IEC 60300-3-11

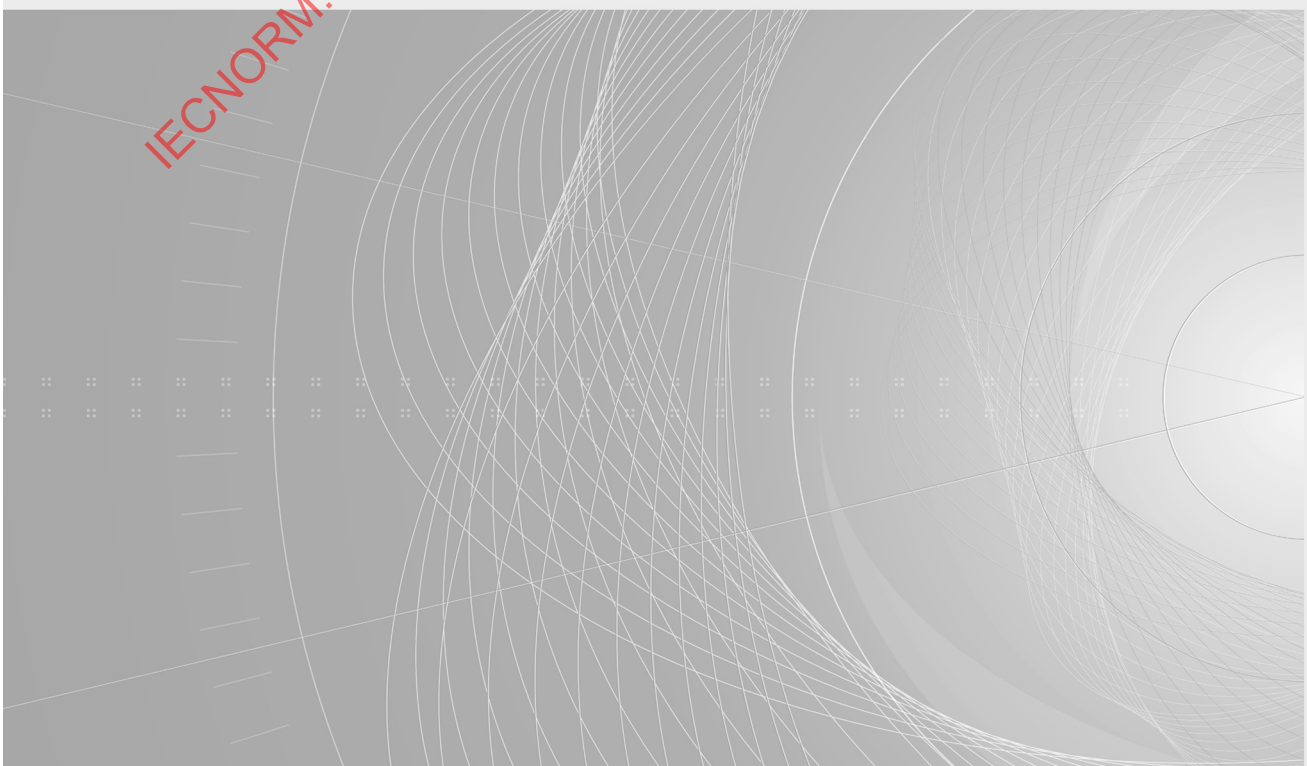
Edition 2.0 2009-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability management – Part 3-11: Application guide – Reliability centred maintenance

Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité



IEC 60300-3-11:2009

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 60300-3-11

Edition 2.0 2009-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability management – Part 3-11: Application guide – Reliability centred maintenance

Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX X

ICS 03.100.40; 03.120.01

ISBN 978-2-88910-098-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 3-11: Application guide – Reliability centred maintenance

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-11 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition, published in 1999, and constitutes a technical revision.

The previous edition was based on ATA[1]-MGS-3; whereas this edition applies to all industries and defines a revised RCM algorithm and approach to the analysis process.

1 The Air Transport Association of America.

The text of this standard is based on the following documents:

FDIS	RVD
56/1312/FDIS	56/1320/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

A list of all parts in the IEC 60300 series, under the general title *Dependability management* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be:

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

Reliability centred maintenance (RCM) is a method to identify and select failure management policies to efficiently and effectively achieve the required safety, availability and economy of operation. Failure management policies can include maintenance activities, operational changes, design modifications or other actions in order to mitigate the consequences of failure.

RCM was initially developed for the commercial aviation industry in the late 1960s, resulting in the publication of ATA-MGS-3 [1][2]. RCM is now a proven and accepted methodology used in a wide range of industries.

RCM provides a decision process to identify applicable and effective preventive maintenance requirements, or management actions, for equipment in accordance with the safety, operational and economic consequences of identifiable failures, and the degradation mechanism responsible for those failures. The end result of working through the process is a judgement as to the necessity of performing a maintenance task, design change or other alternatives to effect improvements.

The basic steps of an RCM programme are as follows:

a) initiation and planning;

b) functional failure analysis;

c) task selection;

d) implementation;

e) continuous improvement.

All tasks are based on safety in respect of personnel and environment, and on operational or economic concerns. However, it should be noted that the criteria considered will depend on the nature of the product and its application. For example, a production process will be required to be economically viable, and may be sensitive to strict environmental considerations, whereas an item of defence equipment should be operationally successful, but may have less stringent safety, economic and environmental criteria.

Maximum benefit can be obtained from an RCM analysis if it is conducted at the design stage, so that feedback from the analysis can influence design. However, RCM is also worthwhile during the operation and maintenance phase to improve existing maintenance tasks, make necessary modifications or other alternatives.

Successful application of RCM requires a good understanding of the equipment and structure, as well as the operational environment, operating context and the associated systems, together with the possible failures and their consequences. Greatest benefit can be achieved through targeting of the analysis to where failures would have serious safety, environmental, economic or operational effects.

2 Figures in square brackets refer to the bibliography.

DEPENDABILITY MANAGEMENT –

Part 3-11: Application guide – Reliability centred maintenance

1 Scope

This part of IEC 60300 provides guidelines for the development of failure management policies for equipment and structures using reliability centred maintenance (RCM) analysis techniques.

This part serves as an application guide and is an extension of IEC 60300-3-10, IEC 60300-3-12 and IEC 60300-3-14. Maintenance activities recommended in all three standards, which relate to preventive maintenance, may be implemented using this standard.

The RCM method can be applied to items such as ground vehicles, ships, power plants, aircraft, and other systems which are made up of equipment and structure, e.g. a building, airframe or ship's hull. Typically, equipment comprises a number of electrical, mechanical, instrumentation or control systems and subsystems which can be further broken down into progressively smaller groupings, as required.

This standard is restricted to the application of RCM techniques and does not include aspects of maintenance support, which are covered by the above-mentioned standards or other dependability and safety standards.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60300-3-10, *Dependability management – Part 3-10: Application guide – Maintainability*

IEC 60300-3-12, *Dependability management – Part 3-12: Application guide – Integrated logistic support*

IEC 60300-3-14, *Dependability management – Part 3-14: Application guide – Maintenance and maintenance support*

IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions of IEC 60050-191 apply, together with the following.

3.1 Definitions

3.1.1
age exploration
systematic evaluation of an item based on analysis of collected information from in-service experience to determine the optimum maintenance task interval

NOTE The evaluation assesses the item's resistance to a deterioration process with respect to increasing age or usage.

3.1.2
criticality
severity of effect of a deviation from the specified function of an item, with respect to specified evaluation criteria

NOTE 1 The extent of effects considered may be limited to the item itself, to the system of which it is a part, or range beyond the system boundary.

NOTE 2 The deviation may be a fault, a failure, a degradation, an excess temperature, an excess pressure, etc.

NOTE 3 In some applications, the evaluation of criticality may include other factors such as the probability of occurrence of the deviation, or the probability of detection.

3.1.3
damage-tolerant
capable of sustaining damage and continuing to function as required, possibly at reduced loading or capacity

3.1.4
failure (of an item)
loss of ability to perform as required

3.1.5
failure effect
consequence of a failure mode on the operation, function or status of the item

3.1.6
failure management policy
maintenance activities, operational changes, design modifications or other actions in order to mitigate the consequences of failure

3.1.7
function
intended purpose of an item as described by a required standard of performance

3.1.8
failure mode
manner in which failure occurs

NOTE A failure mode may be defined by the function lost or the state transition that occurred.

3.1.9
failure-finding task
scheduled inspection or specific test used to determine whether a specific hidden failure has occurred

3.1.10
functional failure
reduction in function performance below desired level

3.1.11
hidden failure mode
failure mode whose effects do not become apparent to the operator under normal circumstances

3.1.12
indenture level
level of subdivision of an item from the point of view of a maintenance action

NOTE 1 Examples of indenture levels could be a subsystem, a circuit board, a component.

NOTE 2 The indenture level depends on the complexity of the item's construction, the accessibility to subitems, skill level of maintenance personnel, test equipment facilities, safety considerations, etc.

[IEV 191-07-05:1990]

3.1.13
inspection
identification and evaluation of the actual condition against a specification

3.1.14
maintenance action
maintenance task
sequence of elementary maintenance activities carried out for a given purpose

NOTE Examples include diagnosis, localization, function check-out, or combinations thereof.

3.1.15 tem

part, component, device, subsystem, functional unit, equipment or system that can be individually considered

NOTE 1 An item may consist of hardware, software or both, and may also, in particular cases, include people. Elements of a system may be natural or man-made material objects, as well as modes of thinking and the results thereof (e.g. forms of organization, mathematical methods and programming languages).

NOTE 2 In French the term "entité" is preferred to the term "dispositif" due to its more general meaning. The term "dispositif' is also the common equivalent for the English term "device".

NOTE 3 In French the term "individu" is used mainly in statistics.

NOTE 4 A group of items, e.g. a population of items or a sample, may itself be considered as an item.

NOTE 5 A software item may be a source code,an object code, a job control code, control data, or a collection of these.

3.1.16
maintenance concept
interrelationship between the maintenance echelons, the indenture levels and the levels of maintenance to be applied for the maintenance of an item

3.1.17
maintenance echelon
position in an organization where specified levels of maintenance are to be carried out on an item

NOTE 1 Examples of maintenance echelons are: field, repair shop, and manufacturer.

NOTE 2 The maintenance echelon is characterized by the level of skill of the personnel, the facilities available, the location, etc.

[IEV 191-07-04:1990]

3.1.18
maintenance policy
general approach to the provision of maintenance and maintenance support based on the objectives and policies of owners, users and customers

3.1.19
maintenance programme
list of all the maintenance tasks developed for a system for a given operating context and maintenance concept

3.1.20
operating context
circumstances in which an item is expected to operate

3.1.21
potential failure
identifiable condition that indicates that a functional failure is either about to occur or is in the process of occurring

3.1.22
potential failure – functional failure (P-F) interval
interval between the point at which a potential failure becomes detectable and the point at which it degrades into a functional failure

3.1.23
reliability centred maintenance
method to identify and select failure management policies to efficiently and effectively achieve the required safety, availability and economy of operation.

3.1.24
safe life
age before which no failures are expected to occur

3.1.25
system
set of interrelated or interacting elements

[ISO 9000, 3.2.1][2]

NOTE 1 In the context of dependability, a system will have:

a) a defined purpose expressed in terms of required functions;

b) stated conditions of operation/use;

c) defined boundaries.

NOTE 2 The structure of a system may be hierarchical.

3.1.26
useful life
time interval to a given instant when a limited state is reached

NOTE 1 Limited state may be a function of failure intensity, maintenance support requirement, physical condition, age, obsolesence, etc.

NOTE 2 The time interval may start at first use, at a subsequent instant, i.e. remaining useful life.

3.2 Abbreviations

FMEA Failure mode and effects analysis

FMECA Failure mode, effects and criticality analysis

ILS Integrated logistic support

HUMS Health usage management systems

LORA Level of repair analysis

NDI Non-destructive inspection

RCM Reliability centred maintenance

4 Overview

4.1 General

The RCM process is fully described in this standard and provides information on each of the following elements:

a) RCM initiation and planning;

b) functional failure analysis;

c) task selection;

d) implementation;

e) on-going improvement.

Figure 1 shows the overall RCM process, divided into five steps. It can be seen from this figure that RCM provides a comprehensive programme that addresses not just the analysis process but also the preliminary and follow-on activities necessary to ensure that the RCM effort achieves the desired results. The RCM process can be applied to all types of systems. Annex D provides guidance on how the process should be interpreted for structures for which the failure mechanisms and resultant tasks are more narrowly defined.

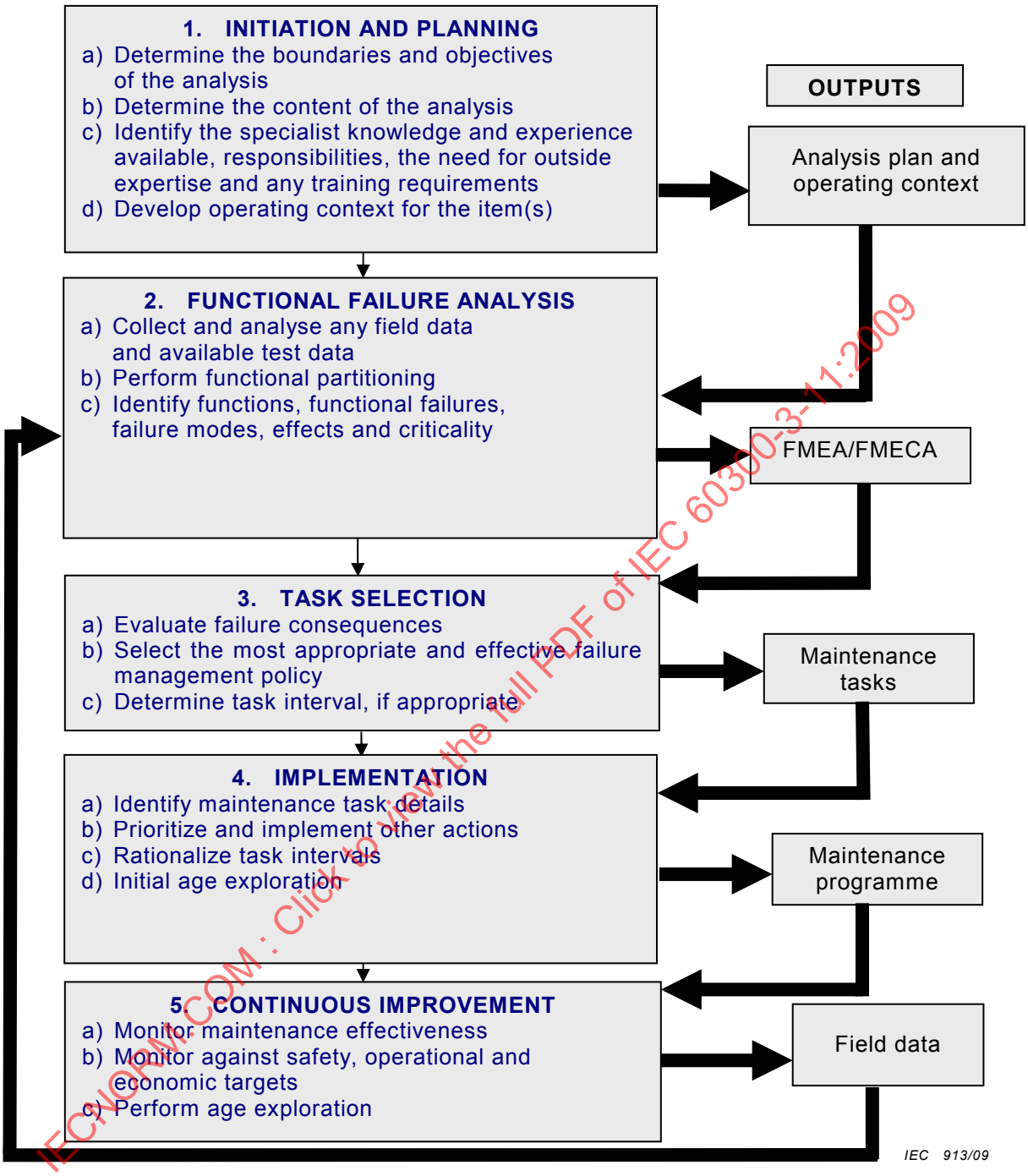


Figure 1 – Overview of the RCM process

4.2 Objectives

As part of a maintenance policy, the objectives of an effective preventive maintenance programme are as follows:

a) to maintain the function of an item at the required dependability performance level within the given operating context;

b) to obtain the information necessary for design improvement or addition of redundancy for those items whose reliability proves inadequate;

c) to accomplish these goals at a minimum total LCC, including maintenance costs and the costs of residual failures;

d) to obtain the information necessary for the ongoing maintenance programme which improves upon the initial programme, and its revisions, by systematically assessing the effectiveness of previously defined maintenance tasks. Monitoring the condition of specific safety, critical or costly components plays an important role in the development of a programme.

These objectives recognize that maintenance programmes, as such, cannot correct design deficiencies in the safety and reliability levels of the equipment and structures. The maintenance programme can only minimize deterioration and restore the item to its design levels. If the reliability intrinsic levels are found to be unsatisfactory, design modification, operational changes or procedural changes (such as training programmes) may be necessary to achieve the desired performance.

RCM improves maintenance effectiveness and provides a mechanism for managing maintenance with a high degree of control and awareness. Potential benefits can be summarized as follows:

1) system dependability can be increased by using more appropriate maintenance activities;
2) overall costs can be reduced by more efficient planned maintenance effort;
3) a fully documented audit trail is produced;
4) a process to review and revise the failure management policies in the future can be implemented with relatively minimum effort;
5) maintenance managers have a management tool which enhances control and direction;
6) maintenance organization obtains an improved understanding of its objectives and purpose and the reasons for which it is performing the scheduled maintenance tasks.

The maintenance programme is a list of all the maintenance tasks developed for a system for a given operating context and maintenance concept, including those arising from the RCM process. Maintenance programmes are generally composed of an initial programme and an on-going, "dynamic" programme. Figure 2 shows the principal factors which need to be considered in the development stage, that is before operation, and those which are used to update the programme, based on operational experience, once the product is in service.

The initial maintenance programme, which is often a collaborative effort between the supplier and the user, is defined prior to operation and may include tasks based on the RCM methodology. The on-going maintenance programme, which is a development of the initial programme, is initiated as soon as possible by the user once operation begins, and is based on actual degradation or failure data, changes in operating context, advances in technology, materials, maintenance techniques and tools. The on-going programme is maintained using RCM methodologies. The initial maintenance programme is updated to reflect changes made to the programme during operation.

An initial RCM programme may be initiated when the product is in service, in order to renew and improve on an existing maintenance programme, based on experience or manufacturer's recommendations, but without the benefit of a standard approach such as RCM.

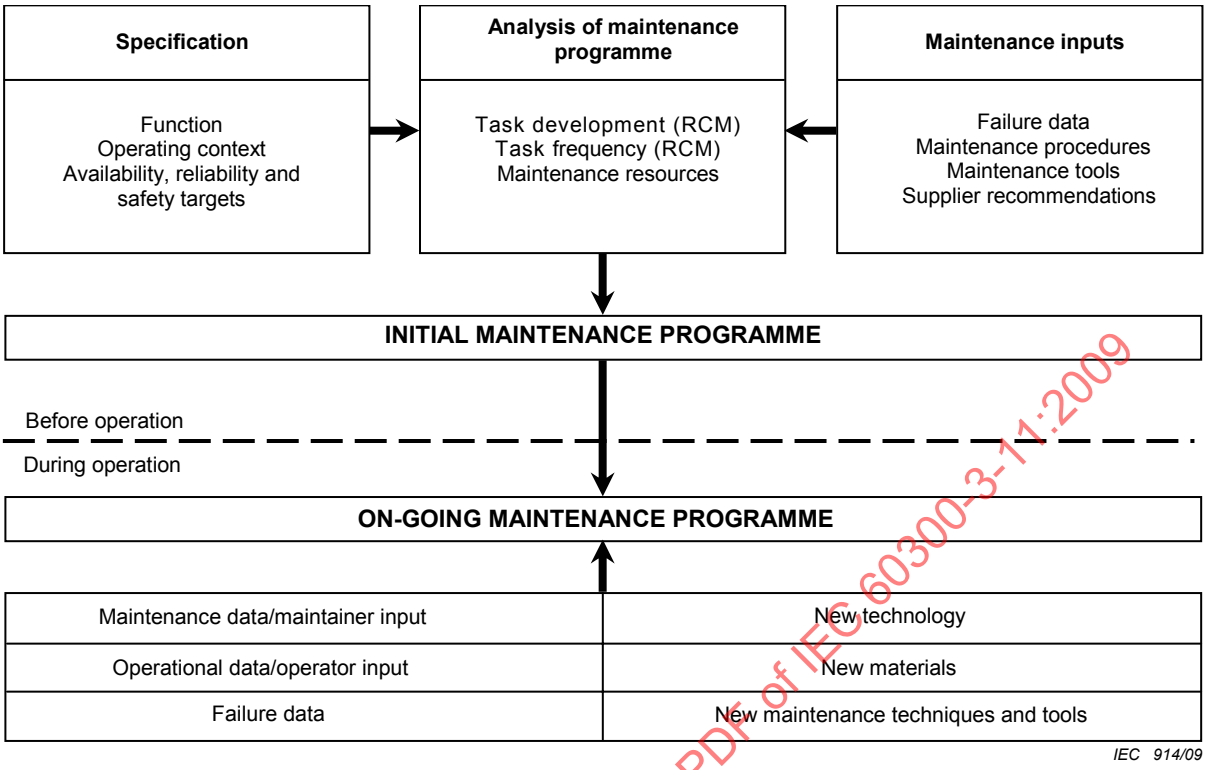


Figure 2 – Evolution of an RCM maintenance programme

4.3 Types of maintenance

Different approaches are taken to maintenance tasks as illustrated in Figure 3. There are two types of maintenance action: preventive and corrective.

