BRITISH STANDARD

BS 5760-5: 1991

Reliability of systems, equipment and components —

Part 5: Guide to failure modes, effects and criticality analysis (FMEA and FMECA)

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Quality, Management and Statistics Standards Policy Committee (QMS/-) to Technical Committee QMS/23, upon which the following bodies were represented:

Association for Consumer Research (ACRE)
Association of Consulting Engineers
British Gas plc
British Railways Board
British Telecommunications plc
Cable and Wireless plc
Cranfield Information Technology Institute
Cranfield Institute of Technology
EEA (the Association of Electronics, Telecommunications and Business Equipment Industries)
Electricity Supply Industry in United Kingdom
Electronic Components Industry Federation
Engineering Equipment and Materials Users' Association
GAMBICA (BEAMA Ltd.)
Institute of Quality Assurance
Institution of Electrical Engineers
Institution of Plant Engineers
Ministry of Defence
National Computing Centre Ltd.
Railway Industry Association of Great Britain
Society of British Aerospace Companies Limited
United Kingdom Atomic Energy Authority

This British Standard, having been prepared under the direction of the Quality, Management and Statistics Standards Policy Committee, was published under the authority of the Standards Board and comes into effect on 20 December 1991

The following BSI references relate to the work on this standard:
Committee reference QMS/23
Draft for comment 86/66800 DC

ISBN 0 580 19660 7

Amendments issued since publication

Amd. No.	Date	Comments

Contents

Foreword

This Part of BS 5760 has been prepared under the direction of the Quality, Management and Statistics Standards Policy Committee. It is based on IEC 812 published by the International Electrotechnical Commission (IEC). In the preparation of this Part of BS 5760, the committee has modified and extended the text of IEC 812 to clarify the nature of failure modes and effects analysis and criticality analysis and to present, and place particular emphasis upon, procedures for carrying out these analyses.

Seven Parts of this standard have now been published and these may be summarized as follows.

Part 0: Introductory guide to reliability. This Part provides guidance to directors of companies who need to know why reliability is important to them, to engineers not trained in quality and reliability to show how reliability should influence their technical decision making, and to middle management not specialized in engineering, to explain how measures to achieve reliability should be integrated with other aspects of project management to give optimum results.

Part 1: Guide to reliability and maintainability programme management. This Part discusses the essential features of a comprehensive reliability and maintainability programme for the planning, organization, direction and control of resources to produce systems, equipment and components which will be reliable and maintainable. It includes consideration of the specification and assessment of reliability and maintainability and of arrangements for the collection of reliability data.

Part 2: Guide to the assessment of reliability. This Part recommends general procedures for the assessment of reliability of hardware systems and contains guidance for the reliability practitioner on the quantitative and statistical aspects of reliability, such as reliability modelling, the provision of data, and the concepts of redundancy and simulation.

Part 3: Guide to reliability practices: examples. This Part contains authentic practical examples illustrating the principles established in Parts 1 and 2 of BS 5760.

Part 4: Guide to specification clauses relating to the achievement and development of reliability in new and existing items. This Part provides more detailed guidance on the specification of reliability.

Part 5: Guide to failure modes, effects and criticality analysis (FMEA and FMECA). This Part describes failure modes and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA), and gives guidance on the application of these techniques.

Part 6: Guide to programmes for reliability growth. This Part describes procedures to expose and remove weaknesses in hardware and software items in order to achieve acceptable reliability in a product. It explains basic concepts, management and test procedures and describes techniques for analysis and correction of failures.

Further Parts are envisaged in order to provide guidance on other techniques of reliability management. At present three further Parts are in the process of being drafted, and these are as follows.

Part 7: Guide to fault tree analysis.

Part 8[1)]: Guide to the assessment of reliability of systems containing software. This Part will provide guidance on the assessment of reliability of systems containing software.

Part 9: Guide to reliability block diagrams.

[1)] Currently published as a Draft for Development, DD 198:1991.

NOTE 1 This British Standard makes reference to BS 4778, the Quality Vocabulary, and in particular to BS 4778-3, a glossary which contains definitions relating to reliability concepts applicable to the guide and it is essential that these definitions and concepts should be fully understood if this guide is to be interpreted correctly. For this reason it is recommended that BS 4778 should be read in conjunction with BS 5760.

NOTE 2 Chapter 191 of IEC 50, the International Electrotechnical Vocabulary, now deprecates the use of the terms "failure modes and effects analysis" and "failure modes, effects and criticality analysis" and favours the use of "fault modes and effects analysis" and "fault modes, effects and criticality analysis" respectively. However, the older terms have been retained in this standard in order to align it with the current version of IEC 812 which has been adopted by CEN.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 38, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

Section 1. General

0 Introduction

Failure modes and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA) are methods of reliability analysis intended to identify failures which have consequences affecting the functioning of a system within the limits of a given application, thus enabling priorities for action to be set.

Generally, failures or failure modes of any component will affect system performance adversely. In the study of system reliability, safety and availability, both qualitative and quantitative analyses are needed and these complement one another. Quantitative analysis methods allow the calculation or prediction of performance measures of the system while fulfulling a specific task or in long-term operation under specific conditions. Typical measures denote reliability, safety, availability, failure rates, and mean time to failure (MTTF).

FMEA begins at the item or subassembly level for which the basic failure criteria (primary failure modes) are available. Starting from the basic failure characteristics of the elements and the functional structure of the system, the FMEA indicates the relationship between element failures and failures, malfunctions, operational constraints and degradation of performance or integrity of the system.To evaluate secondary and higher-order system and subsystem failures, the sequences of events in time may also need to be considered.

In a narrow sense, FMEA is limited to a qualitative analysis of failure modes of hardware, and does not include human errors and software errors, despite the fact that current systems are usually subject to both. In a wider sense, these factors should be included.

Criticality is a measure which combines the concepts of severity of consequences of failure and rate of occurrence or probability of occurrence of failure in a defined period. Severity is usually measured by placing a failure mode in one of a number of categories according to the consequences. Probability or rate of occurrence may also need to be dealt with in this way if numerical data are not available. Criticality is then measured by combining these indices in a defined manner.

1.1 Scope

This Part of BS 5760 describes failure modes and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA), and gives guidance as to how they may be applied to achieve various objectives connected with the development of reliable designs, as follows:

a) by describing the procedural steps necessary to perform an analysis (these are summarized in Appendix A);

b) by identifying appropriate terms, assumptions, failure modes and criticality measures;

c) by determining basic principles;

d) by providing examples of the necessary worksheets;

e) by providing recommendations for applications of FMEA and FMECA.

All the general qualitative considerations presented for FMEA also apply to FMECA. However, FMEA and FMECA are different in the sense that FMEA can be performed on its own, whereas criticality analysis has to be carried out in conjunction with an FMEA. FMECA also differs from FMEA in that the former is quantitative. For these reasons the two methods of analysis are dealt with separately in this standard. Examples of FMECA and FMEA are given in Appendix B.

While this Part of BS 5760 is concerned with the use of FMEA and FMECA for the pursuit of reliable designs, both FMEA and FMECA can also be used in the development of reliable processes. An example of this application is also given in Appendix B. (See example in **B.4**.)

NOTE 1 The titles of the publications referred to in this standard are listed on the inside back cover.
NOTE 2 Additional relevant publications are listed in Appendix C for information.

1.2 Definitions

For the purposes of this British Standard the definitions given in BS 4778-1, BS 4778-2 and BS 4778-3 apply, together with the following.

1.2.1
failure effect

the consequence of a failure mode in terms of the operation, function or status of a system

1.2.2
failure mode

the effect by which a failure is observed

1.2.3
criticality

a combination of the severity of an effect and the probability (or expected frequency) of its occurrence

Section 2. Failure modes and effects analysis

2.1 Introduction

2.1.1 General

FMEA and FMECA (see section 3) are important techniques for a reliability assurance programme. They can be applied to a wide range of problems which may occur in technical systems, and can be carried out in varying degrees of depth, or modified, to suit a particular purpose. The analysis is carried out in a limited way during the conception, planning, and definition phases and more fully in the design and development phase. It is however important to remember that the FMEA is only part of a reliability and maintainability programme which requires many different tasks and activities. FMEA is an inductive method of performing a qualitative system reliability or safety analysis from a low to a high level.

A thorough understanding of the system under analysis is essential prior to undertaking FMEA. Functional diagrams and other system drawings are normally necessary for this understanding. Reliability block diagrams, fault trees and/or state diagrams are then usually derived from these in order to carry out the analysis. In many instances the block diagram descriptions and block diagram failure descriptions are included in the FMEA format. Separate diagrams will be needed for the following:

a) the way in which different criteria for system failure are determined;

b) degradation of function or reduction in assurance of function;

c) safety (as distinct from reliability or economic risk);

d) alternative operational phases.

2.1.2 Purpose of the analysis

The reasons for undertaking FMEA (or FMECA) may include the following:

a) to identify those failures which have unwanted effects on system operation, e.g. safety critical failures;

b) to satisfy contractual conditions that an FMEA should be completed;

c) where appropriate, to quantify the reliability and/or safety of the system;

d) to allow improvements of the system's reliability and/or safety (e.g. by design or quality assurance actions);

e) to produce aids to fault diagnosis;

f) to allow improvement of the system's maintainability (by highlighting areas of risk or non-conformance for maintainability).

In view of these reasons the objectives of an FMEA (or FMECA) may include the following:

1) a comprehensive identification and evaluation of all the unwanted effects within the defined boundaries of the system being analysed, and the sequences of events brought about by each identified item failure mode, from whatever cause, at various levels of the system's functional hierarchy;

2) the determination of the significance (or criticality, see section 3) of each failure mode with respect to the system's correct function or performance and the impact on the reliability and/or safety of the process concerned;

3) a classification of identified failure modes according to relevant characteristics, including detectability, diagnosability, testability, item replaceability, compensating and operating provisions (repair, maintenance, logistics, etc.);

4) an estimation of measures of the significance and probability of failure.

NOTE This applies to criticality analysis only (see section 3).

2.1.3 Basic principles of FMEA

The following concepts are essential to FMEA:

a) breakdown of the system into "elements";

b) a diagram of the system's functional structure and identification of the various data which are needed to perform the FMEA;

c) the failure mode concept (a part may have several failure modes or a failure mode may involve several parts);

d) identification of new physical features or new requirements;

e) the criticality concept and the measure to be used (if criticality analysis is required).

Further, it is essential to specify the existing links between the FMEA (and the FMECA) and other qualitative (and quantitative) analytical methods within the overall reliability programme.

Very few designs are wholly new. Most are to some extent developments of old designs. FMEA should use the information on existing systems and draw attention to the need for tests, etc. for the new parts.

2.2 Procedure

2.2.1 General

The wide variation in complexity of system designs and applications may require the development of highly individualized FMEA procedures consistent with the information available.

Traditionally there have been wide variations in the manner in which FMEA is conducted and presented. However, the analysis is usually done in a standard manner and presented on a worksheet that contains a core of essential information which can be developed and extended to suit the particular system or project to which it is applied. A typical example of a worksheet is shown in Figure 1.

The procedure consists of the following four main stages:

a) preparatory definition of the system including the design, functional, operational, maintenance and environmental requirements;

b) establishment of the basic principles and purposes of the FMEA and the form of its presentation;

c) carrying out the FMEA using the appropriate worksheet designed according to a) and b);

d) reporting of the complete analysis including any conclusions and recommendations made.

A more detailed consideration of the information needed is given in **2.4**.

2.2.2 Preparation

At the commencement of an analysis the following preparations should be made.

a) The analyst should have available the information listed in **2.4.2.2** to **2.4.2.7** that clearly defines the system to be analysed.

b) It will usually be necessary for the analyst to translate the information into some form of functional, hierarchical or reliability block diagrams. An example of a functional diagram is shown in Figure 2. This diagram shows how the failure effects at the part level form the failure modes at the module level, the failure effects at the module level form the failure modes at the subsystem level, and so on. Such a representation of the system should explicitly identify the system's functional structure, the system boundary and the inputs and outputs crossing that boundary. Further information is given in **2.4.2.8** to **2.4.2.10**.

2.2.3 FMEA principles

The following principles should be applied.

a) Define clearly the purposes and uses of the FMEA as indicated in **2.1.2**.

b) Establish and define the relationships with other forms of reliability analysis with which the FMEA may subsequently be integrated. (See **2.3.5**.)

c) Define the scope of the FMEA in relation to the functional structure and hierarchical structure of the system as described by the block diagrams referred to in **2.4.2.10**. It is essential to define the lowest level in the system's hierarchical structure at which the analysis will start. The guidance given in **2.3.4**, **2.4.1.1** and **2.4.2.8** is especially important for this task.

d) Define the format of the FMEA worksheet to suit the project requirements. The core information considered essential is as follows:

1) the name of the item in the system being analysed;

2) function performed by the item;

3) identification number of the item;

4) failure modes of the item;

5) failure causes;

6) failure effects on the system;

7) failure detection methods;

8) compensating provisions;

9) severity of effects;

10) remarks.

Other information required for the particular system and project needs to be defined by the analyst according to the purposes of the FMEA.

