भारतीय मानक
Indian Standard

IS 15474 (Part 3/Sec 11) : 2014
IEC 60300-3-11 : 2009

निर्भरणीयता प्रबन्धन

भाग 3 अनुप्रयोग मार्गदर्शिका

अनुभाग 11 विश्वसनीयता केन्द्रित रखरखाव

Dependability Management

Part 3 Application Guide

Section 11 Reliability Centred Maintenance

ICS 03.100.40; 03.120.01

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली–110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI-110002
www.bis.org.in www.standardsbis.in

September 2014 **Price Group 13**

Reliability of Electronic and Electrical Components and Equipment Sectional Committee, LITD 02

NATIONAL FOREWORD

This Indian Standard (Part 3/Sec 11) which is identical with IEC 60300-3-11 : 2009 'Dependability management — Part 3-11: Application guide — Reliability centred maintenance' issued by the International Electrotechnical Commission (IEC) was adopted by the Bureau of Indian Standards on the recommendation of the Reliability of Electronic and Electrical Components and Equipment Sectional Committee and approval of the Electronics and Information Technology Division Council.

The text of IEC Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions and terminologies are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.
b) Comma (,) has been used as a decimal marker while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

In this adopted standard, reference appears to certain International Standards for which Indian Standards also exist. The corresponding Indian Standards which are to be substituted in their respective places are listed below along with their degree of equivalence for the editions indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
IEC 60050-191 : 1990 International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service	IS 1885 (Part 39) : 1999 Electrotechnical vocabulary : Part 39 Reliability of electronic and electrical items (*second revision*)	Technically Equivalent
IEC 60812 : 2006 Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)	IS 11137 (Part 2) : 2012 Analysis techniques for system reliability: Part 2 Procedure for failure mode and effects analysis (FMEA) (*first revision*)	Identical

The technical committee has reviewed the provisions of the following International Standards referred in this adopted standard and has decided that they are acceptable for use in conjunction with this standard:

International Standard	*Title*
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

For the purpose of deciding whether a particular requirement of this standard is complied with, the final value, observed or calculated, expressing the result of a test or analysis, shall be rounded off in accordance with IS 2 : 1960 'Rules for rounding off numerical values (*revised*)'. The number of significant places retained in the rounded off value should be the same as that of the specified value in this standard.

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.

Indian Standard

DEPENDABILITY MANAGEMENT

PART 3 APPLICATION GUIDE

Section 11 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.

