Resource A

PAPER 2

Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

NORME DE LA CEI

INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC STANDARD

Publication 812

Première édition — First edition

1985

Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)

Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

Bureau Central de la Commission Electrotechnique Internationale

3, rue de Varembé

Genève, Suisse

Prix fixé 56.–

Price

Révision de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la Commission afin d'assurer qu'il reflète bien l'état actuel de la technique.

Les renseignements relatifs à ce travail de révision, à l'établissement des éditions révisées et aux mises à jour peuvent être obtenus auprès des Comités nationaux de la CEI et en consultant les documents ci-dessous:

- **Bulletin de la CEI**
- **Annuaire de la CEI**
- **Catalogue des publications de la CEI**
  Publié annuellement

Terminologie

En ce qui concerne la terminologie générale, le lecteur se reportera à la Publication 50 de la CEI: Vocabulaire Electrotechnique International (VEI), qui est établie sous forme de chapitres séparés traitant chacun d'un sujet défini, l'Index général étant publié séparément. Des détails complets sur le VEI peuvent être obtenus sur demande.

Les termes et définitions figurant dans la présente publication ont été soit repris du VEI, soit spécifiquement approuvés aux fins de cette publication.

Symboles graphiques et littéraux

Pour les symboles graphiques, symboles littéraux et signes d'usage général approuvés par la CEI, le lecteur consultera:

- la Publication 27 de la CEI: Symboles littéraux à utiliser en électrotechnique;
- la Publication 617 de la CEI: Symboles graphiques pour schémas.

Les symboles et signes contenus dans la présente publication ont été soit repris des Publications 27 ou 617 de la CEI, soit spécifiquement approuvés aux fins de cette publication.

Publications de la CEI établies par le même Comité d'Etudes

L'attention du lecteur est attirée sur la page 3 de la couverture, qui énumère les publications de la CEI préparées par le Comité d'Etudes qui a établi la présente publication.

Revision of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information on the work of revision, the issue of revised editions and amendment sheets may be obtained from IEC National Committees and from the following IEC sources:

- **IEC Bulletin**
- **IEC Yearbook**
- **Catalogue of IEC Publications**
  Published yearly

Terminology

For general terminology, readers are referred to IEC Publication 50: International Electrotechnical Vocabulary (IEV), which is issued in the form of separate chapters each dealing with a specific field, the General Index being published as a separate booklet. Full details of the IEV will be supplied on request.

The terms and definitions contained in the present publication have either been taken from the IEV or have been specifically approved for the purpose of this publication.

Graphical and letter symbols

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to:

- IEC Publication 27: Letter symbols to be used in electrical technology;
- IEC Publication 617: Graphical symbols for diagrams.

The symbols and signs contained in the present publication have either been taken from IEC Publications 27 or 617, or have been specifically approved for the purpose of this publication.

IEC publications prepared by the same Technical Committee

The attention of readers is drawn to the inside of the back cover, which lists IEC publications issued by the Technical Committee which has prepared the present publication.

Publication 812

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

NORME DE LA CEI

INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC STANDARD

Publication 812

Première édition — First edition

1985

7086: 24

Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)

Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

Bureau Central de la Commission Electrotechnique Internationale

3, rue de Varembé

Genève, Suisse

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ANALYSIS TECHNIQUES FOR SYSTEM RELIABILITY — PROCEDURE FOR FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

FOREWORD

1) The formal decisions or agreements of the IEC on technical matters, prepared by Technical Committees on which all the National Committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.

2) They have the form of recommendations for international use and they are accepted by the National Committees in that sense.

3) In order to promote international unification, the IEC expresses the wish that all National Committees should adopt the text of the IEC recommendation for their national rules in so far as national conditions will permit. Any divergence between the IEC recommendation and the corresponding national rules should, as far as possible, be clearly indicated in the latter.

PREFACE

This standard has been prepared by IEC Technical Committee No. 56: Reliability and Maintainability.

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

Six Months' Rule	Report on Voting
56(CO)85	56(CO)97

Further information can be found in the Report on Voting indicated in the table above.

The following IEC publication is quoted in this standard.

