

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.

IECNORM.COM: Click to view the full PDF of IEC TS 61000-1-2:2001

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
IECNORM.COM: Click to view the full PDF of IEC TS 61000-1-2:2001

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.

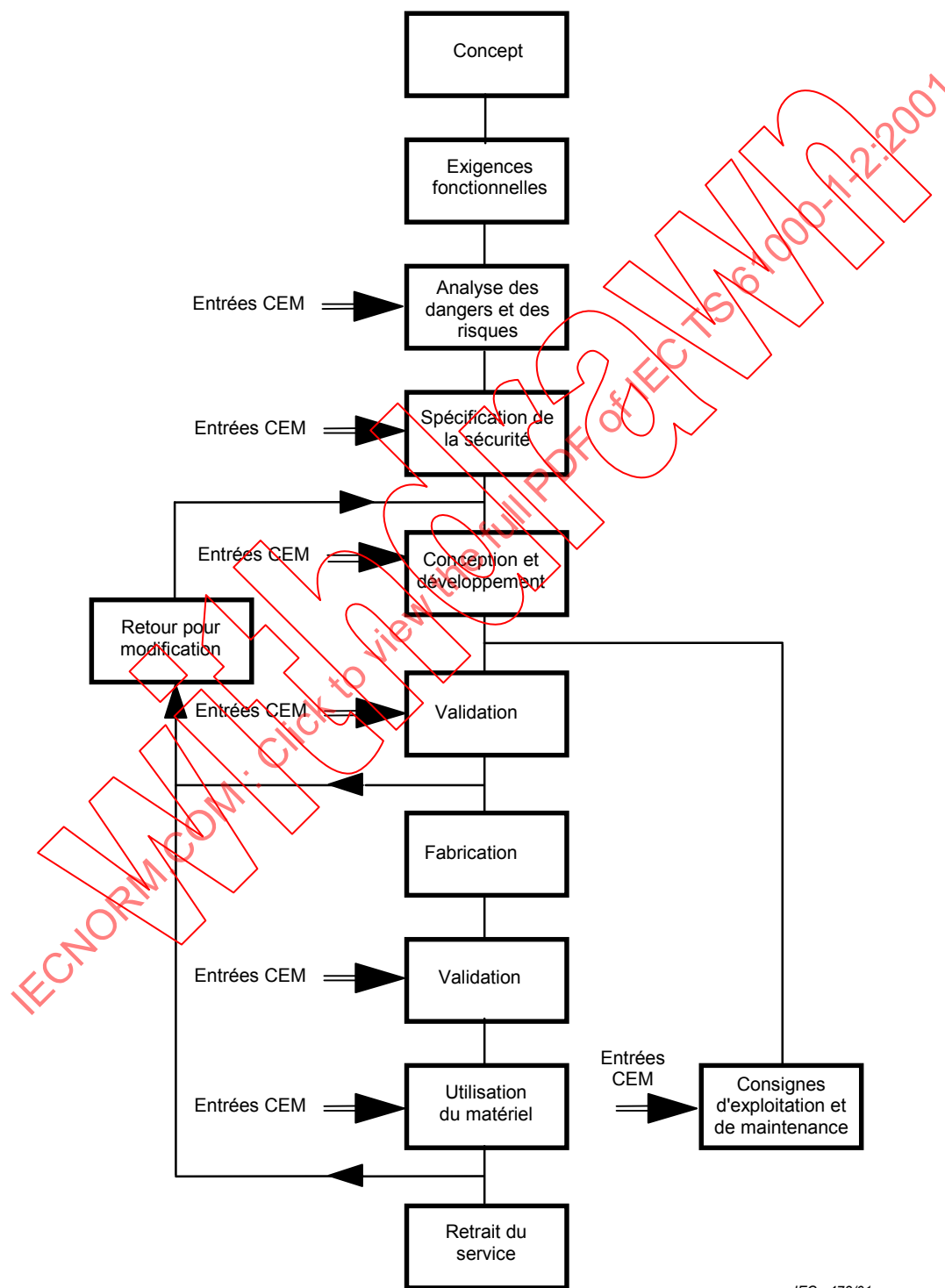
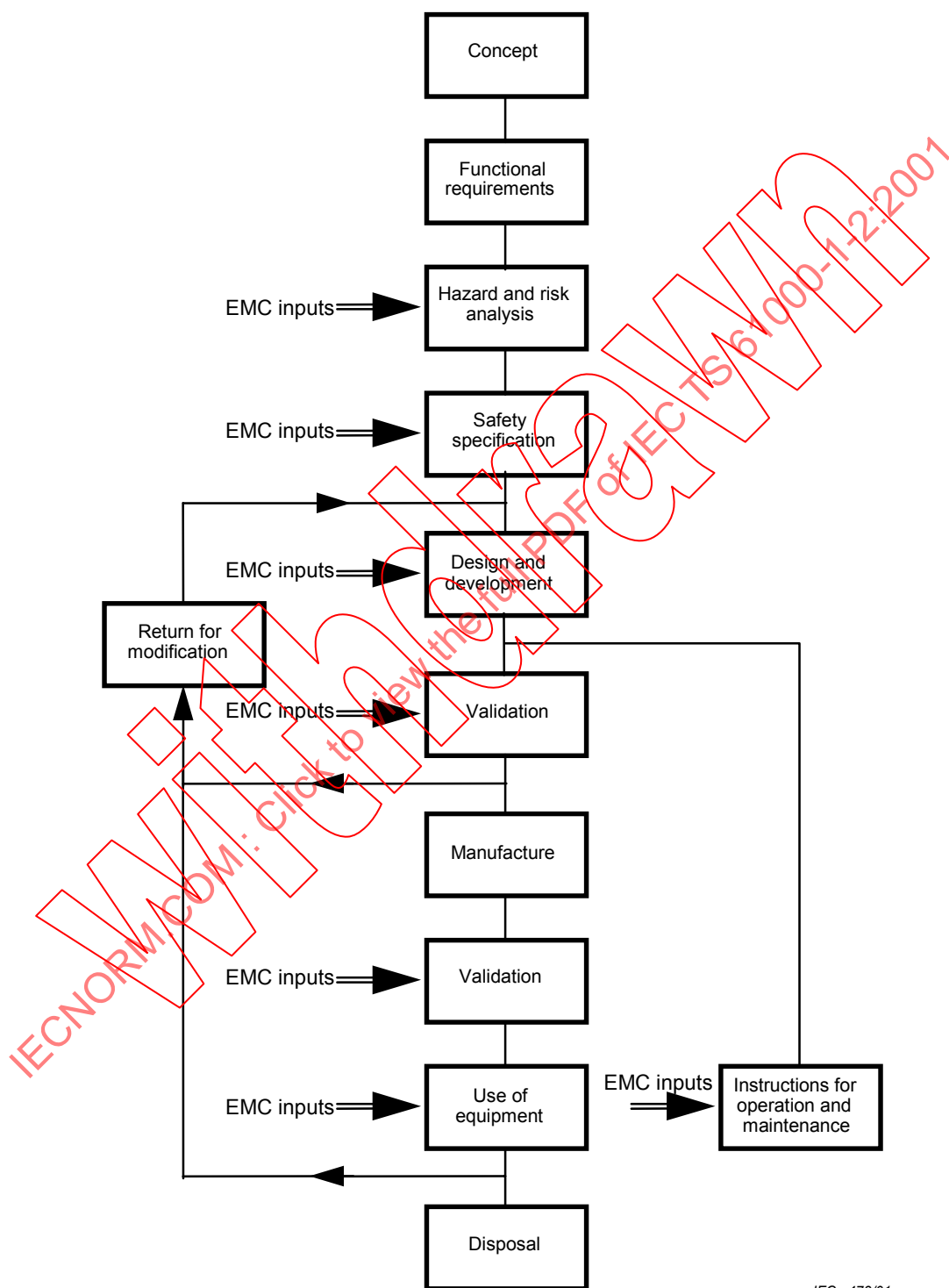


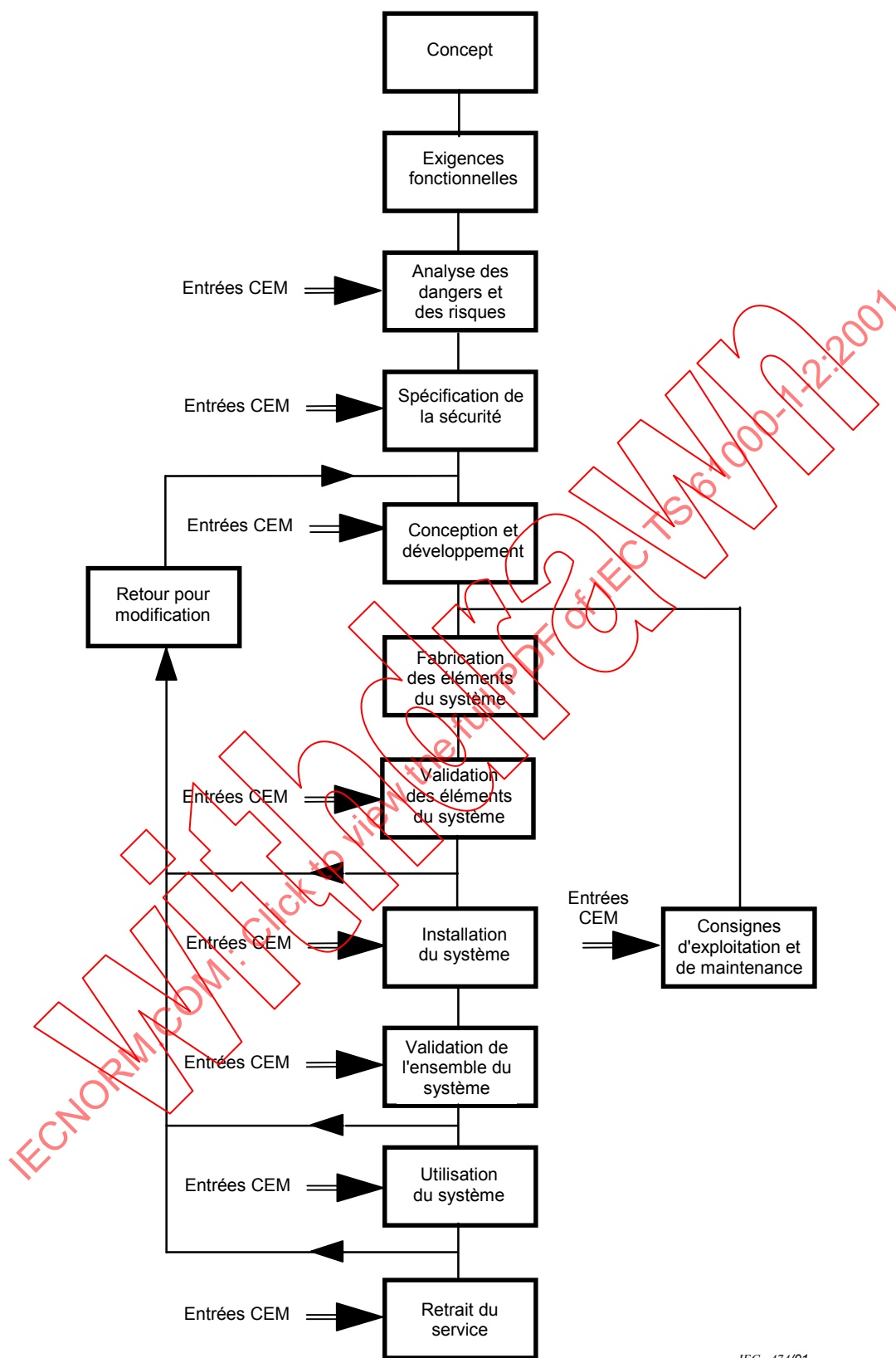
Figure 1 – Cycle de vie de sécurité des matériels individuels

- 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.



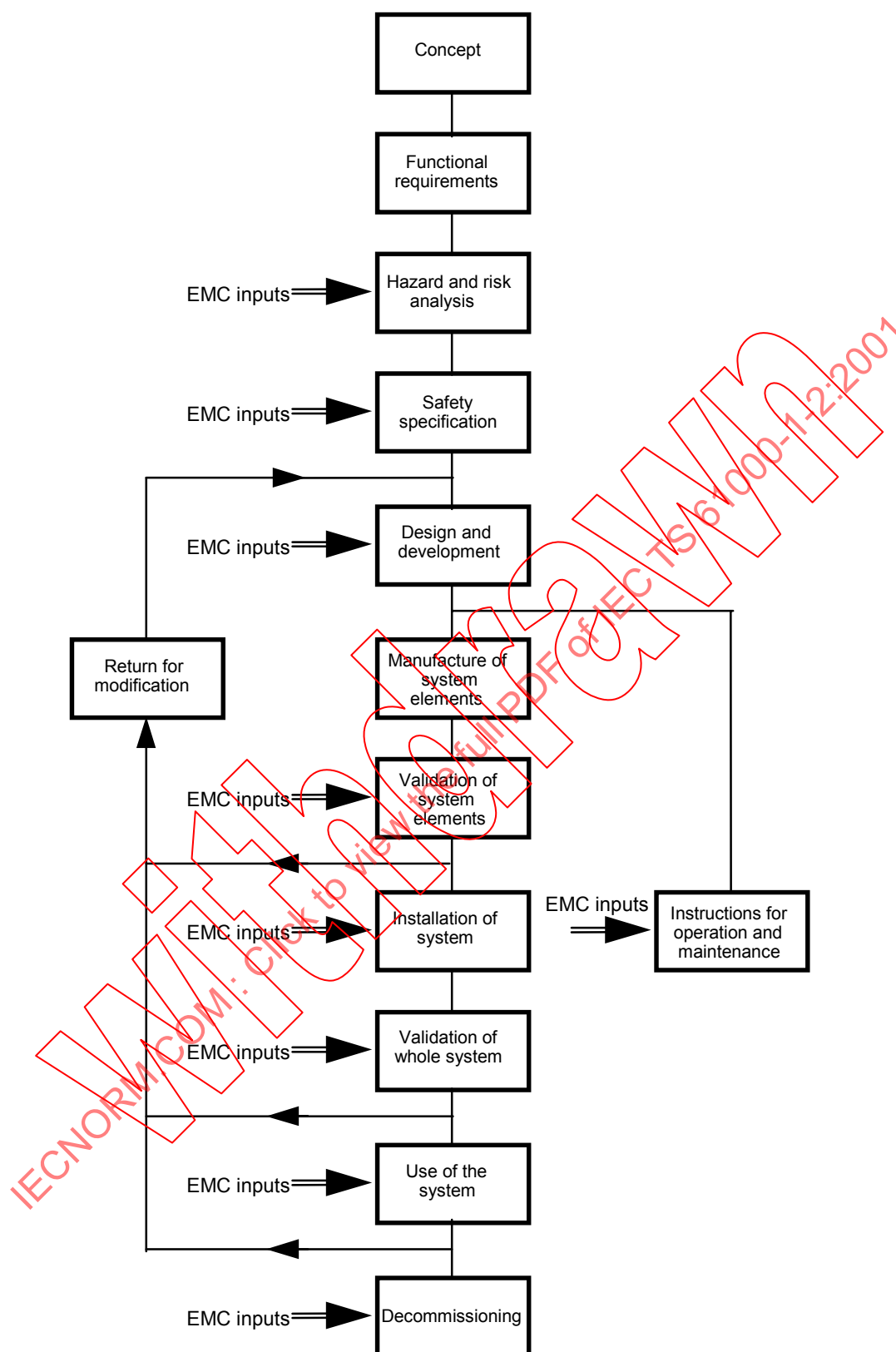
IEC 473/01

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.

- a) 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.

- b) 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.

b) Inductive methodology (see 5.4 of IEC 60300-3-1)

The essence of the inductive method is to identify fault modes at the component level. For each fault mode the corresponding effect on performance is deduced for the next higher system level. Successive iterations result in the eventual identification of the fault effects at all functional levels. This "bottom-up" approach allows the identification of all single fault modes.

With regard to the effect of electromagnetic disturbances on functional safety it is often appropriate to apply the deductive (top-down) method, that is

- first, define the undesirable events: faulty operations or unwanted operations,
- second, proceed to the failure analysis.

An inductive (bottom-up) method considers all the fault modes, including fault modes not relevant to electromagnetic disturbances and would therefore be unnecessarily extensive and complicated for complex systems.

For the purposes of this document fault tree analysis (FTA) is used to show an example of the application of a deductive method. FTA is considered as a very appropriate method for an EMC analysis.

NOTE Of course, particularly within an overall safety study considering all the influencing aspects, other methods could be applied.

8.2 Application of the fault tree analysis to electromagnetic disturbances

The procedure detailing how to carry out a Fault Tree Analysis is explained in IEC 61025. It involves the following steps (which are parts of the overall safety life cycle described in clause 5).

- a) Define: the investigated equipment or system:
 - its physical structure and design rules;
 - the software configuration (if possible with the same structure as the hardware);
 - the intended functions.
- b) Specify the electromagnetic environment to which the investigated equipment is exposed:
 - the locations where it is installed,
 - the influencing electromagnetic disturbances,
 - the most severe disturbance levels,
 - the immunity test levels normally applied for functional purposes.
- c) Specify all undesirable safety events:
 - no operation,
 - unwanted operations,
 - wrong operations.

These safety events will be considered as the top events of the fault tree.

d) Carry out the fault tree analysis.

A fault tree analysis is performed for each hazardous situation and encompasses both hardware and software.

Each hazardous situation represents a top event of the fault tree. It is then necessary to analyse which of the lower events can give rise to the top event.

Les perturbations électromagnétiques sont considérées dans l'arbre de panne comme les événements de base.

Les parties du matériel ou du système où des niveaux d'essai d'immunité renforcés sont requis pour réaliser la sécurité fonctionnelle sont ainsi identifiés.

- e) Si nécessaire, effectuer les modifications à la conception et à l'installation pour corriger les événements indésirables et reprendre l'analyse.

9 Essais CEM relatifs à la sécurité

9.1 Importance et nécessité des essais

Les matériels électriques ou électroniques pour lesquels les analyses décrites dans la présente spécification technique indiquent un risque électromagnétique potentiel pour la sécurité doivent être soumis aux essais appropriés, afin de garantir que leur conception assure la sécurité fonctionnelle requise. Ce point est particulièrement important pour les éléments et les fonctions liés à la sécurité d'un matériel.

Les essais d'immunité CEM d'un matériel ou système sont généralement spécifiés dans la norme CEM de produits applicable. Si une telle norme n'existe pas, une norme générique d'immunité CEM peut être appliquée. Ces exigences fonctionnelles d'essais CEM sont en général basées sur la démonstration de l'immunité «normale» des dispositifs. Les perturbations électromagnétiques étant statistiques par nature, ces essais ne peuvent pas couvrir toutes les situations possibles: les différents environnements, tous les types de perturbations, les niveaux maximaux, etc., auxquels le matériel peut être exposé. Ceci est particulièrement vrai avec les normes génériques qui, en principe, définissent un nombre limité d'essais afin de réaliser un optimum technico-économique. En conséquence, des essais d'immunité CEM plus sévères peuvent être nécessaires du point de vue de la sécurité.

Il est important que les comités de produits et les constructeurs définissent l'étendue et la sévérité des essais d'immunité CEM supplémentaires importants pour la sécurité, proportionnellement aux risques et aux conséquences de la défaillance du matériel. Ce point peut être important du point de vue des implications juridiques.

Toutefois, l'expérience acquise dans l'exploitation de types de matériels particuliers, et de leur capacité à réaliser la sécurité fonctionnelle en dépit de perturbations électromagnétiques importantes dans l'environnement d'utilisation, peut être prise en compte pour l'élaboration d'un plan d'essai CEM de sécurité fonctionnelle.

9.2 Types et niveaux d'essais EM relatifs à la sécurité

Les essais CEM de sécurité demandent certaines considérations particulières:

9.2.1 Types d'essais d'immunité

En général, les essais CEM fonctionnels que l'on trouve dans une norme de produits ou générique ne prennent pas en compte toutes les perturbations électromagnétiques possibles (listées au tableau 1). Il est concevable qu'une perturbation électromagnétique négligée, mais de niveau élevé, puisse avoir des incidences sur la sécurité.

Pour ce qui concerne la sécurité, il est donc nécessaire de déterminer si des perturbations susceptibles d'avoir été négligées dans les normes de produits ou génériques peuvent se produire. Si c'est le cas, leur impact doit être pris en compte.

