AS/NZS IEC 60812:2020
IEC 60812:2018

AS/NZS IEC 60812:2020

Australian/New Zealand Standard™

Failure modes and effects analysis (FMEA and FMECA)

STANDARDS Australia

STANDARDS® NEW ZEALAND
PAEREWA AOTEAROA

Documents
Document Sharing Hub

Full document details: AS NZS IEC 60812-2020

AS/NZS IEC 60812:2020

This Joint Australian/New Zealand Standard™ was prepared by Joint Technical Committee QR-005, Dependability. It was approved on behalf of the Council of Standards Australia on 23 March 2020 and by the New Zealand Standards Approval Board on 5 February 2020.

This Standard was published on 3 April 2020.

The following are represented on Committee QR-005:

Asset Management Council (Australia)
Australian Industry Group
Department of Defence (Australian Government)
Engineering New Zealand
Engineers Australia
Human Factors and Ergonomics Society of New Zealand
Institution of Occupational Safety and Health
National Rail Safety Regulator (Australia)
National Road Carriers Association (New Zealand)
New Zealand Institute of Safety Management
Professionals Australia
Risk Engineering Society (Australia)
Risk Management Institute of Australasia
RiskNZ
University of New South Wales
University of Western Australia
University of Wollongong

This Standard was issued in draft form for comment as DR AS/NZS IEC 60812:2019.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

www.standards.govt.nz

ISBN 978 1 76072 792 5

Documents
Document Sharing Hub

Full document details: AS NZS IEC 60812-2020

Australian/New Zealand Standard™

Failure modes and effects analysis (FMEA and FMECA)

Originated as AS IEC 60812—2008.
Revised and redesignated as AS/NZS IEC 60812:2020.

COPYRIGHT

© IEC 2020 — All rights reserved
© Standards Australia Limited/the Crown in right of New Zealand, administered by the New Zealand Standards Executive 2020

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth) or the Copyright Act 1994 (New Zealand).

Documents
Document Sharing Hub

Full document details: AS NZS IEC 60812-2020

Preface

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee QR-005, Dependability, to supersede AS IEC 60812—2008, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*.

The objective of this Standard is to explain 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 application.

This Standard is identical with, and has been reproduced from, IEC 60812:2018, *Failure modes and effects analysis (FMEA and FMECA)*.

As this document has been reproduced from an International Standard, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

NOTES

Documents
Document Sharing Hub

Full document details: AS NZS IEC 60812-2020

CONTENTS

FOREWORD 6
INTRODUCTION 8
1 Scope 9
2 Normative references 9
3 Terms, definitions and abbreviated terms 9
3.1 Terms and definitions 9
3.2 Abbreviated terms 13
4 Overview 14
4.1 Purpose and objectives 14
4.2 Roles, responsibilities and competences 14
4.3 Terminology 15
5 Methodology for FMEA 15
5.1 General 15
5.2 Plan the FMEA 17
5.2.1 General 17
5.2.2 Define the objectives and scope of analysis 17
5.2.3 Identify boundaries and scenarios 17
5.2.4 Define decision criteria for treatment of failure modes 19
5.2.5 Determine documentation and reporting requirements 20
5.2.6 Define resources for analysis 21
5.3 Perform the FMEA 22
5.3.1 General 22
5.3.2 Sub-divide item or process into elements 22
5.3.3 Identify functions and performance standards for each element 23
5.3.4 Identify failure modes 23
5.3.5 Identify detection methods and existing controls 23
5.3.6 Identify local and final effects of failure modes 24
5.3.7 Identify failure causes 25
5.3.8 Evaluate relative importance of failure modes 26
5.3.9 Identify actions 28
5.4 Document the FMEA 29
Annex A (informative) General considerations for tailoring an FMEA 30
A.1 General 30
A.1.1 Overview 30
A.1.2 Start point for FMEA in the hierarchy 30
A.1.3 Degree of detail in analysis 31
A.1.4 Prioritization of failure modes 32
A.2 Factors influencing FMEA tailoring 33
A.2.1 Reuse of data/information from analysis of similar item 33
A.2.2 Maturity of item design and project progress 34
A.2.3 Degree of innovation 34
A.3 Examples of FMEA tailoring for items and processes 34
A.3.1 General 34
A.3.2 Example of tailoring an FMEA for an office equipment product 35
A.3.3 Example of tailoring an FMEA for a distributed power system 35
A.3.4 Example of tailoring an FMEA for medical processes 36

