NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60812

Deuxième édition
Second edition
2006-01

Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)

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

Numéro de référence
Reference number
CEI/IEC 60812:2006

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**
- **Catalogue des publications de la CEI**

  Le catalogue en ligne sur le site web de la CEI (www.iec.ch/searchpub) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.
- **IEC Just Published**

  Ce résumé des dernières publications parues (www.iec.ch/online_news/justpub) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.
- **Service clients**

  Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

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

Publication numbering

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

Consolidated editions

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

Further information on IEC publications

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

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

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

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

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

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

.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60812

Deuxième édition
Second edition
2006-01

Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)

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

© IEC 2006 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

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

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE X

Pour prix, voir catalogue en vigueur
For price, see current catalogue

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS

Not for Resale

SOMMAIRE

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

CONTENTS

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

TECHNIQUES D'ANALYSE DE LA FIABILITÉ DU SYSTÈME – PROCÉDURE D'ANALYSE DES MODES DE DÉFAILLANCE ET DE LEURS EFFETS (AMDE)

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

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

Cette deuxième édition annule et remplace la première édition publiée en 1985 et constitue une révision technique.

Les modifications majeures par rapport à l'édition précédente sont les suivantes:

– introduction des concepts d'effets des modes de défaillance et de leur criticité ;
– introduction des méthodes largement utilisées dans l'industrie automobile;
– ajout de références et de relations aux autres méthodes d'analyse des modes de défaillance;
– ajout d'exemples;
– fourniture de guides sur les avantages et les inconvénients des différentes méthodes AMDE.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

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

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

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

The main changes from the previous edition are as follows:

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1072/FDIS	56/1091/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.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

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

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

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

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

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

TECHNIQUES D'ANALYSE DE LA FIABILITÉ DU SYSTÈME – PROCÉDURE D'ANALYSE DES MODES DE DÉFAILLANCE ET DE LEURS EFFETS (AMDE)

1 Domaine d'application

La présente Norme Internationale décrit l'analyse des modes de défaillance et de leurs effets (AMDE) et l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC), et apporte des conseils sur l'application de ces méthodes selon les divers objectifs recherchés, de la façon suivante:

– en fournissant la procédure à suivre pour réaliser une analyse,

– en spécifiant les termes pertinents, les hypothèses, les mesures de criticité, les modes de défaillance,

– en déterminant les principes de base,

– en fournissant des exemples-types de documents et tableaux.

Etant donné que l'AMDEC est une suite logique de l'AMDE, toutes les remarques générales d'ordre qualitatif se rapportant à l'une sont applicables à l'autre.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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).

CEI 60300-3-1:2003, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique* (disponible en anglais seulement)

CEI 61025, *Analyse par arbre de panne (AAP)*

CEI 61078, *Techniques d'analyses pour la sûreté de fonctionnement – Méthode du bloc-diagramme de fiabilité*

3 Termes et définitions

Pour les besoins du présent document, les définitions suivantes s'appliquent:

3.1
dispositif / entité
tout élément, composant, sous-système, unité fonctionnelle, équipement ou système que l'on peut considérer individuellement

NOTE 1 Un dispositif/entité peut être constitué de matériel, de logiciel ou des deux à la fois, et peut aussi dans certains cas comprendre du personnel.

NOTE 2 Un ensemble déterminé de dispositifs/entités, par exemple une population ou un échantillon, peut lui-même être considéré comme un dispositif/entité.

[VEI 191-01-01]

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

1 Scope

This International Standard describes Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects and Criticality Analysis (FMECA), and gives guidance as to how they may be applied to achieve various objectives by

– providing the procedural steps necessary to perform an analysis;

– identifying appropriate terms, assumptions, criticality measures, failure modes;

– defining basic principles;

– providing examples of the necessary worksheets or other tabular forms.

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

2 Normative references

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

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

IEC 61025, *Fault tree analysis (FTA)*

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

3 Terms and definitions

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

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

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

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

[IEV 191-01-01]

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Un procédé peut aussi être considéré comme un dispositif/entité qui accomplit une fonction prédéterminée et pour lequel un processus AMDE ou AMDEC peut être mené. Normalement, une AMDE d'un matériel ne traite pas des personnes et de leurs interactions avec les matériels/logiciels, alors qu'une AMDE portant sur un procédé inclut normalement les actions des personnes.

3.2
défaillance
cessation de l'aptitude d'une entité à accomplir une fonction requise

[VEI 191-04-01]

3.3
panne
état d'une entité inapte à accomplir une fonction requise, non comprise l'inaptitude due à la maintenance préventive ou à d'autres actions programmées, ou due à un manque de moyens extérieurs

NOTE 1 Une panne est souvent le résultat d'une défaillance du dispositif lui-même, mais peut exister sans une défaillance préalable.

[VEI 191-05-01]

NOTE 2 Pour des raisons historiques, le mot «panne» est aussi utilisé dans ce document à la place du terme « défaillance ».

3.4
effet de défaillance
conséquence du mode de défaillance en termes de fonctionnement, fonction ou état du dispositif

3.5
mode de défaillance
manière dont un dispositif tombe en panne

3.6
criticité d'une défaillance
combinaison de la sévérité d'un effet et de la fréquence de son apparition, ou d'autres attributs d'une défaillance comme une mesure de la nécessité d'un traitement ou d'une atténuation

3.7
système
ensemble d'éléments interactifs ou reliés entre eux

NOTE 1 Dans un contexte de sûreté de fonctionnement, un système aura

a) divers objectifs exprimés en termes de fonctions requises,

b) l'indication des conditions d'exploitation (voir 191-01-12),

c) une limite définie.

NOTE 2 La structure d'un système est hiérarchique.

[ISO 9000:2000]

3.8
sévérité de la défaillance
signification ou classement de l'effet d'un mode de défaillance sur le fonctionnement du dispositif, sur l'environnement du dispositif, ou sur l'opérateur du dispositif; la sévérité de l'effet d'un mode de défaillance est liée aux limites définies pour le système analysé

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

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

[IEV 191-04-01]

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

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

[IEV 191-05-01]

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

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

3.5
failure mode
manner in which an item fails

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

3.7
system
set of interrelated or interacting elements

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

a) defined purposes expressed in terms of required functions;

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

c) a defined boundary.

NOTE 2 The structure of a system is hierarchical.

[ISO 9000:2000]

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

4 Vue d'ensemble

4.1 Introduction

L'analyse des modes de défaillance et de leurs effets (AMDE) est une procédure systématique, formelle, d'analyse d'un système pour identifier les modes de défaillance potentiels, leurs causes et les effets sur l'aptitude à la fonction du système (aptitude à la fonction de l'assemblage hiérarchiquement au-dessus et du système global ou d'un procédé). Ici, le terme « système » représente un matériel, un logiciel (avec leurs interactions) ou un procédé. L'analyse est menée de préférence tôt dans le cycle de développement de sorte que le retrait ou l'atténuation du mode de défaillance soit le plus efficace. Cette analyse peut être initiée dès que le système est suffisamment défini pour pouvoir être représenté sous forme d'un bloc-diagramme fonctionnel dont l'aptitude à la fonction des éléments peut être définie.

Le moment où a lieu l'AMDE est essentiel; si elle n'est pas faite suffisamment tôt dans le cycle de développement, l'incorporation des modifications de conception pour maîtriser les déficiences identifiées par l'AMDE peut ne pas être efficace. Par conséquent, il est important d'inclure l'AMDE et ses conclusions dans le plan et le programme de développement. Ainsi, l'AMDE est un processus itératif qui est mené conjointement au processus de conception.

L'AMDE est applicable aux différents niveaux de décomposition d'un système, du niveau le plus haut du bloc-diagramme jusqu'aux fonctions des composants discrets et des instructions logicielles. L'AMDE est aussi un processus itératif qui est mis à jour au fur et à mesure de la progression de la conception. Pour les modifications de conception, les parties concernées de l'AMDE doivent être revues et mises à jour.

Une AMDE menée rigoureusement est le résultat obtenu par une équipe composée d'individus qualifiés pour identifier et évaluer l'ampleur et les conséquences de types variés d'inadéquations dans la conception du produit, pouvant conduire à des défaillances. Le travail en équipe a l'avantage de stimuler les processus de réflexion, et d'assurer l'expertise nécessaire.

L'AMDE est considérée comme une méthode pour identifier la sévérité de modes de défaillance potentiels et pour introduire dans la conception des mesures pour réduire les risques. Cependant, dans certaines applications, l'AMDE inclut également une estimation de la probabilité d'apparition des modes de défaillance. Cela améliore l'analyse en fournissant une mesure de la probabilité du mode de défaillance.

L'application de l'AMDE est précédée d'une décomposition hiérarchique du système (matériel et logiciel, ou un procédé) dans ses moindres éléments de base. L'utilisation de blocs-diagrammes simples pour illustrer cette décomposition est utile (CEI 61078). L'analyse débute donc avec les éléments du niveau le plus bas. Un effet du mode de défaillance à bas niveau peut devenir une cause de défaillance d'un mode de défaillance d'un dispositif du niveau juste au-dessus. L'analyse est réalisée du bas vers le haut jusqu'à ce que l'effet final soit identifié sur le système. La Figure 1 illustre ces concepts.

L'AMDEC (Analyses des Modes de Défaillance, de leurs Effets et de leur Criticité) est une extension de l'AMDE qui comprend un moyen de classer les modes de défaillance par sévérité pour permettre de donner la priorité aux contre-mesures. Cela est obtenu en combinant la mesure de la sévérité et la fréquence d'apparition pour fournir une criticité dite métrique.

Les principes de l'AMDE peuvent s'appliquer en dehors de la conception d'ingénierie. La procédure AMDE peut s'appliquer à un procédé de fabrication ou à d'autres processus de travail, telles que dans les hôpitaux, les laboratoires médicaux, les scolarités, ou autres.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

4 Overview

4.1 Introduction

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

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

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

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

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

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

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

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Lorsque l'AMDE est appliquée à un procédé de fabrication, cette procédure est identifiée comme AMDE de procédé ou PAMDE. Pour qu'une AMDE soit efficace, des ressources adéquates pour un travail en équipe doivent être attribuées. Une compréhension approfondie du système sous analyse n'est pas indispensable pour une AMDE préliminaire. Avec le développement de la conception, l'analyse détaillée d'un mode de défaillance nécessite une connaissance approfondie de la conception et de ses spécifications. Les conceptions d'ingénierie complexes nécessitent généralement l'implication de multiples domaines d'expertise de conception (ex.: ingénierie mécanique, ingénierie électrique, ingénierie des systèmes, ingénierie logicielle, support de maintenance, etc.).

L'AMDE porte généralement sur les modes de défaillance individuels et les effets de ces modes de défaillance sur le système. Chaque mode de défaillance est traité en étant considéré comme indépendant. La procédure n'est donc pas adaptée à la prise en considération de défaillance dépendant ou résultant d'une suite d'événements. D'autres méthodes et techniques, telles que l'analyse de Markov (voir CEI 61165) ou Analyse par Arbre de Panne (voir CEI 61025) peuvent être nécessaires pour analyser ces situations.

Lors de la détermination de l'impact d'une défaillance, il faut considérer le niveau plus élevé concerné – défaillances résultantes et éventuellement le même niveau de défaillances induites. Il convient que l'analyse mentionne la combinaison possible de modes de défaillance ou leur succession qui ont été une cause d'un effet de niveau élevé. Dans ce cas, une modélisation complémentaire est requise pour estimer l'ampleur ou la probabilité d'apparition de tels effets.

AMDE est un outil souple qui peut être adapté pour répondre à des besoins spécifiques de l'industrie ou à des produits. Des documents spécialisés avec des données spécifiques peuvent être adaptés à certaines applications. Si des niveaux de sévérité des modes de défaillance sont définis, ils peuvent l'être différemment pour des systèmes différents ou des niveaux de systèmes différents.

4.2 But et objectifs de l'analyse

Les raisons d'entreprendre l'analyse des modes de défaillance et de leurs effets (AMDE) ou l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) peuvent être les suivantes:

a) identifier les défaillances qui ont des effets non souhaités sur le fonctionnement du système, ex.: empêcher ou dégrader significativement le fonctionnement ou affecter la sécurité de l'opérateur;

b) satisfaire aux exigences contractuelles d'un client, si applicable;

c) permettre des améliorations de la fiabilité ou de la sécurité du système (ex. des modifications de la conception ou des actions d'assurance-qualité);

d) permettre des améliorations de la maintenabilité du système (en mettant en évidence les zones de risque ou de non-conformité pour la maintenabilité).

Compte tenu des raisons données ci-dessus pour entreprendre une AMDE, les objectifs d'une AMDE (ou AMDEC) peuvent être les suivants:

a) une évaluation et identification détaillée de tous les effets indésirables dans les limites définies du système sous analyse, et les séquences d'événements amenées par chaque mode de défaillance du dispositif identifié, quelle que soit la cause, à divers niveaux de la hiérarchie fonctionnelle du système,

b) la détermination de la criticité ou de la priorité pour traiter/atténuer (voir Article 6) chaque mode de défaillance par rapport à la fonction correcte du système ou aptitude et l'impact sur le processus concerné,

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

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

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

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

4.2 Purpose and objectives of the analysis

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

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

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

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

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

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

a) a comprehensive identification and evaluation of all the unwanted effects within the defined boundaries of the system being analysed, and the sequences of events brought about by each identified item failure mode, from whatever cause, at various levels of the system's functional hierarchy;

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

c) une classification des modes de défaillance identifiés d'après les caractéristiques en question, comprenant l'aptitude à la détection, au diagnostic, aux essais, au remplacement du dispositif, les provisions de fonctionnement et de compensation (réparation, maintenance, logistique, etc.),

d) l'identification des défaillances fonctionnelles du système et estimation des mesures de la sévérité et de la probabilité de défaillance,

e) le développement d'un plan d'amélioration de la conception pour la réduction des modes de défaillance,

f) le soutien du développement d'un plan de maintenance effectif pour atténuer ou réduire la probabilité de défaillance (voir CEI 60300-3-11).

NOTE Quand il s'agit de criticité ou probabilité d'apparition, les commentaires concernent la méthodologie AMDEC.

5 Analyses des modes de défaillance et de leurs effets

5.1 Approche générale

Traditionnellement, la manière de mener et de présenter l'AMDE a subi de grandes évolutions. L'analyse est généralement faite en identifiant les modes de défaillance, leurs causes respectives et leurs effets immédiats et finaux. Les résultats analytiques peuvent être présentés sur un document contenant un noyau d'informations essentielles pour l'intégralité du système et des éléments détaillés spécifiques à ce système. Ce document expose les potentialités de tomber en panne, les composants et leurs modes de défaillance à l'origine de défaillance du système, et la ou les causes d'apparition de chaque mode de défaillance individuel.

Une AMDE appliquée à des produits complexes peut demander un effort considérable. Cet effort peut parfois être réduit en considérant que la conception de certains sous-ensembles ou des parties de ceux-ci n'est pas entièrement nouvelle et en identifiant les parties de la conception du produit qui sont une répétition ou une modification d'une conception précédente. Il convient que la nouvelle AMDE construite se serve au maximum des informations des sous-ensembles existants. Il faut aussi qu'elle indique le besoin éventuel d'essais ou d'analyse complète des nouveaux dispositifs. Une fois qu'une AMDE détaillée est créée pour une conception, elle peut être mise à jour et améliorée pour les générations futures de cette conception, ce qui consiste en un effort nettement moindre que l'analyse d'origine.

Quand on se sert d'une AMDE d'une version de produit précédente, il est indispensable de s'assurer que la conception reprise est bien utilisée de la même manière et sous les mêmes contraintes que précédemment. Les nouvelles contraintes environnementales et opérationnelles peuvent exiger une révision de l'AMDE précédemment effectuée. Des contraintes environnementales et opérationnelles différentes peuvent exiger la création d'une AMDE entièrement nouvelle au vu des nouvelles conditions opérationnelles.

La procédure AMDE consiste en quatre étapes principales:

a) établissement des règles de bases pour l'AMDE, planification et programmation pour s'assurer que le temps et l'expertise sont disponibles pour mener l'analyse,

b) réaliser l'AMDE en se servant des documents appropriés ou de tout autre moyen tel qu'un diagramme logique ou un arbre de panne,

c) résumer et établir un rapport de l'analyse incluant les conclusions et recommandations faites,

d) mettre à jour l'AMDE au fur et à mesure de la progression de l'activité de développement.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

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

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

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

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

5 Failure modes and effects analysis

5.1 General considerations

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

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

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

The FMEA procedure consists of the following four main stages:

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

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

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

d) updating the FMEA as the development activity progresses.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.2 Tâches préliminaires

5.2.1 Planification des analyses

Il convient que les actions de l'AMDE, les actions en découlant, les procédures, les liens avec les autres actions relatives à la fiabilité, les processus de gestion des actions correctives et de leur finalisation, les planning soient intégrés dans le plan global du programme.

Il convient que le plan du programme de fiabilité décrive la méthode d'AMDE à appliquer. Cette description peut être un résumé ou une référence à un document source décrivant la méthode.

Ce plan comporte les points suivants:

– une définition claire des objectifs spécifiques de l'analyse et les résultats attendus;

– le domaine d'application de la présente analyse, c'est-à-dire comment il convient que l'AMDE se concentre sur certains éléments de conception. Il convient que le domaine d'application reflète la maturité de la conception et les éléments de celle-ci qui peuvent présenter des risques car ils accomplissent une fonction critique ou parce que la technologie est nouvelle;

– la description de comment la présente analyse soutient la sûreté de fonctionnement de l'ensemble du projet;

– l'identification des mesures prises pour le contrôle des révisions de l'AMDE et de la documentation s'y rapportant. Il convient que le contrôle de la révision de la documentation AMDE et des méthodes d'archive soit spécifié;

– la participation d'experts de conception dans l'analyse de façon à ce qu'ils soient disponibles en cas de besoin;

– les dates-clés de la programmation du projet clairement indiquées pour assurer le délai d'exécution de l'analyse;

– la manière de clore toutes les actions identifiées dans le processus d'atténuation des modes de défaillance identifiés qui exigent d'être traités.

Il convient que le plan reflète le consensus de tous les participants et soit approuvé par la gestion du projet. La revue finale de l'AMDE complète dans la phase finale de la conception d'un produit ou de son procédé de fabrication (processus AMDE) identifie toutes les actions enregistrées pour l'atténuation des modes de défaillance posant problème et la manière de les clore.

5.2.2 Structure du système

5.2.2.1 Information sur la structure du système

Les points suivants doivent être inclus dans l'information sur la structure du système:

a) les différents éléments du système avec leurs caractéristiques, aptitudes, rôles et fonctions,

b) les liens logiques entre éléments,

c) le niveau de redondance et la nature des redondances,

d) la position et l'importance du système dans l'installation globale (si possible),

e) les entrées et sorties du système,

f) les modifications dans la structure du système pour faire varier les modes opérationnels variables.

Les données appartenant aux fonctions, les caractéristiques et aptitudes sont requises pour tous les niveaux considérés, jusqu'au plus haut, de telle sorte que l'AMDE traite correctement les modes de défaillance qui empêche une de ces fonctions.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.2 Preliminary tasks

5.2.1 Planning for the analysis

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

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

This plan should contain the following points.

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

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

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

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

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

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

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

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

5.2.2 System structure

5.2.2.1 Information on system structure

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

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

b) logical connections between elements;

c) redundancy level and nature of the redundancies;

d) position and importance of the system within the whole facility (if possible);

e) inputs and outputs of the system;

f) changes in system structure for varying operational modes.

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.2.2.2 Définir la limite du système pour l'analyse

La limite du système constitue l'interface physique et fonctionnelle entre le système et son environnement, y compris les autres systèmes avec lesquels le système analysé interagit. Il convient que la définition de la limite du système pour l'analyse corresponde à la limite telle que définie pour la conception et la maintenance. Il convient que cela s'applique à tous les niveaux d'un système. Il convient que les systèmes et/ou les composants situés hors des limites soient explicitement définis pour leur exclusion.

La conception, l'utilisation prévue, la source d'alimentation, ou les critères commerciaux risquent plus d'influencer la définition de la limite du système que les exigences optimales de l'AMDE. Cependant, quand cela est possible, il est préférable de définir les limites pour faciliter l'AMDE du système et son intégration avec les autres études dans le programme. Cela est particulièrement vrai si le système est fonctionnellement complexe avec de multiples interconnexions entre éléments dans les limites et les diverses données de sortie dépassant la limite. Dans de tels cas, il peut être avantageux de définir une limite d'étude d'un point de vue fonctionnel plutôt que matériel ou logiciel pour réduire le nombre de liens de données d'entrée ou de sortie aux autres systèmes. Cela tendrait à diminuer le nombre d'effets de défaillance du système.

Il convient de prendre soin de s'assurer que les autres systèmes ou composants en dehors des limites du système concerné ne sont pas oubliés, en établissant de façon explicite qu'ils sont exclus de l'étude en question.