Publication No. 271 (1974): List of Basic Terms, Definitions and Related Mathematics for Reliability

ANALYSIS TECHNIQUES FOR SYSTEM RELIABILITY — PROCEDURE FOR FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

1. Scope

This standard describes Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects and Criticality Analysis (FMECA), and gives guidance as to how they may be applied to achieve various objectives, as follows:

- by providing the procedural steps necessary to perform an analysis;
- by identifying appropriate terms, assumptions, criticality measures, failure modes;
- by determining basic principles;
- by providing examples of the necessary forms.

All the general qualitative considerations presented for FMEA will apply to FMEAC, since one is an extension of the other.

2. General

The 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 significant consequences affecting the system performance in the application considered.

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 required and these complement one another. Quantitative analysis methods allow the calculation or prediction of performance indices of the system while fulfulling a specific task or in long-term operation under specific conditions. Typical indices denote reliability, safety, availability, failure rates, MTTF (Mean Time To Failure), etc.

The FMEA is based on that defined component or sub-assembly level where the basic failure criteria (primary failure modes) are available. Starting from the basic element failure characteristics and the functional system structure, the FMEA determines the relationship between the element failures and the system failures, malfunctions, operational constraints and degradation of performance or integrity. To evaluate secondary and higher-order system and subsystem failures, the sequences of events in time may also have to be considered.

In a narrow sense, the 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 could be included.

The severity of the consequences of failure is described by criticality. The criticality is designated by categories or levels which are functions of the dangers and the losses of system capabilities and sometimes of the probability of their occurrence. This probability is best separately identified.

A logical extension of the FMEA is the consideration of the criticality and probability of occurrence of the failure modes. This criticality analysis of the identified failure modes is widely known as FMECA.

2.1 *Purpose of the analysis*

FMEA and FMECA are important techniques for a reliability assurance programme which can be applied to a wide range of problems and may be encountered in technical systems with varying depths and modifications to suit the purpose. The analysis is carried out in a limited way during 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.

The development of reliability block diagrams and state diagrams derived from the system structure is interrelated with the FMEA. Separate diagrams will be needed for:

- differently identified and defined criteria for system failure;
- degradation of function or reduction in assurance of function;
- safety;
- alternative operational phases:

The purposes of FMEA and FMECA may include:

a) evaluation of the effects and the sequences of events caused by each identified item failure mode, from whatever cause, at various levels of a system's functional hierarchy;

b) determination of the significance or criticality of each failure mode as to the system's correct function or performance and the impact on the reliability and/or safety of the related process;

c) classification of identified failure modes according to their detectability, diagnosability, testability, item replaceability, compensating and operating provisions (repair, maintenance and logistics, etc.) and any other relevant characteristics;

d) estimation of measures of the significance and probability of failure, subject to the availability of data.

2.2 *Application*

2.2.1 *FMEA field of application*

FMEA is a method which is primarily adapted to the study of material and equipment failures and which can be applied to categories of systems based on different technologies (electrical, mechanical, hydraulic, etc.) and combinations of technologies. FMEA may also be used for the study of software and human performance.

2.2.2 *FMEA application within the framework of 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 a technique for design review support and for assurance and assessment which should be put into use from the very first steps of system and subsystem design. FMEA is appropriate to all levels of system design. Special training of personel performing FMEA is required, and they must have the close collaboration of systems engineers and designers. The FMEA must be updated as the project progresses and as designs are modified. By the end of the project, FMEA is used to check the project design and may be essential for demonstration of conformity of a designed system to required standards, regulations, and user's requirements.

Information from the FMEA identifies priorities for process controls 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.

In deciding on the extent and the way in which FMEA should be applied to an item or design, one should 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.

To ensure that it is effective, FMEA shall be identified in the reliability programme.

2.2.3 *Uses of FMEA*

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

a) to identify failures which, when they occur alone, have unacceptable or significant effects, and to determine the failure modes which may seriously affect the expected or required operation. Such effects may include secondary failures;

b) to determine the need for:
- redundancy;
- designing features which increase the probability of "fail safe" outcomes of failures;
- further derating and/or design simplification;

c) to determine the need for selecting alternative materials, parts, devices, and components;

d) to identify serious failure consequences and hence the need for design review and revision;

e) to provide the logic model required to evaluate the probability of anomalous operating conditions of the system;

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

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

h) to establish duty cycles which anticipate and avoid wear-out failures;

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

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

k) to establish the need for data recording and monitoring during testing, check-out and use;

l) to provide information for selection of preventive or corrective maintenance points and development of trouble-shooting guides, built-in test equipment and suitable test points;

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

n) to identify circuits requiring worst case analysis (frequently required for failure modes involving parameter drifts);

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

p) to facilitate communication between:
- general and specialized engineers;
- equipment manufacturer and his suppliers;
- system user and the designer or manufacturer;

q) to enhance the analyst's knowledge and understanding of the behaviour of the equipment studied;

r) to provide a systematic and rigorous approach to the study of system facilities.