Preventive maintenance is undertaken prior to failure. This can be condition-based, which can be achieved by monitoring the condition until failure is imminent, or by functional checks to detect failure of hidden functions. Preventive maintenance can also be predetermined, based on a fixed interval (such as calendar time, operating hours, number of cycles) consisting of scheduled refurbishment or replacement of an item or its components.

Corrective maintenance restores the functions of an item after failure has occurred or performance fails to meet stated limits. Some failures are acceptable if the consequences of failure (such as production loss, safety, environmental impact, failure cost) are tolerable compared to the cost of preventive maintenance and the subsequent loss due to failure. This results in a planned run-to-failure approach to maintenance.

Preventive maintenance is normally scheduled or based on a predetermined set of conditions while corrective maintenance is unscheduled. It is not unusual to defer corrective maintenance for a later convenient time when redundancy preserves function. RCM identifies the optimal preventive and corrective maintenance tasks.

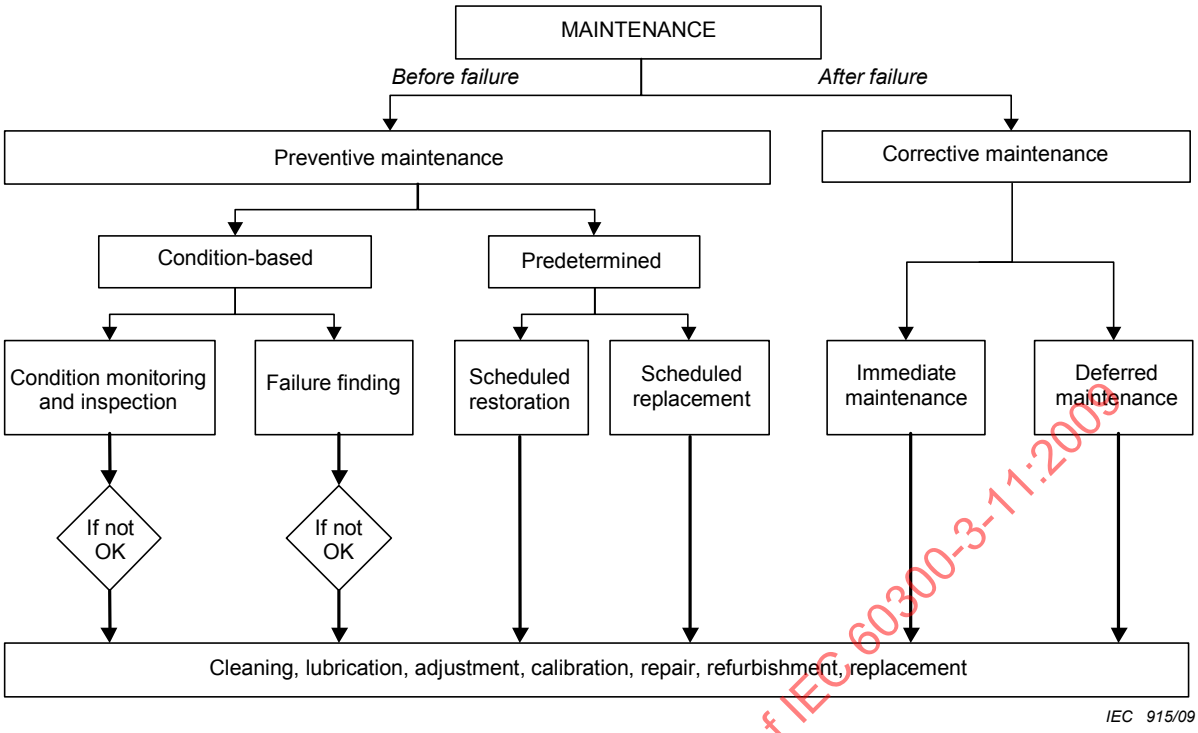


Figure 3 – Types of maintenance tasks

5 RCM initiation and planning

5.1 Objectives for conducting an RCM analysis

The first phase of planning an RCM analysis is to determine the need and extent for the study, taking into consideration the following objectives as a minimum:

a) establish optimal maintenance tasks for the item;
b) identify opportunities for design improvement;
c) evaluate where the current maintenance tasks are ineffective, inefficient or inappropriate;
d) identify the dependability improvements.

The process of assessing the need for RCM analysis should be a regular management activity within the organization's programme of continuous maintenance improvement.

A broad analysis of available data within the organization's maintenance management system will identify target systems, where the current failure management policy has failed or is suspect. Data indicating the following parameters will identify potential items:

1) changes in the operating context;
2) inadequate availability and/or reliability;
3) safety incidents;
4) unacceptably high preventive and/or corrective maintenance man hours;
5) backlog of maintenance work;
6) excessive maintenance cost;
7) unacceptably high ratio of "corrective to preventive" maintenance;
8) new maintenance techniques;
9) item technology changes.

Total reliance on data within a maintenance management system may be misleading and should be supported by additional evidence from maintenance personnel or a system inspection to reveal any features that may not be included in the data. An assessment of the completeness and accuracy of information available should be included in the RCM planning process.

There are other advantages in engaging maintenance personnel in the RCM team; they will become familiar with the item and provide opportunities to understand the operating context and have a direct discussion regarding existing maintenance, failure modes and failure patterns (see Annex C).

5.2 Justification and prioritization

As part of a wider maintenance policy, an RCM analysis should only be implemented when there is confidence that it can be cost effective or when direct commercial cost considerations are overridden by other critical objectives, such as requirements for safety and the environment. These factors should be considered over the entire life time of the item.

Those discrete systems that are judged to have an effect on the overall business goals will be identified as in need of analysis. The selection and priority by which they should be addressed should be based on a wide range of criteria such as:

a) maintenance efficiency;

b) dependability improvement;

c) design/operation change.

The priority of systems will depend on the priority of the organization's business objectives.

The methods used to select and prioritize the systems can be divided into:

1) qualitative methods based on past history and collective engineering judgement,

2) quantitative methods, based on quantitative criteria, such as criticality rating, safety factors, probability of failure, failure rate, life cycle cost, etc., used to evaluate the importance of system degradation/failure on equipment safety, performance and costs. Implementation of this approach is facilitated when appropriate models and data sources exist,

3) combination of qualitative and quantitative methods.

The purpose of this activity is to produce a listing of items ranked by criticality and priority.

5.3 Links to design and maintenance support

The majority of the maintenance support requirements for a system is decided at the initial design, and hence the planning for maintenance and maintenance support should be considered as early as possible so that trade-offs can be considered between functional needs, capability, life cycle cost, dependability and safety.

Maintenance and maintenance support should be considered during all phases of the life cycle. The specific tasks that should be performed are given in IEC 60300-3-14 and maintainability aspects are given in IEC 60300-3-10.

The approach for determining the total support requirements during the life of the system prior to initial operation is known as "integrated logistic support" (ILS) and this should be conducted in accordance with IEC 60300-3-12. Figure 4 illustrates the relationship between RCM and other support and analysis activities.

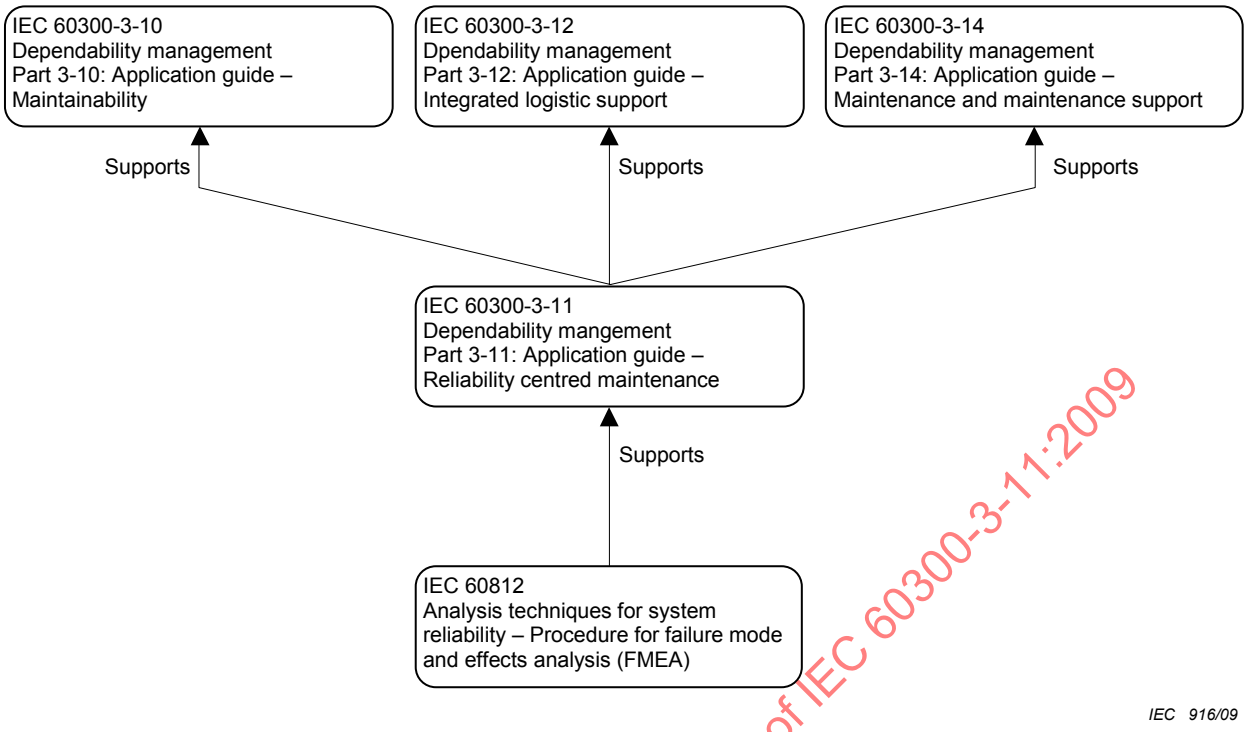


Figure 4 – Relationship between RCM and other support activities

5.4 Knowledge and training

An RCM analysis requires specialist knowledge and experience with the item and its operating context. The analysis requires the following:

a) knowledge of and experience with the RCM process;
b) detailed knowledge of the item and the appropriate design features;
c) knowledge of the item's operating context;
d) knowledge of the condition of the item (when analysing existing equipment);
e) understanding of the failure modes and their effects;
f) specialist knowledge of constraints, such as safety and environmental legislation, regulation etc;
g) knowledge of the maintenance techniques and tools;
h) knowledge of costs.

Where there is a lack of knowledge and experience with the RCM process, additional training should be provided.

5.5 Operating context

Prior to conducting an RCM analysis, it is essential that an operating context statement is developed. The operating context should describe how the item is operated, giving details of the desired performance of the systems.

For the analysis of a large item with many systems it is likely that a hierarchy of operating contexts is necessary.

The highest function level statement is normally written first and describes the item's physical characteristics, its primary role and systems, demand profiles and operating and support environment.

The statement at lowest functional/system level precisely defines the performance characteristics of the function under review. It is important to note that specific performance parameters are necessary to clearly determine what constitutes a failure, and what effects such failures will have upon specific equipment performance.

The operation of an item may vary depending on demand. Therefore, it may be necessary to generate different operating contexts to reflect these different states, as differences in demand may result in different maintenance policies. For example, a system may only be required for a short period of time and the maintenance during this time might be frequent and be based on cycles. However, during long periods of inactivity, the same system might be subject to infrequent maintenance based on calendar time.

The maintenance concept could also be influenced by changing environmental conditions. For example, items in arctic conditions may be subject to a different failure management policy compared to the same item in tropical conditions.

Operating contexts should consider the issue of redundancy very carefully. Redundancy is where multiple systems exist to support a single function. There are two types of redundancy, namely:

a) stand-by redundancy;

b) active redundancy.

Stand-by redundancy is where a system exists on stand-by, operating only in the event of failure of the duty system. The operating context for each system will be different and will result in different failure modes and different failure management policies.

Active redundancy is where two or more systems are operated simultaneously to provide a function, but each individual system has the ability to provide the function. In this situation, the likely failure modes of each system will be similar with the same failure management policies.

A different maintenance programme may be required for inactive equipment, such as equipment stored for infrequent or one time operation and the operating context should consider such items.

5.6 Guidelines and assumptions

As part of any RCM analysis effort, a set of guidelines and assumptions should be made to help direct the analysis process. The guidelines and assumptions should be clearly identified and documented to establish the approach to the analysis process and to ensure it is consistent. Considerations might include:

a) standard operating procedures (including what constitutes "normal duties" for the operator);

b) organizational polices as a source of input on failure definition, acceptable failure rates, etc.;

c) data sources;

d) acceptable probabilities of failure as a function of failure effects;

e) item breakdown structure;

f) analysis approach for interface items such as wiring and tubing;

g) analysis approach for previously repaired or uniquely configured items;

h) analytical methods and tools, such as fault tree analysis, reliability block diagrams, Markov processes and Petri net analysis;

i) cost benefit analysis methods;

j) defined values for parameters such as labour rates, utilization rates, design life conversion factors, and minimum detectable crack sizes;

k) consideration of remote monitoring and advanced inspection/detection techniques such as health usage management systems (HUMS) or non-destructive inspection (NDI);

l) methodologies for identifying potential to functional failure intervals, wear-outages, and for calculating task intervals;

m) human error analysis for considering risks due to human error.

Tasks mandated by legislation should be subject to RCM analysis to verify their validity. It would be necessary to liaise with legislative bodies before implementing changes.

5.7 Information requirements

Performing an RCM analysis requires information on the system regarding operation, and prior history where available. For example, all obtainable failure data should be collated to ensure that all failures that have occurred previously are covered. Maintenance records provide an indication of the condition of the equipment after use. However, where sufficient data are not available, the judgement of experts with a knowledge of the equipment can be used.

RCM analysis is conducted assuming no preventive maintenance is being undertaken and therefore is often referred to as being “zero based”. Therefore field failure data should be used with great caution as it will be dependent on any existing failure management policy. Failures which are known to be eliminated by any existing preventive maintenance tasks shall also be considered. However, consideration of failures which have never occurred before due to the existence of preventive maintenance tasks may be difficult.

Actual or generic failure data used in isolation has limited value without understanding failure mechanisms and the operating context. The information which may assist in conducting an RCM analysis may include:

a) usage profile;

b) performance requirements;

c) operating procedures and actual operating experience;

d) regulatory requirements;

e) reliability analysis;

f) safety case or safety assessments;

g) technical manuals;

h) manufacturer’s handbooks;

i) design documentation;

j) existing preventive maintenance tasks;

k) existing maintenance procedures and actual maintainers’ experience;

l) planned system modifications;

m) maintenance and failure reports;

n) structural survey reports;

o) incident and accident reports;

p) spares usage rates.

6 Functional failure analysis

6.1 Principles and objectives

The ability to develop a successful maintenance programme using RCM requires a clear understanding of item functions, failures and consequences expressed in terms of the organization's objectives in operating the item.

The method by which the item functions, failures and consequences are analysed should be selected by the organization to suit its operational structure and objectives; the output from the analysis should, however, produce the information described in the following clauses to enable the RCM analysis to be completed.

The failure mode and effects analysis (FMEA) and criticality method (IEC 60812) is suitable for application to RCM if the analysis is structured in such way as to conform to the requirements of this standard.

As part of the functional failure analysis, field data should be analysed to determine causes and frequencies to help assess criticality and support the FMEA. Data sources are discussed in 7.5.1.

Annex D provides details on the interpretation of functional failure analysis as applied to structures.

6.2 Requirements for definition of functions

6.2.1 Functional partitioning

When undertaking the analysis of a complex item, it may be necessary to break down the total functionality into more manageable blocks. This is an iterative process in which high level functions are partitioned progressively into lower level functions that combine to form a functional model of the entire item under consideration. It should be noted that there are many ways of undertaking this process and tools are available to help visualize the functional breakdown. Many large organizations have an equipment hierarchy which is already functionally based and is ideal for the basis of the breakdown.

The lowest level in the hierarchy at which functions should be identified is for the item whose maintenance requirements are to be defined by the RCM process. The following clauses dealing with functional failure analysis refer to the items at this level, unless otherwise stated. In general, items at this level are expected to be at a system/unit level (such as a fuel system or pump) rather than component level (such as a bearing).

6.2.2 Development of function statements

All functions of the item should be identified together with a performance standard, which is quantified wherever possible.

All item functions are specific to an operating context; any special factors relating to the operating context of individual items should therefore be documented either against that item or as part of the general statement of operating context within the analysis of the guidelines and assumptions (5.6).

Although an individual item is normally designed to perform a single function, many items may have multiple functions or have secondary functions. Care should be taken in such cases, as these additional functions may only be relevant in specific operating contexts, often in a sub-set of the operating context considered for the primary function or only under "demand" conditions.

Examples of secondary functions could include, but are not limited to:

a) containment of fluids (e.g. water, oil);

b) transfer of structural load;

c) protection;

d) provision of indications to operators via a control system.

The performance standard is the level of performance required of the item to fulfil the stated function of the system in the given operating context; this standard should be stated quantitatively and/or unambiguously to ensure a meaningful analysis. When defining the required standard, the value selected should represent the level of performance essential to achieve the function rather than the capability of the item. For example, the flow rate from a pump should be (400 ± 30) l/min to achieve the correct degree of cooling; however, a standard pump capable of delivering 600 l/min may have been installed. It is the (400 ± 30) l/min which represents the functional requirement. Therefore, this requirement might be expressed as: "To deliver a flow of (400 ± 30) l/min of water".

Functions that provide protective capability should include in their definition a clear statement of the events or circumstances that would activate or require activation of the protective function.

6.3 Requirements for definition of functional failures

All the functional failures associated with each of the defined functions should be identified.

The functional failures listed should always refer to specific functions that have been identified and should be expressed in terms of the failure to achieve the stated item performance standard or standards. The total loss of a function will, normally, always be considered but partial loss may also be relevant and should always be included if the effects of the loss are different to that of total loss.

For example, the pump described above delivering (400 ± 30) l/min will have a functional failure of "fails to deliver any water". In addition, a functional failure described as "pump provides less than 370 l/min" would be valid if the system was such that it could provide a reduced capability at these reduced flow rates.

Functional failures include, but are not limited to

a) complete loss of function,

b) failure to satisfy the performance requirement,

c) intermittent function,

d) functions when not required.

Many other unique functional failures will exist based upon the specific system characteristics and operations requirements or constraints.

This approach makes it possible to differentiate between the consequences of loss of specific functions as it is the loss of function which results in the effects at the highest indenture level.

6.4 Requirements for definition of failure modes

The specific, reasonably likely, physical conditions that cause each functional failure shall be identified.

The failure mode should include the identification of the physical item that has failed and a description of the failure mechanism. For example: "Crack in flange due to fatigue" or "Leaking actuator due to worn seal". The level of detail at which the failure mode is identified shall reflect both the analysis level as a whole and the level at which it is possible to identify a failure management policy.

When listing failure modes, it is important that only those which are “reasonably likely” to occur are included; the definition of “reasonable” should be set as part of the ground rules for the whole RCM analysis and may vary significantly between organizations and applications. In particular, the consequences of failure should be a consideration in that failure modes with a very low probability of occurrence should be included where consequences are very severe.

Failures which are known to have occurred, or are being prevented by an existing preventive maintenance programme, in the given operating context should be included in the analysis. In addition, any other events that may cause functional failure such as operator error, environmental influences and design defects should be included. As RCM addresses all failure management policies, human error may be included; however, if a wider human factor programme is being undertaken it may not be cost effective. If human error is being considered outside of the analysis, the failure modes may be listed for completeness but not subject to any further analysis within RCM. Details concerning which types of human factors are suitable for inclusion in the analysis are outside the scope of this standard.

6.5 Requirements for definition of failure effects

The effects of the functional failure should be identified.

The failure effect describes what happens if the failure mode occurs and generally identifies the effect on the item under consideration, the surrounding items and the functional capability of the end item. The effect described should be that which occurs if no specific task is being performed to anticipate, detect or prevent the failure.

The effect identified should be the most severe effect that can reasonably be expected; again, the definition of “reasonable” should be defined as part of the analysis ground rules.

It is important that the effect description includes sufficient information to enable an accurate assessment of the consequences to be made. The effects on equipment, personnel, the general public and the environment should all be taken into account as applicable.

Most analyses identify effects at the local (i.e. item) level, the next highest indenture level and the end item (i.e. highest indenture level, being the plant, aircraft or vehicle etc. under consideration). The identification of effects at the end item level is necessary when considering the relative importance of failures, as this represents a common reference point for all items.

6.6 Criticality

The application of RCM to every failure mode identified within the failure analysis will not be cost effective in every case. It may therefore be necessary for an organization to employ a logical and structured process for determining which failure modes should proceed through the RCM analysis to achieve an acceptable level of risk.

The method frequently used for this evaluation process is a criticality analysis, which combines severity and rate of occurrence to derive a criticality value representing the level of risk associated with a failure mode. Criticality should cover all aspects of failure consequence, including for example safety, operational performance and cost effectiveness. Annex A shows a typical approach to criticality analysis.

The criticality value is used to identify those failure modes where risk is acceptable, therefore not requiring failure management, and to prioritize or rank those failure modes requiring analysis. For failures where no analysis is required, it is often the case that the failures will be allowed to occur and no active preventive maintenance policy used; however, this decision is dependent upon the organization and its objectives.

7 Consequence classification and RCM task selection

7.1 Principles and objectives

The preventive maintenance programme is developed using a guided logic approach. By evaluating possible failure management policies, it is possible to see the whole maintenance programme reflected for a given item. A decision logic tree is used to guide the analysis process, see Figure 5.

Preventive maintenance consists of one or more of the following tasks at defined intervals:

a) condition monitoring;

b) scheduled restoration;

c) scheduled replacement;

d) failure finding.

Cleaning, lubrication, adjustment and calibration tasks which are required for some systems can be addressed using the group of tasks listed above.

It is this group of tasks which is determined by RCM analysis, i.e. it comprises the RCM based preventive maintenance programme.

