# CHAPTER 5

# THEORETICAL REVIEW OF DESIGN FOR R&M

## CONTENTS

# 1 INTRODUCTION

**1.1** An R&M programme should be established from the commencement of Concept Studies with an Operational Needs Analysis (ONA) (PtCCh1) followed by a Potential Scenario Analysis (PSA) (PtBCh1) to produce an R&M Specification that is fully integrated with the Performance and Functionality Specifications. When this is followed by Design for R&M Performance (PtBCh3), using appropriate techniques as set out in Part C, a design should have been produced that is essentially sound in R&M terms. The purpose of a theoretical review of the design for R&M is to establish that the design, before it enters manufacture, does not contain unexpected and unforeseen features that will be the cause of unreliability or unacceptable maintainability in service.

**1.2** Clearly there is no way of giving such an assurance with absolute certainty, but some degree of confidence can be provided using accepted assessment methods generically referred to as Design Evaluation. A design evaluation is an impartial examination of a design with the objective of ensuring that the designer has taken every reasonable precaution not only to meet the in-service R&M requirements but also to achieve a balanced design. Balance here means the avoidance of over-design or under-design for R&M.

**1.3** The problem is how to decide from design concepts, drawings and engineering specifications whether or not an item will be reliable and maintainable in the field. This Chapter describes the requirements that must be satisfied and methods to be used when carrying out a design evaluation.

**1.4** Design Evaluation is essentially one or more engineering analyses that provide an input or feedback to the design review process and is an key element of the R&M Case. It should not be confused with a Design Review itself which is a formal management activity concerned with overall project control.

**1.5** Design Evaluation involves much detailed and time consuming work but the potential improvements in R&M will invariably lead to savings in development and in-service costs which more than offset the cost of the evaluation. It is always much cheaper to amend a design at the earliest stage than to manufacture and embody modifications later.

# 2 DESIGN EVALUATION REQUIREMENTS

## 2.1 General

**2.2** Effective R&M design evaluation requires:

a) A properly planned programme which is fully integrated with the requirements of other relevant departments such as design, production, quality assurance and logistics and maintenance support;

b) A thorough understanding of the design requirements and the design principles adopted to meet those requirements both of which should be obtained through undertaking an ONA and a PSA;

c) Appraisals planned to critically examine every aspect of the design that may influence reliability and maintainability;

d) Close liaison with design and other departments to ensure that any proposed improvements are introduced quickly. Note: If a Data Reporting, Analysis and Corrective Action System (DRACAS) (see PtCCh18) has been established from the outset it would form an ideal formal means of recording and passing deficiencies in the design, uncovered as a result of the design evaluation process, to the design department (including suggestions for corrective action). The DRACAS procedure would also capture data in a way that would satisfy the requirements of the R&M Case.

**2.3** Throughout design evaluation, the accent must be on attention to detail because often unreliability results from an accumulation of relatively minor points, which have been overlooked, rather than from some major omission.

**2.4** Design evaluation forms a key element of the R&M Case during the Assessment Phase of a Project and comprises two main activities:

a) Design Appraisal. This must assess whether the proposed design will meet its specified (or apportioned) reliability targets at all levels of assembly and in all modes of operation and its maintainability targets at all required maintenance levels. The process should also assess whether there are any major sources of unreliability and whether the inherent reliability and maintainability of the design might be improved. Design analysis techniques such as those described in paragraphs 4, 5 and 7 may be used when making the appraisals;

b) Design Checking. This process ensures that approved reliability and maintainability procedures and practices (e.g. derating, component selection etc.) are being applied consistently throughout the design. Also that requirements affecting reliability and maintainability are specified correctly in drawings specifications, schedules etc. so that causes of unreliability and poor maintainability during manufacture and assembly are minimised. Design checklists as described in paragraph 6 should be used as the basis for these checks.