2.2.4 *Limitations and drawbacks of FMEA*

FMEA is extremely efficient when it is applied to the analysis of elements which cause a failure of the entire system.

However, FMEA may be very difficult and tedious for the case of complex systems which have multiple functions consisting of a number of components. This is because of the quantity of detailed system information which must be considered. This difficulty can be increased by the number of possible operating modes, as well as by considerations of the repair and maintenance policies.

Another limitation is that the results of human error are not usually included. Studies of man-machine interactions are the subject of specific methods (task analysis, for example). Generally, human errors appear during operation of systems in a sequential mode and the study of their impact has to be made by methods such as, for example, cause-consequence analysis. Nevertheless, the FMEA can identify components most sensitive to human factors. A further limitation is apparent when the effects of the environment are significant. The consideration of these effects requires a thorough knowledge of the characteristics and performances of the different components of the system.

It should be noted that human error and environmental effects constitute a major source of common mode or common cause failure. This question is dealt with in Sub-clause 3.6.1.

3. Basic principles of FMEA

3.1 *Terminology*

All terminology, except where specifically identified, is in accordance with IEC Publication 271: List of Basic Terms, Definitions and Related Mathematics for Reliability.

3.2 *Concepts*

FMEA requires:

- the system breakdown into "elements";
- diagrams of the system functional structure and identification of the various data which are needed to perform the FMEA;
- the failure mode concept;
- the criticality concept (if criticality analysis is required).

Finally and before the FMEA application procedure is described more explicitly, it is essential to specify the existing links between the FMEA (and the FMECA) and other qualitative (and quantitative) analytical methods.

3.3 *Definition of the system functional structure*

The analysis is initiated by selecting lowest level of interest (usually the part, circuit, or module level) at which sufficient information is available. At this 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 next higher functional level. 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.

It is important to determine the breakdown level that will be used for the analysis. For example, systems can be broken down into subsystems, least replaceable items, or detail parts (components). Where relevant, non-electrical items must be considered. When quantitative results are required, the level chosen must be one at which it is possible to obtain adequate (and dependable) failure rate data on each failure mode or error mode, or to make reasonable identified assumptions of such failure rates. The chosen breakdown level 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.

3.4 *Information necessary to perform the FMEA*

3.4.1 *System structure*

The following information is required:

- the different system elements with their characteristics, performances, roles and functions;
- the connections between elements;
- redundancy level and nature of the redundant systems;
- location of the system within the whole facility (if possible).

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

3.4.2 *System initiation, operation, control and maintenance*

The status of the different operating conditions of the system shall 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 shall be defined and such specific requirements as availability or safety shall be considered in terms of specified levels of performance and levels of damage or harm.

It is necessary to know:

- the duration of each task;

- the time interval between periodic tests;
- the time available for corrective action before serious consequences occur to the system;

- the entire facility, the environment and/or the personnel;
- repair conditions including corrective actions and the time, equipment and/or personnel to achieve them.

Further information is required on:

- operating procedures during system start-up;
- control during the operational phases;
- preventive and/or corrective maintenance;
- procedures for routine testing, if employed.

3.4.3 *System environment*

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

At the design stage usually these facts are 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.

FMEA or any other analysis requires certain modelling of the system, i.e., a simplification of the relevant information on the system. 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 be made concerning the impact of certain failures on the system.

An FMEA conducted on hardware may result in decisions on effects, criticality and conditional probabilities which involve identifying software elements and their nature, sequence and timing. When this is the case the facts must 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.

3.5 *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 must 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 failure trees or cause-consequence diagrams, contribute to a better understanding of a system, its structure and its operation. Their use, however, raises the problem of the relationship between FMEA and these methods; this question is dealt with in Sub-clause 3.8.

