INTERNATIONAL STANDARD

IEC 60812

Second edition
2006-01

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

*This **English-language** version is derived from the original **bilingual** publication by leaving out all French-language pages. Missing page numbers correspond to the French-language pages.*

Reference number
IEC 60812:2006(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/ justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

INTERNATIONAL STANDARD

IEC 60812

Second edition
2006-01

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

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60812 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition published in 1985 and constitutes a technical revision.

The main changes from the previous edition are as follows:

– introduction of the failure modes effects and criticality concepts;
– inclusion of the methods used widely in the automotive industry;
– added references and relationships to other failure modes analysis methods;
– added examples;
– provided guidance of advantages and disadvantages of different FMEA methods.

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

FDIS	Report on voting
56/1072/FDIS	56/1091/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

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

1 Scope

This International 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 by

– providing the procedural steps necessary to perform an analysis;
– identifying appropriate terms, assumptions, criticality measures, failure modes;
– defining basic principles;
– providing examples of the necessary worksheets or other tabular forms.

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60300-3-1:2003, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram method*

3 Terms and definitions

For the purposes of this document, the following definitions apply.

3.1
item
any part, component, device, subsystem, functional unit, equipment or system that can be individually considered

NOTE 1 An item may consist of hardware, software or both, and may also in particular cases include people.

NOTE 2 A number of items, e.g. a population of items or a sample, may itself be considered as an item.

[IEV 191-01-01]

A process can also be defined as an item which carries out a predetermined function and for which a process FMEA or FMECA is carried out. Normally, a hardware FMEA does not address people and their interactions with hardware/software, while a process FMEA normally includes actions of people.

3.2
failure
termination of the ability of an item to perform a required function

[IEV 191-04-01]

3.3
fault
state of an item characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

NOTE 1 A fault is often the result of a failure of the item itself, but may exist without prior failure.

[IEV 191-05-01]

NOTE 2 In this document "fault" is used interchangeably with the term "failure" for historical reasons.

3.4
failure effect
consequence of a failure mode in terms of the operation, function or status of the item

3.5
failure mode
manner in which an item fails

3.6
failure criticality
combination of the severity of an effect and the frequency of its occurrence or other attributes of a failure as a measure of the need for addressing and mitigation

3.7
system
set of interrelated or interacting elements

NOTE 1 In the context of dependability, a system will have

a) defined purposes expressed in terms of required functions;

b) stated conditions of operation use (see 191-01-12);

c) a defined boundary.

NOTE 2 The structure of a system is hierarchical.

[ISO 9000:2000]

3.8
failure severity
significance or grading of the failure mode's effect on item operation, on the item surrounding, or on the item operator; failure mode effect severity as related to the defined boundaries of the analysed system

4 Overview

4.1 Introduction

Failure Modes and Effect Analysis (FMEA) is a systematic procedure for the analysis of a system to identify the potential failure modes, their causes and effects on system performance (performance of the immediate assembly and the entire system or a process). Here, the term system is used as a representation of hardware, software (with their interaction) or a process. The analysis is successfully performed preferably early in the development cycle so that removal or mitigation of the failure mode is most cost effective. This analysis can be initiated as soon as the system is defined enough to be presented as a functional block diagram where performance of its elements can be defined.

FMEA timing is essential; if done early enough in the development cycle, then incorporating the design changes to overcome deficiencies identified by the FMEA may be cost effective. It is therefore important that the FMEA task and its deliverables be incorporated into the development plan and schedule. Thus, FMEA is an iterative process that takes place coincidentally with design process.

FMEA is applicable at various levels of system decomposition from the highest level of block diagram down to the functions of discrete components or software commands. The FMEA is also an iterative process that is updated as the design develops. Design changes will require that relevant parts of the FMEA be reviewed and updated.

A thorough FMEA is a result of a team composed of individuals qualified to recognize and assess the magnitude and consequences of various types of potential inadequacies in the product design that might lead to failures. Advantage of the team work is that it stimulates thought process, and ensures necessary expertise.

FMEA is considered to be a method to identify the severity of potential failure modes and to provide an input to mitigating measures to reduce risk. In some applications however, FMEA also includes an estimation of the probability of occurrence of the failure modes. This enhances the analysis by providing a measure of the failure mode's likelihood.

Application of FMEA is preceded by a hierarchical decomposition of the system (hardware with software, or a process) into its more basic elements. It is useful to employ simple block diagrams to illustrate this decomposition (IEC 61078). The analysis then starts with lowest level elements. A failure mode effect at a lower level may then become a failure cause of a failure mode of an item in the next higher level. The analysis proceeds in a bottom-up fashion until the end effect on the system is identified. Figure 1 illustrates this relationship.

FMECA (Failure Modes, Effects and Criticality Analysis) is an extension to the FMEA to include a means of ranking the severity of the failure modes to allow prioritization of countermeasures. This is done by combining the severity measure and frequency of occurrence to produce a metric called criticality.

The principles of an FMEA may be applied outside of engineering design. FMEA procedure can be applied to a manufacturing or any other work process such as in hospitals, medical laboratories, school systems, or others. When FMEA is applied to a manufacturing process,

this procedure is known in industry as the Process FMEA, or PFMEA. For an FMEA to be effective, adequate resources for a team work have to be committed. A thorough understanding of the system under analysis may not be essential for a preliminary FMEA. With development of design, a detailed failure mode analysis requires thorough knowledge of the design performance and its specifications. Complex engineering designs usually require the involvement of multiple areas of design expertise (e.g. mechanical engineering, electrical engineering, systems engineering, software engineering, maintenance support, etc).

FMEA generally deals with individual failure modes and the effect of these failure modes on the system. Each failure mode is treated as independent. The procedure is therefore unsuitable for consideration of dependent failures or failures resulting from a sequence of events. To analyse these situations other methods and techniques, such as Markov analysis (see IEC 61165) or fault tree analysis (see IEC 61025), may be required.

In determining the impact of a failure, one must consider higher level induced – resultant failures and possibly the same level of induced failures. The analysis should indicate, wherever possible the combination of failure modes or their sequence that was a cause of a higher level effect. In that case additional modelling is required to estimate the magnitude or probability of occurrence of such an effect.

FMEA is a flexible tool that can be tailored to meet specific industry or product needs. Specialized worksheets requiring specific entries may be adapted for certain applications. If severity levels of failure modes are defined, they may be defined differently for different systems or different system levels.

4.2 Purpose and objectives of the analysis

The reasons for undertaking Failure Mode Effects Analysis (FMEA) or Failure Mode Effects and Criticality Analysis (FMECA) may include the following:

a) to identify those failures which have unwanted effects on system operation, e.g. preclude or significantly degrade operation or affect the safety of the user;

b) to satisfy contractual requirements of a customer, as applicable;

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

d) to allow improvement of the system's maintainability (by highlighting areas of risk or nonconformity for maintainability).

In view of the above reasons for undertaking a FMEA effort, the objectives of an FMEA (or FMECA) may include the following:

a) 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;

b) the determination of the criticality or priority for addressing/mitigation (see Clause 6) of each failure mode with respect to the system's correct function or performance and the impact on the process concerned;

c) a classification of identified failure modes according to relevant characteristics, including their ease of detection, capability to be diagnosed, testability, compensating and operating provisions (repair, maintenance, logistics, etc.);

d) identification of system functional failures and estimation of measures of the severity and probability of failure;

e) development of design improvement plan for mitigation of failure modes;

f) support the development of an effective maintenance plan to mitigate or reduce likelihood of failure (see IEC 60300-3-11).