**2.5** Design evaluation has the potential to improve the reliability and maintainability of an item from the time of construction of the first prototypes. This, in turn, will have a major influence in reducing the test time and cost to achieve specified reliability and maintainability targets. Design evaluation must not be skimped on the grounds that subsequent testing will make good any shortfall. Further, testing low reliability hardware is costly and time-consuming because of the downtime and manpower associated with investigating and correcting the frequent failures that occur.

**2.6** Design evaluation must be started early in the Assessment Phase, once initial high level designs have been established, and be carried out in a rigorous and orderly manner on a continuing basis as the design develops. An individual analysis may be undertaken on the whole system or may be carried out to examine or update a sub-system, equipment or component part. The record of each analysis should therefore:

a) Clearly define the boundaries of the analysis;

b) Explicitly describe the build standard of the system being analysed;

c) Make clear for the sub-system, equipment or component part, whether the results of the analysis changes the interrelationship with other parts of the system - up, down or sideways - and, if so cross refer to other, resultant, analyses;

d) Set out the assumptions made;

e) Describe the data sources used;

f) Show the conclusions drawn.

**2.7** It is not a function of the design evaluation process to develop alternative design solutions but rather to indicate their need. The results of analyses are used to:

a) Provide the Designer and the Reliability Engineer with a deeper understanding of the factors which influence the reliability of the Equipment or System;

b) Identify critical items down to repair and replacement level and compile and update the Critical Items List;

c) Provide a sufficiently detailed understanding of the System or Facility to allow the Designer to devise adequate and relevant monitoring facilities or built-in test equipment, and then to assist in testing its effectiveness;

d) Assist the Designer in considering the allocation and apportionment of reliability characteristics among component parts of the System or Facility, and with the consideration of redundancy optimisation;

e) Provide progressive assurance that the AR&M requirements will be achieved and thus contribute to the build up of the R&M Case;

f) Provide input to, or act as a crosscheck on, safety studies and hazard analyses;

g) Provide input to spares ranging and scaling and Reliability Centred Maintenance (RCM) studies or Integrated Logistic Support (ILS) studies, if the latter are undertaken for the facility in question.

**2.8** A competent engineer should be made responsible for the overall supervision of R&M design evaluation studies. Design appraisal studies will normally be carried out by R&M specialist staff who are experienced in the use of the individual techniques and who, being independent of the design effort, can make a fresh and impartial examination of specific design solutions. Because the techniques are common to and used by other specialists working in disciplines such as Safety and RCM, it is possible and even desirable that either a joint team is set up to undertake the work or the results of the studies are passed on to the appropriate staff as well as to the design team. For the design checking activity, R&M staff will normally prepare the appropriate checklists with the checks being undertaken by design staff. It is most important that sufficient staff of the necessary calibre and experience are allocated to these tasks.

**2.9** Within a design and manufacturing organisation, maximum use should be made of evaluations carried out by other departments for their own purposes. Such evaluations may include, but are not limited to, for example:

a) Stress analysis of mechanical items;

b) Design Department;

c) Tolerance analysis;

d) Design Department;

e) Engineering checks for production;

f) Production Department;

g) Checks of design procedures;

h) Quality Assurance Department.

**2.10** The results of such studies should be examined for any factors that may degrade reliability or maintainability.

**2.11** Normally, design evaluation should be carried out at all levels of assembly. If any item is excluded from the evaluation, for example because it is a well established item of proven reliability in similar applications, then the reason must be recorded. All re-designs and modifications must also be evaluated for their effect on reliability and maintainability.