3.6 *Failure modes*

A failure mode is the effect by which a failure is observed in a system component.

It is important that all possible or potential failure modes of a system be listed, as the essential basis of the FMEA. Component or equipment manufacturers should take part in the identification of the failure modes of their products, in the light of the following:

- for new components, reference can be made to other components with similar functions and structures and to tests performed on them;
- for commonly used components already in service, records on their performance, reported failures and laboratory tests, can be consulted;
- complex components which can be broken down into elements can be analyzed qualitatively, treating each as a system;
- potential failure modes can be deduced from functions and physical parameters typical of the component operation.

Classification of failure modes should be performed. Two common ways of classifying failure modes are:

a) identification of general failure modes, as derived from the definition of reliability (see Table I).

b) by listing, as completely as possible, all generic failure modes (see Table II).

3.6.1 *Common-mode (common cause) failures (CMF)*

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

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

CMF's can be subjected to qualitative analytical techniques, using FMEA. As FMEA is a procedure to examine successively each failure mode and associated causes and also to identify all periodic tests, preventive maintenance measures, etc., it makes possible a study of all the causes which can induce potential CMF.

These causes can be classified into five main categories:

a) environmental effects (normal, abnormal and accidental);

b) design deficiencies;

c) manufacturing defects;

d) assembly errors;

e) human errors (during operation and/or maintenance).

A check list based on these categories may be used to identify in a detailed manner all possible causes which may induce CMF.

Redundancy alone does not solve the CMF problem. 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. Strictly, the examination of preventive measures against CMF is outside the scope of FMEA.

3.6.2 *Human factors*

Some systems have to be designed to allow for some human error, for example by providing mechanical interlocks on railway signals, 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.

3.6.3 *Software errors*

Malfunctions due to software errors or inadequacies will have effects, whose criticality 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 and is beyond the scope of the FMEA. However, the effects upon associated hardware of possible errors in software may be estimated.

3.7 *Criticality concept*

The degree of concern appropriate to any failure situation is clearly related both to its probability of occurrence and the seriousness of its effects. The criticality concept quantifies analysis and complements FMEA. There are no general criteria for criticality applicable to a system, because this concept is fundamentally linked to that of the severity of consequences and their probability of occurrence. The severity concept itself can be defined in various ways depending on whether the objective is related to safety of life, consequential damage or loss, or service availability.

The criticality concept adds greatly to the benefits of the FMEA process by considering:

- items to be given more intensive study to eliminate a particular hazard, to increase the probability of a "fail safe" outcome or reduce the failure rate or extent and risk of resultant damage;
- items requiring special attention during manufacture and stringent quality control, or special control of handling;
- special requirements in purchasing specifications concerning design, performance, reliability, safety, or quality assurance;
- acceptance standards for sub-contractors' products including parameters which should be stringently tested;
- any special procedures, safeguards, protective equipment, monitoring devices, or warning systems;
- the most cost-effective application of accident prevention resources.

In order to define criticality, a value scale is needed to judge the severity of the consequences in terms of the criteria considered. Appendix B gives an example of a classification of consequence severity into four main levels. The actual number of selected levels is fairly arbitrary. In the present example, the number of levels is based on the combination of criteria considered relevant, and concerning respectively:

- harm to personnel (injuries, death);
- loss of system function(s);

— environmental impact and material damage.

The terms "catastrophic", "critical", "major", "minor" are widely used but their definitions in IEC Publication 271 may or may not suit particular FMEA usage. Words such as these could be specifically defined in individual studies.

3.8 *Relationships between the FMEA and other methods of analysis*

It is necessary to discuss how the different analytical methods of system reliability and availability are combined within a project.

The FMEA (or FMECA) can be used alone. As a systematic inductive method of analysis, the 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 the FMEA is an essential design tool. It should, however, be supplemented by other methods particularly where multiple failures and sequential effects must be studied.

According to the project programme, one method might be developed before another. During the early design stages, where only functions, general system structure and subsystems have been defined, good performance or failure paths of the system can be depicted by a reliability block diagram or by a failure tree, respectively. 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 identified in a rigid tabular form. In general, when analyzing a complex system involving several functions, numerous components and interrelations between these components, the FMEA proves to be essential but not sufficient.

