NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60601-1-4

Edition 1.1

2000-04

Edition 1:1996 consolidée par l'amendement 1:1999
Edition 1:1996 consolidated with amendment 1:1999

Appareils électromédicaux –

Partie 1-4:
Règles générales de sécurité –
Norme Collatérale:
Systèmes électromédicaux programmables

Medical electrical equipment –

Part 1-4:
General requirements for safety –
Collateral Standard:
Programmable electrical medical systems



Numéro de référence
Reference number
CEI/IEC 60601-1-4:1996+A1:1999

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
60601-1-4

Edition 1.1

2000-04

Edition 1:1996 consolidée par l'amendement 1:1999
Edition 1:1996 consolidated with amendment 1:1999

Appareils électromédicaux –

Partie 1-4:
Règles générales de sécurité –
Norme Collatérale:
Systèmes électromédicaux programmables

Medical electrical equipment –

Part 1-4:
General requirements for safety –
Collateral Standard:
Programmable electrical medical systems

© IEC 2000 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 CG

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

Pages

AVANT-PROPOS 4
INTRODUCTION 8

Articles

SECTION 1: GÉNÉRALITÉS

1 Domaine d'application, objet et référence à d'autres normes 10
1.201 Domaine d'application 10
1.202 Objet 10
1.203 Références à d'autres normes 12
2 Terminologie et définitions 12
2.201 Termes définis 12
2.202 Degrés d'exigence et termes divers 16
6 Identification, marquage et documentation 16
6.8 DOCUMENTS D'ACCOMPAGNEMENT 16

SECTION 9: FONCTIONNEMENT ANORMAL ET CONDITIONS DE DÉFAUT; ESSAIS D'ENVIRONNEMENT

52 Fonctionnement anormal et conditions de défaut 18
52.201 Documentation 18
52.202 Plan de gestion des RISQUES 22
52.203 CYCLE DE DÉVELOPPEMENT 22
52.204 Traitement de la gestion des RISQUES 24
52.205 Qualification du personnel 28
52.206 Spécification des prescriptions 28
52.207 Architecture 28
52.208 Conception et réalisation 30
52.209 VÉRIFICATION 30
52.210 VALIDATION 30
52.211 Modification 32
52.212 Evaluation 32

Annexes

AAA – Terminologie – Index des termes définis 34
BBB – Justifications 36
CCC – Notion de RISQUE 40
DDD – CYCLE DE DÉVELOPPEMENT 52
EEE – Exemples de structures SEMP/SSEP 60
FFF – Bibliographie 64

Figures

201 – Organigramme du FICHIER DE GESTION DES RISQUES et du RELEVÉ DE GESTION DES RISQUES 20
CCC.1 – Diagramme du RISQUE 42
CCC.2 – Traitement de la gestion des RISQUES 46
DDD.1 – Modèle de CYCLE DE DÉVELOPPEMENT pour un SEMP 54
EEE.1 – Exemples de structures SEMP/SSEP 62

Tableau DDD.1 – Proposition de corrélation entre les documents prescrits et les phases du CYCLE DE DÉVELOPPEMENT 58

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

CONTENTS

Page

FOREWORD 5
INTRODUCTION 9

Clause

SECTION 1: GENERAL

1 Scope, object and relationship to other standards 11
1.201 Scope 11
1.202 Object 11
1.203 Relationship to other standards 13
2 Terminology and definitions 13
2.201 Defined terms 13
2.202 Degrees of requirements and miscellaneous terms 17
6 Identification, marking and documents 17
6.8 ACCOMPANYING DOCUMENTS 17

SECTION 9: ABNORMAL OPERATION AND FAULT CONDITIONS; ENVIRONMENTAL TESTS

52 Abnormal operation and fault conditions 19
52.201 Documentation 19
52.202 RISK management plan 23
52.203 DEVELOPMENT LIFE-CYCLE 23
52.204 RISK management process 25
52.205 Qualification of personnel 29
52.206 Requirement specification 29
52.207 Architecture 29
52.208 Design and implementation 31
52.209 VERIFICATION 31
52.210 VALIDATION 31
52.211 Modification 33
52.212 Assessment 33

Annexes

AAA – Terminology – Index of defined terms 35
BBB – Rationale 37
CCC – RISK concepts 41
DDD – DEVELOPMENT LIFE-CYCLE 53
EEE – Examples for PEMS/PESS structures 61
FFF – Bibliography 65

Figures

201 – Content of RISK MANAGEMENT FILE and RISK MANAGEMENT SUMMARY 21
CCC.1 – RISK chart 43
CCC.2 – RISK management process 47
DDD.1 – A DEVELOPMENT LIFE-CYCLE model for PEMS 55
EEE.1 – Examples of PEMS/PESS structures 63

Table DDD.1 – Suggested correlation of the documentation requirement to the DEVELOPMENT LIFE-CYCLE phases 59

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

_____

APPAREILS ÉLECTROMÉDICAUX –

Partie 1-4: Règles générales de sécurité – Norme Collatérale: Systèmes électromédicaux programmables

AVANT-PROPOS

1) La CEI (Commission Électrotechnique Internationale) 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. 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 intéressés sont représentés dans chaque comité d'études.
3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale 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 60601-1-4 a été établie par le comité d'études 62 de la CEI: Equipements électriques dans la pratique médicale. Elle constitue une Norme Collatérale à la CEI 60601-1: *Appareils électromédicaux – Première partie: Règles générales de sécurité*, appelée Norme Générale dans la suite du texte.

Dans la série des publications CEI 60601, les Normes Collatérales spécifient des règles générales de sécurité applicables à

– un groupe d'APPAREILS ÉLECTROMÉDICAUX (par exemple des appareils de radiologie);
– une caractéristique commune à tous les APPAREILS ÉLECTROMÉDICAUX non traitée complètement dans la Norme Générale (par exemple la compatibilité électromagnétique).

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

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

_____

MEDICAL ELECTRICAL EQUIPMENT –

Part 1-4: General requirements for safety – Collateral Standard: Programmable electrical medical systems

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60601-1-4 has been prepared by IEC technical committee 62: Electrical equipment in medical practice. It constitutes a Collateral Standard to IEC 60601-1: *Medical electrical equipment – Part 1: General requirements for safety*, hereinafter referred to as the General Standard.

In the IEC 60601 series of publications, Collateral Standards specify general requirements for safety applicable to:

– a group of MEDICAL ELECTRICAL EQUIPMENT (e.g. radiological equipment);
– a specific characteristic of all MEDICAL ELECTRICAL EQUIPMENT, not fully addressed in the General Standard (e.g. electromagnetic compatibility).

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

La présente version consolidée de la Norme Collatérale CEI 60601-1-4 comprend la première édition (1996) [documents 62/83/FDIS et 62/87/RVD] et son amendement 1 (1999) [documents 62/114/FDIS et 62/120/RVD].

Le contenu technique de cette version consolidée est donc identique à celui de l'édition de base et à son amendement; cette version a été préparée par commodité pour l'utilisateur.

Elle porte le numéro d'édition 1.1.

Une ligne verticale dans la marge indique où la publication de base a été modifiée par l'amendement 1.

La numérotation des sections, articles et paragraphes de la présente Norme Collatérale correspond à celle de la Norme Générale.

Les paragraphes et figures complémentaires à ceux de la Norme Générale sont numérotés à partir de 201. Les annexes complémentaires sont appelées AAA, BBB, etc., et les points complémentaires aaa), bbb), etc.

L'annexe AAA fait partie intégrante de cette Norme Collatérale.

Les annexes BBB, CCC, DDD, EEE et FFF sont données uniquement à titre d'information.

Dans la présente Norme Collatérale, les caractères suivants sont utilisés:

– prescriptions dont la conformité peut être vérifiée par un essai, et définitions: caractères romains;
– explications, conseils, énoncés de portée générale, exceptions et références: petits caractères romains;
– *modalités d'essais et titres des paragraphes: caractères italiques;*
– TERMES DEFINIS A L'ARTICLE 2 DE LA NORME GENERALE, DE LA CEI 60601-1-1 ET DE LA PRESENTE NORME COLLATERALE OU DANS LA CEI 60788: PETITES CAPITALES.

Les prescriptions sont suivies de la spécification des essais correspondants.

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

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

This consolidated version of Collateral Standard IEC 60601-1-4 consists of the first edition (1996) [documents 62/83/FDIS and 62/87/RVD] and its amendment 1 (1999) [documents 62/114/FDIS and 62/120/RVD].

The technical content is therefore identical to the base edition and its amendment and has been prepared for user convenience.

It bears the edition number 1.1.

A vertical line in the margin shows where the base publication has been modified by amendment 1.

The numbering of sections, clauses and subclauses of this Collateral Standard corresponds with that of the General Standard.

Subclauses and figures which are additional to those of the General Standard are numbered starting from 201; additional annexes are lettered AAA, BBB, etc., and additional items aaa), bbb), etc.

Annex AAA forms an integral part of this Collateral Standard.

Annexes BBB, CCC, DDD, EEE and FFF are for information only.

In this Collateral Standard, the following print types are used:

– requirements, compliance with which can be tested, and definitions: roman type;
– explanations, advice, general statements, exceptions and references: smaller type;
– *test specifications and headings of subclauses: italic type;*
– TERMS DEFINED IN CLAUSE 2 OF THE GENERAL STANDARD OR OF IEC 60601-1-1 OR OF THIS COLLATERAL STANDARD OR IN IEC 60788: SMALL CAPITALS.

The requirements are followed by specifications for the relevant tests.

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

INTRODUCTION

Les ordinateurs sont de plus en plus utilisés dans les APPAREILS ÉLECTROMÉDICAUX, souvent dans des rôles critiques de sécurité. L'emploi des techniques de l'informatique dans les APPAREILS ÉLECTROMÉDICAUX introduit un niveau de complexité qui n'est dépassé que par celui des systèmes biologiques des PATIENTS que ces APPAREILS ÉLECTROMÉDICAUX sont destinés à examiner et/ou à traiter. Cette complexité explique que des défaillances systématiques peuvent échapper aux limites pratiques acceptables des essais. En conséquence, la présente norme de sécurité va au-delà des essais et des évaluations traditionnelles des APPAREILS ÉLECTROMÉDICAUX terminés et comprend des prescriptions pour le développement des APPAREILS ÉLECTROMÉDICAUX. L'essai du produit fini n'est pas, en soi, suffisant pour qualifier la SÉCURITÉ des APPAREILS ÉLECTROMÉDICAUX complexes.

La présente norme est une Norme Collatérale à la Norme Générale. Elle prescrit qu'un traitement soit suivi et qu'un enregistrement de ce traitement soit effectué pour vérifier la SÉCURITÉ des APPAREILS ÉLECTROMÉDICAUX comprenant des SOUS-SYSTÈMES ÉLECTRONIQUES PROGRAMMABLES. Les notions de gestion des RISQUES et de CYCLE DE DÉVELOPPEMENT, qui sont la base de la présente norme, peuvent également être utiles pour le développement des APPAREILS ÉLECTROMÉDICAUX ne comportant pas de SOUS-SYSTÈME ÉLECTRONIQUE PROGRAMMABLE.

L'application efficace de la norme exigera, en raison du sujet traité, des compétences dans les domaines suivants:

- application de l'APPAREIL ÉLECTROMÉDICAL spécifique en insistant sur les problèmes de SÉCURITÉ;
- traitement de développement de l'APPAREIL ÉLECTROMÉDICAL;
- méthodes assurant la SÉCURITÉ;
- techniques de l'analyse des RISQUES et de la maîtrise des RISQUES.

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

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

INTRODUCTION

Computers are increasingly used in MEDICAL ELECTRICAL EQUIPMENT, often in critical-safety roles. The use of computing technologies in MEDICAL ELECTRICAL EQUIPMENT introduces a level of complexity which is exceeded only by the biological systems of the PATIENTS the MEDICAL ELECTRICAL EQUIPMENT is intended to diagnose and/or treat. This complexity means that systematic failures can escape practical accepted limits of testing. Accordingly, this safety standard goes beyond traditional testing and assessment of the finished MEDICAL ELECTRICAL EQUIPMENT and includes requirements for the processes by which the MEDICAL ELECTRICAL EQUIPMENT is developed. Testing of the finished product is not, by itself, adequate to address the SAFETY of complex MEDICAL ELECTRICAL EQUIPMENT.

This standard is a Collateral Standard to the General Standard. It requires that a process be followed and that a record of that process be produced to support the SAFETY of MEDICAL ELECTRICAL EQUIPMENT incorporating PROGRAMMABLE ELECTRONIC SUBSYSTEMS. The concepts of RISK management and a DEVELOPMENT LIFE-CYCLE that are the basis of this standard can also be of value in the development of MEDICAL ELECTRICAL EQUIPMENT that does not include a PROGRAMMABLE ELECTRONIC SUBSYSTEM.

The effective application of the standard will require, subject to the task in hand, competency in the following:

- application of the specific MEDICAL ELECTRICAL EQUIPMENT with emphasis on SAFETY considerations;
- MEDICAL ELECTRICAL EQUIPMENT development process;
- methods by which SAFETY is assured;
- techniques of RISK analysis and RISK control.

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

APPAREILS ÉLECTROMÉDICAUX –

Partie 1-4: Règles générales de sécurité – Norme Collatérale: Systèmes électromédicaux programmables

SECTION 1: GÉNÉRALITÉS

1 Domaine d'application, objet et référence à d'autres normes

1.201 Domaine d'application

La présente Norme Collatérale traite de la SÉCURITÉ des APPAREILS ÉLECTROMÉDICAUX et des SYSTÈMES ÉLECTROMÉDICAUX comprenant des SOUS-SYSTÈMES ÉLECTRONIQUES PROGRAMMABLES (SSEP), appelés SYSTÈMES ÉLECTROMÉDICAUX PROGRAMMABLES (SEMP) dans la suite du texte.

NOTE Certains systèmes qui comportent un logiciel et sont utilisés pour des besoins médicaux ne sont pas dans le domaine d'application de la présente Norme Collatérale, comme c'est le cas de plusieurs systèmes d'informatique médicale. Le facteur/ critère de distinction est la conformité ou non-conformité du système à la définition de l'APPAREIL ÉLECTROMÉDICAL en 2.2.15 de la CEI 60601-1 ou à la définition du SYSTÈME ÉLECTROMÉDICAL en 2.203 de la CEI 60601-1-1.

1.202 Objet

La présente Norme Collatérale fixe les prescriptions à suivre lors de la conception d'un SEMP. Elle fournit aussi la base des prescriptions des Normes Particulières en servant de guide pour les exigences de SÉCURITÉ visant à réduire et à gérer les RISQUES. La présente Norme Collatérale s'adresse

a) aux organismes de certification;

b) aux CONSTRUCTEURS;

c) aux rédacteurs de Normes Particulières.

La présente norme traite les aspects suivants:

d) les spécifications des prescriptions;

e) l'architecture;

f) la conception détaillée et la mise en oeuvre y compris le développement du logiciel;

g) les modifications;

h) la VÉRIFICATION et la VALIDATION;

j) le marquage et les DOCUMENTS D'ACCOMPAGNEMENT.

La présente norme ne traite pas les aspects suivants:

k) la fabrication du matériel informatique;

l) la reproduction du logiciel;

m) l'installation et la mise en service;

n) le fonctionnement et la maintenance;

o) le retrait du service.

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

MEDICAL ELECTRICAL EQUIPMENT –

Part 1-4: General requirements for safety – Collateral Standard: Programmable electrical medical systems

SECTION 1: GENERAL

1 Scope, object and relationship to other standards

1.201 Scope

This Collateral Standard applies to the SAFETY of MEDICAL ELECTRICAL EQUIPMENT and MEDICAL ELECTRICAL SYSTEMS incorporating PROGRAMMABLE ELECTRONIC SUBSYSTEMS (PESS), hereinafter referred to as PROGRAMMABLE ELECTRICAL MEDICAL SYSTEMS (PEMS).

NOTE Some systems which incorporate software and are used for medical purposes fall outside the scope of this Collateral Standard, e.g. many medical informatics systems. The distinguishing factor/criterion is whether or not the system satisfies the definition of MEDICAL ELECTRICAL EQUIPMENT in 2.2.15 of IEC 60601-1 or the definition of MEDICAL ELECTRICAL SYSTEM in 2.203 of IEC 60601-1-1.

1.202 Object

This Collateral Standard specifies requirements for the process by which a PEMS is designed. This Collateral Standard also serves as the basis of requirements of Particular Standards, including serving as a guide to SAFETY requirements for the purpose of reducing and managing RISK. This Collateral Standard is addressed to:

a) certification bodies;

b) MANUFACTURERS;

c) writers of Particular Standards.