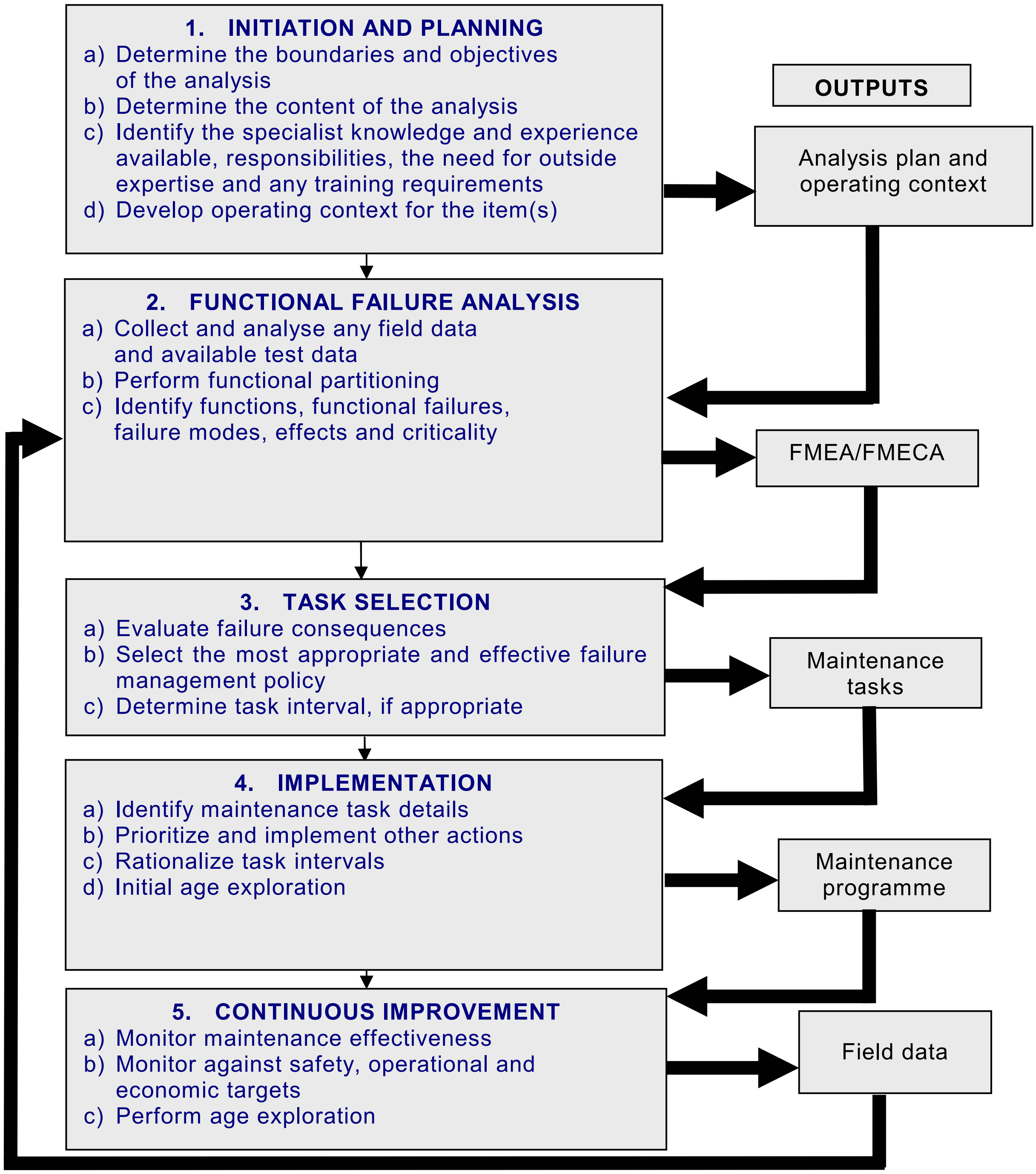

Figure 1 – Overview of the RCM process

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.

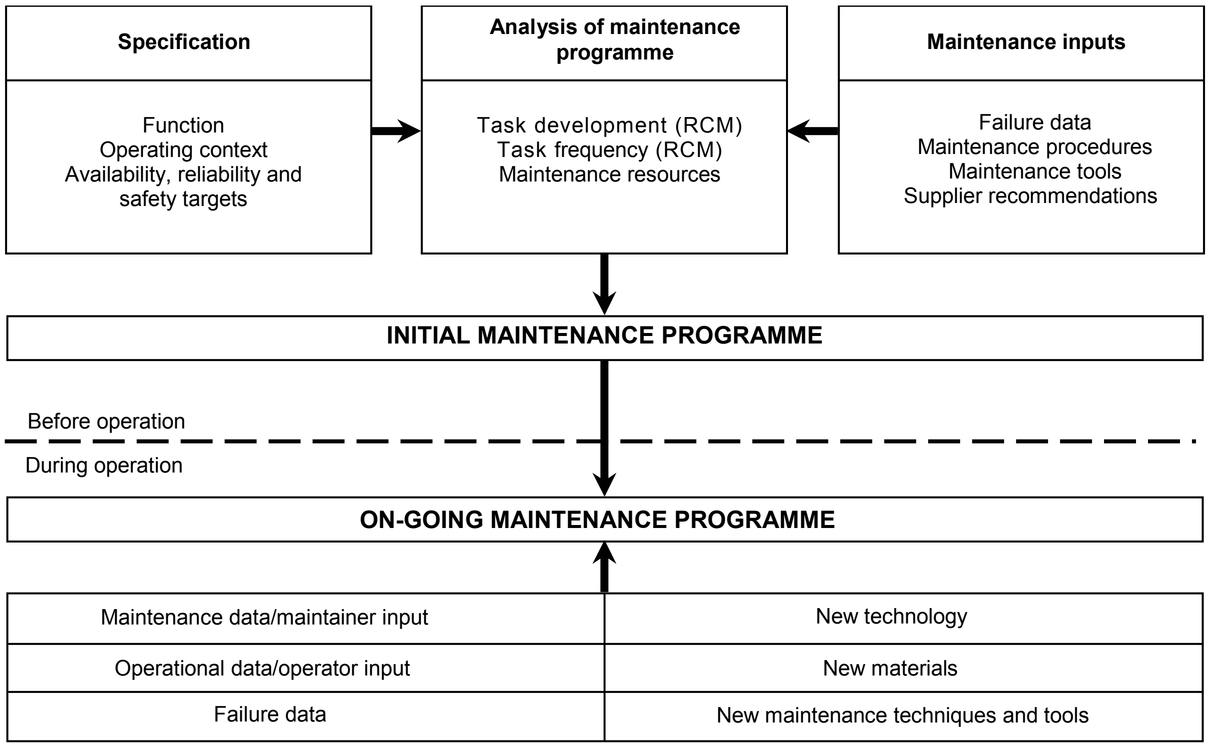

Figure 2 – Evolution of an RCM maintenance programme

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.

