CUTSETS. .092(CP.SEC) TOT.CP.TIME : .552(SEC)
1.476(IO.SEC) TOT.IO.TIME : 1.743(SEC)

PHASE 2 - SUPPRESSION POOL COOLING

```
PROGRAM        :   FAULTTREE     CUTS      ORDER : ALL

SAVE-FILE WILL BE DEVELOPED.

PF-NAME
*******
SAVEFILE  1    :  BWRMCS1     ID = N3KT
SAVEFILE  2    :  BWRMCS2     ID = N3KT

EXTRA OUTPUT PRINTED.
```

PHASED MISSION EXAMPLE (BWR - 1977)

GATES
****

GATE	TYPE	PREDECESSORS.			
G1	OR	ADS	G2		
G2	AND	G3	G4		
G3	OR	HX-A	LPCIA	G5	
G5	AND	LPCIB	LPCIC	HPCS	LPCS
G4	OR	HX-B	LPCIB	G6	
G6	AND	LPCIA	LPCIC	HPCS	LPCS

INDEPENDENT GATES
****

G2 ,

NR.	GATE NAME	TYPE	PREDECESSORS			
2	G2	AND	G4	G3		
3	G1	OR	- ADS	G2		
4	G4	OR	LPCIB	- HX-B	G6	
5	G3	OR	LPCIA	- HX-A	G5	
6	G6	AND	LPCIA	@@001		
7	G5	AND	LPCIB	@@001		
1	@@001	AND	HPCS	LPCIC	LPCS	

NUMBER OF COMPONENTS : 8
NUMBER OF GATES : 7
NUMBER OF SUPEREVENTS: 1
INDEPENDENT BRANCHES : 1
MAX.ORDER OF TOPEVENT: 8
TOP EVENT : G1

GATES MARKED WITH * ARE SUPER EVENTS WITH MORE THEN ONE PATH TO THE TOP.
GATES MARKED WITH + ARE SUPER EVENTS WITH" ONE PATH TO THE TOP.
COMPONENTS MARKED WITH - ARE COMPONENTS WITH ONE PATH TO THE TOP.
GATE-NAMES STARTING WITH @ OR @@ ARE INSERTED BY THE PROGRAM
GATE-NAMES STARTING WITH ONE @ ARE JOINT EVENTS. (JE)
GATE-NAMES STARTING WITH @@ APE LOGICAL COMBINED EVENTS. (LCE) .

MAX.NUMBER OF CUTSETS : 10

PHASE 2 - SUPPRESSION POOL COOLING

END INPUT .223(CP.SEC) TOT.CP.TIME : .775(SEC)
.157(IO.SEC) TOT.IO.TIME : 1.900(SEC)

NUMBER OF MIN.CUTSETS(WITH LOG.COMB.EVENTS.): 7

END MIN.CUTSETS .008(CP.SEC) TOT.CP.TIME : .783(SEC)
.027(IO.SEC) TOT.IO.TIME : 1.927(SEC)

INFORMATION SAVED. PF=BWRMCS2 ID=N3KT

PHASE 2 - SUPPRESSION POOL COOLING

NR.	ORDER	CUTSET			
1	1	ADS			
2	2	LPCIB	LPCIA		
3	2	HX-A	LPCIB		
4	2	HX-B	LPCIA		
5	2	HX-B	HX-A		
6	4	LPCS	LPCIB	LPCIC	HPCS
7	4	LPCS	LPCIA	LPCIC	HPCS

NUMBER OF MIN.CUTSETS OF ORDER 1	1
NUMBER OF MIN.CUTSETS OF ORDER 2	4
NUMBER OF MIN.CUTSETS OF ORDER 3	0
NUMBER OF MIN.CUTSETS OF ORDER 4	2
NUMBER OF MIN.CUTSETS OF ORDER 5	0
NUMBER OF MIN.CUTSETS OF ORDER 6	0
NUMBER OF MIN.CUTSETS OF ORDER 7	0
NUMBER OF MIN.CUTSETS OF ORDER 8	0
TOT.NUMBER OF MIN.CUTSETS	7

END OUTPUT CUTSETS. .096(CP.SEC) TOT.CP.TIME : .879(SEC)
.310(IO.SEC) TOT.IO.TIME : 2.237(SEC)

PHASE 3 - RESIDUAL HEAT REMOVAL

PROGRAM : FAULTTREE CUTS ORDER : ALL

SAVE-FILE WILL BE DEVELOPED.

