

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Safety of machinery – Electro-sensitive protective equipment –
Part 1: General requirements and tests**

**Sécurité des machines – Equipements de protection électro-sensibles –
Partie 1: Prescriptions générales et essais**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2008 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch

Tel.: +41 22 919 02 11

Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,...). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

Email: csc@iec.ch

Tél.: +41 22 919 02 11

Fax: +41 22 919 03 00



IEC 61496-1

Edition 2.1 2008-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Safety of machinery – Electro-sensitive protective equipment –
Part 1: General requirements and tests**

**Sécurité des machines – Equipements de protection électro-sensibles –
Partie 1: Prescriptions générales et essais**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

CQ

ICS 13.110; 29.260.99

ISBN 2-8318-9374-7

CONTENTS

INTRODUCTION.....	5
1 Scope.....	6
2 Normative references	6
3 Terms and definitions	8
4 Functional, design and environmental requirements	12
4.1 Functional requirements	12
4.2 Design requirements	13
4.3 Environmental requirements	20
5 Testing	24
5.1 General	24
5.2 Functional tests	26
5.3 Performance testing under fault conditions	29
5.4 Environmental tests	30
5.5 Validation of programmable or complex integrated circuits	33
6 Marking for identification and for safe use	35
6.1 General	35
6.2 ESPE supplied from a dedicated power supply	35
6.3 ESPE supplied from an internal electrical power source	35
6.4 Adjustment	36
6.5 Enclosures	36
6.6 Control devices	36
6.7 Terminal markings	36
6.8 Marking durability	37
7 Accompanying documents	37
Annex A (normative) Optional functions of the ESPE	39
Annex B (normative) Catalogue of single faults affecting the electrical equipment of the ESPE, to be applied as specified in 5.3.....	46
Annex C (informative) Conformity assessment	51
Bibliography.....	52
Index	53

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SAFETY OF MACHINERY –
ELECTRO-SENSITIVE PROTECTIVE EQUIPMENT –****Part 1: General requirements and tests**

FOREWORD

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

International Standard IEC 61496-1 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects, in collaboration with CENELEC technical committee 44X: Safety of machinery – Electrotechnical aspects.

This edition constitutes a technical revision. In this edition of this part of IEC 61496, general requirements for a Type 3 ESPE have been added. In addition, several small changes and corrections have been made to clarify the requirements and to align this standard with current practice.

This standard has the status of a product family standard and may be used as a normative reference in a dedicated product standard for the safety of machinery.

This standard has been prepared as a specification of general requirements for electro-sensitive protective equipment (ESPE) specifically related to machinery safety and has been developed to meet the needs of manufacturers, industrial users and safety enforcement authorities.

This consolidated version of IEC 61496-1 consists of the second edition (2004) [documents 44/444/FDIS and 44/445/RVD], its amendment 1 (2007) [documents 44/560/FDIS and 44/568/RVD] and its corrigendum of July 2008.

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

It bears the edition number 2.1.

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

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

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

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

INTRODUCTION

An electro-sensitive protective equipment (ESPE) is applied to machinery presenting a risk of personal injury. It provides protection by causing the machine to revert to a safe condition before a person can be placed in a hazardous situation.

This part of IEC 61496 provides general design and performance requirements of ESPEs for use over a broad range of applications. Essential features of equipment meeting the requirements of this standard are the appropriate level of safety-related performance provided and the built-in periodic functional checks/self-checks that are specified to ensure that this level of performance is maintained.

Each type of machine presents its own particular hazards and it is not the purpose of this standard to recommend the manner of application of the ESPE to any particular machine. The application of the ESPE should be a matter for agreement between the equipment supplier, the machine user and the enforcing authority, and in this context attention is drawn to the relevant guidance established internationally, for example ISO TR 12100.

This part of IEC 61496 specifies technical requirements of electro-sensitive protective equipment. The application of this standard may require the use of substances and/or test procedures that could be injurious to health unless adequate precautions are taken. Conformance with this standard in no way absolves either the supplier or the user from statutory obligations relating to the safety and health of persons during the use of the equipment covered by this standard.

SAFETY OF MACHINERY – ELECTRO-SENSITIVE PROTECTIVE EQUIPMENT –

Part 1: General requirements and tests

1 Scope

This part of IEC 61496 specifies general requirements for the design, construction and testing of non-contact electro-sensitive protective equipment (ESPE) designed specifically to detect persons as part of a safety related system. Special attention is directed to functional and design requirements that ensure an appropriate safety-related performance is achieved. An ESPE may include optional safety-related functions, the requirements for which are given in Annex A.

The particular requirements for specific types of sensing function are given in other parts of this standard.

This standard does not specify the dimensions or configuration of the detection zone and its disposition in relation to hazards in any particular application, nor what constitutes a hazardous state of any machine. It is restricted to the functioning of the ESPE and how it interfaces with the machine.

While a data interface can be used to control optional safety-related ESPE functions (Annex A), this standard does not provide specific requirements. Requirements for these safety-related functions can be determined by consulting other standards (for example, IEC 61508, IEC/TS 62046, IEC 62061, and ISO13849-1).

This standard may be relevant to applications other than those for the protection of persons, for example for the protection of machinery or products from mechanical damage. In those applications, different requirements can be necessary, for example when the materials that have to be recognized by the sensing function have different properties from those of persons.

This standard does not deal with electromagnetic compatibility (EMC) emission requirements.

2 Normative references

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

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

IEC 60068-2-6:1995, *Environmental testing – Part 2: Tests – Test Fc: Vibration (sinusoidal)*

IEC 60068-2-29:1987, *Basic environmental testing procedures – Part 2: Tests – Test Eb and guidance: Bump*

IEC 60204-1:1997, *Safety of machinery – Electrical equipment of industrial machines – Part 1: General requirements*

IEC 60249-2, *Base materials for printed circuits – Part 2: Specifications*

IEC 60439-1:1999, *Low-voltage switchgear and controlgear assemblies – Part 1: Type-tested and partially type-tested assemblies*

IEC 60445:1999, *Basic and safety principles for man-machine interface, marking and identification – Identification of equipment terminals and of terminations of certain designated conductors, including general rules for an alphanumeric system*

IEC 60447:1993, *Man-machine interface (MMI) – Actuating principles*

IEC 60529:2001, *Degrees of protection provided by enclosures (IP code)*

IEC 60664-1:1992, *Insulation coordination for equipment within low-voltage systems – Part 1: Principles, requirements and tests*

IEC 60947-5-1:1997, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

IEC 60950 (all parts), *Information technology equipment – Safety*

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

IEC 61000-4-3:2002, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated radio-frequency, electromagnetic field immunity test – Basic EMC publication*

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

IEC 61000-4-5:2001, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity tests – Basic EMC publication*

IEC 61000-4-6:2001, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields – Basic EMC publication*

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

IEC 61131-2:1992, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

ISO 9001:2000, *Quality management systems – Requirements*

ISO/TR 12100-1:1992, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology*

ISO/TR 12100-2:1992, *Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles and specifications*

ISO 13849-1:1999, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

3 Terms and definitions

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

NOTE The index lists, in alphabetical order, the terms and acronyms defined in this Clause and indicates where they are used in the text of this part.

3.1

blanking

optional function that permits an object of a size greater than the detection capability of the ESPE to be located within the detection zone without causing an OFF-state of the OSSD(s)

NOTE 1 Fixed blanking is a technique wherein the locations of the blanked areas of the detection zone do not change during operation. The detection capability of the other parts of the detection zone remain unchanged.

NOTE 2 Floating blanking is a technique wherein the blanked area of the detection zone follows the location of a moving object(s) during operation. The detection capability of the other areas remains unchanged.

3.2

controlling/monitoring device

part of the electro-sensitive protective equipment (ESPE) that:

- receives and processes information from the sensing device and provides signals to the output signal switching devices (OSSD),
- monitors the sensing device and the OSSD

3.3

detection capability

sensing function parameter limit specified by the supplier that will cause actuation of the electro-sensitive protective equipment (ESPE)

3.4

detection zone

zone within which a specified test piece will be detected by the electro-sensitive protective equipment (ESPE)

3.5

electro-sensitive protective equipment

ESPE

assembly of devices and/or components working together for protective tripping or presence-sensing purposes and comprising as a minimum

- a sensing device;
- controlling/monitoring devices;
- output signal switching devices and/or a safety-related data interface

NOTE 1 The safety-related control system associated with the ESPE, or the ESPE itself, may further include a secondary switching device, muting functions, stopping performance monitor, etc. (see Annex A).

NOTE 2 A safety-related communication interface can be integrated in the same enclosure as the ESPE.

3.6

external device monitoring (EDM)

means by which the electro-sensitive protective equipment (ESPE) monitors the state of control devices which are external to the ESPE

3.7

failure

termination of the ability of an item to perform a required function
[IEV 191-04-01, modified]

NOTE 1 After failure the item has a fault.

NOTE 2 'Failure' is an event, as distinguished from 'fault', which is a state.

NOTE 3 This concept, as defined, does not apply to items consisting of software only.

NOTE 4 In practice, the terms fault and failure are often used synonymously.

3.8

failure to danger

failure which prevents or delays all output signal switching devices going to, and/or remaining in the OFF-state in response to a condition which, in normal operation, would result in their so doing

3.9

fault

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

NOTE 2 In English the term "fault" and its definition are identical with those given in IEC 191-05-01. In the field of machinery, the French term "défaut" and the German term "Fehler" are used rather than the terms "panne" and "Fehlzustand" that appear with this definition.

3.10

final switching device

FSD

component of the machine's safety-related control system that interrupts the circuit to the machine primary control element (MPCE) when the output signal switching device (OSSD) goes to the OFF-state

3.11

integrated circuit – complex or programmable

monolithic, hybrid or module circuit which satisfies one or more of the criteria below:

- a) more than 1 000 gates are used in the digital mode,
- b) more than 24 functionally different external electrical connections are available for use;
- c) the functions can be programmed

NOTE 1 Examples include ASICs, ROMs, PROMs, EPROMs, PALs, CPUs, PLAs, and PLDs.