This standard covers:

d) requirement specification;

e) architecture;

f) detailed design and implementation including software development;

g) modification;

h) VERIFICATION and VALIDATION;

j) marking and ACCOMPANYING DOCUMENTS.

Aspects not covered by this standard include:

k) hardware manufacturing;

l) software replication;

m) installation and commissioning;

n) operation and maintenance;

o) decommissioning.

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

1.203 Références à d'autres normes

1.203.1 CEI 60601-1

Pour les APPAREILS ÉLECTROMÉDICAUX, la présente Norme Collatérale complète la CEI 60601-1 et ses amendements.

Quand il est fait référence à la CEI 60601-1 ou à la présente Norme Collatérale, soit seules, soit ensemble, les conventions suivantes sont utilisées:

– «La Norme Générale» désigne la CEI 60601-1 seule;
– «la présente Norme Collatérale» désigne la CEI 60601-1-4 seule;
– «la présente Norme» désigne l'ensemble de la Norme Générale et de la présente Norme Collatérale.

1.203.2 Normes Particulières

Une prescription d'une Norme Particulière a priorité sur la prescription correspondante de la présente Norme Collatérale.

1.203.3 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 60601-1:1988, *Appareils électromédicaux – Première partie: Règles générales de sécurité*
Amendement 1 (1991)
Amendement 2 (1995)

CEI 60601-1-1:1992, *Appareils électromédicaux – Première partie: Règles générales de sécurité – 1. Norme Collatérale: Règles de sécurité pour systèmes électromédicaux*

CEI 60788:1984, *Radiologie médicale – Terminologie*

ISO 9000-3:1991, *Normes pour la gestion de la qualité et l'assurance de la qualité – Partie 3: Lignes directrices pour l'application de l'ISO 9001 au développement, à la mise à disposition et à la maintenance du logiciel*

ISO 9001:1994, *Systèmes qualité – Modèle pour l'assurance de la qualité en conception, développement, production, installation et prestations associées*

2 Terminologie et définitions

2.201 Termes définis

Dans la présente Norme Collatérale, les termes imprimés en PETITES CAPITALES sont utilisés conformément à leurs définitions données dans la Norme Générale, dans la CEI 60601-1-1, dans la présente Norme Collatérale ou dans la CEI 60788.

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

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

1.203 Relationship to other standards

1.203.1 IEC 60601-1

For MEDICAL ELECTRICAL EQUIPMENT, this Collateral Standard complements IEC 60601-1 and its amendments.

When referring to IEC 60601-1 or to this Collateral Standard, either individually or in combination, the following conventions are used:

- "the General Standard" designates IEC 60601-1 alone;
- "this Collateral Standard" designates IEC 60601-1-4 alone;
- "this Standard" designates the combination of the General Standard and this Collateral Standard.

1.203.2 Particular Standards

A requirement in a Particular Standard takes priority over the corresponding requirement in this Collateral Standard.

1.203.3 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60601-1: 1988, *Medical electrical equipment – Part 1: General requirements for safety*
Amendment No. 1 (1991)
Amendment No. 2 (1995)

IEC 60601-1-1:1992, *Medical electrical equipment – Part 1: General requirements for safety – 1. Collateral Standard: Safety requirements for medical electrical systems*

IEC 60788:1984, *Medical radiology – Terminology*

ISO 9000-3:1991, *Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software*

ISO 9001:1994, *Quality systems – Model for quality assurance in design, development, production, installation and servicing*

2 Terminology and definitions

2.201 Defined terms

In this Collateral Standard, terms printed in SMALL CAPITALS are used in accordance with their definitions in the General Standard, IEC 60601-1-1, this Collateral Standard or IEC 60788.

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

Un index des termes définis utilisés dans la présente Norme Collatérale se trouve dans l'annexe AAA.

Pour les besoins de la présente Norme Collatérale, les définitions supplémentaires suivantes sont applicables.

2.201.1
CYCLE DE DÉVELOPPEMENT
activités nécessaires intervenant pendant la période de temps qui commence à la phase de conception d'un projet et s'achève lorsque la VALIDATION du SEMP est terminée

2.201.2
ANALYSE DES DANGERS
identification des DANGERS et de leurs causes d'origine

NOTE La quantification du DANGER ne fait pas partie de l'ANALYSE DES DANGERS.

2.201.3
RISQUE MAXIMAL TOLÉRABLE
valeur du RISQUE spécifiée comme la valeur maximale qu'on peut accepter

NOTE Cette valeur peut être spécifiée pour le SEMP globalement ou pour un DANGER particulier.

2.201.4
SYSTÈME ÉLECTROMÉDICAL PROGRAMMABLE (SEMP)
SYSTÈME ÉLECTROMÉDICAL, ou APPAREIL ÉLECTROMÉDICAL, comportant un ou PLUSIEURS SOUS-SYSTÈMES ÉLECTRONIQUES PROGRAMMABLES

2.201.5
SOUS-SYSTÈME ÉLECTRONIQUE PROGRAMMABLE (SSEP)
système basé sur une ou plusieurs unités centrales de traitement, y compris les logiciels et les interfaces

2.201.6
RISQUE RÉSIDUEL
RISQUE identifié par l'ANALYSE DES DANGERS et qui reste après avoir terminé la gestion des RISQUES

2.201.7
RISQUE
probabilité d'occurrence d'un DANGER provoquant un dommage, et degré de SÉVÉRITÉ de ce dommage

2.201.8
FICHIER DE GESTION DES RISQUES
éléments du dossier de la qualité exigés par la présente norme

2.201.9
RELEVÉ DE GESTION DES RISQUES
document qui fournit, pour chaque DANGER et pour chaque cause du DANGER, la traçabilité de l'analyse des RISQUES et de la VÉRIFICATION que le RISQUE du DANGER est maîtrisé

NOTE Ce document peut être conservé sur papier ou sur support électronique.

2.201.10
SÉCURITÉ
absence de RISQUE inacceptable

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

An index of defined terms used in this Collateral Standard is given in annex AAA.

For the purpose of this Collateral Standard, the following additional definitions apply.

2.201.1
DEVELOPMENT LIFE-CYCLE
necessary activities occurring during a period of time that starts at the concept phase of a project and finishes when the VALIDATION of the PEMS is complete

2.201.2
HAZARD ANALYSIS
identification of HAZARDS and their initiating causes

NOTE The quantification of HAZARD is not a part of the HAZARD ANALYSIS.

2.201.3
MAXIMUM TOLERABLE RISK
value of RISK which is specified as the maximum which may be permitted

NOTE The value may be specified for the PEMS as a whole or for a particular HAZARD.

2.201.4
PROGRAMMABLE ELECTRICAL MEDICAL SYSTEM (PEMS)
MEDICAL ELECTRICAL EQUIPMENT or MEDICAL ELECTRICAL SYSTEM containing one or more PROGRAMMABLE ELECTRONIC SUBSYSTEM

2.201.5
PROGRAMMABLE ELECTRONIC SUBSYSTEM (PESS)
system based on one or more central processing units, including their software and interfaces

2.201.6
RESIDUAL RISK
RISK identified by HAZARD ANALYSIS which remains after RISK management has been completed

2.201.7
RISK
probable rate of occurrence of a HAZARD causing harm, and the degree of SEVERITY of the harm

2.201.8
RISK MANAGEMENT FILE
that part of the quality records required by this standard

2.201.9
RISK MANAGEMENT SUMMARY
document, which provides traceability for each HAZARD and each cause of the HAZARD to the RISK analysis and to the VERIFICATION that the RISK of the HAZARD is controlled

NOTE This document may be held on paper or on electronic media.

2.201.10
SAFETY
freedom from unacceptable RISK

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

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

2.201.11
DANGER POUR LA SÉCURITÉ (appelé DANGER dans ce qui suit)
éventualité d'un effet néfaste pour le PATIENT, d'autres personnes, des animaux ou l'entourage, provenant directement d'un APPAREIL ÉLECTROMÉDICAL

2.201.12

Non utilisé.

2.201.13
SÉVÉRITÉ
évaluation qualitative des conséquences possibles d'un DANGER

2.201.14
VALIDATION
méthode d'évaluation d'un SEMP, ou d'un composant d'un SEMP, pour déterminer, en cours ou à la fin du développement, s'il satisfait aux prescriptions de son utilisation prévue

2.201.15
VÉRIFICATION
méthode d'évaluation d'un SEMP, ou d'un composant d'un SEMP, pour déterminer si les produits d'une phase donnée du développement satisfont aux conditions spécifiées imposées au début de cette phase

2.202 Degrés d'exigence et termes divers

Dans la présente Norme Collatérale, certains termes (qui ne sont pas imprimés en petites capitales) ont une signification particulière:

– «doit» correspond à une prescription impérative pour la conformité;

– «devrait» correspond à une forte recommandation sans qu'elle soit impérative pour la conformité;

– «peut» correspond à une manière autorisée d'être conforme à une prescription ou d'éviter la nécessité d'être conforme;

– «spécifique» correspond à une information précise indiquée dans la présente Norme Collatérale, ou dans d'autres normes, traitant généralement des conditions particulières de fonctionnement, des dispositions d'essai ou des valeurs liées à la conformité;

– «spécifié» correspond à une information précise indiquée par le CONSTRUCTEUR dans les DOCUMENTS D'ACCOMPAGNEMENT ou dans d'autres documents relatifs au SEMP à l'étude, concernant généralement sa destination, ou les paramètres et les conditions d'utilisation ou d'essai pour déterminer la conformité.

6 Identification, marquage et documentation

6.8 DOCUMENTS D'ACCOMPAGNEMENT

6.8.201 Toutes les informations importantes relatives au RISQUE RÉSIDUEL significatif, informations comprenant la description des DANGERS et les actions à entreprendre par L'OPÉRATEUR ou L'UTILISATEUR pour les éviter/les réduire, doivent être reportées à la fois dans les INSTRUCTIONS D'UTILISATION et dans le FICHIER DE GESTION DES RISQUES.

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

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

2.201.11
SAFETY HAZARD (hereinafter referred to as HAZARD)
potentially detrimental effect on the PATIENT, other persons, animals, or the surroundings, arising directly from MEDICAL ELECTRICAL EQUIPMENT

2.201.12

Not used.

2.201.13
SEVERITY
qualitative measure of the possible consequences of a HAZARD

2.201.14
VALIDATION
process of evaluating a PEMS or a component of a PEMS during or at the end of the development process, to determine whether it satisfies the requirements for its intended use

2.201.15
VERIFICATION
process of evaluating a PEMS or a component of a PEMS to determine whether the products of a given development phase satisfy the specified requirements imposed at the start of that phase

2.202 Degrees of requirements and miscellaneous terms

In this Collateral Standard, certain terms (which are not printed in small capitals) have particular meanings, as follows:

- "shall" indicates a requirement that is mandatory for compliance;
- "should" indicates a strong recommendation that is not mandatory for compliance;
- "may" indicates a permitted manner of complying with a requirement or of avoiding the need to comply;
- "specific" is used to indicate definitive information stated in this Collateral Standard or referenced in other standards, usually concerning particular operating conditions, test arrangements or values connected with compliance;
- "specified" is used to indicate definitive information stated by the MANUFACTURER in ACCOMPANYING DOCUMENTS or in other documentation relating to the PEMS under consideration, usually concerning its intended purposes, or the parameters or conditions associated with its use or with testing to determine compliance.

6 Identification, marking and documents

6.8 ACCOMPANYING DOCUMENTS

6.8.201 All relevant information regarding significant RESIDUAL RISK including descriptions of the HAZARDS and any actions by the OPERATOR or the USER necessary to avoid/mitigate them shall be placed in both the INSTRUCTIONS FOR USE and the RISK MANAGEMENT FILE.

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

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

6.8.202 LES DOCUMENTS D'ACCOMPAGNEMENT pour le SEMP doivent identifier, au minimum, le CONSTRUCTEUR et un unique identificateur tel que l'indice de révision et la date de mise en circulation/publication.

NOTE Les informations concernant tout ÉQUIPEMENT avec lequel un logiciel est destiné à être utilisé, ainsi que les moyens grâce auxquels le CONSTRUCTEUR peut être contacté, peuvent être donnés sur l'emballage ou dans les INSTRUCTIONS D'UTILISATION de telle façon qu'ils soient disponibles pour L'UTILISATEUR indépendamment de l'usage du logiciel.

SECTION 9: FONCTIONNEMENT ANORMAL ET CONDITIONS DE DÉFAUT; ESSAIS D'ENVIRONNEMENT

52 Fonctionnement anormal et conditions de défaut

52.201 Documentation

52.201.1 Les documents produits par l'application de la présente norme doivent être conservés et doivent faire partie des enregistrements de la qualité; voir figure 201. Cela devrait être réalisé conformément à 6.3 de l'ISO 9000-3.

52.201.2 L'ensemble de ces documents, appelé ici FICHIER DE GESTION DES RISQUES, doit être approuvé, diffusé et modifié conformément à un système de gestion formel de configuration. Ceci devrait être réalisé conformément à 6.2 de l'ISO 9000-3.

52.201.3 Un RELEVÉ DE GESTION DES RISQUES doit être fait tout au long du CYCLE DE DÉVELOPPEMENT en tant qu'élément du FICHIER DE GESTION DES RISQUES. Il doit comporter

a) les DANGERS identifiés et leurs causes d'origine;

b) l'estimation du RISQUE;

c) référence aux mesures de SÉCURITÉ utilisées pour éliminer ou maîtriser le RISQUE de DANGER;

d) l'estimation de l'efficacité de la maîtrise des RISQUES;

e) la référence de la VÉRIFICATION.

La conformité est vérifiée par examen du FICHIER DE GESTION DES RISQUES.

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

6.8.202 ACCOMPANYING DOCUMENTS for the PEMS shall identify, as a minimum, the MANUFACTURER and a unique identifier such as revision level and date of release/issue.

NOTE Information pertaining to any specific EQUIPMENT that software is intended to be used in conjunction with, and a means by which the MANUFACTURER can be contacted, can be located on the package or in the INSTRUCTIONS FOR USE so that it is available to the USER independently of the software operation.

SECTION 9: ABNORMAL OPERATION AND FAULT CONDITIONS; ENVIRONMENTAL TESTS

52 Abnormal operation and fault conditions

52.201 Documentation

52.201.1 Documents produced from application of this standard shall be maintained and shall form part of the quality records; see figure 201. This should be done in accordance with 6.3 of ISO 9000-3.

52.201.2 These documents, herein referred to as the RISK MANAGEMENT FILE, shall be approved, issued and changed in accordance with a formal configuration management system. This should be done in accordance with 6.2 of ISO 9000-3.