PF-NAME
****
SAVEFILE 1 : BWRMCS1 ID = N3KT
SAVEFILE 2 : BWRMCS2 ID = N3KT
SAVEFILE 3 : BWRMCS3 ID = N3KT

EXTRA OUTPUT PRINTED.

PHASED MISSION EXAMPLE (BWR - 1977)

GATES
****

GATE	TYPE	PREDECESSORS.	
G1	AND	G2	G3
G2	OR	HX-A	LPCIA
G3	OR	HX-B	LPCIB

NR.	GATE NAME	TYPE	PREDECESSORS
1	G3	OR	-LPCIB - HX-B
2	G2	OR	-LPCIA - HX-A
4	G1	.AND	+@0001
3	@0001	AND	+ G3 + G2

NUMBER OF COMPONENTS : 8
NUMBER OF GATES : 4
NUMBER OF SUPEREVENTS: 3
INDEPENDENT BRANCHES : 0
MAX.ORDER OF TOPEVENT: 2
TOP EVENT : G1

GATES MARKED WITH * ARE SUPER EVENTS WITH MORE THEN ONE PATH TO THE TOP.
GATES MARKED WITH + ARE SUPER EVENTS WITH" ONE PATH TO THE TOP.
COMPONENTS MARKED WITH - ARE COMPONENTS WITH ONE PATH TO THE TOP.
GATE-NAMES STARTING WITH @ OR @@ ARE INSERTED BY THE PROGRAM
GATE-NAMES STARTING WITH ONE @ ARE JOINT EVENTS. (JE)
GATE-NAMES STARTING WITH @@ APE LOGICAL COMBINED EVENTS. (LCE)

MAX.NUMBER OF CUTSETS : 4

END INPUT .192(CP.SEC) TOT.CP.TIME : 1.071(SEC)
.159(IO.SEC) TOT.IO.TIME : 2.396(SEC)

NUMBER OF MIN.CUTSETS(WITH LOG.COMB.EVENTS.): 1

PHASE 3 - RESIDUAL HEAT REMOVAL

END MIN.CUTSETS .019(CP.SEC) TOT.CP.TIME : 1.090(SEC)
.028(IO.SEC) TOT.IO.TIME : 2.424(SEC)

INFORMATION SAVED. PF=BWRMCS3 ID=N3KT

PHASE 3 - RESIDUAL HEAT REMOVAL

NR.	ORDER	CUTSET	
1	2	HX-B	HX-A
2	2	HX-B	LPCIA
3	2	HX-A	LPCIB
4	2	LPCIB	LPCIA

NUMBER OF MIN.CUTSETS OF ORDER 1 0
NUMBER OF MIN.CUTSETS OF ORDER 2 4

TOT.NUMBER OF MIN.CUTSETS 4

END OUTPUT CUTSETS. .103(CP.SEC) TOT.CP.TIME : 1.193(SEC)
.171(IO.SEC) TOT.IO.TIME : 2.595(SEC)

PHASE 3 - RESIDUAL HEAT REMOVAL

PROGRAM : PROBCAL

PF-NAME
****
SAVEFILE 1 : BWRMCS1 ID = N3KT
SAVEFILE 2 : BWRMCS2 ID = N3KT
SAVEFILE 3 : BWRMCS3 ID = N3KT

MISSION
****
EPROR CALCULATION PERFORMED.
ALL PHASES WILL BE CALCULATED.
RARE EVENT APPROXIMATION APPLIED.

***** CALCULATIONS BASED ON MIN.CUTSETS UP TO ORDER : ALL. *****

TIME POINTS

T(0)	T(BEGIN)	T(END-PHASE(J))		
0.000	0.000	.500	36.500	120.500

END INPUT PROBCAL .093(CP.SEC) TOT.CP.TIME : 1.286(SEC)
.090(IO.SEC) TOT.IO.TIME : 2.685(SEC)

SCANNED TAPES WILL BE SAVED TEMPORARILY

PHASED MISSION EXAMPLE (BWR - 1977)

PHASE	SAVE FILE	TASK SYSTEM
PHASE 1	BWRMCS1	1
PHASE 2	BWRMCS2	1
PHASE 3	BWRMCS3	1

REMARK : PHASE(J) - TASK(J) = 0 , SYSTEM(J) HAS TO BE FAILED AT THE END OF ITS PHASE
1 , SYSTEM(J) HAS TO BE OPERATIVE AT THE END OF ITS PHASE

CALCULATION RESULTS

MISSION : ALL PHASES HAVE TO BE SURVIVED

PROBABILITY OF MISSION FAILURE : 5.231E-04
MAX. CALCULATED ERROR : 1.044E-06

OTHER MISSIONS

MISSION	PROBABILITY OF MISSION SUCCESS	MAXIMUM CALCULATED ERROR
0 1 1	9.449E-10	9.449E-10
1 0 1	5.119E-04	1.037E-06
1 1 0	1.118E-05	1.036E-06
0 0 1	9.449E-10	----------
0 1 0	1.057E-14	----------
1 0 0	1.036E-06	----------

MISSION: ALL PHASES HAVE TO BE SURVIVED.