NOTE When criticality or probability of occurrence is addressed, the comments regard FMECA methodology.

5 Failure modes and effects analysis

5.1 General considerations

Traditionally there have been wide variations in the manner in which FMEA is conducted and presented. The analysis is usually done by identifying the failure modes, their respective causes and immediate and final effects. The analytical results can be presented on a worksheet that contains a core of essential information for entire system and details developed for that specific system. It shows the ways the system could potentially fail, the components and their failure modes that would be the cause of system failure, and the cause(s) of occurrence of each individual failure mode.

The FMEA effort applied to the complex products might be very extensive. This effort may be sometimes reduced by having in mind that design of some subassemblies or their parts may not be entirely new and by identifying parts of the product design that are a repetition or a modification of a previous product design. The newly constructed FMEA should use information on those existing subassemblies to the highest possible extent. It must also point to the need for eventual test or full analysis of the new features and items. Once a detailed FMEA is created for one design, it can be updated and improved for the succeeding generations of that design, which constitutes a significantly less effort than the entirely new analysis.

When using an existing FMEA from a previous product version, it is essential to make sure that the repeated design is indeed used in the same manner and under the same stresses as the previous design. The new operational or environmental stresses may require review of the previously completed FMEA. Different environmental and operational stresses may require an entirely new FMEA to be created in view of the new operational conditions.

The FMEA procedure consists of the following four main stages:

a) establishment of the basic ground rules for the FMEA and planning and scheduling to ensure that the time and expertise is available to do the analysis;

b) executing the FMEA using the appropriate worksheet or other means such as a logic diagrams or fault trees;

c) summarizing and reporting of the analysis to include any conclusions and recommendations made;

d) updating the FMEA as the development activity progresses.

5.2 Preliminary tasks

5.2.1 Planning for the analysis

FMEA activities, follow up activities, procedures, relationship with other reliability activities, processes for management of corrective actions and for their closure, and milestones, should be integrated into the overall program plan.

The reliability program plan should describe the FMEA analysis method to be used. This description may be a summary description or a reference to a source document containing the method description.

This plan should contain the following points.

– clear definition of the specific purposes of the analysis and expected results;

– the scope of the present analysis in terms of how the FMEA should focus on certain design elements. The scope should reflect the design maturity, elements of the design that may be considered to be a risk because they perform a critical function or because of immaturity of the technology used;

– description of how the present analysis supports the overall project dependability;

– identified measures used for control of the FMEA revisions and the relevant documentation. Revision control of the analysis documents and worksheets and archive methods should be specified;

– participation of design experts in the analysis so that they are available when needed;

– key project schedule milestones clearly marked to ensure the analysis is executed in a timely manner;

– manner of closure of all actions identified in the process of mitigation of identified failure modes that need to be addressed.

The plan should reflect the consensus of all participants and should be approved by project management. Final review of the completed FMEA in the final stage of the design of a product or its manufacturing process (process FMEA) identifies all of the recorded actions for mitigation of failure modes of concern and the manner of their closure.

5.2.2 System structure

5.2.2.1 Information on system structure

The following items need to be included into the information on system structure:

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

b) 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) inputs and outputs of the system;

f) changes in system structure for varying operational modes.

Information pertaining to functions, characteristics and performances are required for all system levels considered up to the highest level so that FMEA could properly address failure modes that preclude any of those functions.

5.2.2.2 Defining system boundary for the analysis

The system boundary forms the physical and functional interface between the system and its environment, including other systems with which the analysed system interacts. The definition of the system boundary for the analysis should correspond to the boundary as defined for design and maintenance. This should apply to a system at any level. Systems and/or components outside the boundaries should explicitly be defined for exclusion.

The definition of the system boundary is more likely to be influenced by design, intended use, 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 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 and software point of view 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.

5.2.2.3 Levels of analysis

It is important to determine the indenture level in the system that will be used for the analysis. For example, systems can be broken down by function or into subsystems, replaceable units, or individual components (see Figure 1). Ground rules for selecting the system indenture 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 selection of 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 details and a correspondingly lower system level are 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.

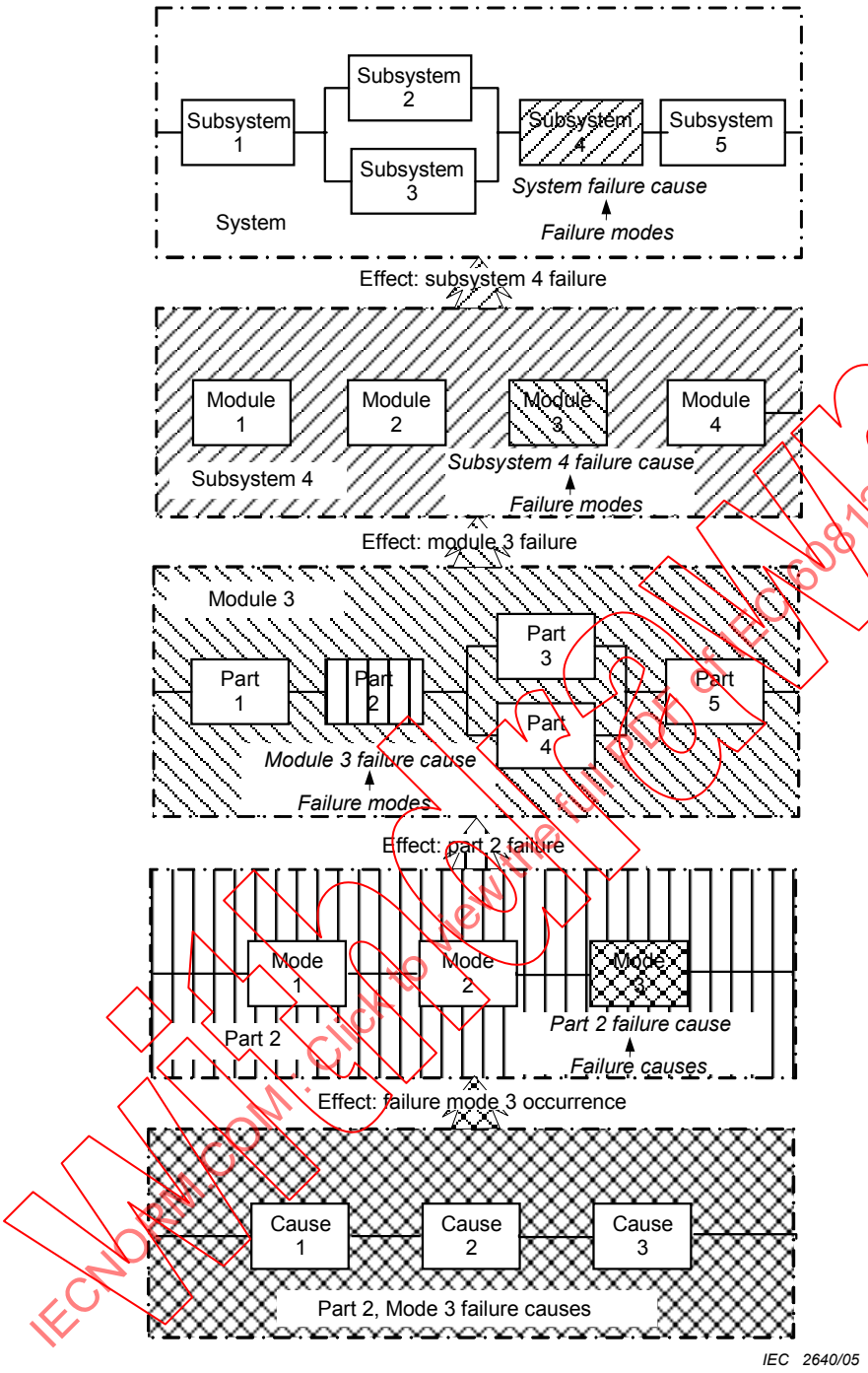

Figure 1 – Relationship between failure modes and failure effects in a system hierarchy

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

When a system is broken down into its elements, effects of one or more of the failure mode causes make a failure mode, which in turn is a cause of the higher level effect, a part failure. Part failure is then the cause of a module failure (effect), which in itself is a cause of a subsystem failure. The effect of a cause of one system level thus becomes a cause of another effect at a higher level. The above rationale is shown in Figure 1.