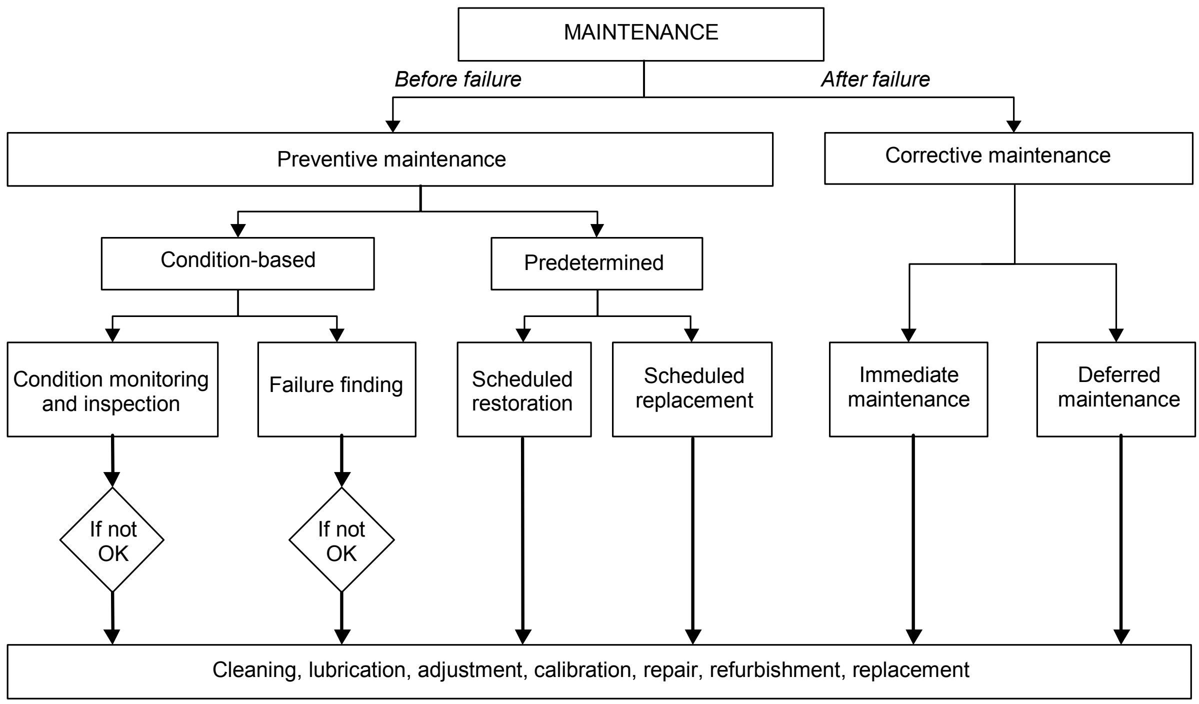

Figure 3 – Types of maintenance tasks

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.