AVA Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

A.3.5 Example of tailoring an FMEA for electronic control systems 36
A.3.6 Example of tailoring an FMEA for a pump hydro block 37
A.3.7 Example of tailoring an FMEA for a wind turbine for power generation 37
Annex B (informative) Criticality analysis methods 38
B.1 General 38
B.2 Measurement scales for criticality parameters 38
B.2.1 General 38
B.2.2 Scale definition 38
B.2.3 Assessing likelihood 39
B.3 Assigning criticality using a matrix or plot 40
B.3.1 General 40
B.3.2 Criticality matrix 40
B.3.3 Criticality plots 41
B.4 Assigning criticality using a risk priority number 42
B.4.1 General 42
B.4.2 Risk priority number 42
B.4.3 Alternative risk priority number method 44
Annex C (informative) Example of FMEA report content 46
C.1 General 46
C.2 Example of generation of reports from a database information system for an FMEA of a power supply unit 46
Annex D (informative) Relationship between FMEA and other dependability analysis techniques 52
Annex E (informative) Application considerations for FMEA 53
E.1 General 53
E.2 Software FMEA 53
E.3 Process FMEA 55
E.4 FMEA for design and development 56
E.5 FMEA within reliability centred maintenance 56
E.6 FMEA for safety related control systems 56
E.6.1 General 56
E.6.2 FMEA in planning a safety application 57
E.6.3 Criticality analysis including diagnostics 57
E.7 FMEA for complex systems with reliability allocation 58
E.7.1 General 58
E.7.2 Criticality assessment for non-repairable systems with allocated unreliability 58
E.7.3 Criticality assessment for repairable systems with allocated availability 59
Annex F (informative) Examples of FMEA from industry applications 60
F.1 General 60
F.2 Health process application for drug ordering process 60
F.3 Manufacturing process application for paint spraying 60
F.4 Design application for a water pump 61
F.4.1 General 61
F.4.2 Item function 61
F.4.3 Item failure modes 61
F.4.4 Item failure effects 61
F.5 Example of an FMEA with criticality analysis for a complex non-repaired system 62

AVA Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

F.6 Software application for a blood sugar calculator 63
F.7 Automotive electronics device 63
F.8 Maintenance and support application for a hi-fi system 64
F.9 Safety related control system applications 65
F.9.1 Electronic circuit 65
F.9.2 Automated train control system 65
F.10 FMEA including human factors analysis 65
F.11 Marking and encapsulation process for an electronic component 66
Bibliography 76

Figure 1 – Overview of FMEA methodology before tailoring 16
Figure B.1 – Example of a qualitative criticality matrix 40
Figure B.2 – Examples of criticality plots 41
Figure C.1 – Database information system to support FMEA report generation 47
Figure C.2 – Diagram of power supply type XYZ 47
Figure C.3 – Criticality matrix for FMECA report in Table C.5 created as a two dimensional image without taking into account detectability 51
Figure E.1 – General software failure model for a component software unit (CSU) 55
Figure E.2 – Allocation of system failure probabilities 59
Figure F.1 – Hierarchy of a series electronic system, its subsystems and assemblies with allocated unreliability values, F(t) 62
Figure F.2 – Automotive air-bag part 64

Table 1 – Example of terms commonly associated with levels of hierarchy 15
Table A.1 – Characteristics of top-down and bottom-up approaches to FMEA 31
Table A.2 – General application of common approaches to FMEA 33
Table C.1 – Example of fields selected for FMEA report of power supply based on database information 48
Table C.2 – Example of report of component FMEA 49
Table C.3 – Example of report of parts with possible common cause failures 50
Table C.4 – Example of report of FMECA using RPN criticality analysis 50
Table C.5 – Example of report of FMECA using criticality matrix for global effect 51
Table F.1 – Extract from FMEA of the process of ordering a drug from a pharmacy 60
Table F.2 – Extract from FMEA of paint spraying step of a manufacturing process 61
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 63
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 63
Table F.5 – Hazards and safe/dangerous failures in an automated train control system 65
Table F.6 – Extract from FMEA of the process of monitoring blood sugar *(1 of 2)* 67
Table F.7 – Extract of automotive electronic part FMEA 69
Table F.8 – Extract from system FMEA for a remote control for a hi-fi system 70
Table F.9 – Extract from design FMEA for a remote control for a hi-fi system 70
Table F.10 – Extract from process FMEA for a remote control for a hi-fi system 71
Table F.11 – Extract from maintenance service FMEA for a remote control for a hi-fi system 71

AVA Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

Table F.12 – Extract from an FMEDA for an electronic circuit in a safety control system *(1 of 2)* 72

Table F.13 – Extract from an FMEA for a coffee-maker 74

Table F.14 – Extract from an FMEA for an electronic component marking and encapsulation process 75

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

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.

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

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.

Documents
Document Sharing Hub
© Standards Australia Limited/Standards New Zealand 2020
Full document details: AS NZS IEC 60812-2020

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.

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

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.

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

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].

AVA Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

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.

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

[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.