52.201.3 A RISK MANAGEMENT SUMMARY shall be developed throughout the DEVELOPMENT LIFE-CYCLE as part of the RISK MANAGEMENT FILE. It shall contain:

a) identified HAZARDS and their initiating causes;

b) estimation of RISK;

c) reference to the SAFETY measures, used to eliminate or control the RISK of the HAZARD;

d) evaluation of effectiveness of RISK control;

e) reference to VERIFICATION.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

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

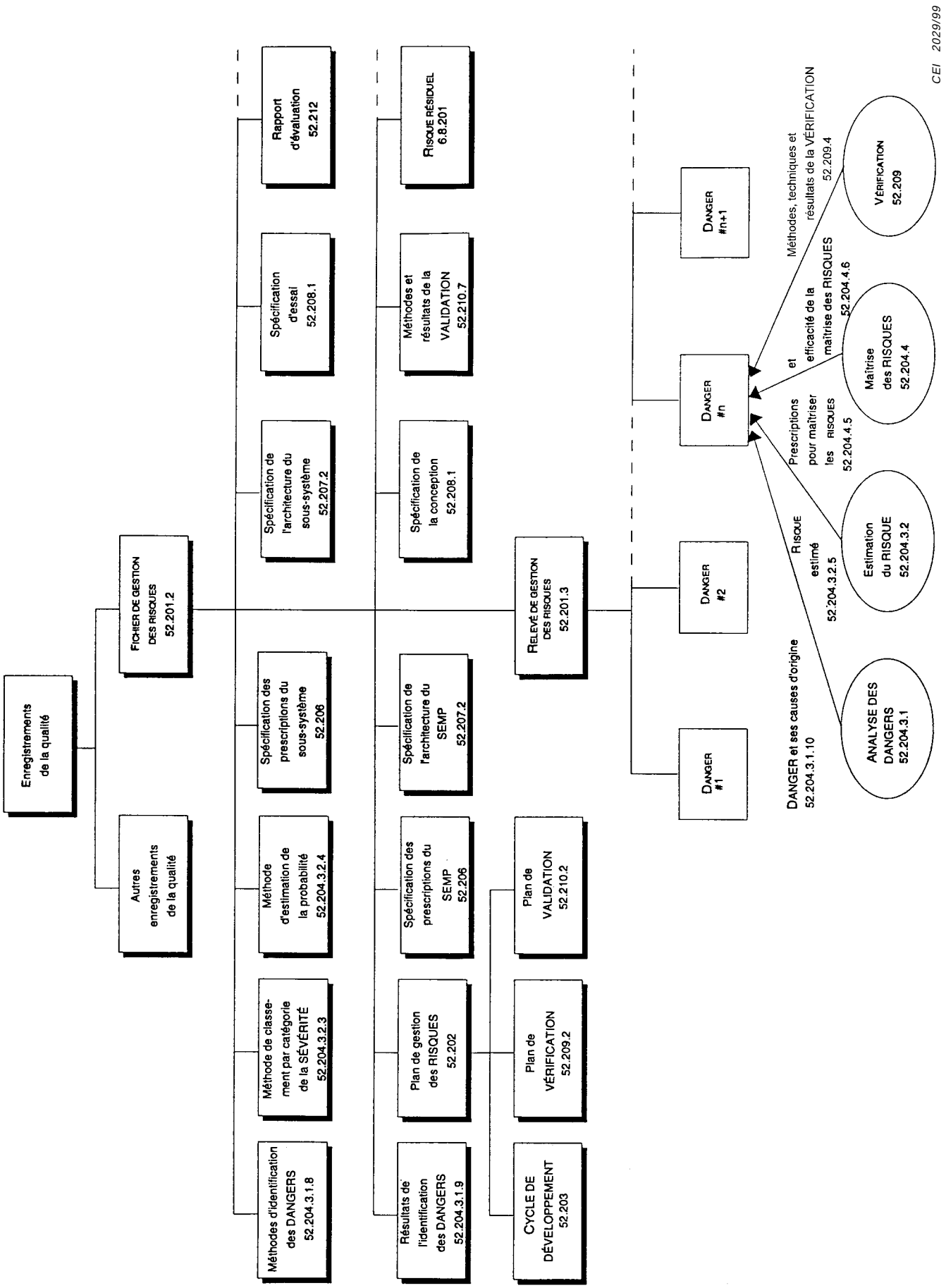


Figure 201 – Organigramme du FICHIER DE GESTION DES RISQUES et du RELEVÉ DE GESTION DES RISQUES

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

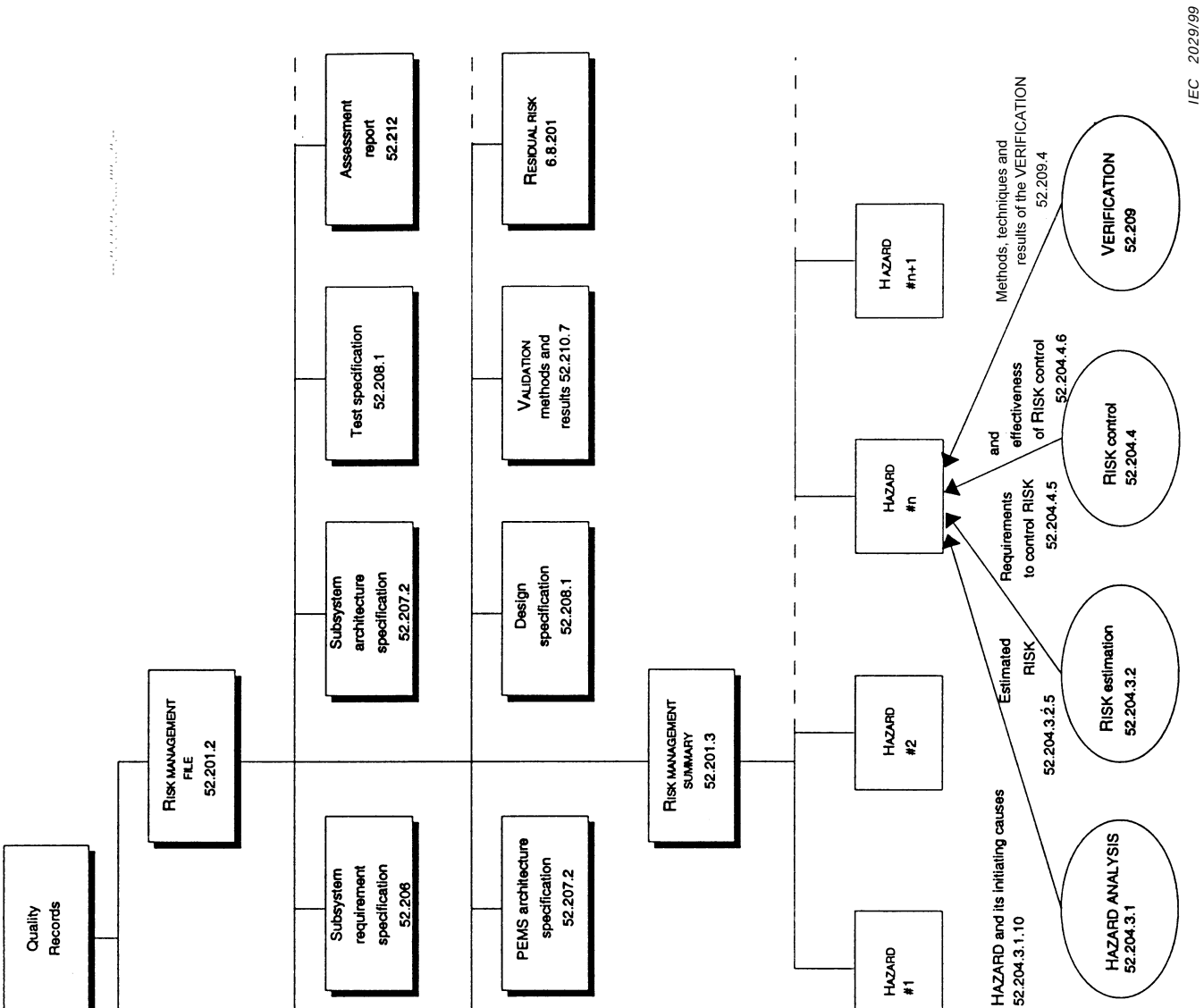


Figure 201 – Content of RISK MANAGEMENT FILE and RISK MANAGEMENT SUMMARY

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

52.202 Plan de gestion des RISQUES

52.202.1 Le CONSTRUCTEUR doit préparer un plan de gestion des RISQUES.

52.202.2 Ce plan doit comporter les points suivants:

a) le domaine d'application du plan, définissant le projet ou le produit et les phases du CYCLE DE DÉVELOPPEMENT auxquelles le plan s'applique;

b) le CYCLE DE DÉVELOPPEMENT à appliquer (voir 52.203), incluant un plan de VÉRIFICATION et un plan de VALIDATION;

c) les responsabilités de la gestion conformément à 4.1 de l'ISO 9001;

d) le traitement de la gestion des RISQUES;

e) les prescriptions des révisions périodiques.

52.202.3 Si le plan change au cours du développement, un enregistrement des changements doit être conservé.

La conformité est vérifiée par examen du FICHIER DE GESTION DES RISQUES.

52.203 CYCLE DE DÉVELOPPEMENT

52.203.1 Un CYCLE DE DÉVELOPPEMENT doit être défini pour la conception et le développement du SEMP.

52.203.2 Le CYCLE DE DÉVELOPPEMENT doit se diviser en phases et tâches avec, pour chacune d'elles, un point de départ, un point final et une activité bien définis.

52.203.3 Le CYCLE DE DÉVELOPPEMENT doit comprendre les traitements complets de la gestion des RISQUES.

52.203.4 Le CYCLE DE DÉVELOPPEMENT doit comprendre les prescriptions pour la documentation.

52.203.5 Les activités de la gestion des RISQUES doivent s'appliquer convenablement tout au long du CYCLE DE DÉVELOPPEMENT; voir 52.204.

NOTE Un exemple de CYCLE DE DÉVELOPPEMENT est donné dans l'annexe DDD.

La conformité est vérifiée par examen du FICHIER DE GESTION DES RISQUES.

52.203.6 Le cas échéant, un système défini pour la résolution des problèmes pendant et entre toutes les phases et tâches du CYCLE DE DÉVELOPPEMENT doit être développé et maintenu en tant qu'une partie du FICHIER DE GESTION DES RISQUES. Selon le problème, le système peut avoir les caractéristiques suivantes:

– être défini en tant que partie du CYCLE DE DÉVELOPPEMENT;

– permettre de rendre compte de problèmes potentiels ou existants de SÉCURITÉ;

– inclure une évaluation de chaque problème pour les RISQUES associés;

– identifier les critères (SÉCURITÉ et/ou performance) à satisfaire pour prononcer une conclusion;

– identifier les actions à entreprendre pour résoudre chaque problème;

– identifier les méthodes de VALIDATION pour chaque action;

– identifier les mesures prises pour vérifier, de façon continue, la conformité.

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

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

52.202 RISK management plan

52.202.1 The MANUFACTURER shall prepare a RISK management plan.

52.202.2 This plan shall include the following:

a) scope of the plan, defining the project or product and the DEVELOPMENT LIFE-CYCLE phases for which the plan is applicable;

b) the DEVELOPMENT LIFE-CYCLE to be applied (see 52.203), including a VERIFICATION plan and a VALIDATION plan;

c) management responsibilities in accordance with 4.1 of ISO 9001;

d) RISK management process;

e) requirements for reviews.

52.202.3 If the plan changes during the course of development, a record of the changes shall be kept.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

52.203 DEVELOPMENT LIFE-CYCLE

52.203.1 A DEVELOPMENT LIFE-CYCLE shall be defined for the design and development of the PEMS.

52.203.2 The DEVELOPMENT LIFE-CYCLE shall be divided into phases and tasks, with a well-defined input, output and activity for each.

52.203.3 The DEVELOPMENT LIFE-CYCLE shall include integral processes for RISK management.

52.203.4 The DEVELOPMENT LIFE-CYCLE shall include documentation requirements.

52.203.5 RISK management activities shall apply throughout the DEVELOPMENT LIFE-CYCLE as appropriate; see 52.204.

NOTE An example of a DEVELOPMENT LIFE-CYCLE is given in annex DDD.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

52.203.6 Where appropriate, a defined system for problem resolution within and between all phases and tasks of the DEVELOPMENT LIFE CYCLE shall be developed and maintained as part of the RISK MANAGEMENT FILE. Depending upon the problem, the system may have the following characteristics:

– be defined as a part of the DEVELOPMENT LIFE-CYCLE;

– allow the reporting of potential or existing SAFETY and/or performance problems;

– include an assessment of each problem for associated RISKS;

– identify the criteria (SAFETY and/or performance) that have to be met for the issue to be closed;

– identify the action to be taken to resolve each problem;

– identify VALIDATION methods for each action;

– identify the steps taken for VERIFICATION of continuing compliance.

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

52.204 Traitement de la gestion des RISQUES

52.204.1 Un traitement de la gestion des RISQUES doit être utilisé et comporter les éléments suivants:

- analyse des RISQUES;
- maîtrise des RISQUES.

52.204.2 Le traitement doit être appliqué tout au long du CYCLE DE DÉVELOPPEMENT.

52.204.3 Analyse des RISQUES

52.204.3.1 ANALYSE DES DANGERS

52.204.3.1.1 L'identification des DANGERS doit être effectuée comme cela est défini dans le plan de gestion des RISQUES; voir 52.202.

52.204.3.1.2 Les DANGERS doivent être identifiés pour toutes les circonstances raisonnablement prévisibles en tenant compte

- de l'UTILISATION NORMALE;
- d'une mauvaise utilisation.

52.204.3.1.3 Les DANGERS à prendre en considération doivent inclure, de façon appropriée:

- les DANGERS pour les PATIENTS;
- les DANGERS pour les OPÉRATEURS;
- les DANGERS pour le personnel de service;
- les DANGERS pour ceux qui assistent;
- les DANGERS pour l'environnement.

52.204.3.1.4 Les séquences des événements raisonnablement prévisibles, qui peuvent provoquer un DANGER, doivent être prises en considération.

52.204.3.1.5 Les causes d'origine à prendre en considération doivent inclure, de façon appropriée

- les facteurs humains, y compris les servitudes ergonomiques;
- les défauts du matériel informatique;
- les défauts du logiciel;
- les erreurs d'intégration;
- les conditions d'environnement.

52.204.3.1.6 Les matières à prendre en considération doivent inclure, de façon appropriée

- la compatibilité des éléments du système, y compris le matériel et le logiciel;
- l'interface utilisateur, y compris le langage de commande, les messages d'avertissement et les messages d'erreur;
- la précision de la traduction du texte employé dans l'interface utilisateur et dans les INSTRUCTIONS D'UTILISATION;
- la protection des données contre les erreurs humaines intentionnelles ou non;
- les critères RISQUE/avantage;
- les logiciels tiers.

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

52.204 RISK management process

52.204.1 A RISK management process shall be used that has the following elements:

- RISK analysis;
- RISK control.

52.204.2 The process shall be applied throughout the DEVELOPMENT LIFE-CYCLE.

52.204.3 RISK analysis

52.204.3.1 HAZARD ANALYSIS

52.204.3.1.1 HAZARD identification shall be carried out as defined in the RISK management plan; see 52.202.

52.204.3.1.2 HAZARDS shall be identified for all reasonably foreseeable circumstances including:

- NORMAL USE;
- incorrect use.

52.204.3.1.3 The HAZARDS considered shall include, as appropriate:

- HAZARDS to PATIENTS;
- HAZARDS to OPERATORS;
- HAZARDS to service personnel;
- HAZARDS to bystanders;
- HAZARDS to the environment.

52.204.3.1.4 Reasonably foreseeable sequences of events, which may result in a HAZARD, shall be considered.

52.204.3.1.5 Initiating causes considered shall include, as appropriate:

- human factors including ergonomic limitations;
- hardware faults;
- software faults;
- integration errors;
- environmental conditions.

52.204.3.1.6 Matters considered shall include, as appropriate:

- compatibility of system components, including hardware and software;
- user interface, including command language, warning and error messages;
- accuracy of translation of text used in the user interface and INSTRUCTIONS FOR USE;
- data protection from human intentional or unintentional causes;
- RISK/benefit criteria;
- third party software.

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

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

52.204.3.1.7 Les méthodes d'identification des DANGERS appropriées à la phase du CYCLE DE DÉVELOPPEMENT doivent être utilisées.

52.204.3.1.8 Les méthodes utilisées (par exemple l'analyse par arbre de panne, l'analyse des modes de défaillance et de leurs effets) doivent être décrites dans le FICHIER DE GESTION DES RISQUES.

52.204.3.1.9 Les résultats de l'application des méthodes doivent figurer dans le FICHIER DE GESTION DES RISQUES.

52.204.3.1.10 Chaque DANGER identifié et ses causes d'origine doivent être notés dans le RELEVÉ DE GESTION DES RISQUES.

La conformité est vérifiée par examen du FICHIER DE GESTION DES RISQUES.

52.204.3.2 Estimation du RISQUE

52.204.3.2.1 Pour chaque DANGER identifié, le RISQUE doit être estimé.

52.204.3.2.2 L'estimation du RISQUE doit reposer sur une estimation de la probabilité de chaque DANGER et/ou de la SÉVÉRITÉ des conséquences de chaque DANGER.

52.204.3.2.3 La méthode de classement par catégorie des niveaux de SÉVÉRITÉ doit être enregistrée dans le FICHIER DE GESTION DES RISQUES.

52.204.3.2.4 La méthode d'estimation de la probabilité doit être soit quantitative, soit qualitative et doit être enregistrée dans le FICHIER DE GESTION DES RISQUES.

52.204.3.2.5 Le RISQUE estimé doit être enregistré en face de chaque DANGER dans le RELEVÉ DE GESTION DES RISQUES.

La conformité est vérifiée par examen du FICHIER DE GESTION DES RISQUES.

52.204.4 Maîtrise des RISQUES

52.204.4.1 Le RISQUE doit être maîtrisé de façon telle que le RISQUE estimé de chaque DANGER identifié devienne acceptable.

52.204.4.2 Un RISQUE est acceptable si le RISQUE est inférieur ou égal au RISQUE MAXIMAL TOLÉRABLE et si le RISQUE est rendu aussi faible qu'on peut raisonnablement le faire.

52.204.4.3 Les méthodes de la maîtrise des RISQUES doivent réduire la probabilité du DANGER ou réduire la SÉVÉRITÉ du DANGER ou les deux.

La probabilité pour que les mesures prises pour réduire les RISQUES soient efficaces doit être spécifiée quantitativement ou qualitativement; voir annexe CCC.