5.2.2.4 Representation of system structure

Symbolic representations of the system structure and operation, especially diagrams, are very useful to aid the analysis.

Simple diagrams should be created, highlighting all the functions essential to the system. In the diagram, the blocks are linked together by lines that represent the inputs and outputs for each function. Usually, the nature of each function and each input needs to be precisely described. There may be several diagrams to cover different phases of system operation.

As the system design progresses, a component block diagram can be created with blocks representing actual components or parts. With this additional knowledge more precise identification of potential failure modes and causes becomes possible.

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 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 protection against system failures.

5.2.2.5 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 function the system may be called upon to perform;

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

f) control during the operational phases;

g) preventive and/or corrective maintenance;

h) procedures for routine testing, if employed.

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 preventive and corrective maintenance.

5.2.2.6 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.

5.2.3 Failure mode determination

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 those 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 environmental stresses;

g) the operational stresses.

An example list of general failure modes is given in Table 1.

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 listing is an example only. Different lists would be required for different types of systems.

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. 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.

It is important that evaluation of all items within the system boundaries at the lowest level commensurately with the objectives of the analysis 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 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:

a) 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;

b) for new items, the design intent and detailed functional analysis yields the potential failure modes and their causes. This method is preferred to the one in a), because the stresses and the operation itself might be different from the similar items. An example of this situation may be the use of a signal processor different than the one used in the similar design;

c) for items in use, in-service records and failure data may be consulted;

d) 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, to mitigate the failure modes effects by design measures, than to know their probability of occurrence. When it is difficult to assign priorities, criticality analysis may be required.

5.2.4 Failure causes

The most likely causes for each potential failure mode should be identified and described. Since a failure mode can have more than one cause, the most likely potential independent causes for each failure mode need to be identified and described.

The identification and description of failure causes is not always necessary for all failure modes identified in the analysis. Identification and description of failure causes, as well as suggestions for their mitigation should be done on the basis of the failure effects and their severity. The more severe the effects of failure modes, the more accurately failure causes should be identified and described. Otherwise, the analyst may dedicate unnecessary effort on the identification of failure causes of such failure modes that have no or a very minor effect on system functionality.

Failure causes may be determined from analysis of field failures or failures in test units. When the design is new and without precedent, failure causes may be established by eliciting the opinion of experts.

When the causes of each failure mode are identified the recommended action will be evaluated based on their estimated probability of occurrence and the severity of their effect.

5.2.5 Failure effects

5.2.5.1 Failure effects definition

A failure effect is the consequence of a failure mode in terms of the operation, function or status of a system (see definition 3.4). 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 activities and system objectives should also be considered whenever pertinent. 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.

5.2.5.2 Local failure 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. 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.

5.2.5.3 Failure effects at the system level

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 failures. (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.

5.2.6 Detection methods

For each failure mode, the analyst should determine the way in which the failure is detected and the means by which the user or maintainer is made aware of the failure. Failure detection may be implemented by an automatic feature of the design (built-in-test), establishment of a special checkout procedure before system operation or by inspection during maintenance activities. It may be implemented at start up of the system or continuously during operation or at prescribed intervals. In either case failure detection and its annunciation should preclude a hazardous operating condition.

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.

For a design FMEA detection considers how likely, when, and where a design deficiency will be identified (by review, by analysis, by simulation, by test, etc.). For a process FMEA detection considers how likely and where in the process a deficiency can be identified and with which probability e.g. by operator, by statistical process control, by quality check procedure or by later steps in the process.

5.2.7 Failure compensating provisions

The identification of any design features at a given system level or other provisions that have the ability to prevent or reduce the effect of the failure mode is of an extreme importance. Thus the FMEA should clearly show the true behaviour of such a feature in the presence of that failure mode. Other provisions against failure that need to be recorded in the FMEA 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 a design process, the functional elements (hardware and software) of an item may be repeatedly rearranged or reconfigured or its capability may be changed. At each stage, the relevancy of the identified failure modes and the FMEA should be updated or even repeated.

5.2.8 Severity classification

Severity is an assessment of the significance of the failure mode's effect on item operation. The classification of the severity effects is highly dependent on the FMEA application and is developed in consideration of several factors:

– the nature of the system in relation to possible effects on users or the environment resulting from failure;

– the functional performance of the system or process;

– any contractual requirements imposed by the customer;

– government or industry safety requirements;

– requirements implied by a warranty.

Table 2 illustrates an example of a set of qualitative severity classification for a product for one of the FMEA types.

Table 2 – Illustrative example of a severity classification for end effects

Class	Severity level	Consequence to persons or environment
IV	Catastrophic	A failure mode which could potentially result in the failure of the system's primary functions and therefore causes serious damage to the system and its environment and/or personal injury.
III	Critical	A failure mode which could potentially result in the failure of the system's primary functions and therefore causes considerable damage to the system and its environment, but which does not constitute a serious threat to life or injury.
II	Marginal	A failure mode, which could potentially degrade system performance function(s) without appreciable damage to system or threat to life or injury.
I	Insignificant	A failure mode which could potentially degrade the system's functions but will cause no damage to the system and does not constitute a threat to life or injury.

5.2.9 Frequency or probability of occurrence

The frequency or probability of occurrence of each failure mode should be determined in order to adequately assess the effect or criticality of the failure mode.

For determination of the probability of occurrence of the failure mode, besides published information regarding the failure rate, it is very important to consider the operational profile (environmental, mechanical, and/or electrical stresses applied) of each component that contribute to its probability of occurrence. This is because the component failure rates, and consequently failure rate of the failure mode under consideration, in most cases increase proportionally with the increase of applied stresses with the power law relationship or exponentially. Probability of occurrence of the failure modes for the design can be estimated from

– data from the component life testing,
– available databases of failure rates,
– field failure data,
– failure data for similar items or for the component class.

When probability of occurrence is estimated, the FMEA must address the time period for which the estimations are made. It usually is the warranty period or the predetermined life period of that item or product.

The application of frequency and probability of occurrence will be further explained in the description of the criticality analysis.

5.2.10 Analysis procedure

The flow chart given in Figure 2 shows how the analysis proceeds.

