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

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 21 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@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

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

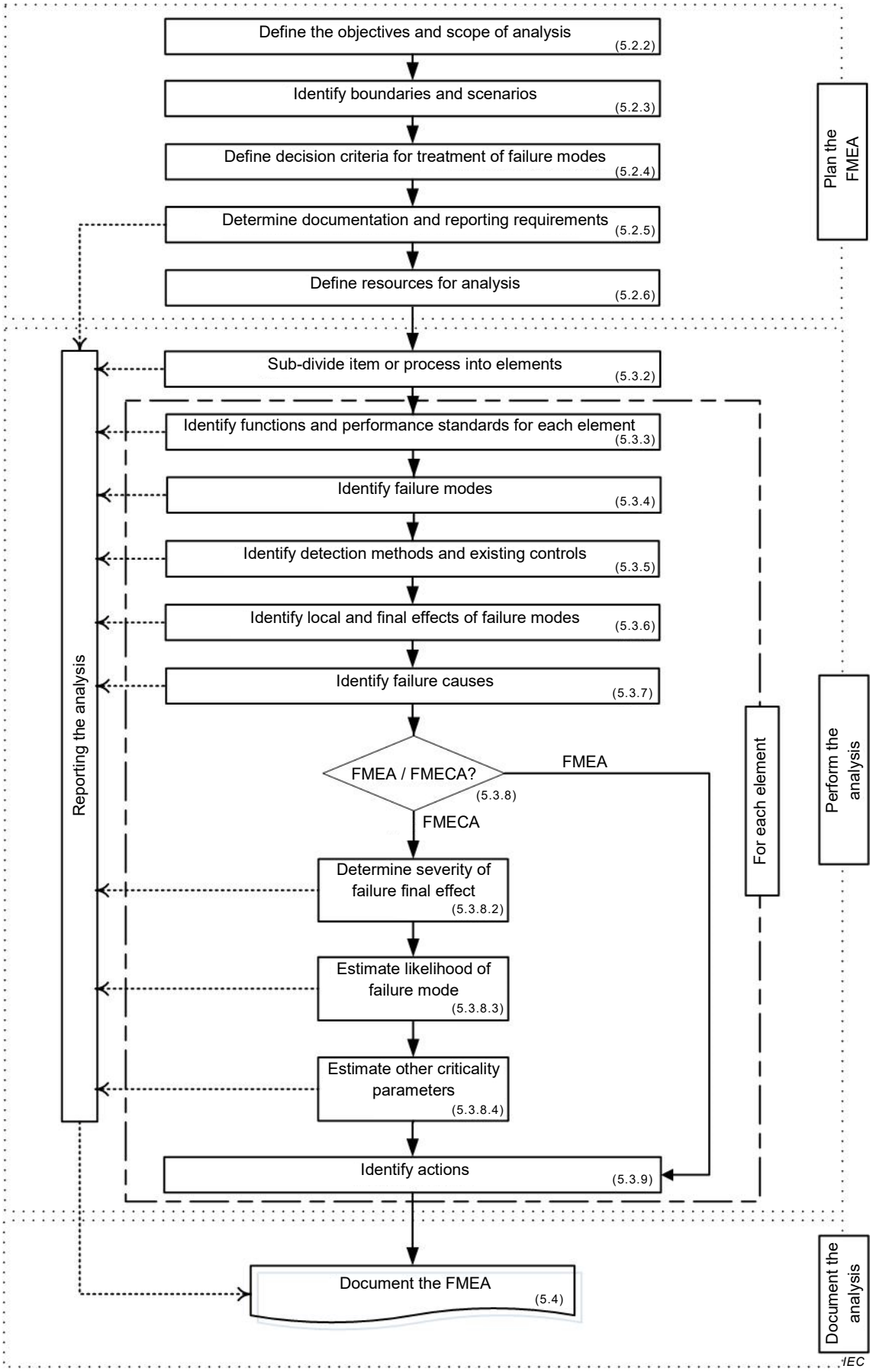
5.1 General

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.



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.

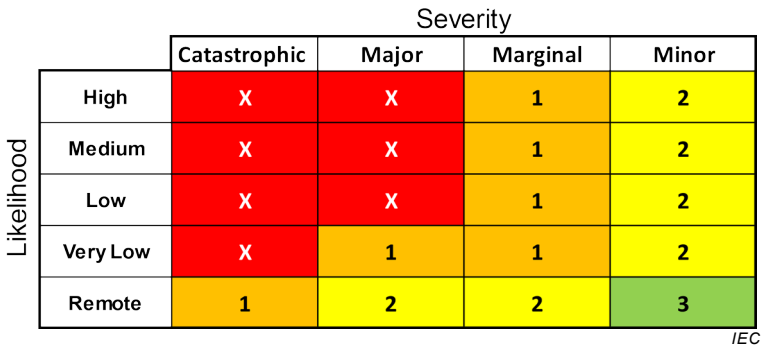


Figure B.1 – Example of a qualitative criticality matrix

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.

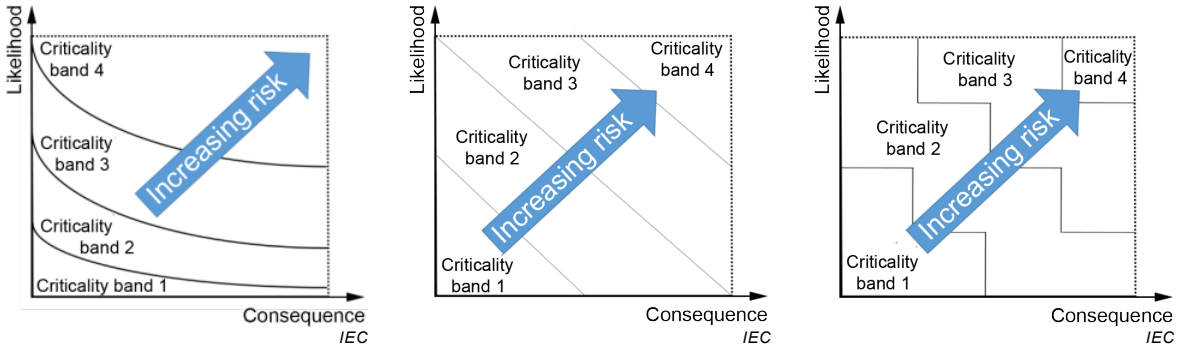
Figure B.1 is only an example of the structure of a matrix and should not be regarded as the definitive form. The actual form will depend on the particular application. If the number of likelihood bands and/or severity of consequence categories differs then the size of the matrix will differ from the 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.

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

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:

$$ARPN = S + O + D$$

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.

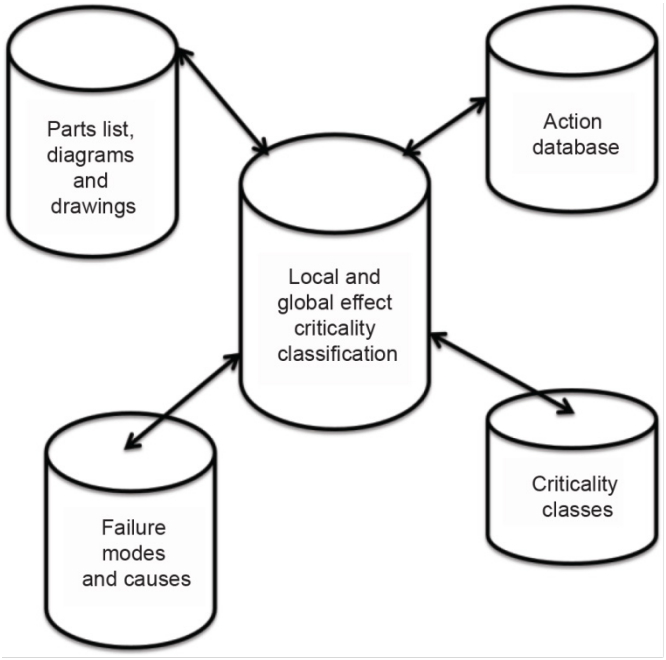


Figure C.1 – Database information system to support FMEA report generation

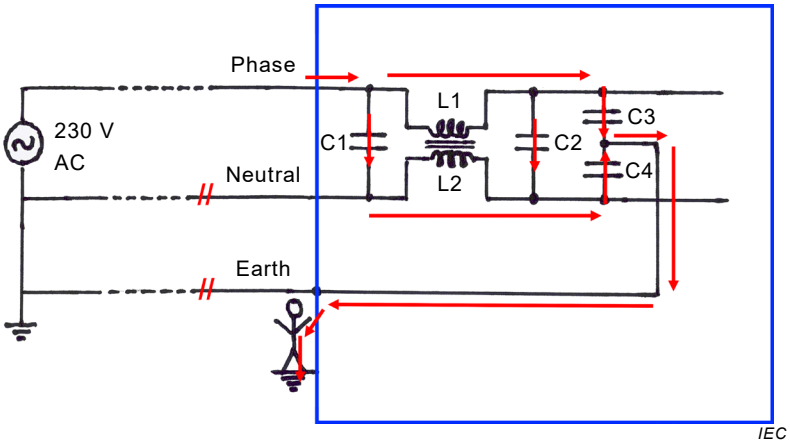


Figure C.2 – Diagram of power supply type XYZ

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.		

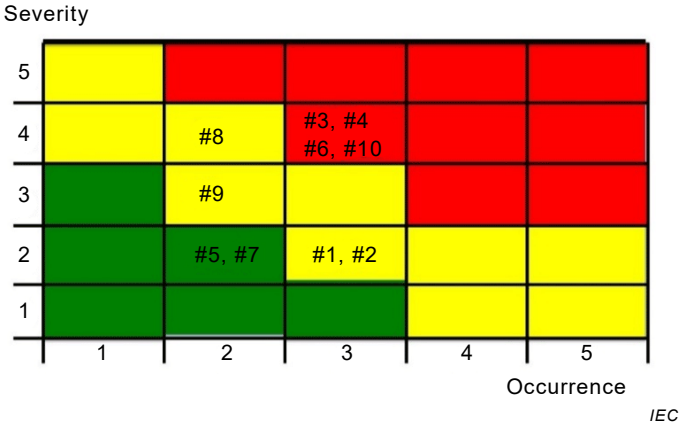


Figure C.3 – Criticality matrix for FMECA report in Table C.5 created as a two dimensional image without taking into account detectability

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.

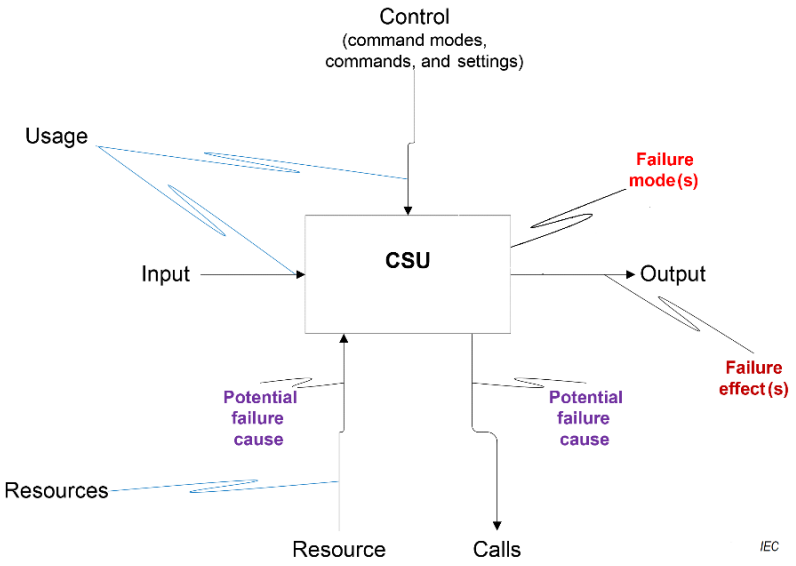


Figure E.1 – General software failure model for a component software unit (CSU)

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.

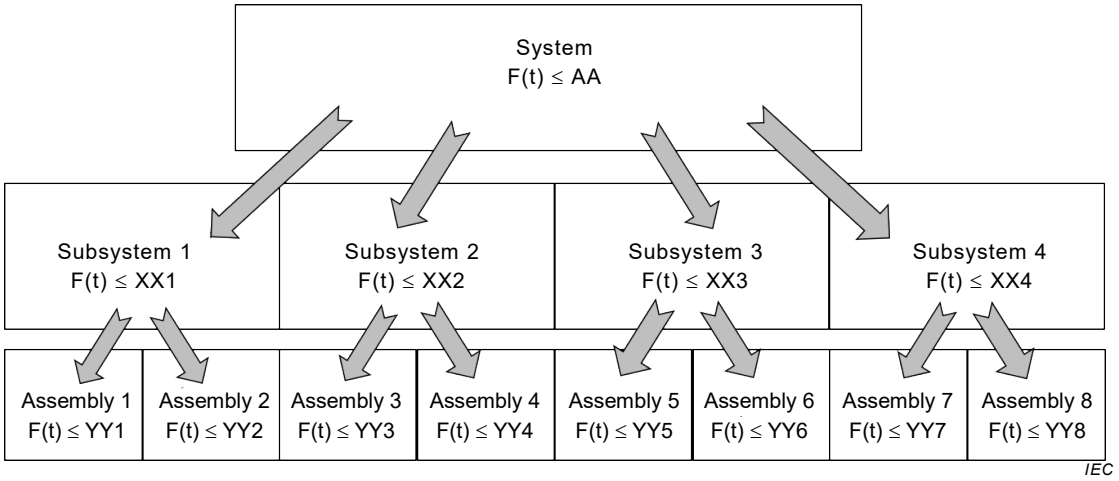


Figure E.2 – Allocation of system failure probabilities

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.

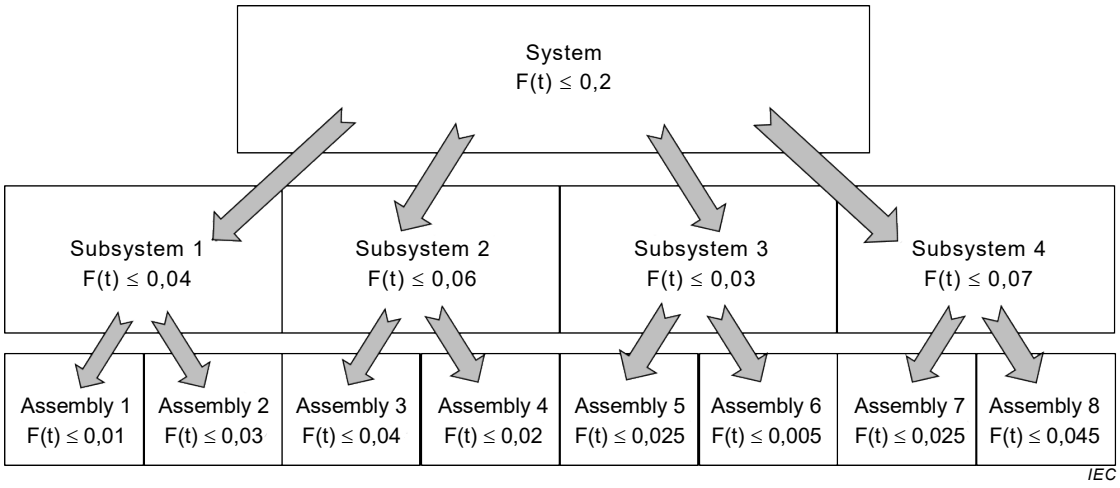


Figure F.1 – Hierarchy of a series electronic system, its subsystems and assemblies with allocated unreliability values, F(*t*)

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.

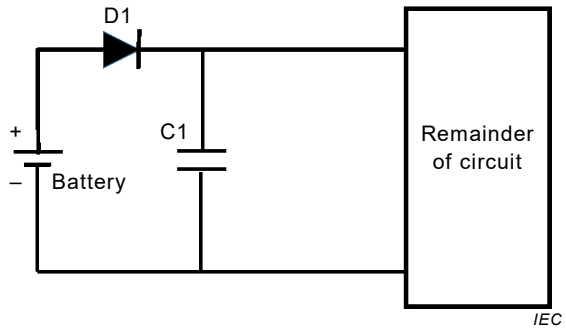


Figure F.2 – Automotive air-bag part

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)/ mecha-nism(s) of failure	O	Current design controls prevention	Current design controls detection	D	RPN	Recom mended action	Responsi bility and target completio n date	Treatment action results				
Sub-system	Assem-bly	Com-pon-ent		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 compo-nent 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 compo-nent 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 compo-nent 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 compo-nent 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

$\lambda_{no\ effect}$ = 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														
		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
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 Analysis											
							Per-ception		Decision					Action								Effect (Damage) analysis			Occurrence score		Severity score		Risk score				
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	Deciphermen t 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.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

ANALYSE DES MODES DE DÉFAILLANCE ET DE LEURS EFFETS (AMDE ET AMDEC)

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60812 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement.

Cette troisième édition annule et remplace la deuxième édition parue en 2006. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) le texte normatif est générique et couvre toutes les applications;
b) des exemples d'applications pour la sécurité, le secteur automobile, les logiciels et les processus (service) ont été ajoutés sous forme d'annexes informatives;
c) l'adaptation de l'AMDE à différentes applications est décrite;
d) différents formats de génération de rapport sont décrits, y compris un système d'informations de base de données;

e) d'autres méthodes de calcul des nombres prioritaires de risque (NPR) ont été ajoutées;

f) une méthode reposant sur la matrice de criticité a été ajoutée;

g) les relations avec d'autres méthodes d'analyse de la sûreté de fonctionnement sont décrites.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
56/1775/FDIS	56/1782/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo «colour inside» qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

L'analyse des modes de défaillance et de leurs effets (AMDE) est une méthode systématique d'évaluation d'une entité ou d'un processus afin d'identifier ses éventuels modes de défaillance et leurs effets sur les performances de l'entité ou du processus, ainsi que sur l'environnement voisin et le personnel. Le présent document décrit la manière de procéder à une AMDE.

L'AMDE vient à l'appui des décisions visant à réduire la probabilité de défaillances et leurs effets. Il s'agit donc d'améliorer les résultats de manière directe ou par l'intermédiaire d'autres analyses. Il s'agit, entre autres, d'améliorer la fiabilité, de réduire l'impact sur l'environnement, de réduire les dépenses d'achats, d'exploitation et d'augmenter la réputation de l'entreprise.

L'AMDE peut être adaptée pour répondre aux besoins d'une industrie ou d'une organisation. L'AMDE s'applique aux matériels, aux logiciels, aux processus, à l'action humaine et à leurs interfaces ou à toute combinaison de ceux-ci.

L'AMDE peut être réalisée plusieurs fois au cours du cycle de vie d'une même entité ou d'un même processus. Une analyse préliminaire peut être réalisée aux premières étapes de la conception et de la planification, suivie d'une analyse plus détaillée quand de plus amples informations sont disponibles. L'AMDE peut inclure des commandes existantes ou des traitements recommandés visant à réduire la probabilité et les effets d'un mode de défaillance. En cas d'analyse en boucle fermée, l'AMDE permet d'évaluer l'efficacité d'un traitement.

L'AMDE peut être adaptée et appliquée de différentes manières en fonction des objectifs.

Les modes de défaillance peuvent être hiérarchisés en fonction de leur importance. La hiérarchisation peut reposer sur un classement de la sévérité seule ou peut être combinée à d'autres mesures d'importance. Si les modes de défaillance sont hiérarchisés, le processus est appelé analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC). Le présent document utilise le terme AMDE pour inclure l'AMDEC.

Le présent document constitue des recommandations générales relatives à la manière de planifier, de réaliser, de documenter et de maintenir une AMDE en:

a) décrivant les principes;

b) précisant les étapes de l'analyse;

c) donnant des exemples de la documentation utilisée;

d) donnant des exemples d'application.

L'AMDE peut être utilisée dans un processus de certification ou d'assurance. Par exemple, l'AMDE peut être utilisée dans le cadre d'une analyse de sécurité avec un objectif réglementaire. Toutefois, le présent document étant générique, il n'aborde pas spécifiquement la sécurité.

Il convient de procéder à une AMDE en respectant la législation qui est en vigueur dans le périmètre de l'AMDE ou selon le type de risque à prendre en compte.

Le présent document s'adresse essentiellement aux utilisateurs qui dirigent l'analyse ou y participent.

ANALYSE DES MODES DE DÉFAILLANCE ET DE LEURS EFFETS (AMDE ET AMDEC)

1 Domaine d'application

Le présent document explique comment l'analyse des modes de défaillance et de leurs effets (AMDE), comprenant la variante d'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC), est planifiée, réalisée, documentée et maintenue.

L'analyse des modes de défaillance et de leurs effets (AMDE) vise à établir dans quelle mesure des entités ou des processus sont susceptibles de ne plus s'acquitter de leur fonction, de manière à pouvoir identifier tout traitement exigé. Une AMDE offre une méthode systématique d'identification des modes de défaillance et de leurs effets sur l'entité ou le processus, tant au niveau local que global. Elle peut également inclure l'identification des causes des modes de défaillance. Les modes de défaillance peuvent être hiérarchisés pour aider au choix du traitement à appliquer. Lorsque le classement de la criticité concerne au moins la sévérité des conséquences, et souvent d'autres mesures d'importance, l'analyse est appelée analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC).

Le présent document s'applique aux matériels, aux logiciels, aux processus incluant les actions humaines et à leurs interfaces, ou à toute combinaison de ceux-ci.

Une AMDE peut être utilisée dans le cadre d'une analyse de sécurité avec des objectifs réglementaires ou autres. Toutefois, la présente norme étant générique, elle ne donne pas de recommandations particulières relatives aux applications de sécurité.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60050-192, *Vocabulaire Électrotechnique International – Partie 192: Sûreté de fonctionnement* (disponible à l'adresse http://www.electropedia.org)

3 Termes, définitions et termes abrégés

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 60050-192 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1.1
mode de défaillance
DÉCONSEILLÉ: mode de panne
manière selon laquelle une défaillance se produit

Note 1 à l'article: Un mode de défaillance peut être déterminé par la fonction perdue ou par la transition d'état qui s'est produite.

Note 2 à l'article: Une vanne qui ne s'ouvre pas ou un moteur qui ne démarre pas sont des exemples de modes de défaillance matérielle.

Note 3 à l'article: Un mode de défaillance humaine est déterminé par la perte de fonction par suite d'une action humaine exécutée ou omise.

[SOURCE: IEC 60050-192:2015, 192-03-17, modifiée — La Note 1 à l'article a été modifiée, les Note 2 et Note 3 à l'article ont été ajoutées.]

3.1.2
effet d'une défaillance
conséquence d'une défaillance, dans ou au-delà de la frontière de l'entité défaillante

Note 1 à l'article: Pour certaines analyses, il peut être nécessaire de tenir compte des modes de défaillance individuels et de leurs effets.

Note 2 à l'article: L'effet d'une défaillance couvre également la conséquence d'une défaillance, dans ou au-delà de la frontière du processus défaillant.

[SOURCE: IEC 60050-192:2015, 192-03-08, modifiée — La Note 2 à l'article a été ajoutée.]

3.1.3
système
combinaison d'éléments interagissant entre eux organisée de façon à atteindre un ou plusieurs objectifs spécifiés

Note 1 à l'article: Un système peut être considéré comme un produit ou comme le service qu'il fournit.

Note 2 à l'article: En pratique, l'interprétation de sa signification est fréquemment clarifiée par le nom associé, par exemple: système avion. Alternativement au mot «système», peut être simplement substitué un synonyme dépendant du contexte, par exemple: avion, même si ceci peut masquer les principes inhérents à une vision système.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.46, modifiée — La Note 3 a été supprimée.]

3.1.4
entité
sujet que l'on considère

Note 1 à l'article: L'entité peut être une pièce isolée, un composant, un dispositif, une unité fonctionnelle, un équipement, un sous-système ou un système.

Note 2 à l'article: L'entité peut être composée de matériel, de logiciel, de personnel ou d'une quelconque de leurs combinaisons.

Note 3 à l'article: L'entité est souvent composée d'éléments dont chacun peut être considéré individuellement.

Note 4 à l'article: L'IEC 60050-191:1990 (supprimée; remplacée par l'IEC 60050-192:2015) identifiait les termes français «dispositif» et «individu» et le terme anglais «entity» comme synonymes, ce qui n'est pas vrai pour toutes les applications.

Note 5 à l'article: Dans l'IEC 60050-191:1990 (supprimée; remplacée par l'IEC 60050-192:2015), la définition de l'entité est une description plus qu'une définition. La nouvelle définition permet une substitution valable au terme tout au long du présent document. Le contenu de l'ancienne définition forme la nouvelle Note 1 à l'article.

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

3.1.5
processus
ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie

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

3.1.6
niveau hiérarchique
niveau de subdivision au sein de la hiérarchie d'un système, d'une entité ou d'un processus

Note 1 à l'article: Le niveau hiérarchique peut également être appelé «niveau dans l'arborescence» [voir l'IEC 60050-192:2015, 192-01-05].

Note 2 à l'article: Le niveau supérieur et le niveau inférieur correspondent respectivement au niveau le plus élevé et au niveau le plus bas de la hiérarchie. Le niveau intermédiaire correspond aux niveaux situés entre le niveau supérieur et le niveau inférieur.

3.1.7
élément
niveau de subdivision de la hiérarchie d'un système, d'une entité ou d'un processus, auquel les modes de défaillance doivent être identifiés

3.1.8
scénario
séquence possible de conditions spécifiées dans lesquelles les fonctions du système, de l'entité ou du processus sont exécutées

Note 1 à l'article: Les conditions peuvent inclure des activités ou des facteurs hors des limites définies de l'entité ou du processus à l'étude, et qui peuvent avoir un impact sur la performance de l'entité ou du processus.

Note 2 à l'article: Les conditions physiques incluent tous les facteurs environnementaux comme la température, l'humidité, les niveaux de luminosité, les chocs, la contamination ou les niveaux de radiation.

Note 3 à l'article: Les conditions organisationnelles peuvent inclure des facteurs tels que le niveau des effectifs ou les contraintes physiques/psychologiques.

3.1.9
cause de défaillance
ensemble de circonstances qui entraîne une défaillance

Note 1 à l'article: La cause d'une défaillance peut trouver son origine pendant la spécification, la conception, la fabrication, l'installation, l'exploitation ou la maintenance d'une entité.

Note 2 à l'article: La contamination ou le graissage inadapté donnant lieu au grippage des roulements peut être un exemple de cause d'une défaillance.

Note 3 à l'article: Les causes d'une défaillance d'un processus peuvent inclure les mécanismes d'erreur humaine tels que le trop grand nombre de stimuli, une perte de mémoire, une mauvaise compréhension ou une hypothèse erronée.

[SOURCE: IEC 60050-192:2015, 192-03-11, modifiée — La Note 2 et la Note 3 à l'article ont été ajoutées.]

3.1.10
mécanisme de défaillance
processus entraînant une défaillance

Note 1 à l'article: Il peut s'agir d'un processus physique, chimique, logique, psychologique ou d'une de leurs combinaisons.

[SOURCE: IEC 60050-192:2015, 192-03-12, modifiée — La Note 1 à l'article a été reformulée.]

3.1.11
vraisemblance
possibilité que quelque chose se produise

Note 1 à l'article: Dans le présent document, le terme «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques [telles une probabilité ou une fréquence sur une période donnée].

Note 2 à l'article: Le terme anglais «*likelihood*» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «*probability*» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «*probability*» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du présent document, le terme «vraisemblance» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «*probability*» (probabilité) dans de nombreuses langues autres que l'anglais.

[SOURCE: ISO Guide 73:2009, 3.6.1.1, modifiée — La Note 1 et la Note 2 à l'article ont été reformulées.]

3.1.12
sévérité
classement relatif des conséquences éventuelles ou réelles d'une défaillance ou d'une panne

Note 1 à l'article: La sévérité peut être liée à n'importe quelle conséquence.

[SOURCE: EN 13306:2010, 5.13, modifiée — Ajout de «classement relatif».]

3.1.13
méthode de détection
moyen de mettre en évidence un mode de défaillance ou une défaillance imminente

3.1.14
commande
caractéristiques de conception ou autres dispositions existantes permettant d'empêcher ou de réduire la vraisemblance du mode de défaillance ou de modifier ses effets

Note 1 à l'article: Les commandes peuvent également être appelées mesures de compensation.

3.1.15
criticité
<d'un mode de défaillance> classement par importance déterminé selon un critère d'évaluation spécifié

Note 1 à l'article: En principe, les critères d'évaluation de la criticité sont liés aux effets du mode de défaillance sur le niveau supérieur de la hiérarchie du système, de l'entité ou du processus.

Note 2 à l'article: En principe, les mesures de criticité combinent la sévérité des effets à au moins une autre caractéristique d'un mode de défaillance.

Note 3 à l'article: La signification particulière de la criticité dépend de la méthode d'évaluation définie dans le cadre d'une analyse, et elle est présentée en détail dans le présent document.

Note 4 à l'article: La criticité est liée au mode de défaillance et pas aux causes d'une défaillance (si ces dernières sont identifiées).

3.1.16
traitement
action de modifier la vraisemblance et/ou les effets d'un mode de défaillance

Note 1 à l'article: Le traitement est parfois appelé atténuation.

Note 2 à l'article: Le traitement peut impliquer des actions visant à éliminer la cause d'une défaillance, à modifier la vraisemblance du mode de défaillance ayant lieu et/ou à changer les conséquences.

3.1.17
erreur humaine
discordance entre l'action humaine effectuée ou omise et l'action prévue ou exigée

EXEMPLE Action incorrecte, omission d'une action exigée, calcul erroné, mauvaise interprétation d'une valeur.