Corrective maintenance tasks may result from the decision not to perform a preventive task, from the findings of a condition-based task, or an unanticipated failure mode.

RCM ensures that additional tasks which increase maintenance costs without a corresponding increase in protection of the level of reliability are not included in the maintenance programme. Reliability decreases when inappropriate or unnecessary maintenance tasks are performed, due to increased incidence of maintainer-induced failures.

The objective of RCM task selection is to select a failure management policy that avoids or mitigates the consequences of each identified failure mode, the criticality of which renders it worthy of consideration. Where a maintenance task has been identified, additional information is typically identified as follows:

a) estimates of the man-hours required for the tasks;

b) skill type and level necessary for executing the task;

c) criteria for task interval selection.

Subclause D.3.3 provides details on the interpretation of task analysis as applied to structures. When applying task analysis to structures, the type of structure tends to dictate the maintenance task.

7.2 RCM decision process

The selection of the most suitable failure management policy is guided using a RCM decision diagram and is presented in Figure 5.

The approach used for identifying applicable and effective preventive maintenance tasks is one which provides a logic path for addressing each failure mode. The decision diagram is used to classify the consequences of the failure mode and then ascertain if there is an applicable and effective maintenance task that will prevent or mitigate it. This results in tasks and related intervals which will form the preventive maintenance programme and management actions.

An applicable maintenance task is one that addresses the failure mode and is technically feasible.

An effective maintenance task is one that's worth doing and successfully deals with the consequences of failure.

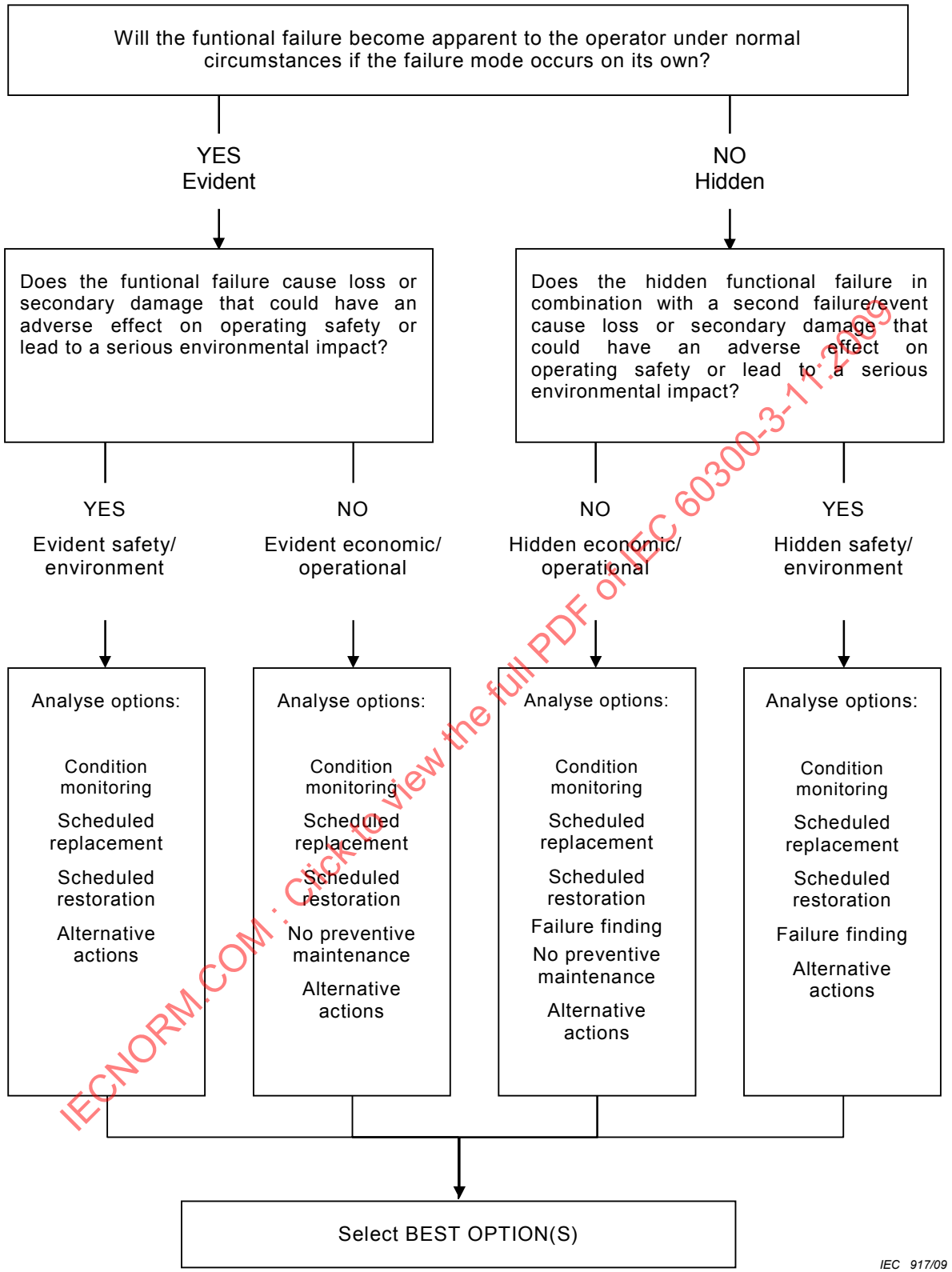


Figure 5 – RCM decision diagram

7.3 Consequences of failure

The process considers each failure mode in turn and classifies it in terms of the consequences of functional failure. These classifications include the following:

a) hidden or evident;

b) safety, economic/operational as identified by the failure analysis.

The classification of whether the failure is hidden or evident, is determined by answering the question, “Will the functional failure become apparent to the operator under normal circumstances if the failure mode occurs on its own?” If the answer to the question is “Yes”, the failure is evident, otherwise the failure is hidden.

The understanding of what is "normal circumstances" is essential to a meaningful RCM analysis and should be captured in the operating context.

The second classification of the failure mode is whether it results in safety/environmental effects, or economic/operational effects.

A failure is deemed to be “safety/environmental” if the effects could harm personnel, the public, or the environment.

If the functional failure does not have an adverse effect on safety or the environment, the failure mode effects are then assessed as being economic/operational. The economic/operational classification refers to functional failure effects that result in degradation of the operational capability, which could be reduced production, mission degradation, failure to complete a journey within the required time, or some other economic impact.

The loss of a hidden function does not, in itself, have any consequences, such as for safety, but it does have consequences in combination with an additional functional failure of an associated stand-by or protected item.

7.4 Failure management policy selection

The next level within the RCM decision process assesses the characteristics of each failure mode to determine the most appropriate failure management policy. There are a number of options available; namely:

a) Condition monitoring

   Condition monitoring is a continuous or periodic task to evaluate the condition of an item in operation against pre-set parameters in order to monitor its deterioration. It may consist of inspection tasks, which are an examination of an item against a specific standard.

b) Scheduled restoration

   Restoration is the work necessary to return the item to a specific standard. Since restoration may vary from cleaning to the replacement of multiple parts, the scope of each assigned restoration task has to be specified.

c) Scheduled replacement

   Scheduled replacement is the removal from service of an item at a specified life limit and replacement by an item meeting all the required performance standards. Scheduled replacement tasks are normally applied to so-called “single-cell parts” such as cartridges, canisters, cylinders, turbine disks, safe-life structural members, etc.

d) Failure-finding

   A failure-finding task is a task to determine whether or not an item is able to fulfill its intended function. It is solely intended to reveal hidden failures. A failure-finding task may vary from a visual check to a quantitative evaluation against a specific performance standard. Some applications restrict the ability to conduct a complete functional test. In such cases, a partial functional test may be applicable.

e) No preventive maintenance

It may be that no task is required in some situations, depending on the effect of failure. The result of this failure management policy is corrective maintenance or no maintenance at all, following a failure.

f) Alternative actions

Alternative actions can result from the application of the RCM decision process, including:

i) redesign;
ii) modifications to existing equipment, such as more reliable components;
iii) operating procedure changes/restrictions;
iv) maintenance procedure changes;
v) pre-use or after-use checks;
vi) modification of the spare supply strategy;
vii) additional operator or maintainer training.

The implementation of alternative actions can be divided into two distinct categories:

1) those that require urgent and immediate action, in particular for failure modes whose occurrence will have an adverse effect on safety or the environment;
2) those that might be desirable when a preventive maintenance task cannot be developed to reduce the consequences of functional failure that affect economic or operations. These should be evaluated through a cost/benefit analysis to determine which option provides the greatest benefit compared to taking no pre-determined action to prevent failure.

The RCM decision diagram in Figure 5 requires consideration of all applicable failure management policies for a given failure mode. The cost of each possible solution plays a significant part in determining which one is ultimately selected. At this point in the analysis, each failure management policy option has already been shown to be appropriate in that it reduces the consequences of failure to an acceptable level. The best option will be determined by the cost of executing that solution and the operational consequences that that option will have on the programme's maintenance operations.

Sometimes no single failure management policy can be found that adequately reduces the probability of failure to an acceptable level. In these cases, it is sometimes possible to combine tasks (usually of differing types) to achieve the desired level of reliability.

7.5 Task interval

7.5.1 Data sources

To set a task frequency or interval, it is necessary to determine the characteristics of the failure mode that suggest a cost-effective interval for task accomplishment. This may be achieved from one or more of the following during the analysis of a new item:

a) prior experience with identical or similar equipment which shows that a scheduled maintenance task has offered substantial evidence of being applicable and effective, see IEC 62308 [10];
b) manufacturer/supplier reliability and test data which indicate that a scheduled maintenance task will be applicable and effective for the item being evaluated, see IEC 62308 [10];
c) reliability data and predictions;
d) assumed failure attributes (e.g. distribution, rate), see IEC 61649 [11] and IEC 61710 [12];
e) life cycle support costs.

In addition to the above, during the analysis of an existing item other sources of information may include:

f) operational and maintenance data (including costs);

g) operator and maintainer experience;

h) age exploration data.

If there is insufficient reliability data, or no prior knowledge from other similar equipment, or if there is insufficient similarity between the previous and current systems, the task interval can only be established initially by experienced personnel using good judgement and operating experience in concert with the best available operating data and relevant cost data.

Mathematical models exist for determining task frequencies and intervals, but these models depend on the availability of appropriate data. Some models are based on exponential distributed data, others on non constant failure rate (IEC 61649) [11] or non constant failure intensity (IEC 61710) [12]. This data will be specific to particular industries and those industry standards and data sheets should be consulted as appropriate.

7.5.2 Condition monitoring

Condition monitoring tasks are designed to detect degradation as functional failure is approached. Potential failure is defined as the early state or condition of the item, indicating that the failure mode can be expected to occur if no corrective action is taken. The potential failure will exhibit a condition or a number of conditions that give prior warning of the failure mode under consideration. Such conditions may include noise, vibration, temperature changes, lubricating oil consumption or degradation of performance.

Condition monitoring can be undertaken manually or by condition monitoring equipment, such as a vibration sensor to measure bearing vibration. When evaluating the condition to be monitored, the life cycle cost of any condition monitoring equipment should be considered, including its own maintenance.

To evaluate the interval for a condition monitoring task it is necessary to determine the time between potential and functional failure. During the degradation process, the interval between the point where the degradation reaches a predetermined level (potential failure) and the point at which it degrades to a functional failure is referred to as the potential failure (P) to functional failure (F) interval, or P-F interval, see Figure 6. Knowledge of the initial condition and the deterioration rate is helpful in predicting when the potential failure and functional failure are likely to occur. This will assist in determining when the initial condition monitoring task should start.

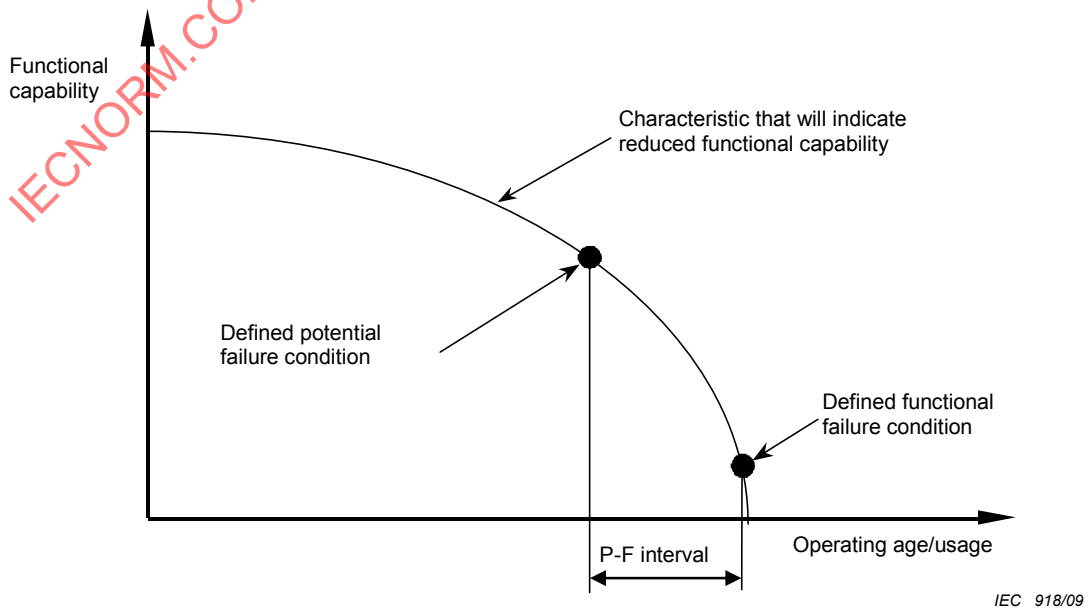


Figure 6 – P-F interval

For a condition monitoring task to be applicable, the following has to be satisfied:

a) the condition has to be detectable;

b) the deterioration needs to be measurable;

c) the P-F interval has to be long enough for the condition monitoring task and actions taken to prevent functional failure to be possible;

d) the P-F interval needs to be consistent.

When there are a number of incipient failure conditions which could be monitored, the analysis should consider the condition which provides the longest lead time to failure and the cost of any equipment and resources required by the potential task.

The interval for the condition monitoring task should be less than or equal to the P-F interval. The relationship between the task interval and P-F interval varies depending on the probability of non-detection the organization is willing to accept and the severity of the failure mode consequences. A task interval equal to half of the P-F interval is typically used, as this potentially provides two chances for the degradation to be detected. When a greater level of protection is desired, some organizations have elected to use smaller fractions of the P-F interval to reduce exposure to safety risks and to protect high value items. The fraction of the P-F interval used for setting the task interval depends on the level of risk and/or cost the organization is willing to accept.

In determining the interval for condition monitoring, the effectiveness of the detection method should be considered. As the effectiveness of the inspection or monitoring technique improves it may be possible to reduce the frequency of the task. Both the successful and unsuccessful identification of potential failure should be recorded.

7.5.3 Scheduled replacement and restoration

The interval for scheduled replacement and restoration tasks is based on an evaluation of the failure mode's safe life or useful life.

For scheduled replacement and restoration tasks which address safety effects, there should be a safe life (i.e. items are expected to survive to this age – see IEC 61649). The safe life can be established from the cumulative failure distribution for the item by choosing a replacement interval which results in an extremely low probability of failure prior to replacement.

Where a failure does not cause a safety hazard, but causes loss of availability, the replacement interval is established in a trade-off process involving the cost of replacement components, the cost of failure and the availability requirement of the equipment.

Useful life limits are used for items whose failure modes have only economic/operational consequences. A useful life limit is warranted for an item if it is cost-effective to remove it before it fails. Unlike safe life limits, which are set conservatively to avoid all failures, useful life limit may be set liberally to maximize the item's useful life and, therefore, may add to the risk of an occasional failure. An item with a steadily increasing conditional probability of failure may support an economic life limit, even without a well defined wear-out age, if the benefits of restoration, e.g. a lower probability of failure, exceed the cost.

Scheduled replacement and restoration tasks can be useful where one or more key items have a clear wear out pattern (see Annex C patterns A and B). Using the Weibull distribution the shape parameter (β), the characteristic life (ή) and the time to first failure (t_0) may be estimated. For items that have a significant time to the first failure (t_0) a scheduled replacement or restoration just before t_0 should be considered. Even for a two parameter Weibull (t_0=0) scheduled replacement and restoration can be performed at a curtain predicted percentage of failures such as 1% (often called L1 or B1) or 10% (often called L10 or B10), see IEC 61649.

7.5.4 Failure finding

Failure-finding tasks are only applicable to hidden failures and are only applicable if an explicit task can be identified to detect the functional failure. A failure-finding task can either be an inspection, function test or a partial function test to determine whether an item would still perform its required function if demanded. Failure-finding is relevant where functions are normally not required, for example in case of redundancy or safety functions that are only seldom activated.

A failure-finding task will be effective if it reduces the probability of a multiple failure to an acceptable level. Annex B provides guidance on methods for determining task intervals for failure-finding tasks.

8 Implementation

8.1 Maintenance task details

The tasks generated as a result of the RCM analysis need additional details before they can be implemented in line with the maintenance concept. Information concerning the task details might include, but is not limited to

a) time to undertake the task,
b) skills and minimum number of people required at each maintenance echelon,
c) procedures,
d) health and safety considerations,
e) hazardous materials,
f) spares at each maintenance echelon,
g) tools and test equipment,
h) packaging, handling, storage and transportation.

In determining this information, it may be necessary to review the assumptions made in selecting the most effective task.

8.2 Management actions

Where the RCM analysis has resulted in a re-design, an operational restriction or a procedural change, a process should be considered for determining the priority of these opportunities. This process should consider the following:

a) effect on safety of the failure mode effects;
b) effect on availability and reliability;
c) cost benefit analysis;
d) likely success of any action.

For items already in service for which no applicable or effective task can be implemented for a failure mode with safety consequences, a temporary action is required until a permanent solution can be effected. Examples of this might include: operational restrictions, temporary redesigns, procedural changes or the implementation of maintenance tasks previously discarded.

8.3 Feedback into design and maintenance support

Maximum benefit can be obtained from an RCM analysis if it is conducted at the design stage so that feedback from the analysis can influence design. The use of a functional failure analysis enables RCM to be undertaken early in the design process. This means that in

addition to design modifications to eliminate failures that cannot be managed by preventive maintenance, the design can be influenced to optimize the support strategy.

The failure identification process and RCM analysis enable the whole range of expected maintenance tasks to be identified and hence permit support planning to be initiated. The identified maintenance tasks will produce the information needed to analyse support activities such as the provisioning of spares, level of repair analysis (LORA), requirements for tools and test equipment, manpower skill levels, and the requirement for facilities necessary to support the derived maintenance concept.

The integrated logistic support (ILS) management method brings these support activities together with customer requirements in a structured manner and is described in IEC 60300-3-12. The whole ILS process and the position of the RCM decision process within ILS is presented in Figure 7.

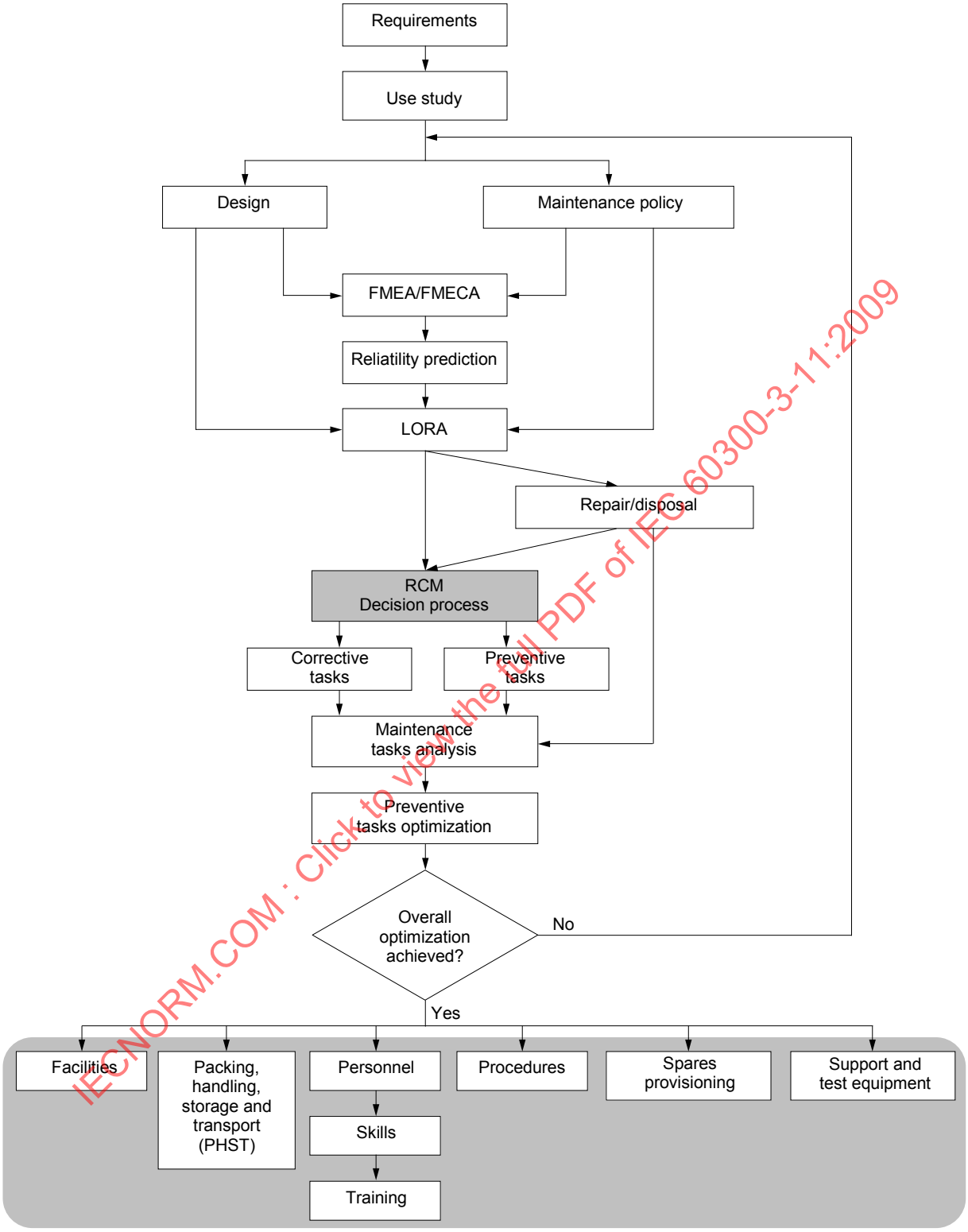


Figure 7 – ILS management process and relationship with RCM analysis

8.4 Rationalization of tasks

The output from the RCM analysis may be many tasks at many different frequencies. The tasks should be rationalized to generate the maintenance schedule for the item by removing duplications and by the alignment of task intervals. This process should be conducted with great care, such that any changes in interval do not compromise safety or the environment, or significantly degrade the operational capability.

