

Australian Standard[®]

**Guide to reliability and
maintainability program
management**

This Australian Standard was prepared by Committee QR/5, Reliability and Maintainability. It was approved on behalf of the Council of Standards Australia on 20 July 1989 and published on 16 February 1990.

The following interests are represented on Committee QR/5:

Australian Electrical and Electronic Manufacturers' Association
Australian Nuclear Science and Technology Organisation
Australian Organization for Quality
Department of Defence
Federal Chamber of Automotive Industries
Federation of Automotive Products Manufacturers
Institute of Quality Assurance
Institution of Engineers, Australia
Institution of Radio and Electronic Engineers, Australia
Telecom Australia

Review of Australian Standards. To keep abreast of progress in industry, Australian Standards are subject to periodic review and are kept up to date by the issue of amendments or new editions as necessary. It is important therefore that Standards users ensure that they are in possession of the latest edition, and any amendments thereto.

Full details of all Australian Standards and related publications will be found in the Standards Australia Catalogue of Publications; this information is supplemented each month by the magazine 'The Australian Standard', which subscribing members receive, and which gives details of new publications, new editions and amendments, and of withdrawn Standards.

Suggestions for improvements to Australian Standards, addressed to the head office of Standards Australia, are welcomed. Notification of any inaccuracy or ambiguity found in an Australian Standard should be made without delay in order that the matter may be investigated and appropriate action taken.

This Standard was issued in draft form for comment as DR 87226.

AS 3960—1990

Australian Standard[®]

Guide to reliability and maintainability program management

First published in part as AS 1211.2—1972.
AS 1211.1 first published 1977.
AS 1211.3 first published 1977.
AS 1211.2—1972, AS 1211.1—1977 and
AS 1211.3—1977 revised, amalgamated and redesignated
AS 3960—1990.

PUBLISHED BY STANDARDS AUSTRALIA
(STANDARDS ASSOCIATION OF AUSTRALIA)
1 THE CRESCENT, HOMEBUSH, NSW 2140

ISBN 0 7262 5892 X



Documents

Document Sharing Hub

PREFACE

This Standard was prepared by the Standards Australia Committee on Reliability and Maintainability, under the direction of the Quality and Reliability Standards Board to supersede AS 1211, *Reliability of electronic equipment and components*, Part 1—1977: *Terminology*, Part 2—1972: *Reliability concepts*, and Part 3—1977: *Reliability program for equipment*.

It is one of a number of Standards to be prepared on various aspects of reliability and maintainability.

It is based largely on BS 5760, *Reliability of constructed or manufactured products, systems, equipments and components*: Part 1: *Guide to reliability and maintainability programme management*. Consideration was also given to IEC Publication 300, *Reliability and maintainability management*, and this Standard is compatible with that publication.

This Standard extends the scope of the AS 1211 series beyond the confines of electronic hardware and increases the detail in which the subject is treated. The presentation of material has been re-formatted so as to provide clear guidance on the separate tasks required for effective reliability and maintainability program management.

© Copyright — STANDARDS AUSTRALIA

Users of Standards are reminded that copyright subsists in all Standards Australia publications and software. Except where the Copyright Act allows and except where provided for below no publications or software produced by Standards Australia may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from Standards Australia. Permission may be conditional on an appropriate royalty payment. Requests for permission and information on commercial software royalties should be directed to the head office of Standards Australia.

Standards Australia will permit up to 10 percent of the technical content pages of a Standard to be copied for use exclusively in-house by purchasers of the Standard without payment of a royalty or advice to Standards Australia.

Standards Australia will also permit the inclusion of its copyright material in computer software programs for no royalty payment provided such programs are used exclusively in-house by the creators of the programs.

Care should be taken to ensure that material used is from the current edition of the Standard and that it is updated whenever the Standard is amended or revised. The number and date of the Standard should therefore be clearly identified.

The use of material in print form or in computer software programs to be used commercially, with or without payment, or in commercial contracts is subject to the payment of a royalty. This policy may be varied by Standards Australia at any time.

CONTENTS

	<i>Page</i>
FOREWORD	4
SECTION 1. SCOPE AND GENERAL	
1.1 SCOPE	6
1.2 REFERENCED DOCUMENTS	6
1.3 DEFINITIONS	6
SECTION 2. RELIABILITY AND MAINTAINABILITY PROGRAM	
2.1 GENERAL	7
2.2 PROGRAM ACTIVITIES	11
SECTION 3. SPECIFICATION OF RELIABILITY AND MAINTAINABILITY	
3.1 GENERAL	19
3.2 WRITING RELIABILITY AND MAINTAINABILITY CLAUSES IN A SPECIFICATION	22
3.3 SPECIFICATION OF RELIABILITY AND MAINTAINABILITY IN PRACTICE	24
SECTION 4. ASSESSMENT AND PREDICTION OF RELIABILITY AND MAINTAINABILITY	
4.1 GENERAL	25
4.2 RELIABILITY ASSESSMENT	25
4.3 RELIABILITY PREDICTION BY MODELLING	25
4.4 PROVISION OF RELIABILITY DATA	25
4.5 RELIABILITY GROWTH TESTING	26
4.6 RELIABILITY DEMONSTRATION AND TESTING	26
4.7 MAINTAINABILITY PREDICTION	27
4.8 MAINTAINABILITY DEMONSTRATION AND TESTING	28
4.9 COMPLIANCE ILLUSTRATION BY MEANS OTHER THAN TESTING	28
SECTION 5. PRODUCTION, FLOW, ANALYSIS AND INTERPRETATION OF RELIABILITY AND MAINTAINABILITY DATA	
5.1 GENERAL	29
5.2 DATA INPUT	29
5.3 DATA SOURCES	34
5.4 DESIGNING THE DATA COLLECTION FORM	35
5.5 VALIDITY OF DATA	35
5.6 COLLECTION AND FLOW OF RELIABILITY DATA	36
5.7 ANALYSIS OF DATA	36
5.8 FAILURE CLASSIFICATION	37
5.9 INTERPRETATION AND PRESENTATION OF DATA	37
APPENDICES	
A TERMS FOR RELIABILITY AND MAINTAINABILITY	38
B EXPLANATION OF RELIABILITY AND MAINTAINABILITY TERMINOLOGY	43
C INDEX OF TERMS FOR RELIABILITY AND MAINTAINABILITY	45