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

3.1.18
redondance
<dans un système> existence de plusieurs moyens d'accomplir une fonction

Note 1 à l'article: Les moyens supplémentaires d'accomplir la fonction peuvent être intentionnellement différents pour réduire l'éventualité de défaillances de mode commun.

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

3.1.19
défaillances de cause commune
défaillances de différentes entités, qui résultent d'une cause unique, mais auraient pu être considérées comme indépendantes

Note 1 à l'article: Les défaillances de cause commune peuvent également être des «défaillances de mode commun».

Note 2 à l'article: L'éventualité de défaillances de cause commune réduit l'efficacité de la redondance du système.

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

3.1.20
défaillances de mode commun
<dans un système> défaillances des différentes entités caractérisées par le même mode de défaillance

Note 1 à l'article: Les défaillances de mode commun peuvent avoir des causes différentes.

Note 2 à l'article: Les défaillances de mode commun peuvent également être des «défaillances de cause commune».

Note 3 à l'article: L'éventualité de défaillances de mode commun réduit l'efficacité de la redondance du système.

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

3.1.21
testabilité
<d'une entité> degré de facilité avec lequel une entité peut être testée, pendant ou après l'utilisation pour détecter et isoler des défaillances/pannes

[SOURCE: IEC 60050-192:2015, 192-09-20, modifiée — «pendant ou après l'utilisation pour détecter et isoler des défaillances/pannes» a été ajouté.]

3.2 Termes abrégés

DCC défaillance de cause commune
COTS commercial off the shelf (produits commerciaux)
CSU component software unit (composant logiciel)
DC diagnostic coverage (couverture du diagnostic)
IEM interférence électromagnétique
IEM impulsion électromagnétique
ESD emergency shutdown (arrêt d'urgence)
AAE analyse par arbre d'événement
FIT failure in time (défaillances dans le temps)
AAP analyse par arbre de panne
AMDE analyse des modes de défaillance et de leurs effets
AMDEC analyses des modes de défaillance, de leurs effets et de leur criticité

AMDED analyse des modes de défaillance, de leurs effets et de leurs diagnostics
MTBF mean (operating) time between failures (moyenne des temps entre pannes)
MTTR mean time to restoration (durée moyenne de réparation)
OEM original equipment manufacturer (fabricant de l'équipement d'origine)
RBD reliability block diagram (bloc-diagramme de fiabilité)
RCM reliability centred maintenance (maintenance basée sur la fiabilité)
NPR nombre prioritaire de risque
NPRA nombre prioritaire de risque alternatif
SFF safe failure fraction (proportion de défaillances en sécurité)
SIL safety integrity level (niveau d'intégrité de sécurité)
SOD severity, occurrence and detectability (sévérité, occurrence et détectabilité)

4 Vue d'ensemble

4.1 But et objectifs

Une AMDE est une méthode de décomposition d'une entité ou d'un processus en éléments dont les modes de défaillance et leurs effets sont identifiés et analysés, afin de déterminer les améliorations à apporter en éliminant les effets néfastes ou en réduisant leur vraisemblance ou sévérité. Une analyse de criticité peut être ajoutée pour hiérarchiser les modes de défaillance pour le traitement potentiel.

Une AMDE est réalisée pour les raisons suivantes:

- pour identifier les modes de défaillance qui ont des effets non souhaités sur le fonctionnement du système, par exemple empêcher ou dégrader significativement le fonctionnement ou affecter la sécurité de l'utilisateur ou d'autres personnes;
- pour améliorer de façon rentable la conception et le développement des entités ou des processus en intervenant très tôt dans le programme de développement;
- pour identifier les risques dans le cadre d'un processus de management du risque (ISO 31000);
- pour satisfaire aux obligations légales et professionnelles en démontrant que les risques prévisibles ont été identifiés et pris en compte;
- pour servir de base à d'autres analyses de sûreté de fonctionnement (l'Annexe D présente les relations entre l'AMDE et d'autres méthodes d'analyse de la sûreté de fonctionnement);
- pour développer et soutenir un programme d'essai de fiabilité;
- pour servir de base à la planification de la maintenance et des programmes de soutien, comme la maintenance basée sur la fiabilité (IEC 60300-3-11);
- comme un processus essentiel au système de gestion des actifs (ISO 55000).

De façon générale, l'AMDE est une méthode d'analyse des effets des défaillances uniques. Si l'AMDE est utilisée pour l'analyse des défaillances des entités interdépendantes, ces dernières peuvent alors être prises en compte dans l'analyse, avec des restrictions (5.3.6 et 5.3.7.2).

4.2 Rôles, responsabilités et compétences

Une AMDE exige qu'une ou plusieurs personnes (une équipe, par exemple) se chargent:

- de gérer le processus de réalisation de l'AMDE;
- de choisir le format de l'AMDE afin qu'elle soit adaptée au contexte d'application;
- d'identifier et d'analyser les modes de défaillance et les effets de l'entité ou du processus;

- de déterminer les traitements exigés;
- de consigner l'AMDE dans un rapport en incluant les traitements et les recommandations.

Le présent document utilise les termes suivants pour décrire les rôles et responsabilités dans la réalisation d'une AMDE.

a) Analyste

Personne chargée d'évaluer la pertinence d'une AMDE, de procéder aux adaptations nécessaires de l'AMDE, de s'assurer que la méthode AMDE est respectée et de communiquer avec les gestionnaires et les autres parties prenantes. Il convient que l'analyste dispose des compétences en matière d'AMDE et d'une bonne compréhension technique afin de motiver les autres personnes compétentes participant à l'analyse.

NOTE Dans le cadre d'un travail d'équipe, ce rôle de motivation peut être assuré par une personne parfois appelée «facilitateur».

b) Personnes compétentes

Personnes disposant des connaissances et de l'expérience nécessaires pour couvrir tous les aspects de l'entité ou du processus à analyser, y compris en matière sociale, économique et environnementale, selon ce qui est exigé.

c) Gestionnaire

Personne chargée de définir l'objectif de l'AMDE, d'autoriser l'utilisation des ressources, d'approuver l'adaptation et de gérer les actions et recommandations de traitement, selon ce qui est exigé. Ce rôle peut être endossé par un gestionnaire qui est l'autorité de conception finale.

d) Parties prenantes

Personnes ou organisations qui peuvent affecter, être affectées ou s'estimer être affectées par une décision ou une action. Par exemple, les clients (les titulaires du contrat, par exemple), les autorités (autorité de règlementation, par exemple), les utilisateurs (les fabricants et les personnes chargées de la maintenance, par exemple), les fournisseurs (les fournisseurs de service, les fournisseurs de composants, par exemple) et les personnes susceptibles d'être affectées par les défaillances peuvent être des parties prenantes.

4.3 Terminologie

Pour des raisons pratiques, dans le présent document, le titre «analyse des modes de défaillance et de leurs effets» abrégé en «AMDE» est utilisé comme terme générique pour représenter une application ou une adaptation de l'analyse, y compris l'AMDEC.

Le terme «entité ou «processus» est utilisé pour désigner le sujet de l'AMDE. L'entité ou le processus peut faire partie intégrante d'un système de plus grande envergure pour lequel plusieurs AMDE sont exigées. Des exemples de termes habituellement associés aux niveaux de hiérarchie supérieur, moyen et inférieur sont donnés dans le Tableau 1. La liste des termes du Tableau 1 n'est pas exhaustive. Par exemple, un logiciel peut être intégré dans un système matériel ou un système peut contenir des aspects humains.

Tableau 1 – Exemples de termes habituellement associés aux niveaux de hiérarchie

	Niveau supérieur	Niveau intermédiaire	Niveau inférieur
Matériel	Assemblage	Sous-ensemble	Composant
Logiciel	Progiciel	Module	Fonction de code exécutable
Processus	Procédure	Tâche	Étape

5 Méthodologie pour l'AMDE

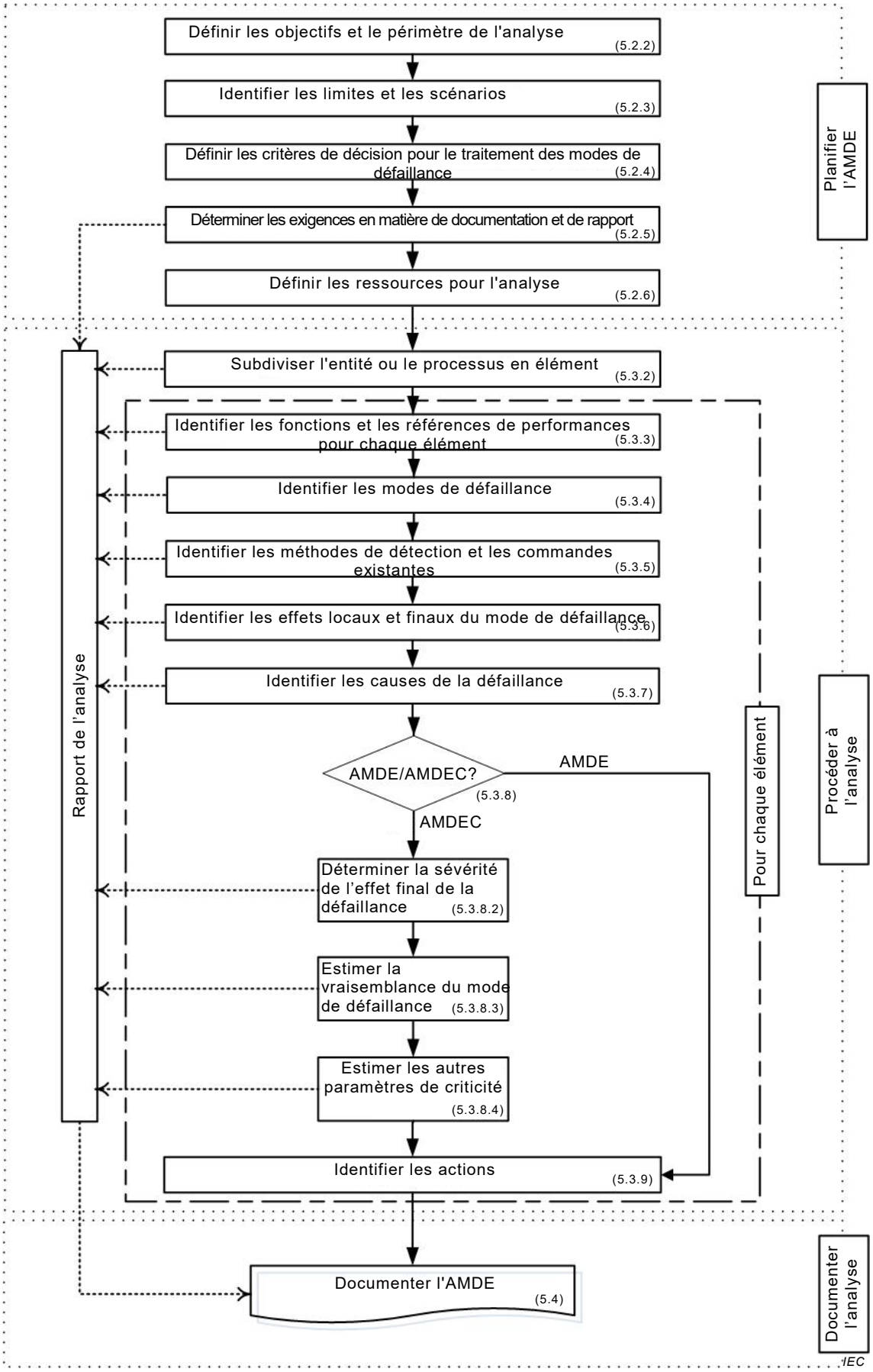
5.1 Généralités

La Figure 1 présente un diagramme des activités réalisées pendant une AMDE. Elle distingue trois phases: la planification, l'exécution et la documentation. Les activités sont en principe réalisées dans l'ordre, mais il y peut y avoir des répétitions lorsque, par exemple, une AMDE est réalisée dans le cadre d'un programme de développement ou que le système analysé est susceptible de changer.

Il convient de procéder à une AMDE en respectant la législation qui est en vigueur dans le périmètre de l'AMDE ou selon le type de risque à prendre en compte.

Si le présent document parle d'enregistrer, d'identifier, de spécifier, de décrire, d'établir ou de documenter certaines informations, cela signifie que les informations doivent être incluses dans la documentation AMDE correspondante (par exemple le rapport d'AMDE, le plan AMDE, la documentation post-AMDE comme le plan d'action).

Il convient d'adapter les activités présentées à la Figure 1 à l'application. Cela signifie que toutes les activités répertoriées ne sont pas nécessairement à réaliser. L'Annexe A constitue des recommandations générales et donne des exemples d'adaptation.



Les chiffres entre parenthèses se réfèrent aux paragraphes.

Figure 1 – Vue d'ensemble de la méthodologie AMDE avant l'adaptation

5.2 Planifier l'AMDE

5.2.1 Généralités

La planification d'une AMDE implique de se demander pourquoi une analyse doit être réalisée, quels sont les éléments de l'entité ou du processus à analyser et dans quels scénarios, et comment il convient de procéder à l'analyse de la manière la plus rentable et efficace. Il convient de consulter les gestionnaires et les parties prenantes, selon le cas, de manière à bien comprendre et prendre en compte leurs objectifs et leurs intérêts dans l'analyse.

Le résultat de la phase de planification est un plan d'AMDE qui décrit une application adaptée et rentable de l'AMDE pour le contexte particulier qui:

- définit les objectifs et le périmètre de l'analyse (5.2.2);
- identifie les limites de l'analyse et les scénarios d'utilisation (5.2.3);
- définit les critères de décision pour le traitement des modes de défaillance (5.2.4);
- détermine comment l'analyse sera documentée et consignée (5.2.5);
- spécifie la manière d'allouer les ressources aux activités d'analyse (5.2.6).

Le plan peut également inclure une description des facteurs ayant une influence sur la démarche de l'analyse, par exemple:

- une description des interfaces avec des jalons du projet pour déterminer le calendrier exigé des résultats d'analyse;
- les méthodologies ou la documentation pour la bonne compréhension de la fonction de l'entité ou de la séquence du processus;
- les exigences contractuelles;
- l'expérience acquise et les informations disponibles.

Le plan AMDE peut être autonome ou faire partie d'un document de niveau supérieur (un plan de projet ou un plan de gestion technique du système, par exemple).

5.2.2 Définir les objectifs et le périmètre de l'analyse

La définition des objectifs et du périmètre fixe les bases de l'analyse et informe du choix de l'approche retenue pour l'AMDE afin que ses résultats soient alignés sur les objectifs.

Il convient que les résultats de cette activité incluent:

- une formulation de but pour définir la raison de l'analyse;

EXEMPLE Explorer la fiabilité de la conception, identifier les moyens d'améliorer un processus ou une procédure pour réduire le nombre de défaillances, identifier les possibilités d'amélioration de la fiabilité, identifier les risques, satisfaire à une exigence contractuelle, suggérer des exigences en matière de programmes de maintenance et de supportabilité.

- une formulation des objectifs, qui définit le livrable final de l'AMDE en des termes permettant d'évaluer l'analyse comme étant aboutie ou pas.

Il convient d'inclure la formulation des objectifs dans le plan AMDE.

Pour certaines applications, il peut être pertinent de consulter les parties prenantes de manière plus formelle et de justifier les décisions et les résultats dans une formulation plus élargie.

5.2.3 Identifier les limites et les scénarios

5.2.3.1 Généralités

Il convient de décrire l'objet de l'analyse, ainsi que ses limites et conditions d'utilisation, afin de s'assurer que les utilisateurs de l'AMDE et le ou les analystes ont bien compris son périmètre. En effet, des aspects importants peuvent être oubliés à cause d'hypothèses erronées concernant le périmètre. Il convient de détailler cette description au fur et à mesure de l'avancée de la planification. Elle peut contenir des schémas (un organigramme, des blocs-diagrammes fonctionnels, des blocs-diagrammes de fiabilité, des diagrammes de structure à hiérarchie fonctionnelle par exemple) ou une référence à des documents contenant ce type d'informations.

Il peut être nécessaire de subdiviser les systèmes importants ou complexes (un réseau de chemin de fer, par exemple) en sous-systèmes (matériel roulant, signalisation, salle de commande, par exemple) et de réaliser une AMDE pour chacun d'eux. La subdivision peut être définie par les limites physiques ou fonctionnelles et peut être influencée par des exigences contractuelles ou des facteurs organisationnels. Il convient de choisir la subdivision de manière à ce que la taille de chaque AMDE reste gérable et de relier ces dernières de manière logique, afin de tenir compte de l'influence qu'exercent les sous-systèmes les uns sur les autres et sur le système dans son ensemble. Il convient de porter une attention particulière aux interfaces entre les sous-systèmes et de définir clairement leurs limites.

5.2.3.2 Déterminer le niveau et la démarche

Une AMDE peut être appliquée à n'importe quel niveau de subdivision d'une hiérarchie de l'entité ou du processus (Tableau 1). L'AMDE peut être abordée de différentes façons selon le but et l'étape de l'analyse. L'Annexe A fournit des recommandations et des exemples.

EXEMPLE Lors des premières étapes du développement, une AMDE peut être appliquée aux niveaux supérieurs ou intermédiaires de la hiérarchie, et les causes des modes de défaillance peuvent être limitées à la défaillance des éléments du ou des niveaux inférieurs suivants. Dans les dernières étapes du développement, les éléments du niveau inférieur de la hiérarchie pertinent par rapport aux objectifs sont pris en compte. Tous les modes de défaillance associés à cet élément et leurs effets sur le niveau supérieur suivant sont identifiés. Cependant, l'AMDE identifiera toujours les effets des modes de défaillance sur le niveau supérieur de la hiérarchie dans le domaine d'application de l'analyse.

5.2.3.3 Définir les limites de l'objet de l'analyse

Il convient de définir les limites, les relations et les interfaces entre l'objet de l'AMDE et les autres parties du système, y compris les interfaces humaines. Il convient que la définition des limites intègre les entrées et les sorties de l'entité ou du processus, et qu'elle précise de manière explicite les interfaces qui entrent dans le périmètre de l'analyse et celles qui en sont exclues.

Les limites dépendent du contexte et peuvent être influencées par des facteurs comme la conception ou l'utilisation prévue. Il peut être nécessaire de placer explicitement des entités ou des étapes de processus en dehors des limites afin de limiter la taille de l'AMDE ou parce que leur connaissance détaillée ne peut pas être obtenue.

Dans la mesure du possible, il convient de définir des limites afin de faciliter chaque AMDE et son intégration avec d'autres études connexes. Dans certains cas, il peut s'avérer utile de définir des limites d'un point de vue fonctionnel afin de limiter le nombre de liens vers d'autres entités ou processus n'entrant pas dans le cadre de l'analyse. Cela est souvent le cas si l'entité ou le processus est fonctionnellement complexe avec de nombreuses interconnexions dans ou au-delà des limites.

5.2.3.4 Définir les scénarios d'utilisation

Une AMDE est toujours réalisée dans le cadre d'un ou de plusieurs scénarios d'utilisation particuliers. Il convient de définir les scénarios d'utilisation dans le cadre desquels l'AMDE

doit être appliquée en fonction des objectifs de l'analyse, et de les décrire de manière suffisamment détaillée pour faciliter l'identification de tous les modes de défaillance pertinents. Les scénarios peuvent inclure des états définis hors de la condition d'utilisation normale spécifiée.

EXEMPLE Les scénarios peuvent être les suivants: «fonctionnement normal» ou «stockage» lors de l'analyse du matériel, «équipe de nuit» ou «intervention d'urgence» dans le cas d'une analyse de processus.

En principe, la description de scénario comprend les conditions environnementales physiques (les conditions ambiantes, par exemple) accompagnées des conditions générées par d'autres entités ou activités à proximité. D'autres facteurs pertinents sont les contraintes organisationnelles telles que les niveaux hiérarchiques, ou les contraintes physiques ou psychologiques qui peuvent avoir un impact sur le comportement humain.

Il convient de spécifier tous les facteurs de stress internes ou externes qui peuvent avoir un impact sur les modes de défaillance et leurs effets de manière à en tenir compte dans l'analyse.

Il convient d'établir un journal d'audit clair pour les documents utilisés pour définir les scénarios.

5.2.4 Définir les critères de décision pour le traitement des modes de défaillance

Avant de procéder à l'analyse, il convient de définir les critères de sélection des modes de défaillance à traiter et des priorités à affecter aux actions. Il convient que ces critères tiennent compte des objectifs de l'analyse, des exigences légales ou contractuelles et du point de vue des parties prenantes sur ce qui est acceptable. Il convient que les critères permettent de faire un choix cohérent et justifiable des modes de défaillance qui exigent un traitement et de ceux qui n'en exigent aucun. Il convient également d'indiquer si les traitements recommandés sont considérés comme étant suffisants. Il convient de faire valider et approuver les critères de traitement des modes de défaillance auprès du chef de projet.

Il convient de définir les types de conséquences pertinents pour l'analyse (par exemple, si les conséquences prises en compte impliquent un impact économique, des préjudices physiques ou psychologiques sur les personnes ou des effets intangibles comme une perte de réputation).

Les critères de décision peuvent être différents selon les applications de l'AMDE, et il convient, par exemple, d'y revenir régulièrement en fonction de l'expérience en service. Des traitements des modes de défaillance peuvent être recommandés dans le cadre de l'AMDE ou séparément dans le cadre du suivi.

En principe, les décisions relatives à la nécessité de traiter un mode de défaillance et aux priorités de traitement tiennent compte de la sévérité de l'effet d'une défaillance sur les objectifs et fonctions de l'ensemble du système, ainsi que des avantages et inconvénients relatifs des options de traitement choisies.

Dans certains cas, une analyse de criticité formelle peut être réalisée de façon à attribuer un classement de la criticité à chaque mode de défaillance. Les critères de définition de la criticité incluent:

- la sévérité de l'effet d'une défaillance sur les objectifs et fonctions du système ou du niveau supérieur pertinent pour l'objet de l'analyse;
- la vraisemblance d'occurrence d'un mode de défaillance, lequel donnant lieu à la sévérité indiquée de la conséquence; et
- l'aptitude à détecter à temps le mode de défaillance pour atténuer ou éviter l'effet d'une défaillance.

La sévérité et la vraisemblance d'une défaillance ou alternativement la sévérité, la vraisemblance et la détectabilité d'une défaillance, peuvent être combinées pour donner une mesure de criticité. Pour ce faire, une matrice/un graphe ou un nombre prioritaire de risque (NPR) peut être utilisé(e). Une unique méthode d'analyse de criticité ne peut être considérée comme étant applicable à tous les cas. L'Annexe B décrit deux méthodes couramment retenues. Elles peuvent être utilisées le cas échéant pour une application particulière ou être adaptées en fonction des besoins organisationnels.

NOTE 1 La méthode utilisée pour l'analyse de criticité peut être différente en fonction des projets, même au sein de la même organisation, bien qu'une approche cohérente de l'analyse de criticité s'avère en général profitable.

L'analyse de criticité est utile, notamment si les traitements font l'objet d'éventuelles contraintes liées aux coûts, à des difficultés techniques ou à des limites de temps.

L'analyse de criticité peut s'avérer inutile si tous les modes de défaillance identifiés doivent être traités ou si la quantité d'informations est insuffisante pour procéder à des estimations raisonnables de la valeur de criticité. De même, elle peut ne pas être rentable dans certaines applications.

NOTE 2 La criticité peut être considérée comme correspondant au risque. L'IEC/ISO 31010 constitue des recommandations supplémentaires relatives à l'analyse des risques.

Il convient que le plan AMDE détaille les critères de décision et, si une analyse de criticité est exigée, la méthode d'établissement de la criticité. Il convient également de détailler les critères de décision dans les rapports AMDE.

5.2.5 Déterminer les exigences en matière de documentation et de rapport

5.2.5.1 Généralités

Il convient que l'objectif soit de documenter de manière logique toutes les informations pertinentes, utilisées et générées pendant l'AMDE. Par conséquent, il convient que l'analyse et les résultats/recommandations qui en sont déduits soient faciles à comprendre. Il convient que la documentation AMDE fournisse un journal d'audit clair qui:

- décrit la façon dont le résultat est censé être utilisé;
- donne les informations pouvant apporter les éléments nécessaires à la justification des décisions reposant sur l'analyse;
- justifie l'adaptation de l'analyse, incluant la méthode utilisée pour le classement de la criticité;
- répertorie les sources d'informations utilisées dans l'AMDE avec des liens vérifiables vers celles-ci;
- respecte les obligations réglementaires et contractuelles et démontre que ces exigences sont satisfaites.

Le résultat de l'AMDE peut servir dans d'autres analyses ou peut simplement faire l'objet d'un rapport d'AMDE.

Il convient de choisir le format de la documentation AMDE dans le cadre de l'activité de planification AMDE. Il convient de mettre en forme le rapport d'AMDE selon les normes et procédures de l'organisation tout en tenant compte des objectifs, de la complexité et de l'étendue de l'AMDE. La documentation générée lors de l'AMDE peut être une combinaison de bases de données, de documents électroniques et de rapports papier. Il convient de définir les moyens de maintenir la traçabilité entre ces supports potentiellement disparates.

L'AMDE étant itérative, la documentation est développée progressivement tout au long de la durée de vie de l'entité ou du processus qui fait l'objet de l'analyse. Il convient de mettre à jour la documentation AMDE à des moments appropriés à l'application (à des moments précis du projet ou au fur et à mesure de la disponibilité des informations, de l'avancée des études

techniques, de l'identification et de la mise en œuvre des actions de traitement/d'atténuation ou du retour d'utilisation et de l'expérience accumulée, par exemple). Il convient de contrôler les révisions de la documentation AMDE tout au long du processus de contrôle des documents de l'organisation. Il convient d'intégrer les enseignements d'une AMDE dans les projets futurs.

5.2.5.2 Contenu du rapport d'AMDE

Il convient que le rapport contienne au moins:

- une description du système, de l'entité ou du processus faisant l'objet de l'analyse, ainsi que le bloc-diagramme, les schémas fonctionnels et les organigrammes appropriés qui définissent la structure;
- une description précise du périmètre et des limites, en notant toutes les exclusions particulières à celui-ci;
- les critères utilisés pour définir si un traitement est nécessaire;
- les hypothèses formulées sur l'entité ou le processus en cours d'analyse et les scénarios d'utilisation pertinents;
- une description claire et détaillée de la méthodologie qui étaye l'analyse;
- une identification de la ou des parties prenantes et du personnel impliqués;
- une description de la méthode d'analyse de criticité utilisée, qu'il convient de décrire avec suffisamment de détails pour permettre une vérification indépendante;
- les sources des données et autres documentations applicables (y compris les états/révisions) sur lesquelles repose l'AMDE;
- l'identification des modes de défaillance, leurs effets et, si approprié, leur criticité et leurs causes. Il convient d'exprimer les modes de défaillance et leurs effets sans faire référence à des documents qui ne sont pas identifiés dans le rapport;
- un récapitulatif des résultats et des traitements recommandés, s'ils ont été générés, y compris les recommandations d'analyses approfondies, si approprié. La documentation AMDE ne peut inclure qu'une brève déclaration des traitements recommandés. Toutefois, ces traitements nécessitent d'être gérés dans un plan d'action hors de la documentation AMDE;
- les limitations ou les insuffisances de l'AMDE auxquelles il convient de remédier par des mises à jour ultérieures de l'AMDE;
- les changements de conception qui ont déjà été intégrés dans l'entité résultant de l'AMDE et toutes les actions non résolues. Dans certains cas, aucune action ne peut être exécutée même si un traitement a été identifié pendant l'AMDE. Dans ce cas, il convient de justifier la décision de ne pas faire l'action dans la documentation de gestion des actions, et de mettre à jour la documentation AMDE avec la décision finale. Il convient, si nécessaire, de surveiller et d'examiner les éventuels impacts de l'absence d'action sur le traitement;
- les enregistrements d'analyse, qui peuvent être inclus dans une annexe du rapport sous la forme de tableaux. Si ces enregistrements sont volumineux ou qu'une base de données a été utilisée, il convient d'indiquer à quel endroit les informations peuvent être consultées.

La collecte des informations, leur enregistrement, leur conservation et leur accès peuvent représenter un coût important pour une organisation, et il convient de veiller à s'assurer que tous les documents présentent une véritable valeur ajoutée pour l'AMDE. De nombreux formats de rapport d'AMDE sont possibles, le format choisi déterminant souvent les informations recueillies, les évaluations réalisées et les processus suivis pour produire les résultats. L'Annexe C fournit des exemples de tableaux d'AMDE.

5.2.6 Définir les ressources pour l'analyse

5.2.6.1 Ressources informationnelles

Les informations suivantes sont en général exigées pour procéder à une AMDE:

- l'entité ou le processus à analyser, ses objectifs et son rôle dans l'ensemble du système;
- les éléments de l'entité ou du processus et leurs caractéristiques, performances, rôles et fonctions;
- les liens logiques, physiques et fonctionnels entre les éléments (blocs-diagrammes de fiabilité, blocs-diagrammes fonctionnels, organigrammes, schémas du système, versions logicielles, structure et processus de contrôle, par exemple). Ces informations peuvent avoir déjà été rassemblées lors de l'analyse de la sûreté de fonctionnement associée (Annexe D);
- le niveau de redondance et la nature des pièces de rechange, les équipements ou processus redondants ou les chemins de traitement parallèles;
- la position et l'importance de l'entité ou du processus dans le contexte de l'organisation (si possible);
- les entrées et sorties de l'entité ou du processus et ses éléments;
- les interfaces avec d'autres entités ou processus connexes, ainsi qu'avec l'environnement dans lequel l'entité opère;
- toutes les modifications apportées à la structure de l'entité pour les différents modes opérationnels;
- les bases de données génériques dans lesquelles figurent les modes de défaillance, leur occurrence relative et les taux de défaillance;
- les données d'expérience en service acquises sur le terrain;
- la précédente AMDE réalisée sur des entités ou processus identiques ou similaires, si approprié.