4. Procedure

The wide variation in complexity of system designs and applications may require the development of highly individualized FMEA procedures consistent with the information available. The following are the fundamental steps used in FMEA studies:

a) definition of the system and its functional and minimal operating requirements;

b) development of functional and reliability block diagrams and other diagrammatic or mathematical models and descriptions;

c) establishment of basic principles and corresponding documentation in performing the analysis;

d) identification of failure modes, their cause and effects, their relative importance, and their sequence;

e) identification of failure detection and isolation provisions and methods;

f) identification of design and operating provisions against particularly undesirable events;

g) determination of event criticality (FMECA only);

h) evaluation of failure probability (FMECA only);

i) search for specific combinations of multiple failures to be considered (optional);

j) recommendations.

The FMEA procedure may be performed with or without criticality analysis. In the latter case steps *g)* and *h)* are omitted.

4.1 *Definition on the system and its requirements*

4.1.1 *Defining the system*

A complete definition of a system includes its primary and secondary functions, its use, expected performance, system constraints and explicit conditions which constitute a failure. Since any given system is designed for one or more operational modes and may be active during various periods of system operational time, the system definition should also include functional narratives of the system's operation for each mode and its duration.

4.1.2 *Defining functional requirements*

It is necessary to define both the acceptable functional performance of the system as a whole and of its constituent elements as well as those performance characteristics considered unacceptable. The functional requirements should include a definition of acceptable performance for all desired or specified characteristics, in all operating and non-operating modes, for all relevant periods of time, and for all environmental conditions.

4.1.3 *Defining environmental requirements*

The environments in which the system is expected to function, to be exposed or stored, should be clearly defined and the performance expected in each should be specified. Environments may include such factors as temperature, humidity, radiation, vibration and pressure. For cybernetic systems consideration should also be given to further factors, psychological, physiological and environmental, in so far as they affect human performances and system design or operation.

4.1.4 *Regulatory requirements*

In defining system requirements, consideration should be given to all applicable regulatory requirements governing production, use, by-products of operation and other factors which would affect the design of the system.

4.2 *Development of 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:

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.

4.3 *Establishment of ground rules*

4.3.1 *Levels of analysis*

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 system level is selected from the design concept and specified output requirements;

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

c) the specified or intended maintenance and repair level may be a valuable guide in determining lower system levels. The lowest system level at which system maintenance will be performed should first be identified (identify the "least replaceable element"). An analysis is then made of the level immediately above the lowest system level at which maintenance will be performed. On critical system elements, the analysis is performed down to the least replaceable element.

4.3.2 *FMEA documentation*

It is helpful to perform FMEA on worksheet forms specifically designed for the system under study and which are consistent with the objectives. The forms are usually arranged in columns as shown in Appendix A. The information entered in the columns is generally:

a) the name of the system element under analysis;

b) function performed by the system element;

c) identification number of the system element;

d) failure modes;

e) failure causes;

f) failure effects;

g) failure detection methods;

h) qualitative statement of failure significance and alternative provisions;

i) remarks:

In the case of FMECA the worksheet forms can be extended to include:

j) criticality;

k) failure probability.

4.4 *Failure modes, causes and effects*

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:

— system usage;

- particular system element involved;
- mode of operation;
- pertinent operational specifications;
- time constraints;
- 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.

4.4.1 *Failure modes*

A list of general failure modes is given in Table I.

Virtually every type of failure mode can be classified into one or more of these categories. These general failure mode categories are, however, too broad in scope for definitive analysis; consequently, they are expanded as shown in Table II. The failure modes listed in Table II 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 thus identified and described.

4.4.2 *Failure causes*

The possible causes associated with each postulated failure mode are 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 must be identified and described. The failure causes within the adjacent system levels are also considered.

The list in Table II allows a more specific definition of both failure modes and failure causes. Thus for example, a power supply may have a general failure mode described as "failure during operation", the specific failure mode "loss of output" (29), and a failure cause "open (electrical)" (31).

4.4.3 *Failure effects*

The consequences of each assumed failure mode on system element operation, function, or status are 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 analyzed which is affected by the failure under consideration.

A failure effect may also influence the next higher level and ultimately the highest level under analysis. Therefore the failure effects at each higher level should be evaluated.