NOTE 2 The circuits may function in the analogue mode, the digital mode, or a combination of the two modes.

3.12

integrated circuit – simple

monolithic, hybrid or module circuit which satisfies none of the criteria in 3.11

NOTE 1 Examples are SSI or MSI logic ICs, comparators.

NOTE 2 The circuits may function in the analogue mode, in the digital mode, or in a combination of the two modes.

3.13

lock-out condition

condition, initiated by a fault, preventing normal operation of the electro-sensitive protective equipment (ESPE). All output signal switching devices (OSSDs) and, where applicable, all secondary switching devices (SSDs) are signalled to go to the OFF-state

3.14 **machine primary control element** **MPCE**

electrically powered element that directly controls the normal operation of a machine in such a way that it is the last element (in time) to function when machine operation is to be initiated or arrested

NOTE This element can be, for example, a mains contactor, a magnetic clutch or an electrically operated hydraulic valve.

3.15 **machine secondary control element** **MSCE**

machine control element, independent of the machine primary control element(s), that is capable of removing the source of power from the prime mover of the relevant hazardous parts

NOTE 1 When fitted, the MSCE is normally controlled by the secondary switching device (SSD).

NOTE 2 This element can be, for example, a mains contactor, a magnetic clutch or an electrically operated hydraulic valve.

3.16 **muting**

temporary automatic suspension of a safety function(s) by safety-related parts of the control system

NOTE For ESPE-muting, see Clause A.7.

3.17 **OFF-state**

state of the output(s) of the ESPE in which the machine under control is caused to stop running and is prevented from starting (for example, the output circuit is interrupted and disables the flow of current)

3.18 **ON-state**

state of the output(s) of the ESPE in which the machine under control is allowed to run (for example, the output circuit is complete and enables the flow of current)

3.19 **output signal switching device** **OSSD**

component of the electro-sensitive protective equipment (ESPE) connected to the machine control system which, when the sensing device is actuated during normal operation, responds by going to the OFF-state

3.20 **overall system stopping performance**

time interval resulting from the sum of the electro-sensitive protective equipment (ESPE) response time and the time to the cessation of hazardous machine operation

3.21 **response time**

maximum time between the occurrence of the event leading to the actuation of the sensing device and the output signal switching devices (OSSD) achieving the OFF-state

NOTE 1 When an ESPE includes a safety-related data interface, the response time is defined at the output of the safety-related data interface.

NOTE 2 When a safety-related communication interface is included in the ESPE enclosure, then the response time is defined at the output of the safety-related communication interface. In this case, the response time is also dependent on the protocol and architecture of the communication network.

NOTE 3 If an ESPE has both a safety-related data interface and OSSDs, the ESPE can have a different response time for the safety-related data interface and for the OSSDs.

3.22**restart interlock**

means of preventing automatic restarting of a machine after actuation of the sensing device during a hazardous part of the machine operating cycle, after a change in mode of operation of the machine, and after a change in the means of start control of the machine

NOTE Modes of operation include inch, single stroke, automatic. Means of start control include foot switch, two-hand control, and single or double actuation of the electro-sensitive protection equipment (ESPE) sensing device.

3.23**safety-related part of a control system**

part or subpart(s) of a control system which respond(s) to input signals and generate(s) safety-related output signals

NOTE 1 This also includes monitoring systems.

NOTE 2 The combined safety-related parts of a control system start at the points where the safety-related signals are initiated and end at the output of the power control elements (see also ISO/TR 12100-1, Annex A)

3.24**secondary switching device****SSD**

device which, in a lock-out condition goes to the OFF-state. It may be used to initiate an appropriate machine control action, for example de-energizing the machine secondary control element (MSCE)

3.25**sensing device**

part of the electro-sensitive protective equipment (ESPE) which uses electro-sensitive means to determine the event or state that the ESPE is intended to detect

EXAMPLE An opto-electronic sensing device would detect an opaque object entering the detection zone.

3.26**start interlock**

means which prevents an automatic machine start when the electrical supply to the electro-sensitive protection equipment (ESPE) is switched on, or is interrupted and restored

3.27**stopping performance monitor****SPM**

monitoring means to determine whether or not the overall system stopping performance is within the preset limit(s)

3.28**supplier**

entity (for example manufacturer, contractor, installer, integrator) that provides equipment or services associated with the machine

NOTE The user may act in the capacity of a supplier to himself.

3.29**safety-related data interface**

direct connection (peer-to-peer) interface between the output of the ESPE and the safety-related communication interface that is used to represent the status of the OSSD(s)

NOTE 1 A data interface will not have addressing capability.

NOTE 2 The safety-related data interface can be bi-directional.

3.30

safety-related communication interface

safety-related connection to a standardized communication network intended for safety-related control functions

4 Functional, design and environmental requirements

4.1 Functional requirements

4.1.1 Normal operation

In normal operation, the ESPE shall respond by giving (an) appropriate output signal(s) when part of a person greater than or equal to the detection capability (as specified in the relevant part of IEC 61496) enters or is in the detection zone.

The ESPE response time shall not exceed that stated by the supplier. No means of adjustment of the response time shall be possible without the use of a key, key-word or tool.

4.1.2 Sensing function

The detection capability shall be effective over the detection zone specified by the supplier. No adjustment of the detection zone, detection capability or blanking function (monitored, unmonitored, fixed or floating) shall be possible without the use of a key, key-word or tool.

4.1.3 Types of ESPE

In this standard, three types of ESPEs are considered. The types differ in their performance in the presence of faults and under influences from environmental conditions. In this part, the effects of electrical and electromechanical faults are considered (such faults are listed in Annex B). Additional requirements are provided in the other parts where faults generated by the particular sensing technology employed are considered. It is the responsibility of the machine manufacturer and/or the user to prescribe which type is required for a particular application.

NOTE Requirements for a type 1 ESPE are not being considered at this time.

A type 2 ESPE shall fulfil the fault detection requirements of 4.2.2.3.

For a type 2 ESPE, in normal operation the output circuit of at least one output signal switching device shall go to the OFF-state when the sensing function is actuated, or when power is removed from the ESPE.

A type 2 ESPE shall have a means of periodic test.

A type 3 ESPE shall fulfil the fault detection requirements of 4.2.2.4.

A type 4 ESPE shall fulfil the fault detection requirements of 4.2.2.5.

For a type 3 ESPE and for a type 4 ESPE, in normal operation the output circuit of at least two output signal switching devices shall go to the OFF-state when the sensing function is actuated, or when power is removed from the ESPE.

When a single safety-related data interface is used to perform the functions of the OSSD(s), then the data interface and associated safety-related communication interface shall meet the requirements of 4.2.4.4. In this case, a single safety-related data interface can substitute for two OSSDs in a type 3 or type 4 ESPE.

4.2 Design requirements

4.2.1 Electrical supply

The ESPE shall be designed to operate correctly with the conditions of the nominal supply as specified below, unless otherwise specified by the user:

AC supplies

Voltage: 0,85 to 1,1 of nominal voltage

Frequency: 0,99 to 1,01 of nominal frequency (continuously)

0,98 to 1,02 of nominal frequency (short-time)

Harmonics: Harmonic distortion not to exceed 10 % of the total r.m.s. voltage between live conductors for the sum of the 2nd through to the 5th harmonic. An additional 2 % of the total r.m.s. voltage between live conductors for the sum of the 6th through to the 30th harmonic is permissible.

DC supplies

From batteries

Voltage: 0,85 to 1,15 of nominal voltage

0,7 to 1,2 of nominal voltage in the case of battery-operated vehicles

From converting equipment

Voltage: 0,9 to 1,1 of nominal voltage

Ripple (peak-to-peak): Shall not exceed 0,05 of nominal voltage.

For protection against electric shock, see 4.2.3.2.

NOTE For protection against electrical interference, the power source should meet the requirements of IEC 61000-6-2.

4.2.2 Fault detection requirements

4.2.2.1 General

The ESPE shall respond to the faults listed in Annex B, in accordance with 4.2.2.3 to 4.2.2.5 as appropriate. It shall not be possible for the ESPE to achieve a reset from a lock-out condition by interruption and restoration of the mains power supply when the fault which initiated the lock-out condition is still present. At power on and prior to OSSD(s) going to the ON-state, a test shall be performed to verify the absence of internal faults within the ESPE.

When an ESPE uses a safety-related communication interface to perform the OSSD functions, the fault-detection requirements in 4.2.2.3 to 4.2.2.5 can be modified to include requirements given in IEC 62061/IEC 61508 in accordance with the appropriate SIL (for example, SIL 3 for Type 4, SIL 2 for Type 3 and SIL 1 for Type 2).

4.2.2.2 Particular requirements for a type 1 ESPE

NOTE Particular requirements for a type 1 ESPE are not under consideration at this time.

4.2.2.3 Particular requirements for a type 2 ESPE

A type 2 ESPE shall have an means of periodic test to reveal a failure to danger (for example loss of detection capability, response time exceeding that specified).

A single fault resulting in the loss of detection capability or the increase in response time beyond the specified time or preventing one or more of the OSSDs going to the OFF-state, shall result in a lock-out condition as a result of the next periodic test.

Where the periodic test is intended to be initiated by an external (for example machine) safety-related control system, the ESPE shall be provided with suitable input facilities (for example terminals).

The duration of the periodic test shall be such that the intended safety function is not impaired.

NOTE If the type 2 ESPE is intended for use as a trip device (for example when used as a perimeter guard), and the duration of the periodic test is greater than 150 ms, it is possible for a person to pass through the detection zone without being detected. In this case a restart interlock should be included.