Les informations relatives aux fonctions, aux caractéristiques et aux performances sont exigées pour tous les niveaux d'entité ou de processus pris en considération, jusqu'au niveau le plus élevé dans les limites du périmètre, de sorte que l'analyse puisse permettre de répondre correctement aux modes de défaillance ayant un impact sur ces fonctions.

La collecte d'informations se poursuit pendant l'AMDE, l'analyse mettant souvent en évidence la nécessité de disposer d'informations supplémentaires. Les informations doivent être correctes et comprises par tous les participants. Les informations de base relatives à l'entité ou le processus analysé peuvent être mises à disposition dans un dossier avant le début de l'analyse, et il convient que l'analyste en charge de l'AMDE ait accès à l'ensemble des informations tout le temps.

5.2.6.2 Personnel

Des personnes aux compétences techniques et à l'autorité suffisante pour procéder à l'AMDE sont exigées. Les aptitudes et compétences nécessaires incluent:

- l'aptitude à appliquer la méthode AMDE;
- une bonne compréhension des aspects techniques de l'entité ou du processus en cours d'analyse et de ses modes de défaillance et de leurs effets;
- les aptitudes en tant que facilitateur (lorsque l'analyse est réalisée en équipe).

Cela peut exiger une approche avec une équipe pluridisciplinaire, dont la composition dépend des objectifs de l'analyse.

EXEMPLE Dans le cas d'un système d'information, un ingénieur système et un expert en logiciel peuvent faire partie de l'équipe.

Des connaissances supplémentaires et spécifiques du produit ou du service peuvent également devenir nécessaires au fur et à mesure de l'avancée de l'analyse. Si c'est le cas, il convient également que d'autres personnes compétentes participent à l'analyse.

5.2.6.3 Ressources physiques

Des ressources physiques sont en général exigées pour distribuer les communications et les analyses entre des équipes ou parties prenantes réelles ou virtuelles. Il peut s'agir de salles de réunion dédiées, de support audiovisuel pour les réunions virtuelles et de systèmes d'information partagés, incluant les bases de données existantes d'AMDE, etc. Il convient de choisir ces ressources sur la base du rapport coût/efficacité et de la valeur obtenue en termes de qualité, d'utilité (initiale et réutilisation) et d'opportunité des résultats de l'analyse.

5.3 Réaliser l'AMDE

5.3.1 Généralités

La procédure d'analyse est décrite de 5.3.2 à 5.3.9.

5.3.2 Subdiviser l'entité ou le processus en éléments

L'objet de l'analyse est subdivisé en éléments afin de procéder à l'AMDE, comme suit:

- un système peut être divisé en blocs fonctionnels;
- les éléments matériels peuvent être divisés en sous-ensembles ou composants matériels plus petits et moins complexes;
- les processus peuvent être exprimés en séquence d'activités, de tâches ou d'étapes;
- les logiciels peuvent être séparés en modules logiciels ou en fonctions de code exécutable;
- les interfaces individuelles peuvent être identifiées entre les éléments et entre un élément et l'utilisateur ou l'environnement.

NOTE 1 Dans une analyse, des éléments peuvent inclure un mélange de matériel, de logiciel et/ou de processus.

NOTE 2 Les personnes peuvent être considérées comme un élément d'un système ou les mécanismes d'erreurs humaines être pris en compte lors de l'analyse des causes de défaillance matérielle et/ou logicielle.

Le niveau de détail approprié pour l'analyse dépend du contexte et du résultat souhaité. En règle générale, un niveau de détail plus important dans le niveau de subdivision de l'objet de l'AMDE donne un niveau de détail équivalent sur les possibles modes de défaillance et leurs effets et permet des stratégies de traitement plus détaillées, mais l'analyse prend plus de temps.

5.3.3 Identifier les fonctions et les références de performances pour chaque élément

Une formulation claire de toutes les fonctions de chaque élément est exigée pour poser les bases de l'AMDE. Il convient de prendre en compte séparément chaque fonction d'un élément dans l'analyse.

Il convient de définir la référence de performance pour chaque fonction identifiée afin d'être en mesure de décider de ce qui constitue une défaillance, et ainsi d'identifier les modes de défaillance. Il convient que la fonction de chaque élément soit déduite de la spécification fonctionnelle ou d'autres sources disponibles.

Il convient que la référence de performance choisie représente le niveau de performance indispensable à la réalisation de la fonction de l'élément dans le contexte d'utilisation de l'entité ou du processus, plutôt qu'à la capacité de l'élément. Il convient que la référence de performance soit exprimée sans ambiguïté et si possible de façon quantitative.

5.3.4 Identifier les modes de défaillance

Il convient d'établir les manières dont chaque élément d'une entité ou d'un processus peut ne pas satisfaire à ses critères de performance. Un élément peut avoir plusieurs modes de défaillance. Il convient d'enregistrer chacun d'eux séparément. Il convient que l'analyse ait pour objet d'identifier tous les modes de défaillance plausibles et pertinents par rapport aux objectifs de l'analyse.

Selon l'objet et le périmètre de l'analyse, les éléments suivants sont pris en compte pour aider à l'identification des modes de défaillance de chaque élément sur l'ensemble du cycle de vie:

- l'application;
- le mode de fonctionnement;
- les spécifications opérationnelles pertinentes;
- les contraintes et tendances environnementales;
- les contraintes psychologiques et les changements sociaux;
- les contraintes opérationnelles liées au stockage, au transport et à la maintenance;
- les contraintes de processus liées au démantèlement ou au démontage.

En règle générale, les informations relatives au mode de défaillance peuvent être obtenues de la manière suivante:

- pour les nouvelles entités ou les nouveaux processus, référence peut être faite à d'autres entités ou processus aux fonction et structure similaires en termes de performance dans les conditions appropriées;
- pour les entités ou processus existants, les modes de défaillance peuvent être connus à partir des précédentes AMDE. Toutefois, il convient de rechercher les éventuelles différences entre l'ancienne et la nouvelle application qui pourraient donner lieu à différents modes de défaillance (A.2.1);
- l'expérience en service;
- les essais de performance et d'environnement, dans ou au-delà des limites spécifiées;
- des listes de vérification reposant sur les modes de défaillance génériques pour des types d'éléments particuliers;
- des bases de données de maintenance et de réparation;
- des bases de données d'incident et d'accident;
- les connaissances en la matière.

5.3.5 Identifier les méthodes de détection et les commandes existantes

5.3.5.1 Généralités

Pour chaque mode de défaillance, il convient d'identifier les commandes existantes et les méthodes de détection.

Dans ce contexte, les commandes sont les dispositions visant à empêcher ou réduire la vraisemblance du mode de défaillance ou visant à atténuer ses effets, alors que les méthodes de détection sont les moyens d'identifier le mode de défaillance, la défaillance ou la défaillance imminente.

La détection précoce d'une défaillance ou d'une défaillance imminente peut permettre aux opérateurs, aux personnes chargées de la maintenance, aux utilisateurs et à d'autres personnes d'intervenir et de réduire la vraisemblance des effets néfastes ou leurs conséquences. Dans les applications spécifiques, la commande et la détection peuvent avoir différentes significations, bien que l'intention soit similaire. L'Annexe E et l'Annexe F donnent respectivement des recommandations et des exemples spécifiques à l'application.

Si les commandes ou les méthodes de détection sont considérées comme étant inappropriées, il convient d'en déterminer de nouvelles et de poser les bases des traitements recommandés (5.3.9).

5.3.5.2 Méthodes de détection

La détection peut prendre différentes formes en fonction du type d'AMDE réalisée.

EXEMPLE Les méthodes de détection peuvent être les suivantes: voyants d'avertissement ou alarmes, indicateurs, jauges ou dispositif de surveillance, essais de fiabilité pendant le développement, contrôle statistique du processus, déverminage sous contraintes, essais de performances, audits, examens, diagnostics.

Si plusieurs modes de défaillance peuvent être détectés par les mêmes moyens, il convient de décrire les moyens de lever les ambiguïtés de sorte qu'aucun des modes de défaillance ne reste non détecté et, si cela est approprié, qu'une action adéquate soit entreprise.

5.3.5.3 Commandes

Il convient de répertorier les caractéristiques de conception ou autres dispositions existantes permettant d'empêcher ou de réduire la vraisemblance du mode de défaillance ou de modifier ses effets, et de décrire la manière dont elles agissent.

EXEMPLE Les commandes peuvent inclure les entités redondantes ou les systèmes de sauvegarde qui assurent le fonctionnement continu si un ou plusieurs éléments venai(en)t à tomber en panne, le respect des normes techniques ou d'autres normes (autres moyens de fonctionnement en cas de détection d'un problème), les spécifications des matériaux, les réglages de la machine, la maintenance, la conception des entités et des processus tenant compte des facteurs humains.

5.3.6 Identifier les effets locaux et finaux du mode de défaillance

L'effet d'une défaillance est la conséquence d'un mode de défaillance dans le scénario défini pour l'analyse. Le même effet d'une défaillance peut être le résultat d'un ou de plusieurs modes de défaillance d'un ou de plusieurs éléments d'une entité ou d'un processus.

L'effet des modes de défaillance d'un élément peut être identifié au niveau local (il s'agit alors de l'effet local) et au niveau supérieur pertinent par rapport au sujet de l'analyse (appelé effet global ou effet final). Les effets aux niveaux intermédiaires peuvent également être identifiés, si pertinent.

NOTE 1 Le niveau local peut signifier qu'il s'agit du même niveau hiérarchique que l'entité en cours d'analyse ou de son emplacement physique.

Il est important d'identifier les effets finaux lors de la prise en compte de l'importance relative des défaillances, cela représentant un point de référence commun. L'identification des effets locaux donne des informations pouvant aider à concevoir des traitements alternatifs. Dans certains cas, le mode de défaillance lui-même peut ne pas générer d'effet local.

Outre les conséquences ayant un impact sur la fonction de l'entité ou du processus ou sur l'ensemble du système, il peut y en avoir d'autres liées, par exemple, aux exigences en matière de sécurité, d'environnement ou de conformité. Il convient d'avoir spécifié leur pertinence dans le plan AMDE.

NOTE 2 L'identification des conséquences finales d'un mode de défaillance peut exiger d'utiliser d'autres formes d'analyse (l'analyse par arbre d'événement, par exemple (IEC 62502)).

Il convient de décrire les effets d'une défaillance de manière suffisamment détaillée pour que l'utilisateur de l'AMDE soit en mesure de juger de leur importance. Les effets d'une défaillance sont déduits de la connaissance de l'entité ou du processus, de ses fonctions, de ses interactions et de sa place dans la hiérarchie en cours d'analyse. Souvent, pour simplifier l'analyse, les effets d'une défaillance sont classés dans des groupes en fonction de leur sévérité ou de la nature de l'effet.

Il convient que la description enregistrée de l'effet d'une défaillance contienne des informations suffisantes pour évaluer avec exactitude la sévérité et l'importance des conséquences. Il convient que la manière d'enregistrer les conséquences et que les types de conséquences à prendre en compte reposent sur ceux décrits dans le plan AMDE.

L'AMDE prenant en compte les effets finaux élément par élément ou fonction par fonction, il s'ensuit que les effets résultant de plusieurs défaillances ne sont en général pas identifiés. Cependant, dans certains cas (lors d'une analyse des fonctions de veille ou de sécurité, par exemple), une défaillance ne présentant aucun effet immédiat détectable (c'est-à-dire qui ne s'est pas révélée) peut avoir des conséquences au niveau supérieur par suite d'une deuxième défaillance qui n'aurait en d'autres circonstances eu aucune importance. Il convient d'enregistrer ces événements pour procéder à un examen ou une analyse plus approfondi(e).

EXEMPLE La défaillance d'un dispositif de protection donne lieu à des conséquences néfastes uniquement si le dispositif de protection et l'entité dont il assure la protection sont défaillants. Les conséquences de ce type de défaillances multiples sont indiquées dans l'enregistrement d'analyse.

NOTE 3 L'analyse par arbre de panne (IEC 61025) peut être utilisée pour déterminer l'impact des combinaisons de défaillances ou comprendre les fonctions redondantes et les relations entre les entités protégées et les entités de protection.

5.3.7 Identifier les causes de la défaillance

5.3.7.1 Généralités

Il est utile de comprendre comment une défaillance se produit afin de déterminer le meilleur moyen de réduire sa vraisemblance ou ses conséquences. Les étapes de l'AMDE n'incluent pas l'intégralité de la méthode d'analyse de causalité. Dans certains cas, il peut être utile d'identifier le mécanisme physique, logique ou psychologique de la défaillance, toutefois, ceci n’est pas toujours nécessaire pour atteindre les objectifs de l'analyse.

EXEMPLE L'identification qu'une fuite est due au mécanisme de corrosion peut donner lieu à une recommandation de changer la matière.

NOTE Des méthodes d'analyse causale plus détaillée sont données dans l’analyse de cause initiale (IEC 62740).

Il convient d’approfondir l’analyse des causes de défaillance en fonction du rapport coût/efficacité de cette opération. Par exemple, plus d'efforts pourraient être consacrés à l'analyse des causes de défaillance ayant un impact significatif sur les fonctions et objectifs qu'à celles ayant un impact moins important.

Lors de l'identification des causes, il convient de tenir compte du contexte d'utilisation. Il convient de prendre en compte les causes liées aux aspects matériels, logiciels, humains et à leurs interfaces.

5.3.7.2 Défaillances de cause commune et défaillances de mode commun

Il convient qu'une AMDE prenne en compte les origines possibles de défaillance de cause commune (DCC). Une défaillance de cause commune est une défaillance dans laquelle plusieurs éléments font l'objet d'une défaillance simultanée ou, sur une durée suffisamment courte, ont l'effet de défaillances simultanées. Par conséquent, les défaillances de cause commune sont contraires à l'hypothèse fondamentale qui stipule que les modes de défaillance pris en compte dans une AMDE sont indépendants. Une défaillance de cause commune se rapporte à des cas où la cause est associée aux éléments eux-mêmes.

EXEMPLE 1 Le dimensionnement incorrect d'un composant prévu pour fonctionner à des températures élevées est une cause de défaillance de l'alimentation électrique. Ainsi, lorsque la température élevée prévue est atteinte, plusieurs alimentations électriques font l'objet d'une défaillance sur une courte période.

NOTE Une entité ou un processus qui utilise la redondance ou plusieurs contrôles (procéduraux) pour assurer le fonctionnement ou pour atténuer les conséquences d'une éventuelle défaillance est sujet(te) aux défaillances de cause commune.

Si une commande est susceptible de faire l'objet d'une défaillance et que la même cause que celle de l'élément qu'il protège en est à l'origine, il convient d'inclure cette DCC en tant que cause de défaillance comme les autres causes, les raisons justifiant cette action étant incluses dans la documentation.

Les défaillances de mode commun se produisent dans un certain nombre d'éléments qui tombent en panne de la même manière (c'est-à-dire selon le même mode de défaillance) par les mêmes causes ou par des causes différentes. C'est souvent le problème lorsque la perte de fonction concerne des entités redondantes utilisant la même technologie et construites de la même façon.

EXEMPLE 2 L'utilisation de composants sous-dimensionnés (condensateurs) présentant un taux de défaillance anormal dû à la surcharge peut donner lieu à une défaillance de mode commun de court-circuit dans les entités redondantes.

Il convient d'identifier et de traiter une défaillance de mode commun dans le cadre d'un processus d'analyse normal si l'élément approprié relève du domaine d'application. Les origines et les effets des défaillances de mode commun peuvent être mieux appréhendés avec des méthodes comme l'analyse par arbre de panne (IEC 61025).

5.3.7.3 Aspects humains

Les êtres humains peuvent être considérés comme un élément de l'entité ou du processus faisant l'objet des modes de défaillance, une erreur humaine pouvant par ailleurs être identifiée comme une cause de défaillance d'un élément matériel, logiciel ou de processus, y compris leurs interfaces.

L'analyse des causes d'erreur humaine tend à être plus complexe que celle des causes de défaillance matérielle ou logicielle, les mécanismes de défaillance éventuels étant bien plus nombreux, et chacun ayant des causes potentielles multiples. Ne pas tenir compte d'un ensemble de mécanismes psychologiques peut donner lieu à une analyse trop simpliste et erronée des causes, et donc à des stratégies de traitement inappropriées.

EXEMPLE 1 Le mode de défaillance «action omise» peut se produire lorsqu'une personne perd le fil d'une séquence par distraction, parce qu'elle a formulé des hypothèses erronées ou parce qu'elle n'a pas les connaissances nécessaires de la séquence exigée. Si une action est omise par distraction ou désinvolture, une formation supplémentaire peut ne servir à rien, voire même être contreproductive.

NOTE 1 Les causes d'erreur humaine et les facteurs qui façonnent les performances humaines sont donnés dans l'IEC 62508. L'IEC 62740 propose une taxonomie des modes d'erreur humaine, de leurs mécanismes et de leurs causes, ainsi que des méthodes formelles qui peuvent être utilisées pour analyser l'erreur humaine.

NOTE 2 Les êtres humains peuvent commettre des erreurs volontaires et involontaires.

Les traitements utilisés pour remédier aux défaillances humaines tentent de réduire la vraisemblance de l'erreur susceptible de se produire. Étant donné qu'il peut s'avérer difficile de l'éliminer, il s'agit en premier lieu de faire en sorte que l'entité ou le processus soit plus tolérant(e) aux erreurs.

EXEMPLE 2 Dans le processus de pilotage d'un train, comme dans celui de rendre les signaux aisément visibles, des verrouillages peuvent être prévus pour empêcher le mécanicien de franchir des signaux en cas de danger, quelle que soit la cause de l'erreur.

5.3.8 Évaluer l'importance relative des modes de défaillance

5.3.8.1 Généralités

Il convient que le plan AMDE précise s'il convient de tenir compte de l'importance relative des modes de défaillance et spécifie la manière dont il convient de le faire.

La hiérarchisation peut avoir lieu soit dans le cadre de l'analyse de chaque mode de défaillance puisque chaque mode de défaillance est analysé pour ses effets, soit après avoir identifié tous les modes de défaillance. Le résultat est une liste de tous les modes de

défaillance hiérarchisés dans l'ordre d'importance, permettant d'identifier les modes de défaillance pouvant nécessiter un traitement. En principe, il convient que les priorités d'action tiennent compte également du rapport coût/efficacité des traitements disponibles, de leur facilité de mise en œuvre et de leur impact sur les autres parties du système.

5.3.8.2 Déterminer la sévérité de l'effet final d'une défaillance

Il convient que la sévérité déterminée pour chaque mode de défaillance représente l'importance de ses effets sur le niveau supérieur du système ou de l'entité (l'effet final) ou sur les objectifs du processus. Il convient de clairement spécifier la signification du niveau supérieur dans le contexte de l'analyse.

EXEMPLE 1 L'analyse d'une entité peut être réalisée par un fabricant qui évalue la conception de son produit, auquel cas la sévérité est exprimée en termes d'effets sur les performances de l'ensemble de l'entité. La même entité peut être analysée dans le cadre d'un groupe d'entités, auquel cas la sévérité est liée aux effets sur les performances du groupe.

EXEMPLE 2 Un processus ou une procédure peut être analysé(e) afin de l'évaluer en termes d'impact sur une petite unité ou un petit groupe, ou dans le cadre d'un processus plus large.

NOTE La sévérité d'un effet peut sembler plus importante aux niveaux inférieurs d'une hiérarchie de l'entité si la redondance ou d'autres fonctions de commande/actions ne sont prises en compte qu'aux niveaux supérieurs de la hiérarchie.

Pour assurer la cohérence de la hiérarchisation des modes de défaillance dans l'AMDE, il convient d'évaluer la sévérité selon une échelle commune clairement identifiée qui couvre les types de conséquences spécifiés dans le plan (5.2.4). Voir l'Annexe B pour de plus amples informations.

5.3.8.3 Estimer la vraisemblance du mode de défaillance

Lorsque cela est exigé, il convient de déterminer la vraisemblance d'occurrence de chaque mode de défaillance comme entrée d'une méthode d'analyse de criticité (Annexe B) ou lorsque des résultats d'analyse doivent alimenter d'autres analyses de sûreté de fonctionnement (Annexe D).

Lors de l'estimation de la vraisemblance d'occurrence d'un mode de défaillance, il convient de tenir compte des facteurs techniques, humains, organisationnels et environnementaux qui peuvent avoir un impact sur la défaillance et sa vraisemblance.

Si la vraisemblance d'occurrence d'un mode de défaillance est estimée, il convient d'indiquer clairement la période de temps prise en compte pour les estimations. Il convient d'adapter la période choisie aux objectifs de l'AMDE.

EXEMPLE Les périodes de temps souvent utilisées sont la période de garantie, la durée de vie utile prévue de l'entité, la période d'utilisation spécifique de l'entité ou du processus et la durée de travail.

La vraisemblance d'occurrence d'un mode de défaillance peut être estimée par un grand nombre de méthodes et de sources, y compris:

- les données d'essai de durée de vie du composant ou les taux d'erreur humaine obtenus en laboratoire;
- les bases de données disponibles des modes, taux et probabilités de défaillance ou des indisponibilités;
- les données sur les défaillances en exploitation;
- la surveillance des performances humaines;
- les données de défaillance pour des entités similaires utilisées de manière comparable.

NOTE Il existe des bases de données des modes de défaillance pour les composants d'équipement les plus souvent utilisés (MIL-HDBK-338B, IEC 62308, par exemple), pour les modes d'erreur humaine (Bell and Holroyd, 2009, par exemple), pour les méthodes d'évaluation de la fiabilité humaine (l'IEC 62508, par exemple) et pour l'évaluation de la défaillance d'entités similaires (l'IEC 61709, par exemple).

5.3.8.4 Estimer d'autres paramètres de criticité

Si une analyse de criticité doit être réalisée, des paramètres autres que la vraisemblance et la sévérité peuvent également être évalués. Par exemple, un paramètre supplémentaire souvent utilisé pour évaluer la criticité est le classement de «détectabilité». Un mode dans lequel une défaillance ou une défaillance imminente peut être aisément détectée est en principe moins important qu'un autre dans lequel il n'existe aucun moyen de détecter la défaillance avant que des conséquences néfastes ne se produisent. L'Annexe B contient des exemples d'utilisation de classement de détectabilité dans l'analyse de criticité.

NOTE Dans certaines applications de l'AMDE, notamment dans le secteur automobile, la détectabilité a un sens différent. Il s'agit d'une partie de l'identification d'un mode de défaillance potentiel pendant un programme de développement.

Comme pour le classement de détectabilité, un autre paramètre exprimant l'efficacité des commandes existantes (atténuation) peut être utile pour le classement de la criticité du mode de défaillance.

5.3.9 Identifier les actions

5.3.9.1 Généralités

Selon le périmètre de l'AMDE, il convient d'identifier, d'évaluer et de documenter les actions possibles pour les modes de défaillance exigeant un traitement (5.2.4). Dans certains cas, seuls les traitements apparaissant évidents de prime abord sont documentés dans l'AMDE, le choix de la solution finale faisant l'objet d'une analyse approfondie et d'un compromis hors du cadre de l'AMDE.

Il peut également s'avérer nécessaire de procéder à une AMDE plus détaillée dans un domaine de préoccupation particulier ou de procéder à une analyse de causalité avant de formuler des recommandations.

Les raisons qu'il convient de documenter et justifiant de recommander ou pas un éventuel traitement reposent sur les critères de décision (5.2.4) convenus dans le plan AMDE. Lors de la détermination d'un traitement, il convient d'être vigilant quant à l'interprétation des facteurs utilisés pour la détermination de l'importance des modes de défaillance.

Lors de la détermination des traitements, il convient que le niveau d'exactitude et de fidélité ne soit pas incohérent avec les données et méthodes utilisées même si l'AMDEC a été quantifiée.

5.3.9.2 Options de traitement

Les traitements peuvent impliquer de modifier la conception de l'entité ou du processus, et les actions à mettre en place pendant l'exploitation ou pendant la maintenance du matériel.

En règle générale, il est plus rentable de procéder aux modifications pendant la conception, notamment pour les entités matérielles.

EXEMPLE 1 Les modifications de conception incluent le remplacement de composants par d'autres composants plus fiables, l'introduction de systèmes de redondance ou de sauvegarde, la conception ergonomique du matériel ou des processus pour réduire la probabilité d'erreur, des moyens nouveaux ou améliorés permettant à une entité, à des opérateurs, à des utilisateurs, entre autres, de pouvoir détecter une défaillance, et des dispositifs de sécurité ou de détente visant à limiter les dommages.

Pendant l'exploitation, une action peut être prise pour détecter un mode de défaillance ou une défaillance imminente de manière à l'éviter ou à réduire ses effets.

EXEMPLE 2 En ce qui concerne le matériel, les traitements éventuels incluent l'isolation, la réduction de charge, le réacheminement et l'activation des fonctions de suppression. Pour ce qui est des processus, les traitements éventuels incluent les vérifications et ajustements réalisés pendant une procédure.

Les programmes de maintenance peuvent également être utilisés comme moyens de contrôle, et il convient de les développer de manière structurée à partir des résultats de l'AMDE.

NOTE La maintenance basée sur la fiabilité (IEC 60300-3-11) est un processus de développement de ce type de programme.

Un traitement peut déboucher sur un ou plusieurs des points suivants:

- l'élimination du mode de défaillance;
- la réduction de la vraisemblance du mode de défaillance;
- l'élimination ou la réduction des effets du mode de défaillance.

Il convient d'utiliser le critère de décision (5.2.4) pour identifier les modes de défaillance qui exigent un traitement. Dans certains cas, aucune action ne peut être exécutée même si un traitement a été identifié pendant l'AMDE.

Il convient également d'envisager de retirer les moyens de contrôle inefficaces ou inutiles.

Il convient que la documentation inclue au minimum une brève formulation de toute recommandation énoncée.

Si les recommandations sont acceptées et que de nouvelles commandes ou méthodes de détection sont introduites, il peut s'avérer nécessaire de réexaminer l'analyse pour vérifier si:

- de nouveaux modes de défaillance ou effets ont été introduits; et
- la criticité des modes de défaillance particuliers est désormais acceptable.

Il convient d'identifier les modifications de la documentation de l'entité ou du processus à prendre en compte dans la prochaine mise à jour de l'AMDE.

5.4 Documenter l'AMDE

Il convient de documenter et d'enregistrer l'analyse conformément au plan AMDE (5.2.5).

Annexe A
(informative)

Considérations générales relatives à l'adaptation d'une AMDE

A.1 Généralités

A.1.1 Vue d'ensemble

L'adaptation permet de personnaliser une AMDE afin de disposer d'un moyen rentable d'atteindre ses objectifs, ce qui implique de choisir:

- les limites du système, de l'entité ou du processus à analyser;
- le point de départ de l'analyse dans la hiérarchie;
- le niveau de détail de la subdivision de l'objet à analyser en éléments;
- les étapes de l'analyse à prendre en compte;
- le niveau de détail de chaque étape de l'analyse;
- si les modes de défaillance sont hiérarchisés en fonction de leur criticité, et la méthode d'évaluation à utiliser.

En règle générale, ces choix sont complétés par des facteurs tels que:

- l'objet de l'analyse (amélioration ou modification d'une entité ou d'un processus, réalisation d'une étude de sûreté de fonctionnement (IEC 62741), démonstration de la conformité, planification de la maintenance ou du support logistique, sécurité, par exemple);
- la mesure dans laquelle le processus ou l'entité est nouveau/nouvelle ou innovant(e) (la technologie, par exemple);
- la disponibilité des données pertinentes (expérience opérationnelle pour des entités similaires, données d'essai, par exemple);
- s'il est exigé de recommander des traitements ou si cela a lieu hors du cadre de l'AMDE;
- les exigences légales ou contractuelles;
- pour une entité, la maturité de la conception ou du projet, et;
- le stade du cycle de vie auquel l'AMDE est réalisée.

En règle générale, il convient également de tenir compte de la possibilité que certaines entités ou certains processus, ou leurs éléments puissent ne pas faire l'objet d'une AMDE sous quelque forme que ce soit, notamment si elle ne présente aucun avantage clairement identifiable ou si d'autres formes d'analyse de sûreté de fonctionnement sont considérées comme étant plus utiles. Une AMDE tire sa valeur dans une affaire du fait, par exemple, d'avoir un impact sur la conception, sur le fonctionnement et sur l'apport d'informations pour le développement de programmes de maintenance préventifs et correctifs rentables. Si les résultats d'analyse ne peuvent pas influencer ces facteurs, une AMDE peut ne pas se justifier.

NOTE Dans la plupart des cas, les entités ou éléments de produits commerciaux (COTS) provenant de fournisseurs spécialisés peuvent uniquement être traités comme des «boîtes noires», dont l'analyse peut uniquement être satisfaisante pour les interfaces (les entrées et les sorties, par exemple).

Des exemples de choix adaptés dans des applications industrielles spécifiques sont donnés à l'Article A.3. Les considérations en matière d'application générale de l'AMDE sont données à l'Annexe E.

A.1.2 Point de départ de l'AMDE dans la hiérarchie

Le choix du point de départ pour l'adaptation d'une AMDE dépend de l'objet et de l'étape de l'analyse et de la façon dont la meilleure valeur est obtenue (5.2.3.2).