5.2.2.3 Niveaux d'analyse

Il est important de déterminer le découpage en niveaux du système qui sera utilisé pour l'analyse. Par exemple, les systèmes peuvent être décomposés par fonction ou en sous-systèmes, en unités remplaçables, ou composants individuels (voir Figure 1). Les règles de base pour sélectionner le découpage des niveaux du système pour analyse dépendent des résultats souhaités et de la disponibilité de l'information de conception. Les lignes directrices suivantes sont utiles.

a) Le plus haut niveau dans le système est sélectionné à partir de la conception et des exigences des données de sortie indiquées.

b) Le plus bas niveau dans le système auquel l'analyse est effective est celui pour lequel l'information est disponible pour établir la définition et la description des fonctions. La sélection du niveau de système approprié est influencée par l'expérience précédente. Des analyses moins détaillées peuvent être justifiées pour un système fondé sur une conception mature, ayant une bonne fiabilité, une bonne maintenabilité et un historique de sécurité. Inversement, plus de détails et un niveau de système correspondant plus bas sont indiqués pour tout système nouvellement conçu ou un système n'ayant pas d'historique de fiabilité.

c) La maintenance spécifiée ou prévue et le niveau de réparation peuvent être un guide très utile pour déterminer les niveaux de système les plus bas.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.2.2.2 Defining system boundary for the analysis

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

The definition of the system boundary is more likely to be influenced by design, intended use, source of supply, or commercial criteria rather than the optimum requirements of the FMEA. However, where it is possible to define the boundaries to facilitate the system FMEA and its integration with other related studies in the programme, such action is preferable. This is especially so if the system is functionally complex with multiple interconnections between items within the boundary and multiple outputs crossing the boundary. In such cases it could be advantageous to define a study boundary from functional rather than hardware and software point of view to limit the number of input and output links to other systems. This would tend to reduce the number of system failure effects.

Care should be taken to ensure that other systems or components outside the boundaries of the subject system are not forgotten, by explicitly stating that they are excluded from the particular study.

5.2.2.3 Levels of analysis

It is important to determine the indenture level in the system that will be used for the analysis. For example, systems can be broken down by function or into subsystems, replaceable units, or individual components (see Figure 1). Ground rules for selecting the system indenture levels for analysis depend on the results desired and the availability of design information. The following guidelines are useful.

a) The highest level within the system is selected from the design concept and specified output requirements.

b) The lowest level within the system at which the analysis is effective is that level for which information is available to establish definition and description of functions. The selection of the appropriate system level is influenced by previous experience. Less detailed analysis may be justified for a system based on a mature design, with a good reliability, maintainability and safety record. Conversely, greater details and a correspondingly lower system level are indicated for any newly designed system or a system with unknown reliability history.

c) The specified or intended maintenance and repair level may be a valuable guide in determining lower system levels.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

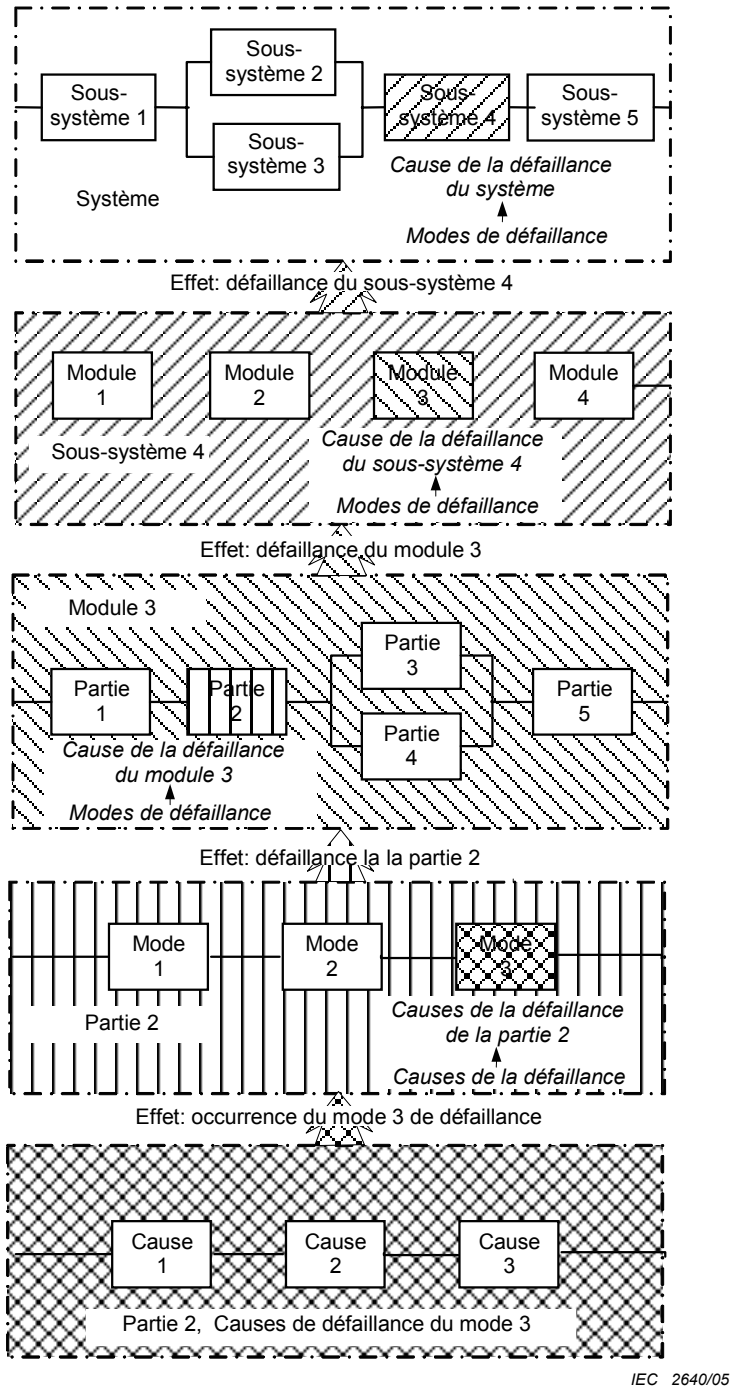

Figure 1 – Relation entre les modes de défaillance et les effets de défaillance dans la hiérarchie d'un système

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

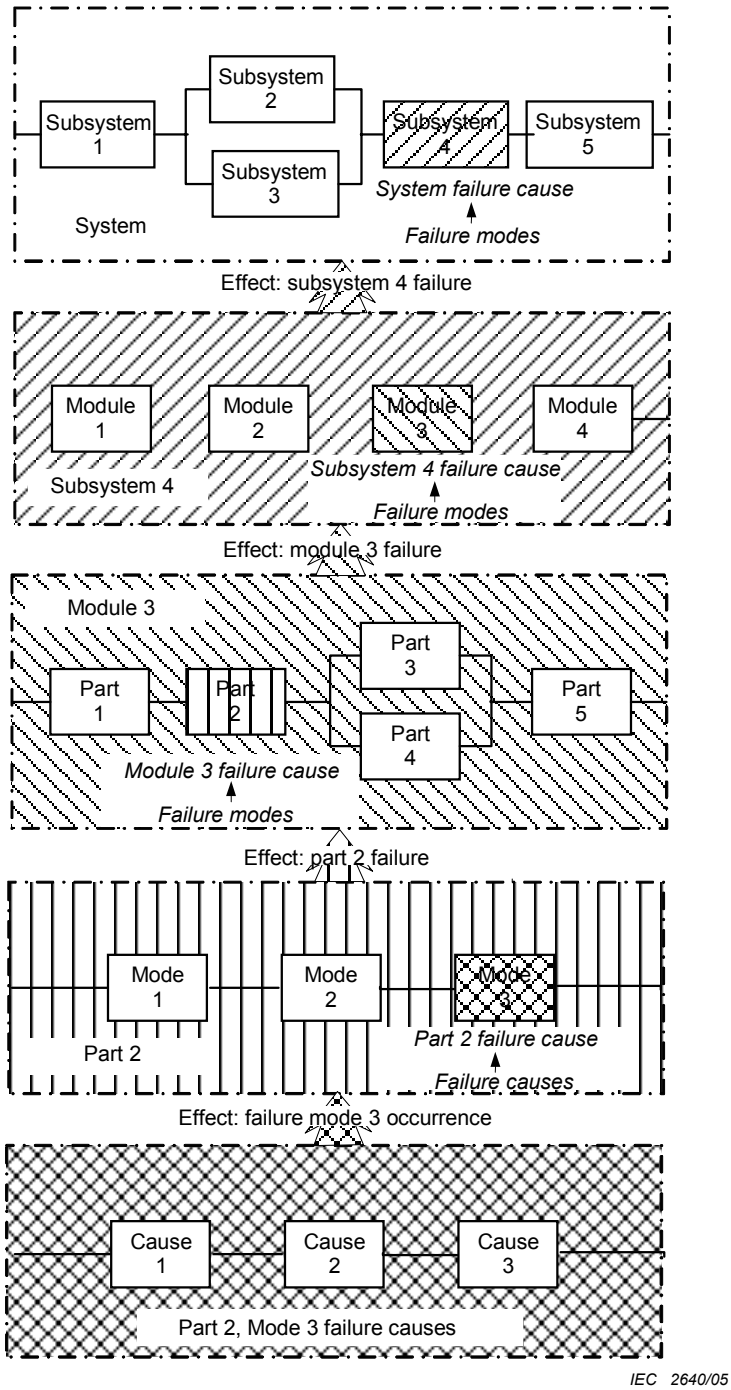

Figure 1 – Relationship between failure modes and failure effects in a system hierarchy

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

Dans l'AMDE, les définitions des modes de défaillance, causes de défaillance et effets de défaillance dépendent du niveau d'analyse et des critères de défaillance du système. Au fur et à mesure de la progression de l'analyse, les effets de défaillance identifiés au plus bas niveau peuvent devenir des modes de défaillance au niveau le plus haut. Les modes de défaillance du niveau le plus bas peuvent devenir les causes de défaillance au niveau le plus haut et ainsi de suite.

Quand un système est découpé en éléments, des effets d'une ou de plusieurs causes de mode de défaillance constituent un mode de défaillance qui devient la cause de l'effet au niveau supérieur, une défaillance de pièce. La défaillance d'une pièce est ainsi la cause de la défaillance d'un module (effet), qui est elle-même une cause de défaillance d'un sous-système. L'effet d'une cause d'un niveau du système devient donc une cause d'un autre effet à un niveau plus élevé. Le raisonnement ci-dessus est illustré à la Figure 1.

5.2.2.4 Représentation de la structure d'un système

Des représentations symboliques de la structure et du fonctionnement du système, en particulier les diagrammes, sont très utiles dans l'analyse.

Il convient de créer des diagrammes simples mettant en lumière toutes les fonctions essentielles du système. Dans le diagramme, les blocs sont reliés par des lignes qui représentent les données d'entrée et de sortie pour chaque fonction. Généralement, il est nécessaire que la nature de chaque fonction et de chaque entrée soit décrite avec précision. Plusieurs diagrammes peuvent être nécessaires pour couvrir différentes phases du fonctionnement du système.

Au cours de la progression de la conception du système, un bloc-diagramme des composants peut être créé avec des blocs représentant les composants ou parties réels. Avec cette connaissance en plus, une identification plus précise des modes et causes de défaillance potentielle devient possible.

Il convient que les diagrammes montrent toutes séries et relations redondantes parmi les éléments et les interdépendances fonctionnelles. Cela permet de traquer les défaillances fonctionnelles du système. On peut avoir besoin de plus d'un diagramme pour exposer les modes alternatifs de fonctionnement du système. Des diagrammes séparés peuvent être nécessaires pour chaque mode opérationnel. Il convient qu'au minimum le diagramme contienne

a) la décomposition du système en principaux sous-systèmes y compris les relations fonctionnelles,
b) toutes les entrées et sorties étiquetées et les numéros d'identification par lesquels chaque sous-système est invariablement référencé,
c) toutes les redondances, chemins de signaux alternatifs et autres caractéristiques d'ingénierie qui protègent des défaillances du système.

5.2.2.5 Initiation du système, fonctionnement, contrôle et maintenance

Il convient que l'état des différentes conditions de fonctionnement du système soit spécifié, de même que les modifications dans la configuration ou la position du système et de ses composants durant les diverses phases de fonctionnement. Il convient que les performances minimales demandées au système soient définies de façon à ce que les critères de réussite et/ou d'échec soient clairement compris. Il convient que les exigences spécifiques telles que la disponibilité ou la sécurité soient considérées en terme de niveaux minimums spécifiés à atteindre et niveaux maximums de dommages à accepter. Une connaissance précise des éléments suivants est nécessaire:

a) la durée de chaque fonction que le système peut être amené à remplir,
b) la durée entre intermédiaire entre chaque essai périodique,

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

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

5.2.2.4 Representation of system structure

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

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

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

The diagrams should display any series and redundant relationships among the elements and the functional interdependencies between them. This allows the functional failures to be tracked through the system. More than one diagram may be needed to display the alternative modes of system operation. Separate diagrams may be required for each operational mode. As a minimum, the block diagram should contain the following:

a) breakdown of the system into major subsystems including functional relationships;

b) all appropriately labelled inputs and outputs and identification numbers by which each subsystem is consistently referenced;

c) all redundancies, alternative signal paths and other engineering features which provide protection against system failures.

5.2.2.5 System initiation, operation, control and maintenance

The status of the different operating conditions of the system should be specified, as well as the changes in the configuration or the position of the system and its components during the different operational phases. The minimum performances demanded of the system should be defined such that success and/or failure criteria can be clearly understood. Such specific requirements as availability or safety should be considered in terms of specified minimum levels of performance to be achieved and maximum levels of damage or harm to be accepted. It is necessary to have an accurate knowledge of

a) the duration of each function the system may be called upon to perform;

b) the time interval between periodic tests;

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

c) le temps disponible pour une action corrective avant de sérieuses conséquences sur le système,

d) le dispositif global, l'environnement et/ou le personnel, y compris les interfaces et interactions avec les opérateurs,

e) les procédures de fonctionnement au démarrage du système, arrêt et autres transitions opérationnelles,

f) le contrôle pendant les phases opérationnelles,

g) la maintenance préventive et/ou corrective,

h) les procédures pour les essais de routine, si utilisés.

Il est établi qu'une des utilités de l'AMDE est l'assistance dans le développement de la stratégie de maintenance. Cependant, si cette dernière a été prédéterminée, il convient que l'information relative aux moyens de maintenance, aux équipements et pièces de rechange soit connue tant pour la maintenance préventive que aussi bien que corrective.

5.2.2.6 Environnement du système

Il convient que les conditions d'environnement du système soient spécifiées, y compris les conditions ambiantes et celles créées par d'autres systèmes voisins. Il convient que le système soit tracé en fonction de ses relations, dépendances, ou interconnexions avec les systèmes auxiliaires ou autres et les interfaces humaines.

Au stade de conception, ces faits ne sont généralement pas tous connus et par conséquent les approximations et hypothèses seront nécessaires. Au fur et à mesure de l'avancement du projet, les données devront être augmentées et l'AMDE modifiée pour permettre de nouvelles informations, hypothèses ou approximations. L'AMDE sera souvent utile pour définir les conditions requises.

5.2.3 Détermination du mode de défaillance

Le bon fonctionnement réussi d'un système est soumis à l'aptitude à la fonction de certains éléments critiques du système. La clé pour l'évaluation de l'aptitude à la fonction du système est l'identification de ces éléments critiques. Les procédures pour l'identification des modes de défaillance, leurs causes et effets peuvent effectivement être améliorées par la préparation d'une liste des modes de défaillance anticipés à la lumière de ce qui suit:

a) l'utilisation du système,

b) les éléments du système concerné,

c) le mode de fonctionnement,

d) les spécifications opérationnelles pertinentes,

e) les contraintes de temps,

f) les contraintes d'environnement,

g) les contraintes fonctionnelles.

Un exemple des modes de défaillance généraux est donné dans le Tableau 1.

Tableau 1 – Exemple d'un ensemble de modes de défaillance généraux

1	Défaillance en fonctionnement
2	Défaillance de fonctionnement à un moment prescrit
3	Défaillance d'arrêt du fonctionnement à un moment prescrit
4	Fonctionnement prématuré

NOTE Il ne s'agit que d'un exemple. Des listes différentes peuvent être requises pour des types de systèmes différents.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

c) the time available for corrective action before serious consequences occur to the system;

d) the entire facility, the environment and/or the personnel, including interfaces and interactions with operators;

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

f) control during the operational phases;

g) preventive and/or corrective maintenance;

h) procedures for routine testing, if employed.

It has been stated that one of the uses of FMEA is to assist in the development of the maintenance strategy. However, if the latter has been pre-determined, information on maintenance facilities, equipment and spares should be known for both preventive and corrective maintenance.

5.2.2.6 System environment

The environmental conditions of the system should be specified, including ambient conditions and those created by other systems in the vicinity. The system should be delineated with respect to its relationships, dependencies, or interconnections with auxiliary or other systems and human interfaces.

At the design stage these facts are usually not all known and therefore approximations and assumptions will be needed. As the project progresses, the data will have to be augmented and the FMEA modified to allow for new information or changed assumptions or approximations. Often the FMEA will be helpful in defining the required conditions.

5.2.3 Failure mode determination

Successful operation of a given system is subject to the performance of certain critical system elements. The key to evaluation of system performance is the identification of those critical elements. The procedures for identifying failure modes, their causes and effects can be effectively enhanced by the preparation of a list of failure modes anticipated in the light of the following:

a) the use of the system;

b) the particular system element involved;

c) the mode of operation;

d) the pertinent operational specifications;

e) the time constraints;

f) the environmental stresses;

g) the operational stresses.

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

Table 1 – Example of a set of general failure modes

1	Failure during operation
2	Failure to operate at a prescribed time
3	Failure to cease operation at a prescribed time
4	Premature operation

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Virtuellement, chaque type de mode de défaillance peut être classé dans une ou plusieurs de ces catégories. Cependant, ces catégories générales de modes de défaillance couvrent un domaine trop large pour une analyse définitive; en conséquence, la liste nécessite d'être élargie pour rendre la catégorie plus spécifique. Tous les modes de défaillance potentiels peuvent être identifiés et décrits quand ils sont utilisés en conjonction avec les spécifications d'aptitude régissant les entrées et sorties sur le diagramme de fiabilité. Il convient de noter qu'un mode de défaillance donné peut avoir plusieurs causes.

Il est important que l'évaluation de tous les dispositifs dans les limites du système au plus bas niveau en proportion avec les objectifs de l'analyse soit entreprise pour identifier les modes de défaillance potentiels. Des investigations pour déterminer les causes de défaillance possibles et également les effets des défaillances sur les sous-systèmes et les fonctions du système peuvent alors être entreprises.

Il convient que les fournisseurs de dispositifs identifient les modes de défaillance potentiels de leurs produits. Pour les données sur les modes typiques de défaillance de fonction, une aide peut être trouvée dans les domaines suivants:

a) pour de nouveaux dispositifs, on peut se référer aux autres dispositifs avec une structure et une fonction similaires et aux résultats d'essais effectués sur ces dispositifs aux niveaux de contraintes appropriés;

b) pour les nouveaux dispositifs, l'analyse de l'objectif de la conception et l'analyse fonctionnelle détaillée conduisent aux modes de défaillance potentiels et à leurs causes. Cette méthode est préférée à celle en a) parce que les contraintes et le fonctionnement lui-même peuvent être différents pour des dispositifs similaires. Un exemple de cette situation peut être l'utilisation d'un processeur de signal différent dans une autre conception similaire;

c) pour les dispositifs utilisés, les enregistrements «en service» et les données de défaillance peuvent être consultés;

d) les modes de défaillance potentiels peuvent être déduits des paramètres fonctionnels et physiques typiques du fonctionnement du dispositif.

Il est important de ne pas omettre des modes de défaillance de dispositif par manque de données, et d'améliorer les estimations initiales par des résultats d'essai et la progression de la conception. Il convient que l'AMDE enregistre l'état de telles estimations.

L'identification des modes de défaillance et, si nécessaire, la détermination des actions de conception correctives, d'assurance qualité préventives ou de maintenance préventives est primordiale. Il est plus important d'identifier et, si possible, d'atténuer les modes de défaillance par la conception, que de connaître leur fréquence d'apparition. Quand il est difficile de déterminer les priorités, une analyse de criticité peut être requise.

5.2.4 Causes de défaillance

Il convient d'identifier et de décrire les causes les plus probables pour chaque mode de défaillance potentiel. Puisqu'un mode de défaillance peut avoir plusieurs causes, les causes indépendantes les plus probables pour chaque mode de défaillance doivent être identifiées et décrites.

