

SPÉCIFICATION TECHNIQUE

**CEI
IEC**

TECHNICAL SPECIFICATION

TS 61000-1-2

Première édition
First edition
2001-06

PUBLICATION FONDAMENTALE EN CEM
BASIC EMC PUBLICATION

Compatibilité électromagnétique (CEM) –

Partie 1-2:

**Généralités – Méthodologie pour la réalisation
de la sécurité fonctionnelle des matériels
électriques et électroniques du point de vue
des phénomènes électromagnétiques**

Electromagnetic compatibility (EMC) –

Part 1-2:

**General – Methodology for the achievement
of the functional safety of electrical and
electronic equipment with regard to
electromagnetic phenomena**



Numéro de référence
Reference number
CEI/IEC/TS 61000-1-2:2001

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/catlg-f.htm) 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/JP.htm) 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/catlg-e.htm) 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/JP.htm) 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

SPÉCIFICATION TECHNIQUE

**CEI
IEC**

TECHNICAL SPECIFICATION

TS 61000-1-2

Première édition
First edition
2001-06

PUBLICATION FONDAMENTALE EN CEM
BASIC EMC PUBLICATION

Compatibilité électromagnétique (CEM) –

**Partie 1-2:
Généralités – Méthodologie pour la réalisation
de la sécurité fonctionnelle des matériels
électriques et électroniques du point de vue
des phénomènes électromagnétiques**

Electromagnetic compatibility (EMC) –

**Part 1-2:
General – Methodology for the achievement
of the functional safety of electrical and
electronic equipment with regard to
electromagnetic phenomena**

© IEC 2001 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
Telefax: +41 22 919 0300

3, rue de Varembe Geneva, Switzerland
e-mail: inmail@iec.ch IEC web site <http://www.iec.ch>



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

XA

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

SOMMAIRE

AVANT-PROPOS.....	4
INTRODUCTION.....	8
1 Domaine d'application et objet.....	10
2 Références normatives.....	10
3 Définitions et abréviations	14
4 Considérations générales	20
5 Réalisation de la sécurité fonctionnelle.....	20
5.1 Cycle de vie de sécurité	20
5.2 Etapes de réalisation de la sécurité fonctionnelle	22
6 Environnement électromagnétique.....	28
7 Exigences de sécurité et critères de défaillances.....	30
8 Analyse de la sûreté de fonctionnement	32
8.1 Considérations générales relatives au choix d'une méthode appropriée	32
8.2 Application de l'analyse par arbre de panne aux perturbations électromagnétiques	34
9 Essais CEM relatifs à la sécurité	36
9.1 Importance et nécessité des essais.....	36
9.2 Types et niveaux d'essais EM relatifs à la sécurité.....	36
9.3 Fonctionnement du matériel pendant les essais	38
9.4 Mettre l'accent sur les événements indésirables (matériels/logiciels).....	38
9.5 Favoriser les effets observables.....	38
9.6 Critères de performances	40
9.7 Validation et documentation de la planification des essais.....	40
10 Compte rendu.....	40
Annexe A (informative) Exemples de niveaux d'essai d'immunité CEM	44
Annexe B (informative) Exemples d'analyses de sûreté de fonctionnement du point de vue des phénomènes électromagnétiques.....	50
Annexe C (informative) Considérations de conception et d'installation.....	90
Annexe D (informative) Liste de contrôle type des mesures et techniques permettant de réaliser la sécurité fonctionnelle du point de vue des perturbations CEM	98
Annexe E (informative) Techniques d'analyse de la sûreté de fonctionnement et application du point de vue de la CEM	102
Bibliographie.....	110

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	9
1 Scope and object.....	11
2 Normative references	11
3 Definitions and abbreviations.....	15
4 General considerations.....	21
5 The achievement of functional safety.....	21
5.1 Safety life cycle.....	21
5.2 Steps for the achievement of functional safety.....	23
6 The electromagnetic environment.....	29
7 Safety requirements and failure criteria	31
8 Dependability analysis.....	33
8.1 General considerations for the choice of an appropriate method.....	33
8.2 Application of the fault tree analysis to electromagnetic disturbances.....	35
9 EMC testing with regard to safety.....	37
9.1 Importance and need for testing.....	37
9.2 Types and EM test levels with regard to safety.....	37
9.3 Operation of the equipment during testing.....	39
9.4 Focus on undesirable events (hardware/software).....	39
9.5 Promote observable effects.....	39
9.6 Performance criteria.....	41
9.7 Test planning validation and documentation	41
10 Report.....	41
Annex A (informative) Examples of EMC immunity test levels	45
Annex B (informative) Examples of dependability analyses with regard to electromagnetic phenomena	51
Annex C (informative) Design and installation considerations	91
Annex D (informative) Typical check list of measures and techniques for the achievement of functional safety with regard to EMC disturbances	99
Annex E (informative) Dependability analysis techniques and their application with regard to EMC	103
Bibliography.....	111

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

COMPATIBILITÉ ÉLECTROMAGNÉTIQUE (CEM) –

Partie 1-2: Généralités – Méthodologie pour la réalisation de la sécurité fonctionnelle des matériels électriques et électroniques du point de vue des phénomènes électromagnétiques

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 spécification technique 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 tâche principale des comités d'études de la CEI est l'élaboration des Normes internationales. Exceptionnellement, un comité d'études peut proposer la publication d'une spécification technique

- lorsqu'en dépit de maints efforts, l'accord requis ne peut être réalisé en faveur de la publication d'une Norme internationale, ou
- lorsque le sujet en question est encore en cours de développement technique ou quand, pour une raison quelconque, la possibilité d'un accord pour la publication d'une Norme internationale peut être envisagée pour l'avenir mais pas dans l'immédiat;

La CEI 61000-1-2, qui est une spécification technique, a été établie par le comité d'études 77 de la CEI: Compatibilité électromagnétique. Elle a le statut de publication fondamentale en CEM conformément au Guide 107 de la CEI.

Le texte de cette spécification technique est issu des documents suivants:

Projet d'enquête	Rapport de vote
77/231/CDV	77/235/RVC

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ELECTROMAGNETIC COMPATIBILITY (EMC) –**Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena**

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 technical specification may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

IEC 61000-1-2, which is a technical specification, has been prepared by technical committee 77: Electromagnetic compatibility. It has the status of a basic EMC publication in accordance with IEC Guide 107.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
77/231/CDV	77/235/RVC

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

Cette publication a été rédigée selon les Directives ISO/CEI, partie 3.

Les annexes A, B, C, D et E sont données seulement à titre d'information.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2005.
A cette date, la publication sera

- transformée en Norme internationale;
- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

Withdrawn

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

Annexes A, B, C, D, and E are for information only.

The committee has decided that the contents of this publication will remain unchanged until 2005. At this date, the publication will be:

- transformed into an International Standard;
- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

Withdrawn

INTRODUCTION

La norme CEI 61000 est publiée en parties séparées, conformément à la structure suivante:

Partie 1: Généralités

Considérations générales (introduction, principes fondamentaux)

Définitions, terminologie

Partie 2: Environnement

Description de l'environnement

Classification de l'environnement

Niveaux de compatibilité

Partie 3: Limites

Limites d'émissions

Limites d'immunité (dans la mesure où elles ne tombent pas sous la responsabilité des comités de produits)

Partie 4: Techniques d'essai et de mesure

Techniques de mesure

Techniques d'essai

Partie 5: Directives d'installation et d'atténuation

Guides d'installation

Méthodes et dispositifs d'atténuation

Partie 6: Normes génériques

Partie 9: Divers

Chaque partie est à son tour subdivisée en plusieurs parties, publiées soit comme Normes internationales, soit comme spécifications techniques ou rapports techniques, dont certaines ont déjà été publiées en tant que sections. D'autres seront publiées sous le numéro de la partie, suivi d'un tiret et complété d'un second chiffre identifiant la subdivision (exemple: 61000-3-11)

Il convient que le fonctionnement du matériel électrique ou électronique ne soit pas affecté par les influences extérieures au point d'entraîner un danger inacceptable pour les utilisateurs, les autres personnes, les animaux ou les biens. Il convient qu'une étude de sécurité complète prenne en compte divers facteurs de nature climatique, mécanique, électrique, voire même les cas de mauvaises utilisations raisonnablement prévisibles. Des perturbations électromagnétiques sont présentes dans la plupart des environnements, et il convient donc qu'elles soient prises en compte par ladite analyse.