# 3 DESIGN EVALUATION TECHNIQUES

## 3.1 General

**3.2** There are four main techniques that may be used during design evaluation:

a) Success Tree Analysis (STA)/Fault Tree Analysis (FTA). STA and FTA are 'cause and effect' analyses that take each possible system running or failure state in turn and logically traces it back to one or more successful operation states or failure causes at sub-system or lower level. This 'top down' approach makes the technique particularly suitable for starting reliability design evaluation possibly as early as concept studies, but certainly during the early assessment stage of a project. The main features of STA/FTA are described briefly in paragraph 4 and the subject is treated comprehensively in PtCCh29 and in British Standard 5760, Parts 2 and 7;

b) Failure Modes and Effects Analysis (FMEA). FMEA is another 'cause and effects' analysis but, in this case, the approach is to consider the failure of one item at a time and to determine its effect in turn on the performance of the next higher level of functional assembly and so on, up to system level. This technique is most suited to later in the assessment phase and during the demonstration phase of a project when detailed drawings at part and component level are available. The main features of FMEA are described briefly in paragraph 5 and the subject is treated comprehensively in PtCCh33 and in British Standard 5760, Parts 2 and 5. The analysis also provides a starting point for the Reliability Centred Maintenance (RCM) process which is used to

determine the maintenance requirements of any physical asset in its operating environment;

c) Design Checklists. Disciplined and formal design checks provide a method of ensuring that reliability and maintainability design requirements have been satisfied and included in design drawings and specifications. Design checklists are used to document the essential features that need to be checked and are prepared before the check commences. They are also used to record the results of the checks. The main features of design checklists are described briefly in paragraph 6 and the subject is treated comprehensively in PtCCh23;

d) Human Factors Analysis. The R&M achievements of a system depend on all aspects of the system design and operation including hardware, software, people and man/machine interfaces. Once in the field, apart from logistics support arrangements, the availability of a system is dependent, not only on its inherent "engineered in" characteristics but also on the capability of the operator(s) and maintainer(s) considered in terms of their intrinsic abilities and training. Human Factors Analysis examines the design to establish ease of operation and maintenance of the system and of the potential for human error to cause the system to fail. The main features of human factors analysis are described briefly in paragraph 7 and the subject is treated comprehensively in PtCCh31 - 32.

**3.3** The foregoing does not preclude the use of other design analysis techniques such as Sneak Circuit Analysis or Worst Case Stress Analysis. The principles and methods of these techniques are described in PtCCh19 and 25 respectively. Generally, such techniques are likely to be more limited in their application, for example to areas of the design that has been shown by standard design evaluation methods to be reliability or maintainability sensitive.

# 4 SUCCESS TREE/FAULT TREE ANALYSES

## 4.1 General

**4.1.1** Success trees and fault trees provide an objective basis for analysing system design, performing trade-off studies, analysing common mode failures, justifying design improvements or additions and also provide an important foundation for many safety and risk assessment activities. The advantage of STA/FTA is that it is undertaken as a series of small steps that are independent of each other using simple standard symbols and logical connections. A complex system may be broken down into a number of simple arrangements, each of which is easy to comprehend. In this paragraph, unless otherwise stated, a comment identifying FTA can also be read across to STA.

**4.1.2** A fault tree shows graphically, by means of a defined notation, the logical relationship between a particular system failure mode (TOP event) and the basic failure causes (PRIME events). Similarly, a success tree shows the logical relationship between a particular system running state and the lower level operational states. The technique can be applied between any levels, for example - system down to assembly level, line replaceable unit (LRU) down to component level etc. However, the TOP event and the level to which the analysis is to be taken must always be clearly specified.

## 4.2 Procedure

**4.2.1** FTA involves the following steps:

a) Definition of the system; the items comprising the system, their functional relationships and performance requirements. All of these will be available as outputs from the Potential Scenario Analysis (PtBCh1) and the Operational Needs Analysis (PtCCh1);

b) Definition of the TOP event to be analysed and the bounds of the analysis;

c) Construction of the fault tree by tracing the TOP event (failure) down to one or more causes at the specified functional (or item) level within the design;

d) Estimation of the probability of occurrence of each of the failure causes;

e) Calculation of the probability of occurrence of the TOP event.

**4.2.2** The principles of success/fault tree analyses and their use both qualitatively and quantitatively are amplified and illustrated in PtCCh29 and in British Standard 5760.