If the periodic test is automatically initiated, the correct functioning of the periodic test shall be monitored and a single fault in the parts implementing the monitoring function shall be detected. In the event of a fault, the OSSD(s) shall be signalled to go to the OFF-state.

If one or more OSSDs does not go to the OFF-state, a lock-out condition shall be initiated.

An ESPE with only one OSSD shall have a minimum of one SSD (see Clause A.4).

4.2.2.4 Particular requirements for a type 3 ESPE

A single fault resulting in a loss of detection capability or an increase in response time beyond the specified value or a single fault preventing one or more OSSD going to the OFF-state shall cause the ESPE to go to a lock-out condition within a time specified in the relevant part of this standard, or immediately upon any of the following demand events where fault detection requires a change in state:

- on actuation of the sensing function;
- on reset of the start or restart interlock, if available (see Clauses A.5 and A.6).

In cases where a single fault which in itself does not cause a failure to danger is not detected, the occurrence of one additional fault shall not cause a failure to danger. For verification of this requirement, see 5.3.4.

4.2.2.5 Particular requirements for a type 4 ESPE

A single fault resulting in a loss of detection capability shall cause the ESPE to go to a lock-out condition within the response time.

A single fault resulting in an increase in response time beyond the specified value or a single fault preventing one or more than one OSSD going to the OFF-state, shall cause the ESPE to go to a lock-out condition immediately, i.e. within the response time, or immediately upon any of the following demand events where fault detection requires a change of state:

- on actuation of the sensing function;
- on reset of the start or restart interlock, if available (see Clauses A.5 and A.6).

In cases where a single fault which in itself does not cause a failure to danger is not detected, the occurrence of further faults shall not cause a failure to danger. For verification of this requirement, see 5.3.5.

NOTE 1 Design measures for a type 4 ESPE may include:

- single-channel technique with dynamic fault detection measures; or
- single-channel technique with an internally generated automatic check, performed frequently so that the automatic check interval for fault detection is included in the safety device response time; and
- multiple channel techniques such that any disparity between channels results in a lock-out condition.

NOTE 2 For additional requirements for integrated circuits, complex or programmable, see 4.2.10.

4.2.3 Electrical equipment of the ESPE

4.2.3.1 General

The electrical equipment (components) of the ESPE shall:

- conform to appropriate IEC standards where they exist;
- be suitable for the intended use; and
- be operated within their specified ratings.

4.2.3.2 Protection against electric shock

Protection against electric shock shall be provided in accordance with 6.1 of IEC 60204-1.

4.2.3.3 Protection of electrical equipment

Overcurrent protection shall be provided in accordance with 7.2.1, 7.2.3, 7.2.7, 7.2.8, and 7.2.9 of IEC 60204-1.

NOTE Information may need to be given to the user of the ESPE as to the maximum rating of fuses, or setting of an overcurrent protective device for the circuit(s) connected to the OSSD(s) output connection points.

4.2.3.4 Pollution degree

The electrical equipment shall be suitable for pollution degree 2 (see 6.1.2.3 of IEC 60439-1).

4.2.3.5 Clearance, creepage distances and isolating distances

The electrical equipment shall be designed and constructed in accordance with 7.1.2 of IEC 60439-1.

4.2.3.6 Wiring

The electrical equipment shall be wired in accordance with 7.8.3 of IEC 60439-1.

4.2.4 Output signal switching devices (OSSD)

4.2.4.1 General

Separate output connection points (terminals) shall be provided for each OSSD.

The OSSD should be so rated that their loads can be switched without the use of arc suppression devices.

NOTE In the interest of improved reliability, it is strongly recommended that switching voltage-suppression devices are fitted, which should be connected across the loads and not across the contacts.

The output circuit of the OSSDs should be adequately protected to prevent failure to danger, for example welded contacts under overcurrent conditions (see 7.2.9 of IEC 60204-1).

Measures should be provided to minimize the possibility of failure to danger from common cause failures.

Some functions of the machine safety-related control system may be performed by the ESPE, for example the OSSD may perform the function of a FSD.

Both a type 3 ESPE and a type 4 ESPE shall incorporate a minimum of two independently operated OSSDs.

A reference to an OSSD action (for example, go to the OFF-state) will also mean a corresponding action of a safety-related data interface. A single safety-related data interface can meet the requirements of having two OSSDs.

4.2.4.2 Relay OSSDs

If relay OSSDs are provided, the state (i.e. position) of the contacts shall be monitored. This can be achieved by monitoring the state of an auxiliary contact(s) on relays with mechanically linked (positively guided) contacts. The mechanical link ensures that the monitored contact follows the change of state of the OSSD contact(s).

Special design and constructional measures shall be used to ensure that the make (normally-open) contact(s) and the break (normally-closed) contact(s) cannot be in the closed position simultaneously.

NOTE 1 The mechanical link ensures that the monitored contact follows the change of state of the OSSD contact(s).

NOTE 2 It is important that relay drop out voltage and the separation distance between the contacts are maintained at a proper level over the entire stated life of the relay.

4.2.4.3 Solid state OSSDs

Solid state OSSD outputs may be either current sourcing or current sinking types. When current sourcing outputs are provided, they shall meet the requirements of this Subclause.

NOTE 1 Requirements for current sinking outputs which may be required for certain applications are not defined in this standard. Special care should be exercised in their use (when current sinking outputs are used, a short-circuit to the reference potential or an open circuit will be interpreted by the inputs and loads as the ON-state). The requirements of IEC 60204-1, 9.1.4 should also be considered.

NOTE 2 For a nominal rated supply voltage of 24 V d.c., the output voltage and current values for the ON-state and the OFF-state should be in accordance with the following Table:

Nominal supply voltage	Output range OFF-state	Output range ON-state	Output OFF-state (max. leakage current)	Output ON-state
24 V d.c.	-3 V ... +2 V r.m.s. (+5 V peak)	+11 V ... +30 V	< 2 mA	> 6 mA

NOTE 3 The values in the Table above meet the requirements of IEC 61131-2 (see 3.3 of IEC 61131-2), for a nominal rated supply voltage of 24 V d.c. When other supply voltages are used, this standard may be used as a guide. IEC 61131-2 may be referred to for additional information.

The output(s) shall be protected against the effects of overvoltage, overcurrent and short circuit.

The maximum leakage current shall not exceed 2 mA, including in the case of faults (for example an open circuit).

When there is more than one OSSD, short circuits between the outputs of the OSSDs shall be detected.

The supplier of the ESPE shall provide the following information in the accompanying documents:

- nominal and maximum output current in the ON-state for resistive and inductive loads;
- maximum OFF-state voltage;
- maximum output current in OFF-state (leakage current);
- maximum capacitive load;
- maximum resistance of the connection(s) between the OSSD(s) and the load(s).

4.2.4.4 Safety-related data interface and safety-related communication interface

When the sensing device is actuated during normal operation, the ESPE shall respond by sending information indicating the status of the sensing device or ESPE through a safety-related data interface. The status information is converted to a data telegram by a safety-related communication interface.

The safety-related data interface shall have the same protection against faults as is appropriate for the type of ESPE.

Depending on the ESPE design, the safety-related communication interface can either be external in a separate enclosure (Figure 1a) or it can be integrated in the same enclosure of the ESPE (Figure 1b).

The safety-related communication interface shall meet the relevant requirements of IEC 62061/IEC 61508 for an appropriate SIL (for example, SIL 3 for Type 4, SIL 2 for Type 3 and SIL 1 for Type 2) in addition to the requirements of this standard (IEC 61496-1).

When the safety-related communication interface is integrated in the ESPE, the entire ESPE shall meet the relevant requirements of IEC 62061/IEC 61508.

NOTE Because of the specific technology of communication interfaces, different standards from IEC 61496-1 apply. To avoid overlapping with other standards, functional requirements for the safety-related communication interface are not defined in this standard.

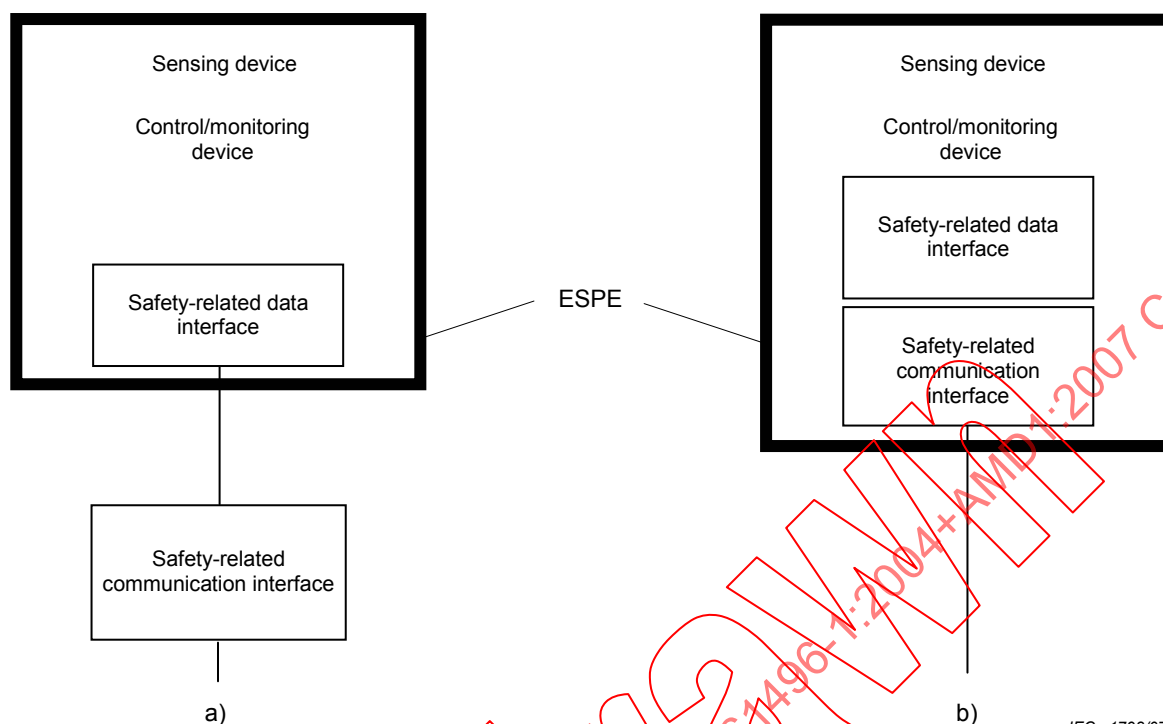


Figure 1 – Examples of ESPEs using safety-related communication interfaces

4.2.5 Indicator lights and displays

Devices shall be provided by the ESPE manufacturer to:

- indicate the actuation of the sensing device. Neither the time from the actuation of the sensing device to the indicator achieving 50 % of its final brightness (luminescence), nor the time from the de-actuation of the sensing device to the indicator brightness decaying to 50 % of its initial brightness, shall exceed 100 ms;
- indicate the output status of an OSSD. The ON-state shall be represented by a green indicator, the OFF-state by a red indicator. When two or more OSSDs are intended to operate in co-ordination, a single set of indicators may be shared.