52.204.4.4 Les méthodes de la maîtrise des RISQUES doivent viser les causes du DANGER (par exemple en réduisant sa probabilité) ou introduire des mesures de protection qui interviennent lorsque la cause du DANGER est présente, ou les deux, avec la priorité suivante:

- sécurité inhérente à la conception;
- mesures de protection incluant des alarmes;
- information suffisante de l'UTILISATEUR sur le RISQUE RÉSIDUEL.

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

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

52.204.3.1.7 HAZARD identification methods appropriate to the DEVELOPMENT LIFE-CYCLE phase shall be used.

52.204.3.1.8 The methods used (e.g. fault tree analysis, failure modes and effects analysis) shall be documented in the RISK MANAGEMENT FILE.

52.204.3.1.9 The results of the application of the methods shall be documented in the RISK MANAGEMENT FILE.

52.204.3.1.10 Each identified HAZARD and its initiating causes shall be recorded in the RISK MANAGEMENT SUMMARY.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

52.204.3.2 RISK estimation

52.204.3.2.1 For each identified HAZARD the RISK shall be estimated.

52.204.3.2.2 The estimation of the RISK shall be based on an estimation of the likelihood of each HAZARD and/or the SEVERITY of the consequences of each HAZARD.

52.204.3.2.3 The SEVERITY level categorization method shall be recorded in the RISK MANAGEMENT FILE.

52.204.3.2.4 The likelihood estimation method shall be either quantitative or qualitative and shall be recorded in the RISK MANAGEMENT FILE.

52.204.3.2.5 The estimated RISK shall be recorded against each HAZARD in the RISK MANAGEMENT SUMMARY.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

52.204.4 RISK control

52.204.4.1 RISK shall be controlled so that the estimated RISK of each identified HAZARD is made acceptable.

52.204.4.2 A RISK is acceptable if the RISK is less than or equal to the MAXIMUM TOLERABLE RISK and the RISK is made as low as reasonably practicable.

52.204.4.3 Methods of RISK control shall reduce the likelihood of the HAZARD or reduce the SEVERITY of the HAZARD or both.

The likelihood that the means for RISK reduction will perform correctly shall be specified quantitatively or qualitatively; see annex CCC.

52.204.4.4 RISK control methods shall be directed at the cause of the HAZARD (e.g. by reducing its likelihood) or by introducing protective measures which operate when the cause of the HAZARD is present, or both, using the following priority:

- inherent safe design;
- protective measures including alarms;
- adequate USER information on the RESIDUAL RISK.

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

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

52.204.4.5 La ou les prescriptions de la maîtrise des RISQUES doivent figurer dans le RELEVÉ DE GESTION DES RISQUES (directement ou par référence).

52.204.4.6 Une évaluation de l'efficacité de la maîtrise des RISQUES doit être enregistrée dans le RELEVÉ DE GESTION DES RISQUES.

La conformité est vérifiée par examen du FICHIER DE GESTION DES RISQUES.

52.205 Qualification du personnel

La conception et la modification des SEMP doivent être considérées comme une tâche assignée conformément à 4.18 de l'ISO 9001.

La conformité est vérifiée par examen des fichiers appropriés.

52.206 Spécification des prescriptions

52.206.1 Pour le SEMP et pour chacun de ses sous-systèmes (par exemple pour un SSEP), il doit exister une spécification des prescriptions.

NOTE Des exemples de structures d'un SEMP sont donnés dans l'annexe EEE.

52.206.2 La spécification des prescriptions doit détailler les fonctions qui sont liées au RISQUE. Cela comprend des fonctions qui maîtrisent le RISQUE dû

a) à des causes provenant des conditions d'environnement;

b) à des causes extérieures au SEMP;

c) à des mauvais fonctionnements possibles.

52.206.3 La spécification des prescriptions doit contenir les informations utiles en vue de s'assurer que les mesures prises pour la maîtrise des RISQUES réduisent de façon satisfaisante les RISQUES identifiés.

52.207 Architecture

52.207.1 L'architecture doit satisfaire à la spécification des prescriptions.

52.207.2 Pour le SEMP et pour chacun de ses sous-systèmes, une architecture doit être spécifiée.

52.207.3 Le cas échéant, la spécification de l'architecture d'un SEMP et de ses sous-systèmes doit aborder les prescriptions de la MAÎTRISE DU RISQUE par la diminution de la probabilité correspondante du DANGER ou par la diminution de la SÉVÉRITÉ des conséquences du DANGER ou les deux.

52.207.4 Le cas échéant, pour diminuer la probabilité des DANGERS, la spécification de l'architecture doit recommander d'utiliser ce qui suit:

a) des composants hautement fiables;

b) des fonctions à sécurité positive;

c) la redondance;

d) la diversité;

e) une conception défensive;

f) des limitations de conséquences potentiellement dangereuses, par exemple en réduisant la puissance de sortie et/ou en introduisant des moyens de limiter le déplacement pour les organes de manoeuvres.

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

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

52.204.4.5 The requirement(s) to control the RISK shall be documented in the RISK MANAGEMENT SUMMARY (directly or as a cross reference).

52.204.4.6 An evaluation of the effectiveness of the RISK controls shall be recorded in the RISK MANAGEMENT SUMMARY.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

52.205 Qualification of personnel

The design and modification of a PEMS shall be considered as an assigned task in accordance with 4.18 of ISO 9001.

Compliance is checked by inspection of the appropriate files.

52.206 Requirement specification

52.206.1 For the PEMS and each of its subsystems (e.g. for a PESS) there shall be a requirement specification.

NOTE Example structures of a PEMS are given in annex EEE.

52.206.2 The requirement specification shall detail the functions that are RISK-related. This includes functions that control RISKS arising from

a) causes arising from environmental conditions;

b) causes elsewhere in the PEMS;

c) possible malfunctions.

52.206.3 The requirement specification shall include the information necessary to assure that RISK control measures satisfactorily reduce the identified RISKS.

52.207 Architecture

52.207.1 The architecture shall satisfy the requirement specification.

52.207.2 For the PEMS and each of its subsystems, an architecture shall be specified.

52.207.3 Where appropriate, the architecture specification of a PEMS and its subsystems shall address the RISK CONTROL requirements by reducing the corresponding likelihood of the HAZARD or by reducing the SEVERITY of the HAZARD or both.

52.207.4 Where appropriate, to reduce the likelihood of the HAZARD, the architecture specification shall make use of:

a) highly reliable components;

b) fail-safe functions;

c) redundancy;

d) diversity;

e) defensive design;

f) limits on potentially hazardous effects, for example by restricting the available output power and/or by introducing means to limit the travel of actuators.

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

52.207.5 La spécification de l'architecture doit prendre en compte ce qui suit:

a) l'allocation des mesures de la maîtrise des RISQUES aux sous-systèmes et aux éléments du SEMP.

NOTE Les sous-systèmes et les éléments comprennent les capteurs, les dispositifs de commande, le SSEP et les interfaces.

b) les types de pannes et leurs conséquences;

c) les pannes ayant les mêmes causes;

d) les pannes systématiques;

e) l'intervalle de temps entre les essais, la durée des essais et la couverture du diagnostic;

f) la maintenabilité;

g) la protection contre les erreurs humaines intentionnelles ou non.

52.208 Conception et réalisation

52.208.1 La conception doit être scindée de façon appropriée en sous-systèmes, chaque sous-système ayant une spécification pour la conception et pour les essais.

52.208.2 Les données descriptives pour l'environnement de la conception doivent être comprises dans le FICHIER DE GESTION DES RISQUES.

NOTE Voir en annexe DDD des exemples d'éléments d'environnement de la conception.

52.209 VÉRIFICATION

52.209.1 Une VÉRIFICATION de l'exécution des prescriptions de SÉCURITÉ doit être effectuée.

52.209.2 Un plan de VÉRIFICATION doit être établi pour indiquer comment les prescriptions de SÉCURITÉ sont vérifiées à chaque phase du CYCLE DE DÉVELOPPEMENT. Ce plan doit comprendre

a) le choix et la documentation des stratégies, activités et techniques de VÉRIFICATION;

b) la sélection et l'utilisation des outils de VÉRIFICATION;

c) les critères de couverture pour la VÉRIFICATION.

NOTE Méthodes et techniques sont par exemple

– lectures croisées et examens;

– analyses statiques/dynamiques;

– essais boîte blanche/boîte noire.

52.209.3 La VÉRIFICATION doit être conduite conformément au plan de VÉRIFICATION. Les résultats des activités de VÉRIFICATION doivent être documentés, analysés et évalués.

52.209.4 Une référence aux méthodes, techniques et résultats de la VÉRIFICATION doit figurer dans le RELEVÉ DE GESTION DES RISQUES.

52.210 Validation

52.210.1 La VALIDATION de la SÉCURITÉ des SEMP doit être faite dans les conditions d'usage prévues.

52.210.2 Un plan de VALIDATION doit être établi pour montrer que les bonnes prescriptions de SÉCURITÉ ont été exécutées.

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

52.207.5 The architecture specification shall take the following into consideration:

a) allocation of RISK control measures to subsystems and components of the PEMS;

NOTE Subsystems and components include sensors, actuators, PESS and interfaces.

b) failure modes of components and their effects;

c) common cause failures;

d) systematic failures;

e) test interval, test duration and diagnostic coverage;

f) maintainability;

g) protection from human intentional or unintentional causes.

52.208 Design and implementation

52.208.1 Where appropriate, the design shall be decomposed into subsystems, each having a design and test specification.

52.208.2 Descriptive data regarding the design environment shall be included in the RISK MANAGEMENT FILE.

NOTE See annex DDD for examples of design environment elements.

52.209 VERIFICATION

52.209.1 VERIFICATION of the implementation of SAFETY requirements shall be carried out.

52.209.2 A VERIFICATION plan shall be produced to show how the SAFETY requirements for each DEVELOPMENT LIFE-CYCLE phase will be verified. The plan shall include

a) the selection and documentation of VERIFICATION strategies, activities and techniques;

b) the selection and utilization of VERIFICATION tools;

c) coverage criteria for VERIFICATION.

NOTE Examples of methods and techniques are

– walkthroughs and inspections;

– static/dynamic analyses;

– white/black box testing.

52.209.3 The VERIFICATION shall be performed according to the VERIFICATION plan. The results of the VERIFICATION activities shall be documented, analyzed and assessed.

52.209.4 A reference to the methods, techniques and results of the VERIFICATION shall be included in the RISK MANAGEMENT SUMMARY.

52.210 VALIDATION

52.210.1 VALIDATION of the SAFETY of PEMS under the conditions of the intended use shall be carried out.

52.210.2 A VALIDATION plan shall be produced to show that correct SAFETY requirements have been implemented.

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

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

52.210.3 La VALIDATION doit être conduite conformément au plan de VALIDATION. Les résultats des activités de VALIDATION doivent être documentés, analysés et évalués.

52.210.4 Le chef de l'équipe effectuant la VALIDATION doit être indépendant de l'équipe de conception.

52.210.5 Toutes les relations professionnelles entre les membres de l'équipe de VALIDATION et les membres de l'équipe de conception doivent figurer dans le FICHIER DE GESTION DES RISQUES.

52.210.6 L'équipe de conception ne doit pas être entièrement responsable de la VALIDATION de son propre produit.

52.210.7 Une référence aux méthodes et aux résultats de la VALIDATION doit figurer dans le FICHIER DE GESTION DES RISQUES.

La conformité est vérifiée par examen du FICHIER DE GESTION DES RISQUES.

52.211 Modification

52.211.1 Si tout ou partie d'un projet résulte de la modification d'un projet antérieur, soit la présente norme s'applique intégralement comme s'il s'agissait d'un nouveau projet, soit la validité conservée de toute la documentation du précédent projet doit être évaluée selon une procédure de modification.

52.211.2 Tous les documents correspondants du CYCLE DE DÉVELOPPEMENT doivent être révisés, modifiés, revus, approuvés selon un schéma de contrôle de la documentation conformément à 4.5.2 de l'ISO 9001 ou des références équivalentes.

La conformité est vérifiée par examen du FICHIER DE GESTION DES RISQUES.

52.212 Evaluation

52.212.1 Une évaluation doit être effectuée pour s'assurer que les SEMP ont été développés selon les prescriptions de la présente norme, et doit être enregistrée dans le FICHIER DE GESTION DES RISQUES. Cela peut être réalisé par un audit interne.

La conformité est vérifiée par examen du FICHIER DE GESTION DES RISQUES.

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

52.210.3 The VALIDATION shall be performed according to the VALIDATION plan. The results of VALIDATION activities shall be documented, analyzed and assessed.

52.210.4 The leader of the team carrying out the VALIDATION shall be independent of the design team.

52.210.5 All professional relationships of the members of the VALIDATION team with members of the design team shall be documented in the RISK MANAGEMENT FILE.

52.210.6 No member of a design team shall be responsible for the VALIDATION of his own design.

52.210.7 A reference to the methods and results of the VALIDATION shall be included in the RISK MANAGEMENT FILE.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

52.211 Modification

52.211.1 If any or all of a design results from a modification of an earlier design then either all of this standard applies as if it were a new design or the continued validity of any previous design documentation shall be assessed under a modification/change procedure.

52.211.2 All relevant documents in the DEVELOPMENT LIFE-CYCLE shall be revised, amended, reviewed, approved under a document control scheme in accordance with 4.5.2 of ISO 9001 or equivalent.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

52.212 Assessment

52.212.1 Assessment shall be carried out to ensure that the PEMS has been developed in accordance with the requirements of this standard and recorded in the RISK MANAGEMENT FILE. This may be carried out by internal audit.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

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

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

Annexe AAA
(normative)

Terminologie – Index des termes définis

CEI 60788 ..... rm-..-..
Nom d'unité dans le Système International SI ..... rm-..-.. *
Terme dérivé sans définition ..... rm-..-..+
Terme sans définition ..... rm-..-..-
Nom de l'ancienne unité ..... rm-..-..•
Terme abrégé ..... rm-..-..s
Article 2 de la Norme Général ..... NG-2. .
Article 2 de la présente publication CEI 60601-1-4 ..... 2.201. .

ANALYSE DES DANGERS 2.201.2
APPAREIL ÉLECTROMÉDICAL NG-2.2.15
CONDITION DE PREMIER DÉFAUT NG-2.10.11
CONSTRUCTEUR rm-85-03-
CYCLE DE DÉVELOPPEMENT 2.201.1
DANGER (voir DANGER POUR LA SÉCURITÉ)
DANGER POUR LA SÉCURITÉ 2.201.11
DOCUMENTS D'ACCOMPAGNEMENT NG-2.1.4
FICHIER DE GESTION DES RISQUES 2.201.8
INSTRUCTIONS D'UTILISATION rm-82-02
OPÉRATEUR rm-85-02
PATIENT NG-2.12.4
RELEVÉ DE GESTION DES RISQUES 2.201.9
RISQUE 2.201.7
RISQUE MAXIMAL TOLÉRABLE 2.201.3
RISQUE RÉSIDUEL 2.201.6
SÉCURITÉ 2.201.10
SÉVÉRITÉ 2.201.13
SYSTÈME ÉLECTROMÉDICAL ..... CEI 60601-1-1, 2.203
SYSTÈME ÉLECTROMÉDICAL PROGRAMMABLE (SEMP) 2.201.4
SOUS-SYSTÈME ÉLECTRONIQUE PROGRAMMABLE (SSEP) 2.201.5
UTILISATEUR rm-85-01
UTILISATION NORMALE NG-2.10.8
VALIDATION 2.201.14
VÉRIFICATION 2.201.15

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

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

Annex AAA
(normative)

Terminology – Index of defined terms

IEC 60788 ..... rm-..-..
Name of unit in the International System SI ..... rm-..-..*
Derived term without definition ..... rm-..-..+
Term without definition ..... rm-..-..-
Name of earlier unit ..... rm-..-..•
Shortened term ..... rm-..-..s
Clause 2 of the General Standard ..... NG-2. .
Clause 2 of IEC 60601-1-4 (present publication) ..... 2.201. .