The electromagnetic disturbances are considered in the fault tree as the basic events.

Those parts of the equipment or system where enhanced immunity test levels are required to achieve functional safety are thereby identified.

- e) If necessary, carry out design and installation modifications to overcome undesirable events and repeat the analysis.

9 EMC testing with regard to safety

9.1 Importance and need for testing

Electric or electronic equipment for which the analyses described in this document indicate a potential for an EM safety risk shall be tested appropriately, in order to ensure that their design provides the required functional safety. This is particularly important for safety-related elements and functions of an equipment.

The EMC immunity tests for an equipment or system are specified generally in the relevant EMC product standard. If such a standard does not exist, a generic EMC immunity standard can be applied. These functional EMC test requirements are usually based on demonstrating the "normal" immunity of the devices. Because the electromagnetic disturbances are statistical by nature, these tests may not cover all the possible situations: various environments, all types of disturbance, maximum levels, etc. to which the equipment may be exposed. This is particularly true with the generic standards which, in principle, define a limited number of tests in order to achieve a technical/economical optimum. Accordingly more severe EMC immunity testing may be needed with regard to safety.

It is important for product committees and manufacturers to balance the extent and rigour of additional safety-related EMC immunity testing with the risk and consequences of equipment failure. This could also be important from the viewpoint of legal implications.

However, past experience with the operation of particular types of equipment and their ability to achieve functional safety in spite of significant EM disturbances in the operating environment can be considered in the development of a functional safety EMC test plan.

9.2 Types and EM test levels with regard to safety

EMC testing for safety requires some special considerations:

9.2.1 Types of immunity test

Usually the functional EMC tests in a product or generic standard do not consider all the possible EM disturbances (as listed in Table 1). It is conceivable that a neglected EM disturbance with a high level could have a safety implication.

With regard to safety, it is therefore necessary to consider whether disturbances which may have been neglected in the product or generic standards can occur. If so their impact shall be considered.

9.2.2 Niveaux d'essai

Les niveaux d'essais fonctionnels spécifiés dans les normes CEM de produits ou génériques, correspondent à des niveaux «normaux» de perturbations pour l'environnement. Pour les besoins de la sécurité, les comités de produits ou les constructeurs doivent spécifier des niveaux d'essai basés sur les niveaux maximaux susceptibles de se produire dans tous les environnements où le matériel est destiné à être installé. Il est également nécessaire de prendre en compte la distribution statistique des niveaux de perturbations, ainsi que les conséquences possibles des défaillances en termes de blessures ou de dommages corporels.

Il sera donc nécessaire d'augmenter les niveaux d'essais de CEM fonctionnels d'un «facteur de sécurité». Il n'est pas possible de donner un conseil général pour ce facteur de sécurité, qui dépend de nombreuses conditions. Il doit être spécifié au cas par cas, et peut être différent pour chaque type de perturbation électromagnétique. Dans certaines circonstances, il sera nécessaire de spécifier ce facteur de sécurité de manière à conduire à un niveau d'essai supérieur à celui requis par les impératifs de fonctionnement.

Dans les matériels ou systèmes contenant des parties importantes pour la sécurité, deux séries d'essai peuvent être prises en compte:

- une série pour les parties du système sans impact sur la sécurité;
- une série pour les parties du système importantes pour la sécurité, avec des exigences d'immunités plus sévères.

NOTE L'annexe A contient, pour information, un résumé des exigences d'essai d'immunité fonctionnelle contenues dans les normes d'immunité CEM génériques.

9.3 Fonctionnement du matériel pendant les essais

Lorsqu'un système constitué de plusieurs dispositifs doit être soumis à essai, il est important que les essais soient effectués au niveau d'intégration le plus élevé.

Du fait de la complexité d'un défaut de fonctionnement logiciel dû à une perturbation électromagnétique, il est recommandé que la totalité du système soit chaque fois que possible soumise à essai en fonctionnement.

Si cela n'est pas faisable du fait de contraintes de taille ou pour d'autres raisons, les sous-systèmes peuvent être soumis à essai séparément. Il convient d'ajouter si possible des «simulateurs fonctionnels» pour représenter les parties manquantes du système, et les éventuels défauts de fonctionnement constatés au cours de cet essai partiel doivent être analysés pour déterminer leur impact sur les performances d'ensemble du système.

Si les essais sont effectués dans des conditions autres que celles de l'installation proprement dite, les montages d'essais nécessiteront d'être aussi représentatifs que possible, en particulier en termes d'implantation, de parcours de câblage, et de modes d'utilisation.

9.4 Mettre l'accent sur les événements indésirables (matériels/logiciels)

Lors de la préparation du plan d'essais, l'accent doit être mis sur les événements indésirables (logiciels et matériels) déterminés par les procédures recommandées à l'article 8.

9.5 Favoriser les effets observables

Il peut être utile de forcer le matériel en essai à mal fonctionner afin de déterminer si, et comment, il crée des dangers pour la sécurité lorsqu'il est soumis aux extrêmes de l'environnement électromagnétique. On peut procéder de différentes manières, comme par exemple:

- niveaux d'essais plus élevés;
- réduction de l'immunité aux perturbations;

9.2.2 Testing levels

Functional testing levels specified in the EMC product or generic standards are related to "normal" environmental disturbance levels. For safety purposes product committees or manufacturers shall specify test levels which are based on the maximum levels likely to occur in all the environments where the equipment is intended to be installed. It is also necessary to take the statistical distribution of the disturbance levels into consideration together with the possible consequences of failures in terms of degree of injury or harm to health.

It will therefore be necessary to enhance the functional EMC test levels by a "safety factor". It is not possible to give a general advice on this safety factor which depends on numerous conditions. It must be specified case by case and may be different for each type of EM disturbance. In certain circumstances, it will be necessary that this safety factor is specified so that it leads to a greater test level than for performance reasons.

In equipment or systems with specific safety-related parts two series of test may be considered:

- a series for system parts not relevant for safety;
- a series for system parts relevant for safety with more severe immunity requirements.

NOTE Annex A shows, for information, a summary of the functional immunity testing requirements in the generic EMC immunity standards.

9.3 Operation of the equipment during testing

When a system of several devices is to be tested, it is important that the testing be carried out at the highest degree of integration.

Due to the complexities of a software malfunction due to an EM disturbance, it is recommended that, if possible, the entire system be tested while operating.

If this is not feasible due to size constraints or other reasons, subsystems could be tested separately. "Functional simulators" should be added if possible to represent the missing parts of the system, and any malfunctions noted during this partial testing must be analysed to determine their impact on the overall system performance.

If testing is carried out in conditions other than in the actual installation, then the test arrangements will need to be as representative as possible, particularly in terms of layout and cabling runs and the modes of use.

9.4 Focus on undesirable events (hardware/software)

In preparing the test plan, the focus shall be on the undesirable events (software and hardware) determined through the procedures recommended in clause 8.

9.5 Promote observable effects

It may be useful to force the equipment under test to malfunction in order to determine whether and how it creates safety hazards when subject to extremes of the electromagnetic environment. This can be initiated in different manners, e.g.:

- higher test levels;
- reducing immunity from disturbances;

- accélération de la cadence de répétition des perturbations (particulièrement important pour les perturbations à faible probabilité d'occurrence, comme par exemple les décharges électrostatiques (DES), les transitoires électriques rapides en salves (TER/S), etc.).

Il peut être nécessaire dans certaines circonstances de déterminer précisément le niveau d'immunité afin de déterminer la valeur d'une éventuelle marge de sécurité. Pour ce faire, un essai peut être effectué au cours duquel on augmente le niveau de perturbation tout en observant les performances du matériel ou du système jusqu'à ce qu'un défaut de fonctionnement soit constaté.

L'essai en conditions de défaut, c'est-à-dire un essai où un défaut est volontairement introduit dans le matériel, n'est pas requis par les normes relatives à la CEM. Toutefois, un tel essai peut être utile dans une norme relative à la sécurité, afin de contrôler le comportement du matériel après une éventuelle dégradation de ses parties ou de ses composants.

9.6 Critères de performances

Les défauts de fonctionnement impliquant des risques pour la sécurité doivent être évalués soigneusement, comme par exemple:

- le non-fonctionnement lorsque le fonctionnement est requis;
- le fonctionnement indésirable lorsque le non fonctionnement est requis;
- les écarts par rapport au fonctionnement normal.

Il convient d'accorder une attention particulière:

- au comportement des éléments importants pour la sécurité (qui peuvent être soumis à essai séparément);
- aux modes «à sécurité intrinsèque».

9.7 Validation et documentation de la planification des essais

Les essais CEM de sécurité doivent être effectués conformément aux spécifications produites par le comité de produits, le concepteur, le constructeur et l'installateur du matériel.

Un plan d'essai doit être élaboré pour valider les caractéristiques du matériel dans les environnements d'exploitation prévus. Les essais doivent être des essais d'homologation de type, ou des essais par échantillonnage effectués conformément à la recommandation du comité de produits, ou du concepteur (un essai à 100 % est dans certains cas déconseillé car un essai à un niveau élevé risque d'endommager un trop grand nombre de dispositifs). Les résultats des essais doivent être documentés et conservés.

En cas de modification du matériel au cours ou après les essais, le programme d'essais CEM correspondant doit être répété après exécution et documentation des éventuelles modifications jugées nécessaires.

10 Compte rendu

Un compte rendu de l'influence des phénomènes électromagnétiques sur la sécurité fonctionnelle d'un matériel électrique/électronique est requis et doit comprendre les informations indiquées dans les points a) à h) ci-dessous.

NOTE Les considérations relatives aux phénomènes électromagnétiques peuvent être intégrées à un compte rendu de sécurité complet prenant en compte d'autres phénomènes pertinents (isolement, risques mécaniques, etc.).

- accelerating the repetition rate of disturbances (particularly important for disturbances with a rare probability of occurrence, e.g. Electrostatic Discharge (ESD), Electrical Fast Transients (EFT), etc.).

In some circumstances it may be necessary to determine the precise immunity level in order to determine the magnitude of any safety margin. This can be determined by undertaking a test where the disturbance level is increased whilst observing the performance of the equipment or system until a malfunction is observed.

Testing under fault conditions, i.e. testing with a fault deliberately introduced in the equipment, is not required in EMC standards. However this may be useful in a safety standard in order to check the behaviour of the equipment after a possible degradation of its parts or components.

9.6 Performance criteria

Malfunctions involving safety risks shall be carefully evaluated, e.g.:

- non-operation when operation is required;
- unwanted operation when no operation is required;
- deviation from normal operation.

Particular attention should be given to

- the behaviour of safety-related elements (which may be tested separately),
- "fail safe" modes.

9.7 Test planning validation and documentation

EMC safety testing shall be undertaken in accordance with the specifications produced by the product committee, designer, manufacturer, and installer of the equipment.

A test plan shall be designed to validate the performance of the equipment in the intended operating environments. Testing shall be performed on a type approval or sample basis according to the recommendation of the product committee or designer. (A 100 % test is in some cases not advisable as testing with a high test level may damage too many devices.) The results of the testing shall be documented and retained.

In the event that the equipment is modified during or after the test, the relevant EMC test programme shall be repeated after the completion and documentation of any modifications deemed necessary.

10 Report

A report on the influence of EM phenomena on the functional safety of an electrical/electronic equipment is required and shall include the following information.

NOTE EM considerations may be a part of a comprehensive safety report considering other relevant phenomena (insulation, mechanical risks, etc.).

a) Spécification du matériel considéré

constructeur, type, numéro de série, etc.

b) Objet et fonctions du matériel

c) Description du matériel

(Dans la mesure où celle-ci est utile du point de vue des influences électromagnétiques.)

d) Sites où le matériel est installé et spécification du ou des environnements électromagnétiques

Identifier les phénomènes perturbateurs listés au tableau 1 considérés importants sur le site prévu, y compris les valeurs maximales et la fréquence d'occurrence.

Prendre en compte les phénomènes non couverts par les normes existantes, c'est-à-dire les champs de basse à moyenne fréquence entre la fréquence du réseau et 150 kHz.

e) Spécification des exigences de sécurité

Il convient que les exigences de sécurité soient spécifiées également pour l'analyse de sécurité, selon le point f), comme pour les essais de sécurité, selon le point g).

f) Analyse de sécurité

1) Spécification de la méthode d'analyse (c'est-à-dire AAP, etc.)

2) Compte rendu de la procédure d'analyse de sécurité c'est-à-dire:

- dans le cas d'une AAP: arbre de panne pour chaque événement;
- autres méthodes: tableaux correspondants.

3) Compte rendu des résultats de l'analyse de sécurité:

- phénomènes électromagnétiques critiques;
- éléments critiques du matériel;
- conditions d'installation critiques;
- éléments critiques pour la maintenance (du point de vue du vieillissement).

g) Essai de sécurité

1) Spécification des niveaux d'essai électromagnétiques nécessaires à la réalisation de la sécurité fonctionnelle requise.

2) Spécification d'autres types d'essais, comme par exemple les essais mécaniques, nécessaires pour assurer la stabilité de la sécurité dans le temps (du point de vue du blindage, par exemple)

3) Compte rendu des essais de sécurité.

h) Conclusions

a) Specification of the considered equipment

Manufacturer, type, serial number.

b) Purpose and functions of the equipment

c) Description of the equipment

(As far as relevant with regard to EM influences.)

d) Locations where the equipment is installed and specification of the EM environment(s)

Identify the disturbance phenomena listed in Table 1 which are considered to be of importance in the intended location including the maximum values and frequency of occurrence.

Consider further phenomena not covered by existing standards – i.e. low to middle frequency fields between power frequency and 150 kHz.

e) Specification of the safety requirements

The safety requirements should be specified as well for the safety analysis – according to item f) – as for safety testing – according to item g).

f) Safety analysis

1) Specification of the analysis method (i.e. FTA, etc.).

2) Report on the safety analysis procedure:

- in case of FTA: fault tree for each event;
- other methods: relevant tables.

3) Report on the result of the safety analysis:

- critical EM phenomena;
- critical elements of the equipment;
- critical installation conditions;
- critical maintenance items (with regard to ageing).

g) Testing for safety

1) Specification of the EM test levels necessary to achieve the required functional safety.

2) Specification of other types of test, e.g. mechanical tests – necessary to assure the stability of safety in course of time (e.g. with regard to shielding).

3) Report on the safety tests.

h) Conclusions

Annexe A (informative)

Exemples de niveaux d'essai d'immunité CEM

La présente annexe est fournie pour l'information des non experts en CEM.

Comme indiqué aux articles 6 et 9, les normes CEM de produits ou les articles relatifs à la CEM des normes générales de produits spécifient des niveaux d'essai d'immunité adaptés aux exigences fonctionnelles du matériel.

Du point de vue des exigences de sécurité, il convient d'augmenter ces niveaux d'essai d'immunité «fonctionnels» d'une marge de sécurité appropriée.

Le tableau A.1 donne pour information générale un résumé des essais d'immunité «fonctionnels» et des niveaux d'essai spécifiés dans les normes génériques de CEM.

- Les deux colonnes de gauche contiennent une liste des normes d'essai d'immunité correspondant aux diverses perturbations électromagnétiques qui ont été prises en compte. Il convient de noter que tous les phénomènes de perturbation ne sont pas inclus dans cette liste. Pour des raisons de sécurité, d'autres essais critiques peuvent également être pris en compte.
- Le tableau indique ensuite, pour deux environnements «classiques», environnements résidentiels et industriels, les niveaux typiques indiqués par les normes des séries CEI 61000-2 ou CEI 61000-4.
- Le tableau donne ensuite les niveaux d'essai d'immunité correspondants.

Il est important de noter que les normes génériques de CEM sont des normes d'application générale lorsqu'il n'existe aucune norme CEM de produits spécifique. Ces normes spécifient des essais et des niveaux d'essai suffisants pour assurer un niveau d'immunité acceptable, et peuvent de ce fait être considérées comme une référence générale. Toutefois, elles ne prennent pas en compte les cas extrêmes et peuvent donc ne pas être adaptées pour assurer la sécurité fonctionnelle.

Annex A (informative)

Examples of EMC immunity test levels

This annex is provided for the information of non-EMC experts.

As explained in clauses 6 and 9, the EMC product standards – or EMC clauses in general product standards – specify immunity tests levels normally with regard to functional requirements to the equipment.

With regard to safety requirements these "functional" immunity test levels should be increased by an appropriate safety margin.

Table A.1 gives for general information a summary of the "functional" immunity test and tests levels specified in the EMC generic standards.

- In the two left columns the table shows a list of the immunity test standards related to the various electromagnetic disturbances which have been considered. It should be noted that not all disturbance phenomena are listed. For safety purposes also further critical tests may be considered.
- The table then shows for two "classical" environments – residential and industrial environments – typical environmental levels as indicated in the relevant IEC 61000-2 or IEC 61000-4 series standard.
- It then shows the corresponding functional immunity test levels.

It is important to note that EMC generic standards are standards for general application when no specific product EMC standard exists. They specify tests and test levels sufficient to ensure an acceptable level of immunity and can therefore be considered as general reference. However, they do not consider extreme cases and therefore may not be adequate to ensure functional safety.

**Tableau A.1 – Niveaux de perturbations électromagnétiques typiques –
Niveaux des essais d'immunité donnés par les normes génériques d'immunité CEM**

Le présent tableau est un résumé simplifié donné **seulement pour information**. Comme pour les niveaux et les conditions d'essais réels, l'utilisateur se référera aux dernières versions des normes génériques.

Environnements résidentiel, commercial, industrie légère					Environnements industriels			
Normes fondamentales	Phénomènes et accès	Unités	Niveaux de perturbation typiques	Niveaux d'essai de la norme générique CEI 61000-6-1	Critères d'aptitude ^a	Niveaux de perturbation typiques	Niveaux d'essai de la norme générique CEI 61000-6-2	Critères d'aptitude
CEI 61000-4-13	Harmoniques: THD 5 ^{ème}	% U_n	8	Pas d'essai	–	10	Pas d'essai	
CEI 61000-4-11	Creux de tension alternative	% U_n	6	Pas d'essai	–	8	Pas d'essai	
CEI 61000-4-11	Coupures de tension alternative	$\Delta\%$ U_n	10 à 95	30 60	B/C	10 à 95	30 60	B/C
CEI 61000-4-14	Fluctuations de tension alternative	périodes	0,5 à 150	0,5 5	C	0,5 à 300	0,5 50	C
		périodes	2 500	250		2 500	250	
		$\Delta U_n\%$	+10, –10	Pas d'essai	–	+10, –15	Pas d'essai	–
CEI 61000-4-8	Champs magnétiques à la fréquence du réseau	A/m	0,5 à 5	3	A	10 à 30	30	A
CEI 61000-4-6	Perturbations HF conduites 0,15 MHz à 80 MHz ^b	V mod						
	– puissance en alternatif mc		1 à 10	3	A	1 à 10	10	A
	– puissance en continu mc		1 à 10	3	A	1 à 10	10	A
	– commande/signal mc		1 à 10	3	A	1 à 10	10	A
	– terre fonctionnelle		–	3	A	–	10	A
CEI 61000-4-3	Champs RF ≤80 MHz à 1 000 MHz	V/m mod	3 à 5	3	A	10	10	A
Amendement CEI 61000-4-3	Champs RF téléph. num. ^c 0,9 (1,8) GHz	V/m mod	3 à 10	3 ^c	A	–	Pas d'essai	–

Table A.1 – Typical EM disturbance levels – Immunity test levels in EMC immunity generic standards

This table is a simplified summary given for information purposes only. As for the actual test levels and testing conditions, users are referred to the latest versions of the generic standards.

Residential, commercial, light industrial environments			Industrial environments					
Basic standard	Phenomena and ports	Units	Typical disturbance levels	Test levels Generic standard IEC 61000-6-1	Performance criteria ^a	Typical disturbance levels	Test levels Generic standard IEC 61000-6-2	Performance criteria
IEC 61000-4-13	Harmonics: THD	% U_n	8	no test	–	10	No test	
IEC 61000-4-11	5th	% U_n	6	no test	–	8	No test	
	AC voltage dips	$\Delta\%$ U_n	10 to 95	30 60	B/C	10 to 95	30 60	B/C
IEC 61000-4-11	AC volt. interruptions >95%	periods	0,5 to 150	0,5 5		0,5 to 300	0,5 50	
IEC 61000-4-14	AC volt. fluctuations	periods	2 500	250	C	2 500	250	C
IEC 61000-4-8	Power frequency magnetic fields	$\Delta U_n\%$	+10, –10	No test	–	+10, –15	No test	–
		A/m	0,5 to 5	3	A	10 to 30	30	A
IEC 61000-4-6	Conducted h.f. disturbances 0,15 MHz to 80 MHz ^b	V mod						
	– AC power cm – DC power cm – control/signal cm – functional earth		1 to 10	3	A	1 to 10	10	A
			1 to 10	3	A	1 to 10	10	A
			1 to 10	3	A	1 to 10	10	A
			–	3	A	–	10	A
IEC 61000-4-3	R.F. fields ≤ 80 MHz to 1 000 MHz	V/m mod	3 to 5	3	A	10	10	A
IEC 61000-4-3 Amendment	R.F. fields digit. teleph. ^c 0,9 (1,8) GHz	V/m mod	3 to 10	3 ^c	A	–	No test	–

CEI 61000-4-5	Ondes de choc 1,2/50 (8/20) - puissance en alternatif ligne→terre ligne→ligne - puissance en continu ligne→terre ligne→ligne - commande/signal ligne→terre ligne→ligne	kV	1 à 2 0,5 à 1 - - 1 0,5	±2 ±1 ±0,5 ±0,5 - -	B B B B - -	2 à 4 0,5 à 2 1 à 2 0,5 à 1	±2 ±1 ±0,5 ±0,5 ±1 ±1	B B B B B B
CEI 61000-4-4	Transitoires rapides ^d - puissance en alternatif - puissance en continu - commande/signal - terre fonctionnelle	kV	1 à 2 - 0,5 à 1	±1 ±0,5 ±0,5 ±0,5	B B B B	2 à 4 2 à 4 1 à 2	±2 ±2 ±1° ±1	B B B B
CEI 61000-4-12	Transitoires oscillatoires - 0,1 MHz (puissance en alternatif) - 1 à 5 MHz (commande)	kV	1 à 4	Pas d'essai Pas d'essai	- -	1 à 4 0,5 à 2	Pas d'essai Pas d'essai	- -
CEI 61000-4-2	DES dans l'air au contact	kV	4 à 8 ^f	±8 ^f ±4	B B	4 à 8 ^f	±8 ^f ±4	B B

THD = Distorsion harmonique totale
5^{ème} = 5^{ème} harmonique (exemple)
NOTE 1 Les «niveaux de perturbation typiques» indiquent les valeurs supérieures des phénomènes qui se produisent dans des conditions environnementales normales. Ils peuvent être dépassés notablement dans certaines circonstances particulières. Les niveaux d'essai spécifiés dans les normes génériques ont été choisis afin de satisfaire aux exigences fonctionnelles d'une grande majorité d'articles en conditions normales. Les niveaux d'essai de sécurité doivent être augmentés d'un facteur de sécurité approprié – voir article 9.
NOTE 2 Certains phénomènes EM dont le contrôle n'est pas prévu par les normes génériques peuvent néanmoins avoir un effet sur la sécurité fonctionnelle et il convient qu'ils soient pris en compte par le comité de produits responsable (par exemple, champs dans la plage de fréquence de 3 kHz à 150 kHz).

^a Critères d'aptitude
A: L'appareil doit continuer à fonctionner comme prévu pendant et après l'essai.
B: L'appareil doit continuer à fonctionner comme prévu après l'essai. Pendant l'essai, une certaine dégradation du fonctionnement est autorisée, comme spécifié par le constructeur.
C: Une perte de fonction temporaire est autorisée pendant et après l'essai, à condition que la fonction soit auto-récupérable ou puisse être rétablie par une intervention sur les commandes.
^b Niveaux d'essai spécifiés = valeur eff. de la porteuse non modulée; mod ≡ 1 kHz, 80 %
^c UE seulement
^d Essai avec pince capacitive
^e Lignes impliquées directement dans la commande du processus
^f Tension de charge

IEC 61000-4-5	Surges 1,2/50 (8/20) - AC power L→G - AC power L→L - DC power L→G - DC power L→L - control/signal L→G - control/signal L→L	kV	1 to 2 0,5 to 1 - - 1 0,5	±2 ±1 ±0,5 ±0,5 - -	B B B B - -	2 to 4 0,5 to 2 1 to 2 0,5 to 1	±2 ±1 ±0,5 ±0,5 ±1 ±1	B B B B B B
IEC 61000-4-4	Fast transients ^d - AC power - DC power - control/signal - functional earth	kV	1 to 2 - 0,5 to 1 -	±1 ±0,5 ±0,5 ±0,5	B B B B	2 to 4 2 to 4 1 to 2	±2 ±2 ±1 ^e ±1	B B B B
IEC 61000-4-12	Oscillatory transients - 0,1 MHz (AC power) - 1 to 5 MHz (control)	kV	1 to 4	No test No test	- -	1 to 4 0,5 to 2	No test No test	- -
IEC 61000-4-2	ESD air contact	kV	4 to 8 ^f	±8 ^f ±4 ^f	B B	4 to 8 ^f	±8 ^f ±4 ^f	B B

THD = Total harmonic distortion
5th = Example 5th harmonic

RF = Radio frequency
ESD = Electrostatic discharge

cm = Common mode
dm = Differential mode

L→G = Line to Ground
L→L = Line to Line

NOTE 1 The "typical disturbance levels" show upper values of the phenomena occurring under normal environmental conditions. They may be notably exceeded in some particular circumstances. The test levels specified in the generic standards have been chosen in order to meet the functional requirements of a great majority of items under normal conditions. Test levels for safety have to be enhanced by an appropriate safety factor – see clause 9.

NOTE 2 Some EM phenomena not to be checked according the generic standards may still have an functional safety effect and should also be considered by the responsible product committee (e.g. fields in the frequency range 3 kHz to 150 kHz).

^a Performance criteria:
A: Apparatus shall continue to operate as intended during and after the test.
B: Apparatus shall continue to operate as intended after the test. During the test, a certain degradation of performance is allowed as specified by the manufacturer.
C: Temporary loss of function is allowed during and after the test, provided the function is self-recoverable or can be restored by operation of the controls.

^b Specified test levels = r.m.s. value of unmodulated carrier; mod ≡ 1 kHz, 80 %.

^c EU only.

^d Test with capacitive clamp.

^e Lines directly involved in process control.

^f Charge voltage.

Annexe B (informative)

Exemples d'analyses de sûreté de fonctionnement du point de vue des phénomènes électromagnétiques

Cette annexe présente deux exemples pratiques basés sur la méthode de l'analyse par arbre de panne (AAP) pour l'application des principes décrits dans les articles 8 et 9 de la présente spécification technique.

- B.1 Appareil unique: Contrôleur électronique pour brûleur à gaz;
- B.2 Système compliqué de plusieurs appareils (à l'étude).

Conformément à 8.2, les étapes suivantes sont prises en compte:

- a) but et fonctions attendues du matériel considéré;
- b) structure physique (matérielle) du matériel;
- c) configuration logicielle (si possible avec la même structure que le matériel) ;
- d) environnement électromagnétique et niveaux d'essais fonctionnels;
- e) buts de l'analyse des dangers et des risques (événements de tête);
- f) analyse par arbre de panne:
 - 1) construction de l'arbre de panne;
 - 2) évaluation de l'arbre de panne du point de vue de la sécurité;
- g) recommandations pour la conception du matériel;
- h) conclusions relatives au plan d'essais de sécurité:
 - 1) quels sont les essais pertinents;
 - 2) quels niveaux d'essai.

Annex B (informative)

Examples of dependability analyses with regard to electromagnetic phenomena

This annex presents two practical examples based on the method of fault tree analysis (FTA) for the application of the principles described in clause 8 and 9 of this technical specification:

- B.1 Single apparatus: Electronic gas burner controller;
- B.2 Complicated system of several apparatus (under consideration).

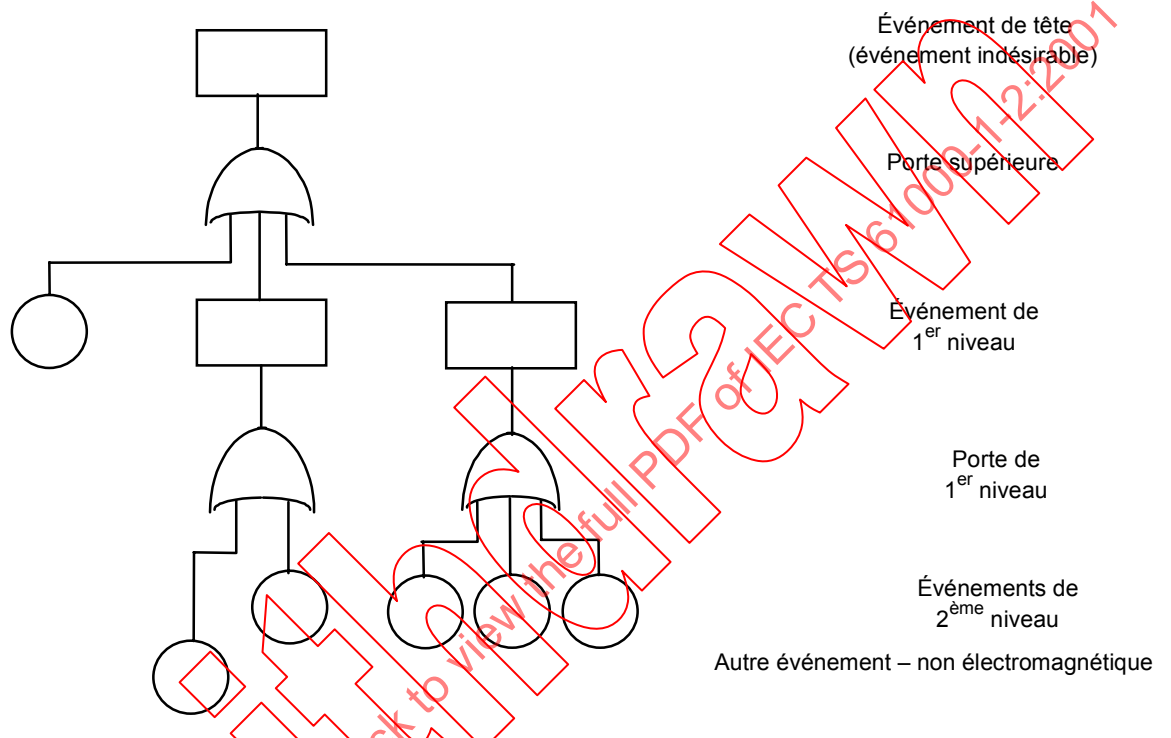
According to 8.2 the following steps have to be considered:

- a) aim and intended functions of the equipment considered;
- b) physical (hardware) structure of the equipment;
- c) software configuration (if possible with the same structure as the hardware);
- d) electromagnetic environment and functional test levels;
- e) purposes of the hazard and risk analysis (top events);
- f) fault tree analysis:
 - 1) construction of the Fault tree;
 - 2) evaluation of the Fault tree with regard to safety;
- g) recommendations for the design of the equipment
- h) conclusions with regards to the test plan for safety:
 - 1) which tests are relevant;
 - 2) which test levels.

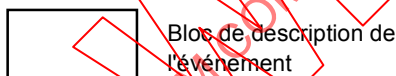
Extraits de la CEI 61025 – Analyse par arbre de panne (AAP)

Extrait des paragraphes 6.4 et 7.4.2:

L'élaboration de l'arbre de panne commence par la définition de l'événement de tête. Cet événement de tête est l'événement de sortie de la porte du sommet de l'arbre, alors que les événements d'entrée correspondants se rapportent à des causes et à des conditions possibles de l'apparition de l'événement de tête. Chaque événement d'entrée peut, lui-même être un événement de sortie d'une porte se trouvant à un niveau inférieur. Ainsi, l'analyste progresse vers le bas de l'arbre de panne, en passant du mécanisme au mode, jusqu'au moment où les limites de résolution de l'arbre sont atteintes.

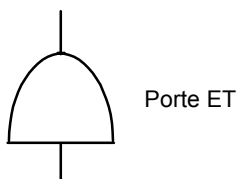


Légende:

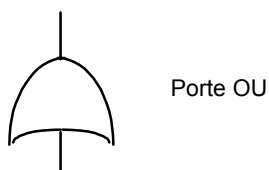


Informations requises:

- code événement
- nom ou description de l'événement
- niveau
- probabilité d'occurrence (le cas échéant)



Porte ET



Porte OU



Entrée transfert



Sortie transfert

pour cause commune

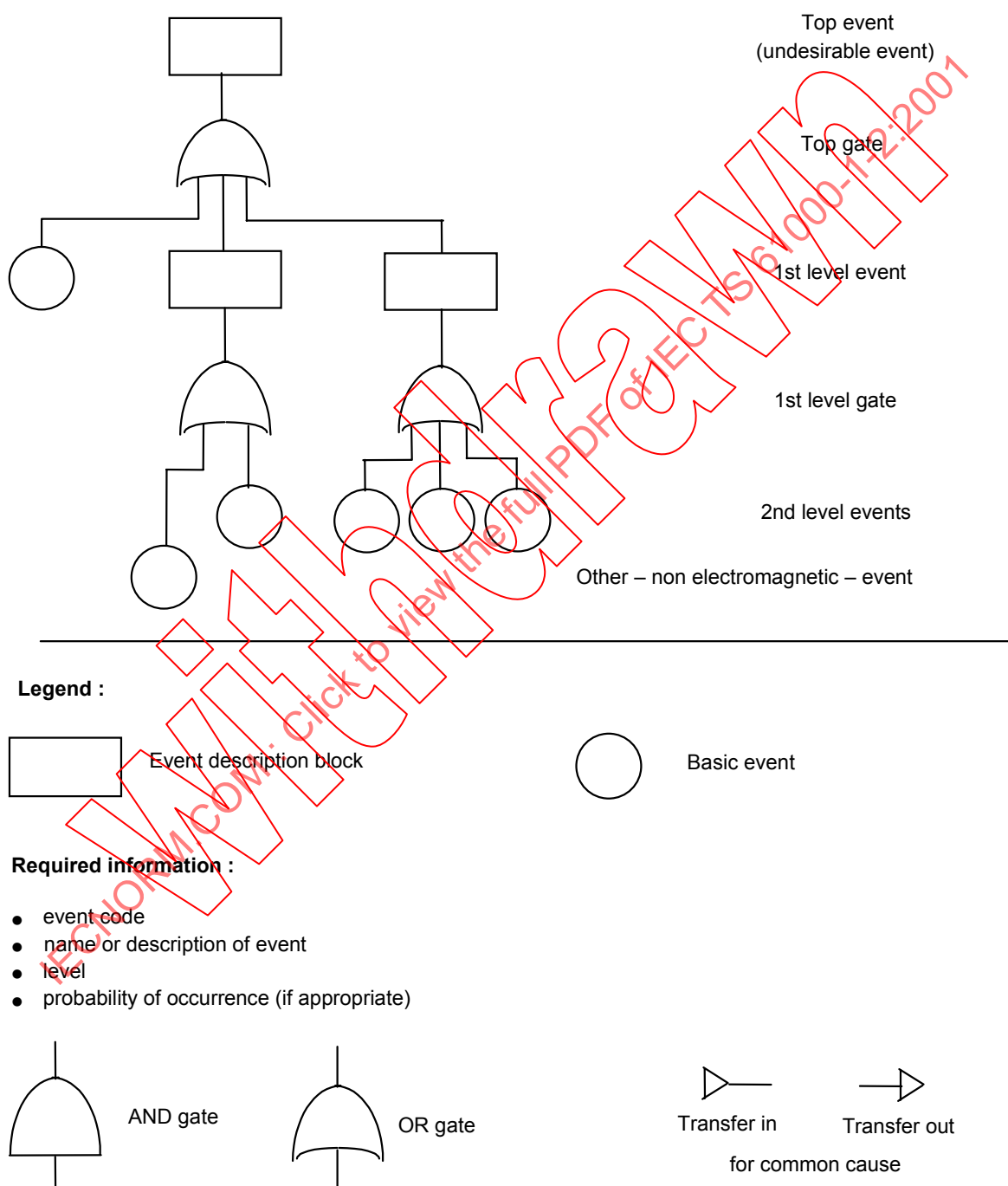
IEC 475/01

Figure B.1 – Symboles pour la construction d'un arbre de panne

Extracts from IEC 61025 – Fault Tree Analysis (FTA)

Extract from 6.4 and 7.4.2:

Fault tree development starts with the definition of the top event. The top event is the output of the top gate while the corresponding input events identify possible causes and conditions for the occurrence of the top event. Each input event may itself be an output event of a lower level gate. In this way the analyst proceeds down the tree transferring attention from mechanism to mode, until ultimately the limit of resolution is reached.

**Figure B.1 – Symbols for the construction of a fault tree**

B.1 Exemple B.1: Contrôleur électronique pour brûleur à gaz

B.1.1 Objet et fonctions attendues du matériel

Le contrôleur électronique pour brûleur à gaz est destiné à commander un brûleur à gaz. Un brûleur à gaz est considéré comme un appareil critique pour la sécurité qui doit satisfaire aux normes de produits correspondantes. Le contrôleur assure deux fonctions principales:

a) commander les fonctions de l'appareil:

c'est-à-dire fournir de l'eau chaude de chauffage central ou de l'eau chaude sanitaire avec régulation de la température;

b) protection:

c'est-à-dire détection jusqu'à deux défaillances indépendantes susceptibles d'entraîner une situation dangereuse. Si une telle défaillance est détectée, une vanne de gaz doit être fermée. Ceci implique un contrôle séquentiel avant chaque démarrage et un contrôle continu pendant le fonctionnement. Les paramètres dépendent des propriétés de l'appareil. En général, une défaillance critique primaire doit être détectée dans un délai maximal de 3 s, tandis qu'une défaillance secondaire (c'est-à-dire pour contrôler la première protection) doit être détectée dans un délai maximal de 24 h.

B.1.2 Structure matérielle du matériel

Voir figures B.2 et B.3.

a) Les mesures générales de sécurité sont liées aux processus (risques pour la sécurité):

- surveillance de la flamme (capteur optique) pour éviter l'écoulement de gaz non brûlé;
- thermostat à limite haute, pour éviter une élévation excessive de la température;
- détection de la pression d'air, pour éviter la combustion toxique.

b) Des mesures de sécurité spécifiques sont liées au contrôleur de brûleur proprement dit:

- protections primaires: contrôle de l'alimentation, chien de garde, contrôle des ROM/RAM et contrôle des capteurs;
- protections secondaires: contrôle de l'alimentation secondaire, contrôle du chien de garde, contrôle des ROM/RAM secondaires et contrôle de l'amplificateur de flamme.

B.1.3 Configuration logicielle

Pour simplifier cet exemple, seules les fonctions importantes pour la sécurité sont prises en compte ci-dessous (sans être décrites en détail).

Il existe deux groupes de fonctions de sécurité:

a) les contrôles lancés à la suite d'une demande de chaleur; les contrôles séquentiels:

- pression d'air;
- fausse flamme;
- dégagement de gaz;
- allumage.

b) des autocontrôles de diagnostic effectués en continu pendant le fonctionnement du contrôleur et du brûleur (voir B.1.5).

B.1 Example B.1: Electronic gas burner controller

B.1.1 Aim and intended functions of the equipment

The electronic burner controller is intended to control a gas burner. A gas burner is regarded as a safety-critical appliance which has to meet the relevant product standards. The controller should carry out two main functions:

- a) control the functions of the appliance:
 - i.e. provide hot water for central heating or domestic hot water with a temperature control;
- b) safeguarding:
 - i.e. check for up to two independent failures which might cause a hazardous situation. If such a failure is detected, an independent gas valve has to be shut down. This involves a sequential checking before each start and a continuous checking during the process. Parameters depend on the properties of the appliance. In general, a primary critical failure has to be detected within 3 s while a secondary failure (i.e. to check the first safeguard) has to be detected within 24 h.

B.1.2 Hardware structure of the equipment

See Figures B.2 and B.3.

- a) General safety measures are related to the process (safety risks):
 - flame supervision (optical sensor) to prevent the flow of unburned gas;
 - high limit thermostat, to prevent a too high temperature;
 - air pressure detection, to prevent poisonous burning.
- b) Specific safety measures are related to the burner controller itself:
 - primary safeguards: power supply check, watchdog, ROM/RAM check and sensor checks;
 - secondary safeguards: secondary power supply check, watchdog check, secondary ROM/RAM check and flame amplifier check.

B.1.3 Software configuration

For simplification in this example, only the safety-related functions are considered here (without being described in detail).

Two groups of safety functions should be mentioned:

- a) safety checks initiated after a heat demand; sequential checks:
 - air pressure;
 - false flame;
 - gas release;
 - ignition.
- b) diagnostic self-checks made continuously during the operation of the controller and the burner (see B.1.5).

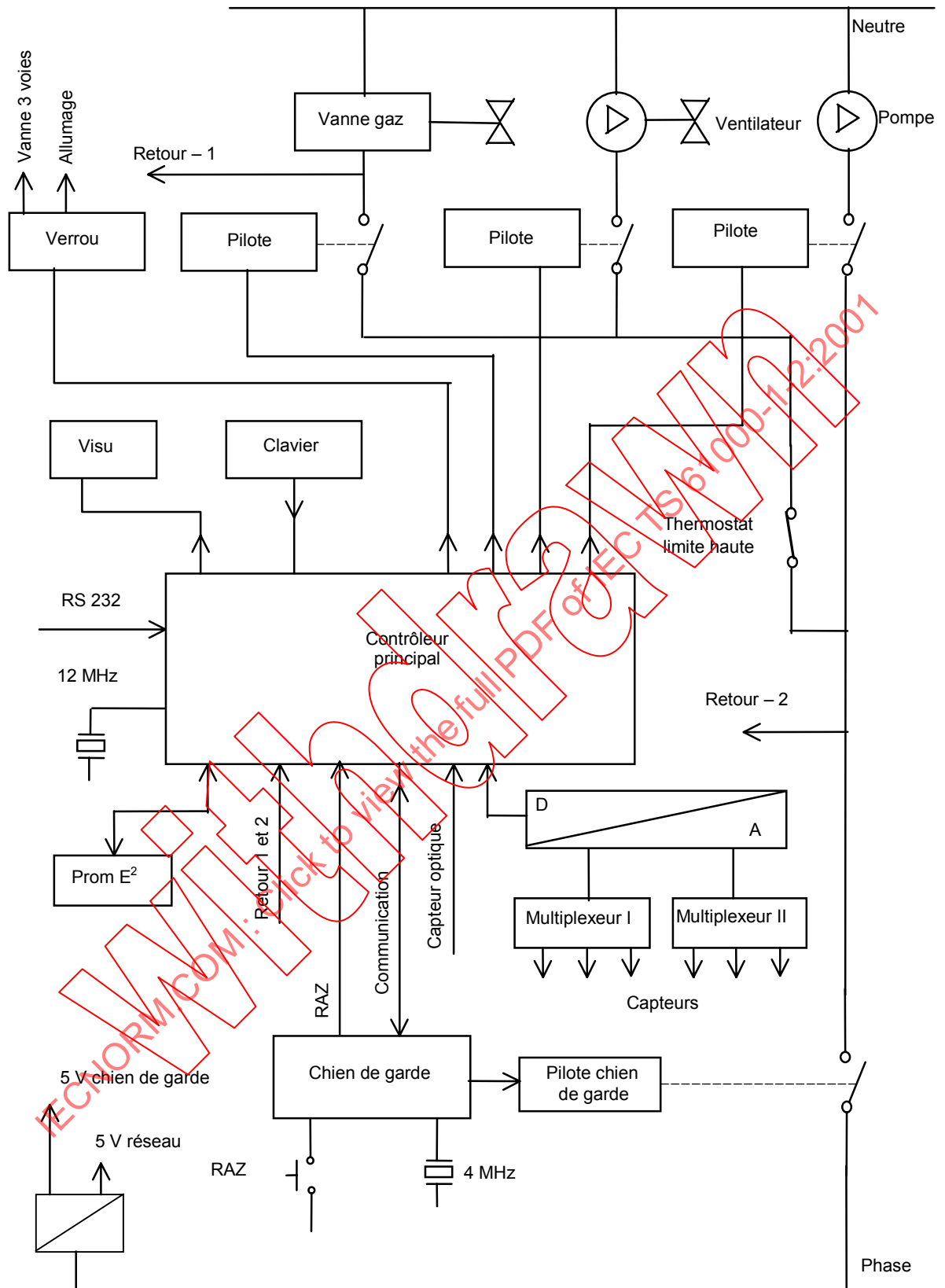


Figure B.2 – Contrôleur pour brûleur à gaz: structure matérielle

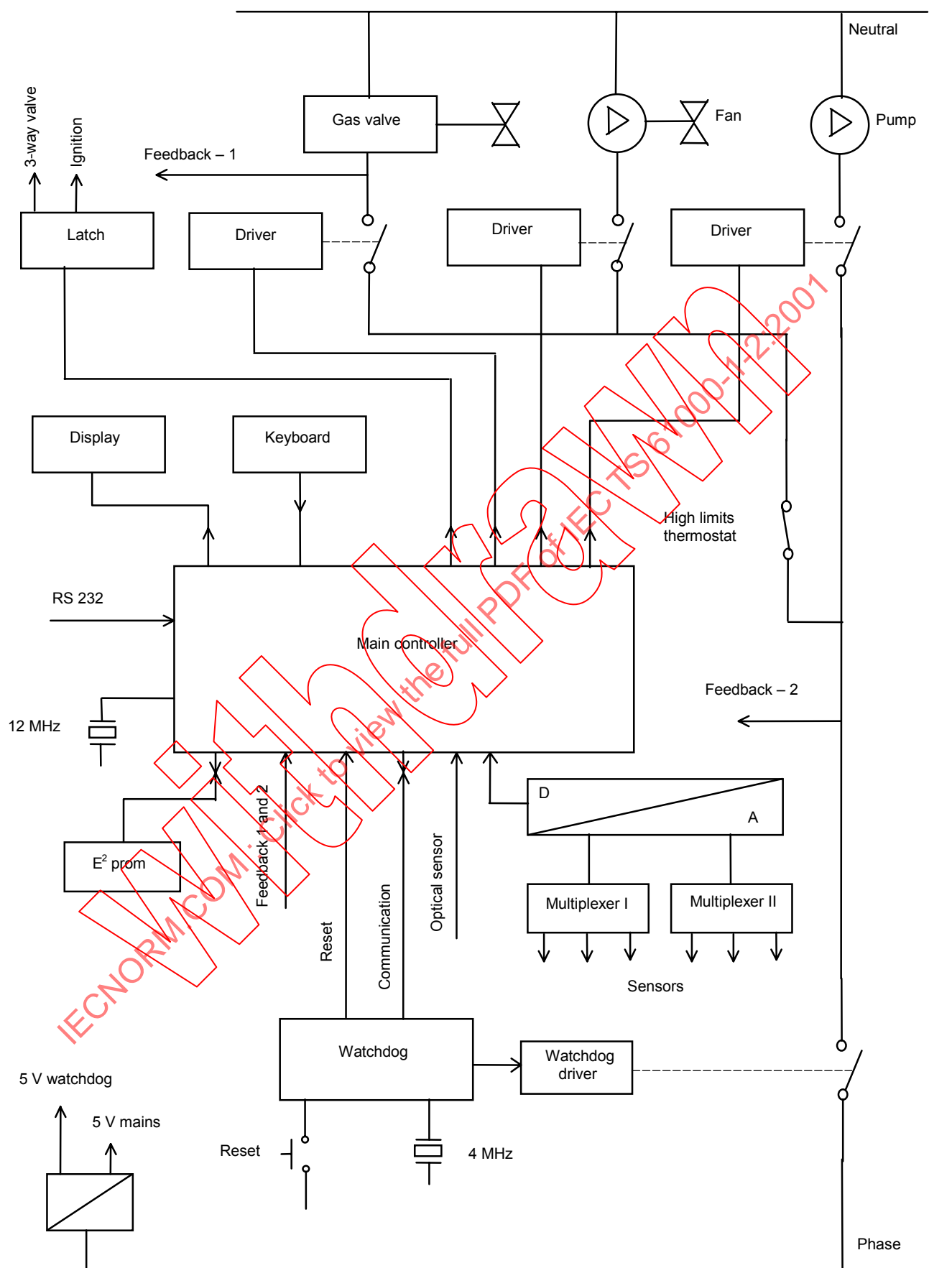
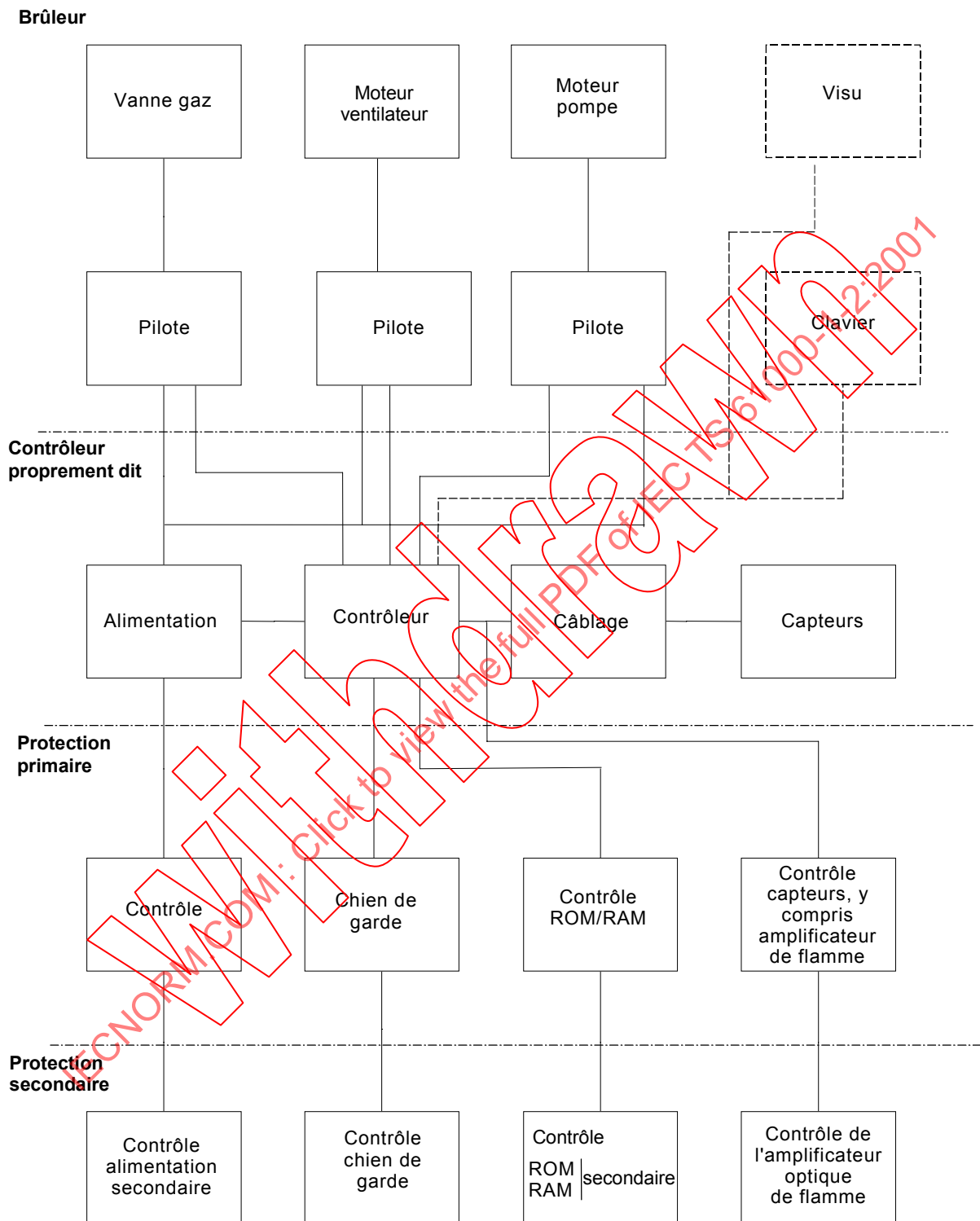
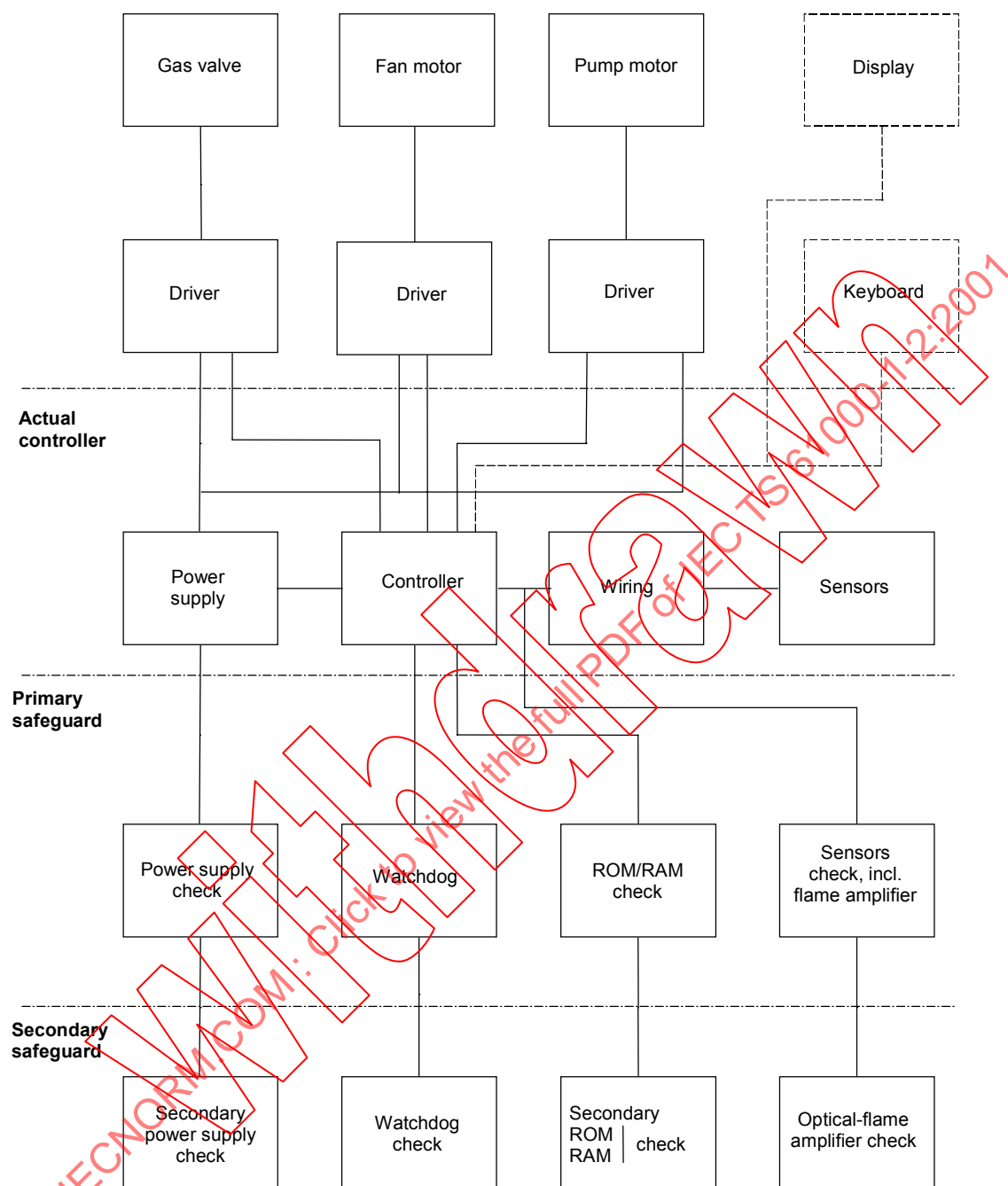


Figure B.2 – Gas burner controller: hardware structure



IEC 477/01

Figure B.3 – Contrôleur pour brûleur à gaz: synoptique

Burner

IEC 477/01

Figure B.3 – Gas burner controller: Block diagram

B.1.4 Environnement électromagnétique et niveaux d'essai fonctionnel

Le brûleur considéré est destiné à être installé dans un environnement résidentiel. Les essais d'immunité CEM et de sécurité fonctionnelle correspondants sont spécifiés par exemple dans le tableau B.1. Pour un environnement industriel, des niveaux d'essai d'immunité et de sécurité supérieurs sont pris en compte.

Noter que tous les phénomènes électromagnétiques listés dans le tableau 1 n'ont pas été jugés pertinents pour ce type de matériel.

B.1.5 Objet de l'analyse des dangers et des risques

L'objet de l'analyse des dangers et des risques est, pour les risques de sécurité indésirables (événements de tête), de déterminer:

- quels phénomènes électromagnétiques peuvent provoquer ces risques (événements de base),
- et à quels endroits du dispositif, afin de prendre les mesures de correction appropriées.

Les événements suivants – événements de tête – ne doivent pas se produire avec un brûleur à gaz:

- gaz non brûlé
cause: pas d'allumage et détection défectueuse de la flamme;
- température trop élevée
cause: capteur de commande de température défectueux ou absence d'eau (circulation);
- combustion toxique
cause: air insuffisant (ventilateur défectueux ou vitesse incorrecte).

B.1.6 Analyse par arbre de panne (AAP)

Pour les besoins du présent exemple, seul le cas du «gaz non brûlé» est développé ci-dessous. Dans la pratique, il convient d'élaborer des AAP similaires pour les autres cas: «température trop élevée» et «combustion toxique».

B.1.6.1 Construction de l'arbre de panne

L'arbre de panne a été élaboré conformément à la CEI 61025 (les caractéristiques importantes sont résumées dans le tableau en introduction de la présente annexe).

L'arbre de panne pour «gaz non brûlé» est représenté à la figure B.4. Noter que

- l'arbre de panne ne prend en compte que les influences électromagnétiques. Tous les autres effets susceptibles d'avoir une incidence sur la sécurité du contrôleur, tels qu'une défaillance d'un composant, un erreur de manipulation de l'opérateur, etc. ne sont pas inclus à cet arbre de panne afin que celui-ci soit strictement limité aux effets électromagnétiques;
- les événements et influences électromagnétiques non directement liés à l'événement de tête ne sont pas inclus dans l'arbre de panne:
par exemple, dans le cas du «gaz non brûlé», on pourrait penser qu'une défaillance du ventilateur pourrait affecter cet événement. En fait, une défaillance du ventilateur est détectée par une «combustion toxique»;
- la «tension d'alimentation» sera prise en compte dans ce cas comme une «cause commune» et traitée une fois seulement au niveau le plus bas (avec un symbole de sortie de transfert).

Le circuit d'alimentation peut être très compliqué et sera analysé comme un sous-système séparé dans un arbre de panne séparé.

Le «contrôle de l'alimentation» (voir figure B.3) peut être utilisé aussi bien pour la tension secteur que pour la tension 5 V = des circuits électroniques de sorte qu'un seul contrôle de l'alimentation est nécessaire.

B.1.4 Electromagnetic environment and functional test levels

The considered burner is intended to be installed in a residential environment. The corresponding EMC functional immunity and safety tests are specified for example in Table B.1. For an industrial environment higher immunity and safety test levels are considered.

Note that not all the electromagnetic phenomena listed in Table 1 have been judged as being relevant for this kind of equipment.

B.1.5 Purpose of the hazard and risk analysis

Purpose of the hazard and risk analysis is for the undesirable safety risks (top events) to detect:

- which electromagnetic phenomena can cause these risks (basic events),
- at which places in the device, in order to take appropriate mitigation measures.

The following events – top events – should not occur with a gas burner:

- unburned gas:
cause: no ignition and defective flame detection;
- temperature too high:
cause: defective control temperature sensor or no water (circulation)
- poisonous burning:
cause: insufficient air (fan defective or incorrect speed).

B.1.6 Fault tree analysis (FTA)

For the purpose of this example, only the case of "unburned gas" is developed here. In practice similar FTA's should be made for the other cases: "temperature too high" and "poisonous burning".

B.1.6.1 Construction of the fault tree

The construction of the fault tree has been carried out according to IEC 61025 (the relevant important features of which are summarised in the table in introduction to this annex).

The fault tree for "unburned gas" is represented in Figure B.4. The following points should be noted.

- The fault tree considers only EM influences. All other effects which may have an influence on the controller safety like component failure, wrong handling by the operator etc., shall not be included in this fault tree, in order to be specific with regard to electromagnetic effects.
events and EM influences which are not directly related to the top event shall not be included in the fault tree.
- For example, in the case of "unburned gas", it could be thought that a fan failure could affect this event. In fact a fan failure is detected by a "poisonous burning".
- The "supply voltage" has to be considered in this case as a "common cause" and is treated only once at the lowest level (with a transfer-out symbol).

The supply circuit may be quite complicated and should be analysed as a separate sub-system in a separate sub-fault tree.

The "power supply check" (see Figure B.3) can be used as well for the mains voltage as for the 5 V = supply of the electronic circuits so that only one power supply check is necessary.

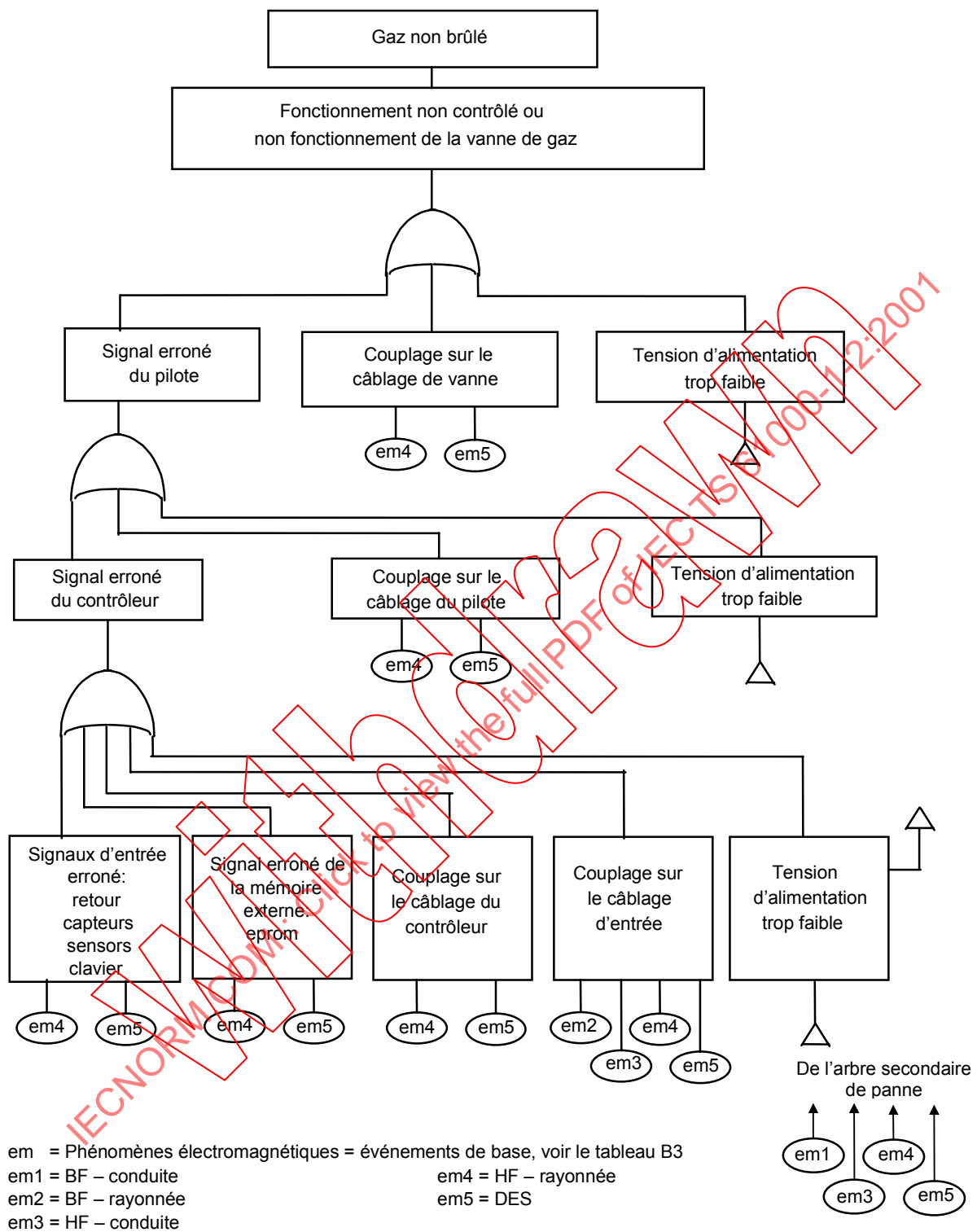
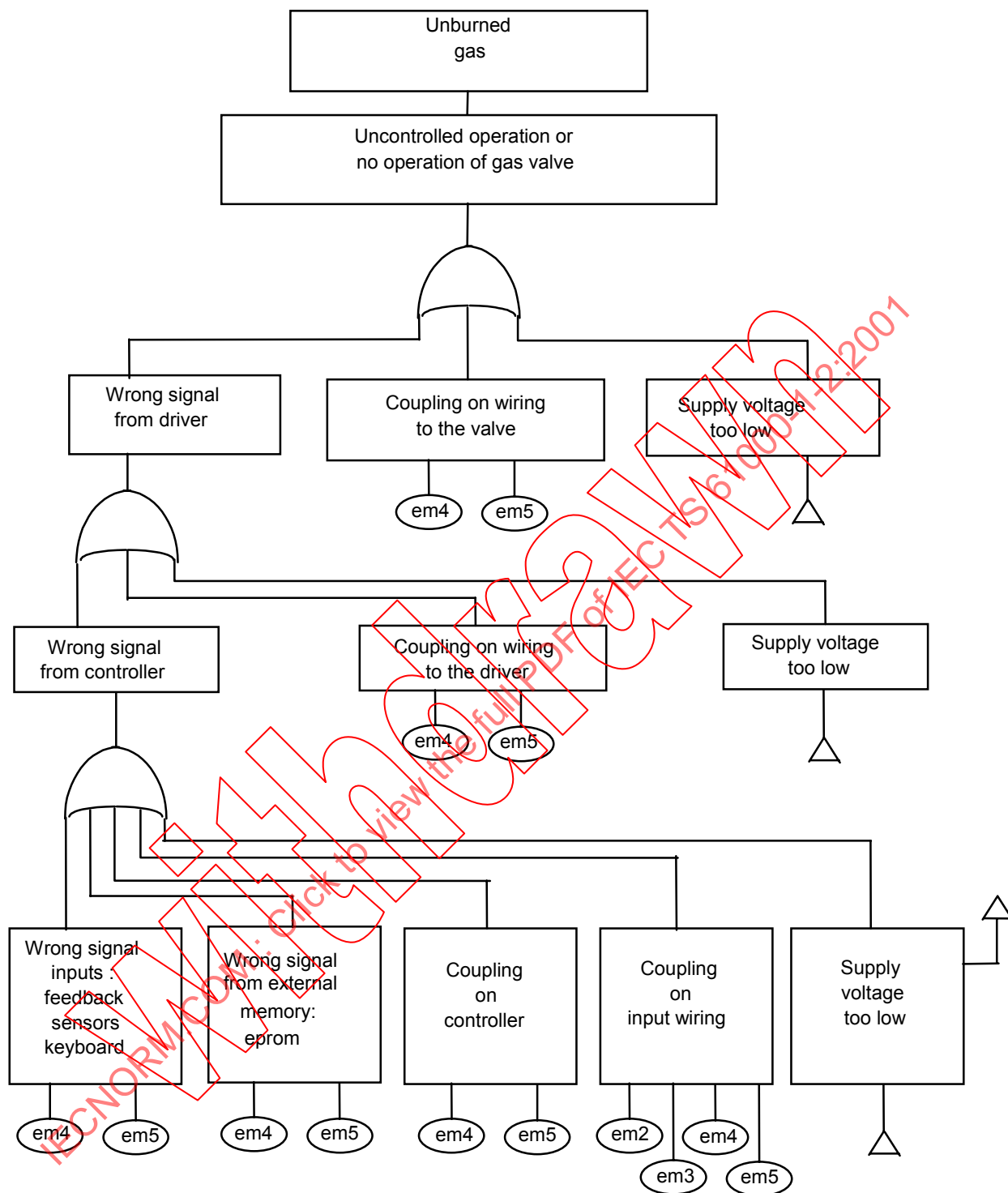


Figure B.4 – Contrôleur pour brûleur à gaz: AAP pour l'événement de tête gaz non brûlé



EM = Electromagnetic phenomena = basic events, see table B.1

em1 = LF – conducted

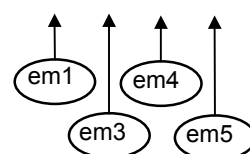
em2 = LF – radiated

em3 = HF – conducted

em4 = HF – radiated

em5 = ESD

From sub-fault tree



IEC 478/01

Figure B.4 – Gas burner controller; FTA for the top event unburned gas

Tableau B.1 – Exemple de phénomènes électromagnétiques et niveaux d'essai pour un appareil unique

Événement perturbateur de base	Essais d'immunité Niveaux d'essai fonctionnel typiques	Essais de sécurité Niveaux d'essai fonctionnel typiques
Harmoniques sur le secteur	Non applicable	Non applicable
Signaux sur le secteur	Non applicable	Non applicable
Creux de tension (critères B) Coups de tension (critères C)	50 % > 20 ms 100 % > 20 ms	50 % > 20 ms 100 % > 20 ms
Champ magnétique à la fréquence du réseau	Non applicable	Non applicable
Onde de choc 1,2/50 µs alimentation secteur et lignes de commande non symétriques: entre lignes entre ligne et terre	0,5 kV _p 1 kV _p	1 kV _p 2 kV _p
Transitoires oscillatoires	Non applicable	Non applicable
Transitoires rapides en salves sur l'alimentation secteur sur les lignes de commande	1 kV _p 0,5 kV _p	2 kV _p 1 kV _p
Perturbations conduites induites par les radiofréquences 150 kHz à 80 MHz	3 V _{emf} + 6 dB aux fréquences CB et ISM	10 V _{emf} + 6 dB aux fréquences CB et ISM
Champ RF rayonné 80 MHz à 1 000 MHz	3 V/m, + 6 dB aux fréquences CB et ISM	10 V/m, + 6 dB aux fréquences CB et ISM
Téléphones mobiles 900 MHz et 1,89 GHz, <i>d</i> > 0,5m	6 V/m	20 V/m
DES au contact dans l'air	4 kV 4 kV	6 kV 8 kV
NOTE 1 Valeurs issues de la norme CENELEC EN 50165. NOTE 2 Les «niveaux d'essais d'immunité» impliquent qu'à ces niveaux le matériel en essai (EST) doit continuer de satisfaire à ses exigences de bon fonctionnement (article 7, a)). Les «niveaux d'essais de sécurité» impliquent qu'à ces niveaux le matériel en essai peut être influencé, mais qu'il n'y a pas obligation qu'il satisfasse à ses exigences de bon fonctionnement. Toutefois, il doit continuer d'assurer sa sécurité après les essais (article 7, b) ou c)). NOTE 3 Pour les autres implications de sécurité et pour les environnements plus sévères, des niveaux d'essais plus élevés peuvent être nécessaires (comme par exemple environnements industriels, téléphones mobiles situés à moins de 0,5 m).		

B.1.6.2 Évaluation de l'arbre de panne du point de vue de la sécurité

L'arbre de panne illustre d'une manière générale quels phénomènes électromagnétiques – les événements de base – ont une influence sur les diverses parties du dispositif. Ces phénomènes électromagnétiques peuvent avoir, en fonction de leur niveau, un effet plus ou moins grand sur ce dispositif, susceptible de donner lieu aux différentes classes de dégradation spécifiées dans l'article 7 (pas d'effet significatif, effet auto-récupérable, effet récupéré par l'opérateur sans dommage, dommage). Toutefois, tous ces effets n'ont pas nécessairement un impact critique sur la sécurité.

Sur la base de la conception du matériel (mesures de protection, par exemple) et de l'expérience (résultats obtenus avec des matériels similaires), l'ingénieur en CEM peut évaluer quels phénomènes électromagnétiques – au niveau le plus élevé des perturbations dans l'environnement – peuvent avoir ou auront un impact critique sur la sécurité.

Table B.1 – Example of EM phenomena and test levels for a single apparatus

Disturbance basic event	Immunity tests Typical functional test levels	Safety tests Typical safety test levels
Harmonics on mains	Not applicable	Not applicable
Signals on mains	Not applicable	Not applicable
Voltage dips (criteria B) Interruptions (criteria C)	50 % > 20 ms 100 % > 20 ms	50 % > 20 ms 100 % > 20 ms
Power frequency magnetic field	Not applicable	Not applicable
Surges 1,2/50 μ s mains and unbalanced control lines: line-to-line line-to-earth	0,5 kV _p 1 kV _p	1 kV _p 2 kV _p
Oscillatory transients	Not applicable	Not applicable
Fast transient bursts on mains on control lines	1 kV _p 0,5 kV _p	2 kV _p 1 kV _p
Conducted disturbances induced by radio-frequencies 150 kHz – 80 MHz	3 V _{emf} + 6 dB at CB- and ISM frequencies	10 V _{emf} + 6 dB at CB- and ISM frequencies
Radiated radio-frequency field 80 – 1 000 MHz	3 V/m, + 6 dB at CB- and ISM frequencies	10 V/m, + 6 dB at CB- and ISM frequencies
Mobile phones 900 MHz and 1.89 GHz, $d > 0,5$ m	6 V/m	20 V/m
ESD contact air	4 kV 4 kV	6 kV 8 kV
NOTE 1 Values quoted from CENELEC EN 50165. NOTE 2 The "immunity test levels" imply that at these levels the equipment under test (EUT) has to maintain its functional requirements (clause 7, item a)). The "safety test levels" imply that at these levels the EUT may be influenced, but does not have to fulfil the functional requirements, however it has to maintain a safe state after the tests (clause 7, items b) and c)). NOTE 3 For other safety implications and for more severe environments higher test levels may be necessary (e.g. industrial environments, mobile phones closer than 0,5 m).		

B.1.6.2 Evaluation of the fault tree with regard to safety

The fault tree represents in a general manner which EM phenomena – the basic events – have an influence on the various parts of the device. These EM phenomena can have, according to their level, a more or less strong effect on this device, which may lead to the different classes of degradation specified in clause 7 (no significant effect, self-recoverable effect, operator recovered effect but no damage, damage). However, not all off these effects may have a critical safety effect.

Basing on the design of the equipment (e.g. protection measures) and on experience (results with other similar equipment), the EMC engineer can evaluate which EM phenomena – at the highest environmental level of the disturbances – can/will have a critical safety impact.

Une telle évaluation est faite pour le cas du «gaz non brûlé» dans le tableau B.2. Elle montre que

- les creux et coupures de tension secteur, tous les phénomènes conduits et rayonnés à haute fréquence, les DES peuvent avoir une influence critique en termes de sécurité;
- les champs magnétiques à la fréquence du réseau et les harmoniques de la tension secteur sont peu susceptibles d'avoir une influence critique mais il convient peut-être de ne pas les négliger entièrement;
- les phénomènes rayonnés à haute fréquence peuvent affecter tous les éléments du contrôleur.

Le tableau permet d'identifier quelles parties il est nécessaire

- de concevoir avec soin du point de vue de la sécurité;
- d'examiner avec soin en cas de défaillances lors des essais de sécurité.

Noter que le tableau B.2 montre que certains phénomènes peuvent être critiques pour la sécurité mais n'ont pas encore été pris en compte dans la norme de produits correspondante. Ils est néanmoins nécessaire qu'ils fassent l'objet d'essais.

Tableau B.2 – Evaluation de l'influence des perturbations électromagnétiques sur le fonctionnement sûr du contrôleur pour brûleur à gaz en ce qui concerne le gaz non brûlé

Phénomènes électromagnétique		BF – conduits		BF- rayonnés	HF – conduits				HF – rayonnés		DES
Partie de l'EST		Harm.	Creux Coup.	Champ Mag.	Surt.	Tr. osc.	Tr. salv.	CW	CW	Tél. mobile	
1	Alimentation y compris secteur	?	X	–	X	X	X	X	X	X	X
2	Mémoire contrôleur	–	–	–	–	–	–	–	X	X	X
3	Accessoires Capteurs Clavier	–	–	–	–	–	–	–	X	X	X
4	Câblage interne	–	–	?	–	–	–	–	X	X	X
5	Câblage externe	–	–	?	X	?	X	X	X	X	X
EST = Matériel en essai BF = Basse fréquence HF = Haute fréquence DES = Décharge électrostatique Harm. = Harmoniques Coup. = Coupures Mag. = Magnétique Surt. = Surtensions Surt. = Surtensions Tr. osc. = Transitoires oscillatoires Tr. salv. = Transitoires en sèves CW = Ondes continues Tél. mobile = Téléphone mobile											
NOTE X indique une influence critique probable; ? indique une influence critique improbable; – indique qu'une influence critique peut être négligée.											

B.1.7 Recommandations pour la conception du contrôleur pour brûleur à gaz

La norme de produits pour brûleurs à gaz exige un «critère à deux défaillances»: il convient qu'aucune situation dangereuse ne soit créée par une défaillance unique ou deux défaillances indépendantes.

Un exemple de cette philosophie est donné à la figure B.2. Si une défaillance se produit dans le circuit de contrôle de l'alimentation uniquement, il s'agit d'une défaillance dite dormante qui n'entraîne pas de situation dangereuse. Lorsque le circuit d'alimentation est défaillant et fournit une tension trop faible, le contrôleur principal ne fonctionne donc pas correctement et produit des signaux aléatoires vers les sorties, qui peuvent entraîner une ouverture de la vanne de gaz. Il convient que deux défaillances indépendantes de ce type n'entraînent pas de situation dangereuse.

Such an evaluation is made for the case of "unburned gas" in Table B.2. It shows that

- voltage dips and interruptions in the mains, all high frequency conducted and radiated phenomena and ESD may have a critical influence with regard to safety;
- power frequency magnetic fields and harmonics of the mains voltage are unlikely to have a critical influence but should perhaps not be fully neglected;
- high frequency radiated phenomena may affect all the elements of the controller.

The table allows to identify which parts must be

- carefully designed with regard to safety;
- carefully examined in case of failure when testing for safety.

It should be noted that Table B.2 shows that some phenomena may be critical for safety which have not yet been considered in the relevant product standard. They nevertheless should be tested.

Table B.2 – Evaluation of the influence of the EM disturbances on the safe operation of the gas burner controller with regard to unburned gas

EM phenomena		LF-conducted		LF-radiated	HF-conducted				HF-radiated		ESD
Part of the EUT		Harm.	Dips, Interr.	Magnetic field	Surge	Osc. tr.	FT B	CW	CW	Mobile Phone	
1	Power supply including mains	?	X	–	X	X	X	X	X	X	X
2	Controller memory	–	–	–	–	–	–	–	X	X	X
3	Accessories Sensors Keyboard	–	–	–	–	–	–	–	X	X	X
4	Internal wiring	–	–	?	–	–	–	–	X	X	X
5	External wiring	–	–	?	X	?	X	X	X	X	X
EUT = Equipment under test LF = Low frequency ESD = Electrostatic discharge Harm. = Harmonics HF = High frequency Interr. = Interruptions Osc. tr. = Oscillatory transients FTB = Fast transient bursts CW = Continuous wave NOTE X indicates a probable critical influence; ? indicates an unlikely critical influence; – indicates that a critical influence can be neglected.											

B.1.7 Recommendations for the design of the gas burner controller

The product standard for gas burners requires a "two failure criterion": no hazardous situation should be created by a single failure or two independent failures.

An example of this philosophy is shown in Figure B.2. If a failure occurs in the power supply check circuit only, it is a so-called sleeping failure which does not cause a hazardous situation. When then the power supply circuit fails and provides a too low voltage, the main controller does not operate properly and generates random signals to the outputs which can cause an opening of the gas valve. Two such independent failures should not lead to a hazardous situation.

De ce fait, la conception nécessite les trois couches illustrées à la figure B.3:

- la couche de commande;
- la couche de protection primaire, capable de détecter les défaillances dans la couche de commande et de fermer le robinet de gaz indépendamment, et
- la couche de protection secondaire, capable de détecter une (deuxième) défaillance dans la couche de protection primaire et de fermer la vanne de gaz indépendamment. (Dans les systèmes à microprocesseur, les couches de protection peuvent être combinées: le processeur de commande et le processeur de protection peuvent se protéger mutuellement, voir l'exemple de la figure B.2: contrôleur principal et chien de garde, qui est un deuxième microprocesseur).

Cette explication montre clairement qu'il convient d'éviter les erreurs de cause commune dues aux phénomènes électromagnétiques. Il est important que le circuit de commande, le circuit de protection primaire et le circuit de protection secondaire ne souffrent pas de défaillances simultanées. De ce fait, la conception nécessite des circuits construits avec des technologies différentes et des niveaux d'immunité différents.

En outre, il faut savoir que si les essais ont démontré une susceptibilité critique, les mesures de correction seront considérées avec soin. Un condensateur supplémentaire destiné à supprimer une tension transitoire qui entraînait l'ouverture intempestive de la vanne de gaz peut devenir défectueux et créer de ce fait une défaillance dormante.

Il faut enfin savoir que l'immunité électromagnétique d'un contrôleur pour brûleur à gaz peut évoluer lorsque ce module est intégré à un appareil ou à une installation à gaz. L'implantation du câblage ainsi que les propriétés du boîtier peuvent avoir une influence importante. Un essai d'immunité de l'application est nécessaire.

B.1.8 Conclusions concernant le plan d'essai de sécurité

A la suite de l'analyse ci-dessus, le plan d'essai de sécurité peut être élaboré. Il contiendra les informations suivantes:

- a) les perturbations électromagnétiques à prendre en compte
 - ainsi qu'éventuellement les perturbations qui ne sont pas spécifiées dans la norme de produits correspondante du strict point de vue de l'immunité fonctionnelle – dans notre exemple d'un contrôleur pour brûleur à gaz: harmoniques et transitoires oscillatoires;
- b) les niveaux d'essais de sécurité
 - soit de la norme de produits correspondante, si celle-ci prescrit des niveaux d'essais spécifiques pour la sécurité;
 - soit les niveaux d'essais fonctionnels renforcés par une marge de sécurité appropriée;
 - soit encore les exigences nationales spécifiques;
- c) les événements de sécurité indésirables
 - dont la non-occurrence sera contrôlée.

Dans le présent exemple d'un contrôleur pour brûleur à gaz, les niveaux d'essai de sécurité requis sont spécifiés dans le tableau B.1.

Normalement, le montage et les procédures d'essai spécifiés dans les normes fondamentales CEI 61000-4 seront appliqués mais des procédures plus sévères peuvent être prises en compte. Il est recommandé de ne pas soumettre à essai le contrôleur seul mais l'ensemble du système y compris le brûleur et le câblage entre le brûleur et le contrôleur qui est susceptible d'être influencé par le rayonnement à haute fréquence.

This implies that the design requires the three layers as shown in Figure B.3:

- the control layer,
- the primary safeguard layer, being able to detect failures in the control layer and to shut down the gas valve independently,
- the secondary safeguard layer, being able to detect a (second) failure in the primary safeguard layer and to shut down the gas valve independently. (In microprocessor systems the safeguard layers may be combined: the control processor and the safeguard processor can safeguard each other; see the example of Figure B.2: main controller and watchdog, which is a second microprocessor.)

This explanation makes it clear that common cause errors due to electromagnetic phenomena have to be avoided. The control circuit, the primary safeguard circuit and the secondary safeguard circuit should not suffer from simultaneous failures. Therefore the design requires circuits built with different technologies and different immunity levels.

Furthermore, it is important to realise that if testing has demonstrated critical susceptibility, mitigation measures should be considered carefully. One additional capacitor to suppress a transient voltage which caused an unwanted opening of the gas valve can become defective and thus creating a sleeping failure.

Finally, it should be realised that the electromagnetic immunity of a burner control unit can change when this module is built into a gas appliance or installation. The layout of the wiring as well as the properties of the enclosure can have a large influence. An immunity test of the application is necessary.

B.1.8 Conclusions with regard to the test plan for safety

Following the above analysis, the test plan for safety can be set up. It has to include the following information:

- a) the electromagnetic disturbances to consider
 - possibly also such disturbances which are not specified in the relevant product standard just with regard to functional immunity – in our example of a gas burner controller: harmonics and oscillatory transients;
- b) the test levels for safety.
 - either from the relevant product standard if the latter prescribes specific test levels for safety,
 - or the functional test levels enhanced by an appropriate security margin,
 - or possibly specific national requirements;
- c) the unwanted safety events
 - the non-occurrence of which has to be checked.

In the present example of a gas burner controller the required safety test levels are specified for example in Table B.1.

Normally the test set-up and procedures specified in the basic standards of the IEC 61000-4 series should be applied, but more severe procedures may be considered. It is recommended not to test the controller alone but the whole system, including the burner and the wiring between burner and controller, which may be influenced by high frequency radiation.

B.2 Exemple B.2: contrôle-commande d'un poste à haute tension

L'analyse par arbre de panne (AAP) est également appliquée pour l'analyse de sécurité des gros systèmes, comme par exemple, dans le domaine électrique, les matériels de contrôle-commande des centrales électriques ou des postes à haute tension. Ces systèmes sont constitués par un grand nombre de dispositifs individuels, et une AAP complète donne lieu à un travail long et parfois compliqué. Le but du présent exemple n'est pas, dans le contexte de la présente spécification technique, même s'il est limité à la CEM, d'effectuer une analyse de sécurité complète. La présente annexe se borne à indiquer le chemin qui peut être suivi pour les gros systèmes. Elle traitera du système de contrôle-commande d'un poste HT/MT et d'un exemple d'équipement de protection, à savoir la protection contre les courts-circuits sur une ligne HT.

B.2.1 But et fonctions attendues du matériel

Un schéma d'un poste HT/MT est donné à la figure B.5.

Le matériel de contrôle-commande a de nombreuses fonctions à remplir, qui peuvent être résumées et regroupées comme suit:

- protection des lignes et des transformateurs (courts circuits, surchauffe, caractéristiques des huiles, etc.);
- commandes de fermeture/ouverture des disjoncteurs (opérations automatiques ou manuelles);
- commandes de fermeture/ouverture des interrupteurs d'isolement (opérations automatiques ou manuelles);
- verrouillage;
- traitement EN/HORS-ligne;
- mesure et comptage;
- affichage;
- alarmes;
- télécommunication (avec le centre de commande du réseau et autres postes).

B.2.2 Structure matérielle des appareils

La figure B.5 montre la structure générale d'un système de contrôle-commande de poste. Elle présente une structure à trois couches:

- dans les domaines de la haute et de la moyenne tension, les «appareils installés sur le terrain»: transformateurs de tension ou de courant, filtres de courant porteur, capteurs, etc.;
- pour chaque départ: ligne, transformateur, bus barres, une «unité de contrôle terrain». Il s'agit d'une armoire ou de tout autre type d'enceinte dans laquelle sont montés les appareils installés sur le terrain: relais de protection, commande et mesure locale, communication avec l'unité centrale, etc.;
- dans le bâtiment de contrôle: l'unité centrale qui permet la télécommande des appareils installés sur le terrain, des fonctions centrales de traitement et de la télécommunication avec un réseau de distribution central ou autres postes.

La figure B.6 montre cette structure à trois couches pour la fonction de protection contre les courts-circuits.

B.2 Example B.2: Control-command of a high voltage substation

Fault tree analysis (FTA) is also applied for the safety analysis of large systems, as for example, in the electrical field, control-command equipment of generating stations or high voltage substations. Such systems are constituted by a large number of single devices and a comprehensive FTA leads to a long, sometimes complicated, work. It is not the aim of this example in the context of this document, even if limited to EMC, to carry out a complete safety analysis. This annex is limited to showing the route which can be followed for large systems. It will deal with the control-command system of an HV/MV substation and of one example of protection equipment: protection against short-circuits on an HV line.

B.2.1 Aim and intended functions of the equipment

A schematic of an HV/MV substation is depicted in figure B.5.

The control command equipment has numerous functions to fulfil, which can be summarised and grouped as follows:

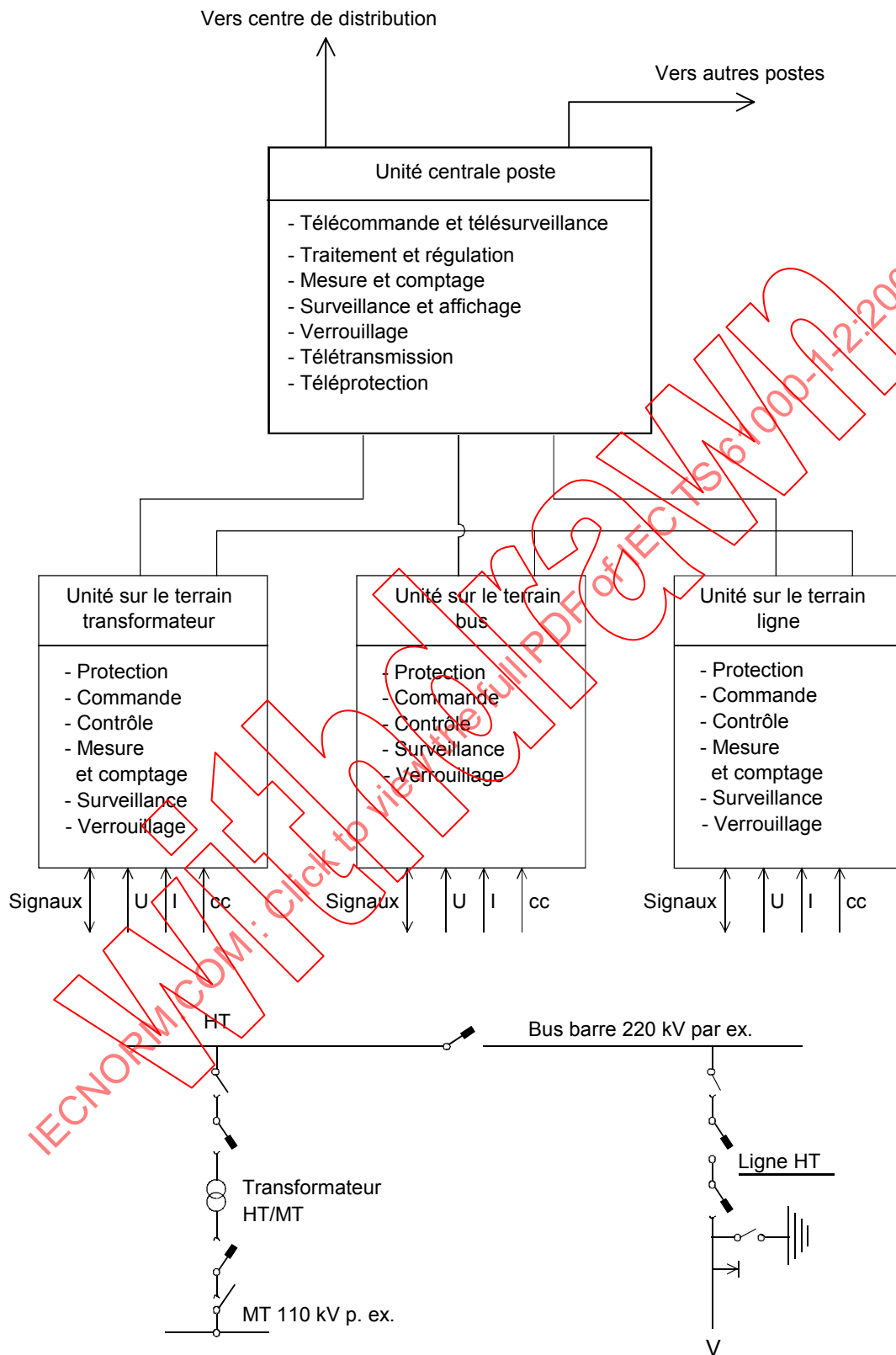
- protection of the lines and transformers (short circuits, overheating, oil characteristics, etc.),
- ON/OFF commands of the circuit breakers (automatic or manual operations),
- ON/OFF commands of the isolating switches (automatic or manual operations),
- interlocking,
- ON/OFF-line processing,
- measurement and metering,
- display,
- alarms,
- telecommunication (with the network control centre and other substations).

B.2.2 Hardware structure of the equipment

Figure B.5 shows the general structure of a control-command system for a substation. It has a three-layer structure:

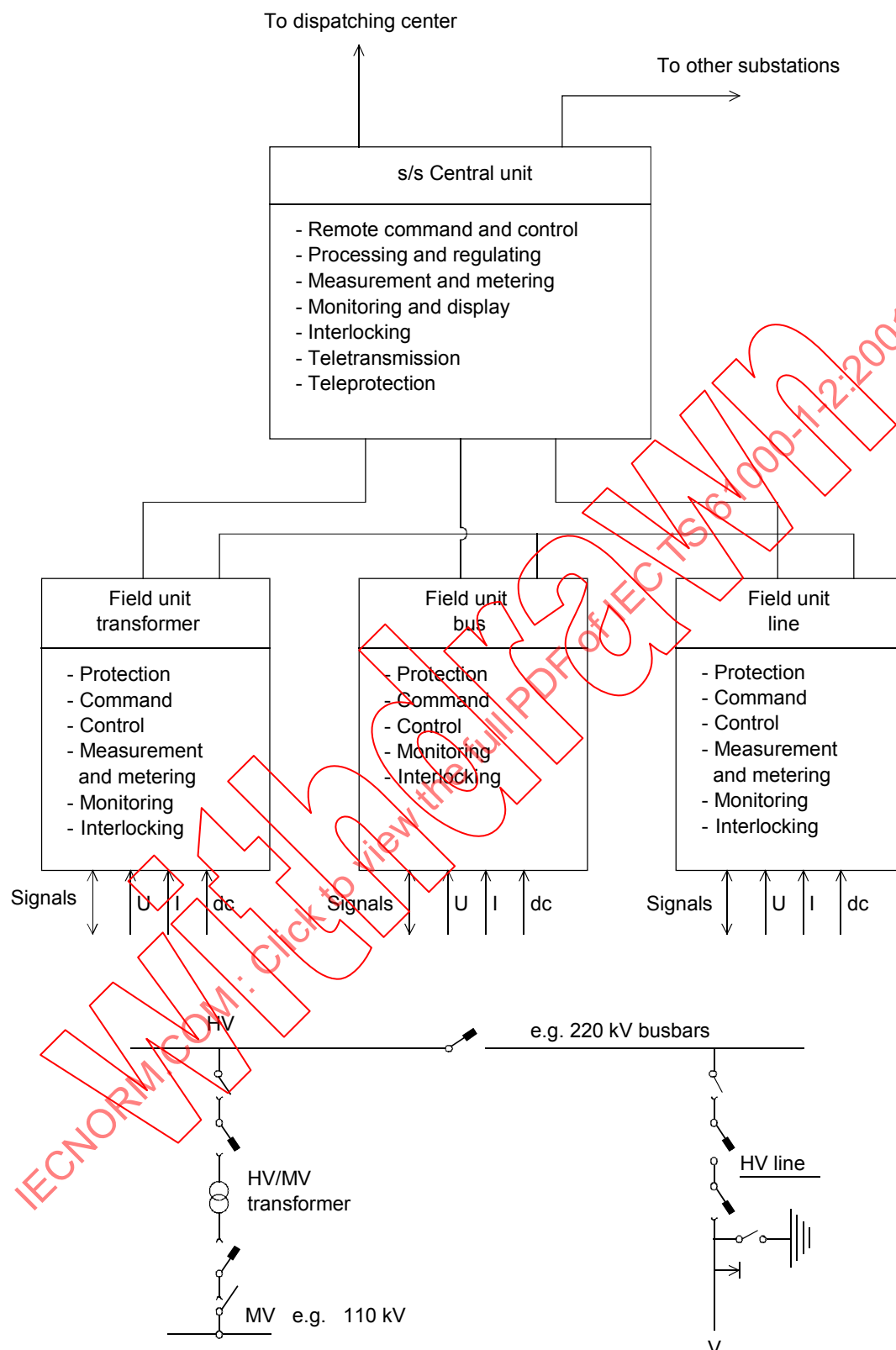
- in the high or medium voltage areas, the "field devices": voltage or current transformers, power line carrier filters, sensors, ...
- for each feeder: line, transformer, bus bars a "field control unit". It is a cabinet or another kind of enclosure in which are mounted the field devices: protection relays, local command and measurement, communication with the central unit, ...
- in the control building: the central unit, which allows the remote control of the field units, central processing functions and telecommunication with a central network dispatching or with other substations.

Figure B.6 shows this three-layer structure for the short-circuit protection function.



IEC 479/01

Figure B.5 – Structure générale du contrôle-commande d'un poste haute tension



IEC 479/01

Figure B.5 – General structure of the control command of a high voltage substation

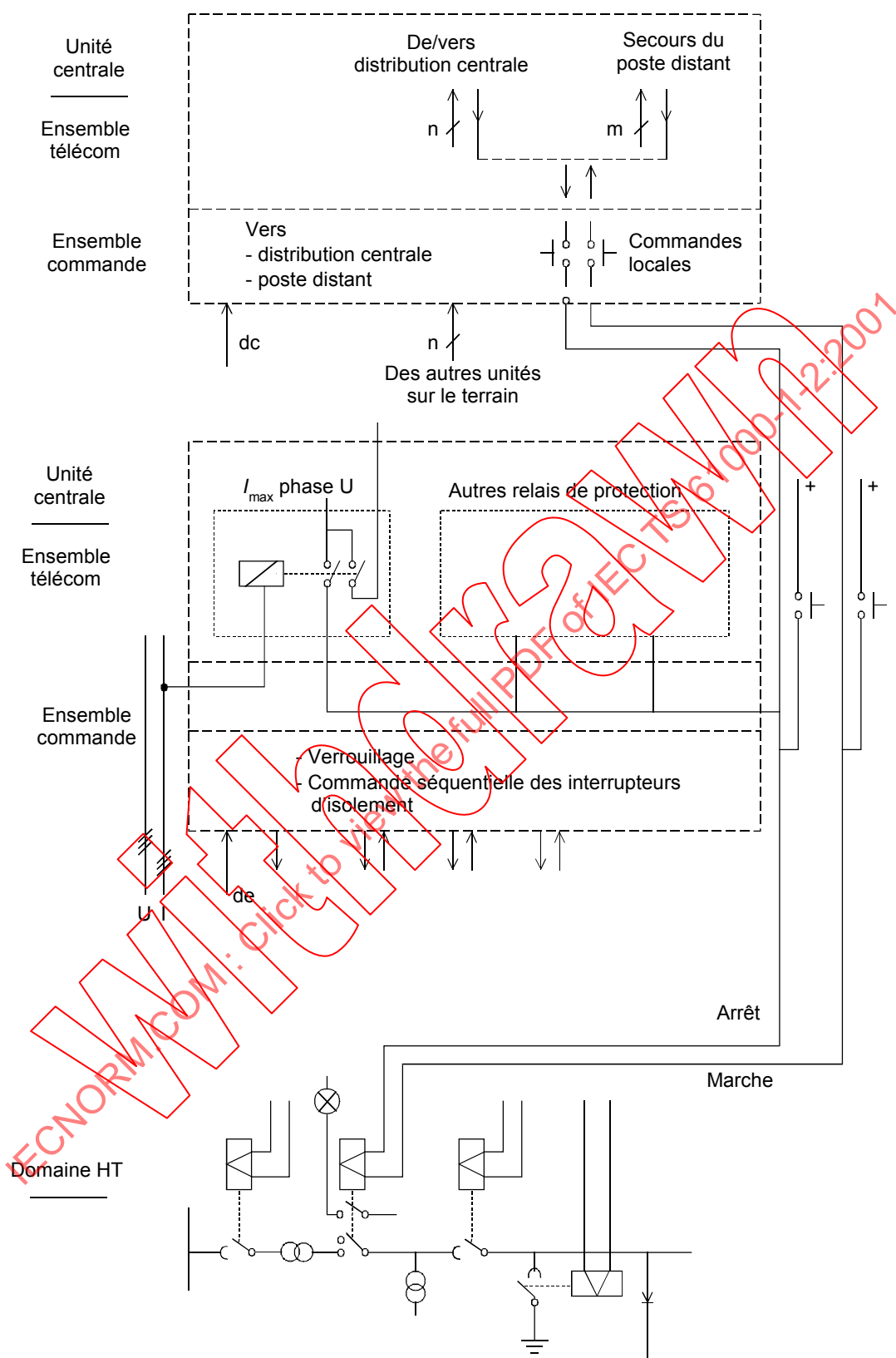
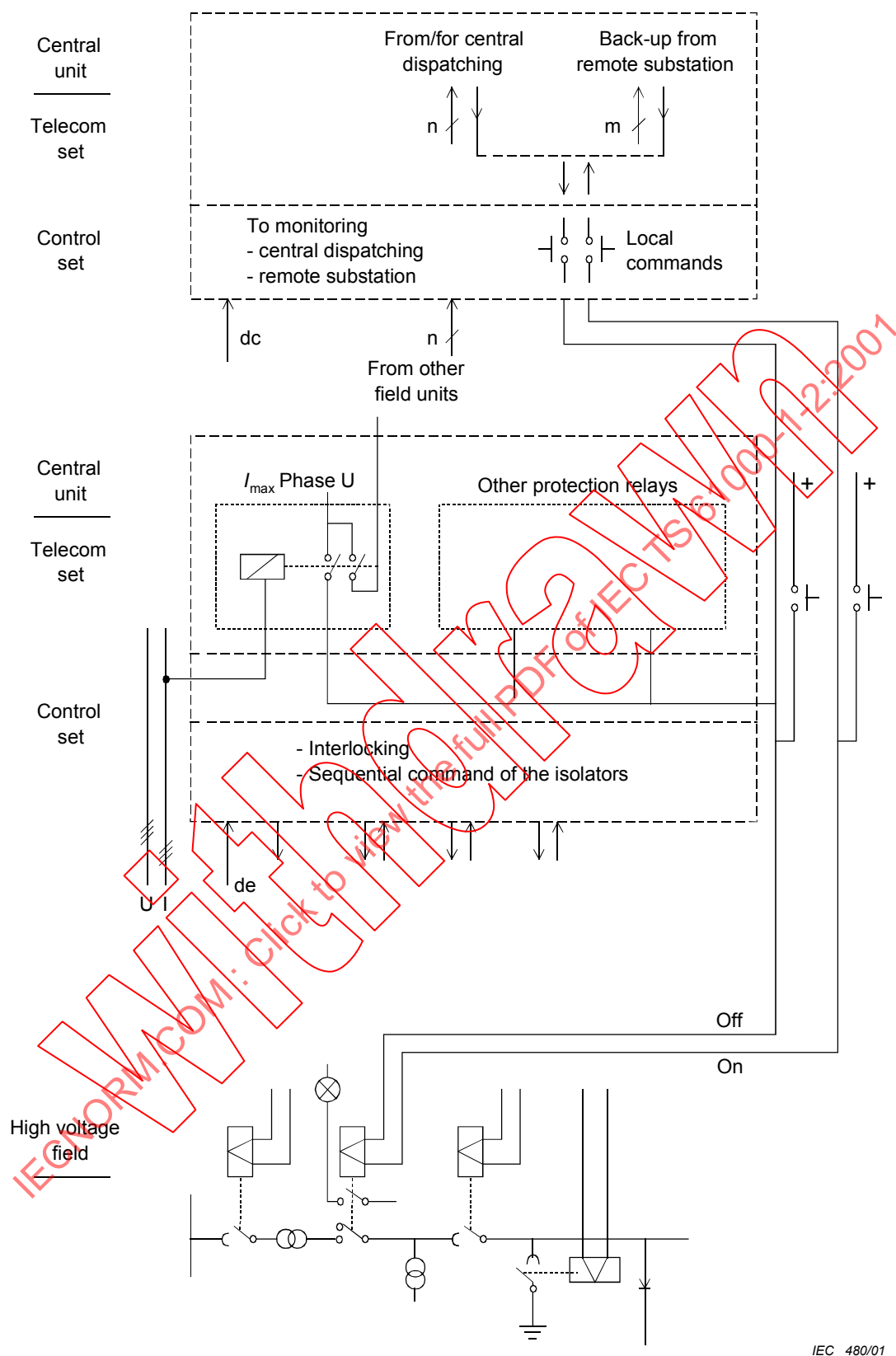


Figure B.6 – Schéma de la protection contre les courts-circuits



IEC 480/01

Figure B.6 – Schematic of the short-circuit protection

Dans les postes classiques – anciens, une grande partie du matériel est constituée d'éléments électriques/mécaniques: relais, instrumentation, etc. Une autre partie est électronique. Le câblage est constitué de câbles cuivre blindés.

Dans les postes modernes, le matériel est presque entièrement électronique, seuls les relais intermédiaires d'entrée/sortie étant mécaniques. Le câblage est constitué de liaisons à fibre optique moins sensibles.

Pour ce qui concerne les fonctions de protection considérées dans le présent exemple, les dispositifs de protection placés dans les unités sur le terrain nécessitent un système de secours: il peut s'agir d'un deuxième jeu de dispositifs de protection ou d'un secours dans l'unité centrale. Dans le présent exemple, une troisième solution est présentée pour la protection des lignes: le secours est assuré par les relais de protection à l'autre extrémité de la ligne dans l'autre poste et la commande de déconnexion est transmise via la liaison de télécommunication.

B.2.3 Configuration logicielle

Les défaillances logicielles se manifestent, du point de vue de la sécurité, par le mauvais fonctionnement des dispositifs matériels et il n'est pas nécessaire de les aborder en détail ici.

B.2.4 Environnement électronique et niveaux d'essais fonctionnels

En principe, tous les phénomènes électromagnétiques listés au tableau 1, ou la plupart d'entre eux, seront analysés en termes d'implications pour la sécurité. Les niveaux d'essais fonctionnels pour chaque matériel sont donnés dans les normes de produits correspondantes: automation et appareils de commande des postes [CEI 60870], relais de protection [série CEI 60255-22 par exemple]. Toutefois, elles ne recommandent pas encore de niveaux d'essai de sécurité et ceux-ci seront spécifiés par l'organisme chargé du projet.

Les experts en CEM pour postes électriques font une distinction entre trois catégories de perturbations:

- les perturbations permanentes;
- les perturbations de courte durée à occurrence élevée;
- les perturbations de courte durée à faible occurrence.

Les perturbations permanentes et, dans une large mesure, les perturbations de courte durée à occurrence élevée sont faciles à évaluer et il est facile d'assurer des mesures de protection. Toutefois, les perturbations à faible occurrence peuvent être difficiles à évaluer, en particulier leur valeur maximale, et peuvent être les plus dangereuses en termes d'intégrité de la sécurité.

Une vue d'ensemble des perturbations électromagnétiques se produisant dans un poste HT/MT est donnée pour information générale dans le tableau B.3.

In classical – older – substations, a great part of the equipment consists of electrical/mechanical items: relays, instrumentation, etc. Another part is electronic. The wiring is made of shielded copper cables.

In modern substations the equipment is almost fully electronic, with only the in-/output intermediate relays being mechanical. The wiring is made of less sensitive fibre optic links.

With regard to the protection functions considered in this example, the protection devices placed in the field units need a back-up: this can be a second set of protection devices or a back-up in the central unit. In this present example for the protection of lines a third solution is presented: the back-up is provided by the protection relays at the other end of the line in the other substation and the disconnecting order is transmitted via the telecommunication link.

B.2.3 Software configuration

Software failures are reflected with regard to safety by the wrong operations of the hardware devices and need not to be considered in detail here.

B.2.4 Electronic environment and functional test levels

In principle all or most of the electromagnetic phenomena listed in Table 1 should be analysed with regard to safety implications. The functional tests levels for each piece of equipment are given in the relevant product standards: automation and control apparatus for substations [IEC 60870], protection relays [e.g. the IEC 60255-22 series]. However they do not yet recommend test levels for safety, which are to be specified by the responsible project body.

Experts on EMC for electrical substations make a differentiation between three categories of disturbances:

- continuous disturbances;
- short duration disturbances with high occurrence;
- short duration disturbances with low occurrence.

Continuous disturbances and to a large extent short duration disturbances with high occurrence are easy to assess and it is easy to provide protection measures. However disturbances with low occurrence may be difficult to assess, particularly their maximum magnitude, and may be the more dangerous with regard to safety integrity.

An overview on the electromagnetic disturbances occurring in an HV/MV substation is given for general information in Table B.3.

Table B.3 – Vue d'ensemble des perturbations électromagnétiques dans les postes HT/MT (voir la CEI 61000-6-5)

Perturbations permanentes	Perturbations de courte durée à occurrence élevée	Perturbations de courte durée à faible occurrence
Variations et fluctuations de la tension d'alimentation – alimentations à courant alternatif et continu	Creux de tension d'alimentation ($t \leq 0,02s$) – alimentations à courant alternatif et continu	Creux de tension d'alimentation ($t > 0,20 s$) – alimentations à courant alternatif et continu
Harmoniques, inter-harmoniques,	Transitoires rapides en sauts.	Coupures de la tension d'alimentation ($\Delta U = 100 \%$) – alimentations à courant alternatif et continu
Perturbations conduites dans la plage courant continu à 150 kHz	Ondes de surtensions oscillatoires transitoires amorties de 0,01 MHz à 1 MHz	Surtensions transitoires
Champ magnétique à la fréquence du réseau	Décharges électrostatiques	Champs magnétiques de surtensions transitoires.
Champs radiofréquence rayonnés dans la plage de 0,15 MHz à 3 MHz ^a		
Champs radiofréquence rayonnés émis par les radiotéléphones portables		
^a Le tableau ne prend en compte qu'un seul phénomène sur l'ensemble de la plage de fréquence, mais deux méthodes différentes sont appliquées pour les essais: un essai avec une tension conduite entre 0,15 MHz et (26) 80 MHz, un champ rayonné entre (26) 80 MHz et 3 000 MHz.		

Table B.3 – Overview on EM disturbances in HV/MV substations (see IEC 61000-6-5)

Continuous disturbances	Short time disturbances with high occurrence	Short time disturbances with low occurrence
Supply voltage variations and fluctuations – a.c. and d.c. supplies	Supply voltage dips ($t \leq 0,02$ s) – a.c. and d.c. supplies	Supply voltage dips ($t > 0,20$ s) – a.c. and d.c. supplies
Harmonics, interharmonics	Fast transient bursts	Supply voltage interruptions ($\Delta U = 100$ %) – a.c. and d.c. supplies
Conducted disturbances in the range d.c. to 150 kHz	Transient damped oscillatory overvoltage waves 0,01 MHz to 1 MHz	Transient voltage surges
Power frequency magnetic field	Electrostatic discharges	Transient surge magnetic fields.
Radiated radio frequency EM fields in the range 0,15 to 3 MHz ^a		
Radiated radio frequency EM fields from portable radio telephones		

^a The table considers only one phenomenon over the whole frequency range, but two different methods are applied for testing purposes: a test with a conducted voltage. between 0,15 MHz to (26) 80 MHz, a radiated field between (26) 80 MHz to 3 000 MHz.

B.2.5 Objet de l'analyse des dangers et des risques

L'objet de l'analyse des dangers et des risques consiste, pour les risques de sécurité indésirables (événements de tête), à déterminer, aux fins de prendre les mesures de correction appropriées:

- quels phénomènes électromagnétiques peuvent provoquer ces risques (événements de base), et
- à quels endroits du système.

Il est important, du point de vue de l'intégrité de la sécurité, que les événements suivants – événements de tête – ne se produisent pas dans un poste HT/MT:

- défaut d'ouverture de disjoncteurs par commande manuelle (dont la cause peut être un défaut du mécanisme d'ouverture ou du circuit de commande);
- défaut d'ouverture de disjoncteurs par fonctionnement des relais de protection (cause supplémentaire: défaut des relais de protection et des circuits associés).

Les relais de protection peuvent être:

- pour une ligne: relais de protection contre les courts-circuits ($I_{\max}$), éventuellement le relais de protection contre les surcharges (température $> \vartheta^{\circ}$);
- pour un transformateur: relais de protection contre les courts-circuits ($I_{\max}$), relais de protection contre les surcharges (température $> \vartheta^{\circ}$), caractéristiques des huiles;
- défaut d'ouverture des interrupteurs d'isolement et défaut de fermeture des dispositifs de mise à la terre (cause supplémentaire: mauvais fonctionnement des circuits de verrouillage).

Le présent rapport rendu traitera, à titre d'exemple, de la déconnexion d'une ligne HT en cas de court-circuit sur une ligne HT.

B.2.6 Analyse par arbre de panne (AAP)

B.2.6.1 Construction de l'arbre de panne

Un arbre de panne peut être élaboré conformément à la CEI 61025 pour les systèmes compliqués, mais certaines caractéristiques particulières peuvent être abordées comme dans le présent exemple.

- a) Le système représenté à la figure B.6 comporte une structure à trois couches et, en principe, il convient d'étudier chaque couche:
- AAP au niveau des appareils individuels (comme dans l'exemple B.1);
 - AAP au niveau des groupes d'appareils dans une enceinte commune (comme les armoires des unités sur le terrain ou de la salle de conduite centralisée);
 - AAP au niveau d'un système complet de dispositifs répartis sur une zone étendue.

Pour ce qui concerne l'AAP d'un groupe d'appareils implantés dans une enceinte commune, on peut observer que cette enceinte peut avoir un effet d'amortissement sur le niveau des perturbations externes, par l'effet de blindages ou l'utilisation de filtres. D'autre part, des tensions perturbatrices peuvent être induites dans le câblage interne. Toutefois, ces phénomènes n'entraînent pas de nouveaux types de perturbations fonctionnelles et peuvent être pris en compte par le biais d'une conception appropriée et de niveaux d'essai pour les appareils individuels.

B.2.5 Purpose of the hazard and risk analysis

The purpose of the hazard and risk analysis is to detect, for undesirable safety risks (top events), in order to take appropriate mitigation measures:

- which electromagnetic phenomena can cause these risks (basic events);
- at which places in the system they occur.

The following events – top events – should not occur in an HV/MV station from a safety integrity perspective:

- non-opening of circuit-breakers by manual command
(can be caused by a defect of the opening mechanism or of the control circuit);
- non-opening of circuit breakers by operation of protection relays
(additional cause: defect in the protection relays and associated circuits).
The protection relays can be
 - for a line: short circuit relays ($I_{\max}$), possibly overload relay (temperature $> \vartheta^{\circ}$);
 - for a transformer: short circuit relays ($I_{\max}$), overload relays (temperature $> \vartheta^{\circ}$), oil characteristics;
- non-opening of the insulating switches and non-closing of the grounding devices
(additional cause: wrong operation of the interlocking circuits).

For the purpose of this report, the example dealt with here will concern the disconnecting of an HV-line in the case of a short circuit on an HV-line.

B.2.6 Fault tree analyses (FTA)

B.2.6.1 Construction of the fault tree

A fault tree can be constructed according to IEC 61025 for complicated systems, but certain specific features may be considered as in the present example.

- a) The system as represented in Fig B.6 has a three-layer structure, and in principle each layer should be examined:
- FTA at the level of the individual apparatuses (as in example B.1);
 - FTA at the level of groups of apparatuses in a common enclosure (such as the cabinets in the field units or in the central control room);
 - FTA at the level of a complete system of devices spread over a large area.

With regard to the FTA of a group of apparatuses in a common enclosure, it can be observed that this enclosure may have a damping influence on the level of external disturbances by shielding effects or the use of filters. On the other hand, disturbance voltages may be induced in the internal wiring. However, these phenomena do not cause new kinds of functional disturbances and can be taken into account by appropriate design and testing levels for the individual apparatuses.

- b) Le présent exemple traite de la déconnexion d'une ligne HT par le fonctionnement d'un relais de protection contre les courts-circuits sur $I_{\max}$. Le schéma matériel de la figure B.7 montre que le circuit de sortie du relais est étroitement lié au circuit de commande manuelle. Les deux circuits seront représentés sur le schéma de l'AAP.
- c) Comme expliqué en B.6, le secours pour les relais à $I_{\max}$ est assuré par les relais à $I_{\max}$ à l'autre extrémité de la ligne via la liaison de télécommunication.

L'arbre de panne pour déconnexion de la ligne en cas de court-circuit est représenté à la figure B.7. Comme d'habitude,

- l'arbre de panne ne prend en compte que les influences électromagnétiques;
- les autres événements ne sont pas pris en compte;
- la tension d'alimentation est considérée comme une «cause commune» et traitée comme un sous-système séparé dans les AAP des appareils individuels.

B.2.6.2 Evaluation de l'arbre de panne du point de vue de la sécurité

Comme indiqué plus haut, on suppose que chaque appareil individuel a déjà été analysé du point de vue de la sécurité. Il convient maintenant de déterminer quel risque est ajouté par le regroupement de ces appareils en un système. Comme indiqué plus haut également (B.1.6.2) toutes les influences électromagnétiques n'ont pas nécessairement un impact critique pour la sécurité et il appartient à l'ingénieur CEM d'évaluer, sur la base de la conception du matériel et de son expérience celles qui seront prises en compte.

L'événement de tête concerné par le présent exemple est le défaut de fonctionnement de la protection d'une ligne HT en cas de court-circuit. On entend par défaut de fonctionnement la non-ouverture des disjoncteurs aux deux extrémités de la ligne. L'évaluation de sécurité de cet événement de tête est résumée au tableau B.4:

a) trois éléments système ont été ajoutés pour compléter le système:

- le montage des appareils individuels dans une ou plusieurs enceintes communes: armoires, bordsiers;
ces enceintes assurent un blindage plus ou moins efficace contre les champs externes et, si les circuits d'entrée/sortie sont munis des filtres appropriés, un affaiblissement plus ou moins important des perturbations conduites sera réalisé;
- le câblage entre les appareils individuels; le câblage interne à l'intérieur des enceintes communes ou le câblage externe entre ces matériels;
- le matériel de télécommunication entre le poste et le poste central de distribution ou les autres postes. Ce matériel peut toutefois être considéré comme un appareil individuel indépendant, analysé séparément pour prendre en compte la communication dans les deux sens:

poste considéré	→	autres postes
autres postes	→	poste considéré

- b) Les phénomènes électromagnétiques à prendre en compte dans le contexte d'un système sont donc essentiellement les champs électromagnétiques sur l'ensemble de la plage de fréquences:
 - champs permanents: champs à basse fréquence et de faible puissance issus des lignes de transport d'énergie, matériels ou transformateurs HT (champs magnétiques à la fréquence du réseau), ou champs haute fréquence, comme ceux rayonnés par les téléphones mobiles,
 - champs haute fréquence transitoires tels que ceux provoqués par les effets de la foudre ou par les opérations de commutation.

- b) The present example deals with the disconnecting of an HV-line by the operation of an $I_{\max}$ short circuit protection relay. From the hardware diagram of Figure B.7 it can be seen that the relay output circuit is closely connected with the manual operation circuit. Both should be represented in the FTA diagram.
- c) As explained in B.6 the back-up for the $I_{\max}$ relays is provided by the $I_{\max}$ relays at the other end of the line via the telecommunication link.

The fault tree for short circuit disconnection of the line is represented in Figure B.7. As usual:

- the fault tree considers only EM influences;
- other events are not considered;
- supply voltage is considered as a "common cause" and treated as a separate sub-system in the FTAs of the individual apparatus.

B.2.6.2 Evaluation of the fault tree with regard to safety

As stated before it is assumed that each single apparatus has already been analysed with regard to safety. The task is now to determine which risk is added by grouping these apparatus into a system. Also as already stated (B.1.6.2) not all EM influences can have a critical safety impact and the EMC engineer has to evaluate, based on the design of the equipment and on his experience, which ones should be considered.

The present example refers, as top event, to the non-operation of the short-circuit protection of an HV line. Non-operation means not opening of the circuit breakers at both ends of the line. The safety evaluation of this top event is summarised in table B.4.

- a) Three system items have been added to complete the system:

- the mounting of the single apparatus in (a) common enclosure(s): cabinets, cases; these enclosures provide a more or less strong shielding of the external fields and, if the input/output circuits are fitted with appropriate filters, a more or less strong attenuation of the conducted disturbances will be achieved;
- the wiring between the single apparatuses; internal wiring inside the common enclosures or external wiring between these units;
- the telecommunication equipment between the substation and the central dispatching or the other substations. This equipment, however, may be considered as one independent single apparatus, analysed separately to take care of the communication in both directions.

considered substation → other stations

other stations → considered substation

- b) The EM phenomena to consider in the context of a system are therefore mainly the EM fields in the whole frequency range:
 - continuous fields: low-power-frequency fields from the power lines, HV equipment or transformers (e.g. magnet fields at power frequency), or high frequency fields (e.g from mobile phones);
 - transient high frequency fields such as the ones caused by lighting effects or by switching operations.

Les décharges électrostatiques peuvent éventuellement être prises en compte du point de vue de leur effet dans les enceintes communes. Cet effet n'est pas susceptible d'être critique si les appareils individuels sont déjà correctement protégés contre cet effet.

Les phénomènes électromagnétiques conduits devraient avoir déjà été pris en compte dans le cadre de l'analyse des appareils individuels.

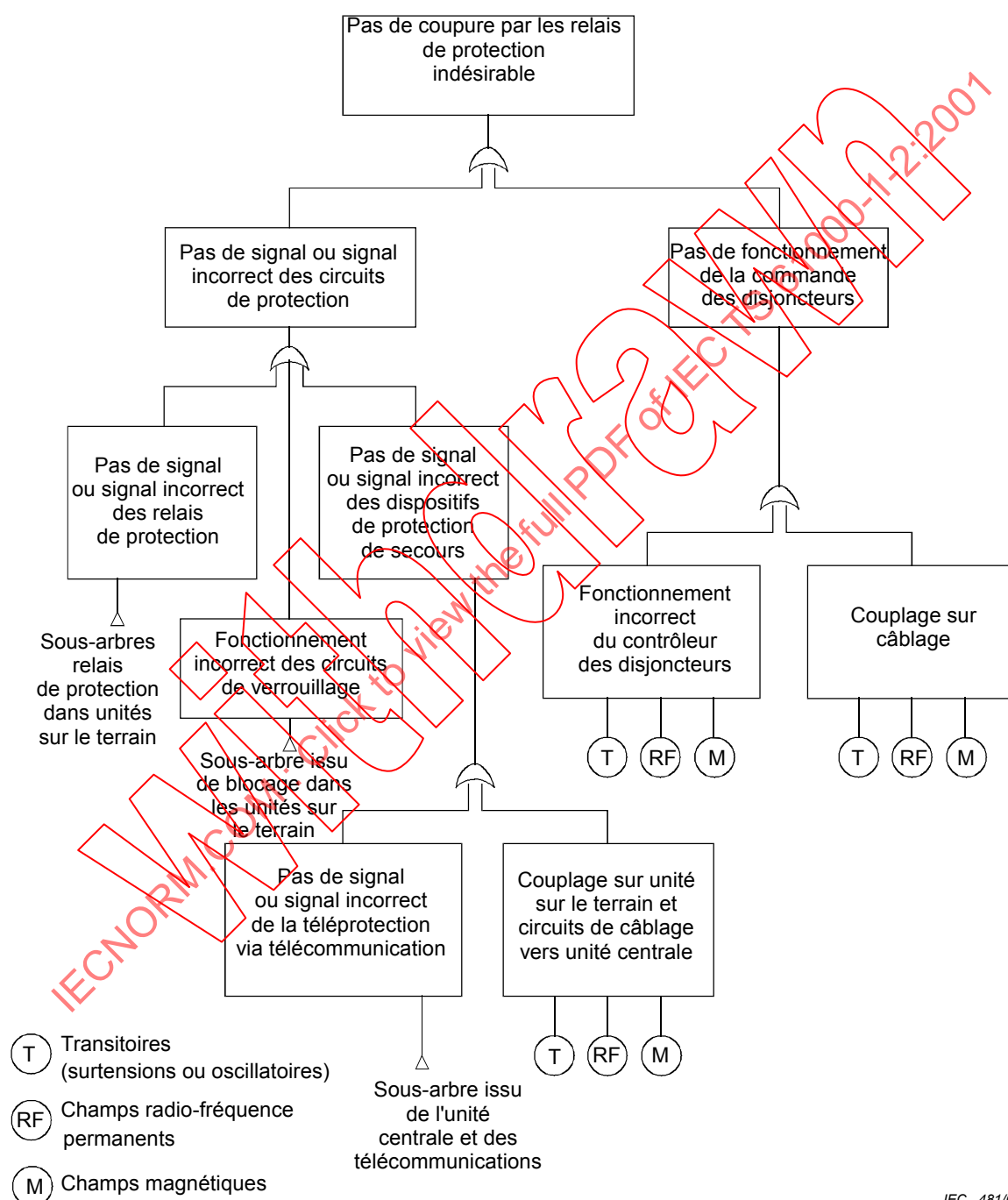
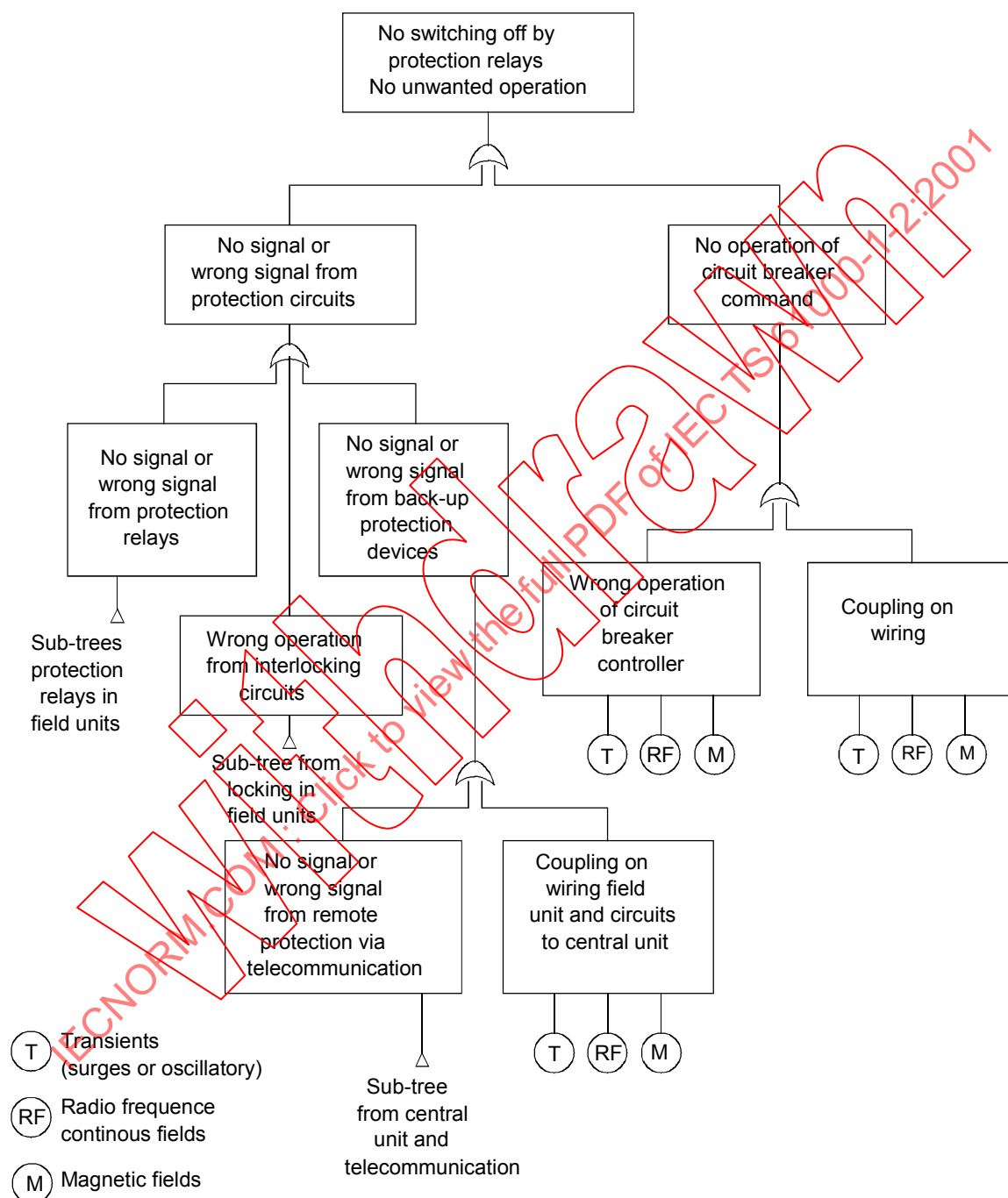


Figure B.7 – AAP pour la protection contre les courts-circuits

Possibly electrostatic discharges should also be considered with regard to their effect in the common enclosures. This effect is not likely to be critical if the single apparatuses are already correctly protected against this effect.

Conducted EM phenomena should have been already taken into consideration in the analysis of the single apparatuses.



IEC 481/01

Figure B.7 – FTA for short-circuit protection

Tableau B.4 – Evaluation de l'influence des perturbations électromagnétiques à l'extérieur des appareils individuels sur le fonctionnement sans danger de la protection contre les courts-circuits d'une ligne HT

Partie du système	Phénomènes EM					
	BF/HF conduits	BF rayonnés	HF rayonnés			DES
		Champ magnétique	Permanent	Téléphone mobile	Transitoires	Enceinte
Câblage interne dans enceinte	Non pertinent	?	?	X	?	X
Câblage externe		X	X	X	X	–
NOTE 1 On suppose que chacun des composants du système a été analysé séparément et assure un niveau de sécurité approprié.						
NOTE 2 X indique une influence critique possible; ? indique une influence critique improbable; – indique l'absence d'influence.						

B.2.7 Recommandations pour l'installation du système de contrôle/commande d'un poste

Comme dans les chapitres précédents, on suppose que les appareils individuels sont conçus et soumis à essais pour un certain niveau d'intégrité de sécurité. La même hypothèse vaut également pour les armoires ou boîtiers.

Concernant l'installation du système complet, les indications suivantes sont importantes:

- Il est nécessaire que tous les câblages soient protégés soigneusement, c'est-à-dire:
 - dans le cas du câble cuivre, par l'utilisation de câbles coaxiaux ou blindés,
 - ou, mieux et plus moderne, en particulier pour les connexions longues, par l'utilisation de liaisons à fibre optique.
- Il est nécessaire que les armoires ou boîtiers assurent un facteur de protection élevé contre les champs à la fréquence du réseau ou à haute fréquence.
- En ce qui concerne les DES, les caractéristiques de protection normales sont probablement suffisantes.

Un point important à prendre en compte est que les relais de protection primaire contre les courts-circuits nécessitent un dispositif de secours. En principe, le dispositif de secours utilisera une autre technique que le dispositif primaire. Dans le présent exemple, un autre principe est appliqué: on utilise, via la liaison de télécommunication, le relais de protection contre les courts-circuits à l'autre extrémité de la ligne HT. Ceci exige une fiabilité élevée de la liaison de télécommunication, et ce dans les deux sens.

B.2.8 Conclusions concernant le plan d'essai de sécurité

En principe, le plan d'essai de sécurité d'un gros système tel que le système de contrôle/commande présenté dans le présent exemple exige une procédure en trois étapes:

- La première étape consiste à soumettre à essais les appareils individuels selon leurs normes de produits
 - avec les niveaux d'essai de sécurité si de tels niveaux sont spécifiés,
 - avec un niveau d'essai fonctionnel renforcé si aucun niveau d'essai de sécurité n'est prescrit.

Table B.4 – Evaluation of the influence of EM disturbances outside the single apparatuses on the safe operation of the short circuit protection of an HV line.

Part of the system	EM Phenomena					
	LF/HF conducted	LF radiated	HF radiated			ESD
		Magnetic field	Continuous	Mobile phone	Transients	Enclosure
Internal wiring in enclosure	Not relevant	?	?	X	?	X
External wiring		X	X	X	X	–
NOTE 1 It is assumed that each system component has been analysed separately and provides an appropriate safety.						
NOTE 2 X indicates a possible critical influence; ? indicates an unlikely critical influence; – indicates no influence.						

B.2.7 Recommendations for the installation of the control/command system of a substation

As in the previous chapters, it is assumed that the single apparatuses are designed and tested for a certain safety integrity level. This is assumed also for the whole cabinets or cases.

Concerning installation of the complete system, the following indications are important:

- a) All wirings have to be carefully protected, i.e.:
 - in case of cu-wiring by the use of coaxial or shielded cables;
 - or (better and more modern), particularly for long connections, by the use of fibre optic links.
- b) Cabinets or cases have to provide a high shielding factor with regard to power frequency or high frequency fields.
- c) As for ESD, normal protection characteristics are probably sufficient.

An important point to consider is that the primary short circuit protection relays require a back-up. In principle the back-up should make use of another technique than the primary device. In the present example, another principle is applied: use is made via the telecommunication link of the short circuit protection relay at the other end of the HV line. This requires a high reliability of this telecommunication link, and this namely in both directions.

B.2.8 Conclusions with regard to the test plan for safety

In principle the test plan for safety of a large system like the control/command system presented in this example should require a three-step procedure.

- a) The first step is to test the single apparatuses according to their product standards
 - with the safety test levels if such levels are specified;
 - with an enhanced functional test level if no safety test level is prescribed.

- b) La deuxième étape consiste à soumettre à essais les matériels regroupant les appareils individuels: armoires ou boîtiers, toujours selon les exigences des normes de produits. Ce point est en général applicable.
- c) Un troisième étape consiste à soumettre à essai l'ensemble du système, mais ceci peut souvent être difficile ou même impossible si les matériels du système sont répartis sur une zone étendue, comme dans le cas d'un poste en plein air.

Dans ce dernier cas, la procédure d'essai se limite aux deux premières étapes et les travaux d'essai supplémentaires peuvent ne pas être très importants. La documentation de sécurité peut contenir des explications sur les mesures qui ont été prises concernant le câblage, le blindage et la mise à la terre de l'ensemble du système.

IECNORM.COM: Click to view the full PDF of IEC TS 61000-1-2:2001

Withdrawn

- b) The second step should be to test the units grouping the single apparatuses: cabinets or cases, also according to the product standard requirements. This should be generally applicable.
- c) A third step would be to test the whole system but often this may be difficult or even impossible if the system units are spread over a large area as in the case of an open-air substation.

In the latter case the test procedure is limited to the two first steps and the additional testing work may not be very important. In the safety documentation it can be explained which measures have been taken with regard to wiring, shielding and earthing of the whole system.

IECNORM.COM: Click to view the full PDF of IEC TS 61000-1-2:2001

Withdrawing

Annexe C (informative)

Considérations de conception et d'installation

C.1 Principes généraux

Tout matériel électrique/électronique est installé dans un environnement électromagnétique donné où les perturbations basse fréquence ou haute fréquence, conduites ou rayonnées ne dépassent pas, en principe, les valeurs normales spécifiées par les normes correspondantes (c'est-à-dire les séries CEI 61000-2 et CEI 61000-3 ou les normes du CISPR). Le matériel est conçu ou installé de telle manière qu'il soit conforme aux exigences fonctionnelles spécifiées (voir article 8). Toutefois, il peut se produire que les niveaux de perturbation dépassent ces valeurs normales et, pour éviter que le matériel ne puisse arriver à un état où il se comporte de manière dangereuse, des mesures de protection adéquates sont nécessaires.

Il faut également prendre soin, chaque fois que possible, que l'émission de perturbations par un matériel soit limitée à des valeurs qui n'entraînent pas de risques pour la sécurité d'autres matériels.

Il faut également savoir que les mesures d'installation sont souvent une manière efficace d'aboutir à l'immunité et à la sécurité requises.

L'objet de la présente annexe est de donner une vue d'ensemble informative des moyens de protection.

C.2 Moyens techniques pour la prévention de la pénétration et de la propagation des perturbations: réduction des risques

Les moyens techniques qui peuvent être utilisés et les aspects de conception qui ont été pris en compte sont les suivants:

- blindage,
- filtrage,
- protection contre les surtensions (protection contre les transitoires),
- câblage approprié,
- mise à la terre et liaisons équipotentiellles,
- conception des cartes à circuit imprimé pour obtenir une bonne immunité,
- circuits redondants (avec différentes technologies),
- utilisation de techniques numériques.

Plusieurs normes ou rapports techniques de la CEI (par exemple la série CEI 61000-5) apportent des informations détaillées sur la manière d'appliquer les moyens de protection, qui peuvent également faire l'objet de recommandations dans les normes de produits spécifiques.

Annex C (informative)

Design and installation considerations

C.1 General principles

Any electrical/electronic equipment is installed in a given electromagnetic environment in which low frequency or high frequency, conducted or radiated disturbances should not exceed the normal values specified by the relevant standards (e.g. the IEC 61000-2 and IEC 61000-3 series or CISPR standards). The equipment is designed or installed in such a way that it complies with the specified functional requirements (see clause 8). However it can happen that the disturbance levels exceed these normal values and in order that the equipment not come to a state where it behaves dangerously, adequate protection measures are necessary.

It is also important to take care that, when possible, the emission of disturbances by an equipment is limited to values that do not cause safety risks to other equipment.

It is equally important to recognise that installation measures are often an effective way to achieve the required immunity and safety.

The aim of the present annex is to give an informative overview of the protection means.

C.2 Technical means for the prevention of the penetration and propagation of perturbations: risk reduction

The technical means that can be used and the design aspects which have to be considered include:

- shielding,
- filtering,
- overvoltage protection (protection against transients),
- appropriate wiring,
- earthing and bonding,
- immunity design of printed circuit boards (PCBs),
- redundant circuits (with different technologies),
- use of digital techniques.

Several IEC standards or technical reports (e.g. the IEC 61000-5 series) give detailed guidance on how to apply the protection means. They may be also recommended in the specific product standards.

C.3 Blindage

Le blindage est réalisé par des barrières métalliques utilisées pour éviter la propagation d'un champ électromagnétique d'un endroit à un autre. Il peut également être utilisé pour évacuer l'énergie transportée par d'autres types de perturbations. De ce fait, le blindage peut être utilisé soit pour contenir un champ électromagnétique issu d'une source donnée située à l'intérieur de la zone blindée, soit pour empêcher des champs électromagnétiques externes d'agir dans un endroit où se trouvent des circuits sensibles aux perturbations électromagnétiques.

Toutefois, le blindage peut être partiellement, voire totalement, inefficace, si les câbles d'entrée et de sortie du système ne sont pas eux-mêmes correctement blindés ou équipés de filtres de pénétration. L'efficacité du blindage peut également être affectée s'il contient de nombreuses ouvertures ou si sa continuité électrique est insuffisante.

C.4 Filtrage

Le filtrage est utilisé pour réduire les éventuelles perturbations conduites à un niveau acceptable. Le filtre, composé d'un circuit conçu spécialement, est placé dans la liaison où les perturbations tendent à passer, et peut agir sur les perturbations entrantes ou sortantes.

Les filtres sont placés sur deux sortes de lignes:

- filtres sur les lignes d'alimentation, et
- filtres sur les lignes de signaux.

Ils sont conçus en fonction du courant ou du type de signal transporté par la ligne et des perturbations qui doivent être supprimées.

C.5 Mise à la terre et liaisons équipotentielles

L'objet de la mise à la terre est de maintenir le potentiel des structures métalliques (blindages, enceintes, châssis) à une valeur constante. Ceci peut être fait en un ou plusieurs points. La CEI 61000-5-2 (article 5) recommande un réseau de mise à la terre maillé comportant plusieurs électrodes de mise à la terre.

L'objet des liaisons équipotentielles est d'assurer une homogénéité électrique sur les structures métalliques afin de réduire les différences de potentiel. Il est nécessaire que l'impédance des tresses de liaison soit faible sur une large plage de fréquence, et que les tresses soient aussi courtes que possible. Si elles sont sensibles à la corrosion, elles seront faciles à démonter et à remplacer (voir la CEI 61000-5-2, article 6).

C.6 Câblage approprié

Une technique de câblage appropriée devrait éviter

- l'induction de tensions ou courants perturbateurs par des champs externes, et
- la diaphonie entre conducteurs.

Le schéma de câblage sera conçu avec soin. L'effet des perturbations électromagnétiques peut être réduit par l'utilisation des techniques suivantes:

- blindage des câbles;
- utilisation de câbles coaxiaux à double blindage;
- utilisation de câbles à paires torsadées;
- séparation des câbles transportant des signaux de niveaux et/ou de types différents;