- PHASED MISSION -	
TIME POINT	UNAVAILABILITY
0.	0.
5.000E-01	9.44933E-10
5.000E-01	7.00111E-06
3.650E+01	5.11899E-04
3.650E+01	5.12928E-04
1.205E+02	5.23090E-04

```
*****************************************************************************************
END PROBCAL.                              .748(CP.SEC)      TOT.CP.TIME :         2.034(SEC)
                                         1.317(IO.SEC)      TOT.IO.TIME :         4.002(SEC)
*****************************************************************************************


*******************************
TOTAL WORK-SPACE USED :     154

*******************************
```

SAMENVATTING

"Betrouwbaar zijn" en "beschikbaar zijn" of "betrouwbaarheid" en "beschikbaarheid" zijn begrippen welke al sinds lange tijd een bekende klank bezitten in de dagelijkse omgang tussen personen. "Betrouwbaar zijn" als persoon wil bijv. zeggen dat de betrokkene geen misbruik maakt van aan hem (of haar) verstrekte informatie, *gedurende langere tijd*. Een zegswijze als "door de jaren heen kun je op hem (haar) bouwen", geeft een duidelijke relatie aan met "betrouwbaar zijn". Voor "beschikbaar zijn" geldt iets dergelijks. "Beschikbaar zijn" als persoon houdt in dat op *elk moment* aanspraak op de betrokkene gemaakt kan worden. Als voorbeeld hiervan kan men denken aan huis- en keukenpersoneel dat gedurende de diensturen steeds beschikbaar moet zijn voor diegenen welke hen ingehuurd hebben.
Voor door de mens gemaakte werktuigen geldt iets dergelijks. Men zegt bijv. dat een auto "betrouwbaar is" als gedurende langere tijd geen mankementen aan deze auto optreden. Dezelfde auto heet "beschikbaar te zijn" als hij, op het ogenblik dat men een rit wil ondernemen, start en kan rijden.
Blijkbaar is het zo dat "betrouwbaarheid" iets te maken heeft met het *ongestoord functioneren gedurende langere tijd*, en dat "beschikbaarheid" iets zegt over het functioneren op een *zeker moment*.
In het begin van deze eeuw is de behoefte ontstaan om de tot nu gevoelsmatig omschreven begrippen als "betrouwbaarheid" en "beschikbaarheid" preciezer te omschrijven. Deze behoefte is gevoed door een steeds voortschrijdende technische ontwikkeling, waarbij het van belang geacht werd vooraf iets te kunnen zeggen over het gedrag van materialen, d.w.z. een voorspelling te kunnen geven over de "levensduur", de tijd van ongestoord functioneren van het materiaal. Men heeft daartoe de "betrouwbaarheid" van een materiaal wiskundig gedefinieerd als een kans, d.w.z. "de betrouwbaarheid op tijdstip t" wordt geformuleerd als "de kans dat het materiaal geen defecten vertoont gedurende minstens een tijd t". Naast de "betrouwbaarheid" wordt vaak de z.g. "levensduurverdeling" gebruikt. De "levensduurverdeling" is complementair aan de "betrouwbaarheid", d.w.z. hij beschrijft de kans dat het materiaal binnen een tijd t bezwijkt. In de jaren '30 heeft bijv. Weibull voor de beschrijving van het vermoeiingsgedrag van metalen de later zo genoemde "Weibull verdeling (levensduurverdeling)" voorgesteld. Een ander voorbeeld betreft de levensduurverdeling van electronische compo-