ACCOMPANYING DOCUMENTS NG-2.1.4
DEVELOPMENT LIFE-CYCLE 2.201.1
HAZARD (see SAFETY HAZARD)
HAZARD ANALYSIS 2.201.2
INSTRUCTIONS FOR USE rm-82-02
MANUFACTURER rm-85-03-
MAXIMUM TOLERABLE RISK 2.201.3
MEDICAL ELECTRICAL EQUIPMENT NG-2.2.15
MEDICAL ELECTRICAL SYSTEM ..... IEC 60601-1-1, 2.203
NORMAL USE NG-2.10.8
OPERATOR rm-85-02
PATIENT NG-2.12.4
PROGRAMMABLE ELECTRICAL MEDICAL SYSTEM (PEMS) 2.201.4
PROGRAMMABLE ELECTRONIC SUBSYSTEM (PESS) 2.201.5
RESIDUAL RISK 2.201.6
RISK 2.201.7
RISK MANAGEMENT FILE 2.201.8
RISK MANAGEMENT SUMMARY 2.201.9
SAFETY 2.201.10
SAFETY HAZARD 2.201.11
SEVERITY 2.201.13
SINGLE FAULT CONDITION NG-2.10.11
USER rm-85-01
VALIDATION 2.201.14
VERIFICATION 2.201.15

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

Annexe BBB
(informative)

Justifications

Généralités

La présente norme nécessite qu'un traitement avec certains éléments soit établi et suivi car la technologie en question n'est pas soumise à des essais «bon/mauvais» sur le produit fini. L'approche est de fixer ce qui est exigé en laissant à l'utilisateur de la présente Norme Collatérale le soin de déterminer comment cela est réalisé. On retrouve la même approche dans la série des normes ISO 9000. Comme les utilisateurs sont supposés être qualifiés, on a conservé un minimum de détails. On a prévu la répétition de parties du traitement mais on n'a fourni aucune prescription car la nécessité de répéter les procédures est propre à un projet particulier. Les répétitions proviennent aussi d'une compréhension plus détaillée qui apparaîtra au cours du développement de l'étude.

En tant qu'élément du développement, la documentation est exigée car elle est nécessaire pour contrôler le développement. De plus, l'examen de la documentation permet de vérifier la conformité aux prescriptions de développement de la présente norme. Un RELEVÉ DE GESTION DES RISQUES fait partie de la documentation pour s'assurer que les problèmes et les mesures concernant la SÉCURITÉ peuvent être facilement compris au cours et à la fin du développement.

Bien qu'elle ne soit pas propre à un SEMP, la gestion des RISQUES est soulignée afin de noter la complexité inhérente à la technologie en question et pour s'assurer que les DANGERS sont rapidement identifiés. Une identification rapide des DANGERS est nécessaire si la rigueur qui en découle doit être efficace pour aborder la SÉCURITÉ.

L'utilisation de la présente Norme Collatérale par du personnel qualifié est soulignée. Cela est fait pour ne garder dans les prescriptions que les éléments essentiels et en raison de la littérature de plus en plus vaste et approfondie dans le domaine de l'assurance des logiciels et des techniques d'évaluation des DANGERS. Les utilisateurs de la présente Norme Collatérale devront employer les éléments de ces publications quand des circonstances spécifiques se présenteront au cours du développement des SEMP. Dans les premières phases, des outils tels que l'analyse par arbre de panne seront d'une utilisation plus fréquente. Quand la conception est plus avancée, des outils plus élaborés tels que l'analyse des modes de défaillance et de leurs effets seront plus largement utilisés.

Terminologie et définitions

Les termes et définitions sont donnés pour faciliter le travail du lecteur et réduire la longueur du texte. Un grand effort a été fait pour rendre claires les prescriptions dans le texte de manière que les définitions ne deviennent pas des prescriptions par défaut.

Identification, marquage et documentation

La prescription pour l'identification du SEMP est destinée à s'assurer que les UTILISATEURS ne peuvent utiliser par mégarde un mauvais logiciel ou une version obsolète de logiciel. L'information sur le RISQUE RÉSIDUEL est incluse, car il n'est pas toujours possible, ou pratique, d'éliminer tous les DANGERS. Dans ce cas, la responsabilité minimale du CONSTRUCTEUR est de prévenir les UTILISATEURS de ces DANGERS et de fournir les informations qui peuvent aider à les éviter/les minimiser.

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

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

Annex BBB
(informative)

Rationale

General

This standard requires that a process with certain elements be established and followed because the subject technology is not amenable to pass/fail tests on the finished product. The approach is to state what is required, leaving the user of this Collateral Standard to determine how this is achieved. This is similar to the approach taken in the ISO 9000 series. As users are expected to be qualified, detail has been kept to a minimum. Iteration of portions of the process is expected, but no requirements have been given because the need to repeat processes is unique to a particular project. Iterations also arise from the more detailed understanding that emerges during the design process.

As part of the process, documentation is required because it is necessary for process control. In addition, inspection of the documentation permits checking compliance with the process requirements of this standard. A RISK MANAGEMENT SUMMARY is part of the documentation to assure that SAFETY issues and measures can be readily comprehended during and at the end of the process.

While not unique to PEMS, RISK management is emphasized in order to address the essential complexity of the subject technology and to ensure the early identification of HAZARDS. Early identification of HAZARDS is necessary if subsequent rigour is to be effective in addressing SAFETY.

The use of this Collateral Standard by qualified people is emphasized. This is done to keep requirements to the essential elements and in recognition of the extensive and growing literature in the fields of software assurance and HAZARD assessment techniques. Users of this Collateral Standard will need to employ the tools in this literature as specific circumstances arise in the development of PEMS. In early phases, "top down" tools such as fault tree analysis will be in more frequent use. When the design is more detailed, "bottom up" tools such as failure modes and effects analysis will come into wider use.

Terminology and definitions

These are given as a convenience for the reader and to reduce the length of the text. Every effort has been made to make requirements clear in the text so that definitions do not become requirements by default.

Identification, marking and documents

The requirement to identify the PEMS is intended to ensure that USERS do not inadvertently use the wrong software or an obsolete version of the software. Information on RESIDUAL RISK is included, because it may not be possible or practical to eliminate all HAZARDS. Where this is the case, it is the MANUFACTURER'S minimum responsibility to make the USERS aware of those HAZARDS and provide information that may help avoid/mitigate them.

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

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

Documentation

Un RELEVÉ DE GESTION DES RISQUES est exigé pour s'assurer que les RISQUES des DANGERS identifiés sont maîtrisés. Ce RELEVÉ DE GESTION DES RISQUES est terminé à l'achèvement du CYCLE DE DÉVELOPPEMENT.

CYCLE DE DÉVELOPPEMENT

Un CYCLE DE DÉVELOPPEMENT est exigé pour s'assurer que la SÉCURITÉ est traitée de manière systématique, et en particulier, pour permettre d'identifier les DANGERS le plus tôt possible dans des systèmes complexes.

Un système défini est exigé pour la résolution des problèmes car les approches particulières peuvent générer leurs propres problèmes. Les problèmes envisagés comprennent des éléments tels que prescriptions contradictoires ou ambiguës, spécifications manquantes et «bugs» apparus lors des évaluations.

Traitement de la gestion des RISQUES

Les prescriptions sont destinées à fournir un cadre dans lequel l'expérience, la perspicacité et le jugement s'appliquent pour gérer les RISQUES avec succès.

La conception de base est la suivante: plus grand est le RISQUE prévisible, plus l'analyse est rigoureuse et plus grande est l'intégrité des mesures de maîtrise du RISQUE. Le niveau de détail a été choisi pour être approprié à la présente Norme Collatérale. Pour une application médicale particulière à l'étude, une Norme Particulière fournira des méthodes plus spécifiques pour gérer les RISQUES, y compris des prescriptions «bon/mauvais».

Le traitement est appliqué tout au long du CYCLE DE DÉVELOPPEMENT de façon telle que, lorsque les causes des DANGERS sont identifiées, les méthodes appropriées pour la maîtrise des RISQUES soient spécifiées.

Estimation du RISQUE

Les défaillances de logiciel et les autres défaillances systématiques ne sont pas considérées en probabilité comme des événements en eux-mêmes. Cependant, un objectif majeur de cette norme est de réduire la probabilité de l'existence d'erreurs systématiques. Une autre considération est la probabilité que des erreurs dangereuses se présentent en cours d'utilisation. Alors qu'elles ne sont que rarement quantifiables, ces composantes du RISQUE associées aux erreurs systématiques sont considérées attentivement pour tout traitement responsable de la conception. L'estimation du RISQUE est une étape nécessaire à la fois pour déterminer où l'on doit concentrer ses efforts pour la conception et pour juger des résultats. Une méthode pour quantifier ou qualifier la probabilité d'une erreur de logiciel systématique est à l'étude.

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

Documentation

A RISK MANAGEMENT SUMMARY is required to ensure that the RISKS of identified HAZARDS are controlled. The RISK MANAGEMENT SUMMARY is complete at the completion of the DEVELOPMENT LIFE-CYCLE.

DEVELOPMENT LIFE-CYCLE

A DEVELOPMENT LIFE-CYCLE is required to ensure that SAFETY is dealt with in a systematic manner, and in particular to enable the early identification of HAZARDS in complex systems.

A defined system for problem resolution is required because ad hoc approaches can bring problems of their own. Anticipated problems include such things as inconsistent or ambiguous requirements, missing specifications and "bugs" found during evaluations.

RISK management process

The requirements are intended to be a framework within which experience, insight and judgement are applied to manage RISK successfully.

The basic concept is that the greater the foreseeable RISK, the more rigorous the analysis and the greater the integrity of the RISK control measures are. The level of detail has been chosen to be appropriate to this Collateral Standard. For a particular medical application under consideration, a Particular Standard will provide more specific methods for managing RISK, including pass/fail requirements.

The process is applied throughout the DEVELOPMENT LIFE-CYCLE so that, as HAZARD causes are identified, appropriate RISK control methods are specified.

RISK estimation

Software and other systematic failures do not fit into the concept of likelihood or probability as events in themselves. A major objective of this standard, however, is to reduce the likelihood of systematic errors being present. Another related concern is the likelihood of the hazardous error being encountered in use. While seldom quantifiable, these components of the RISK associated with systematic errors are carefully considered in any responsible design process. RISK estimation is a necessary step both in determining where to focus design effort and in judging results. How to quantify or qualify the likelihood of a systematic software error is under consideration.

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

Annexe CCC
(informative)

Notion de RISQUE

RISQUE

La notion de RISQUE comporte deux éléments:

- la probabilité d'un événement dangereux;
- la SÉVÉRITÉ de l'effet d'un événement dangereux.

Les RISQUES peuvent être classés en trois zones:

- zone de RISQUE intolérable;
- zone de RISQUE «aussi faible qu'il est raisonnablement possible» (acronyme ALARP);
- zone de RISQUE tout à fait acceptable.

Zone de RISQUE intolérable

Le RISQUE de certains DANGERS est si grave qu'un système comportant de tels dangers ne serait pas toléré. Dans cette zone, le RISQUE sera réduit en diminuant la SÉVÉRITÉ et/ou la probabilité du DANGER.

Zone «ALARP»

La zone comprise entre l'intolérable et le tout à fait acceptable est appelée zone «ALARP». Les RISQUES de cette zone sont réduits au niveau le plus bas possible, en tenant compte des bénéfices que procure l'acceptation du RISQUE par rapport au coût d'une réduction ultérieure. Tout RISQUE devrait être réduit à un niveau «aussi faible qu'il est raisonnablement possible» (ALARP). Près de la frontière du RISQUE intolérable, les RISQUES devraient normalement être réduits même si le coût est important.

Zone de RISQUE tout à fait acceptable

Dans certains cas, la SÉVÉRITÉ et/ou la probabilité d'un DANGER sont si faibles que le RISQUE peut être négligé comparé au RISQUE d'autres DANGERS qui sont acceptés. Pour ces DANGERS, il n'est pas nécessaire de chercher activement à réduire le RISQUE.

La notion des trois zones de RISQUE est représentée à la figure CCC.1.

Niveaux de SÉVÉRITÉ

La SÉVÉRITÉ est une des composantes du RISQUE. Les quatre niveaux suivants sont une évaluation qualitative des conséquences possibles d'un DANGER et sont recommandés pour les SEMP:

- catastrophique: possibilité de causer plusieurs morts ou des lésions graves;
- critique: possibilité de mort ou de lésion grave;
- moyen: possibilité de lésion;
- négligeable: possibilité de lésion faible ou nulle.

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

Annex CCC
(informative)

RISK concepts

RISK

The concept of RISK has two elements:

- likelihood of a hazardous event;
- SEVERITY of the consequence of the hazardous event.

RISKS can be categorised into three regions:

- intolerable region;
- ALARP (As Low As Reasonably Practicable) region;
- broadly acceptable region.

Intolerable region

The RISK of some HAZARDS is so severe that a system in which they exist would not be tolerated. A RISK in this region will be reduced by reducing the SEVERITY and/or the likelihood of the HAZARD.

ALARP region

The region between the intolerable and the broadly acceptable regions is called the ALARP region. In the ALARP region RISKS are reduced to the lowest level practicable, bearing in mind the benefits of accepting the RISK and the cost of further reduction. Any RISK should be reduced to a level which is "as low as reasonably practicable" (ALARP). Near the limit of intolerable RISK, RISKS would normally be reduced even at considerable cost.

Broadly acceptable region

In some cases, either the SEVERITY and/or the probability of a HAZARD is so low that the RISK is negligible compared with the RISK of other HAZARDS which are accepted. For these HAZARDS, RISK reduction need not be actively pursued.

The three region concept of RISK is shown in figure CCC.1.

SEVERITY levels

SEVERITY is one of the components of RISK. The following four levels are a qualitative measure of the possible consequences of a HAZARD and are suggested for PEMS:

- catastrophic: potential of multiple deaths or serious injuries;
- critical: potential of death or serious injury;
- marginal: potential of injury;
- negligible: little or no potential of injury.