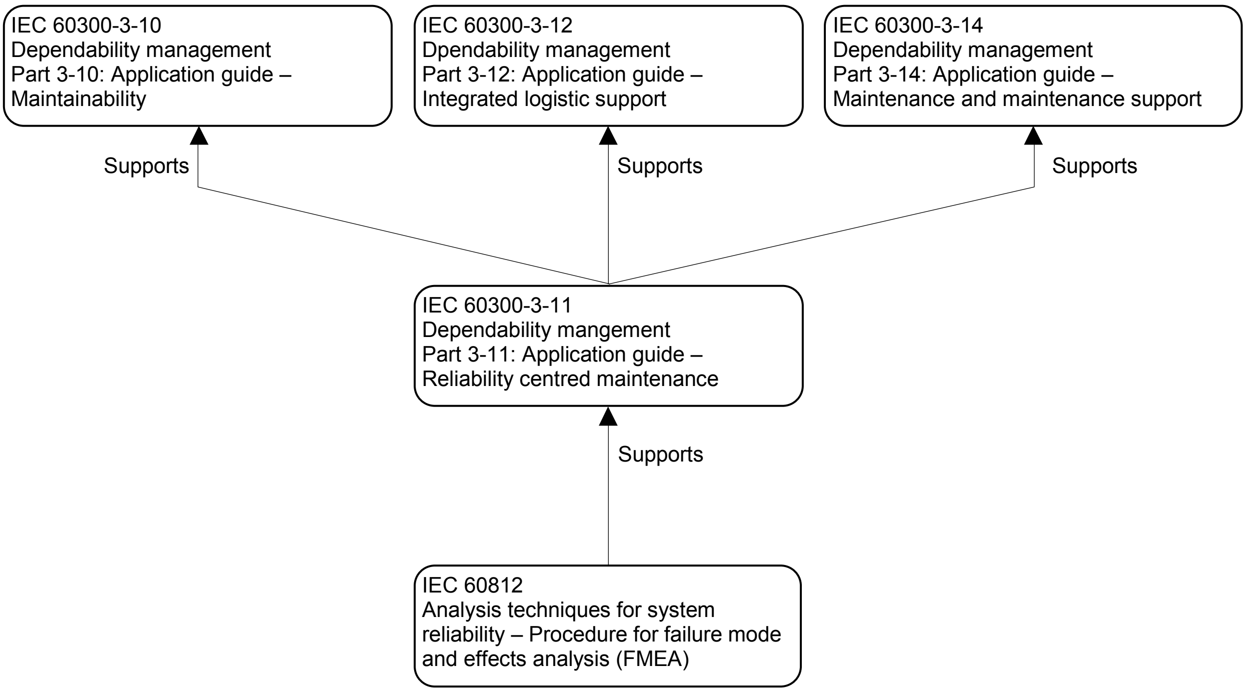

Figure 4 – Relationship between RCM and other support activities

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.