FMEA

Indenture level: **Design by:** **Prepared by:**

Sheet no: **Item:** **Approved by:**

Mission phase: **Issue:** **Date:**

Item ref.	Item description-function	Failure entry code	Failure mode	Possible failure causes	Symptom detected by	Local effect	Effect on unit output	Compensating provision against failure	Severity class	Failure rate (F/Mhr)	Data source	Recommendations and actions taken

Figure 1 — Example of the format of an FMEA worksheet

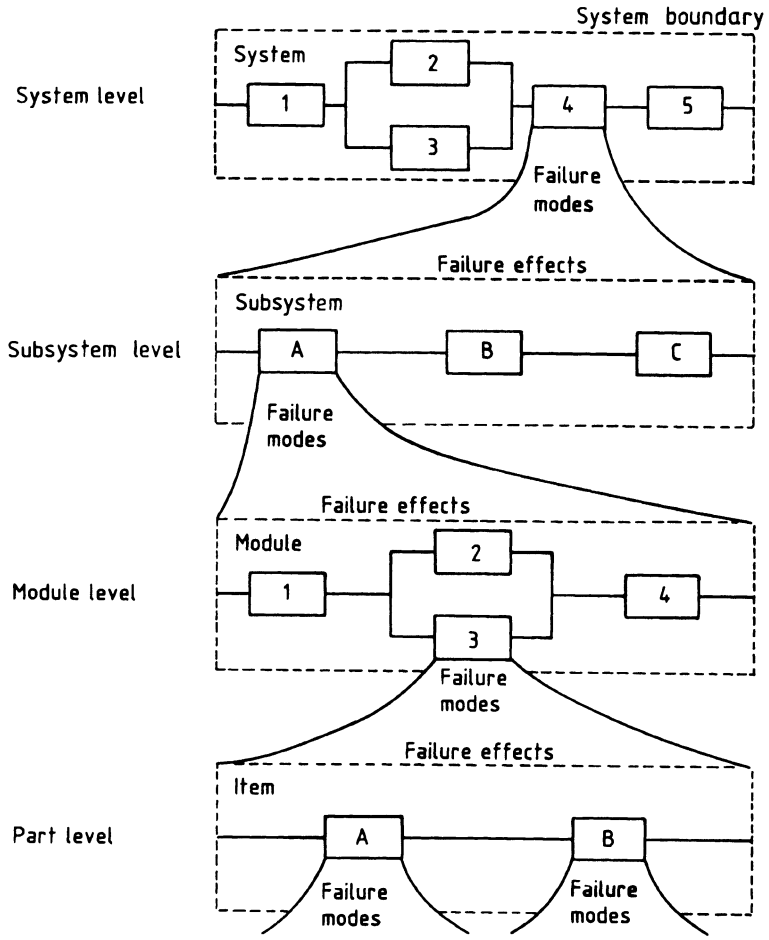


Figure 2 — Relationship between failure modes and failure effects in a system hierarchy

2.2.4 Analysis

2.2.4.1 *Single stage*

The usual requirement and purpose of an FMEA is to identify the effect of *all* failure modes of *all* constituent items at the lowest level in the system. To achieve this the worksheet should be used in the following manner.

a) Identify all items in the system or subsystem, each of which is to have its failure modes and effects analysed. The system of identification by name and number should be such that no items will be omitted.

b) Select the first item for analysis and enter the item name and identification number in the appropriate columns of the worksheet. Determine the function of that item in the system and enter that on the worksheet.

c) Deduce all the possible failure modes of the item due to any possible cause and individually enter these modes on the worksheet. (Failure modes are discussed in **2.4.1.2**.)

d) Postulate the most likely failure causes for each failure mode of the item and enter these on the worksheet.

It will usually not be possible to consider all possible causes because the range is so vast, but the most significant with regard to the item, the failure mode and the application should be identified.

e) Deduce the effects of the failure on the subsystem and system, as determined by the scope of the FMEA defined in accordance with **2.2.3**.

f) Complete the remaining columns of the worksheet for the first failure mode of the first item.

g) Repeat c) to f) for all other failure modes of the first item.

h) Repeat b) to g) for all other items.

2.2.4.2 *Multiple stages*

If the FMEA is to be done in stages that each relate to separate levels in the system's hierarchical structure, the failure effects from the lower level become the failure modes at the next level up. This form of overall FMEA for large systems is recommended in **2.3.4**. The analysis should then proceed as follows.

a) Identify the lower level FMEAs that are appropriate for the next stage in the system FMEA according to the system's hierarchical structure defined by the block or functional diagrams [see **2.2.2** b)]. Where appropriate also include items defined as being at the lowest level in that part of the system structure.

b) Perform the FMEA for each failure of each item at this higher level in the system structure as given in **2.2.4.1** b) to h).

c) Repeat a) and b) above for any further higher levels in the system structure.

2.2.4.3 *Worksheet remarks*

The last worksheet entry should give any pertinent remarks to clarify other entries. Possible future actions such as recommendations for design improvements may be recorded and then amplified in the report. This column may also include the following:

a) any unusual conditions;

b) effects of redundant element failures;

c) recognition of specially critical design features;

d) any remarks to amplify the entry;

e) references to other entries for sequential failure analysis;

f) significant maintenance requirements;

g) dominant failure causes;

h) dominant failure effects;

i) decisions taken, e.g. at design review.

2.2.4.4 *Report of analysis*

The report on the FMEA (or FMECA) may be included in a wider study or may stand alone. In either case, the report should include a summary and a detailed record of the analysis and the block or functional diagrams which define the system structure. The report should also contain a list of the drawings (including issue status) on which the FMEA is based.

The summary should contain a brief description of the method of analysis and the level to which it was conducted, the assumptions and the ground rules (see **2.4.1**). In addition it should include listings of the following:

a) recommendations for the attention of designers, maintenance staff, planners and users;

b) failures which, when initially occurring alone, result in serious effects;

c) failures which have no effect;

d) design changes which have already been incorporated as a result of the FMEA (or FMECA).

2.3 Application

2.3.1 Field of application

FMEA is a method that is primarily adapted to the study of material and equipment failures and that can be applied to categories of systems based on different technologies (electrical, mechanical, hydraulic, etc.) and combinations of technologies. FMEA should also include the consideration of software and human performance where these are relevant to the reliability of the system. An FMEA can be a study for general use or it may be specific to particular pieces of equipment, to systems or to projects as a whole.

2.3.2 Application within a project

The user should determine how and for what purposes he uses FMEA within his own technical discipline. It may be used alone or to complement and support other methods of reliability analysis. The requirements for FMEA originate from the need to understand hardware behaviour and its implications for the operation of the system or equipment. The need for FMEA can vary widely from one project to another.

FMEA is the principal reliability engineering activity in support of the design review concept (see **4.2.1.4** of BS 5760-1:1985) and should be put into use from the very first steps of system and subsystem design. FMEA is applicable to all levels of system design but is most appropriate for lower levels where large numbers of items are involved and/or there is functional complexity. Special training of personnel performing FMEA is essential and they need the close collaboration of systems engineers and designers. The FMEA should be updated as the project progresses and as designs are modified. At the end of the project, FMEA is used to check the design and may be essential for demonstration of conformity of a designed system to the required standards, regulations, and user's requirements.

Information from the FMEA identifies priorities for statistical process control sampling and inspection tests during manufacture and installation and for qualification, approval, acceptance and start-up tests. It provides essential information for diagnostic and maintenance procedures for inclusion in handbooks.

In deciding on the extent and the way in which FMEA should be applied to an item or design, it is important to consider the specific purposes for which FMEA results are needed, the time phasing with other activities and the importance of establishing a predetermined degree of awareness and control over unwanted failure modes and effects. This leads to the planning of FMEA in qualitative terms at specified levels (system, subsystem, component, item) to relate to the iterative design and development process (see BS 5760-1).

To ensure that it is effective, the place of FMEA should be clearly established in the reliability programme, together with the time, manpower and other resources needed to make it effective. It is vital that FMEA is not abridged to save time and money. If time and money are short the FMEA should concentrate on those parts of the design which are new or are used in new ways. FMEA can be economically directed to areas identified as crucial by other methods of analysis, e.g. fault tree analysis (FTA).

2.3.3 Uses of FMEA

Some of the detailed applications and benefits of FMEA are listed below:

a) to avoid costly modifications by the early identification of design deficiencies;

b) to identify failures which, when they occur alone or in combination, have unacceptable or significant effects, and to determine the failure modes which may seriously affect the expected or required operation;

NOTE Such effects may include secondary failures.

c) to determine the need for the following:

1) redundancy;

2) design improvement;

3) more generous stress allowances (derating);

4) screening of items;

5) design of features that ensure that the system fails in a preferred failure mode, e.g. “fail-safe” outcomes of failures;

6) selection of alternative materials, parts, devices, and components;

d) to identify serious failure consequences and hence the need for changes in design and/or operational rules;

e) to provide the logic model required to evaluate the probability or rate of occurrence of anomalous operating conditions of the system in preparation for criticality analysis;

f) to disclose safety hazard and product liability problem areas, or non-compliance with regulatory requirements;

NOTE Frequently, separate studies will be required for safety, but overlap is inevitable and therefore cooperation is highly advisable.

g) to ensure that the development test programme can detect potential failure modes;

h) to focus upon key areas in which to concentrate quality control, inspection and manufacturing process controls;

i) to assist in defining various aspects of the general maintenance strategy, such as:

1) establishing the need for data recording and condition monitoring during testing, checking-out and use;

2) provision of information for development of trouble-shooting guides;

3) establishing maintenance cycles which anticipate and avoid wear-out failures;

4) the selection of preventative or corrective maintenance schedules, facilities, equipment and staff;

5) selection of built-in test equipment and suitable test points;

j) to provide a systematic and rigorous approach to the study of the installation in which the system is embedded;

k) to facilitate or support the determination of test criteria, test plans and diagnostic procedures, for example: performance testing, reliability testing;

l) to identify parts and assemblies requiring worst case analysis (frequently required for failure modes involving parameter drifts);

m) to support the design of fault isolation sequences and to support the planning for alternative modes of operation and reconfiguration;

n) to facilitate communication between the following:

1) general and specialized engineers;

2) equipment manufacturer and his suppliers;

3) system user and the designer or manufacturer;

o) to enhance the analyst’s knowledge and understanding of the behaviour of the equipment studied;

p) to provide designers with an understanding of the factors which influence the reliability of the system;

q) to provide a final document that is proof of the fact that (and of the extent to which) care has been taken to ensure that the design will meet its specification in service. (This is especially important in the case of product liability.)

2.3.4 Limitations and drawbacks

FMEA is extremely efficient when it is applied to the analysis of elements that cause a failure of the entire system or of a major function of the system. However, FMEA may be difficult and tedious for the case of complex systems that have multiple functions involving different sets of system components. This is because of the quantity of detailed system information that needs to be considered. This difficulty can be increased by the existence of a number of possible operating modes, as well as by consideration of the repair and maintenance policies.

FMEA can be a laborious and inefficient process unless it is judiciously applied. The uses to which the results are to be put subsequently should be defined and FMEA should not be included in requirements specifications indiscriminately.

Complications, misunderstandings and errors can occur when FMEA attempts to span several levels in a hierarchical structure if redundancy is applied in the system design.

It is therefore preferable for an FMEA to be restricted to relating two levels only in the hierarchical structure. For example, it is a relatively straightforward task to identify failure modes of items and to determine their effects on the assembly. These effects then become the failure modes at the next level up, e.g. the module, and so on. However, successful multi-level FMEAs are often carried out.

FMEA is applicable to all levels of a system but is most appropriate to lower levels where large numbers of items are involved and/or there is functional complexity.

2.3.5 Relationships with other methods

FMEA (or FMECA) can be used alone. As a systematic inductive method of analysis, FMEA is most often used to complement other approaches, especially deductive ones. At the design stage, it is often difficult to decide whether the inductive or deductive approach is dominant, as both are combined in processes of thought and analysis. Where levels of risk are identified in industrial facilities and systems, the inductive approach is preferred and therefore FMEA is an essential design tool. However, it should be supplemented by other methods. This is particularly the case when problems need to be identified and solutions need to be found in situations where multiple failures and sequential effects need to be studied. The method used first will depend on the project programme.

During the early design stages, where only functions, general system structure and subsystems have been defined, successful performance of the system can be depicted by a reliability block diagram or a failure path by a fault tree. However, to assist in drawing these diagrams of the system, an FMEA inductive process should be applied to the subsystems before they are designed. Under these circumstances, the FMEA approach cannot be a set procedure but is instead a thought process not readily expressed in a rigid tabular form. In general, when analysing a complex system involving several functions, numerous items and interrelations between these items, the FMEA proves to be essential but not sufficient.

Fault tree analysis (FTA) is a complementary deductive method. It traces the low level causes of a postulated high level failure. Though the logical analysis can be, and sometimes is, used for purely qualitative analysis of fault sequences it is usually a precursor to estimating the frequency of the postulated high level failure.

FTA concentrates on the logic of coincident (or sequential) and alternative events causing undesirable consequences. The FMEA format is more descriptive. Both methods have their uses in a full analysis for safety and reliability in a complex system. However, if the system is based mainly on series logic, with few redundancies and few functions, then FTA is an unnecessarily complicated way of presenting the logic and identifying the failure modes. In such cases FMEA and reliability block diagrams are adequate. In other cases where FTA is preferred, it still needs to be enhanced with descriptions of the failure modes and effects.