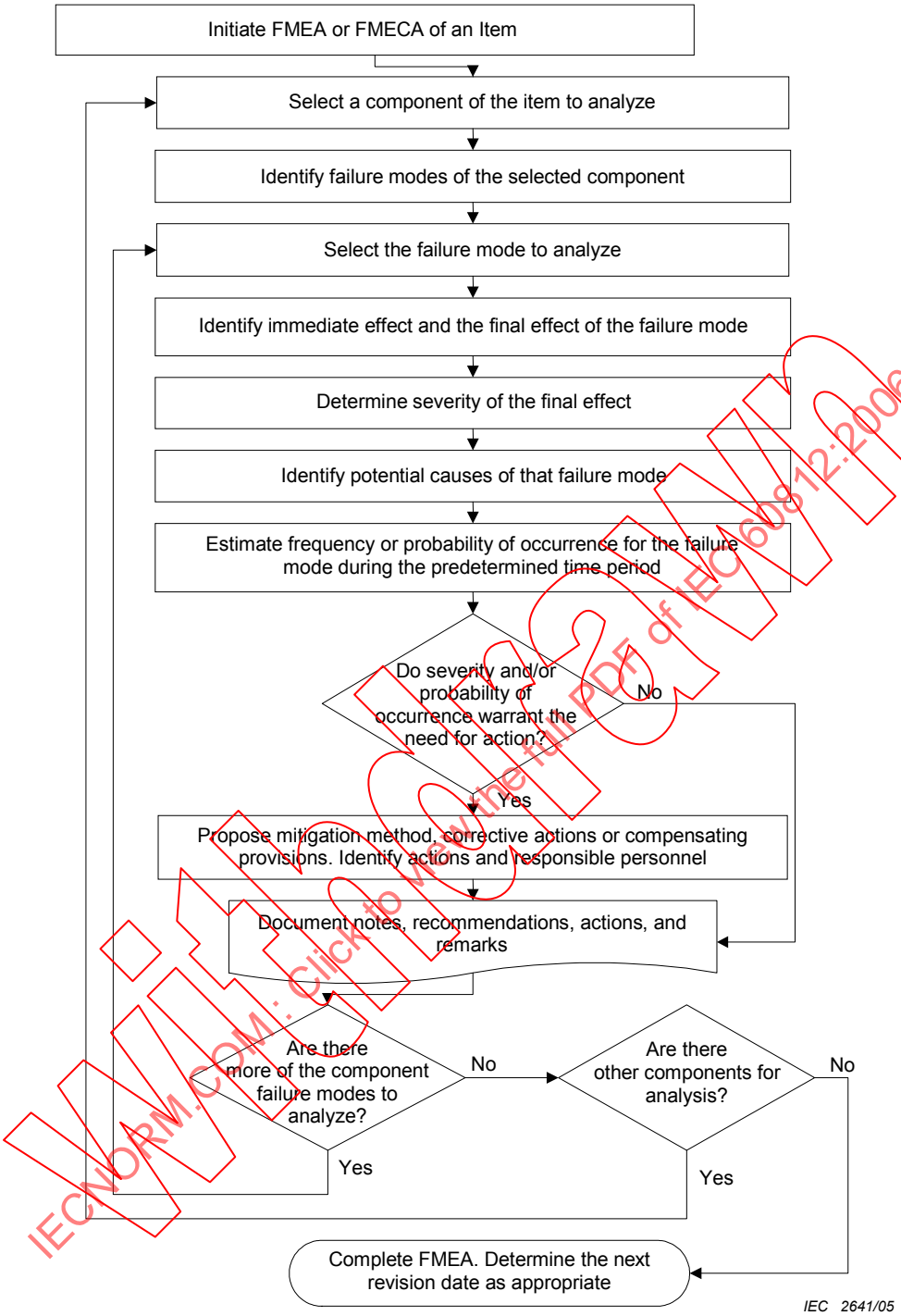

Figure 2 – Analysis flowchart

5.3 Failure mode, effects, and criticality analysis (FMECA)

5.3.1 Purpose of analysis

Symbol C added to FMEA denotes that the failure mode analysis yields also the criticality analysis. Criticality determination implies addition of a qualitative measure of magnitude of a failure mode effect. Criticality has a multitude of definitions and measures, most of which assume a similar meaning: impact or importance of a failure mode that would demand it to be addressed and mitigated. Some of those measures are explained in 5.3.2 and 5.3.4. The purpose of a criticality analysis is to quantify the relative magnitude of each failure effect as an aid to decision making, so that with a combination of criticality and severity, priority for action to mitigate or minimize effect of certain failures may be set.

5.3.2 Risk, R, and risk priority number (RPN)

One of the methods of quantitative determination of criticality is the Risk Priority Number, RPN. Risk is here evaluated by a subjective measure of the severity of the effect and an estimate of the expected probability of its occurrence for a predetermined time period assumed for analysis. In some cases where these measures are not available, it may become necessary to refer to a simpler form of a non-numeric FMEA.

A general relation regarding a measure of a potential risk, R, in a FMECA is in some analysis types expressed as follows:

$$R = S \times P$$

where

S is a non-dimensional number that stands for severity, i.e. an estimate of how strongly the effects of the failure will affect the system or the user.

P is also a non-dimensional number that denotes probability of occurrence. When it is less than 0,2 it can be substituted by criticality number that is used in some quantitative FMEA methods, C, explained in 5.3.4, i.e. an estimate of the likelihood that the failure effect will occur.

Some FMEA or FMECA applications distinguish additionally the level of failure detection at system level. In these applications an additional category for failure detection, D (also a non-dimensional number), is employed to form a risk priority number, RPN:

$$RPN = S \times O \times D$$

where

O denotes probability of occurrence of a failure mode for a predetermined or stated time period – even though it may be defined as a ranking number rather than the actual probability of occurrence;

D means detection, i.e. an estimate of the chance to identify and eliminate the failure before the system or customer is affected. This number is usually ranked in reverse order from the severity or occurrence numbers: the higher the detection number, the less probable the detection is. The lower probability of detection consequently leads to a higher RPN, and a higher priority for resolution of the failure mode.

Risk priority number may then be used for prioritization in addressing the mitigation of failure modes. In addition to the magnitude of the risk priority number, the decision for mitigation is primarily influenced by the severity of the failure mode, meaning that if there are failure modes with similar or identical RPN, the failure modes that are to be addressed first are those with the high severity numbers.

These relations can be evaluated numerically either on a continuous or discrete scale (a finite number of defined values).

The failure modes are then ordered with respect to their RPN and high priority is assigned to high RPN. In some applications effects with a RPN exceeding a defined threshold are not acceptable, while in other applications, the high importance is given to the high severity numbers, regardless of the RPN value.

Different types of FMECA assign different scales for the values of S, O, and D. Some are 1 through 4 or 5, some, such as the FMECA used widely in the automotive industry for analysis of design and production process, known as DFMEA and PFMEA, use scales for all of the three attributes from 1 through 10.

5.3.3 Relationship between FMECA and risk analysis

Criticality combined with severity is a measure of risk, which differs from the usually accepted measures of risk only in the less rigorous, and hence often less costly, approach to its evaluation. The difference shows not only in the manner of prediction of the severity of a failure effect but also that far less complex interaction between the contributing factors can be modelled in the typical bottom-up procedure applied in a FMECA. Also FMECA usually results in a relative ranking of the contributions to the overall risk, while a risk analysis for high-risk systems generally aims at risk acceptability. However for low-risk and low-complexity systems FMECA may be a very cost-effective and appropriate method. Whenever during the FMECA the likelihood of high-risk effects is recognized it is advised that a probabilistic risk analysis (PRA) should be used in preference to a FMECA.