L'objet de la présente spécification technique est de fournir des indications concernant la réalisation de la sécurité fonctionnelle des matériels électriques et électroniques exposés aux perturbations électromagnétiques. Aux fins de cohérence au sein de la CEI, cette spécification technique utilise, chaque fois que possible, les normes fondamentales applicables de la CEI. Elle prend en particulier en compte les travaux du SC 65A relatifs aux concepts de sécurité (c'est-à-dire la CEI 61508), les travaux du CE 56 relatifs aux méthodes d'évaluation (c'est-à-dire les normes CEI 60300-3-1 et CEI 61025) et bien sûr les travaux du CE 77, de ses sous-comités et du CISPR, relatifs aux environnements électromagnétiques. Il convient de se reporter aux normes de ces comités pour tous détails sur ces sujets.

INTRODUCTION

IEC 61000 is published in separate parts according to the following structure:

Part 1: General

General considerations (introduction, fundamental principles)

Definitions, terminology

Part 2: Environment

Description of the environment

Classification of the environment

Compatibility levels

Part 3: Limits

Emission limits

Immunity limits (insofar as they do not fall under the responsibility of the product committees)

Part 4: Testing and measurement techniques

Measurement techniques

Testing techniques

Part 5: Installation and mitigation guidelines

Installation guidelines

Mitigation methods and devices

Part 6: Generic standards

Part 9: Miscellaneous

Each part is further subdivided into several parts, published either as International Standards or technical reports, some of which have already been published as sections. Others will be published with the part number followed by a dash and completed by a second number identifying the subdivision (example: 61000-3-11).

The function of electrical or electronic equipment should not be affected by external influences in a way which could lead to an unacceptable risk of harm to the users, other persons, animals or property. A comprehensive safety analysis should consider various factors of climatic, mechanical, electrical nature and even reasonably foreseeable misuse. Electromagnetic disturbances are present in most environments and should therefore be considered during such an analysis.

The purpose of this document is to provide guidance relating to the achievement of functional safety of electrical or electronic equipment exposed to electromagnetic disturbances. With respect to consistency within IEC, the document makes use, as far as appropriate, of existing relevant basic IEC standards. It considers in particular the work of SC 65A relating to safety concepts (e.g. IEC 61508), of TC 56 relating to assessment methods (e.g. IEC 60300-3-1 and IEC 61025) and of course of TC 77, its subcommittees and CISPR relating to the electromagnetic environments. For details on these subjects reference should be made to the standards of these committees.

COMPATIBILITÉ ÉLECTROMAGNÉTIQUE (CEM) –

Partie 1-2: Généralités – Méthodologie pour la réalisation de la sécurité fonctionnelle des matériels électriques et électroniques du point de vue des phénomènes électromagnétiques

1 Domaine d'application et objet

La présente spécification technique spécifie une méthodologie pour la réalisation de la sécurité fonctionnelle du point de vue des phénomènes électromagnétiques (EM) des matériels électriques et électroniques: appareils, systèmes et installations, installés et utilisés en conditions opérationnelles.

Elle spécifie des procédures pour

- la détermination des exigences;
- les prescriptions;
- les aspects relatifs à la conception, y compris l'installation du matériel;
- les méthodes analytiques d'évaluation;
- les recommandations relatives aux essais;
- la documentation.

Elle ne porte pas sur les risques directs que font courir les champs électromagnétiques aux êtres vivants, ni sur la sécurité liée au claquage d'un isolant ou d'autres mécanismes, par lesquels les personnes peuvent être exposées aux risques électriques.

La présente spécification technique s'applique à l'influence de l'environnement électromagnétique, y compris les dispositifs avoisinants, sur les appareils et les systèmes petits ou gros, mais pas à l'influence des sources internes contenues dans les appareils, qu'il y a lieu de prendre en compte dans le cadre de leur conception.

Elle est destinée aux comités de produits, aux concepteurs, constructeurs et installateurs de matériels et de systèmes.

Elle porte sur les méthodes d'analyse de sécurité et d'essais liées aux influences électromagnétiques. En ce qui concerne les méthodes quantitatives d'évaluation, c'est-à-dire la probabilité de défaillance, les méthodes décrites dans la série CEI 61508 peuvent être appliquées.

2 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 spécification technique. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente spécification technique sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

ELECTROMAGNETIC COMPATIBILITY (EMC) –

Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena

1 Scope and object

This technical specification specifies a methodology for the achievement of functional safety with regard to electromagnetic (EM) phenomena of electrical and electronic equipment: apparatuses, systems and installations, as installed and used under operational conditions.

It specifies procedures for

- determining requirements;
- requirements;
- design aspects including installation of the equipment;
- analytical assessment methods;
- testing recommendations;
- documentation.

It is not concerned with direct hazards from electromagnetic fields on living beings nor is it concerned with safety related to breakdown of insulation or other mechanisms by which persons can be exposed to electrical hazards.

This technical specification applies to the influence of the electromagnetic environment including adjacent devices on apparatuses and small or large systems, however not to the influence of internal sources in the apparatuses, which have to be considered in relation with their design.

It is intended for product committees, designers, manufacturers and installers of equipment and systems.

This document is focused on the safety analysis and testing methods related to electromagnetic influences. With regard to quantitative assessment methods, i.e. probability of failures, the methods described in the IEC 61508 series can be applied.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this technical specification. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this technical specification are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

CEI 60050(161):1990, *Vocabulaire Electrotechnique International (VEI). Chapitre 161: Compatibilité électromagnétique*

CEI 60050(191):1990, *Vocabulaire Electrotechnique International (VEI). Chapitre 191: Sûreté de fonctionnement et qualité de service*

ISO/CEI Guide 51:1999, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

CEI 60300-3-1:1991, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application – Section 1: Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique*

CEI 61000-1-1:1992, *Compatibilité électromagnétique (CEM) – Partie 1: Généralités – Section 1: Application et interprétation de définitions et termes fondamentaux*

CEI 61000-2 (toutes les parties), *Compatibilité électromagnétique (CEM) – Partie 2: Environnement*

CEI 61000-4 (toutes les parties), *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure*

CEI 61000-4-1:2000, *Compatibilité électromagnétique (CEM) – Partie 4-1: Techniques d'essai et de mesure – Vue d'ensemble de la série CEI 61000-4*

NOTE La CEI 61000-4-1 donne des informations générales sur tous les essais fondamentaux d'immunité.

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

CEI 61508-1:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-2:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-3:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

CEI 61508-4:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61508-5:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

CEI 61508-6:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

CEI 61508-7:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

IEC 60050(161):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 161: Electromagnetic compatibility*

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

IEC 60300-3-1:1991, *Dependability management – Part 3: Application guide – Section 1: Analysis techniques for dependability: Guide on methodology*

IEC 61000-1-1:1992, *Electromagnetic compatibility (EMC) – Part 1: General – Section 1: Application and interpretation of fundamental definitions and terms*

IEC 61000-2 (all parts), *Electromagnetic compatibility (EMC) – Part 2: Environment*

IEC 61000-4 (all parts), *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques*

IEC 61000-4-1:2000, *Electromagnetic compatibility (EMC) – Part 4-1: Testing and measurement techniques – Overview of IEC 61000-4 series*

NOTE IEC 61000-4-1 provides general information on all the basic immunity tests.

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

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

3 Définitions et abréviations

Pour les besoins de la présente spécification technique, les définitions données dans la CEI 60050(161) et la CEI 60050(191), ainsi que les suivantes, s'appliquent.

3.1

perturbation électromagnétique

phénomène électromagnétique susceptible de créer des troubles de fonctionnement d'un dispositif, d'un appareil ou d'un système, ou d'affecter défavorablement la matière vivante ou inerte

NOTE Une perturbation électromagnétique peut être un bruit électromagnétique, un signal non désiré ou une modification du milieu de propagation lui-même.

[VEI 161-01-05]

3.2

brouillage électromagnétique

trouble apporté au fonctionnement d'un appareil, d'une voie de transmission ou d'un système par une perturbation électromagnétique

[VEI 161-01-06]

NOTE La perturbation et le brouillage sont respectivement la cause et l'effet.

3.3

compatibilité électromagnétique (CEM)

aptitude d'un appareil ou d'un système à fonctionner dans son environnement électromagnétique de façon satisfaisante sans produire lui-même des perturbations électromagnétiques intolérables pour tout ce qui se trouve dans cet environnement

[VEI 161-01-07]

3.4

niveau de compatibilité électromagnétique

niveau de perturbation électromagnétique utilisé comme niveau de référence pour assurer la coordination de l'établissement des limites d'émission et d'immunité

[VEI 161-03-10, modifiée]

NOTE 1 Par convention, le niveau de compatibilité est choisi de telle sorte qu'il n'ait qu'une faible probabilité d'être dépassé par le niveau réel de perturbation. Cela étant, la compatibilité électromagnétique n'est assurée que si les niveaux d'émission et d'immunité sont maîtrisés de telle sorte qu'en chaque endroit le niveau de perturbation résultant de l'ensemble des émissions soit plus faible que le niveau d'immunité de chaque dispositif, appareil ou système situé en ce même endroit.