The main consideration in selecting the method of analysis should depend on the particular requirements of the project, not only with regard to technical requirements but also timescale, cost, efficiency and usage of the results. General guidelines are as follows.

a) FMEA is appropriate when comprehensive knowledge of the failure characteristics of an item are required.

b) FMEA is more appropriate for smaller systems, modules or assemblies.

c) FMEA is an essential tool at the research and development or design stage when unacceptable effects of failures need to be identified and solutions found.

d) FMEA can be necessary for items that are of innovatory design so that their failure characteristics cannot be known from previous operational experience.

e) FMEA is usually more applicable to items having large numbers of components to be considered that are related by predominantly series failure logic.

f) FTA is generally more suitable for the analysis of single failure modes involving complex failure logic and redundancy. This would usually be so for the higher levels in the hierarchical structure of large systems or entire plants.

g) FTA can be used at the higher levels in the system structure early in the design stage and can help in identifying the need for detailed FMEA at lower levels during detailed design.

2.4 Supplementary information

2.4.1 Establishment of ground rules

2.4.1.1 *Levels of analysis*

It is important to determine the level in the system that will be used for the analysis. For example, systems can be broken down into subsystems, replaceable units, or individual components (see Figure 2). Basic principles for selecting the system levels for analysis depend on the results desired and the availability of design information. The following guidelines are useful.

a) The highest level within the system is selected from the design concept and specified output requirements.

b) The lowest level within the system at which the analysis is effective is that level for which information is available to establish definition and description of functions. The appropriate system level is influenced by previous experience. Less detailed analysis may be justified for a system based on a mature design, with a good reliability, maintainability and safety record. Conversely, greater detail and a correspondingly lower system level is indicated for any newly designed system or a system with unknown reliability history.

c) The specified or intended maintenance and repair level may be a valuable guide in determining lower system levels.

2.4.1.2 *Failure modes*

Successful operation of a given system is subject to the performance of certain critical system elements. The key to evaluation of system performance is the identification of critical elements. The procedures for identifying failure modes, their causes and effects can be effectively enhanced by the preparation of a list of failure modes anticipated in the light of the following:

a) the use of the system;

b) the particular system element involved;

c) the mode of operation;

d) the pertinent operational specifications;

e) the time constraints;

f) the environment.

In the FMEA, the definitions of failure modes, failure causes and failure effects depend on the level of analysis. As the analysis progresses, the failure effects identified at the lower level may become failure modes at the higher level. Similarly, the failure modes at the lower level may become the failure causes at the higher level, and so on.

A list of general failure modes is given in Table 1. Virtually every type of failure mode can be classified into one or more of these categories. However, these general failure mode categories are too broad in scope for definitive analysis; consequently, the list needs to be expanded to make the categories more specific as shown in Table 2. Failure modes such as those listed in Table 2 can describe the failure of any system element in sufficiently specific terms. When used in conjunction with performance specifications governing the inputs and outputs on the reliability block diagram, all potential failure modes can be identified and described. It should be noted that a given failure mode may have several causes.

Table 1 — Example of a set of general failure modes

1	Failure during operation
2	Failure to operate at a prescribed time
3	Failure to cease operation at a prescribed time
4	Premature operation

NOTE This list is an example only. Different lists would be required for different types of system.

It is important that evaluation of all items within the system boundaries at the lowest practicable level is undertaken to identify all potential failure modes. Investigation to determine possible failure causes and also failure effects on subsystem and system function can then be undertaken.

Item or equipment suppliers should identify the potential item failure modes within their products. To assist this function typical failure mode data can be sought from the following areas.

1) For new items, reference can be made to other items with similar function and structure and to the results of tests performed on them under appropriate stress levels.

2) For items in use, in-service records and failure data may be consulted.

3) Potential failure modes can be deduced from functional and physical parameters typical of the operation of the item.

It is important that item failure modes are not omitted for lack of data and that initial estimates are improved by test results and design progression. The FMEA should record the status of such estimates.

The identification of failure modes and where necessary the determination of remedial design actions, preventative quality assurance actions or preventative maintenance actions is of prime importance. It is more important to identify and, if possible, design out modes than to know their rate of occurrence. When it is difficult to assign priorities, criticality analysis may be required.

2.4.1.3 *Failure causes*

The possible causes associated with each possible failure mode should be identified and described. The causes of each failure mode are identified in order to estimate its probability of occurrence, to uncover secondary effects and to devise recommended corrective action. Since a failure mode can have more than one cause, all potential independent causes for each failure mode need to be identified and described. The failure causes within the adjacent system levels should also be considered. The list given in Table 3 illustrates how a more specific definition of failure causes can be developed.

Table 2 — Example of an expanded list of failure modes

1	Cracked/fractured	21	Binding/jamming
2	Distorted	22	Loose
3	Undersize	23	Incorrect adjustment
4	Oversize	24	Seized
5	Fails to open	25	Worn
6	Fails to close	26	Sticking
7	Fails open	27	Overheated
8	Fails closed	28	False response
9	Internal leakage	29	Displaced
10	External leakage	30	Delayed operation
11	Fails to stop	31	Burned
12	Fails to start	32	Collapsed
13	Corroded	33	Overloaded
14	Contaminated	34	Omitted
15	Intermittent operation	35	Incorrect assembly
16	Open circuit	36	Scored
17	Short circuit	37	Noisy
18	Out of tolerance (drifted)	38	Arcing
19	Fails to operate	39	Unstable
20	Operates prematurely	40	Chafed

NOTE This list is an example only. The modes contained in the list cannot be applied to all items and the list is not exhaustive.

Table 3 — Possible failure causes

Type	Examples
Specification	Omitted statements Erroneous statements Support system failure
Design	Misapplication Design error Design omission Support equipment failure
Manufacture	Omitted action Erroneous action Procedural error Manufacturing equipment failure
Installation	Omitted action Erroneous action Procedural error Installation equipment failure
Operation	Omitted action Erroneous action Procedural error Off-line equipment failure
Maintenance	Omitted action Erroneous action Procedural error Maintenance equipment failure
Environment	Temperature Humidity Vibration Corrosion
Uncontrollable forces	Fire Flood Earthquake Explosion

2.4.1.4 *Common-cause (common mode) failures*

In a reliability analysis, it is not sufficient to consider only random and independent failures. Some "common-cause" (or "common mode") failures (CCF) can occur, that cause system performance degradation or failure through simultaneous deficiency in several system components, due to a single source such as design error or human error.

A CCF is the result of an event that, because of logical dependencies, causes a coincidence of failure states in two or more components (excluding secondary failures caused by the effects of a primary failure).

CCFs can be analysed qualitatively using FMEA. As FMEA is a procedure to examine successively each failure mode and associated causes and also to identify all periodic tests, preventative maintenance measures, etc., it makes possible a study of all the causes which can induce potential CCF.

A check list developed from Table 3 may be used to identify in a detailed manner all possible causes which may induce CCF. A combination of several methods is useful in dealing with these failures: functional diversity, redundancies of different types, physical separation, tests, etc. Check lists, as above, may be used to examine the relevance and effectiveness of each method. The examination of preventative measures against CCF is usually considered to be outside the scope of FMEA, but this need not be the case.

2.4.1.5 *Human factors*

Some systems have to be designed to cater for some human error, for example by providing mechanical interlocks on railway signals, and passwords for computer usage or data retrieval. Where such provisions exist in a system, the effect of failure of the provisions will depend on the type of error. Some modes of human error should also be considered for an otherwise fault-free system, to check the effectiveness of the provisions. Although incomplete, even a partial listing of these modes is beneficial for the identification of design and procedural deficiencies; the identification of all possible forms of human error would probably be impossible.

Many CCFs involve human factors. For example, incorrect maintenance of similar items can negate redundancy. To avoid this, material diversity in redundant elements is often introduced.

2.4.1.6 *Software errors*

Malfunctions due to software errors or inadequacies will have effects whose significance will be determined by both hardware and software design. The postulation of such errors or inadequacies and the analysis of their effects is possible only to a limited extent. The effects upon associated hardware of possible errors in software may be estimated and the provision of fall-back arrangements either in software or hardware is often suggested by such analysis.

2.4.1.7 *Failure detection methods*

The methods for detection of the failure mode should be described. Failure modes other than the one being considered which give rise to an identical manifestation should be analysed and listed. The need for separate detection of failure of redundant elements during operation should be considered.

2.4.1.8 *Failure effects*

2.4.1.8.1 *General*

A failure effect is the consequence of a failure mode in terms of the operation, function or status of a system (see **1.2.1**). A failure effect may be caused by one or more failure modes of one or more items.

The consequences of each failure mode on system element operation, function, or status need to be identified, evaluated and recorded. Maintenance, personnel and system objectives should also be considered whenever pertinent. Failure effects focus on the specific system element in the block diagram being analysed that is affected by the failure under consideration.

A failure effect may also influence the next level up and ultimately the highest level under analysis. Therefore, at each level the effect of failures on the level above should be evaluated.

2.4.1.8.2 *Local effects*

The expression "local effects" refers to the effects of the failure mode on the system element under consideration. The consequences of each possible failure on the output of the item should be described along with the secondary effects. The purpose of identifying the local effects is to provide a basis for judgement when evaluating existing alternative provisions or devising recommended corrective actions. In certain instances there may not be a local effect beyond the failure mode itself.

2.4.1.8.3 *End effects*

When identifying end effects, the impact of a possible failure on the highest system level is defined and evaluated by the analysis of all intermediate levels. The end effect described may be the result of multiple failure. (For example, failure of a safety device results in a catastrophic end effect only in the event that both the safety device fails and the prime function for which the safety device is designed goes beyond allowed limits.) These end effects resulting from a multiple failure should be indicated on the worksheets.

2.4.1.8.4 *Effects summary*

A listing of the system failure effects highlighted by the FMEA should be undertaken. Table 4 gives a typical set of failure effects for a motor vehicle starter motor and circuitry.

A failure effects summary may be required in order to determine the system failure effects probability and to establish priorities for remedial or preventative actions. The failure effects summary should be based on the list of end failure effects (see **2.4.1.8.3**) and should contain details of the item failure modes contributing to each failure effect. See Table 5 for a typical failure effects summary.

Table 4 — Example of a set of failure effects (for a motor vehicle starter)

1	Starter motor fails to operate
2	Starter motor speed less than specified
3	Starter motor fails to engage ring gear
4	Starter motor operates prematurely

NOTE This list is an example only. Each system or subsystem being analysed will have its own set of failure effects.

2.4.1.9 ***Consequences of system failure***

A system FMEA can be carried out without reference to any particular application and could then be adapted subsequently for project use. This applies to relatively small assemblies that might themselves be regarded as generic components (for example an electronic amplifier, an electric motor, a mechanical valve).

However, it is more usual to develop a project-specific FMEA and to have regard to the particular consequences of system failure. It might be necessary to categorize the effects of failures on the system according to the consequences of these failures, for example, fail-safe, fail-danger, repairable failure, non-repairable failure, mission degraded, mission failed, effects on individuals, groups or society generally.

The need to relate an FMEA to the ultimate consequence of system failure will depend on the project and the relationship between the FMEA and other forms of analysis, such as fault trees.

Table 5 — Example of a failure effects summary

Number	Description	Contributing failure mode reference	Failure effect probability
1	Starter motor fails to operate	1, 3, 7, 8, 9, 16, 21, 22	8×10^{-3}
2	Starter motor speed less than specified	6, 11, 12, 19, 20	6×10^{-4}
3	Starter motor fails to engage ring gear	2, 4, 5, 10, 13	1.1×10^{-5}
4	Starter motor operates prematurely	14, 15, 17, 18	3.6×10^{-7}

NOTE This list is an example only. The failure effect probability may be presented in the form most suited to the specified reliability requirements for the system.

2.4.2 Information required

2.4.2.1 *General*

Company management should be aware that the success of FMEA (and FMECA) depends upon the free availability to analysts of all relevant information and upon the active cooperation of the designer. Information in the categories listed in **2.4.2.2** to **2.4.2.11** needs to be obtained.

2.4.2.2 *System structure*

Information on system structure needs to include the following items:

a) the different system elements with their characteristics, performances, roles and functions;

b) the logical connections between elements;

c) redundancy level and nature of the redundancies;

d) position and importance of the system within the whole facility (if possible);

e) the inputs and outputs of the system;

f) the changes in system structure for varying operational modes.

Data pertaining to functions, characteristics and performances are required for all levels considered, up to the highest level.

2.4.2.3 *System initiation, operation, control and maintenance*

The status of the different operating conditions of the system should be specified, as well as the changes in the configuration or the position of the system and its components during the different operational phases. The minimum performances demanded of the system should be defined such that success and/or failure criteria can be clearly understood. Such specific requirements as availability or safety should be considered in terms of specified minimum levels of performance to be achieved and maximum levels of damage or harm to be accepted.

It is necessary to have an accurate knowledge of:

a) the duration of each task the system may be called upon to fulfil;

b) the time interval between periodic tests;

c) the time available for corrective action before serious consequences occur to the system;

d) the entire facility, the environment and/or the personnel, including interfaces and interactions with operators;

e) repair conditions including corrective actions and the time, equipment and/or personnel needed to achieve them;

f) operating procedures during system start-up, shut-down and other operational transitions;

g) control during the operational phases;

h) preventative and/or corrective maintenance (see note);

i) procedures for routine testing, if employed.