L'identification et la description des causes de défaillance ne sont pas toujours nécessaires pour tous les modes de défaillance identifiés dans l'analyse. Il convient de baser l'identification et la description des causes de défaillance, de même que les suggestions pour leur atténuation sur les effets des défaillances et leur gravité. Plus sévères sont les effets des modes de défaillance, plus précises doivent être les causes de défaillances identifiées et décrites. Sinon, l'analyste risque de prodiguer des efforts non nécessaires à l'identification des causes de défaillance de tels modes de défaillance qui n'ont pas ou très peu d'effet sur la fonctionnalité du système.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Virtually every type of failure mode can be classified into one or more of these categories. However, these general failure mode categories are too broad in scope for definitive analysis; consequently, the list needs to be expanded to make the categories more specific. When used in conjunction with performance specifications governing the inputs and outputs on the reliability block diagram, all potential failure modes can be identified and described. It should be noted that a given failure mode may have several causes.

It is important that evaluation of all items within the system boundaries at the lowest level commensurately with the objectives of the analysis is undertaken to identify all potential failure modes. Investigation to determine possible failure causes and also failure effects on subsystem and system function can then be undertaken.

Item suppliers should identify the potential item failure modes within their products. To assist this function typical failure mode data can be sought from the following areas:

a) for new items, reference can be made to other items with similar function and structure and to the results of tests performed on them under appropriate stress levels;

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

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

d) potential failure modes can be deduced from functional and physical parameters typical of the operation of the item.

It is important that item failure modes are not omitted for lack of data and that initial estimates are improved by test results and design progression. The FMEA should record the status of such estimates.

The identification of failure modes and, where necessary, the determination of remedial design actions, preventative quality assurance actions or preventative maintenance actions is of prime importance. It is more important to identify and, if possible, to mitigate the failure modes effects by design measures, than to know their probability of occurrence. When it is difficult to assign priorities, criticality analysis may be required.

5.2.4 Failure causes

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Les causes de défaillance peuvent être déterminées par l'analyse des défaillances en exploitation ou lors des essais. Quand la conception est nouvelle et sans précédent, les causes de défaillance peuvent être établies en obtenant l'opinion d'experts.

Lorsque les causes de chaque mode de défaillance sont identifiées, l'action préconisée sera évaluée sur la base de l'estimation de la probabilité d'apparition et de la sévérité de leurs effets.

5.2.5 Effets de défaillance

5.2.5.1 Définition des effets de défaillance

Un effet d'une défaillance est la conséquence d'un mode de défaillance en termes de fonctionnement, de fonction ou d'état d'un système (voir définition 3.7). Un effet d'une défaillance peut être provoqué par un ou plusieurs modes de défaillance d'un ou plusieurs dispositifs.

Il est nécessaire que les conséquences de chaque mode de défaillance sur le fonctionnement d'élément du système, fonction, ou état, soient identifiées, évaluées et enregistrées. Il convient de prendre en considération les activités de maintenance et les objectifs du système. Un effet de défaillance peut également influencer le niveau supérieur suivant et en dernier lieu le plus haut niveau analysé. Par conséquent, il convient d'évaluer à chaque niveau l'effet des défaillances sur le niveau supérieur.

5.2.5.2 Effets de défaillance locaux

L'expression «effets locaux» fait référence aux effets du mode de défaillance sur l'élément du système en considération. Il convient de décrire les conséquences de chaque défaillance possible sur la sortie du dispositif. Le but de l'identification des effets locaux est de fournir une base de jugement pour évaluer les alternatives existantes ou échanger sur les actions correctives recommandées. Dans certains cas, il peut ne pas y avoir d'effet local au-delà du mode de défaillance lui-même.

5.2.5.3 Effets de défaillance au niveau du système

En identifiant les effets finaux, l'impact d'une défaillance possible sur le plus haut niveau du système est défini et évalué par l'analyse de tous les niveaux intermédiaires. L'effet final décrit peut être le résultat de multiples défaillances. Par exemple, la défaillance d'un dispositif de sécurité résulte en un effet final catastrophique seulement dans le cas où à la fois le dispositif de sécurité tombe en panne et la fonction première pour laquelle le dispositif est conçu sort des limites autorisées. Il convient d'indiquer ces effets finaux résultant de défaillances multiples sur les documents de travail.

5.2.6 Méthodes de détection

Il convient que l'analyste détermine pour chaque mode de défaillance la façon dont la défaillance est détectée et les moyens par lesquels l'utilisateur ou la personne responsable de la maintenance se rend compte de la défaillance. La détection de la défaillance peut être réalisée par un dispositif automatique de la conception (essai intégré), établissement d'une procédure de vérification spéciale avant le fonctionnement du système ou par inspection pendant les activités de maintenance. Il peut être mis en œuvre au démarrage du système ou en continuité durant le fonctionnement ou à des intervalles prescrits. Dans tous les cas, il convient que l'annonce et la détection de la défaillance éliminent les conditions de fonctionnement dangereux.

Il convient d'analyser et de lister les modes de défaillance autres que celui considéré qui donnent lieu à une manifestation identique. Il convient de prendre en considération le besoin d'une détection spécifique des défaillances d'éléments redondants pendant le fonctionnement.

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

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

5.2.5 Failure effects

5.2.5.1 Failure effects definition

A failure effect is the consequence of a failure mode in terms of the operation, function or status of a system (see definition 3.4). A failure effect may be caused by one or more failure modes of one or more items.

The consequences of each failure mode on system element operation, function, or status need to be identified, evaluated and recorded. Maintenance activities and system objectives should also be considered whenever pertinent. A failure effect may also influence the next level up and ultimately the highest level under analysis. Therefore, at each level, the effect of failures on the level above should be evaluated.

5.2.5.2 Local failure effects

The expression “local effects” refers to the effects of the failure mode on the system element under consideration. The consequences of each possible failure on the output of the item should be described. The purpose of identifying the local effects is to provide a basis for judgement when evaluating existing alternative provisions or devising recommended corrective actions. In certain instances, there may not be a local effect beyond the failure mode itself.

5.2.5.3 Failure effects at the system level

When identifying end effects, the impact of a possible failure on the highest system level is defined and evaluated by the analysis of all intermediate levels. The end effect described may be the result of multiple failures. (For example, failure of a safety device results in a catastrophic end effect only in the event that both the safety device fails and the prime function for which the safety device is designed goes beyond allowed limits.) These end effects resulting from a multiple failure should be indicated on the worksheets.

5.2.6 Detection methods

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

Failure modes other than the one being considered which give rise to an identical manifestation should be analysed and listed. The need for separate detection of failure of redundant elements during operation should be considered.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Pour une AMDE portant sur une conception, la détection considère comment, quand et où une déficience de conception sera identifiée (par revue, par analyse, par simulation, par essais, etc.). Pour une AMDE portant sur un procédé, la détection considère comment, quand et où une déficience peut être identifiée et avec quelle probabilité, par exemple par un opérateur, par un contrôle statistique de procédé, par une procédure de contrôle qualité ou par les dernières étapes du procédé.

5.2.7 Dispositions compensant une défaillance

L'identification de toutes caractéristiques de conception à un niveau donné du système ou d'autres dispositions que la capacité à prévenir ou réduire l'effet du mode de défaillance est d'une extrême importance. Ainsi, il convient que l'AMDE identifie clairement le comportement d'une telle caractéristique en présence de ce mode de défaillance. D'autres dispositions contre la défaillance exigeant d'être enregistrées dans l'AMDE comprennent

a) les dispositifs redondants qui permettent la continuité du fonctionnement si un ou plusieurs éléments tombent en panne,

b) les moyens alternatifs de fonctionnement,

c) la surveillance et les dispositifs d'alarme,

d) tout autre moyen permettant un fonctionnement effectif ou limitant les dommages.

Lors d'un processus de conception, les éléments fonctionnels (matériels et logiciels) d'un dispositif peuvent être réarrangés ou reconfigurés de façon répétitive, ou leur capacité peut être modifiée. Il convient qu'à chaque étape la pertinence des modes de défaillance identifiés et l'AMDE soient mis à jour ou effectuées à nouveau.

5.2.8 Classification de la sévérité

La sévérité est une évaluation de l'impact de l'effet du mode de défaillance sur le fonctionnement du dispositif. La classification des effets de sévérité est hautement dépendante de l'application AMDE et est développée en considération de plusieurs facteurs:

– la nature du système en relation avec les effets possibles sur les utilisateurs ou l'environnement découlant d'une défaillance,

– l'aptitude à la fonction du système ou du procédé,

– toute exigence contractuelle imposée par le client,

– exigences de sécurité industrielles ou gouvernementales,

– exigences induites par une garantie.

Le Tableau 2 illustre un exemple de classification de sévérité qualitative pour un produit pour un des types d'AMDE.

Tableau 2 – Exemple illustré de classification de la sévérité pour effets finaux

Classe	Niveau de sévérité	Conséquence sur les personnes ou l'environnement
IV	Catastrophique	Un mode de défaillance qui peut potentiellement provoquer la défaillance des fonctions primaires du système et par conséquent entraîner de sérieux dommages au système et à son environnement et/ou des blessures humaines.
III	Critique	Un mode de défaillance pouvant potentiellement provoquer la défaillance des fonctions primaires du système et par conséquent entraîner des dommages considérables au système et à son environnement, mais ne constitue pas une menace sérieuse de blessures ou menace pour la vie.
II	Marginal	Un mode de défaillance pouvant potentiellement dégrader l'aptitude du système sans dommage appréciable au système ou menace de blessure fatale.
I	Insignifiant	Un mode de défaillance pouvant potentiellement dégrader les fonctions du système mais ne provoquant pas de dommage au système et ne constituant pas une menace de blessures ou une menace pour la vie.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

5.2.7 Failure compensating provisions

The identification of any design features at a given system level or other provisions that have the ability to prevent or reduce the effect of the failure mode is of an extreme importance. Thus the FMEA should clearly show the true behaviour of such a feature in the presence of that failure mode. Other provisions against failure that need to be recorded in the FMEA include the following:

a) redundant items that allow continued operation if one or more elements fail;

b) alternative means of operation;

c) monitoring or alarm devices;

d) any other means of permitting effective operation or limiting damage.

During a design process, the functional elements (hardware and software) of an item may be repeatedly rearranged or reconfigured or its capability may be changed. At each stage, the relevancy of the identified failure modes and the FMEA should be updated or even repeated.

5.2.8 Severity classification

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

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

– the functional performance of the system or process;

– any contractual requirements imposed by the customer;

– government or industry safety requirements;

– requirements implied by a warranty.

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

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.2.9 Fréquence ou probabilité d'apparition

Il convient de déterminer la fréquence ou la probabilité d'apparition de chaque mode de défaillance pour évaluer de façon adéquate l'effet ou la criticité du mode de défaillance.

Pour déterminer la probabilité d'apparition du mode de défaillance au-delà des informations publiées sur le taux de défaillance, il est très important de considérer le profile opérationnel (contraintes environnementales, mécaniques, et/ou électriques appliquées) de chaque composant contribuant à la probabilité d'apparition. C'est parce que dans la plupart des cas les taux de défaillance des composants, et, en conséquence, le taux de défaillance relatif au mode de défaillance considéré, croît avec la contrainte appliquée selon la loi en puissance ou exponentiellement. La probabilité d'apparition des modes de défaillance pour une conception peut être estimée à partir

– des données d'essai de durée de vie du composant,
– des taux de défaillances disponibles dans les bases de données,
– des données sur les défaillances en exploitation,
– des données de défaillance pour des dispositifs similaires ou pour la classe du composant.

Une fois la probabilité d'apparition estimée, l'AMDE doit indiquer la période de temps pour laquelle l'estimation est faite. C'est généralement la période de garantie, ou la durée de vie prédéterminée pour ce dispositif ou produit.

L'application de la fréquence d'apparition sera expliquée plus loin dans la description de l'analyse de criticité.

5.2.10 Procédure d'analyse

Le diagramme donné à la Figure 2 montre comment l'analyse est menée.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.2.9 Frequency or probability of occurrence

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

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

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

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

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

5.2.10 Analysis procedure

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

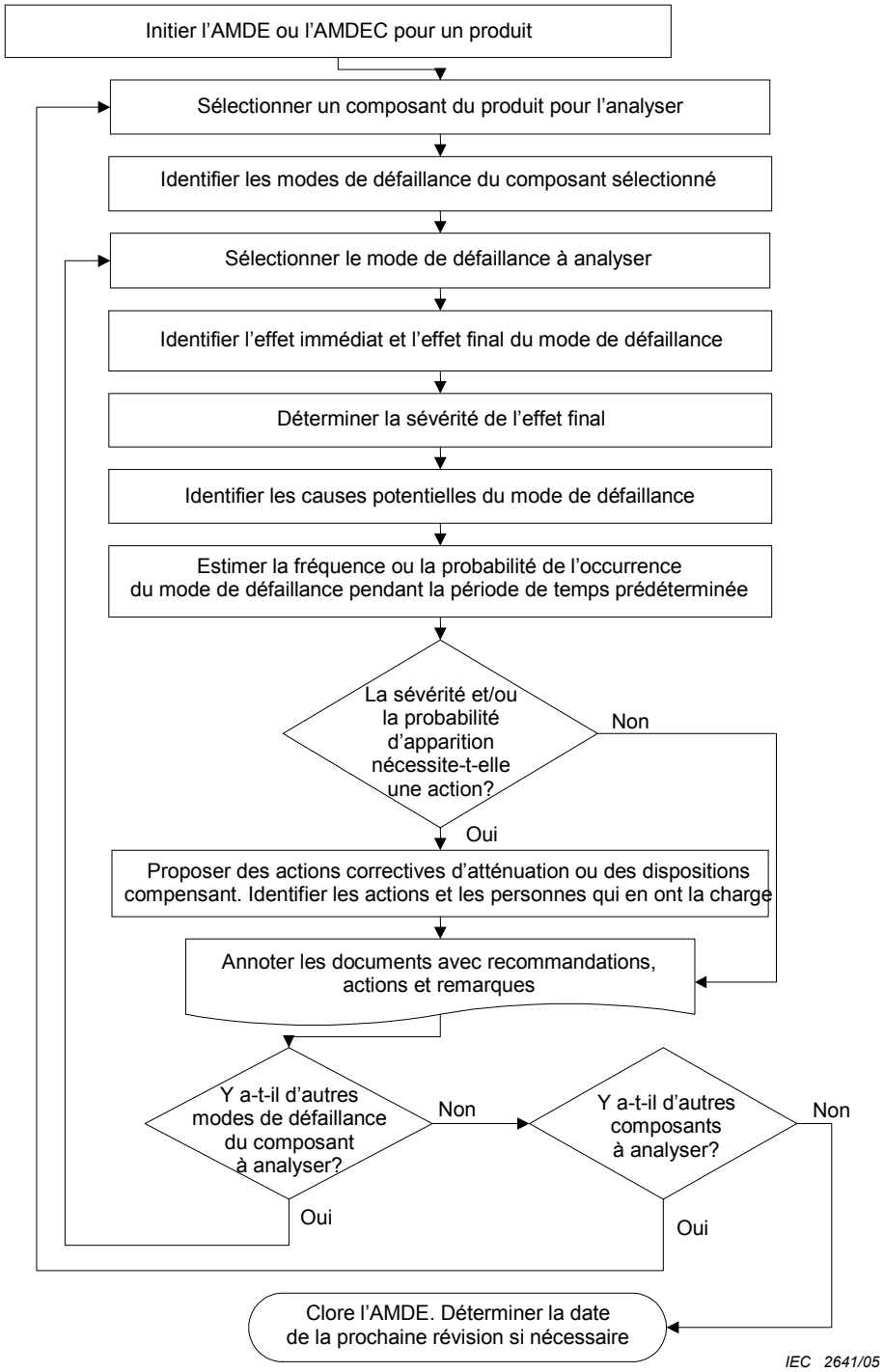

Figure 2 – Schéma fonctionnel d'analyse

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

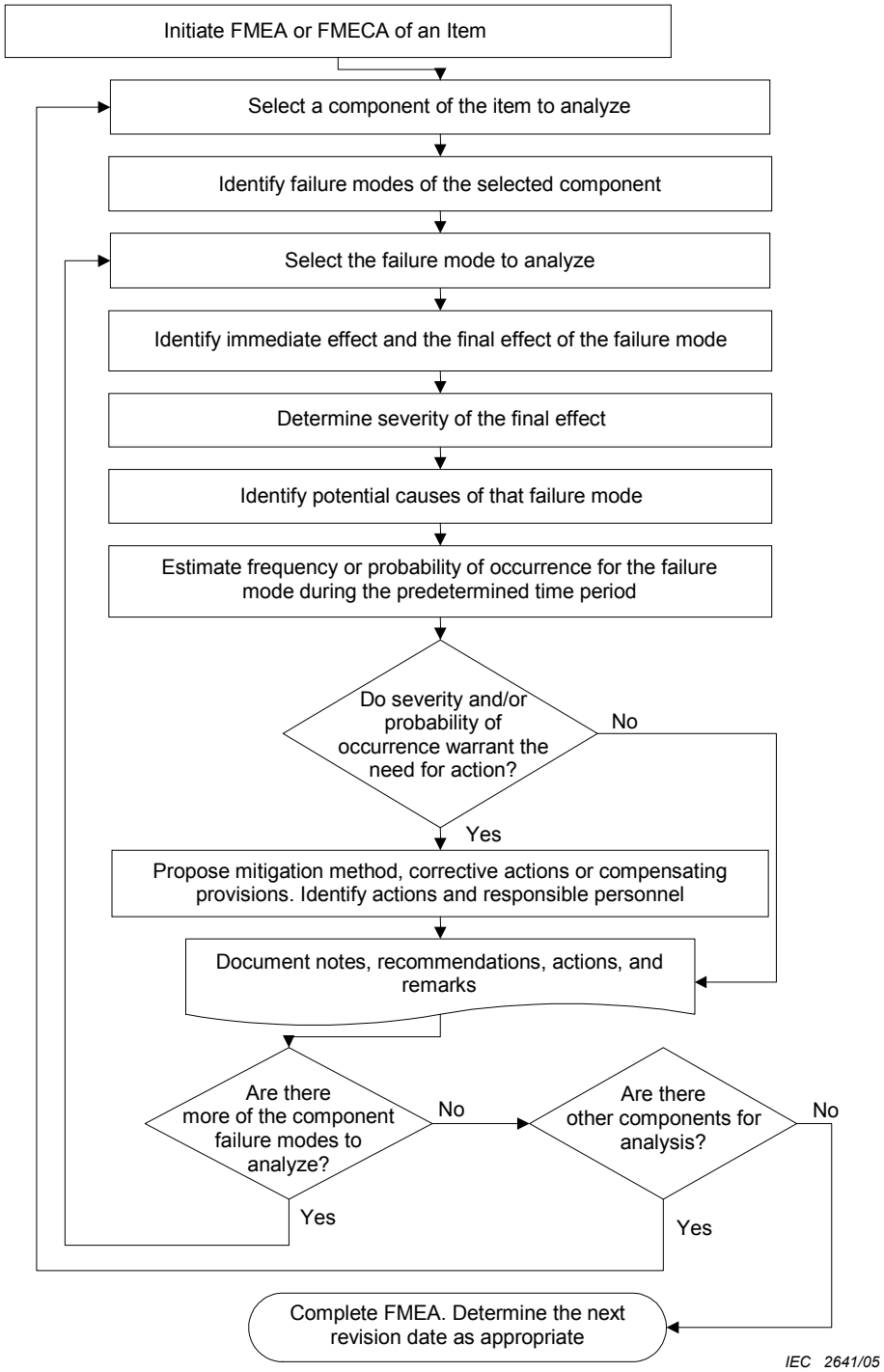

Figure 2 – Analysis flowchart

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

5.3 Analyse des modes de défaillance, de leurs effets et analyses de criticité (AMDEC)

5.3.1 But de l'analyse

Le symbole C ajouté à l'AMDE indique que l'analyse du mode de défaillance inclut également l'analyse de criticité. La détermination de la criticité implique l'ajout de mesures qualitatives de l'amplitude de l'effet du mode de défaillance. La criticité a une multitude de définitions et de mesures, dont la plupart ont pour hypothèse une signification commune: impact ou importance d'un mode de défaillance qu'il convient de traiter et de réduire. Certaines de ces mesures sont expliquées en 5.3.2 et 5.3.4. La finalité d'une analyse de criticité est de quantifier l'amplitude relative de chaque effet de défaillance en tant qu'aide à la décision, de telle sorte qu'avec une combinaison de la criticité et de la sévérité, une priorité pour l'action de réduire ou minimiser l'effet de certaines défaillances puisse être établie.

5.3.2 Risque, R, et nombre prioritaire de risque (NPR)

L'une des méthodes de détermination quantitative de la criticité est le Nombre Prioritaire de Risque (NPR). Ici le risque est évalué par une mesure subjective de la sévérité de l'effet et une estimation de la probabilité attendue de son apparition pour une période de temps prédéterminée et supposée pour l'analyse. Dans certains cas, ces mesures ne sont pas disponibles. Alors, il devient nécessaire de revenir à une forme plus simple d'une AMDE non numérique.

Dans certains types d'analyse, la mesure d'un risque potentiel, R, dans une AMDEC se résume en une formule ci-dessous:

$$R = S \times P$$

où

S est un nombre sans dimension pour la sévérité, c'est-à-dire une estimation de la force des effets de la défaillance sur le système ou l'utilisateur;

P est également un nombre sans dimension qui indique la probabilité d'apparition. Quand il est inférieur à 0,2, on peut lui substituer un nombre de criticité C qui est utilisé dans certaines méthodes quantitatives d'AMDE, expliqué en 5.3.4, c'est-à-dire une estimation de la probabilité que l'effet de défaillance survienne.

Certaines applications AMDE ou AMDEC distinguent en plus le niveau de détection de défaillance au niveau du système. Dans ces applications une catégorie supplémentaire pour la détection de défaillance, D (également un nombre sans dimension), est utilisée pour former un ordre de priorité du risque, NPR :

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

où

O désigne la fréquence d'apparition d'un mode de défaillance pour une période de temps prédéterminée ou établie – même s'il peut être défini comme un classement plutôt que comme l'actuelle probabilité d'apparition;

D signifie détection, c'est-à-dire une estimation de la chance d'identifier et d'éliminer la défaillance avant que le système ou le client n'en soit affecté. Ce nombre est classé dans le sens inverse de la sévérité ou des nombres d'apparition: plus le nombre de détection est élevé, moins la détection est probable. La probabilité la plus basse de détection mène conséquemment à un NPR plus élevé, et une priorité plus haute pour la résolution du mode de défaillance.

L'ordre de priorité du risque peut alors être utilisé pour donner la priorité en considérant l'atténuation des modes de défaillance. En plus de la magnitude de l'ordre de priorité du risque, la décision pour l'atténuation est initialement influencée par la sévérité du mode de défaillance, signifiant que s'il y a des modes de défaillance avec des NPR similaires ou identiques, les modes de défaillance qui sont couverts en premier sont ceux ayant les nombres les plus élevés de sévérité.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

5.3.1 Purpose of analysis

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

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

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

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

$$R = S \times P$$

where

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

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

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

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

where

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

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

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Ces relations peuvent être évaluées numériquement sur une échelle discrète ou continue (un nombre fini de valeurs définies).

Les modes de défaillance sont classés suivant leur NPR et une priorité haute est assignée à un NPR élevé. Dans certains applications, les effets avec un NPR dépassant un seuil défini ne sont pas acceptables, alors que dans d'autres applications l'importance est donnée aux numéros de sévérité élevés, sans se préoccuper de la valeur NPR.

Certains types d'AMDEC assignent des échelles différentes pour les valeurs de S, O et D. certaines de ces échelles vont de 1 à 4 ou 5, d'autres utilisées largement dans l'industrie automobile pour l'analyse de conception et de procédé de production, connues sous les appellations DAMDEC et PAMDEC, utilisent pour les trois attributs des échelles de 1 à 10.

5.3.3 Relations entre l'AMDEC et l'analyse de risque

La criticité combinée à la sévérité est une mesure de risque, qui diffère des mesures de risque habituellement acceptées uniquement dans de moins rigoureuses et par conséquent moins coûteuses approches de son évaluation. La différence se voit non seulement dans la façon de prédire la sévérité d'un effet de défaillance mais aussi par le fait qu'une interaction beaucoup moins complexe entre les facteurs peut être modélisée dans la procédure typique du bas vers le haut appliquée dans une AMDE. Une AMDE résulte généralement en un classement relatif des contributions au risque complet, alors qu'une analyse de risque pour les systèmes à haut risque aboutit généralement à l'acceptabilité du risque. Cependant pour les systèmes à haut risque et complexité basse, l'AMDE peut être une méthode appropriée et peu coûteuse. Lorsque durant l'AMDE la probabilité d'effets à haut risque est reconnue, il est conseillé d'utiliser une analyse de probabilité de risque (APR) de préférence à l'AMDE.

Il convient alors de ne pas utiliser une AMDEC comme base unique pour juger si oui ou non le risque d'un effet particulier d'un système à haut risque ou haute complexité est suffisamment faible pour être acceptable, même si l'estimation de la fréquence et de la sévérité est basée sur des données fiables. Cela serait la tâche d'une analyse de probabilité de risque, où plus de paramètres d'influence (et leurs interactions) peuvent être pris en compte, par exemple temps d'exposition, probabilité d'éviter, latence des défaillances, mécanismes de détection de panne.

En utilisant les effets de défaillances identifiés par l'AMDE, chaque effet est alloué à une classe de sévérité appropriée. Une fréquence de l'événement est calculée à partir de données de défaillances ou estimations pour la partie concernée. Multiplié par le temps de mission concerné, la fréquence donne un nombre de criticité, qui peut ensuite s'appliquer à une échelle selon sa valeur, ou, si l'échelle représente la probabilité d'apparition d'un événement, alors cette probabilité d'apparition est mesurée sur l'échelle. La classe de sévérité et criticité (ou probabilité d'apparition) considérées ensemble pour chaque effet constitue l'amplitude de l'effet. Deux approches principales d'évaluation de la criticité peuvent se distinguer: l'approche matricielle de la criticité et le concept d'ordre de priorité du risque (NPR).

5.3.4 Détermination du taux de défaillance, de la probabilité et du nombre de criticité d'un mode de défaillance

Si les taux de défaillance pour les modes de défaillance des dispositifs sont disponibles, sous des conditions environnementales et opérationnelles similaires à celles supposées pour le système étant analysé, les fréquences pour les effets peuvent être ajoutées directement à l'AMDEC. Si, comme c'est le plus souvent le cas, des taux de défaillance sont disponibles pour des dispositifs, plutôt que pour des modes de défaillance, et pour des conditions environnementales ou de fonctionnement, il est nécessaire de calculer les taux de défaillance des modes de défaillance. En général la relation suivante s'applique:

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

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

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

5.3.3 Relationship between FMECA and risk analysis

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

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

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

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

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

où

λ_i désigne le taux de défaillance pour un mode de défaillance i supposées constant;

λ_j désigne le taux de défaillance du composant j;

α_i est le ratio du mode de défaillance i, c'est-à-dire la probabilité que le dispositif ait un mode de défaillance i;

β_i est la probabilité conditionnelle de l'effet de défaillance donnée par le mode de défaillance i.

Les principaux inconvénients de cette approche sont l'hypothèse implicite d'un taux de défaillance constant et le fait que plusieurs des facteurs sont des prédictions ou seulement des suppositions. Cela s'applique spécialement aux composants du système qui ne peuvent pas avoir un taux de défaillance associé, mais seulement une probabilité de défaillance calculée pour l'application spécifique, sa durée, et des contraintes associées, comme les composants et les systèmes mécaniques.

Les conditions environnementales, de charge et de maintenance différentes de celles se rapportant aux données du taux de défaillance sont prises en compte par un facteur correcteur. Des conseils sur les valeurs appropriées pour cette modification peuvent être trouvés dans les publications traitant de données de fiabilité. Une attention particulière doit être apportée pour s'assurer que les correcteurs choisis sont corrects et applicables au système considéré et à ses conditions de fonctionnement.

Dans certaines applications telles que l'approche quantitative d'analyse de criticité, une criticité du mode de défaillance C_i (sans relation avec le terme général "criticité" qui peut avoir différentes significations) au lieu d'une fréquence du mode de défaillance λ_i est utilisée. Le nombre de criticité crée un lien entre la fréquence de la défaillance conditionnelle et la durée de fonctionnement, ce qui peut ainsi aider à obtenir une évaluation plus réaliste du risque du mode de défaillance pendant la période prédéterminée d'utilisation du produit:

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

où t_j désigne la durée de fonctionnement pendant la durée globale prédéterminée utilisée pour l'AMDEC, pour laquelle la probabilité est évaluée – temps de fonctionnement du composant actif.

Le nombre de criticité pour le composant ayant m modes de défaillance est ainsi:

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

Il faut noter que le nombre de criticité n'est pas lié au terme « criticité » lui-même. C'est juste une valeur calculée pour certains types d'AMDEC dans le contexte d'une mesure relative des conséquences d'un mode de défaillance et de sa probabilité d'apparition. Ici, le nombre de criticité est une mesure du risque et non la mesure d'une probabilité d'apparition.

Pour déterminer la probabilité P_i d'apparition d'un mode de défaillance pour un temps t_j, à partir de la criticité calculée:

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

Quand les taux de défaillance de modes de défaillance et les nombres de criticité en résultant sont faibles, on peut dire avec une approximation grossière que pour une probabilité d'apparition inférieure à 0,2 (où la criticité serait égale à 0,223), les valeurs des nombres de criticité et de probabilité de défaillance sont très comparables.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

where

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

λ_j stands for the failure rate of the component j.

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

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

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

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

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

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

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

Criticality number for the component having m failure modes is then

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

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

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

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

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Dans le cas de taux de défaillance ou de fréquences de défaillance variables, la probabilité d'apparition doit être calculée, et non la criticité, qui est fondée sur l'hypothèse d'un taux (fréquence) de défaillance constant.

5.3.4.1 Criticité matricielle

La criticité peut être présentée sous forme de matrice, comme montrée à la Figure 3. Il convient de noter qu'il n'y a pas de définition en tant que telle mais que la criticité a besoin d'être définie par l'analyste et acceptée par la gestion du programme ou du projet. Les définitions diffèrent largement entre les divers secteurs d'application.

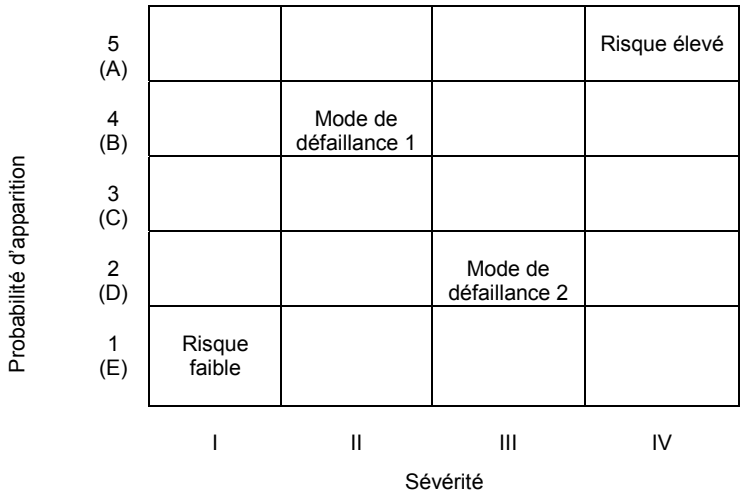

Figure 3 – Matrice de criticité

La Figure 3 implique que la sévérité augmente avec l'ordre ascendant des nombres, où le chiffre IV indique la sévérité la plus élevée (perte de vie humaine et/ou mission/opération, blessure). Cela implique que la probabilité d'apparition, sur l'axe Y est aussi représentée dans l'ordre ascendant. Si la plus haute probabilité de catégorie d'apparition n'excède pas une valeur 0,2, la probabilité d'apparition et les valeurs de criticité sont approximativement égales les unes aux autres. L'une des matrices fréquemment vues peut avoir l'échelle suivante:

– Criticité 1 ou E, improbable, probabilité d'apparition: $0 \leq P_i < 0{,}001$
– Criticité 2 ou D, éloigné, probabilité d'apparition $0{,}001 \leq P_i < 0{,}01$
– Criticité 3 ou C, occasionnelle, probabilité d'apparition: $0{,}01 \leq P_i < 0{,}1$
– Criticité 4 ou B, probable, probabilité d'apparition: $0{,}1 \leq P_i < 0{,}2$
– Criticité 5 ou A, fréquente, probabilité d'apparition: $P_i \geq 0{,}2$

La Figure 3 est présentée uniquement à titre d'exemple. D'autres méthodes peuvent présenter la criticité ou la sévérité avec des classements différents et avec diverses descriptions.

Dans l'exemple donné dans la Figure 3, le mode de défaillance 1 a une criticité plus élevée que le mode de défaillance 2, qui, lui, a une sévérité plus élevée. La décision d'affecter une priorité plus élevée pour traiter un mode de défaillance dépend de la graduation de la sévérité et des classes de fréquence et principes de classement. Alors que sur une échelle linéaire un mode de défaillance 1 (comme généralement suggéré par la matrice) aurait une criticité plus élevée (ou probabilité d'apparition) qu'un mode de défaillance 2, il peut y avoir des applications où la sévérité a une priorité absolue par rapport à la fréquence, faisant ainsi du

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

5.3.4.1 Criticality matrix

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

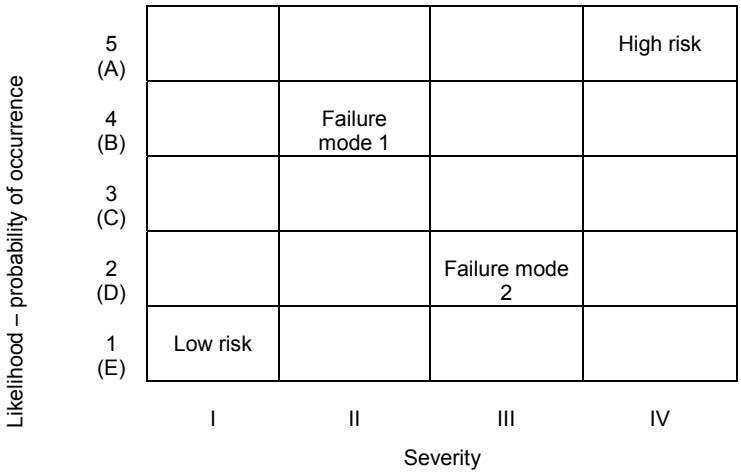

Figure 3 – Criticality matrix

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

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

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

mode de défaillance 2 le mode de défaillance le plus critique. Une autre observation évidente est que seuls les modes de défaillance reliés au même niveau d'intervention du système peuvent significativement être comparés à la matrice de criticité car pour les systèmes de faible complexité les modes de défaillance sur un niveau plus bas tendent à avoir une fréquence plus basse.

La matrice de criticité (comme montrée à la Figure 3) peut être appliquée qualitativement et quantitativement comme expliqué ci-dessus.

5.3.5 Evaluation de l'acceptabilité du risque

Quand le résultat requis de l'analyse est une matrice de criticité, elle peut être tracée à partir des sévérités allouées et des fréquences. L'acceptabilité du risque est définie subjectivement ou est menée par des décisions professionnelles et financières et elle varie selon les types d'industrie. Le Tableau 3 donne des exemples des classes d'acceptabilité du risque et une matrice de criticité modifiée.

Tableau 3 – Matrice risque/criticité

Fréquence d'apparition de l'effet de défaillance	Niveau de sévérité			
	1 Insignifiant	2 Marginal	3 Critique	4 Catastrophique
5: Fréquente	Indésirable	Intolérable	Intolérable	Intolérable
4: Probable	Tolérable	Indésirable	Intolérable	Intolérable
3: Occasionnelle	Tolérable	Indésirable	Indésirable	Intolérable
2: Eloignée	Négligeable	Tolérable	Indésirable	Indésirable
1: Improbable	Négligeable	Négligeable	Tolérable	Tolérable

5.3.6 Types d'AMDEC avec des échelles de classement

Les types d'AMDEC décrit en 5.3.2 sont très largement utilisés dans l'industrie automobile pour l'analyse de la conception de produits aussi bien que pour l'analyse de procédés de production de ces produits.

La méthodologie d'analyse est la même que celle décrite pour la forme générale de l'AMDE/AMDEC, sauf que les définitions sont prédéterminées en trois tableaux préparés pour la sévérité S, pour l'apparition O et pour la détection D.

5.3.6.1 Détermination alternative de la sévérité

Le Tableau 4 donne un exemple de niveaux de sévérité qui sont principalement utilisés dans l'industrie automobile.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

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

5.3.5 Risk acceptability assessment

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

Table 3 – Risk/criticality matrix

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

5.3.6 FMECA types with the ranking scales

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

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

5.3.6.1 Alternate severity determination

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Tableau 4 – Sévérité du mode de défaillance

Sévérité	Critère	Classement
Aucune	Aucun effet perceptible	1
Très mineure	Les grincements et cliquetis ne correspondent pas à ceux d'une bonne finition. Défaut remarqué par des clients perspicaces (moins de 25 %)	2
Mineure	Les grincements et cliquetis ne correspondent pas à ceux d'une bonne finition. Défaut remarqué par 50 % des clients.	3
Très basse	Les grincements et cliquetis ne correspondent pas à ceux d'une bonne finition. Défaut remarqué par la plupart des clients (plus de 75 %)	4
Basse	Véhicule/élément utilisable mais élément de commodité/confort utilisable à un niveau de performance réduit. Client quelque peu mécontent.	5
Modérée	Véhicule/élément utilisable mais élément de confort/commodité inutilisable. Client mécontent.	6
Elevée	Véhicule/élément utilisable mais à un niveau de performance réduit. Client très mécontent.	7
Très haute	Véhicule/élément inutilisable (perte des fonctions principales)	8
Dangereuse avec avertissement	Classement de sévérité très élevé quand un mode de défaillance potentiel affecte le fonctionnement sécurisé d'un véhicule et/ou concerne la non-conformité aux règles gouvernementales avec avertissement.	9
Dangereuse sans avertissement	Classement de sévérité très élevé quand un mode de défaillance potentiel affecte le fonctionnement sécurisé d'un véhicule et/ou concerne la non-conformité aux règles gouvernementales sans avertissement.	10

NOTE A partir de SAE J1739.

Un classement de sévérité est alloué à l'effet de la défaillance de chaque mode de défaillance en se basant sur la sévérité de l'effet sur l'aptitude à la fonction et de la sécurité du système global, à la lumière des exigences relatives au système, des objectifs et des contraintes, le véhicule étant considéré comme un système. Cela est visible sur le document AMDEC. La détermination de la sévérité en accord avec le Tableau 4 est très directe pour les nombres 6 et supérieurs. La détermination de la sévérité de 3 à 5 peut être subjective.

5.3.6.2 Détermination alternative de l'apparition

Le Tableau 5 (également emprunté à l'industrie automobile) donne des exemples de mesures d'apparition qualitative, pouvant être utilisés dans le concept NPR.

Tableau 5 – Apparition du mode de défaillance reliée à la fréquence et probabilité d'apparition

Apparition du mode de défaillance	Classement, *O*	Fréquence	Probabilité
Eloigné La défaillance est improbable	1	≤ 0,010 pour mille véhicules/éléments	≤ $1x10^{-5}$
Faible Relativement peu de défaillances	2	0,1 pour mille véhicules/éléments	$1x10^{-4}$
	3	0,5 pour mille véhicules/éléments	$5x10^{-4}$
Modéré Défaillance occasionnelle	4	1 pour mille véhicules/éléments	$1x10^{-3}$
	5	2 pour mille véhicules/éléments	$2x10^{-3}$
	6	5 pour mille véhicules/éléments	$5x10^{-3}$
Elevé Répétition de défaillance	7	10 pour mille véhicules/éléments	$1x10^{-2}$
	8	20 pour mille véhicules/éléments	$2x10^{-2}$
Très élevé La défaillance est quasiment inévitable	9	50 pour mille véhicules/éléments	$5x10^{-2}$
	10	≥100 sur mille véhicules/éléments	≥$1x10^{-1}$

NOTE Source: AIAG: Mode de défaillance potentiel et analyses d'effet, AMDE, 3e édition.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Table 4 – Failure mode severity

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

NOTE From SAE J1739.

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

5.3.6.2 Alternate determination of occurrence

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

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

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Il convient de noter que dans le Tableau 5, le terme «fréquence» est utilisé pour le taux d'apparition exprimé en nombre d'apparition pendant une mission ou une durée de vie définie, qui peut être comparée à la « fraction manquée » ou à la probabilité d'occurrence, et les probabilités correspondantes reflètent le plus souvent cette fraction. Par exemple, un mode de défaillance qui est classé à une valeur O de 9 provoquera une défaillance d'un des trois systèmes durant une période de mission prédéterminée. Ici, il faut que la détermination de cette probabilité d'apparition soit reliée à la durée étudiée. Il est conseillé d'établir cette durée dans l'en-tête de l'analyse.

La meilleure pratique est obtenue quand la probabilité d'apparition est calculée pour les composants et que leurs modes de défaillance sont fondés sur leur propre taux de défaillance dans les conditions de contraintes attendues (environnementales et opérationnelles). Quand cette information n'est pas disponible, une estimation peut être allouée, mais en faisant cela l'équipe en charge de l'analyse doit garder à l'esprit que la signification des nombres d'apparition – le nombre d'apparition par millier de véhicules sur une durée prédéterminée pour l'analyse (garantie, durée de vie du véhicule, ou autre) –, est la probabilité calculée ou estimée d'apparition sur le durée prédéterminée. Il faut aussi noter que contrairement à l'échelle de sévérité l'échelle d'apparition n'est pas linéaire ni logarithmique. En conséquence, il convient de garder à l'esprit que le nombre NPR résultant, quand il est calculé ou évalué, est aussi non linéaire et doit être traité avec beaucoup de précaution.

5.3.6.3 Classement de la probabilité de détection d'une défaillance

Dans le concept NPR, la probabilité qu'une défaillance soit détectée, c'est-à-dire la probabilité que les aides/dispositifs de conception ou procédures de vérification détectent les modes de défaillance potentiels à temps pour éviter une défaillance du niveau du système, doit être estimée. Pour une application à un procédé (AMDE, ou AMDEC de procédé), cela se réfère à la probabilité qu'un ensemble de contrôles de procédé couramment en place soit en position de détecter et isoler une défaillance avant qu'elle ne soit transmise aux procédés suivants ou au produit fini.

En particulier, pour les produits génériques, qui peuvent être utilisés dans plusieurs applications et systèmes différents, la probabilité de détection peut être difficile à estimer.

Le Tableau 6 donne une des méthodes relatives aux critères de détection, telles qu'utilisées dans l'industrie automobile.

Tableau 6 – Critère d'évaluation de la détection du mode de défaillance

Détection	Critères: Probabilité de détection par contrôle-conception	Classement
Quasi certain	Le contrôle-conception détectera très probablement une cause/un mécanisme potentiel et le mode de défaillance ultérieur.	1
Très haut	Très forte probabilité de détection par le contrôle-conception d'une cause/d'un mécanisme potentiel et du mode de défaillance ultérieur	2
Elevé	Forte probabilité de détection par le contrôle-conception d'une cause/d'un mécanisme potentiel et du mode de défaillance ultérieur	3
Modérément élevé	Probabilité modérée de détection par le contrôle-conception d'une cause/d'un mécanisme potentiel et du mode de défaillance ultérieur	4
Modéré	Probabilité modérée de détection par le contrôle-conception d'une cause/d'un mécanisme potentiel et du mode de défaillance ultérieur	5
Basse	Faible probabilité de détection par le contrôle-conception d'une cause/d'un mécanisme potentiel et du mode de défaillance ultérieur	6
Très bas	Très faible probabilité de détection par le contrôle-conception d'une cause/d'un mécanisme potentiel et du mode de défaillance ultérieur	7
Eloigné	Probabilité éloignée de détection par le contrôle-conception d'une cause/d'un mécanisme potentiel et du mode de défaillance ultérieur	8
Très éloigné	Probabilité très éloignée de détection par le contrôle-conception d'une cause/d'un mécanisme potentiel et du mode de défaillance ultérieur	9
Incertitude absolue	Le contrôle-conception ne pourra pas et/ou ne détectera pas une cause/un mécanisme potentiel et le mode de défaillance; ou il n'y a pas de contrôle-conception.	10

NOTE Source: AIAG: Mode de défaillance potentiel et analyses d'effet, AMDE, 3e édition.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

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

5.3.6.3 Rating of failure detection probability

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

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

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

Table 6 – Failure mode detection evaluation criteria

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.3.6.4 Evaluation du risque

Cette approche très intuitive décrite ci-dessus doit être suivie par un classement de priorité des actions à réaliser pour assurer le meilleur niveau de sécurité pour le client. Par exemple, un mode de défaillance avec une sévérité élevée, un taux bas d'apparition et une très haute détection (10, 3 et 2 respectivement) peut avoir un NPR beaucoup plus bas (dans ce cas 60) qu'un mode de défaillance dont tous les paramètres sont moyens (5 dans chaque cas donnant un NPR de 125). Ainsi, des procédures complémentaires sont souvent définies pour assurer que les modes de défaillance ayant un classement élevé de sécurité ont la plus grande priorité et sont réduits les premiers. Dans ce cas, il convient que la décision soit guidée par l'amplitude de la sévérité plutôt qu'uniquement par le NPR. Dans tous les cas, une bonne pratique est de considérer le classement de la sévérité d'un mode de défaillance avec le NPR pour un meilleur processus de prise de décision.

Les numéros d'ordre de priorité de risque sont également déterminés dans d'autres méthodes AMDE, plus particulièrement celles qui sont principalement qualitatives.

Avec les tableaux ci-dessus, les NPR sont calculés et souvent utilisés comme un guide pour la réduction des modes de défaillance. Les précautions données en 5.3.2 doivent être rappelées et les inconvénients du NPR doivent rester à l'esprit.

Certaines des déficiences du NPR sont les suivantes:

– lacunes dans les gammes, 88 % de la gamme est vide, seulement 120 des 1000 nombres sont générés,

– duplication de NPR: pour plusieurs combinaisons de différents facteurs conduisant au même NPR,

– changements de sensibilité trop faibles: une petite évolution d'un facteur a un effet beaucoup plus grand quand les autres facteurs sont eux-mêmes plus grands: (par exemple, 9x9x3 = 243, et 9x9x4 = 324 par rapport à 3x4x3= 36 et 3x4x4 = 48),

– échelle inadaptée: les rapports du tableau d'apparition ne sont pas proportionnels ou linéaires; par exemple, le rapport peut être 2,5 ou 2 entre les deux classements consécutifs,

– échelle NPR inadaptée. Les différences dans les nombres NPR peuvent apparaître négligeables alors qu'ils sont significatifs. Par exemple: les valeurs: S = 6, O = 4, D = 2, peuvent conduire à NPR = 48, alors que S = 6, O = 5, et D = 2 peuvent conduire à NPR = 60. Le second NPR n'est pas deux fois le premier nombre, alors qu'en fait O = 5 est deux fois la probabilité d'apparition avec O = 4. Donc, le nombre NPR ne peut pas être comparé de façon linéaire.

– les échelles étant ordinales et non rationnelles, la comparaison des NPR peut conduire à des conclusions erronées.

Le revue d'un NPR exige des précautions et un bon jugement. Une bonne pratique consiste en une revue complète des valeurs de sévérité, d'apparition et de détection, avant de se faire une opinion et d'engager des mesures correctives.

5.4 Rapport d'analyse

5.4.1 Domaine d'application et contenu d'un rapport

Le rapport sur l'AMDE peut être inclus dans une étude plus large ou être présenté seul. Dans tous les cas, il convient que le rapport inclue un résumé et un relevé détaillé de l'analyse et des diagrammes fonctionnels qui définissent la structure du système. Il convient également que le rapport contienne une liste des dessins (incluant les états) sur lesquels l'AMDE est basée.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.3.6.4 Risk evaluation

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

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

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

Some of the deficiencies of the RPN are as follows:

– gaps in the ranges: 88% of the range is empty, only 120 of 1000 numbers are generated,

– duplicate RPNs: for several combinations where different factors lead to the same RPN,

– sensitivity to small changes: a small change in one factor has a much larger effect when the other factors are larger than when they are small (example: 9x9x3 = 243, and 9x9x4 = 324 versus 3x4x3 = 36 and 3x4x4=48),

– inadequate scaling: the ratios on occurrence table are not proportional or linear; e.g. the ratio can be 2,5 or 2 between the two consecutive ratings,

– inadequate scale of RPN. The differences in RPN number might appear negligible while in fact significant. An example would be: the values: S = 6, O = 4, D = 2, would produce an RPN = 48, while S = 6, O = 5, and D = 2 would produce RPN = 60. The second RPN is not twice the first number, while in fact O = 5 is twice the probability of occurrence with O = 4. Therefore the RPN numbers should not be compared linearly.

– misleading conclusions from RPN comparison as the scales are ordinal and not rational.

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

5.4 Report of analysis

5.4.1 Scope and content of a report

The report on the FMEA may be included in a wider study or may stand alone. In either case, the report should include a summary and a detailed record of the analysis and the block or functional diagrams which define the system structure. The report should also contain a list of the drawings (including issue status) on which the FMEA is based.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.4.2 Résumé des effets

Il convient qu'une liste des effets de défaillance sur un système spécifique éclairée par l'AMDE soit préparée. Le Tableau 7 donne un ensemble typique des effets de défaillance pour moteur de démarreur de véhicule à moteur et circuit.

Tableau 7 – Exemple d'un ensemble d'effets de défaillance (pour un démarreur de véhicule à moteur)

1	Le moteur du démarreur ne fonctionne pas
2	Le moteur du démarreur va moins vite que spécifié
3	Le moteur du démarreur n'embraye pas
4	Le moteur du démarreur fonctionne prématurément

NOTE 1 Cette liste n'est qu'un exemple. Chaque système ou sous-système étant analysé aura son propre ensemble d'effets de défaillance.

Un résumé des effets de défaillance peut être nécessaire pour déterminer la probabilité de défaillance du système résultant des effets de défaillance listés et pour établir les priorités des actions préventives ou curatives. Il convient que le résumé des effets de défaillance soit basé sur la liste des effets de défaillance finaux et contienne les détails des modes de défaillance du dispositif contribuant à chaque effet de défaillance. Cette probabilité d'apparition pour chacun des modes de défaillance est calculée pour la durée prédéterminée d'utilisation du dispositif aussi bien que pour le profile d'utilisation et les contraintes attendus. Le Tableau 8 illustre un résumé des effets de défaillance typiques.

Tableau 8 – Exemple de probabilités d'effets de défaillance

Numéro	Effet	Référence mode défaillance	Probabilité d'apparition des effets de la défaillance
1	Le moteur du démarreur ne fonctionne pas	1, 3, 7, 8, 9, 16, 21, 22	8×10^{-3}
2	Le moteur du démarreur va moins vite que spécifié	6, 11, 12, 19, 20	6×10^{-4}
3	Le moteur du démarreur n'embraye pas	2, 4, 5, 10, 13	$1{,}1\times10^{-5}$
4	Le moteur du démarreur fonctionne prématurément	14, 15, 17, 18	$3{,}6\times10^{-7}$

NOTE 2 Ce tableau peut être construit pour des classements qualitatifs et quantitatifs d'un dispositif ou d'un système.

Il convient que le résumé contienne une brève description de la méthode d'analyse et du niveau auquel elle était conduite, les hypothèses et les règles de base. De plus, il convient qu'il contienne les listes suivantes:

a) modes de défaillance qui entraînent des effets sérieux,

b) recommandations à l'attention des concepteurs, personnel de maintenance, planificateurs et utilisateurs,

c) modifications dans la conception ayant été déjà incorporées à la suite de l'AMDE,

d) effets atténués par les modifications de conception incorporées.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

5.4.2 Effects summary

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

Table 7 – Example of a set of failure effects (for a motor vehicle starter)

1	Starter motor fails to operate
2	Starter motor speed less than specified
3	Starter motor fails to engage ring gear
4	Starter motor operates prematurely

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

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

Table 8 – Example of a failure effects probability

Number	Effect	Contributing failure mode reference	Failure effect probability of occurrence
1	Starter motor fails to operate	1, 3, 7, 8, 9, 16, 21, 22	8×10^{-3}
2	Starter motor speed less than specified	6, 11, 12, 19, 20	6×10^{-4}
3	Starter motor fails to engage ring gear	2, 4, 5, 10, 13	$1{,}1\times10^{-5}$
4	Starter motor operates prematurely	14, 15, 17, 18	$3{,}6\times10^{-7}$

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

The summary should also contain a brief description of the method of analysis and the level to which it was conducted, the assumptions and the ground rules. In addition it should include listings of the following:

a) failure modes, that result in serious effects;

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

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

6 Autres considérations

6.1 Défaillances de cause commune

Dans une analyse de fiabilité, il ne suffit pas de considérer uniquement les défaillances indépendantes et aléatoires. Certaines défaillances de «cause commune» (CCF) peuvent survenir, qui entraînent une dégradation ou défaillance d'aptitude du système au travers de déficiences simultanées dans plusieurs composants du système et qui sont dues à une source unique telle qu'une erreur de conception (point d'assignation de composants impropre), contraintes environnementales (foudre), ou erreur humaine.

Les défaillances de cause commune (CCF) sont celles qui sont contraires à l'hypothèse fondamentale qui stipule que les modes de défaillance considérés dans une AMDE sont indépendants. Une CCF provoquera simultanément plusieurs défaillances du dispositif ou, sur une durée suffisamment courte, l'effet de défaillances simultanées.

Typiquement, les sources de CCF comprennent

– en conception, les logiciels, les assignations,
– en production, les défauts de composant liés à un lot,
– l'environnement, les interférences électriques, cycles de température, vibrations,
– les facteurs humains: les actions non conformes lors du fonctionnement ou de la maintenance,

Il faut donc que l'AMDE prenne en considération les sources possibles de CCF quand elle porte sur un système qui utilise des redondances pour maintenir une fonction ou des dispositifs multiples pour réduire les conséquences d'une défaillance.

Une CCF est le résultat d'un événement qui, du fait de dépendances logiques, provoque une coïncidence d'états de défaillance dans deux ou plusieurs composants (à l'exclusion des défaillances secondaires provoquées par les effets d'une défaillance primaire). Les défaillances de cause commune peuvent être des parties identiques avec les mêmes modes de défaillance et faiblesses utilisées dans divers ensembles d'un système – pouvant être redondant, quand la redondance est exclue.

Les CCF peuvent être analysées qualitativement en utilisant l'AMDE, mais l'aptitude à analyser complètement les CCF est assez limitée. Cependant, l'AMDE est une procédure pour examiner successivement chaque mode de défaillance et causes associées et aussi identifier les essais périodiques, mesures de maintenance préventive, etc., ce qui rend possible une étude de toutes les causes pouvant induire de potentielles CCF.

Une combinaison de plusieurs méthodes est utile pour prévenir ou réduire une CCF (modélisation du système, analyses physiques de composants): diversité fonctionnelle (où les branches redondantes, ou parties du système réalisant les mêmes fonctions ne sont pas identiques et donnent divers modes de défaillance), séparation physique pour éliminer l'influence de l'environnement ou les contraintes EMI provoquant des CCF, les essais, etc. Habituellement, l'AMDE ne prend pas en considération l'examen de mesures préventives contre les CCF. Cependant, ces mesures doivent être incluses dans la colonne des remarques, pour aider à la compréhension de toute l'AMDE.

6.2 Facteurs humains

Certains systèmes doivent être conçus pour atténuer certaines erreurs humaines. Par exemple, fournir des verrouillages mécaniques sur les signaux de chemin de fer, et des mots de passe pour l'usage d'ordinateurs et la restitution de données. Lorsque de telles dispositions existent dans un système, l'effet de défaillance de la disposition dépendra du type d'erreur. Certains modes d'erreurs humaines peuvent aussi être considérés autrement

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

6 Other considerations

6.1 Common-cause failures

In a reliability analysis, it is not sufficient to consider only random and independent failures. Some “common-cause” failures (CCF) can occur, that cause system performance degradation or failure through simultaneous deficiency in several system components, due to a single source such as design error (improper components derating), environmental stresses (lightning), or human error.

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

Typically, sources of CCF include

– design: software, rating;

– manufacturing: batch related component flaws;

– environment: electrical interference, temperature cycling, vibration;

– human factors: incorrect operating or maintenance actions.

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

A CCF is the result of an event that, because of logical dependencies, causes a coincidence of failure states in two or more components (excluding secondary failures caused by the effects of a primary failure). Common-cause failures can be in identical parts with the same failure modes and weaknesses used in various assemblies of a system – possibly redundant, where redundancy is voided.

CCFs can be analysed qualitatively using FMEA, but the ability of FMEA to fully analyse CCF is quite limited. However, FMEA is a procedure to examine successively each failure mode and associated causes and also to identify all periodic tests, preventative maintenance measures, etc. It makes possible a study of all the causes that can induce potential CCF.

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

6.2 Human factors

Some systems have to be designed to prevent or mitigate some human errors. An example of those measures would be providing mechanical interlocks on railway signals, and passwords for computer usage or data retrieval. Where such provisions exist in a system, the effect of failure of the provisions will depend on the type of error. Some modes of human error should

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

pour un système sans panne, pour contrôler l'efficacité des dispositions. Bien qu'incomplète, une liste même partielle de ces modes est bénéfique pour l'identification de la conception et les déficiences de procédure; l'identification de toutes formes possibles d'erreurs humaines serait probablement impossible.

Les erreurs humaines sont impliquées dans beaucoup de CCF. Par exemple, une maintenance incorrecte de dispositifs similaires peut annuler la redondance. Pour l'éviter, la diversité matérielle est souvent introduite dans les éléments redondants.

6.3 Erreurs logicielles

Une AMDE conduite sur le matériel d'un système complexe peut avoir des répercussions sur le logiciel dans le système. Ainsi, les décisions sur les effets, probabilités conditionnelles et de criticité résultant de l'AMDE peuvent dépendre des éléments logiciels et de leur nature, séquentielle et temporelle. Quand c'est le cas, les relations entre matériel et logiciel doivent être clairement identifiées car toute altération ultérieure ou amélioration du logiciel peut modifier l'AMDE et les évaluations qui en découlent. L'approbation de développement et de changement de logiciel peut être conditionnée par une révision de l'AMDE et les évaluations relatives, par exemple la logique du logiciel peuvent être altérées pour améliorer la sécurité au dépend de la fiabilité opérationnelle.

Les dysfonctionnements dus aux erreurs de logiciels ou inadéquations auront des effets dont la signification sera déterminée à la fois par la conception matérielle et logicielle. Le postulat de telles erreurs ou inadéquations et l'analyse de leurs effets sont possibles uniquement jusqu'à un certain point. Les effets sur le matériel associé de possibles erreurs dans le logiciel peuvent être estimés, et la provision d'arrangements de repli, soit en matériel, soit en logiciel, est souvent suggérée par de telles analyses.

6.4 L'AMDE et les conséquences de la défaillance du système

Une étude AMDE peut être menée sans référence à une application particulière et peut alors être adaptée ensuite à l'utilisation du projet. Cela s'applique à des ensembles relativement petits qui peuvent eux-mêmes être regardés comme composants génériques (par exemple un amplificateur électronique, un moteur électrique, une valve mécanique).

Cependant, il est plus habituel de développer une AMDE pour un projet spécifique et d'avoir à considérer les conséquences particulières des défaillances du système. Il peut être nécessaire de catégoriser les effets de défaillances sur le système suivant les conséquences de ces défaillances, par exemple, sans panne, défaillance réparable, défaillance non réparable, mission dégradée, mission manquée, effets sur les individus, généralement groupes ou sociétés.

Le besoin de lier une AMDE à la conséquence ultime d'une défaillance du système dépendra du projet et de la relation entre l'AMDE et les autres formes d'analyse, telles que l'arbre de défaillance, les graphes de Markov, les réseaux de Pétri, etc.

7 Applications

7.1 Utilisation d'une AMDE/AMDEC

L'AMDE est une méthode qui est principalement adaptée à l'étude des défaillances de matériels et équipements et qui peut être appliquée à des catégories de systèmes basées sur diverses technologies (électrique, mécanique, hydraulique, etc.) et combinaisons de technologies ou qui peut être spécifique à des pièces particulières d'équipement, à des systèmes ou à des projets en tant que tels.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

also be considered for an otherwise fault-free system, to check the effectiveness of the provisions. Although incomplete, even a partial listing of these modes is beneficial for the identification of design and procedural deficiencies; the identification of all possible forms of human error would probably be impossible.

Many CCFs involve human errors. For example, incorrect maintenance of similar items can negate redundancy. To avoid this, material diversity in redundant elements is often introduced.

6.3 Software errors

An FMEA conducted on the hardware of a complex system may have repercussions on the software in the system. Thus, decisions about effects, criticality and conditional probabilities resulting from the FMEA may be dependent upon the software elements and their nature, sequence and timing. When this is the case, the interrelationships between hardware and software need to be clearly identified because any subsequent alteration or improvement of the software may modify the FMEA and the assessments derived from it. Approval of software development and change may be conditional upon a revision of the FMEA and the related assessments, e.g. software logic may be altered to improve safety at the expense of operational reliability.

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

6.4 FMEA regarding consequences of system failure

A system FMEA can be carried out without reference to any particular application and could then be adapted subsequently for project use. This applies to relatively small assemblies that might themselves be regarded as generic components (for example an electronic amplifier, an electric motor, a mechanical valve).

However, it is more usual to develop a project-specific FMEA and to have regard to the particular consequences of system failure. It might be necessary to categorize the effects of failures on the system according to the consequences of these failures, for example, fail-safe, repairable failure, non-repairable failure, mission degraded, mission failed, effects on individuals, groups or society generally.

The need to relate an FMEA to the ultimate consequence of system failure will depend on the project and the relationship between the FMEA and other forms of analysis, such as fault trees, Markov graphs, Petri nets, etc.

7 Applications

7.1 Use of FMEA/FMECA

FMEA is a method that is primarily adapted to the study of material and equipment failures and that can be applied to categories of systems based on different technologies (electrical, mechanical, hydraulic, etc.) and combinations of technologies or it may be specific to particular pieces of equipment, to systems or to projects as a whole.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Il convient que l'AMDE prenne aussi en considération les logiciels et l'aptitude humaine lorsqu'elle s'applique à la sûreté de fonctionnement du système. Une AMDE peut être une étude d'application générale pour étudier différents procédés (médical, de laboratoire, de production, de développement, d'éducation, etc.) quand elle porte généralement le nom d'AMDE de procédé ou PAMDE. Quand une AMDE de procédé est réalisée, elle l'est toujours par rapport aux objectifs finaux du procédé et, ainsi, elle considère chaque étape de ce procédé comme une potentialité de résultat incorrect au niveau d'autres étapes ou à la fin du procédé.

7.1.1 Application dans un projet

Il convient qu'un utilisateur détermine comment et pour quels objectifs l'AMDE est utilisée dans sa propre discipline technique. Elle peut être utilisée seule ou en complément et support d'autres méthodes d'analyses de fiabilité. Les exigences pour l'AMDE ont pour origine le besoin de comprendre le comportement du matériel et ses implications sur le fonctionnement du système ou équipement. Le besoin d'une AMDE peut varier largement d'un projet à un autre.

L'AMDE assiste le concept de revue de conception et il convient de la mettre en application dès que possible dans la phase de conception du système ou sous-système. L'AMDE est applicable à tous les niveaux de conception du système mais elle est plus appropriée aux niveaux inférieurs où un grand nombre de dispositifs sont impliqués et/ou la fonctionnalité est complexe. Une formation spéciale pour le personnel réalisant l'AMDE est essentielle. Ce personnel a besoin d'une collaboration étroite avec les concepteurs et ingénieurs des systèmes. Il convient que l'AMDE soit mise à jour au fur et à mesure de la progression du projet et de la modification des conceptions. A la fin du projet, l'AMDE est utilisée pour vérifier la conception et peut être essentielle pour la démonstration de la conformité de la conception d'un système aux normes requises, réglementations, et exigences de l'utilisateur.

L'information fournie par l'AMDE identifie les priorités pour l'échantillonnage statistique du contrôle des procédés et les essais d'inspection durant la fabrication et l'installation, et pour la qualification, l'approbation, l'acceptation et les essais de démarrage. Elle fournit l'information essentielle aux procédures de diagnostic et de maintenance à inclure dans les manuels.

En décidant de l'étendue et de la façon dont l'AMDE doit être appliquée à un dispositif ou à une conception, il est important de considérer les objectifs spécifiques pour lesquels les résultats de l'AMDE sont nécessaires, le phasage avec les autres activités et l'importance d'établir un degré prédéterminé de perception et de contrôle sur les modes et effets de défaillance non désirés. Cela mène au planning d'une AMDE en termes qualitatifs à des niveaux spécifiés (système, sous-système, composant, dispositif) pour faire référence au processus itératif de conception et de développement.

Pour s'assurer que cela est effectif, l' AMDE doit être clairement située dans le programme de sûreté de fonctionnement, de même que le temps, les ressources humaines et autres ressources nécessaires. Il est vital que l'AMDE ne soit pas abrégée pour économiser du temps ou de l'argent. S'il manque de l'argent ou du temps, il convient que l'AMDE se concentre sur ces parties de la conception, qui sont nouvelles ou utilisées de façon nouvelle. L'AMDE peut être économiquement dirigée vers des domaines identifiés comme cruciaux par les autres méthodes d'analyse.

7.1.2 Application à un procédé

Quand elle est préparée pour un procédé, la réalisation d'une PAMDE exige ce qui suit:

a) une définition claire du but du procédé. Quand le procédé est complexe , le but du procédé peut être redéfini comme étant le but global ou le produit du procédé, ou le but ou le produit issu d'un ensemble d'étapes ou de séquence de précédé, et d'un produit ou d'une étape individuelle de procédé;

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

7.1.1 Application within a project

A user should determine how and for what purposes FMEA is used within his/her own technical discipline. It may be used alone or to complement and support other methods of reliability analysis. The requirements for FMEA originate from the need to understand hardware behaviour and its implications for the operation of the system or equipment. The need for FMEA can vary widely from one project to another.

FMEA supports the design review concept and should be put into use as early as possible in the period of system and subsystem design. FMEA is applicable to all levels of system design but is most appropriate for lower levels where large numbers of items are involved and/or there is functional complexity. Special training of personnel performing FMEA is essential and they need the close collaboration of systems engineers and designers. The FMEA should be updated as the project progresses and as designs are modified. At the end of the project, FMEA is used to check the design and may be essential for demonstration of conformity of a designed system to the required standards, regulations, and user's requirements.

Information from the FMEA identifies priorities for statistical process control, sampling and inspection tests during manufacture and installation and for qualification, approval, acceptance and start-up tests. It provides essential information for diagnostic and maintenance procedures for inclusion in handbooks.

In deciding on the extent and the way in which FMEA should be applied to an item or design, it is important to consider the specific purposes for which FMEA results are needed, the time phasing with other activities and the importance of establishing a predetermined degree of awareness and control over unwanted failure modes and effects. This leads to the planning of FMEA in qualitative terms at specified levels (system, subsystem, component, item) to relate to the iterative design and development process.

To ensure that it is effective, the place of FMEA should be clearly established in the dependability programme, together with the time, manpower and other resources needed to make it effective. It is vital that FMEA is not abridged to save time and money. If time and money are short the FMEA should concentrate on those parts of the design which are new or are used in new ways. FMEA can be economically directed to areas identified as crucial by other methods of analysis.

7.1.2 Application with a process

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

b) la compréhension des étapes individuelles du procédé;

c) la compréhension des défauts potentiels dans chaque étape de procédé;

d) la compréhension de l'effet que chaque défaut individuel (défaillance potentielle) peut avoir sur le produit du procédé;

e) la compréhension des causes potentielles de chaque défaut ou défaillance/panne potentielle de procédé.

Si un procédé réalise plus d'un produit, alors il peut être analysé en ayant à l'esprit le produit spécifique pour lequel la PAMDE est réalisée. Le procédé peut aussi être analysé en termes d'étapes ou de résultats incorrects potentiels, ce qui mènera à un PAMDE généralisée pour le procédé sans considération d'un type de produits individuels.

7.2 Avantages d'une AMDE

Certaines des applications détaillées et des bénéfices de l'AMDE sont listées ci-dessous:

a) éviter les modifications coûteuses par l'identification précoce des déficiences de conception,

b) identifier les défaillances qui, lorsqu'elles surviennent seules ou en combinaison, ont des effets inacceptables ou significatifs, et déterminer les modes de défaillance qui peuvent sérieusement affecter le fonctionnement attendu ou requis.

NOTE 1 De tels effets peuvent inclure des défaillances secondaires.

c) déterminer le besoin pour les méthodes de conception pour l'amélioration de la fiabilité (redondance, contraintes opérationnelles, sans panne, sélection de composants et déclassement, etc.),

d) fournir le modèle logique requis pour évaluer la probabilité ou le taux d'apparition des anomalies de fonctionnement du système en préparation d'analyses de criticité,

e) révéler la localisation de problème de responsabilité du produit et de sécurité, ou la non-conformité aux exigences réglementaires,

NOTE 2 Fréquemment, des études séparées seront requises pour la sécurité, mais le chevauchement est inévitable et par conséquent la coopération est hautement recommandée.

f) assurer que le programme d'essai de développement peut détecter les modes de défaillance potentiels,

g) se focaliser sur les emplacements-clés où concentrer le contrôle qualité, l'inspection et les contrôles du procédé de fabrication,

h) aider à définir les divers aspects de la stratégie et du programme de maintenance générale préventive,

i) faciliter ou apporter un soutien pour déterminer les critères d'essai, les plans d'essai et procédures de diagnostic, par exemple: essai de performances, à la fonction, essai de fiabilité,

j) soutenir la conception de séquences d'isolation de défaut et l'établissement des plannings pour les modes alternatifs de fonctionnement et les reconfigurations,

k) fournir aux concepteurs une compréhension des facteurs qui influencent la fiabilité du système,

l) fournir un document final qui est une preuve de l'attention portée à la conception pour qu'elle réponde en service aux spécifications (cela est particulièrement important dans le cas de responsabilité de produit).

7.3 Limitations et inconvénients de l'AMDE

L'AMDE est extrêmement efficace quand elle est appliquée à l'analyse d'éléments qui causent une défaillance totale du système en totalité ou d'une fonction majeure du système. Cependant, l'AMDE peut être difficile et fastidieuse dans le cas de systèmes complexes qui ont de multiples fonctions impliquant différents ensembles de composants de système. La cause en est la quantité d'information du système détaillé qui doit être prise en considération.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

b) understanding of the individual steps in the process;

c) understanding of potential flaws in each process step;

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

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

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

7.2 Benefits of FMEA

Some of the detailed applications and benefits of FMEA are listed below:

a) to avoid costly modifications by the early identification of design deficiencies;

b) to identify failures which, when they occur alone or in combination, have unacceptable or significant effects, and to determine the failure modes which may seriously affect the expected or required operation;

NOTE 1 Such effects may include secondary failures.

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

d) to provide the logic model required to evaluate the probability or rate of occurrence of anomalous operating conditions of the system in preparation for criticality analysis;

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

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

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

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

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

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

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

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

l) to provide a final document that is proof of the fact that (and of the extent to which) care has been taken to ensure that the design will meet its specification in service. (This is especially important in the case of product liability.)

7.3 Limitations and deficiencies of FMEA

FMEA is extremely efficient when it is applied to the analysis of elements that cause a failure of the entire system or of a major function of the system. However, FMEA may be difficult and tedious for the case of complex systems that have multiple functions involving different sets of system components. This is because of the quantity of detailed system information that needs

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Cette difficulté peut être accrue par l'existence de plusieurs modes de fonctionnement possibles, et ainsi que par la considération de politiques de maintenance et de réparation.

L'AMDE peut être un processus inefficace et laborieux si elle n'est pas judicieusement appliquée. Il convient de définir les utilisations auxquelles les résultats sont destinés et de ne pas inclure aveuglément l'AMDE dans des spécifications d'exigences.

Des complications, incompréhensions et erreurs peuvent survenir quand l'AMDE tente de balayer plusieurs niveaux dans une structure hiérarchique si la redondance est appliquée dans la conception du système.

Les relations entre des modes ou des causes de défaillance considérés individuellement ou en groupe ne peuvent pas être réellement présentées dans une AMDE puisque la principale hypothèse d'un telle analyse est l'indépendance des modes de défaillance. Cette déficience est même plus prononcée pour les interactions logiciel/matériel, où l'hypothèse d'indépendance ne s'applique pas. Le même type de difficulté peut être rencontré quand on ajoute les interactions humaines avec le matériel et la modélisation de ces interdépendances. L'hypothèse d'indépendance peut obscurcir un mode de défaillance, ce qui peut avoir des conséquences graves en présence d'une conséquence d'un autre mode de défaillance, alors que chacun des deux modes peut avoir une faible probabilité d'apparition. Les scénarii d'interrelation sont de loin mieux modélisés en utilisant une approche d'analyse de mode de défaillance avec l'outil AAD (CEI 60300-3-1, édition 2).

Il est donc préférable pour une AMDE de se limiter à deux niveaux seulement de la structure hiérarchique. Par exemple, identifier les modes de défaillance de dispositifs et déterminer leurs effets sur un ensemble est une tâche relativement simple. Ces effets deviennent donc des modes de défaillance au niveau supérieur suivant, par exemple le module, et ainsi de suite. Cependant, des AMDE même sur plusieurs niveaux sont souvent menées avec succès.

Une autre déficience de l'AMDE réside dans son incapacité à fournir une mesure de la fiabilité globale du système, et, pour la même raison, elle n'est pas capable de fournir de mesures des améliorations et choix de conceptions.

7.4 Relations avec les autres méthodes

L'AMDE (ou AMDEC) peut être utilisée seule. Comme méthode inductive systématique d'analyse, l'AMDE est très souvent utilisée pour compléter d'autres approches, plus particulièrement déductives, telle que AAD. Au stade de la conception, il est souvent difficile de décider si l'approche déductive ou inductive est dominante, les deux étant combinées dans les processus d'analyse et de réflexion. L'approche déductive est préférée dans les installations et systèmes industriels où les niveaux de risque sont identifiés mais l'AMDE reste un outil de conception utile. Cependant, il convient de la compléter par d'autres méthodes. C'est particulièrement le cas lorsque des problèmes nécessitent d'être identifiés et des solutions trouvées dans des situations où de multiples défaillances et effets séquentiels doivent être étudiés. La méthode utilisée en premier dépendra du programme du projet.

Durant les premiers stades de la conception, où seules les fonctions, la structure générale du système et des sous-systèmes ont été définies, l'aptitude à la fonction réussie du système peut être décrite par un bloc-diagramme de fiabilité ou par un arbre de défaillance. Cependant, pour aider à dessiner ces diagrammes du système, il convient d'appliquer une AMDE inductive aux sous-systèmes avant qu'ils ne soient conçus. Dans de telles circonstances, l'approche AMDE ne peut être une procédure détaillée mais plutôt un processus réfléchi difficilement exprimé dans un tableau figé. En général, quand on analyse un système complexe impliquant diverses fonctions, de nombreux dispositifs et relations entre ces dispositifs, l'AMDE est essentielle mais insuffisante.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

to be considered. This difficulty can be increased by the existence of a number of possible operating modes, as well as by consideration of the repair and maintenance policies.

FMEA can be a laborious and inefficient process unless it is judiciously applied. The uses to which the results are to be put subsequently should be defined, and FMEA should not be included in requirements specifications indiscriminately.

Complications, misunderstandings and errors can occur when FMEA attempts to span several levels in a hierarchical structure if redundancy is applied in the system design.

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

It is therefore preferable for an FMEA to be restricted to relating two levels only in the hierarchical structure. For example, it is a relatively straightforward task to identify failure modes of items and to determine their effects on the assembly. These effects then become the failure modes at the next level up, e.g. the module, and so on. However, successful multi-level FMEAs are often carried out.

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

7.4 Relationships with other methods

FMEA (or FMECA) can be used alone. As a systematic inductive method of analysis, FMEA is most often used to complement other approaches, especially deductive ones, such as FTA. At the design stage, it is often difficult to decide whether the inductive or deductive approach is dominant, as both are combined in processes of thought and analysis. Where levels of risk are identified in industrial facilities and systems, the deductive approach is preferred but FMEA is still a useful design tool. However, it should be supplemented by other methods. This is particularly the case when problems need to be identified and solutions need to be found in situations where multiple failures and sequential effects need to be studied. The method used first will depend on the project programme.

During the early design stages, where only functions, general system structure and subsystems have been defined, successful performance of the system can be depicted by a reliability block diagram or by a failure path by a fault tree. However, to assist in drawing these diagrams of the system, an FMEA inductive process should be applied to the subsystems before they are designed. Under these circumstances, the FMEA approach cannot be a comprehensive procedure but is instead a thought process not readily expressed in a rigid tabular form. In general, when analysing a complex system involving several functions, numerous items and interrelations between these items, the FMEA proves to be essential but not sufficient.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

L'analyse par arbre de défaillance (AAD) est une méthode déductive complémentaire pour l'analyse des modes de défaillance et leurs causes respectives. Elle trace les causes de bas niveau d'une défaillance de haut niveau postulée. Bien que l'analyse logique puisse être et soit parfois utilisée pour des analyses purement qualitatives de séquences de panne, c'est habituellement un précurseur pour l'estimation de la fréquence de la défaillance de haut niveau postulée. L'AAD est capable de modéliser l'interdépendance de différents modes de défaillance, où cette interaction peut résulter en un événement de proportion substantielle, et peut-être de sévérité élevée. C'est particulièrement important quand l'apparition d'un premier mode de défaillance peut induire l'apparition d'un autre, de probabilité et de sévérité plus élevées. Ce scénario ne peut pas être modélisé avec succès avec une AMDE où chaque mode de défaillance est considéré indépendamment et individuellement. Une des déficiences de l'AMDE est son incapacité à voir l'interaction et les dynamiques des apparitions des modes de défaillance dans un système.

L'AAD se concentre sur la logique d'événements alternatifs et coïncidents (ou séquentiels) ayant des conséquences indésirables. Elle peut produire un modèle correct du système analysé ainsi qu'une estimation de sa fiabilité (ou probabilité de défaillance), et peut aussi évaluer l'influence des améliorations de la conception et de l'atténuation du mode de défaillance sur la fiabilité de l'ensemble du système, ce qui peut être avantageux. Le format AMDE peut être plus descriptif. Les deux méthodes ont leur utilité dans une analyse complète pour la sécurité et la sûreté de fonctionnement dans un système complexe. Cependant, si le système est basé principalement sur des logiques de séries, avec peu de redondances et peu de fonctions, alors l'AAD est une façon inutilement compliquée de présenter la logique et d'identifier les modes de défaillance. Dans de tels cas, l'AMDE et les blocs-diagrammes de fiabilité sont adéquats. Dans les autres cas où l'AMDE est préférée, elle doit tout de même toujours être agrémentée de descriptions des modes de défaillance et de leurs effets.

Il convient que la principale considération pour sélectionner la méthode d'analyse porte sur les exigences particulières du projet, pas seulement vis-à-vis des exigences techniques, mais aussi de l'échelle de temps, du coût, de l'efficacité et de l'utilisation des résultats. Les guides généraux sont les suivants:

a) l'AMDE est appropriée lorsqu'une connaissance détaillée des caractéristiques de défaillance d'un dispositif est requise;

b) l'AMDE s'applique plus aux petits systèmes, modules et ensembles;

c) l'AMDE est un outil essentiel au stade de la recherche et du développement ou de la conception lorsque des effets inacceptables de défaillance ont besoin d'être identifiés et des solutions trouvées;

d) l'AMDE peut être nécessaire pour des dispositifs de conception novatrice tels que leurs caractéristiques de défaillance ne peuvent être connues d'expérience de fonctionnement précédente;

e) l'AMDE s'applique habituellement plus à des systèmes ayant un nombre important de composants à considérer, reliés par des logiques de défaillance de séries prédominantes;

f) l'AAD est généralement plus adaptée à l'analyse de modes de défaillance multiples et dépendances impliquant des redondances et logiques de défaillance complexes. L'AAD peut être utilisée aux plus hauts niveaux dans la structure du système tôt dans la conception et peut aider à identifier le besoin d'AMDE détaillée à des niveaux plus bas durant la conception.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Fault Tree Analysis (FTA) is a complementary deductive method for analysis of failure modes and their respective causes. It traces the low-level causes of a postulated high-level failure. Though the logical analysis can be, and sometimes is, used for purely qualitative analysis of fault sequences, it is usually a precursor to estimating the frequency of the postulated high-level failure. FTA is capable of modelling the interdependency of various failure modes, where that interaction might result in an event of substantial proportions, and perhaps of high severity. This is especially important where occurrence of one failure mode first would induce occurrence of another with high probability and high severity. This scenario could not be modelled successfully with an FMEA, where each failure mode is considered independently and individually. One of the deficiencies of an FMEA is its inability to view interaction and dynamics of failure mode occurrences in a system.

FTA concentrates on the logic of coincident (or sequential) and alternative events causing undesirable consequences. It can produce a correct model of the system being analysed as well as an estimate of its reliability (or probability of failure), and can also evaluate the influence of the design improvements and failure mode mitigation on the overall system reliability, which can be advantageous. The FMEA format can be more descriptive. Both methods have their uses in a full analysis for safety and dependability in a complex system. However, if the system is based mainly on series logic, with few redundancies and few functions, then FTA is an unnecessarily complicated way of presenting the logic and identifying the failure modes. In such cases FMEA and reliability block diagrams are adequate. In other cases where FTA is preferred, it still needs to be enhanced with descriptions of the failure modes and effects.

The main consideration in selecting the method of analysis should depend on the particular requirements of the project, not only with regard to technical requirements but also timescale, cost, efficiency and usage of the results. General guidelines are as follows.

a) FMEA is appropriate when comprehensive knowledge of the failure characteristics of an item is required.

b) FMEA is more appropriate for smaller systems, modules or assemblies.

c) FMEA is an essential tool at the research and development or design stage when unacceptable effects of failures need to be identified and solutions found.

d) FMEA can be necessary for items that are of innovatory design and their failure characteristics cannot be known from previous operational experience.

e) FMEA is usually more applicable to systems having large numbers of components to be considered that are related by predominantly series failure logic.

f) FTA is generally more suitable for the analysis of multiple failure modes and dependency involving complex failure logic and redundancy. FTA can be used at the higher levels in the system structure early in the design stage and can help in identifying the need for detailed FMEA at lower levels during detailed design.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Annexe A
(informative)

Récapitaualtif des procédures pour AMDE et AMDEC

A.1 Etapes de la réalisation de l'analyse

Les étapes de procédure nécessaires pour mener une analyse sont les suivantes.

a) Décider si une AMDE ou AMDEC est nécessaire.
b) Définir des limites du système pour l'analyse.
c) Comprendre les exigences du système et sa fonction.
d) Définir les critères de réussite/défaillance.
e) Déterminer les modes de défaillance de chaque système et leurs effets de défaillance et les enregistrer.
f) Résumer chaque effet de défaillance.
g) Rapporter les constatations.

Les étapes supplémentaires pour l'AMDEC sont les suivantes.

h) Déterminer les classes de sévérité du système.
i) Etablir la sévérité du mode de défaillance du dispositif.
j) Déterminer le mode de défaillance du dispositif et les fréquences des effets.
k) Déterminer les fréquences des modes de défaillance.
l) Dresser des matrices de criticité pour les modes de défaillance du dispositif.
m) Résumer la criticité des effets de défaillance de la matrice de criticité.
n) Dresser des matrices de criticité pour les effets de défaillance du système.
o) Rapporter les constatations à tous les niveaux d'analyse.

NOTE Une quantification du mode de défaillance et des fréquences des effets peut être entreprise dans une AMDE en réalisant les étapes h), i) et j) à la fin de l'AMDE.

A.2 Document de travail AMDE

A.2.1 Domaine d'application d'un document

Le document AMDE présente les détails de l'analyse sous forme de tableau. Bien qu'une norme sur la procédure générale AMDE existe, la conception d'un document particulier peut être adaptée pour répondre aux exigences du projet et de l'application.

La Figure A.1 est un exemple de format pour un document AMDE.

A.2.2 En-tête de document

La partie en-tête de ce formulaire englobe les informations suivantes:

– le système, en qualité de dispositif final, identifie le dispositif pour lequel les effets finaux sont identifiés. Il convient que cette identification soit cohérente avec la terminologie utilisée dans les blocs-diagrammes, schémas et autres dessins;

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Annex A
(informative)

Summary of procedures for FMEA and FMECA

A.1 Steps for performance of analysis

Procedural steps needed to perform an analysis are as follows.

a) Decide whether FMEA or FMECA is required.
b) Define system boundaries for analysis.
c) Understand system requirements and function.
d) Define failure/success criteria.
e) Determine each item's failure modes and their failure effects and record these.
f) Summarize each failure effect.
g) Report findings.

Additional steps to be taken for FMECA are as follows.

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

NOTE Quantification of failure mode and effect frequencies may be undertaken in an FMEA by carrying out steps h), i) and j) at the end of the FMEA.

A.2 FMEA worksheet

A.2.1 Scope of a worksheet

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

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

A.2.2 Worksheet header

The header part of the form captures the following information:

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

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

- le mode de fonctionnement retenu pour l'analyse;
- le dispositif se réfère au dispositif (module, composant ou pièce) étant analysé sur ce document;
- niveau de révision, date et nom de l'analyste coordinateur de l'AMDE ainsi que les noms des membres de l'équipe de base, ce qui fournit des informations supplémentaires pour le contrôle documentaire.

A.2.3 Entrées du document

Les entrées pour «référence du dispositif» et «description du dispositif – fonction» doivent identifier le sujet de l'analyse. Il convient que la référence soit sur le bloc-diagramme ou les autres supports. Une brève description du dispositif et de sa fonction est donnée.

La manière dont le dispositif peut tomber en panne est entrée sous «mode de défaillance». Le Paragraphe 5.2.3 est un guide pour identifier les modes de défaillance potentiels. Le fait d'entrer un identifiant unique («code mode de défaillance») pour chaque défaillance unique du dispositif facilitera le résumé des résultats de l'analyse.

Les causes les plus probables de mode de défaillance sont listées sous «causes de défaillance possibles».

Une description précise des effets du mode de défaillance sur le dispositif en analyse est donnée sous «effet local». Des informations similaires sont entrées dans la colonne «effet du dispositif final» pour indiquer les effets du mode de défaillance sur le dispositif final. Pour certaines analyses AMDE, il est souhaitable d'évaluer l'effet de défaillance à un niveau intermédiaire. Dans ce cas, l'effet sur «l'ensemble suivant, le plus haut» est entré dans une colonne supplémentaire. L'identification des effets des modes de défaillance est discutée en 5.2.5.

Une brève description de la façon dont le mode de défaillance est détecté est indiquée sous «méthode de détection». La méthode de détection peut être faite automatiquement par un dispositif d'essai intégré (DTI) de la conception ou peut nécessiter des procédures de diagnostic par le personnel de maintenance ou d'opération. Il est important d'identifier la méthode de détection pour que l'analyste soit sûr que des actions correctives interviendront.

Les dispositifs de la conception qui atténuent un mode de défaillance particulier, tel que la redondance, sont à noter sous «provisions compensatoires». Il convient que la compensation due à une maintenance spécifique ou à des actions de l'opérateur soit également notée là.

La «Classe de sévérité» identifie le niveau de sévérité tel que déterminé par l'analyste de l'AMDE.

«Fréquence d'apparition» identifie la fréquence d'apparition du mode de défaillance particulier. L'échelle de fréquence est construite pour correspondre à l'application (ex. défaillances par million d'heures, défaillances par distance parcourue, c'est-à-dire 1 000 km, etc.)

L'entrée «Remarques» saisit les informations et recommandations des analystes comme décrit en 5.3.4.

A.2.4 Remarques du document

Il convient que la dernière entrée du document donne des remarques pertinentes pour clarifier les autres. Des actions possibles futures telles que des recommandations pour des améliorations de la conception peuvent être enregistrées et ensuite développées dans le rapport. Cette colonne peut également contenir ce qui suit:

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

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

A.2.3 Worksheet entries

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

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

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

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

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

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

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

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

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

A.2.4 Worksheet remarks

The last worksheet entry should give any pertinent remarks to clarify other entries. Possible future actions such as recommendations for design improvements may be recorded and then amplified in the report. This column may also include the following:

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

a) toutes conditions inhabituelles;
b) les effets de défaillances d'éléments redondants;
c) mise en évidence de dispositifs de conception spécialement critique;
d) toutes remarques pour développer l'entrée;
e) références à d'autres entrées pour des analyses de défaillance séquentielles;
f) exigences de maintenance significatives;
g) causes de défaillance dominantes;
h) effets de défaillance dominants;
i) décisions prises, par exemple à la revue de conception.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

a) any unusual conditions;
b) effects of redundant element failures;
c) recognition of specially critical design features;
d) any remarks to amplify the entry;
e) references to other entries for sequential failure analysis;
f) significant maintenance requirements;
g) dominant failure causes;
h) dominant failure effects;
i) decisions taken, e.g. at design review.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

AMDE

Dispositif final Durée de fonctionnement			Article Révision:					Etabli par: Date:			
Réf. dispositif	**Description du dispositif – fonction**	**Mode de défaillance**	**Code du mode de défaillance**	**Causes de défaillance possibles**	**Effet local**	**Effet final**	**Méthodes de détection**	**Provision compensatoire contre les défaillances**	**Classe de sévérité**	**Fréquence ou probabilité d'apparition**	**Remarques**

Figure A.1 – Exemple de formulaire de document AMDE

IEC 2643/05

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

FMEA

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

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

IEC 2643/05

Annexe B
(informative)

Exemples d'analyses

B.1 Exemple 1 – AMDE pour une partie de l'électronique automobile avec calcul NPR

La Figure B.1 illustre une petite partie d'une très large AMDEC menée pour un produit automobile. L'assemblage analysé est l'alimentation, et seulement ses connexions à la batterie.

Le câblage de la batterie comporte une diode D1 et un condensateur C9 connectant le « plus » de la batterie à la masse. La diode est en polarisation inverse de telle sorte que le pôle négatif de la batterie est connecté au dispositif, cette tension négative pouvant court-circuiter à la masse, protégeant ainsi le dispositif de dommages. Le condensateur est un filtre EMI. Si l'un de ces composants est en court-circuit avec la masse, la batterie le sera aussi, ce qui peut conduire à vider la batterie du véhicule. Une telle défaillance est probablement sans avertissement et le fait de « devoir rentrer à pied » est considérer comme un danger dans l'industrie automobile. En conséquence, pour les modes de défaillance « court-circuit » des deux composants, le classement S est 10. Les apparitions ont été calculées à partir des taux de défaillance des composants sous les contraintes respectives pour la durée de vie du véhicule, et ensuite portées sur l'échelle O de l'AMDE automobile. La détection est très faible, étant donné que le court-circuit de chacun des composants peut être immédiatement constaté en essai – produit non opérationnel.

La mise en circuit ouvert de l'un ou l'autre des composants ci-dessus ne peut causer aucun dommage au produit, sauf que l'ouverture de la diode entraîne l'absence de protection en inverse de la batterie, et que l'ouverture du condensateur entraînera l'absence de filtrage EMI – bruit possible pour les autres équipements du véhicule.

Une bobine L1 est placée entre la batterie et le circuit du dispositif, principalement pour filtrer. Si la bobine est ouverte, le dispositif peut ne pas être opérationnel et la batterie être déconnectée. Le dispositif ne sera pas opérationnel, de sorte que l'alarme visuelle ne sera pas allumée. Les bobines ont un taux de défaillance très faible, de sorte que le classement de l'apparition est 2.

La résistance R91 apporte la tension de la batterie aux transistors de commutation; si elle est ouverte, elle rend le dispositif non opérationnel, ce qui a aussi une sévérité égale à 9. Puisque les résistances ont un très faible taux de défaillance, le classement de l'apparition est 2. Celui de la détection est 1, puisque le dispositif sera non opérationnel.

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Annex B
(informative)

Examples of analyses

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

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

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

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

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

Dispositif/Fonction			Mode de défaillance potentiel	Effet(s) potentiel(s) de la défaillance		SÉVÉR	CLASSE	Cause(s) potentielle/ Mécanisme(s) de défaillance	Cause(s) détaillée/ Mécanisme(s) de défaillance	Appar	Contrôle de prévention actuel en conception	Contrôle de détection actuel en conception	Détec	NPR	Action(s) recom-mandée(s)	Respon-sabilité et date cible de clôture	Résultats de l'action				
Sous-système	Assem-blage	Com-posant		Effet local	Effet final												Actions prises	Sévér	Appar	Détec	NPR
Alimentation																					
	V1																				
		D1	Court-circuit	+ de la tension de batterie court-circuitée à la masse	Batterie vidée, « retour à pied »	10		Défaut inhérent au composant	Matériau claqué	3	Sélection d'une qualité et d'un point de consigne plus élevés	Essai de validation et de fiabilité	1	30							
		D1	Circuit ouvert	Pas de protection de tension inverse	Non détectable	2		Défaut inhérent au composant	Soudure ou semi-conducteur ou cassure	3	Sélection d'une qualité et d'un point de consigne plus élevés	Essai de validation et de fiabilité	2	12							
		C9	Court-circuit	+ de la tension de batterie court-circuitée à la masse	Batterie vidée, « retour à pied »	10		Défaut inhérent au composant	Claquage diélectrique ou cassure	3	Sélection d'une qualité et d'un point de consigne plus élevés	Essai de validation et de fiabilité	1	30							
		C9	Circuit ouvert	Pas de filtrage EMI	Fonction-nement du dispositif hors des spécifica-tions	2		Défaut inhérent au composant	Diélectrique ouvert, fuite, trou ou fissure	2	Sélection d'une qualité et d'un point de consigne plus élevés	Essai de validation et de fiabilité	1	4							
		L1	Circuit ouvert	Pas de V1 -	Dispositif non opération-nel. Pas de visualisation d'alarme	9		Défaut inhérent au composant	Matériau claqué	2	Sélection d'une qualité et d'un point de consigne plus élevés	Essai de validation et de fiabilité	1	18							
		R91	Circuit ouvert	Pas de tension pour le circuit de commu-tation	Dispositif non opéra-tionnel. Pas de visuali-sation d'alarme	9		Défaut inhérent au composant	Soudure ou matériau fissuré	2	Sélection d'une qualité et d'un point de consigne plus élevés	Essai de validation et de fiabilité	1	18							

Figure B.1 – FMEA pour une partie de dispositif électronique d'automobile avec calcul de NPR

IEC 2644/05

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

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

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

IEC 2644/05

B.2 Exemple 2 – AMDE pour sous-système d'un ensemble générateur-moteur

Cet exemple illustre l'application de la technique AMDE à un système générateur-moteur (G-M). Le but de cette étude était confiné à ce système uniquement et ne concernait pas les effets de défaillance de charges fournies avec courant électrique de l'ensemble G-M ou tout autre effet externe ou défaillance. Par conséquent, cela définit les limites de l'analyse. L'exemple, montré partiellement, illustre comment le système est représenté sous forme de bloc-diagramme hiérarchique. Les sous-divisions initiales identifient cinq sous-systèmes (voir Figure B.2) et une de celle-ci, l'enveloppe chauffante, la ventilation et le système de refroidissement, est développée au travers de niveaux plus bas de la structure hiérarchique au niveau des composants auquel il a été décidé de commencer l'AMDE (voir Figure B.3). Les bloc-diagrammes montrent aussi le système de numérotation adopté qui a été utilisé comme référence croisée avec les documents AMDE.

Un exemple de feuille de travail est montré pour un des sous-systèmes de l'ensemble G-M (voir Figure B.4), qui est généralement conforme au format recommandé dans cette norme.

Un pré-requis essentiel pour une telle AMDEC est la définition et la classification de la sévérité des effets et défaillances sur le système G-M complet. Pour l'application particulière du système exemple, ceux-ci sont définis dans le Tableau B.1.

Tableau B.1 – Définition et classification de la sévérité des effets de défaillance sur le système G-M complet

Niveau	Sévérité	Description
5	Catastrophique	Défaillance à produire du courant pour le reste de la mission
4	Critique	Dégradation du système pour le reste de la mission
3	Principal	Perte de production du courant due à coupure forcée jusqu'à réparation
2	Mineur	Dégradation temporaire du système en attendant réparation possible
1	Effet négligeable	Pas de perte ou de dégradation significative de la capacité de production

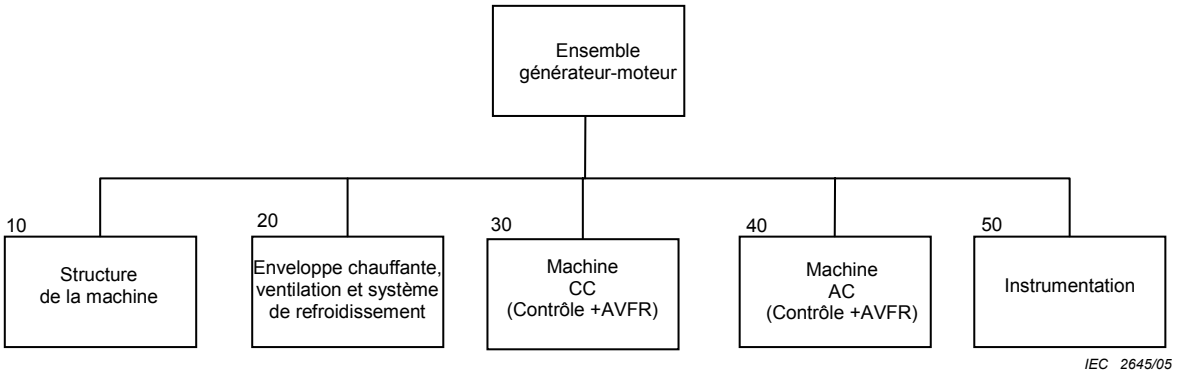

Figure B.2 – Diagramme des sous-systèmes d'un ensemble générateur-moteur

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

B.2 Example 2 – FMEA for sub-subsystem of a motor-generator set

This example illustrates the application of the FMEA technique to a motor-generator (M-G) system. The objective of the study was confined to that system only and was not concerned with the effects of failure on any loads supplied with electrical power from the M-G set or any other external effects of failures. This therefore defines the boundaries of the analysis. The example, shown in part only, illustrates how the system was represented in a hierarchical block diagram form. Initial sub-division identified five subsystems (see Figure B.2) and one of these, the enclosure heating, ventilation and cooling system, is developed through lower levels of the hierarchical structure to the component level at which it was decided to start the FMEA (see Figure B.3). The block diagrams also show the numbering system adopted that was used as a cross reference with the FMEA worksheets.

One example of a worksheet is shown for one of the sub-subsystems of the M-G set (see Figure B.4), which generally conforms to the format recommended in this standard.

An essential prerequisite for such an FMEA is the definition and classification of the severity of the effects of failures on the complete M-G system. For the particular application of the example system these were defined as in Table B.1.

Table B.1 – Definition and classification of the severity of the effects of failures on the complete M-G system

Level	Severity	Description
5	Catastrophic	Failure to generate power for remainder of mission
4	Critical	System degradation for remainder of mission
3	Major	Loss of power generation due to forced outage until repaired
2	Minor	Temporary system degradation until convenient to repair
1	Negligible	No loss or significant degradation of generating capability

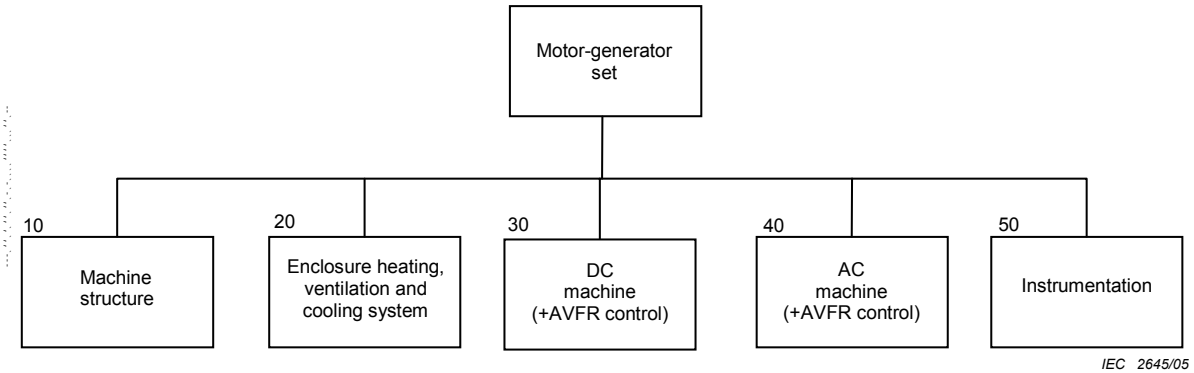

Figure B.2 – Diagram of subsystems of a motor generator set

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

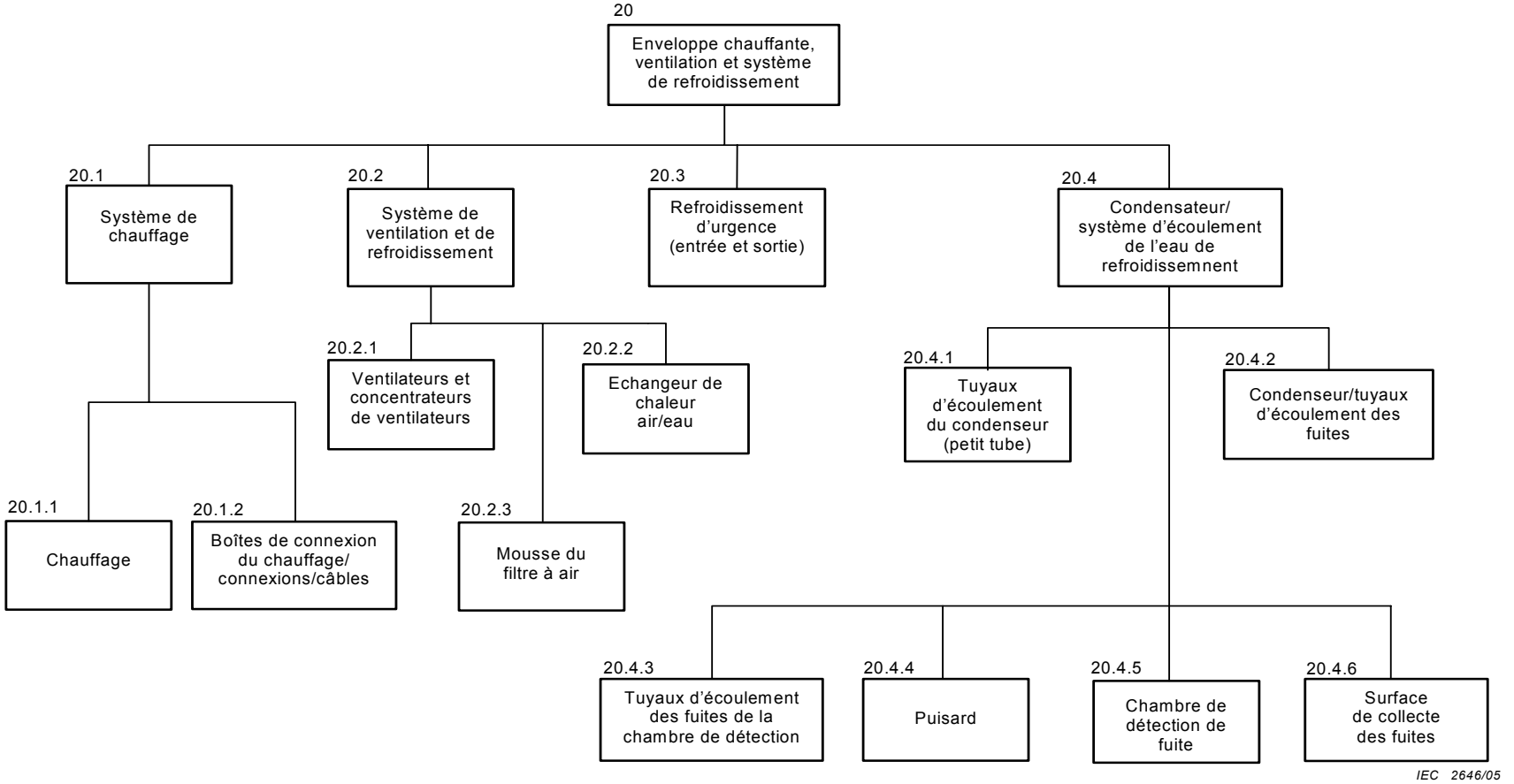

Figure B.3 – Diagramme d'enveloppe chauffante, ventilation et systèmes de refroidissement