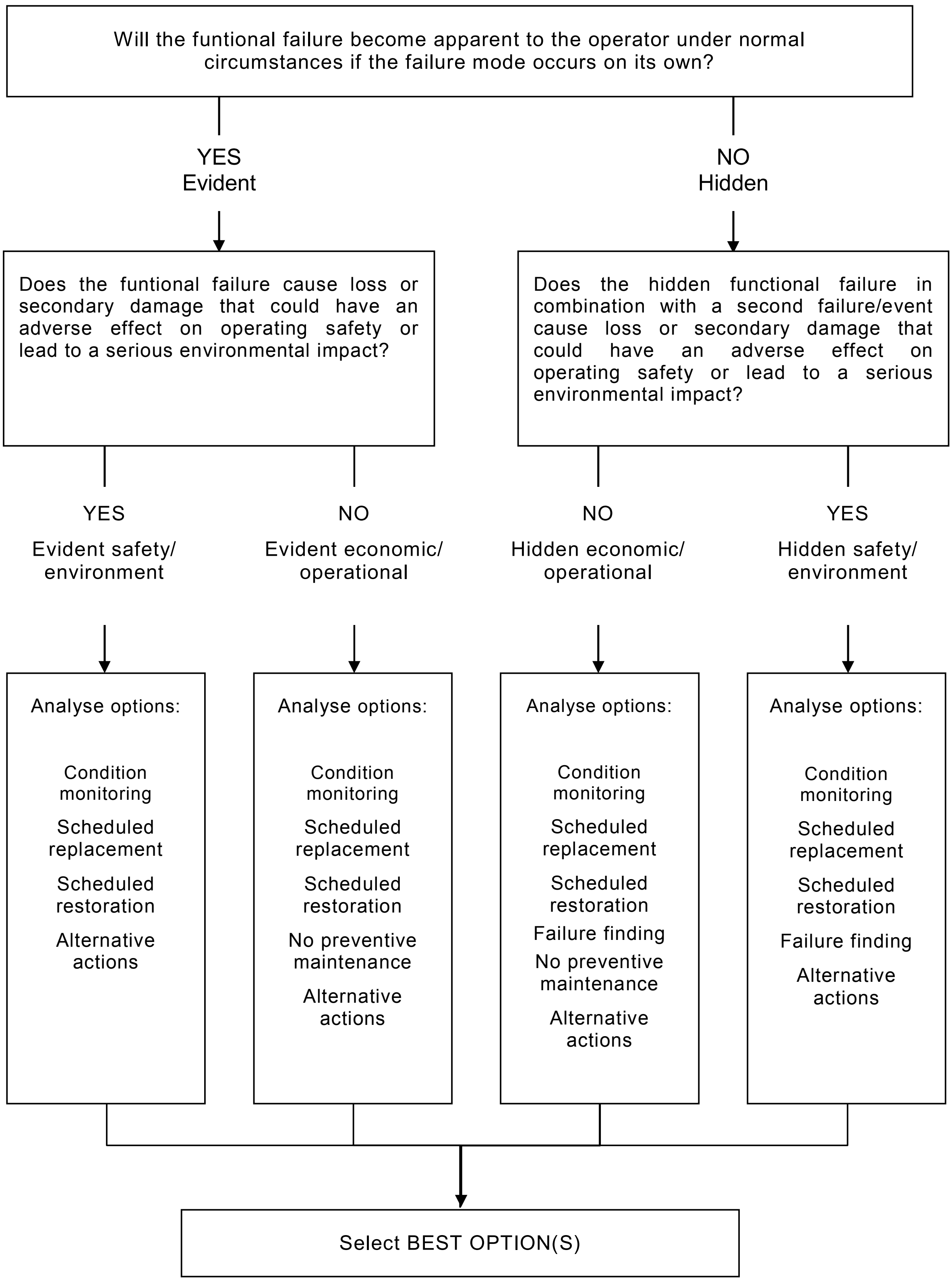

Figure 5 – RCM decision diagram

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.

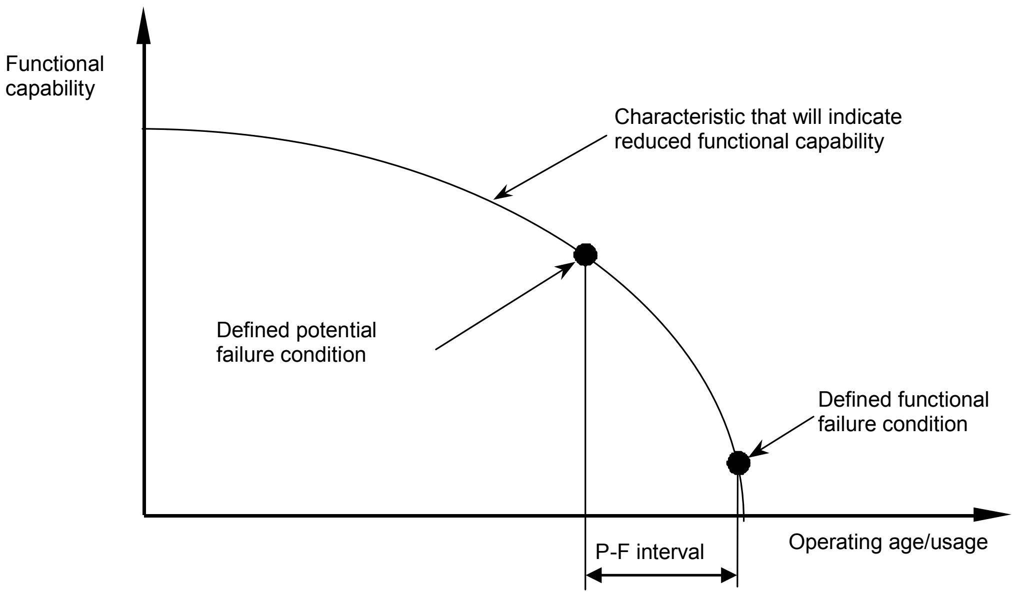

Figure 6 – P-F interval

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.