NOTE It has been stated that one of the uses of FMEA is to assist in the development of the maintenance strategy. However, if the latter has been pre-determined, information on maintenance facilities, equipment and spares should be known for both preventative and corrective maintenance.

2.4.2.4 *System environment*

The environmental conditions of the system should be specified, including ambient conditions and those created by other systems in the vicinity. The system should be delineated with respect to its relationships, dependencies, or interconnections with auxiliary or other systems and human interfaces.

At the design stage these facts are usually not all known and therefore approximations and assumptions will be needed. As the project progresses, the data will have to be augmented and the FMEA modified to allow for new information or changed assumptions or approximations. Often the FMEA will be helpful in defining the required conditions.

NOTE The FMEA should be updated for each design review milestone (see BS 5760-1).

2.4.2.5 *Modelling*

FMEA requires some modelling of the system, i.e. a logical representation of the relevant information on the system (reliability block diagram or fault tree, etc.; see **2.4.2.9** and **2.4.2.10**). Some assumptions may be made about the nature of failure modes, and the seriousness of their consequences. For example, in safety studies conservative hypotheses may have to be formed concerning the impact of certain failures on the system unless or until better information comes to hand.

2.4.2.6 *Software*

An FMEA conducted on the hardware of a complex system may have repercussions on the software in the system. Thus, decisions about effects, criticality and conditional probabilities resulting from the FMEA may be dependent upon the software elements and their nature, sequence and timing. When this is the case, the interrelationships between hardware and software need to be clearly identified because any subsequent alteration or improvement of the software may modify the FMEA and the assessments derived from it. Approval of software development and change may be conditional upon a revision of the FMEA and the related assessments, e.g. software logic may be altered to improve safety at the expense of operational reliability.

2.4.2.7 *System boundary*

The definition of the system boundary is more likely to be influenced by design, source of supply, or commercial criteria rather than the optimum requirements of the FMEA. However, where it is possible to define the boundaries to facilitate the system FMEA and its integration with other related studies in the reliability programme, such action is preferable. This is especially so if the system is functionally complex with multiple interconnections between items within the boundary and multiple outputs crossing the boundary. In such cases it could be advantageous to define a study boundary from functional rather than hardware divisions to limit the number of input and output links to other systems. This would tend to reduce the number of system failure effects.

Care should be taken to ensure that other systems or components outside the boundaries of the subject system are not forgotten, by explicitly stating that they are excluded from the particular study.

2.4.2.8 *Definition of the system's functional structure*

The analysis should be initiated by selecting the lowest level of interest (usually the part, circuit, or module level) at which sufficient information is available or at which it is judged that it needs to be obtained (by tests etc.) to ensure a reliable design. Thus new features of the design should be thoroughly investigated but old features under known stress levels can be incorporated into the analysis at a higher level. If the analysis starts at the lowest level, the various failure modes that can occur for each item at that level are tabulated. The corresponding failure effect for each, taken singly and in turn, is interpreted as a failure mode for consideration of the failure effect at the functional level immediately above. Successive iterations result in the identification of the failure effects, in relation to specific failure modes, at all necessary functional levels up to the system or highest level.

The choice of breakdown level (which may vary for different areas of the system) requires a dependable and detailed knowledge of the failure modes of the elements. Apart from this requirement, it is neither possible nor desirable to set strict rules about the choice of the breakdown level. When quantitative results are required, the level chosen should be one at which it is possible to obtain adequate (and dependable) failure data on each failure mode or error mode, or to make reasonable identified assumptions of such failure rates.

The analyst should investigate all aspects which might be important until satisfied they are not.

2.4.2.9 *Representation of system structure*

Symbolic representations of the system structure and operation, especially diagrams, can be used. Usually block diagrams are adopted, highlighting all the functions essential to the system.

In the diagram, the blocks are linked together by lines which represent the inputs and outputs for each function. Usually, the nature of each function and each input needs to be precisely described. There may also be several diagrams to cover different phases of system operation.

Generally, graphical presentations, including those closely related to analytical methods, like fault trees or cause-consequence diagrams, contribute to a better understanding of a system, its structure and its operation. Their use is discussed in **2.3.5**.

2.4.2.10 *Block diagrams*

Diagrams showing the functional elements of the system are necessary both for technical understanding of the functions and the subsequent analysis.

The diagrams should display any series and redundant relationships among the elements and the functional interdependencies between them. This allows the functional failures to be tracked through the system. More than one diagram may be needed to display the alternative modes of system operation. Separate logic diagrams may be required for each operational mode. As a minimum, the block diagram should contain the following:

a) breakdown of the system into major subsystems including functional relationships;

b) all appropriately labelled inputs and outputs and identification numbers by which each subsystem is consistently referenced;

c) all redundancies, alternative signal paths and other engineering features which provide "fail-safe" measures.

2.4.2.11 *Failure significance and compensating provisions*

The relative significance of the failure should be recorded on the worksheet. Also recorded on the worksheet should be the identification and evaluation of any design features at a given system level for other provisions to prevent or reduce the effect of the failure mode. Thus the worksheet should clearly show the true behaviour of the equipment in the presence of an internal malfunction. Other provisions against failure which need to be recorded on the worksheet include the following:

a) redundant items that allow continued operation if one or more elements fail;

b) alternative means of operation;

c) monitoring or alarm devices;

d) any other means of permitting effective operation or limiting damage.

During the design stage the functional elements (hardware and software) of a piece of equipment may be rearranged or reconfigured to change its capability. Following this, the relevant failure modes should be re-examined before repeating the FMEA.

Section 3. Criticality analysis

3.1 Introduction

3.1.1 Purpose of analysis

Criticality is a combination of the severity of an effect and the probability or expected frequency of its occurrence. When associated with, for example, a failure mode the criticality of the effect is spoken of as the criticality of the failure mode. It may be desirable to quantify criticality as an aid to decision making on the corrective actions needed and their priorities.

The purpose of a criticality analysis is to quantify the relative importance of each failure effect, so that priorities for action to eliminate or contain the failures may be set. Criticality is evaluated by a subjective measure of the severity of the effect and an estimate of the probability or expected frequency of its occurrence. When the estimate of probability or frequency is based on trustworthy data the analysis may be used as a basis for judging whether or not the likelihood of a particular effect is acceptably small.

3.1.2 Principles of criticality analysis

Criticality analysis is applied as an extension of an FMEA, to give a failure modes, effects and criticality analysis (FMECA). A set of severity classes ranging from catastrophic to trivial should be drawn up first, with particular reference to the range of possible damage to people, plant and economics resulting from the failure of the item under analysis. Using the failure effects identified by the FMEA each effect is allocated to an appropriate severity class. A probability or frequency for the event is calculated from failure data for the part concerned and modifying factors such as environment, the probability of the system failing as a consequence of the failure mode and the proportion of elapsed time during which the part is at risk. The severity class and frequency or probability for each effect together constitute the criticality of the effect. They can be presented on a criticality grid, as shown in Figure 3, where they can be placed in criticality bands, or presented in the form of ranked contributions to the total frequency of each severity class.

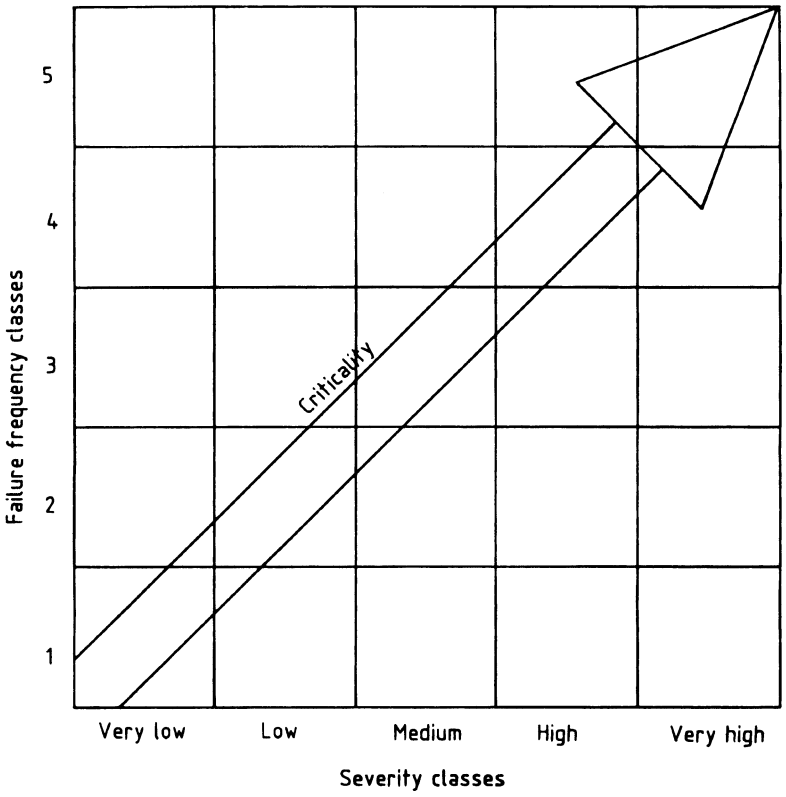


Figure 3 — Example of a criticality grid

3.2 Procedure

3.2.1 General

The fundamental steps in the procedure for an FMECA are the same as those summarized for an FMEA in **2.2.1** and detailed in **2.2.2** to **2.4.2**. However, the criticality analysis incorporated in the FMECA requires two additional steps to be performed as follows:

a) determination of failure effect severity;

b) evaluation of event frequency.

These additional steps are detailed in **3.2.2** to **3.2.6**.

3.2.2 Effect severity

Effect severities should be determined as follows.

a) Define the severity classes. Guidance on this step is given in **3.3** and **B.1**.

b) Allocate a severity class to the effect from each failure mode. This is most readily done on the FMEA sheet. The form shown in Figure 1 provides a column for this purpose.

3.2.3 Event frequency

The easiest approach to the evaluation of event frequency will be determined by the data available. If failure rates for the failure modes of like items are available, under environmental and operational conditions similar to those envisaged for the system being analysed, the event frequencies for the effects can be added directly to the FMEA.

If, as is more often the case, failure rates are available for items, rather than for failure modes, and for different environmental or operating conditions, the effect frequencies need to be calculated.

Environmental, loading and maintenance conditions different from those relating to the failure rate data are accounted for by a single modifying factor, m. Guidance on appropriate values for this factor can be found in publications dealing with reliability data. These include MIL HBK 217, British Telecommunications Handbook of reliability data for electronic components and "Non electronic parts reliability data" (issued by the Reliability Analysis Center).

Items can fail in a number of ways and how they fail will determine the effect of the failure on the system. A value, a, the failure mode factor, is applied to the item failure rate to describe the proportion of that rate due to the particular failure mode. If all failure mode factors are listed their sum is equal to one.

Given that a particular failure mode occurs, a value, b, the conditional probability of the loss of system function given the occurrence of the failure mode, needs to be assigned, based on a judgement. The value of "b" used should be within the following ranges:

actual loss	$b = 1.0$
probable loss	$0.1 < b < 1.0$
possible loss	$0 < b < 0.1$
no effect	$b = 0$

When the system includes redundant items, the latter may be at risk for only part of the operating time. This is expressed by the time-at-risk proportion, i.e. the proportion of the required operating time for which an item is at risk.

The event frequency λ is given by:

$\lambda = \lambda_b \times m \times a \times b \times r$

where

λ_b is the base failure rate of the item

m is a modifying factor

a is the failure mode factor

b is the conditional probability of system failure

r is the time-at-risk proportion

The calculation is most easily carried out in tabular form. The first 13 columns of Figure B.1.2 show a suitable arrangement (see Appendix B).

3.2.4 Criticality matrix

When the required end product of the analysis is a criticality matrix, this can be plotted from the allocated severities and the event frequencies reached by either of the routes described in **3.2.3**. Guidance is given in **3.3.2** and **3.3.3**.

3.2.5 Ranked contributions — system basis

When ranked contributions are required further steps are necessary. When contributions to failure frequency of the system are required regardless of severity (system basis) these steps are as follows.

a) *Calculation of event frequencies for different inventory levels.* Assuming inventory levels of failure mode, item, subsystem and system, the item event frequency is given by the sum of the frequencies of the modes associated with the item; the subsystem event frequency by the sum of the frequencies of the items making up the subsystem; and so on.

b) *Calculation of contributions to system frequency from each inventory level.* These are given by:

$$\text{subsystem contribution} = \frac{\text{subsystem frequency}}{\text{system frequency}}$$

$$\text{item contribution} = \frac{\text{item frequency}}{\text{system frequency}}$$

and so on.

c) *Ranking of contributions.* This calls for subsystems to be ranked in order of their contributions to system frequency, then for items to be ranked by contribution within the subsystems to which they contribute, and finally for modes to be ranked within the items to which they contribute.