nenten. In de beginjaren '50 heeft men, gebaseerd op waarnemingen, gevonden dat de "negatief exponentiële verdeling" een goede representatie vormt voor de levensduurverdeling van dergelijke componenten. Tijdens en na de Tweede Wereldoorlog zijn systemen steeds ingewikkelder geworden. Vandaar dat niet alleen de betrouwbaarheid van componenten van belang was, maar men ook steeds meer geïnteresseerd raakte in de "systeembetrouwbaarheid", de kans dat een systeem gedurende een zekere periode ongestoord functioneert.
Omdat een systeem opgebouwd is uit componenten en hun structurele samenhang, is de "systeembetrouwbaarheid" vanzelfsprekend een functie van de betrouwbaarheid van elk der componenten. De belangrijkheid van de systeembetrouwbaarheid komt in de jaren '50 vooral naar voren bij militaire systemen en in de ruimtevaart. De techniek welke in die jaren gebruikt wordt ter bepaling van de systeembetrouwbaarheid berust op de z.g. "betrouwbaarheids-blokdiagrammen". De werking van een systeem wordt bij deze methode aangegeven door blokken welke onderling verbonden zijn door lijnen. Elk blok vertegenwoordigt een deelsysteem (of deelfunctie). Voor elk blok wordt de betrouwbaarheid berekend en de systeembetrouwbaarheid kan daarna bepaald worden aan de hand van de betrouwbaarheden van de blokken.
De betrouwbaarheidsberekeningen via blokschema's zijn eigenlijk gebaseerd op handrekentechnieken. Want naarmate systemen complexer worden, groeien ook de overeenkomstige blokschema's. Dit heeft tot gevolg dat de blokschematechniek voor complexe systemen praktisch niet zo goed hanteerbaar is.
In het begin van de jaren '60 is men dan ook m.b.t. betrouwbaarheidsberekeningen voor complexe systemen overgegaan op een nieuwe methodiek, de z.g. "foutenboom analyse". Foutenboom analyse, afgekort FTA*, is een techniek die gericht is op de analyse van een specifieke systeemstoring.
De constructie van de foutenboom voor de betreffende storing, aangeduid met "TOP-gebeurtenis", verloopt als volgt.
De TOP-gebeurtenis (systeem storing) wordt door middel van een logische "OF" of "EN" gerelateerd aan storingen van subsystemen welke de systeem storing mogelijkerwijs zouden kunnen laten optreden. Elke subsysteem storing wordt daarna gekoppeld aan storingen op het volgende, lagere, systeemniveau, enz. Deze ontwikkeling stopt op het moment waarop storingen van componenten

---

*FTA: Fault Tree Analysis

(het laagste systeemniveau) ingevoegd zijn. De gehele structuur, welke begint bij de TOP-gebeurtenis en eindigt op het niveau van de componenten, heet nu een "foutenboom voor de betreffende systeem storing".
Met behulp van FTA kunnen zowel *kwalitatieve* als *kwantitatieve* karakteristieke grootheden voor de betreffende systeemfunctie bepaald worden. *Kwalitatieve* grootheden zijn o.a. de mogelijke manieren waardoor de systeem storing tot stand komt. Deze storingsmogelijkheden noemt men "minimale sneden". Iedere minimale snede bestaat uit een combinatie van componenten, welke de systeem storing laten optreden op het moment waarop elke component van de combinatie gefaald is. Andere kwalitatieve grootheden, de z.g. "minimale paden", vormen de combinaties van componenten welke het functioneren van de systeemfunctie garanderen. Als iedere component van zo'n minimaal pad functioneert, dan functioneert het systeem. *Kwantitatieve* grootheden zijn o.a. de "systeem niet-beschikbaarheid" en de "levensduurverdeling" van het systeem. Deze twee grootheden zijn complementair aan de "systeem beschikbaarheid" en de "systeem betrouwbaarheid". Maar omdat FTA in principe een analyse is van een systeem storing i.p.v. het functioneren van een systeem, worden de eerstgenoemde grootheden meestal berekend. De berekening van de "niet-beschikbaarheid" en de "levensduurverdeling" voor een systeemfunctie is gebaseerd op de "minimale sneden" en kan daarom pas plaatsvinden nadat deze "minimale sneden" bepaald zijn. De complexiteit van de kwantitatieve berekeningen neemt sterk toe als onderhoudsprocedures mede in rekening gebracht dienen te worden.
In welke gevallen het aanbeveling verdient om de "niet-beschikbaarheid" en in welke gevallen het aanbeveling verdient om de "levensduurverdeling" voor een systeem te berekenen, hangt enigermate af van het soort systeem. Men kan, voor wat dit aspect betreft, onderscheid maken tussen z.g. "actieve" en "niet-actieve" systemen. Een systeem heet "actief" als het gedurende een zekere tijd (bijv. een dag of een maand) onafgebroken moet blijven functioneren. Een "niet-actief" systeem daarentegen behoeft alleen maar in werking te komen wanneer daar vraag naar is. Een "actief" systeem is bijv. de motor van een auto tijdens een rit; het remsysteem van die auto kan gedurende die rit beschouwd worden als een "niet-actief" systeem. Het verschil tussen beide soorten systemen bestaat hieruit, dat een systeem storing voor een "actief" systeem fataal is terwijl dit voor een "niet-actief" systeem niet zo behoeft te zijn. Als de storing van een "niet-actief" systeem tijdig ontdekt en hersteld wordt voor de eerstvolgende