NOTE 2 Le niveau de compatibilité peut dépendre du phénomène, du temps ou de l'endroit.

3.5

environnement électromagnétique

ensemble des phénomènes électromagnétiques existant à un endroit donné

[VEI 161-01-01]

3.6

sûreté de fonctionnement

ensemble des propriétés qui décrivent la disponibilité et les facteurs qui la conditionnent: fiabilité, maintenabilité et logistique de maintenance

NOTE La sûreté de fonctionnement est une notion générale sans caractère quantitatif.

[VEI 191-02-03]

3 Definitions and abbreviations

For the purposes of this technical specification, the definitions contained in IEC 60050(161) and IEC 60050(191), as well as the following apply.

3.1

electromagnetic disturbance

any electromagnetic phenomenon which may degrade the performance of a device, equipment or system, or adversely affect living or inert matter

NOTE An electromagnetic disturbance may be an electromagnetic noise, an unwanted signal or a change in the propagation medium itself.

[IEV 161-01-05]

3.2

electromagnetic interference (EMI)

degradation of the performance of an equipment, transmission channel or system caused by an electromagnetic disturbance

[IEV 161-01-06]

NOTE Disturbance and interference are respectively cause and effect.

3.3

electromagnetic compatibility (EMC)

ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment

[IEV 161-01-07]

3.4

electromagnetic compatibility level

specified electromagnetic disturbance level used as a reference level for co-ordination in the setting of emission and immunity limits

[IEV 161-03-10, modified]

NOTE 1 By convention, the compatibility level is chosen so that there is only a small probability that it will be exceeded by the actual disturbance level. However electromagnetic compatibility is achieved only if the emission and immunity levels are controlled such that, at each location, the disturbance level resulting from the cumulative emissions is lower than the immunity level for each device, equipment and system situated at the same location.

NOTE 2 The compatibility level may be phenomena-, time- or location-dependent.

3.5

electromagnetic environment

the totality of electromagnetic phenomena existing at a given location

[IEV 161-01-01]

3.6

dependability

collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance

NOTE Dependability is used only for general descriptions in non-quantitative terms.

[IEV 191-02-03]

3.7

dégradation (de fonctionnement)

écart non désiré des caractéristiques de fonctionnement d'un dispositif, d'un appareil ou d'un système par rapport aux caractéristiques attendues

NOTE Une dégradation peut être un défaut de fonctionnement temporaire ou permanent.

[VEI 161-01-19]

3.8

défaillance

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

[VEI 191-04-01]

3.9

panne

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

[VEI 191-05-01]

NOTE

- a) Une «défaillance» est un événement par opposition à une «panne» qui est un état.
- b) A la suite d'une défaillance, l'entité est en panne.
- c) Ce concept ne s'applique pas aux entités constituées uniquement de logiciel.
- d) Une panne est souvent la conséquence d'une défaillance de l'entité elle-même, mais elle peut exister sans défaillance préalable.

3.10

dommage

blessure physique ou atteinte à la santé des personnes, ou atteinte aux biens ou à l'environnement

[ISO/CEI Guide 51:1999, définition 3.3]

3.11

phénomène dangereux

source potentielle de dommage

[ISO/CEI Guide 51:1999, définition 3.5]

3.12

risque

combinaison de la probabilité d'un dommage et de sa gravité

[ISO/CEI Guide 51:1999, définition 3.2]

3.13

mauvais usage raisonnablement prévisible

utilisation d'un produit, procédé ou service dans des conditions ou à des fins non prévues par le fournisseur mais qui peuvent provenir d'un comportement humain envisageable

[ISO/CEI Guide 51:1999, définition 3.14]

3.14

sécurité fonctionnelle

absence de risque de dommage inacceptable dû au mauvais fonctionnement d'un matériel ou d'un système, y compris celui résultant d'un mauvais usage raisonnablement prévisible

3.7**degradation (of performance)**

undesired departure in the operational performance of any device, equipment or system from its intended performance

NOTE The term "degradation" can apply to temporary or permanent failure.

[IEV 161-01-19]

3.8**failure**

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

[IEV 191-04-01]

3.9**fault**

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

[IEV 191-05-01]

NOTE

- a) "Failure" is an event, as distinguished from "fault", which is a state.
- b) After failure the item has a fault.
- c) This concept as defined does not apply to items consisting of software only.
- d) A fault is often the result of a failure of the item itself, but may exist without prior failure.

3.10**harm**

physical injury and/or damage to health or property

[ISO/IEC Guide 51:1999, definition 3.3]

3.11**hazard**

potential source of harm

[ISO/IEC Guide 51:1999, definition 3.5]

3.12**risk**

probable rate of occurrence of a hazard causing harm and the degree of severity of the harm

[ISO/IEC Guide 51:1999, definition 3.2]

3.13**reasonably foreseeable misuse**

use of a product, process or service under conditions or for purposes not intended by the supplier, but which may happen, induced by the design of the product in combination with, or as result of, common human behaviour

[ISO/IEC Guide 51:1999, definition 3.14]

3.14**functional safety**

freedom from an unacceptable risk of harm due to the malfunctioning of the equipment or a system including that resulting from reasonably foreseeable misuse

3.15

intégrité de la sécurité

probabilité pour qu'un matériel électrique ou électronique exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et dans une période de temps spécifiée

[CEI 61508-4:1998, définition 3.5.2, modifiée]

3.16

validation

confirmation par examen et apport de preuves objectives que les exigences particulières à une utilisation prévue spécifiée sont remplies

[ISO 9000:2000, définition 3.8.5]

3.17

analyse par arbre de panne (AAP)

méthode déductive (descendante) pour l'analyse de la sûreté de fonctionnement d'un système

3.18

événement de base

dans l'analyse par arbre de panne, événement d'entrée unique – au pied de l'arbre de panne – qui est susceptible d'influencer le fonctionnement du matériel ou du système considéré

NOTE 1 Un événement de base peut être un événement indépendant (voir note 2) ou la sortie d'un autre arbre de panne.

NOTE 2 Dans le contexte de la présente spécification technique, un événement de base est une perturbation électromagnétique.

3.19

événement de tête

dans l'analyse par arbre de panne, événement de sortie – en haut de l'arbre – résultant de l'effet d'un état externe, interne ou autre

NOTE Dans le contexte de la présente spécification technique, l'événement de tête est une situation dangereuse qu'il convient d'éviter.

3.20

appareil (dans le contexte des documents de CEM)

matériel unique ayant une ou plusieurs fonctions directes destinées à une utilisation finale

3.21

système (dans le contexte des documents de CEM)

combinaison d'appareils et/ou de composants actifs constituant une unité fonctionnelle unique et destinés à être installés et exploités pour assurer une ou plusieurs tâches spécifiques

NOTE Les «systèmes relatifs à la sécurité» sont des matériels spécialement «conçus» qui:

- mettent en œuvre les fonctions de sécurité requises pour atteindre un état de sécurité d'un matériel commandé ou pour maintenir un tel état;
- sont prévus pour atteindre, par eux mêmes ou avec d'autres matériels de sécurité ou moyens de réduction des risques, le niveau d'intégrité de sécurité nécessaire à la mise en œuvre des fonctions de sécurité requises.

[CEI 61508-4, définition 3.4.1 modifiée]

3.22

installation (dans le contexte des documents de CEM)

combinaison d'appareils, composants et systèmes assemblés et/ou montés (individuellement) dans une zone donnée. Pour des raisons physiques (comme par exemple des distances importantes entre les différents éléments) il est dans de nombreux cas impossible de soumettre à essai une installation en tant qu'unité

3.15**safety integrity**

probability that electric or electronic equipment will perform satisfactorily with regards to the safety functions under all the stated conditions within a stated period of time

[IEC 61508-4, 1998, definition 3.5.2, modified]

3.16**validation**

confirmation by examination and provision of objective evidence that the particular requirements for a specified intended use are fulfilled

[ISO 9000:2000, definition 3.8.5]

3.17**fault tree analysis (FTA)**

deductive (top-down) method for analysing system dependability

3.18**basic event**

in fault tree analysis, a single input event – at the bottom of the fault tree – which may influence the operation of the considered equipment or system

NOTE 1 A basic event may be an independent event (see note 2) or the output of another fault tree.

NOTE 2 In the context of this technical specification a basic event is an electromagnetic disturbance.

3.19**top event**

in fault tree analysis, the output event – at the top of the fault tree – resulting from the effect of all external, internal and other conditions

NOTE In the context of this technical specification the top event represents a hazardous situation which should be avoided.