Une approche descendante fait référence dans le présent document à une analyse dont le point de départ se situe aux niveaux supérieurs ou intermédiaires de la hiérarchie, et dont les causes des modes de défaillance se limitent à la défaillance des éléments du ou des niveaux inférieurs suivants.

Une approche ascendante fait référence dans le présent document à une analyse dont le point de départ se situe aux éléments du niveau inférieur pertinent de la hiérarchie par rapport aux objectifs.

L'approche descendante décrite est généralement utilisée lors des premières étapes de la conception, par conséquent elle peut produire des résultats approfondis et/ou étendus incomplets en raison de la limitation délibérée du domaine d'application ou du manque d'information disponible. Toutefois, un début précoce de l'analyse (à l'aide d'évaluations si nécessaire) peut avoir un effet positif sur la sûreté de fonctionnement et le coût de la future entité. Si le projet se poursuit vers un développement à grande échelle, il convient que l'AMDE soit complétée via l'approche ascendante détaillée afin qu'elle remplisse ses fonctions.

NOTE 1 Dans le présent document, le terme «descendante» est utilisé pour décrire l'approche de développement de l'AMDE. Il n'est pas destiné à être interprété de la même façon que dans une analyse par arbre de panne.

NOTE 2 Si le domaine d'application de l'analyse est plus vaste que la performance inhérente de l'entité (s'il inclut des événements externes comme les incendies, les inondations ou l'influence de l'opérateur, par exemple), ou que la poursuite de son développement est peu probable (une étude de faisabilité contrainte, par exemple), alors une analyse par arbre de panne peut constituer une technique plus utile qu'une AMDE.

Le Tableau A.1 récapitule les caractéristiques des approches descendantes et ascendantes. Ces caractéristiques permettent de prendre en compte la valeur de chaque approche.

Tableau A.1 – Caractéristiques des approches descendantes et ascendantes de l'AMDE

	Caractéristiques
Descendante	Il s'agit le plus souvent d'une analyse fonctionnelle destinée à concentrer les efforts sur les exigences ou fonctions les plus importantes de l'entité ou du processus. Aux premières étapes du développement, lorsque seules les exigences fonctionnelles d'un niveau supérieur sont connues. Pour aider à déterminer la structure d'AMDE plus détaillées et réalisées ultérieurement (qui peuvent être ascendantes), particulièrement dans les systèmes complexes. Peut être appliquée lorsque des effets particuliers présentent un intérêt et que seuls les modes de défaillance exigent d'être examinés. Peut être rentable si l'analyse met l'accent sur des éléments ou fonctions particuliers présentant un intérêt. Permet d'évaluer la perte de fonction au niveau de l'entité, mais limite les résultats à une évaluation de la manière dont des événements de défaillance prédéfinis sont susceptibles de se produire, plutôt que de tenter d'identifier toutes les défaillances qui peuvent se produire. L'approche exige du jugement pour évaluer à quel moment de l'analyse le passage aux niveaux inférieurs de la hiérarchie ne fournirait que peu d'informations ou des informations inutiles pour répondre aux objectifs de l'analyse. Peut assurer l'identification des exigences aux niveaux inférieurs.
Ascendante	Cette approche est le plus souvent appliquée lorsque les éléments individuels d'une entité ou d'un processus sont examinés au niveau détaillé le plus pertinent et que les effets de leur défaillance sont analysés aux niveaux supérieurs spécifiés de la hiérarchie. Permet de s'assurer dans une plus large mesure que tous les modes de défaillance potentiels ont été pris en compte au fur et à mesure de la formulation des hypothèses en fonction des boîtes noires COTS ou des éléments agrégés dans des modules jetables non réparables complexes. Adaptée à l'identification de tous les effets possibles lors du déploiement d'une nouvelle structure de composants ou d'entités existantes dans un nouvel environnement ou une nouvelle application. Souvent utilisée pour les nouvelles conceptions où l'éventail des effets au niveau supérieur ou plus élevé peut ne pas être connu. N'exige aucune connaissance des exigences fonctionnelles au niveau supérieur de l'entité, la perte de fonction à ce niveau étant déduite de la propagation des effets d'une défaillance du composant dans toute la structure de la hiérarchie de l'entité. Peut considérablement augmenter la taille de l'AMDE et, de ce fait, l'effort nécessaire pour réaliser l'analyse.

A.1.3 Niveau de détail de l'analyse

L'AMDE peut être développée à différents niveaux de détail de manière à apporter des informations supplémentaires (pour analyser les éventuelles options de traitement ou faciliter les analyses connexes du programme d'exploitation, de maintenance ou de support logistique, par exemple). La profondeur et l'ampleur d'une AMDE dépendent inévitablement de la complexité du système, de l'entité ou du processus qui fait l'objet de l'analyse.

A.1.4 Hiérarchisation des modes de défaillance

Il peut être utile d'étendre une AMDE en intégrant une analyse de criticité lorsqu'il est exigé de mesurer l'importance relative d'un mode de défaillance particulier. Ces informations sur l'importance relative peuvent être utilisées lors de la planification des priorités pour l'évaluation du traitement et les actions à exécuter. Si tous les modes de défaillance doivent être traités de la même façon (pour la conformité réglementaire, par exemple), il peut ne pas être utile de procéder à une analyse de criticité.

Il n'est pas nécessaire de ne tenir compte que de la sévérité ou de la criticité lors du choix des priorités de traitement. Par exemple, le rapport coût/efficacité des traitements disponibles, leur facilité de mise en œuvre et leur impact sur les autres parties du système peuvent également être pris en compte.

L'évaluation des paramètres (la sévérité et la vraisemblance, par exemple) peut reposer sur des échelles de mesure quantitative ou qualitative.

- Des échelles quantitatives peuvent être utiles lorsque l'expérience en service, les données d'essai ou les prévisions sont pertinentes, disponibles et qu'elles permettent d'attribuer un taux ou une probabilité de défaillance à des modes de défaillance spécifiques.
- Des échelles qualitatives peuvent être utiles lorsque les défaillances doivent être hiérarchisées, mais qu'aucune information détaillée n'est disponible ou que l'entité n'est pas suffisamment définie pour être en mesure d'utiliser les données quantitatives pertinentes.

Le Tableau A.2 récapitule les caractéristiques d’application générales des évaluations de criticité qualitatives et quantitatives des approches ascendantes et descendantes de l’AMDE.

L'Annexe B donne des recommandations détaillées relatives aux méthodes d’analyse de criticité.

Les recommandations présentées à l'Article A.1 sont d’ordre général. Des considérations plus spécifiques peuvent être exigées dans les applications données. Par exemple, les systèmes essentiels pour la sécurité peuvent exiger une preuve tangible démontrant qu'ils ont été conçus ou choisis de manière à identifier, analyser, évaluer et traiter en toute transparence la vraisemblance et la sévérité d'une défaillance. L'AMDE peut être personnalisée pour présenter, par exemple, la traçabilité de l'atténuation ou du traitement tout en démontrant que la méthode utilisée est appropriée au contexte de l'application. D'autres considérations relatives aux questions liées aux types d’application communs sont présentées à l'Annexe E.

Tableau A.2 – Application générale des approches communes de l'AMDE

	Analyse qualitative	Analyse quantitative
Descendante	En général réalisée dès le début de la conception d'une entité, lorsque l'approche peut être rentable, permettant d'arrêter l'analyse lorsqu'elle a atteint un niveau auquel l'entité ne peut plus être décomposée ou auquel, pour une raison ou une autre, le mode de défaillance ne peut plus être connu. Un exemple d'application est une vérification de fiabilité à bas coût du programme de soutien mise en place par un OEM pour une entité mature, qui présente certaines correspondances avec les modes de défaillance prévus lors de la conception. Cela peut être obtenu par une analyse descendante indiquant la traçabilité entre les tâches de maintenance définies et les modes de défaillance atténués ou gérés. Au début de la conception, une approche descendante peut ne pas faire appel à une évaluation qualitative s'il s'agit uniquement d'explorer et de comprendre les modes de défaillance et leurs effets.	En général compatible avec la conception de nouvelles entités, lorsque l'architecture est connue et que le traitement porte sur l'identification des opportunités d'amélioration de la conception en hiérarchisant les modes de défaillance et leurs effets. Cette forme d'analyse fournit également un journal d'audit entre les modes de défaillance, leurs effets et la valeur potentielle des actions d'atténuation, mais elle peut être plus difficile à réaliser. Généralement justifiée lorsque des résultats vérifiables sont nécessaires tels que pour des demandes réglementaires ou si la démonstration d'un retour sur investissement positif est exigée.
Ascendante	Généralement appliquée à des entités existantes, complexes et souvent anciennes, lorsque les données de performances quantitatives réelles peuvent ne pas être aisément disponibles. Peut être utilisée lorsqu'une modification importante d'une entité exige d'intégrer un nouvel équipement pendant la conception, et que les données ne sont pas disponibles pour procéder à une analyse quantitative. Incite l'analyse à commencer à un niveau de détail qui répond à ses intentions (éviter d'appliquer une AMDE à des entités COTS, par exemple, lorsque l'effort ne facilite pas la compréhension et que peu d'options permettent de modifier la conception).	Généralement utile à la fin de la conception de l'élément, pour démontrer la conformité à la spécification de conception et fournir une documentation détaillée à utiliser dans d'autres analyses (sécurité ou support logistique, par exemple). Une analyse présentée sous cette forme peut être longue et coûteuse. Elle est en général justifiée uniquement lorsqu'un volume de production important ou que les effets sévères d'une défaillance d'une entité particulière indiquent que l'application du processus AMDE est susceptible d'assurer un retour sur investissement.

A.2 Facteurs ayant un impact sur l'adaptation de l'AMDE

A.2.1 Réutilisation des données/informations de l'analyse d'une entité similaire

La réutilisation des données issues d'une analyse précédente présente l'avantage de réduire les efforts et de gagner du temps. Toutefois, les données doivent être valides pour la nouvelle analyse. La pertinence des données issues d'une analyse précédente pour l'AMDE en cours peut être évaluée en se posant les questions suivantes, par exemple:

- la conception de l'entité ou du processus est-elle similaire ou identique à celle déjà utilisée par l'organisation?
- les données disponibles issues d'entités ou de processus similaires répondent-elles aux objectifs de l'analyse?
- le contexte de l'environnement d'utilisation et d'exploitation reflète-t-il avec exactitude celui de l'entité pour laquelle l'AMDE doit être réalisée?

NOTE Les entités produites en série (les produits commerciaux (COTS), par exemple) et utilisées par de nombreux clients et éventuellement dans plusieurs secteurs industriels, peuvent ne pas disposer de données AMDE fournies par le fabricant de l'équipement d'origine (OEM). Dans ce cas, une AMDE risque d'apporter peu de valeur ajoutée, sauf s'il s'agit d'un moyen permettant d'avoir confiance dans le programme de maintenance proposé par le fabricant de l'équipement d'origine. De même, les produits commerciaux peuvent être considérés comme une «boîte noire» et traités au niveau le plus bas de la hiérarchie de l'entité.

L'AMDE peut être une méthode appliquée dans le cadre du programme de sûreté de fonctionnement et, si c'est le cas, les données peuvent être partagées avec les applications d'autres méthodes d'analyse (voir l'Annexe D).

A.2.2 Maturité de la conception de l'entité et avancement du projet

La maturité concerne tant celle du projet (c'est-à-dire l'avancement du projet sur la durée de vie de l'entité) que celle de la conception. La maturité de conception et la maturité du projet étant étroitement liées, elles sont traitées conjointement.

Au stade de la conception, lorsque l'ensemble de l'architecture d'une entité est en cours de maturation, l'AMDE descendante fonctionnelle offre la possibilité d'identifier les modes de défaillance de niveau élevé pour aider à choisir l'architecture. Au fur et à mesure de la maturation de la conception vers une conception détaillée, le choix des conceptions existantes pour les éléments de l'entité peut privilégier l'approche ascendante. Le point de départ d'une analyse ascendante dépend en général du choix du point de départ dans la hiérarchie des entités, réalisé dans le cadre d'une analyse fonctionnelle descendante ou d'une décomposition d'architecture.

Les conceptions d'entités commerciales évoluent sur de longues périodes grâce à des vagues successives de modifications et d'évolution, pour améliorer la sûreté de fonctionnement. Les conceptions arrivées à maturité peuvent ne pas disposer d'une documentation AMDE formelle. Les conceptions ayant, par exemple, évolué avant l'acceptation générale de la valeur ajoutée d'une AMDE ou sans faire appel aux processus d'amélioration basés sur l'AMDE. Toutefois, les conceptions matures peuvent faire l'objet de programmes de fiabilité connus et de programmes de maintenance associés pour assurer la continuité des performances. La réalisation d'une AMDE sur ce type d'entités peut avoir peu d'influence, le cas échéant, sur la conception ou le programme de maintenance.

Les conceptions immatures se caractérisent souvent par de récentes innovations architecturales ou par l'application de nouveaux matériaux et de nouveaux composants permettant d'améliorer les capacités et/ou le rapport coût/efficacité. Les fabricants de l'équipement d'origine (OEM) peuvent disposer d'une AMDE formelle à inclure dans l'analyse globale de l'entité. L'absence d'AMDE pour ce type de conceptions peut justifier une action supplémentaire (un essai environnemental pour assurer les performances exigées, par exemple). Une conception immature peut être le fruit de l'utilisation de composants matures ou de composants immatures, lesquels peuvent avoir un impact sur le degré d'effort consenti dans l'analyse.

A.2.3 Degré d'innovation

L'évaluation et le traitement des modes de défaillance associés à l'innovation technologique peuvent être pris en charge par les quatre combinaisons d'AMDE, avec différentes formes utilisées au fur et à mesure du passage d'un projet du stade de la conception à une entité expérimentale grandeur nature.

EXEMPLE Une innovation technologique peut être une technologie nouvelle, des processus nouveaux ou de nouvelles applications d'une technologie existante.

Des technologies matures sont similaires par nature à des conceptions matures. L'évolution à long terme des technologies matures peut entraver le mode de développement et les descriptions fonctionnelles de l'entité et des éléments. Par conséquent, un moyen utile de mesurer les avantages que présente une AMDE consiste à évaluer l'impact éventuel sur la conception, à faire varier ou définir le potentiel de fiabilité et de maintenance probable et à vérifier les besoins de maintenance et les besoins de support intégré associés.

A.3 Exemples d'adaptation d'AMDE pour les entités et les processus

A.3.1 Généralités

Pour démontrer comment l'adaptation a permis de définir la profondeur et l'ampleur d'une AMDE dans la pratique, plusieurs exemples sont donnés dans les paragraphes ci-après. Pour chaque exemple, l'objet de l'analyse et le contexte de l'application sont décrits, puis les raisons pour lesquelles l'AMDE a été adaptée de manière particulière sont indiquées. Pour les exemples contenant une analyse de criticité, seules les raisons justifiant le choix de la méthode sont présentées. L'Annexe B donne les détails des méthodes d'analyse de criticité.

A.3.2 Exemple d'adaptation d'une AMDE pour un équipement de bureau

L'entité prise en considération était une nouvelle conception d'équipement de bureau composée d'éléments matériels et logiciels intégrés à évaluer au stade préliminaire et au stade de conception détaillée. La conception de l'entité était une variante importante d'une famille de produits établie. Les éléments de la nouvelle conception sont originaux et sont basés sur une nouvelle technologie. La société a géré une base de données de fiabilité contenant des données relatives, par exemple, aux contraintes, au mode de défaillance, au mécanisme, à la structure d'entité, ainsi que d'autres informations concernant toutes les parties en présence. Les éléments de l'entité étaient tous reliés en série, afin d'exécuter la fonctionnalité exigée par le produit de niveau supérieur.

Une AMDE a été réalisée dans le cadre du programme de fiabilité afin d'examiner la conception de l'entité et son processus de fabrication. La prévision et l'atténuation du mode de défaillance lors de la phase de conception ont été considérées comme étant des éléments très importants pour le développement d'un produit compétitif. L'organisation jouit d'une expérience opérationnelle considérable en matière de performances et connaissances sur les défaillances de la famille de produit. Par conséquent, l'AMDE pouvait s'appuyer sur ce type de données pour corriger les faiblesses techniques identifiées lors de la phase de conception du produit et du processus.

Une AMDE ascendante a été choisie en raison de la simplicité de l'entité et de l'objectif du programme, visant à assurer la fonctionnalité et la fiabilité au niveau du système en s'appuyant sur une compréhension approfondie des performances de l'élément de niveau inférieur dans les conditions de fonctionnement spécifiées par le client. De plus, la solution de conception du produit mélangeait technologie existante et technologie nouvelle. Même en utilisant la technologie existante, une variation de condition opérationnelle pouvait donner lieu à différents modes de défaillance, ce qui a justifié le choix d'une AMDE ascendante.

L'AMDE a inclus l'analyse de criticité, car cela permettait de revoir les priorités à définir en mesurant la sévérité et la vraisemblance d'une défaillance. Étant donné que le cycle de conception était court, l'AMDE a été utilisée pour savoir où allouer les ressources afin de vérifier les interfaces entre les éléments et les paramètres de conception, puisqu'il n'était pas possible de soumettre à l'essai et d'analyser toutes les combinaisons. Ce type d'AMDE et la garantie de sa validité ont reposé sur une grande expérience opérationnelle de produits similaires.

La criticité a été déterminée par une méthode qualitative NPR (Annexe B), car il s'agit d'une méthode simple à appliquer et considérée comme exhaustive. Des tableaux normalisés qui définissent les échelles de mesure des catégories de sévérité et de vraisemblance ont été développés au sein de la société pour assurer la cohérence de l'application et de l'évaluation. L'utilisation de ces tableaux pour évaluer les paramètres de criticité a permis de comparer facilement l'AMDE pour différents types de produits.

A.3.3 Exemple d'adaptation d'une AMDE pour un système d'alimentations décentralisées

Une AMDE a été exigée pour identifier les faiblesses de la conception, la robustesse et la tolérance aux pannes d'un système d'alimentations décentralisées. L'analyse était également

la première étape vers une étude de disponibilité complète du système. Le système d'alimentations décentralisées était une nouvelle conception à l'intérieur de la famille de produits. La nouvelle conception était considérée comme une variante importante de conceptions antérieures, même si la technologie utilisée était bien maîtrisée. La structure du système était hétérogène, mais avec des fonctions identiques. L'AMDE était à réaliser pendant la conception détaillée, au cours de laquelle de nouvelles données relatives à la conception et aux aspects de ses performances ont été mises à disposition à partir d'autres analyses de sûreté de fonctionnement et d'ingénierie.

Une approche descendante a été choisie. L'AMDE a commencé par la définition détaillée des fonctions du système. Cela a permis de définir les écarts par rapport à ces fonctions pour procéder à l'analyse des causes de défaillance au niveau inférieur. Le développement d'une AMDE descendante a permis de caractériser la fonctionnalité du système en décomposant ses fonctions et en identifiant les modes de défaillance, leurs effets et leurs causes.

L'AMDE contenait également une analyse de criticité, des informations quantifiables relatives à l'occurrence d'un mode de défaillance et à ses effets venant à l'appui de la méthode d'analyse de disponibilité subséquente. Dans le premier cycle de l'AMDE, une méthode NPR qualitative a été utilisée (lorsque plus de détails concernant la conception étaient disponibles) et les taux de défaillance réels ont été utilisés pour évaluer la vraisemblance quantitative d'occurrence.

A.3.4 Exemple d'adaptation d'une AMDE pour un processus médical

De nombreux organismes de santé officiant dans de nombreux pays doivent, dans le cadre de leurs prérogatives, évaluer régulièrement leurs procédures pour identifier dans quelle mesure leur système peut faire l'objet de défaillances. Il s'agit d'identifier les parties du processus qui ont le plus besoin d'évoluer afin de limiter les problèmes thérapeutiques. L'AMDE est un moyen éprouvé de satisfaire à cette exigence. Une AMDE peut être appliquée à n'importe quelle procédure médicale (préparer une dose exigée et administrer un médicament, procéder à une opération et anesthésier un patient, par exemple).

Cet exemple prend en considération une AMDE pour une procédure médicale pour laquelle la conception est assez simple, mais les personnes sont susceptibles de faire des erreurs ou de ne pas être en mesure de suivre la procédure comme prévu à cause du matériel ou de facteurs environnementaux.

Il convient de définir clairement le début et la fin de la procédure, et de diviser les tâches effectuées en étapes pour lesquelles chaque mode de défaillance est identifié.

Lorsqu'une AMDE est appliquée en contexte médical, les traitements recommandés impliquent le plus souvent l'ajout de contrôle et de recherche d'équilibre plutôt que la modification des procédures entières.

Une AMDE secondaire peut être réalisée lorsque, par exemple, une défaillance du matériel peut empêcher d'exécuter correctement une étape du processus ou lorsqu'une étape d'une procédure écrite comporte en réalité plusieurs étapes.

En règle générale lorsqu'une AMDE est appliquée à une procédure médicale, tous les modes de défaillance ayant des conséquences désastreuses pour les patients sont couverts. Lorsqu'une analyse de criticité est réalisée, la méthode NPR est généralement utilisée. Cela est dû au fait que les défaillances potentielles qui sont facilement détectées avant une conséquence négative sont moins importantes qu'un mode de défaillance qui n'aurait pas été détecté jusqu'à ce que la catastrophe se produise.

L'analyse quantitative des taux d'erreur humaine est en général complexe et peut donc s'avérer peu fiable. Une méthode simple comme un NPR ou une matrice de criticité est souvent suffisante pour évaluer utilement la criticité et procéder à une hiérarchisation afin d'améliorer le processus.

A.3.5 Exemple d'adaptation d'une AMDE pour des systèmes de commande électronique

Une AMDE a été demandée pour venir à l'appui d'une analyse pendant la phase de définition du concept et la phase de la conception détaillée de systèmes de commande électronique de sécurité (systèmes de freinage de train et systèmes de prévention des collisions, par exemple). Les systèmes étaient des variantes de conceptions antérieures. Les changements entre les nouveaux et les systèmes existants tendaient à être dans l'architecture de conception, et la technologie utilisée a été bien comprise.

L'AMDE avait pour objet de démontrer les caractéristiques de sécurité du système. Pour cette raison, une AMDE ascendante a été choisie, car cette approche permet à l'analyste de démontrer systématiquement que les mesures définies peuvent atténuer de manière appropriée tous les scénarios d'erreurs identifiés du système, quel que soit l'élément de niveau inférieur concerné par la défaillance.

L'AMDE est élaborée en mettant l'accent sur une analyse des capacités d'atténuation du risque de défaillance du système. Il s'agit d'une partie indispensable de l'analyse réalisée sur des systèmes ayant une sécurité. Pour l'essentiel, les effets des défaillances sont classés selon qu'ils sont considérés comme sûrs ou non. Pour prendre une décision éclairée, il convient que le sens du domaine d'application de la description des effets soit évident. Par exemple, si le niveau est trop axé sur les effets locaux, l'analyste risque de ne pas bien percevoir la criticité de l'effet sur l'ensemble du système. A l'inverse, si le niveau du système est trop global, l'analyse peut ne pas être en mesure de suivre la défaillance jusqu'à son effet final.

Cette approche de l'AMDE donne lieu à des discussions sur un certain nombre de questions. Par exemple, des discussions ont lieu concernant les modes de défaillance qui affectent purement les capacités de diagnostic du système sans compromettre sa fonctionnalité principale. Une autre question à prendre en compte est le temps de réaction des mesures d'atténuation (c'est-à-dire à quel point des mesures d'atténuation peuvent être prises en compte, si leur occurrence est trop rare pour permettre de détecter une défaillance imminente).

Les outils utilisés à l'appui de l'AMDE vont de listes sur mesure présentées sous forme de feuille de calcul, aux outils spécialisés de base de données relationnelle permettant de générer les modes de défaillance dans les modèles de performance. Par exemple, les sous-systèmes peuvent faire appel à des instances de composants avec leur définition de mode de défaillance inhérente, dans lesquels différents modes de défaillance peuvent donner lieu aux mêmes effets, étroitement liés à un certain régime de classification.

A.3.6 Exemple d'adaptation d'une AMDE pour une pompe hydraulique

Une AMDE de base a été réalisée pour compléter la conception préliminaire d'une pompe hydraulique pour une chaudière à gaz. Les fonctions de la pompe hydraulique incluent le fonctionnement de la pompe (débit, pression), le fonctionnement de l'inverseur (faire passer la chaudière du mode de chauffage central au mode eau chaude), la purge de l'air du circuit de chauffage central (séparer et évacuer l'air du liquide), l'étanchéité à l'eau dans les conditions de pression du système, le raccordement hydraulique externe, etc. La société est forte d'une grande expérience opérationnelle dans des entités similaires, et il s'agissait d'une variation mineure d'un produit existant dont la conception de l'entité avait été modifiée.

L'AMDE devait être mise en œuvre de manière à utiliser au mieux les compétences de l'équipe d'étude de conception. Compte tenu du stade de conception préliminaire et de l'expérience de l'équipe de conception, le point de départ logique de l'AMDE était l'identification des fonctions de niveau supérieur de l'entité. Un atelier a été utilisé pour identifier les modes de défaillance, fonction par fonction. Le processus adopté consistait à rassembler les personnes compétentes pour un atelier dans lequel elles ont fait part de leurs préoccupations. Il s'agissait de trouver des compromis techniques concernant les modes de défaillance connus et leurs causes, plutôt que de mener une AMDE exhaustive.

Les données collectées pendant l'atelier se présentaient sous la forme d'une suite de modes de défaillance, de composants et de causes. Par exemple, dans le cas d'un problème de fuite dont les effets pourraient aller, par exemple, d'une insatisfaction du client à une inondation, une fuite à l'extérieur ou un préjudice, le mode de défaillance pourrait être la fuite, l'élément être le composant X, et la cause une fissure de fatigue.

A.3.7 Exemple d'adaptation d'une AMDE pour une éolienne

Une AMDE était exigée pour venir à l'appui de la conception détaillée d'une éolienne produisant de l'électricité.

Le périmètre de l'AMDE était l'ensemble de l'éolienne composée de sous-systèmes comme la structure, le moyeu, le groupe motopropulseur, le système de commande, etc. Sur la base de l'expérience déjà acquise, l'objectif était de prendre en charge une nouvelle génération d'éolienne. Dans ce projet, il était demandé d'évaluer tout l'éventail des effets sur chaque niveau de système, par hiérarchisation des modes de défaillance sur la base des risques qu'ils représentaient.

Une approche ascendante a été adoptée pour chacun des sous-systèmes individuels et interdépendants dont les effets à l'interface entre sous-systèmes ont été pris en compte, donnant éventuellement lieu à des effets au niveau du système. Le point de départ était le montage de structure du système/sous-système avec, par exemple, les organes d'entrée-sortie, les unités de commande, la boîte d'engrenages, les moteurs, les encodeurs, les moteurs électriques, les capteurs, les alimentations électriques, les convertisseurs, les roulements.

Cette approche ascendante a été adoptée car un examen approfondi de tous les effets possibles au niveau du sous-système et du système était exigé, pour tous les aspects liés à la fiabilité, à la disponibilité et à la sécurité. L'analyse de criticité a été utilisée pour avoir une indication des défaillances méritant une attention particulière. La méthode de criticité NPR a été choisie compte tenu de sa simplicité, et les trois mesures de sévérité, d'occurrence et de détectabilité étaient exigées par la règlementation pour atteindre les objectifs de l'AMDE.

Annexe B
(informative)

Méthodes d'analyse de criticité

B.1 Généralités

Les méthodes de criticité offrent un moyen de hiérarchiser les modes de défaillance. L'Annexe B décrit uniquement les méthodes qui combinent les mesures de paramètres, c'est-à-dire la vraisemblance, les conséquences (dans le cas du nombre prioritaire de risque) et la détectabilité d'une défaillance.

NOTE L'utilisation d'un seul paramètre pour le classement d'importance n'est pas considérée comme une analyse de criticité.

Ces paramètres peuvent être combinés d'un certain nombre de façons pour générer une criticité. L'Annexe B décrit quatre méthodes: la matrice de criticité, le graphe de criticité, le nombre prioritaire de risque et le nombre prioritaire de risque alternatif.

Il convient de convenir, au stade de la planification, des types de conséquences pris en compte, des échelles à utiliser pour chacun des paramètres et de la méthode de combinaison pour obtenir une criticité. Les méthodes décrites sont générales, et il convient de les adapter à l'application pour leur donner un sens en fonction du contexte et des objectifs de l'analyse.

B.2 Échelles de mesure des paramètres de criticité

B.2.1 Généralités

Les paramètres de criticité peuvent être mesurés qualitativement, quantitativement ou semi quantitativement.

- Les paramètres de criticité peuvent être exprimés qualitativement par des catégories descriptives et classés par degré. Par exemple, «mineur», «majeur» ou «catastrophique» (sévérité des effets) ou «fréquent», «occasionnel» ou «rare» (vraisemblance du mode de défaillance qui se produit).
- Les paramètres de criticité peuvent être exprimés quantitativement par des données empiriques ou d'autres données sous la forme d'un taux de défaillance ou d'une probabilité de défaillance, et par des conséquences quantifiables (le coût économique ou financier de la défaillance, par exemple). Les échelles sont établies de manière à correspondre à la plage de données pertinente avec les unités spécifiées.
- Si les données ne permettent que des estimations descriptives ou d'ordre de grandeur, les paramètres de criticité peuvent être exprimés à l'aide d'échelles d'appréciation ordinales, parfois appelées «échelles ordinales». Si des étiquettes numériques sont associées aux classes ordinales de probabilité, de sévérité ou de zones de taux de défaillance et des plages de coûts financiers, l'approche est parfois dite semi-quantitative.