3.2.6 Ranked contributions — severity basis

Where contributions are to be ranked on the basis of severity the necessary steps are as follows.

a) *Calculation of event frequencies within severities for different inventory levels.* Assuming inventory levels of failure mode, item, subsystem and system, the item event frequency is given by the sum of the frequencies of the modes associated with the item which have a given severity, subsystem event frequency by the sum of the frequencies of the items associated with the subsystem which have the appropriate severity, and so on.

b) *Calculation of contributions to system frequency from different inventory levels.* These are given by:

$$\text{subsystem contribution} = \frac{\text{subsystem frequency for severity x}}{\text{system frequency for severity x}}$$

$$\text{item contribution} = \frac{\text{item frequency for severity x}}{\text{system frequency for severity x}}$$

and so on.

c) *Ranking of contributions.* This calls for subsystems to be ranked in order of their contributions to system frequency within each severity, then for items to be ranked by contribution within the subsystems to which they contribute within each severity and finally for modes to be ranked within the items to which they contribute within each severity.

3.2.7 Report of analysis

The information given in respect of the report on an FMEA (see **2.2.4.4**) equally applies to the reporting on FMECAs.

3.3 Supplementary information

3.3.1 General

Criticality is a measure of risk (see BS 4778). It differs from the usually accepted measures of risk only in the less rigorous, and hence less costly, approach to its evaluation. The difference shows primarily in the manner of prediction of the severity of a failure effect. In probabilistic risk analysis (PRA) the consequences of that effect are evaluated in detail; in criticality analysis the severity of an effect is judged to lie in one of a small number of severity classes defined in general terms. When at the outset of an analysis the real possibility of very severe effects is recognized a probabilistic risk analysis should be used in preference to a criticality analysis and the greater costs accepted. Similarly if a criticality analysis reveals very critical effects their more detailed evalution by PRA should be considered.

In conducting a criticality analysis each failure effect is classified by the severity of its effect on the overall system performance and safety in the light of the system requirements, objectives and constraints. A list of possible failures and their severity should be drawn up for each item of equipment. There are, however, generally accepted categories that can apply to most equipment, based on the consequences listed in a) to e), which are classified qualitatively according to their severity:

a) death or injury to operation personnel or to the public;

b) damage to the environment;

c) damage to external equipment or the equipment itself;

d) economic loss due to lack of output or function;

e) failure to complete a task due to inability of equipment to perform its major function.

The choice of severity categories requires careful and judicious decisions. Clearly, it is essential that all relevant factors are considered because of their impact on system evaluation with respect to such factors as performance, cost, time, safety and risk.

The examples of severity scales shown in Table 6 are based on degradation of equipment, system function or mission, injury and damage to the enterprise. Two or more such factors may be combined in defining severity classes.

Table 6 — Examples of failure effect severity scales

Severity	Equipment	System/mission	People	Enterprise
5	Definite or presumed destruction or degradation of other functional equipment	Complete loss of capability	Loss of life	Major plant and production loss. Enterprise survival doubtful
4	Complete failure of or damage to functional equipment under consideration	40 % to 80 % loss of capability	Severe injury and long term damage	Moderate plant and production loss
3	Important degradation of functional equipment under consideration or substantial increase in operator workload	10 % to 40 % loss of capability	Moderate injury with full recovery	Significant production loss
2	Minor degradation of functional equipment under consideration	Less than 10 % loss of capability	Minor injury	Minor production loss
1	Negligible effect on performance of functional equipment under consideration	No or negligible effect on success	No injury	No or negligible production loss

3.3.2 Failure effect frequency or probability

The occurrence of a failure effect in a specified period may be evaluated as effect frequency or the probability of effect occurrence. Which is most easily used depends on the type of item involved at the lowest level. If it is a part, any failure data available will be in the form of failure rates and frequency is the output quantity most easily reached. If the lowest level items are assemblies whose reliabilities have been established analytically, and which are expressed as probabilities, it is easiest to work in probabilities. In the former case the units of criticality would be events/unit time; in the latter the probability of an event occurring per demand or in unit time. Frequency is used in the discussion below but the arguments apply equally to the use of probability.

The frequency of occurrence of each failure effect is predicted, ideally, from the historical failure rate of the part concerned. Uncertainty is always associated with such predictions, the degree depending on the relevance, quality and quantity of the historical data. Estimates of the frequency of a particular failure effect in a particular operating environment require a statistically significant reliability data base.

Predictions are performed as part of the FMECA using failure rate data directly from cited sources. The prediction should take into account the following:

a) the time for which the system function is required, referred to as operating cycle or mission, or a time unit such as a year;

b) the item failure rate under reference environmental and loading conditions;

c) the environment in which the item will be employed;

d) the difference between the expected item loading and reference loading;

e) the proportion of the item failure rate attributable to the relevant failure mode;

f) the probability that the occurrence of the failure mode will cause the failure of the system function;

g) the proportion of the required time for which the item will be in use;

h) the extent to which the maintenance procedures will affect the failure rate.

Data are often needed for basic components of assemblies that are regarded as components themselves, for example, an electric motor. Whilst it can be desirable to examine the item for its failure modes, data are rarely collected at the lower levels, e.g. casing, end plates. The subjective apportionment of a total failure rate to each component is difficult if not impossible. It is preferable to apportion the total to the grouped failure modes.

3.3.3 Criticality assessment

Quantitive evaluation of criticality demands quantitive prediction of the consequence of each failure event and thus lies in the realms of probability risk analysis. The following two approaches to quantitive evaluation are possible which yield outputs helpful in making decisions about required actions:

a) constructing a criticality matrix;

b) ranking failure events by their contribution to the total failure frequency of each severity.

A criticality matrix conveniently displays the severity classes as abscissae and the failure frequency classes as ordinates (see **3.1.2**). In the example shown in Figure 3 the frequency range spanning the failure frequency axis is arbitrarily divided into five classes corresponding to very low, low, medium, high and very high frequencies. For each criticality analysis a specific range of frequencies should be identified for each failure frequency class. In many instances the frequencies will be classified non-linearly.

When the severity of the failure effects has been classified and a frequency class assigned to each one, the effects are plotted in the appropriate square of the chart identified by reference to the failure mode causing the effect. The further this square is from the origin, along the diagonal, the greater the criticality and the more urgent the need for corrective action.

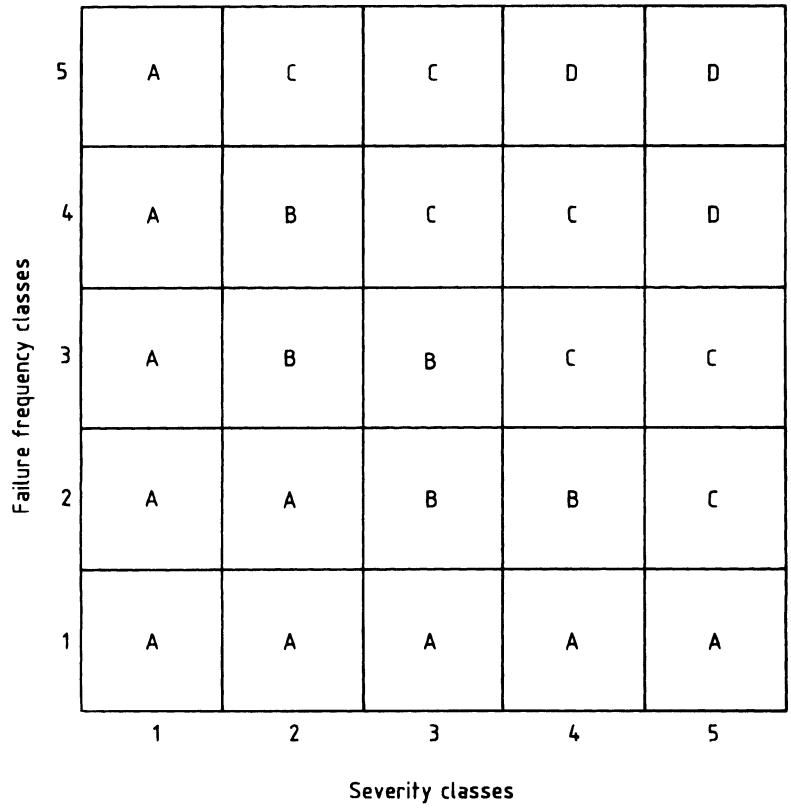
The latter method involves predicting the frequency of failures at mode, item, subsystem and system levels within each severity class and calculating the contribution of each mode, item and subsystem to its associated severity class. Ranking each of the predicted events within its material category within the associated severity identifies the dominant contributors in each category and each severity. Judgements have to be made about the relative importance of contributions near the boundaries between severity classes, e.g. whether a low frequency subsystem failure of severity 3 is more critical than a high frequency failure of severity 2, but the information on which to base such a judgement should be available and accessible in the results of the analysis. An example of this approach is given in **B.1**.

3.3.4 Criticality bands

If the severity and frequency scales are chosen so that the top left square represents the highest tolerable frequency for the most trivial event and the bottom right square the highest tolerable frequency for the most severe event, then a rational relative scale is created for a criticality index, i.e. the product of severity and frequency class numbers. These may be used to define criticality bands which give meaning to squares on the plot which do not lie on the diagonal. The example in Figure 4 shows a criticality matrix with letters indicating the criticality band to which each square belongs. Band A is acceptable while B, C and D have increasing degrees of unacceptability.

When this approach is used the number of classes on the severity or frequency scale can be chosen to suit the system under examination but the number of classes on each scale should be the same.

Upon completion of the analysis in which individual failure modes and their contributions have been considered, it is essential to consider next the frequency of failure effects to which more than one failure mode contributes.



A, B, C and D are criticality bands

Figure 4 — Example of a criticality matrix showing criticality bands

Appendix A Summary of procedure for FMEA and FMECA

Procedural steps needed to perform an analysis are as follows:

a) decide whether FMEA or FMECA is required;

b) define system boundaries for analysis;

c) understand system requirements and function;

d) define failure/success criteria;

e) determine each item's failure modes and their failure effects and record these;

f) summarize each failure effect;

g) report findings.

Additional steps to be taken for FMECA are as follows:

1) determine system severity classes;

2) establish item failure mode severity;

3) determine item failure mode and effect frequencies;

4) determine event frequencies;

5) draw up criticality matrix for item failure modes;

6) summarize the criticality of failure effects from the criticality matrix;

7) Draw up criticality matrix for system failure effects;

8) report findings at all levels of analysis.

NOTE Quantification of failure mode and effect frequencies may be undertaken in an FMEA by carrying out steps 1), 2) and 3) at the end of the FMEA.

Appendix B Examples of analyses

B.1 Ranked contribution approach to criticality analysis

Figure B.1.1 shows a worksheet from an FMEA constructed generally in the manner described in this standard. In this case the essential information from the FMEA is extracted and used to carry out predictions of the failure frequencies associated with each failure mode, item, and subsystem and the system under consideration.

Figure B.1.2 shows a frequency analysis. Columns 1 to 7 have been extracted from the FMEA. The base failure rate for the item is entered in column 8 and modified by factors to account for environment, the proportion of the item failure rate attributable to the failure mode, the probability that a mode failure will cause a mission or operating cycle failure, and the proportion of the time for which the item is at risk. The result is the expected failure mode frequency (column 13).

Failure mode frequencies are summed for each item to yield item failure frequencies (column 14), for each subsystem to yield subsystem failure frequencies (column 15), and for the system to yield the system failure frequency (column 16).

The proportional contributions made to system failure by each subsystem, item and mode are shown in columns 17, 18 and 19. Those contributions are displayed as bar charts in Figure B.1.3. The charts have been arranged with the subsystems ranked in order of their contribution to system failure, with items ranked in order of their contribution to the associated subsystem, and with failure modes ranked in order of their contribution to the associated item.

The result is an ordering of failure frequencies enabling the dominant subsystem, item and mode to be identified for their reliability implications. A similar analysis can be done for the contributions of failure mode, item and subsystem to the failure frequency of each severity.

Figure B.1.4 shows the calculation table of such an analysis. Though in different order down the column, because they are grouped by severity, the values for failure mode frequency (column 13) and their derivation are the same as those for failure mode frequency in Figure B.1.2. Contributions of subsystem, item and failure mode to the frequency of the severity class are shown in columns 15 to 17.

The results are displayed as bar charts in Figure B.1.5. These have been arranged with subsystems ranked in order of their contribution to the failure frequency for the respective severity classes, with items ranked in order of their contribution to the associated subsystem, and with failure modes ranked in order of their contribution to the associated item.

This approach does not put a value on the combination of severity and frequency, i.e. criticality, but it provides a ready means of identifying the dominant contributors to each severity. Judgements have to be made about the relative importance of contributions near severity boundaries, e.g. whether a low frequency subsystem failure of severity 3 is more critical than a high frequency failure of severity 2, but the information on which to base such a judgement should be available and accessible in the results of the analysis.

B.2 FMECA Example 1. Fire protection system of an electric locomotive

Figure B.2 illustrates the application of FMECA to the fire protection system on an electric locomotive.