FOREWORD

A standardized systematic approach to reliability and maintainability of manufactured and constructed products is essential to ensure that pertinent statements are consistent and unambiguous in all communications. As well as providing a basis for the preparation of reliability and maintainability programs, this Standard can be used in preparing documents concerned with the specification of reliability and maintainability or the reporting of reliability and maintainability data or tests. Maintainability is applicable for systems and equipments that are repaired following failure.

It is vital that reliability and maintainability be considered in a manner similar to the other characteristics of a system, equipment or item, from its design conception to the end of its working life, and that the reliability and maintainability experience of one generation of products, engineers or technology is used by the next. This requires that each factor affecting reliability and maintainability at any stage in the life of an item be identified and considered in its relationship to the other factors. A reliability and maintainability program is the formalization of this procedure. It may be necessary to divide such a program into two parts, one of which may be the concern of the designer and manufacturer, and the other the concern of the user. It is most important that consideration be given to the reliability and maintainability of items or parts which are used by one manufacturer but produced by another, i.e. subcontractor evaluation and vendor appraisal (see AS 1821, AS 1822, AS 3901 and AS 3902).

Satisfactory reliability and maintainability have traditionally been achieved by the use of codes of practice or methods of working that have been shown by experience to give good results for established products. However, with the increase in pace of change and performance expectations, it is no longer sufficient to consider reliability and maintainability in purely qualitative terms when their achievement often demands the specification of quantitative criteria. Accordingly, the onus should be on all parties (i.e. the designer, supplier, purchaser or any other responsible authority) to specify quantitative requirements wherever possible.

With the need to satisfy competing constraints, including stricter health and safety requirements, the advent of new materials and pressure to reduce costs, reliability and maintainability should be expressed in quantitative terms if they are to be given their proper weight. For example, a product may be required to achieve at least a certain useful life, not to exceed a certain failure rate or to have an extremely high availability. Quantitative statements relating to reliability and maintainability should then be made which may be accompanied by stipulations that certain codes of practice be followed.

One aspect of quantitative reliability and maintainability that requires emphasizing is that often reliability and maintainability can be predicted even for products of new design and high cost, such as a ship's propulsion system or a new kind of nuclear reactor pressure vessel, but only if there is sufficient knowledge of the processes leading to failure, including data based on the statistical analysis of observations made.

The designer's or user's confidence that reliability and maintainability requirements will be met depends on the following:

- (a) Adequacy of the data about failures.
- (b) Correct interpretation of such data in the existing environment.
- (c) A disciplined approach to the specification and design of the product or service.

Data should be obtained about failures from the following sources:

- (a) Reliability testing.
- (b) Field data.
- (c) Knowledge of the physical processes leading to failure.

A reliability and maintainability program sets out to provide products with acceptable levels of reliability and maintainability at an acceptable cost rather than products with improved reliability and maintainability regardless of cost. For this reason the quantitative approach is essential. The qualitative approach can be effective in improving reliability and maintainability but the improvement can not be quantified.

In general terms and philosophy this Standard is equally applicable to all parts of a system, including the software. The subject of software reliability and maintainability is considered to be a separate discipline, and the techniques of software reliability and maintainability are not dealt with in detail in this Standard, except where they interface at the system level.

However, it is important to recognize that software as a product is different from all other engineering products in that it is not tangible, and it does not wear out. Software exhibits faults, but, unlike hardware faults, they originate in undetected errors in the software specification, design logic and the coding process. These errors generate faults only when that part of the program is executed and specific (input) conditions exist. The errors mature into failures when they affect the response of the system. Such software-induced system failures exhibit time dependency because the range of system inputs may vary with time, and the process of a mistake maturing into a failure is of uncertain duration and depends on the application of the system. Software reliability and maintainability assurance is therefore not a question of showing, avoiding or compensating for changes such as wear, but of attempting to detect or limit the effect of mistakes in design.

While systems have always had a logic content, the advent of computers has afforded the opportunity to incorporate very large, complicated and often subtle logic structures. These structures often exceed the capability of the human mind to perceive them in total and thus the difference in scale of the logic now possible brings a greater chance of human error at all stages of the life cycle.