## 4.3 Benefits of FTA

**4.3.1** Fault tree analysis is particularly suitable for use during the early stages of a project because it employs a 'top down' approach and is event oriented. It can be used qualitatively to identify those items within a design that are likely to contribute most to a particular system failure and therefore merit closest attention. In this respect, FTA can be considered as a complementary technique to Failure Modes and Effects Analysis (paragraph 5), that is FTA can identify potentially critical items during the early design stage for deeper analysis during the detailed design stage using FMEA. A further feature of FTA is that, being event oriented, it can include failure causes such as 'operator error' and can therefore be used to evaluate safety or maintenance requirements.

**4.3.2** Fault tree analysis benefits the design by:

a) Directing the analyst to discover failures deductively;

b) Indicating those parts of a system which are important with respect to the failure of interest;

c) Providing a clear and concise means of imparting reliability information to management;

d) Providing a means for qualitative or quantitative reliability analysis;

e) Allowing the analyst to concentrate on one system failure mode, or ‘effect’, at a time;

f) Providing the analyst and designer with a clear understanding of the reliability characteristics and features of the design;

g) Enabling the analyst to identify possible reliability problems in a design even before detailed drawings has been completed;

h) Enabling human and other non-hardware failure causes to be evaluated.

### 4.4 Limitations

Fault tree analysis does have practical limitations for a large system if it has to be repeated for every top event, mainly due to the time and effort required. It is acceptable to edit the list of top events in order to consider only those that are safety critical and those where the probability of occurrence is high. Fault trees (or sub-trees) of more general items, or parts of a system, which may be used again in other designs should be indexed and stored for future use.

## 5 FMEA and FMECA

### 5.1 General

**5.1.1** FMEA (Failure Modes and Effects Analysis) is an objective method for evaluating system design by considering the various failure modes of the individual items comprising a system and analysing their effects on the reliability of the system. By tracing the effects of individual item failures up to system level, the criticality of particular items can be assessed and corrective action taken to improve the design by determining ways to eliminate or reduce the probability of occurrence of critical failure modes. Criticality is normally assessed as a function of the 'severity' and frequency of occurrence of the effects on the system, of particular item failure modes (PtCCh33); this is known as a FMECA (Failure Modes, Effects and Criticality Analysis).

**5.1.2** FMEA can be performed at any level of assembly, but the bounds of the analysis must always be clearly specified. Generally, FMEA is most effective when performed on a system which is in its simplest state, that is, it does not involve redundancy and therefore comprises the minimum number of items necessary to perform the system function (PtCCh33). It can then be used to identify critical areas needing redundancy or other reliability improvement techniques.

### 5.2 Procedure

**5.2.1** FMEA and FMECA involve much detailed and time-consuming work and it must be fully documented to provide a clear and well-related hierarchy of data. The procedure involves the following activities:

a) System Definition. Define the system to be evaluated, the functional relationships of the items in the system and the level of analysis to be performed;

b) Failure Modes Analysis. Define all potential failure modes to be evaluated at the lowest level of assembly and their relative frequency of occurrence;

c) Failure Effects Analysis. Define the effect of each failure mode on the immediate function or assembly, each higher level of assembly, the system and the mission to be performed;

d) Criticality Analysis. Compute a criticality value (paragraph 5.1.1) for each item failure mode. Construct a list of items ranked in order of criticality;

e) Evaluate feasible methods of improving the reliability of the most critical items. This should be done in consultation with the design staff who are responsible for taking any necessary action to improve the design.

More detailed information, illustrated by an example, is given in Part C Chapter 33.

## 5.3 Benefits, Use and Limitations of FMEA and FMECA

**5.3.1** Benefits to the design by:

a) Providing the analyst and the designer with a deeper understanding of the factors that influence the reliability of the system. This will also benefit future development work;

b) Identifying critical items and providing an objective basis for deciding the priorities for corrective action;

c) Providing a means of checking whether a design is well balanced from a reliability viewpoint

d) Providing the basis for securing a more accurate prediction of potential reliability than that obtained by use of part count techniques (PtCCh36);

e) Providing the detailed understanding of the system necessary to assess the test effectiveness of any Built-in Test Equipment (BITE);

f) Providing assurance that potential areas of significant unreliability have been identified early in the project.