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

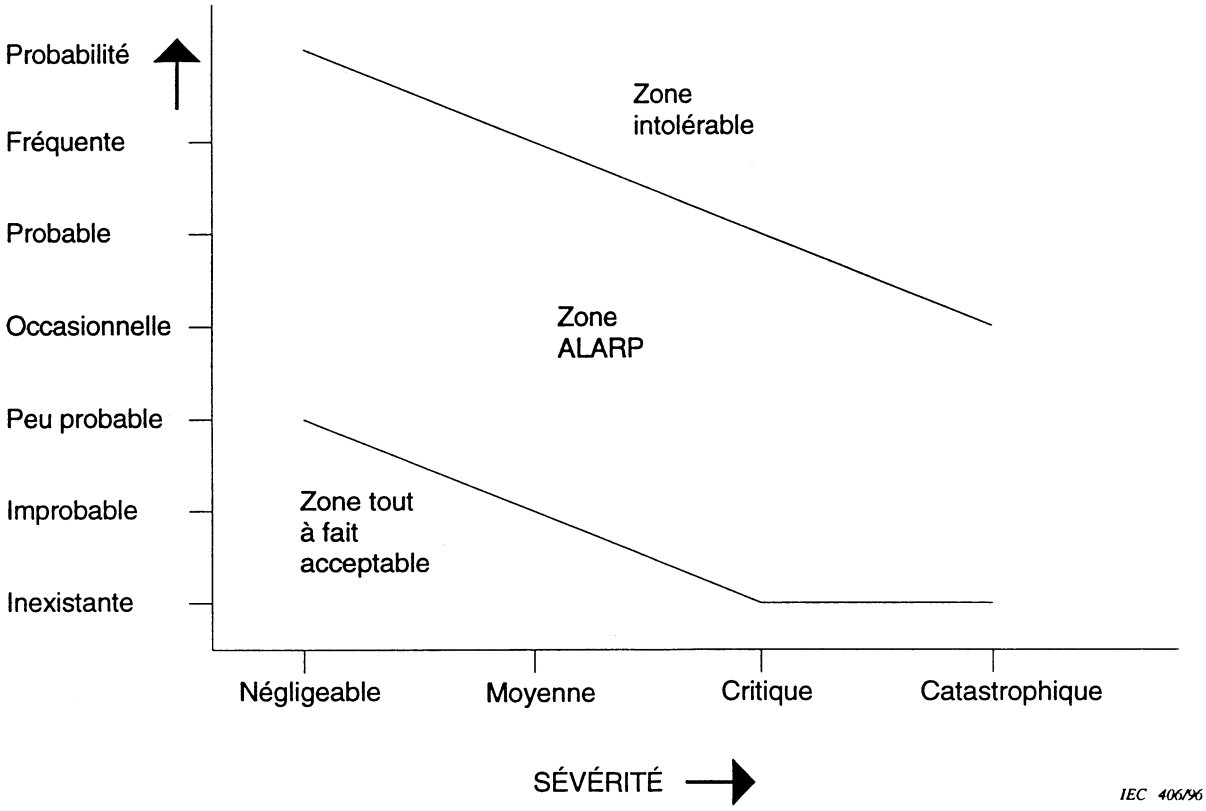


Figure CCC.1 – Diagramme du RISQUE

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

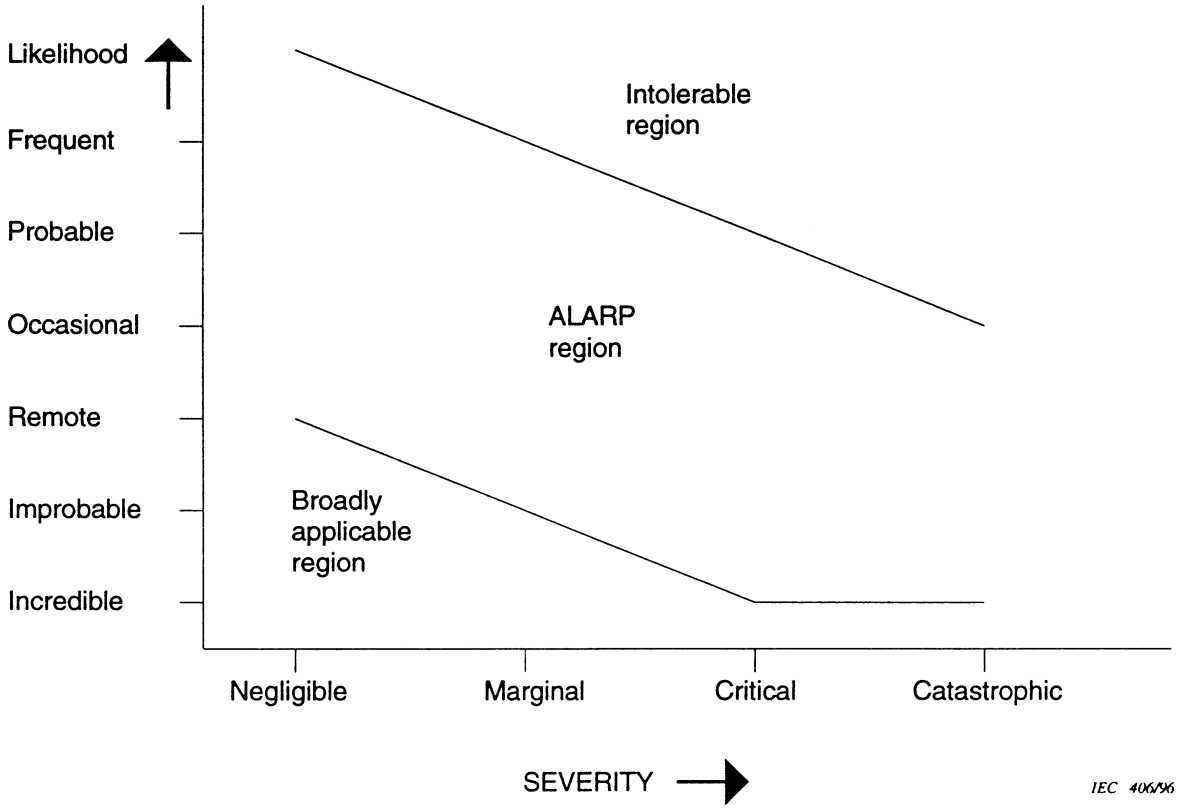


Figure CCC.1 – Risk chart

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

Décision pour le RISQUE acceptable

La présente norme ne spécifie pas le RISQUE acceptable. Il est prévu que des Normes Particulières fourniront des indications. Souvent, le RISQUE acceptable sera déterminé cas par cas. Quelques indications peuvent être obtenues en utilisant la philosophie de la CONDITION DE PREMIER DÉFAUT (décrite à l'article 3 de la Norme Générale) et/ou à partir des performances d'APPAREILS ÉLECTROMÉDICAUX similaires déjà en service.

Tout RISQUE associé à un SEMP pourrait être acceptable si les pronostics du PATIENT étaient améliorés. Cela ne peut pas être utilisé comme justification pour accepter un RISQUE non nécessaire. Le principe du RISQUE «aussi faible qu'il est raisonnablement possible» (ALARP) devrait toujours être appliqué.

Gestion du RISQUE

La présente norme exige qu'un traitement de la gestion des RISQUES soit utilisé tout au long du CYCLE DE DÉVELOPPEMENT. L'objectif de ce traitement est de gérer le RISQUE de façon telle qu'il soit à la fois inférieur au RISQUE MAXIMAL TOLÉRABLE et aussi faible que possible dans les conditions pratiques raisonnables. Un traitement typique de la gestion des RISQUES est présenté à la figure CCC.2.

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

Deciding on acceptable RISK

This standard does not specify acceptable RISK. It is planned that Particular Standards will give guidance. Often, acceptable RISK will be established on a case-by-case basis. Some guidance can be obtained by using the SINGLE FAULT CONDITION philosophy (described in clause 3 of the General Standard) and/or from the performance of similar MEDICAL ELECTRICAL EQUIPMENT already in use.

It may be that any RISK associated with PEMS would be acceptable if the PATIENT's prognosis were improved. This cannot be used as a rationale for the acceptance of unnecessary RISK. The ALARP principle should always be applied.

RISK management

This standard requires that a RISK management process be used throughout the DEVELOPMENT LIFE-CYCLE. The objective of the process is to manage RISK so that it is both less than the MAXIMUM TOLERABLE RISK and also is as low as reasonably practicable. A typical RISK management process is shown in figure CCC.2.

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

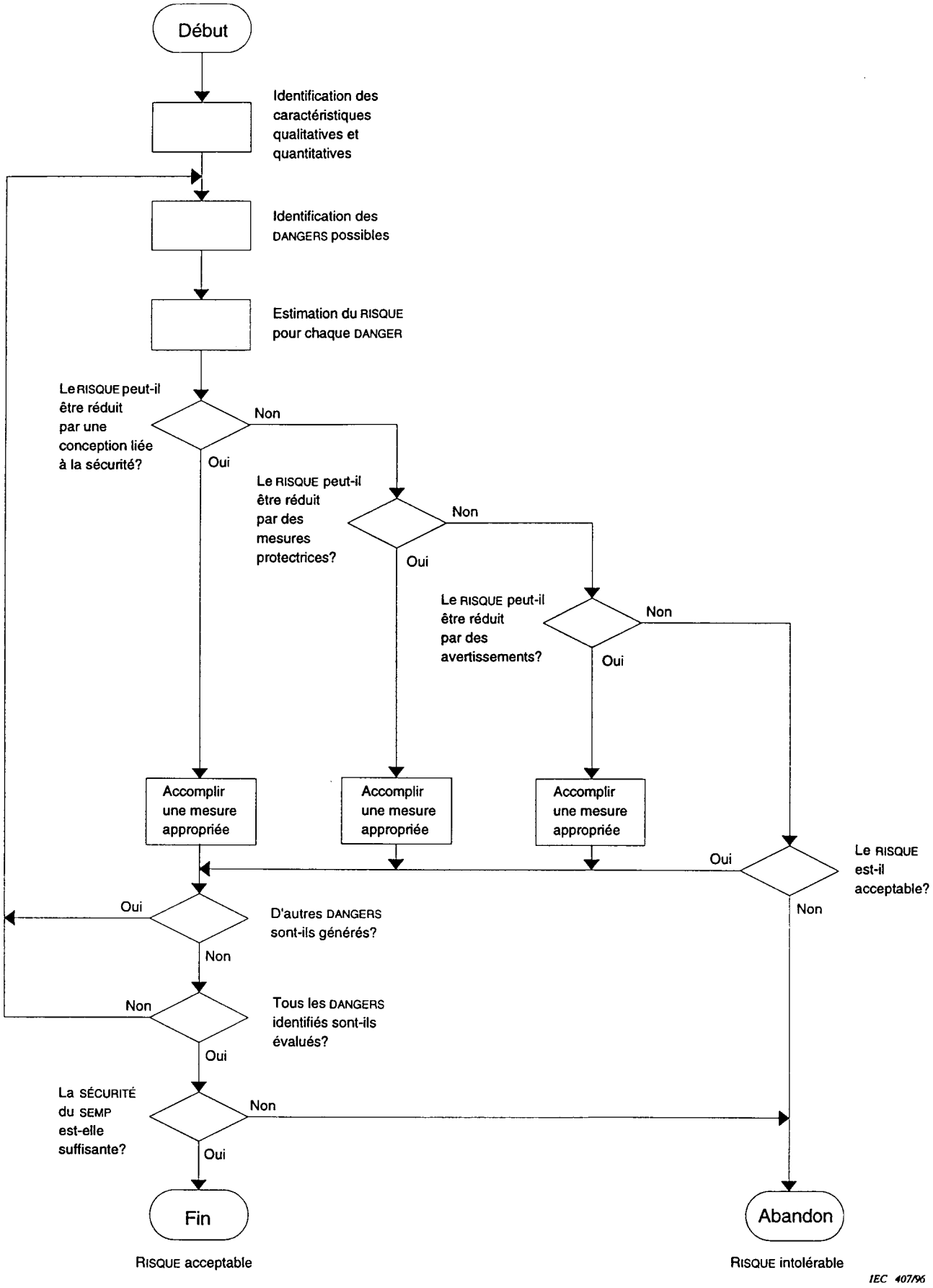


Figure CCC.2 – Traitement de la gestion des RISQUES

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

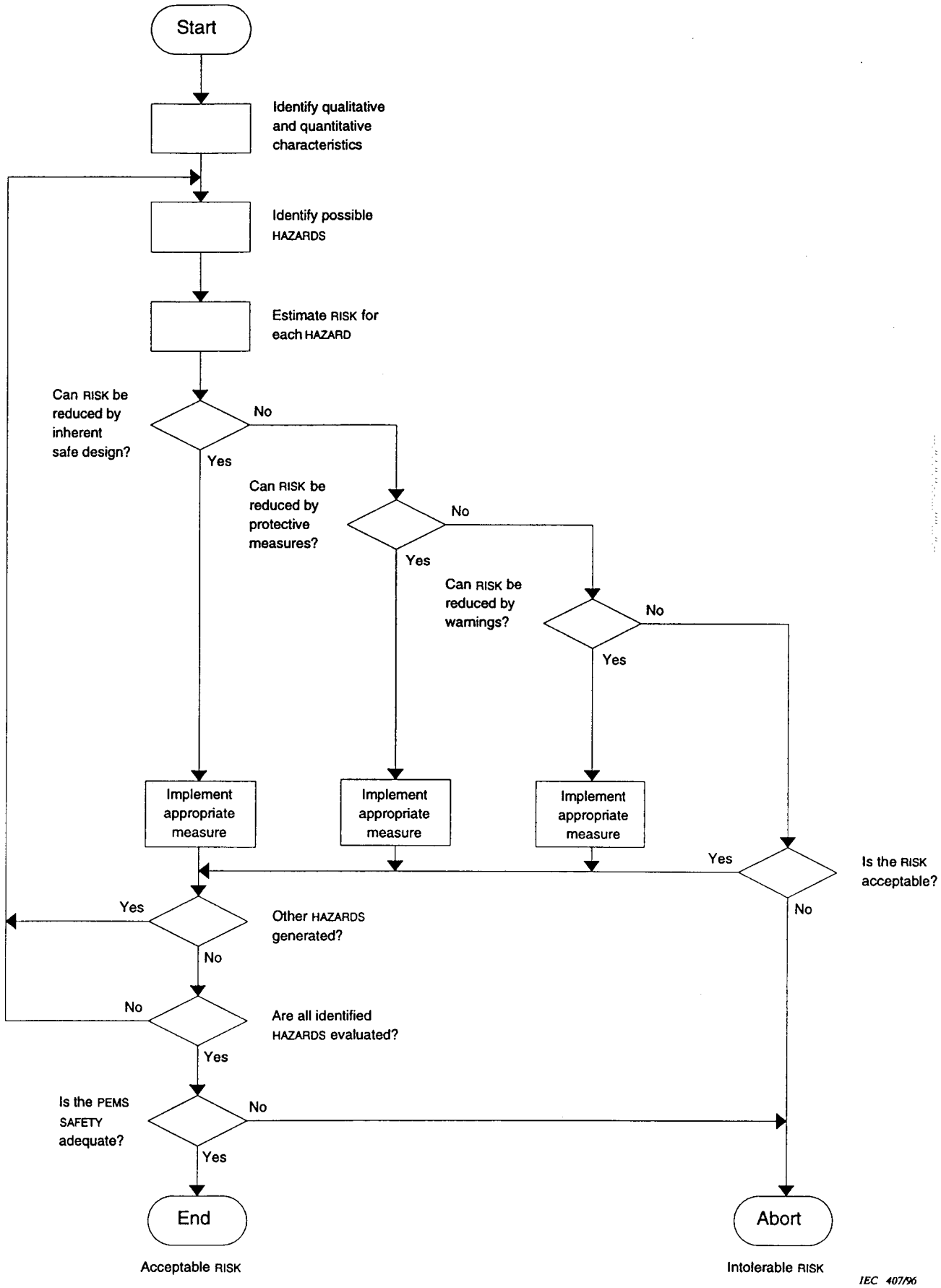


Figure CCC.2 – RISK management process

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

Cause de défaillance

Un événement dangereux peut provenir d'une défaillance d'un système. Il existe deux types possibles de défaillances:

– les défaillances aléatoires;

– les défaillances systématiques.

Défaillance aléatoire

Pour beaucoup d'événements, on peut associer une probabilité statistique de défaillance; par exemple, la probabilité de défaillance d'un ensemble électronique est souvent estimée à partir des probabilités de défaillance des composants de l'ensemble. Dans ce cas, une valeur numérique peut être fournie pour la probabilité de défaillance. Une supposition essentielle est que les défaillances sont aléatoires par nature. On admet que le matériel informatique tombe en panne de manière aléatoire ou systématique. On admet que le logiciel tombe en panne de manière aléatoire, pourtant la cause de défaillance du logiciel est toujours systématique.

Défaillance systématique

Les défaillances systématiques sont dues à des erreurs (y compris les erreurs de commande et les oublis) dans toute activité du CYCLE DE DÉVELOPPEMENT qui, suivant certaines combinaisons particulières des entrées ou dans certaines conditions d'environnement, provoqueront une défaillance.

Des défaillances systématiques peuvent se produire à la fois pour le matériel et pour le logiciel et peuvent avoir lieu à n'importe quel moment du CYCLE DE DÉVELOPPEMENT du produit. Un exemple de défaillance systématique pourrait être une valeur limite incorrecte dans une base de données qui conduirait à une condition dangereuse. Les données incorrectes peuvent avoir été mal spécifiées, mal saisies au cours de la préparation ou modifiées de façon incorrecte au cours de l'utilisation. La probabilité de ce type d'événement est difficile à prévoir. Il existe cependant une relation entre la qualité des traitements utilisés au cours du CYCLE DE DÉVELOPPEMENT et la probabilité qu'une erreur soit introduite ou ne soit pas détectée.

Estimation du RISQUE

Différentes méthodes sont utilisées pour estimer le risque. Un exemple de méthode d'estimation qualitative du RISQUE est donné. Alors que la présente Norme Collatérale n'exige pas qu'une méthode particulière soit utilisée, elle exige qu'une estimation du RISQUE soit effectuée; voir 52.204.3.2. L'estimation quantitative du RISQUE est également possible si des données convenables sont disponibles. Les méthodes pour l'estimation quantitative du RISQUE pourraient inclure l'adaptation d'une méthode qualitative, ou bien une approche alternative peut être appropriée. La méthode utilisée pour l'estimation du RISQUE fait partie du traitement de la gestion des RISQUES et devrait être définie dans le plan de gestion des RISQUES; voir 52.202.2 d).

Un diagramme du RISQUE tel que celui de la figure CCC.1 peut être utilisé pour définir les niveaux de RISQUE.

Les niveaux de RISQUE peuvent être classés dans une des zones de RISQUE, c'est-à-dire intolérable, ALARP et tout à fait acceptable.

La figure CCC.1 est un exemple de diagramme du RISQUE; elle est donnée ici pour indiquer la méthode mais cela n'implique pas qu'on l'applique de façon générale aux SEMP. Si une approche de diagramme du RISQUE est utilisée pour estimer le RISQUE, le diagramme du RISQUE particulier et l'interprétation qui en est faite devraient être justifiés pour cette application.

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

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

Cause of failure

A hazardous event can result from the failure of a system. There are two possible types of failure:

– random failures;

– systematic failures.

Random failure

For many events a statistical probability of failure can be assigned; for example the probability of failure of an electronic assembly is often estimated from the failure probabilities of the components which make up the assembly. In this case, a numerical value can be given for the probability of failure. An essential presumption is that the failures are random in nature. Hardware is assumed to fail either in a random or in a systematic manner. Software can appear to fail in a random manner, nevertheless the cause of a software failure is always systematic.