STANDARDS AUSTRALIA

Australian Standard

Guide to reliability and maintainability program management

SECTION 1. SCOPE AND GENERAL

1.1 SCOPE. This Standard provides guidance on reliability and maintainability program management of manufactured and constructed products. It discusses the essential features of a comprehensive program for the planning, organization, direction and control of resources to produce systems, equipment and components which will be reliable and maintainable. In management terms it is concerned with what has to be done, and why, and when and how it has to be done, but it cannot be specific about who should do it and where, because organizations and projects vary widely.

Section 2 reviews the essential features of a comprehensive reliability and maintainability program, setting out a logical framework in which the activities described in the other Sections can take place.

Section 3 describes the steps that should be followed when a specification of reliability and maintainability is drafted. The Section provides guidance on the inclusion of reliability and maintainability clauses in specifications relating to the performance, construction, testing and installation of manufactured products, and indicates the nature of the reliability and maintainability statements appropriate to each specification.

Section 4 is an introduction to the means by which quantitative values can be assigned to the reliability and maintainability of systems, equipment and components at various stages in their life cycle, and the factors that influence that assignment.

Section 5 describes the processes of assimilation and utilization of the data on which assessment and prediction of reliability and maintainability are based.

Appendix A provides the user with a supplementary list of terms for reliability and maintainability, taken from IEC Publication 271, which are not found in AS 1057.

NOTES:

1. Appendix B provides an explanation of reliability and maintainability terminology.
2. Appendix C provides a complete index of terms for reliability and maintainability.
3. Many but not all of the program elements described in this Standard are applicable to the achievement of reliability and maintainability of services.

1.2 REFERENCED DOCUMENTS. The following documents are referred to in this Standard:

AS

- | | |
|------|--|
| 1057 | Quality assurance and quality control—Glossary of terms |
| 1199 | Sampling procedures and tables for inspection by attributes |
| 1821 | Suppliers quality systems for design, development, production and installation |
| 1822 | Suppliers quality systems for production and installation |
| 2490 | Sampling procedures and charts for inspection by variables for percent defective |
| 2529 | Collection of reliability, availability and maintainability data for electronics and similar engineering use |
| 2530 | Presentation of reliability data on electronic and similar components |
| 2990 | Quality systems for engineering and construction projects |
| 3900 | Quality systems—Guide to selection and use |
| 3901 | Quality systems for design/development, production, installation and servicing |
| 3902 | Quality systems for production and installation |

BS

- | | |
|------|--|
| 5760 | Reliability of systems, equipments and components—
Part 2: Guide to the assessment of reliability |
|------|--|

IEC

- | | |
|-----|--|
| 271 | List of basic terms, definitions and related mathematics for reliability |
|-----|--|

1.3 DEFINITIONS. For the purpose of this Standard the definitions given in AS 1057 and the terms listed in Appendix A of this Standard apply.

SECTION 2. RELIABILITY AND MAINTAINABILITY PROGRAM

2.1 GENERAL.

2.1.1 Life cycle concept. The reliability and maintainability activities to be implemented for each phase of the product life cycle need to be selected within the context of the total life cycle of the product. Decisions made at any time have an impact on product reliability, maintainability and cost at that time, and in subsequent phases of the product life.

The product life cycle has a number of distinct phases as follows:

- (a) *Definition phase*—in which the concept and the need for the product are decided and its basic requirements are defined, usually in the form of a product specification agreed upon between manufacturer and user.
- (b) *Design and development phase*—in which the product hardware and software are created to perform the functions described in the product specification. This phase will normally include the assembly and testing of a prototype product, under laboratory simulated conditions or in actual field trials, and the formulation of detailed manufacturing specifications and instructions for operation and maintenance.
- (c) *Production phase*—in which the design is put into production.
- (d) *Installation and commissioning phase*—in which, in the case of large complex products, the installation of the product on a particular site may be regarded as an extension of the production phase.
- (e) *Operation and maintenance phase*—in which the product is operated for the period of its useful life. During this phase, essential preventive and corrective maintenance actions are taken and product performance is monitored. The useful life of a product ends when its operation becomes uneconomic because of increasing repair costs or other factors, or the product becomes technically obsolete.
- (f) *Disposal phase*—in which the product reaches the end of its planned useful life, or the requirement no longer exists for the product, and it is disposed of, destroyed, or, if economically feasible, modernized.

2.1.2 Aim of a reliability and maintainability program. The aim of a reliability and maintainability program as part of a quality system is to ensure that adequate and effective effort is brought to bear on reliability, and maintainability (for maintained products), during all phases of the life-cycle of an item; and to ensure activities which contribute to reliability and maintainability are properly integrated with other contract/specification activities. The program should provide continuous study of both quantitative and qualitative requirements throughout all phases of a project; reliability and maintainability assessments should be updated; specified requirements should be verified; and the reliability and maintainability activities should be integrated with other elements of the development, production and operation program.

In many projects there are no sharp demarcations between the definition, design and development, production and operation phases. However, for clarity, distinctions are drawn in this Section. The activities appropriate to the different phases are as given in Table 1.

Activities are also shown in flow diagram form in Figure 1. They are explained in the text of this Section in relation to overall project management responsibilities and time scale. Some of these activities have a direct bearing on the reliability and maintainability achieved in service but they are contained in other program elements. The reliability and maintainability program should therefore be prepared and implemented in conjunction with the other parts of the quality program and safety program.