Les points sur l'échelle de mesure sont exprimés en fonction de l'application. Pour les approches qualitative, quantitative et semi-quantitative, les points correspondent respectivement aux catégories de description, aux estimations chiffrées et/ou aux classes/zones.

Lorsque les échelles sont développées pour mesurer les paramètres de criticité, il convient de veiller à utiliser les meilleures informations disponibles pour ne pas fausser les résultats. Il peut déjà exister un système de classification utile dans l'organisation, et il convient de le prendre en compte pour l'application.

B.2.2 Définition de l'échelle

Il convient que les échelles s'étendent de la conséquence la plus sévère à la moins sévère, de la vraisemblance la plus élevée à la moins élevée et du degré de détectabilité le plus élevé au plus bas qui peut être associé aux modes de défaillance à l'étude pour le scénario envisagé.

Il convient de définir clairement et précisément les points sur les échelles de mesure adoptées, significatifs dans le contexte de l'analyse de manière à assurer la cohérence et l'exactitude de l'évaluation. Il convient que la définition corresponde aux données disponibles et qu'elle soit exprimée en termes significatifs pour les personnes qui procèdent à l'analyse.

Les échelles logarithmiques peuvent se révéler plus appropriées que les échelles linéaires pour les données quantitatives des conséquences et de la vraisemblance. Il convient de définir en conséquence les points sur les échelles utilisées pour les approches qualitatives et semi-quantitatives.

EXEMPLE Le coût d'une défaillance catastrophique est censé être de plusieurs ordres de grandeur, plutôt que plusieurs fois, supérieur à celui d'une défaillance mineure.

Il convient que le choix des catégories (ou zones) pour les échelles qualitatives et semi-quantitatives repose sur la prise en compte de la signification des paramètres choisis. Il convient de prévoir un nombre suffisant de catégories pour pouvoir classer et séparer convenablement la plage complète des effets. En règle générale, au moins trois catégories sont exigées pour assurer une différentiation suffisante sur l'ensemble de la plage prise en considération. Il peut ne pas être judicieux d'envisager un grand nombre de catégories, cela pouvant rendre difficile l'identification de la bonne catégorie lorsqu'il n'y a pas une grande différence de traitement entre les catégories.

NOTE À titre indicatif, entre trois et dix catégories sont le plus souvent utilisées.

Il convient de bien choisir les descriptions de catégorie et le sens de chacune d'elles en tenant compte de la manière dont elles vont être utilisées. Il convient d'être très attentif lors du choix des descriptions verbales ou des étiquettes de nombres/lettres dans une approche qualitative, car elles peuvent en soi influencer les choix faits pendant l'analyse. Il convient que chaque échelle soit accompagnée d'un tableau qui définit le sens des mots utilisés.

B.2.3 Évaluation de la vraisemblance

La valeur de vraisemblance peut être exprimée de manière quantitative, semi-quantitative ou qualitative.

Dans une approche quantitative utilisant des échelles, les valeurs de vraisemblance peuvent être obtenues pour les modes de défaillance spécifiques, être déduites de sources de données génériques ou être estimées avec des données liées au fonctionnement d'entités similaires dans des environnements et applications comparables.

En règle générale, si des données quantitatives sont disponibles, elles tendent à concerner la défaillance d'une entité ou d'un processus dans son ensemble, plutôt que chaque mode de défaillance particulier dudit élément. Une estimation de la vraisemblance d'un mode de défaillance peut être obtenue en répartissant la vraisemblance de défaillance de l'ensemble de l'entité entre les vraisemblances de ses modes de défaillance potentiels. De plus, un ajustement peut être apporté pour représenter la vraisemblance selon laquelle le mode de défaillance donnera lieu à une conséquence particulière (en principe une sévérité définie).

NOTE Si la vraisemblance est exprimée sous la forme d'un taux de défaillance alors, sauf indication contraire, cette approche part implicitement du principe qu'il est constant et qu'il peut donc être inapproprié dans certaines circonstances. De plus, le taux de défaillance d'une entité pouvant être obtenu à partir de données spécifiques, la probabilité relative de ses modes de défaillance et la probabilité qu'un niveau particulier d'effets corresponde à un mode de défaillance donné sont souvent également obtenues à partir d'un ensemble différent de sources de données ou s'appuient sur le jugement.

Si des zones/catégories de vraisemblance sont utilisées, les descriptions peuvent s'appuyer sur des données empiriques applicables, sur les jugements d'expert de l'équipe de conception ou sur d'autres sources appropriées. Il est essentiel d'appliquer l'échelle de manière cohérente, de sorte que la fréquence relative des modes de défaillance soit évaluée avec exactitude et soit compatible avec les données disponibles.

Pour aider à une application précise et cohérente, il convient de tenir compte de ce qui suit.

a) Si des mesures quantitatives (probabilités ou fréquences, par exemple) sont utilisées, il convient d'établir clairement les unités.

EXEMPLE 1 Si une valeur de pourcentage est utilisée, ce à quoi le pourcentage fait référence est précisé (pourcentage d'entités qui font l'objet d'une défaillance en un an, par exemple).

b) Dans la mesure du possible, pour aider à la compréhension commune, il convient d'inclure une explication chiffrée de la description de catégorie correspondant à la plage de vraisemblances prévue pour l'application donnée.

EXEMPLE 2 Avec des systèmes matériels très fiables, le classement du mode de défaillance d'un élément dans la catégorie «fréquent» peut correspondre à une défaillance en plusieurs années, alors que pour des systèmes moins fiables, un mode de défaillance classé «fréquent» peut correspondre à plusieurs défaillances par an.

Il convient que le descripteur de vraisemblance des défaillances rares soit réaliste lorsqu'il s'applique à la conséquence la plus défavorable.

B.3 Attribution de la criticité à l'aide d'une matrice ou d'un graphe

B.3.1 Généralités

La relation entre les paramètres de criticité peut être représentée de différentes manières pour permettre d'identifier la classe de criticité. La vraisemblance et les conséquences d'une défaillance peuvent être exprimées sur des échelles continues ou dans des catégories qui sont alors combinées pour être représentées sous la forme d'un graphe ou d'une matrice, respectivement. Le graphe ou la matrice de criticité est alors utilisé(e) pour définir les priorités de traitements.

Il convient de définir la signification de chaque classe de criticité et le lien avec les traitements qui y sont associés, et d'en convenir avec les parties prenantes, et ce avant l'analyse dans le cadre de la planification de l'AMDE. Cela assure une compréhension claire et sans équivoque de la manière dont il convient de traiter les modes de défaillance, et permet de bien saisir l'éventuel impact commercial de ce type de décisions. Sinon, l'intérêt de l'analyse de criticité est limité, et des activités superflues ou un traitement inapproprié des défaillances peu(ven)t rallonger la durée et augmenter les coûts. Le nombre de classes de criticité exigé est déterminé en fonction des exigences de l'organisation et de l'application de l'analyse.

B.3.2 Matrice de criticité

Une analyse par matrice de criticité permet de mesurer l'importance en combinant les valeurs de vraisemblance et de conséquence. Une matrice de criticité peut également être appelée matrice des risques. Les valeurs de chacun des paramètres sont placées dans une matrice et une classe de criticité est allouée à chacune des cellules de la matrice. La classe de criticité peut être associée au niveau de traitement qu'il convient d'appliquer pour gérer le ou les modes de défaillance associés. Pour les modes de défaillance de classe inférieure, ce type de traitement peut inclure «aucune action». La Figure B.1 donne un exemple de matrice de criticité qualitative.

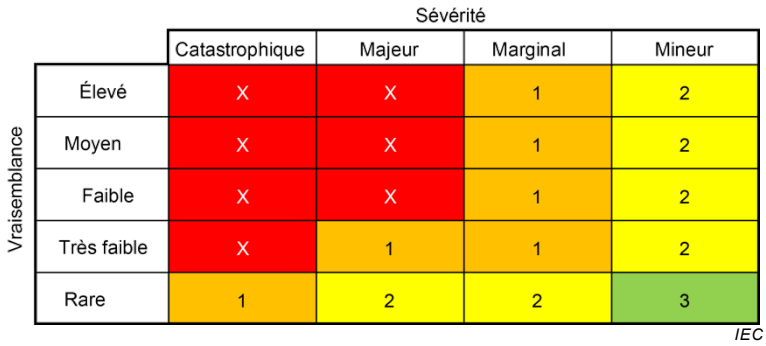


Figure B.1 – Exemple de matrice de criticité qualitative

NOTE 1 Un exemple de classement de la criticité à quatre niveaux (comme à la Figure B.1) serait:

Catégorie X: «Inacceptable»;

Catégorie 1: «Indésirable»;

Catégorie 2: «Acceptable»;

Catégorie 3: «Mineur».

Dans certains cas, un mode de défaillance peut donner lieu à une plage de conséquences différentes, en fonction des circonstances. Si c'est le cas, il convient de spécifier les conséquences auxquelles s'applique la probabilité. Il peut être utile, dans ce cas, de prendre en compte la criticité pour plusieurs conséquences possibles.

Dans l'exemple de matrice de la Figure B.1, le risque représenté par chaque catégorie de criticité augmente en partant de la cellule en bas à droite de la matrice vers la cellule en haut à gauche. Toutefois, les traitements prévus pour chaque mode de défaillance dépendent uniquement de la classification de criticité (c'est-à-dire de la couleur ou du numéro du code de criticité) et pas de la cellule de la matrice.

NOTE 2 Même si des termes comme «acceptable» peuvent être utilisés, cela ne sous-entend pas que d'autres traitements peuvent ne pas être souhaitables.

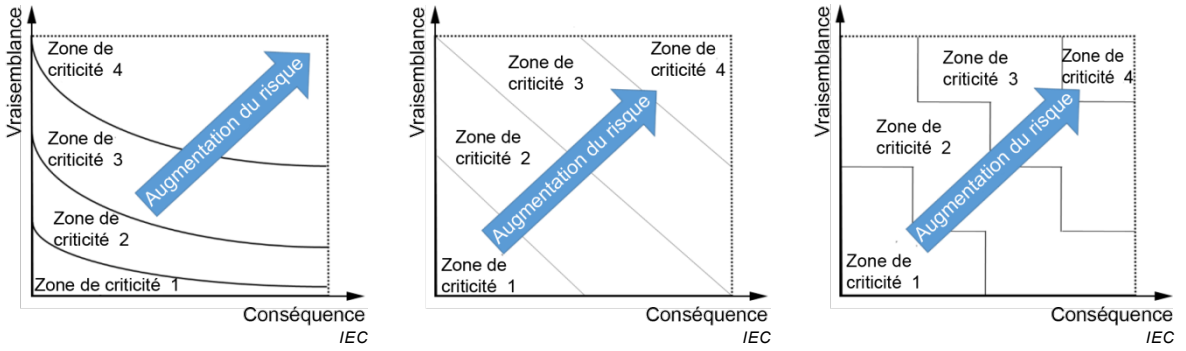
La Figure B.1 n'est qu'un exemple de structure d'une matrice, et il convient de ne pas la considérer comme sa forme définitive. La forme réelle dépend de l'application particulière. Si le nombre de zones de vraisemblance et/ou le nombre de catégories de sévérité des conséquences est (sont) différent(s), la taille de la matrice n'est pas celle représentée à la Figure B.1. De même, la criticité associée aux combinaisons conséquence/vraisemblance peut être différente, auquel cas le code couleur est également différent.

Il n'est pas utile de limiter une matrice à deux dimensions. Elle peut être étendue pour ajouter un troisième paramètre ou, en théorie, autant de paramètres qu'exigé. Toutefois, la complexité et les efforts nécessaires à la formulation d'une grille multidimensionnelle valide et gérable peuvent être considérables et peu rentables en cas d'évaluation de chaque combinaison de paramètres.

Il convient d'étalonner la matrice de criticité afin de s'assurer que les modes de défaillance d'importance similaire ont la même valeur de criticité, de manière à recevoir le même traitement. De plus, si les catégories de sévérité ou de vraisemblance reposent sur des évaluations quantitatives ou semi-quantitatives, il convient de prendre en compte l'acceptabilité des différents traitements appliqués aux modes de défaillance dont chaque côté de la limite de criticité présente des valeurs numériques.

B.3.3 Graphes de criticité

La Figure B.2 donne des exemples de simples graphes de vraisemblance en fonction des conséquences, les classes de criticité étant attribuées selon les zones à l'intérieur du graphe. Dans ce cas, la vraisemblance et la conséquence (sévérité) sont des échelles quantitatives continues.



Exemple A **Exemple B** **Exemple C**

Figure B.2 – Exemples de graphes de criticité

Il n'est pas nécessaire que les limites entre les zones soient de simples lignes droites (Exemple A) ou des courbes (Exemple B). Selon les exigences des traitements pour les modes de défaillance identifiés, une limite en escaliers (Exemple C) ou une combinaison de droites et de courbes peut être appropriée.

NOTE 1 Dans l'Exemple B, les limites des zones représentent des lignes de niveau de risque égal. Lorsque la vraisemblance et la conséquence sont indiquées sur une échelle linéaire, les lignes sont des courbes. Si une échelle logarithmique est utilisée, des lignes droites sont tracées.

NOTE 2 Lorsque la vraisemblance est indiquée sur une échelle linéaire, elle peut prendre la valeur zéro. Cela peut fausser les classes de criticité des défaillances à haute conséquence et faible vraisemblance.

Dans la pratique, des limites de zone lisses n'ont un sens que si la vraisemblance peut être exprimée de manière quantitative et que les conséquences d'une défaillance sont continues (financières, par exemple) et peuvent être totalement identifiées.

Il n'est pas nécessaire de limiter un graphe de criticité à deux paramètres. Il peut être étendu à trois paramètres, si cela est exigé. Toutefois, la complexité et les efforts nécessaires à la formulation de plans valides et gérables peuvent être très importants et pas rentables.

Si l'échelle des conséquences/de sévérité est quantifiable mais que ses valeurs ou zones de valeurs sont différentes, un graphe de sévérité est toujours applicable, les limites de valeur de criticité étant toutefois presque certainement échelonnées. Cela donne lieu à une représentation s'apparentant à la matrice de criticité.

B.4 Attribution de la criticité à l'aide d'un nombre prioritaire de risque

B.4.1 Généralités

Le nombre prioritaire de risque (NPR) est déduit de la combinaison des évaluations semi-quantitatives réalisées sur des échelles ordinales avec des valeurs de conséquence, de vraisemblance et de détectabilité. Dans cette méthode, ces paramètres sont respectivement la sévérité (S), l'occurrence (O) et la détectabilité (D) qui, dans certaines applications, donnent également ce qu'il est convenu d'appeler la méthode «SOD». Deux méthodes d'évaluation du NPR sont données.

B.4.2 Nombre prioritaire de risque

La forme habituelle du nombre prioritaire de risque (NPR) est le produit de trois niveaux de sévérité, d'occurrence et de détection.

$$NPR = S \times O \times D$$

La plage de valeurs NPR dépend des échelles de mesure des trois paramètres, qui utilisent souvent les échelles d'appréciation ordinales de 1 à 10, produisant des valeurs NPR globales comprises entre 1 et 1 000.

NOTE 1 Certaines applications de l'AMDE ignorent le paramètre de détectabilité D, produisant ainsi une échelle NPR globale comprise entre 1 et 100.

NOTE 2 La nature de l'application va déterminer le nombre de points sur l'échelle, moins de 10 pouvant s'avérer appropriés.

Les nombres pour S, O et D sont déterminés à l'aide des tables de classement dans lesquelles les niveaux de chaque paramètre sont associés à une phrase descriptive qui aide l'analyste à choisir le classement de façon précise et cohérente.

Le numéro de détectabilité D peut représenter la vraisemblance à laquelle un mode de défaillance est censé être détecté pendant l'exploitation avant que ne se produisent les effets d'une défaillance. Ce numéro est en général classé dans l'ordre inverse du numéro de sévérité ou d'occurrence. Plus le numéro de détection est élevé, moins la détection est probable. Une vraisemblance de détection inférieure donne donc un NPR plus élevé, et une priorité plus élevée de résolution du mode de défaillance.

EXEMPLE 1 Cet exemple concerne une éolienne. Une échelle de mesure classique pour le classement de sévérité peut s'apparenter à celle présentée ci-dessous (abrégée):

Classe de sévérité (S)	Description
1	Aucun effet sur la production d'énergie électrique. Visite exigée dans 14 jours. L'alarme ne provoque pas l'arrêt de l'éolienne. Probablement causé par la défaillance du composant.
2	Courte interruption de la production d'énergie électrique. Visite exigée dans 14 jours. Arrêt de l'éolienne, mais réarmement à distance possible. Probablement causé par la défaillance du composant.
:	: .
8	Interruption de la production d'énergie électrique sur une longue période (2 à 4 semaines). Remplacement du composant concerné exigeant l'intervention d'un navire de service.
9	Interruption de la production d'énergie électrique sur une période prolongée (plus de quatre semaines). Remplacement du composant concerné exigeant l'intervention d'un important navire de service.
10	Incident de sécurité. Perte de l'ensemble de la structure. Interruption totale de la production pendant plusieurs mois.

EXEMPLE 2 Cet exemple concerne une éolienne. Une échelle de mesure classique pour le classement de l'occurrence peut s'apparenter à celle présentée ci-dessous (abrégée):

Classement de l'occurrence (O)	Description
1	Le mode de défaillance se produit une fois par an pour 10 000 machines.
2	Le mode de défaillance se produit une fois par an pour 2 000 machines.
:	: .
8	Le mode de défaillance se produit une fois par an par machine.
9	Le mode de défaillance se produit une fois tous les 4 mois par machine.
10	Le mode de défaillance se produit une fois par mois par machine.

EXEMPLE 3 Cet exemple concerne une éolienne. Une échelle de mesure classique pour le classement de détectabilité peut s'apparenter à celle présentée ci-dessous (abrégée):

Classement de détectabilité (D)	Description
1	Le mode de défaillance est toujours détecté avant que ses conséquences ne surviennent.
2	Le mode de défaillance est apparent et est en principe détecté avant que ses conséquences ne surviennent.
:	:
8	Le mode de défaillance peut uniquement être détecté par des contrôles (des contrôles d'échantillon, par exemple).
9	Le mode de défaillance est difficile à détecter et ses conséquences seront donc pratiquement inévitables.
10	Les fonctions ne peuvent pas être contrôlées et le mode de défaillance ne peut pas être détecté (inaccessibilité, par exemple).

Les modes de défaillance sont alors classés en fonction de leur NPR et une priorité plus élevée est en général attribuée à un NPR plus élevé. Outre l'importance du NPR, le choix du traitement peut être influencé par la sévérité du mode de défaillance, ce qui signifie que si des modes de défaillance ont un NPR similaire ou identique, les modes de défaillance qui doivent être traités en premier sont ceux dont le classement de sévérité est le plus élevé.

NOTE 3 Dans certaines applications, les effets liés à un NPR qui dépasse un certain seuil ne sont pas acceptables, alors que dans d'autres applications, une grande importance est donnée aux numéros de sévérité élevés, quelle que soit la valeur NPR.

La définition des échelles a un impact sur l'ordre d'importance du NPR. Au moment de tirer les conclusions à partir d'une valeur NPR ou de comparer des valeurs, il convient de prendre en considération les caractéristiques suivantes de cette méthode qui, si elles ne l'étaient pas, pourraient donner lieu à des décisions inappropriées:

a) L'échelle NPR n'est pas continue.

EXEMPLE 4 Avec trois échelles de 1 à 10, seuls 120 sur 1 000 numéros disponibles sont générés.

b) Les rapports numériques entre les valeurs n'ont aucun sens particulier.

NOTE 4 Ce résultat s'explique par le caractère ordinal des échelles et par le fait que les valeurs de sévérité, d'occurrence et de détection ont la même importance. Par conséquent, les numéros NPR peuvent être très proches, mais leur sens être sensiblement différent. Par exemple, les valeurs: S = 6, O = 4 et D = 2 produiraient un NPR égal à 48, alors que S = 6, O = 5 et D = 2 produiraient un NPR de 60. Ce dernier NPR est sensiblement supérieur, alors que O = 5 pourrait, par exemple, correspondre à plusieurs fois la vraisemblance d'occurrence avec O = 4.

c) Le NPR peut être sensible à de petites variations de valeur d'un paramètre.

NOTE 5 Une petite variation d'un paramètre a en apparence un effet plus important sur les autres paramètres élevés (exemple: 9 x 9 x 3 = 243, et 9 x 9 x 4 = 324 par rapport à 3 x 4 x 3 = 36 et 3 x 4 x 4 = 48).

Une bonne pratique d'utilisation du NPR consiste à procéder à un examen minutieux des valeurs de sévérité, d'occurrence et de détection avant de se faire une opinion sur l'évaluation de la criticité et de déterminer les actions de traitement.

B.4.3 Méthode du nombre prioritaire de risque alternatif

La méthode du nombre prioritaire de risque alternatif (NPRA) est une version modifiée de la méthode NPR habituellement utilisée et décrite en B.4.2. Elle a été développée avec pour objectif d'évaluer la criticité de manière plus cohérente lorsque les paramètres peuvent être quantifiés sur une échelle logarithmique (Braband, 2003) [27][1].

1 Les chiffres entre crochets se réfèrent à la Bibliographie.

Pour la méthode NPRA, les points sur les échelles de mesure correspondant aux paramètres sont définis et étalonnés de manière à garder le sens des échelles de mesure quantitatives. Une échelle logarithmique est alors utilisée lorsque chaque valeur associée à un niveau est un multiple fixe de celle qui la précède (10 ou la racine carrée de 10, par exemple). Le même multiple doit être utilisé pour chacune des échelles de sévérité, de vraisemblance d'occurrence et de détection. Il en résulte que le nombre de niveaux de classement des échelles de paramètres est déterminé en fonction des intérêts spécifiques, et peut être supérieur ou inférieur aux dix niveaux en principe utilisés pour le NPR (voir B.4.2).

Il convient que les tableaux de définition des classements de sévérité, de vraisemblance d'occurrence et de détection indiquent la valeur associée à chaque niveau de classement, accompagnée d'une phrase descriptive.

EXEMPLE 1 Cet exemple concerne une application ferroviaire. L'échelle de vraisemblance d'occurrence peut être étalonnée selon un multiple de 10 ou la racine carrée de 10 qui correspond à 3 environ. Dans ce dernier cas, les valeurs des deux niveaux adjacents de l'échelle donnent un ordre de grandeur. Les niveaux correspondants de l'échelle de vraisemblance d'occurrence pour un mode de défaillance donné d'une entité peuvent être:

Classement de l'occurrence (O)	Description
1	Taux de défaillance inférieur ou égal à 1 en 100 000 ans.
2	Taux de défaillance supérieur à 1 en 100 000 ans et inférieur ou égal à 1 en 30 000 ans.
3	Taux de défaillance supérieur à 1 en 30 000 ans et inférieur ou égal à 1 en 10 000 ans.
4	Taux de défaillance supérieur à 1 en 10 000 ans et inférieur ou égal à 1 en 3 000 ans.

EXEMPLE 2 Cet exemple concerne une application ferroviaire. L'échelle suivante de dangerosité (c'est-à-dire de sévérité) dans l'industrie ferroviaire repose en gros sur la racine carrée de 10 qui correspond à 3 environ.

Classe de sévérité (S)	Description
1	Dangerosité insignifiante, aucune blessure à prévoir.
2	Une personne légèrement blessée.
:	:
6	Critique, un accident mortel ou plusieurs personnes gravement blessées.
7	Catastrophique avec plusieurs accidents mortels.
8	Catastrophique avec de nombreux accidents mortels.

EXEMPLE 3 Cet exemple concerne une application ferroviaire. L'échelle suivante d'évitement des conséquences (c'est-à-dire de détection) dans l'industrie ferroviaire repose en gros sur la racine carrée de 10 qui correspond à 3 environ.

Classement de détectabilité (D)	Description
1	Il est presque toujours possible d'éviter les conséquences, au moyen par exemple d'un système technique indépendant.
2	Il est souvent possible d'éviter les conséquences, en raison de conditions favorables.
3	Il est seulement parfois possible d'éviter les conséquences, en raison de conditions défavorables.
4	Il est quasiment impossible d'éviter les conséquences.

Parfois, aucune valeur des échelles de sévérité, de vraisemblance d'occurrence ou de détection n'est clairement associée à chaque point de l'échelle (en plus d'une phrase descriptive). Dans ce cas, il convient que l'analyste s'assure que les niveaux adjacents sont à peu près des multiples fixes les uns par rapport aux autres. Pour ce faire, il convient de procéder à une évaluation tenant compte du fait qu'une augmentation ou une diminution d'un niveau implique une augmentation ou une diminution, par exemple, du degré de sévérité ou de vraisemblance de la détection selon un multiple de 10 ou la racine carrée de 10, en fonction du multiple choisi.

Une fois les paramètres établis pour un mode de défaillance, il est approprié d'ajouter les niveaux de paramètres S, O et D pour un mode de défaillance plutôt que de les multiplier, les échelles de paramètres étalonnées étant de fait logarithmiques. Ainsi:

$$NPRA = S + O + D$$

De manière comparable à B.4.2, les modes de défaillance peuvent alors être classés en fonction de leur NPRA, et une priorité plus élevée est en général attribuée à un NPRA plus élevé. Outre l'importance du NPRA, le choix du traitement peut être influencé par la sévérité du mode de défaillance, ce qui signifie que si des modes de défaillance ont un NPRA similaire ou identique, les modes de défaillance qui doivent être traités en premier sont ceux évalués comme présentant une sévérité élevée.

NOTE 1 Dans certaines applications, les effets liés à un NPRA qui dépasse un certain seuil ne sont pas acceptables, alors que dans d'autres applications, une grande importance est donnée aux valeurs de sévérité élevées, quelle que soit la valeur NPRA.

L'approche NPRA satisfait aux exigences d'une échelle continue de criticité et de mise en correspondance monotone du risque associé à chaque mode de défaillance à son numéro NPR. De plus, de petites variations des niveaux de paramètres de criticité ne se traduisent que par de légères variations du NPR obtenu, ce qui signifie que le NPRA est moins sensible que le NPR (B.4.2). Il convient de noter que les valeurs NPRA sont en général inférieures à celles obtenues avec la méthode NPR pour les mêmes valeurs d'entrée de paramètres de criticité.

EXEMPLE 4 Les niveaux correspondants d'un mode de défaillance identifié qui est toujours considéré comme étant acceptable peuvent être S = 5, O = 5 et D = 5, ce qui génère un NPR de 125 avec la méthode NPR habituellement utilisée. Avec la méthode NPR alternative, cela donnerait un NPRA de 15.

NOTE 2 Si des données quantitatives sont disponibles pour les trois paramètres, il peut être plus judicieux de simplement calculer le risque en multipliant directement les valeurs plutôt qu'en définissant des zones semi-quantitatives.

Annexe C
(informative)

Exemple de contenu de rapport d'AMDE

C.1 Généralités

L'Annexe C présente différents formats de consignation d'un exemple d'analyse d'une alimentation électrique via des tableaux et des schémas depuis un système d'informations de base de données.

En général, il convient que le rapport complet établisse les objectifs de l'analyse et décrive le résultat de l'analyse en fonction des objectifs. Puisque les exemples de l'Annexe C sont des tableaux d'AMDE et des schémas créés depuis une base de données, ils ne constituent qu'une partie du rapport d'AMDE (5.2.5.2). Conformément aux exigences d'un rapport d'AMDE complet, il convient d'inclure les informations décrites en 5.2.5.2 afin que le rapport soit compris même par les personnes qui ne sont pas impliquées directement dans l'analyse. Les informations supplémentaires peuvent être consignées sur des fiches séparées du rapport d'AMDE.

Des exemples supplémentaires de formats de tableaux pour des applications différentes d'AMDE sont donnés à l'Annexe F. Il n'existe pas de format de rapport unique, car le rapport d'AMDE dépend des objectifs et du contexte de l'analyse.

NOTE 1 Le format de rapport réel utilisé peut être différent des formats présentés dans les exemples.

Il existe des progiciels commerciaux permettant de générer des rapports sur la base des résultats d'une AMDE.

NOTE 2 Des feuilles de calcul peuvent être utiles pour une simple analyse impliquant peu de participants. Une base de données relationnelle pour gérer plusieurs relations entre des modes de défaillance, des fonctions, des entités, des composants et des causes de défaillance peut être utile pour une analyse plus complexe avec plusieurs sources d'informations et des exigences compliquées en matière de génération de rapport.

C.2 Exemple de génération de rapports à partir d'un système d'informations de base de données pour une AMDE d'une alimentation électrique

La Figure C.1 présente comment un système d'informations de base de données peut être structuré. Si un système d'informations de base de données est disponible, l'AMDE peut être un fichier qui relie les bases de données suivantes:

- liste des spécifications;
- liste des pièces (nomenclature);
- liste des modes de défaillance pertinents pour les composants et produits de la société;
- liste des actions potentielles de traitement (base de données d'actions).

L'utilisation d'une base de données présente l'avantage de ne pas obliger à entrer plusieurs fois les informations et de faciliter la mise à jour de l'AMDE au fur et à mesure de l'avancée du projet et des modifications apportées.

L'ensemble des champs du rapport d'AMDE qui peuvent être renseignés à partir de ce système d'informations de base de données est présenté dans le Tableau C.1 pour l'exemple d'alimentation électrique de la Figure C.2. En choisissant différentes combinaisons de champs, différents tableaux d'AMDE (Tableau C.2 à Tableau C.5) et schémas (Figure C.3) peuvent être créés.