FMEA

Indenture level: **Design by:** **Prepared by:**

Sheet no.: **Item:** **Approved by:**

Mission phase: **Issue:** **Date:**

Item ref	Item description-function	Failure entry code	Failure mode	Possible failure causes	Symptom detected by	Local effect	Effect on unit output	Compensating provision against failure	Severity class	Failure rate (F/Mhr)	Data source	Recommendations and actions taken
1.1.1	motor stator	1111	open circuit	winding fracture	low speed roughness	low power	trip	single phase protection temperature trip	4			
		1112	open circuit	connection fracture	low speed roughness	low power	trip	single phase protection temperature trip	3			
		1113	insulation breakdown	persistant high temp. manufacturing defect	protection system	overload	no output	annual inspection temperature trip	4			
		1114	thermistor open circuit	ageing connection fracture	protection system	none	no output	fitted spare	3			recommend consideration spare connected through to outside casing
		1115	thermistor short circuit	failure thermistor	protection system	reduced trip margin	no output if load high	fitted spare temperature trip	3			recommend consideration spare connected through to outside casing
1.1.2	motor cooling system	1121	inadequate cooling	blockage low diff. pressure	high temperature stator detected by thermistor	winding excessive temperature	motor excessive temperature	temperature trip stator	2			
		1122	leakage to atmosphere	piping connection	motor temperature	motor inadequate cooling	motor excessive temperature	temperature trip 2 hourly check	2			
		1123	leakage from atmosphere	piping connection	low output	air in system	none	2 hourly check	2			
1.1.3	motor bearing	1131	seal external leakage	wear bearing failure	low level lub oil sump	loss of lub oil	none unless leak severe	daily check	3			

Figure B.1.1 — Example of an FMEA worksheet

CASYS

Indenture level: **Design by:** **Prepared by:**

Sheet no.: **Item:** **Approved by:**

Mission phase: **Issue:** **Date:**

Item ref.	Item description-function	Failure mode	Possible failure causes	Failure entry code	Severity class	Data source	Failure rate (F/Mhr)	Modify. factor	Mode proportion	Mission failure probab.	Time at risk proportion	Failure mode frequency	Item failure frequency	Subsystem failure frequency	System failure frequency	Subsystem contrib. system	Item contrib. system	Mode contrib. system
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1.1.1	motor	open circuit	winding	1111	4		1.90	1.00	0.05	1.00	1.00	0.10	1.43	5.39	82.88	0.07	0.02	0.00
		open circuit	connection	1112	3		1.90	1.00	0.05	1.00	1.00	0.10	1.43	5.39	82.88	0.07	0.02	0.00
		insulation breakdown	persistent high temp.	1113	4		1.90	1.00	0.15	1.00	1.00	0.29	1.43	5.39	82.88	0.07	0.02	0.00
		thermistor	ageing	1114	3		1.90	1.00	0.25	1.00	1.00	0.48	1.43	5.39	82.88	0.07	0.02	0.01
		thermistor	failure	1115	3		1.90	1.00	0.50	0.50	1.00	0.48	1.43	5.39	82.88	0.07	0.02	0.01
1.1.2	motor	inadequate cooling	blockage	1121	2		0.97	2.00	0.33	0.80	1.00	0.51	1.51	5.39	82.88	0.07	0.01	0.01
		leakage to	piping	1122	2		0.97	2.00	0.33	0.50	1.00	0.32	1.15	5.39	82.88	0.07	0.01	0.00
		leakage from	piping	1123	2		0.97	2.00	0.33	0.50	1.00	0.32	1.15	5.39	82.88	0.07	0.01	0.00
1.1.3	motor	seal	wear	1131	3		2.10	2.00	0.66	0.50	1.00	1.39	2.81	5.39	82.88	0.07	0.03	0.02
		bearing	inadequate flow	1132	3		2.10	2.00	0.34	1.00	1.00	1.43	2.81	5.39	82.88	0.07	0.03	0.02
1.2.1	gear wheel	seal	wear	1211	3		2.10	1.00	0.75	0.50	1.00	0.79	1.31	2.66	82.88	0.03	0.02	0.01
		bearing	inadequate flow	1212	3		2.10	1.00	0.25	1.00	1.00	0.53	1.31	2.66	82.88	0.03	0.02	0.01
1.2.2	gear pinion	bearing	inadequate flow	1221	3		0.50	1.00	1.00	1.00	1.00	0.50	0.50	2.66	82.88	0.03	0.01	0.01
1.2.3	gear train	strip	manufacturing defect	1231	4		0.85	1.00	1.00	1.00	1.00	0.85	0.85	2.66	82.88	0.03	0.01	0.01
1.3.1	inlet guide vanes	seizure open	seizure	1311	3		2.20	2.00	0.50	1.00	1.00	2.20	4.40	8.60	82.88	0.10	0.05	0.02
		seizure shut	seizure	1312	3		2.20	2.00	0.25	1.00	1.00	1.10	4.40	8.60	82.88	0.10	0.05	0.01
		seizure shut	seizure	1313	3		2.20	2.00	0.25	1.00	1.00	1.10	4.40	8.60	82.88	0.10	0.05	0.01

Figure B.1.2 — Example of a frequency analysis

CASYS

Indenture level: **Design by:** **Prepared by:**

Sheet no.: **Item:** **Approved by:**

Mission phase: **Issue:** **Date:**

Item ref.	Item description-function	Failure mode	Possible failure causes	Failure entry code	Severity class	Data source	Failure rate (F/Mhr)	Modify. factor	Mode proportion	Mission failure probab.	Time at risk proportion	Failure mode frequency	Item failure frequency	Subsystem failure frequency	System failure frequency	Subsystem contrib. system	Item contrib. system	Mode contrib. system
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1.3.2	main bearing	bearing	inadequate flow	1321	3		0.50	2.00	1.00	1.00	1.00	1.00	1.00	8.60	82.88	0.10	0.01	0.01
1.3.3	ring seal	seal	wear	1331	3		1.60	2.00	1.00	1.00	1.00	3.20	3.20	8.60	82.88	0.10	0.04	0.04
1.4.1	reservoir	leakage from	connection	1411	2		0.80	2.00	1.00	0.50	1.00	0.80	0.80	37.69	82.88	0.45	0.01	0.01
1.4.2	sump oil heaters	no output	open circuit	1421	3		0.80	2.00	1.00	0.10	1.00	0.16	0.16	37.69	82.88	0.45	0.00	0.00
1.4.3	boost lub oil pump	relief open	seizure or broken spring	1431	3		2.40	2.00	0.60	0.50	1.00	1.44	2.86	37.69	82.88	0.45	0.03	0.02
		relief shut	seizure shut	1432	3		2.40	2.00	0.40	0.30	1.00	0.58	2.86	37.69	82.88	0.45	0.03	0.01
		flow control valve	seizure open	1433	3		2.40	2.00	0.50	0.10	1.00	0.24	2.86	37.69	82.88	0.45	0.03	0.00
		flow control valve	seizure shut	1434	3		2.40	2.00	0.50	0.25	1.00	0.60	2.86	37.69	82.88	0.45	0.03	0.01
1.4.4	auxiliary lub oil pump	no flow	motor failure, seized	1441	2		11.0	2.00	0.95	1.00	1.00	20.90	20.96	37.69	82.88	0.45	0.25	0.25
		leakage from	shaft seal	1442	2		11.0	2.00	0.05	0.05	1.00	0.06	20.96	37.69	82.88	0.45	0.25	0.00
1.4.5	low speed lub oil pump	low output	blockage	1451	3		0.60	2.00	1.00	1.00	1.00	1.20	1.20	37.69	82.88	0.45	0.01	0.01
1.4.6	high speed lub oil pump	low output	blockage	1461	3		0.60	2.00	1.00	1.00	1.00	1.20	1.20	37.69	82.88	0.45	0.01	0.01
1.4.7	oil cooler	inadequate cooling	fouling	1471	2		1.00	2.00	0.20	0.80	1.00	0.32	1.92	37.69	82.88	0.45	0.02	0.00

Figure B.1.2 — Example of a frequency analysis *(concluded)*

Casub. sys				Cait. sys				Camod. sys				
Failure entry code	Severity class	Subsystem contrib. system	Percentage contribution of subsystem to system frequency * = 1 % ‡ ≥50 %	Failure entry code	Severity class	Item contrib. system	Percentage contribution of item to system frequency * = 1 % ‡ ≥50 %	Failure entry code	Severity class	Mode contrib. system	Mode frequency	Percentage contribution of failure modes to system frequency * = 1 % ‡ ≥50 %
1441	4	0.45	.....	1441	4	0.25	.....	1441	4	0.25	20.90	.....
1442	4	0.45	.....	1442	4	0.25	.....	1442	4	0.00	0.06	
1491	4	0.45	.....	1491	4	0.07	.....	1491	4	0.05	4.14	.....
1493	3	0.45	.....	1493	3	0.07	.....	1493	3	0.01	0.74	.
1494	3	0.45	.....	1494	3	0.07	.....	1494	3	0.01	0.74	.
1492	4	0.45	.....	1492	4	0.07	.....	1492	4	0.00	0.37	
1431	3	0.45	.....	1431	3	0.03	...	1431	3	0.02	1.44	..
1434	3	0.45	.....	1434	3	0.03	...	1434	3	0.01	0.60	.
1432	3	0.45	.....	1432	3	0.03	...	1432	3	0.01	0.58	.
1433	3	0.45	.....	1433	3	0.03	...	1433	3	0.00	0.24	
1481	4	0.45	.....	1481	4	0.03	...	1481	4	0.03	2.60	...
1472	4	0.45	.....	1472	4	0.02	..	1472	4	0.01	0.80	.
1473	3	0.45	.....	1473	3	0.02	..	1473	3	0.01	0.80	.
1471	4	0.45	.....	1471	4	0.02	..	1471	4	0.00	0.32	
1451	3	0.45	.....	1451	3	0.01	.	1451	3	0.01	1.20	.
1461	3	0.45	.....	1461	3	0.01	.	1461	3	0.01	1.20	.
1411	4	0.45	.....	1411	4	0.01	.	1411	4	0.01	0.80	.
1421	3	0.45	.....	1421	3	0.00		1421	3	0.00	0.16	
1551	3	0.18	.....	1551	3	0.08	.....	1551	3	0.04	3.00	....
1553	4	0.18	.....	1553	4	0.08	.....	1553	4	0.02	2.00	..
1552	3	0.18	.....	1552	3	0.08	.....	1552	3	0.02	1.50	..
1511	4	0.18	.....	1511	4	0.05	.....	1511	4	0.01	1.12	.
1512	4	0.18	.....	1512	4	0.05	.....	1512	4	0.01	1.12	.
1513	4	0.18	.....	1513	4	0.05	.....	1513	4	0.01	1.12	.
1514	4	0.18	.....	1514	4	0.05	.....	1514	4	0.01	0.56	.
1516	4	0.18	.....	1516	4	0.05	.....	1516	4	0.01	0.56	.
1532	4	0.18	.....	1532	4	0.02	..	1532	4	0.01	1.20	.
1531	4	0.18	.....	1531	4	0.02	..	1531	4	0.01	0.60	.
1521	4	0.18	.....	1521	4	0.02	..	1521	4	0.01	1.12	.
1522	4	0.18	.....	1522	4	0.02	..	1522	4	0.01	0.48	.
1561	3	0.18	.....	1561	3	0.00		1561	3	0.00	0.28	
1562	3	0.18	.....	1562	3	0.00		1562	3	0.00	0.06	
1541	4	0.18	.....	1541	4	0.00		1541	4	0.00	0.01	
2022	4	0.15	.....	2022	4	0.13	.....	2022	4	0.10	8.16	.....
2023	4	0.15	.....	2023	4	0.13	.....	2023	4	0.02	2.04	..
2021	4	0.15	.....	2021	4	0.13	.....	2021	4	0.01	0.82	.