A FMECA should therefore not be used as the single basis for judging whether or not the risk of a particular effect of a high-risk or high-complexity system is acceptably small, even if the estimate of frequency and severity is based on trustworthy data. This would be the task of a probabilistic risk analysis, where also more influential parameters (and their interactions) can be taken into account, e.g. exposure time, probability of avoidance, latency of failures, fault detection mechanisms.

Using the failure effects identified by the FMEA each effect is allocated to an appropriate severity class. A frequency for the event is calculated from failure data or estimates for the part concerned. Multiplied with the mission time of concern, the frequency yields a criticality number, which can then be applied to a scale either in accordance with its own value, or, if the scale represents probability of event occurrence, then this probability of occurrence is measured per the scale. The severity class and criticality (or probability of occurrence) class for each effect together constitute the magnitude of the effect. Two major criticality assessment approaches can be distinguished: the criticality matrix approach and the risk priority numbers (RPN) concept.

5.3.4 Failure mode failure rate, probability, and criticality number determination

If failure rates for the failure modes of like items are available, and those were determined under environmental and operational conditions similar to those assumed for the system being analysed, the event frequencies for the effects can be added directly to the FMECA. 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 failure rates of the failure modes need to be calculated. In general the following relation holds:

$$\lambda_i = \lambda_j \times \alpha_i \times \beta_i$$

where

λ_i denotes the estimate of failure rate for failure mode i assumed constant.

λ_j stands for the failure rate of the component j.

α_i is the failure mode ratio of failure mode i, i.e. the probability that the item will have failure mode i.

β_i is the conditional probability of the failure effect given the failure mode i.

The major deficiencies of this approach are the implicit assumption of constant failure rate and that many of the factors are predictions or best guesses only. This is especially the case when the system components cannot have an associated failure rate, just the calculated failure probability for the specific application, its duration, and associated stresses, such as mechanical components and systems.

Environmental, loading and maintenance conditions different from those relating to the failure rate data are accounted for by a modifying factor. Guidance on appropriate values for this modification may be found in publications dealing with reliability data. A special care needs to be exercised to ensure that the chosen modifiers are correct and applicable for the specific system and its operating conditions.

In some applications, such as quantitative approach to criticality analysis, a failure mode criticality number C_i (unrelated to the general term "criticality" that can assume different meanings) is used instead of a failure mode failure rate λ_i. The criticality number makes a connection between the conditional failure frequency and the time of operation, which then may help get a more realistic assessment of a failure mode risk during the predetermined period of the product use.

$$C_i = \lambda_i \times t_j$$

$$C_i = \lambda_j \times \alpha_i \times \beta_i \times t_j$$

where t_j denotes the time of component operation during the entire predetermined time used for FMECA, for which the probability is evaluated – time of active component operation.

Criticality number for the component having m failure modes is then

$$C_j = \sum_{i=1}^{m} \lambda_j \times \alpha_i \times \beta_i \times t_j$$

It is to be noted that the criticality number is not related to the term criticality itself. It is just a value calculated for some FMECA types in context that it is a relative measure of the consequence of a failure mode and its probability of occurrence. Here, criticality number is a measure of risk, and not the measure of probability of occurrence.

To determine P_i, the failure mode probability of occurrence for a time t_j, from the calculated criticality:

$$P_i = 1 - e^{-C_i}$$

With a rough approximation, when the failure rates of failure modes and the resultant criticality numbers are small, it can be said that for probabilities of occurrence less than 0,2 (where criticality would be equal to 0,223), values of criticality number and probability of failure are very similar.

In case of variable failure rates or failure frequencies, probability of occurrence is to be calculated rather than the criticality which is based on the assumption of a constant failure rate (frequency).

5.3.4.1 Criticality matrix

Criticality can be presented on a criticality matrix, as shown in Figure 3. It should be noted that there is no universal definition of criticality but that criticality needs to be defined by the analyst and accepted by the project or programme management. The definitions differ widely between different application sectors.

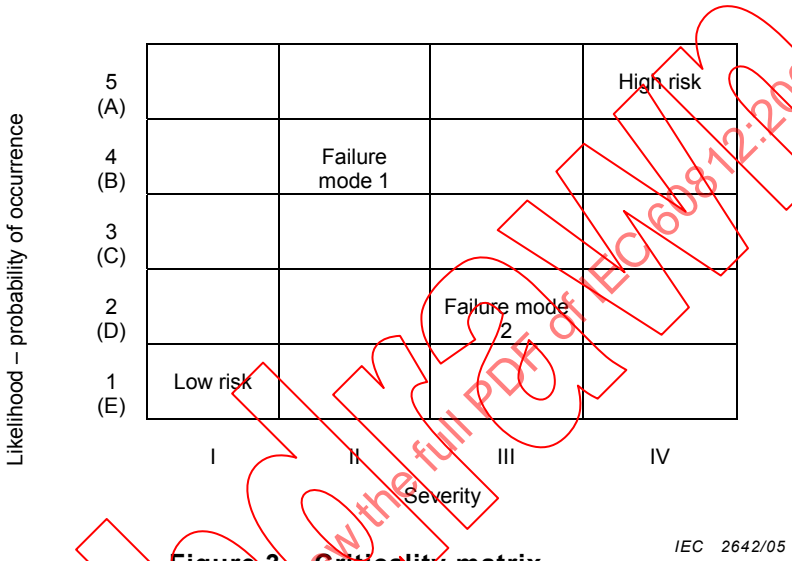

Figure 3 – Criticality matrix

In Figure 3 it is implied that the severity increases with the ascending order of numbers, where number IV has the highest severity (loss of human life and/or mission/operation, injury). It is also implied that likelihood of occurrence, on the Y-axis is also represented in ascending order. If the highest probability of occurrence category does not exceed a value 0,2, probability of occurrence and criticality values are approximately equal to each other. One of the matrices that is often seen has the following scale:

– Criticality number 1 or E, Improbable, probability of occurrence: $0 \leq P_i < 0{,}001$
– Criticality number 2 or D, Remote, probability of occurrence: $0{,}001 \leq P_i < 0{,}01$
– Criticality number 3 or C, Occasional, probability of occurrence: $0{,}01 \leq P_i < 0{,}1$
– Criticality number 4 or B, Probable, probability of occurrence: $0{,}1 \leq P_i < 0{,}2$
– Criticality number 5 or A, Frequent, probability of occurrence: $P_i \geq 0{,}2$

Figure 3 is presented as an example only. Other methods may present criticality or severity with different labels and with different definitions.

In the example given by Figure 3, failure mode 1 has a higher likelihood of occurrence than failure mode 2, which in turn has a higher severity. The decision which failure mode has higher priority to be addressed depends on the scaling of the severity and frequency classes and the ranking principles. While in a linear scaling failure mode 1 (as usually suggested by the matrix) would have a higher criticality (or probability of occurrence) than failure mode 2,

there may be applications where severity has absolute priority over frequency thus making failure mode 2 the more critical failure mode. Another evident observation is that only failure modes related to the same system indenture level may be meaningfully compared with the criticality matrix because for low-complexity systems failure modes on a lower level usually tend to have a lower frequency.

The criticality matrix (as shown in Figure 3) can be applied qualitatively and quantitatively as explained above.