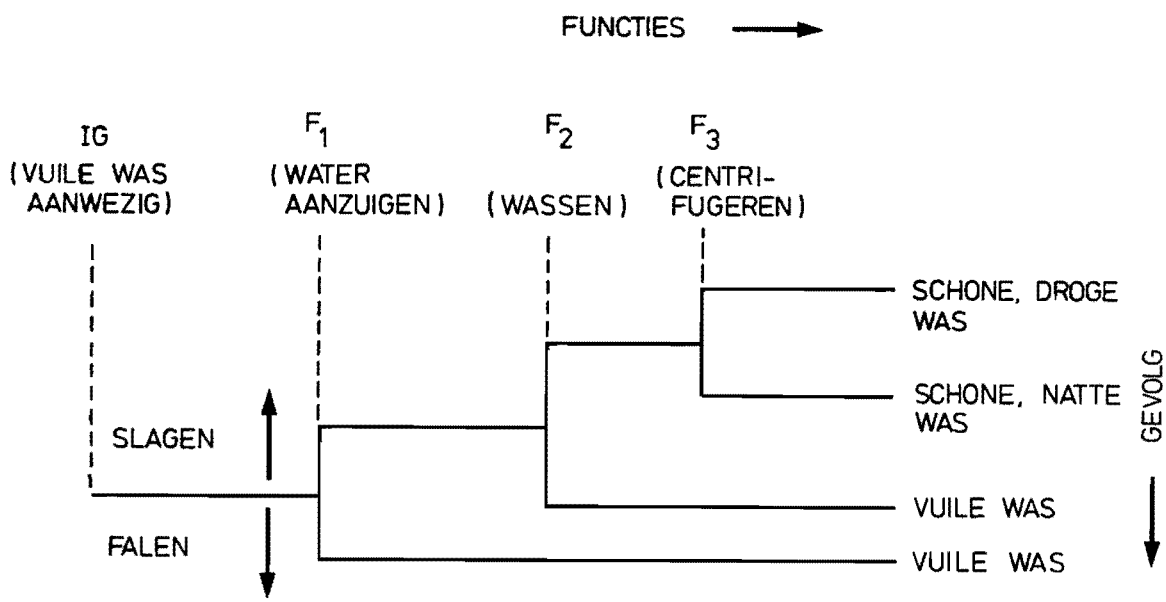
keer dat er gebruik van het systeem gemaakt wordt, dan is zo'n storing niet fataal.
Als bijv. de motor van een auto tijdens de rit afslaat en niet weer op gang te brengen is, dan is de rit voortijdig afgelopen. Als echter het indicatielichtje van het remsysteem tijdens de rit gaat branden, ten teken dat het remsysteem defect is, bestaat de mogelijkheid om tijdig te stoppen en de storing te verhelpen, waarna de rit voortgezet kan gaan worden. Vandaar ook dat voor een "actief" systeem de "levensduurverdeling" en voor een "niet-actief" systeem de "niet-beschikbaarheid" een kenmerkende kwantitatieve grootheid is.
In de praktijk van de afgelopen twintig jaar is gebleken dat voor complexe systemen FTA eigenlijk de enige mogelijkheid biedt tot het verkrijgen van inzicht in deze systemen. Met behulp van FTA kunnen o.a. zwakke plekken in een systeem worden opgespoord en kunnen vergelijkende studies voor diverse systemen uitgevoerd worden. Hoewel aanvankelijk FTA vooral in de ruimtevaart is toegepast, heeft men omstreeks het midden van de zestiger jaren ingezien dat deze techniek ook voor andere terreinen toepasbaar is. Vandaar dat vanaf die tijd FTA ook is toegepast voor systemen binnen nucleaire centrales, vooral voor de "niet-actieve" veiligheidssystemen. Bij de uitvoering van de grote risico-studie m.b.t. de veiligheid van kerncentrales in de Verenigde Staten, de z.g. Rasmussen studie (eindrapport 1975), is voor het eerst op grote schaal FTA toegepast. Bij dergelijke studies gaat het echter niet alleen om de analyse van een enkelvoudig systeem, maar veelal om de analyse van een aantal, procesmatig verbonden systemen welke niet gelijktijdig maar na elkaar functioneren en waarbij vaak afhankelijkheid tussen de systemen onderling bestaat. Eén van de afhankelijkheden kan zijn dat door meerdere systemen van eenzelfde component (bijv. een pomp) gebruik wordt gemaakt. Door deze afhankelijkheden wordt de berekening van kwantitatieve grootheden nogal wat ingewikkelder.
In de moderne ruimtevaart treft men ook afhankelijke systemen aan. Een voorbeeld hiervan is een raket. Zo'n raket bezit in het algemeen meerdere trappen d.w.z. meerdere systemen. Elk van deze trappen werkt tijdens de vlucht gedurende een bepaalde periode en stopt dan zijn werking, waarna de volgende trap in werking treedt. De trappen zelf maken vaak gebruik van een algemeen besturingssysteem. Voor een dergelijke raketvlucht

(de z.g. missie van een raket) is men geïnteresseerd in de kans dat de totale vlucht goed uitgevoerd wordt, d.w.z. de kans op succes van de raketvlucht.
In de literatuur wordt een dergelijke vlucht omschreven als een *gefaseerde missie*. Blijkbaar is een *gefaseerde missie* een opdracht voor een complex systeem, waarbij de opdracht in gedeelten (fasen) uitgevoerd wordt, het ene deel na het andere. Iedere deelopdracht wordt uitgevoerd door een deelsysteem van het totale systeem. De deelsystemen kunnen onderling afhankelijkheid vertonen. Voor het uitvoeren van elke deelopdracht is een bepaalde tijd nodig. De opdracht (missie) is geslaagd (is een succes) als elke deelopdracht slaagt, d.w.z. elke fase overleefd wordt. De missie mislukt als er een deelopdracht mislukt, d.w.z. als er een storing van een deelsysteem tijdens het uitvoeren van zijn deelopdracht optreedt. De karakteristieke grootheid is de kans op het succesvol uitvoeren van de missie, of het complement hiervan, nl. de kans op het falen van de missie. In het eerste geval zou men kunnen spreken over de *betrouwbaarheid* van het gehele systeem.
Het opmerkelijke is dat studies m.b.t. *gefaseerde missies* en gebaseerd op FTA later in de literatuur verschijnen dan de risico-studies welke met behulp van FTA uitgevoerd zijn. Toch bestaat er overeenkomst tussen de modellen van beide probleemgebieden. Om dit in te zien is het handig om eerst een schets te geven van de opzet en uitvoering van grote risico-analyses. We zullen dit doen aan de hand van een alledaags voorbeeld: het wasproces van vuile was.
De bedoeling van het wasproces is om uiteindelijk een schone, droge was te krijgen. Zo'n wasproces wordt pas aangevangen wanneer er vuile was aanwezig is. Het proces zelf in de wasmachine denken we ons opgebouwd uit de volgende drie gesimplificeerde functies:

(a) het aanzuigen van water (functie F_1);
(b) het wassen (functie F_2);
(c) het centrifugeren (functie F_3).

Het aanzuigen van water, het wassen en het centrifugeren vinden plaats in deze vaste volgorde. Daarbij neemt iedere functie een zekere tijd in beslag. Het uitvoeren van elk der functies gebeurt door het daartoe ontworpen systeem. Voor het aanzuigen van water zijn de klok van de wasmachine, de klep welke voor de watertoevoer zorgt en de waterniveauregelaar nodig.

Tijdens het wassen moeten de klok, de waterniveauregelaar, de verwarming, de motor en de snaar functioneren. Het centrifugeren wordt correct uitgevoerd als de klok, de snaar en de motor hun respectievelijke functies goed vervullen.
(Opgemerkt zij dat er verondersteld wordt dat alle andere onderdelen van de wasmachine, zoals de trommel, lagers, enz. goed werken). Het deelsysteem voor het uitvoeren van bijv. functie F_1 (aanzuigen van water) bestaat hier dus uit de klok, de klep en de waterniveauregelaar.
Als alle drie functies (F_1, F_2 en F_3) goed uitgevoerd worden, is het resultaat (of gevolg) een schone, droge was. Als echter functie F_3 (centrifugeren) niet uitgevoerd wordt (omdat het daartoe benodigde systeem faalt) dan bestaat het gevolg uit een schone, natte was. En wanneer functie F_1 (aanzuigen van water) of functie F_2 (wassen) niet uitgevoerd worden, dan is het gevolg dat men met een vuile was blijft zitten. Onmiskenbaar is deze situatie de meest dramatische.
Het hierboven beschrevene is samengevat in onderstaand schema.