3.20**apparatus (in the context of EMC documents)**

a single piece of equipment with (a) direct function(s) intended for final use

3.21**system (in the context of EMC documents)**

a combination of apparatuses and/or active components constituting a single functional unit and intended to be installed and operated to perform (a) specific task(s)

NOTE "Safety related systems" are specifically "designed" equipment that both:

- implement the required safety functions necessary to achieve or maintain a safe state for a controlled equipment ;
- are intended to achieve on their own or with other safety-related equipment or external risk reduction facilities, the necessary safety integrity for the required safety requirements.

[IEC 61508-4, definition 3.4.1, modified]

3.22**installation (in the context of EMC documents)**

a combination of apparatuses, components and systems assembled and/or erected (individually) in a given area. For physical reasons (e.g. long distances between individual items) it is in many cases not possible to test an installation as a unit

4 Considérations générales

Des perturbations électromagnétiques peuvent influencer la sécurité fonctionnelle du matériel ou du système.

L'objet, du point de vue de la CEM et de la sécurité fonctionnelle, est d'évaluer les éventuels effets des perturbations électromagnétiques sur le risque total, et de concevoir, fabriquer et installer le matériel ou le système de manière à ce que ces phénomènes ne contribuent pas au risque dans des mesures dépassant le tolérable.

Il est à noter que le matériel ou le système peut comprendre, outre les éléments (pièces et composants) nécessaires à la réalisation de ses fonctions, des éléments ou sous-systèmes et fonctions de sécurité spéciaux. Une attention particulière sera accordée à la sécurité fonctionnelle de ces éléments [voir les parties 1 à 7 de la CEI 61508].

Le fonctionnement correct et, dans le contexte de la présente spécification technique, sûr, d'un matériel ou système électrique ou électronique dépend de deux facteurs:

- l'environnement électromagnétique et les niveaux d'émission des diverses sources;
- l'immunité des dispositifs influencés.

Pour ce qui concerne les émissions électromagnétiques, les niveaux d'émission maximaux autorisés sont spécifiés par les comités horizontaux compétents¹, et leur dépassement n'est pas autorisé en conditions normales. Toutefois, un tel dépassement peut se produire en conditions anormales.

Pour ce qui concerne l'immunité, il convient de prendre en compte les effets d'une variation de performance en fonction de la distribution statistique des produits de série ainsi que les effets éventuels du vieillissement.

Ces deux aspects de la CEM doivent être pris en compte lors de la spécification des exigences de sécurité; des marges de sécurité appropriées peuvent également être nécessaires.

La nécessité d'intégrer un essai portant sur l'influence d'un phénomène électromagnétique sur le comportement d'un matériel à une norme (ou à un article d'une norme) de CEM, ou à une norme (ou à un article d'une norme) de sécurité, dépend du critère d'approbation:

- s'il est exigé que pendant ou après l'essai le matériel continue de fonctionner comme prévu, il convient d'inclure l'essai à une norme (ou à un article d'une norme) traitant de l'immunité CEM d'un produit (famille de produits);
- s'il est exigé que pendant ou après l'essai aucune situation dangereuse ne se produise (les performances peuvent être dégradées temporairement ou de manière permanente, mais ne doivent pas produire de situation dangereuse), il convient d'intégrer l'essai à une norme (ou à un article d'une norme) de sécurité. Il va de soi que pour des produits assurant des fonctions de sécurité, des niveaux d'immunité supérieurs à ceux des normes génériques pour cet environnement peuvent être choisis.

5 Réalisation de la sécurité fonctionnelle

5.1 Cycle de vie de sécurité

La réalisation de la sécurité fonctionnelle exige la prise en compte de la CEM pendant tout le cycle de vie du matériel ou du système, de la conception au retrait du service. Cette prise en compte est représentée à la figure 1 pour les matériels individuels et à la figure 2 pour les systèmes.

¹ CE 77 et CISPR essentiellement.

4 General considerations

Electromagnetic disturbances can influence the functional safety of the equipment or system.

The aim with regard to EMC and functional safety is to assess the possible effects of electromagnetic disturbances on the total risk and to design, manufacture and install the equipment or system so that there will be no more than a tolerable risk contribution from these phenomena.

It shall be noted that the equipment or system may comprise, in addition to the elements (parts and components) necessary for the achievement of its functions, special safety-related elements or subsystems and functions. Particular attention has to be given to the functional safety of these parts [see parts 1 to 7 of IEC 61508].

The correct and – in the context of this document – safe operation of an electrical or electronic equipment or system depends on two factors:

- the EM environment and the emission levels of the various sources;
- the immunity of the influenced devices.

As for the EM emissions, the allowed maximum emission levels are specified by the relevant committees¹, and it is not allowed under normal conditions to exceed these levels. However, this can occur occasionally under abnormal conditions.

As for immunity, the effects of a variation in performance according to statistical distribution for mass products and also the possible effects of ageing should be considered.

These two aspects of EMC shall be taken into account when specifying safety requirements and appropriate safety margins may be necessary.

Whether a test on the influence of an electromagnetic phenomenon on the behaviour of an equipment should be included in an EMC standard (or clause) or in a safety standard (or clause) is dependent on the approval criterion:

- If it is required that during or after the test the equipment continue to operate as intended, the test should be included in an EMC immunity standard (or clause) of a product (product family).
- If it is required that during or after the test no unsafe situation occurs (performance may be degraded incidentally or permanently, but not resulting in an unsafe situation), the test should be included in a safety standard (or clause). It is obvious that for products with safety functions the immunity levels may be chosen to be higher than in the generic standards for that environment.

5 The achievement of functional safety

5.1 Safety life cycle

The achievement of functional safety requires consideration to be given to EMC throughout the life cycle of the equipment or system from the concept stage to decommissioning. This is represented for individual equipment in figure 1, for systems in figure 2.

¹ Mainly TC 77 and CISPR.

Des activités d'assurance de la qualité doivent être conduites parallèlement pendant tout le cycle de vie.

Les aspects suivants doivent être inclus à cette prise en compte.

- a) **Concept:** une compréhension générale du matériel ou système et de son environnement physique, social et législatif est nécessaire pour permettre d'effectuer également de manière satisfaisante les autres activités pendant le cycle de vie.
- b) **Analyse des dangers et des risques:** le type et l'importance des dangers associés au fonctionnement du matériel doivent être analysés en détail en tenant compte de l'environnement électromagnétique où il est prévu de l'installer. Une évaluation des risques associés aux dangers doit être conduite afin de déterminer si les risques sont acceptables et, dans le cas contraire, s'ils peuvent être réduits à un niveau acceptable. Priorité doit être donnée d'abord à la réduction des risques par des mesures de conception et d'installation, puis à la protection et enfin à la fourniture de consignes.
- c) **Spécifications de sécurité:** il convient que la spécification de sécurité précise les mesures et techniques qui doivent être utilisées pour assurer la sécurité fonctionnelle en présence de perturbations électromagnétiques.
- d) **Conception et développement:** la conception doit être telle que la sécurité fonctionnelle requise soit réalisée. Pendant cette phase, il peut être nécessaire d'utiliser des techniques telles que des méthodes d'évaluation de la sûreté de fonctionnement, la modélisation et la réalisation de prototypes afin d'acquies l'assurance que les exigences seront vraisemblablement satisfaites. Une attention particulière doit être accordée aux fonctions importantes pour la sécurité.
- e) **Installation:** le matériel ou le système est installé en utilisant les procédures et les composants spécifiés pendant la phase de conception.
- f) **Validation:** l'objet de la validation est de confirmer que la sécurité fonctionnelle prévue est préservée dans toutes les conditions de fonctionnement spécifiées.
- g) **Exploitation et maintenance:** le système ou le matériel doit être exploité et entretenu de telle manière que la sécurité fonctionnelle prévue soit préservée.
- h) **Modifications:** les incidences des éventuelles modifications proposées sur la sécurité fonctionnelle doivent être évaluées.
- i) **Utilisation du matériel/système:** il est recommandé de mettre en place un système de surveillance de sécurité qui enregistre les défaillances en cours d'utilisation et prenne en compte les effets de ces défaillances sur la sécurité. Il convient que le système conserve des enregistrements afin de permettre l'examen des effets électromagnétiques liés à ces défaillances.
- j) **Retrait du service:** enfin, avant le retrait du service du système ou du matériel, une analyse doit être effectuée pour évaluer l'impact du retrait du service proposé sur la sécurité fonctionnelle des éventuels autres systèmes et matériels.

5.2 Etapes de réalisation de la sécurité fonctionnelle

Pour réaliser la sécurité fonctionnelle, les actions spécifiques suivantes concernant les influences électromagnétiques doivent être entreprises.

- a) Définition de la structure, de la conception et des fonctions prévues du matériel ou du système projeté ou existant.
- b) Description de l'environnement électromagnétique correspondant (voir article 6).
- c) Spécification des exigences de sécurité (voir article 7).
- d) Exécution d'une analyse de la sûreté de fonctionnement afin d'identifier les dangers (en termes d'événements et des parties correspondantes du matériel ou système) qui peuvent entraîner des risques pour la sécurité dus aux perturbations électromagnétiques (voir article 8).
- e) Essais de compatibilité électromagnétique pour la sécurité (voir article 9).

Quality assurance activities shall run in parallel across the whole life cycle.

The following aspects shall be included in this consideration:

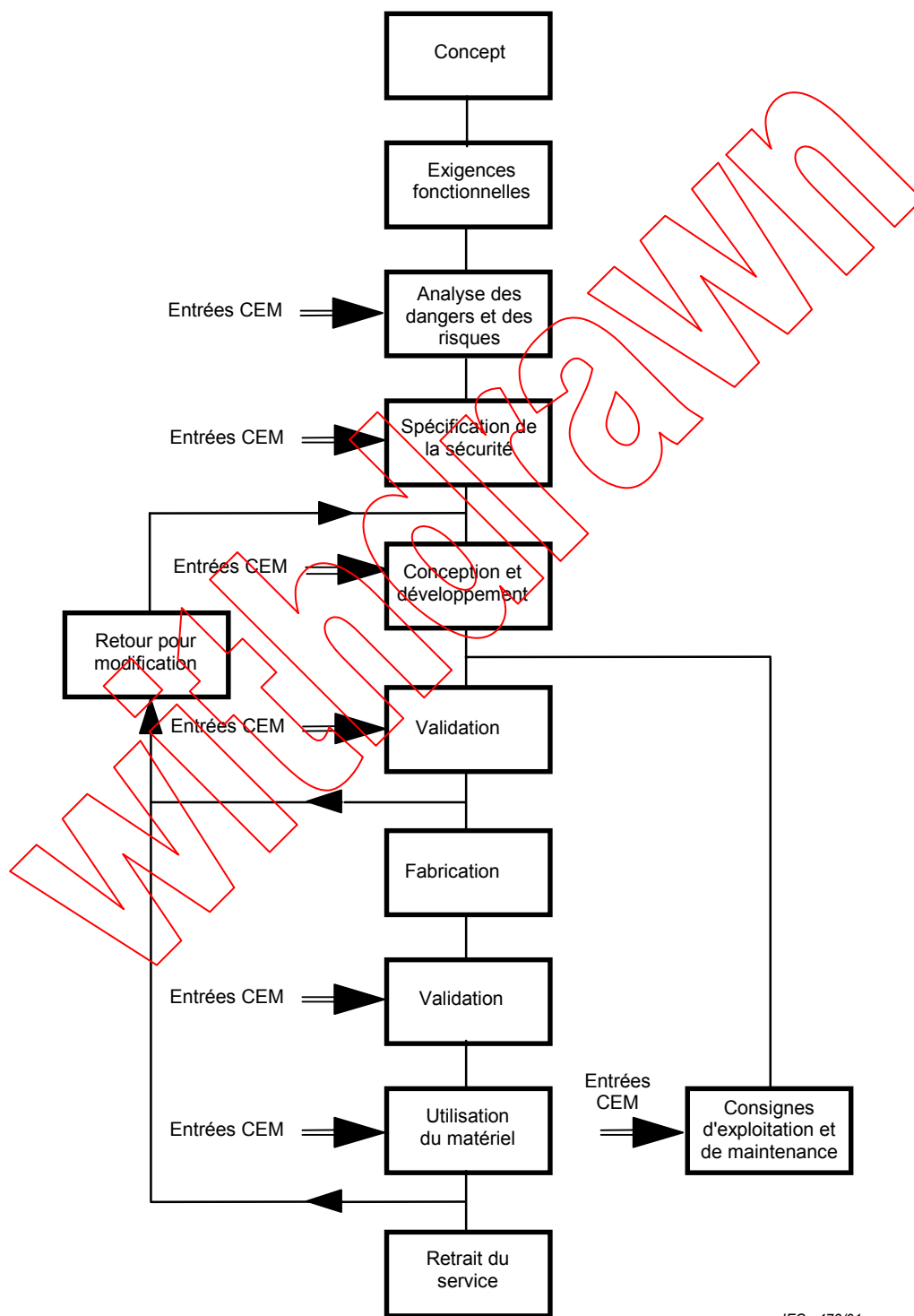
- a) **Concept:** A general understanding of the equipment or system and its environment: physical, social and legislative, is necessary to enable also the other life cycle activities to be satisfactorily performed.
- b) **Hazard and risk analysis:** The type and extent of hazards associated with operation of the equipment shall be analysed in detail taking into account the electromagnetic environment where it is intended to be installed. There shall be an assessment of the risks associated with the hazards to determine whether the risks are acceptable, and if not, whether they can be reduced to an acceptable level. Priority shall be given firstly to risk reduction by design and installation measures, followed by safeguarding and finally by the provision of instructions.
- c) **Safety specifications:** The safety specification should specify the measures and techniques which shall be used to ensure functional safety in the presence of electromagnetic disturbances.
- d) **Design and development:** The design shall be such that the required functional safety is achieved. During this phase it may be necessary to use techniques such as dependability assessment methods, modelling and prototype construction to gain confidence that the requirements are likely to be satisfied. Particular attention is to be given to safety related functions.
- e) **Installation:** The equipment or system is installed using procedures and components specified during the design phase.
- f) **Validation:** The purpose of validation is to confirm that under all specified conditions of operation the intended functional safety is preserved.
- g) **Operation and maintenance:** The system or equipment shall be operated and maintained so that the intended functional safety is preserved.
- h) **Modifications:** The impact of any proposed modifications on functional safety shall be assessed.
- i) **Use of the equipment/system:** It is recommended that a safety monitoring system be set up for recording failures in use taking into account the effects of these failures on safety. The system should keep records to allow the examination of EM effects with regard to these failures.
- j) **Decommissioning:** Finally, before the system or equipment is decommissioned there shall be an analysis carried out to assess the impact of the proposed decommissioning on the functional safety of any other systems or equipment.

5.2 Steps for the achievement of functional safety

To achieve functional safety the following specific actions with regard to electromagnetic influences shall be undertaken:

- a) Define the structure, design and intended functions of the projected or existing equipment or system.
- b) Describe the relevant electromagnetic environment (see clause 6).
- c) Specify the safety requirements (see clause 7).
- d) Perform a dependability analysis in order to identify the hazards (in terms of the events and the corresponding parts of the equipment or system) which can cause safety risks due to electromagnetic disturbances (see clause 8).
- e) Electromagnetic compatibility tests for safety (see clause 9).

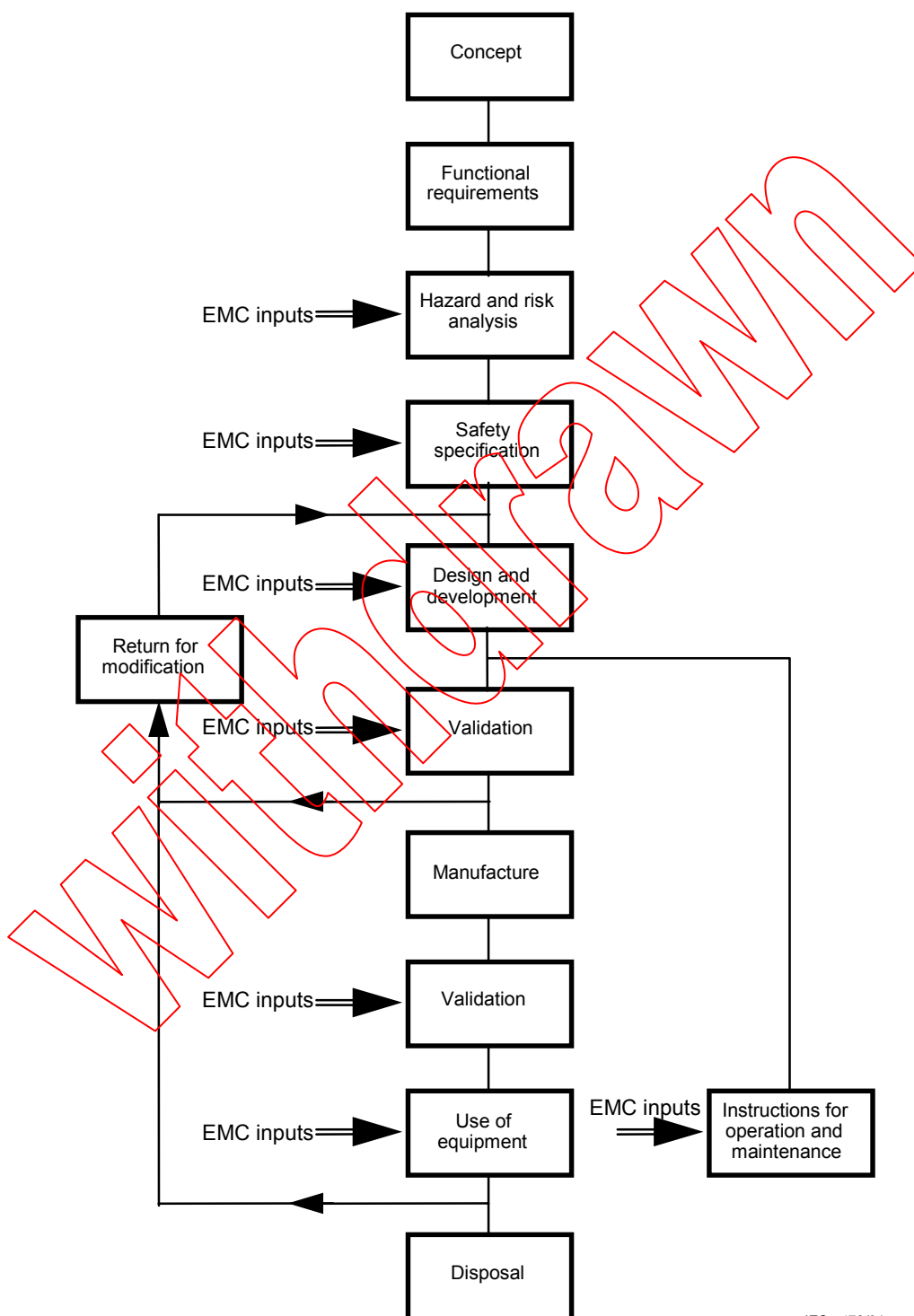
- f) Modification des mesures de conception ou d'installation, si nécessaire, afin de réduire les risques à des valeurs acceptables.
- g) Mise en œuvre d'un processus de validation afin de démontrer que le matériel ou le système fonctionne conformément aux exigences de sécurité spécifiées.
- h) Production des consignes d'exploitation et de maintenance afin d'assurer la sécurité fonctionnelle dans le temps.



IEC 473/01

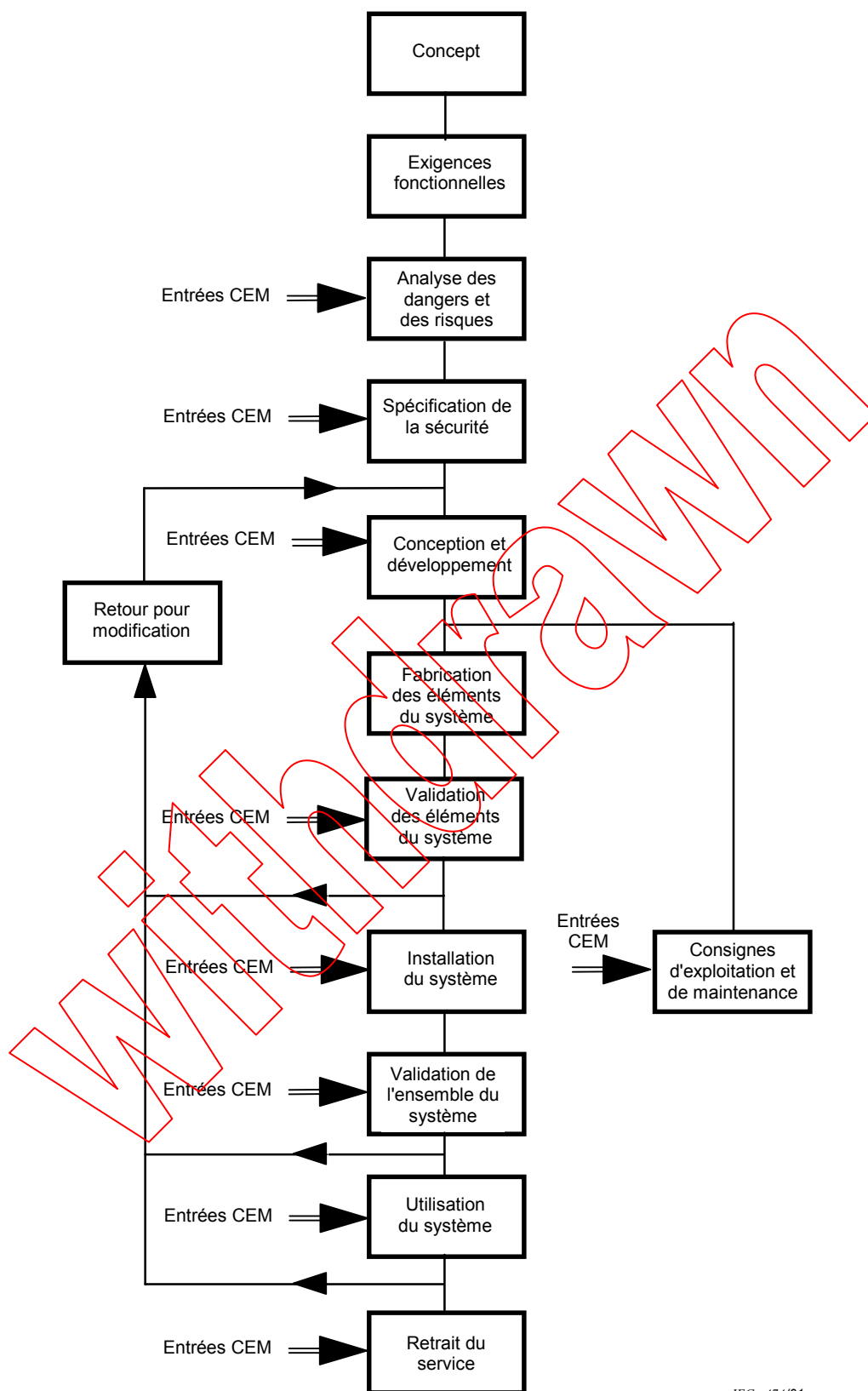
Figure 1 – Cycle de vie de sécurité des matériels individuels

- f) Modify the design or installation measures, if necessary, in order to reduce the risks to acceptable values.
- g) Undertake a process of validation to demonstrate that the equipment or system performs according to the specified safety requirements.
- h) Produce operation and maintenance instructions to ensure the specified functional safety in the course of time.



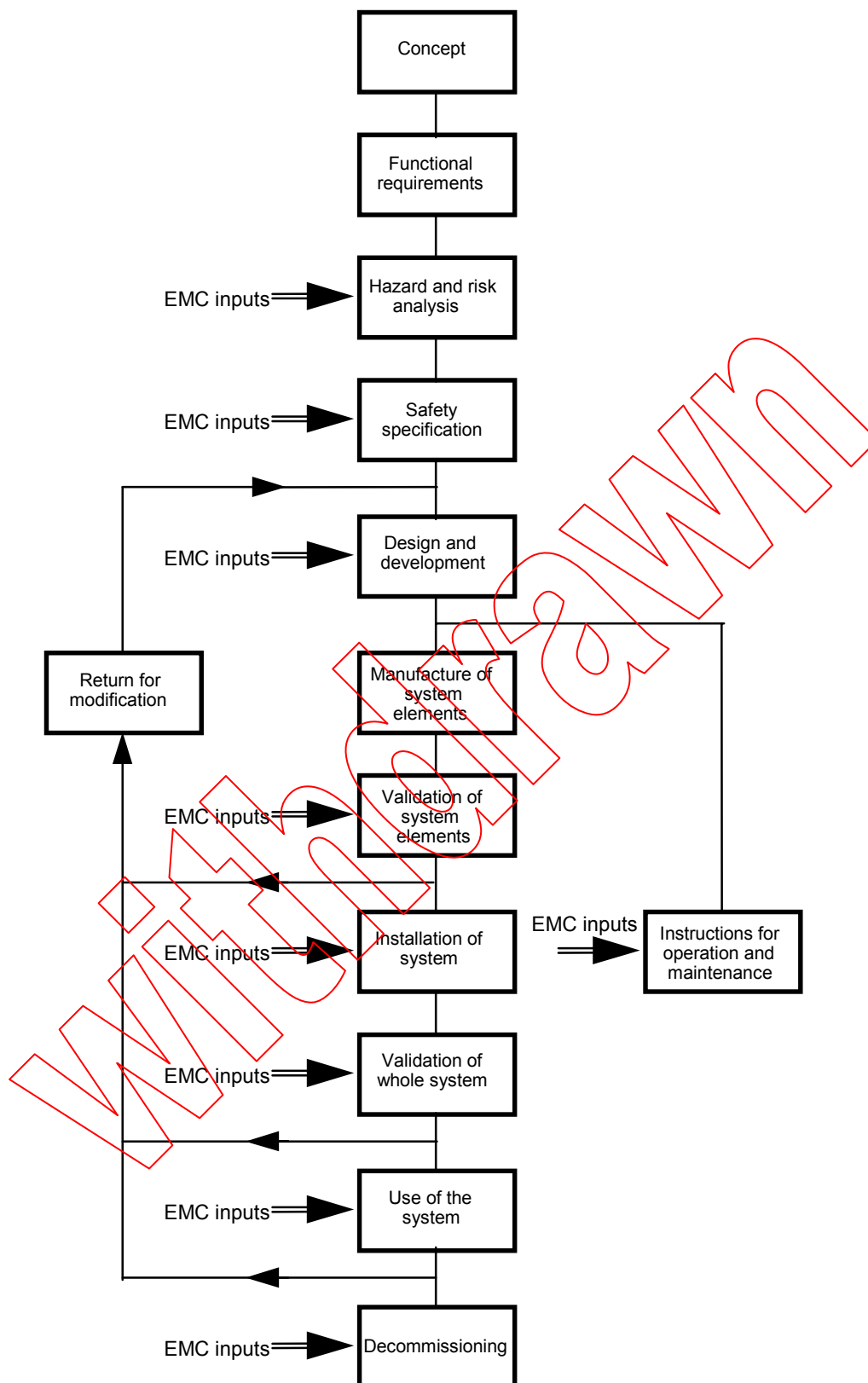
IEC 473/01

Figure 1 – Safety life cycle for individual equipment



IEC 474/01

Figure 2 – Cycle de vie de sécurité des systèmes



IEC 474/01

Figure 2 – Safety life cycle for systems

6 Environnement électromagnétique

Le tableau 1 donne une vue d'ensemble des principales perturbations électromagnétiques qui doivent être prises en compte.

On trouvera des informations générales sur les niveaux de perturbations électromagnétiques dans divers environnements dans les normes ou rapports techniques de la série CEI 61000-2 ou de la série CEI 61000-4. Le tableau A.1 donne une indication des niveaux qui ne devraient théoriquement pas être dépassés dans les environnements les plus courants.

Certains phénomènes électromagnétiques qui se produisent rarement ne font pas encore l'objet de normes de la CEI mais il convient cependant de les prendre en compte dans des cas particuliers. Il s'agit par exemple de phénomènes conduits ou rayonnés dans la gamme de fréquences de 3 kHz à 150 kHz.

Il convient d'insister sur le fait que les niveaux de perturbations électromagnétiques indiqués dans les diverses normes, rapports ou spécifications techniques, doivent être pris en considération avec grande prudence en ce qui concerne leurs incidences sur la sécurité. Noter en particulier ce qui suit.

- a) Les niveaux de perturbations varient selon une distribution statistique et les niveaux donnés en exemple au tableau A.1 peuvent être sensiblement dépassés dans des circonstances particulières. Toutefois ces circonstances peuvent ne se présenter que rarement ou sur des sites particuliers (voir la CEI 61000-1-1).
- b) Les niveaux d'essai et critères d'aptitude à la fonction normalisés sont en général liés aux exigences fonctionnelles et non à la sécurité. Une marge de sécurité appropriée doit être prise en compte.
- c) Les caractéristiques d'immunité du matériel peuvent se dégrader avec le vieillissement.
- d) Il peut être nécessaire de restreindre l'utilisation de certains types de matériel (téléphones mobiles par exemple) dans certains environnements particuliers afin d'éviter les situations dangereuses.

NOTE Un niveau de perturbation de référence fréquemment rencontré est le niveau de compatibilité, choisi de manière qu'il existe une faible probabilité qu'il soit dépassé par le niveau d'émission réel. On suppose souvent que le niveau de compatibilité couvre 95 % des cas et peut être dépassé dans 5 % des cas. Pour cette raison, ce ne sont pas les niveaux de compatibilité mais les valeurs indiquées dans les normes d'immunité de la série CEI 61000-4 qui ont été utilisées dans le tableau A.1 comme niveaux de perturbations typiques.

Dans certaines circonstances, par exemple dans un système ou une installation, il peut également être nécessaire de restreindre les niveaux d'émission en dessous des niveaux normaux ou d'empêcher l'utilisation de certains matériels à proximité de matériels voisins impliqués dans la sécurité.

6 The electromagnetic environment

Table 1 gives an overview of the principal electromagnetic disturbance which shall be considered.

General information about levels of electromagnetic disturbances in various environments can be found in the standards or technical reports of the IEC 61000-2 series or the IEC 61000-4 series. Table A.1 in Annex A gives an indication of the levels which, it is expected, will not normally be exceeded in typical environments.

Some EM phenomena which occur infrequently are not yet the subject of IEC standards but still should be considered in particular cases. Examples of such phenomena are conducted or radiated phenomena in the frequency range 3 kHz to 150 kHz.

It is stressed that the levels of electromagnetic disturbances indicated in the various standards, reports or technical specifications must be considered very cautiously with regard to their implications for safety. In particular, note the following.

- a) The disturbance levels vary according to a statistical distribution, and the levels shown as examples in Table A.1 can be exceeded notably in some particular circumstances. However such circumstances may only exist infrequently or on particular sites (see IEC 61000-1-1).
- b) The standardised test levels and performance criteria are generally related to functional requirements and not to safety. An appropriate safety margin has to be considered.
- c) The immunity characteristics of the equipment may worsen with ageing.
- d) It may be necessary to restrict the use of certain types of equipment (e.g. mobile phones) within particular environments in order to prevent hazardous situations.

NOTE A reference disturbance level often referred to is the compatibility level, a level which is chosen so that a small probability exists that it will be exceeded by the actual emission level. Often it is assumed that the compatibility level cover 95 % of the cases and could be exceeded in 5 % of the cases. For this reason not the compatibility levels but values indicated in the immunity standards of the IEC 61000-4 series have been used in Table A1 as typical disturbance levels.

In some circumstances, for example within a system or an installation, it may be also necessary to restrict the emission levels below the normal levels, or to prevent the use of certain equipment in proximity to safety implicated neighbouring equipment.

Tableau 1 – Vue d'ensemble des phénomènes de perturbation

Phénomènes conduits à basse fréquence	Harmoniques, inter-harmoniques Tensions de signalisation Fluctuations de tension Creux de tension et coupures Déséquilibre de tension Variations de la fréquence du réseau Tensions induites à basse fréquence Tension continue dans les réseaux alternatif
Phénomènes de champs rayonnés à basse fréquence	Champs magnétiques ^a Champs électriques
Phénomènes conduits à haute fréquence	Tensions ou courants permanents à couplage direct ou induits Transitoires unidirectionnels ^b Transitoires oscillatoires ^b
Phénomènes de champs rayonnés à haute fréquence	Champs magnétiques Champs électriques Champs électromagnétiques – ondes entretenues – transitoires ^c
Phénomènes de décharges électrostatiques (DES)	
Impulsion électromagnétique à haute altitude (IEMN) ^d	
^a Continus ou transitoires ^b Simples ou répétitifs (salves) ^c Simples ou répétitifs ^d A prendre en compte dans des conditions spéciales NOTE Il n'existe bien sûr aucune limite bien marquée entre le domaine basse fréquence et le domaine haute fréquence mais une transition progressive entre 9 kHz à 150 kHz. Pour les applications formelles, la limite est fixée à 9 kHz (domaine d'activité du CISPR).	

7 Exigences de sécurité et critères de défaillances

Afin de réaliser la sécurité fonctionnelle des matériels ou systèmes électriques et électroniques en présence de perturbations électromagnétiques, les aspects de fonctionnement suivants doivent être pris en compte.

- Premièrement, la sécurité fonctionnelle du matériel ou système ne doit pas être indûment affectée par l'environnement électromagnétique à l'endroit où le matériel est utilisé. Cela exige que le niveau d'immunité du matériel ou du système soit suffisant pour que les éventuelles défaillances dues aux perturbations électromagnétiques se produisent à une cadence qui, combinée à d'autres causes ou défaillances, entraîne un risque globalement acceptable.
- Deuxièmement, les éventuelles perturbations électromagnétiques produites à l'intérieur d'un système ou d'une installation ne doivent pas indûment affecter la sécurité fonctionnelle des autres parties du système ou de l'installation. Cela exige des émissions électromagnétiques «internes» suffisamment faibles dans ce système ou cette installation (les influences électromagnétiques internes à un appareil doivent être résolues lors de la conception).

Table 1 – Overview of disturbance phenomena

Conducted low frequency phenomena	Harmonics, interharmonics Signalling voltages Voltage fluctuations Voltage dips and interruptions Voltage unbalance Power frequency variations Induced low frequency voltages d.c. in a.c. networks
Radiated low frequency field phenomena	Magnetic fields ^a Electrical fields
Conducted high frequency phenomena	Directly coupled or induced continuous voltages or currents Unidirectional transients ^b Oscillatory transients ^b
Radiated high frequency field phenomena	Magnetic fields Electrical fields Electromagnetic fields – continuous waves – transients ^c
Electrostatic discharge phenomena (ESD)	
High altitude electromagnetic pulse (HEMP) ^d	
^a Continuous or transients. ^b Single or repetitive (bursts). ^c Single or repetitive. ^d To be considered under special conditions. NOTE There is of course no abrupt limit between the low frequency domain and the high frequency domain but a soft transition between 9 kHz and 150 kHz. For formal applications the limit is set at 9 kHz (scope of CISPR).	

7 Safety requirements and failure criteria

In order to achieve the functional safety of electrical and electronic equipment or systems in the presence of electromagnetic disturbances the following aspects of performance shall be considered.

- Firstly the functional safety of the equipment or system shall not be unduly affected by the electromagnetic environment in the place where the equipment is used.
This requires that the level of immunity of the equipment or system is sufficient so that any failures due to electromagnetic disturbances occur at a rate which, when combined with other causes of failures, result in an overall acceptable risk.
- Secondly any electromagnetic disturbances generated inside of a system or installation shall not unduly affect the functional safety of the other parts of the system or installation. This requires sufficiently low "internal" electromagnetic emissions in these system or installation (the internal electromagnetic influences within an apparatus shall be solved at the design stage).

c) Concernant les critères utilisés pour déterminer le résultat des essais d'immunité (appelés «critères de défaillances») on spécifie en général, lors de la prise en compte des effets des perturbations sur le matériel ou le système, des classes de dégradation, comme par exemple dans les essais d'immunité CEM de la série CEI 61000-4:

- 1) aptitude à la fonction normale dans les limites spécifiées par le constructeur;
- 2) perte de fonction ou dégradation du fonctionnement temporaire qui cesse lorsque les perturbations cessent. Le matériel retrouve son aptitude normale après l'essai, sans intervention de l'opérateur ou remise à l'état initial du système. La perte ou la dégradation du fonctionnement peut éventuellement persister pendant un certain temps;
- 3) perte de fonction ou dégradation du fonctionnement temporaire, dont la correction exige une intervention de l'opérateur ou la remise à l'état initial du système;
- 4) perte de fonction ou dégradation du fonctionnement non récupérable, du fait des dommages au matériel ou au logiciel, ou de la perte de données.

L'apparition de chacune de ces situations, à l'exception de 1) peut avoir une incidence sur la sécurité, et donc un risque associé, qui doit impérativement être analysé au cas par cas.

Noter qu'il peut y avoir une différence entre défaillance matériel et défaillance système: il convient également de considérer une défaillance matériel à la lumière de la conception du système (par exemple, en cas de redondance, les voies parallèles ne doivent pas être affectées de la même manière par une perturbation électromagnétique).

Noter également que, dans le contexte de la sécurité fonctionnelle, il est parfois acceptable qu'un dispositif exposé à des perturbations électromagnétiques tombe en panne de telle manière que tout danger soit évité (comportement à sécurité intrinsèque).

8 Analyse de la sûreté de fonctionnement

Une analyse de la sûreté de fonctionnement peut être requise pour identifier les parties du matériel ou du système qui entraînent un risque pour la sécurité dû aux perturbations électromagnétiques.

8.1 Considérations générales relatives au choix d'une méthode appropriée

Il existe plusieurs méthodes d'étude de la sûreté de fonctionnement (voir annexe E). En général, elles sont basées sur deux principes:

- méthodologie déductive (méthodologie descendante);
- méthodologie inductive (méthodologie ascendante).

Elles peuvent être caractérisées comme suit:

a) méthodologie déductive (voir 5.3 de la CEI 60300-3-1)

L'essence de l'approche déductive est de partir du niveau d'intérêt ou de préoccupation le plus élevé – ce qu'on appelle «l'événement de tête» – et de descendre successivement de niveaux afin d'identifier ceux qui présentent un fonctionnement système indésirable.

Une méthode déductive est une méthode orientée événement: elle permet d'identifier, pour chacun des événements de tête spécifiques, les niveaux système et composants responsables.

c) With regard to the criteria used to determine the result of immunity testing (so-called "failure criteria") it is conventional when considering the effects of disturbances on equipment or system to specify classes of degradation, such as in EMC immunity tests of the IEC 61000-4 series:

- 1) normal performance within limits specified by the manufacturer;
- 2) temporary loss of function or degradation of performance which ceases after the disturbances ceases. The equipment recovers its normal performance after the test without operator intervention or system reset. Possibly the loss or degradation of performance may persist during a certain time interval;
- 3) temporary loss of function or degradation of performance, the correction of which requires operator intervention or system reset;
- 4) loss of function or degradation of performance which is not recoverable, owing to damage to hardware or software or loss of data.

The occurrence of each of these, except 1) can have implications for safety, and thus an associated risk, which must be analysed case by case.

Note that there may be a difference between equipment failure and system failure: an equipment failure should also be considered in the light of the system design (for example, in case of redundancy, the parallel channels shall not be affected in the same manner by an electromagnetic disturbance).

Note also that, in the context of functional safety, it is sometimes acceptable for a device, when exposed to electromagnetic disturbances, to fail in such a way that danger is averted (fail-to-safe behaviour).

8 Dependability analysis

A dependability analysis may be required to identify the parts of the equipment or system which may cause a risk to safety due to electromagnetic disturbances.

8.1 General considerations for the choice of an appropriate method

Several methods for dependability studies are available (see Annex E). In general, they are based on two principles:

- deductive methodology (top-down methodology);
- inductive methodology (bottom-up methodology).

They can be characterised as follows:

a) Deductive methodology (see 5.3 of IEC 60300-3-1)

The essence of the deductive approach is to proceed from the highest level of interest or concern – the "top event" – to successively lower levels in order to identify the levels with undesirable system operation.

A deductive method is an event-oriented method: it allows, for each defined specific top event, to identify the responsible system levels and components.

b) méthodologie inductive (voir 5.4 de la CEI 60300-3-1)

L'essence de la méthode inductive est d'identifier les modes de défaut au niveau composant. Pour chaque mode de défaut, l'effet correspondant sur les caractéristiques est déduit pour le niveau système immédiatement supérieur. Les itérations successives entraînent l'identification éventuelle des effets du défaut à tous les niveaux fonctionnels. Cette approche «ascendante» permet l'identification de tous les modes de défaut uniques.

Concernant l'effet des perturbations électromagnétiques sur la sécurité fonctionnelle, c'est souvent la méthode déductive (descendante) qui convient, à savoir:

- premièrement, définir les événements indésirables: défauts de fonctionnement ou fonctionnements indésirables;
- deuxièmement, procéder à l'analyse des défaillances.

Une méthode inductive (ascendante) prend en compte tous les modes de défaut, y compris les modes de défaut non relatifs aux perturbations électromagnétiques et est donc inutilement extensive et compliquée pour les systèmes complexes.

Pour les besoins de la présente spécification technique, l'analyse par arbre de panne (AAP) est utilisée pour donner un exemple de l'application d'une méthode déductive. L'AAP est considérée comme une méthode bien adaptée à une analyse CEM.

NOTE Il va de soi, particulièrement dans le cadre d'une étude globale prenant en compte tous les aspects ayant une incidence, que d'autres méthodes peuvent être appliquées.

8.2 Application de l'analyse par arbre de panne aux perturbations électromagnétiques

La procédure d'exécution d'une analyse par arbre de panne est décrite en détail dans la CEI 61025. Elle implique les étapes suivantes (qui font partie du cycle de vie global de sécurité décrit à l'article 5).

- a) Définir le matériel ou le système étudié:
 - sa structure physique et les règles de conception;
 - la configuration logicielle (si possible avec la même structure que le matériel);
 - les fonctions prévues.
- b) Spécifier l'environnement électromagnétique auquel le matériel étudié est exposé:
 - les sites où le matériel est installé;
 - les perturbations électromagnétiques ayant une influence;
 - les niveaux de perturbation les plus sévères;
 - les niveaux d'essai d'immunité normalement appliqués à des fins fonctionnelles.
- c) Spécifier tous les événements de sécurité indésirables:
 - non fonctionnement;
 - fonctionnements indésirables;
 - fonctionnements incorrects.

Ces événements de sécurité seront considérés comme les événements de tête de l'arbre de panne.

d) Effectuer l'analyse par arbre de panne:

Une analyse par arbre de panne est effectuée pour chaque situation dangereuse et englobe à la fois le matériel et le logiciel.

Chaque situation dangereuse représente un événement de tête de l'arbre de panne. Il est alors nécessaire d'analyser lequel des événements de niveau inférieur peut donner lieu à l'événement de tête.