Dans l'exemple concernant l'alimentation électrique, cette AMDE évalue l'impact possible, pour l'utilisateur uniquement, d'une défaillance dans le dispositif. Les résultats présentés sont valides sous toutes les conditions ambiantes telles que décrites dans la fiche technique. Cette AMDE ne reflète que les dangers se produisant lors de l'utilisation, et non ceux des autres phases du cycle de vie du produit.

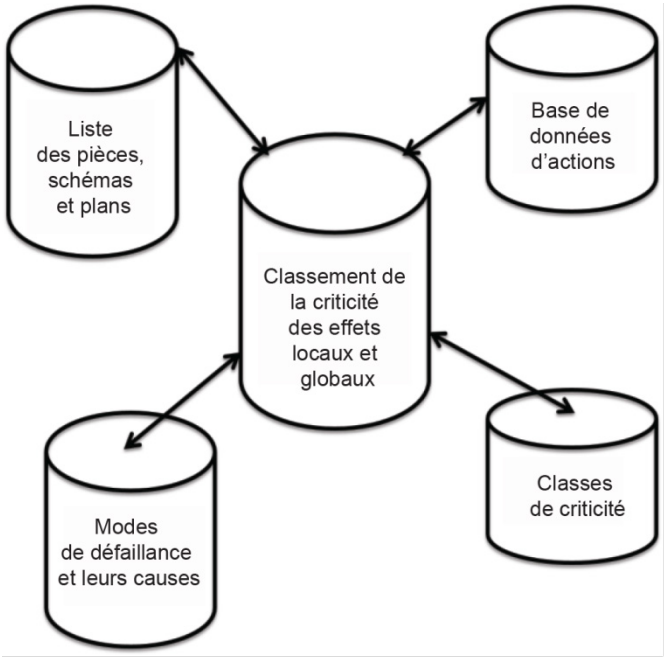


Figure C.1 – Système d'informations de base de données pour la génération d'un rapport d'AMDE

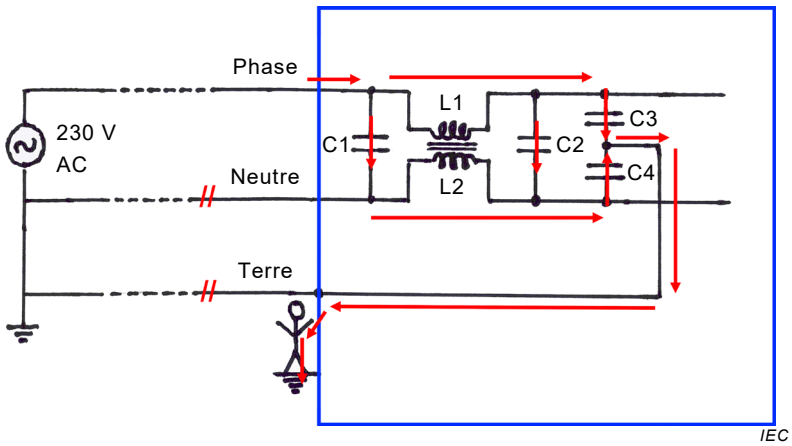


Figure C.2 – Schéma d'un type d'alimentation électrique XYZ

Tableau C.1 – Exemple de champs sélectionnés pour un rapport d'AMDE d'une alimentation électrique en fonction des informations de base de données

Description du rapport d'AMDE	Schéma d'entité	AMDE composant	AMDE pièces	AMDEC avec NPR	AMDEC avec matrice de criticité	
	Figure C.2	Tableau C.2	Tableau C.3	Tableau C.4	Tableau C.5	Figure C.3
Cas N°					Ligne	
Composants			Ligne	Ligne	Colonne	
Liste des pièces		Ligne				
Modes de défaillance		Colonne	Colonne	Colonne		
Effet local						
Effet global (final)			Colonne	Colonne	Colonne	
Sévérité			Colonne	Colonne		
Occurrence				Colonne		
Détectabilité				Colonne		
DCC possible		Colonne				
Actions de traitement (à partir de la base de données d'actions)			Colonne			
Définitions de la sévérité						
Définitions de l'occurrence						
Définitions de la détection						
Liens vers les rapports			Colonne			
Schéma/Dessins	Oui					
Matrice de criticité						Oui
Analyse par arbre de panne						

Légende

Ligne (Colonne) indique le champ sélectionné et à présenter dans la ligne (colonne) du rapport d'AMDE.

«Oui» indique le type de figure sélectionné.

NOTE La deuxième ligne de cette matrice se reporte aux différents tableaux d'AMDE (tableaux) et matrices de criticité (figure) données dans l'Annexe C.

Tableau C.2 – Exemple de rapport d'AMDE composant

Rapport d'AMDE Nº XX Date: jj.mm.aaaa Dernière mise à jour: jj.mm.aaaa

Produit analysé: Type d'alimentation électrique XYZ

Facilitateur: NN1

Équipe d'analyse: NN2, NN3, NN4, NN5, NN6, NN7

Approuvé par: NN8

Composant	Mode de défaillance	Effet global	Sévérité	Échéance de l'action	Lien vers les rapports (cliquer sur l'icône pour afficher le rapport)
C1	s/c	L'alimentation ne fonctionne pas	2	Aucun	NA
C2	s/c	Le fusible interne a sauté L'alimentation ne fonctionne pas	2	Aucun	NA
C3	s/c	230 V dans l'armoire électrique	4	NN3 jjmmaa	Icône du rapport sur les condensateurs de sécurité
C4	s/c	230 V dans l'armoire électrique	4	NN3 jjmmaa	Icône du rapport sur les condensateurs de sécurité
L1	o/c	L'alimentation ne fonctionne pas	2	Aucun	NA
L2	o/c	Neutre non raccordé. L'alimentation ne fonctionne pas	4	NN4 jjmmaa	Icône du rapport sur L2 Probabilité de défaillance
Interrupteur/Phase	o/c	L'alimentation ne fonctionne pas	2	Aucun	NA
Interrupteur/Neutre	o/c	Neutre non raccordé. L'alimentation ne fonctionne pas	4	NN4 jjmmaa	Pas encore d'échéance
Interrupteur/Masse	o/c	Neutre non raccordé. L'alimentation ne fonctionne pas	4	NN4 jjmmaa	Pas encore d'échéance
Soudure	o/c	Neutre non raccordé. L'alimentation ne fonctionne pas	4	NN5 jjmmaa	Icône du rapport sur l'essai de durabilité de la soudure

NOTE La sévérité peut aller d'une influence de l'expérience de l'utilisateur à des risques pour la santé. Dans l'AMDE, les décisions sur les actions entreprises se basaient uniquement sur une classe de sévérité.

Tableau C.3 – Exemple de rapport des pièces présentant des défaillances possibles de cause commune

Rapport d'AMDE N° XX Date: jj.mm.aaaa Dernière mise à jour: jj.mm.aaaa

Produit analysé: Type d'alimentation électrique XYZ

Facilitateur: NN1

Équipe d'analyse: NN2, NN3, NN4, NN5, NN6, NN7

Approuvé par: NN8

Liste des pièces/Type/Fabricant	Désignation	Mode de défaillance
#15-Condensateur – Type XYZ, Valeur XYZ, Tension XY, Fournisseur XYZ	C1, C2, C3, C4	s/c
#71Bobine-Type XYZ, Classement XYZ, Fournisseur XYZ	L1, L2	o/c
#83 Interrupteur-Type XYZ, Classement XYZ, durée de vie prévue XYZ, Fournisseur XYZ	Interrupteur	o/c

Cette liste a été créée à partir d'une liste des pièces. Elle indique les modes de défaillance qu'il est nécessaire de traiter dans une application. En règle générale, la sélection est effectuée pour un certain type de dispositif développé par une entreprise, et les informations concernant cette sélection (5.3.4) doivent être disponibles et joignables au présent rapport.

NOTE Dans cet exemple figurent les composants de même type avec le même mode de défaillance. Les autres causes initiales de modes de défaillance ne sont pas analysées pendant une AMDE de base. Par conséquent, l'examen de la base de données pour identifier les composants pouvant présenter une éventuelle cause commune peut aider et permettre de gagner du temps dans la recherche des défaillances de cause commune.

Tableau C.4 – Exemple de rapport d'AMDEC utilisant l'analyse de criticité NPR

Rapport d'AMDE N° XX Date: jj.mm.aaaa Dernière mise à jour: jj.mm.aaaa

Produit analysé: Type d'alimentation électrique XYZ

Facilitateur: NN1

Équipe d'analyse: NN2, NN3, NN4, NN5, NN6, NN7

Approuvé par: NN8

Sévérité	Occurrence	Détectabilité	NPR	Composant	Mode de défaillance	Effet global
4	3	5	60	L2	o/c	Neutre o/c – Voyant lumineux «ON»
4	3	5	60	Soudure joints	o/c	Neutre o/c – Voyant lumineux «OFF»
4	2	5	40	Interrupteur neutre	o/c	Neutre o/c – Voyant lumineux «OFF»
4	3	3	36	C3	s/c	230 V dans l'armoire électrique
4	3	3	36	C4	s/c	230 V dans l'armoire électrique
3	2	5	30	Interrupteur masse	o/c	Pas de mise à la terre pour la sécurité
2	3	1	6	C1	s/c	L'alimentation ne fonctionne pas
2	3	1	6	C2	s/c	L'alimentation ne fonctionne pas
2	2	1	4	Interrupteur de phase	o/c	L'alimentation ne fonctionne pas
2	2	1	4	L1	o/c	L'alimentation ne fonctionne pas

NOTE Cette AMDE a été créée afin d'évaluer un NPR. Elle se base sur un circuit mis à jour qui comprend également un interrupteur qui commute les trois contacts d'alimentation et un voyant lumineux qui signale que le dispositif est sous tension.

Tableau C.5 – Exemple de rapport d'AMDEC utilisant la matrice de criticité pour l'effet global

Rapport d'AMDE N° XX Date: jj.mm.aaaa Dernière mise à jour: jj.mm.aaaa
Produit analysé: Type d'alimentation électrique XYZ
Facilitateur: NN1
Équipe d'analyse: NN2, NN3, NN4, NN5, NN6, NN7
Approuvé par: NN8

Cas N°	Composant	Effet global
#1	C1	L'alimentation ne fonctionne pas
#2	C2	L'alimentation ne fonctionne pas
#3	C3	230 V dans l'armoire électrique
#4	C4	230 V dans l'armoire électrique
#5	L1	L'alimentation ne fonctionne pas
#6	L2	Neutre non raccordé. L'alimentation ne fonctionne pas
#7	Interrupteur/Phase	L'alimentation ne fonctionne pas
#8	Interrupteur/Neutre	Neutre non raccordé. L'alimentation ne fonctionne pas
#9	Interrupteur/Masse	Neutre non raccordé. L'alimentation ne fonctionne pas
#10	Soudure	Neutre non raccordé. L'alimentation ne fonctionne pas

NOTE Cet exemple de rapport présente les mêmes fonctions de sécurité comprises dans une matrice de criticité. Le graphe a été créé en une image à deux dimensions sans prendre en compte la détectabilité pour l'évaluation de l'impact sur l'utilisateur.

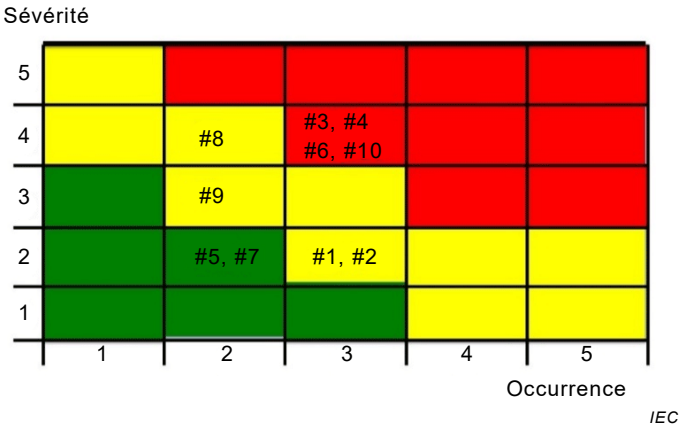


Figure C.3 – Matrice de criticité pour le rapport d'AMDEC du Tableau C.5 créée en une image à deux dimensions sans prendre en compte la détectabilité

Annexe D
(informative)

Relations entre l'AMDE et d'autres techniques d'analyse de sûreté de fonctionnement

La combinaison de l'AMDE à d'autres méthodes d'analyse de sûreté de fonctionnement peut augmenter son efficacité. Par exemple:

- Pour définir le périmètre et faciliter le développement d'une AMDE, un bloc-diagramme de fiabilité (RBD) du système peut être utile. Les résultats de l'AMDE peuvent être utilisés par la suite pour réviser ou mettre à jour le bloc-diagramme de fiabilité.

  NOTE 1 À l'inverse de l'AMDE, le point de vue d'analyse d'un RBD est le bon fonctionnement du système.

- Pour choisir les entités importantes d'un système complexe pour une AMDE, une analyse par arbre de panne (AAP) d'un événement de tête pertinent peut être utilisée pour identifier les entités du système à analyser.

  NOTE 2 Comme l'AMDE, le point de vue d'analyse d'une AAP est la défaillance du système.

- Les résultats d'une AMDE (de niveau inférieur) peuvent identifier les événements de base pour l'AAP, qu'il convient d'inclure comme tels dans l'AAP.
- Les informations provenant d'une analyse de cause initiale peuvent venir à l'appui de l'identification des causes de défaillance d'un processus (IEC 62740).
- Pour compléter l'AMDE, qui en principe ne tient compte que des défaillances indépendantes, des méthodes d'analyse plus détaillées (AAP, RBD, analyse par arbre d'événement, analyse de Markov ou réseaux de Petri) peuvent être utilisées pour tenir compte de l'interdépendance des événements de défaillance comme leur ordre d'apparition, la probabilité conditionnelle d'occurrence, la redondance, l'exclusivité de l'occurrence, les défaillances de cause commune.
- L'AMDE peut être utilisée de manière incrémentielle en combinaison avec d'autres techniques d'analyse de sûreté de fonctionnement pendant le développement d'une entité ou d'un processus. Au stade du concept, l'AMDE peut être combinée à un bloc-diagramme de fiabilité et à une analyse par arbre de panne pour prendre en compte les défaillances au niveau d'une fonction. Pendant la conception détaillée, l'AMDE peut être développée à un niveau plus détaillé. Pour les composants ou processus critiques sélectionnés, une AMDE peut être réalisée à un niveau plus détaillé.
- La prévision de fiabilité et l'analyse des résultats d'essai ou des défaillances en utilisation peuvent être utilisées pour aider à quantifier la vraisemblance dans une AMDE.

  NOTE 3 Les références à d'autres normes d'analyse de sûreté de fonctionnement qui peuvent être applicables sont: RBD (IEC 61078); AAP (IEC 61025); ETA (IEC 62502); Analyse de Markov (IEC 61165); Réseaux de Petri (IEC 62551). Pour la prévision de fiabilité, voir l'IEC 61709 et l'IEC 62308.

Les résultats d'une AMDE donnent des informations relatives aux aspects critiques d'une conception de l'entité ou du processus complexe, et peuvent être utilisés pendant le processus de développement en entrée ou en combinaison avec:

- une analyse de maintenance;
- une identification et une résolution des problèmes pendant la maintenance;
- une analyse de testabilité;
- une définition et une spécification des cas d'essai et d'une analyse des résultats d'essai;
- une analyse du soutien logistique;
- une analyse de la fiabilité en mission;
- une analyse de disponibilité;
- une évaluation des conséquences des modifications de conception;
- une documentation pour les besoins réglementaires (approbation de sécurité d'un système particulier ou d'un certain type de système, par exemple).

Annexe E
(informative)

Considérations relatives à l'application d'une AMDE

E.1 Généralités

L'Annexe E aborde les applications communes de l'AMDE et les questions spécifiques à prendre en compte lors de sa réalisation, conformément à la méthodologie générale donnée dans le présent document et aux recommandations en matière d'adaptation données à l'Annexe A. Les applications présentées ne sont pas exhaustives.

Les applications présentées peuvent faire l'objet d'un certain nombre d'exigences eu égard à l'analyse de criticité (la sécurité, par exemple) ou peuvent assurer la compatibilité aux normes particulières (l'AMDEC dans la maintenance basée sur la fiabilité, par exemple). L'utilisation de l'AMDE pour les systèmes complexes est également prise en compte (allocation de fiabilité et de disponibilité entre les modules et les composants, par exemple).

E.2 AMDE logicielle

L'AMDE logicielle s'apparente à une AMDE pour le matériel ou les procédures et concerne les fonctions. Pour le logiciel, les conventions suivantes établissent que:

- l'erreur logicielle est une erreur dans le code logiciel,
- le défaut logiciel est un problème d'exécution de la fonction/procédure,
- la défaillance logicielle est une dégradation totale ou partielle de la fonction logicielle spécifique.

Les défauts de conception du logiciel (communément appelés «bugs») peuvent causer la défaillance du logiciel. Les conséquences de ce type de défaillance pour les fonctions et la sortie logicielles peuvent être analysées comme pour toutes les autres entités. La probabilité de défaillance peut être estimée comme étant le nombre d'activations de la fonction contenant un «bug» divisé par le nombre total d'exécutions de la fonction, mais ces informations étant rarement disponibles, une analyse quantitative est rarement possible. Les états de défaillance dans un logiciel sont souvent intermittents et certains d'entre eux peuvent être réparés en réinitialisant le logiciel. Tous les défauts logiciels sont liés à la conception et leur origine est soit une interprétation incorrecte des exigences, soit des erreurs de code, soit une mémoire insuffisante, soit des boucles ouvertes, soit des erreurs de syntaxe, etc.

Le logiciel peut faire l'objet d'une analyse descendante ou ascendante. Comme le matériel, le logiciel est divisé en plusieurs niveaux: progiciel, modules logiciels et fonctions de code exécutable par exemple (Tableau 1). Pour chaque élément, il convient que l'analyse prenne en considération l'entrée, le traitement et la sortie. Le traitement dépend des conditions initiales avant l'entrée (la position dans une structure de menus, le contenu des registres et des mémoires (RAM et ROM), par exemple). Dans les niveaux inférieurs, des défauts peuvent se produire dans les entrées (données illégales ou corrompues, par exemple), dans les conditions initiales (position incorrecte dans le menu, contenu incorrect ou corrompu des mémoires) ou traitement incorrect (des algorithmes, par exemple). Les défaillances au niveau du système sont souvent liées à la sortie (sortie corrompue ou données non valides, par exemple). Enfin, la sortie logicielle peut interagir avec le matériel (problèmes de synchronisation, par exemple). En règle générale, l'analyse porte sur les modes de défaillance liés au logiciel. Toutefois, les causes, les mesures et les effets d'une défaillance peuvent être liés au matériel en question. Par conséquent, il convient que les analystes qui connaissent le logiciel et ceux qui connaissent le matériel participent ensemble à l'analyse.

La profondeur et l'ampleur de l'AMDE logicielle peuvent varier. L'AMDE peut être limitée aux composants logiciels ou aux modules uniquement. Si cette AMDE commence assez tôt dans le développement du logiciel, elle peut se concentrer sur les fonctions logicielles indispensables au fonctionnement du système, et sur les défauts ou erreurs éventuels qui pourraient être la cause d'une défaillance de fonction dans un ou plusieurs de ses modes de défaillance. Ce type d'analyse est réalisé au début du développement du logiciel et fait office de source d'informations pour créer des cas d'essai de logiciel. Au fur et à mesure de l'avancée de la conception du système, l'effet des défaillances, erreurs ou défauts logiciels et les circonstances ou leur combinaison à l'origine de l'événement de défaillance peuvent être mieux définis.

Les causes initiales de défaillances peuvent inclure les erreurs commises par le programmeur («bugs») et les causes matérielles. Pour réaliser une AMDE, il est nécessaire de déterminer si une seule défaillance dans le logiciel peut provoquer un effet local inacceptable (outre les effets finaux/globaux), par exemple:

- une variable prend une valeur inattendue;
- un message contient des données inattendues ou une synchronisation inattendue;
- un module produit des sorties inattendues.

L'AMDE analyse ensuite chaque mode de défaillance pour déterminer les effets (finaux) sur le système. Cette démarche s'appuie sur des règles et est complexe, les effets dépendant du temps et de l'état. Avant de procéder à une AMDE logicielle, il convient de procéder à une analyse séparée de la spécification des exigences. Les défauts ou erreurs logiciels donnant souvent lieu à des effets matériels indésirables, il convient de procéder d'abord à une AMDE matérielle pour établir les effets sur le système. Les effets sur le système logiciel peuvent alors reposer sur les effets sur le système matériel.

La liste suivante s'appuie sur des exemples donnés dans Ozarin (2016) [29]. L'AMDE logicielle doit également tenir compte des conditions de fonctionnement, par exemple:

- défaillances matérielles de la mémoire;
- défaillance périphérique projetée en mémoire (convertisseurs analogique/numérique ou dispositifs d'entrée/sortie, par exemple);
- défaillance de l'alimentation électrique (réinitialisation due à une chute de tension d'alimentation, par exemple);
- interférence électromagnétique (IEM), impulsion électromagnétique (IEM);
- données d'entrée erronées incorrectement traitées, y compris les erreurs d'amorçage.

Voici des exemples de causes de défaillance au niveau du système:

- mauvaise utilisation des appels du système d'exploitation;
- synchronisation (collision de données due à une modification du temps de propagation, par exemple);
- interruption du traitement et analyse inadaptée;
- traitement inadapté ou absent des exceptions.

Voici des exemples d'erreurs de programmation (causes de défaillance):

- erreurs de conception et de mise en œuvre (codage, mise à l'échelle, algorithmes, par exemple);
- détection d'erreurs inadaptée (violations de limite, pointeurs hors de portée, par exemple);
- détection inadaptée de plage valide;
- écrasement accidentel des mémoires;
- traitement inadapté des erreurs logicielles (un cas inattendu, par exemple).

Voici des exemples de modes de défaillance:

- point de sortie incorrect, dépassement de temps, interaction d'E/S inattendue;
- données manquantes, données incorrectes, synchronisation des données, données supplémentaires;
- fin anormale, événements ignorés, logique incorrecte, synchronisation/ordre;
- arrêt, plantage, suspension, réponse lente, défaillance au démarrage, faux messages.

Si l'analyse est réalisée avec une feuille de calcul, les colonnes suivantes peuvent en général être utilisées:

a) système hiérarchique et composants;
b) codes de composant;
c) modes de défaillance;
d) causes de défaillance;
e) conséquences de l'indisponibilité de la fonction qui fait l'objet de la défaillance (si le logiciel est réparé);
f) mesures d'atténuation de la conception (mesures de récupération de la conception, chemins alternatifs, protection contre les défauts);
g) mesures de compensation;
h) clôture du problème;
i) indisponibilité réduite finale de la fonction par suite de l'identification du mode de défaillance.

La Figure E.1 donne un exemple de modèle de défaillance logicielle.

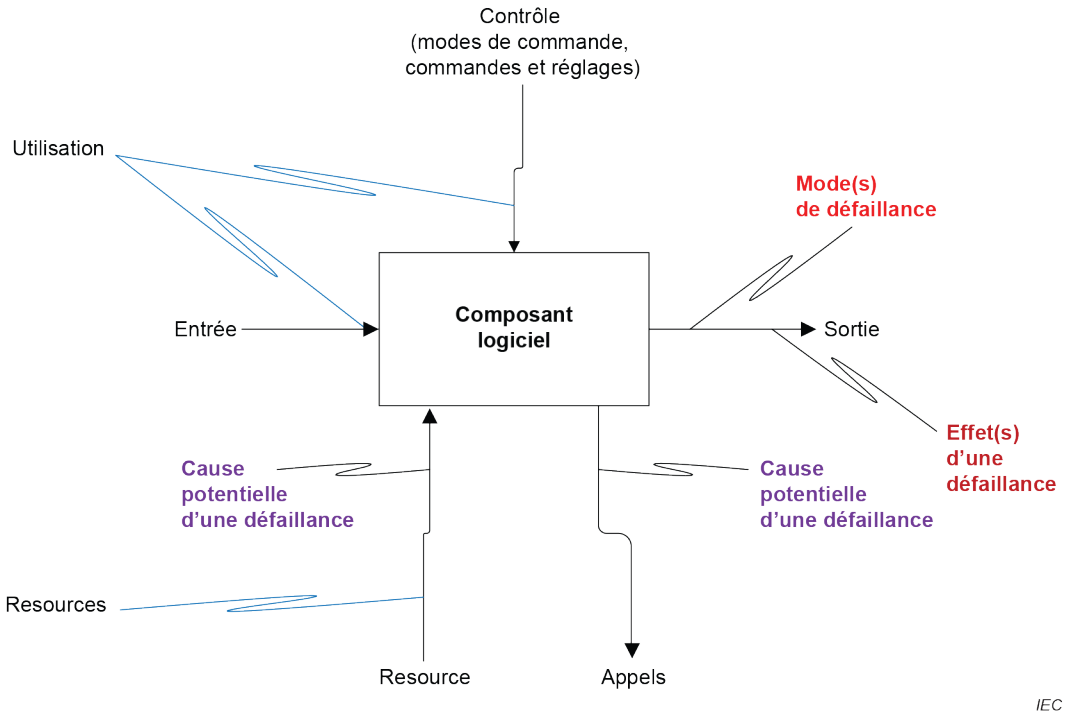


Figure E.1 – Modèle de défaillance général d'un composant logiciel (CSU)

Au fur et à mesure de l'avancée de la conception, l'analyse perçoit le système dans son ensemble, contenant les logiciels et le matériel, l'analyse déterminant les fonctions du système et leurs enchaînements.

Si une AMDE matérielle est modifiée par une partie d'un logiciel, l'analyse peut prendre des proportions non souhaitées lors de la recherche de l'enchaînement d'effets qui a donné lieu à la défaillance du système, et lors de l'évaluation du degré de leur dégradation ou sévérité de leur perte sur les performances du système. Lors de l'analyse d'un système mixte matériel/logiciel, une pratique préférentielle consiste à suivre la fonction du système jusqu'aux branches afin d'identifier les composants logiciels (CSU), leur(s) erreur(s) ou défaut(s) potentiel(le)s et à identifier les modes de défaillance potentiels, ainsi que les causes potentielles.

Il convient de ne pas oublier que l'AMDE détermine un seul mode de défaillance à la fois. Elle n'est pas censée déterminer les dépendances fonctionnelles, les séquences d'événements (défaillances) ou les combinaisons d'événements. Une défaillance matérielle peut être à l'origine de la défaillance logicielle, mais dans le cadre de l'AMDE, la défaillance logicielle est alors l'effet de la défaillance matérielle.

L'AMDE logicielle est une méthode (en plus des essais) qui aide à améliorer la fiabilité logicielle. Les essais peuvent également être un traitement des modes de défaillance considérés comme étant critiques.

E.3 AMDE processus

Pour les processus et procédures, la méthodologie d'AMDE générale est la même que celle utilisée pour les entités matérielles et logicielles. Le point de départ de l'analyse est le schéma du processus, l'organigramme des tâches ou l'analyse des tâches. Le processus est subdivisé en éléments qui sont les étapes du processus. Le niveau de décomposition est choisi en fonction de l'application. La fonction de chaque étape ou son résultat prévu est défini(e) avec la description de la fonction de manière suffisamment spécifique que le niveau de performance qui compose une défaillance est clair. Comme avec l'AMDE réalisée pour les entités matérielles et logicielles, les moyens par lesquels la fonction de processus peut faire l'objet d'une défaillance sont répertoriés en tant que modes de défaillance dans l'AMDE processus. Les effets d'une défaillance, les mécanismes et les causes de défaillance possibles sont également définis. Les mécanismes et causes de défaillance impliquent souvent des défaillances humaines et matérielles. L'analyse de criticité peut être appliquée de la même manière que celle décrite dans les recommandations générales de l'AMDE.

L'AMDE processus a été en premier lieu appliquée aux processus de fabrication, mais elle est aujourd'hui utilisée dans une plus large mesure. Par exemple, elle est largement utilisée dans les procédures d'analyse médicale dans le domaine de la santé.

E.4 AMDE pour la conception et le développement

L'AMDE est une partie essentielle du processus de conception, du concept jusqu'au développement de systèmes complexes. L'AMDE est itérative et initiée dès que les informations de conception préliminaires sont disponibles au niveau supérieur du système, puis elle est étendue aux niveaux inférieurs de la hiérarchie du système dès que de plus amples informations sont disponibles. Il convient que l'adaptation de l'AMDE (Annexe A) permette de s'assurer qu'elle contribue de manière significative aux décisions organisationnelles, telles que la faisabilité et l'adéquation d'une approche en matière de conception.

Pendant la conception, une AMDE a pour objectif d'identifier les modes de défaillance au sein d'un système, ainsi que les défaillances critiques potentielles qui peuvent être éliminées ou réduites par une action de conception exécutée le plus tôt possible.

Outre la fiabilité, l'AMDE vient à l'appui des efforts de maintenabilité et de supportabilité, et de l'analyse des risques.

E.5 AMDE dans le cadre d'une maintenance basée sur la fiabilité (RCM)

L'aptitude à développer un programme de maintenance abouti à l'aide d'une maintenance basée sur la fiabilité (RCM) exige une bonne compréhension des fonctions, des défaillances de l'entité et des conséquences en termes d'objectifs de l'organisation dans le cadre du fonctionnement de l'entité.