When there are two or more indicators of the same colour, the function of each indicator shall be unambiguously marked.

NOTE For some modes of operation, the same set of indicators for a) can also be used for b).

The indicators are intended for the machine operator. Therefore they shall be capable of being located near the detection zone and visible when the equipment is installed. They can be integrated in the sensor elements or as an external equipment installed near by the detection zone.

4.2.6 Adjustment means

All adjustment means shall be so designed that a failure to danger is not possible at any point in the range of adjustment. A failure in the adjustment means shall not cause an unintended change to the configuration of the ESPE.

4.2.7 Disconnection of subsystems

When means are provided to permit disconnection of any subsystem, part of a subsystem or any plug-in component, such disconnection shall result in at least one OSSD going to the OFF-state, in accordance with 4.2.2.

4.2.8 Non-electrical components

Non-electrical components shall be suitable for the intended use.

4.2.9 Common cause failures

The design should be such as to minimize the possibility of a failure to danger from common cause failures arising from:

- environmental influences;
- multichannel systems using a common substrate;
- short circuits between channels of multichannel systems.

NOTE 1 Common cause failures can also result from the use of components degraded by mishandling, faulty manufacture, etc.

NOTE 2 Common cause failures are treated as a single failure.

None of the components in a common semi-conductor substrate shall be used for more than one channel of a multi-channel system.

4.2.10 Programmable or complex integrated circuits

Where programmable or complex integrated circuits are used in a type 4 ESPE, the safety-related performance shall be maintained by at least two independent controlling/monitoring channels. This requirement shall be verified in accordance with 5.5.

4.2.11 Software, programming, functional design of integrated circuits

4.2.11.1 General

Where an ESPE implements its safety-related performance by any of the following means, the additional requirements of 4.2.11.2 shall apply:

- a) a software program(s) executed during operation;
- b) a programmed device(s), the functions of which were set by a process subsequent to its original manufacture, for example PAL, PLA, PLD, PROM;
- c) a device(s) manufactured to a specific user functional specification, for example ASIC, mask programmed microprocessor, ROM.

Conformance to these requirements shall be validated in accordance with 5.5.

4.2.11.2 Requirements

- a) The software, device programme and the device function design shall be developed in accordance with IEC 61508-3 for the appropriate SIL (for example, SIL3 for Type 4, SIL2 for Type 3 or SIL1 for Type 2).
- b) Documentary evidence shall be available under the quality management system procedures to demonstrate that the required level of safety-related performance has been achieved.
- c) A documented quality plan, clearly identifying the stages of development, and setting out the acceptance criteria for each stage, shall be produced. Examples of development stages are requirements specification, design specification, verification, and validation.

- d) Prior to any development, the conceptual design of the ESPE shall be analysed for the identification of hazards and failure modes, in order to identify, in a safety requirements specification, the ESPE safety-related functions. Some or all of the ESPE safety-related functions shall then be allocated to the means in 4.2.11, and the required safety-related performance for each element shall be determined. Suitable engineering techniques for specification, design, implementation and maintenance shall be adopted to achieve the required safety-related performance.
- e) The requirements for software, program design, and functional design, for each part relevant to 4.2.11.1 shall be complete and unambiguous. Each requirements specification shall enable an assessor or validator (i.e. a person other than the designer) to trace back readily to the safety requirements specification to confirm that the required safety-related functions are adequately addressed.
- f) A comprehensive test plan shall be devised in order to demonstrate that the design is a correct implementation of the safety-related functions required by the safety requirements specification. The test of software, program, and functional specification, shall be documented in the project records as evidence that the design satisfies the safety requirements specification.
- g) The software, program design, and functional specification design, shall be subject to effective configuration management and change control. During development, effective procedures shall confirm that changes in requirements, specification, design, etc. are adequately documented and that the impact of all changes is analysed to confirm that the safety requirements specification remains traceable through all stages of the design process. The design shall be protected from unauthorized change, and its precise configuration (for example list of modules, version number) shall be recorded accurately.
- h) Where a software program is executed during operation of the ESPE, the entire operational instruction software shall be contained in read-only memory which cannot be overwritten by the processor. Appropriate techniques shall be included to monitor correct program flow, and to confirm the integrity of the software.
Such techniques can include a watchdog, RAM/ROM checks, CPU tests, etc.
- i) Where software tools such as compilers or translators (but not assemblers) are used to develop software, software diversity shall not be considered to be present unless:
 - the software tools used for the diverse programs are entirely unrelated; or
 - the software tool(s) has a “certificate of validation” to a recognized national/international standard; or
 - the test plan incorporates adequate measures to detect common cause errors introduced by the software tool.
- j) As a principle of design, the safety-related software should be isolated, as far as is practicable, from non-safety-related software in order to minimize the possibility of corruption of the safety functions, and to assist the task of assessing the safety performance.

4.3 Environmental requirements

4.3.1 Ambient air temperature range and humidity

The ESPE shall comply with the requirements of this standard when subjected to ambient temperature variations from 0 °C to 50 °C. Where it is intended for use outside this range, the supplier shall specify the temperature range over which the system will continue normal operation. Compliance with this requirement shall be verified by the tests specified in 5.4.2 at a non-condensing humidity of 95 % for temperatures between 20 °C and the highest ambient temperature according to 5.4.2.

4.3.2 Electrical disturbances

4.3.2.1 Supply voltage variations

The ESPE shall not fail to danger when the external supply voltage is reduced steadily and continuously from the nominal voltage to zero voltage, over a period of 10 s to 20 s, and then increased in a similar manner from zero voltage to the nominal voltage.

The ESPE shall not fail to danger when each internally derived supply voltage, in turn, is varied steadily and continuously over a period of 10 s to 20 s, from nominal voltage to zero voltage, and then increased in a similar manner from zero voltage to nominal voltage.

4.3.2.2 Supply voltage interruptions

When supply voltage interruptions (dips) are applied as in Table 1:

Table 1 – Supply voltage interruptions

Test number	Dip value of rated voltage	Dip time	Dip repetition rate
	%	ms	Hz
1)	100	10	10
2)	50	20	5
3)	50	500	0,2

the ESPE shall respond to test 1) and to test 2) by continuing in normal operation, and to test 3) by not failing to danger.

When the ESPE is designed to be supplied from a specific type of power supply(s) (for example, supplied direct from a safety-related communication interface), the supply interruptions in this clause may be applied to the primary input of the specified power supply instead of direct to the ESPE.

4.3.2.3 Fast transient/burst

4.3.2.3.1 General requirements

The ESPE shall continue in normal operation when subjected to fast transient/burst in accordance with IEC 61000-4-4:

Ports for power lines for less than 50 V a.c. or d.c. Ports for signal lines, etc. with a length exceeding 1 m	1 kV (peak) according to test severity level 2 of IEC 61000-4-4
Ports for power lines for 50 V a.c. and above	2 kV (peak) according to test severity level 3 of IEC 61000-4-4

4.3.2.3.2 Additional requirements

A type 3 ESPE and a type 4 ESPE shall not fail to danger when subjected to fast transient/burst in accordance with IEC 61000-4-4:

Ports for power lines for d.c. and for less than 50 V a.c. Ports for signal lines, etc. with a length exceeding 1 m	2 kV (peak) according to test severity level 3 of IEC 61000-4-4
Ports for power lines for 50 V a.c. and above	4 kV (peak) according to test severity level 4 of IEC 61000-4-4

4.3.2.4 Fast transient/surge

4.3.2.4.1 General requirements

The ESPE shall continue in normal operation when subjected to surge in accordance with IEC 61000-4-5:

Ports for signal lines with a length exceeding 1 m Power ports for d.c. and for less than 50 V a.c.	1 kV (peak) common mode according to test severity level 2 of IEC 61000-4-5
Ports for power lines for 50 V a.c. and above	2 kV (peak) common mode and 1 kV (peak) differential mode according to test severity level 3 of IEC 61000-4-5

4.3.2.4.2 Additional requirements

A type 3 ESPE and a type 4 ESPE shall not fail to danger when subjected to fast transient/surge in accordance with IEC 61000-4-5:

Ports for signal lines with a length exceeding 1 m Power ports for d.c. and for less than 50 V a.c.	2 kV (peak) common mode according to test severity level 3 of IEC 61000-4-5
Power ports for 50 V a.c. and above	4 kV (peak) common mode and 2 kV (peak) differential mode according to test severity level 4 of IEC 61000-4-5

4.3.2.5 Electromagnetic field

4.3.2.5.1 General requirements

The ESPE shall continue in normal operation when subjected to an electromagnetic field in accordance with 5.1 of IEC 61000-4-3:

