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 On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.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

IEC

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.