L'AMDE et la méthode de criticité sont applicables à la RCM si l'analyse est structurée de manière à satisfaire aux exigences de la norme IEC 60300-3-11 relative à la maintenance basée sur la fiabilité.

La structure de l'analyse exige que tous les modes de défaillance soient clairement liés à la perte de fonction à un niveau approprié dans la hiérarchie de l'entité, et que les aspects tels que les «moyens de détection» déterminent les tâches de maintenance potentielles.

E.6 AMDE pour les systèmes de commande relatifs à la sécurité

E.6.1 Généralités

Les applications de sécurité utilisent l'AMDE dans différents contextes. La méthode AMDE représente une alternative pour la gestion d'une fonction relative à la sécurité ou lors de l'analyse des risques.

EXEMPLE 1 Certaines normes (l'IEC 62061 et l'IEC 61508 (toutes les parties), par exemple) exigent de procéder à certaines formes d'analyse pour établir les traitements appropriés du risque dans les applications, lors de la création de fonctions relatives à la sécurité ou lors du développement de dispositifs à utiliser dans ces fonctions. Une AMDE est une méthode qui peut être utilisée pour la gestion d'une fonction relative à la sécurité.

Les applications de sécurité d'une AMDE classent les modes de défaillance d'une fonction de sécurité comme étant sûrs ou dangereux. La classification peut être différente en cas de modification des conditions d'utilisation ou de la structure ou l'environnement du système.

EXEMPLE 2 La plupart des systèmes ont un état hors tension (état d'arrêt) comme état en sécurité (état invariable du système sûr). La défaillance du système de freinage d'un aéronef peut être considérée comme sûre lorsque l'aéronef en question est au sol, mais elle peut devenir dangereuse au décollage ou à l'atterrissage (état variable du système sûr, voir Yoshimura and Sato, 2008 [30]).

Selon certaines normes de sécurité, il convient de détecter les pannes uniques de sorte qu'elles donnent lieu à l'état en sécurité ou de maintenir l'état en sécurité (c'est-à-dire par redondance fonctionnelle). Une AMDE offre un moyen systématique de démontrer qu'aucune panne unique ne conduit à une condition dangereuse.

Pour définir les priorités dans une application de sécurité, il convient que les actions de conception prennent compte en premier lieu des effets d'une défaillance sans considération de compromis économique. Par conséquent, si une action de conception est exigée, il convient que les fonctions aient, par exemple, pour objet:

- de réduire la vraisemblance d'une défaillance dangereuse;
- de reconnaître ou de détecter la défaillance dangereuse se produisant, et de réagir en conséquence;
- de signaler l'état en sécurité du dispositif à l'utilisateur;
- d'éliminer ou de réduire la probabilité d'une défaillance provoquée par une erreur humaine ou par une mauvaise compréhension.

E.6.2 AMDE dans la gestion d'une application de sécurité

Une AMDE peut être appliquée au niveau du système pendant la phase de gestion du développement d'une application de sécurité. Les modes de défaillance et leurs effets de tous

les composants d'un système, ainsi que leur interaction, sont systématiquement évalués pour déterminer leur impact sur la sécurité du système.

Une AMDE peut également être appliquée à d'autres stades d'un projet, lorsque l'identification des risques et l'analyse de leurs impacts sur une fonction relative à la sécurité peuvent permettre de déterminer les traitements visant à améliorer la sécurité. Une AMDE dont l'objet est d'améliorer la sécurité consiste à trouver toutes les entités impliquées dans la fonction de sécurité et à identifier de manière exhaustive les sources de danger. Les méthodes permettant l'identification exhaustive incluent les listes de vérification, les recherches et l'utilisation d'expertises éclairées.

Une mesure du risque s'appuyant sur la sévérité du danger et une évaluation qualitative de sa probabilité permet de définir l'intégrité de sécurité exigée des systèmes relatifs à la sécurité, électriques, électroniques et électroniques programmes (voir l'IEC 62061).

La probabilité du danger tient compte:

- de la fréquence et de la durée d'exposition des personnes au phénomène dangereux;
- de la probabilité d'occurrence d'un événement dangereux;
- de l'aptitude à éviter ou limiter le danger.

Ces trois facteurs permettent (avec le niveau de sécurité) de générer une classe pour la réduction du risque nécessaire d'une application. Ces classifications sont utilisées dans plusieurs normes relatives à la sécurité.

NOTE L'IEC 61508 (toutes les parties) et l'IEC 62061 utilisent le terme SIL (*safety integrity level* – niveau d'intégrité de sécurité) pour cette classification.

EXEMPLE Dans l'IEC 62061, la catégorie la plus élevée de réduction du risque exige SIL3, ce qui équivaut à un taux de défaillance de la fonction de commande de sécurité compris entre 10^{-8} et 10^{-7} par heure.

E.6.3 Analyse de criticité incluant des diagnostics

Un autre niveau de détail est ajouté dans ladite analyse des modes de défaillance, de leurs effets et de leurs diagnostics (AMDED).

NOTE 1 La méthode AMDED est également utilisée pour les systèmes non relatifs à la sécurité.

L'aptitude du système ou du sous-système à détecter les défaillances internes, de préférence grâce à des diagnostics en ligne automatiques est un élément essentiel à l'obtention et au maintien du bon fonctionnement de systèmes complexes et de systèmes qui peuvent ne pas totalement assurer toutes les fonctionnalités dans des circonstances normales (un système d'arrêt d'urgence (ESD) à faible demande, par exemple). Lorsque l'intégrité de sécurité d'un système est évaluée, les données quantitatives du taux de défaillance (taux de défaillance et distribution des modes de défaillance) est ajoutée à tous les composants analysés. De plus, la capacité du système à détecter les défaillances internes est déterminée et quantifiée.

Si les composants analysés sont des dispositifs électroniques, il convient que les taux de défaillance fassent l'objet d'une documentation d'accompagnement appropriée pour justifier leur écart, par rapport au retour d'expérience en service. Les taux de défaillance de chaque composant sont déduits de bases de données dont il a été démontré qu'elles sont appropriées. De plus, les distributions de mode de défaillance peuvent être déduites de sources similaires ou de normes (l'IEC 61709, par exemple), leurs valeurs étant en général exprimées en pourcentage du total.

NOTE 2 Les taux de défaillance sont souvent donnés en FIT (*failure in time* – défaillances dans le temps), en 10^{-9} par heure.

NOTE 3 Dans ce contexte, les «distributions de mode de défaillance» se rapportent à la proportion du taux de défaillance total du composant qui peut être attribuée à chacun de ses modes de défaillance.

Dans la plupart des cas, les taux de défaillance n'ayant aucun effet sur la fonction de sécurité ou les défaillances des éléments qui ne font pas partie de la fonction de sécurité sont également donnés mais n'ont aucun impact sur les calculs.

Lors de l'évaluation d'un dispositif électronique, l'analyse prend en considération chaque composant électronique et son influence sur une fonction de sécurité, ce qui permet de connaître les effets d'une défaillance sur une fonction de sécurité.

Les effets sont en principe divisés en défaillances en sécurité, défaillances détectées dangereuses, défaillances non détectées dangereuses et défaillances qui n'ont aucun effet sur la fonction de sécurité. Pour vérifier l'exhaustivité de l'évaluation, il est parfois approprié de répertorier les composants qui n'ont pas d'impact sur la fonction de sécurité.

La décision de considérer ou pas une défaillance dangereuse comme étant détectée ou non détectée est déterminée par une valeur de couverture du diagnostic qui peut être déduite des composants du circuit couverts par le diagnostic et de leur efficacité estimée. Les valeurs sont analysées après l'évaluation et représentent la qualité du dispositif à être utilisé dans la fonction de sécurité. Les chiffres obtenus peuvent également être utilisés pour calculer le taux de défaillance ou autres valeurs de fiabilité pour la fonction de sécurité comme la proportion de défaillances en sécurité (SFF) ou une couverture du diagnostic (DC) globale. Les définitions de ces valeurs caractéristiques dépendent du contexte dans lequel elles sont définies.

Le résultat est un classement des valeurs de probabilité de défaillance qui permet d'estimer le risque global lié à la défaillance d'une fonction de sécurité si elle est demandée.

En l'absence d'informations suffisantes relatives aux modes de défaillance possibles et à leurs distributions pour un composant électrique, une AMDE est véritablement une méthode appropriée pour collecter ces informations. De cette analyse, des valeurs issues du retour d’expériences ou d’approches théoriques peuvent être déterminées.

NOTE 4 Cette méthode et les possibilités d'exclusion de défaut sont décrits dans l’ISO 13849-1.

E.7 AMDE pour les systèmes complexes avec allocation de fiabilité

E.7.1 Généralités

L'AMDE peut être utilisée pour les systèmes complexes et critiques, du secteur de la défense à celui de l'aérospatiale, en passant par le secteur hydraulique, l'assainissement, le transport, les communications et la production et distribution d'électricité. Dans ces systèmes, les exigences de sûreté de fonctionnement en termes de valeurs de disponibilité, maintenabilité et fiabilité sont allouées aux éléments du système. Une AMDE adaptée peut être réalisée pour prendre en considération les défaillances de chaque élément et bien comprendre les effets systémiques sur les fonctions de conception (les composants communs et l'application de redondance, par exemple).

E.7.2 Évaluation de la criticité des systèmes non réparables avec allocation de fiabilité

Lors d'une AMDE réalisée pour un système non réparé complexe, les fréquences, probabilités et taux d'occurrence ou d'autres mesures pertinentes liées aux défaillances peuvent être alloués à chaque effet au niveau du système. Cette allocation peut être comparée au risque acceptable pour le système, et les probabilités allouées être représentées sous la forme d'une matrice en fonction de la sévérité de leurs effets.

Les effets locaux de chaque défaillance au niveau le plus bas de la hiérarchie du système peuvent être remontés jusqu'aux ensembles de niveau supérieur et enfin au niveau système. Ces appréciations effectives du risque peuvent alors être comparées au niveau acceptable

des risques. Si la criticité dépasse la valeur acceptable, il convient de la tracer au niveau de la partie du système dont elle provient.

Les probabilités de défaillance évaluées peuvent être comparées aux limites acceptables pour chaque niveau de sévérité, afin d'identifier les ensembles de niveau inférieur ou composants présentant une criticité excessive. Des actions techniques sont alors réalisées pour diminuer la criticité des composants en diminuant leur probabilité de défaillance ou par d'autres mesures d'atténuation des effets de leur défaillance. Ce processus descendant est représenté à la Figure E.2.

Il est souvent admis que si la criticité d'un composant de niveau inférieur ne dépasse pas le niveau acceptable, aucune action n'est nécessaire. Cela peut ne pas être le cas en présence de nombreux composants similaires, qui peuvent produire les mêmes effets sur les sous-systèmes ou sur le système. Il convient que la somme totale des probabilités de défaillance de tous les composants dont la sévérité des effets est la même ne dépasse pas la probabilité acceptable de défaillance de l'ensemble dans lequel ils résident. Cette mesure permet de ne pas dépasser la criticité définie au niveau du système.

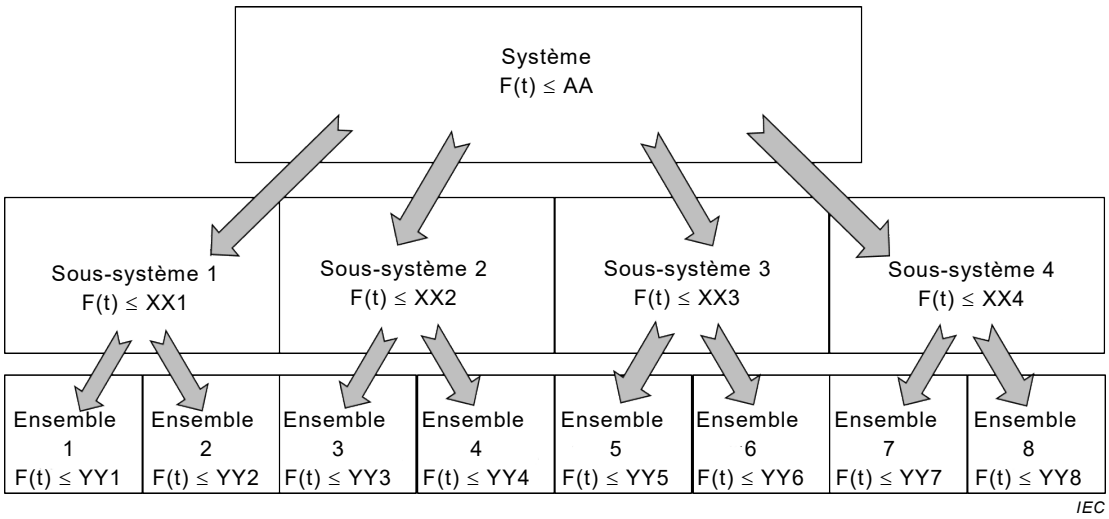


Figure E.2 – Allocation de probabilités de défaillance du système

E.7.3 Évaluation de la criticité des systèmes réparables avec allocation de disponibilité

Les exigences de disponibilité des systèmes réparés sont allouées aux valeurs de sûreté de fonctionnement (la durée moyenne entre pannes (MTBF) pour la fiabilité et la durée moyenne de réparation (MTTR) pour la maintenabilité du système, par exemple). Les valeurs d'indisponibilité du système sont en général utilisées pour évaluer la criticité du système. L'évaluation de l'indisponibilité s'apparente à celle de la probabilité de défaillance (manque de fiabilité). L'indisponibilité est attribuée, mais cette fois, il s'agit d'une entité à deux dimensions, car elle dépend de deux mesures: MTBF et MTTR.

Le processus d'allocation au niveau du système, du sous-système ou de l'ensemble s'apparente aux allocations présentées pour les systèmes non réparés (E.7.2), sauf qu'au lieu d'utiliser la probabilité d'occurrence du mode de défaillance, l'indisponibilité du système, du sous-système ou des ensembles résultant du mode de défaillance est indiquée. Les modes de défaillance à l'origine d'un niveau inacceptable d'indisponibilité doivent être traités.

Annexe F
(informative)

Exemples d'AMDE pour les applications industrielles

F.1 Généralités

Des exemples d'extraits de tableaux d'AMDE sont présentés avec une brève explication du périmètre.

NOTE Les extraits d'exemple concernent principalement les tableaux d'AMDE et seules de brèves descriptions sont données du périmètre. Cela signifie que toutes les considérations relatives aux objectifs et aux limites d'une AMDE ne sont pas expliquées, même si elles s'avèrent adaptées à l'analyse industrielle sur laquelle reposent les exemples.

F.2 Application au processus de santé pour le processus de commande de médicaments

Un extrait d'une AMDE relative au processus de commande d'un médicament dans une pharmacie est présenté dans le Tableau F.1. L'exemple présente une étape du processus avec les effets et les causes des modes de défaillance.

Tableau F.1 – Extrait d'une AMDE relative au processus de commande d'un médicament dans une pharmacie

Étape du processus	Fonction	Mode de défaillance	Effet d'une défaillance	Mécanisme de défaillance	Cause de défaillance
Médicament préparé	Médicament préparé avec le bon principe actif et la bonne concentration	Mauvais médicament	En fonction du médicament particulier choisi	Choix incorrect (bonne intention) Ordonnance mal lue Ordonnance ambiguë	Produits ressemblants Ordonnance illisible Utilisation d'abréviations
		Mauvaise concentration	Surdose Sous-dose	Erreur de calcul Manque de connaissances Ordonnance mal lue	Distraction Ordonnance illisible Manque d'expérience
		Mauvais diluant	Toxicité possible du diluant	Choix incorrect (mauvaise intention) Choix incorrect (bonne intention)	Manque de connaissances Diluant correct indisponible Produits ressemblants

F.3 Application au processus de fabrication pour la peinture au pistolet

Un extrait d'une AMDE relative à une étape de peinture au pistolet du processus de fabrication est présenté dans le Tableau F.2. L'exemple présente une étape du processus avec les effets et les causes des modes de défaillance.

Tableau F.2 – Extrait d'une AMDE relative à l'étape de peinture au pistolet d'un processus de fabrication

Étape du processus	Fonction	Mode de défaillance	Effet d'une défaillance	Mécanisme de défaillance	Cause de défaillance
Peinture au pistolet	Appliquer une couche lisse de 75 microns	Peinture trop épaisse	Mauvais rendu Rejet d'article	Trop de peinture	Pistolet à peinture trop proche Régulateur de peinture défaillant
		Effet peau d'orange	Mauvais rendu	Gouttelettes de peinture avant coalescence	Trop peu d'air Température d'usine trop élevée Ventilateur trop large Pistolet trop éloigné

F.4 Application à la conception d'une pompe à eau

F.4.1 Généralités

Un exemple d'AMDE est présenté ci-dessous, qui met en évidence les informations qu'il convient d'inclure pour chaque étape de l'analyse d'une pompe à eau dont le débit est de 600 l/min et qui fournit de l'eau de refroidissement à un échangeur de chaleur. Un débit de 400 l/min offre les conditions idéales de refroidissement. L'analyse est présentée sous forme narrative, mais elle peut être enregistrée dans un tableau ou une base de données adapté(e).

F.4.2 Fonction de l'entité

Les fonctions de la pompe sont les suivantes:

1) elle fournit de l'eau à un débit de 400 l/min ± 30 l/min à l'échangeur de chaleur primaire;
2) elle contient l'eau avec un taux de fuite inférieur à 0,01 l/h.

NOTE La pompe présente par conception une capacité supplémentaire d'assurer le service exigé (critère de résistance par rapport à la contrainte). Dans ce contexte, si la pompe n'atteint pas sa capacité totale, une sortie inférieure à la valeur maximale peut ne pas correspondre à une perte de fonction.

F.4.3 Modes de défaillance de l'entité

Les modes de défaillance de la pompe pour la fonction 1 sont les suivants:

A. elle fournit de l'eau à un débit inférieur à 370 l/min à l'échangeur de chaleur primaire;
B. elle fournit de l'eau à un débit supérieur à 430 l/min à l'échangeur de chaleur primaire;

Les modes de défaillance de la pompe pour la fonction 2 sont les suivants:

A. elle permet une fuite d'eau à un débit supérieur à 0,01 l/h mais inférieur ou égal à 1 l/h;
B. elle permet une fuite d'eau à un débit supérieur à 1 l/h.

NOTE Les modes de défaillance sont souvent simplement l'opposé de la fonction exigée (comme pour la fonction 1) mais peuvent souvent être étendus pour inclure des niveaux spécifiques auxquels la fonction est perdue (comme dans la fonction 2). Cela n'a en principe un intérêt que si différentes conséquences sont associées à chaque niveau.

F.4.4 Effets de la défaillance de l'entité

Les effets du mode de défaillance de la pompe 1A sont les suivants:

- local: Aucun;
- final: Arrêt du processus (dû à un refroidissement insuffisant).

Les effets du mode de défaillance de la pompe 1B sont les suivants:

- local: Aucun;
- final: Produit en dehors des spécifications (en raison d'un refroidissement excessif).

Les effets du mode de défaillance de la pompe 2A sont les suivants:

- local: Aucun;
- final: Pollution chimique (l'eau s'évapore dans la digue et libère des produits chimiques).

Les effets du mode de défaillance de la pompe 2B sont les suivants:

- local: Aucun;
- final: Arrêt du processus (trop-plein de la digue, dommage aux équipements électriques).

NOTE Par suite de cette analyse, une alarme de niveau peut être placée dans la digue. Une analyse de ce type d'alarme démontrerait que sa défaillance n'a aucune conséquence en soi, mais qu'elle donnerait lieu à un arrêt du processus en cas de fuite de la pompe.

F.5 Exemple d'AMDE avec analyse de criticité pour un système non réparé complexe

Cet exemple utilise les valeurs de fiabilité comme mesure de vraisemblance de défaillance. La Figure F.1 présente la structure hiérarchique d'un système électronique composé de quatre sous-systèmes en série, chacun d'eux étant composé de deux circuits imprimés (CI) avec différents composants électroniques également en série. La Figure F.1 présente également l'allocation des valeurs de fiabilité au niveau du système, du sous-système et de l'ensemble.

Le Tableau F.3 présente l'allocation et l'évaluation des valeurs de fiabilité pour différentes catégories critiques de modes de défaillance pour ce système. Les informations du Tableau F.3 indiquent que les modes de défaillance dans la catégorie III (Majeur) et dans la catégorie II (Critique) dépassent les niveaux acceptables et qu'il est nécessaire de les traiter. Pour savoir lesquels des sous-systèmes/ensembles participent le plus au problème, l'allocation de fiabilité aux sous-ensembles/ensembles est examinée.

À titre d'exemple, le Tableau F.4 présente l'allocation et l'évaluation des valeurs de fiabilité pour le sous-système 2. Les informations du Tableau F.4 indiquent que les modes de défaillance dans la catégorie majeur et dans la catégorie critique dépassent les allocations de fiabilité. En conclusion, l'atténuation des modes de défaillance critique et majeur dans le sous-système 2 est exigée pour réduire l'impact de fiabilité au niveau système des modes de défaillance dans les ensembles 3 et 4 et amener la criticité du système dans des limites de risque admissibles.

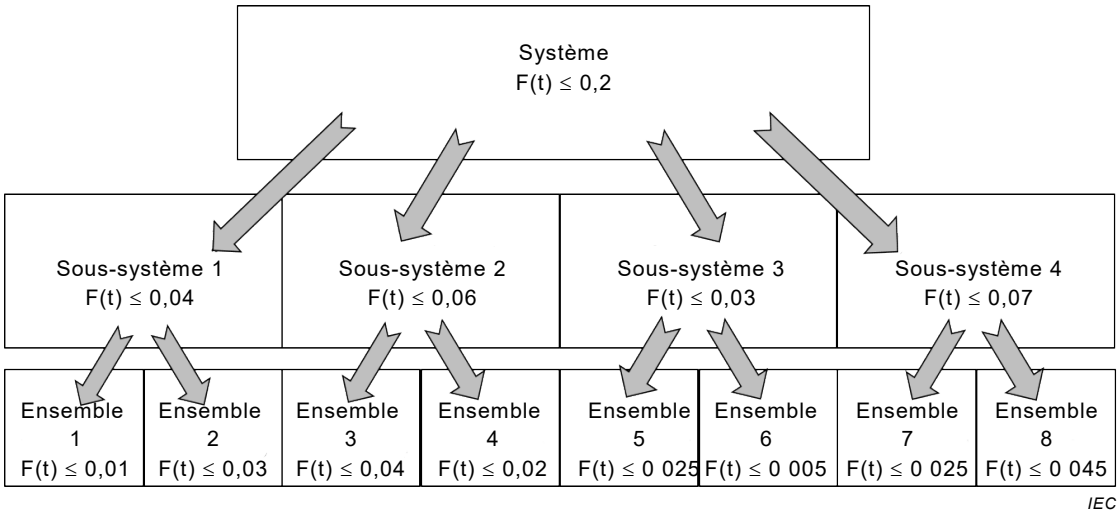


Figure F.1 – Hiérarchie d'un système électronique en série, de ses sous-systèmes et ensembles avec des valeurs de fiabilité allouées F(*t*)

Tableau F.3 – Allocation et évaluation des valeurs de fiabilité pour différentes catégories de criticité des modes de défaillance pour le système électronique représenté à la Figure F.1

	V Négligeable	IV Mineur	III Majeur	II Critique	I Catastrophique
Allocation de fiabilité	≤ 0,1	≤ 0,08	≤ 0,012	≤ 0,007 2	≤ 0,000 8
Évaluation de fiabilité	0,06	0,05	0,03	0,01	0,000 2

Tableau F.4 – Allocation et évaluation des valeurs de fiabilité pour différentes catégories de criticité des modes de défaillance pour le sous-système 2 du système représenté à la Figure F.1

	V Négligeable	IV Mineur	III Majeur	II Critique	I Catastrophique
Allocation de fiabilité	≤ 0,03	≤ 0,02	≤ 0,005 2	≤ 0,004 7	≤ 0,000 07
Évaluation de fiabilité	0,006	0,002 1	0,029	0,008	0,000 02

Ces allocation et évaluation de fiabilité seraient réalisées pour les quatre sous-systèmes et ensembles connexes. Si le niveau de fiabilité est inacceptable, une action visant à améliorer la fiabilité et obtenir un résultat équilibré peut être entreprise pour ces ensembles. À l'issue de cette action et après l'identification des nouvelles performances de l'ensemble, ces valeurs peuvent être progressivement cumulées jusqu'au niveau du sous-ensemble, puis jusqu'à celui du système, grâce aux traitements mathématiques d'un bloc-diagramme de fiabilité ou d'un arbre de panne. Il convient de bien faire attention lorsque des composants identiques sont utilisés au niveau de l'ensemble et veiller à identifier les défaillances de mode commun.

F.6 Application logicielle pour un calculateur du taux de glycémie

Le Tableau F.6 présente une AMDE pour un calculateur du taux de glycémie avec les modes de défaillance, les causes et les effets locaux. Il indique comment les étapes d'utilisation du moniteur et des différents composants utilisés sont tour à tour prises en compte pour identifier les effets et causes des modes de défaillance pour ces dispositifs. Un mode de défaillance très important du calculateur du taux de glycémie est le rétablissement des réglages d'usine du logiciel par suite de la réinitialisation du microprocesseur. Si les réglages d'usine sont en unités US et que l'utilisateur avait utilisé les réglages européens, cette erreur est susceptible de mettre sa vie en danger.

F.7 Dispositifs électroniques automobiles

Le Tableau F.7 présente une petite partie d'une AMDE plus complète réalisée pour un airbag automobile. L'ensemble analysé est l'alimentation électrique et uniquement ses raccordements à la batterie (voir la Figure F.2).

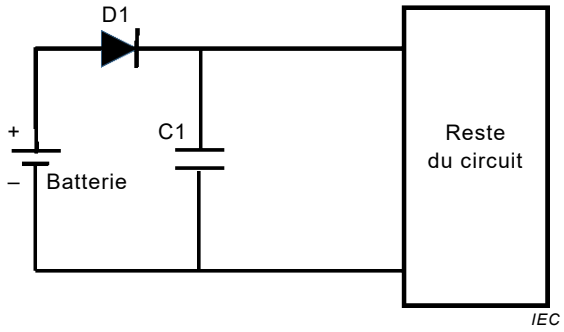


Figure F.2 – Pièce d'airbag automobile

Le circuit est composé d'une diode D1 en ligne avec la borne positive de la batterie et d'un condensateur C1 reliant la ligne positive à la terre. D1 est installé de sorte qu'aucun courant ne puisse circuler dans le circuit si la batterie est connectée en polarité inverse. C1 est fourni pour le filtrage.

Si C1 se retrouve en court-circuit, la borne positive de la batterie est directement reliée à la terre, ce qui provoque le claquage de D1 en raison d'un passage de courant excessif et donne lieu à un circuit ouvert de D1. Le circuit d'airbag est alors inopérant. Ce type de défaillance est considéré comme dangereux, d'où le classement de sévérité S = 10. Des occurrences ont été calculées à partir des taux de défaillance des composants sous leurs contraintes respectives pendant la durée de vie du véhicule, puis ont été mises en correspondance avec une échelle d'occurrences en 10 points, résultant au choix de O = 3. La détection a été considérée comme étant faible car, en cas de défaillance pendant la conduite du véhicule, aucune indication n'est donnée au conducteur, d'où le choix D = 10.

De plus, un circuit ouvert dans la connexion de C1 permettrait au circuit d'airbag de continuer à fonctionner, mais aurait un impact sur l'aptitude de C1 à filtrer la puissance à l'entrée du circuit. Un défaut de circuit ouvert de D1 rendrait également le circuit d'airbag inopérable, aucun courant ne pouvant circuler à partir de la batterie. Un défaut de court-circuit de D1 permettrait au circuit d'airbag de continuer à fonctionner, mais il n'y aurait plus aucune protection contre une inversion de polarité de la batterie.

À l'AMDE du Tableau F.7, les colonnes «action recommandée», «responsabilité et date d'exécution cible» et «résultats de l'action de traitement» n'ont pas été complétées. Cela correspond à la situation d'une équipe AMDE qui délivre une AMDE partiellement complétée à l'équipe projet. L'équipe projet doit alors traiter les risques et proposer des actions et échéances. L'AMDE peut ensuite être complétée en remplissant les colonnes «résultats de l'action de traitement».

F.8 Application à la maintenance et au support d'un système hi-fi

Une télécommande est un dispositif qui permet à l'utilisateur de commander un système hi-fi à distance par infrarouge ou radiocommunication. L'objectif de cet exemple est de présenter la façon dont différentes AMDE peuvent être appliquées à un même produit. Le choix de l'exemple s'est porté sur un produit très simple, et les différentes AMDE ont été considérablement réduites pour économiser de l'espace.

Des exemples d'AMDE système, de conception, processus et de maintenance pour la même entité (une télécommande de système hi-fi) sont présentés aux Tableaux F.8 à F.11 respectivement. L'AMDE système est réalisée au début du projet afin de prendre en compte de façon globale le niveau supérieur du produit (architecture). L'AMDE de conception s'intéresse aux solutions de conception. L'AMDE processus couvre les processus de fabrication, tandis que l'AMDE en service couvre la facilité de réparation du produit (maintenabilité).

Cet exemple présente les différences entre ces types d'AMDE pour la même entité. L'indice de priorité utilisé est le NPR.