In zo'n schema zijn de functies welke achtereenvolgens uitgevoerd moeten worden gekoppeld aan het gevolg, dat afhankelijk is van het wel of niet geslaagd uitvoeren van elk der functies. Voorafgaand aan de functies wordt vermeld wat de reden voor het in gang zetten van het proces is geweest, de z.g. "initiërende gebeurtenis (IG)". In ons voorbeeld is dat

het aanwezig zijn van vuile was.
Binnen de risico-analyse noemt men een dergelijk schema een *gebeurtenissenboom*. Elk der wegen welke tot een gevolg leidt heet een *tak* van de gebeurtenissenboom. De gebeurtenissenboom wordt in de regel zo opgesteld, dat de "gevolgen" in het schema van boven naar beneden steeds ernstiger worden. Daarbij moet men wel bedenken dat de "initiërende gebeurtenis" in geval van risico-studies veelal storingen binnen een systeem voorstellen, en de functies (F_1, F_2, enz.) zorg moeten dragen voor de goede afloop van een dergelijk incident. De functies moeten dus zorgen voor een zo klein mogelijk schadelijk gevolg. Een voorbeeld van een initiërende gebeurtenis binnen een kernreactor zou kunnen zijn: een breuk in een van de leidingen waardoor water stroomt om de kern te koelen.
Bij risico-studies heten de takken van een gebeurtenissenboom vaak *ongeluksverlopen*. Van zo'n ongeluksverloop is het van belang om niet alleen het *gevolg* te kennen, maar ook de *kans op het optreden* ervan. En hier krijgen we te maken met kansrekening van een aantal, vaak afhankelijke, functies (deelsystemen).
Als we teruggaan naar de hiervoor omschreven *gefaseerde missie*, dan is het duidelijk dat die tak van de gebeurtenissenboom waarbij elk van de functies goed uitgevoerd wordt, als een gefaseerde missie beschouwd mag worden. In de huidige literatuur is dit nog niet onderkend. *De huidige studie gaat echter nog een stap verder en definieert iedere tak van een gebeurtenissenboom als een gefaseerde missie*. Tevens wordt een nieuwe methodiek geïntroduceerd voor de berekening van de kans op optreden van een gefaseerde missie. Deze nieuwe methodiek maakt gebruik van FTA en is hoofdzakelijk ontwikkeld om onderlinge afhankelijkheden van deelsystemen op een juiste manier te behandelen. Bij de tot nog toe uitgevoerde risico-studies is dit vrijwel nooit methodisch maar veelal gevoelsmatig gebeurd. De nieuwe methodiek beperkt zich tot componenten en systemen welke zich slechts in één van de volgende twee toestanden kunnen bevinden: de functionerende of de gefaalde toestand. Men spreekt dan ook van een binair gedrag. Verder wordt verondersteld dat inspecties en reparaties niet uitgevoerd worden bij "actieve" systemen. De methodiek berust op een scheiding van de analyse van het gedrag van componenten en de analyse van het gedrag van systemen. Vanwege dit aspect is het mogelijk gebleken om de inspectie en reparatie procedures gestalte te geven in de mathematische modelvorming van de componenten. Ten opzichte van de bestaande literatuur zijn een aan-

tal nieuwe varianten toegevoegd aan de diverse bestaande componenten-modellen. Deze nieuwe modellen worden uitvoerig behandeld in deze studie.
De oplossingsmethodiek is gebaseerd op FTA, d.w.z. op de minimale sneden (storingsmogelijkheden) van een systeem. Aangezien het aantal minimale sneden voor complexe systemen zeer groot kan zijn (soms miljoenen) is het meestal niet mogelijk de exacte analytische oplossing te produceren. Vandaar dat ook onder- en bovengrenzen voor de kans op het optreden van een gefaseerde missie (tak van een gebeurtenissenboom) gepresenteerd worden.
Uit berekeningsresultaten blijkt dat indien de afhankelijkheden tussen de systemen niet volledig meegenomen worden, de kans op het optreden van die takken in gebeurtenissenbomen welke de grootste gevolgen met zich meedragen, te laag afgeschat worden. Tevens biedt de nieuwe methodiek op kwantitatieve wijze inzicht in de mate van afhankelijkheid tussen systemen. Beide laatst genoemde aspecten zijn van wezenlijk belang voor risico-analyses.
Om de methodiek hanteerbaar te maken voor complexe systemen is zij geïmplementeerd in het betrouwbaarheids-computerprogramma PHAMISS. Het programma is geschreven in de programmeertaal FORTRAN-IV voor de CDC-Cyber 175.
In de praktijk is aangetoond dat PHAMISS een zeer snel en efficient programma is en tevens een hoge mate van gebruikersvriendelijkheid bezit.