10 V/m according to test severity level 3.

4.3.2.5.2 Additional requirements

A type 3 and a type 4 ESPE shall not fail to danger when subjected to an electromagnetic field in accordance with 5.2 of IEC 61000-4-3:

30 V/m according to test severity level 4.

4.3.2.6 Conducted disturbances induced by radio-frequency fields

4.3.2.6.1 General requirements

The ESPE shall continue in normal operation when subjected to conducted radio-frequency disturbances in accordance with IEC 61000-4-6:

Ports for signal lines, etc. with a length of 1 m to 10 m	3 V (r.m.s.) according to test severity level 2 of IEC 61000-4-6
Ports for signal lines with a length exceeding 10 m Power ports. Earth ports	10 V (r.m.s.) according to test severity level 3 of IEC 61000-4-6

4.3.2.6.2 Additional requirements

A type 3 ESPE and a type 4 ESPE shall not fail to danger when subjected to conducted radio-frequency disturbances in accordance with IEC 61000-4-6:

Ports for signal lines, etc. with a length of 1 m to 10 m	10 V (r.m.s.) according to test severity level 3 of IEC 61000-4-6
Ports for signal lines with a length exceeding 10 m Power ports. Earth ports	30 V (r.m.s.) according to test severity level X of IEC 61000-4-6

4.3.2.7 Electrostatic discharge

4.3.2.7.1 General requirements

The ESPE shall continue in normal operation when subjected to an electrostatic discharge in accordance with IEC 61000-4-2:

6 kV contact or 8 kV air discharge,
according to test severity level 3 of IEC 61000-4-2.

4.3.2.7.2 Additional requirements

A type 3 ESPE and a type 4 ESPE shall not fail to danger when subjected to an electrostatic discharge in accordance with IEC 61000-4-2:

8 kV contact or 15 kV air discharge,
to test severity level 4 of IEC 61000-4-2.

4.3.3 Mechanical environment

4.3.3.1 Vibration

The ESPE shall be capable of continuing in normal operation during the vibration tests of 5.4.4.1.

4.3.3.2 Bump

The ESPE shall be capable of continuing in normal operation during the bump tests of 5.4.4.2.

4.3.4 Enclosures

The ESPE shall have its own enclosure(s).

All enclosures of the ESPE, including those mounted remotely, shall provide a degree of protection of at least IP54 (see IEC 60529), when mounted as specified by the supplier. However, when mounted in a machine controlgear enclosure having a degree of protection of at least IP54, the ESPE enclosure shall have a degree of protection of at least IP20.

NOTE Protection against mechanical damage can be achieved by:

- a suitable location;
- the use of suitable materials and form of construction providing adequate strength; or
- the use of a protective barrier.

The method of cable entry for incoming cables shall not impair the degree of protection.

Sealing compounds which adhere to the two surfaces being joined, such that the environmental protection is degraded when the joint is separated, shall not be used to seal covers which might be removed for service access.

Enclosures shall be free from sharp edges or corners capable of causing damage to cable insulation. Compliance shall be checked by inspection.

Enclosures shall provide adequate access to enable any necessary adjustments and maintenance work to be carried out safely and effectively. The covers enabling such access shall have captive fasteners.

5 Testing

5.1 General

5.1.1 Type tests

5.1.1.1 Test samples

In so far as it is practicable, all parts of an ESPE shall be tested together. Where this is not practicable, parts of the ESPE may be tested separately. Examples of such situations include integrated ESPEs (ESPEs integrated in, and normally not separable from machinery) in the case of environmental tests. In such cases:

- any input signals necessary for the operation of the ESPE shall be simulated;
- these exceptions and any omissions of tests shall be stated in the test report.

Where a particular test would be destructive and identical results could be obtained by testing part of the ESPE in isolation, a sample of that part may be used instead of the whole equipment sample for the purpose of obtaining the results of the test.

Where the ESPE is designed for operation at a number of different supply voltages (for example for differing applications), more than one sample may be required.

When the ESPE is designed to be supplied from an external dedicated power supply, the ESPE shall undergo testing with the specified dedicated power supply (see 6.2).

5.1.1.2 Operating condition

Unless otherwise stated in the test procedure, the tests shall be carried out with the test sample operating within the conditions specified in the accompanying documents.

For the purposes of electrical disturbance immunity tests, the equipment shall be in as near its final operating configuration as is possible (i.e. with all peripheral devices and covers attached, connected to the power supply and, where applicable, connected to the external protective conductor and/or the external functional bonding conductor (see IEC 60204-1)).

When several mounting positions are specified, the least favourable mounting position shall be used.

Where a safety-related data interface is used in place of an OSSD(s), the ESPE shall be connected to a communication system in accordance with the supplier's instructions that has a means of monitoring the ESPE status.

5.1.1.3 Simulated intrusion into detection zone

In the following tests, introduction of the test piece (as defined in the relevant part of this standard) into the detection zone may be simulated if the method can be shown to be equivalent.

5.1.2 Test conditions

5.1.2.1 Test environment

Except where otherwise specified in 5.4, the tests shall be carried out with the ESPE operated under the following conditions:

- rated voltage (or a voltage within the rated voltage range);
- rated frequency (or a frequency within the rated frequency range);
- ambient temperature: $20\text{ }^{\circ}\text{C} \pm 5\text{ }^{\circ}\text{C}$;
- relative humidity: 25 % to 75 %;
- barometric pressure: 86 kPa to 106 kPa.

NOTE Values stated in the marking and in the accompanying documents are considered as rated values.

5.1.2.2 Measurement accuracy

The errors of measurement shall not exceed:

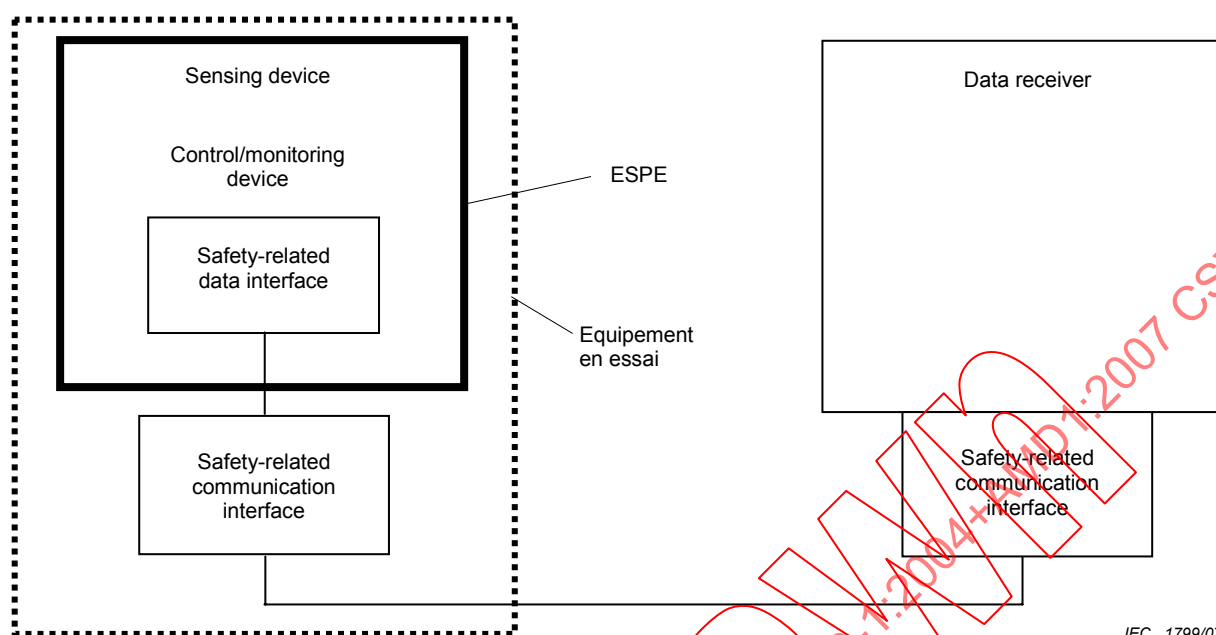
- for measurement of ESPE response time: $\pm 1\text{ ms}$;
- for temperature measurements: $\pm 3\text{ }^{\circ}\text{C}$;
- for electrical measurements: $\pm 1\%$, where technically possible and/or appropriate;
- for relative humidity (RH) measurements: $\pm 3\%$ RH;
- for linear measurements: $\pm 1\text{ mm}$ or $\pm 1\%$, whichever is the greater.

All measurements shall be made after stable temperature conditions have been achieved. This is considered to be fulfilled when the rate of temperature rise or fall is less than 2 K/h.

5.1.2.3 Environmental test conditions for an ESPE intended to be used with a safety-related communication interface

The ESPE and the safety-related communication interface shall be tested together (see Figure 2). Due to the fact that the safety-related communication interface does not show a static output signal, it is necessary to use a data receiver. The test setup consists of the equipment under test and a data receiver (for example, a PLC or monitoring device) which indicates the status of the sensing device or ESPE.

When testing for susceptibility to electrical disturbances, an appropriate test adapter which isolates the ESPE under test from the communication bus may be required.



IEC 1799/07

Figure 2 – Test setup for the EMC test of ESPEs with safety-related communication interfaces

5.1.3 Test results

The results of the tests and analyses listed in this Subclause shall be documented. The test results shall be arranged in a form that shows the details of each individual test and its effects. Details of any special test procedures shall be included in the test report.

NOTE It is recommended that test results are reviewed in accordance with Annex C.

5.2 Functional tests

5.2.1 Sensing function

The sensing function and the integrity of the detection capability and zone (for example size, shape and location) of the ESPE shall be verified as specified in the relevant part of IEC 61496.

5.2.2 Response time

The response time shall be verified by systematic analysis and test.

The response time may be determined by electrical simulation of an actuation, provided that it includes the maximum time between the event triggering the actuation of the sensing device and the actuation.