Figure B.1.3 — Bar chart of subsystem contributions to system failure

Indenture level:				Design by:							Prepared by:					CASEV
Sheet no.:				Item:							Approved by:					
Mission phase:				Issue:							Date:					
Item ref.	Item description-function	Failure mode	Possible failure causes	Failure entry code	Severity class	Data source	Failure rate (F/Mhr)	Modify. factor	Mode proportion	Mission failure probab.	Time at risk proportion.	Failure mode frequency	Severity frequency	Mode contrib. severity	Item contrib. severity	Subsystem contrib. severity
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1.1.1	motor	open circuit	winding	1111	4		1.90	1.00	0.05	1.00	1.00	0.10	1.23	0.08	0.31	0.31
		insulation breakdown	persistent high temp.	1113	4		1.90	1.00	0.15	1.00	1.00	0.29	1.23	0.23	0.31	0.31
1.2.3	gear train	strip	manufacturing defect	1231	4		0.85	1.00	1.00	1.00	1.00	0.85	1.23	0.69	0.69	0.69
		open circuit	connection	1112	3		1.90	1.00	0.05	1.00	1.00	0.10	28.80	0.00	0.04	0.13
		thermistor	ageing	1114	3		1.90	1.00	0.25	1.00	1.00	0.48	28.80	0.02	0.04	0.13
		thermistor	failure	1115	3		1.90	1.00	0.50	0.50	1.00	0.48	28.80	0.02	0.04	0.13
1.1.3	motor	seal	wear	1131	3		2.10	2.00	0.66	0.50	1.00	1.39	28.80	0.05	0.10	0.13
		bearing	inadequate flow	1132	3		2.10	2.00	0.34	1.00	1.00	1.43	28.80	0.05	0.10	0.13
1.2.1	gear wheel	seal	wear	1211	3		2.10	1.00	0.75	0.50	1.00	0.79	28.80	0.03	0.05	0.06
		bearing	inadequate flow	1212	3		2.10	1.00	0.25	1.00	1.00	0.53	28.80	0.02	0.05	0.06
1.2.2	gear pinion	bearing	inadequate flow	1221	3		0.50	1.00	1.00	1.00	1.00	0.50	28.80	0.02	0.02	0.06
1.3.1	inlet guide vanes	seizure open	seizure	1311	3		2.20	2.00	0.50	1.00	1.00	2.20	28.80	0.08	0.15	0.30
		seizure shut	seizure	1312	3		2.20	2.00	0.25	1.00	1.00	1.10	28.80	0.04	0.15	0.30
		seizure shut	seizure	1313	3		2.20	2.00	0.25	1.00	1.00	1.10	28.80	0.04	0.15	0.30
1.3.2	main bearing	bearing	inadequate flow	1321	3		0.50	2.00	1.00	1.00	1.00	1.00	28.80	0.03	0.03	0.30
1.3.3	ring seal	seal	wear	1331	3		1.60	2.00	1.00	1.00	1.00	3.20	28.80	0.11	0.11	0.30
1.4.2	sump oil heaters	no output	open circuit	1421	3		0.80	2.00	1.00	0.10	1.00	0.16	28.80	0.01	0.01	0.27
1.4.3	boost lub oil pump	relief open	seizure or broken spring	1431	3		2.40	2.00	0.60	0.50	1.00	1.44	28.80	0.05	0.10	0.27
		relief shut	seizure shut	1432	3		2.40	2.00	0.40	0.30	1.00	0.58	28.80	0.02	0.10	0.27
		flow control valve	seizure open	1433	3		2.40	2.00	0.50	0.10	1.00	0.24	28.80	0.01	0.10	0.27

Figure B.1.4 — Analysis of contributions to system failure

Indenture level:				**Design by:**							**Prepared by:**					CASEV
Sheet no.:				**Item:**							**Approved by:**					
Mission phase:				**Issue:**							**Date:**					
Item ref.	**Item description-function**	**Failure mode**	**Possible failure causes**	**Failure entry code**	**Severity class**	**Data source**	**Failure rate (F/Mhr)**	**Modify. factor**	**Mode proportion**	**Mission failure probab.**	**Time at risk proportn.**	**Failure mode frequency**	**Severity frequency**	**Mode contrib. severity**	**Item contrib. severity**	**Subsystem contrib. severity**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
		flow control valve	seizure shut	1434	3		2.40	2.00	0.50	0.25	1.00	0.60	28.80	0.02	0.10	0.27
1.4.5	low speed lub oil pump	low output	blockage	1451	3		0.60	2.00	1.00	1.00	1.00	1.20	28.80	0.04	0.04	0.27
1.4.6	high speed lub oil pump	low output	blockage	1461	3		0.60	2.00	1.00	1.00	1.00	1.20	28.80	0.04	0.04	0.27
		leak water to oil	tube	1473	3		1.00	2.00	0.40	1.00	1.00	0.80	28.80	0.03	0.03	0.27
		low flow	boost pump nrv blocked	1493	3		3.70	2.00	0.10	1.00	1.00	0.74	28.80	0.03	0.05	0.27
		low flow	bearing nrv blocked	1494	3		3.70	2.00	0.10	1.00	1.00	0.74	28.80	0.03	0.05	0.27
1.5.5	hot gas bypass solenoid	fail open	seized — broken	1551	3		5.00	2.00	0.30	1.00	1.00	3.00	28.80	0.10	0.16	0.17
		fail closed — mech.	seized — broken	1552	3		5.00	2.00	0.30	0.50	1.00	1.50	28.80	0.05	0.16	0.17
1.5.6	hot gas bypass valve	fail open	spring — dirt	1561	3		0.20	2.00	0.70	1.00	1.00	0.28	28.80	0.01	0.01	0.17
		fail closed	pilot blocked — dirt	1562	3		0.20	2.00	0.30	0.50	1.00	0.06	28.80	0.00	0.01	0.17

Figure B.1.4 — Analysis of contributions to system failure *(concluded)*

Casub. sev				Cait. sev				Camod. sev				
Failure entry code	Severity class	Subsystem contrib. severity	Percentage contribution of sybsystem to frequency of severity class * = 1 % ‡ ≥50 %	Failure entry code	Severity class	Item contrib. severity	Percentage contribution of item to frequency of subsystem in severity class * = 1 % ‡ ≥50 %	Failure entry code	Severity class	Mode contrib. severity	Mode frequency	Percentage contribution of failure mode to frequency of item in severity class * = 1 % ‡ ≥50 %
1231	4	0.69	::	1231	4	0.69	::	1231	4	0.69	0.85	::
1113	4	0.31	....	1113	4	0.31	....	1113	4	0.23	0.29	....
1111	4	0.31	....	1111	4	0.31	....	1111	4	0.08	0.10	....
1311	3	0.30	....	1311	3	0.15	....	1311	3	0.08	2.20	....
1312	3	0.30	....	1312	3	0.15	....	1312	3	0.04	1.10	....
1313	3	0.30	....	1313	3	0.15	....	1313	3	0.04	1.10	....
1331	3	0.30	....	1331	3	0.11	....	1331	3	0.11	3.20	....
1321	3	0.30	....	1321	3	0.03	...	1321	3	0.03	1.00	...
1431	3	0.27	....	1431	3	0.10	....	1431	3	0.05	1.44	.....
1434	3	0.27	....	1434	3	0.10	....	1434	3	0.02	0.60	..
1432	3	0.27	....	1432	3	0.10	....	1432	3	0.02	0.58	..
1433	3	0.27	....	1433	3	0.10	....	1433	3	0.01	0.24	.
1493	3	0.27	....	1493	3	0.05	.....	1493	3	0.03	0.74	...
1494	3	0.27	....	1494	3	0.05	.....	1494	3	0.03	0.74	...
1451	3	0.27	....	1451	3	0.04	....	1451	3	0.04	1.20	....
1461	3	0.27	....	1461	3	0.04	....	1461	3	0.04	1.20	....
1473	3	0.27	....	1473	3	0.03	...	1473	3	0.03	0.80	...
1421	3	0.27	....	1421	3	0.01	.	1421	3	0.01	0.16	.
1551	3	0.17	....	1551	3	0.16	....	1551	3	0.10	3.00	....
1552	3	0.17	....	1552	3	0.16	....	1552	3	0.05	1.50	.....
1561	3	0.17	....	1561	3	0.01	.	1561	3	0.01	0.28	.
1562	3	0.17	....	1562	3	0.01	.	1562	3	0.00	0.06	
1132	3	0.13	....	1132	3	0.10	....	1132	3	0.05	1.43	.....
1131	3	0.13	....	1131	3	0.10	....	1131	3	0.05	1.39	.....
1114	3	0.13	....	1114	3	0.04	....	1114	3	0.02	0.48	..
1115	3	0.13	....	1115	3	0.04	....	1115	3	0.02	0.48	..
1112	3	0.13	....	1112	3	0.04	....	1112	3	0.00	0.10	
1211	3	0.06	......	1211	3	0.05	.....	1211	3	0.03	0.79	...
1212	3	0.06	......	1212	3	0.05	.....	1212	3	0.02	0.53	..
1221	3	0.06	......	1221	3	0.02	..	1221	3	0.02	0.50	..
2012	3	0.03	...	2012	3	0.03	...	2012	3	0.02	0.50	..
2013	3	0.03	...	2013	3	0.03	...	2013	3	0.02	0.50	..
3013	3	0.03	...	3013	3	0.03	...	3013	3	0.03	0.99	...
1441	2	0.57	::	1441	2	0.40	....	1441	2	0.40	20.90	....
1442	2	0.57	::	1442	2	0.40	....	1442	2	0.00	0.06	
1491	2	0.57	::	1491	2	0.09	....	1491	2	0.08	4.14	....

Figure B.1.5 — Bar chart showing ranked contributions

Failure mode effect and criticality analysis

Project: Electric locomotive **FMECA document no.:** BREL/FMECA/E.LOCO/001 **Issue:** Issue A

System: Fire protection system (single locomotive) **Originator:** BREL Reliability engineers **Date:** 18/1/88

Sub-system RAVERS Z **Design authority:** BREL **Drawing no.:** E.LOCO **Reliability function block diagram no.:** BREL/RBD/E.LOCO/001 **Issue:**

Function: To detect and extinguish a fire within the locomotive **Reliability prediction document no.:** **Issue:**

Ref.	Item	Item fail mode	Failure cause	Block function desc.	Fun. fail mode	Effect on sub-sys. outputs	Effect on sys. reliab.	Effect on sys. safety	Prev. act. design	Prev. act. QA	Comments	Severity	Fail rate (alpha)
01	1) Fire detector(s)	Failed to open circuit conditions		Any fire detector block	Detection of false fire	All 3 fire valves energized when M.S. off	B.T.M. released when M.S. returned to "OFF"	None	Continuity test of detector wiring	Open circuit test of detectors	Alarm sounds, B.T.M. released when returning M.S. switch to "OFF"	Signif.	0.0080 (1.0)
		Failed to short circuit conditions		Any fire detector block	Individual fire detector will not detect fire	Fire is not detected	No B.T.M. and vehicle not isolated when needed	Safety may be affected	Design to evaluate detector location		Fire may be detected later but may be too hot to extinguish	Haz.	0.0080 (1.0)
02	Relay FR/3	Coil failed	Coil wire failed to open circuit conditions	Fire alarm operates and coil FDR 1/2 de-energized	Alarm sounded and relay FDR 1/2 de-energized needlessly	Fire valves energized when M.S. returned to "OFF"	B.T.M. released when M.S. returns to "OFF"	None	Risk accepted — right side failure			Signif.	0.070 (1.0)
		Contact 1 failed to short circuit conditions	Contactor broken or dirt ingression	Coil FDR 1/2 de-energized	Coil FDR 1/2 not de-energized when required	Fire valves cannot be energized and vehicle cannot be isolated when needed	No B.T.M. and vehicle not isolated when needed	Safety may be affected	Manual override		Driver must initiate manual release when alarm sounds	Haz.	0.0035 (1.0)
		Contact 1 failed to open circuit conditions	Contactor broken	Coil FDR 1/2 de-energized	Coil FDR 1/2 de-energized without need	Fire valves energized when M.S. returned to "OFF"	B.T.M. released when M.S. returned to "OFF"	None	Risk accepted — right side failure		No alarm sounded when B.T.M released	Signif.	0.018 (1.0)

Figure B.2 — FMECA of the fire protection system of an electric locomotive

Ref.	Item	Item fail mode	Failure cause	Block function desc.	Fun. fail mode	Effect on sub-sys. outputs	Effect on sys. reliab.	Effect on sys. safety	Prev. act. design	Prev. act. QA	Comments	Severity	Fail rate (alpha)
		Contact 2 failed to short circuit conditions	Contactor broken or dirt ingression	Fire alarm operates	Alarm rings needlessly	Alarm rings needlessly	Alarm rings without need		Isolate system state in drivers manual		Driver may think that there is a fire and may op. manual backup	Signif.	0.0035 (1.0)
		Contact 2 failed to open circuit conditions	Contactor broken	Fire alarm operates	No alarm when required	No alarm when required	No alarm when needed	None	Both bells to be tested during drivers prep.		No alarm sent to driver	Haz.	0.018 (1.0)

Figure B.2 — FMECA of the fire protection system of an electric locomotive *(concluded)*

B.3 FMECA Example 2. Sub-subsystem of a motor-generator set

This example illustrates the application of the FMECA technique to a motor-generator (M-G) system. The objective of the study was confined to that system only and was not concerned with the effects of failure on any loads supplied with electrical power from the M-G set or any other external effects of failures. This therefore defines the boundaries of the analysis. The example, shown in part only, illustrates how the system was represented in a hierarchical block diagram form. Initial sub-division identified five subsystems (Figure B.1.3) and one of these, the enclosure heating, ventilation and cooling system, is developed through lower levels of the hierarchical structure to the component level at which it was decided to start the FMEA (Figure B.3.2). The block diagrams also show the numbering system adopted that was used as a cross reference with the FMEA worksheets.

One example of a worksheet is shown for one of the sub-subsystems of the M-G set (Figure B.3.3), which generally complies with the recommended format in this standard. It also includes a particular method of using this same document to present a quantitative assessment of failure rates for the individual failure modes of each item. An FMEA worksheet was then used to combine all sub-subsystem FMEAs to present the FMEA for each subsystem and finally a third level worksheet presented the complete system FMECA.

An essential prerequisite for such an FMECA is the definition and classification of the severity of the effects of failures on the complete M-G system. For the particular application of the example system these were defined as follows (based on general definitions in DEF STAN 00-41).

a) *Catastrophic:* failure to generate power for remainder of mission.

b) *Critical:* system degradation for remainder of mission.

c) *Major:* loss of power generation due to forced outage until repaired.

d) *Minor:* temporary system degradation until convenient to repair.

e) *Negligible effect:* no loss or significant degradation of generating capability.

B.4 Example of a process FMEA

A manufacturing or process FMEA considers each of the processes involved in the manufacture of the item concerned, what could go wrong, what safeguards exist against the failure, how often it might occur, and how it might be eliminated by redesign of the item or the process. The objective is to concentrate attention on possible (or known) problems in sustaining or achieving required output quality. Assemblers of complex goods such as motor cars are well advised to insist that their component suppliers carry out such analyses, but the component manufacturers are usually the principal beneficiaries. The exercise forces a re-examination of entrenched methodology in manufacture and seldom fails to lead to cost improvements.