AVA Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

[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

Documents
Document Sharing Hub
© Standards Australia Limited/Standards New Zealand 2020
Full document details: AS NZS IEC 60812-2020

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'.

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

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.

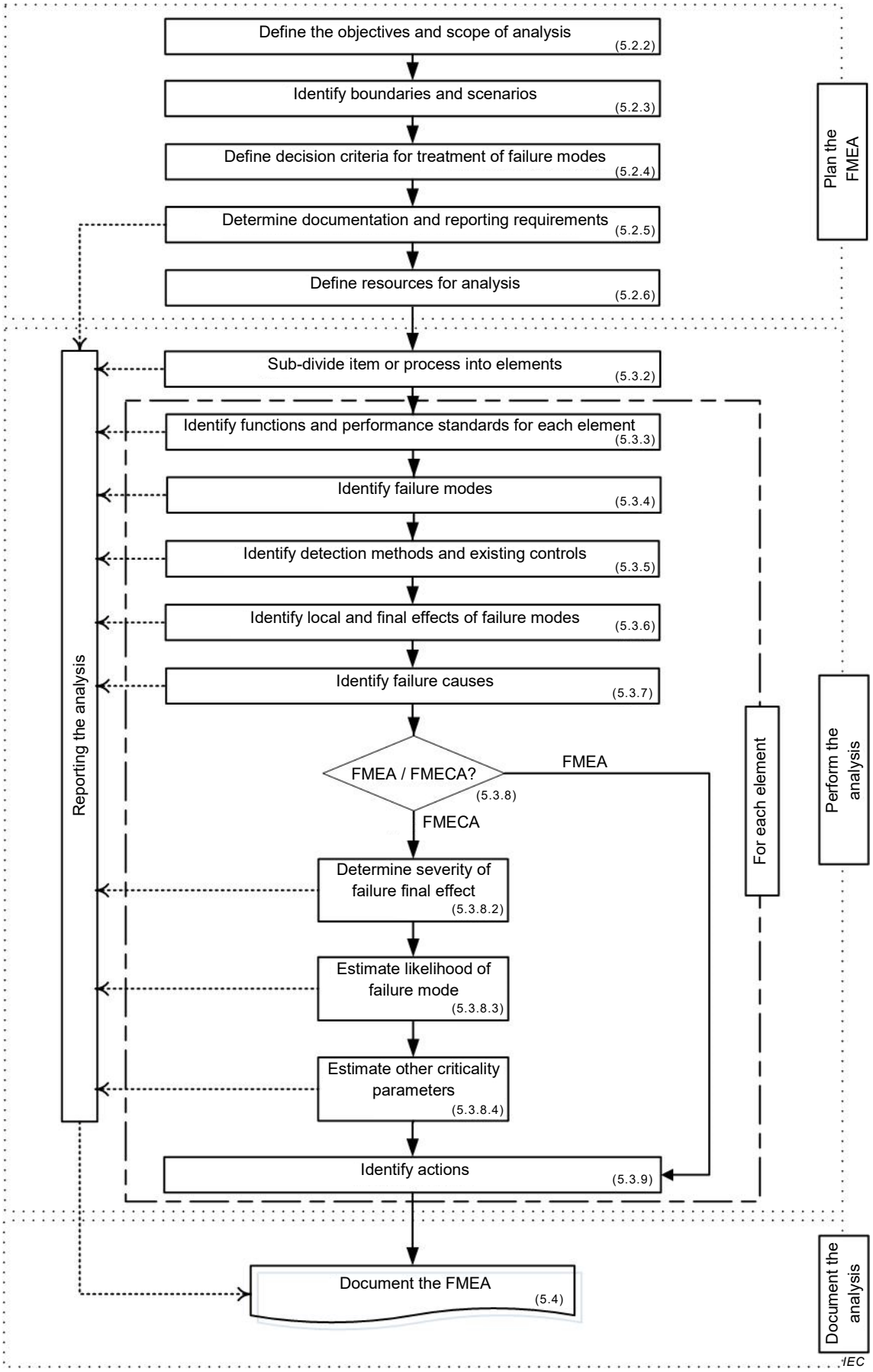
When reference is made in this document to record/identify/specify/describe/state/document some information, it means the information is to be included in the relevant FMEA documentation, for example FMEA report, FMEA plan, post-FMEA documentation such as the action plan.

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.

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020



Numbers in brackets refer to subclauses.

Figure 1 – Overview of FMEA methodology before tailoring

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

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

Documents
Document Sharing Hub

Full document details: AS NZS IEC 60812-2020

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.

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

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.

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

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;

Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020

- 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.

AVA Documents
Document Sharing Hub

© Standards Australia Limited/Standards New Zealand 2020

Full document details: AS NZS IEC 60812-2020