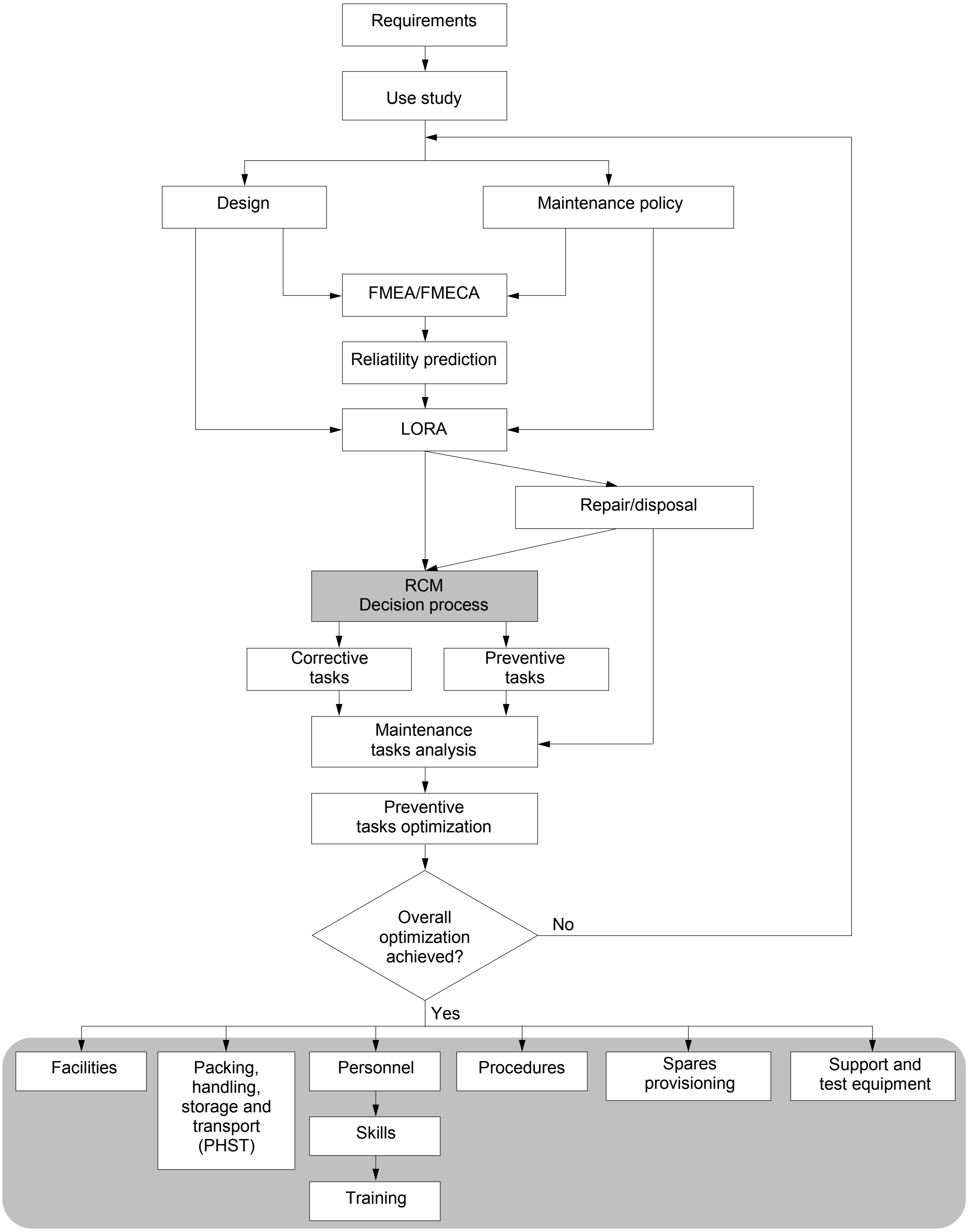

Figure 7 – ILS management process and relationship with RCM analysis

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.

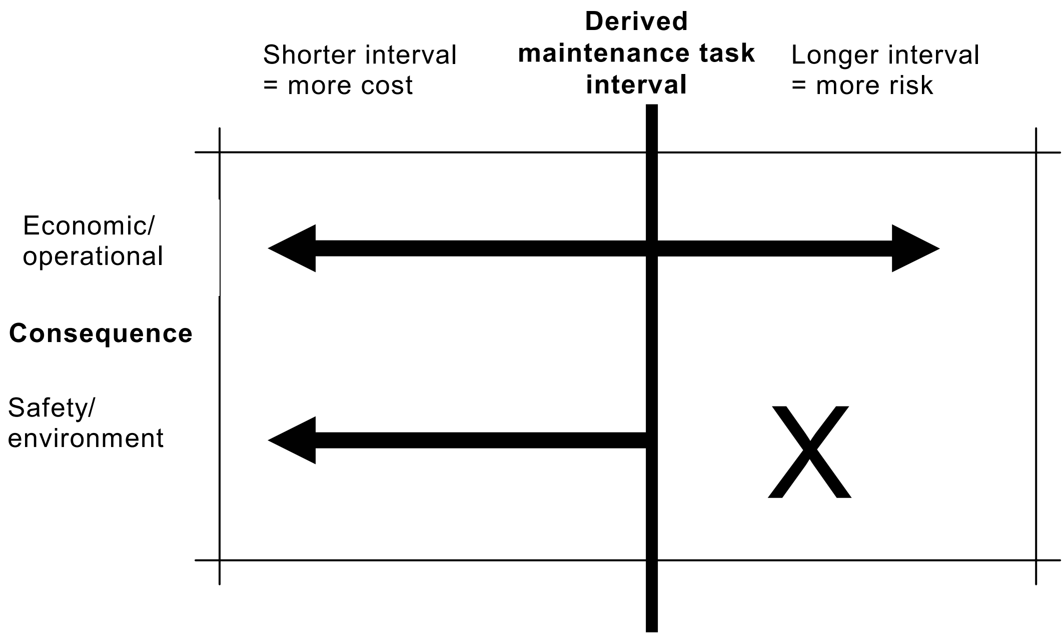

Figure 8 – Risk versus cost considerations for rationalization of tasks

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.

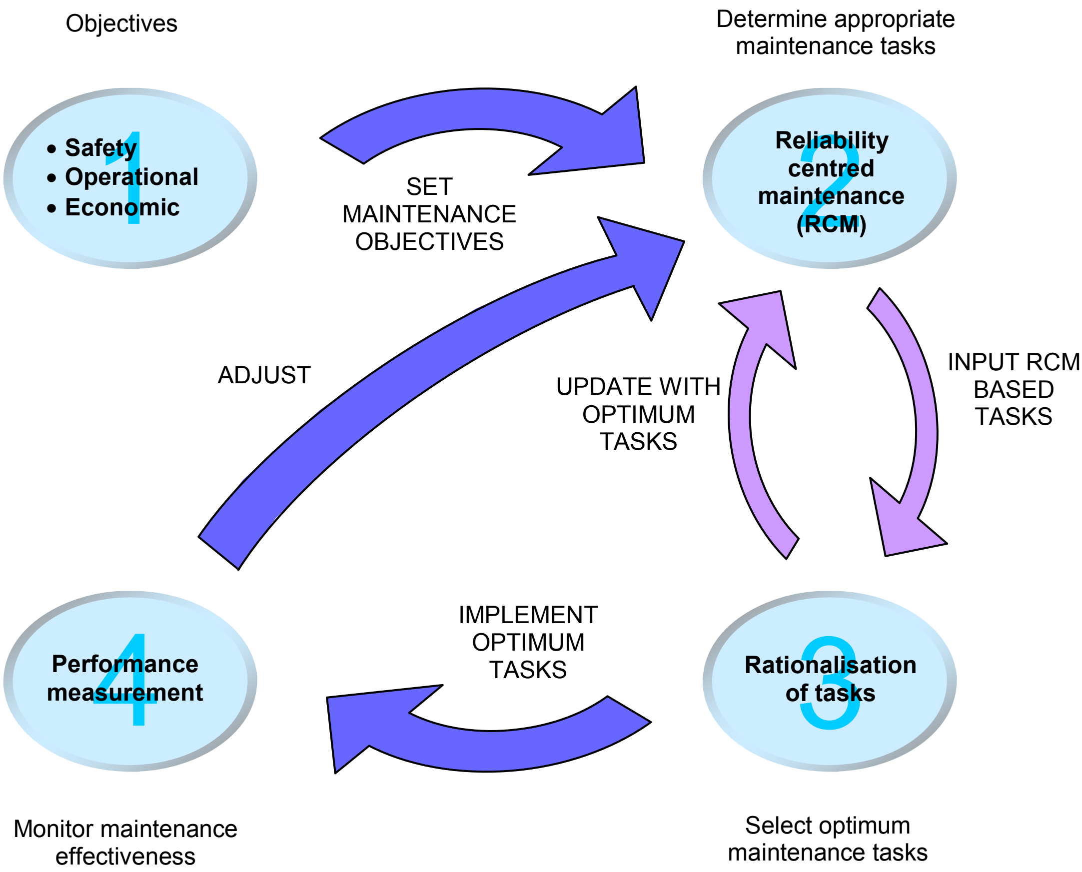

Figure 9 – RCM continuous improvement cycle

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:

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

where

FFI is the failure finding interval;

$MTBF_{\text{pv}}$ 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:

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

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:

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

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:

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

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.