Additional requirements for the measurement of the response time of the ESPE may be given in the relevant part of IEC 61496.

5.2.3 Limited functional tests

5.2.3.1 General

The following limited functional tests A, B and C shall be performed to verify that under normal environmental conditions the ESPE shall continue normal operation and that, under abnormal environmental conditions or under fault conditions, the ESPE shall not fail to danger.

When an ESPE is fitted with a restart interlock function, that function shall be by-passed or not selected during the performance of the tests. The restart interlock function shall be tested separately (see Annex A).

When using a safety-related communication interface, in the following limited functional tests, OSSDs going to the ON-state or OFF-state are replaced by a safety-related message (for example, a data telegram) indicating the corresponding status of the sensing device or ESPE.

5.2.3.2 Limited functional test A (A test)

With no intrusion in the detection zone, it shall be observed, for a period of at least 5 s, unless otherwise specified, that the OSSD(s) shall be in the ON-state and shall not go to OFF-state.

5.2.3.3 Limited functional test B (B test)

With no intrusion in the detection zone, it shall be observed, for a period of at least 5 s, unless otherwise specified, that the OSSD(s) shall be in the ON-state and shall not go to the OFF-state.

The test piece shall be brought into the detection zone. The OSSD(s) shall respond by going from the ON-state to the OFF-state. It shall be observed that, for a period of at least 5 s unless otherwise specified, the OSSD(s) remain(s) in the OFF-state with the test piece being present in the detection zone, or otherwise staying actuated.

The test piece shall be removed from the detection zone or the sample shall be otherwise deactivated. The OSSD(s) shall respond by going from the OFF-state to the ON-state. It shall be observed that, for a period of at least 5 s unless otherwise specified, the OSSD(s) remain(s) in the ON-state with the test piece not being present in the detection zone, or otherwise staying physically deactivated.

The above tests may need to be repeated continuously depending on test requirements.

5.2.3.4 Limited functional test C (C test)

This test is the same as the limited functional test B but, where the OSSD(s) should be in the ON-state, the OSSD(s) are allowed to be in the OFF-state. No failure to danger shall occur. At the end of each of the relevant tests in 5.4, the ESPE shall continue to operate normally or shall resume normal operation following recovery from a lock-out condition.

If the ESPE cannot resume normal operation due to a permanent component failure, it is acceptable if it is verified that the failure was only in components of the communication interface and that the OSSD(s) remain in the OFF-state.

NOTE Under extreme electrical disturbances (as in the fail-to-danger tests), it is possible that some components of the communication interface will fail permanently and will not allow the ESPE to resume normal operation.

5.2.4 Periodic test

For a type 2 ESPE, the requirements of 4.2.2.3 shall be verified by analysis and measurement.

5.2.5 Indicator lights and displays

The functions and colours of indicator lights and displays shall be verified in accordance with the requirements of 4.2.5 by applying a B test.

5.2.6 Means of adjustment

The requirements of 4.1.1 and 4.1.2 shall be verified by inspection. The requirements of 4.2.6 shall be verified by inspection and by carrying out C tests as necessary.

5.2.7 Rating of components

The operation of each component within its specified ratings, throughout the entire operating range of the ESPE, shall be verified by analysis and/or inspection.

5.2.8 Output signal switching devices (OSSD)

5.2.8.1 General

The provision of separate output connection points (terminals) for each OSSD shall be verified by inspection.

When two OSSDs are provided, verify by inspection or test that the OSSDs are operated independently.

Verify by inspection that the OSSD(s) are protected by current limiting devices or that information for installation of current limiting devices is provided in information for use.

It shall be verified that foreseeable faults will not cause the OSSD(s) to go to or remain in the ON-state. All tests shall be carried out with the maximum inductive load and the maximum length of the connection cable specified by the manufacturer.

Foreseeable faults include:

- short circuit of the OSSD to supply voltage;
- short circuit of the OSSD to ground;
- short circuit between the OSSDs;
- open circuit at the power supply return cable;
- open circuit of the functional bonding conductor;
- open circuit of the screen of a screened cable;
- incorrect wiring.

5.2.8.2 Relay OSSDs

Verify by inspection or tests that the relays meet the requirements of 4.2.4.2.

5.2.8.3 Solid state OSSDs

The output voltage and current levels specified in 4.2.4.3 of this standard shall be verified.

5.2.8.4 Safety-related data interface and safety-related communication interface

It shall be verified by test that disconnection of components does not lead to a failure to danger.

Electrical tests specified in 5.2.8.1 (shorts, opens, improper loading) which would be applied to OSSD(s) may be excluded if not applicable.

The safety integrity of an integrated communication interface shall be verified by tests, systematic analysis and by reference to data sheets and test reports in accordance with the requirements of 4.2.4.4.

5.3 Performance testing under fault conditions

5.3.1 General

Tests for the effects of single faults selected according to 4.2.2 shall be carried out on all the relevant components of the ESPE. If further faults occur as a result of the first single fault, the first and all consequent faults shall be considered as a single fault.

A fault catalogue including all components shall be prepared recording the results of the fault considerations listed in Annex B. In order to reduce unnecessary testing according to 5.3.3, 5.3.4 and 5.3.5 where the results of a single fault or combination of faults can be predicted theoretically, an analysis statement shall be included as part of the test results statement. That statement shall be validated in accordance with 5.5.4. In such cases, only selected (sample) tests need be carried out to confirm such analysis statements.

NOTE 1 Typical methods used for the fault assessment include fault mode and effect analysis (FEMA) according to IEC 60812 and fault tree analysis (FTA) according to IEC 61025.

NOTE 2 In the case of complex circuit structures or components (for example microprocessor, complete redundancy) the review of faults is generally carried out on the structural level. See B.1.2 for exclusion of short circuits on assembled circuit boards. See B.1.3 and B.1.4 for exclusion of short circuits between adjacent terminals for external connection.

5.3.2 Type 1 ESPE

NOTE Requirements for a type 1 ESPE are not being considered at this time.

5.3.3 Type 2 ESPE

The ESPE shall be subjected to single faults to establish that a fault leading to a hazardous condition (for example loss of detection capability or increased response time) is detected by the periodic test function and results in a lock-out condition in accordance with 4.2.2.3.

When internal initiation of the periodic test is provided, it shall be verified that faults in the monitoring function are detected and result in a lock-out condition or cause at least one of the OSSDs to go to the OFF-state.

5.3.4 Type 3 ESPE

The ESPE shall be subjected to single faults to establish that the fault is detected by the ESPE going to a lock-out condition and that no failure to danger occurs, in accordance with 4.2.2.4.

When a single fault is not detected and the analysis specified in 5.3.1 cannot be carried out, the tests for the ESPE going to a lock-out condition and no failure to danger occurring shall be continued with that fault applied first and all other faults added and removed in turn. Tests shall be carried out for all undetected single faults.

Testing for accumulation of more than two faults need not be carried out.

5.3.5 Type 4 ESPE

The ESPE shall be subjected to single faults to establish that the fault is detected by the ESPE going to a lock-out condition and that no failure to danger occurs, in accordance with 4.2.2.5.

When a single fault is not detected and the analysis specified in 5.3.1 cannot be carried out, the tests for the ESPE going to a lock-out condition and no failure to danger occurring shall be continued with that fault applied first and all other faults added and removed in turn. Tests shall be carried out for all undetected single faults.

When a sequence of two faults is not detected and the analysis specified in 5.3.1 cannot be carried out, the tests shall be continued for those two faults, applied in sequence, and all other single faults added and removed in turn. No failure to danger shall occur. Tests shall be carried out for all undetected double faults.

Testing for the accumulation of more than three faults need not be carried out provided that the probability of more than three faults, largely independent of each other and having to appear in a specific sequence in time, is low.

5.4 Environmental tests

5.4.1 Rated supply voltage

The design measures specified in 4.2.1 shall be verified by inspection.

The ESPE shall be subjected to the following sequence of tests using the relevant values specified in 4.2.1:

- a) the ESPE shall be supplied with the lowest rated supply voltage. A B test shall be carried out;
- b) the supply voltage shall be increased, within a period of 10 s to 20 s, to the highest rated voltage, during which time an A test shall be performed;
- c) after the highest test supply voltage has been reached, a B test shall be carried out.

The requirements for frequency variation and for harmonic distortion shall be verified either by testing or by using analytical methods.

5.4.2 Ambient temperature variation and humidity

The highest ambient temperature in the tests below shall be as specified in the marking and/or the accompanying documents, but shall not be lower than +50 °C. The lowest ambient temperature in the tests below shall be as specified in the marking and/or the accompanying documents, but shall not be higher than 0 °C.

The ESPE shall be subjected to the following sequence of tests:

- a) With the ESPE operating under the conditions specified in 5.1.2.1, an A test shall be performed with a duration of at least 2 h. At the end of that time, a B test shall be carried out.
- b) The ambient temperature shall be increased by not more than 0,3 °C per minute up to the highest ambient temperature, during which time an A test shall be performed.
- c) An A test shall be performed with a duration of at least 2 h at the highest ambient temperature. During that time, the humidity shall be increased to 95 % and held at that value for at least 1 h. Following the A test, a B test shall be carried out.

- d) The ambient temperature shall be decreased by not more than 0,3 °C per minute, whilst maintaining the humidity at 95 %, until a temperature of 20 °C is reached, during which time an A test shall be performed.
- e) The ambient temperature shall be decreased by not more than 0,3 °C per minute, without condensation occurring, until the lowest ambient temperature is reached, during which time an A test shall be performed.
- f) An A test shall be performed with a duration of at least 2 h at the lowest ambient temperature. At the end of that time, a B test shall be carried out.
- g) The ambient temperature shall then be increased by not more than 0,3 °C per minute to the value specified in 5.1.2.1, during which time an A test shall be performed.
- h) An A test shall be performed with a duration of at least 2 h at the temperature specified in 5.1.2.1. At the end of that time a B test shall be carried out.