4.4.3.1 *Local effects*

The expression "local effects" refers to the effects of the failure mode on the system element under consideration. The consequences of each postulated failure on the output of the item are described along with the secondary effects. The purpose of defining 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.

4.4.3.2 *End effects*

When identifying end effects, the impact of a postulated 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 a 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 are indicated on the worksheets.

4.5 *Failure detection methods*

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

4.6 *Qualitative statement of failure significance and alternative provisions*

The relative significance of the failure should be recorded on the worksheet. Also recorded on the worksheet is 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 this worksheet clearly shows the true behaviour of the equipment in the presence of an internal malfunction. Other provisions include:

- redundant items that allow continued operation if one or more elements fail;
- alternative means of operation;
- monitoring or alarm devices;
- any other means permitting effective operation or limiting damage.

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

4.7 *Worksheet remarks*

If criticality analysis is not to be undertaken, then the last worksheet entry should give any pertinent remarks to clarify entries. Recommendations for design improvement are recorded and further amplified in the summary. This entry may also include:

- any unusual conditions;
- effects of redundant element failures;
- recognition of specially critical design features;
- any remarks to amplify the line entry;
- references to other entries for sequential failure analysis.

5. **Criticality analysis**

It may be desirable to quantify the criticality of a failure effect and to estimate the probability of occurrence of the relevant failure mode. The quantification of both the criticality and the probability of failure is undertaken as an aid to decision-making on the resulting corrective actions and their priorities, and to establish clear demarcation between acceptable and non-acceptable risk.

Each failure effect considered is classified by its criticality to the overall system performance in the light of system requirements, objective and constraints. A list of critical failures shall be defined for each item of equipment. There are, however, generally accepted categories and classifications which can apply to most equipment, based on the consequences listed below, which are classified qualitatively according to their severity:

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

b) damage to external equipment or the equipment itself;

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

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

The example of a criticality scale shown in Appendix B is based on injury, equipment damage and degradation of function.

The choice of criticality categories requires careful and judicious decisions. Clearly all relevant factors must be considered because of their impact on system evaluation with respect to such factors as performance, cost, schedules, safety and risk.

5.1 *Probability of a failure mode*

The probability of occurrences of each postulated failure mode is assessed in quantitative terms using analytically derived estimates. Estimates of probability of a particular failure mode in a particular operating environment require a statistically significant reliability data base.

Predictions are performed in parallel with the FMEA and using data directly from the sources cited.

5.2 *Criticality evaluation*

The evaluation of criticality may be undertaken using the criticality grid which conveniently displays the criticality categories as ordinates and the failure probabilities or frequencies as abscissae. In the example shown in Figure 1, page 37, the probabilities or frequencies are arbitrarily classified in four categories: very low, low, medium and high. In many instances the probabilities or frequencies will be classified non-linearly.

When the failure modes have been classified and assigned a probability or frequency they are identified in the appropriate square of the chart. The further this square is from the origin, along the diagonal, the greater the criticality and the more urgent the need for corrective action. For each criticality analysis, a specific range of probabilities or frequencies shall be identified for each classification.

6. **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 shall include a summary and a detailed record of the analysis.

The summary shall include a brief description of the method of analysis and the level to which it was conducted, the assumptions and the ground rules. In addition it shall include listings of:

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

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

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

TABLE I

Example of a set of general failure modes

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

TABLE II

Generic failure modes

1	Structural failure (rupture)
2	Physical binding or jamming
3	Vibration
4	Fails to remain (in position)
5	Fails to open
6	Fails to close
7	Fails open
8	Fails closed
9	Internal leakage
10	External leakage
11	Fails out of tolerance (high)
12	Fails out of tolerance (low)
13	Inadvertent operation
14	Intermittent operation
15	Erratic operation
16	Erroneous indication
17	Restricted flow
18	False actuation
19	Fails to stop
20	Fails to start
21	Fails to switch
22	Premature operation
23	Delayed operation
24	Erroneous input (increased)
25	Erroneous input (decreased)
26	Erroneous output (increased)
27	Erroneous output (decreased)
28	Loss of input
29	Loss of output
30	Shorted (electrical)
31	Open (electrical)
32	Leakage (electrical)
33	Other unique failure conditions as applicable to the system characteristics, requirements and operational constraints.