Systematic failure

Systematic failures are due to errors (including errors of commission and omission) in any DEVELOPMENT LIFE-CYCLE activity which, under some particular combination of inputs or environmental conditions, will permit a failure.

Systematic failures can occur in both hardware and software, and can take place at any time during a product DEVELOPMENT LIFE-CYCLE. An example of a systematic failure would be an incorrect limit value in a database which permitted a hazardous condition. The incorrect data may have been wrongly specified, wrongly copied during data preparation or incorrectly changed during use. The likelihood of this type of event is difficult to predict. There is, however, a relationship between the quality of the processes used during the DEVELOPMENT LIFE-CYCLE and the likelihood of the fault being introduced or remaining undetected.

RISK estimation

Various methods are used to estimate RISK. An example method of qualitative RISK estimation is given. While this Collateral Standard does not require that a particular method be used, it does require that RISK estimation is carried out; see 52.204.3.2. Quantitative RISK estimation is also possible where suitable data is available. Methods for quantitative RISK estimation could include the adaption of a qualitative method, or an alternative approach may be appropriate. The method used for RISK estimation is part of the RISK management process and should be defined in the RISK management plan; see 52.202.2 d).

A RISK chart such as figure CCC.1 can be used to define RISK levels.

The RISK levels can be classified into one of the RISK regions, i.e. intolerable, ALARP and broadly acceptable.

Figure CCC.1 is an example RISK chart; it is included here to show the method and does not imply that it has general application to PEMS. If a RISK chart approach is used for estimating RISK, the particular RISK chart and the interpretation used should be justified for that application.

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

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

Probabilité pour un fonctionnement correct

Le paragraphe 52.204.4.3 prescrit que la probabilité doit être spécifiée quantitativement ou qualitativement. Ci-dessous sont donnés des conseils pour ce faire.

Probabilité quantitative

Si la probabilité de défaillance peut être calculée ou démontrée (par exemple un calcul basé sur une panne aléatoire pour un système électronique du matériel), cette valeur peut être utilisée pour spécifier la probabilité d'un fonctionnement correct. Typiquement celle-ci peut être exprimée en temps moyen entre défaillances ou comme une probabilité de défaillance.

Probabilité qualitative

Si les défaillances sont systématiques, comme dans le cas d'un logiciel, il est souvent impossible de démontrer ou calculer une probabilité de défaillance. Si c'est le cas, une méthode qualitative peut être utilisée pour spécifier et vérifier la probabilité.

Cette norme ne prescrit aucune méthode particulière pour déterminer une mesure qualitative de la probabilité pour les défaillances systématiques. L'approche décrite est donnée à titre d'information.

Cette approche est basée sur l'idée que plus les processus utilisés pour créer un SSEP sont rigoureux et de bonne qualité, plus il y a de chances pour que celui-ci assure les fonctions prévues. De tels processus comprennent ce qui suit:

– techniques et méthodes de développement;
– sélection de l'architecture;
– assurance de la qualité;
– gestion de projet.

Avec les technologies les plus répandues il n'y a pas de moyen absolu de déterminer les processus adaptés à chaque cas particulier. Il est recommandé pour les utilisateurs de la norme de faire appel à leur jugement, basé sur ce qui est raisonnablement faisable et prenant en compte les principes ALARP.

Des indications supplémentaires pour la détermination de la relation entre processus utilisés et probabilité attendue de réduction des risques pour le logiciel peuvent être trouvées dans les références [5] et [7] de l'annexe FFF. Dans la référence [5], l'expression «sécurité absolue» est utilisée pour spécifier la probabilité que le SSEP assure les fonctions prévues.

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

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

Likelihood of correct performance

Subclause 52.204.4.3 requires that likelihood be specified quantitatively or qualitatively. Advice on how to do this is given below.

Quantitative likelihood

Where the probability of failure can be calculated or demonstrated (for example a calculation based on random failure for an electronic hardware system), this figure can be used to specify the likelihood of correct performance. Typically this would be expressed as a mean time between failures or as the probability of failure on demand.

Qualitative likelihood

Where failures are systematic, as is the case with software, it will often be impractical to demonstrate or calculate a probability of failure. If this is the case, a qualitative method should be used to specify and verify likelihood.

This standard does not require any particular method for determining a qualitative measure of likelihood for systematic failures. The approach suggested is for guidance only.

The approach is based on the idea that the more rigorous and the higher the quality of the processes used to create a PESS, the more likely it is that the PESS will carry out its intended function. Such processes may include

– development methods and techniques;
– selection of architecture;
– quality assurance;
– project management.

With current technology there is no definitive way to determine what processes are appropriate for any particular case. Users of the standard should use their best judgement, based on what is reasonably practicable and taking account of the ALARP principle.

Further guidance on determining a relationship between the processes used and the likelihood of the software carrying out its intended risk reduction can be found in references [5] and [7] in annex FFF. In reference [5] the term "safety integrity" is used to specify the likelihood of the PESS carrying out its intended function.

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

Annexe DDD
(informative)

CYCLE DE DÉVELOPPEMENT

Modèle de CYCLE DE DÉVELOPPEMENT – *Conception et mise en oeuvre*

Pendant l'usage du modèle de CYCLE DE DÉVELOPPEMENT, la conception et la mise en oeuvre incluront la sélection de ce qui suit:

a) méthodes de développement des logiciels;

b) composants électroniques;

c) outils de développement de logiciel assisté par ordinateur;

d) matériels redondants;

e) interface homme-SEMP;

f) sources d'énergie;

g) conditions d'environnement;

h) langages de programmation;

j) logiciels tierce partie.

Ces éléments de l'environnement de la conception peuvent être caractérisés de façon générale et de la façon spécifique pour leur utilisation dans le processus de conception et de mise en oeuvre.

La VALIDATION est conçue pour s'assurer que le produit correct est fabriqué. La VALIDATION du SEMP comme un tout à la dernière phase du CYCLE DE DÉVELOPPEMENT peut inclure des essais pour un grand volume de données, des charges et contraintes importantes, les facteurs humains, la sécurité, les performances, la compatibilité de configuration, les tests d'erreur, la documentation de L'UTILISATEUR et la mise en oeuvre des prescriptions de SÉCURITÉ.

La conformité à la présente Norme Collatérale demande qu'un CYCLE DE DÉVELOPPEMENT soit spécifié, puis suivi; elle n'exige pas qu'un CYCLE DE DÉVELOPPEMENT particulier soit utilisé, mais elle impose que le CYCLE DE DÉVELOPPEMENT comporte certaines qualités. Ces prescriptions peuvent être trouvées en 52.203.

La figure DDD.1 donne un modèle du CYCLE DE DÉVELOPPEMENT. Dans ce modèle, un procédé de décomposition est suivi d'un procédé d'intégration. Comme la conception est décomposée à partir des prescriptions, les blocs fonctionnels de construction, l'architecture et la technologie sont décidés. Le procédé de décomposition est terminé lorsque l'information de conception permet aux composants du SEMP d'être fabriqués (des exemples d'une telle information de conception sont les diagrammes des circuits et la codification du logiciel). Suivant la décomposition, les composants sont intégrés ensemble. La VÉRIFICATION est effectuée, si les composants sont intégrés, pour déterminer si l'exécution satisfait aux prescriptions ou pas. A la conclusion du procédé d'intégration, une VALIDATION est effectuée pour déterminer si le SEMP fonctionne comme prévu ou pas.

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

Annex DDD
(informative)

DEVELOPMENT LIFE-CYCLE

DEVELOPMENT LIFE-CYCLE model – *Design and implementation*

During application of the DEVELOPMENT LIFE-CYCLE model, design and implementation will include the selection of

a) software development methods;

b) electronic components;

c) computer aided software engineering (CASE) tools;

d) redundant hardware;

e) human-PEMS interface;

f) energy sources;

g) environmental conditions;

h) programming language;

j) third party software.

These elements of the design environment can be characterized in general and in the specific manner of their use in the design and implementation process.

VALIDATION is designed to assure that the right product is built. VALIDATION of the PEMS as a whole at the final phase of the DEVELOPMENT LIFE CYCLE can include tests for a high volume of data, heavy loads or stresses, human factors, security, performance, configuration compatibility, fault testing, USER documentation and implementation of SAFETY requirements.

Compliance with this Collateral Standard requires that a DEVELOPMENT LIFE-CYCLE be specified and then followed; it does not require that any particular DEVELOPMENT LIFE-CYCLE is used, but it does require that the DEVELOPMENT LIFE-CYCLE has certain attributes. These requirements can be found in 52.203.

Figure DDD.1 illustrates a model of the DEVELOPMENT LIFE-CYCLE. In this model a decomposition process is followed by an integration process. As the design is decomposed from the requirements, the functional building blocks, architecture and technology are decided. The decomposition process ends when the design information enables the components of the PEMS to be built (examples of such design information are circuit diagrams and software code). Following the decomposition the components are integrated together. VERIFICATION is carried out as the components are integrated to determine whether or not the implementation satisfies the requirements. At the conclusion of the integration process, a VALIDATION is carried out to determine whether or not the PEMS works as intended.

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

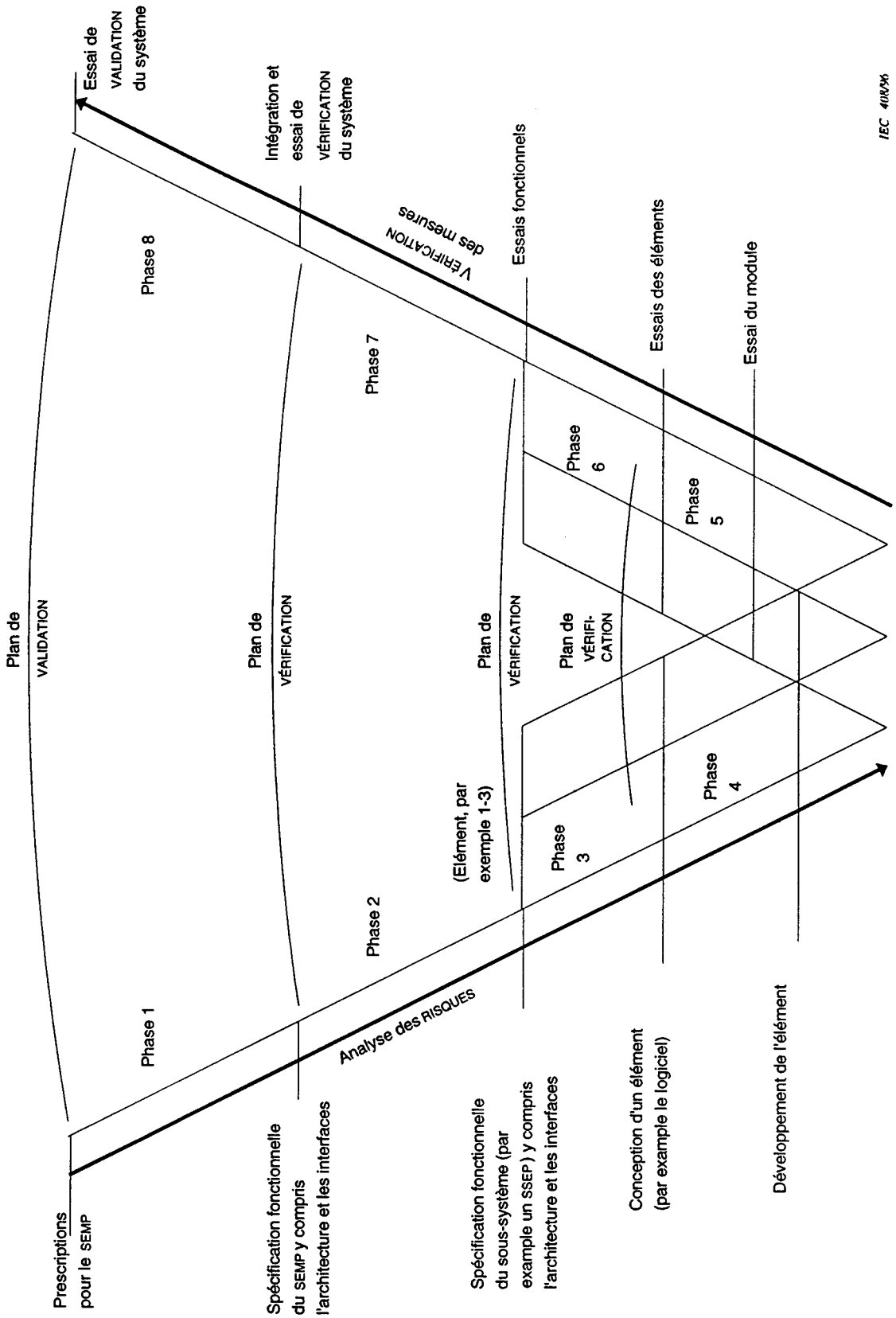


Figure DDD.1 – Modèle de CYCLE DE DÉVELOPPEMENT pour un SEMP

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

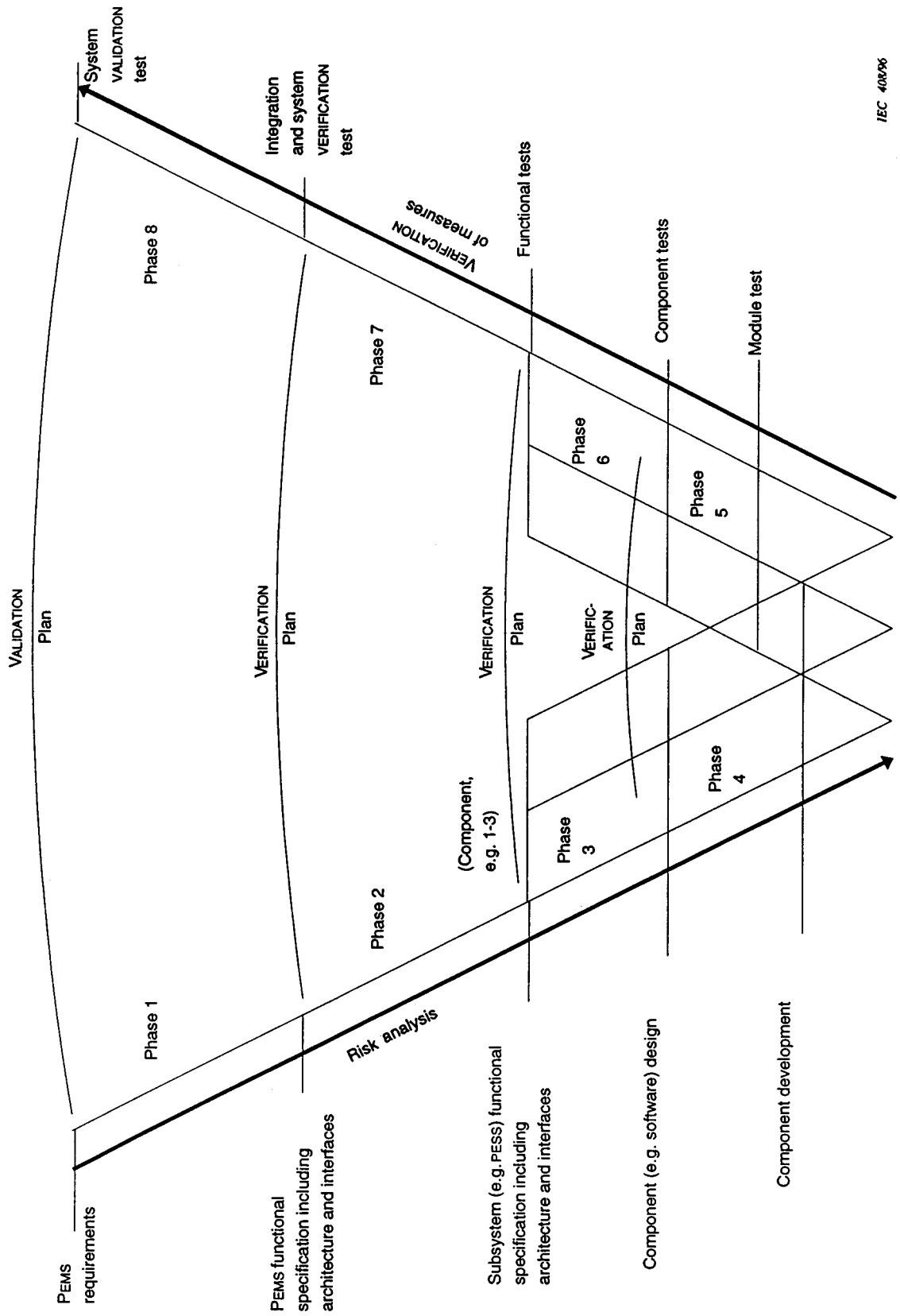


Figure DDD.1 – A DEVELOPMENT LIFE-CYCLE model for PEMS

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

Documentation

La présente Norme Collatérale demande que le CYCLE DE DÉVELOPPEMENT utilisé spécifie les prescriptions de documentation. Elle ne spécifie pas, toutefois, le lien entre la documentation et le CYCLE DE DÉVELOPPEMENT. Le tableau DDD.1 suggère une corrélation entre les prescriptions de documentation et les phases du CYCLE DE DÉVELOPPEMENT.

L'un des documents exigés est le RELEVÉ DE GESTION DES RISQUES. Pour ce dernier, les contributions suivantes pour les différentes phases sont appropriées:

– DANGERS identifiés et leurs causes d'origine..... 52.204.3.1.10
– RISQUES estimés 52.204.3.2.5
– prescriptions pour la maîtrise du RISQUE 52.204.4.5
– référence aux méthodes et résultats de la VÉRIFICATION 52.209.4
– évaluation de l'efficacité de la maîtrise du RISQUE 52.204.4.6

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

Documentation

This Collateral Standard requires that the DEVELOPMENT LIFE-CYCLE used specifies the documentation requirements. It does not, however, specify the relationship of documentation to the DEVELOPMENT LIFE-CYCLE. Table DDD.1 suggests a correlation of the documentation requirements with the DEVELOPMENT LIFE-CYCLE phases.

One of the required documents is the RISK MANAGEMENT SUMMARY. This has the following contributions from all phases as appropriate:

– identified HAZARDS and their initiating causes 52.204.3.1.10
– estimated RISK 52.204.3.2.5
– requirements to control the RISK 52.204.4.5
– reference to VERIFICATION methods and results 52.209.4
– evaluation of effectiveness of RISK control 52.204.4.6

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

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

Tableau DDD.1 – Proposition de corrélation entre les documents prescrits et les phases du CYCLE DE DÉVELOPPEMENT

	Phase							
Document	1	2	3	4	5	6	7	8
DANGERS identifiés et leurs causes d'origine 52.204.3.1.10	*	*	*					
RISQUES estimés..... 52.204.3.2.5	*	*	*					
Prescriptions pour la maîtrise du RISQUE..... 52.204.4.5	*	*	*					
Plan de gestion des RISQUES..... 52.202	*							
CYCLE DE DÉVELOPPEMENT 52.203	*							
Spécification des prescriptions du SEMP.. 52.206	*							
Plan de VÉRIFICATION 52.209.2	*							
Plan de VALIDATION 52.210.2	*							
Spécification des prescriptions du sous-système (par exemple SSEP)..... 52.206		*						
Spécification de l'architecture du SEMP 52.207.2		*						
Spécification de l'architecture du SSEP. 52.207.2			*					
Spécification de conception du sous-système 52.208.1			*					
Spécification d'essai du sous-système. 52.208.1			*	*				
Méthodes et résultats de la VÉRIFICATION 52.209.4				*	*	*	*	
Méthodes et résultats de la VALIDATION 52.210.7								*
Evaluation de l'efficacité de la maîtrise du RISQUE..... 52.204.4.6								*
RISQUE RÉSIDUEL 6.8.201								*
Rapport d'évaluation..... 52.212								*
RELEVÉ DE GESTION DES RISQUES..... 52.201.3	*	*	*	*	*	*	*	*
*) Le document est suggéré pour la phase correspondante.								

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

Table DDD.1 – Suggested correlation of the documentation requirement to the DEVELOPMENT LIFE-CYCLE phases

	Phase							
Document	1	2	3	4	5	6	7	8
Identified HAZARDS and their initiating causes..... 52.204.3.1.10	*	*	*					
Estimated RISK..... 52.204.3.2.5	*	*	*					
Requirements to control RISK..... 52.204.4.5	*	*	*					
RISK management plan..... 52.202	*							
DEVELOPMENT LIFE-CYCLE..... 52.203	*							
PEMS requirement specification..... 52.206	*							
VERIFICATION plan 52.209.2	*							
VALIDATION plan 52.210.2	*							
Subsystem (e.g. PESS) requirement specification 52.206		*						
PEMS architecture specification..... 52.207.2		*						
PESS architecture specification 52.207.2			*					
Subsystem design specification 52.208.1			*					
Subsystem test specification..... 52.208.1			*	*				
VERIFICATION methods and results ... 52.209.4				*	*	*	*	
VALIDATION methods and results 52.210.7								*
Evaluation of effectiveness of the RISK controls 52.204.4.6								*
RESIDUAL RISK..... 6.8.201								*
Assessment report 52.212								*
RISK MANAGEMENT SUMMARY..... 52.201.3	*	*	*	*	*	*	*	*
*) The document is suggested for that phase.								

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

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

Annexe EEE
(informative)

Exemples de structures SEMP/SSEP

Un SEMP peut être un dispositif électromédical très simple ou un SYSTÈME ÉLECTROMÉDICAL complexe ou entre les deux.

La figure EEE.1 montre quelques exemples possibles de SEMP.

La figure EEE.1 a) montre un système complexe. Le SEMP est divisé en un nombre de sous-systèmes majeurs qui, à leur tour, sont décomposés en sous-systèmes comportant un SSEP.

La figure EEE.1 b) montre un système plus simple. Dans ce cas, le niveau intermédiaire du sous-système majeur n'existe pas et le SSEP est un sous-système du SEMP lui-même.

La figure EEE.1 c) illustre le système le plus simple de SEMP. Dans ce cas, le SEMP et le SSEP sont un seul et même système.

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

Annex EEE
(informative)

Examples for PEMS/PESS structures

A PEMS can be a very simple medical electrical device or a complex MEDICAL ELECTRICAL SYSTEM or anything in between.

Figure EEE.1 shows some possible examples of a PEMS.

Figure EEE.1 a) shows a complex system. The PEMS breaks down into a number of major subsystems which in turn are made up of subsystems which include a PESS.

Figure EEE.1 b) shows a simpler implementation. In this case the intermediate major subsystem level is missing and the PESS is a subsystem of the PEMS itself.

Figure EEE.1 c) illustrates the simplest implementation of a PEMS. In this case the PEMS and the PESS are the same.

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

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

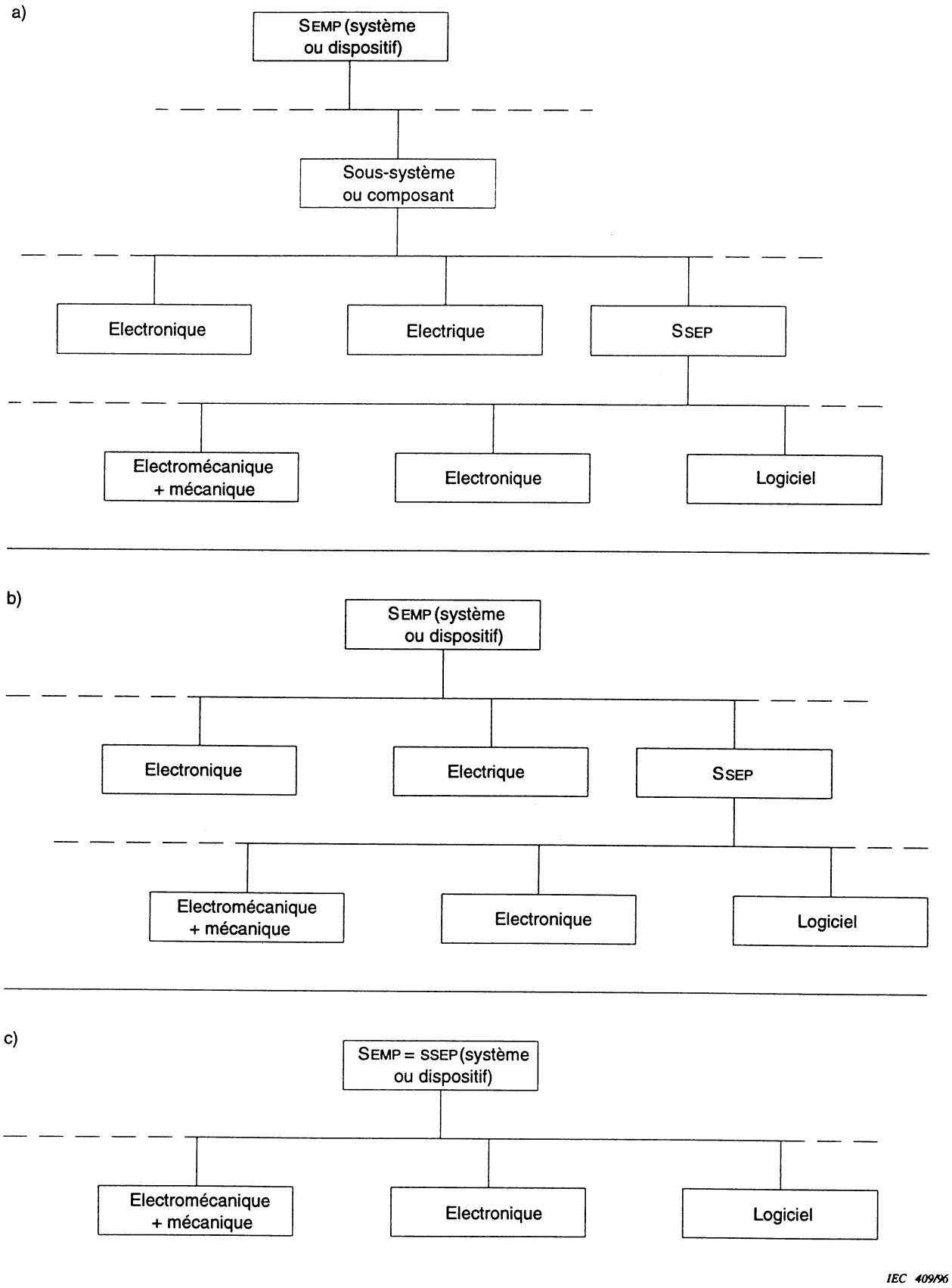


Figure EEE.1 – Exemples de structures SEMP/SSEP

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

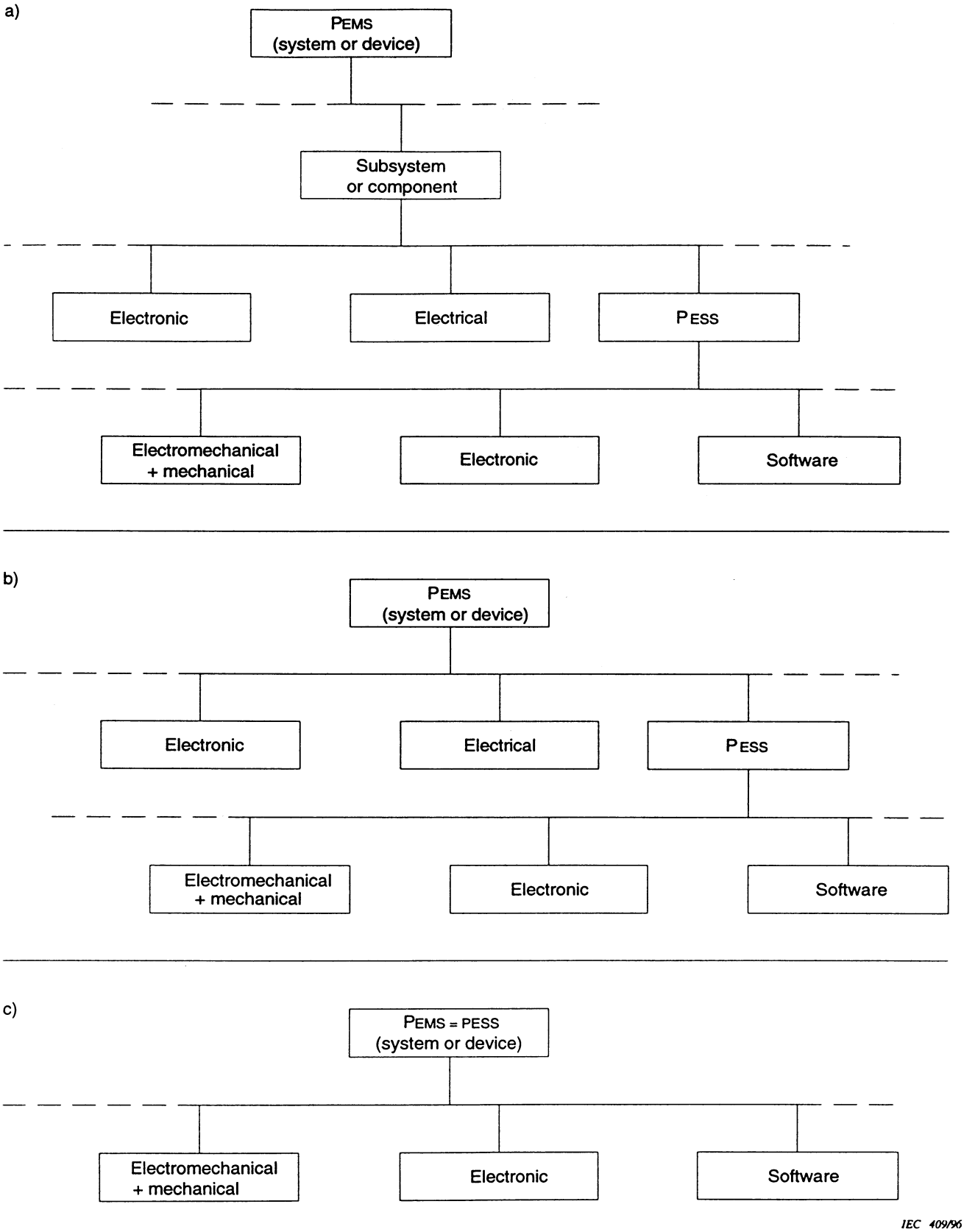


Figure EEE.1 – Examples of PEMS/PESS structures

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

Annexe FFF
(informative)

Bibliographie

La présente annexe donne une liste des documents qui servent de guide pour les méthodes et les procédures de traitement des RISQUES.

[1] CEI 60513:1994, *Aspects fondamentaux des normes de sécurité pour les appareils électromédicaux*

[2] CEI 60812:1985, *Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

[3] CEI 60880:1986, *Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires*

Compléments à la CEI 60880 (45A(Sec)189 CD et 45(UK)98)

[4] CEI 61025:1990, *Analyse par arbre de panne (AAP)*

[5] CEI 61508, *Sûreté fonctionnelle – Systèmes relatifs à la sûreté* (à l'étude)

Partie 1: Prescriptions générales

Partie 2: Prescriptions pour les systèmes électroniques programmables

Partie 3: Prescriptions concernant les logiciels

Partie 4: Définitions et abréviations

Partie 5: Lignes directrices pour la mise en oeuvre de la Partie 1

Partie 6: Lignes directrices pour l'application des Parties 2 et 3

Partie 7: Bibliographie des techniques et des mesures

[6] ISO/CEI 12119:1994, *Technologie de l'information – Logiciels – Prescriptions pour la qualité et essais* (publiée actuellement en anglais seulement)

[7] ISO/CEI 15026, *Niveaux d'intégrité des systèmes et des logiciels* (à l'étude)

[8] prEN 1441, *Dispositifs électromédicaux – Analyse des risques* (à l'étude)

———————

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

Annex FFF
(informative)

Bibliography

This annex lists references which give guidance on methods and processes used to manage RISKS.

[1] IEC 60513:1994, *Fundamental aspects of safety standards for medical electrical equipment*

[2] IEC 60812:1985, *Analysis techniques for system reliability – Procedure for failure modes and effects analysis (FMEA)*

[3] IEC 60880:1986, *Software for computers in the safety systems of nuclear power stations*
Supplements to IEC 60880 (45A(Sec)189 CD and 45(UK)98)

[4] IEC 61025:1990, *Fault tree analysis (FTA)*

[5] IEC 61508, *Functional safety – Safety-related systems* (in preparation)
Part 1: General requirements
Part 2: Requirements for electrical/electronic/programmable electronic systems
Part 3: Software requirements
Part 4: Definitions and abbreviations of terms
Part 5: Guidelines on the application of Part 1
Part 6: Guidelines on the application of Parts 2 and 3
Part 7: Bibliography of techniques and measures

[6] ISO/IEC 12119:1994, *Information technology – Software packages – Quality requirements and testing*

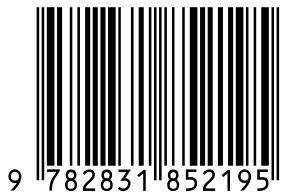
[7] ISO/IEC 15026, *Systems and software integrity level* (in preparation)

[8] prEN 1441, *Medical devices/Risk analysis* (in preparation)

———————

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

ISBN 2-8318-5219-6



ICS 11.040.01

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