5.4.3 Effects of electrical disturbances

NOTE Modifications of tests for ESPEs utilising communication bus interfaces are under consideration.

5.4.3.1 Supply voltage variations

The external supply voltage and each internally derived supply voltage shall in turn be varied in accordance with 4.3.2.1. During each test, a C test(s) shall be carried out as necessary to confirm that no failure to danger occurs at reduced voltage values.

5.4.3.2 Supply voltage interruptions

The tests specified in 4.3.2.2 shall be carried out with the duration of each test sufficiently long to cover at least 10 dips and to enable for each of tests 1) and 2) that a B test shall be carried out, and for test 3) that a C test shall be carried out.

5.4.3.3 Fast transient/burst

5.4.3.3.1 General requirements

The ESPE shall be subjected to fast transient/burst to the levels specified in 4.3.2.3.1 in accordance with IEC 61000-4-4 (using Figure 9 of IEC 61000-4-4 for coupling of d.c. and less than 50 V a.c. power and signal ports, and Figure 8 for other a.c. power ports).

During each exposure, a B test shall be carried out.

5.4.3.3.2 Additional tests

A type 3 or a type 4 ESPE shall also be subjected to fast transient/burst to the levels specified in 4.3.2.3.2 in accordance with IEC 61000-4-4 (using Figure 9 of IEC 61000-4-4 for coupling d.c. and less than 50 V a.c. power and signal ports, and Figure 8 for other a.c. power ports).

During each exposure, a C test shall be carried out.

5.4.3.4 Fast transient/surge

5.4.3.4.1 General requirements

The ESPE shall be subjected to fast transient/surge to the levels specified in 4.3.2.4.1 in accordance with IEC 61000-4-5 (using Figure 10 or 12 of IEC 61000-4-5 for coupling of signal ports, Figure 7 of IEC 61000-4-5 for coupling of less than 50 V a.c. and d.c. power ports, and Figures 6 and 7 of IEC 61000-4-5 for other a.c. power ports).

During each exposure, a B test shall be carried out.

5.4.3.4.2 Additional tests

The type 3 or a type 4 ESPE shall be subjected to fast transient/surge to the levels specified in 4.3.2.4.2 in accordance with IEC 61000-4-5 (using Figure 10 or 12 of IEC 61000-4-5 for coupling of signal ports, Figure 7 of IEC 61000-4-5 for coupling of less than 50 V a.c. and d.c. power ports, and Figures 6 and 7 of IEC 61000-4-5 for other a.c. power ports).

During each exposure, a C test shall be carried out.

5.4.3.5 Electromagnetic field

5.4.3.5.1 General tests

The ESPE shall be subjected to an electromagnetic field to the levels specified in 4.3.2.5.1 in accordance with 5.1 of IEC 61000-4-3. During the exposure to severity level 3, a B test shall be carried out.

NOTE The result of this test is dependent on the surrounding structures which may differ from when the ESPE is fitted to a machine.

5.4.3.5.2 Additional tests

A type 3 and a type 4 ESPE shall also be subjected to an electromagnetic field to the levels specified in 4.3.2.5.2 in accordance with 5.2 of IEC 61000-4-3. During the exposure to severity level 4, a C test shall be carried out.

NOTE The result of this test is dependent on the surrounding structures which may differ from when the ESPE is fitted to a machine.

5.4.3.6 Conducted disturbances induced by radio-frequency fields

5.4.3.6.1 General tests

The ESPE shall be subjected to conducted radio-frequency disturbances to the levels specified in 4.3.2.6.1 in accordance with IEC 61000-4-6. During each exposure, a B test shall be carried out.

5.4.3.6.2 Additional tests

A type 3 or a type 4 ESPE shall also be subjected to conducted radio-frequency disturbances to the levels specified in 4.3.2.6.2 in accordance with IEC 61000-4-6.

During each exposure, a C test shall be carried out.

5.4.3.7 Electrostatic discharge

5.4.3.7.1 General tests

The ESPE shall be subjected to electrostatic discharge to the levels specified in 4.3.2.7.1 in accordance with IEC 61000-4-2. During each exposure, a B test shall be carried out.

5.4.3.7.2 Additional tests

A type 3 or a type 4 ESPE shall also be subjected to electrostatic discharge to the levels specified in 4.3.2.7.2 in accordance with IEC 61000-4-2.

During each exposure a C test shall be carried out.

5.4.4 Mechanical influences

5.4.4.1 Vibration

The test sample shall be exposed to vibration tests according to IEC 60068-2-6.

The following conditions shall apply:

Frequency range:	10 Hz to 55 Hz
Sweep rate:	1 octave/min
Amplitude:	0,35 mm ± 0,05 mm. The test shall be carried out without anti-vibration mountings
Number of sweeps:	20 for each of three mutually perpendicular axes (no delay at resonant frequencies)

The following limited functional tests shall be performed for each axis:

- an A test shall be performed during each of the first and last sweeps;
- a B test shall be carried out, so that the test piece is brought into the detection zone at the beginning of the second sweep and is removed at the end of the 19th sweep.

5.4.4.2 Bump

The test sample shall be exposed to bump tests according to IEC 60068-2-29.

The following conditions shall apply:

Acceleration:	10 g
Duration of pulse:	16 ms
Number of bumps:	1 000 ± 10 for each of three mutually perpendicular axes

The following tests shall be performed for each axis:

- an A test shall be performed during each of the first and last (100 ± 10) bumps;
- a B test shall be carried out, so that the test piece is brought into the detection zone after the first (100 ± 10) bumps.

5.4.5 Enclosures

The requirements of 4.3.4 for degrees of protection shall be tested in accordance with IEC 60529 after the tests of 5.4.4 have been completed. The remaining requirements shall be verified by inspection.

5.5 Validation of programmable or complex integrated circuits

5.5.1 General

This subclause deals with the validation of the requirements of 4.2.10 and 4.2.11, and any analysis statement included as part of the test results statement required by 5.3.1.

Validation shall be undertaken by a competent person(s) who should be independent of those responsible for any aspect of the system design, the hardware design and the software design. A written validation report shall be compiled.

NOTE The validation provides independent confirmation that specific requirements have been achieved. The process is intended to confirm that systematic faults in the design have been avoided, that procedures are in place to maintain safety performance during the life cycle of the product (including, for example, following modification) and that the design of the ESPE fulfils the fault detection requirements appropriate to its type.

5.5.2 Complex or programmable integrated circuits

For a Type 4 ESPE employing a complex or programmable integrated circuit(s), the following requirements shall be validated by analysis:

- a) there are a minimum of two independent decision-making channels;
- b) the detection of disparity between channels, and the initiation of a lock-out condition, shall be maintained under all applicable fault conditions.

5.5.3 Software, programming, functional design of integrated circuits

It shall be verified that the specified procedures and supporting documentation for the quality system(s) under which the system design and software were developed meet the requirements of a quality management system (for example, ISO 9001).

The operation of the quality system(s) shall be verified by an audit inspection of the documentary records pertaining to the development of the equipment and the procedures established for the maintenance of quality during the life cycle of the product.

The adequacy, completeness, and traceability of the project development documentation shall be validated by audit inspection.

The safety requirements specification shall be analysed to confirm that the requirements for software, program design, and functional design, not addressed therein have been addressed elsewhere in the system design.

The test plan shall be analysed to confirm that all the requirements of the safety requirements specification can be verified by successful completion of the tests.

When software specific to fault detection is used in operation, the test plan shall be analysed to confirm that all faults considered in B.4.4 which cannot be tested by direct hardware fault simulation are tested by the software.

The test results for the latest issued version of the design shall be subjected to an audit inspection. Sample tests, chosen at random, shall be repeated for validation and the results shall agree in detail with those held in the project records.

When software specific to fault detection is used in operation, the test results for simulated faults shall verify that the specified coverage is achieved and shall be compared with any analysis statement included as part of the test results statement.

For software used in operation, it shall be verified that the entire operational instruction program is contained within read-only memory which cannot be overwritten by the processor.

For programmable devices, the means for verification that the device performs all its programmed functions shall be validated.

NOTE 1 Incorrectly or incompletely programmed devices can allow the equipment to perform the primary protective function correctly but fail to implement fault detection functions, particularly when multiple similar programmable devices are used within a design which depends upon cross-monitoring for fault detection.

The means employed to monitor program flow and/or the operation of complex/programmable devices shall be validated. The means shall be appropriate for the level of safety-related performance claimed by the supplier, and the system architecture employed.

NOTE 2 Further guidance can be found in IEC 61508-3.

5.5.4 Test results analysis statement

When analysis is employed to define the result of any test required by 5.3, the adequacy, suitability, and validity of the techniques used shall be validated. The correct implementation of the methods used shall be verified by repeating parts of the analysis selected at random.

6 Marking for identification and for safe use

6.1 General

In accordance with 5.4 of ISO/TR 12100-2, all parts of the ESPE shall bear all markings which are necessary:

- for its unambiguous identification;
- for its safe use,

and supplementary information shall be given, as appropriate:

- permanently on the ESPE;
- in accompanying documents such as instruction handbooks;
- on the packaging.

The enclosure of the most appropriate part of the ESPE shall carry the following permanent markings:

- a) identification of the product, including name and address of the supplier, designation of series or type, serial number and year of construction;
- b) parameters, for example dimensions, of the detection zone;
- c) detection capability;
- d) response time;
- e) rated voltage(s) including number of phases and frequency where relevant;
- f) rated input power (if greater than 25 W) or rated current;
- g) designation of IP code;
- h) for class II equipment only, symbol for classification for protection against electric shock;
- i) warning sign of hazards arising from dangerous voltages;
- j) type of ESPE according to 4.1.3.

6.2 ESPE supplied from a dedicated power supply

Where an ESPE is designed to be supplied from an external dedicated power supply, details of the model or type of dedicated power supply with which it has been tested shall be permanently marked on the enclosure of the most appropriate part of the ESPE and/or included in the instructions for use.