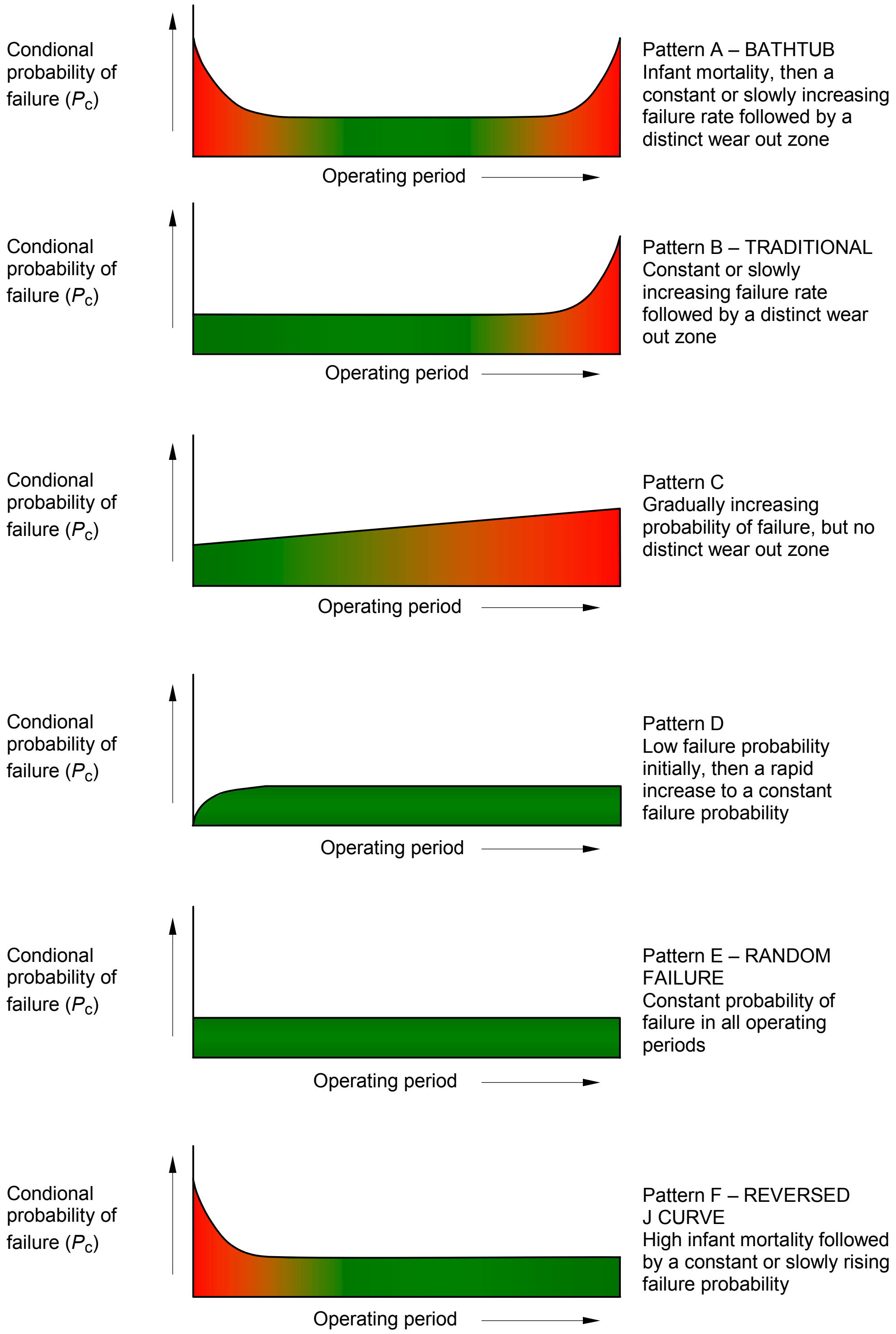

Figure C.1 – Dominant failure patterns

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

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: LITD 02 (3268).

Amendments Issued Since Publication

Amendment No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.org.in

Regional Offices:		*Telephones*
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110002	2323 7617, 2323 3841
Eastern	: 1/14, C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi KOLKATA 700054	2337 8499, 2337 8561, 2337 8626, 2337 9120
Northern	: SCO 335-336, Sector 34-A, CHANDIGARH 160022	260 3843, 260 9285
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600113	2254 1216, 2254 1442, 2254 2519, 2254 2315
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400093	2832 9295, 2832 7858, 2832 7891, 2832 7892

Branches: AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KOCHI. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAJKOT. VISAKHAPATNAM.

Published by BIS, New Delhi