5.3.5 Risk acceptability assessment

When the required end product of the analysis is a criticality matrix, this can be plotted from the allocated severities and the event frequencies. Risk acceptability is defined subjectively or is driven by professional and financial decisions and varies in different industry types. Table 3 gives some examples of risk acceptability classes and a modified criticality matrix.

Table 3 – Risk/criticality matrix

Frequency of occurrence of failure effect	Severity levels			
	1 Insignificant	2 Marginal	3 Critical	4 Catastrophic
5: Frequent	Undesirable	Intolerable	Intolerable	Intolerable
4: Probable	Tolerable	Undesirable	Intolerable	Intolerable
3: Occasional	Tolerable	Undesirable	Undesirable	Intolerable
2: Remote	Negligible	Tolerable	Undesirable	Undesirable
1: Improbable	Negligible	Negligible	Tolerable	Tolerable

5.3.6 FMECA types with the ranking scales

FMECA types described in 5.3.2 are very commonly used in the automobile industry for analysis of product design as well as for the analysis of the production process for that product.

The analysis methodology is the same as described in general form FMEA/FMECA except the definitions are predetermined in three tables prepared for Severity, *S*, Occurrence, *O*, and for the Detection, *D*.

5.3.6.1 Alternate severity determination

Table 4 gives an example of severity ratings that are primarily used in the automotive industry.

Table 4 – Failure mode severity

Severity	Criteria	Ranking
None	No discernible effect.	1
Very minor	Fit and finish/squeak and rattle item does not conform. Defect noticed by discriminating customers (less than 25 %).	2
Minor	Fit and finish/squeak and rattle item does not conform. Defect noticed by 50 % of customers.	3
Very low	Fit and finish/squeak and rattle item does not conform. Defect noticed by most customers (greater than 75 %).	4
Low	Vehicle/item operable but comfort/convenience item(s) operable at a reduced level of performance. Customer somewhat dissatisfied.	5
Moderate	Vehicle/item operable but comfort/convenience item(s) inoperable. Customer dissatisfied.	6
High	Vehicle/item operable but at a reduced level of performance. Customer very dissatisfied.	7
Very high	Vehicle/item inoperable (loss of primary function)	8
Hazardous with warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves non-compliance with government regulation with warning.	9
Hazardous without warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves non-compliance with government regulation without warning.	10

NOTE From SAE J1739.

A severity rank is allocated to the failure effect from each failure mode based on the severity of the effect on the overall system performance and safety in the light of the system requirements, objectives and constraints, in view of the vehicle as a system. This is most readily done on the FMECA sheet. The determination of severity according to Table 4 is very straightforward for severity numbers 6 and up. Determination of severity from 3 through 5 may be subjective.

5.3.6.2 Alternate determination of occurrence

Table 5 (also borrowed from the automotive industry) gives examples of qualitative occurrence measures, which may be used in the RPN concept.

Table 5 – Failure mode occurrence related to frequency and probability of occurrence

Failure mode occurrence	Rating, O	Frequency	Probability
Remote: Failure is unlikely	1	≤ 0,010 per thousand vehicles/items	$\leq 1x10^{-5}$
Low: Relatively few failures	2	0,1 per thousand vehicles/items	$1x10^{-4}$
	3	0,5 per thousand vehicles/items	$5x10^{-4}$
Moderate: Occasional failures	4	1 per thousand vehicles/items	$1x10^{-3}$
	5	2 per thousand vehicles/items	$2x10^{-3}$
	6	5 per thousand vehicles/items	$5x10^{-3}$
High: Repeated failures	7	10 per thousand vehicles/items	$1x10^{-2}$
	8	20 per thousand vehicles/items	$2x10^{-2}$
Very high: Failure is almost inevitable	9	50 per thousand vehicles/items	$5x10^{-2}$
	10	≥100 in thousand vehicles/items	$\geq 1x10^{-1}$

NOTE Source: AIAG: Potential Failure Mode and Effects Analysis, FMEA, Third Edition.

It should be noted that in Table 5 the term “frequency” is used as a ratio of occurrence in number of opportunities during a mission or designated lifetime, which can be compared to a “fraction failed” or probability of occurrence, and the corresponding probabilities merely reflect this fraction. For example, a failure mode which is rated with an O value of 9 would cause failure of one of three systems during a predetermined mission period. Here, determination of this probability of occurrence must be related to the time period of interest. It is advisable to state this time period in the heading of the analysis.

The best practice is applied when the probability of occurrence is calculated for the components and their failure modes based on their own specific failure rates under the applied expected stresses (environmental and operational). When that information is not available, an estimate may be assigned, but, while doing so, the analysis team must keep in mind the meaning of the occurrence numbers – the number of occurrences per a thousand vehicles in the predetermined time used for the analysis (warranty, vehicle life, or other); it is the calculated or estimated probability of occurrence of that failure mode in a time period of interest. It is also to be noted that, unlike the severity scale, occurrence scale is not linear and also is not logarithmic. Therefore, it should be kept in mind that the resultant RPN number when calculated and evaluated is also not linear and must be addressed with a special care.

5.3.6.3 Rating of failure detection probability

In the RPN concept, the likelihood that a failure will be detected has to be estimated; that is, the probability that the design features/aids or verification procedures will detect potential failure modes in time to prevent a system-level failure. For a process application (process FMEA, or PFMEA), this refers to the probability that a set of process controls currently in place will be in a position to detect and isolate a failure before it gets transferred to the subsequent processes or to the ultimate product output.

In particular for generic products, which may be used in several different systems and applications, the probability of detection may be difficult to estimate.

Table 6 gives one of the methods of detection criteria, as used in the automotive industry.

Table 6 – Failure mode detection evaluation criteria

Detection	Criteria: Likelihood of detection by Design Control	Ranking
Almost certain	Design Control will almost certainly detect a potential cause/mechanism and subsequent failure mode	1
Very high	Very high chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	2
High	High chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	3
Moderately high	Moderately high chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	4
Moderate	Moderate chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	5
Low	Low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	6
Very low	Very low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	7
Remote	Remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	8
Very remote	Very remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	9
Absolutely uncertain	Design Control will not and/or cannot detect a potential cause/mechanism and subsequent failure mode; or there is no Design Control	10

NOTE Source: AIAG: Potential Failure Mode and Effects Analysis, FMEA, Third Edition.

5.3.6.4 Risk evaluation

This very intuitive approach described above shall be followed by a ranking of priority of actions to be performed to assure the best level of safety to the customer. For example, a failure mode with high severity, low rate of occurrence and very high detection (say 10, 3 and 2 respectively) may have a much lower RPN (here 60) than one which has all average parameters (say 5 in each case resulting in a RPN of 125). Thus additional procedures are often defined, to ensure that failure modes with high severity ranking (say 9 or 10) are given priority and are mitigated first. In that case, the decision should be guided by the magnitude of severity, rather than RPN alone. In all cases, a good practice is to view severity rank of a failure mode along with the RPN for a better decision-making process.

Risk priority numbers are also determined in other FMEA methods, especially those that are primarily qualitative.

With the above tables, RPNs are calculated and often used as a guide for failure mode mitigation. The words of caution from 5.3.2 must be remembered and the RPN deficiencies must be kept in mind.