The first stage in this process is to identify the staff that will undertake the tasks. This will require identifying the trade and the level at which maintenance will be undertaken, for example, by the operator, a maintainer, a remote workshop or by the original equipment manufacturer.

The tasks should be categorized by trade and level and then subject to a series of rationalization rules.

The task intervals produced by the RCM analysis are based on the P-F intervals, safe and useful life or the calculation of failure free intervals. The tasks will not automatically align and some manipulation will be necessary to generate a realistic maintenance schedule with acceptable levels of downtime for preventive maintenance. As illustrated in Figure 8, moving the task intervals to the left increases cost, moving them to the right increases risk. When reducing the task interval, consideration should be given to the cost, safety and environmental impact of conducting the task at the increased frequency.

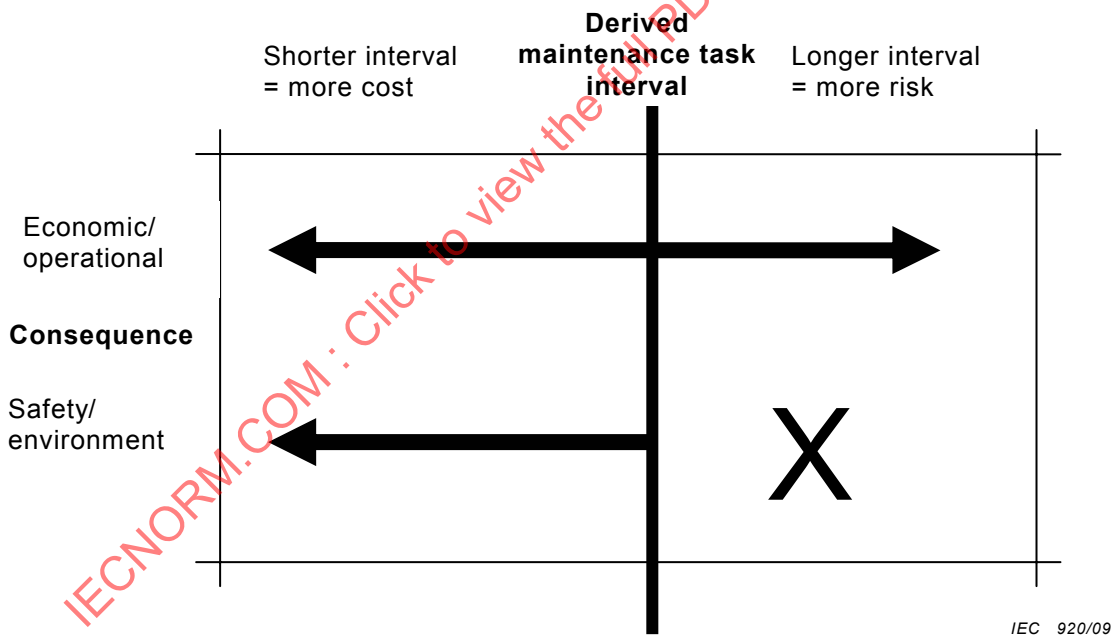


Figure 8 – Risk versus cost considerations for rationalization of tasks

Rationalization is achieved by converting individual derived task intervals to a common time base and then aligning their frequencies to achieve the optimum item maintenance schedule. The rationalization process should initially consider areas where there is less flexibility, e.g. failures with safety or environment consequences and maintenance that requires shutdown. Economic/operational tasks should then be overlaid to identify mismatches. However, it may not be possible to rationalize some tasks and it may be necessary to return to the original analysis.

Tasks that, during the task selection process, have been rejected for operational/cost reasons should be reconsidered as they could be effective in conjunction with other tasks. In particular,

a potential task might be rejected due to restricted access, but in conjunction with other tasks the task may be justified.

An item will have some maintenance tasks with derived intervals which are time based and others that are usage based. If there is a close alignment between time and usage, rationalization should consider selecting either a time or a usage based maintenance schedule. However, if this approach is taken, the operator should monitor usage and ensure that the correlation between time and usage is maintained.

Following the rationalization process, any modified task intervals should be recorded within the original reviews such that both the derived and rationalized intervals are recorded.

8.5 Implementation of RCM recommendations

Every effort should be made at the beginning of the development of a maintenance programme to institute a procedure for documenting electronically the results of the RCM analysis and all in-service modifications. Commercial software, particularly in the field of ILS, is available to document, throughout the life of the equipment, important background information used in the decision-making process which, for example, assists in determining why a task was put in place or later modified.

The RCM based maintenance programme can be implemented in specific detail in the maintenance plans.

The initial maintenance programme is based on the best possible information available before the equipment goes into service. The maintenance requirements generated by the initial maintenance programme may be unique to individual users and may require applicable regulatory authority approval.

The clauses above describe the development of the item maintenance schedule. However, external factors to maintenance have an influence on the implementation, such as manpower resource limitations, availability of facilities and changing operational requirements.

8.6 Age exploration

The purpose of age exploration is to systematically evaluate an item's maintenance task interval based on analysis of collected information from in-service experience to determine the optimum maintenance task interval. Age exploration is normally directed at specific tasks and includes the collection of data for any default or uncertain inputs for the RCM process, in order to refine tasks, intervals or calculations. This may result in tasks whose only purpose is to collect data.

Two common methods can be used to generate data for age exploration programmes, as follows:

a) lead concept: the first few items entering service are used extensively. This allows the early identification of dominant failure modes as well as wear out patterns (see Annex C). It identifies design problems quickly;

b) sample data collection: a sample of a population system is closely monitored.

8.7 Continuous improvement

RCM will only achieve its objective with further development. This standard therefore provides guidance on continuous maintenance improvement. Figure 9 illustrates the four main components of the cycle.

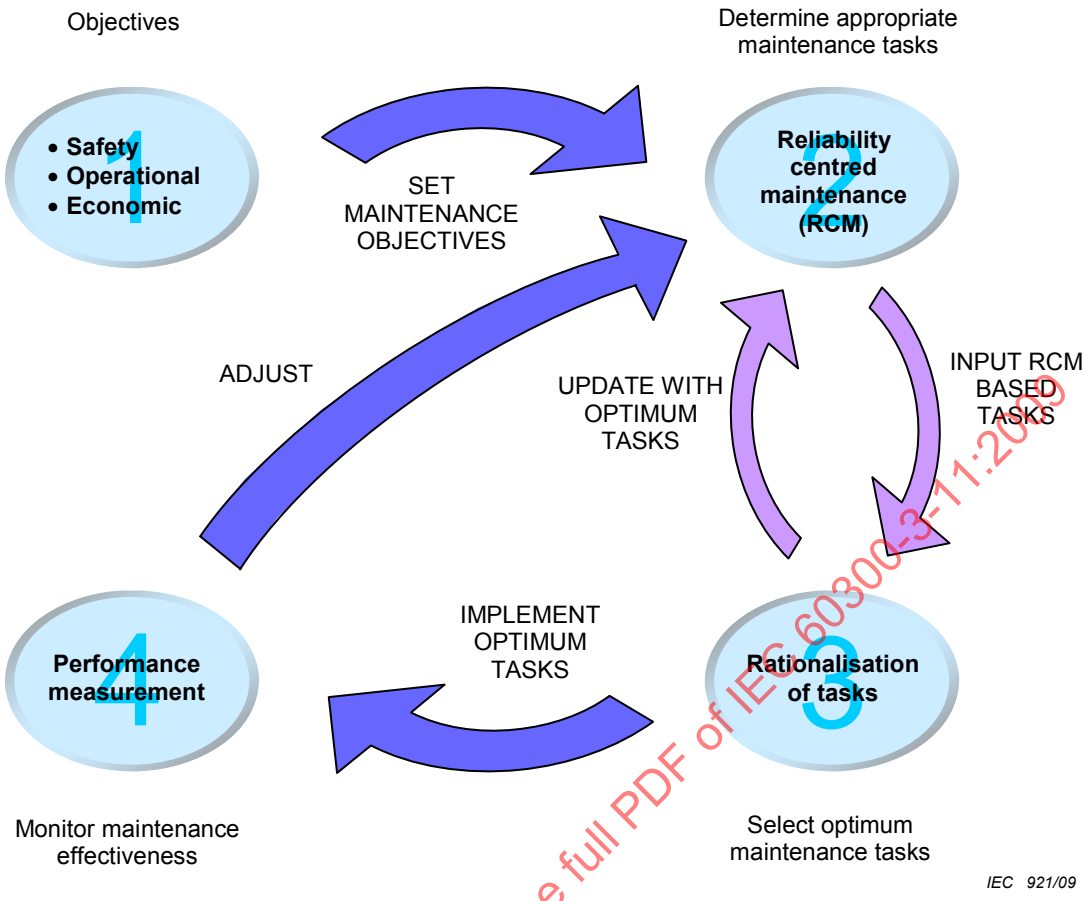


Figure 9 – RCM continuous improvement cycle

The operating context and assumption statements should be considered as living documents and be maintained throughout the item's life. They should be reviewed regularly as item configuration or operation demands change. Changes in the operating context may result in changes to selected maintenance tasks or intervals.

Once the maintenance schedule has been derived, it will need to be reviewed periodically to take into account the maintenance data feedback acquired on the implemented RCM analysis and also the requirement for system upgrades.

Any system modifications, unique repairs or configuration changes should be subject to an RCM analysis. They may not actually result in any changes to the maintenance programme, but the changes in the system functions should be documented in the operating context statement and failure analysis. However, a significant change in the item or its operation could result in a completely different maintenance programme.

8.8 In-service feedback

The initial maintenance programme evolves each time it is revised by the operating organization, based on the experience gained and in-service failures that result from operating the equipment.

To make these revisions throughout the life of the equipment, the operating organization should be able to collect in-service maintenance data throughout the equipment operating life, such as:

a) failure times and dates;

b) causes of failure;

c) maintenance times;

d) inspection efficiency;

e) utilization;

f) cost.

Degradation rates and support requirements can also be determined by monitoring the condition of specific components. Experience can then be used to improve the maintenance programme by examining how effective a task is, by considering its frequency, and by measuring its cost against the estimated cost of the failure it prevents.

Feedback on the performance of the derived RCM maintenance schedules should be acquired from the data collected by the organization's maintenance management system or equivalent and personnel where appropriate. This information should provide the feedback of the success on the derived intervals and details of the condition of items following condition monitoring, scheduled replacement and restoration tasks and the outcome of failure-finding tasks. It is important that the structure and content of the maintenance management system is carefully selected to ensure it provides appropriate data for future analysis. Dependability data from the field should be collected in accordance with the guidance given in IEC 60300-3-2.

Annex A
(informative)

Criticality analysis

A.1 General

Criticality analysis is performed to rank failure modes according to the risk they represent for the organization, covering safety, environmental, operational and economic consequences. For this reason, all elements within the analysis should be chosen and defined in a way that is meaningful to the organization and is specifically applicable to the analysis being undertaken. This means that, even within one organization, the definitions and assumptions may differ between analyses; they should however, be consistently applied within any one analysis and be established prior to the analysis.

Criticality is a measure of risk and hence is a combination of consequence and likelihood. The first stage in the analysis is therefore to define the range of consequences and likelihood that are relevant to the item being considered; in this case, "item" refers to that at the highest indenture level, for example building, offshore platform, aircraft, vessel etc.

A.2 Consequence categorization

The types of consequence and their severity should be defined in terms that are relevant to the item under consideration and divided into a sufficient number of categories to enable the complete range of effects to be classified and adequately separated.

Typically, consequences may be described in terms of safety and financial effects of failure but other consequences, such as environmental damage may also be relevant. In many cases, consequences specific to the item or industry may be included, for example measures of passenger delay or building occupancy comfort.

The severity of the consequence is categorized into, normally, at least four levels. An example addressing safety and operational consequences is provided below:

a) Category 1: Catastrophic (failure resulting in death of personnel, power plant shut down for more than 1 week);

b) Category 2: Major (failure resulting in hospitalization or loss of limb, power plant shut down for more than 1 day and less than 1 week);

c) Category 3: Marginal (failure resulting in injury requiring hospital treatment, power plant shut down for less than 1 day);

d) Category 4: Minor (failure resulting in injury requiring no more than first aid treatment, reduced output from power plant).

For some analyses, significantly more levels may be needed to distinguish between meaningful levels of consequence, although fewer than this is rarely required.

The categories should be defined for each consequence type so that the severity levels for each would require the same level of action from the organization. Thus, for example, a financial consequence category 1 would most likely be extremely high in order to equate with the safety category 1 above.

A.3 Likelihood categorization

The likelihood of each failure mode is categorized into bands according to their mean time between failure (MTBF), probability or other likelihood measure. The definition of each band and the number of bands required will be dependent upon the items under analysis and their operating context. Typically five bands are defined for likelihood, for example:

a) Category A: Frequent (e.g. more than one occurrence in an operating cycle);

b) Category B: Likely (e.g. one occurrence in an operating cycle);

c) Category C: Occasional (e.g. more than one occurrence in the item's life);

d) Category D: Unlikely (e.g. one occurrence in twice the item's life);

e) Category E: Remote (e.g. one occurrence in more than twice the item's life).

The allocation of these bands may be by use of applicable reliability data, engineering judgement of the design team or other methods. Whichever approach is used, it is essential that it is consistently applied so that the relative frequency of failure modes is accurately assessed.

The number and meaning of each band should be determined according to the organization's needs and the reliability of the equipment; for example, with highly reliable systems the "frequent" categorization may be equivalent to one failure in several years.

A.4 Use of failure data

When assessing likelihood of failure for criticality analysis, values of failure rate or failure intensity are often calculated from in-service data or vendor or manufacturer data. Where this is the case, the FMECA should clearly record the sources of data and any assumptions made (see IEC 62308 [10] and IEC 61709 [13]).

It is necessary to ensure that failure rate or failure intensity data represent the failure modes as if there are no preventive maintenance tasks in place. Values derived from in-service data may need to be adjusted to compensate for the influence that preventive maintenance tasks have on the failure rate or failure intensity or the differences in equipment design or operational context.

Particular care should be taken when using in-service data to calculate failure rate or failure intensity for a number of reasons:

a) the occurrence of one failure mode may cause a corrective action which prevents the occurrence of other failure modes. For example, removing an assembly for repair may correct as yet undetected or incipient failure modes;

b) the data may include the effects of a current or past preventive action;

c) items or functions may be dormant for extended periods of time, so that failures which occur during this period may not become evident until the item is activated, causing the failure rate/failure intensity to appear to be longer than the true value;

d) equipment design, operating environment, maintenance processes and other factors may have changed during the in-service period so altering the observed failure rate.

A.5 Criticality categories

Criticality categories are defined in terms of a combination of consequence and likelihood categories and are set so that failure management policies can be clearly linked to each criticality value.

The number of levels required will be determined by the organization's requirements and the analysis application. An example of a three-level criticality categorization would be

1) undesirable,
2) acceptable,
3) minor.

The allocation of each of these to a consequence/likelihood combination is normally, and most simply expressed, in terms of a matrix; an example is presented in Table A.1.

Table A.1 – Example of a criticality matrix

Likelihood	Category	Consequence			
		Catastrophic	Major	Marginal	Minor
		1	2	3	4
Frequent	A	1	1	2	2
Likely	B	1	2	2	3
Occasional	C	2	2	3	3
Unlikely	D	2	3	3	3
Remote	E	3	3	3	3

A.6 Application of criticality analysis

Criticality analysis is normally used to guide the application of RCM and the alternative actions to be taken when no applicable and effective failure management policy can be found.

The exact usage will be dependent upon the organization's needs and the items to which the analysis is applied; more than three categories may be needed in some cases, but less than this is unlikely to give meaningful results.

For example, an organization may decide that failures which are given the lowest criticality value (3 in this example) are not subjected to the RCM decision logic and a non-analytically based failure management policy will be applied.

Failure modes with the highest criticality category will typically be subject to mandatory re-design if no applicable and effective failure management policy can be found as the impact on the organization is significant.

The approach to be taken in the case of other categories will vary between organizations. In the example given above, it is likely that failure modes with a criticality value of 2 will be subject to RCM but where the resulting failure management policy indicates that it is acceptable to allow the failure to occur, no further action need be taken.

Annex B
(informative)

Failure finding task intervals

B.1 General

There are a number of different ways of determining the task interval for a failure finding task. Annex B presents a number of examples. The methods in this annex are applicable for the hidden failure case (see Figure 5). In this case, the task is to estimate the probability that a hidden failure will cause the function to fail if/when it is demanded. This is used, for example, in the safety integrity level (SIL) method where it is required to estimate the probability that a safety function will fail if/when its function is required (failure on demand). The method is also applicable to estimate the probability of loss of redundancy in a redundant system. For simplicity and in order to make a safe (conservative) estimate, the exponential distribution i.e. constant failure rate/ failure intensity is often used. In case of increasing failure rate (wear out) this will result in a conservative estimate. The exponential failure rate often expressed as an MTBF or MTTF is then used to compute the probability that the "hidden" function has failed when it is demanded. The worst case is of course for a failure to occur just before the inspection. In this way, the failure finding interval can be estimated.

B.2 Task intervals based on availability and reliability

Andrews and Moss [3] show that there is a linear correlation between the unavailability, the failure-finding interval and the reliability of the protective function as given by its MTBF, as follows:

$$\text{Unavailability} = 0{,}5 \times \frac{FFI}{MTBF_{pv}} \tag{B.1}$$

where

FFI is the failure finding interval;

$MTBF_{pv}$ is the MTBF of the protective function.

This linear relationship is valid for unavailabilities of less than 5 %, provided that the protective function conforms to an exponential survival distribution. This is because the formula is based on an approximation of the exponential distribution.

The unavailability of the protective function above does not include unavailability caused by the need to restore the function if it is found to have failed. However, the time to perform the failure finding task and make any repair is likely to be small when compared to the unrevealed unavailability between tasks.

B.3 SAE JA1012 method

SAE JA1012 [4] provides Equation (B.2) which considers the reliability of the protective function, protected function and the probability of multiple failures:

$$FFI = \frac{2 \times MTBF_{pv} \times MTBF_{pt}}{PR_{mf}} \tag{B.2}$$

where

$MTBF_{pt}$ is the MTBF of the protected function;

$MTBF_{mf}$ is the MTBF of a multiple failure.

PR_{mf} is the probabiltity of a multiple failure

B.4 NAVAIR 00-25-403 method

NAVAIR 00-25-403 [5] provides the following process, based on the probability of multiple failure, hidden failure and the additional failure.

Equation (B.3) can be used to model the probability of multiple failure condition:

$$P_{mf} = P_h \times P_{add} \quad \text{(B.3)}$$

where

P_{mf} is the probability of multiple failure occurring;

P_h is the probability of hidden failure occurring;

P_{add} is the probability of additional failure occurring.

Assuming a random failure distribution for P_h and P_{add}, Equation (B.4) can be used to model these probabilities by establishing the probability over time:

$$P = 1 - e^{\frac{-t}{MTBF}} \quad \text{(B.4)}$$

where

P is the probability over the time period;

t is the time period;

$MTBF$ is the mean time between failures.

The desired MTBF for the function (i.e. multiple failure) can be established by setting an acceptable probability of failure over a known time frame (e.g. life of the item) and solving for MTBF. If the MTBF for the hidden and additional failure (or event) can be determined (or estimated), the equation is easily solved by iterating the two equations on a spreadsheet to find the appropriate time period (t), which becomes the inspection interval.

Annex C
(informative)

Failure patterns

Figure C.1 below presents the 6 dominant failure patterns. Scheduled replacement and scheduled restoration tasks are used to mitigate age-related failures, as presented by the failure patterns A, B and C presented below. The conditional probablity of failure does not increase with time in failure patterns D, E and F, and alternative failure management policies should be used.