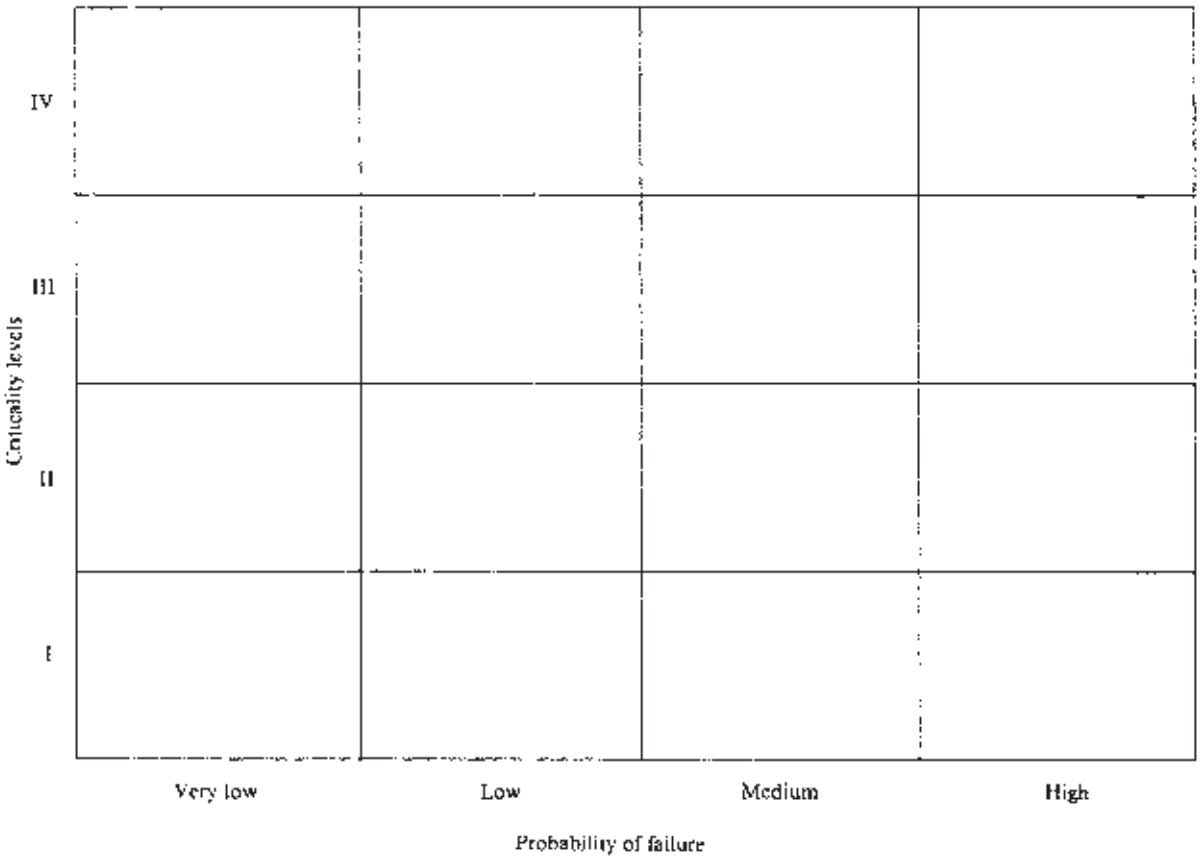

FIG. 1. — Example of criticality grid.

APPENDIX A

EXAMPLE OF A FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS WORKSHEET

Date .....

Code No. ..... Name of analyst ..... Name of design engineer .....

Equipment name	Function	Ident. No.	Failure mode	Failure cause	Failure effect		Failure detection	Alternative provisions	Failure probability	Criticality level	Remarks
					Local effect	End effect					

APPENDIX B

EXAMPLE OF FAILURE EFFECT CRITICALITY SCALE

Criticality level	Criticality conditions
IV	Any event which could potentially cause the loss of primary system function(s) resulting in significant damage to the system or its environment, and or cause the loss of life or limb.
III	Any event which could potentially cause the loss of primary system function(s) resulting in significant damage to the said system or its environment and negligible hazard to life or limb.
II	Any event which degrades system performance function(s) without appreciable damage to either system or life or limb.
I	Any event which could cause degradation of system performance function(s) resulting in negligible damage to either system or its environment; and no damage to life or limb.