NOTE: Examples of requirements for a quality system are given in AS 1821, AS 1822, AS 2990 and AS 3900.

2.1.3 General considerations on maintainability.

In common usage, maintainability is concerned with two very different concepts—

- (a) hardware; where the purpose is to retain the item in, or restore it to its required state; and
- (b) software; where the purpose is to correct inadequacies.

In hardware systems, maintainability has a direct influence on system availability. Reliability and maintainability should be planned together throughout design and development and integrated wherever possible to maintain a balance with life cycle costs.

In systems containing software, maintainability refers to the ease with which the software can be modified in order to bring it in line with the original requirements. The maintainability program should ensure that software maintenance can be performed with the minimum effect on the reliability of the system.

2.1.4 Cost considerations. It may be neither necessary nor desirable to fully implement all the activities described in this Section. A suitable compromise should be reached whereby reliability and maintainability needs are balanced against all the other factors. Whole life costs are the sum of the initial acquisition costs and costs of subsequent ownership. For complex equipment the ownership cost can be a high proportion of whole life costs. Furthermore, a properly integrated reliability and maintainability program, as illustrated in Figure 2, can show an overall cost benefit to the manufacturer in terms of reduced costs of technical support, repair and replacement, and warranties. It can also lead to increased competitiveness and goodwill and have a vital significance in the prevention of product liability claims. It follows, therefore, that there should be continuous communication between the design authority/manufacturer and the customer/user after the customer has formulated his reliability and maintainability requirements. The procedures set out in this Section give guidance on implementing an effective reliability and maintainability program, which should be integrated with design, development and production activities, thus allowing its overall

objectives to be achieved in the most cost-effective way. Maintainability is only applicable to systems and equipment that are subject to repair and maintenance. The product development and production activity decision making process should consider the impact of—

- (a) the complexity, the development risk and function of the product, and the hostility of the environment in which it is to be used;
- (b) the availability of reliability and maintainability data;
- (c) the value of the appropriate reliability and maintainability (if applicable) characteristic for the principal phases in the total life;
- (d) demonstration and guarantees required;
- (e) facilities, workload and schedule;
- (f) reliability and maintainability aspects of operation and safety;

- (g) maintenance, logistics support and future requirements;
- (h) design, development and manufacture; and
- (i) ownership costs, e.g. operation, maintenance, energy, etc.

2.1.5 Relative effectiveness of program activities.

It is not possible to predict accurately the relative effectiveness of each activity on improving reliability and maintainability. The choice of activities and the resources to be expended on each should be based on past experience of similar projects. The following statements are offered as a general guide:

- (a) The earlier a design change can be agreed, the lower the total cost is likely to be. The cost of making a design change at the production or usage stage is normally many times the cost of doing so at the initial design and development stage.

TABLE 1
RELIABILITY AND MAINTAINABILITY PROGRAM ACTIVITIES DURING
THE PRINCIPAL PHASES OF A PROJECT

Phase	Activities	Subclause
Definition	Feasibility study	2.2.1.1
	Statement of reliability and maintainability objectives and requirements	2.2.1.1
	Reliability and maintainability specification and contract formulation	2.2.1.2
Design and development (including initial manufacture)	Analysis of parts, materials and processes	2.2.2.3(b)
	Analysis of established and novel features	2.2.2.3(c)
	Failure mode, effect and criticality analysis	2.2.2.3(d)
	Incident sequence analysis (fault tree analysis)	2.2.2.3(e)
	Stress and worst case analysis	2.2.2.3(f)
	Reliability prediction	2.2.2.3(g)
	Redundancy analysis	2.2.2.3(h)
	Human factors	2.2.2.3(i)
	Design review	2.2.2.3(j)
	Design audit	2.2.2.3(k)
	Design change control	2.2.2.3(l)
	Maintainability analysis	2.2.2.3(m)
	Maintainability prediction	2.2.2.3(n)
	Maintainability design criteria	2.2.2.3(o)
	Safety program	2.2.2.4
	Test plans	2.2.2.5(a)
	Parts and sub-assembly testing	2.2.2.5(b)
	Performance and environmental testing	2.2.2.5(c)
	Accelerated testing	2.2.2.5(d)
	Endurance testing	2.2.2.5(e)
	Reliability growth testing	2.2.2.5(f)
	Development reliability demonstration testing	2.2.2.5(g)
	Maintainability test and demonstration	2.2.2.5(h)
	Data collection, analysis and feedback	2.2.2.5(i)
Production	Preservation of reliability achievement	2.2.3.1
	Quality conformance verification	2.2.3.2
	Screening (run-in, bed-in or burn-in) of components and assemblies	2.2.3.3
	Production reliability demonstration testing	2.2.3.4
	Maintainability in production	2.2.3.5
	Additional software check	2.2.3.6
Installation and commissioning	System acceptance	2.2.4.1
	Commissioning tests	2.2.4.2
	Reliability growth	2.2.4.3
	Reliability and maintainability demonstration	2.2.4.4
	Data collection	2.2.4.5
	Reliability and maintainability assessment	2.2.4.6
Operation-Usage and maintenance	Data collection, analysis, feedback and redesign/modification	2.2.5.1
	Maintenance	2.2.5.2

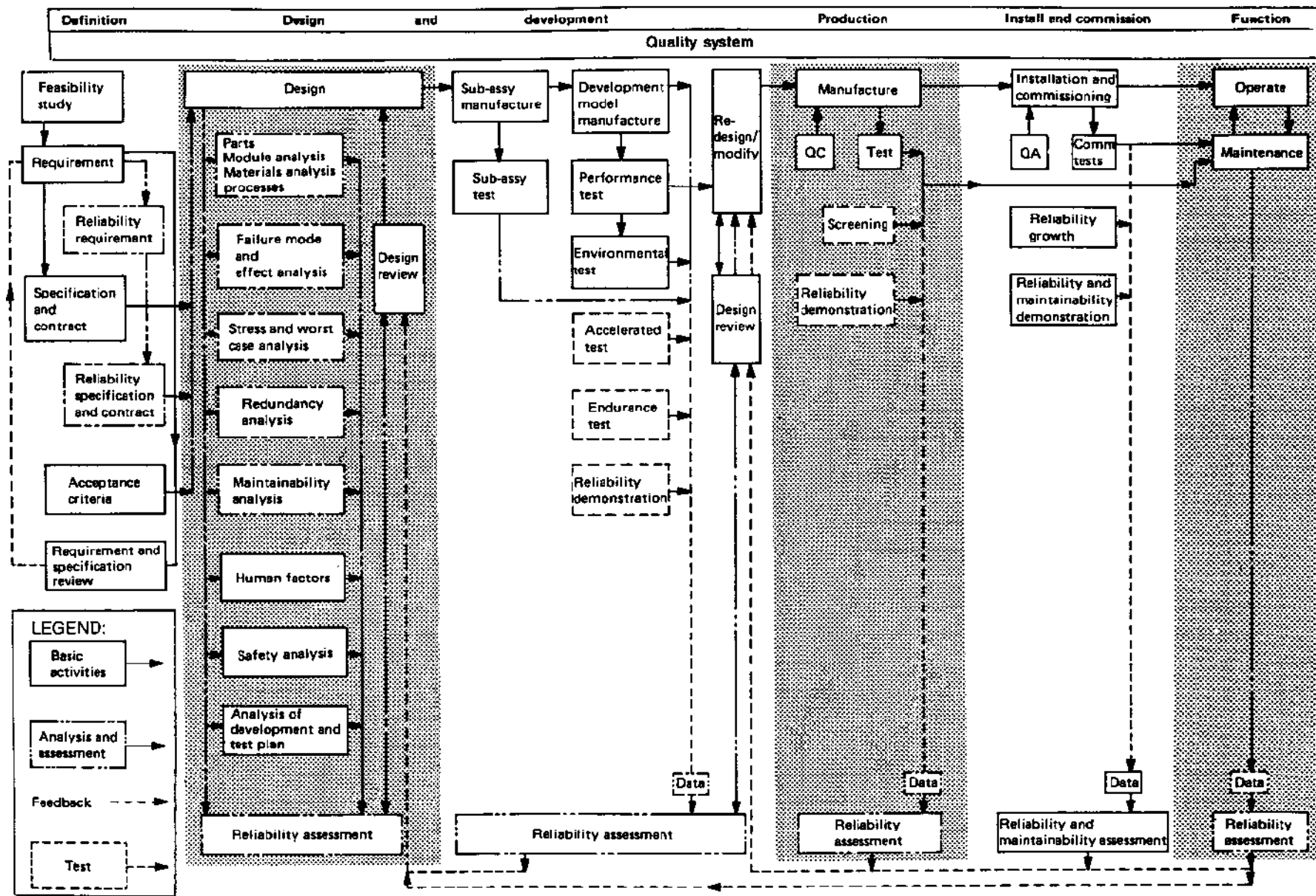


FIGURE 1 RELIABILITY AND MAINTAINABILITY PROGRAM CONCEPT

COPYRIGHT

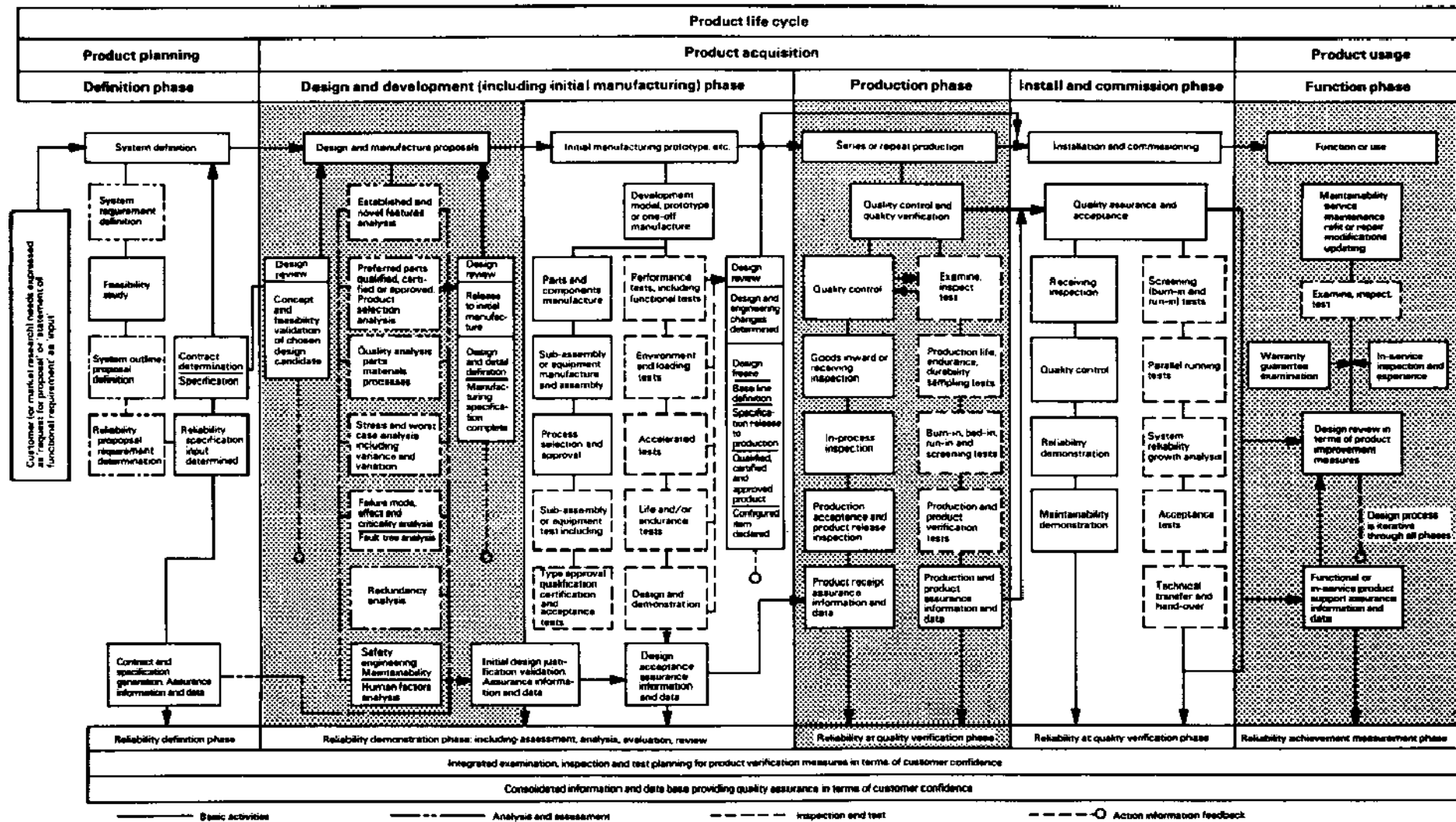


FIGURE 2 TYPICAL RELIABILITY AND MAINTAINABILITY PROGRAM

- (b) For complex items, design evaluation and review, use of proven parts and processes, and the use of redundancy or derating within the design can greatly enhance overall system reliability and maintainability. Large scale use of system redundancy can greatly improve overall system reliability and maintainability, but at an increase in initial cost and maintenance load. It should be noted that the useful system redundancy may be limited by common mode (or common cause) failures.
- (c) Reliability testing, including corrective action, carried out during the development and production phases, is an effective means of increasing the reliability and maintainability of complex products as well as increasing confidence that the required level has been attained.
- (d) Reliability improvement depends on several factors, such as the effectiveness of procedures for identifying, reporting and taking action on failures, the way the program is managed and the use to which failure analyses are put.
- (e) The achievement of good maintainability in design depends upon the thorough analysis of the requirement through prediction, modelling and allocation, followed by adherence to specific design techniques. Maintainability demonstration is applied iteratively during the design and development phase to provide confidence that maintainability requirements will be met.

2.1.6 Training. Personnel should have training and experience relevant to their reliability and maintainability tasks.

Reliability and maintainability disciplines should be incorporated in training programs for personnel who will be responsible for operating, maintaining and supporting the product. The training and support programs should consider the types and levels of training that will be needed by the different personnel.

Training requirements should be planned early in the reliability and maintainability program. Training and support programs should be co-ordinated with product development planning, maintenance policy, and the operational requirements of the product.

2.2 PROGRAM ACTIVITIES.

2.2.1 Definition phase.

2.2.1.1 Feasibility study and statement of objectives and requirements. At the definition phase, the originator of the requirement should consider the reliability and maintainability characteristic that will be required of the product in its different phases, and the factors which will influence this. These factors include—

- (a) the complexity of the product;
- (b) the state of development of similar products and of the parts to be used including the availability, accuracy and relevancy of reliability data;
- (c) the method of use of the product, such as duty cycles, maintenance, frequency of inspection and expected life;
- (d) the expected environmental conditions, which should include operating and non-operating conditions, packaging, transport and storage;

- (e) the constraints imposed by other requirements, e.g. performance, size, mass, safety and costs;
- (f) provision for changes in requirements during the life of the product; and
- (g) maintenance and logistic support philosophy.

For complex products it may be necessary to carry out a preliminary study to assess the reliability and maintainability likely to be attainable under the conditions expected, in order to set a sensible target. This study should be in accordance with Section 4.

2.2.1.2 Specification and contract. When the feasibility of each relevant reliability and maintainability characteristic has been determined and its value set and agreed on, it should be stated as the specified reliability and maintainability that is to be achieved and demonstrated for the product. This requirement or objective should then be included in a specification or contract. The specification should take into account factors such as those given in Clause 2.2.1.1 of this Standard, in as much detail as is necessary, and it should be drawn up in accordance with Clause 2.1.1. Arrangements should be made in the overall program to allow for the reliability and maintainability elements to be reviewed in terms of the overall program, at predetermined intervals.

2.2.2 Design and development phase.

2.2.2.1 Establishment of product design guidelines and codes. Design guidelines and codes should be compiled for use by design and development engineers. These will include the producer's and customer's preferred or required design disciplines and maintenance policy, and a listing of all relevant Industry and Government Standards and Regulations, Codes and Practices.

2.2.2.2 Evaluation of costs. Consideration of product cost is a significant element of each product design and development program. An evaluation of life cycle cost of design alternatives should be part of the program.

2.2.2.3 Analyses and other activities.

The reliability and maintainability plan should establish a preliminary schedule for these analyses which takes into account major program milestones and the costs of performing these analyses.

Analyses and other activities are as follows:

- (a) *Allocation of reliability and maintainability objectives.* Reliability and maintainability targets should be allocated to subsystems so that the system's reliability and maintainability requirements can be achieved in an optimal manner; considerations, for example are—product development time, system availability and life cycle cost.
- (b) *Parts, materials and process analysis.* The design stage should include an analysis of the reliability and maintainability implications of all parts, materials and processes called up in the initial design. As far as practicable, parts or sub-assemblies whose reliability and maintainability characteristics (at the stress levels expected) are known, should be selected. Wherever possible, the number of different part types should be minimized by use of standard products.

For systems containing software, the designer should select (based on known reliability and maintainability data) existing software, proven languages and compilers, etc.

- (c) *Established and novel features analysis.* The design should be analysed to identify those features that are established practice and those that are novel, including features that use novel components, novel software techniques, etc or use established components in novel ways. The reliability and maintainability of each innovation in the design should be assessed by analysis or testing in order to justify the proposed innovation objectively.
- (d) *Failure mode, effect and criticality analysis (FMECA).* The design should be analysed in order to determine possible modes of failure and their effects on system operation. The primary objective of such analysis is to discover critical failure areas and design characteristics. It can be carried out either by starting at the system level and expanding downwards, or from the component level upwards, to a level commensurate with necessity, time available and required assurance. Within the analysis, each potential failure should be considered in the light of the probability of occurrence and categorized as to its probable effect on the successful operation of the system or item.

This will aid in allocating resources for corrective design action, reliability and maintainability, and development engineering. Such analysis should be a major consideration in design reviews and should always be used to provide acceptance criteria for test planning and the establishment of check out and diagnosis procedures when required. Depending upon the nature of the system, major sub-units may require separate analysis, often to meet specific legal or safety code requirements, e.g. ships, bridges, aircraft, high pressure vessels in process plants and real time computing systems.

Elements of the analysis are as follows:

- (i) *Failure mode analysis*—a study of the system and the working interrelationships of its components under various anticipated conditions of operation (normal and abnormal) in order to determine probable failure location, mode and mechanism.
 - (ii) *Failure effect analysis*—a study of the potential failures that might occur in any section of the system, in order to determine the probable effect of each on all other components, or sections, and on operational success.
 - (iii) *Failure criticality analysis*—a study of the potential failures in any section of the system in relationship to other sections of the system, in order to determine the severity of each failure effect in terms of a probable safety or environmental hazard, unacceptable degradation of performance, or loss of operation or availability of the system.
 - (iv) *Fault recovery analysis (applicable to software)*—a study of the extent to which a fault can be bypassed or corrected automatically.
- (e) *Incident sequence analysis (fault tree analysis).* In cases where a major system failure can be identified, it may be helpful to use a fault tree analysis to identify possible causes. This consists of an analysis of possible causes starting at system

level and working down to component level, identifying all possible causes.

NOTE: This technique is often used for the development of maintainability programs and maintenance procedures.

- (f) *Stress and worst case analysis.* This is an analysis to ensure that the design will not cause overstressing of components due to specified (or postulated abnormal) combinations of input conditions, output loading, environmental conditions and parts' tolerances. This has the purpose of ensuring that safety and reliability and maintainability margins are adequate. Stress conditions may be specified by regulating codes of practice, e.g. boiler and pressure vessel codes, lifting and winding gear codes, civil air worthiness and in-flight requirements and motor vehicle safety legislation requirements. A complete analysis can be time consuming and costly, and priority should be given to possible trouble areas indicated by the failure mode, effect and criticality analysis.

NOTE: In systems containing software the analogous activity will be ensuring that, under conditions of specified (or postulated abnormal) stimuli from the outside world, no part of the system will operate outside permitted time bounds, capacity bounds, etc.