Curriculum Vitae

The author was born in Minnertsga (province of Friesland) in 1944. After his secondary school education (HBS-B, 1963, Leeuwarden) he was in military service (1964/1965). In 1965 he entered the Delft University of Technology where he got his masters degree in mathematical engineering in 1971. For the next five years he was employed by the National Defense Organisation of the Netherlands (RVO-TNO), The Hague.
In 1976 he joined the Netherlands Energy Research Foundation ECN, Petten, where he is engaged in reliability and risk analysis.

STELLINGEN

bij het proefschrift

PHASED MISSION ANALYSIS OF MAINTAINED SYSTEMS

A Study in Reliability and Risk Analysis

van

K. Terpstra

Datum promotie: 4 december 1984

STELLINGEN

1

Ook bij het gebruik van kernfusie-reactoren doen zich risico-aspecten voor, hoewel in geringere mate dan bij kernsplijtingsreactoren.

2

Het nut van de kwantificering van betrouwbaarheid en risico van systemen is mede gelegen in het verkrijgen van een grondige systeemkennis.

3

Het uitvoeren van gevoeligheidsanalyses bij risico- en betrouwbaarheids-studies dient onder geen voorwaarde achterwege te blijven.

4

De interpretatie van resultaten van uitgevoerde risico-analyses vereist een grote mate van deskundigheid. In het bijzonder dient het interpreteren van kansen, welke optreden als uitkomsten bij betrouwbaarheids-studies, met de grootste zorgvuldigheid te geschieden.

5

De verslaggeving van risico- en betrouwbaarheidsanalyses dient doorzichtig te zijn; de uitgevoerde berekeningen moeten gecontroleerd kunnen worden.

6

Bij het vaststellen van een procedure voor uit te voeren risico-analyses dient nauwkeurig de doelstelling en het gebruik van de te verkrijgen resultaten omschreven te worden; doelstelling en gebruik van een risico-analyse stellen hun eisen aan de detaillering van het systeemmodel.

7

Bij het stellen van normen door de overheid omtrent het veilig gebruik van complexe technische installaties, verdient het aanbeveling een norm vast te stellen met betrekking tot de procedures volgens welke risico-analyses uitgevoerd moeten worden.

8

In de verslaggeving van uitkomsten van betrouwbaarheidsberekeningen dienen ten aanzien van de beschrijving van de invoergegevens vermeld te worden:

(i) de gevolgde procedure ter verkrijging van de waarnemingen;

(ii) de statistische methodieken welke voor het verwerken van de waarnemingen zijn toegepast.

9

De in Nederland van overheidswege gesubsidieerde grote onderzoeksinstituten (bijvoorbeeld TNO, ECN, NLR, enz.) zijn bij uitstek geschikt voor het ontwikkelen van hoogwaardige produktie software.

10

Bij het beschikbaar stellen van computer programma-pakketten voor het uitvoeren van betrouwbaarheidsanalyses, dient naast doelmatigheid in sterke mate rekening gehouden te worden met operationele gebruikersvriendelijkheid.

11

Voor programma-pakketten waarmee veelsoortige berekeningen betreffende eenzelfde vakgebied uitgevoerd kunnen worden, verdient het aanbeveling een filosofie te ontwikkelen betreffende de structuur van de invoer zodanig dat voor elk soort berekening de invoer eenzelfde opbouw bezit.

12

De benodigde tijd voor het ontwikkelen van grote, doelmatige en efficiënte computerprogramma's kan enigszins afgeschat worden als de programmeertaal en het aantal correcte opdrachten (software statements) dat gemiddeld per dag geproduceerd kan worden door een goede programmeur in deze taal bekend zijn; voor de taal FORTRAN ligt dit aantal tussen de 5 à 15 per dag.