**5.3.2** There are two main approaches to a FMEA, one based on the functional structure of the system and one based on its physical (equipment or item) structure. The former would be undertaken initially as a design evaluation process and the latter (once the detailed design is substantially complete) to assist in maintenance analysis and the RCM process and also to feedback into the design of test equipment including Built-in Test Equipment (BITE).

**5.3.3** The use of FMEA and FMECA is generally limited by the time and resources available and the capability to derive a sufficiently detailed database at the time of the analysis (ie. an accurate system definition, up-to-date design drawings, failure rate data, etc.). To ensure the best use of available effort, they should generally be confined to items shown to be critical by earlier analyses (for example, a FTA, RBD Analysis or Availability Modelling) or by some other criteria, such as safety, high cost, complexity or difficulty of access for maintenance. Failure rate data and assumptions used in the study should be the same as that used in the Availability Model. The output of the study should be compared to the results of availability modelling to ensure compatibility and may be used to inform the allocation and apportionment process, trade-off studies, initial consideration of fault diagnosis, monitoring and test requirements (including the design of any BITE), and maintenance policy.

# 6 DESIGN CHECKLISTS

## 6.1 General

**6.1.1** Design checklists provide a means of ensuring that design checks are carried out in a detailed and ordered manner in order to identify and record any design features that may cause unreliability or poor maintainability and to note intended corrective actions.

**6.1.2** A design checklist is a list of questions addressed to any design feature that may influence the reliability of the item concerned. Checklists can be used from the earliest stages of the project and their depth and scope will vary according to the item being checked. For example, at assembly level they will pose many detailed questions; at sub-system level they will be concerned with interfaces and compatibility, and at system level they will concentrate on whether the overall requirements and specifications have been satisfied.

## 6.2 Procedure

**6.2.1** Design checklists must be compiled for each item on which a design check is to be carried out. Once compiled, they must be updated to take account of any changes, and any checklists that have a general application must always be reviewed before they are used.

**6.2.2** A design checklist is compiled by first identifying the particular design requirements which apply to the item to be checked. A series of questions must then be developed which ensure that a critical examination is made of all design, manufacturing and procedural aspects that are essential to the reliability of the item. In broad terms, the check must ensure that:

a) The designer was aware of the reliability objectives and has interpreted them correctly;

b) The designer has met;

c) Reliability design requirements;

d) Those general engineering design requirements which impact on reliability;

e) Any new design concepts have been evaluated fully from a reliability viewpoint;

f) Any potential causes of unreliability during manufacture have been minimised (e.g. in drawings, specifications, schedules, etc.).

**6.2.3** PtCCh23 describes how checklists should be prepared and gives examples of representative questions as a guide to the type of questioning which must be developed.

## 6.3 Benefits, Use and Limitations of Checklists

**6.3.1** In any project, there are inevitably many inter-relating design considerations, among which are performance, reliability, maintainability, time-scale and cost. Consequently, important aspects that may have long-term repercussions may be overlooked, particularly during the early design stages. Reliability and Maintainability Design Checklists benefit the design by:

a) Providing a disciplined and fully documented basis for checking the design of both hardware and software;

b) Providing the design evaluator and the designer with a comprehensive questionnaire on all design aspects that may affect the reliability and maintainability of the particular design;

c) Identifying sources of potential unreliability and/or poor maintainability and recording the corrective action necessary to eliminate them;

d) Providing assurance that reliability and maintainability requirements have been fully considered during the early design stage;

f) Providing a documented input to Design Reviews and to the R&M Case.