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

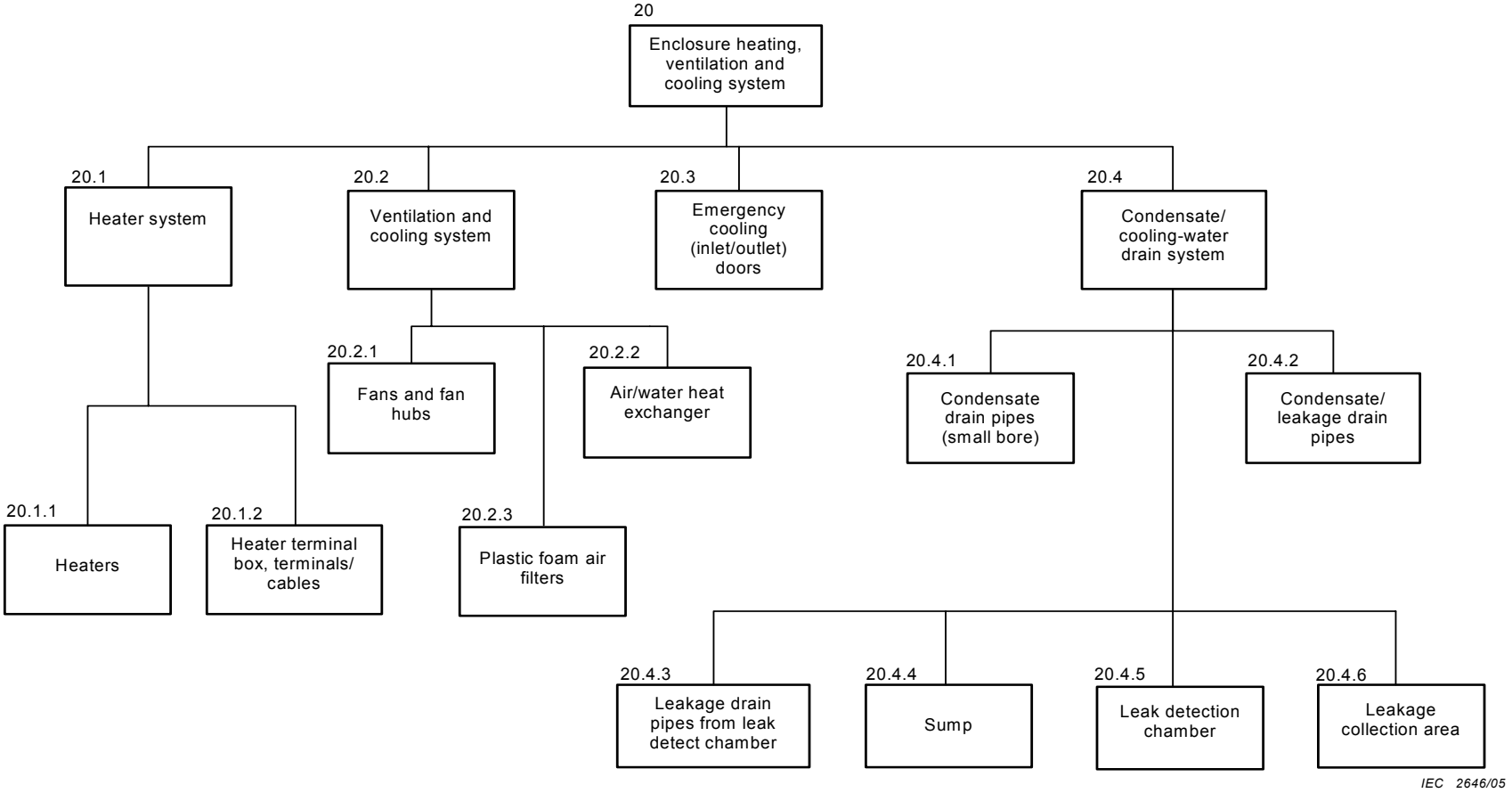

Figure B.3 – Diagram of enclosure heating, ventilation and cooling systems

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

Sous-système –20 Enveloppe chauffante, ventilation et système de refroidissement												
Réf.	**Composant**	**Fonction**	**Mode de défaillance**	**Effet de la défaillance**	**Méthode de détection ou symptôme**	**Redondance fournie**	**Taux du mode de défaillance / niveau de sévérité F/ Mhr**					**Remarques**
							1	2	3	4	5	
20.1	Système de chauffage (12 arrêts – 6 arrêts à chaque fin (uniquement en utilisation quand la machine est non opérationnelle)	Toutes										NOTE La machine peut être en surchauffe si les chauffages ne commutent pas à l'état Arrêt automatiquement quand elle tourne
20.1.1	Chauffages	Chauffer l'enveloppe	a) Circuit ouvert, brûle du chauffage b) Court-circuit ou panne de terre due au claquage de l'isolation	Chauffage réduit Perte de tout chauffage – condensation possible	a) Indication de température <5° au-dessus de l'ambiant b) Alimentation, fusible, ou surveillance du coupe-circuit	Tous en parallèle, pas de redondance d'alimentation				1,2 0,3		Il convient qu'une faute de terre n'entraîne pas la défaillance du système
20.1.2	Boîtier de terminaison des chauffage, terminaisons, câble	Connecter l'alimentation aux chauffages	a) Circuit ouvert des terminaisons ou des câbles qui peuvent rendre défaillant un, trois, six ou tous les chauffages b) Court-circuit des terminaisons (cheminement)	Perte ou réduction du chauffage – condensation Perte du chauffage – condensation	Température <5° au-dessus de l'ambiant Alimentation surveillée					0,5 Néglig.		
						Totaux				2,0		

IEC 2647/05

Figure B.4 – AMDE pour sous-système 20

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

Subsystem – 20 Enclosure heating, ventilation and cooling system												
Ref.	**Component**	**Function**	**Failure mode**	**Failure effect**	**Detection method or symptom**	**Redundancy provided**	**Mode failure rate severity level F/Mhr**					**Remarks**
							1	2	3	4	5	
20.1	Heater system (12 off – 6 off at each end (only in use when machine non-operational)	All										NOTE: the machine may overheat if heaters do not turn off automatically when running
20.1.1	Heaters	To heat up enclosure	a) o/c, burnt out heater b) s/c or earth fault due to insulation breakdown	Reduced heating Loss of all heating – possible condensation	a) Temp. indication <5° above ambient b) Supply, fuse, or circuit breaker monitored	All in parallel, no supply redundancy				1,2 0,3		One earth fault should not fail system
20.1.2	Heater terminal box, terminals, cable	Connect supply to heaters	a) o/c terminal or cable can fail one, three, six or all heaters b) s/c terminals (tracking)	Loss or reduction of heating – condensation Loss of all heating – condensation	Temp. <5° above ambient Supply monitored					0,5 neglig.		
						Totals				2,0		

Figure B.4 – FMEA for sub-system 20

IEC 2647/05

B.3 Exemple 3 – AMDE pour un procédé de fabrication

L'AMDEC de fabrication ou de procédé considère chacun des procédés impliqués dans la fabrication du dispositif concerné; elle regarde ce qui pourrait aller mal, quelles mesures de protection existent contre les défaillances, la fréquence d'apparition de celles-ci, et comment elles peuvent être supprimées en re-concevant le dispositif ou le procédé. Le but est de concentrer l'attention sur les problèmes possibles (ou connus) dans le maintien ou l'atteinte du niveau de qualité requis pour le produit fini. Il est vivement conseillé aux assembleurs de pièces complexes tels que les moteurs de voitures d'insister pour que les fournisseurs de composants mènent de telles analyses, mais les fabricants de composants sont généralement les principaux bénéficiaires. L'exercice oblige à réexaminer la méthodologie bien établie dans la fabrication et conduit souvent à réduire le coût.

Le format est en principe similaire à celui pour un produit AMDEC mais certaines modifications sont imposées par des exigences légèrement différentes (voir Figure B.5). La mesure de la criticité est l'ordre de priorité d'action (APN) mais est essentiellement équivalent à l'ordre de priorité du risque (NPR) discuté ci-dessus. Le procédé AMDEC examine comment des défauts et défectuosités peuvent survenir et atteindre les clients, ou être trouvés par des procédures de contrôle qualité. Il n'examine pas comment le produit peut tomber en panne due à l'usure ou un fonctionnement impropre. Il y a inévitablement des chevauchements, parce que certains défauts affectent la durabilité des composants en service, alors que d'autres provoquent des défaillances immédiates ou précoces.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

B.3 Example 3 – FMECA for a manufacturing process

A manufacturing or process FMECA considers each of the processes involved in the manufacture of the item concerned; it considers what could go wrong, what safeguards exist against the failure, how often it might occur, and how it might be eliminated by redesign of the item or the process. The objective is to concentrate attention on possible (or known) problems in sustaining or achieving required output quality. Assemblers of complex goods such as motor cars are well advised to insist that their component suppliers carry out such analyses, but the component manufacturers are usually the principal beneficiaries. The exercise forces a re-examination of entrenched methodology in manufacture and seldom fails to lead to cost improvements.

The format is basically similar to that for a product FMECA but some changes are forced by the slightly different requirements (see Figure B.5). The criticality metric is the Action Priority Number (APN) but it is essentially equivalent to the Risk Priority Number (RPN) discussed above. The process FMECA examines how defects and defectives can arise and reach customers, or be found by quality control procedures. It does not examine how the product may fail in service due to wear or improper operation. There is inevitably some overlap, because some defects affect the durability of the components in service, while others cause immediate or early failure.

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

								Conditions existantes						Conditions révisées			
Réf.	**Procédé**	**Mode de défaillance**	**Effet sur**	**Effet potentiel**	**V**	**Cause potentielle**	**Contrôles existants**	**App**	**Sev**	**Det**	**NPR**	**Action recommandée**	**Action prise**	**App**	**Sev**	**Det**	**APN**
01-01-01	Insertion	Taille ou angle de pliage de l' épaulement incorrect	i)a	Insertion sans charge sur la puce Productivité réduite		Procédé de fabrication ou contrôle qualité défectueux	Producteur et plans d'échantillon-nage d'acceptation	1	9	9	81	Revue des plans d'échantillon-nage Ségrégation des stocks défec-tueux et des stocks corrects Formation des opérateurs d'assemblage.					
02			i)b	Insertion mal alignée													
03			i)a	Epaisseur incorrecte de la jupe entourant l'insert													
04			iv)b	Performance réduite													
05			iv)c	Durée de vie réduite													
01-02-01	Insertion	Flash de dépôt de nickel défectueux	ii)a	Corrosion Rejet à l'étape de finition			Inspection visuelle pendant le plan d'échantillon-nage d'acceptation	5	6	1	30	Introduire des instructions dans l'inspec-tion par échan-tillonnage pour effectuer un contrôle visuel pour le dépôt					
01-03-01	Insertion	Inadéquat état de surface	1)a	Débit de métal défectueux. Epaisseur incorrecte. Arrachement.		Procédé de fabrication ou contrôle qualité défectueux	Inspection visuelle pendant le plan d'échantillon-nage d'acceptation	2	8	6	96	Introduire des instructions dans l'inspec-tion par échan-tillonnage pour effectuer un contrôle visuel pour le dépôt					
02			ii)a	Epaisseurs trop faibles détectées pendant l'usinage Arrachement													
03			iv)a	Durée de vie réduite													

Code d'effet :
Effet sur le procédé de moulage
Effet sur le procédé de finition
Effet sur l'assemblage
Effet sur l'utilisateur final

Code de criticité :
Occ = Prob. d'apparition × 10
Sev = Sévérité de l'effet sur une échelle de 1 à 10
Det = prob. de ne pas être détecté avant d'arriver chez le client × 10
APN = Nombre de Risque de Priorité = Occ × Sev × Det

IEC 2648/05

Figure B.5 – Partie du processus AMDEC pour coulage d'aluminium par machine

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

								Existing conditions						Revised conditions			
Ref.	**Process**	**Failure mode**	**Effect on**	**Potential effect**	**V**	**Potential cause**	**Existing controls**	**Occ**	**Sev**	**Det**	**RPN**	**Recommended action**	**Action taken**	**Occ**	**Sev**	**Det**	**APN**
01-01-01	Inserts	Incorrect size or shoulder bend angles	i)a	Inserts without load onto die. Reduced productivity.		Poor manufacture or quality control	Producer and acceptance sampling plans	1	9	9	81	Review of sampling plans. Segregation of defective stock from good stock. Training assemblers.					
02			i)b	Insert mis-aligned.													
03			i)a	Incorrect thickness of skirt surrounding insert.													
04			iv)b	Reduced performance.													
05			iv)c	Reduced life.													
01-02-01	Inserts	Poor flash nickel plating	ii)a	Corrosion. Rejected at finishing stage			Visual inspection during acceptance sampling plan	5	6	1	30	Include instructions in sampling inspection to carry out visual check for correct plating.					
01-03-01	Inserts	Inadequate face scoring	i)a	Poor metal flow. Incorrect wall thickness. Scrap.		Poor manufacture or quality control	Visual inspection during acceptance sampling	2	8	6	96	Include instructions in sampling inspection to carry out visual check for correct plating					
02			ii)a	Thin walls found during machining. Scrap													
03			iv)a	Reduced life													

Effect code:
Effect on the casting processq
Effect on the finishing process
Effect on the assembler
Effect on the end user

Criticality code:
Occ = Prob. of occurrence × 10
Sev = Severity of effect on 1 – 10 scale
Det = Prob. not detected before reaching customer × 10
APN = Action Priority Number = Occ × Sev × Det

Figure B.5 – Part of a process FMECA for machined aluminium casting

IEC 2648/05

Bibliographie

[1] BS 5760-5:1991, *Reliability of systems equipment and components – Part 5: Guide to failure modes, effects and criticality analysis (FMEA and FMECA)*

[2] SAE J1739:2000, *Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery*

[3] SAE ARP5580:2001, *Failure Modes, Effects, and Criticality Analysis Procedures*

[4] AIAG, *Potential Failure Mode and Effects Analysis*, Third Edition, 2001

[5] M. Krasich, *Fault Tree Analysis for Failure Modes Identification and Product Reliability Improvement*, Tutorial presented at the Reliability and Maintainability Symposium; Tutorial Proceedings of 2002, 2003, and 2005.

[6] J. Bowles, *An Assessment of NPR Prioritization in a Failure Modes Effects and Criticality Analysis*, technical paper presented at the Reliability and Maintainability Symposium, 2003.

[7] CEI 60050(191):1990, *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

[8] CEI 60300-1, *Gestion de la sûreté de fonctionnement – Partie 1: Gestion du programme de sûreté de fonctionnement* (disponible en anglais seulement)

[9] CEI 60300-2, *Gestion de la sûreté de fonctionnement – Partie 2: Lignes directrices pour la gestion de la sûreté de fonctionnement*

[10] CEI 60300-3-9, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 9: Analyse du risque des systèmes technologiques*

[11] CEI 61160, *Revue de conception formalisée*

[12] CEI 61165, *Application des techniques de Markov*

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

[14] ISO 9000 :2000, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Bibliography

[1] BS 5760-5:1991, R*eliability of systems, equipment and components – Part 5: Guide to failure modes, effects and criticality analysis (FMEA and FMECA)*

[2] SAE J1739:2000, *Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery*

[3] SAE ARP5580:2001, *Failure Modes, Effects, and Criticality Analysis Procedures*

[4] AIAG, *Potential Failure Mode and Effects Analysis*, Third Edition, 2001

[5] M. Krasich, *Fault Tree Analysis for Failure Modes Identification and Product Reliability Improvement*, tutorial presented at the Reliability and Maintainability Symposium; Tutorial Proceedings of 2002, 2003, and 2005.

[6] J. Bowles, *An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis*, technical paper presented at the Reliability and Maintainability Symposium, 2003.

[7] IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

[8] IEC 60300-1, *Dependability management – Part 1: Dependability management systems*

[9] IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management*

[10] IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*

[11] IEC 61160, *Formal design review*

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

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

[14] ISO 9000:2000, *Quality management systems – Fundamentals and vocabulary*

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

Enquête sur les normes

La CEI ambitionne de vous offrir les meilleures normes possibles. Pour nous assurer que nous continuons à répondre à votre attente, nous avons besoin de quelques renseignements de votre part. Nous vous demandons simplement de consacrer un instant pour répondre au questionnaire ci-après et de nous le retourner par fax au +41 22 919 03 00 ou par courrier à l'adresse ci-dessous. Merci !

Centre du Service Clientèle (CSC)

Commission Electrotechnique Internationale
3, rue de Varembé
1211 Genève 20
Suisse

ou

Télécopie: **CEI**/CSC +41 22 919 03 00

Nous vous remercions de la contribution que vous voudrez bien apporter ainsi à la Normalisation Internationale.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Centre du Service Clientèle (CSC)
Commission Electrotechnique Internationale
3, rue de Varembé
1211 GENÈVE 20
Suisse

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS Not for Resale

Q1 Veuillez ne mentionner qu'**UNE SEULE NORME** et indiquer son numéro exact: (*ex. 60601-1-1)*

.....

Q2 En tant qu'acheteur de cette norme, quelle est votre fonction?
(cochez tout ce qui convient)
Je suis le/un:

agent d'un service d'achat ❑
bibliothécaire ❑
chercheur ❑
ingénieur concepteur ❑
ingénieur sécurité ❑
ingénieur d'essais ❑
spécialiste en marketing ❑
autre(s).....

Q3 Je travaille:
(cochez tout ce qui convient)

dans l'industrie ❑
comme consultant ❑
pour un gouvernement ❑
pour un organisme d'essais/ certification ❑
dans un service public ❑
dans l'enseignement ❑
comme militaire ❑
autre(s).....

Q4 Cette norme sera utilisée pour/comme
(cochez tout ce qui convient)

ouvrage de référence ❑
une recherche de produit ❑
une étude/développement de produit ❑
des spécifications ❑
des soumissions ❑
une évaluation de la qualité ❑
une certification ❑
une documentation technique ❑
une thèse ❑
la fabrication ❑
autre(s).....

Q5 Cette norme répond-elle à vos besoins:
(une seule réponse)

pas du tout ❑
à peu près ❑
assez bien ❑
parfaitement ❑

Q6 Si vous avez répondu PAS DU TOUT à Q5, c'est pour la/les raison(s) suivantes:
(cochez tout ce qui convient)

la norme a besoin d'être révisée ❑
la norme est incomplète ❑
la norme est trop théorique ❑
la norme est trop superficielle ❑
le titre est équivoque ❑
je n'ai pas fait le bon choix ❑
autre(s) .....

Q7 Veuillez évaluer chacun des critères ci-dessous en utilisant les chiffres
(1) inacceptable,
(2) au-dessous de la moyenne,
(3) moyen,
(4) au-dessus de la moyenne,
(5) exceptionnel,
(6) sans objet

publication en temps opportun .....
qualité de la rédaction.....
contenu technique .....
disposition logique du contenu .....
tableaux, diagrammes, graphiques, figures.....
autre(s) .....

Q8 Je lis/utilise: *(une seule réponse)*

uniquement le texte français ❑
uniquement le texte anglais ❑
les textes anglais et français ❑

Q9 Veuillez nous faire part de vos observations éventuelles sur la CEI:

.....
.....
.....
.....
.....
.....

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS
Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS

Not for Resale

ISBN 2-8318-8425-X

ICS 03.120.01; 03.120.30; 21.020

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND

Copyright International Electrotechnical Commission
Provided by IHS under license with IEC
No reproduction or networking permitted without license from IHS

Not for Resale