Some of the deficiencies of the RPN are as follows:

– gaps in the ranges: 88% of the range is empty, only 120 of 1000 numbers are generated,
– duplicate RPNs: for several combinations where different factors lead to the same RPN,
– sensitivity to small changes: a small change in one factor has a much larger effect when the other factors are larger than when they are small (example: 9x9x3 = 243, and 9x9x4 = 324 versus 3x4x3 = 36 and 3x4x4=48),
– inadequate scaling: the ratios on occurrence table are not proportional or linear; e.g. the ratio can be 2,5 or 2 between the two consecutive ratings,
– inadequate scale of RPN. The differences in RPN number might appear negligible while in fact significant. An example would be: the values: S = 6, O = 4, D = 2, would produce an RPN = 48, while S = 6, O = 5, and D = 2 would produce RPN = 60. The second RPN is not twice the first number, while in fact O = 5 is twice the probability of occurrence with O = 4. Therefore the RPN numbers should not be compared linearly.
– misleading conclusions from RPN comparison as the scales are ordinal and not rational.

Review of an RPN requires caution and good judgment. A good practice would require a thorough review of the values for the Severity, Occurrence, and Detection, before forming an opinion and undertaking corrective measures.

5.4 Report of analysis

5.4.1 Scope and content of a report

The report on the FMEA 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.

5.4.2 Effects summary

A listing of the failure effects on a specific system highlighted by the FMEA should be prepared. Table 7 gives a typical set of failure effects for a motor vehicle starter motor and circuitry.

Table 7 – 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 1 This list is an example only. Each system or subsystem being analysed will have its own set of failure effects.

A failure effects summary may be required in order to determine the probability of failure of the system resultant from the listed failure effects and to establish priorities for remedial or preventive actions. The failure effects summary should be based on the list of end failure effects and should contain details of the item failure modes contributing to each failure effect. The probability of occurrence for each of the failure modes is calculated for the established pre-determined time period of item use as well as for the expected use profile and stresses. Table 8 illustrates an example of failure effects summary.

Table 8 – Example of a failure effects probability

Number	Effect	Contributing failure mode reference	Failure effect probability of occurrence
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	$1{,}1\times10^{-5}$
4	Starter motor operates prematurely	14, 15, 17, 18	$3{,}6\times10^{-7}$

NOTE 2 This table can be constructed for other qualitative and quantitative rankings of an item or a system.

The summary should also contain 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 should include listings of the following:

a) failure modes, that result in serious effects;

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

c) design changes which have already been incorporated as a result of the FMEA;

d) effects that are mitigated by the incorporated design changes.

6 Other considerations

6.1 Common-cause failures

In a reliability analysis, it is not sufficient to consider only random and independent failures. Some “common-cause” 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 (improper components derating), environmental stresses (lightning), or human error.

Common cause failures (CCF) are those failures which defeat the fundamental assumption that the failure modes under consideration in the FMEA are independent. The CCF will cause more than one item to fail simultaneously, or within a sufficiently short period of time as to have the effect of simultaneous failures.

Typically, sources of CCF include

– design: software, rating;
– manufacturing: batch related component flaws;
– environment: electrical interference, temperature cycling, vibration;
– human factors: incorrect operating or maintenance actions.

The FMEA must therefore consider possible sources of CCF when analysing a system that uses redundancy to maintain function or multiple items to mitigate consequences in the event of failure.

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). Common-cause failures can be in identical parts with the same failure modes and weaknesses used in various assemblies of a system – possibly redundant, where redundancy is voided.

CCFs can be analysed qualitatively using FMEA, but the ability of FMEA to fully analyse CCF is quite limited. However, 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 that can induce potential CCF.

A combination of several methods is useful to prevent or mitigate CCF (system modelling, physical analysis of components): functional diversity (where the redundant branches or parts of the system performing the same function are not identical and have different failure modes), physical separation to eliminate influence of environmental or EMI (electromagnetic interference) stresses causing CCF, tests, etc. Usually the FMEA does not consider the examination of preventive measures against CCF. However, these measures have to be included in the remarks column, to help in understanding the whole FMEA.

6.2 Human factors

Some systems have to be designed to prevent or mitigate some human errors. An example of those measures would be 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 errors. For example, incorrect maintenance of similar items can negate redundancy. To avoid this, material diversity in redundant elements is often introduced.

6.3 Software errors

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.

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

6.4 FMEA regarding 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, 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, Markov graphs, Petri nets, etc.

7 Applications

7.1 Use of FMEA/FMECA

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 or it may be specific to particular pieces of equipment, to systems or to projects as a whole.

FMEA should also include the consideration of software and human performance where these are relevant to the dependability of the system. An FMEA can be a study for general use to study various processes (medical, laboratory, manufacturing, development, educational, etc.) when it usually assumes the name of the Process FMEA or PFMEA. When a Process FMEA is performed, it is always done in regards to the process end goal or the target of a process, and then considers each step within that process as a potential to produce an unfavourable outcome of the other steps in the process or of the process end goal.

7.1.1 Application within a project

A user should determine how and for what purposes FMEA is used within his/her 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 supports the design review concept and should be put into use as early as possible in the period 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.

To ensure that it is effective, the place of FMEA should be clearly established in the dependability 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.

7.1.2 Application with a process

When prepared for a process, performance of PFMEA requires the following:

a) a clear definition of the process goal. When a process is complex, the process goal can be broken down to the overall goal or the product of the process, goal or a product of a set of process sequences or steps, and product of individual process step;

b) understanding of the individual steps in the process;

c) understanding of potential flaws in each process step;

d) understanding of the effect that each individual flaw (potential failure) can have on the product of the process;

e) understanding of potential causes of each of the flaws or potential process failures/faults.

If a process has more than one product, then it can be analysed with the specific product in mind; that is a PFMEA is made for individual products. The process can also be analysed in terms of its steps and potential unfavourable outcomes, which would result in a generalized PFMEA for the process regardless of types of individual products.

7.2 Benefits 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 1 Such effects may include secondary failures.

c) to determine the need for the design methods for reliability improvement (redundancy, operational stresses, fail safe, component selection and de-rating, etc.);

d) 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;

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

NOTE 2 Frequently, separate studies will be required for safety, but overlap is inevitable and therefore cooperation is highly advisable.

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

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

h) to assist in defining various aspects of the general preventive maintenance strategy and schedule;

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

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

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

l) 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.)

7.3 Limitations and deficiencies of FMEA

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.

Any relationships between individual or groups of failure modes or causes of failure modes cannot be effectively presented in FMEA, since the main assumption of such analysis is independency of failure modes. This deficiency becomes even more pronounced in view of software/hardware interactions, where independency assumption does not apply. The same type of difficulty can be encountered when adding the human interactions with hardware and modelling their interdependencies. Assumption of independency may obscure a failure mode that may have drastic consequences when a result of another failure mode, whilst each of them separately might have a low probability of occurrence. The interrelationship scenarios are far better modelled using the approach of failure mode analysis with the FTA tool (IEC 60300-3-1, Edition 2).

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.

Additional deficiency of FMEA is found in its inability to provide a measure of overall system reliability, and for the same reason it is not capable to provide any measure of design improvements or tradeoffs.

7.4 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, such as FTA. 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 deductive approach is preferred but FMEA is still a useful 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 by 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 comprehensive 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 for analysis of failure modes and their respective causes. 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 is capable of modelling the interdependency of various failure modes, where that interaction might result in an event of substantial proportions, and perhaps of high severity. This is especially important where occurrence of one failure mode first would induce occurrence of another with high probability and high severity. This scenario could not be modelled successfully with an FMEA, where each failure mode is considered independently and individually. One of the deficiencies of an FMEA is its inability to view interaction and dynamics of failure mode occurrences in a system.