**6.3.2** The main danger in using design checklists is that of making the complacent assumption that they are exhaustive. Their use must not be allowed to relieve the evaluator from a continuing responsibility for identifying and checking all design aspects that may influence reliability and maintainability.

# 7 HUMAN FACTORS ANALYSIS

## 7.1 General

**7.1.1** Human factors engineering examines the way that operators in particular, but also maintainers, will interact with the system as a workplace (also referred to as the 'man/machine interface'), once it is deployed in the field. A workplace is defined as any environment in which an operator is required to carry out tasks. The definition covers the complete range of working environments from an office desk through to a complex compartment with several operators, either static on land or in a mobile sea, land or air vehicle.

**7.1.2** The aim of human factors engineering is to design the workplace including the controls and displays of the system in such a way that it may be operated efficiently, safely and reliably, with the minimum possibility of operator induced error. As such human factors engineering is a design function that bears on a number of aspects in addition to the reliability and maintainability of the system. The following procedure sets out, at high level, the steps followed by the designer when considering the man/machine interface. From an R&M viewpoint, human factors analysis would consist of a specialised checklist based on a detailed examination of the human factors considerations of the design in question.

## 7.2 Procedure

**7.2.1** Undertake a Task Analysis; that is, work out the functions that will be required of one or more individuals in order to accomplish the output goal(s) of the system.

**7.2.2** Using formal methodologies, design the workplace. This will have to take account of a number of elements:

a) Range of possible tasks that the operator will call on the system to perform;

b) Range of possible operator body size, agility, strength and stamina, eyesight and hearing;

c) The physical surroundings and environment;

d) The health and safety of the operator(s);

e) Psychological and physiological factors;

and will result in the determination of:

a) Optimum workspace envelope;

b) Critical dimensions within the workspace;

c) Functional factors such as positioning and dimensions of controls and displays;

d) Field of view - within the workspace, outside the compartment or vehicle, to other personnel and to other equipment;

e) Clearance into and out of the workplace and also while present in the workplace to allow for comfort and also to allow manipulation of controls taking account of special and/or life support clothing;

f) Communications - direct with other operators, the giving or receiving of instructions, awareness of alarms and any auditory interaction with the system being operated.

**7.2.3** Once the design has progressed to the provision of high level drawings it will be advantageous to prepare simulations, mock-ups or rigs of the workplace where tests and measurements will lead to feedback into design reviews and possible modification of the design.

**7.2.4** At a later stage, during the Demonstration Phase, there will be a prototype or early build standard of the system during which time users, including operators and maintainers should participate in evaluation tests.

### 7.3 Benefits of Human Factors Analysis

The aim of Human Factors Engineering is the design of systems that match and allow for the operators' abilities and limitations rather than the operator having to adapt to an unsuitable machine that creates physical and mental stress and tiredness. By so doing the possibility of human error adding to the list of events that create unavailability of the system is reduced to a reasonable minimum. An R&M based human factors checklist will ensure that the designer has taken full account of reliability and maintainability issues when undertaking this aspect of the design. An example of such a checklist is included within the design checklists at PtCh23.

# LEAFLET B5/0

# REFERENCE

1. DEF STAN 00-41 (PART 1) Issue 3. 25 June 1993. *Reliability and Maintainability MOD Guide to Practices and Procedures.*

2. BRITISH STANDARD 5760 Reliability of systems, equipment and components. Part 1: 1996 Dependability programme elements and tasks.

3. BRITISH STANDARD 5760 Reliability of systems, equipment and components. Part 5: Guide to failure modes, effects and criticality analysis (FMEA and FMECA).

4. BRITISH STANDARD 5760 Reliability of systems, equipment and components. Part 2: 1994 Guide to the assessment of reliability.

5. BRITISH STANDARD 5760 Reliability of systems, equipment and components. Part 7: 1991 Guide to fault tree analysis.

6. DEF STAN 00-250 Series. *Human Factors for Designers of Equipment. Parts 1 to 4.*