- (g) *Reliability prediction.* Using an appropriate mathematical model the relevant reliability and maintainability characteristics of the product should be predicted from published, laboratory, field parts or subsystem reliability and maintainability data, for the purpose of providing an indication as to whether the product's target reliability and maintainability specification can be met.
- (h) *Redundancy analysis.* An analysis to ascertain the need for redundancy should be performed on design of items, failure of which may be critical in terms of safety, costs, down time, etc. The analysis consists of a review of any aspect of the design that can be replicated in order to provide an alternative means of performing the required function in case of failure. This analysis should consider the possible options in terms of effect on overall reliability and maintainability, balanced against other features such as cost, size and mass. The type of redundancy selected will be determined largely by the effects of failures against which redundancy is provided, in which case the designer should consider the provision of indicators, warnings or alarms to draw attention to a failure on one path. This is essential in the case of critical items where redundancy is active or automatic. The effect of tandem working upon individual item reliability and maintainability (reduced stress), the increased maintenance load and the reliability and maintainability of changeover should also be considered in reaching a decision on whether to add redundancy and, if so, what form it should take (active or standby).
- (i) *Human factors.* The possibility of human error leading to unreliability and maintenance errors should be considered over and throughout the life cycle of the product. In particular, careful consideration should be given to the way in which reliability and maintainability of an item or system may be reduced by the following:
- (i) *Communication.* Good communication is essential for reliability and maintainability throughout the life-cycle of a system. One of the most difficult and sophisticated communi-

cation phases occurs when a design specification is being created, when it should be visible or communicable to those involved and affected, e.g. designers, maintainers, and quality controllers.

- (ii) *Design.* Care should be given to the structure of the design, the design teams and the design interface so that at every level the logic of the design can be perceived. Nevertheless, in the design phase human error produces faults. To eliminate such faults, methods of fault detection and well-structured procedures are required e.g. drawing inspection, computer program walk-through (check), simulation and task analysis.
- (iii) *Operation.* Careful consideration should be given to the way in which the reliability and maintainability of the product may be influenced by the performance and attitude of the operator. This requires an analysis of the operator's function and information needs, the way in which the information is provided, the operation response required, the physical actions required to respond and the response time allowed. Where the analysis reveals unsatisfactory features, design changes may be necessary. In some cases it may be possible to quantify the element of human (personnel) unreliability and maintainability in the total system, but in general this analysis is qualitative.
- (j) *Design review.* The design program should include formal reviews at appropriate stages of design, development, production and in-service usage, to evaluate achievement of the reliability and maintainability and maintenance requirements. The review(s) should be a formal systematic study of the design, to be carried out jointly by specialists from the supplier's(s') and purchaser's organization(s) and should take account of such considerations as—
 - (i) current reliability and maintainability estimates and achievements, identification of principal items inhibiting reliability and maintainability, and reviews of reliability and maintainability effort;
 - (ii) potential design/production/installation problem areas;
 - (iii) reliability and maintainability analysis reports;
 - (iv) proposed design trade-offs, solutions to reliability and maintainability problems, and status of previous review actions;
 - (v) effects of reliability and maintainability engineering on design;
 - (vi) the extent of software in the system and the effect on reliability and maintainability of the design approach adopted for the software; and
 - (vii) evaluation of significant differences between the present and proven designs.

Minutes should be kept of these formal reviews, and provision should be made for the issuing of progress reports.

- (k) *Design audit.* A critical examination of the design should be made in order to ensure that there will be an acceptable level of reliability and maintainability in operational use. It should be carried out by engineers independent of the design process, and should cover all aspects of the manufacturing process from the design concept to testing, installation, operation, and degradation of performance in service and maintenance. The audit should identify any design weaknesses requiring modifications but it should not offer a solution to the problems; the latter is the province of the designer.
- (l) *Design control and design change control.* A systematic procedure for review of evaluations, analyses, appraisals and assessments of each change during the evolution of the design should be established to ensure that 'reliability and maintainability growth' during initial design and development phases is shown to be adequate and satisfactory. All changes to the design after it has reached the point of release for production or installation are regarded as engineering changes. These also should be governed by design change control measures to ensure reliability and maintainability is not unacceptably reduced by later design changes made for reasons not concerned with reliability and maintainability, e.g. ease of production, value analysis and value engineering.
- (m) *Maintainability analysis.* Maintainability analysis uses information from feasibility analyses, failure mode and effect analyses, and trade off studies to provide design guidance for maintainability. The analysis should include assessment of accessibility, interchangeability, modularity, standardization, operator/maintainer requirements, test and maintenance requirements, spares provisioning and maintenance policy.
- (n) *Maintainability prediction.* Maintainability prediction enables an early assessment of the maturity of the design and enables early decisions concerning the compatibility of a proposed design with specified requirements or the choice of other alternatives. Mathematical models are available to aid the prediction process.
- (o) *Maintainability design criteria.* This involves the development and application of design criteria and guidelines, with the following aims:
 - (i) Providing adequate accessibility, work space, and work clearance.
 - (ii) Reducing the need for and frequency of maintenance activities.
 - (iii) Reducing maintenance downtime.
 - (iv) Reducing maintenance support costs.
 - (v) Reducing maintenance personnel requirements.
 - (vi) Reducing potential for maintenance error.
 - (vii) Providing a built-in test capability.

NOTE: The above describe those activities which, during the design and development (including initial manufacturing) stages, can be carried out by the supplier, by an independent assessor, or may be undertaken by the purchaser. Because of the complexity of some systems, the level at which the above are carried out should be carefully selected, taking into account costs, complexity of analysis and potential benefits.