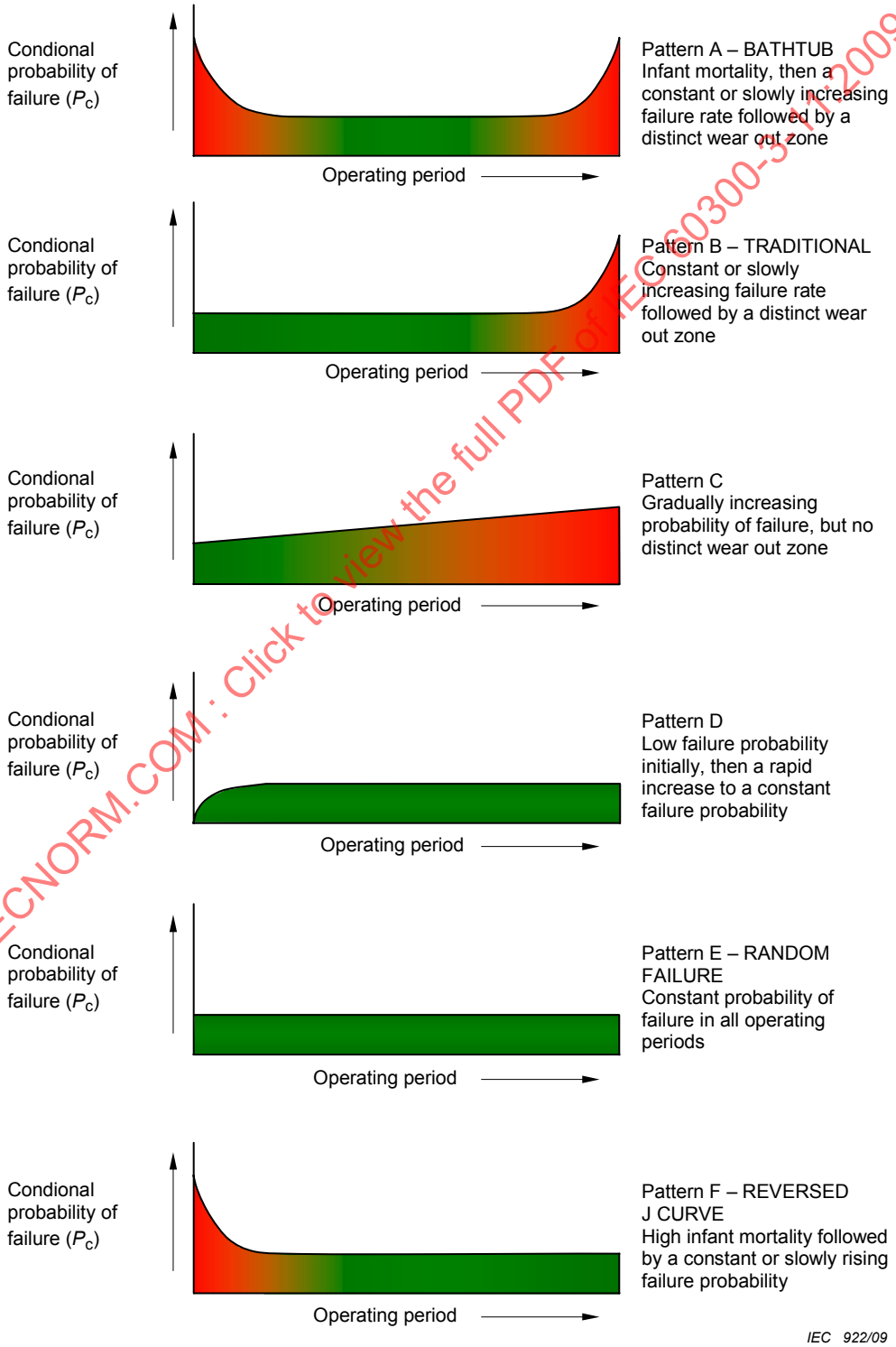


Figure C.1 – Dominant failure patterns

Research into failure patterns revealed that the majority of failures in modern complex equipment/systems are not age related. Table C.1 below illustrates the frequency of occurrence of each failure pattern found by various research activities.

Table C.1 – Failure pattern categories and frequency of occurrence

	Data source (bibliographic references)			
Failure pattern	**Broberg 1973 [7]** %	**UAL 1978 [6]** %	**MSP 1982 [8]** %	**SUBMEPP 2001 [9]** %
A	3	4	3	2
B	1	2	17	10
C	4	5	3	17
D	11	7	6	9
E	15	14	42	56
F	66	68	29	6

Annex D
(informative)

Application of RCM to structures

D.1 General

The objective of Annex D is to illustrate how the RCM process described in this standard is applied to structures.

This annex contains guidelines for developing failure management policies for all structures (including aviation, marine, land, civil and space systems). Once these policies are established, a maintenance programme is determined which will assure continued safe operation throughout the structure's life.

D.2 Structures

D.2.1 Classification

For analysis purposes, the structures consist of all load-carrying parts (including those for fluid pressure, propulsion, and dynamic loads). These parts include pressure vessels, pressure tubes, hangers, civil structures, vehicle frames, suspensions, hulls, as well as aircraft components etc., and related points of attachment.

There are two failure management philosophies for structures, safe life and damage tolerant. They are differentiated by

a) what happens when one or more elements fails,

b) the deterioration rate (e.g. crack propagation).

D.2.2 Safe life structures

Safe life structure is designed to be free from failure during its operational life. It is characterized by the following features:

a) failure of one or more structural elements results in complete loss of function;

b) rapid progression from potential to functional failure (e.g. the crack propagation rate is too fast to allow inspection before failure).

Failure management is achieved in two ways:

1) by building the structure with a large margin of strength above the expected loads;

2) by limiting use of the structure to a life less than that for which the structure was tested or analysed.

D.2.3 Damage-tolerant structures

A damage-tolerant structure is designed to be resistant to the effects of damage during its operational life. It is characterized by the following features:

a) failure of part of the structure does not result in complete loss of function;

b) gradual progression from potential to functional failure (e.g. the crack propagation rate allows for inspection before failure).

A typical damage-tolerant design requirement is that, after a single primary structural failure, the equipment as a whole should withstand a significant percentage of its design loading without functional failure. The percentage should be defined and documented in the design requirements and for RCM purposes presented in the guidelines for the analysis.

Failure management is achieved in three ways:

a) by using multiple load paths;

b) by choosing materials that exhibit gradual deterioration (e.g. application of protective coatings);

c) by using a deterioration inhibiting design (e.g. crack arresting design).

D.3 Structural maintenance programme development

D.3.1 General

The structural maintenance programme is based on an assessment of structural design information and analysis, fatigue and damage tolerance evaluations, service experience with similar structure and relevant test results.

The assessment of the structure for selection of maintenance tasks should be performed as follows:

a) functional failure analysis;

b) maintenance task selection.

A prerequisite for performing functional failure analysis is to perform static and/or dynamic analyses of the structure.

D.3.2 Functional failure analysis

The functional failure analysis is performed in accordance with Clause 6 of this standard, together with the following individual steps:

a) functions are described in terms of the load requirements (e.g. to support a single point load of 100 N, or to support a distributed load of 10 N/mm^2);

b) functional failures are described as loss or partial loss of the load-carrying ability defined by the functions;

c) failure modes describe the mechanisms which result in the functional failure. The failure modes should be described as in 6.4;

d) failure effects should be described in terms of the

   i) loss of function,

   ii) reduction of residual strength,

   iii) multiple location damage.

D.3.3 Maintenance task selection

The maintenance task selection is performed in accordance with Clause 7 of this standard, together with the following individual steps:

a) consequence identification which considers each failure mode in turn and classifies it in terms of the consequences of failure. These classifications include the following:

   i) is the structural failure hidden or evident?

   ii) are the consequences safety related or economic/operational?

b) assessment of the characteristics of each failure mode to determine the most appropriate failure management policy.

For safe life structure, the appropriate failure management policy is typically a scheduled replacement. When the replacement interval exceeds the operational life effectively, no action will be required.

For damage-tolerant structures, there are a number of appropriate failure management policies which should be selected using the RCM decision diagram in Figure 5 and the process described in Clause 7.

Bibliography

[1] ATA-MGS-3:2003, Operator/Manufacturer Scheduled Maintenance Development

[2] ISO 9000, Quality management systems – Fundamentals and vocabulary

[3] ANDREWS, J.D. and MOSS, T.R., Reliability and Risk Assessment. Longman, Harlow, Essex, UK, 1993

[4] A Guide to the Reliability-Centred Maintenance (RCM) Standard, SAE JA1012, January 2002

[5] Guidelines for the Naval Aviation Reliability-Centred Maintenance Process, Navair 00-25-403, 1 March 2003

[6] NOWLAN, F.S. and HEAP, H.F. (1978). Reliability-Centered Maintenance. Report AD/A066-579, National Technical Information Service, US Department of Commerce, Springfield, Virginia. (UAL-DOD)

[7] Broberg Study under NASA sponsorship (reported in 1973) and cited in Failure Diagnosis & Performance Monitoring Vol. 11 edited by L.F. Pau, published by Marcel-Dekker, 1981

[8] MSP Age Reliability Analysis Prototype Study by American Management Systems under contract to U.S. Naval Sea Systems Command Surface Warship Directorate reported in 1993 but using 1980's data from the Maintenance System (Development) Program

[9] SUBMEPP reported in 2001, using data largely from 1990s, summarized in "U.S. Navy Analysis of Submarine Maintenance Data and the Development of Age and Reliability Profiles": 2001, Tim Allen, Reliability Analyst Leader at Submarine Maintenance Engineering, Planning and Procurement (SUBMEPP) a field activity of the Naval Sea Systems Command at Portsmouth NH

[10] IEC 62308, Equipment reliability – Reliability assessment methods

[11] IEC 61649, Weibull analysis

[12] IEC 61710, Power law model – Goodness-of-fit tests and estimation methods

[13] IEC 61709, Electronic components – Reliability - Reference conditions for failure rates and stress models for conversion

[14] IEC 61164, Reliability growth – Statistical test and estimation methods

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 60300-3-11 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Cette deuxième édition annule et remplace la première édition, publiée en 1999, et elle constitue une révision technique.

L'édition précédente était basée sur l'ATA[1]-MG-3; tandis que la présente édition est applicable à toutes les industries et elle définit un algorithme révisé du MBF et une méthode pour le processus d'analyse.

---

1 The Air Transport Association of America.

Le texte de cette norme est issu des documents suivants:

FDIS	RVD
56/1312/FDIS	56/1320/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Une liste de toutes les parties de la série CEI 60300, sous le titre général *Sûreté de fonctionnement,* est disponible sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

La maintenance basée sur la fiabilité (MBF) est une méthode pour identifier et sélectionner les politiques de gestion des défaillances permettant d'atteindre réellement et efficacement la sécurité, la disponibilité et le fonctionnement à l'optimum économique requis. Les politiques de gestion des défaillances peuvent inclure des activités de maintenance, des modifications opérationnelles, des modifications de conception et d'autres actions afin de réduire les conséquences d'une défaillance.

La MBF fut initialement développée à la fin des années 1960 pour l'industrie aéronautique civile et elle a eu pour résultat la publication de l'ATA-MGS-3[1][2]. La MBF est désormais une méthodologie démontrée et acceptée, utilisée dans de larges domaines de l'industrie.

La MBF fournit un processus décisionnel destiné à identifier des exigences efficaces en matière de maintenance préventive ou des actions de gestion applicables pour des équipements, en fonction des conséquences opérationnelles et économiques ainsi que des conséquences sur la sécurité liées à chaque défaillance identifiable et à chaque mécanisme de dégradation responsable de ces défaillances. Le résultat final obtenu grâce à l'emploi du processus constitue un jugement sur la nécessité d'effectuer une opération de maintenance ou des alternatives de conception pour effectuer des améliorations.

Les étapes fondamentales d'un programme de MBF sont les suivantes:

a) début et planification;

b) analyse des défaillances fonctionnelles;

c) sélection des tâches;

d) mise en œuvre;

e) amélioration continue.

Toutes les tâches sont fondées sur des considérations relatives à la sécurité tant du personnel que de l'environnement et d'ordre opérationnel ou économique. Toutefois, il convient de noter que les critères pris en considération dépendent de la nature du produit et de ses applications. Par exemple, un processus de production doit être économiquement viable et peut être sensible à des considérations strictes relatives à l'environnement, alors qu'il convient qu'un matériel de défense soit fiable en opération mais peut supporter des critères de sécurité, économiques et environnementaux moins sévères.

Une analyse de MBF peut conduire à un bénéfice maximal si elle est conduite à l'étape de la conception de sorte que le retour de l'analyse peut influencer la conception. Cependant la MBF est aussi judicieuse en phases opérationnelles et de maintenance pour améliorer les tâches de maintenance existante et faire les modifications nécessaires ou mettre en place des alternatives.

La réussite de l'application de la MBF nécessite la connaissance des équipements et des structures, de l'environnement opérationnel, du contexte en exploitation et des systèmes associés ainsi que la compréhension de leurs défaillances et des conséquences de celles-ci. Le bénéfice le plus grand peut être obtenu quand l'analyse est menée là où les défaillances auraient des effets sévères sur la sécurité, l'environnement, l'économie ou l'exploitation.

---

2 Les chiffres entre crochets se réfèrent à la bibliographie.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité

1 Domaine d'application

La présente partie de la CEI 60300 fournit des lignes directrices permettant l'élaboration d'une politique de gestion des défaillances pour des équipements et des structures, fondée sur une analyse de maintenance basée sur la fiabilité (MBF).

Cette partie sert comme guide d'application et est un prolongement des CEI 60300-3-10, CEI 60300-3-12 et CEI 60300-3-14. Les activités de maintenance recommandées dans les trois normes et qui se rapportent à la maintenance préventive peuvent être mises en œuvre en utilisant la présente norme.

La méthode MBF peut être appliquée à des entités telles que des véhicules terrestres, des bateaux, des centrales électriques, des avions, et d'autres systèmes, qui sont constituées d'équipements et de structures, tels qu'une construction, une structure d'avion ou la coque d'un bateau. Généralement, un équipement comprend un certain nombre de systèmes électriques, mécaniques, d'instrumentation ou de commande et des sous-systèmes qui peuvent encore être décomposés en sous-ensembles de plus en plus petits, selon le besoin.

La présente norme concerne seulement l'application des techniques de MBF et ne comprend pas les aspects relatifs au support de maintenance qui sont traités dans les normes mentionnées ci-dessus ou dans d'autres normes de sûreté de fonctionnement et de sécurité.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60050-191 :1990, *Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-3-2, *Gestion de la sûreté de fonctionnement – Partie 3-2: Guide d'application – Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*

CEI 60300-3-10, *Gestion de la sûreté de fonctionnement – Partie 3-10: Guide d'application – Maintenabilité*

CEI 60300-3-12, *Gestion de la sûreté de fonctionnement – Partie 3-12: Guide d'application – Soutien logistique intégré*

CEI 60300-3-14, *Gestion de la sûreté de fonctionnement – Partie 3-14: Guide d'application – Maintenance et support de maintenance*

CEI 60812, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes et les définitions de la CEI 60050-191et ceux qui suivent s'appliquent.

3.1 Définitions

3.1.1
évaluation de l'effet du vieillissement
évaluation systématique d'un élément fondée sur une analyse des données tirées de l'expérience en exploitation, afin de déterminer l'intervalle optimum entre les tâches de maintenance

NOTE L'évaluation estime la résistance de l'élément au processus de détérioration dû au vieillissement ou à l'utilisation.

3.1.2
criticité
sévérité de l'effet d'un écart par rapport à la fonction spécifiée de l'entité, par rapport aux critées d'évaluation spécifiés

NOTE 1 Le prolongement des effets considérés peut être limité à l'entité ou au système à laquelle est appartient ou au delà des frontières du système

NOTE 2 L'écart peut être une panne, une défaillance, une dégradation, une température excessive, une pression excessive, etc.

NOTE 3 Dans certaines applications l'évaluation de la criticité peut inclure d'autres facteurs tels que la probabilité d'apparition de l'écart, la probabilité de détection.

3.1.3
tolérant aux dommages
capable de supporter des dommages et de continuer à fonctionner comme il est requis, éventuellement à charge ou capacité réduite

3.1.4
défaillance (d'une entité)
cessation de l'aptitude d'une entité à accomplir la fonction requise

3.1.5
effet d'une défaillance
conséquence d'un mode de défaillance en termes d'exploitation, de fonctionnement ou d'état de l'entité

3.1.6
politique de gestion des défaillances
activités de maintenance, modifications opérationnelles, modifications de conception ou toute autre action dans le but de réduire les conséquences d'une défaillance

3.1.7
fonction
destination prévue d'un élément, telle que décrite par une norme requise d'aptitude à la fonction

3.1.8
mode de défaillance
manière dont se produit une défaillance

NOTE Un mode de défaillance peut être défini par la perte de la fonction ou le changement d'état qui survient.

3.1.9
tâche relative à la détection d'une défaillance
inspection programmée ou essai spécifique utilisé pour déterminer si une défaillance cachée spécifique s'est produite ou non

3.1.10
défaillance fonctionnelle
réduction de l'aptitude à la fonction sous le niveau requis

3.1.11
mode de défaillance caché
mode de défaillance dont les effets ne sont pas visibles par l'opérateur dans des circonstances normales

3.1.12
niveau d'intervention
niveau de subdivision d'une entité du point de vue des opérations de maintenance

NOTE 1 Par exemple, des niveaux d'intervention peuvent être un sous-système, une carte électronique, un composant.

NOTE 2 Le niveau d'intervention dépend de la complexité de la construction de l'entité, de l'accessibilité aux sous-systèmes, du niveau de compétence du personnel de maintenance, des installations d'essai, de considérations de sécurité, etc.

[VEI 191-07-05 :1990, modifiée]

3.1.13
inspection
identification et évaluation de la condition réelle par rapport à une spécification

3.1.14
opération de maintenance
tâche de maintenance
succession d'actions élémentaires de maintenance effectuées dans un but donné

NOTE Des exemples d'opérations de maintenance sont le diagnostic de panne, la localisation de panne, la vérification de fonctionnement, ou leurs combinaisons.

3.1.15

entité
tout élément, composant, dispositif, sous-système, unité fonctionnelle, équipement ou système qui peut être considéré individuellement

NOTE 1 Une entité peut être constituée de matériel, de logiciel, ou des deux à la fois, et peut aussi, dans certains cas, comprendre du personnel. Des éléments du système peuvent être des objets naturels ou créés par l'homme, tout autant que des modes de pensée ou leurs résultats (par exemple, des formes d'organisation, des méthodes mathématiques ou des langages de programmation).

NOTE 2 Le terme français "entité" est préféré au terme "dispositif" en raison de son sens plus général. Le terme "dispositif" a aussi un autre sens usuel équivalent au terme anglais "device".

NOTE 3 Le terme français "individu" est employé principalement en statistique.

NOTE 4 Un ensemble déterminé d'entités, par exemple une population d'entités ou un échantillon, peut lui-même être considéré comme une entité.

NOTE 5 Une entité logicielle peut être un code source, un code objet, un code de contrôle des tâches, des données de contrôle, ou un ensemble de ces différents éléments.

3.1.16
concept de maintenance
relations entre les échelons de maintenance, les niveaux d'intervention et les niveaux de maintenance qui interviennent dans la maintenance d'une entité

3.1.17
échelon de maintenance
position dans une organisation où des niveaux spécifiés de maintenance sont effectués sur une entité

NOTE 1 Exemples d'échelons de maintenance: exploitation, atelier de réparation, et fabricateur.

NOTE 2 L'échelon de maintenance est caractérisé par le niveau de compétence du personnel, les installations disponibles, l'emplacement, etc.

[VEI 191-07-04:1990]

3.1.18
politique de maintenance
approche générale des dispositions de maintenance et de support de maintenance fondée sur les objectifs et politiques de gestion des propriétaires, utilisateurs et clients

3.1.19
programme de maintenance
liste de toutes les tâches de maintenance élaborées pour un système, pour un contexte de fonctionnement et un concept de maintenance donnés

3.1.20
contexte de fonctionnement
circonstances dans lesquelles une entité est supposée fonctionner

3.1.21
défaillance potentielle
condition identifiable qui indique qu'une défaillance fonctionnelle est soit imminente soit en train de se réaliser

3.1.22
intervalle entre la défaillance potentielle et la défaillance fonctionnelle (P-F)
intervalle entre le point au niveau duquel une défaillance potentielle devient détectable et le point au niveau duquel elle se dégrade en défaillance fonctionnelle

3.1.23
maintenance basée sur la fiabilité
méthode pour identifier et sélectionner des politiques de gestion des défaillances à mettre en œuvre pour atteindre réellement et efficacement la sécurité la disponibilité et un fonctionnement à l'optimum économique requis

3.1.24
durée de vie de sécurité
temps avant lequel aucune défaillance ne doit se produire

3.1.25
système
ensemble d'éléments corrélés ou interactifs

[ISO 9000, 3.2.1][2]

NOTE 1 Dans le contexte de la sûreté de fonctionnement, un système présentera:

a) un but défini exprimé en termes de fonctions requises;

b) des conditions spécifiées de fonctionnement/d'utilisation

c) des limites définies.

NOTE 2 La structure d'un système peut être hiérarchique.

3.1.26
durée de vie en utilisation
duré avant l'instant auquel un état limité est atteint

NOTE 1 Un état limité peut être une fonction d'intensité de défaillance, une exigence de support de maintenance, une condition physique, un âge, une obsolescence, etc.

NOTE 2 La durée peut débuter à la première utilisation, à un instant ultérieur, c'est à dire la durée de vie en utilisation restante.

3.2 Abréviations

AMDE Analyse des modes de défaillance et de leurs effets

AMDEC Analyse des modes de défaillance, de leurs effets et de leur criticité

SLI Soutien logistique intégré

HUMS Systèmes de gestion à usage médical (HUMS *en anglais: Health usage management systems*)

LORA Analyse du niveau de réparation (LORA *en anglais: Level of repair analysis*)

NDI Inspection non destructive (NDI *en anglais: Non-destructive inspection*)

MBF Maintenance basée sur la fiabilité (RCM en anglais: *Reliability centred maintenance*)

4 Vue d'ensemble

4.1 Généralités

Le processus de la MBF est entièrement décrit dans la présente norme et il donne des informations sur chacun des éléments suivants:

a) début et planification de la MBF;

b) analyse des défaillances fonctionnelles;

c) sélection des tâches;

d) mise en œuvre;

e) amélioration continue.

La Figure 1 présente le processus global de la MBF, qui comprend les cinq étapes. On peut constater d'après cette figure que la MBF fournit un programme complet concernant non seulement le processus d'analyse, mais aussi les activités préliminaires et de suivi nécessaires pour garantir que l'investissement dans la MBF permet d'atteindre les résultats souhaités. Le processus de la MBF peut s'appliquer à tous les types de systèmes. L'Annexe D donne des lignes directrices sur la façon dont il convient d'interpréter le processus pour les structures pour lesquelles les mécanismes de défaillance et les tâches résultantes sont plus étroitement définis.