The format is basically similar to that for a product FMEA but some changes are forced by the slightly different requirements (see Figure B.4). The process FMEA examines how defects and defectives can arise and reach customers, or be found by quality control procedures. It does not examine how the product may fail in service due to wear or maloperation. There is inevitably some overlap, because some defects affect the durability of the components in service, while others cause immediate or early failure.

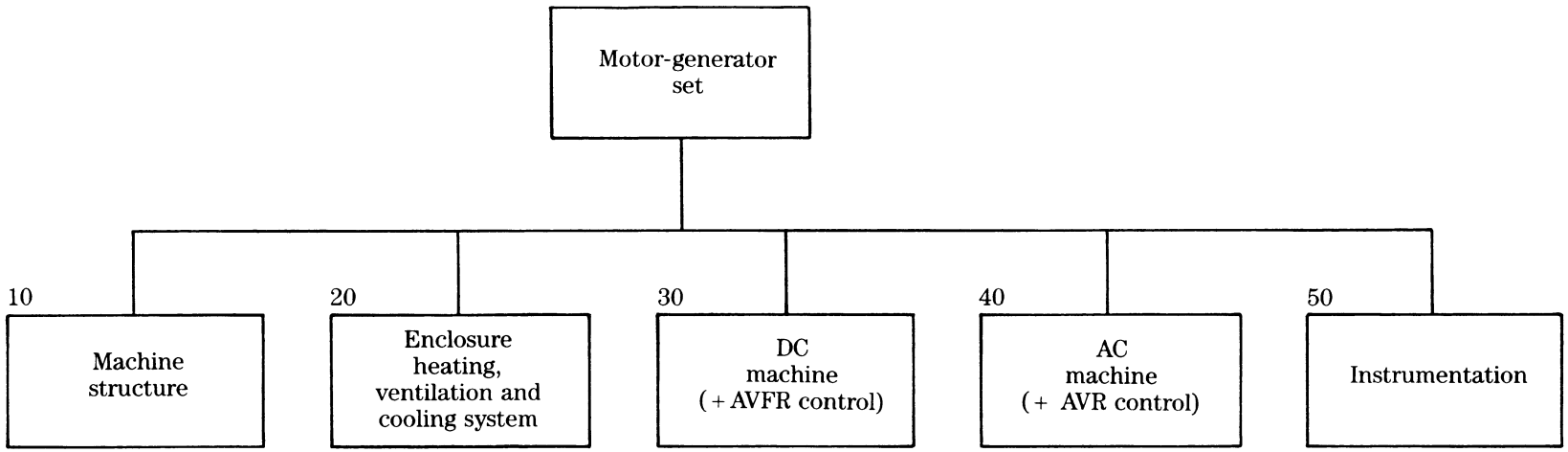


Figure B.3.1 — Block diagram of subsystems of a motor-generator set

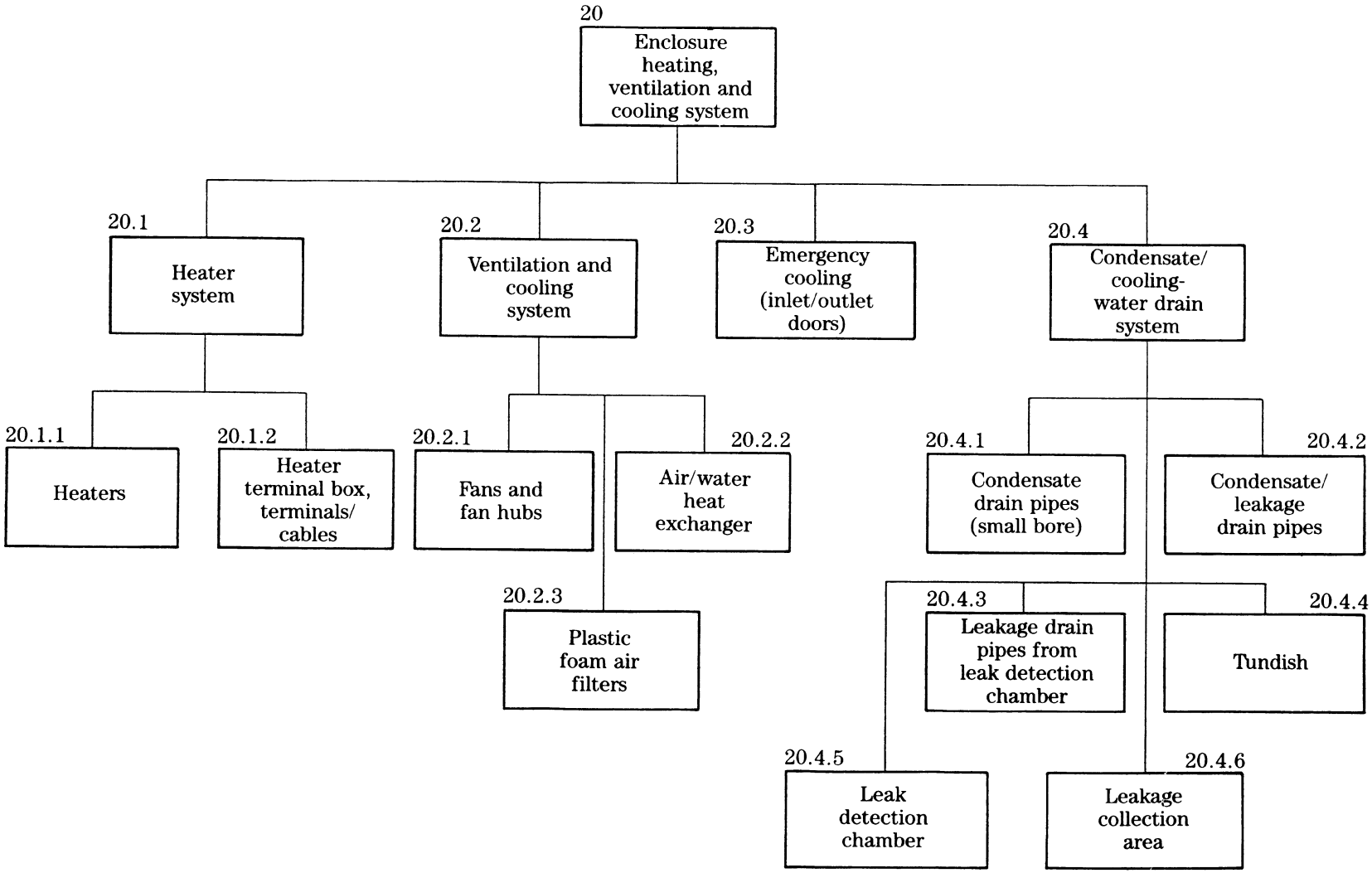


Figure B.3.2 — Block diagram of enclosure heating, ventilation and cooling systems

Subsystem — 20 Enclosure heating, ventilation and cooling system												
Ref.	**Component**	**Function**	**Failure mode**	**Failure effect**	**Detection method or symptom**	**Redundancy provided**	**Mode failure rate severity level f/10^6 h**					**Remarks**
							1	2	3	4	5	
20.1	Heater system (12 off – 6 off at each end) (Only in use when machine non-operational)	To keep machine at temperature > 5 °C above ambient to prevent condensation on machine internals when not in use	All									NOTE The machine may overheat if the heaters do not turn off automatically when running
20.1.1	Heaters	To heat up enclosure	a) o/c, burnt out heater	Reduced heating	a) Temperature indication < 5°C above ambient					1.2		
			b) s/c or earth fault due to insulation breakdown	Loss of all heating — possible condensation	b) Supply, fuse, or circuit breaker monitored	All in parallel, no supply redundancy				0.3		One earth fault should not fail system
20.1.2	Heater terminal box, terminals, cables	Connect supply to heaters	a) o/c terminal or cable can fail one, three, six or all heaters	Loss or reduction of heating — condensation	Temperature < 5 °C above ambient					0.5		
			b) s/c terminals (tracking)	Loss of all heating — condensation	Supply monitored					neglig.		
						Totals				2.0		

Figure B.3.3 — FMEA of subsystem including failure rate assessment

								Exiting conditions						Resulting conditions			
Ref.	Process	Failure mode	Effect on	Potential effect	V	Potential cause	Existing controls	Occ	Sev	Det	APN	Recommended action	Action taken	Occ	Sev	Det	APN
01-01-01	Inserts	Incorrect size or shoulder bend angle	i)a	Inserts without load onto die. Reduced productivity		Poor manufacture or quality control	Producer and acceptance sampling plans	1	9	1	9	Review of sampling plans. Segregation of defective stock from good stock. Training assemblers					
02			i)b	Insert malaligned. Scrap													
03			i)a	Incorrect thickness of skirt surrounding insert. Scrap													
04			iv)b	Reduced performance													
05			iv)c	Reduced life													
01-02-01	Inserts	Poor flash nickel plating	ii)a	Corrosion. Rejected at finishing stage			Visual inspection during acceptance sampling plan	5	6	1	30	Include instructions in sampling inspection to carry out visual check for correct plating					
01-03-01	Inserts	Inadequate face scoring	i)a	Poor metal flow. Incorrect wall thickness. Scrap		Poor manufacture or quality control	Visual inspection during acceptance sampling plan	2	8	6	96	Include instructions in sampling inspection to carry out visual check for correct plating					

Figure B.4 — Part of a process or manufacturing FMECA for machined aluminium castings

								Exiting conditions						Resulting conditions			
Ref.	**Process**	**Failure mode**	**Effect on**	**Potential effect**	**V**	**Potential cause**	**Existing controls**	**Occ**	**Sev**	**Det**	**APN**	**Recommended action**	**Action taken**	**Occ**	**Sev**	**Det**	**APN**
02			ii)a	Thin walls found during final machining. Scrap													
03			iv)a	Reduced life													
01-04-01	Inserts	Contaminated (dust or grease)	i)a	Blow holes, thin walls. Scrap		Contaminated during storage, handling or casting process	Sampling inspection on receipt from supplier. Arbitrary pre-use inspection of suspect contaminated struts after prolonged storage	.5	5	5	12.5	Issue formal instructions for pre-use inspection following prolonged storage					
02			ii)a	Blow holes found during final machining			Use of spatula by caster for transfer					Rotation of inserts stored for long periods					

Effect code:

i Effect on the casting process
ii Effect on the finishing process
iii Effect on the assembler
iv Effect on the end user

Criticality code:

Occ = Prob. of occurrence × 10
Sev = Severity of effect on 1-10 scale
Det = Prob. not detected before reaching customer × 10
APN = Occ × Sev × Det (Action Priority Number)

Figure B.4 — Part of a process or manufacturing FMECA for machined aluminium castings *(concluded)*

Appendix C Bibliography

DEF STAN 00-41[2], *MOD Practices and procedures for reliability and maintainability — Part 3: Reliability prediction.*

GREEN A.E., and BOURNE A.J. *Reliability technology*. Wiley, 1972.

HAMMER, W. *Handbook of system and product safety*. Prentice Hall, 1972.

MIL STAN 1629A[3][4] Procedures for performing a failure modes, effects and criticality analysis.

SMITH, D.J. *Reliability and maintainability in perspective*. 3rd ed. Macmillan, 1988.

[2] Available from Ministry of Defence Directorate of Standardization, Kentigern House, 65 Brown Street, Glasgow G2 8EX.

[3] Available from US Government Printing Office, Washington DC. 20402 USA.

[4] MIL STAN 1629A has been included to provide the user of BS 5760-5 with information on an alternative procedure for carrying out FMEAs.

Publication(s) referred to

BS 4778, *Quality vocabulary.*

BS 4778-1, *International terms.*

BS 4778-2, *Quality concepts and related definitions.*

BS 4778-3, *Availability, reliability and maintainability terms.*

BS 5760, *Reliability of systems, equipment and components.*

BS 5760-0, *Introductory guide to reliability*[5)].

BS 5760-1, *Guide to reliability and maintainability programme management.*

BS 5760-2, *Guide to the assessment of reliability*[5)].

BS 5760-3, *Guide to reliability practices: examples*[5)].

BS 5760-4, *Guide to specification clauses relating to the achievement and development of reliability in new and existing items*[5)].

BS 5760-6, *Guide to programmes for reliability growth.*

IEC 50, *International Electrotechnical Vocabulary*[5)].

IEC 812, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*[5)].

British Telecommunications handbook of reliability data for electronic components[6)].

MIL HBK 217[7)] Reliability prediction of electrical equipment.

Non electronic parts reliability data. Reliability Analysis Center[8)].

[5)] Referred to in the foreword only.

[6)] Published by IMI, Index House, Ascot, Berks SL5 7EU.

[7)] Available from US Government Printing Office, Washington DC. 20402, USA.

[8)] IIT Research Institute, Reliability Analysis Center, P.O. Box 4700, Rome, NY 13440-8200, USA.

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: 020 8996 9000. Fax: 020 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: 020 8996 9001. Fax: 020 8996 7001.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: 020 8996 7111. Fax: 020 8996 7048.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: 020 8996 7002. Fax: 020 8996 7001.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL