Norma Española

UNE-EN IEC 60812:2018

Idioma: Inglés

Análisis de los modos de fallo y de sus efectos (AMFE y AMFEC). (Ratificada por la Asociación Española de Normalización en noviembre de 2018.)

Asociación Española
de Normalización
Génova, 6 - 28004 Madrid
915 294 900
info@une.org
www.une.org

UNE-EN IEC 60812:2018

Análisis de los modos de fallo y de sus efectos (AMFE y AMFEC). (Ratificada por la Asociación Española de Normalización en noviembre de 2018.)

Failure modes and effects analysis (FMEA and FMECA) (Endorsed by Asociación Española de Normalización in November of 2018.)

Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC) (Entérinée par l'Asociación Española de Normalización en novembre 2018.)

En cumplimiento del punto 11.2.5.4 de las Reglas Internas de CEN/CENELEC Parte 2, se ha otorgado el rango de documento normativo español UNE al documento normativo europeo EN IEC 60812:2018 (Fecha de disponibilidad 2018-10-12)

Este documento está disponible en los idiomas oficiales de CEN/CENELEC/ETSI.

Este anuncio causará efecto a partir del primer día del mes siguiente al de su publicación en la revista AENOR.

La correspondiente versión oficial de este documento se encuentra disponible en la Asociación Española de Normalización (Génova 6 28004 MADRID, www.une.org).

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 60812

October 2018

ICS 03.120.01; 03.120.30; 21.020

Supersedes EN 60812:2006

English Version

Failure modes and effects analysis (FMEA and FMECA) (IEC 60812:2018)

Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)
(IEC 60812:2018)

Ausfalleffektanalyse (FMEA und FMECA)
(IEC 60812:2018)

This European Standard was approved by CENELEC on 2018-09-14. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN IEC 60812:2018 E

European foreword

The text of document 56/1775/FDIS, future edition 3 of IEC 60812, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 60812:2018.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2019-06-14
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2021-09-14

This document supersedes EN 60812:2006.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 60812:2018 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60300-1	NOTE Harmonized as EN 60300-1
IEC 60300-3-1	NOTE Harmonized as EN 60300-3-1
IEC 60300-3-12	NOTE Harmonized as EN 60300-3-12
IEC 60300-3-11	NOTE Harmonized as EN 60300-3-11
IEC 61025	NOTE Harmonized as EN 61025
IEC 61078	NOTE Harmonized as EN 61078
IEC 61165	NOTE Harmonized as EN 61165
IEC 61508 series	NOTE Harmonized as EN 61508 series
IEC 61709	NOTE Harmonized as EN 61709
IEC 62061	NOTE Harmonized as EN 62061
IEC 62308	NOTE Harmonized as EN 62308
IEC 62502	NOTE Harmonized as EN 62502
IEC 62508	NOTE Harmonized as EN 62508
IEC 62551	NOTE Harmonized as EN 62551
IEC 62740	NOTE Harmonized as EN 62740
IEC 62741	NOTE Harmonized as EN 62741
ISO 9000	NOTE Harmonized as EN ISO 9000
ISO 13849-1	NOTE Harmonized as EN ISO 13849-1

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 60050-192	-	International electrotechnical vocabulary Part 192: Dependability	--	-

IEC 60812

Edition 3.0 2018-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Failure modes and effects analysis (FMEA and FMECA)

Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)

IEC 60812:2018-08(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC 60812

Edition 3.0 2018-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Failure modes and effects analysis (FMEA and FMECA)

Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.120.01 03.120.30 21.020

ISBN 978-2-8322-5915-3

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

FAILURE MODES AND EFFECTS ANALYSIS (FMEA and FMECA)

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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 third edition cancels and replaces the second edition published in 2006. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) the normative text is generic and covers all applications;
b) examples of applications for safety, automotive, software and (service) processes have been added as informative annexes;
c) tailoring the FMEA for different applications is described;
d) different reporting formats are described, including a database information system;
e) alternative means of calculating risk priority numbers (RPN) have been added;
f) a criticality matrix based method has been added;
g) the relationship to other dependability analysis methods have been described.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
56/1775/FDIS	56/1782/RVD

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

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Failure modes and effects analysis (FMEA) is a systematic method of evaluating an item or process to identify the ways in which it might potentially fail, and the effects of the mode of failure upon the performance of the item or process and on the surrounding environment and personnel. This document describes how to perform an FMEA.

The purpose of performing an FMEA is to support decisions that reduce the likelihood of failures and their effects, and thus contribute to improved outcomes either directly or through other analyses. Such improved outcomes include, but are not limited to, improved reliability, reduced environmental impact, reduced procurement and operating costs, and enhanced business reputation.

FMEA can be adapted to meet the needs of any industry or organization. FMEA is applicable to hardware, software, processes, human action and their interfaces, in any combination.

FMEA can be carried out several times in the lifetime for the same item or process. A preliminary analysis can be conducted during the early stages of design and planning, followed by a more detailed analysis when more information is available. FMEA can include existing controls, or recommended treatments, to reduce the likelihood or the effects of a failure mode. In the case of a closed loop analysis, FMEA allows for evaluation of the effectiveness of any treatment.

FMEA can be tailored and applied in different ways depending on the objectives.

Failure modes may be prioritized according to their importance. The prioritization can be based on a ranking of the severity alone, or this can be combined with other measures of importance. When failure modes are prioritized, the process is referred to as failure modes, effects and criticality analysis (FMECA). This document uses the term FMEA to include FMECA.

This document gives general guidance on how to plan, perform, document and maintain an FMEA by:

a) describing the principles;

b) providing the steps in analysis;

c) giving examples of the documentation;

d) providing example applications.

FMEA may be used in a certification or assurance process. For example, FMEA may be used in safety analysis for regulatory purposes but, as this document is a generic standard, it does not specifically address safety.

FMEA should be conducted in a manner that is consistent with any legislation, which is in effect within the scope of FMEA, or the type of risks involved.

Primary users of this document are those who are leading or participating in the analysis.

FAILURE MODES AND EFFECTS ANALYSIS (FMEA and FMECA)

1 Scope

This document explains how failure modes and effects analysis (FMEA), including the failure modes, effects and criticality analysis (FMECA) variant, is planned, performed, documented and maintained.

The purpose of failure modes and effects analysis (FMEA) is to establish how items or processes might fail to perform their function so that any required treatments could be identified. An FMEA provides a systematic method for identifying modes of failure together with their effects on the item or process, both locally and globally. It may also include identifying the causes of failure modes. Failure modes can be prioritized to support decisions about treatment. Where the ranking of criticality involves at least the severity of consequences, and often other measures of importance, the analysis is known as failure modes, effects and criticality analysis (FMECA).

This document is applicable to hardware, software, processes including human action, and their interfaces, in any combination.

An FMEA can be used in a safety analysis, for regulatory and other purposes, but this being a generic standard, does not give specific guidance for safety applications.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60050-192, *International electrotechnical vocabulary – Part 192: Dependability* (available at http://www.electropedia.org)

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purpose of this document, the terms and definitions given in IEC 60050-192 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
failure mode
DEPRECATED: fault mode
manner in which failure occurs

Note 1 to entry: A failure mode may be determined by the function lost or other state transition that occurred.

Note 2 to entry: Examples of hardware failure modes might be for a valve, "does not open", or for an engine, "does not start".

Note 3 to entry: A human failure mode is determined by the function lost as a result of human action, whether committed or omitted.

[SOURCE: IEC 60050-192:2015, 192-03-17, modified — Note 1 has been modified, Note 2 and Note 3 have been added.]

3.1.2
failure effect
consequence of a failure, within or beyond the boundary of the failed item

Note 1 to entry: For some analyses, it may be necessary to consider individual failure modes and their effects.

Note 2 to entry: Failure effect also covers the consequence of a failure, within or beyond the boundary of the failed process.

[SOURCE: IEC 60050-192:2015, 192-03-08, modified — Note 2 has been added.]

3.1.3
system
combination of interacting elements organized to achieve one or more stated purposes

Note 1 to entry: A system is sometimes considered as a product or as the services it provides.

Note 2 to entry: In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g., aircraft system. Alternatively, the word “system” is substituted simply by a context-dependent synonym, e.g., aircraft, though this potentially obscures a system principles perspective.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.46, modified — Note 3 has been deleted.]

3.1.4
item
subject being considered

Note 1 to entry: The item may be an individual part, component, device, functional unit, equipment, subsystem, or system.

Note 2 to entry: The item may consist of hardware, software, people or any combination thereof.

Note 3 to entry: The item is often comprised of elements that may each be individually considered.

Note 4 to entry: IEC 60050-191:1990 (now withdrawn; replaced by IEC 60050-192:2015) identified the term “entity” as an English synonym, which is not true for all applications.

Note 5 to entry: The definition for item in IEC 60050-191:1990 (now withdrawn; replaced by IEC 60050-192:2015) is a description rather than a definition. This new definition provides meaningful substitution throughout this document. The words of the former definition form new note 1.

[SOURCE: IEC 60050-192:2015, 192-01-01]

3.1.5
process
set of interrelated or interacting activities that transforms inputs into outputs

[SOURCE: IEC 60050-192:2015, 192-01-08]

3.1.6
hierarchy level
level of sub-division within a system, item or process hierarchy

Note 1 to entry: Hierarchy level may also be known as the indenture level [see IEC 60050-192:2015, 192-01-05].

Note 2 to entry: Top-level and low-level corresponds to the highest and lowest levels of the hierarchy, respectively. Mid-level corresponds to levels between the highest and lowest levels.

3.1.7
element
level of sub-division of a system, item or process hierarchy at which failure modes are to be identified

3.1.8
scenario
possible sequence of specified conditions under which the system, item or process functions are performed

Note 1 to entry: Conditions may include activities or factors outside the defined item or process boundaries under study which may affect the performance of the item or process.

Note 2 to entry: Physical conditions include all environmental factors such as temperature, humidity, light levels, shock, contamination, radiation levels.

Note 3 to entry: Organizational conditions include factors such as staffing levels, physical/psychological stresses.

3.1.9
failure cause
set of circumstances that leads to failure

Note 1 to entry: A failure cause may originate during specification, design, manufacture, installation, operation or maintenance of an item.

Note 2 to entry: Examples of a failure cause may be contamination or inadequate lubrication which leads to the failure mode of bearing seizure.

Note 3 to entry: Failure causes for a process might include human error mechanisms such as stimulus overload, memory failure, misunderstanding, false assumption.

[SOURCE: IEC 60050-192:2015, 192-03-11, modified — Note 2 and Note 3 have been added.]

3.1.10
failure mechanism
process that leads to failure

Note 1 to entry: The process may be physical, chemical, logical, psychological or a combination thereof.

[SOURCE: IEC 60050-192:2015, 192-03-12, modified — Note 1 has been reworded.]

3.1.11
likelihood
chance of something happening

Note 1 to entry: In this document, the term “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as probability or a frequency over a given time period].

Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in terminology used in this document, the term “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

[SOURCE: ISO Guide 73:2009, 3.6.1.1, modified — Note 1 and Note 2 have been reworded.]

3.1.12
severity
relative ranking of potential or actual consequences of a failure or a fault

Note 1 to entry: The severity may be related to any consequence.

[SOURCE: EN 13306:2010, 5.13, modified — “relative ranking” has been added.]

3.1.13
detection method
means by which a failure mode or incipient failure become evident

3.1.14
control
design features, or other existing provisions, that have the ability to prevent or reduce the likelihood of the failure mode or modify its effect

Note 1 to entry: Controls can also be referred to as compensating provisions.

3.1.15
criticality
<of a failure mode> importance ranking determined using a specified evaluation criteria

Note 1 to entry: The criticality evaluation criteria normally refer to the effects of the failure mode on the top-level in the system, item or process hierarchy.

Note 2 to entry: Criticality measures normally combine severity of effect with at least one other characteristic of a failure mode.

Note 3 to entry: The specific meaning of criticality is dependent upon the evaluation method defined within an analysis and is discussed in detail within this document.

Note 4 to entry: Criticality relates to the failure mode and not to the failure causes (if the latter are identified at all).

3.1.16
treatment
action to modify the likelihood and/or effects of a failure mode

Note 1 to entry: Treatment is sometimes referred to as mitigation.

Note 2 to entry: Treatment may involve actions to eliminate the failure cause, change the likelihood of the failure mode occurring, and/or change the consequences.

3.1.17
human error
discrepancy between the human action taken or omitted, and that intended or required

EXAMPLE Performing an incorrect action; omitting a required action; miscalculation; misreading a value.

[SOURCE: IEC 60050-192:2015, 192-03-14]

3.1.18
redundancy
<in a system> provision of more than one means for performing a function

Note 1 to entry: The additional means of performing the function can be intentionally different (diverse) to reduce the potential for common mode failures.

[SOURCE: IEC 60050-192:2015, 192-10-02]

3.1.19
common cause failures
failures of multiple items, which would otherwise be considered independent of one another resulting from a single cause

Note 1 to entry: Common cause failures can also be "common mode failures".

Note 2 to entry: The potential for common cause failures reduces the effectiveness of system redundancy.

[SOURCE: IEC 60050-192:2015, 192-03-18]

3.1.20
common mode failures
<within a system> failures of different items characterized by the same failure mode

Note 1 to entry: Common mode failures can have different causes.

Note 2 to entry: Common mode failures can also be “common cause failures”.

Note 3 to entry: The potential for common mode failures reduces the effectiveness of system redundancy.

[SOURCE: IEC 60050-192:2015, 192-03-19]

3.1.21
testability
<of an item> degree to which an item can be tested, during and after operation to detect and isolate failures/faults

[SOURCE: IEC 60050-192:2015, 192-09-20, modified — "during and after operation to detect and isolate failures/faults" has been added.]

3.2 Abbreviated terms

ARPN	alternative risk priority number
CCF	common cause failure
COTS	commercial off the shelf
CSU	component software unit
DC	diagnostic coverage
EMI	electromagnetic interference
EMP	electromagnetic pulse
ESD	emergency shutdown
ETA	event tree analysis
FIT	failure in time
FTA	fault tree analysis
FMEA	failure modes and effects analysis
FMECA	failure modes, effects and criticality analysis
FMEDA	failure modes, effects and diagnostic analysis
MTBF	mean operating time between failures
MTTR	mean time to restoration
OEM	original equipment manufacturer
RBD	reliability block diagram
RCM	reliability centred maintenance
RPN	risk priority number
SFF	safe failure fraction
SIL	safety integrity level
SOD	severity, occurrence and detectability

4 Overview

4.1 Purpose and objectives

An FMEA is a method in which an item or a process is broken down into elements and, for each element in turn, failure modes and effects are identified and analysed. This is to identify any required improvements by eliminating adverse effects or reducing their likelihood or severity. The purpose of adding a criticality analysis is to enable prioritization of the failure modes for potential treatment.

The reasons for which FMEA is undertaken include the following:

- to identify those failure modes which have unwanted effects on system operation, for example preclude or significantly degrade operation or affect the safety of the user and other persons;
- to improve the design and development of items or processes in a cost effective manner by intervening early in the development programme;
- to identify risks as part of a risk management process (ISO 31000);
- to satisfy statutory and business obligations by demonstrating that foreseeable risks have been identified and accounted for;
- to provide a foundation for other dependability analyses (Annex D discusses the relationship between FMEA and other dependability analysis methods);
- to develop and support a reliability test programme;
- to provide a basis for planning maintenance and support programmes such as through reliability centred maintenance (IEC 60300-3-11);
- as a key process within an asset management system (ISO 55000).

In general, FMEA is a method to analyse the effect of single failures. If FMEA is used to analyse failure of interdependent items, then these can be considered, with limitations, in the analysis (5.3.6 and 5.3.7.2).

4.2 Roles, responsibilities and competences

An FMEA requires a person or persons (e.g. team) to take responsibility for the following:

- managing the process of conducting the FMEA;
- deciding the form of the FMEA so that it is tailored for the application context;
- identifying and analysing the failure modes and effects of the item or process;
- determining required treatments;
- reporting the FMEA including treatments and recommendations.

This document uses the following terms to describe the roles and responsibilities for conducting an FMEA.

a) Analyst

Person with responsibility for considering the suitability of FMEA, leading the tailoring of the FMEA, making sure that the FMEA method is followed and communicating with managers and other stakeholders. The analyst should be competent in FMEA and should have adequate technical understanding to challenge the other competent people involved in the analysis.

NOTE In case of a team effort, the role of challenging the people involved can be taken over by a person who sometimes is called 'facilitator'.

b) Persons with relevant competence

Persons with relevant knowledge and experience to cover all the aspects of the item or process to be analysed, including social, economic and environmental considerations, as required.

c) Manager

Person with responsibility for defining the purpose of the FMEA, for authorizing the use of resources, approving the tailoring, and handling treatment actions and recommendations, as required. This role may be undertaken by a manager who has the final design authority.

d) Stakeholders

Persons or organizations that can affect, be affected by, or perceive themselves to be affected by a decision or action. For example, stakeholders might include customers (e.g. contract owners), authorities (e.g. regulators), users (e.g. manufacturers and maintainers), suppliers (e.g. service providers, component suppliers) and those persons which might be adversely affected by failures.

4.3 Terminology

For convenience in this document, the title "failure modes and effects analysis" abbreviated to "FMEA" is used as a generic term to represent any application or degree of tailoring of the analysis, including FMECA.

The term "item" or "process" is used to denote the subject of the FMEA analysis. The item or process can be part of a larger system for which multiple FMEA analyses are required. Examples of the terms commonly associated with the top, mid and low hierarchy levels are given in Table 1. The terms within Table 1 are not exhaustive. For example, software can be embedded within a hardware system, or a system can contain human aspects.

Table 1 – Example of terms commonly associated with levels of hierarchy

	Top-level	Mid-level	Low-level
Hardware	Assembly	Sub-assembly	Component
Software	Package	Module	Executable code function
Process	Procedure	Task	Step

5 Methodology for FMEA

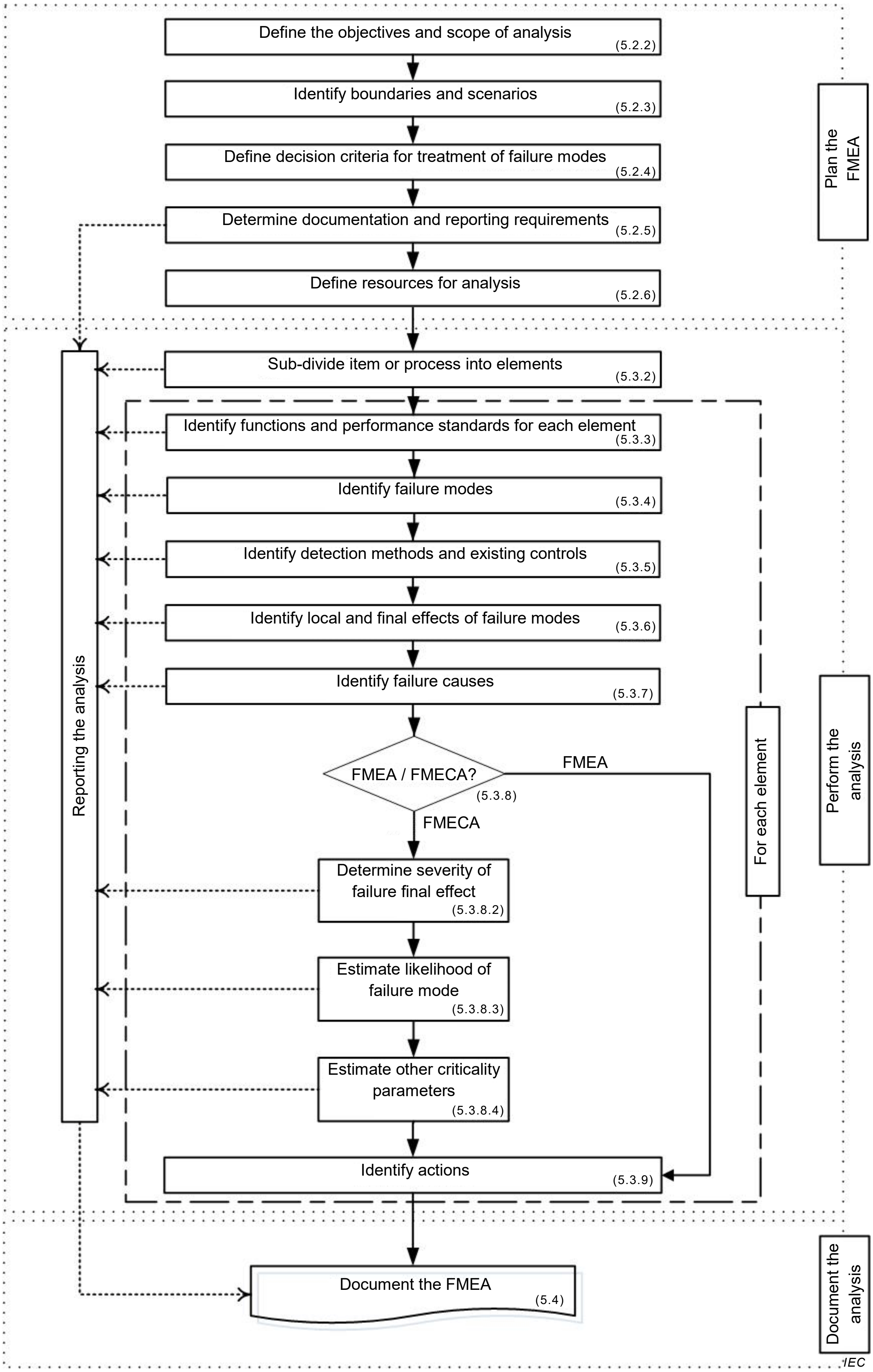
5.1 General

Figure 1 shows a flowchart of the activities undertaken during an FMEA. It distinguishes three phases: planning, performing, and documenting. The activities are normally performed sequentially but there can be iterations, for example when FMEA is performed as part of a development programme, or where the analysed system is subject to change.

An FMEA should be conducted in a manner that is consistent with any legislation, which is in effect within the scope of FMEA, or the type of risks involved.

When reference is made in this document to record/identify/specify/describe/state/document some information, it means the information is to be included in the relevant FMEA documentation, for example FMEA report, FMEA plan, post-FMEA documentation such as the action plan.

The activities shown in Figure 1 should be tailored to the application. This means that not all the listed activities always need to be performed. Annex A gives general guidance and examples of tailoring.


Define the objectives and scope of analysis (5.2.2)
Identify boundaries and scenarios (5.2.3)
Define decision criteria for treatment of failure modes (5.2.4)
Determine documentation and reporting requirements (5.2.5)
Define resources for analysis (5.2.6)
Plan the FMEA
Sub-divide item or process into elements (5.3.2)
Identify functions and performance standards for each element (5.3.3)
Identify failure modes (5.3.4)
Identify detection methods and existing controls (5.3.5)
Identify local and final effects of failure modes (5.3.6)
Identify failure causes (5.3.7)
FMEA / FMECA? (5.3.8)
FMEA
FMECA
Determine severity of failure final effect (5.3.8.2)
Estimate likelihood of failure mode (5.3.8.3)
Estimate other criticality parameters (5.3.8.4)
Identify actions (5.3.9)
Reporting the analysis
For each element
Perform the analysis
Document the FMEA (5.4)
Document the analysis
IEC

Numbers in brackets refer to subclauses.

Figure 1 – Overview of FMEA methodology before tailoring

5.2 Plan the FMEA

5.2.1 General

Planning an FMEA involves considering why an analysis is to be performed, what item or process elements are to be analysed and under what scenarios, and how the analysis should be most effectively and efficiently performed. Managers and stakeholders should be consulted, as appropriate, so that their objectives and interests in the analysis are properly understood and taken into account.

The output of the planning phase is an FMEA plan that describes a tailored, cost effective application of the FMEA for the particular context that:

- defines the objectives and scope of analysis (5.2.2);
- identifies the analysis boundaries and use scenarios (5.2.3);
- defines decision criteria for the treatment of failure modes (5.2.4);
- determines how the analysis will be documented and reported (5.2.5);
- specifies how resources will be allocated to the analysis activities (5.2.6).

The plan can also include a description of the factors which influence the approach to analysis, such as:

- a description of the interfaces with project milestones to determine the required timing of analysis outcomes;
- methodologies or documentation for understanding the item function or process sequence;
- contractual requirements;
- previous experience and available information.

The FMEA plan can be stand-alone or part of a higher level document, such as a project plan or a system engineering management plan.

5.2.2 Define the objectives and scope of analysis

The definition of the objectives and scope sets the foundations for the analysis effort, and informs the choice of approach to FMEA so that the outcome of analysis is aligned with the objectives.

The output of this activity should include the following:

- a purpose statement to define the reason for the analysis;

EXAMPLE To explore conceptual design robustness; to identify means of improving a process or procedure to reduce failures; to identify opportunities for reliability improvement; to identify risks; to satisfy a contractual requirement; to suggest requirements for maintainability and supportability programmes.

- an objectives statement, which defines the ultimate deliverable of the FMEA in terms that allow the analysis to be assessed as successful or otherwise.

The statement of objectives should be included in the FMEA plan.

For some applications, it may be appropriate to consult more formally with stakeholders and to document the decisions and outcomes into a more extensive scoping statement.

5.2.3 Identify boundaries and scenarios

5.2.3.1 General

The subject of the analysis, and its boundaries and use conditions should be described to ensure that the scope of the analysis is understood by both the users of the FMEA and the analyst(s) so that important aspects are not omitted due to incorrect assumptions concerning the scope. This description should become more detailed as planning progresses and may include diagrams, such as a flow diagram, functional block diagrams, reliability block diagrams, functional-hierarchy structure diagrams, or reference to documents where such information can be found.

For large or complex systems (e.g. a railway), it might be necessary to sub-divide the system into subsystems (e.g. rolling stock, signalling, control room) for each of which an FMEA is performed. The sub-division may be along physical or functional boundaries, and might be influenced by contractual requirements or organizational factors. The sub-division should be selected so that the size of each FMEA is manageable and each FMEA is logically connected to any others so that the influences of the subsystems on each other, and on the system as a whole are considered. Special attention should be paid to the interfaces between the subsystems and the boundaries within which they fall should be clearly defined.

5.2.3.2 Determine level and approach

An FMEA can be applied at any level of sub-division of an item or process hierarchy (Table 1). The FMEA may be approached in different ways depending on the analysis purpose and stage. Annex A provides guidance and examples.

EXAMPLE During early development stages an FMEA can be applied to the top- or mid-levels in the hierarchy and the causes for the failure modes limited to the failure of the elements in the next lower level(s). In later stages of development, elements at the lowest level of the hierarchy relevant to the objectives are considered. All failure modes associated with that element and their effects on the next higher level are identified. The FMEA will, however, always identify the effects of failure modes on the top level of the hierarchy within the analysis scope.

5.2.3.3 Define the boundaries of the subject of the analysis

The boundaries, relationships, dependencies and interfaces between the subject of the FMEA and other parts of the system, including human interfaces, should be delineated. The definition of boundaries should include inputs to, and outputs from, the item or process and explicitly specify which interfaces are within the scope of analysis and which are excluded.

The boundaries depend on the context and might be influenced by factors such as design or intended use. It may be necessary to explicitly place items or process steps outside the boundaries in order to constrain the size of the FMEA or because detailed knowledge of them cannot be obtained.

Where possible, boundaries should be defined to facilitate each FMEA and its integration with other related studies. In some cases, it might be useful to define boundaries from a functional viewpoint to limit the number of links to other items or processes outside the analysis. This is often the case if the item or process is functionally complex with multiple interconnections within or across the boundaries.

5.2.3.4 Define use scenarios

When an FMEA is undertaken, it is always in the context of one or more specific use scenarios. Use scenarios to which the FMEA is to be applied should be defined in line with the objectives of the analysis and described in sufficient detail to facilitate the identification of all relevant failure modes. The scenarios might include defined states outside specified normal use condition.

EXAMPLE Scenarios can be “normal operation” or “storage” when analysing hardware, or “night shift” or “emergency response” when analysing a process.

The scenario description normally includes the physical environmental conditions, such as ambient conditions in conjunction with conditions created by other items or activities in the vicinity. Other relevant factors include organizational constraints, such as staffing levels, or physical or psychological stresses that could influence human behaviour.

All internal and external stress factors that might affect failure modes and effects should be specified so they are considered in the analysis.

A clear audit trail should be established for documents used to define scenarios.

5.2.4 Define decision criteria for treatment of failure modes

The criteria for deciding which failure modes require treatment and priorities for action should be defined prior to undertaking the analysis. These criteria should take into account the objectives of the analysis, any legal or contractual requirements and stakeholder views on what is acceptable. The criteria should enable consistent and justifiable selection of those failure modes which require treatment, and those which do not, and should also indicate when recommended treatments are considered to be sufficient. Decision criteria for treatment of failure modes should be validated and approved by project management.

The types of consequence that are relevant to the analysis should be defined. For example, whether the consequences that are taken into account include economic impact, physical or psychological harm to humans, or intangible effects such as loss of reputation.

Decision criteria may vary between FMEA applications and should be regularly reviewed, for example, in the light of operating experience. Treatments for failure modes may be recommended as part of the FMEA, or as part of the follow up.

Decisions about the need to treat a failure mode and treatment priorities normally take account of the severity of the failure effect on the objectives and functions of the system as a whole, as well as the relative benefits and costs of treatment options.

In some cases, a formal criticality analysis can be carried out so that each failure mode is assigned a criticality rating. The criteria for defining criticality include:

- the severity of the failure effect on the objectives and functions of the system, or top-level relevant for the subject of analysis;
- the likelihood that the failure mode might occur and lead to the indicated severity of consequence; and
- the ability to detect the failure mode in time to mitigate or prevent the failure effect.

Severity and likelihood of failure, or alternatively severity, likelihood and detectability of failure, can be combined to give a criticality measure. This may be done using a matrix/plot or a risk priority number (RPN). There is no single method of criticality analysis can be universally applicable; Annex B describes two common methods. These can be used where appropriate for a specific application or adapted to suit organizational needs.

NOTE 1 The method used for criticality analysis can vary between projects, even within the same organization although a consistent approach to criticality analysis is usually beneficial.

Criticality analysis is useful particularly where there are constraints on the treatments possible based on cost, technical difficulty or time limitations.

Criticality analysis might not be useful if all identified failure modes are to be treated, or if there is insufficient information to make reasonable estimates of the criticality value. Also, it might not be cost effective in some applications.

NOTE 2 Criticality can be considered to correspond with risk. Further guidance on analysing risk can be found in IEC/ISO 31010.

The FMEA plan should include details of the decision criteria and, where criticality analysis is required, the method by which criticality is to be established. Decision criteria should also be detailed in FMEA reports.

5.2.5 Determine documentation and reporting requirements

5.2.5.1 General

The objective should be to document in a logical way all relevant information used and produced during the FMEA. Thus, the analysis and conclusions/recommendations derived therefrom should be easy to understand. The FMEA documentation should provide a clear audit trail that:

- describes how the output is expected to be used;
- provides information that could serve as evidence to inform decisions based on the analysis;
- describes the rationale for tailoring analysis including the method used for criticality rating;
- lists the sources of information used in the FMEA with auditable links to the sources;
- satisfies regulatory and contractual obligations, and demonstrate that those requirements are met.

Output from the FMEA might form input into other analyses or may stand alone as an FMEA report.

The form of the FMEA documentation should be decided as a part of the FMEA planning activity. The FMEA report should be formatted in accordance with the standards and procedures of the organization while considering the objectives, complexity and extent of the FMEA. The documentation generated in performing the FMEA may be a combination of databases, electronic documents and paper reports. The means by which traceability will be maintained across such potentially disparate media should be defined.

Since FMEA is iterative, the documentation is developed progressively throughout the life of the item or process which is the subject of the analysis. The FMEA documentation should be updated at times appropriate to the application. For example, at key project milestones, or as new information becomes available, design work progresses, as treatments/mitigating actions are identified and implemented, or utilization feedback and experience is gained. The revisions of FMEA documentation should be controlled through the document control process of the organization. Learning from an FMEA should be incorporated into future projects.

5.2.5.2 Content of the FMEA report

As a minimum, the report should include:

- a description of the system, item or process under analysis together with the appropriate block, functional or flow diagrams which define the structure;
- a clear description of the scope and boundaries, noting any particular exclusions from the scope;
- criteria used to define when treatment is needed;
- assumptions made about the item or process being analysed and the relevant use scenarios;
- a clear, detailed description of the methodology underpinning the analysis;
- identification of stakeholder(s) and personnel involved;
- a description of the method used to undertake the criticality analysis, which should be described in sufficient detail to allow independent verification;
- sources of data and other applicable materials (including issue status/revision) on which the FMEA is based;
- identification of failure modes, their effects and, if appropriate, their criticality and causes. Failure modes and effects should be expressed in a way that does not require reference to documents not identified in the report;

- a summary of the results and recommended treatments where generated, including recommendations for further analysis, if appropriate. The FMEA documentation might include only a brief statement of the recommended treatments. These treatments, however, then need to be managed in an action plan outside the FMEA documentation;
- limitations or shortcomings in the FMEA that should be addressed by future updates of the FMEA;
- design changes that have already been incorporated in the item as a result of the FMEA and any unresolved action items. In some cases, no action may be taken even when a treatment has been identified during the FMEA. In such cases, the justification for not taking the action should be documented in the action management documentation and the FMEA documentation should be updated with the final decision. The potential impacts of not taking actions on treatments should be monitored and reviewed as necessary;
- analysis records, which can be included as an annex to the report in the form of worksheets. Where these are extensive or a database has been used, references to where the information can be found should be provided.

Information collection, storage, retention and access might represent significant cost to an organization and care should be taken to ensure that any documents produced clearly add value to the FMEA. Any number of FMEA report formats is possible and the selected format will often determine the information captured, the assessments made and the process followed to produce the results. Annex C gives examples of FMEA worksheet reports.

5.2.6 Define resources for analysis

5.2.6.1 Information resources

The following information is typically required to perform an FMEA:

- the item or process to be analysed, its objectives and role in the system as a whole;
- the elements of the item or process and their characteristics, performances, roles and functions;
- the logical, physical and functional connections between elements, for example reliability block diagrams, functional block diagrams, flow charts, system charts, software versions, structure and control processes. This information might have already been gathered when carrying out related dependability analysis (Annex D);
- redundancy level and nature of spare equipment, redundant equipment or processes or parallel processing paths;
- position and importance of the item or process within the organizational context (if possible);
- inputs and outputs of the item or process and its elements;
- interfaces with other related items or processes and with the environment in which the item operates;
- any changes in item structure for varying operational modes;
- generic databases listing failure modes, their relative occurrence and failure rates;
- field operating experience data;
- previous FMEA analysis on the same, or similar items or processes, if appropriate.

Information pertaining to functions, characteristics and performance are required for all item or process levels considered up to the highest level within scope so that the analysis can properly address failure modes that affect any of those functions.

Collection of information continues during the FMEA as the analysis will often highlight where extra information is needed. Information shall be correct and understood by all participants. The basic information on the item or process analysed may be made available as an information package before the analysis begins and the analyst leading the FMEA should have access to all related information throughout.

5.2.6.2 Personnel

People with the technical competence and authority to perform the FMEA are required. Necessary skills and competencies include:

- the ability to apply the FMEA method;
- an understanding of the technical aspects of the item or process being analysed and its failure modes and effects;
- skills as a facilitator (where the analysis is performed by a team).

Achieving these might require a multidisciplinary team approach, where composition of the team depends on the objectives of the analysis.

EXAMPLE In the case of an information system, a systems engineer and a software expert can participate in a team.

Additional specific product or service knowledge might also become necessary as the analysis proceeds. If this is the case then other persons with relevant competences should also contribute to the analysis.

5.2.6.3 Physical resources

Physical resources are normally required in order to distribute communications and analyses amongst real or virtual teams or stakeholders. These might comprise dedicated meeting rooms, audio visual support for virtual meetings and shared information systems, including existing FMEA databases, etc. Such resources should be selected on the basis of cost effectiveness and the value achieved in terms of the quality, usefulness (initial and reuse) and timeliness of the analysis results.

5.3 Perform the FMEA

5.3.1 General

The steps to perform the analysis are described in 5.3.2 to 5.3.9.

5.3.2 Sub-divide item or process into elements

The subject of analysis is sub-divided into elements in order to perform the FMEA as follows:

- a system can be divided into functional blocks;
- hardware items can be divided into smaller, less complex hardware sub-assemblies or components;
- processes can be expressed as a sequence of activities, tasks or steps;
- software can be broken down into software modules or executable code functions;
- individual interfaces can be identified between the elements, and between an element and the user or the environment.

NOTE 1 Within an analysis, elements can include a mixture of hardware, software and/or processes.

NOTE 2 People can be considered as an element of a system, or human performance error mechanisms can be considered when analysing causes of hardware and/or software failure.

The appropriate level of detail for the analysis depends on the context and the results desired. In general, greater detail in the level of sub-division of the subject of the FMEA provides an equivalent level of detail on possible failure modes and effects and more detailed treatment strategies, but the analysis is more time consuming to undertake.

5.3.3 Identify functions and performance standards for each element

A clear statement of all the functions of each element is required to form the basis of the FMEA. Each function of an element should be considered separately in the analysis.

The performance standard for each identified function should be defined in order to be able to decide what constitutes a failure, and hence to identify failure modes. The function of each element should be derived from the functional specification or other available sources.

The performance standard selected should represent the level of performance essential to achieve the function of the element in the context of use of the item or process rather than the capability of the element. The performance standard should be expressed unambiguously and if possible quantitatively.

5.3.4 Identify failure modes

The ways in which each element of an item or process could fail to meet its performance criteria should be stated. An element might have a number of ways of failing (i.e. several failure modes). Each failure mode should be recorded separately. The analysis should aim to identify all credible failure modes relevant to the analysis objectives.

Depending on the purpose and scope of the analysis, the following are considered to help in identification of the failure modes of each element over the lifecycle:

- the application;
- the mode of operation;
- the pertinent operational specifications;
- environmental stresses and trends;
- psychological stresses and social change;
- storage, transport and maintenance operational stresses;
- disposal or dismantling process stresses.

Typically, failure mode information can be obtained from the following:

- for new items or processes, reference may be made to other items and processes with similar function and structure to their performance under appropriate conditions;
- for existing items or processes, the failure modes might be known from previous FMEA. However, checks should be carried out to seek any differences between the old and new application which could result in different failure modes (A.2.1).
- operating experience;
- performance and environmental tests, within or beyond specified limits;
- checklists based on generic failure modes for specific types of element;
- maintenance and repair databases;
- incident and accident databases;
- subject matter knowledge.

5.3.5 Identify detection methods and existing controls

5.3.5.1 General

For each failure mode, the existing controls and detection methods should be identified.

In this context, controls are the arrangements used to prevent or reduce the likelihood of the failure mode or mitigate its effects, while detection methods are the means to identify the failure mode, failure or incipient failure.

Early detection of a failure or imminent failure can allow operators, maintainers, users and others to intervene and reduce either the likelihood of adverse effects or their consequences. In specific applications, control and detection might have different meanings, although usually the intent is similar. Annex E and Annex F provide application specific guidance and examples, respectively.

When controls or detection methods are considered inadequate, then new or improved controls or detection methods should be determined and form the basis of treatments recommended (5.3.9).

5.3.5.2 Detection methods

Detection can take different forms depending on the type of FMEA being conducted.

EXAMPLE Detection methods can include the following: warning lights or alarms; indicators, gauges or monitoring; reliability tests during development; statistical process control; reliability stress screening; performance tests; audits; inspections; diagnostics.

When more than one failure mode can be detected by the same means, the ways in which ambiguities are to be resolved should be described so that none of the failure modes remain undetected and, where appropriate, correct action could be taken.

5.3.5.3 Controls

Design features, or other existing provisions, that have the ability to prevent or reduce the likelihood of the failure mode or modify its effect should be listed and the way in which they act should be described.

EXAMPLE Controls can include the following: redundant items or back-up systems that allow continued operation if one or more elements fail; adhering to engineering or other standards: alternative means of operation when detection identifies an issue; material specifications; machine settings; maintenance; design of items and processes that consider human factors.

5.3.6 Identify local and final effects of failure modes

A failure effect is the consequence of a failure mode in the scenario defined for the analysis. The same failure effect might be caused by one or more failure modes of one or more elements of an item or process.

The effect of failure modes for an element can be identified at the local level (i.e. local effect) together with the effect at the top level relevant for the subject of analysis (known as the global effect or the final effect). Effects at intermediate levels can also be identified if relevant.

NOTE 1 Local level can mean the same hierarchical level as the item being analysed or its physical location.

Identifying final effects is important when considering the relative importance of failures, as this represents a common reference point. Identifying the local effects provides information which can help when devising alternative treatments. In certain instances, there might not be a local effect beyond the failure mode itself.

In addition to consequences affecting the function of the item or process, or the system as a whole, there might be other consequences of concern, for example, relating to safety, environmental or to compliance requirements. Their relevance should have been specified in the FMEA plan.

NOTE 2 The identification of the final consequences of a failure mode can require the use of other forms of analysis, for example, event tree analysis (IEC 62502).

Failure effects should be described in sufficient detail for the user of the FMEA to be able to judge their significance. The failure effects are derived from the knowledge of the item or process, its functions, interactions and place in the hierarchy under analysis. Often, failure effects are classified into groups depending on the severity, or the nature of the effect, to simplify the analysis.

The recorded description of the failure effect should include sufficient information to enable an accurate assessment of the severity and significance of the consequences to be made. The manner in which consequences are recorded and the types of consequence to be considered should be based on those described in the FMEA plan.

Since FMEA considers the final effects on an element by element, or function by function, basis, it follows that the effects resulting from multiple failures are usually not identified. However, in some situations, such as analysis of standby or safety features, a failure that has no detectable immediate effect (i.e. it is not revealed) could result in top-level consequences following a second failure which would not otherwise be important. These events should be recorded for further investigation or analysis.

EXAMPLE Failure of a protective device results in adverse consequences only in the event that both the protective device fails and the item which it is designed to protect fails. Consequences resulting from such multiple failures are indicated in the analysis record.

NOTE 3 Fault tree analysis (IEC 61025) could be used to investigate the impact of combinations of failures, or to understand redundant functions and the relationship between protected and protective items.

5.3.7 Identify failure causes

5.3.7.1 General

Understanding how the failure occurs is useful in order to identify the best way to reduce the likelihood of failure or its consequences. The FMEA steps do not include a method for a full causal analysis. In some cases it can be useful to identify the physical, logical or psychological mechanism of the failure however this is not always necessary to achieve the goals of the analysis.

EXAMPLE Identifying that a failure mode of a leak is due to the mechanism of corrosion could lead to a recommendation to change the material.

NOTE Methods for more detailed causal analysis are given in root cause analysis (IEC 62740).

The extent to which failure causes should be explored depends on the cost effectiveness of doing so. For example, more effort could be dedicated to analysing causes of failure modes that have significant effect on functions and objectives than those with a lesser effect.

In identifying causes, the context of use should be taken into account. Causes relating to hardware, software, human aspects and the interfaces between them should be considered.

5.3.7.2 Common cause and common mode failures

An FMEA should consider possible sources of common cause failure (CCF). A CCF is a failure where more than one element fails simultaneously, or within a sufficiently short period of time, as to have the effect of simultaneous failures. Therefore common cause failures defeat the fundamental assumption that the failure modes under consideration in the FMEA are independent. A CCF refers to instances where the cause is associated with the elements themselves.

EXAMPLE 1 A cause of power supply failure is incorrect component rating for expected high temperature operation. Thus, when the expected high temperature occurs, more than one power supply will fail within a short period.

NOTE An item or process that uses redundancy or multiple (procedural) controls to maintain function or to mitigate consequences in the event of failure is prone to common cause failures.

Where a control might fail from the same cause as the element which it protects, then that CCF should be included as a failure cause in the same manner as other causes and the reasoning for its inclusion included in the documentation.

Common mode failures occur in a number of elements that fail in the same way (i.e. with the same failure mode) either due to the same or different causes. This is often a problem where the function loss is of redundant items using the same technology and construction.

EXAMPLE 2 Using insufficiently rated components (capacitors) with abnormal failure rate due to overstressing might lead to a short circuit common mode failure in redundant items.

A common mode failure should be identified and actioned as part of the normal analysis process if the appropriate element is within the scope. The sources and the effects of common mode failures might be better addressed with methods such as fault tree analysis (IEC 61025).

5.3.7.3 Human aspects

Humans may be considered to be an element of the item or process that has failure modes, alternatively human error may be identified as a cause of failure of a hardware, software or process element including their interfaces.

Analysing the causes of human error modes tends to be more complex than analysing causes of hardware or software failure as there are many more potential failure mechanisms, each with multiple potential causes. Failure to consider a range of psychological mechanisms might result in over simplistic and incorrect allocation of cause and hence inappropriate treatment strategies.

EXAMPLE 1 The failure mode “action omitted” could occur because a person loses their place in a sequence as a result of distraction or because they make false assumptions or because they have insufficient knowledge of the sequence required. If an action is omitted as a result of distraction or over familiarity, additional training might be of no use or even counterproductive.

NOTE 1 The causes of human error and factors that shape human performance are given in IEC 62508. A taxonomy of human error modes, mechanisms and causes as well as formal methods which can be used to analyse human error are given in IEC 62740.

NOTE 2 Humans are capable of intentional, as well as unintentional error.

Treatments to address human failures attempt to reduce the likelihood of the error occurring. Since it might be difficult to eliminate the error then the aim is to make the item or process more error tolerant.

EXAMPLE 2 In the process of driving a train, as well as making signals easily visible, interlocks can be provided to prevent drivers passing signals at danger, regardless of the cause of the error.

5.3.8 Evaluate relative importance of failure modes

5.3.8.1 General

The FMEA plan should specify whether the relative importance of failure modes should be considered and how this should be done.

Prioritization can be carried out either as part of the analysis for each failure mode as each failure mode is analysed for its effects, or following identification of all failure modes. The result is a list of all failure modes, prioritized in rank order, identifying failure modes which may require treatment. Priorities for action should normally also consider the cost effectiveness of available treatments, the ease with which they can be implemented and the way in which they affect other parts of the system.

5.3.8.2 Determine severity of failure final effect

The severity determined for each failure mode should represent the significance of its effect on the top-level of the system or item (the final effect), or on the objectives of the process. The meaning of top-level in the context of the analysis should be clearly specified.

EXAMPLE 1 An analysis of an item might be performed by a manufacturer to assess their product design, in which case the severity would be expressed in terms of the effects of the performance of the whole item. The same item might be analysed as part of a group of items, in which case the severity would be associated with the effects on the group performance.

EXAMPLE 2 A process or procedure can be analysed in order to evaluate it in terms of its impact on a small unit or group, or as part of a wider process.

NOTE The severity of an effect might appear more significant at low levels in an item hierarchy if redundancy or other control features/actions only get accounted for at higher levels in the hierarchy.

To ensure consistent failure mode prioritization within the FMEA, severity should be assessed using a clearly identified and common scale that covers the types of consequence (5.2.4) specified in the plan. Annex B provides further details.

5.3.8.3 Estimate likelihood of failure mode

The likelihood of occurrence of each failure mode should be determined when required as input to a criticality analysis method (Annex B) or when analysis findings are required as input by other dependability analyses (Annex D).

When estimating the likelihood of occurrence of a failure mode, the technical, human, organizational and environmental factors which might influence the failure and its likelihood should be considered.

When the likelihood of occurrence of a failure mode is estimated, the time period for which the estimations are made should be clearly stated. The period selected should be appropriate to the objectives of the FMEA.

EXAMPLE Commonly used time periods include: the warranty period; the anticipated useful life of the item; the specific usage period of the item or process; and shift duration.

The likelihood of occurrence of a failure mode can be estimated using a variety of methods and sources including:

- data from component life testing or laboratory derived human error rates;
- available databases of failure modes, failure rates, failure probabilities or unavailability;
- field failure data;
- human performance monitoring;
- failure data for similar items with comparable use.

NOTE Databases of failure modes exist for commonly used components of equipment (e.g. MIL-HDBK-338B, IEC 62308), for human error modes (e.g. Bell and Holroyd, 2009), human reliability assessment methods (e.g. IEC 62508), and for assessing failure of similar items (e.g. IEC 61709).

5.3.8.4 Estimate other criticality parameters

Where a criticality analysis is to be undertaken, parameters other than likelihood and severity can also be evaluated. For instance, a common additional parameter used in criticality assessment is a ‘detectability’ rating. A failure mode where failure, or imminent failure, might be detected easily is normally less important than one where there is no means of detecting the failure prior to adverse consequences occurring. Annex B contains examples where detectability rating is used in criticality analysis.

NOTE In some FMEA applications, particularly automotive, detectability has a different meaning; and is a part of identification of a potential failure mode during a development programme.

In a similar manner to that for a detectability rating, an additional parameter expressing the effectiveness of existing control (mitigation) measures may be of value in formulating a failure mode criticality ranking.

5.3.9 Identify actions

5.3.9.1 General

Depending on the scope of the FMEA, possible actions for those failure modes requiring treatment (5.2.4) should be identified, evaluated and documented. In some cases only treatments that are immediately obvious are documented as part of the FMEA, and the selection of the final solution is subject to further analysis and trade-off outside the FMEA.

It might also be necessary to undertake an FMEA in greater detail in an area of specific concern or undertake causal analysis before making recommendations.

The reasons for recommending, or not, any potential treatment are based on the decision criteria (5.2.4) agreed in the FMEA plan and should be documented. When determining treatment, care should be taken in the interpretation of the factors used in determining the failure mode importance.

When determining treatments, a level of accuracy and precision should not be attributed inconsistent with the data and methods employed even when full quantification of an FMECA has been carried out.

5.3.9.2 Treatment options

Treatments can involve changes in the item or process design, actions to take place during operation or during the maintenance of hardware.

Generally, it is more cost effective to introduce changes during design, particularly for hardware items.

EXAMPLE 1 Changes in design include: replacing components with more reliable ones; introducing redundancy or back-up systems; ergonomic design of hardware or processes to make errors less likely; new or improved ways in which item, operators, users and others might detect failure, and safety or relief devices that limit damage.

During operation, action can be taken to detect a failure mode, or imminent failure, so as to prevent it or reduce its effects.

EXAMPLE 2 For hardware, potential treatments include isolation, load reduction, rerouting and activation of suppression functions. For processes, potential treatments include checks and adjustments made during a procedure.

Maintenance programmes can also be used as a means of control and should be developed in a structured manner from the results of the FMEA.

NOTE A process for developing such programmes is reliability centred maintenance (IEC 60300-3-11).

Treatments may result in one or more of the following:

- elimination of the failure mode;
- reduction of the likelihood of the failure mode;
- elimination or reduction of the effects of the failure mode.

The decision criteria (5.2.4) should be used to identify which failure modes require treatment. In some cases, no action might be taken even when a treatment has been identified during the FMEA.

Consideration should also be given to removing means of control that are ineffective or unnecessary.

Documentation should include, as a minimum, a brief statement of any recommendations made.

Where recommendations are accepted, and new controls or detection methods introduced, it might be necessary to revisit the analysis to check whether:

- any new failure modes or effects have been introduced; and
- the criticality of the particular failure modes is now acceptable.

Changes in the item or process documentation to be taken into account in the next FMEA update should be identified.

5.4 Document the FMEA

The analysis should be documented and reported as agreed in the FMEA plan (5.2.5).

Annex A
(informative)

General considerations for tailoring an FMEA

A.1 General

A.1.1 Overview

Tailoring customizes an FMEA to provide a cost effective way to achieve the FMEA objectives and involves making choices about:

- the boundaries of the system, item or process to be analysed;
- the start point in the hierarchy for the analysis;
- the level of detail of sub-division of the subject of the analysis into elements;
- which analysis steps to consider;
- the level of detail within each analysis step;
- whether failure modes will be prioritized based on their criticality and the assessment method to be used.

In general these choices will be informed by factors such as:

- the purpose of analysis (e.g. to improve or modify an item or process, to produce a dependability case (IEC 62741), to demonstrate compliance, to plan maintenance or logistics support, safety);
- the extent to which the process or item is new or innovative (e.g. technology);
- the availability of relevant data (e.g. operational experience for similar items, test data);
- whether it is required to recommend treatments or whether this will be done by others outside the FMEA;
- legal or contractual requirements;
- for an item, the maturity of the design or project, and;
- the stage of the life cycle at which the FMEA is carried out.

In general, the possibility that some items or processes, or their elements, might not require an FMEA in any form should also be considered, particularly if there is no clearly identifiable benefit in performing the analysis or if other forms of dependability analysis are considered more useful. An FMEA gains its business value by, for example, influencing design, operations and providing information for the development of cost effective preventive and corrective maintenance programmes. If the analysis results cannot influence these factors, then it might not be justified.

NOTE In many cases, commercial-off-the-shelf (COTS) items or elements from specialist suppliers can only be treated as 'black boxes' which can only be satisfactorily analysed for interfaces, such as inputs and outputs.

Examples of tailoring choices in specific industry applications are given in Clause A.3. General application considerations for FMEA are given in Annex E.

A.1.2 Start point for FMEA in the hierarchy

The choice of start point for tailoring an FMEA depends upon the purpose and stage of the analysis and how best value is achieved (5.2.3.2).

Where the start point to the analysis is the top- or mid-levels in the hierarchy and the causes for the failure modes limited to the failure of the elements in the next lower level(s), this is referred to in this document as a top-down approach.

Where the start point to the analysis is for elements at the lowest level of the hierarchy relevant to the objectives, this is referred to in this document as a bottom-up approach.

The top-down approach described is normally used in the early stages of design and hence may produce a result that is incomplete in depth and/or breadth as a result of deliberate limitation of scope or lack of available information. However, an early start to the analysis (using estimates where necessary) can have a positive impact on future item dependability and cost. If the project is continued to full scale development, the FMEA should be completed using the detailed 'bottom-up' approach so that it can fulfil its purposes.

NOTE 1 In this document, the term 'top-down' is used to describe the approach to developing the FMEA and it is not intended to be interpreted in the manner associated with fault tree analysis.

NOTE 2 If the analysis scope is more extensive than the inherent performance of the item (e.g. includes external events such as fire, flood or operator influence), or continued development is unlikely (e.g. a constrained feasibility study), then a fault tree analysis might be a more useful technique than FMEA.

Table A.1 summarizes the characteristics of top-down and bottom-up approaches. These characteristics allow the value for a given approach to be considered.

Table A.1 – Characteristics of top-down and bottom-up approaches to FMEA

	Characteristics
Top-down	Most often realized as a functional analysis that is intended to focus effort on the most important requirements or functions of the item or process. In early stages of development where only the functional requirements on an upper level are known. To help determine the structure of more detailed, later FMEAs (which may be then bottom-up), especially for complex systems. Can be applied where specific effects are of interest and only the failure modes require investigation. Can be cost effective if analysis needs to place emphasis on specific elements or functions of interest. Allows assessment of the loss of function at item level, but limits the results to an assessment of how pre-defined failure events might occur, rather than attempting to identify all failures that could occur. Requires judgement in assessing the point in the analysis where continuing to lower levels of the hierarchy would provide little or no useful information supporting the objectives of the analysis. Can support identification of requirements at lower levels.
Bottom-up	Most often applied where the individual elements of an item or process are examined at the most detailed level relevant and the effects of their failure analysed at specified higher levels of the hierarchy. Provides greater assurance that all potential failure modes have been considered as few assumptions are made regarding black box COTS or aggregated elements in complex throw-away modules. Well suited to identifying all possible effects when deploying an entirely new arrangement of components or existing items into a new environment or application. Often employed for new designs where the range of top-level or higher level effects might not be known. Requires no knowledge of the item top-level functional requirements since the loss of function at the item top-level is inferred by propagating the component failure effects up through the structure of the item hierarchy. Can significantly increase the scale of the FMEA and hence the effort required for the analysis.

A.1.3 Degree of detail in analysis

FMEA can be developed to different degrees of detail to provide additional information, for example, to analyse potential treatment options or to assist related analyses in operating, maintenance or supporting a logistics programme. The depth and breadth of an FMEA will inevitably depend on the complexity of the system, item or process that is the subject of analysis.

A.1.4 Prioritization of failure modes

Extending an FMEA to include a criticality analysis might be useful when a measure of the relative importance of a particular failure mode is required. Such information about relative importance can be used when planning priorities for treatment assessment and actions. If all failure modes are to be treated in some way (e.g. if required for regulatory compliance) then conducting a criticality analysis might not be useful.

Severity or criticality need not be the only consideration when deciding priorities for treatment. For example, the cost effectiveness of available treatments, the ease with which they can be implemented and the way in which they affect other parts of the system can also be considered.

Assessment of parameters, such as severity and likelihood, might be based on quantitative, or qualitative measurement scales.

- Quantitative scales might be useful when relevant operating experience, test data or prediction is available enabling a failure rate or probability to be assigned to specific failure modes.
- Qualitative scales might be useful when failures have to be prioritized, but detailed information is unavailable or the item is insufficiently defined to enable relevant quantitative data to be applied.

Table A.2 summarizes the general application characteristics of qualitative and quantitative criticality assessments for top-down and bottom-up approaches to FMEA.

Annex B provides detailed guidance on criticality analysis methods.

The guidance in Clause A.1 is general. More specific consideration might be required in given applications. For example, safety critical systems may require demonstrable evidence that they have either been designed or selected in a manner that transparently identifies, analyses, evaluates and treats the likelihood and severity of failure. The FMEA may be customized to show, for example, the traceability of mitigation or treatment together with evidence that the method used is appropriate to the application context. Further consideration of issues associated with common types of applications are discussed in Annex E.

Table A.2 – General application of common approaches to FMEA

	Qualitative analysis	Quantitative analysis
Top-down	Generally conducted in the early stage of an item design when the approach might be cost effective because it allows analysis to stop when reaching a level at which no further breakdown of the item design is possible or failure mode knowledge is unavailable for some other reason. An example application is a low cost confidence check that a defined OEM support regime for a mature item, which has some match to the expected failure modes in the design. This can be achieved by top-down analysis showing traceability between defined maintenance tasks and the failure modes mitigated or managed. A top-down approach in early design might not involve even a qualitative assessment if the purpose is to explore and understand failure modes and their effects only.	Generally compatible with design of new items where the architecture is known and treatment is focused on identification of design improvement opportunities by prioritizing failure modes and their effects. Analyses of this form also provides an audit trail between the failure modes, their effects and the potential value of mitigating actions, but can be more difficult to do. Generally justified where verifiable outcomes are necessary such as regulatory submissions or demonstration of a positive return on the invested effort is required.
Bottom-up	Generally applied to existing, complex and often aging items where actual quantitative performance data might not be readily available. Might be used where significant modification of an item requires integration of new equipment during design and data is not available for a quantitative analysis. Encourages analysis to start at a level of detail that satisfies the intent of the analysis (e.g. prevent application of FMEA to COTS items, where the effort will not assist understanding and there are few if any options to change the design).	Generally useful at the completion of the item design to demonstrate compliance with design specification and provide detailed material for use by other analyses such as in safety or logistics support. Analysis of this form might be lengthy, costly and generally justified only where large production volume or severe failure effects of a particular item mean that application of the FMEA process is likely to achieve a return on the invested effort.

A.2 Factors influencing FMEA tailoring

A.2.1 Reuse of data/information from analysis of similar item

Reusing data from a previous analysis has the advantage of reducing effort and time. However, the data shall be valid for the new analysis. The relevance of data from a previous analysis to the FMEA being carried out can be assessed by considering questions such as:

- is the item or process design similar or the same as the one used before by the organization?
- does the data which is available from similar items or processes satisfy the analysis objectives?
- does the context of use and operating environment accurately reflect that of the item for which FMEA is to be conducted?

NOTE Items that are mass-produced, such as commercial-off-the-shelf (COTS) for use by multiple clients and potentially across multiple industries, might not have FMEA data available from the original equipment manufacturer (OEM). In these cases an FMEA might add little value except as a means of gaining some confidence in the OEM's offered maintenance programme. Also, the COTS can be regarded as a "black box" and treated at the lowest level of the item hierarchy.

FMEA can be one method applied as part of a dependability programme and, if so, data can be shared with the applications of other analysis methods; see Annex D.

A.2.2 Maturity of item design and project progress

Maturity relates to both project maturity (i.e. progress of the project across the item lifecycle) and to design maturity. Maturity of design and of project are considered together due to their association.

At the concept design stage, when the overall architecture of an item is maturing, then functional top-down FMEA provides an opportunity to identify high-level failure modes to assist in selection of the architecture. As the design matures beyond concept stage to detailed design, the selection of existing designs for elements of the item can shift the emphasis to a bottom-up approach. The start point for a bottom-up approach to analysis usually depends on having selected the start point in the item hierarchy through the top-down functional analysis or architecture decomposition.

Commercial item designs often evolve over long periods of time through progressive waves of modifications and evolution, which improve dependability. Mature evolved designs might not have any formal FMEA documentation available. For example, because the item design evolved before the general acceptance of the value of an FMEA, or without the use of FMEA based improvement processes. However, mature designs might have known reliability performance and associated maintenance programmes that ensure continued performance. Conducting a detailed FMEA on such items might have little, if any, influence on either the design or the maintenance programme.

Immature designs are often characterized by recent innovations in architecture or the application of novel materials and parts to achieve improved capability and/or cost effectiveness. Original equipment manufacturers (OEMs) may have formal FMEA available for inclusion in the overall item analysis. Absence of an FMEA for such designs may be a reason to take additional action such as environmental testing to ensure required performance. Immature design can result from using mature components or immature components either of which can influence the degree of effort applied in the analysis.

A.2.3 Degree of innovation

The assessment and treatment of failure modes associated with technological innovation can be supported by all four combinatorial forms of an FMEA with different forms used as the project moves from concept design to full scale developmental item.

EXAMPLE Technological innovation might be new technology, processes, or novel applications of existing technology, or a novel process.

Mature technologies are similar in nature to mature designs. The long term evolution of mature technologies might obscure the development path along with the functional descriptions of the item and elements. Therefore a useful way of establishing the benefit of the FMEA will be to assess the potential to impact design, to vary or define the likely reliability and maintainability capability, and to verify the maintenance and associated integrated support needs.

A.3 Examples of FMEA tailoring for items and processes

A.3.1 General

To show how FMEA tailoring has been approached to define the depth and breadth of FMEA in practice, several examples are given in the following subclauses. For each example, the subject of the analysis and the context of the application is described before the reasons for tailoring the FMEA in a particular way are explained. For examples that contain criticality analysis, only the reasons for the choice of method are discussed. Annex B gives details of criticality analysis methods.

A.3.2 Example of tailoring an FMEA for an office equipment product

The item of interest was a new design of office equipment comprising integrated hardware and software to be assessed in its preliminary and detailed design stages. The item design was a major variant of an established product family. Elements of the new design were novel and new technology was to be used. The company maintained a reliability database which contains data on, for example, stress, failure mode, mechanism, item structure and other relevant information for all existing parts. The elements of the item were all connected in series to perform the required functionality of the top-level product.

An FMEA was conducted as part of a reliability programme to support the review of the item design and its manufacturing process. Failure mode prediction and mitigation at the design phase was considered very important to realize competitive product development. The organization had considerable operational experience about performance and failure of the product family. Therefore FMEA could use such data with the objective of improving technical weaknesses identified at the product and process design phase.

Bottom-up FMEA was chosen because of the simplicity of the item and a programme objective to ensure system level functionality and reliability based on a complete understanding of low-level element performance under use conditions specified by the customer. Additionally, the product design solution was a mix of existing and new technology. Even by using existing technology, operational condition change might lead to different failure modes, thus a bottom-up FMEA was applied.

The FMEA included criticality analysis because it allowed redesign priorities to be set by measuring the severity and likelihood of failure. Since the design cycle was short, FMEA was used to advise where to allocate resources to verify interfaces between elements and design parameters since it was not feasible to test and analyse all combinations. There was considerable operational experience of similar products to support this type of FMEA and ensure validity.

Criticality was determined using an RPN qualitative method (Annex B) as the method was simple to apply and considered comprehensive. Standard tables that define the measurement scales of the severity and likelihood categories had been developed within the company to keep consistency in application and assessment. The use of the standard tables for assessing criticality parameters enabled ready comparison of the FMEA across various types of product.

A.3.3 Example of tailoring an FMEA for a distributed power system

An FMEA was required to identify weaknesses in the design, achieve robustness and fault tolerance of a distributed power system. The analysis was also the first-step towards a full system availability study. The distributed power system was a new design within the product family. The new design was regarded as a major variant of earlier designs even though the technology being used was well understood. The structure of the system was heterogeneous but with identical functions. The FMEA was to be conducted during detailed design during which new data about the design and aspects of its performance would become available from other dependability and engineering analyses.

A top-down approach to FMEA was selected. The FMEA started by defining in detail the functions of the system. This allowed the deviations from these functions to support analysis of failure causes at a lower level. The system functionality was characterized through the development of a top-down FMEA which decomposed system functions to enable identification of failure modes, their causes and effects.

The FMEA also included criticality analysis as quantifiable information of failure mode occurrence and effect would support the subsequent availability analysis method. In the first cycle of the FMEA a qualitative RPN method was used and when more detail of the design became available, actual failure rates were used to assess quantitative likelihood of occurrence.

A.3.4 Example of tailoring an FMEA for medical processes

Many healthcare organizations across several countries are required, as part of their accreditation, to assess their procedures on a regular basis to identify where and how they might fail. The aim is to identify the parts of the process most in need of change and to reduce medical adverse events. FMEA is an approved way of achieving this requirement. An FMEA can be applied to any medical procedure. For example, making up a required dose and administering a drug, undertaking an operation, and anaesthetizing a patient.

This example considers FMEA for a medical procedure where designing the procedure might be straightforward, but people have the potential to make errors or they might be unable to perform the step in the way intended because of equipment or environmental factors.

The start and end of the procedure to be analysed should be clearly defined and the tasks carried out divided into steps for which each of the failure modes are identified.

When FMEA is applied in a medical context, recommended treatments most often involve adding checks and balances rather than changing the design of the procedure as a whole.

One may need to perform a subsidiary FMEA for situations such as, where equipment failure can lead to failure to perform a step of a process correctly or where one step in a written procedure in fact has multiple steps.

In general when FMEA is applied to a medical procedure, all failure modes with a serious consequence to patients are addressed. Where a criticality analysis is carried out, the RPN method is usually used. This is because potential failures that are easily detected before an adverse consequence occurs are less important than a failure mode that remains hidden until disaster strikes.

Quantitative analysis of human error rates is usually complex and can be unreliable. A simple method, such as RPN, or criticality matrix, is often all that is needed to provide useful assessments of criticality and provide prioritization to guide process improvement.

A.3.5 Example of tailoring an FMEA for electronic control systems

An FMEA was required to support analysis during concept and detailed design of safety electronic control systems, such as train braking systems and collision prevention systems. The systems were variants of earlier system designs. Changes between the new and existing systems tended to be in the design architecture and the technology used was well understood.

The purpose of the FMEA was to demonstrate the safety characteristics of the system. For this reason a bottom-up FMEA was chosen because that approach allows the analyst to systematically prove that the defined measures are able to appropriately mitigate all identified error scenarios of the system no matter which lowest level element fails.

The FMEA is written with an emphasis on an analysis of the failure risk mitigation capabilities of the system. This is an indispensable part of the analysis performed on systems which have safety. Essentially, the effects of failures are classified whether they are considered safe or not. In order to come to a sound decision, the scope of the effect description should be meaningful. For example: if the level is too focused on local effects, then the analyst might not deduce the criticality of the effect on the system as a whole; if the system level is too global, the analysis may not be able to follow the failure to the final effect.

This approach to FMEA gives rise to discussion around a number of issues. For example, typically, discussions arise when it comes to failure modes that are purely affecting the diagnosis capabilities of the system without impairing the main functionality. Another consideration is the reaction time of mitigation measures (i.e. to what extent can mitigation measures be taken into account if they occur too seldom to detect incipient failure before the occurrence of a failure event).

The tools used to support the FMEA range from bespoke spreadsheet lists to specialized relational database tools that apply RBDs to build the failure modes into item performance models. For example, subsystems may refer to instances of components with their inherent failure mode definition where differing failure modes might lead to the same failure effect that is tightly related to some classification regime.

A.3.6 Example of tailoring an FMEA for a pump hydro block

A basic FMEA was to be conducted to inform the preliminary design of a pump hydro block for a gas boiler. The functions of the hydro block include the pump function (flow, pressure), diverter valve function (switch boiler operation between central heating- and portable hot water mode), air-venting of central heating circuit (separate and discharge air from the liquid), water tight under the systems pressure conditions, able to connect to external hydraulic connection fitting and so on. The company had considerable operational experience in similar items and this was a minor variation of an existing product where the item design was being modified.

The FMEA was to be implemented in a way that would make best use of the design engineering team. Given the preliminary design stage and the experience of the design team, the logical starting point for the FMEA was identification of top level functions for the item. A workshop was used to identify failure modes, function by function. The process adopted was to bring the relevant people together for a workshop in which they stated their concerns. The intention was to explore and focus on engineering trade-offs for known failure modes and causes rather than to conduct an exhaustive FMEA.

The data collected during the workshop was in the form of sequences of failure modes, parts and their causes. For example, in case of a leakage-centred problem where the effect could range from unsatisfied customer to water on floor, external leakage, liability loss, etc. then failure mode could be leakage, the part was component X and the cause could be stress fatigue cracking.

A.3.7 Example of tailoring an FMEA for a wind turbine for power generation

An FMEA was required to support the detailed design of a wind turbine for power generation.

The scope of the FMEA was the complete turbine comprising subsystems such as structure, hub, power train, control system, etc. The objective was, based on experience with previous designs, to support the development of a new generation of turbine. In this project, it was required to assess the complete range of effects on each system level by prioritization of failure modes on the basis of risk.

A bottom-up approach was taken for each of the individual, interdependent subsystems where interface effects among subsystems were taken into account, leading eventually to system level effects. The starting point was the system/subsystem structure layout with, for example, input-output units, control units, gearbox, motors, encoders, electric motors, sensors, power supplies, converters, bearings.

A bottom-up approach was used because a thorough investigation of all possible effects on subsystem and system level was required, both with respect to reliability and availability as well as safety aspects. Criticality analysis was used in order to have an indication of which failures required more attention. The RPN criticality method was selected because it was simple and the three measures of severity, occurrence and detectability were required by regulation to meet FMEA objectives.

Annex B
(informative)

Criticality analysis methods

B.1 General

Criticality methods provide a means of prioritizing failure modes. The methods described in Annex B are only those which combine measures for the parameters: likelihood of failure, the consequences of failure, and (in the case of the risk priority number) the detectability of the failure.

NOTE Use of a single parameter to rank importance is not classed as a criticality analysis.

There are a variety of ways these parameters might be combined to produce a criticality. Annex B describes four methods: the criticality matrix, the criticality plot, the risk priority number and the alternative risk priority number.

The types of consequence considered, the scales that are to be used for each of the parameters and the method of combination to give a criticality should be decided during the planning stage. The methods described are general and should be tailored for the application in order to be meaningful in relation to the context and objectives of the analysis.

B.2 Measurement scales for criticality parameters

B.2.1 General

Criticality parameters can be measured qualitatively, quantitatively or semi-quantitatively.

- Criticality parameters might be expressed qualitatively using descriptive categories, ordered by degree. For example, 'minor', 'major' or 'catastrophic' (for severity of effect); or 'frequent', 'occasional' or 'remote' (for the likelihood of the failure mode occurring).
- Criticality parameters might be expressed quantitatively using empirical or other data in the form of a failure rate or probability of failure, and quantifiable consequences such as the economic or financial cost of failure. Ratio scales are established to match the relevant range of data with specified units.
- When the data only allows descriptive or order of magnitude estimates to be made, then criticality parameters might be expressed using ordinal rating scales, sometimes called ranking scales. If numerical labels are associated with ordinal ranks of likelihood and severity, or bands of failure rates and financial cost ranges, the approach is sometimes referred to as semi-quantitative.

The points on the measurement scale are expressed according to the application. For qualitative, quantitative and semi-quantitative approaches, the points correspond to the descriptive categories, the numerical estimates and the ranks/bandings respectively.

When developing the scales for measuring criticality parameters, care should be taken to use the best available information to help avoid biased results. A useful classification system might already exist in the organization and should be considered for application.

B.2.2 Scale definition

The range of the scales should span from the most severe to the most benign consequence of interest, from the highest to lowest likelihood, and from the highest to the lowest degree of detectability that can be associated with the failure modes under consideration for the scenario of interest.

The points on the measurement scales adopted should have a clear and precise definition that is meaningful in the context of the analysis to facilitate consistent and accurate assessment. The definitions should align with available data and be expressed in terms that are meaningful to those carrying out the analysis.

Logarithmic scales might be more appropriate than linear scales for quantitative data for both consequences and likelihood. Points on the scales used for qualitative and semi-quantitative approaches should be defined accordingly.

EXAMPLE The cost of a catastrophic failure is expected to be several orders of magnitude, rather than several times higher, than the cost of a minor failure.

The choice of categories (or bands) for qualitative and semi-quantitative scales should be based on consideration of the meaningfulness for the chosen parameters. There should be a sufficient number of categories to enable the complete range of effects to be classified and adequately separated. Generally, at least three categories are required in order to provide sufficient differentiation across the complete range considered. A large number of categories might be inappropriate because it can lead to excessive effort being required to identify the correct category when subsequent treatment does not significantly differ between categories.

NOTE As a guide, between three and ten categories are commonly used.

The selection of the category descriptions and the meanings of each should be carefully considered taking into account the manner in which they are to be used. Care should be exercized in the selection of verbal descriptions or number/letter labels for a qualitative approach as these can in themselves influence the choices made during the analysis. Each of the scales should be supported by a table defining the meaning of the words used.

B.2.3 Assessing likelihood

The likelihood value can be expressed quantitatively, semi-quantitatively or qualitatively.

In a quantitative approach using ratio scales, the likelihood values might be obtained for the specific failure modes, or they might be derived from generic data sources or estimated using data related to operation of similar items in comparable environments and applications.

Generally, where quantitative data are available, they tend to relate to the failure of an item or process as a whole rather than of that of each particular failure mode of that element. An estimate of the likelihood of a failure mode might be obtained by apportioning the likelihood of failure of the item as a whole into likelihoods of its potential failure modes. In addition, an adjustment might be made to represent the likelihood that the failure mode will result in a particular consequence (normally a defined severity).

NOTE If the likelihood is expressed as a failure rate then, unless otherwise stated, this approach implicitly assumes a constant failure rate and hence can be inappropriate in some circumstances. In addition, while the failure rate of an item might be obtained from specific data, the relative probability of its failure modes and the probability that a particular level of effect will follow a given failure mode are often also obtained from a different set of data sources or are based on judgement.

Where likelihood bands/categories are used, the descriptions might make use of applicable empirical data, expert judgement of the design team or other appropriate sources. It is essential that the scale is consistently applied so that the relative frequency of failure modes is accurately assessed and is compatible with available data.

In order to facilitate accurate and consistent application, the following should be taken into account.

a) If quantitative measures such as probabilities or frequencies are used, the units should be clearly stated.

EXAMPLE 1 If a percentage value is used, then what the percentage refers to is stated, such as, the percentage of items that fail in a year.

b) A numerical explanation of the category description that is relevant for the range of likelihoods expected for the given application should be included, if possible, to aid common understanding.

EXAMPLE 2 With highly reliable hardware systems, a “frequent” categorization for a failure mode of an element might be equivalent to one failure in several years whereas for less reliable systems, a "frequent" failure mode of an element might occur several times a year.

The likelihood descriptor for rare failures should be realistic when applied to the worst case consequence.

B.3 Assigning criticality using a matrix or plot

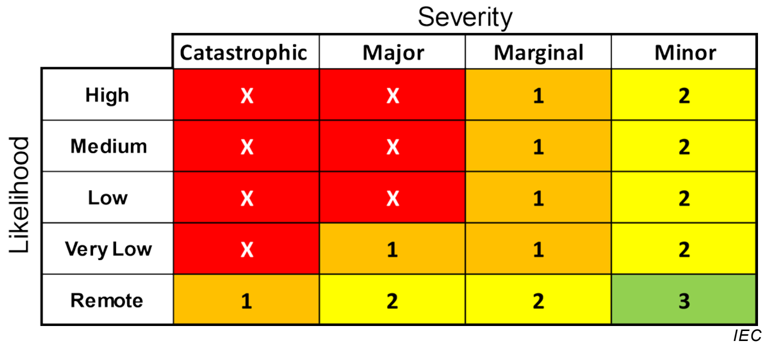
B.3.1 General

The relationship between criticality parameters may be represented in many ways to enable identification of the criticality rank. The likelihood and consequences of failure might be expressed on continuous scales, or in categories, then combined to be visually represented in the form of a plot, or matrix, respectively. This criticality plot or matrix is then utilized to set priorities for treatments.

The meaning of each criticality rank, and the link to treatments that are associated with them, should be discussed and agreed with the stakeholders prior to analysis as part of the FMEA planning. This gives a clear and unambiguous understanding of how failure modes should be handled and the potential business impact of such decisions. Failure to do this negates the value of the criticality analysis and can add significant time and cost through superfluous activities or inadequate treatment of failures. The number of criticality ranks required will be determined by the organization’s requirements and the analysis application.

B.3.2 Criticality matrix

A criticality matrix analysis produces a measure of importance by combining values for likelihood and consequence. A criticality matrix might also be known as a risk matrix. The values for each of the parameters are formed into a matrix and a criticality rank is allocated to each of the cells within the matrix. The criticality rank can be associated with the level of treatment which should be applied to manage the associated failure mode(s). For low rank failure modes such treatments may include “no action”. Figure B.1 shows an example of a qualitative criticality matrix.



		Severity			
		Catastrophic	Major	Marginal	Minor
Likelihood	High	X	X	1	2
	Medium	X	X	1	2
	Low	X	X	1	2
	Very Low	X	1	1	2
	Remote	1	2	2	3

IEC

Figure B.1 – Example of a qualitative criticality matrix

NOTE 1 An example of a four level criticality categorization (as used in Figure B.1) would be:

Category X: "Unacceptable”;

Category 1: “Undesirable";

Category 2: "Acceptable";

Category 3: "Minor”.

In some cases a failure mode can result in a range of different consequences, depending on circumstances. Where this is the case, the consequence to which the likelihood applies should be specified. It can be useful in this case to consider the criticality for several of the possible consequences.

In the example matrix in Figure B.1 the risk represented by each criticality category increases from the lower right of the matrix to the upper left. However, the treatments taken for each failure mode will depend only upon the criticality classification (i.e. the colour or number of the criticality code) and not the cell of the matrix.

NOTE 2 Even though terms such as "acceptable" can be used, this does not imply that further treatment might not be desirable.

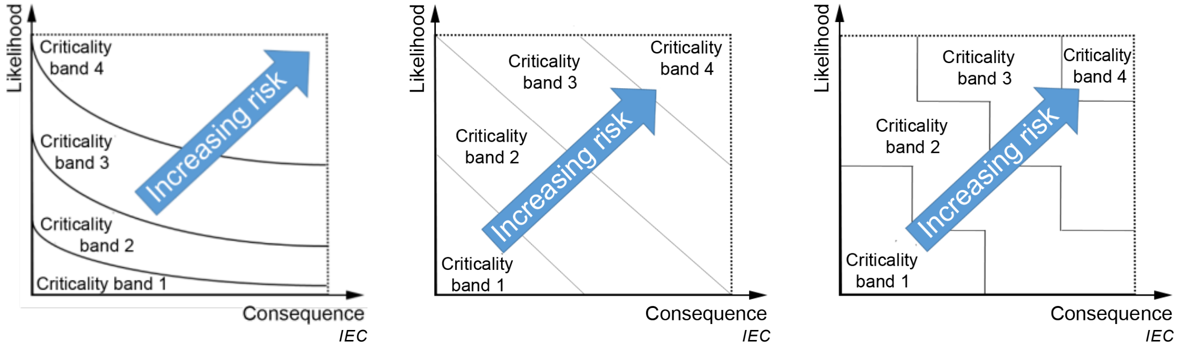
Figure B.1 is only an example of the structure of a matrix and should not be regarded as the definitive form. The actual form will depend on the particular application. If the number of likelihood bands and/or severity of consequence categories differs then the size of the matrix will differ from the one shown in Figure B.1. Equally, the criticality associated with consequence-likelihood combinations might differ in which case the colour coding pattern will also differ.

A matrix need not be limited to two dimensions, it can be extended to add a third parameter or, theoretically, as many other parameters as required. However, the complexity and effort needed to formulate a valid and manageable multi-dimensional grid can be considerable and not cost effective as every combination of parameters requires assessment.

The criticality matrix should be calibrated to ensure that failure modes with similar importance have the same criticality value, so that they receive the same treatment. In addition, where severity or likelihood categories are based on quantitative, or semi-quantitative assessments, consideration should be given to the acceptability of different treatments being applied to failure modes which have numerical values either side of a criticality boundary.

B.3.3 Criticality plots

Figure B.2 shows examples of simple plots of likelihood against consequence with criticality ranks being assigned according to bands within the plot. In this case both the likelihood and consequence (severity) are continuous quantitative scales.



Example A **Example B** **Example C**

Figure B.2 – Examples of criticality plots

The boundaries between bands need not be simple straight lines (Example A) or curves (Example B). According to the requirements of the treatments for the identified failure modes, a stepped boundary (Example C) or combination of lines and curves may be appropriate.

NOTE 1 In Example B, the boundaries of the bands represent lines of equal level of risk. Where likelihood and consequence are plotted on a linear scale, the lines will be curves. If a log-log scale is used straight lines will be produced.

NOTE 2 Where likelihood is plotted on a linear scale it can take a value of zero. This can lead to misleading criticality ranks for high consequence, low likelihood failures.

In practice, smooth band boundaries will only be meaningful if likelihood can be expressed quantitatively and the consequences of failure are continuous (e.g. financial) and can be fully identified.

A criticality plot need not be limited to two parameters, it can be extended to a third if required. However, the complexity and effort needed to formulate valid, manageable planes can be considerable and not cost effective.

In cases where the consequence/severity scale are quantifiable but have distinct, or bands of values, a criticality plot is still applicable but the boundaries of criticality value will almost certainly be stepped. This results in a similar representation to the criticality matrix.

B.4 Assigning criticality using a risk priority number

B.4.1 General

The risk priority number (RPN) is derived by combining semi-quantitative assessments made on ordinal scales with values for consequence, likelihood and detectability. In this method these parameters are respectively referred to as severity (S), occurrence (O) and detectability (D), which in some applications, leads to this also being referred to as the 'SOD' method. Two methods of evaluating the RPN are given.

B.4.2 Risk priority number

The common form of the risk priority number (RPN) is a product of the three ratings for severity, occurrence and detection.

$$\mathrm{RPN} = \mathrm{S} \times \mathrm{O} \times \mathrm{D}$$

The range of the RPN values depends on the measurement scales for the three parameters, which usually use ordinal rating scales of 1 to 10, producing overall RPN values ranging from 1 to 1 000.

NOTE 1 Some FMEA applications omit the parameter for detectability D, thus producing an overall RPN scale of 1 to 100.

NOTE 2 The nature of the application will determine the number of points on the scale so that less than 10 might be appropriate.

The numbers for S, O and D are determined using the ratings tables in which the levels for each parameter are associated with a descriptive sentence that assists the analyst in an accurate and consistent choice of rating.

The detectability number D can represent the likelihood with which a failure mode is expected to be detected during operation before significant failure effects occur. This number is usually ranked in reverse order from the severity or occurrence numbers; the higher the detection number, the less likely the detection. A lower likelihood of detection consequently leads to a higher RPN, and a higher priority for resolution of the failure mode.

EXAMPLE 1 This example is for a wind turbine. A typical measurement scale for severity rating might look like (abbreviated):

Severity rating (S)	Description
1	No effect on power generation; visit required in next 14 days; warning alarm not causing turbine to stop; possibly caused by component failure.
2	Short loss of power generation; visit required in next 14 days; turbine shutdown but remotely resettable; possibly caused by component failure.
:	: .
8	Loss of power generation over longer period (2 to 4 weeks); replacement of significant component requiring service vessel.
9	Loss of power generation over prolonged period (more than four weeks); replacement of significant component requiring major service vessel.
10	Safety incident; loss of whole structure; total loss of production for several months.

EXAMPLE 2 This example is for a wind turbine. A typical measurement scale for occurrence rating might look like (abbreviated):

Occurrence rating (O)	Description
1	Failure mode occurs once in 10 000 machine years.
2	Failure mode occurs once in 2 000 machine years.
:	: .
8	Failure mode occurs once a year per machine.
9	Failure mode occurs once every 4 months per machine.
10	Failure mode occurs once a month per machine.

EXAMPLE 3 This example is for a wind turbine. A typical measurement scale for detectability rating might look like (abbreviated):

Detectability rating (D)	Description
1	The failure mode will always be discovered before consequences come into effect.
2	The failure mode is apparent and will normally be discovered before consequences come into effect.
:	:
8	The failure mode can only be discovered by checks e.g. by sample inspections.
9	The failure mode is hard to discover and will therefore almost inevitably come into effect.
10	The features cannot be checked and the failure mode cannot be detected, e.g. inaccessible.

The failure modes are then ordered with respect to their RPN and higher priority is usually assigned to a higher RPN. In addition to the magnitude of the RPN, the decision for treatment may be 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 rating.

NOTE 3 In some applications, effects with an 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.

The rank order of the RPN is influenced by the way in which the scales are defined. When drawing conclusions from an RPN value or comparing values, the following characteristics of this method should be taken into consideration as failure to do so can result in inappropriate decisions:

a) The RPN scale is not continuous.

EXAMPLE 4 With three scales of 1 to 10, only 120 of 1 000 available numbers are generated.

b) Numerical ratios between values have no specific meaning.

NOTE 4 This is the result of the scales being ordinal and the measurement of severity, occurrence and detection being weighted equally; therefore the difference between RPN numbers can be small but actually have significant difference in meaning. For example, the values: S = 6, O = 4 and D = 2 would produce an RPN equal to 48, while S = 6, O = 5, and D = 2 would produce an RPN equal to 60. The latter RPN is only slightly higher, while O = 5 might, for instance, correspond to many times the likelihood of occurrence with O = 4.

c) The RPN can be sensitive to small changes in the value of one parameter.

NOTE 5 A small change in one parameter has an apparently much larger effect when the other parameters are large than when they are small (example: 9 x 9 x 3 = 243, and 9 x 9 x 4 = 324 versus 3 x 4 x 3 = 36 and 3 x 4 x 4 = 48).

Good practice for the use of the RPN is to conduct a thorough review of the values for the severity, occurrence, and detection, before forming an opinion about the criticality assessment and determining treatment actions.

B.4.3 Alternative risk priority number method

The so-called alternative RPN method (ARPN) is a modified version of the commonly used RPN described in B.4.2 that has been developed with the aim of providing a more consistent assessment of criticality when parameters can be quantified on a logarithmic scale (Braband, 2003) [27][1].

For the ARPN the points on the measurement scales for the parameters are defined and calibrated so that the meanings of the quantitative measurement scales are retained. A logarithmic scale is then used where each value associated with a level is a fixed multiple of the one before (such as 10, or the square root of 10). The same multiple has to be used for each of the scales for severity, likelihood of occurrence and detection. As a result, the number of rating levels of the parameter scales will be determined by the specific range of interest, and can be more or less than the ten levels normally used for the RPN described in B.4.2.

The tables defining the ratings for severity, likelihood of occurrence and detection should normally state the value associated with each rating level in addition to a descriptive sentence.

EXAMPLE 1 This example is for a railway application. The likelihood of occurrence scale might be calibrated based on a multiple of 10, or the square root of 10 which is approximately 3. In the latter case, the values of two adjacent levels of the scale comprise one order of magnitude. The corresponding levels of the likelihood of occurrence scale for a given failure mode of an item might be:

Occurrence rating (O)	Description
1	Failure rate less than or equal to 1 in 100 000 years.
2	Failure rate is more than 1 in 100 000 years and less than or equal to 1 in 30 000 years.
3	Failure rate is more than 1 in 30 000 years and less than or equal to 1 in 10 000 years.
4	Failure rate is more than 1 in 10 000 years and less than or equal to 1 in 3 000 years.

[1] Numbers in square brackets refer to the Bibliography.

EXAMPLE 2 This example is for a railway application. The following scale for hazard potential (i.e., severity) from railway industry is roughly based on the square root of 10 which is approximately 3.

Severity rating (S)	Description
1	Insignificant hazard potential, no injuries expected.
2	One person with minor injuries.
:	:
6	Critical, one fatality or many persons with severe injuries.
7	Catastrophic with several fatalities.
8	Catastrophic with many fatalities.

EXAMPLE 3 This example is for a railway application. The following scale for avoidance of consequences (i.e., detection) from railway industry is roughly based on the square root of 10 which is approximately 3.

Detectability rating (D)	Description
1	Avoidance of consequences is almost always possible, for instance by means of an independent technical system.
2	Avoidance of consequences is frequently possible due to favourable conditions.
3	Avoidance of consequences is only sometimes possible due to unfavourable conditions.
4	Avoidance of consequences is virtually not possible.

Sometimes the scales for severity, likelihood of occurrence, or detection do not have a value readily associated with each point on the scale (in addition to a descriptive sentence). In this case the analyst should still make sure that adjacent levels are approximately a fixed multiple in relation to each other. This can be done by means of judgement taking into account that an increase or decrease by one level should mean an increase or decrease of, for example, the degree of severity or likelihood of detection by a multiple of 10 or the square root of 10, depending on the chosen multiple.

Having established the parameters for a failure mode, it is appropriate to add the levels of the parameters S, O and D for a failure mode rather than multiply them, as the calibrated parameter scales are effectively logarithmic. Thus:

$$\text{ARPN} = S + O + D$$

Analogously to B.4.2, the failure modes may then be ordered with respect to their ARPN and higher priority is usually assigned to a higher ARPN. In addition to the magnitude of the ARPN, the decision for treatment may be influenced by the severity of the failure mode, meaning that if there are failure modes with a similar or identical ARPN, the failure modes that are to be addressed first are those assessed to have high severity.

NOTE 1 In some applications, effects with an ARPN exceeding a defined threshold are not acceptable, while in other applications, the high importance is given to the high severity values, regardless of the ARPN value.

The APRN approach satisfies the requirements for a continuous scale for criticality and for a monotonic mapping of the risk associated with each failure mode to its RPN number. Moreover, small changes in the levels of the criticality parameters only lead to small changes in the resulting RPN, meaning that the ARPN is less sensitive than the RPN (B.4.2). It should be noted that the ARPN values are usually lower than those from the RPN method for the same input values of the criticality parameters.

EXAMPLE 4 An identified failure mode that is still considered acceptable might have the corresponding levels S = 5, O = 5 and D = 5 and would produce an RPN equal to 125 with the commonly used RPN method. With the alternative RPN method, this would result in an ARPN of 15.

NOTE 2 Where quantitative data is available for all three parameters it can be more appropriate to simply calculate the risk directly by multiplying the values rather than set up semi-quantitative bands.

Annex C
(informative)

Example of FMEA report content

C.1 General

Annex C illustrates how one example analysis, for a power supply unit, can be reported in different formats by creating worksheets and diagrams from a database information system.

In general, the full report should state the objectives of the analysis and describe the outcome of the analysis consistent with the objectives. Since the examples in Annex C are FMEA worksheets and diagrams generated from a database, they form only a part of the FMEA report (5.2.5.2). A complete FMEA report requires that the information described in 5.2.5.2 should be included so that the report can be understood by those persons other than those involved directly in the analysis. The additional information can be reported on separate sheets of the FMEA report.

Additional examples of forms of worksheet for different applications of FMEA are given in Annex F. There is no single reporting format because the FMEA report will depend on the objectives and context of analysis.

NOTE 1 The actual reporting format used can be different from the formats shown in the examples.

Commercial software packages exist to generate reports on the results of an FMEA.

NOTE 2 Spreadsheets can be useful for simple analysis with few participants. A relational database to manage several relationships between failure modes, functions, items, components and failure causes can be useful for more complex analysis with multiple information sources and complex reporting requirements.

C.2 Example of generation of reports from a database information system for an FMEA of a power supply unit

Figure C.1 shows how a database information system might be structured. If a database information system is available, then the FMEA can be a file that links the following databases:

- list of specifications;
- parts list (bill of material);
- list of failure modes relevant for the components and products of the company;
- list of potential treatment actions (action database).

An advantage of using a database is that information does not have to be entered several times and that it is easier to keep the FMEA updated as the project progresses and changes occur.

The full set of fields for FMEA reporting that can be populated from this database information system are shown in Table C.1 for the example of the power supply shown in Figure C.2. By selecting different combinations of fields, different FMEA worksheets (Table C.2 to Table C.5) and diagrams (Figure C.3) can be generated.

For the power supply example, this FMEA evaluates the possible impact of a failure within the device on the user only. The results shown are valid under all ambient conditions as given in the data sheet. This FMEA only reflects dangers arising within use, and not in other phases within the product life cycle.

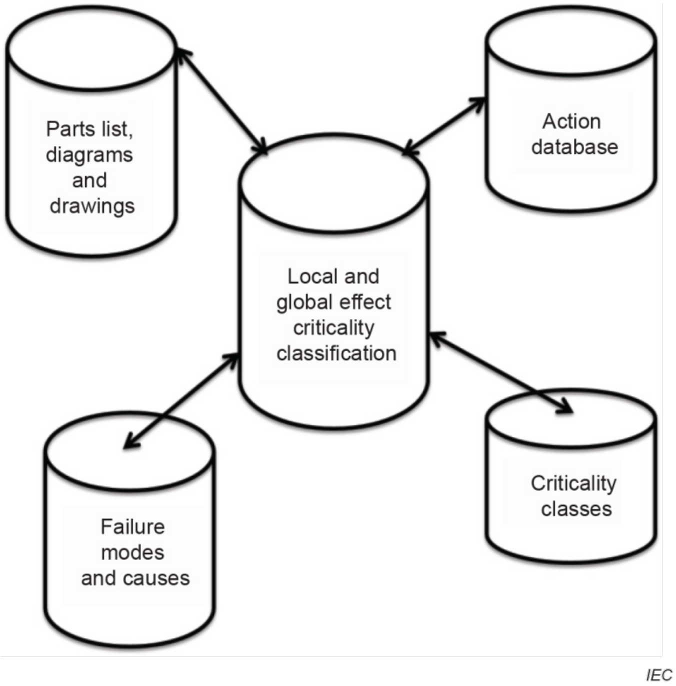

Parts list, diagrams and drawings
Action database
Local and global effect criticality classification
Criticality classes
Failure modes and causes
IEC

Figure C.1 – Database information system to support FMEA report generation

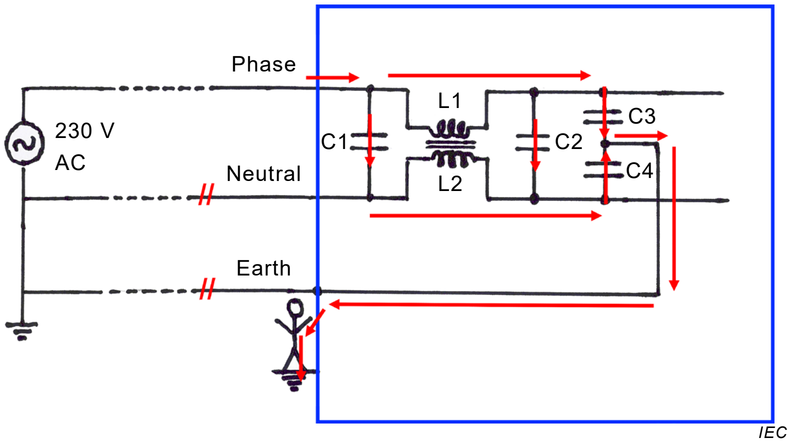


Figure C.2 – Diagram of power supply type XYZ

Table C.1 – Example of fields selected for FMEA report of power supply based on database information

FMEA report description	Item drawing	Component FMEA	Parts FMEA	FMECA with RPN	FMECA with criticality matrix	
	Figure C.2	**Table C.2**	**Table C.3**	**Table C.4**	**Table C.5**	**Figure C.3**
Case No.					Row	
Components			Row	Row	Column	
Parts list		Row				
Failure modes		Column	Column	Column		
Local effect						
Global (final) effect			Column	Column	Column	
Severity			Column	Column		
Occurrence				Column		
Detectability				Column		
Possible CCF		Column				
Treatment actions (from action database)			Column			
Definitions of severity						
Definitions of occurrence						
Definitions of detection						
Links to reports			Column			
Diagram/Drawings	Yes					
Criticality matrix						Yes
Fault tree analysis						

Key

Row (Column) indicates field selected and to be shown in FMEA report row (column).

Yes indicates figure type selected.

NOTE The second row of this matrix refers to the subsequent different FMEA worksheets (tables) and criticality matrix (figure) given in Annex C.

Table C.2 – Example of report of component FMEA

FMECA report No. XX Date: yyyy.mm.dd Last update: yyyy.mm.dd

Product analysed: power supply type XYZ

Facilitator: NN1

Analysis team: NN2, NN3, NN4, NN5, NN6, NN7

Approved by: NN8

Component	Failure mode	Global effect	Severity	Action due date	Link to reports (click on icon to see report)
C1	s/c	Supply does not work	2	None	NA
C2	s/c	Internal fuse blows Supply does not work	2	None	NA
C3	s/c	230 V on cabinet	4	NN3 yymmdd	Icon-Report on safety capacitors
C4	s/c	230 V on cabinet	4	NN3 yymmdd	Icon-Report on safety capacitors
L1	o/c	Supply does not work	2	None	NA
L2	o/c	Neutral disconnected Supply does not work	4	NN4 yymmdd	Icon-Report on L2 Failure probability
Power switch-Phase	o/c	Supply does not work	2	None	NA
Power switch-Neutral	o/c	Neutral disconnected Supply does not work	4	NN4 yymmdd	Not due yet
Power switch-Earth	o/c	Neutral disconnected Supply does not work	4	NN4 yymmdd	Not due yet
Solder	o/c	Neutral disconnected Supply does not work	4	NN5 yymmdd	Icon-Report on solder durability testing

NOTE Severity can rank from affected user experience to health hazards. Within this FMEA, the decision on actions taken was solely based on a severity ranking.

Table C.3 – Example of report of parts with possible common cause failures

FMECA report No. XX Date: yyyy.mm.dd Last update: yyyy.mm.dd

Product analysed: power supply type XYZ

Facilitator: NN1

Analysis team: NN2, NN3, NN4, NN5, NN6, NN7

Approved by: NN8

Parts list line-Type-Manufacturer	Designation	Failure mode
#15-Capacitor –Type XYZ, Value XYZ, Voltage XY, Supplier XYZ	C1, C2, C3, C4	s/c
#71Coil-Type XYZ, Rating XYZ, Supplier XYZ	L1, L2	o/c
#83 Switch-Type XYZ, Rating XYZ, life expectancy XYZ, Supplier XYZ	Power switch	o/c

This list was generated from a parts list and shows, which failure modes were found necessary to be treated within an application. This selection is usually done for a certain type of devices developed by a company and the information how these were chosen (5.3.4) needs to be available and connectable to this report.

NOTE This example lists components of the same type with the same failure mode. Often the root causes of the failure modes are not analysed during a basic FMEA. Therefore examining the database to identify components where a common cause is possible might help and save time when searching for possible common cause failures.

Table C.4 – Example of report of FMECA using RPN criticality analysis

FMECA report No. XX Date: yyyy.mm.dd Last update: yyyy.mm.dd

Product analysed: power supply type XYZ

Facilitator: NN1

Analysis team: NN2, NN3, NN4, NN5, NN6, NN7

Approved by: NN8

Severity	Occurrence	Detectability	RPN	Component	Failure mode	Global effect
4	3	5	60	L2	o/c	Neutral o/c – Indicator lamp “ON”
4	3	5	60	Solder joints	o/c	Neutral o/c – Indicator lamp “OFF”
4	2	5	40	Switch neutral	o/c	Neutral o/c – Indicator lamp “OFF”
4	3	3	36	C3	s/c	230 V on cabinet
4	3	3	36	C4	s/c	230 V on cabinet
3	2	5	30	Switch earth	o/c	No safety earth
2	3	1	6	C1	s/c	Supply does not work
2	3	1	6	C2	s/c	Supply does not work
2	2	1	4	Switch phase	o/c	Supply does not work
2	2	1	4	L1	o/c	Supply does not work

NOTE This FMECA has been created to evaluate an RPN. It is based on an updated circuit that also includes a power switch that switches all three supply contacts and an indicator lamp that signals that the device was switched on.

Table C.5 – Example of report of FMECA using criticality matrix for global effect

FMECA report No. XX Date: yyyy.mm.dd Last update: yyyy.mm.dd

Product analysed: power supply type XYZ

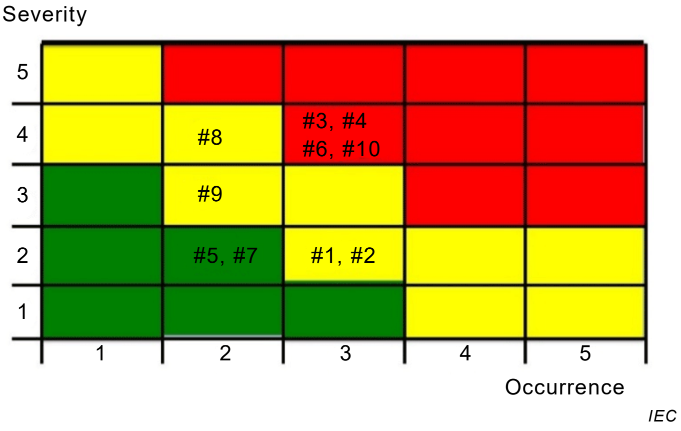
Facilitator: NN1

Analysis team: NN2, NN3, NN4, NN5, NN6, NN7

Approved by: NN8

Line No.	Component	Global effect
#1	C1	Supply does not work
#2	C2	Supply does not work
#3	C3	230 V on cabinet
#4	C4	230 V on cabinet
#5	L1	Supply does not work
#6	L2	Neutral not connected – Supply does not work
#7	Power switch – Phase	Supply does not work
#8	Power switch – Neutral	Neutral not connected – Supply does not work
#9	Power switch – Earth	Neutral not connected – Supply does not work
#10	Soldering	Neutral not connected – Supply does not work

NOTE This example of report shows the same safety function included in a criticality matrix. The plot was created as two dimensional image without taking credit from detectability for the evaluation of the impact on the user.



Severity					
5	🟨	🟥	🟥	🟥	🟥
4	🟨	🟨 #8	🟥 #3, #4 #6, #10	🟥	🟥
3	🟩	🟨 #9	🟨	🟥	🟥
2	🟩	🟩 #5, #7	🟨 #1, #2	🟨	🟨
1	🟩	🟩	🟩	🟨	🟨
	1	2	3	4	5
				Occurrence	

Figure C.3 – Criticality matrix for FMECA report in Table C.5 created as a two dimensional image without taking into account detectability

Annex D
(informative)

Relationship between FMEA and other dependability analysis techniques

Combining FMEA with other dependability analysis methods can increase its effectiveness. For example:

- To define the scope and aid development of an FMEA, a reliability block diagram (RBD) of the system can be useful. The results of the FMEA might be used subsequently to revise or update the RBD.

  NOTE 1 Unlike the FMEA, the analysis viewpoint of an RBD is system success.

- To select the important items of a complex system for an FMEA, a fault tree analysis (FTA) with a suitable top event can be used to identify the items of the system to be analysed.

  NOTE 2 Similarly to the FMEA, the analysis viewpoint of an FTA is system failure.

- The results of a (lower level) FMEA can identify basic events for the FTA and these events should be included as basic events of the FTA.
- Information from a root cause analysis can support identification of failure causes for a process (IEC 62740).
- To supplement FMEA, which normally only considers independent failures, more detailed analysis methods such as FTA, RBD, event tree analysis (ETA), Markov analysis or Petri nets can be used to address interdependency of failure events such as their order of appearance, conditional probability of occurrence, redundancy, exclusiveness of occurrence, common cause failures.
- FMEA can be used incrementally in combination with other dependability analysis techniques during the development of an item or process. At the concept stage, FMEA can be combined with RBD and FTA to consider failures at a function level. During detailed design, the FMEA can be developed at a more detailed level. For selected critical components or processes, an FMEA at the most detailed level can be carried out.
- Reliability prediction and analysis of test results or failures in the field can be used to support quantification of likelihood in an FMEA.

  NOTE 3 The references to other dependability analysis standards that might be applicable are: RBD (IEC 61078); FTA (IEC 61025); ETA (IEC 62502); Markov analysis (IEC 61165); Petri nets (IEC 62551); for reliability prediction see IEC 61709 and IEC 62308.

The results of an FMEA provide information on the critical aspects of a complex item or process design and during the development process might be used as input to or can be combined with:

- maintenance analysis;
- troubleshooting tactics during maintenance;
- testability analysis;
- definition and specification of test cases and analysis of test results;
- logistic support analysis;
- mission reliability analysis;
- availability analysis;
- evaluation of the consequences of design changes;
- documentation for regulatory purpose (e.g. safety approval for a specific system or for a certain type of systems).

Annex E
(informative)

Application considerations for FMEA

E.1 General

Annex E considers common applications of FMEA and specific issues to be considered when conducting an FMEA according to the general methodology given in this document and the guidance for tailoring given in Annex A. The applications discussed are not exhaustive.

The applications discussed might have certain requirements regarding the criticality analysis (e.g. safety), or might ensure compatibility with specific standards (e.g. FMECA within reliability centred maintenance). Consideration is also given to the use of FMEA for complex systems (e.g. reliability and availability allocation across modules and components).

E.2 Software FMEA

Software FMEA is similar to FMEA for hardware or procedures and addresses functions. For software, the following conventions establish that:

- software error is a mistake in the software code,
- software fault is an issue with procedure/function executions,
- software failure is total or partial degradation of the specific software function.

Design defects in software (popularly named “bugs”) can cause software to fail. The consequences of such a failure for the software functions and the software output can be analysed as for any other item. The probability of failure can be estimated as the number of times the function containing a “bug” is activated divided by the total number of function executions, but since this information is seldom available, quantitative analysis is rarely possible. Fault states in software are often intermittent and some fault states can be repaired by resetting the software. All software faults are design related whether they originated from incorrect interpretation of requirements, error in codes, insufficient memory, open loops, syntax errors, etc.

Software can be analysed top-down or bottom-up. Like hardware, the software is broken down in different levels, for example, software package, software modules and executable code functions (Table 1). For each element, the analysis should consider the input, the processing and the output. The processing depends on the initial conditions before the input for example position in a menu structure, contents of registers and memories (RAM as well as ROM). In lower levels, faults can occur in inputs (for example, illegal or corrupted data), in initial conditions (for example, wrong position in menu, incorrect or corrupted content of memories) or wrong processing (for example, in algorithms). System level failures are often associated with the output (for example, corrupted output or invalid data). Finally, the software output can cause problems interacting with the hardware, for example timing problems. The analysis typically focuses on failure modes related to software, however failure causes, measures and effects may be related to the relevant hardware. Therefore, analysts who know the software as well as analysts who know the hardware should participate together in the analysis.

The depth and breadth of the software FMEA may vary. FMEA can be limited to the software components or modules only. When started early in software development, this FMEA may focus on the software functions that are required for system operation and the potential error or faults that could be the causes of a function failure in one or more of its failure modes. Such analysis is done at the beginning of the software development and is used as the source of information for creation of the software test cases. As the system design progresses, the effect of software errors, faults or failures can be defined better as well as the circumstances or their combination that would trigger the failure event.

The root causes of the failures can include errors by the programmer ("bugs") as well as hardware causes. To make an FMEA there is a need to determine whether any single failure in the software can cause an unacceptable local effect (besides final/global effects), for example:

- a variable assumes an unexpected value;
- a message carries unexpected data or unexpected timing;
- a module produces unexpected outputs.

The FMEA then analyses each failure mode for system (final) effects. It is rule based and complex, since the effects depend on time and state. Before a software FMEA is performed, a separate analysis should be made on the requirement specification. Since software error or fault often result in undesired hardware effects, a hardware FMEA should be done first to establish system effects. Software system effects can then be based on hardware system effects.

The following list is based on examples given in Ozarin (2016) [29]. Software FMEA also have to consider the operating conditions, for example:

- memory hardware failures;
- memory mapped peripheral failure (e.g. analogue/digital converters or I/O devices);
- power supply failure, for example reset due to drop in supply voltage;
- electromagnetic interference (EMI), electromagnetic pulse (EMP);
- improperly handled bad input data, including bootloading errors.

Examples of system level failure causes are:

- improper use of operating system calls;
- timing, for example data collision due to change in propagating time;
- interrupted handling and inadequate analysis;
- inadequate or absent exception handling.

Examples of programming errors (failure causes) are:

- design and implementation errors (e.g. coding, scaling, algorithms);
- inadequate error detection (e.g. boundary violations, out-of-range pointers);
- inadequate valid range detection;
- unintentional overwriting in memories;
- inadequate software error handling (e.g. an unexpected case).

Examples of failure modes are:

- incorrect exit point, time overrun, unexpected I/O interaction;
- missing data, incorrect data, timing of data, extra data;
- abnormal termination, omitted events, incorrect logic, timing/order;
- stop, crash, hang, slow response, start-up failure, faulty messages.

When the analysis is performed using a spreadsheet, the following columns might generally be used:

a) hierarchical system and components;

b) component designators;

c) failure modes;

d) failure causes;

e) consequences of unavailability of failed function (when the software is repaired);

f) mitigating design provisions (design recovery measures, alternate paths, fault protection);

g) compensating provisions;

h) closure of the issue;

i) final reduced unavailability of function resulting from the identified failure mode.

Figure E.1 shows an example of software failure model.

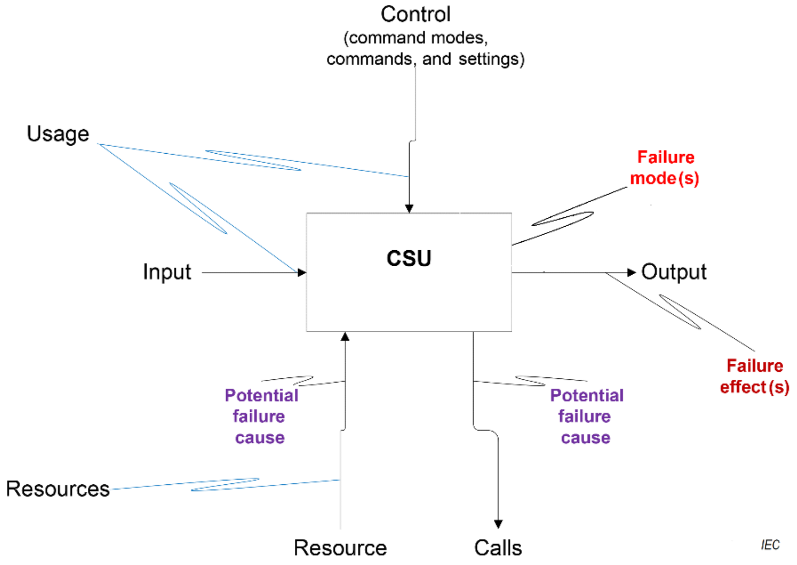


Figure E.1 – General software failure model for a component software unit (CSU)

When the hardware design progresses, the analysis views the system as a whole, containing software and hardware and the analysis addresses the system functions and their chains.

When a hardware FMEA is amended by a software part, the analysis may grow to unwanted proportions while searching for the chain of effect leading to system failure and evaluating the degree of their degradation or severity of their loss on system performance. A preferred practice when analysing the mixed hardware/software system is to follow the system function down the branches to identify component software units (CSUs), their potential error(s) or fault(s) and identify potential failure modes as well as the potential causes.

It should be remembered that FMEA addresses only one failure mode at a time; it is not meant to address functional dependencies, sequences of events (failures), or the combinations of events. Hardware failure may cause the software failure, but in view of FMEA, the software failure is then the effect of the hardware failure.

Software FMEA is one method (besides testing) that helps to improve software reliability. Testing may also be a treatment for failure modes that are considered critical.

E.3 Process FMEA

For processes and procedures, the general FMEA methodology is the same as for hardware and software items. The starting point for the analysis is the process flow diagram, work breakdown structure or task analysis. The process is sub-divided into elements which are the steps of the process. The level of decomposition is selected to suit the application. The function of each step or its intended outcome is defined with the description of function sufficiently specific that the level of performance that constitutes failure is clear. As with

FMEA for hardware and software items, the ways in which the process function could fail to be achieved are listed as failure modes in the process FMEA. Failure effects, mechanisms and possible failure causes are also defined. Failure mechanisms and causes often involve both human and hardware failures. Criticality analysis can be applied in the same way as described in the general guidance for FMEA.

Process FMEA was first applied to manufacturing processes but is now used more widely. For example it has widespread use in analysing medical procedures in healthcare.

E.4 FMEA for design and development

The FMEA is an essential part of the design process, from concept through to development of complex systems. The FMEA is iterative and initiated as soon as preliminary design information is available at the system top level and extended to the lower levels of the system hierarchy as more information becomes available. Tailoring of the FMEA (Annex A) should ensure that it contributes meaningfully to organizational decisions, such as feasibility and adequacy of a design approach.

The objective of an FMEA during design is to identify the modes of failure within a system and the potential critical failures which can be eliminated, or reduced by, design action at the earliest possible time.

In addition to the focus on reliability, the FMEA supports the maintainability and supportability efforts, and risk analysis.

E.5 FMEA within reliability centred maintenance

The ability to develop a successful maintenance programme using reliability centred maintenance (RCM) requires a clear understanding of the item functions, failures and consequences expressed in terms of the organization’s objectives in operating the item.

The FMEA and criticality method are suitable for application to RCM if the analysis is structured in such a way as to conform to the requirements of the RCM standard (IEC 60300-3-11).

The structuring of the analysis requires that all failure modes shall be clearly linked to loss of function at an appropriate level in the item hierarchy and that aspects such as “means of detection” address potential maintenance tasks.

E.6 FMEA for safety related control systems

E.6.1 General

Safety applications use FMEA in various contexts. The FMEA method is one alternative when planning a safety related function or analysing risks.

EXAMPLE 1 Some standards (e.g. IEC 62061 and IEC 61508 (all parts)) require certain forms of analysis when establishing appropriate risk treatments in applications, when creating safety related functions or in the development of devices for use in such functions. An FMEA is one method which can be used when planning a safety related function.

Safety applications of FMEA classify failure modes of a safety function as either safe or dangerous. The classification may be different for a change in usage conditions, system structure or environment.

EXAMPLE 2 Many systems have a de-energized state (shutdown state) as safe state (invariable safe system state). A failure of an aircraft’s braking system design can be considered to be a safe failure when the aircraft is on the ground, but it might change to be a dangerous failure during take-off or landing (variable safe system state, see Yoshimura and Sato, 2008 [30]).

Some safety standards require that single faults should be detected so that they lead to the safe state or to keep the safe state i.e. by functional redundancy. An FMEA provides a systemic means to prove that no single fault directly leads to an unsafe condition.

In prioritizing action in a safety application, design actions should primarily consider the failure effects and should not use an economic trade-off. Therefore, if design action is required, features should, for example, aim to:

- reduce the likelihood of a dangerous failure;
- recognize, or detect, the dangerous failure occurring and react to it accordingly;
- signal the safety status of the device to the user;
- eliminate, or reduce, the probability of a failure caused by human error or misunderstanding.

E.6.2 FMEA in planning a safety application

An FMEA can be applied at the system level during the planning phase of the development of a safety application. The failure modes and effects of all components of a system and their interaction are evaluated systematically to determine their influence on the safety of the system.

An FMEA can also be applied at other points in a project where identifying risks and analysing their influences on a safety related function can be used to determine treatments to improve safety. The purpose of an FMEA involving safety topics is to find all the items involved in the safety function and to comprehensively identify the sources of harm. Methods to aid comprehensive identification include checklists, research and the use of wide ranging expert opinion.

A measure of risk based on the severity of harm and a qualitative assessment of its probability is used to define the required safety integrity of safety related, electrical, electronic and programmable electronic control systems as given in IEC 62061.

The probability of harm takes into account:

- the frequency and duration of the exposure of persons to the hazard;
- the probability of occurrence of a hazardous event;
- the ability to avoid or limit the harm.

These three factors are – along with the severity level – used to produce a class for the necessary risk reduction for an application. These classifications are used in several safety related standards.

NOTE IEC 61508 (all parts) and IEC 62061 use the term SIL (safety integrity level) for this classification.

EXAMPLE In IEC 62061 the highest category of risk reduction requires SIL3, which is equivalent to a failure rate of the safety control function between 10^{-8} to 10^{-7} per hour.

E.6.3 Criticality analysis including diagnostics

A further level of detail is added within the so-called failure modes, effects and diagnostic analysis (FMEDA).

NOTE 1 The FMEDA method is also used for non-safety related systems.

The ability of the system or subsystem to detect internal failures, preferably via automatic on-line diagnostics is crucial in achieving and maintaining correct function in complex systems and for systems that might not be fully exercising all functionality under normal circumstances, such as a low demand emergency shutdown system (ESD system). Where safety relevant integrity of a system is evaluated, quantitative failure rate data (failure rates and the distribution of failure modes) is added for all components being analysed. Additionally, the ability of the system to detect internal failures is determined and quantified.

Where the components under analysis are electronic devices, failure rates should have appropriate accompanying documentation to justify their derivation, ideally from operating field experience. Failure rates for each component are derived from databases that are proven to be appropriate for the given purpose. Additionally, the failure mode distributions can be derived from similar sources or from standards (e.g. IEC 61709), their values generally being given as a percentage of the total.

NOTE 2 The failure rates are often given in FIT (failure in time), denoting 10^{-9} per hour.

NOTE 3 In this context, 'failure mode distributions' refers to the proportion of the total component failure rate which can be assigned to each of its failure modes.

In many cases, failure rates for failures that have no effect on the safety function or failures of parts that are not part of the safety function are also given but have no effect on further calculations.

When evaluating an electronic device, the analysis considers each electrical component and its influence on the safety function, making it possible to conclude what effects a failure has on the safety function.

The effects are normally divided into safe failures, dangerous detected failures, dangerous undetected failures and failures which have no effect on the safety function. To check the completeness of the evaluation it is sometimes appropriate to list components that do not influence the safety function.

The decision as to whether a dangerous failure is regarded as detected or undetected is determined by a diagnostic coverage value that might be derived from specific diagnostic circuit parts and their estimated efficiency. The values are summarized subsequent to the evaluation and represent the quality of the device for use within the safety function. The resulting figures may also be used to calculate failure rate or other reliability values for the safety function or other indicators of the quality of a safety function such as a safe failure fraction (SFF) or an overall diagnostic coverage (DC). The definitions of these characteristic values depend on the context for which they are defined.

The result is a rating of failure probability values that make it possible to estimate the overall risk related to the failure of a safety function in the event that a demand for it occurs.

Where there is insufficient information regarding the possible failure modes and distributions of an electrical component, an FMEA again is an appropriate method to collect information about possible failure modes. From this, practical experiments or theoretical discussions can be initiated to determine these values.

NOTE 4 This method and possibilities for fault exclusion are described in ISO 13849-1.

E.7 FMEA for complex systems with reliability allocation

E.7.1 General

FMEA can be used for complex and critical systems, from the defence and aerospace sector, to water, sewerage, transport, communications and power production and distribution. In these systems, dependability requirements in terms of availability, maintainability and reliability measures can be allocated to the procurable elements of the system. A tailored FMEA can be conducted to consider the failure characteristics of each element to understand the systemic effects of such design features as common components and the application of redundancy.

E.7.2 Criticality assessment for non-repairable systems with allocated unreliability

During an FMEA for a complex non-repaired system, occurrence frequencies, probabilities, rates, or other relevant failure related measures can be allocated to each effect at the system level. This allocation can be compared with the acceptable risk for the system and the allocated probabilities plotted against their effect severity in a form of matrix.

Local effects of each failure at the lowest level of the system hierarchy can be rolled up to increasingly higher level assemblies and finally to the system level. These actual risk assessments can then be compared to the agreed level of acceptable risks. Where the criticality exceeds the acceptable value, it should be traced to the part of the system from which it originates.

The assessed failure probabilities can be compared with the acceptable limits for each severity level to identify lower level assemblies or components with excessive criticality. Engineering actions are then taken to lower the criticality of components by lowering their probability of failure or by other measures for mitigation of their failure effects. This flow down process is shown in Figure E.2.

It is often assumed that if the criticality of a lower level component does not exceed the acceptable level then no action need be taken. This might not be the case when there are many similar components, which might cause the same effect on the subsystems or on the system. The total sum of failure probabilities of all those components having the same effect severity should not exceed the acceptable probability of failure for the assembly in which they reside. This measure would ensure that the defined criticality at the system level is not exceeded.

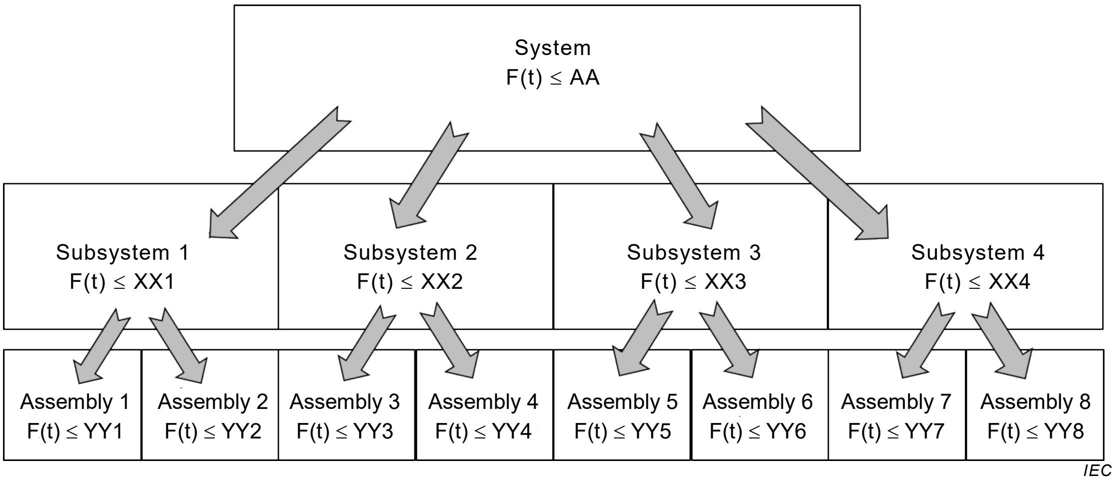


Figure E.2 – Allocation of system failure probabilities

E.7.3 Criticality assessment for repairable systems with allocated availability

Availability requirements for repaired systems are allocated to dependability measures such as the mean time between failures (MTBF) for reliability and mean time to restoration (MTTR) for maintainability of the system. System unavailability measures are usually used to assess system criticality. Assessing unavailability is similar to assessment of probability of failure (unreliability). Unavailability is allocated but this time, unavailability is a two dimensional entity because it depends on two measures, MTBF and MTTR.

The allocation process at the system, subsystem or assembly levels is similar to allocations discussed for non-repaired systems in E.7.2 except that, instead of using the probability of occurrence of the failure mode, the unavailability of the system, subsystem or assemblies resulting from the failure mode is plotted. Failure modes causing an unacceptable level of unavailability shall be treated.

Annex F
(informative)

Examples of FMEA from industry applications

F.1 General

Example extracts from FMEA worksheets are described together with a brief explanation of the application domain.

NOTE The example extracts are primarily for the FMEA worksheets and only brief descriptions are given of the application domain. This means that full consideration of the FMEA objectives and boundaries are not explained, even though they would have been core to the industry analysis upon which the examples are based.

F.2 Health process application for drug ordering process

An extract from an FMEA of the process of ordering a drug from a pharmacy is shown in Table F.1. The example shows one step of the process with specimen failure modes, effects and causes.

Table F.1 – Extract from FMEA of the process of ordering a drug from a pharmacy

Step of process	Function	Failure mode	Failure effect	Failure mechanism	Failure cause
Medication prepared	Medication with correct active ingredient and concentration prepared	Wrong drug	Depends on particular drug selected	Incorrect selection (correct intent) Misread prescription Prescription ambiguous	Products look alike Poor writing on prescription Use of abbreviations
		Wrong concentration	Overdose Under-dose	Calculation error Knowledge deficit Misread prescription	Distraction Poor writing on prescription Inexperience
		Wrong diluent	Possible toxicity from diluent	Incorrect selection (incorrect intent) Incorrect selection (correct intent)	Lack of knowledge Unavailability of correct diluent Look alike products

F.3 Manufacturing process application for paint spraying

An extract from an FMEA of the paint spraying step of a manufacturing process is shown in Table F.2. The example shows one step of the process with specimen failure modes, effects and causes.

Table F.2 – Extract from FMEA of paint spraying step of a manufacturing process

Step of process	Function	Failure mode	Failure effect	Failure mechanism	Failure cause
Spray paint	Apply smooth film of 75 microns	Paint too thick	Poor appearance Article reject	Too much paint	Spray gun too close Failed paint regulator
		Orange peel effect	Poor appearance	Paint droplets dry before they coalesce	Too little air Factory temperature too high Fan pattern too wide Gun distance too large

F.4 Design application for a water pump

F.4.1 General

The following is a simple example of an FMEA to highlight the information which should be included for each step of the analysis for a single water pump with a design flow rate of 600 l/min which provides cooling water to a heat exchanger. A flow rate of 400 l/min provides the ideal cooling conditions. The analysis is presented as a narrative, but might be recorded in any suitable tabular or database format.

F.4.2 Item function

The pump functions are to:

1) provide water at a rate of 400 l/min ± 30 l/min to the primary heat exchanger;
2) contain water with a leakage rate less than 0,01 l/h.

NOTE The pump has additional design capability in order to ensure that it provides the required service (strength versus stress criteria). In this context, if the pump does not achieve its full design capacity, output below maximum might not represent loss of function.

F.4.3 Item failure modes

The pump failure modes for function 1 are:

A. provides water at a rate less than 370 l/min to the primary heat exchanger;
B. provides water at a rate greater than 430 l/min to the primary heat exchanger.

The pump failure modes for function 2 are:

A. permits water leakage at a rate greater than 0,01 l/h but less than or equal to 1 l/h;
B. permits water leakage at a rate greater than 1 l/h.

NOTE Failure modes are often simply the opposite of the required function, as for function 1, but can often be extended to include specific levels at which the function is lost as in function 2. This is normally only of value if there are different consequences associated with each level.

F.4.4 Item failure effects

The failure effects of pump failure mode 1A are:

- local: None;
- final: Process shut-down (due to insufficient cooling).

The failure effects of pump failure mode 1B are:

- local: None;
- final: Product out of specification (due to excessive cooling).

The failure effects of pump failure mode 2A are:

- local: None;
- final: Chemical contamination (water evaporates in bund releasing dosing chemicals).

The failure effects of pump failure mode 2B are:

- local: None;
- final: Process shutdown (bund overflows, damage to electrical equipment).

NOTE As a result of this analysis, a level alarm might be placed in the bund. Analysis of such an alarm would show that its failure has no consequence in itself, but would result in process shutdown if pump leakage occurred.

F.5 Example of an FMEA with criticality analysis for a complex non-repaired system

This example uses the unreliability values as the measure of failure likelihood. Figure F.1 shows the hierarchical structure of an electronic system consisting of four subsystems in series where each of the subsystems has two circuit card assemblies (CCAs) with various electronic components also in series. Figure F.1 also shows the allocation of unreliability values at the system, subsystem and assembly levels.

Table F.3 shows the allocation and assessment of unreliability values for different critical categories of failure modes for this system. The information in Table F.3 indicates that the failure modes in categories III (Major) and II (Critical) exceed the acceptable levels and need to be addressed. To find out which of the subsystems/assemblies contribute most to the problem, the unreliability allocation to the sub-assemblies/assemblies is reviewed.

As an example, Table F.4 shows the allocation and assessment of unreliability values for subsystem 2. The information in Table F.4 indicates that the failure modes in the major and critical categories exceed unreliability allocations. The conclusion is that mitigation of critical and major failure modes in subsystem 2 is required to reduce the system unreliability of failure modes in assemblies 3 and 4 to bring the system criticality within allowable risk limits.

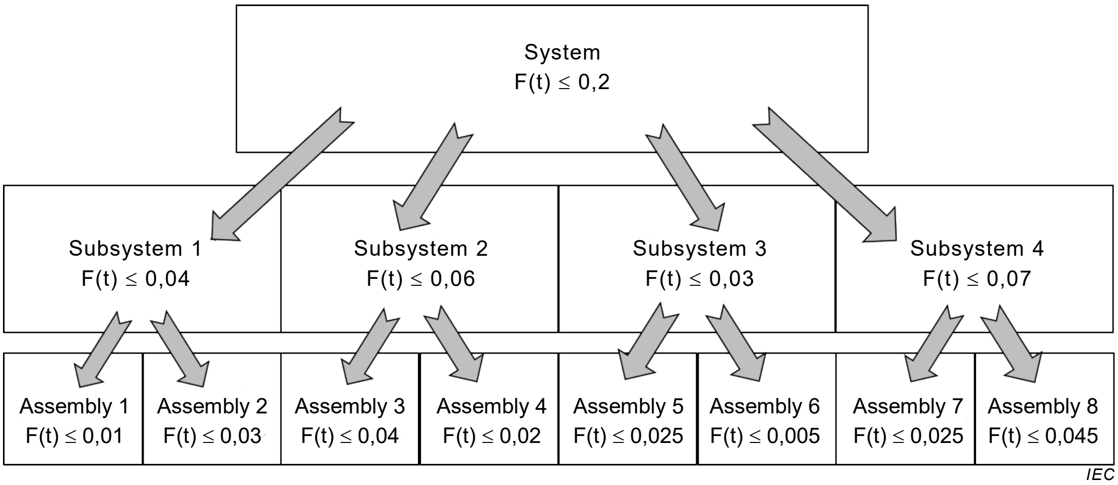


Figure F.1 – Hierarchy of a series electronic system, its subsystems and assemblies with allocated unreliability values, F(*t*)

Table F.3 – Allocation and assessment of unreliability values for different criticality categories of failure modes for the electronic system represented in Figure F.1

	V Negligible	IV Minor	III Major	II Critical	I Catastrophic
Allocation of unreliability	≤ 0,1	≤ 0,08	≤ 0,012	≤ 0,007 2	≤ 0,000 8
Assessment of unreliability	0,06	0,05	0,03	0,01	0,000 2

Table F.4 – Allocation and assessment of unreliability values for different criticality categories of failure modes for subsystem 2 of the system represented in Figure F.1

	V Negligible	IV Minor	III Major	II Critical	I Catastrophic
Allocation of unreliability	≤ 0,03	≤ 0,02	≤ 0,005 2	≤ 0,004 7	≤ 0,000 07
Assessment of unreliability	0,006	0,002 1	0,029	0,008	0,000 02

This allocation and assessment of unreliability would be completed for the four subsystems and associated assemblies. Where unreliability is unacceptable, action can be taken to improve reliability for those assemblies and achieve a balanced outcome. Following this action and the identification of the new assembly performance, these assembly values can be rolled up progressively to the sub-assembly level and finally to the system level using the mathematics of a reliability block diagram or a fault tree. Care should be taken when identical components are used at the assembly level, to identify potential for common mode failures in those components.

F.6 Software application for a blood sugar calculator

Table F.6 illustrates an FMEA for a blood sugar calculator showing the failure modes, causes and local effects. This shows how the steps of using the monitor and the different components used are considered in turn to identify failure modes, effects and causes for these devices. One very important failure mode of a blood sugar calculator is that a reset of the microprocessor will cause the software to return to the factory setting. If the factory settings are in US units and the user had changed these to European settings then a life threatening mistake is likely.

F.7 Automotive electronics device

In Table F.7, a small part of an extensive FMEA performed for an automotive air-bag product is presented. The assembly analysed is the power supply, and its connections to the battery line only, as per Figure F.2.

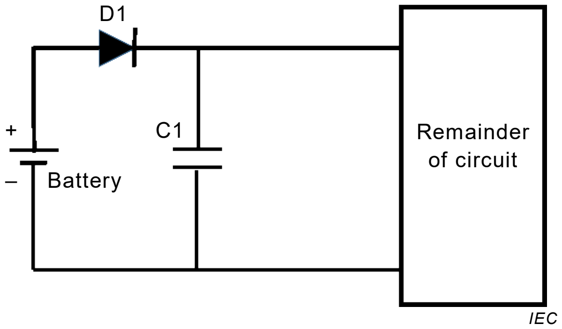


Figure F.2 – Automotive air-bag part

The circuit has a diode D1 in line with the positive terminal of the battery and a capacitor C1 connecting the positive line to ground. D1 is installed such that if the battery is connected in reverse no current could flow into the circuit. C1 is provided for filtering.

If C1 should short circuit, the positive side of the battery would become directly connected to ground, which would cause D1 to burn out due to excessive current flow and result in an open circuit of D1. The air-bag circuit would then be inoperable. Such a failure is considered dangerous, resulting in a severity rank S = 10. Occurrences were calculated from the parts failure rates under their respective stresses for the vehicle life, and then matched to a 10 point occurrence scale, resulting in a selection of O = 3. Detection was considered to be low because if the failure occurs during driving there will be no indication to the driver, resulting in a selection of D = 10.

Furthermore, an open circuit in either connection of C1 would allow the air-bag circuit to continue to operate but would affect the ability of C1 to filter the power input to the circuit. An open circuit fault of D1 would also render the air-bag circuit inoperable as no current can flow from the battery. A short circuit fault of D1 would allow the air-bag circuit to continue to operate, but there would be no reverse battery protection.

In the FMEA in Table F.7 the columns “recommended action", "responsibility and target completion date" as well as "treatment action results" have not been filled out. This reflects the situation where the FMEA team delivers a partially filled FMEA to the project team. The project team then has to address the risks and come up with proposed actions and due dates. The FMEA can then be completed by filling out the columns “treatment action results".

F.8 Maintenance and support application for a hi-fi system

A remote control is a small device that allows the user to control a hi-fi system from a distance by infrared or radio communication. The purpose of the example is to show how different FMEAs can be applied to the same product. A very simple product has been chosen as an example and the different FMEAs have been shortened extensively to save space.

Examples of a system FMEA, a design FMEA, a process FMEA and a maintenance service FMEA for the same item – a remote control for a hi-fi system are shown in Tables F.8 to F.11 respectively. The system FMEA is made early in the project in order to consider the general top level lay-out (architecture) of the product. The design FMEA looks at the design solutions. The process FMEA addresses the manufacturing processes, while the service FMEA addresses the ease of repairing the product (maintainability).

This example illustrates the differences between these types of FMEA for the same item. The priority index used is the RPN.

F.9 Safety related control system applications

F.9.1 Electronic circuit

An FMEA is conducted for the evaluation of risks connected to the user interface of a safety product. An example for a failure modes, effects and diagnostic analysis (FMEDA) is given that evaluates an electronic circuit. The example is not complete; it determines the failure modes, effects and diagnostic capabilities of the main parts of a power supply circuit that uses a linear regulator for internal supply voltages in a device. The extract from the FMEDA is shown in Table F.12.

F.9.2 Automated train control system

An automated train control system is an on-board system that brings a train to a stop and keeps it stopped in case the track is occupied by a further train to avoid a collision. If the stop signal is given within a tunnel, it is necessary that the train can still be moved so that, in case a fire on the train causes a hazard, persons on the train have sufficient escape possibilities. For this FMEA, the risk to the health of passengers is considered.

If an automated train control system fails to stop the train when required, a collision may occur. On the other hand, it is dangerous if the automated train control system fails to allow the train to move from the tunnel in case of fire.

Those collision and fire hazards are mutually reciprocal hazards because in one case it is right to stop the train while in the other case it is a problem.

Table F.5 shows the relationship between the failure modes of the automated train control system, hazards, and safe and dangerous failures.

Table F.5 – Hazards and safe/dangerous failures in an automated train control system

Hazards to be controlled by an automated train control system	Failure modes of an automated train control system	
	Failure mode 1 (e.g., short–circuit)	Failure mode 2 (e.g., disconnection)
Fail to avoid collision	Dangerous failure	Safe failure
Fire in a tunnel	Dangerous failure	Dangerous failure

F.10 FMEA including human factors analysis

Table F.13 shows an FMEA for the process of using a coffee-maker (Masuda, 2003) [28]. In this FMEA, human behaviour and the associated risks are evaluated. This includes an analysis of the possible interaction between the involved person, equipment and the environment to derive failure modes and mitigation options. It also separates the risks for humans and equipment to allow more distinct treatment of the risks.

Human factors can be divided into positive factors (by preventing a failure or reducing the severity) or negative factors (by causing the failure or reacting wrongly). Humans can also be affected, and in some cases it is logical to distinguish between damage to equipment and environment and harm to humans. The example in Table F.13 includes the human as source of the failure.

In the field ‘Attention category’, phases in which the human behaves incorrectly are distinguished. In the field ‘Psychological error cause analysis’, guidewords for error causes are given. The time at which, or over which, these error categories are reached depends on the number of phases in which they might occur. This might influence the likelihood of occurrence assumed for this type of error.

On the left side, the necessary circumstances for the error are evaluated. In the field ‘Human error mode’ it might be beneficial to distinguish different groups of persons and by this also reduce or increase the probability value depending on the size of the group to which this error might be limited. Here, a distinction can be made between adults (A) and children (C), female or male (F/M), persons with disabilities (D) and aged persons (O) or unspecified persons (G).

In this case, the decision was taken to add the equipment and human risk scores to generate a system risk value. Countermeasures are also classified so that possible ways of actions are distinguished: can the error occurrence be prevented (O), can the occurrence be avoided by instructing personnel (I), is a management system curing the occurrence (M) or can warnings for the public be issued (E).

The use of such methods is highly dependent on the application.

F.11 Marking and encapsulation process for an electronic component

Table F.14 gives an extract from the process FMEA performed for the encapsulation and marking process for an electronic component: a so-called back end process.

Table F.6 – Extract from FMEA of the process of monitoring blood sugar *(1 of 2)*

End item: Blood sugar calculator Operating period: 5 years			Item: Software Revision: 0.6		Prepared by: NN Date: 2015-07-31		Updated: By:	
Step	**Item used**	**Function**	**Failure mode**	**Mechanism**	**Cause**	**Local effect**	**Detection method**	**Compensating provision**
Set meter	Meter	Measure time since last dose, data for morning averages	Incorrect time set	12 h / 24 h clock confusion		Incorrect morning averages displayed, User might calculate times since last dose incorrectly	Only if time > 12 h	Show AM / PM in display, show time since last dose in display
Calibration		Set coding for batch of test strips	Miscoded	Miscoded	Reading error	False high or low (up to 30 %)	Display shows mismatched numbers at time of coding but easy to misread	Recalibrate each batch with sample solution
Prick finger	Lancet	Produce blood sample	Insufficient blood	Fingers cold, insufficient depth of prick		False low	None	
Transfer blood to test strip	Test strips	To collect blood and react with it	Faulty test strip	Out of date	Run out of in date strips	False high or low	Date on strip	Instructions to user to check date before using
			Reaction fails	Strips stored at too high/low temperature or high humidity	Weather extremes	False high or low	None	
			Blood sample contaminated	Residue on pricked finger contains sugar	Hands not washed	False high	None	Instructions to user
			Blood sample contaminated	Residue from hand cream, etc.	Hands not washed	False low	None	Instructions to user
Insert test strip	Test strip, meter	To apply reader to strip	Not inserted sufficiently	Inexperienced user		False low	Error message displayed	Instructions to user
Note any alarms	Hi/Lo indicator	Shows when blood sugar abnormally high or low		Is not noticed	Indicator small			Audible alarm different for high and low

Table F.6 *(2 of 2)*

End item: Blood sugar calculator **Operating period: 5 years**			**Item: Software** **Revision: 0.6**		**Prepared by: NN** **Date: 2015-07-31**		**Updated:** **By:**	
Step	**Item used**	**Function**	**Failure mode**	**Mechanism**	**Cause**	**Local effect**	**Detection method**	**Compensating provision**
Read meter	Meter	Measure electrical signal at electrode and display as blood sugar level	Wrong number displayed	Some segments of numbers are lost e.g. 8 reads as 6	Battery low	False high or low	Battery low indicator	
			Over concentrated blood	Subject dehydrated		False high	None	
			Incorrect units displayed	Wrong units set by user	Lack of knowledge	False high or low (depending on direction of units error) by factor of 10	Units indicator, patient trained to recognise abnormal reading and recalibrate against standard solution	Units indicator large letters, recommendation to modify software so units hard wired in
			Wrong units	Units reset to factory settings when battery power lost	Intentional when battery changed	False high or low (depending on direction of units error) by factor of 10		
					Unintentional when dropped	False high or low (depending on direction of units error) by factor of 10		
					US person purchases meter in Europe does not notice units different (or vice versa)	False high or low (depending on direction of units error) by factor of 10		
				Correct number/units displayed – reading error	Insufficiently clear display			Ergonomically designed display for easy reading
NOTE The unit for blood sugar level is mg/dl in the USA, and mmol/l in Europe. There is a factor of approximately 10 between the numerical values.								

Table F.7 – Extract of automotive electronic part FMEA

Item/Function			Potential failure mode	Potential effect(s) of failure		S	Potential cause(s)/ mechanism(s) of failure	Detail cause(s)/ mechanism(s) of failure	O	Current design controls prevention	Current design controls detection	D	RPN	Recommended action	Responsibility and target completion date	Treatment action results				
Sub-system	Assembly	Component		Local effect	Final effect											Action taken	S	O	D	RPN
Power supply																				
	V1																			
		D1	Short	No reverse voltage protection.	Item operates out of specification.	2	Inherent defect of the component with the probability of a short = 80 %	Material breakdown	3	Selection of higher quality and rating	Evaluation and reliability validation testing	10	60							
		D1	Open	No voltage provided to the item.	Item inoperable.	10	Inherent defect of the component with the probability of an open = 20 %	Bonding or semiconduct or crack	3	Selection of higher quality and rating	Evaluation and reliability validation testing	10	300							
		C1	Short	Battery voltage + shorts to ground. D1 burns out.	No voltage provided to the item. Item inoperable.	10	Inherent defect of the component with the probability of a short = 10 %	Dielectric breakdown or crack	3	Selection of higher quality and rating	Evaluation and reliability validation testing	10	300							
		C1	Open	No filtering	Item operates out of specification.	2	Inherent defect of the component with the probability of an open = 90 %	Dielectric open, leak, void, or crack	2	Selection of higher quality and rating	Evaluation and reliability validation testing	10	40							

Key

S = Severity, O = Occurrence, D = Detectability

NOTE This is a partially filled out FMEA. The project team has to address the risks and come up with proposed actions and due dates. The FMEA can then be completed by filling out the columns “treatment action results".

Table F.8 – Extract from system FMEA for a remote control for a hi-fi system

Component	Function	Failure mode	Local consequence	Global consequence	Severity	Probability	Detectability	RPN	Treatment action
Keyboard	To enable control action selection when applying between 20 and 50 of force by finger	Keys below front plate preventing any force from being applied by thumb	Keys cannot be pressed	Remote control cannot control hi-fi	4	3	2	24	PCB fastened to top plate to reduce tolerance problems
PCB	To interpret commands from keyboard and communicate control action to LED within 100 ms	Solder joints and contact failures due to mechanical resonance	Some signals cannot be communicated to LED	Remote control cannot control some hi-fi functions	4	2	5	40	Supports to increase resonance frequencies
Display	To visually display the selected control action within 100 ms of selection	Display dislodges from remote control front plate due to weak fastening technique	Display loose	Repair needed	3	2	3	18	Larger area for glue

Table F.9 – Extract from design FMEA for a remote control for a hi-fi system

Component	Function	Failure mode	Local consequence	Global consequence	Severity	Probability	Detectability	RPN	Treatment action
Keyboard	To convert kinetic energy into electrical signal	Fluid contamination not prevented	High contact resistance	No function	4	5	5	100	Plastic cover under keys
PCB	To process and communicate signals	Fluid contamination not prevented	High contact resistance	No function	4	5	5	100	Plastic cover under keys
Display	To display signal from PCB	Connector resistance high	Bad contact	Display blank	4	2	5	40	Connector specification and production test

Table F.10 – Extract from process FMEA for a remote control for a hi-fi system

Step	Function	Potential problem	Local consequence	Global consequence	Severity	Probability	Detectability	RPN	Treatment action
Solder keyboard connector	To form connection between keyboard and PCB	Excess flux	High resistance	Intermittent connection	4	2	4	32	No clean flux
Solder SMD component	To form connection between SMD component and PCB	Tombstone	No connection of SMD to PCB	Low yield resulting in high manufacturing costs	2	2	2	8	PCB layout
Adhere LCD display to front plate	To secure LCD display to front plate	Small glue area	Weak adhesion	Separation of LCD display from front plate	4	4	5	80	FEM analysis

Table F.11 – Extract from maintenance service FMEA for a remote control for a hi-fi system

Component	Function	Potential problem	Local consequence	Global consequence	Severity	Probability	Detectability	RPN	Treatment action
Keyboard	To assess keyboard operability	Short connection cable between keyboard and display	Difficult to look at screen and operate keys at the same time	Time to conduct maintenance task increased Risk of inducing fault increased	3	5	5	75	Service cable
PCB	To remove and replace PCB	Removal process requiring unscrewing of screws	Screw hole destroyed	New front plate required	4	4	4	64	Metal insert
Display	To replace failed display	Inability to separate display from front plate without damage	New front plate	High cost repair	4	2	4	32	Display reliability

Table F.12 – Extract from an FMEDA for an electronic circuit in a safety control system *(1 of 2)*

Circuit diagram:
Parts list:
Created by:
Review by:
Failure rate and distribution database: company specific (example)
Date of analysis:

Name	Component	Function	Failure rate [FIT]	Failure mode	Failure mode ratio	Effect	Behaviour effect S: Safety D: Dangerous	Diagnostic coverage
F50	Fuse	Short-circuit protection at the input	25	Fail to open	50 %	None in normal operation	No effect	-
				Premature open	10 %	Outputs de-energized	S	-
				Slow to open	40 %	No effect on safety function	No effect	-
D12	Suppressor diode	Over voltage protection (EMC)	7	Short	95 %	F50 blows	S	-
				Open circuit	5 %	No effect on safety function	No effect	-
R100	Resistor, SMD	Current limitation, EMC	0,2	Short	5 %	No current limitation – failure	D	60 %
				Open	65 %	Outputs de-energized	S	-
				Parameter change	30 %	Function still given	No effect	-
C13	Capacitor ceramic, HDC / MDC	EMC	2	Short	50 %	F50 blows	S	-
				Open	30 %	None in normal operation (no protection)	No effect	-
				Change in value	20 %	Function still given	No effect	-
D25	Small signal diode, < 0,1 W	Bridge rectifier	1	Short	50 %	F50 blows	S	-
				Open	35 %	No correct rectification in case of AC supply	S	-
				Parameter change	15 %	Function still given	No effect	-

Table F.12 *(2 of 2)*

Name	Component	Function	Failure rate [FIT]	Failure Mode	Distribution	Effect	Behaviour Effect S: Safety D: Dangerous	Diagnostic Coverage
C2	Electrolytic capacitor, aluminium electrolytic, non-solid electrolyte	Smoothing capacitor	5	Short	53 %	F50 blows	S	-
				Open	35 %	None in normal operation with DC supply	No effect	-
				Electrolyte leak	10 %	No effect on safety function	No effect	-
				Decrease in capacitance	2 %	Function still given	No effect	-
IC18	Regulator, power > 1 W, minor complexity	Voltage regulator used with R100 as current source	25	Stuck-hi	30 %	No regulation -> output switching	D	0 %
				Stuck-lo	30 %	Outputs de-energized	S	-
				Short	15 %	No regulation -> over current at the relays (diverse)	No effect	-
				Open	15 %	Outputs de-energized	S	-
				Drift	5 %	Function still given	No effect	-
				Function	5 %	Function still given	No effect	-

Summary:

λ_{du} = 7,504 FIT = (Σ Failure_Rate x % distribution) of all components with “D” behaviour and 0 % DC

λ_{dd} = 0,006 FIT = (Σ Failure_Rate x % distribution x % DC) of all components with “D” behaviour and DC >0 %

λ_{d} = 7,510 FIT = (Σ λ_{du}, λ_{dd})

λ_{s} = 25,03 FIT = (Σ Failure_Rate x % distribution) of all components with “S” behaviour

$\lambda_{\text{no effect}}$ = 32,66 FIT = (Σ Failure_Rate x % distribution) of all components with “no effect” behaviour

λ_{total} = 65,2 FIT = (Σ Failure_Rate) of all components

SFF (Safe failure fraction) = {(total of safe and dangerous failure rates)-(total of dangerous-undetected failure rates)}/(total of safe and dangerous failure rates)

= ((25,03 + 7,510) – 7,504) / (7,510 + 25,03) = 25,036/32,54 = 77,8 %

NOTE Distribution represents the failure mode as a percentage of the total number of failures.

Table F.13 – Extract from an FMEA for a coffee-maker

Attention category			Error potential (Error rate)				Psychological error cause analysis															Effect Analysis											
Fatigue, monotonous work			High (0,1 or more)				x			x	x				x	x																	
Routine work, rest			Fairly high (0,01 to 0,000 01)							x	x																						
Positive action			Low (0,000 001 or less)							x	x																						
Hectic, panic			High (0,1 or more)							x	x				x	x			x														
							Error guidewords															Effect (Damage) analysis			Occurrence score		Severity score		Risk score				
							Per-ception			Decision				Action																			
Operation phase	Activity	Concerned environment	Affected equipment	Relation	Human error mode	Category of human	Hard to see or hear	Wrong perception	Not understandable	Lack of understanding	Insufficient knowledge	Slow understanding	Misunderstanding	No execution	Forgetting execution	Inadequate execution	Excessive execution	Too late execution	Too early execution	Different execution	Wrong order of execution	Equipment	Human	System	Equipment	Human	Equipment	Human	Equipment	Human	System = Human + Equipment	Countermeasure classification	Counter-measure (Corrective action)
Heat-up	Power the device, put coffee pot to heating plate	Being in a hurry/ missing care	Temperature sensor failure	AND	Coffee left on too long	G									x							Malfunction	Second-ary damage caused by fire	Fire	2	1	4	4	8	4	12	O	Reserve time for cleaning phase
Usage	To pour coffee in a cup	Fatigue	None	AND	Spilling coffee	G										x		x				None	Burn injury / wound	---	1	2	1	3	1	6	7	O	Reserve time for customer contact
Cleaning	Remove old coffee	Being in a hurry	None	(OR)	Spilling hot coffee	G	x															None	Burn injury / wound	---	1	2	1	4	1	8	9	O	Reserve time for cleaning
	To wash by hands	Being in a hurry	Presence of sharp corners and edges	AND	Touching the edge with bare hands	G	x												x			None	Burn injury / wound	---	1	2	2	4	2	8	10	W	Only allow machine cleaning
Storage	To store	In the cold region	Pipe breakage due to freezing of water	←	Water not removed	G	x								x							Damage	None	Not available	4	4	4	2	16	8	24	W	Warning in instruction manual

NOTE 1 Category of human – G: Unspecified M: Male A: Adult F: Female C: Child O: Elderly I: Illness.

NOTE 2 Countermeasure classification – O: Damage occurrence prevention measures, S: Damage spread prevention measures, W: Damage warning measures, E: Customer education for safety use, M: Safety management system review

Table F.14 – Extract from an FMEA for an electronic component marking and encapsulation process

Process function requirement	Potential failure mode	Potential effect(s) of failure	S	Potential cause(s)/ mechanism(s)	O	Current process controls	D	RPN	Recommended action(s)	Responsibility and target completion date	Action taken	New S	New O	New D	New RPN
Marking	Become blurred	Decipherment of printing cannot be performed	8	Laser condition management is not appropriate	2	Visual check at start of work – check cycle Every 1 sheet/lot	2	32	None						
	Marking shifts	Poor appearance	8	A conveyance position shifts	2	Test marking cycle every 1 sheet/lot	1	16	None						
	Marking is the opposite direction	Poor appearance	8	The product is set in the opposite direction	2	The direction of the product is judged by the image recognition frequency total	1	16	None						
Breaking	Barricade and scoop out occurs for a product	A poor product size	8	The clearance when setting a substrate to an exclusive tool is too large	4	The maintenance of an exclusive tool self-check	2	64	Introducing new dicer inspected when introduced	Production Manufacturing Technology 31 Jan. 2003	Introducing new dicer inspected when introduced Product size check Cpk: 2.58	7	2	2	28
	The outside of a product becomes larger	A poor product size	8	The grind wheel is worn out	4	Sampling size measurement Sampling cycle: It is 4 pcs every five sheets	2	64	Introducing new dicer inspected when introduced	As above	As above	7	2	2	28
Removing for burrs	A barricade is not removed	A poor product size	8	A jig is shaking-timing is not proper	1	Self-check	2	16	None						

Key

S = Severity, O = Occurrence, D = Detectability

Bibliography

[1] IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*

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

[3] IEC 60300-3-12, *Dependability management – Part 3-12; Application guide – Integrated logistic support*

[4] IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

[5] IEC 61025, *Fault tree analysis (FTA)*

[6] IEC 61078, *Reliability block diagrams*

[7] IEC 61165, *Application of Markov techniques*

[8] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[9] IEC 61709, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

[10] IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[11] IEC 62308, *Equipment reliability – Reliability assessment methods*

[12] IEC 62502, *Analysis techniques for dependability – Event tree analysis (ETA)*

[13] IEC 62508, *Guidance on human aspects of dependability*

[14] IEC 62551, *Analysis techniques for dependability – Petri net techniques*

[15] IEC 62740, *Root cause analysis (RCA)*

[16] IEC 62741, *Demonstration of dependability requirements – The dependability case*

[17] IEC/TR 63039, *Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state*

[18] ISO 9000, *Quality management systems – Fundamentals and vocabulary*

[19] ISO 31000, *Risk management – Guidelines*

[20] IEC/ISO 31010, *Risk management – Risk assessment techniques*

[21] ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

[22] ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*

[23] ISO 55000, *Asset management – Overview, principles and terminology*

[24] EN 13306:2010, *Maintenance – Maintenance terminology*

[25] MIL-HDBK-338B, *Electronic reliability design handbook, Defense Quality and Standardization Office* (DLSC-LM), Fort Belvoir, Virginia 22060-6221, October 1998

[26] Bell, J., and Holroyd, J., *Review of human reliability assessment methods*, Research Report RR 679 for Health and Safety Executive, Sudbury: HSE Books, 2009

[27] Braband, J., *Improving the Risk Priority Number concept, Journal of System Safety*, 3, 2003, p.21-23

[28] Masuda A., *A Proposal of service reliability study and its practical application on maintenance support of electronic products*, Proceeding of International IEEE Conference on the Business of Electronic Product Reliability and Liability, pp.119-126, 2003

[29] Ozarin, N., *Understanding, planning and performing Failure Modes & Effects Analysis on software*, Tutorial, RAMS Conference, 2016

[30] Yoshimura, I., Sato, Y., *Safety achieved by the Safe Failure Fraction (SFF) in IEC 61508*, IEEE Transactions on Reliability, Vol.57, No.4, 662-669, Dec. 2008

[31] ISO Guide 73:2009, *Risk management – Vocabulary*

[32] IEC 60050-191[2]*, International Electrotechnical Vocabulary – Part 191: Dependability and quality of service*

____

[2] Withdrawn, replaced by IEC 60050-191.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch