DRAFT FOR DEVELOPMENT

DD IEC TS 61000-1-2:2001

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

ICS 33.100

National foreword

This Draft for Development reproduces verbatim IEC TS 61000-1-2:2001.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature because the source document is an IEC Technical Specification which is not an international standard. It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for its conversion into an international standard. A review of this publication will be initiated 2 years after its publication by the international organization so that a decision can be taken on its status at the end of its three-year life. The commencement of the review period will be notified by an announcement in *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international standard. Comments should be sent in writing to the Secretary of BSI Subcommittee GEL/210/12, EMC – Basic and generic standards, at 389 Chiswick High Road, London W4 4AL, giving the document reference and clause number and proposing, where possible, an appropriate revision of the text.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled "International Standards Correspondence Index", or by using the "Find" facility of the BSI Standards Electronic Catalogue.

Summary of pages

This document comprises a front cover, an inside front cover, the IEC TS title page, pages 2 to 58, an inside back cover and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

This Draft for Development, having been prepared under the direction of the Electrotechnical Sector Policy and Strategy Committee, was published under the authority of the Standards Policy and Strategy Committee on 14 January 2002

Amendments issued since publication

Amd. No.	Date	Comments

ISBN 0 580 38831 X

SP…CIFICATION TECHNIQUE

TECHNICAL SPECIFICATION

CEI
IEC

TS 61000-1-2

PremiËre Èdition
First edition
2001-06

PUBLICATION FONDAMENTALE EN CEM
BASIC EMC PUBLICATION

CompatibilitÈ ÈlectromagnÈtique (CEM) ñ

Partie 1-2: GÈnÈralitÈs ñ MÈthodologie pour la rÈalisation de la sÈcuritÈ fonctionnelle des matÈriels Èlectriques et Èlectroniques du point de vue des phÈnomËnes ÈlectromagnÈtiques

Electromagnetic compatibility (EMC) ñ

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

NumÈro de rÈfÈrence
Reference number
CEI/IEC/TS 61000-1-2:2001

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

ELECTROMAGNETIC COMPATIBILITY (EMC) ñ

Part 1-2: General ñ 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

ï the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or

ï 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.

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.

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.

ELECTROMAGNETIC COMPATIBILITY (EMC) ñ

Part 1-2: General ñ 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

ñ determining requirements;

ñ requirements;

ñ design aspects including installation of the equipment;

ñ analytical assessment methods;

ñ testing recommendations;

ñ 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.

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

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

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

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

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

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

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

IEC 61000-4-1:2000, *Electromagnetic compatibility (EMC) ñ Part 4-1: Testing and measurement techniques ñ 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 ñ Part 1: General requirements*

IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems ñ 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 ñ Part 3: Software requirements*

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

IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems ñ 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 ñ 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 ñ Part 7: Overview of techniques and measures*

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
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
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 ñ at the bottom of the fault tree ñ 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 ñ at the top of the fault tree ñ 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:

ñ implement the required safety functions necessary to achieve or maintain a safe state for a controlled equipment ;

ñ 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 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 ñ in the context of this document ñ safe operation of an electrical or electronic equipment or system depends on two factors:

ñ the EM environment and the emission levels of the various sources;

ñ the immunity of the influenced devices.

As for the EM emissions, the allowed maximum emission levels are specified by the relevant committees[1], 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:

ñ 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).

ñ 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.

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) 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.

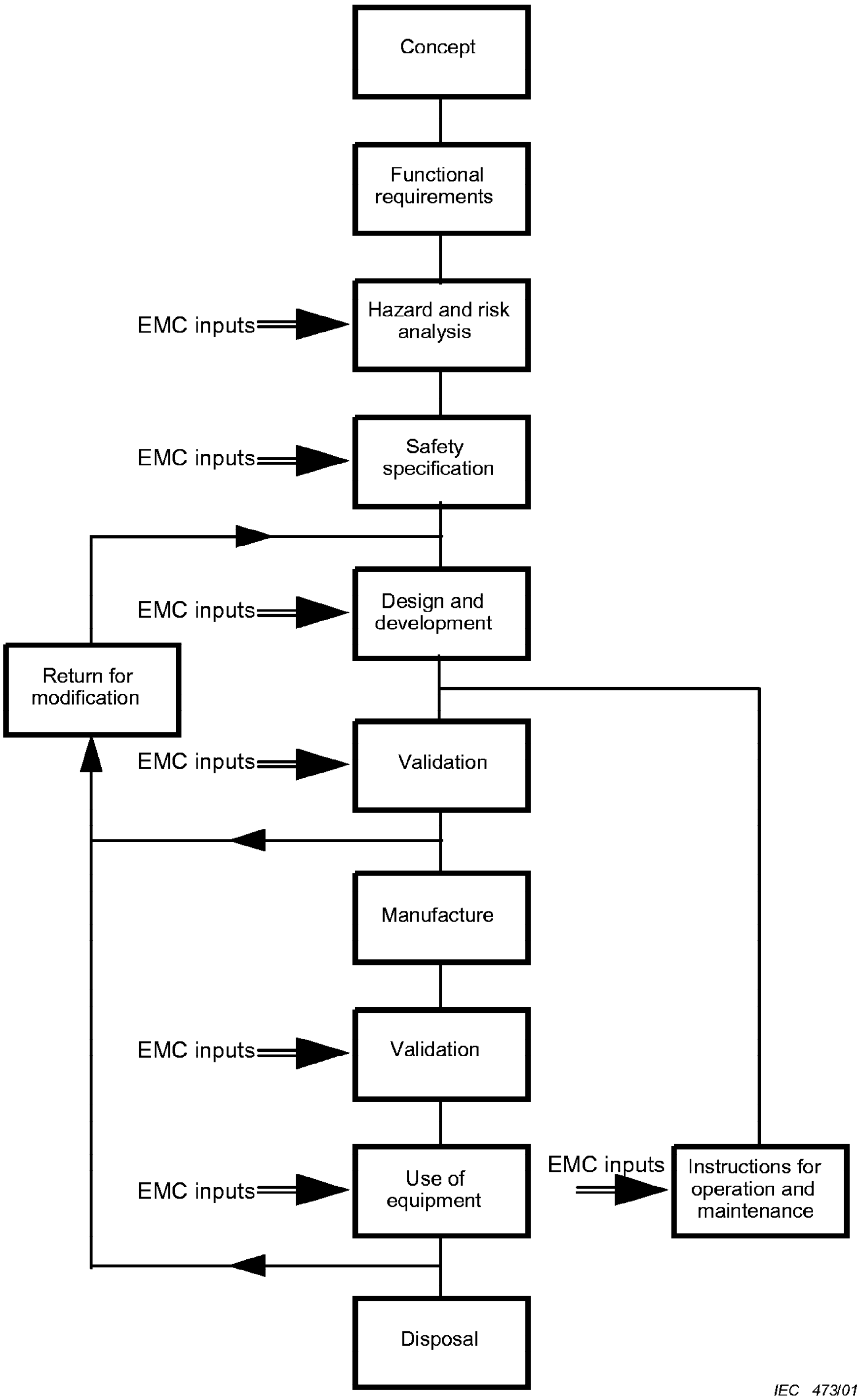

Figure 1 ñ Safety life cycle for individual equipment

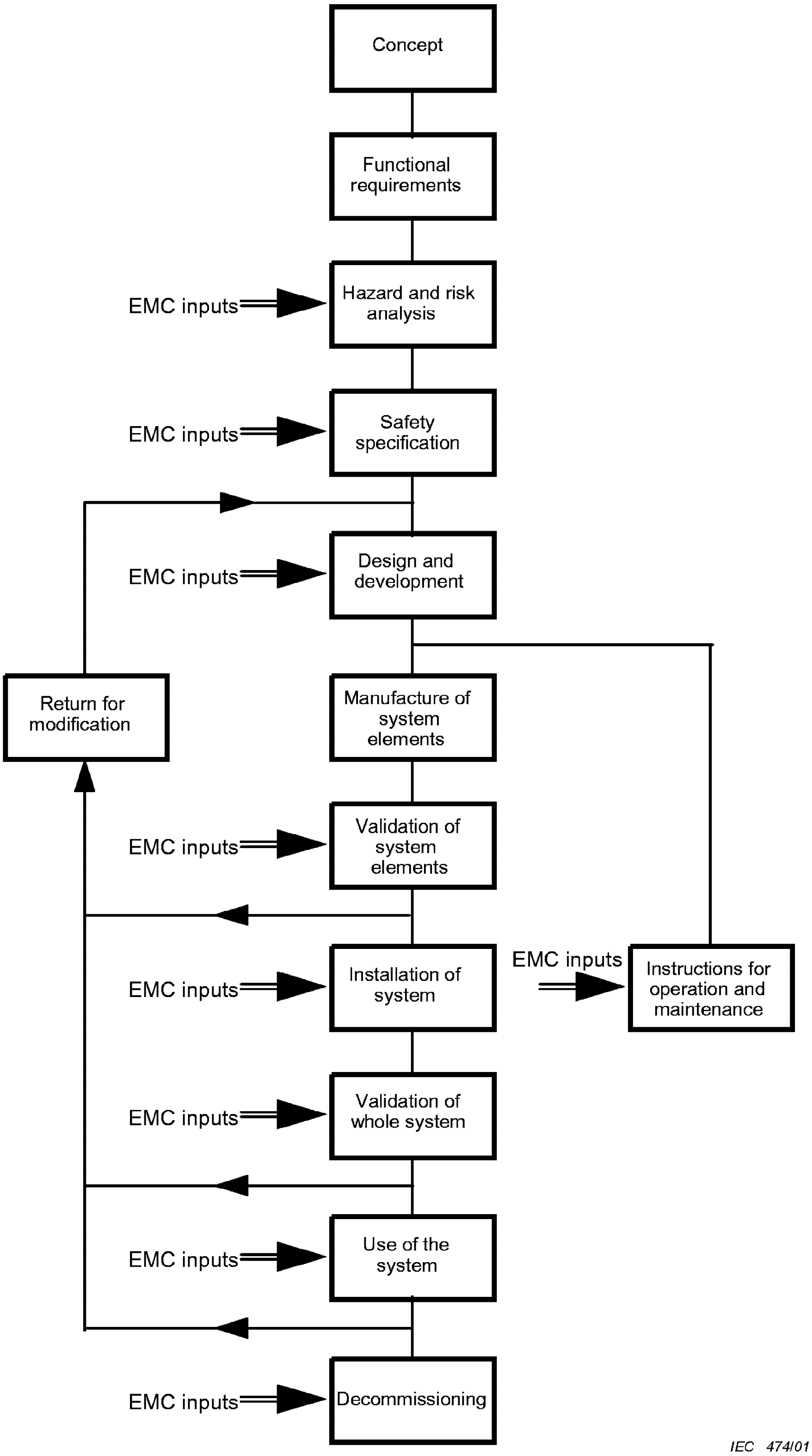

Figure 2 ñ Safety life cycle for systems

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.

Table 1 ñ 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 ñ continuous waves ñ 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) 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, owning 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:

ñ deductive methodology (top-down methodology);

ñ 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 ñ the "top event" ñ 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) 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:
   ñ its physical structure and design rules;
   ñ the software configuration (if possible with the same structure as the hardware);
   ñ the intended functions.

b) Specify the electromagnetic environment to which the investigated equipment is exposed:
   ñ the locations where it is installed,
   ñ the influencing electromagnetic disturbances,
   ñ the most severe disturbance levels,
   ñ the immunity test levels normally applied for functional purposes.

c) Specify all undesirable safety events:
   ñ no operation,
   ñ unwanted operations,
   ñ 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.

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 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:

ñ a series for system parts not relevant for safety;

ñ 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.:

ñ higher test levels;

ñ reducing immunity from disturbances;

- ñ 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. testng 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.:

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

Particular attention should be given to

- ñ the behaviour of safety-related elements (which may be tested separately),
- ñ "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) 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 ñ 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 ñ according to item f) ñ as for safety testing ñ 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 ñ 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

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 ñ or EMC clauses in general product standards ñ 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 ñ residential and industrial environments ñ 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.

Table A.1 ñ Typical EM disturbance levels ñ 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	ñ	10	No test	
	5th	% U_n	6	no test	ñ	8	No test	
IEC 61000-4-11	AC voltage dips	Δ% U_n	10 to 95	30 ∣ 60	B/C	10 to 95	30 ∣ 60	B/C
		periods	0,5 to 150	0,5 ∣ 5		0,5 to 300	0,5 ∣ 50	
IEC 61000-4-11	AC volt. interruptions >95%	periods	2 500	250	C	2 500	250	C
IEC 61000-4-14	AC volt. fluctuations	ΔU_n%	+10, ñ10	No test	ñ	+10, ñ15	No test	ñ
IEC 61000-4-8	Power frequency magnetic fields	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						
	ñ AC power cm		1 to 10	3	A	1 to 10	10	A
	ñ DC power cm		1 to 10	3	A	1 to 10	10	A
	ñ control/signal cm		1 to 10	3	A	1 to 10	10	A
	ñ functional earth		ñ	3	A	ñ	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	ñ	No test	ñ

IEC 61000-4-5	Surges 1,2/50 (8/20) ñ AC power L! G ñ AC power L! L ñ DC power L! G ñ DC power L! L ñ control/signal L! G ñ control/signal L! L	kV	1 to 2 0,5 to 1 ñ ñ 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] ñ AC power ñ DC power ñ control/signal ñ functional earth	kV	1 to 2 ñ 0,5 to 1 ñ	±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 ñ 0,1 MHz (AC power) ñ 1 to 5 MHz (control)	kV	1 to 4	No test No test	ñ ñ	1 to 4 0,5 to 2	No test No test	ñ ñ
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 RF = Radio frequency cm = Common mode L! G = Line to Ground
5th = Example 5th harmonic ESD = Electrostatic discharge dm = Differential mode 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 ñ 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.

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:

ñ B.1 Single apparatus: Electronic gas burner controller;

ñ 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.

Extracts from IEC 61025 ñ 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.

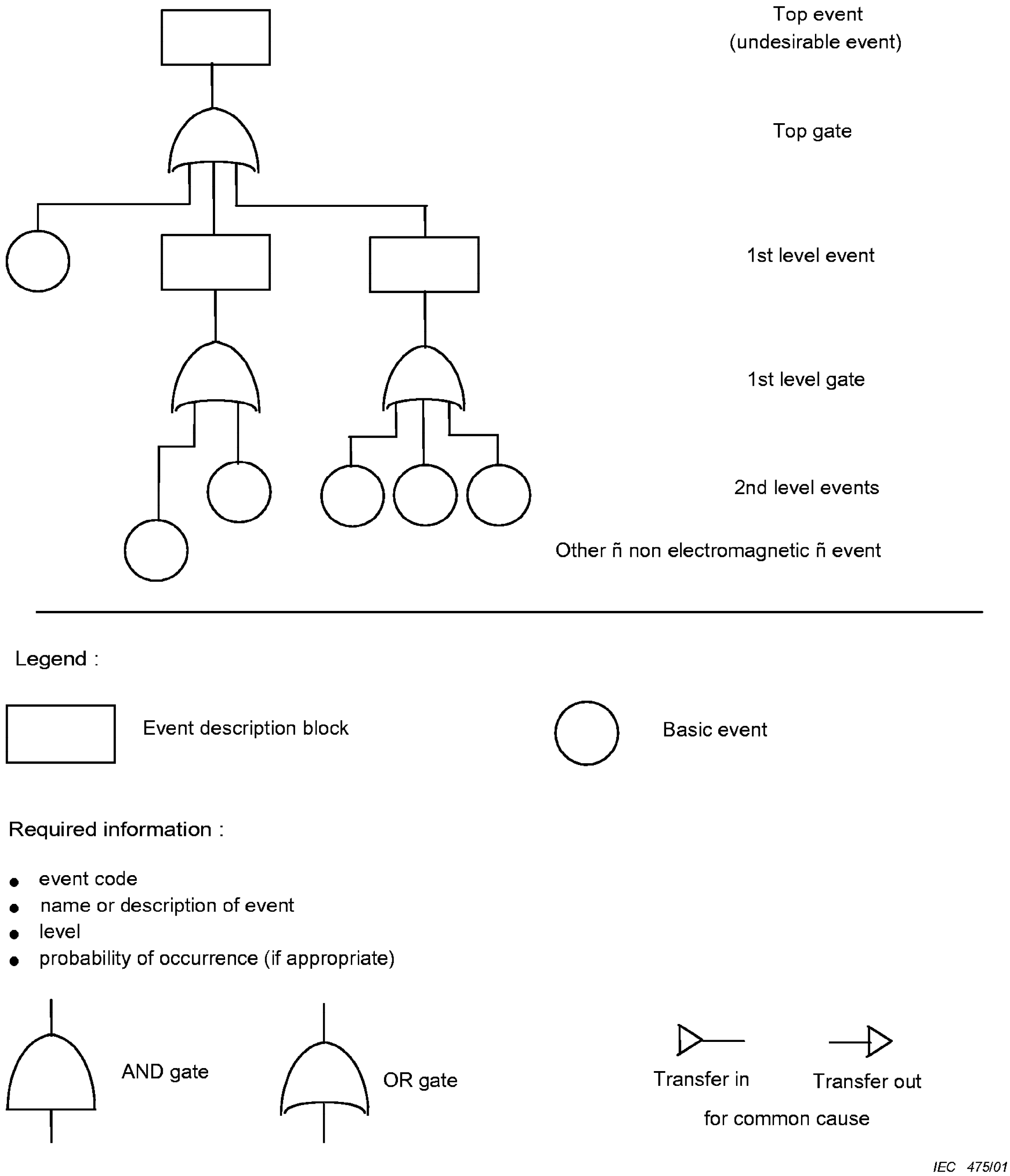

Figure B.1 ñ Symbols for the construction of a fault tree

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):

   ñ flame supervision (optical sensor) to prevent the flow of unburned gas;

   ñ high limit thermostat, to prevent a too high temperature;

   ñ air pressure detection, to prevent poisonous burning.

b) Specific safety measures are related to the burner controller itself:

   ñ primary safeguards; power supply check, watchdog, ROM/RAM check and sensor checks;

   ñ 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:

   ñ air pressure;

   ñ false flame;

   ñ gas release;

   ñ ignition.

b) diagnostic self-checks made continuously during the operation of the controller and the burner (see B.1.5).

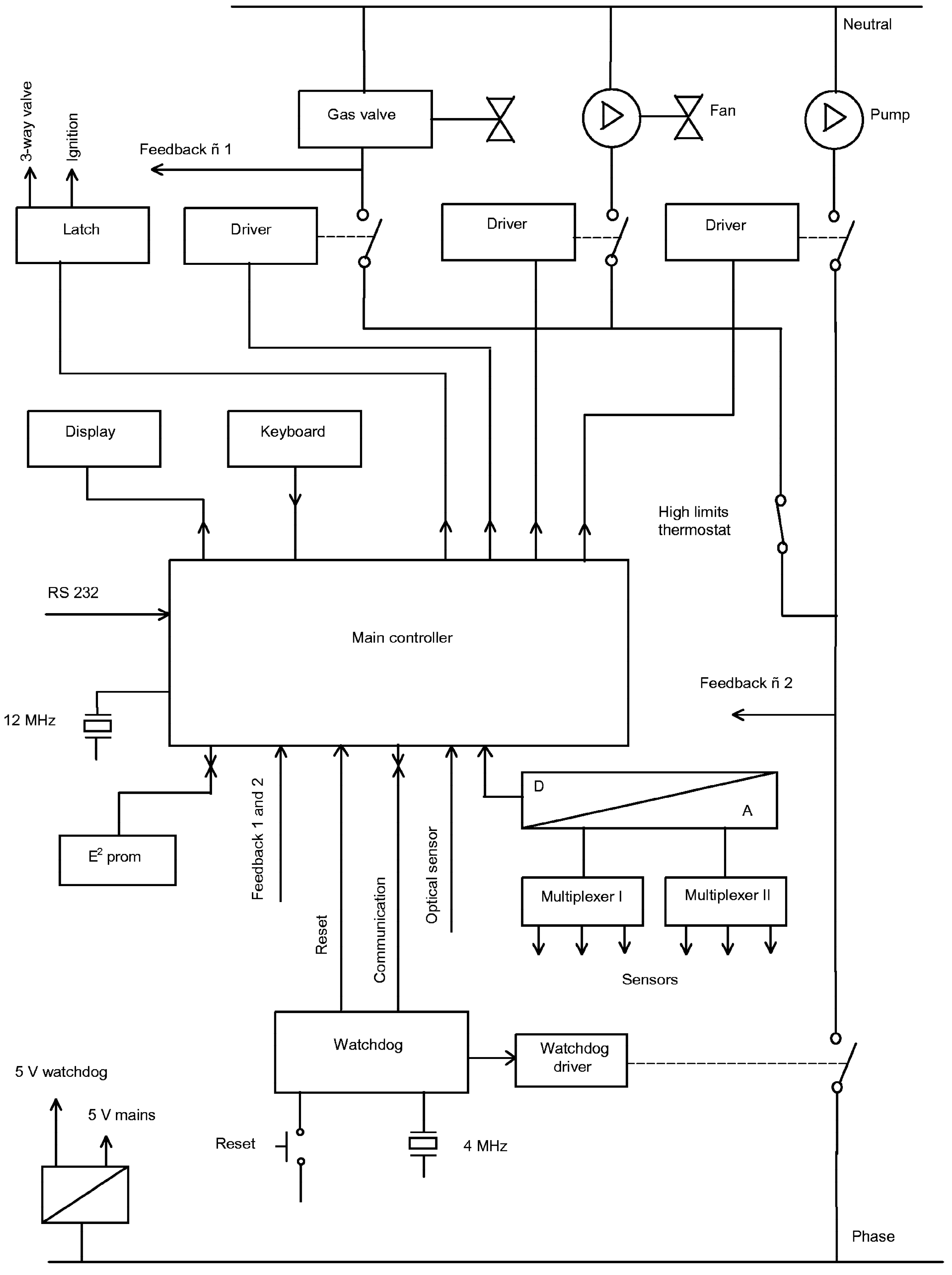

Figure B.2 ñ Gas burner controller: hardware structure

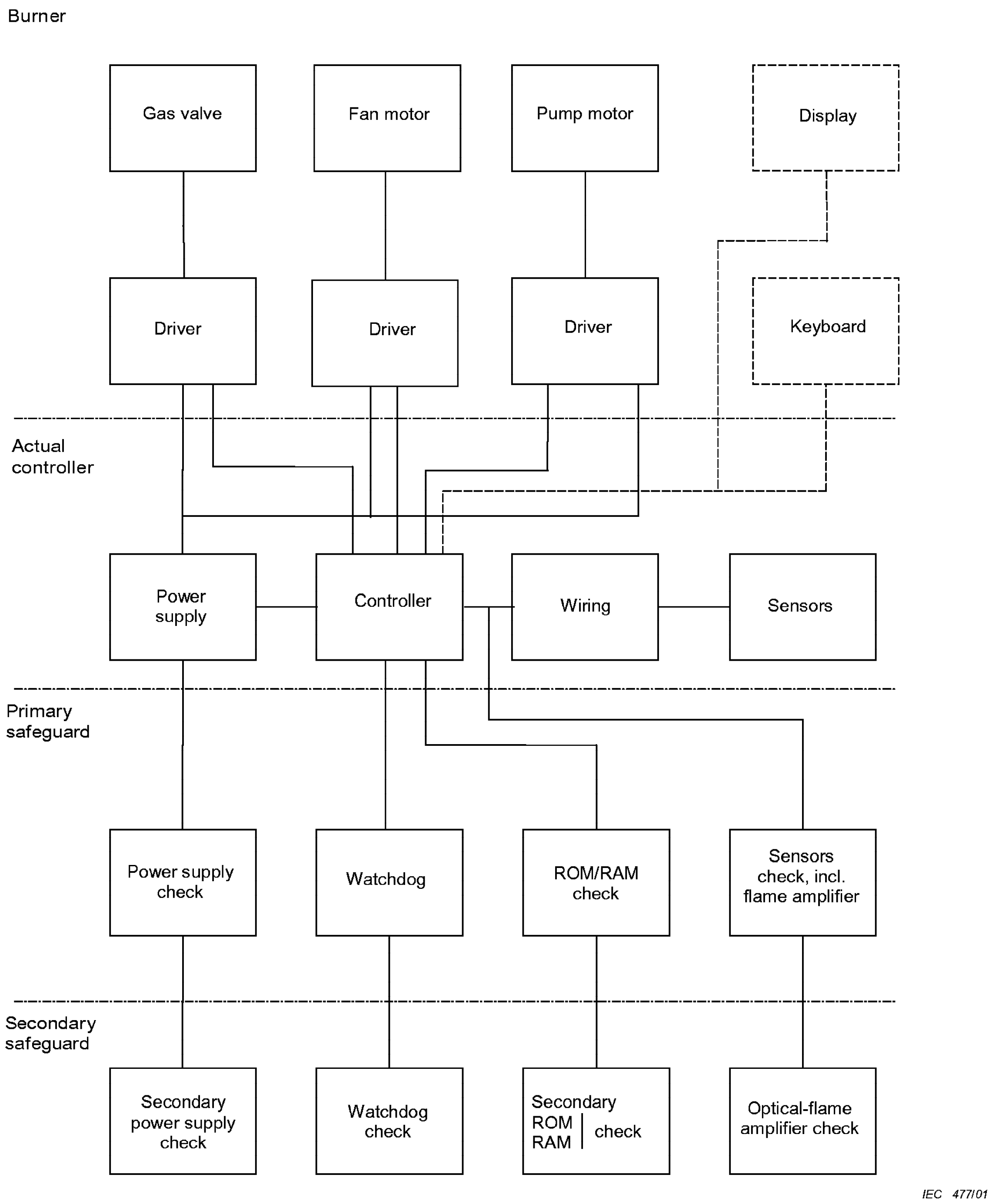

Figure B.3 ñ Gas burner controller: Block diagram

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:

ñ which electromagnetic phenomena can cause these risks (basic events),

ñ at which places in the device, in order to take appropriate mitigation measures.

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

ñ unburned gas:

cause: no ignition and defective flame detection;

ñ temperature too high:

cause: defective control temperature sensor or no water (circulation)

ñ 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 FTAís 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.

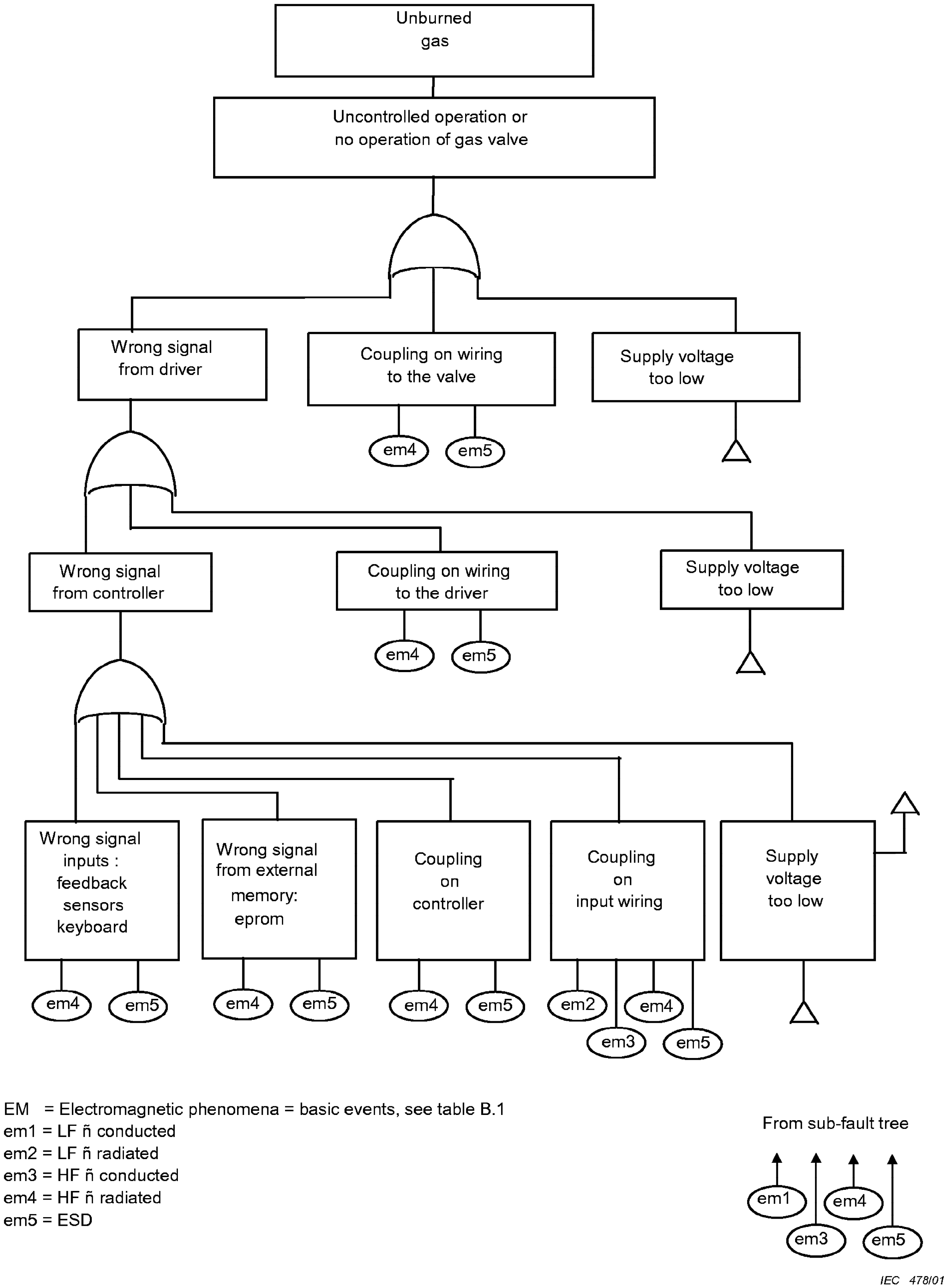

Figure B.4 ñ Gas burner controller; FTA for the top event unburned gas

Table B.1 ñ 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 μs 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 ñ 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 ñ 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* > 0,5m	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 ñ the basic events ñ 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 ñ at the highest environmental level of the disturbances ñ can/will have a critical safety impact.

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 ñ 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	ñ	X	X	X	X	X	X	X
2	Controller memory	ñ	ñ	ñ	ñ	ñ	ñ	ñ	X	X	X
3	Accessories Sensors Keyboard	ñ	ñ	ñ	ñ	ñ	ñ	ñ	X	X	X
4	Internal wiring	ñ	ñ	?	ñ	ñ	ñ	ñ	X	X	X
5	External wiring	ñ	ñ	?	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;
ñ 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.

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

ñ the control layer,

ñ the primary safeguard layer, being able to detect failures in the control layer and to shut down the gas valve independently,

ñ 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

   ñ possibly also such disturbances which are not specified in the relevant product standard just with regard to functional immunity ñ in our example of a gas burner controller: harmonics and oscillatory transients;

b) the test levels for safety

   ñ either from the relevant product standard if the latter prescribes specific test levels for safety,

   ñ or the functional test levels enhanced by an appropriate security margin,

   ñ 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 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.

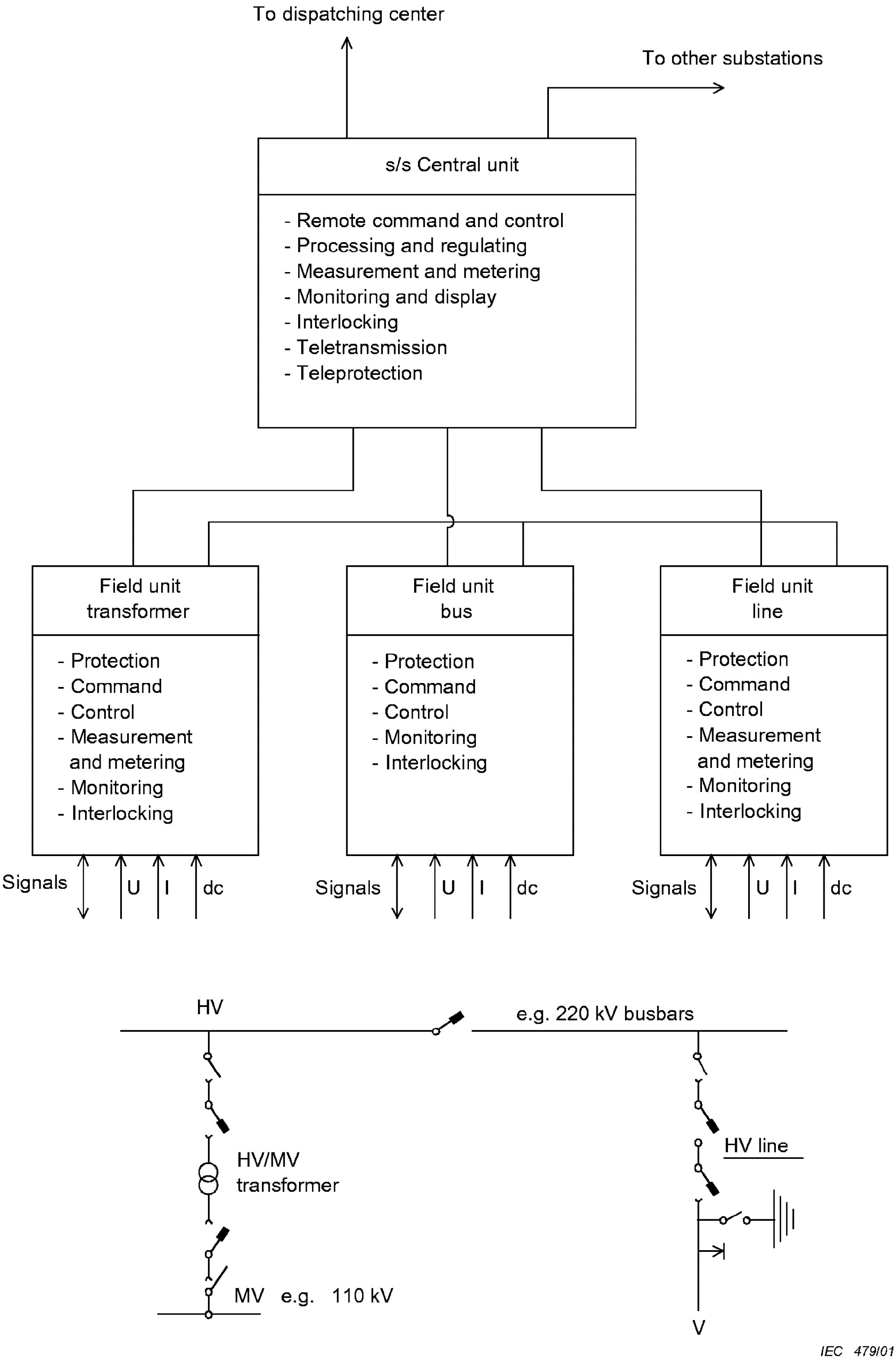

Figure B.5 ñ General structure of the control command of a high voltage substation

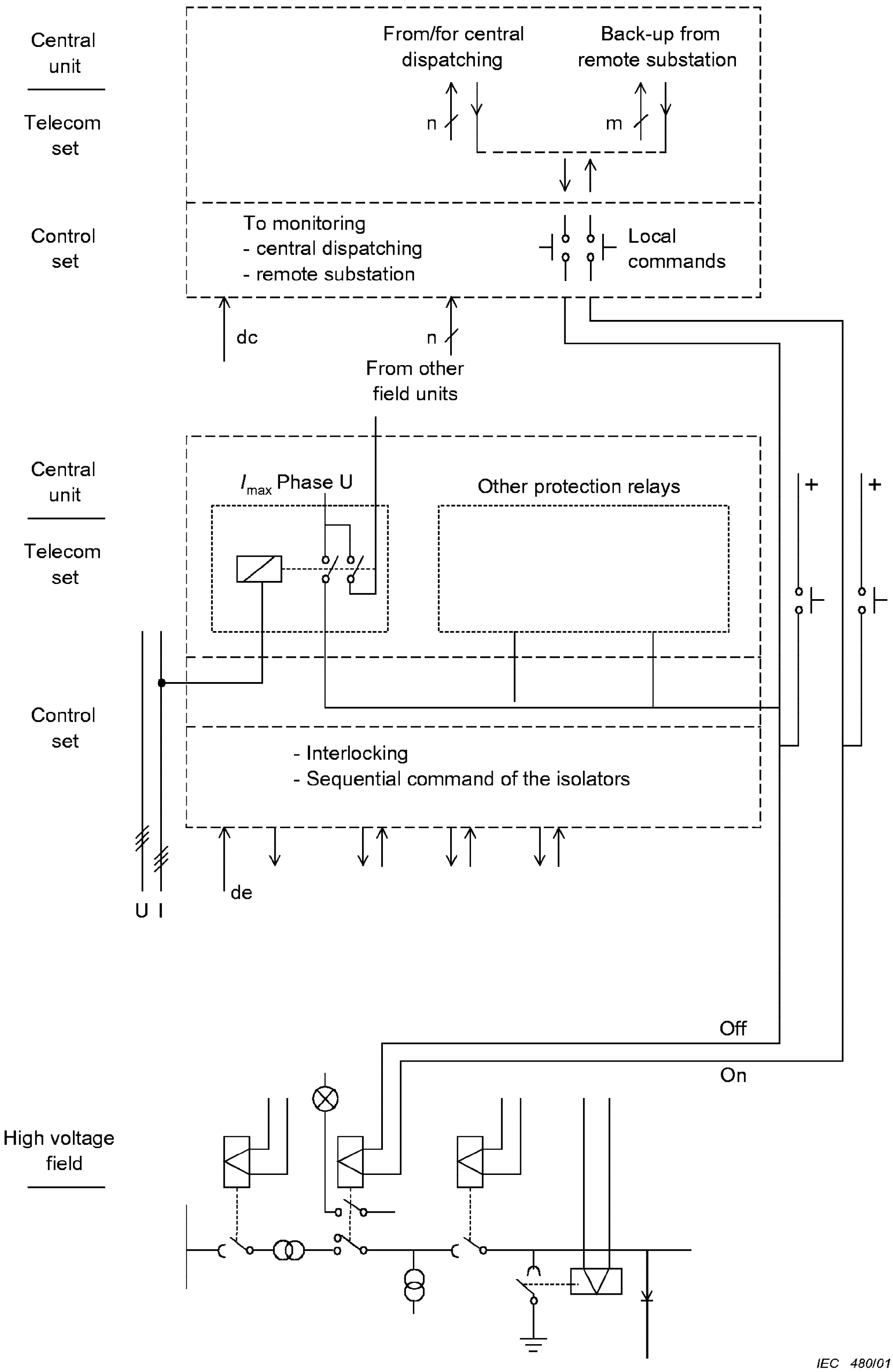

Figure B.6 ñ Schematic of the short-circuit protection

In classical ñ older ñ 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 ñ 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 ñ a.c. and d.c. supplies	Supply voltage dips ($t \leq$ 0,02 s) ñ a.c. and d.c. supplies	Supply voltage dips (t > 0,20 s) ñ a.c. and d.c. supplies
Harmonics, interharmonics	Fast transient bursts	Supply voltage interruptions (ΔU = 100 %) ñ 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 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 ñ top events ñ 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 > $\vartheta°$);
  - for a transformer: short circuit relays (I_{max}), overload relays (temperature > $\vartheta°$), 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:

   ñ FTA at the level of the individual apparatuses (as in example B.1);

   ñ 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);

   ñ 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) 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:

   ñ 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;

   ñ the wiring between the single apparatuses; internal wiring inside the common enclosures or external wiring between these units;

   ñ 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:

   ñ 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);

   ñ transient high frequency fields such as the ones caused by lighting effects or by switching operations.

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.

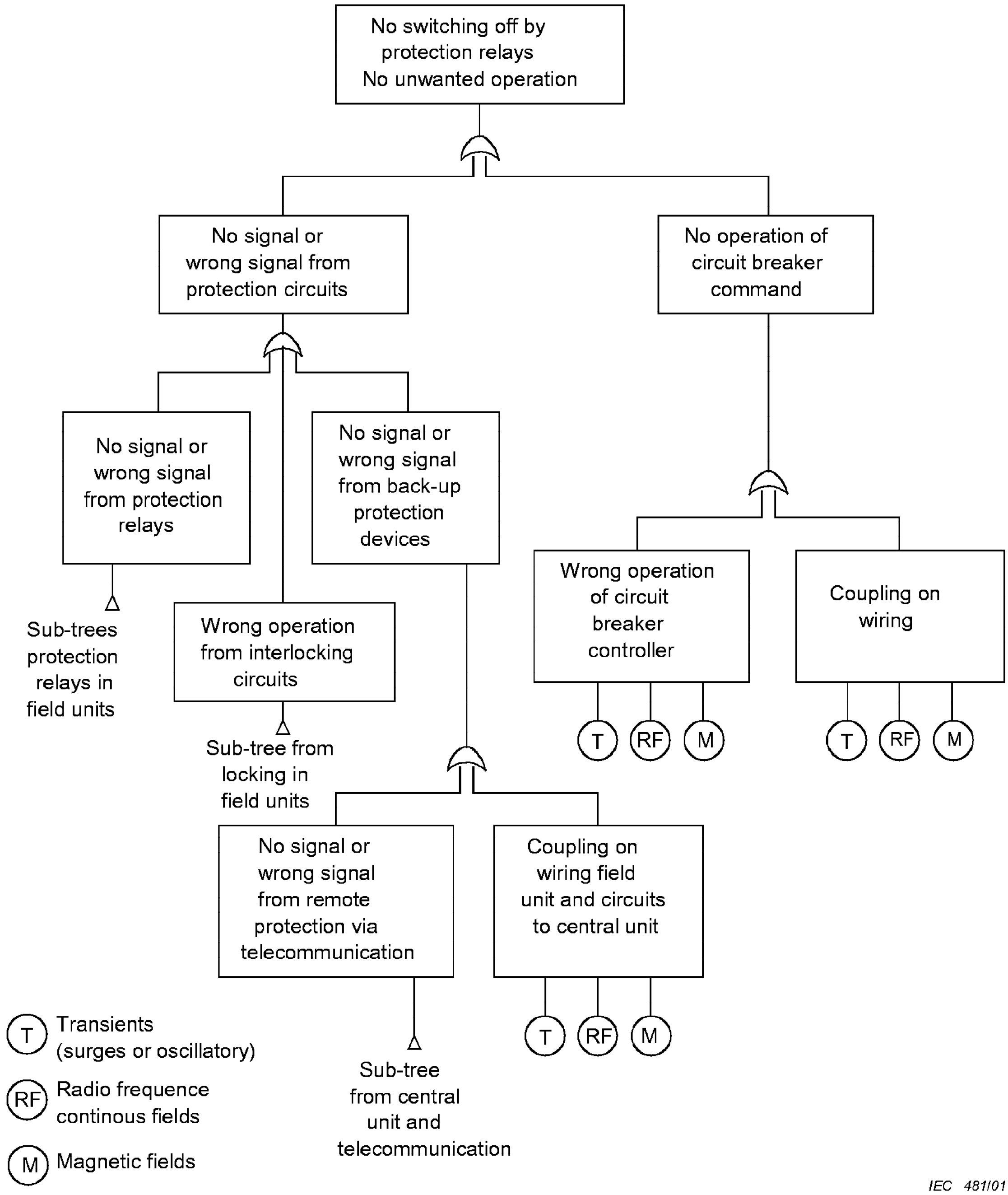

Figure B.7 ñ FTA for short-circuit protection

Table B.4 ñ 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	ñ

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;

ñ 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

ñ with the safety test levels if such levels are specified;

ñ with an enhanced functional test level if no safety test level is prescribed.

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.

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 Shielding

Shielding is done with metallic barriers that are used to prevent the propagation of an electromagnetic field from one region to another. It can also be used to channel off the energy carried by other types of disturbances. As a result, shielding can be used to either contain an electromagnetic field from a given source within the shielded area, or to keep external electromagnetic fields from acting on a region where there are circuits sensitive to radiated electromagnetic disturbance.

However, shielding can be partially, or even totally ineffective if the input and output cables of the system are themselves not properly shielded or equipped with penetration filters. The efficiency of the shielding can also be affected if it contains many openings, or if its electrical continuity is insufficient.

C.4 Filtering

Filtering is used to reduce any conducted disturbances to an acceptable level. The filter, consisting of a specially designed circuit, is placed in the link where disturbances tend to pass, and can act on incoming or outgoing disturbances.

Filters are placed in two kinds of lines:

ñ filters on the power supply lines;

ñ filters on signal lines.

They are designed as a function of the current or the type of signal carried on the line and of the disturbances that are to be suppressed.

C.5 Earthing and bonding

The purpose of earthing is to maintain the potential of metallic structures (shields, enclosures, chassis) at a constant value. This can be done at one or several points. Clause 5 of IEC 61000-5-2, recommends a meshed earthing network with several earth electrodes.

Bonding is intended to provide an electrical homogeneity on metallic structures in order to reduce potential differences. The impedance of bond traps should be low over a wide frequency range, and they should thus be as short as possible. If they are susceptible to corrosion, they should be easy to remove and replace (see clause 6 of IEC 61000-5-2).

C.6 Appropriate wiring

A proper wiring technique should avoid:

ñ the induction of disturbing voltages or currents by external fields;

ñ crosstalk between conductors.

The wiring scheme should be designed carefully. The effect of electromagnetic perturbations can be reduced by using the following techniques:

ñ cable shielding;

ñ use of coaxial cables with double shield;

ñ use of twisted wire pairs;

ñ separation of cables carrying signals of different levels and/or types;

- use of reducing effect of metallic structures;
- use of optic links (a modern, very effective method).

C.7 Immunity design of printed circuit boards (PCBs)

The layout of the tracks and components of a printed circuit plays an important role in the mastery of EMC problems, in the areas of emission as well as immunity. A good circuit layout consists of a well meshed network of grounding and power supply circuits. An even better method is to use a multi-layer PCB with one layer connected to the ground and another one connected to the power supply.

Decoupling capacitors should be mounted as close as possible to the different components, as well as to the critical points of a meshed network.

Low-level analogue circuits should be separated from digital circuits, which themselves are to be separated according to their working speed. In this manner, any internal crosstalk is avoided.

Conducted and/or radiated electromagnetic disturbances produced by component or sub-assembly of the PCB are thus controlled to prevent any intra-system interference.

C.8 Redundant circuits

Important elements or circuits with regard to safety may be duplicated and connected in parallel in order to ensure the equipment behaviour in case of failure. It is recommended that each parallel circuit should be designed in a different technology in order to avoid both circuits failing at the same time.

The global architecture of the system must also be considered. The redundancy principle must be applied to both hardware and software. The response of each functional channel should be compared, thus allowing mismatches to be detected, which in turn causes the system to react and orient itself to safe operation.

C.9 Digital techniques

As far as digital circuits are concerned, software techniques can be used to ensure safe operation:

- digital information coding;
- error detection algorithms;
- correction algorithms.

Error correction circuits work in such a way that, in the presence of a transient perturbation, the system can resume normal operation as signal errors are detected and corrected. This should be done without posing any risk to the system users.

The safety of a system can also be improved through judicious software design and the design of its structure. In particular it should be able to account for the occurrence of errors caused by the action of electromagnetic disturbances (unexpected program jump, or change in operating instructions, address codes, etc.).

C.10 Maintenance

As a rule, the designer provides instructions relative to the proper maintenance of the EMC (emission and immunity) of a system in the General Maintenance Manual, and must therefore ensure that maintenance work can be performed safely.

Maintenance sometimes requires that certain installed components serving to ensure EMC be removed or disassembled. Those people performing the maintenance work should thus be warned of the risks linked to any malfunctions that may result from the lowering of the level of EMC immunity. Although this can be done in the manual, warning signs or panels should be posted on or near the equipment in question.

Resumption of normal operation of the system, either manually or automatically, must be done only in the absence of any foreseeable risk.

Annex D
(informative)

Typical check list of measures and techniques for the achievement of functional safety with regard to EMC disturbances

The following check list is presented to assist in the application of this document.

D.1 Safety requirements with regard to electromagnetic influences

ñ Specify the unwanted safety events

- non-operation when operation required;
- operation when no operation required;
- wrong operations.

D.2 Necessary background information

ñ Reference to standards (or bibliography) to determine electromagnetic disturbance levels to be expected in the intended environment.

ñ Measurement of the electromagnetic environment in the place of use when necessary.

D.3 Design and development (see annex C)

ñ Design of a structure reducing the probability of dangerous failures due to electromagnetic interference (e.g. fail-safe features, use of parallel redundant channels employing different technologies).

ñ Avoiding the use of components and circuits known to be susceptible to electromagnetic disturbances.

ñ Development of a software reducing the probability of dangerous failures due to electromagnetic interference.

ñ Dependability analysis (e.g. fault tree analysis) with regard to safety.

ñ Testing to determine safety levels of components and circuits when exposed to electromagnetic disturbances representative of the intended environment.

ñ Use of computer-aided design tools for minimising electromagnetic coupling paths.

ñ Use of checklists.

D.4 Implementation and integration

ñ Implementation of procedures to ensure the procurement of components and materials according to specification.

ñ Implementation of procedures to ensure the correct assembly of equipment, using the correct materials, according to specification.

ñ Use of verification and quality assurance procedures to ensure that the design is faithfully translated to a working system.

D.5 Installing

- ñ Specification of any constraints on lengths and routing of interconnecting cables.
- ñ Specification of types of cable and method of terminating screens.
- ñ Specification of types of connectors.
- ñ Specification of constraints on physical positioning with respect to other equipment.
- ñ Specification of power supply requirements (protection measures against harmonics, voltage dips, transients etc.).
- ñ Specification of any screening/shielding required in addition to that provided by the equipment.
- ñ Specification of earthing and bonding requirements.
- ñ Installation according to specified procedures and using specified materials.

D.6 Safety validation

- ñ Dependability analysis, to be used.
- ñ Verification of correct implementation of the safety requirements.
- ñ Survey of electromagnetic environment to confirm expectations/assumptions.
- ñ Laboratory testing of safety behaviour and functions.
- ñ Immunity testing using disturbance levels higher than those expected to be present in the intended environment to determine possible safety related failure modes and maximum acceptable disturbances levels.
- ñ Use of special test procedures to exercise operating modes known to be vulnerable to electromagnetic disturbances.
- ñ In situ testing of safety behaviour and functions.
- ñ Quantitative evaluation of failure rates based on statistical distributions of disturbance levels and immunity levels of equipment.

D.7 Operation and maintenance

- ñ Specification and use of operating procedures necessary to preserve EMC performance and EM safety.
- ñ Specification and observance of restrictions on the operation of other equipment which may not have an adequate level of electromagnetic compatibility (e.g. mobile radio transmitters).
- ñ Specification and use of disassembly/reassembly techniques to preserve EMC performance, and EM safety.
- ñ Periodic testing (proof testing) of critical components for EM safety (e.g. transient suppressors).
- ñ Periodic replacement of sensitive protection devices (e.g. transient suppressors).
- ñ Periodic testing of safety-related functions.

D.8 Modification

- ñ Assessment of the effect of proposed modifications on EM safety of both equipment under consideration and any other equipment which might be affected.

Annex E
(informative)

Dependability analysis techniques and their application with regard to EMC

E.1 Introduction

Dependability analysis techniques are used for the review and prediction of the reliability, availability, maintainability and safety of an equipment: apparatus, system or installation.

The aim of the present annex is to give an overview of the dependability analysis techniques described in IEC standards and of some other important ones and to assess their applicability to electromagnetic disturbances.

The analysis can be conducted mainly during the concept and definition phase, the design and development phase and the operation and maintenance phase. They can be conducted at various equipment levels and degrees of detail in order to evaluate and determine the dependability aspects of an equipment. They can then be used to compare the results of analysis with specified requirements.

With regards to safety, the dangerous fault modes are of interest. These lead to unsafe or potentially unsafe conditions (hazards), of the equipment or system. If the combination of events causing a hazard is not so easy to identify, then a hazard analysis using special techniques may need to be carried out.

Several of the analysis techniques referred to in IEC 60300-3-1 can be used to undertake a hazard analysis. In addition, other techniques are used in particular applications. Each of the techniques has particular strengths and weaknesses and fields of application. There is no single "correct" approach to a particular problem and often a combination of measures is required. Different techniques may be appropriate according to the equipment level and life-cycle phase.

It should also be noted that it may be necessary, for a single hazard analysis to take account of several different influences on system behaviour. These may encompass non-electromagnetic influences (such as temperature and vibration) as well as different types of electromagnetic disturbance.

E.2 Particular requirements of analysis technique for EMC

The analysis technique(s) used should be capable of modelling the system behaviour in the presence of the electromagnetic disturbances which are likely to be present in the intended environment. In particular, the following characteristics of electromagnetic disturbances and possible interference should be considered when selecting an analysis technique:

- a single disturbance can cause several faults in different parts of the system (common cause faults);
- the probability of occurrence of electromagnetic disturbances often varies with time;

ñ the characteristics of electromagnetic disturbances (for example level, frequency) often vary with time and site;

ñ there may only be a limited knowledge of the statistical properties of disturbances;

ñ the possibility of a disturbance causing interference may depend on the state of the equipment at the time of the disturbance;

ñ the effect of disturbances on parts of the equipment may be influenced by the way in which the overall equipment is integrated and installed;

ñ many different types of disturbance may be present at the same time.

As explained in clause 8.1 there are two basic types of risk analysis:

ñ deductive methods (top-down methods);

ñ inductive methods (bottom-up methods).

With regard to the effects of electromagnetic phenomena on functional safety it appears appropriate to apply a top-down method which consists of

ñ first, defining the undesirable events;

ñ secondly, analysing which electromagnetic phenomena can cause these undesirable events and in which part of the device.

E.3 Dependability analysis techniques in IEC standards

IEC 60300-3-1 gives an overall description of important and widely used dependability analysis techniques (see also IEC 61508-7). Some of these are described in more detail in dedicated standards. The following comments and recommendations are made with regard to EMC.

E.3.1 Fault tree analysis (FTA) (IEC 61025)

Fault tree analysis is a deductive method which offers some advantages with regard to EMC:

ñ it can handle common cause failures;

ñ it can handle time varying failure/event rates;

ñ the events in a fault tree are not limited merely to faults ñ they can involve degradation in performance;

ñ an FTA can be based on qualitative reasoning;

ñ FTA allows a calculation method using Boole algebra.

It is possible to undertake an FTA at different levels of system design. If an FTA is undertaken at an early stage of the design it may assist in identifying those parts of the equipment or system where enhanced immunity test levels may be required to achieve the required level of safety.

The key advantage of FTA is that it only requires consideration of those parts of the equipment or system which can contribute to hazards. This approach can therefore be economical.

The examples in Annex B are based on FTA.

E.3.2 Fault modes and effects analysis (FMEA) (IEC 60812)

A FMEA is an inductive method which can be performed using a hardware approach or a functional approach.

The hardware approach considers the failure modes of identifiable items of hardware. The effect of each failure mode of the individual items on the overall system behaviour is considered. This type of analysis is not considered, in general, to be applicable to EMC for the following reasons:

ñ it does not easily consider common cause failures;

ñ electromagnetic interference usually results from disturbances to the operating conditions (currents and voltages) of components rather than actual failures of components;

ñ it does not easily deal with time sequences and system states.

On the other hand, the functional approach to FMEA may be more applicable to EMC. In applying this approach the analyst asks "in what ways can this function deviate from the specified requirement?"

For example, if one function of a system consists of closing a valve when the temperature exceeds a certain level, then some of the functional failure modes are:

a) valve closes at a higher than specified temperature;

b) valve closes at lower than specified temperature;

c) valve remains permanently open;

d) valve remains permanently closed.

Using this approach it may be possible to identify which functions are more critical and therefore require higher levels of immunity. Such an analysis can be carried out like FTA at different levels of system design: During the early phase of design, before component design is undertaken it does not require a detailed knowledge of component level failure modes.

Both types of FMEA suffer from the general disadvantage that they require consideration of many parts of the equipment or system which may not be related to safety.

E.3.3 Event tree analysis (see IEC 60300-3-1 ñ Table 2)

Event tree analysis can be used to investigate possible sequences of events resulting from loss of performance or degradation in specific parts of the equipment or system. Such an analysis may be useful, for example, in investigating the effect of a dip or interruption in the mains power supply. The analysis would reveal whether the degradation could lead to a hazard.

It is therefore considered that event tree analysis does have possible applications in the assessment of functional safety and EMC.

E.3.4 Hazard and operability study (HAZOP) (see C.6.2 of IEC 61508-7)

A HAZOP study is a systematic technique for identifying hazards or operability problems for a whole system. Each section of a process is examined and all possible deviations from normal operating conditions and how they might occur are listed. The consequences on the process are assessed, and the measures to detect "probable" deviations that could lead to hazardous events or operability problems are identified.

This technique can be used to identify safety functions. It can therefore be used to identify the parts of a system which require particular attention with regard to EMC and functional safety.

Bibliography

General documents concerning functional safety

IEC Guide 104:1997, *The preparation of safety publications and the use of basic safety publications and group safety publications*

IEC Guide 107:1998, *Electromagnetic compatibility ñ Guide to the drafting of electromagnetic compatibility publications*

CENELEC BTWG 99-2: *Interim Report to the BT concerning EC Directives, functional safety and the role of CENELEC standardisation*

As for a specific information on the methods and test procedures indicated in this document, it can be referred to the publications of the following Technical Committees (see also clause 2)

- TC 77: Electromagnetic compatibility
- TC 56: Dependability
- SC 65A: System aspects

Technical information on functional safety

LIMNIOS, N. *Arbres de dÈfaillances.* Paris: Editions HermËs, 1991. 183 p. (Handbook)

EMC and Functional Safety (Draft) IEE Technical Guidelines (this very thorough document gives detailed information on eight important domains of application)

BROWN SJ. EMC and Safety related Systems. *Proceedings of the IEE International Conference on EMC,* Coventry 1997

ARMSTRONG, K. Some EMC Issues for safety and business critical systems. *Proceedings of the IEE International Conference on EMC,* Coventry 1997

Practical examples of specifications for functional safety and the application of the Fault Tree Method

IEC 61496-1:1997, *Safety of machinery ñ Electrosensitive protection equipment ñ Part 1: General requirements and tests*

IEC 60601-1-2:1993,[2] *Medical electrical equipment ñ Part 1: General requirements for safety ñ 2. Collateral standard ñ Electromagnetic compatibility ñ Requirements and tests*

IEC 60601-1-4:1996, *Medical electrical equipment ñ Part 1: General requirements for safety ñ 4.Collateral standard ñ Programmable electrical medical systems*

IEC 60335-1:1991, *Safety of household and similar electrical appliances (Third edition)*

EN 50165:1997, *Electrical Equipment of non-electric appliances for household and similar purposes ñ Safety requirements*

---

2 A second edition of IEC 60601-1-2 is to be published.

Other publications

IEC 60255-22 (all parts), *Electrical relays ñ Part 22: Electrical disturbance tests for measuring relays and protection equipment*

IEC 60812:1985, *Analysis techniques for system reliability ñ Procedure for failure mode and effects analysis (FMEA)*

IEC 60870 (all parts), *Telecontrol equipment and systems*

IEC 61000-2-3:1992, *Electromagnetic compatibility (EMC) ñ Part 2: Environment ñ Section 3: Description of the environment ñ Radiated and non-network-frequency-related conducted phenomena*

IEC 61000-2-4:1994, *Electromagnetic compatibility (EMC) ñ Part 2: Environment ñ Section 4: Compatibility levels in industrial plants for low-frequency conducted disturbances*

IEC 61000-2-5:1995, *Electromagnetic compatibility (EMC) ñ Part 2: Environment ñ Section 5: Classification of electromagnetic environments. Basic EMC publication*

IEC 61000-4-2:1995, *Electromagnetic compatibility (EMC) ñ Part 4: Testing and measurement techniques ñ Section 2: Electrostatic discharge immunity test. Basic EMC Publication*

IEC 61000-4-3:1995, *Electromagnetic compatibility (EMC) ñ Part 4: Testing and measurement techniques ñ Section 3: Radiated, radio-frequency, electromagnetic field immunity test*

Amendment 1 (1998)
Amendment 2 (2000)

IEC 61000-4-4:1995, *Electromagnetic compatibility (EMC) ñ Part 4: Testing and measurement techniques ñ Section 4: Electrical fast transient/burst immunity test. Basic EMC Publication*

IEC 61000-4-5:1995, *Electromagnetic compatibility (EMC) ñ Part 4: Testing and measurement techniques ñ Section 5: Surge immunity test*

IEC 61000-4-6:1996, *Electromagnetic compatibility (EMC) ñ Part 4: Testing and measurement techniques ñ Section 6: Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61000-4-8:1993, *Electromagnetic compatibility (EMC) ñ Part 4: Testing and measurement techniques ñ Section 8: Power frequency magnetic field immunity test. Basic EMC Publication*

IEC 61000-4-11:1994, *Electromagnetic compatibility (EMC) ñ Part 4: Testing and measuring techniques ñ Section 11: Voltage dips, short interruptions and voltage variations immunity tests*

IEC 61000-4-12:1995, *Electromagnetic compatibility (EMC) ñ Part 4: Testing and measurement techniques ñ Section 12: Oscillatory waves immunity test. Basic EMC Publication*

IEC 61000-4-13:ó , [3] *Electromagnetic compatibility (EMC) ñ Part 4: Testing and measurement techniques ñ Harmonics and interharmonics including mains signalling at a.c. power port, low frequency immunity tests ñ Basic EMC Publication*

IEC 61000-4-14:1999, *Electromagnetic compatibility (EMC) ñ Part 4-14: Testing and measurement techniques ñ Voltage fluctuation immunity test*

IEC/TR3 61000-5-1:1996, *Electromagnetic compatibility (EMC) ñ Part 5: Installation and mitigation guidelines ñ Section 1: General considerations ñ Basic EMC publication*

IEC/TR3 61000-5-2:1997, *Electromagnetic Compatibility (EMC) ñ Part 5: Installation and mitigation guidelines ñ Section 2: Earthing and cabling*

IEC 61000-5-6: ó ,[4] *Electromagnetic Compatibility (EMC) ñ Part 5-6: Installation and mitigation guidelines ñ Mitigation of external EM influences*

IEC 61000-6-1:1997, *Electromagnetic compatibility (EMC) ñ Part 6: Generic standards ñ Section 1: Immunity for residential, commercial and light-industrial environments*

IEC 61000-6-2:1999, *Electromagnetic compatibility (EMC) ñ Part 6-2: Generic standards ñ Immunity for Industrial environments*

CISPR 61000-6-3:1996, *Electromagnetic compatibility (EMC) ñ Part 6: Generic standards ñ Section 3: Emission standard for residential, commercial and light-industrial environments*

IEC 61000-6-4:1997, *Electromagnetic compatibility (EMC) ñ Part 6: Generic standards ñ Section 4: Emission standard for industrial environments*

IEC 61000-6-5: ó ,[5] *Electromagnetic compatibility (EMC) ñ Part 6: Generic standards ñ Immunity for power station and substation environments*

IEC 61069-1:1991, *Industrial-process measurement and control ñ Evaluation of system properties for the purpose of system assessment ñ Part 1: General considerations and methodology*

IEC 61069-2:1993, *Industrial-process measurement and control ñ Evaluation of system properties for the purpose of system assessment ñ Part 2: Assessment methodology*

[3] To be published.

[4] To be published

[5] To be published

BSI —British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

Details and advice can be obtained from the Copyright & Licensing Manager. Tel: +44 (0)20 8996 7070. Fax: +44 (0)20 8996 7553. Email: copyright@bsi-global.com.

BSI
389 Chiswick High Road
London
W4 4AL