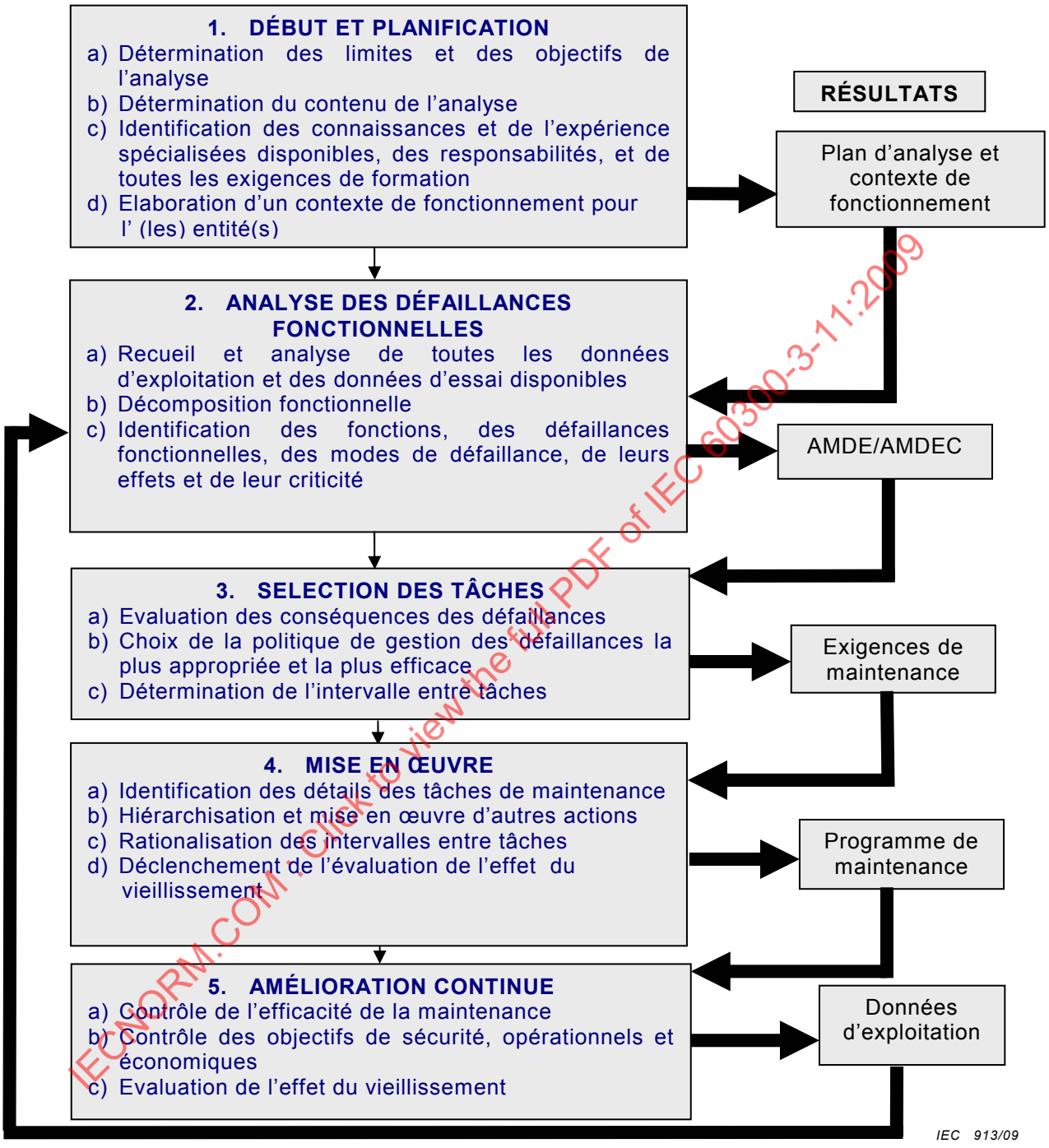


Figure 1 – Présentation générale du processus de la MBF

4.2 Objectifs

En tant que partie d'une politique de maintenance, les objectifs d'un programme de maintenance préventive efficace sont les suivants:

a) maintenir la fonction au niveau requis de sûreté de fonctionnement dans le contexte de fonctionnement donné;

b) obtenir les informations nécessaires pour améliorer la conception ou ajouter une redondance de moyens pour les entités dont la fiabilité s'avère inadéquate;

c) atteindre ces objectifs pour un coût total du cycle de vie minimal, incluant les coûts relatifs à la maintenance ainsi que les coûts relatifs aux défaillances résiduelles.

d) obtenir les informations nécessaires à l'établissement d'un programme de maintenance évolutif, plus performant que le programme de maintenance initial et ses révisions, par une évaluation systématique de l'efficacité des tâches de maintenance précédemment définies. La surveillance de l'état de composants critiques pour la sécurité ou coûteux, joue un rôle important dans le développement d'un programme.

Ces objectifs tiennent compte du fait que les programmes de maintenance, en tant que tels, ne peuvent corriger les déficiences de conception des niveaux de sécurité et de fiabilité des équipements et des structures. Le programme de maintenance ne peut que réduire la dégradation de tels niveaux et rétablir les niveaux de sécurité et de fiabilité à leurs niveaux de conception. Si les niveaux de fiabilité se révèlent insatisfaisants, une modification de la conception ou des modifications en exploitation ou des changements de procédure (tels les programmes de formation) peuvent être nécessaires pour obtenir une amélioration.

La MBF améliore l'efficacité de la maintenance et fournit un mécanisme de gestion de la maintenance à degré élevé de contrôle et de vigilance. Les bénéfices potentiels peuvent être résumés comme suit:

1) la sûreté de fonctionnement du système peut être augmentée à l'aide d'activités de maintenance plus appropriées;

2) les coûts totaux peuvent être réduits par un effort de maintenance planifié de manière plus efficace;

3) parution d'un journal d'audit complètement documenté;

4) un processus pour examiner et revoir les politiques de gestion des défaillances dans l'avenir, avec un investissement relativement minime;

5) les gestionnaires de maintenance disposent d'un outil de gestion qui renforce le contrôle et la direction;

6) le service de maintenance a une meilleure compréhension de ses objectifs et des raisons pour lesquelles il effectue les tâches de maintenance programmée.

Le programme de maintenance est constitué d'une liste de toutes les tâches de maintenance élaborées pour un système, pour un contexte de fonctionnement et un concept de maintenance donnés, y compris celles provenant du processus de MBF. Les programmes de maintenance sont généralement composés d'un programme initial et d'un programme évolutif «dynamique», La Figure 2 présente les principaux facteurs à prendre en considération lors de la phase de développement, c'est-à-dire avant l'exploitation, ainsi que les facteurs utilisés pour mettre à jour le programme, basés sur l'expérience en exploitation, une fois que le produit est en service.

Le programme de maintenance initial, qui est souvent le résultat d'une collaboration entre le fournisseur et l'utilisateur, est défini préalablement à l'exploitation et peut inclure des tâches basées sur la méthodologie de MBF. Le programme de maintenance évolutif qui est un développement du programme initial, est initié aussi tôt que possible par l'utilisateur dès le début de l'exploitation et est fondé sur les données réelles de dégradation, ou les données concernant les défaillances, sur les modifications du contexte de fonctionnement, ainsi que sur les progrès effectués sur la technologie et les matériaux et les données relatives aux techniques et outils de maintenance. Le programme évolutif est maintenu à l'aide de méthodologies de MBF. Le programme de maintenance initial est mis à jour pour refléter les modifications apportées au programme au cours du fonctionnement.

Un programme initial de MBF peut être entrepris lorsque le produit est en exploitation, afin de rénover et poursuivre l'amélioration d'un programme de maintenance existant, préparée sur la base de l'expérience ou de recommandations du fabricant, et sans bénéficier d'une approche structurée telle que l'approche MBF.

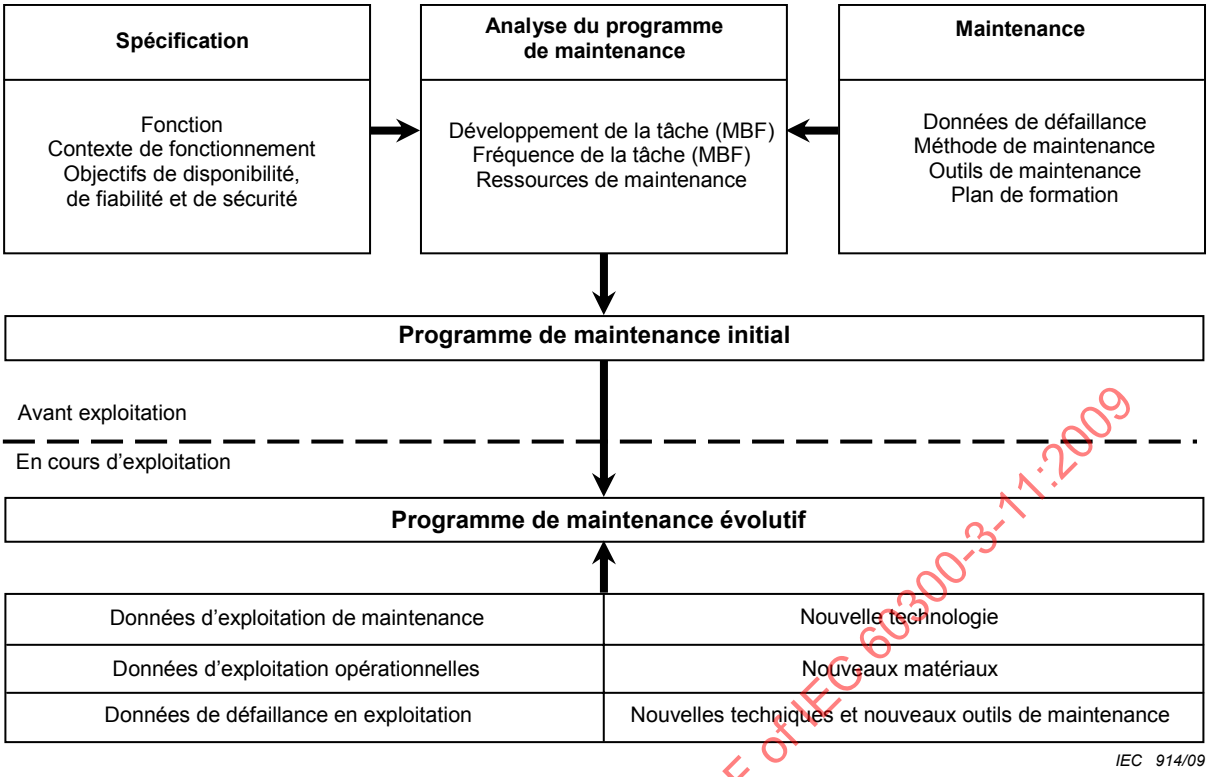


Figure 2 – Evolution d'un programme de maintenance MBF

4.3 Types de maintenance

Comme le montre la Figure 3, différentes approches sont suivies pour les tâches de maintenance. Il existe deux types des opérations de maintenance: préventive et corrective.

La maintenance préventive est entreprise avant la défaillance. Cela peut être lié à des conditions et atteint en surveillant ces conditions jusqu'à ce que la défaillance devienne imminente, ou par des vérifications du fonctionnement pour détecter la défaillance de fonctions cachées. La maintenance préventive peut aussi être prédéterminée, basée sur un intervalle fixe (tel que durée calendaire, heures d'exploitation, nombres de cycles), ce qui consiste en une mise à neuf régulière ou en un remplacement d'une entité ou de ses composants.

La maintenance corrective rétablit les fonctions d'une entité après une défaillance ou une inaptitude à respecter des limites données. Certaines défaillances sont acceptables si les conséquences (telles que perte de production, sécurité, impact sur l'environnement, coût) sont tolérables en comparaison du coût de la maintenance préventive et des pertes provoquées par la défaillance. Il en résulte une approche de la maintenance par la planification de la défaillance.

La maintenance préventive est généralement programmée ou basée sur un ensemble prédéterminé de conditions tandis que la maintenance corrective n'est pas programmée. Il n'est pas inhabituel de reporter une maintenance corrective à un moment plus adapté lorsqu'une redondance maintient la fonction. La MBF identifie les tâches de maintenance préventive optimales.

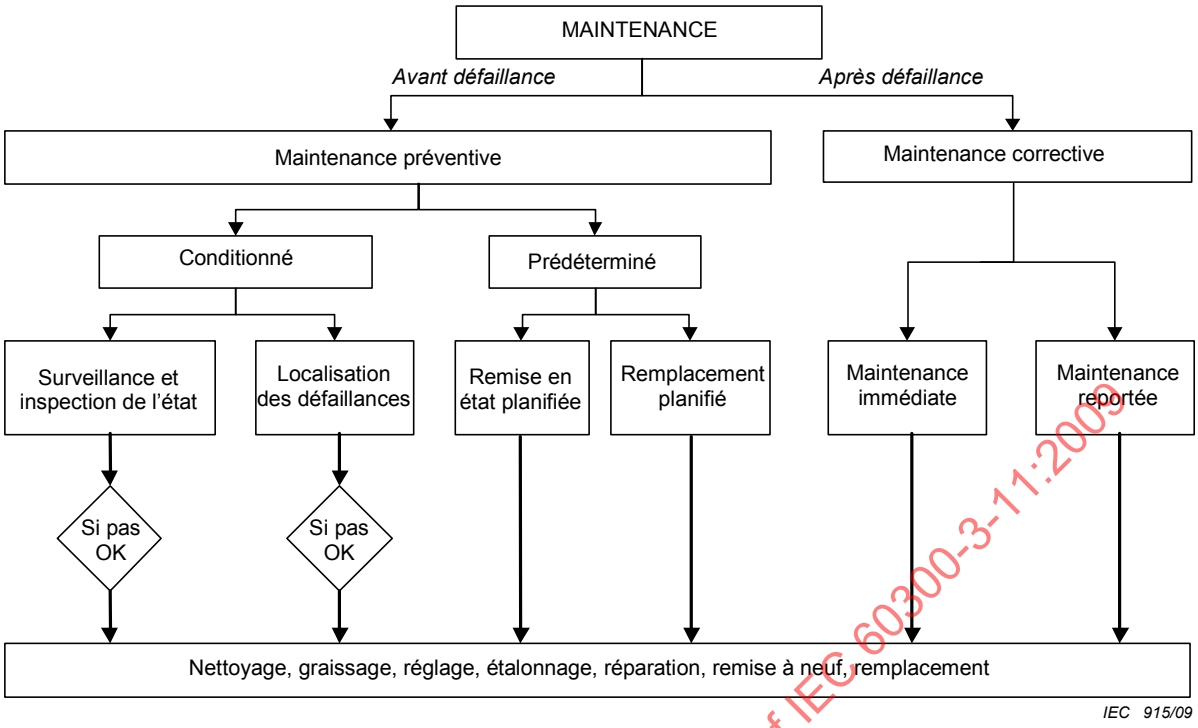


Figure 3 – Types de tâches de maintenance

5 Début et planification de la MBF

5.1 Objectifs pour la réalisation d'une analyse de MBF

La première phase de planification d'une analyse de MBF consiste à déterminer la nécessité et l'étendue de l'étude, en prenant en compte les objectifs suivants:

a) établir les tâches de maintenance optimales pour l'entité;

b) identifier les opportunités pour améliorer la conception;

c) évaluer où les tâches de maintenance actuelles sont inopérantes, inefficaces ou inappropriées;

d) identifier les bénéfices de la sûreté de fonctionnement.

Il convient que le processus d'évaluation de la nécessité d'une analyse de MBF pour un système soit une activité de gestion régulière du programme d'amélioration continue de la maintenance.

Une vaste analyse des données disponibles au sein du système de gestion de la maintenance permettra d'identifier les systèmes cibles, où la politique actuelle de gestion des défaillances a échoué ou est suspecte. Les données indiquant les paramètres suivants permettront d'identifier les entités potentielles:

1) modifications apportées au contexte de fonctionnement;

2) disponibilité et/ou fiabilité inadéquates;

3) incidents de sécurité;

4) temps de main-d'œuvre pour de maintenance préventive et/ou corrective anormalement élevés;

5) retard des travaux de maintenance;

6) coûts de maintenance élevés;

7) ratio «maintenance corrective sur la maintenance préventive » anormalement élevé;

8) nouvelles techniques de maintenance;

9) modifications technologiques de l'entité.

Se fier totalement aux données d'un système de gestion de la maintenance peut de révéler trompeur et il convient que le personnel de maintenance applique des dispositions supplémentaires ou une inspection du système pour détecter toutes ce que les données peuvent ne pas prendre en compte. Il convient d'inclure dans le processus de planification de la MBF une évaluation de l'exhaustivité et de la précision des informations disponibles.

Il existe d'autres avantages liés à l'incorporation de personnels de maintenance dans l'équipe de MBF qui se familiarisera alors avec le système et son personnel de maintenance, du fait des opportunités offertes pour comprendre le contexte de fonctionnement du système et avoir une discussion directe concernant la maintenance existante, les modes de défaillance et les modèles de défaillance (voir Annexe C).

5.2 Justification et hiérarchisation

Il convient que l'analyse de la MBF ne fasse partie intégrante d'une politique de maintenance plus étendue, que lorsqu'il y a un degré de confiance suffisant pour indiquer que ceci peut être tout à fait rentable ou lorsque les considérations de coûts commerciaux directs sont dépassées par d'autres objectifs critiques, comme par exemple les exigences relatives à la sécurité et à l'environnement. Il convient de prendre en compte ces facteurs pendant toute la durée de vie de l'entité.

Ces systèmes discrets qui sont jugés comme ayant un effet sur l'ensemble des objectifs commerciaux seront identifiés comme nécessaires dans l'analyse. Il convient que le choix et la hiérarchisation avec lesquels il est recommandé de les traiter soient basés sur une grande variété de critères, comme par exemple:

a) l'efficacité de la maintenance;

b) l'amélioration de la sûreté de fonctionnement;

c) les modifications de conception/de fonctionnement.

La priorité des systèmes dépendra de la priorité des objectifs commerciaux de la société.

Les méthodes utilisées pour sélectionner ces systèmes et les hiérarchiser peuvent être réparties entre :

1) les méthodes qualitatives fondées sur l'historique et un jugement d'ingénierie collectif,

2) les méthodes quantitatives, fondées sur des critères quantitatifs tels qu'une évaluation de la criticité, des facteurs de sécurité, la probabilité de défaillance, le taux de défaillance, le coût du cycle de vie, etc, utilisées pour évaluer l'importance de la dégradation/défaillance du système sur la sécurité de l'équipement, les aptitudes à la fonction et les coûts. La mise en œuvre de cette approche est facilitée lorsque des modèles et des bases de données appropriés existent,

3) les méthodes qui sont une combinaison de méthodes quantitatives et qualitatives.

L'objectif de cette activité est de constituer la liste ordonnée des systèmes suivant leur criticité et leur priorité.

5.3 Liens entre la conception et le support de maintenance

La majorité des exigences liées au support de maintenance pour un système sont décidées lors de la conception initiale, et il convient par conséquent que la planification pour la maintenance et le support de maintenance soit considérée aussitôt que possible, pour que des arbitrages puissent être pris en compte entre les besoins fonctionnels, la capacité, le coût du cycle de vie, la sûreté de fonctionnement et la sécurité.

Il convient que la maintenance et le support de maintenance soient considérés pendant toues les phases du cycle de vie. Les tâches spécifiques qu'il convient de réaliser sont données dans la CEI 60300-14 et les aspects liés à la maintenance sont donnés dans la CEI 60300-3-10.

L'approche pour déterminer la totalité des exigences de soutien au cours de la vie du système avant le fonctionnement initial est désignée par « soutien logistique intégré », et il convient de la réaliser conformément à la CEI 60300-3-12. La Figure 4 illustre la relation entre la MBF et d'autres activités de support et d'analyse.

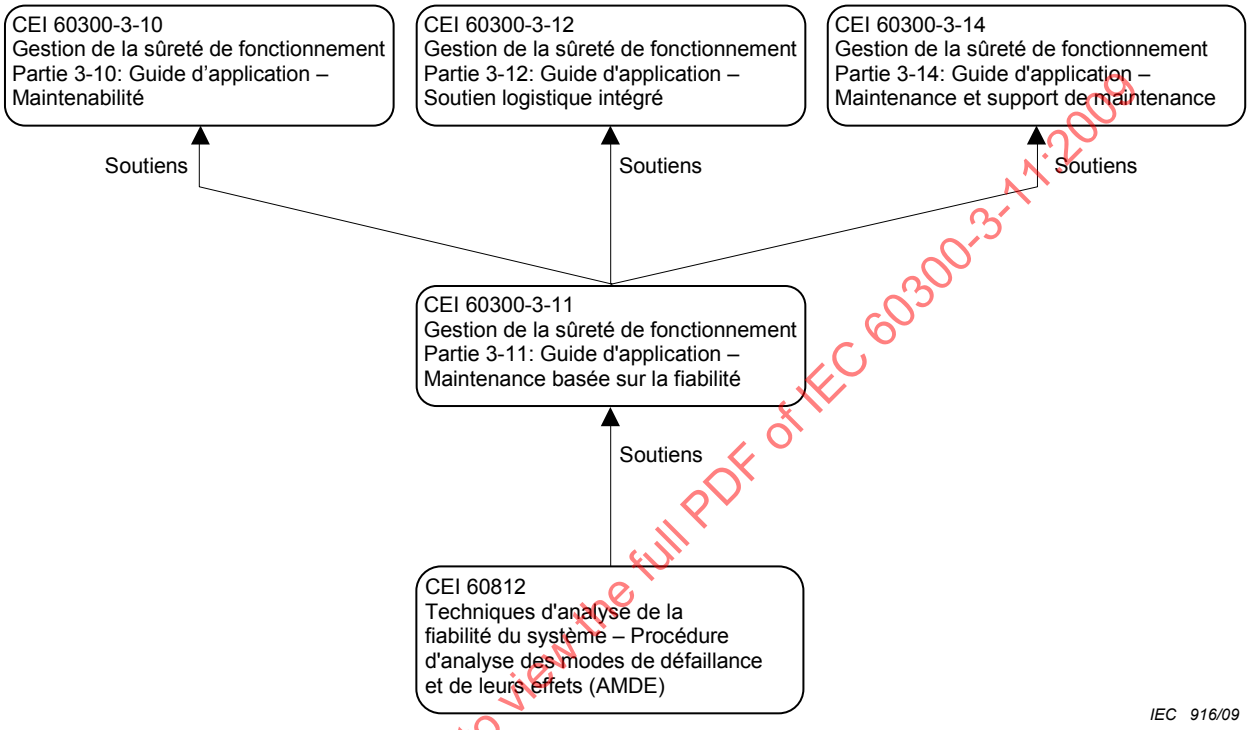


Figure 4 – Relation entre la MBF et d'autres activités de soutien

5.4 Connaissances et formation

Une analyse de la MBF nécessite des connaissances et une expérience particulière de l'ntité et de son contexte de fonctionnement. L'analyse exige les éléments suivants:

a) connaissance et expérience du processus de la MBF;

b) connaissance approfondie de l'entité et des caractéristiques de conception appropriées;

c) connaissance du contexte de fonctionnement de l'entité;

d) connaissance de l'état de l'entité (lors de l'analyse de l'équipement existant);

e) compréhension des modes de défaillance et de leurs effets;

f) connaissance approfondie des contraintes, comme les législations et réglementations en matière de sécurité et d'environnement, etc.;

g) connaissance des techniques et des outils de maintenance;

h) connaissance des coûts.