FTA concentrates on the logic of coincident (or sequential) and alternative events causing undesirable consequences. It can produce a correct model of the system being analysed as well as an estimate of its reliability (or probability of failure), and can also evaluate the influence of the design improvements and failure mode mitigation on the overall system reliability, which can be advantageous. The FMEA format can be more descriptive. Both methods have their uses in a full analysis for safety and dependability 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 is 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 and their failure characteristics cannot be known from previous operational experience.

e) FMEA is usually more applicable to systems 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 multiple failure modes and dependency involving complex failure logic and redundancy. 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.

Annex A
(informative)

Summary of procedures for FMEA and FMECA

A.1 Steps for performance of analysis

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.

h) Determine system failure severity classes.
i) Establish item's failure mode severity.
j) Determine item's failure mode and effect frequencies.
k) Determine failure mode frequencies.
l) Draw up criticality matrix for item failure modes.
m) Summarize the criticality of failure effects from the criticality matrix.
n) Draw up criticality matrix for system failure effects.
o) 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 h), i) and j) at the end of the FMEA.

A.2 FMEA worksheet

A.2.1 Scope of a worksheet

The FMEA worksheet captures the details of the analysis in a tabularized manner. Although the general FMEA procedure is a standard, the design of a particular worksheet can be tailored to fit the application and project requirements.

Figure A.1 is an example of a format for an FMEA worksheet.

A.2.2 Worksheet header

The header part of the form captures the following information:

– the system, as an end item, identifies the item for which the end effects are being identified. This identifier should be consistent with the terminology used in the block diagrams, schematics or other drawings;

- the operating mode assumed for the analysis;
- item refers to the item (module, component or part) being analysed on this worksheet;
- revision level, date and the name of the analyst coordinating the FMEA effort as well as the names of the core team members who provide additional information for document control purposes.

A.2.3 Worksheet entries

The entries for "Item reference" and "Item description and function" are to identify the subject of the analysis. The reference should be keyed to the block diagram or other supporting documents. A brief description of the item and its function is entered.

The manner in which the item might fail is entered under "Failure mode". Subclause 5.2.3 provides guidance for identifying potential failure modes. Entering a unique identifier ("Failure mode code") for each unique item failure mode will facilitate summarizing the results of the analysis.

The most likely causes of the failure mode are listed under "Possible failure causes".

A concise description of the effects of the failure mode on the item being analysed is entered under "Local effect". Similar information is entered in the "Final effect" column to indicate the effects of the failure mode on the end item. For some FMEA analyses it is desirable to evaluate the failure effect at an intermediate level. In this case the effect on “Next higher assembly” is entered in an additional column. Identifying failure mode effects is discussed further in 5.2.5.

A brief description of how the failure mode is detected is indicated under "Detection method". The detection method may be done automatically by a built-in-test (BIT) feature of the design or may require diagnostic procedures by operating or maintenance personnel. It is important to identify the detection method so that the analyst can be assured that corrective action will occur.

Features of the design that mitigate the particular failure mode, such as redundancy, are to be noted under "Compensating provision against failure". Compensation provided by specific maintenance or operator actions should also be noted here.

The "Severity class" identifies the severity level as determined by the FMEA analysts.

"Frequency or probability of occurrence" identifies the rate of occurrence of the particular failure mode. The frequency scale is tailored to fit the application (e.g. failures per million hours, failures per distance travelled, i.e. 1 000 km, etc.).

The "Remarks" entry captures the observations and recommendations of the analysts as described in 5.3.4.

A.2.4 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.

FMEA

End item: Operating period:			Item: Revision:					Prepared by: Date:			
Item ref.	**Item description and function**	**Failure mode**	**Failure mode code**	**Possible failure causes**	**Local effect**	**Final effect**	**Detection method**	**Compensating provision against failure**	**Severity class**	**Frequency or probability of occurrence**	**Remarks**

Figure A.1 – Example of the format of an FMEA worksheet

IEC 2643/05

Annex B
(informative)

Examples of analyses

B.1 Example 1 – FMECA for a part of automotive electronics with RPN calculation

In Figure B.1, a small part of an extensive FMECA done for an automotive product is presented. The assembly analysed is the power supply, and only its connections to the battery line.

The battery line has a diode D1, and a capacitor C9 connecting the plus side of the battery to the ground. The diode is reversed polarity such that if a negative battery side is connected to the item, this negative voltage would short to ground, protecting the item from damage. The capacitor is for the EMI filtering. If any of those parts should short to ground, the battery would also short to ground which could lead to the draining of the vehicle battery. Such failure is certainly without a warning, and a "walk home" failure in the automotive industry is considered hazardous. Therefore, for the failure modes of both parts "short", the *S* rank is 10. Occurrences were calculated from the parts failure rates under their respective stresses for the vehicle life, and then matched to the *O* scale of the automotive FMEA. Detection is very low, as shorting of any of the parts would be immediately noticed in test – item not operational.

Opening of any of the above parts would not cause any damage to the item, except if the diode opens, then there would be no reverse battery protection, while with the capacitor open, there would be no EMI filtering – possible noise for the other equipment in the vehicle.

There is a coil, L1, between the battery and the item's circuitry, primarily for filtering. If the coil opens, the item would not be operational as the battery would be disconnected and the warning display would not be lit. Coils do have a very low failure rate, so that the occurrence is 2.

Resistor R91 carries the battery voltage to the switching transistors; if failed open, it would render the item inoperable, which also would be severity 9. Since resistors have a very low failure rate, the occurrence is 2. Detection is 1, since the item would not be operational.

Item/ Function			Potential failure mode	Potential effect(s) of failure		SEV	CLASS	Potential cause(s)/ mechanism(s) of failure	Detail cause(s)/ mechanism(s) of failure	Occur	Current design controls prevention	Current design controls detection	Detec	RPN	Recommended action(s)	Responsibility and target completion date	Action results				
Subsystem	Assembly	Component		Local effect	Final effect												Actions taken	Sev	Occur	Detec	RPN
Power supply																					
	V1																				
		D1	Short	Battery voltage + shorts to ground –	Battery drain, walk home	10		Inherent defect of the component	Material breakdown	3	Selection of higher quality and rating	Evaluation and reliability validation testing	1	30							
		D1	Open	No reverse voltage protection	Not noticeable	2		Inherent defect of the component	Bonding or semiconductor crack	3	Selection of higher quality and rating	Evaluation and reliability validation testing	2	12							
		C9	Short	Battery voltage + shorts to ground	Battery drain – walk home;	10		Inherent defect of the component	Dielectric breakdown or crack	3	Selection of higher quality and rating	Evaluation and reliability validation testing	1	30							
		C9	Open	No EMI filtering	Item operation out of specification	2		Inherent defect of the component	Dielectric open, leak, void, or crack	2	Selection of higher quality and rating	Evaluation and reliability validation testing	1	4							
		L1	Open	No V1 –	Item inoperable No warning display	9		Inherent defect of the component	Material breakdown	2	Selection of higher quality and rating	Evaluation and reliability validation testing	1	18							
		R91	Open	No voltage for the item switching circuit	Item inoperable. No warning display	9		Inherent defect of the component	Bonding or material crack	2	Selection of higher quality and rating	Evaluation and reliability validation testing	1	18							

Figure B.1 – FMEA for a part of automotive electronics with RPN calculation

IEC 2644/05