F.9 Applications à des systèmes de commande relatifs à la sécurité

F.9.1 Circuit électronique

Une AMDE est réalisée pour évaluer les risques liés à l'interface utilisateur d'un produit de sécurité. Un exemple d'analyse des modes de défaillance, de leurs effets et de leurs diagnostics (AMDED) est donné pour évaluer un circuit électronique. L'exemple n'est pas exhaustif. Il détermine les modes de défaillance, les effets et les capacités de diagnostic des principales parties d'un circuit d'alimentation électrique qui utilisent un régulateur linéaire des tensions d'alimentation internes d'un dispositif. L'extrait de l'AMDE est présenté dans le Tableau F.12.

F.9.2 Système de commande automatique des trains

Un système de commande automatique des trains est un système de bord qui permet l'arrêt d'un train dans le cas où la voie est occupée par un autre train, et ce faisant évite une collision. Si le signal d'arrêt est émis dans un tunnel, il est nécessaire que le train puisse toujours être déplacé afin qu'en cas d'incendie dans ce train, les personnes à bord aient des possibilités de sortie suffisantes. Concernant cette AMDE, le risque sur la santé des passagers est pris en compte.

Si un système de commande automatique des trains ne réussit pas à arrêter le train lorsque cela est exigé, une collision peut se produire. D'un autre côté, il est dangereux que le système de commande automatique des trains ne permette pas au train de sortir du tunnel en cas d'incendie.

Ces dangers d'incendie et de collision sont mutuellement réciproques: si dans un cas il est correct d'arrêter le train, dans l'autre cela pose problème.

Le Tableau F.5 présente les relations entre les modes de défaillance du système de commande automatique des trains, les dangers et les défaillances en sécurité et dangereuses.

Tableau F.5 – Dangers et défaillances en sécurité/dangereuses dans un système de commande automatique des trains

Dangers à commander par un système de commande automatique des trains	Modes de défaillance d'un système de commande automatique des trains	
	Mode de défaillance 1 (court-circuit, par exemple)	Mode de défaillance 2 (déconnexion, par exemple)
Ne réussit pas à éviter la collision	Défaillance dangereuse	Défaillance en sécurité
Incendie dans un tunnel	Défaillance dangereuse	Défaillance dangereuse

F.10 AMDE incluant une analyse des facteurs humains

Le Tableau F.13 présente une AMDE relative au processus d'utilisation d'une cafetière (Masuda, 2003) [28]. Cette AMDE évalue le comportement humain et les risques associés. Il s'agit d'une analyse de l'interaction possible entre la personne, l'équipement et l'environnement, permettant de déduire les modes de défaillance et les options d'atténuation. Elle distingue également les risques pour l'être humain et pour l'équipement, afin de permettre un traitement plus différencié des risques.

Les facteurs humains peuvent être divisés en facteurs positifs (en empêchant une défaillance ou en réduisant la sévérité) ou en facteurs négatifs (en provoquant une défaillance ou en réagissant de manière inappropriée). Les êtres humains peuvent également être affectés et, dans certains cas, il est logique de faire la distinction entre les dommages à l'équipement et à l'environnement et les préjudices aux êtres humains. L'exemple du Tableau F.13 intègre l'être humain comme source de défaillance.

Le champ «Catégorie d'attention» distingue les phases dans lesquelles l'être humain ne se comporte pas correctement. Dans le champ «Analyse des causes d'erreur psychologique», des mots-guides pour les causes d'erreur sont donnés. Le moment et la période auxquels ces catégories d'erreur sont atteintes dépendent du nombre de phases dans lesquelles elles peuvent se produire. Cela peut avoir un impact sur la vraisemblance d'occurrence estimée de ce type d'erreur.

À gauche, les circonstances nécessaires de l'erreur sont évaluées. Dans le champ «Mode d'erreur humaine», il peut être judicieux de faire la distinction entre différents groupes de personnes et, de ce fait, de réduire la valeur de probabilité en fonction de la taille du groupe auquel cette erreur peut être limitée. Ici, une distinction peut être faite entre les adultes (A) et les enfants (E), les femmes et les hommes (F/H), les personnes handicapées (PH) et les personnes âgées (V) ou les personnes indéfinies (I).

Dans ce cas, la décision a été prise d'ajouter les scores en fonction du risque vis-à-vis de l'équipement et de l'être humain afin de générer une valeur de risque au niveau du système. Les contremesures sont également classées de manière à distinguer les moyens d'action possibles: l'occurrence de l'erreur peut-elle être évitée (O), l'occurrence peut-elle être évitée en formant le personnel (F), un système de gestion remédie-t-il à l'occurrence (G) ou des mises en garde adressées au public peuvent-elles être formulées (M).

L'utilisation de ces méthodes dépend dans une large mesure de l'application.

F.11 Processus de marquage et d'encapsulation d'un composant électronique

Le Tableau F.14 donne un extrait de l'AMDE processus réalisée pour le marquage et l'encapsulation d'un composant électronique: un processus dit d'arrière-plan.

Tableau F.6 – Extrait d'une AMDE relative au processus de surveillance de la glycémie *(1 sur 3)*

Entité finale: Calculateur du taux de glycémie **Période d'exploitation: 5 ans**			**Entité: Révision** **logicielle: 0.6**		**Préparé par: NN** **Date: 31/07/2015**		**Mise à jour:** **Par:**	
Étape	**Entité utilisée**	**Fonction**	**Mode de défaillance**	**Mécanisme**	**Cause**	**Effet local**	**Méthode de détection**	**Mesures de compensation**
Réglage de l'appareil de mesure	Appareil de mesure	Mesurer le temps écoulé depuis la dernière dose administrée, données pour les moyennes du matin	Réglage de l'heure incorrect	Confusion 12 h / 24 h		Moyennes du matin affichées incorrectes, l'utilisateur a pu se tromper dans le calcul du temps écoulé depuis la dernière dose administrée	Uniquement si la durée > 12 h	Afficher AM/PM à l'écran, afficher à l'écran la durée écoulée depuis la dernière dose administrée
Étalonnage		Régler le codage pour le lot de bandelettes	Codage erroné	Codage erroné	Erreur de lecture	Valeur erronée élevée ou basse (jusqu'à 30 %)	L'affichage présente un décalage de nombres au moment du codage, facilitant les erreurs de lecture	Réétalonner chaque lot avec la solution d'échantillon
Piqûre au doigt	Lancette	Prélever un échantillon de sang	Quantité de sang insuffisante	Doigts froids, profondeur de piqûre insuffisante		Valeur erronée basse	Aucun	
Transfert de sang sur la bandelette	Bandelettes	Recueillir le sang et le faire réagir	Bandelette défectueuse	Périmé	Utilisation de bandelettes périmées	Valeur erronée élevée ou basse	Date sur la bandelette	Instructions données à l'utilisateur pour vérifier la date avant utilisation
			Réaction inadaptée	Bandelettes stockées à une température ou un taux d'humidité trop élevé(e)/bas(se)	Conditions météorologiques extrêmes	Valeur erronée élevée ou basse	Aucun	
			Échantillon de sang contaminé	Le résidu sur le doigt piqué contient du sucre	Mains non lavées	Valeur erronée élevée	Aucun	Instructions données à l'utilisateur
			Échantillon de sang contaminé	Résidus de crème pour les mains, etc.	Mains non lavées	Valeur erronée basse	Aucun	Instructions données à l'utilisateur

Tableau F.6 *(2 sur 3)*

Entité finale: Calculateur du taux de glycémie **Période d'exploitation: 5 ans**			**Entité: Révision logicielle: 0.6**		**Préparé par: NN** **Date: 31/07/2015**		**Mise à jour:** **Par:**	
Étape	**Entité utilisée**	**Fonction**	**Mode de défaillance**	**Mécanisme**	**Cause**	**Effet local**	**Méthode de détection**	**Mesures de compensation**
Insérer la bandelette	Bandelette, lecteur	Mettre la bandelette dans le lecteur	Pas suffisamment insérée	Utilisateur novice		Valeur erronée basse	Message d'erreur affiché	Instructions données à l'utilisateur
Noter les éventuelles alarmes	Indicateur Hi/Lo (élevé / bas)	Indique que la glycémie est anormalement élevée ou basse		N'est pas indiqué	Indicateur petit			Alarme sonore différente selon que la glycémie est élevée ou basse
Lecture de l'appareil de mesure	Appareil de mesure	Mesurer le signal électrique au niveau de l'électrode et afficher le niveau de glycémie	Nombre affiché incorrect	Certains des segments sont perdus (le 8 s'affiche 6, par exemple)	Batterie faible	Valeur erronée élevée ou basse	Indicateur de batterie faible	
			Sang excessivement concentré	Sujet déshydraté		Valeur erronée élevée	Aucun	
			Unités affichées incorrectes	Unités mal réglées par l'utilisateur	Manque de connaissances	Valeur erronée élevée ou basse (selon le sens de l'erreur d'unités) d'un facteur 10	Indicateur d'unités, patient formé à la reconnaissance d'un relevé anormal et au réétalonnage par rapport à une solution témoin	Indicateur d'unités à lettres de grande taille, recommandation de modifier le logiciel en fonction des unités
			Unités incorrectes	Rétablissement des réglages d'usine lorsque la batterie est déchargée	Intentionnel lorsque la batterie est remplacée	Valeur erronée élevée ou basse (selon le sens de l'erreur d'unités) d'un facteur 10		
					Involontaire lorsque la batterie est tombée	Valeur erronée élevée ou basse (selon le sens de l'erreur d'unités) d'un facteur 10		

Tableau F.6 *(3 sur 3)*

Entité finale: Calculateur du taux de glycémie **Période d'exploitation: 5 ans**			**Entité: Révision** **logicielle: 0.6**		**Préparé par: NN** **Date: 31/07/2015**		**Mise à jour:** **Par:**	
Étape	**Entité utilisée**	**Fonction**	**Mode de défaillance**	**Mécanisme**	**Entité utilisée**	**Effet local**	**Méthode de détection**	**Mesures de compensation**
					Les Américains qui achètent l'appareil de mesure en Europe ne remarquent pas la différence d'unités (ou inversement)	Valeur erronée élevée ou basse (selon le sens de l'erreur d'unités) d'un facteur 10		
				Corriger le numéro/les unités qui s'affichent – erreur de relevé	Affichage pas suffisamment clair			Affichage ergonomique pour faciliter la lecture
NOTE L'unité du taux de glycémie est le mg/dl aux États-Unis et le mmol/l en Europe. Il y a un facteur d'environ 10 entre les valeurs numériques.								

Tableau F.7 – Extrait d'une AMDE relative aux composants électroniques d'une automobile *(1 sur 2)*

Entité/Fonction			Mode de défaillance potentiel	Effet(s) potentiel(s) de la défaillance		S	Causes/mécanismes potentiel(le)s de défaillance	Causes/mécanismes détaillé(e)s de défaillance	O	Prévention des commandes de conception en cours	Détection des commandes de conception en cours	D	NPR	Action recommandée	Responsabilité et date d'exécution cible	Résultats de l'action de traitement				
Sous-système	Ensemble	Composant		Effet local	Effet final											Action entreprise	S	O	D	NPR
Alimentation électrique																				
	V1																			
		D1	Court-circuit	Pas de protection contre les tensions inverses.	L'entité fonctionne hors spécifications.	2	Défaut inhérent du composant avec une probabilité de court-circuit = 80 %	Panne du matériel	3	Choix d'une qualité ou de caractéristiques assignées supérieure(s)	Évaluation et essai de validation de la fiabilité	10	60							
		D1	Circuit ouvert	Pas de tension fournie à l'entité.	Entité inopérable.	10	Défaut inhérent du composant avec une probabilité de circuit ouvert = 20 %	Liaison équipotentielle ou fissure du semi-conducteur	3	Choix d'une qualité ou de caractéristiques assignées supérieure(s)	Évaluation et essai de validation de la fiabilité	10	300							
		C1	Court-circuit	Tension de batterie + courts-circuits à la terre. Claquage de D1.	Pas de tension fournie à l'entité. Entité inopérable.	10	Défaut inhérent du composant avec une probabilité de court-circuit = 10 %	Rupture diélectrique ou fissure	3	Choix d'une qualité ou de caractéristiques assignées supérieure(s)	Évaluation et essai de validation de la fiabilité	10	300							

Tableau F.7 *(2 sur 2)*

Entité/Fonction			Mode de défaillance potentiel	Effet(s) potentiel(s) de la défaillance		S	Causes/mécanismes potentiel(le)s de défaillance	Causes/mécanismes détaillé(e)s de défaillance	O	Prévention des commandes de conception en cours	Détection des commandes de conception en cours	D	NPR	Action recommandée	Responsabilité et date d'exécution cible	Résultats de l'action de traitement				
Sous-système	Ensemble	Composant		Effet local	Effet final											Action entreprise	S	O	D	NPR
		C1	Circuit ouvert	Pas de filtrage	L'entité fonctionne hors spécifications.	2	Défaut inhérent du composant avec une probabilité de circuit ouvert = 90 %	Circuit ouvert diélectrique, fuite, vide ou fissure	2	Choix d'une qualité ou de caractéristiques assignées supérieure(s)	Évaluation et essai de validation de la fiabilité	10	40							

Légende

S = Sévérité, O = Occurrence, D = Détectabilité

NOTE Il s'agit d'une AMDE partiellement complétée. L'équipe projet doit traiter les risques et proposer des actions et échéances. L'AMDE peut ensuite être complétée en remplissant les colonnes «résultats de l'action de traitement».

Tableau F.8 – Extrait d'une AMDE système pour une télécommande de système hi-fi

Composant	Fonction	Mode de défaillance	Conséquence locale	Conséquence globale	Sévérité	Probabilité	Détectabilité	NPR	Action de traitement
Clavier	Permettre la sélection de l'action de commande en appliquant une force de 20 à 50 g avec le doigt	Les touches situées sous la face avant empêchent l'application de toute force par le pouce	Les touches ne peuvent être pressées	La télécommande ne peut commander la hi-fi	4	3	2	24	Fixation du circuit imprimé à la face supérieure afin de réduire les problèmes de tolérance
Circuit imprimé	Interpréter les commandes du clavier et transmettre l'action de commande aux LED en 100 ms	Défaillance des joints de soudure et des contacts à cause de la résonance mécanique	Certains signaux ne peuvent être transmis aux LED	La télécommande ne peut commander certaines fonctions hi-fi	4	2	5	40	Augmentation des fréquences de résonance
Affichage	Afficher l'action de commande sélectionnée en 100 ms	L'affichage se déplace de la face avant de la télécommande à cause d'une fixation insuffisante	L'affichage est perdu	Une réparation est nécessaire	3	2	3	18	Zone de collage plus grande

Tableau F.9 – Extrait d'une AMDE de conception pour une télécommande de système hi-fi

Composant	Fonction	Mode de défaillance	Conséquence locale	Conséquence globale	Sévérité	Probabilité	Détectabilité	NPR	Action de traitement
Clavier	Convertir l'énergie cinétique en signal électrique	Contamination par des liquides non évitée	Haute résistance de contact	Pas de fonction	4	5	5	100	Revêtement en plastique sous les touches
Circuit imprimé	Traiter et transmettre les signaux	Contamination par des liquides non évitée	Haute résistance de contact	Pas de fonction	4	5	5	100	Revêtement en plastique sous les touches
Affichage	Afficher un signal à partir du circuit imprimé	Résistance élevée du connecteur	Faux contact	Affichage vierge	4	2	5	40	Spécification du connecteur et essai en production

Tableau F.10 – Extrait d'une AMDE processus pour une télécommande de système hi-fi

Étape	Fonction	Problème potentiel	Conséquence locale	Conséquence globale	Sévérité	Probabilité	Détectabilité	NPR	Action de traitement
Soudure du connecteur du clavier	Connecter le clavier et le circuit imprimé	Excès de flux	Haute résistance	Connexion intermittente	4	2	4	32	Pas de flux pur
Soudure du composant CMS	Connecter le composant CMS et le circuit imprimé	Pierre tombale	Pas de connexion du CMS au circuit imprimé	Peu de rendement causant des coûts de production élevés	2	2	2	8	Montage circuit imprimé
Coller l'écran LCD à la face avant	Sécuriser l'écran LCD sur la face avant	Petite zone de collage	Faible adhésion	Séparation de l'écran LCD de la face avant	4	4	5	80	Analyse MEF

Tableau F.11 – Extrait d'une AMDE en service de maintenance pour une télécommande de système hi-fi

Composant	Fonction	Problème potentiel	Conséquence locale	Conséquence globale	Sévérité	Probabilité	Détectabilité	NPR	Action de traitement
Clavier	Évaluer l'opérabilité du clavier	Raccordement de câble court entre le clavier et l'affichage	Difficile de regarder l'écran tout en tapant sur le clavier	Durée de réalisation de la maintenance augmentée Risque accru de faute	3	5	5	75	Câble de raccordement
Circuit imprimé	Retirer et replacer le circuit imprimé	Le processus de retrait exige le dévissage des vis	Pas de vis abîmée	Nouvelle face avant exigée	4	4	4	64	Insertion métallique
Affichage	Replacer l'affichage défaillant	Incapacité de séparer l'affichage de la face avant sans dommage	Nouvelle face avant	Réparation onéreuse	4	2	4	32	Fiabilité de l'affichage

Tableau F.12 – Extrait d'une AMDED de processus pour le circuit électronique d'un système de commande de sécurité *(1 sur 3)*

Schéma de circuit:

Liste des pièces:

Créé par:

Revu par:

Taux de défaillance et base de données de distribution: spécifique à la société (exemple)

Date de l'analyse:

Nom	Composant	Fonction	Taux de défaillance [FIT]	Mode de défaillance	Rapport du mode de défaillance	Effet	Effet du comportement S: Sécurité D: Dangereux	Couverture du diagnostic
F50	Fusible	Protection contre les courts-circuits à l'entrée	25	Ouverture impossible	50 %	Aucun en fonctionnement normal	Aucun effet	-
				Ouverture prématurée	10 %	Pas de tension en sortie	S	-
				Ouverture lente	40 %	Aucun effet sur la fonction de sécurité	Aucun effet	-
D12	Diode de suppression	Protection contre les surtensions (CEM)	7	Court-circuit	95 %	F50 saute	S	-
				Circuit ouvert	5 %	Aucun effet sur la fonction de sécurité	Aucun effet	-
R100	Résistance, CMS	Limitation de courant, CEM	0,2	Court-circuit	5 %	Pas de limitation de courant – défaillance	D	60 %
				Circuit ouvert	65 %	Pas de tension en sortie	S	-
				Modification de paramètre	30 %	Fonction toujours assurée	Aucun effet	-
C13	Condensateur céramique, HDC/MDC	CEM	2	Court-circuit	50 %	F50 saute	S	-
				Circuit ouvert	30 %	Aucun en fonctionnement normal (pas de protection)	Aucun effet	-
				Modification de valeur	20 %	Fonction toujours assurée	Aucun effet	-

Tableau F.12 *(2 sur 3)*

Nom	Composant	Fonction	Taux de défaillance [FIT]	Mode de défaillance	Rapport du mode de défaillance	Effet	Effet du comportement S: Sécurité D: Dangereux	Couverture du diagnostic
D25	Diode de signal, < 0,1 W	Redresseur en pont	1	Court-circuit	50 %	F50 saute	S	-
				Circuit ouvert	35 %	Pas de redressement correct en cas d'alimentation en courant alternatif	S	-
				Modification de paramètre	15 %	Fonction toujours assurée	Aucun effet	-
C2	Condensateur électrolytique, électrolyte à l'aluminium, électrolyte non solide	Condensateur de filtrage	5	Court-circuit	53 %	F50 saute	S	-
				Circuit ouvert	35 %	Aucun en fonctionnement normal avec une alimentation en courant continu	Aucun effet	-
				Fuite d'électrolyte	10 %	Aucun effet sur la fonction de sécurité	Aucun effet	-
				Diminution de la capacité	2 %	Fonction toujours assurée	Aucun effet	-

Tableau F.12 *(2 sur 3)*

Nom	Composant	Fonction	Taux de défaillance [FIT]	Mode de défaillance	Rapport du mode de défaillance	Effet	Effet du comportement S: Sécurité D: Dangereux	Couverture du diagnostic
IC18	Régulateur, puissance > 1 W, complexité mineure	Régulateur de tension utilisé avec R100 comme source de courant	25	Stuck-hi	30 %	Pas de régulation -> commutation de sortie	D	0 %
				Stuck-lo	30 %	Pas de tension en sortie	S	-
				Court-circuit	15 %	Pas de régulation -> surintensité au niveau du relais (diverse)	Aucun effet	-
				Circuit ouvert	15 %	Pas de tension en sortie	S	-
				Dérive	5 %	Fonction toujours assurée	Aucun effet	-
				Fonction	5 %	Fonction toujours assurée	Aucun effet	-

Récapitulatif:

λ_{du} = 7,504 FIT = (Σ Taux_Défaillance x % de distribution) de tous les composants avec comportement «D» et 0 % DC

λ_{dd} = 0,006 FIT = (Σ Taux_Défaillance x % de distribution x % DC) de tous les composants avec comportement «D» et DC > 0 %

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

λ_{s} = 25,03 FIT = (Σ Taux_Défaillance x % de distribution) de tous les composants avec comportement «S»

$\lambda_{no\ effect}$ = 32,66 FIT = (Σ Taux_Défaillance x % de distribution) de tous les composants avec comportement «aucun effet»

λ_{total} = 65,2 FIT = (Σ Taux_Défaillance) de tous les composants

SFF (proportion de défaillances en sécurité) = {(total des taux de défaillance de «sécurité» et des taux de défaillance «dangereuse») – (total des taux de défaillance «dangereuse» non détectée)}/(total des taux de défaillance de «sécurité» et «dangereuse»)

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

NOTE La distribution représente le mode de défaillance sous la forme d'un pourcentage du nombre total de défaillances.

Tableau F.13 – Extrait d'une AMDE relative à une cafetière *(1 sur 2)*

Catégorie d'attention	**Potentiel d'erreur (taux d'erreur)**	**Analyse des causes d'erreur psychologique**															**Analyse des effets**
Fatigue, travail monotone	Élevé (au moins 0,1)	x			x	x				x	x						
Travail routinier, repos	Assez élevé (0,01 à 0,000 01)				x	x											
Action positive	Bas (0,000 001 ou moins)				x	x											
Intense, panique	Élevé (au moins 0,1)				x	x				x	x			x			

Phase d'exploitation	Activité	Environnement concerné	Équipement affecté	Relation	Mode d'erreur humaine	Catégorie d'êtres humains	Mots-guides d'erreur															Analyse des effets (dommages)			Score d'occurrence		Score de sévérité		Score de risque			Classement des contremesures	Contremesures (Action corrective)
							Percep-tion			Décision				Action																			
							Difficile de voir ou d'entendre	Mauvaise perception	Incompréhensible	Manque de compréhension	Connaissances insuffisantes	Compréhension lente	Mauvaise compréhension	Pas d'exécution	Oubli d'exécution	Exécution inadaptée	Exécution excessive	Exécution trop tardive	Exécution prématurée	Exécution différente	Mauvais ordre d'exécution	Matériel	Être humain	Système	Matériel	Être humain	Matériel	Être humain	Matériel	Être humain	Système = Être humain + Matériel		

Tableau F.13 *(2 sur 2)*

Chauffage	Mettre l'appareil sous tension et placer la cafetière sur la plaque chauffante	Être pressé/oubli	Défaillance du capteur de température	ET	Café laissé trop longtemps sur le feu	I									x							Dysfonctionnement	Dommage secondaire provoqué par le feu	Incendie	2	1	4	4	8	4	12	O	Prévoir du temps pour la phase de nettoyage
Utilisation	Verser le café dans une tasse	Fatigue	Aucun	ET	Renversement du café	I										x		x				Aucun	Blessure/ plaie par brûlure	---	1	2	1	3	1	6	7	O	Prévoir du temps pour contacter le client
Nettoyage	Jeter l'ancien café	Être pressé	Aucun	(OU)	Renversement du café chaud	I	x															Aucun	Blessure/ plaie par brûlure	---	1	2	1	4	1	8	9	O	Prévoir du temps pour le nettoyage
	Laver à la main	Être pressé	Présence de coins et d'arêtes vifs	ET	Contact à mains nues avec l'arête	I	x												x			Aucun	Blessure/ plaie par brûlure	---	1	2	2	4	2	8	10	W	Permettre uniquement le nettoyage de la machine
Stockage	Stocker	Dans les régions froides	Rupture des tuyaux en raison de l'eau gelée	←	Eau non retirée	I	x								x							Dommage	Aucun	Non disponible	4	4	4	2	16	8	24	W	Mise en garde dans le manuel d'instructions

NOTE 1 Catégorie d'êtres humains – I: Indéfini H: Homme A: Adulte F: Femme E: Enfant V: Personne âgée M: Malade.

NOTE 2 Classement des contremesures – O: Mesures de prévention contre l'occurrence de dommages, S: Mesures de prévention contre la propagation des dommages, W: Mesures de mise en garde contre les dommages, E: Éducation du client en matière d'utilisation en toute sécurité, M: Examen du système de management de la sécurité

Tableau F.14 – Extrait d'une AMDE pour le processus de marquage et d'encapsulation d'un composant électronique *(1 sur 2)*

Exigence de fonctionnement du processus	Mode de défaillance potentiel	Effet(s) potentiel(s) de la défaillance	S	Mécanisme s(s)/ cause(s)/ potentiel(s)	O	Contrôles du processus en cours	D	NPR	Action(s) recommandée (s)	Responsabilité et date d'exécution cible	Action entreprise	Nouveau S	Nouveau O	Nouveau D	Nouveau NPR
Marquage	Devient flou	Impossible de déchiffrer l'impression	8	Gestion de la condition laser inappropriée	2	Contrôle visuel au début du travail – vérifier le cycle toutes les 1 feuille /lot	2	32	Aucun						
	Décalages du marquage	Mauvais rendu	8	Décalage de position d'un acheminement	2	Essai du cycle de marquage toutes les 1 feuille / lot	1	16	Aucun						
	Le marquage est dans le sens opposé	Mauvais rendu	8	Le produit est placé dans le sens opposé	2	Le sens du produit est jugé par la fréquence de reconnaissance d'image	1	16	Aucun						

Tableau F.14 *(2 sur 2)*

Exigence de fonctionnement du processus	Mode de défaillance potentiel	Effet(s) potentiel(s) de la défaillance	S	Mécanisme s(s)/ cause(s)/ potentiel(s)	O	Contrôles du processus en cours	D	NPR	Action(s) recommandée (s)	Responsabilité et date d'exécution cible	Action entreprise	Nouveau S	Nouveau O	Nouveau D	Nouveau NPR
Rupture	Bavure et creux dans un produit	Taille incorrecte du produit	8	Le jeu lors de la définition d'un substrat avec un outil exclusif est trop important	4	La maintenance d'un contrôle automatique d'un outil exclusif	2	64	Introduction d'une pastilleuse neuve, inspectée lors de l'introduction	Technologie de fabrication de production 31 janvier 2003	Introduction d'une pastilleuse neuve, inspectée lors de l'introduction Vérification de la taille du produit Cpk: 2.58	7	2	2	28
	L'extérieur d'un produit s'élargit	Taille incorrecte du produit	8	La meule est usée	4	Mesurage de la taille d'échantillonnage Cycle d'échantillonnage: 4 pcs toutes les cinq feuilles	2	64	Introduction d'une pastilleuse neuve, inspectée lors de l'introduction	Comme ci-dessus	Comme ci-dessus	7	2	2	28
Suppression des bavures	Une bavure n'a pas été retirée	Taille incorrecte du produit	8	Un gabarit a bougé – la synchronisation est incorrecte	1	Autocontrôle	2	16	Aucun						

Légende

S = Sévérité, O = Occurrence, D = Détectabilité

Bibliographie

[1] IEC 60300-1, *Gestion de la sûreté de fonctionnement – Partie 1: Lignes directrices pour la gestion et* l'application

[2] IEC 60300-3-1, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique*

[3] IEC 60300-3-12, *Gestion de la sûreté de fonctionnement – Partie 3-12: Guide d'application – Soutien logistique intégré*

[4] IEC 60300-3-11, *Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité*

[5] IEC 61025, *Analyse par arbre de panne (AAP)*

[6] IEC 61078, *Diagrammes de fiabilité*

[7] IEC 61165, *Application des techniques de Markov*

[8] IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

[9] IEC 61709, *Composants électriques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles de contraintes pour la conversion*

[10] IEC 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

[11] IEC 62308, *Fiabilité de l'équipement – Méthodes d'évaluation de la fiabilité*

[12] IEC 62502, *Techniques d'analyse de la sûreté de fonctionnement – Analyse par arbre d'événement (AAE)*

[13] IEC 62508, *Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement*

[14] IEC 62551, *Techniques d'analyse de sûreté de fonctionnement – Techniques des réseaux de Pétri*

[15] IEC 62740, *Analyse de cause initiale (RCA)*

[16] IEC 62741, *Démonstration des exigences de sûreté de fonctionnement – Argumentaire dans le cadre de la sûreté de fonctionnement*

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

[18] ISO 9000, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

[19] ISO 31000, *Management du risque – Lignes directrices*

[20] IEC/ISO 31010, *Gestion des risques – Techniques d'évaluation des risques*

[21] ISO 13849-1, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

[22] ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes* (disponible en anglais seulement)

[23] ISO 55000, *Gestion d'actifs – Aperçu général, principes et terminologie*

[24] EN 13306:2010, *Maintenance – Terminologie de la maintenance*

[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, *Management du risque – Vocabulaire*

[32] IEC 60050-191[2], *Vocabulaire Électrotechnique International – Partie 191: Sûreté de fonctionnement et qualité de service*

_____

[2] Supprimée, remplacé par IEC 60050-192

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