Lorsqu'il y a un manque de connaissances ou d'expérience du processus de MBF, il convient de prodiguer une formation supplémentaire.

5.5 Contexte de fonctionnement

Avant de réaliser une analysais MBF, il est essentiel de déterminer le contexte de fonctionnement. Il convient que le contexte de fonctionnement décrive la façon dont l'entité fonctionne, en décrivant en détails l'aptitude à la fonction attendue des systèmes.

Pour l'analyse d'un grand système constitué de nombreux sous-systèmes, il est probable qu'une hiérarchie des contextes de fonctionnement sera nécessaire.

La détermination du niveau de fonctionnement le plus élevé est en principe écrite en premier et elle décrit les caractéristiques physiques du système, son rôle principal et ses sous-systèmes, les profils de sollicitation et l'environnement de fonctionnement et de soutien.

La détermination au niveau fonction/sous-système le plus bas définit précisément les caractéristiques d'aptitude à la fonction de la fonction examinée. Il est important de noter que des paramètres d'aptitude à la fonction spécifiques sont nécessaires pour déterminer clairement ce qui constitue une défaillance, et quels effets les défaillances auront sur l'aptitude à la fonction spécifique de l'équipement.

Le fonctionnement d'une entité peut varier en fonction de la sollicitation. Il peut par conséquent être nécessaire de générer différents contextes de fonctionnement pour refléter ces différents états, dans la mesure où les différences de sollicitations peuvent donner lieu à des politiques de maintenance différentes. Par exemple, un système peut n'être exigé que pour une courte durée et la maintenance pendant cette période peut être fréquente et fondée sur des cycles. Toutefois, au cours de longues inactivités, le même système peut être soumis à une maintenance basée sur une fréquence calendaire peu élevée.

Le concept de maintenance peut également être influencé par des conditions environnementales variables. Par exemple, des entités dans un climat arctique peuvent être soumises à une politique de gestion des défaillances différente de celle à laquelle seraient soumis les mêmes entités dans un climat tropical.

Il convient que les contextes de fonctionnement prennent très attentivement en considération la question de la redondance. Il y a redondance lorsqu'il existe des systèmes multiples pour soutenir une seule fonction. Il y a deux types de redondance, à savoir:

a) la redondance en attente;

b) la redondance active.

Il y a redondance en attente lorsqu'un système existe à l'état de veille, fonctionnant uniquement en cas de défaillance du système actif. Le contexte de fonctionnement pour chaque système sera différent et entraînera différents modes de défaillance et différentes politiques de maintenance.

Il y a redondance active lorsque deux systèmes ou plus fonctionnement simultanément pour satisfaire une même sollicitation, mais chaque système a la capacité de satisfaire seul cette sollicitation. Dans cette situation, les modes de défaillance probables de chaque système seront semblables avec des politiques de maintenance similaires.

Une politique de maintenance différente peut être exigée pour les équipements inactifs, tels que les équipements stockés pour un fonctionnement unique ou peu fréquent, et il convient que le contexte de fonctionnement prenne en compte les entités de ce type.

5.6 Lignes directrices et hypothèses

En tant que partie de l'investissement dans l'analyse de la MBF, il convient qu'un ensemble de lignes directrices et d'hypothèses soit établi pour faciliter la réalisation du processus d'analyse. Il convient que les lignes directrices et les hypothèses soient clairement identifiées et

documentées pour établir l'approche du processus d'analyse et pour garantir sa cohérence. Les considérations peuvent comprendre:

a) des procédures de fonctionnement normalisées (y compris ce qui constitue «les tâches usuelles» de l'opérateur);

b) des politiques organisationnelles comme source d'entrées sur la définition de la défaillance, les taux de défaillance acceptables, etc.

c) des sources de données;

d) des probabilités acceptables de défaillance en fonction des effets des défaillances;

e) une structure de rupture de l'entité;

f) une approche de l'analyse pour les entités d'interface tels que les câblages et les tuyauteries;

g) une approche de l'analyse pour les entités réparées précédemment ou configurées de manière unique;

h) des méthodes et des outils analytiques, tels que l'analyse par arbre de panne, les diagrammes de fiabilité, les processus de Markov et analyse par réseaux de Petri;

i) des méthodes d'analyse coûts/bénéfices;

j) des valeurs définies pour les paramètres comme le coût de la main-d'œuvre, les facteurs d'utilisation, les facteurs de conversion de la durée de vie de conception, et les tailles minimales des fissures détectables;

k) des procédures pour la prise en compte des techniques avancées d'inspection/de détection, comme par exemple les systèmes de gestion à usage médical (HUMS) ou l'inspection non destructive (NDI);

l) des méthodologies pour identifier les temps entre l'apparition d'une défaillance potentielle et sa transformation en défaillance fonctionnelle, les défaillances d'usure, et pour calculer les intervalles entre mises en oeuvre des modifications;

m) une analyse des erreurs humaines (HEA, *en anglais: human error analysis*) pour prendre en compte de ces risques.

Il convient que les tâches exigées par la législation soient soumises à une analyse de MBF afin de vérifier leur mise en oeuvre correcte. Une concertation avec les organismes de règlementation compétents peut être nécessaire avant la réalisation de modifications.

5.7 Exigences relatives aux informations

La réalisation d'une analyse de MBF nécessite de connaître le fonctionnement du système et le cas échéant l'historique du système. Par exemple, il convient de rassembler toutes les données pouvant être obtenues sur les défaillances précédentes afin de garantir que toutes leurs causes sont traitées. Les enregistrements de maintenance donnent une indication de l'état de l'équipement après utilisation. Néanmoins, lorsqu'il n'y a pas suffisamment de données, l'avis d'experts connaissant l'équipement peut être utilisé.

L'analyse de MBF est réalisée en supposant qu'aucune maintenance préventive n'est entreprise, et est par conséquent souvent mentionnée «à base zéro». Il convient par conséquent d'utiliser avec prudence les données de défaillance en exploitation, dans la mesure où elles dépendront de la politique de gestion des défaillances existante. Les défaillances réputées être éliminées par les tâches de maintenance préventive existantes doivent également être prises en compte. Cependant, la prise en considération de défaillances qui ne se sont pas produite auparavant du fait de l'existence d'une maintenance préventive peut se révéler difficile.

Les données de défaillance actuelles ou génériques utilisées isolement ont une valeur limitée si les mécanismes de défaillance et le contexte opérationnel ne sont pas connus. Les informations pouvant aider à la réalisation d'une analyse de MBF peuvent comprendre:

a) le profil d'utilisation;
b) des exigences relatives à l'aptitude à la fonction;
c) des procédures de fonctionnement et l'expérience réelle du fonctionnement;
d) des exigences réglementaires;
e) une analyse de fiabilité;
f) un dossier de sécurité ou des évaluations de sécurité;
g) des manuels techniques;
h) les manuels d'utilisation du fabricant;
i) la documentation de conception;
j) les tâches de maintenance préventive existantes;
k) les procédures de maintenance existantes et l'expérience réelle du personnel de maintenance;
l) les modifications planifiées du système;
m) les rapports de maintenance et de défaillance;
n) les rapports d'expertise;
o) les rapports d'incident et d'accident
p) les taux d'utilisation des pièces de rechange.

6 Analyse des défaillances fonctionnelles

6.1 Principes et objectifs

La capacité à élaborer un programme de maintenance réussi à l'aide de la MBF nécessite une compréhension claire des fonctions et des défaillances de l'entité et des conséquences exprimées en termes d'objectifs de l'organisation dans le fonctionnement de l'entité.

Il convient que la méthode d'analyse des fonctions, des défaillances de l'entité et des conséquences, soit choisie par la société, afin d'adapter sa structure opérationnelle à ses objectifs; il est toutefois recommandé que les résultats de l'analyse donnent les informations décrites dans les articles suivants pour permettre à l'analyse de MBF d'aboutir.

Les méthodes d'analyse des modes de défaillance et de leurs effets (AMDE) et de leur criticité (AMDEC) (CEI 60812) sont adaptées à l'application à la MBF si l'analyse est structurée de telle sorte qu'elle soit conforme aux exigences de cette norme.

Il convient d'analyser les données d'exploitation en tant que partie de l'analyse des défaillances fonctionnelles afin de déterminer les causes et les fréquences de défaillance afin d'évaluer la criticité et le contribuer à l'AMDE , Les sources de données sont traitées en 7.5.1.

L'Annexe D donne des détails sur l'interprétation de l'analyse des défaillances fonctionnelles appliquée aux structures.

6.2 Exigences relatives à la définition des fonctions

6.2.1 Décomposition fonctionnelle

Lorsque l'on entreprend l'analyse d'une entité complexe, il peut être nécessaire de décomposer la fonctionnalité totale en plusieurs blocs mieux gérables. Il s'agit d'un processus itératif dans lequel des fonctions de haut niveau sont décomposées progressivement en des fonctions de niveau inférieur, qui sont assemblées pour former un modèle fonctionnel de l'ensemble de l'entité à l'étude. Il convient de noter qu'il existe de nombreuses façons d'entreprendre ce processus et des outils sont disponibles pour aider à visualiser la décomposition fonctionnelle. De nombreuses sociétés de grande taille ont une hiérarchie des

équipements qui est déjà basée sur la fonctionnalité et qui est idéale pour la base de la décomposition.

Le niveau le plus bas dans la hiérarchie, auquel il convient d'identifier les fonctions, est celui de l'entité dont les exigences de maintenance doivent être définies par le processus de la MBF. Les articles suivants traitant de l'analyse des défaillances fonctionnelles se rapportent aux entités à ce niveau, sauf spécification contraire. En général, les entités à ce niveau sont prévues pour être au niveau d'un système/d'une unité (comme un circuit d'alimentation ou une pompe) plutôt qu'au niveau d'un composant (comme un palier).

6.2.2 Elaboration de la détermination des fonctions

Il convient d'identifier toutes les fonctions de l'entité avec une norme d'aptitude à la fonction qui, si possible, est quantifiée.

Toutes les fonctions de l'entité sont spécifiques à un contexte de fonctionnement; par conséquent, il convient que tous les facteurs particuliers relatifs au contexte de fonctionnement des entités individuelles soient documentés soit par rapport à cette entité, soit en tant que partie de la détermination générale du contexte de fonctionnement, dans l'analyse des lignes directrices et des hypothèses (5.6).

Bien qu'une entité individuelle soit en principe conçu pour réaliser une seule fonction, de nombreuses entités peuvent avoir des fonctions multiples ou des fonctions secondaires. Il convient de prendre des précautions dans de tels cas, puisque ces fonctions supplémentaires ne peuvent être appropriées que dans des contextes de fonctionnement spécifiques, souvent dans un sous-ensemble du contexte de fonctionnement pris en compte pour la fonction principale ou uniquement dans des conditions de «sollicitation».

Des exemples de fonctions secondaires peuvent inclure, sans que l'énumération ne soit exhaustive:

a) le confinement des fluides (par exemple, eau, huile);

b) le transfert de la charge structurelle;

c) la protection;

d) la fourniture d'indications aux opérateurs par l'intermédiaire d'un système de commande.

La norme d'aptitude à la fonction est le niveau d'aptitude à la fonction exigé de l'entité pour remplir la fonction établie du système dans le contexte de fonctionnement donné; il convient d'établir cette norme quantitativement et/ou sans ambiguïté pour garantir une analyse significative. En définissant la norme exigée, il convient que la valeur choisie représente le niveau d'aptitude à la fonction essentiel pour atteindre la fonction plutôt que la capacité de l'entité. Par exemple, il convient que le débit d'une pompe soit de (400 ± 30) l/min pour obtenir le degré correct de refroidissement; néanmoins, une pompe pouvant délivrer 600 l/min peut être installée. Un débit de (400 ± 30) l/min représente l'exigence fonctionnelle. Par conséquent, cette exigence peut être exprimée comme suit: «Fournir un débit de (400 ± 30) l/min d'eau».

Il convient que les fonctions qui fournissent une capacité de protection incluent dans leur définition une indication claire des événements ou des circonstances qui activeraient ou exigeraient une activation de la fonction de protection.

6.3 Exigences relatives à la définition des défaillances fonctionnelles

Il convient d'identifier toutes les défaillances fonctionnelles associées à chacune des fonctions définies.

Il convient que les défaillances fonctionnelles énumérées se rapportent toujours à des fonctions spécifiques qui ont été identifiées et qu'elles soient exprimées en termes d'incapacité d'atteindre le niveau d'aptitude à la fonction indiqué ou à respecter les normes appliquées. La perte totale d'une fonction sera en principe toujours prise en compte, mais la perte partielle

peut aussi être pertinente, et il convient qu'elle soit toujours incluse si les effets de la perte sont différents de ceux de la perte totale.

Par exemple, la pompe décrite ci-dessus ayant un débit de (400 ± 30) l/min présentera la défaillance fonctionnelle suivante: "ne parvient pas à fournir d'eau". De plus, la défaillance fonctionnelle suivante: "la pompe fournit moins de 370 l/min", serait valide si le système était tel qu'il puisse fournir une capacité réduite à ces débits réduits.

Les défaillances fonctionnelles comprennent, sans que l'énumération soit exhaustive:

a) une perte fonctionnelle totale;

b) une incapacité à satisfaire à l'exigence d'aptitude à la fonction;

c) un fonctionnement intermittent;

d) un fonctionnement alors qu'il n'a pas été exigé.

De nombreuses autres défaillances fonctionnelles particulières existeront, reposant sur les caractéristiques spécifiques du système et sur les exigences ou les contraintes de fonctionnement.

Cette approche permet de faire une distinction entre les conséquences des pertes de fonctions spécifiques, dans la mesure où la perte fonctionnelle entraîne les effets au niveau d'intervention le plus élevé.

6.4 Exigences relatives à la définition des modes de défaillance

On doit identifier les conditions physiques spécifiques raisonnablement probables qui provoquent chaque défaillance fonctionnelle.

Il convient que le mode de défaillance inclut l'identification de l'entité physique défaillant et une description du mécanisme de défaillance. Par exemple: "Fissure dans la bride due à la fatigue" ou "Fuite de l'organe de commande due à l'usure d'un joint d'étanchéité". Le niveau de détail auquel le mode de défaillance est identifié doit refléter à la fois le niveau d'analyse dans son ensemble et le niveau auquel il est possible d'identifier une politique de gestion des défaillances.

En établissant la liste des modes de défaillance, il est important que seuls ceux qui sont "raisonnablement susceptibles" de se produire soient inclus; il convient que la définition de "raisonnable" soit indiquée comme partie des règles de base pour l'ensemble de l'analyse de la MBF et elle peut varier de manière significative entre les sociétés et les applications. En particulier, il convient que les conséquences des défaillances soient prises en compte dans la mesure où il est recommandé d'inclure les modes de défaillance avec une probabilité très faible d'apparition lorsque les conséquences sont très graves.

Il convient d'inclure dans l'analyse les défaillances dont l'apparition est connue, ou qui sont évitées par un programme de maintenance préventive existant, dans le contexte de fonctionnement donné. De plus, il convient d'inclure tout autre événement pouvant entraîner une défaillance fonctionnelle, comme par exemple une erreur de l'opérateur, les influences environnementales et les défauts de conception. Puisque la MBF traite de toutes les politiques de gestion des défaillances, une erreur humaine peut être incluse; néanmoins, si un programme plus vaste incluant les facteurs humains est entrepris, cela peut ne pas être économiquement justifié. Si l'erreur humaine est prise en compte en dehors de l'analyse, les modes de défaillance qui leur sont liés peuvent être énumérés pour assurer l'exhaustivité, mais pas soumis à une analyse supplémentaire dans la MBF. Les détails indiquant quels types de facteurs humains sont adaptés à une prise en compte dans l'analyse n'entrent pas dans le domaine d'application de la présente norme.

6.5 Exigences relatives à la définition des effets des défaillances

Il convient d'identifier les effets des défaillances fonctionnelles.

L'effet de la défaillance décrit ce qui se produirait si le mode de défaillance devait se produire et identifiera généralement l'effet sur l'entité considérée, les entités voisines et la capacité fonctionnelle de l'entité finale. Il convient que l'effet décrit soit celui qui se produit si aucune tâche spécifique n'est réalisée afin d'anticiper, de détecter ou d'empêcher la défaillance.

Il importe que l'effet identifié soit l'effet le plus grave auquel on peut raisonnablement s'attendre; encore une fois, il convient que la définition de «raisonnable» fasse partie des règles de base de l'analyse.

Il est important que la description des effets comprenne des informations suffisantes pour permettre l'évaluation précise des conséquences. Il convient que les effets sur l'équipement, le personnel, le public et l'environnement soient tous pris en compte.

La plupart des analyses identifient les effets au niveau local (c'est-à-dire au niveau de l'entité), au niveau d'intervention suivant le plus élevé et au niveau de l'entité finale (le niveau d'intervention le plus élevé étant l'usine, l'avion ou le véhicule, etc. considéré). L'identification des effets au niveau de l'entité finale est nécessaire si l'on prend en compte l'importance relative des défaillances, dans la mesure où ceci représente un point de référence commun pour toutes les entités.

6.6 Criticité

L'application de la MBF à chaque mode de défaillance identifié dans l'analyse des défaillances ne sera pas rentable dans tous les cas. Il peut par conséquent être nécessaire pour une société d'utiliser un processus logique et structuré pour déterminer quels sont les modes de défaillance dont il convient de traiter dans l'analyse de la MBF afin d'atteindre un niveau de risque acceptable.

La méthode fréquemment utilisée pour ce processus d'évaluation est une analyse de la criticité, qui combine la sévérité et le taux d'apparition afin de déduire une valeur de criticité représentant le niveau de risque associé à un mode de défaillance. Il convient que la criticité traite de tous les aspects des conséquences des défaillances, y compris par exemple la sécurité, l'aptitude à la fonction opérationnelle et la rentabilité. L'Annexe A présente une approche type de l'analyse de la criticité.

La valeur de la criticité est utilisée pour identifier les modes de défaillance dans lesquels le risque est acceptable et par conséquent ne nécessitant pas de gestion des défaillances, et pour hiérarchiser ou classer les modes de défaillance nécessitant une analyse. Pour les défaillances pour lesquelles aucune analyse n'est exigée, il arrive souvent que les défaillances se produisent et aucune politique de maintenance préventive active n'est utilisée; cependant, cette décision dépend de la société et de ses objectifs.

7 Classement des conséquences et sélection des tâches de la MBF

7.1 Principes et objectifs

Le programme de maintenance préventive est élaboré à l'aide d'une approche logique guidée. En évaluant les politiques de gestion des défaillances possibles, on peut considérer l'ensemble du programme de maintenance élaboré pour une entité donnée. Un arbre de décision logique est utilisé pour guider le processus d'analyse, voir la Figure 5.

La maintenance préventive se compose d'une ou plusieurs des tâches suivantes, à des intervalles définis:

a) la surveillance de l'état;

b) la remise en état programmée;

c) le remplacement programmé;

d) la localisation des défaillances.

Les tâches de nettoyage, de graissage, de réglage et d'étalonnage qui sont exigées pour certains systèmes peuvent être traitées en utilisant le groupe de tâches énumérées ci-dessus.

Il s'agit du groupe de tâches défini par l'analyse de MBF, c'est-à-dire qu'il comprend le programme de maintenance préventive basé sur la MBF.

Les tâches de maintenance corrective peuvent résulter de la décision visant à ne pas effectuer de tâche préventive à la suite de la détection d'une tâche conditionnelle ou d'un mode de défaillance non prévu.

La MBF garantit que les tâches supplémentaires susceptibles d'entraîner une augmentation des coûts de maintenance sans pour autant améliorer l'atteinte du niveau de fiabilité sont exclues du programme de maintenance. La fiabilité décroît lorsque l'on accomplit des tâches de maintenance inappropriées ou non nécessaires, en raison de l'incidence croissante de pannes induites par l'opérateur de maintenance.

L'objectif de la sélection des tâches de MBF est de choisir une politique de gestion des défaillances afin d'atténuer les conséquences de chaque mode de défaillance identifié; l'analyse de la criticité participe largement à l'atteinte de cet objectif. Lorsqu'une tâche de maintenance a été identifiée, les informations associées sont généralement identifiées comme suit:

a) estimation des heures de main-d'œuvre exigées pour les tâches;

b) type et niveau de compétence nécessaires pour accomplir la tâche;

c) critères pour la sélection des intervalles entre tâches.

Le paragraphe D.3.3 apporte des détails sur l'interprétation de l'analyse des tâches appliquée aux structures. En appliquant l'analyse des tâches aux structures, le type de structure tend à indiquer la tâche de maintenance.

7.2 Processus décisionnel de la MBF

Le choix de la politique la plus adaptée de gestion des défaillances est guidé par l'utilisation d'un diagramme décisionnel de MBF, tel que celui présenté à la Figure 5.

L'approche utilisée afin d'identifier les tâches de maintenance préventive applicables et efficaces fournit un cheminement logique pour la prise en compte de chaque mode de défaillance. Le diagramme décisionnel est utilisé pour classer les conséquences du mode de défaillance, puis pour déterminer s'il existe une tâche de maintenance applicable et efficace, qui permettra d'empêcher ou d'atténuer ces conséquences. Ceci entraîne des tâches et des intervalles associés qui constitueront le programme de maintenance préventive et les actions de gestion.

Une tâche de maintenance applicable est celle qui traite le mode de défaillance et qui est techniquement réalisable.

Une tâche effective de maintenance est celle qui convient et qui traite avec succès les conséquences d'une défaillance.

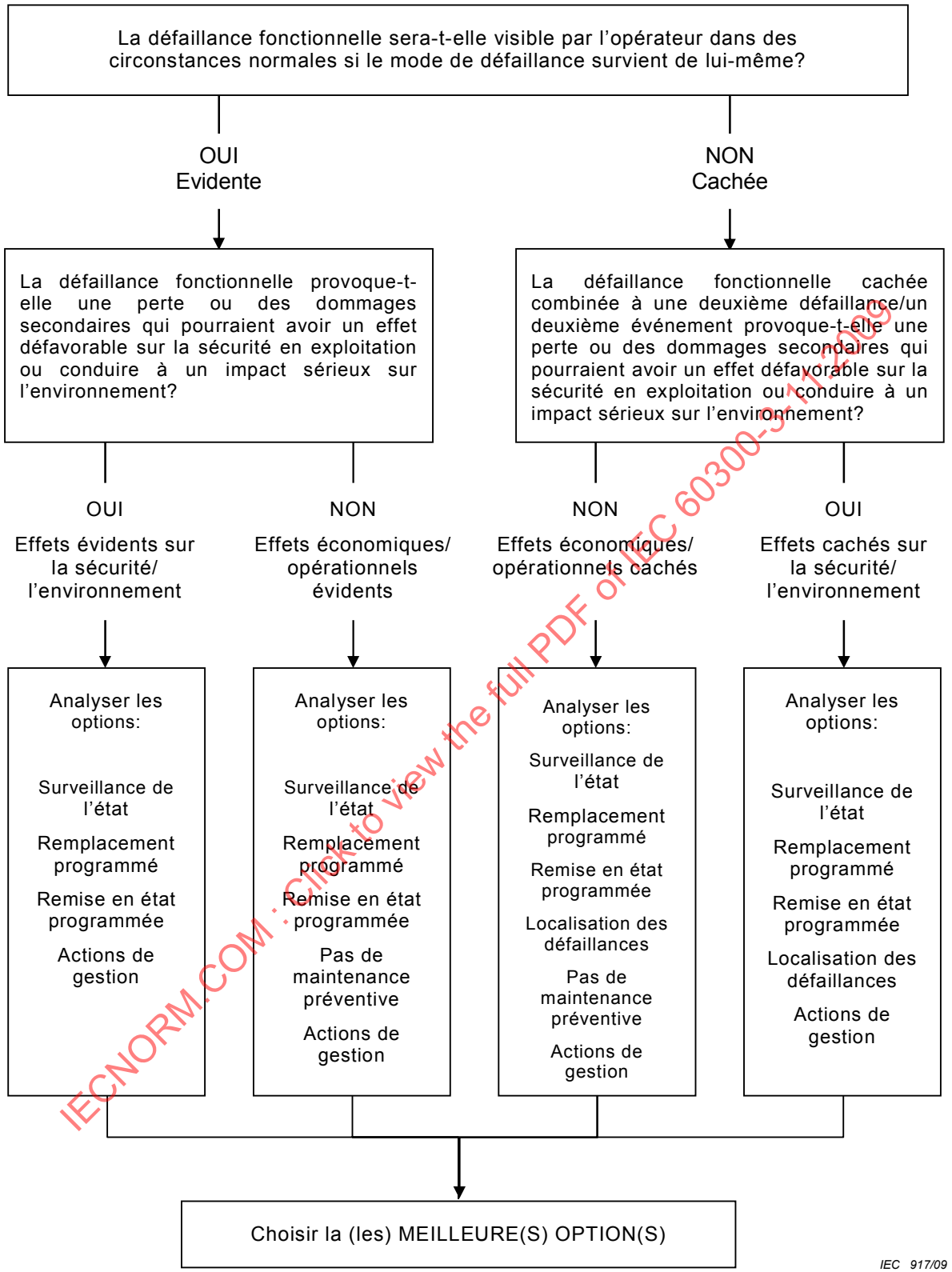


Figure 5 – Diagramme décisionnel de MBF

7.3 Conséquences d'une défaillance

Le processus prend en compte chaque mode de défaillance successivement et les classe en termes de conséquences des défaillances fonctionnelles. Ces classifications incluent les éléments suivants:

a) caché ou évident;

b) effets sur la sécurité, économiques/opérationnels, identifiés par l'analyse des défaillances.

Le classement d'une défaillance en "cachée" ou "évidente" est déterminé en répondant à la question suivante: « La défaillance fonctionnelle sera-t-elle visible par l'opérateur dans des circonstances normales si le mode de défaillance survient de lui-même? » Si la réponse à la question est «Oui», la défaillance est évidente, sinon la défaillance est cachée.

La compréhension de ce qui caractérise «les circonstances normales» st essentielle pour une analyse significative de la MBF, et il convient que ceci soit saisi dans le contexte de fonctionnement.

Le second classement des modes de défaillance indique ceux-ci entraînent des effets sur la sécurité et l'environnement ou des effets économiques et opérationnels.

Une défaillance est considérée comme entrant dans la catégorie « sécurité/environnement» si les effets peuvent nuire au personnel, au public ou à l'environnement.

Si la défaillance fonctionnelle ne présente pas d'effet défavorable sur la sécurité ou l'environnement, les effets des modes de défaillance sont ensuite évalués comme étant économiques/opérationnels. La classification économique/opérationnelle fait référence aux effets des défaillances fonctionnelles qui entraînent une dégradation de la capacité opérationnelle, ce qui pourrait se traduire par une production réduite, une dégradation de la mission, une défaillance pour terminer une mission au cours de la durée exigée, ou tout autre impact économique.

La perte d'une fonction cachée ne présente pas en elle-même de conséquences, comme la sécurité, mais elle a des conséquences lorsqu'elle est combinée avec une défaillance fonctionnelle supplémentaire d'une entité associée à l'arrêt ou protégée.

7.4 Choix de la politique de gestion des défaillances

Le niveau suivant dans le processus de décision de la MBF évalue les caractéristiques de chaque mode de défaillance pour déterminer la politique de gestion des défaillances la plus appropriée. Il y a un certain nombre d'options disponibles, à savoir:

a) Surveillance de l'état

La surveillance de l'état est une tâche effectuée de façon permanente ou périodique, qui consiste à surveiller l'état d'une entité en fonctionnement, par rapport à des paramètres prédéfinis afin de détecter sa détérioration. Elle peut consister en des tâches d'inspection, qui sont un examen de l'entité par rapport à une norme donnée.

b) Remise en état programmée

Une remise en état consiste à exécuter les travaux nécessaires pour ramener l'entité à une norme donnée. Puisque la remise en état peut aller du simple nettoyage au remplacement de pièces multiples, il est nécessaire de spécifier le contenu de chaque tâche de remise en état.

c) Remplacement programmé

Le remplacement programmé consiste à retirer de l'exploitation une entité lorsque sa limite spécifiée de durée de vie est atteinte, et à le remplacer par une entité satisfaisant à toutes les normes d'aptitude à la fonction requises. Les tâches de remplacement programmé s'appliquent généralement à des pièces dites consommables ou «d'un seul bloc», telles

que des cartouches, des boîtes métalliques, des vérins, des disques de turbines, des éléments structuraux à durée de vie de sécurité, etc.

d) Localisation des défaillances

Une tâche de localisation des défaillances est une tâche effectuée pour déterminer si une entité remplit ou non sa fonction. Elle est uniquement destinée à révéler des défaillances cachées. Une tâche de localisation des défaillances peut varier entre une vérification visuelle et une évaluation quantitative par rapport à une norme d'aptitude à la fonction spécifique. Certaines applications restreignent la capacité à réaliser un essai fonctionnel complet. Dans de tels cas, un essai fonctionnel partiel peut être applicable.

e) Pas de maintenance préventive.

En fonction des effets des défaillances, il peut être décidé qu'aucune tâche n'est spécifiée dans certaines situations. Le résultat de cette politique de gestion des défaillances est une maintenance corrective ou pas de maintenance du tout, à la suite d'une défaillance.

f) Actions de gestion complémentaires

D'autres actions peuvent résulter de l'application du processus décisionnel de la MBF, comprenant:

i) une nouvelle conception;
ii) modification de l'équipement existant, comme à l'aide d'entités plus fiables;
iii) des modifications/restrictions de la procédure de fonctionnement;
iv) des modifications de la procédure de maintenance;
v) des vérifications avant ou après utilisation;
vi) une modification de la stratégie de fourniture des pièces de rechange;
vii) une formation supplémentaire de l'opérateur ou du personnel de maintenance.

La mise en œuvre d'actions de gestion peut être répartie en deux catégories distinctes:

1) celles qui exigent une action urgente et immédiate, en particulier pour les modes de défaillance dont l'apparition aura un impact défavorable sur la sécurité ou sur l'environnement;
2) celles qui peuvent être souhaitables lorsqu'une tâche de maintenance préventive ne peut pas être accomplie pour réduire les conséquences des défaillances fonctionnelles qui affectent les coûts ou le fonctionnement. Il convient de les évaluer par une analyse des coûts/bénéfices, afin de déterminer quelle option donne le plus grand bénéfice par rapport au fait d'entreprendre une action non prédéterminée pour empêcher les défaillances.

Le diagramme décisionnel de MBF de la Figure 5 exige une prise en compte de toutes les politiques de gestion des défaillances applicables pour un mode de défaillance donné. Le coût de chaque solution possible joue un rôle significatif dans la détermination de celle qui sera choisie en définitive. A cette étape de l'analyse, chaque option de la politique de gestion des défaillances s'est déjà révélée appropriée, dans la mesure où chacune d'entre elles réduit à un niveau acceptable les conséquences des défaillances. La meilleure option sera déterminée par le coût de mise en place de cette solution et les conséquences opérationnelles que cette option présentera sur les opérations de maintenance du programme.

Il n'est parfois pas possible de trouver de politique de gestion des défaillances qui réduise seule et de manière adéquate la probabilité de défaillance à un niveau acceptable. Dans ces cas, il est parfois possible de combiner des tâches (généralement de types différents) pour atteindre le niveau souhaité de fiabilité.

7.5 Intervalle entre tâches

7.5.1 Sources de données

De manière à fixer la périodicité des tâches, il est nécessaire de déterminer les caractéristiques des modes de défaillance qui suggèrent un intervalle rentable pour l'exécution

des tâches. Ceci peut être obtenu par un ou plusieurs des éléments suivants au cours de l'analyse d'une nouvelle entité:

a) expérience préalablement acquise sur des équipements identiques ou semblables et démontrant qu'une tâche de maintenance programmée a apporté une preuve suffisante de son efficacité; voir la CEI 62308 [10];

b) des données d'essais en provenance du fabricant/fournisseur, indiquant qu'une tâche de maintenance programmée sera applicable et efficace pour l'entité concernée concernée; voir la CEI 62308 [10];

c) des données de fiabilité et des prévisions de fiabilité;

d) des attributs de défaillances supposés (par exemple, distribution, taux); voir la CEI 61649 [11] et la CEI 61710 [12];

e) les coûts de soutien du cycle de vie.

En plus des éléments ci-dessus, au cours de l'analyse d'une entité existante, d'autres sources d'informations peuvent comprendre:

f) les données opérationnelles et de maintenance (y compris les coûts);

g) l'expérience de l'opérateur et du personnel de maintenance;

h) les données relatives à l'effet du vieillissement.

Si les données de fiabilité sont insuffisantes, ou qu'il n'y a pas de connaissance préalable relative à un équipement similaire, ou si la similitude est insuffisante entre l'ancien et le nouveau système, l'intervalle entre tâches peut uniquement être établi initialement par du personnel qualifié ayant une bonne connaissance et une bonne expérience en exploitation associées aux meilleures données d'exploitation disponibles et aux données économiques adéquates.

Il existe des modèles mathématiques pour déterminer la fréquence et la périodicité des tâches, mais ces modèles dépendent de la disponibilité des données appropriées. Certains modèles sont basés sur des données de distributions exponentielles, d'autres sur un taux de défaillance non constant (CEI 61649) [11] ou une intensité de défaillance non constante (CEI 61710) [12]. Ces informations seront spécifiques aux industries particulières et il convient que ces normes industrielles et les relevés de données correspondantes soient consultés de manière appropriée.

7.5.2 Surveillance de l'état

Les tâches de surveillance de l'état consistent à détecter la dégradation à mesure que la défaillance fonctionnelle approche. La défaillance potentielle est définie comme l'état ou la condition précoce de l'entité, indiquant que le mode de défaillance peut se produire si aucune action corrective n'est prise. La défaillance potentielle présentera un état ou un certain nombre d'états qui sont autant d'avertissements préalables de la présence du mode de défaillance considéré. Ces conditions peuvent inclure les bruits, les vibrations, les variations de températures, la consommation ou la dégradation de l'aptitude à la fonction de lubrifiants.

La surveillance de l'état peut être entreprise manuellement ou par un équipement de surveillance d'état, comme par exemple un capteur de vibrations placé au niveau d'un palier. En évaluant l'état à surveiller, il convient de prendre en compte le coût du cycle de vie de tout équipement de surveillance d'état.

Pour évaluer l'intervalle pour une tâche de surveillance de l'état, il est nécessaire de déterminer la durée entre la défaillance potentielle et la défaillance fonctionnelle. Au cours du processus de dégradation, l'intervalle entre le point où la dégradation atteint un niveau prédéterminé (défaillance potentielle) et le point où elle se dégrade en défaillance fonctionnelle est désigné par l'intervalle entre la défaillance potentielle (P) et la défaillance fonctionnelle (F), ou intervalle P-F, voir la Figure 6
. Une connaissance de l'état initial et de la vitesse de détérioration est utile pour prédire quand la défaillance potentielle et la défaillance fonctionnelle sont susceptibles de se produire.Ceci

facilitera la détermination du moment où il convient d'entreprendre les tâches initiales de surveillance de l'état.

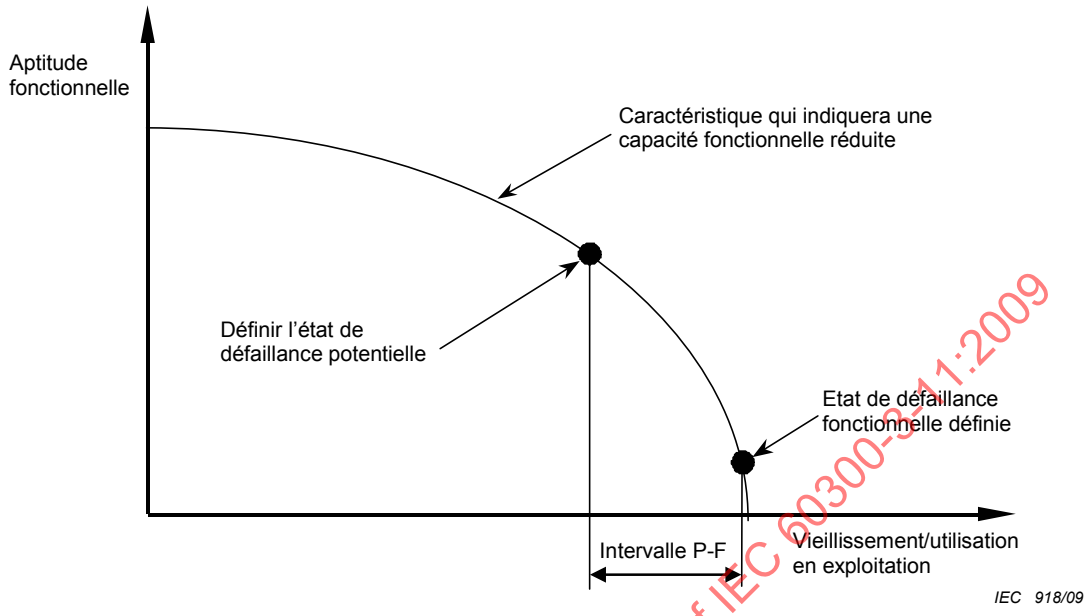


Figure 6 – Intervalle P-F

Pour qu'une tâche de surveillance de l'état soit applicable, il convient que les conditions suivantes soient satisfaites:

a) il convient que l'état soit détectable;

b) il convient que la détérioration soit mesurable;

c) il convient que l'intervalle P-F soit suffisamment long pour qu'une tâche soit physiquement possible;

d) il convient que l'intervalle P-F soit cohérent.

Lorsqu'il y a un certain nombre de conditions de défaillance naissantes pouvant être surveillées, il convient que l'examen prenne en compte l'état qui fournit le temps d'attente le plus long avant défaillance et le coût de tous les équipements et ressources exigés par la tâche potentielle.

Il convient que l'intervalle pour la tâche de surveillance de l'état soit inférieur ou égal à l'intervalle P-F. La relation entre l'intervalle entre les tâches et l'intervalle P-F varie en fonction de la probabilité de non-détection que la société consent à accepter et de la sévérité des conséquences du mode de défaillance. Un intervalle entre tâches égal à la moitié de l'intervalle P-F est généralement utilisé, puisqu'il donne potentiellement deux occasions de détecter la dégradation. Lorsqu'un niveau plus élevé de protection est souhaité, certaines sociétés choisissent d'utiliser des fractions plus petites de l'intervalle P-F pour réduire l'exposition aux risques pour la sécurité, et pour protéger les composants de grande valeur. La fraction de l'intervalle P-F utilisée pour établir l'intervalle entre tâches dépend du niveau de risque et/ou du coût que la société consent à accepter.

Lors de la détermination de l'intervalle pour la surveillance de l'état, il convient de prendre en compte l'efficacité de la méthode de détection. A mesure que l'efficacité de la technique d'inspection ou de surveillance s'améliore, il peut être possible de réduire la fréquence de la tâche. Il convient d'enregistrer les identifications de défaillance cachée réussies tout autant que celles qui n'ont pas réussi.

7.5.3 Remplacement et remise en état programmés

L'intervalle pour les tâches de remplacement et de remise en état programmés est fondé sur une évaluation de la durée de vie de sécurité ou de la vie utile résultant du mode de défaillance.

Pour les tâches de remplacement et de remise en état programmés qui traitent des effets sur la sécurité, il convient qu'il y ait une durée de vie de sécurité (c'est-à-dire que les entités sont supposées survivre à cette durée de vie – voir la CEI 61649). La durée de vie de sécurité peut être établie à partir de la fonction de répartition cumulée des défaillances de l'entité, en choisissant un intervalle de remplacement qui implique une très faible probabilité de défaillance avant les interventions de remplacement.

Lorsqu'une défaillance ne provoque pas de danger impliquant la sécurité, mais seulement une perte de la disponibilité, l'intervalle de remplacement est établi selon un processus d'analyse de compromis entre le coût des composants de remplacement, le coût de la défaillance et l'exigence de disponibilité de l'équipement.

Les limites de la vie utile sont utilisées pour les entités dont les modes de défaillance ont uniquement des conséquences économiques/opérationnelles. Une limite de la vie utile est garantie pour une entité s'il est rentable de la retirer avant qu'elle ne soit défaillante. Contrairement aux limites de la durée de vie de sécurité, qui sont fixées de manière conventionnelle pour éviter toutes les défaillances, la limite de la vie utile peut être fixée librement pour augmenter au maximum la vie utile de l'entité et, par conséquent, elle peut s'ajouter au risque d'une défaillance occasionnelle. Une entité dont une probabilité conditionnelle de défaillance augmente progressivement peut supporter une limite de durée de vie économique, même sans vieillissement par usure bien défini, si les bénéfices du rétablissement, par exemple une probabilité inférieure de défaillance, dépassent le coût.

Les tâches de remplacement et de remise en état programmés peuvent être utiles lorsque une ou plusieurs entités clé ont un mécanisme d'usure net (voir Annexe C, modèles A et B). En utilisant la distribution de Weibull, le paramètre de forme (β), la durée de vie caractéristique (ή) et le temps sans défaillance (t_0) peuvent être estimés. Pour les entités qui ont un temps sans défaillance (t_0) significatif, il convient de considérer un remplacement ou une remise en état programmés juste avant t_0. Même pour t_0 d'une distribution de Weibull à deux paramètres, le remplacement et la remise en état programmés peuvent être réalisés à un pourcentage prédéfini de défaillances, par exemple 1 % (souvent appelé L1 ou B1), ou 10 % (souvent appelé L10 ou B10); voir le CEI 61649.

7.5.4 Localisation des défaillances

Les tâches de localisation des défaillances ne sont applicables qu'aux défaillances cachées et ne sont applicables que si une tâche explicite peut être identifiée pour détecter la défaillance fonctionnelle. Une tâche de localisation des défaillances peut être un essai d'inspection, un essai fonctionnel ou un essai fonctionnel partiel pour déterminer si une entité accomplira toujours sa fonction requise, à la sollicitation. La localisation de défaillance est pertinente lorsque des fonctions ne sont normalement pas nécessaires, par exemple en cas de redondance ou des fonctions de sécurité qui sont uniquement rarement activées.

Une tâche de localisation des défaillances est efficace si elle réduit la probabilité d'une défaillance multiple à un niveau acceptable. L'Annexe B donne des lignes directrices sur les méthodes de détermination des intervalles entre tâches pour les tâches de localisation des défaillances.

8 Mise en œuvre

8.1 Détails des tâches de maintenance

Les tâches générées comme résultat de l'analyse de MBF doivent être décrites en détails avant qu'elles puissent être mises en œuvre conformément au concept de maintenance. Les