6.3 ESPE supplied from an internal electrical power source

An ESPE supplied from an internal power source shall be marked with details of the rated current of the supply fuse, if applicable, on the enclosure of the most appropriate part of the ESPE.

6.4 Adjustment

When the ESPE can be adjusted to suit different rated voltages or different inputs, a marking showing the voltage or input to which the ESPE is adjusted shall be clearly and easily discernible at the point of adjustment.

6.5 Enclosures

Any enclosure which contains electrical devices shall be marked with a warning sign in accordance with 17.2 of IEC 60204-1.

6.6 Control devices

6.6.1 Markings for switches, indicating lamps, and other control devices shall be placed adjacent to those components; they shall not be placed on removable parts which can be replaced in such a way that the marking is misleading.

6.6.2 Functional identification of control and indicating devices shall be in accordance with 17.3 of IEC 60204-1.

6.6.3 The positions of any power supply switches shall be marked according to 5.3.1 of IEC 60204-1.

6.6.4 Devices intended for the adjustment of a characteristic during or after installation, shall be provided with markings of the direction of adjustment to increase or decrease the value of that characteristic. See also IEC 60447.

6.7 Terminal markings

6.7.1 Terminals to which cable connections are to be made at the time of installation, or re-established after maintenance of the ESPE, shall be marked and related to a diagram.

6.7.2 Terminals for external connections provided with, and relating to the ESPE and user replaceable components shall be marked and related to a diagram.

6.7.3 All terminals for the incoming supply connections shall be marked in accordance with IEC 60445.

6.7.4 Protective conductor connection points shall be marked in accordance with 8.2.7 of IEC 60204-1.

This marking shall not be placed on screws, removable washers or other parts which might be removed when conductors are being connected/disconnected.

6.7.5 Where an ESPE is to be connected to more than two supply conductors, it shall be provided with a connection diagram, fixed to the ESPE, unless the correct mode of connection is obvious.

6.7.6 If more than one supply is taken to an ESPE, the marking shall include a warning that all supplies shall be switched off before the terminal cover may be removed.

6.8 Marking durability

Marking shall be capable of withstanding the environmental influences of an industrial environment with respect to temperature and humidity as defined by this standard, and liquids such as water, soapy water, machine oil, benzine, etc.

Markings shall be capable of withstanding being rubbed lightly for 15 s with a piece of cloth soaked with petroleum spirits, and with a piece of cloth soaked in water.

7 Accompanying documents

The supplier of the ESPE shall provide documentation in the languages agreed between the user and the supplier.

The accompanying documents shall contain the information required for the installation, use and subsequent disposal of the ESPE, including the following information where applicable:

- a) a statement that other devices shall not be connected to the internally generated power supplies of the ESPE;
- b) details of the optional functions of the ESPE, described in Annex A, which have been included;
- c) a description of facilities for connection of Stopping Performance Monitor (SPM) if provided;
- d) for a type 2 ESPE, information on the means of applying an external test signal, where required (see 4.2.2.3);
- e) a recommendation that security keys/special tools, if provided for adjustments, operations or access, be kept under the control of a responsible or authorized person(s);
- f) the size and type of the test piece and the test procedure, or description of other methods for checking the detection capability and the operation of the visual indicator;
- g) the response time.
When a safety-related communication interface is used, procedures for determining overall system response time shall be explained;
- h) the rated operating conditions for the ESPE including:
 - temperature range;
 - humidity;
 - voltage range;
 - range of separation distances between the subsystems, and the maximum length of interconnecting cables.
- i) advice on the prevention of mutual interference of sensing functions;
- j) block diagrams, functional description chart showing sequence of relay switching operations;
- k) the location of all input and output terminals;
- l) the ratings and characteristics of all input/output terminals;
- m) the minimum and maximum voltage and current that the OSSDs (and if provided, the SSDs) are capable of switching into a resistive, capacitive or inductive load, and the maximum switching rate with this load, and the anticipated life of the switching device depending on load;
- n) information to enable the user to carry out maintenance using the supplier's recommended spares;

- o) special requirements regarding input cables and terminations, if applicable;
- p) the total load/power requirements of the ESPE;
- q) details of the space required around the equipment for removal and maintenance purposes;
- r) a list of the user-replaceable parts specified by the supplier;
- s) a list of colour and coding systems (see IEC 60204-1);
- t) the overall dimensions of the equipment;
- u) operating instructions;
- v) the location and dimensions of the detection zone(s) and definitions of other functional limits;
- w) a schedule of checks to be carried out after installation, after maintenance, or periodically, to establish that the device is functioning correctly;
- x) the method and frequency of regular testing to confirm that proper operation is maintained;
- y) a statement of the IP rating of the enclosures, or where the ESPE is intended to be mounted in a machine controlgear enclosure, the minimum IP rating required of that enclosure according to 4.3.4;
- z) a clear statement of any particular application for which the ESPE is intended;
- aa) the recommended maximum period between periodic tests for a type 2 ESPE;
- bb) the installation and mounting instructions for any switches, controls and indicators remotely mounted from the ESPE that are connected to the ESPE;
- cc) instructions on where parts with restart interlock should be located in relation to the danger zone;
- dd) instructions on where parts with sensing functions should be located in relation to the danger zone and methods for determination of safety distances between those parts and the danger zones, for example formulae for calculation;
- ee) instructions on how the ESPE should be interfaced with the machine control system;
- ff) the details of any special precautions necessary to be taken into account;
- gg) the dimensions of the space(s) to be provided for the ESPE;
- hh) the dimensions and position of the means for supporting and fixing the ESPE within the space(s);
- ii) the minimum clearances between the various parts of the ESPE and the surrounding parts of the fitment;
- jj) the means of connection of the ESPE to the supply, and the interconnection of separate components, if any;
- kk) information for proper connection of solid state outputs in accordance with 4.2.4.3, if used.

When a communications interface (4.2.4.4) is integrated into the ESPE, the operating limitations and timing characteristics necessary for proper integration shall be provided;

- ll) when blanking functions (monitored, unmonitored, fixed or floating) or adjustment of detection capability are provided their intended use shall be explained.

Annex A (normative)

Optional functions of the ESPE

A.1 General

An ESPE may include additional functions, or devices arranged to perform functions within the safety-related control system. The ESPE together with any separate devices specifically intended to perform these optional functions shall meet the requirements of this standard.

NOTE Where the optional functions are performed by a separate device(s) that is not specifically intended to be used as part of an ESPE, this separate device(s) should meet the relevant requirements of other appropriate standards (for example ISO 13849-1, IEC 61508, future IEC 62061). In this case, the requirements of this Annex may be used as a guide in conjunction with the other standards.

The following are optional devices or functions:

- external device monitoring (see Clause A.2);
- stopping performance monitor (see Clause A.3);
- secondary switching device (see Clause A.4);
- start interlock (see Clause A.5);
- restart interlock (see Clause A.6);
- muting (see Clause A.7);
- ESPE used as a machine reinitiation device (see Clause A.8).

The following requirements are minimum requirements and may not be sufficient for all applications. These requirements are intended to be used in conjunction with the relevant requirements given in other standards (for example IEC 60204-1, ISO 13849-1), as the result of a risk assessment.

Where signals for optional functions are provided via a safety-related data interface, the requirement for hard-wired connections at the ESPE can be excluded if the equivalent functions are performed by a safety-related communication system which has a SIL claim limit that is appropriate for the type of ESPE or safety function. Other requirements do not change.

NOTE SIL claim limit of 3 is appropriate for a Type 4 ESPE, SIL2 for a Type 3 ESPE and SIL1 for a Type 2 ESPE.

A.2 External device monitoring (EDM)

A.2.1 Functional requirements

EDM shall provide a means to monitor the state of external contacts (for example FSDs or MPCEs).

The ESPE shall go to a lock-out condition when an incorrect state is detected in one of the devices being monitored by the EDM.

A.2.2 Fault condition requirements

The ESPE shall respond in accordance with 4.2.2 to faults in the EDM.

A.2.3 Verification

It shall be verified by inspection and test that:

- the necessary means are provided in the ESPE for the monitoring of the devices for which the EDM is intended to be used;
- the ESPE goes to the lock-out condition when any one of the devices being monitored is in an incorrect state;
- the ESPE responds according to 4.2.2 to faults occurring in the EDM.

A.2.4 Information for use

The ESPE supplier shall provide information for the connection of the EDM to the appropriate devices. The supplier shall specify the type of any device for which the EDM is intended to be used. Where the monitored devices require particular characteristics (for example mechanically linked contacts, duplicate inputs, N/O, N/C), these shall be specified.

Unless response time of the external contacts is monitored, information for use shall include a notice that external means of monitoring the response time of the contacts can be required.

A.3 Stopping performance monitor (SPM)

A.3.1 Functional requirements

The SPM shall provide signals to the ESPE related to the time taken by, or the amount of travel of, the hazardous parts of the machine in coming to rest or reverting to a safe condition. The ESPE shall go to a lock-out condition when a signal(s) from the SPM indicates that the preset limit of stopping performance has been exceeded.

For a type 4 ESPE, the SPM shall provide at least two signalling channels to the ESPE. Each channel shall be capable of initiating a lock-out condition of the ESPE.

The SPM shall apply an automatic stopping performance test to monitor the overall system stopping performance.

The SPM shall be capable of initiating the automatic stopping performance test in response to signals derived from the ESPE, immediately upon actual or simulated actuation of the sensing device.

Any means by which the preset limit(s) within the SPM may be adjusted shall require the use of a key, keyword or special tool.

A.3.2 Fault condition requirements

The ESPE shall go to a lock-out condition in response to any of the following:

- upon failure to apply, or to complete the automatic test;
- upon failure of transmission of motion to the SPM or, when duplicated transmission means are used, upon failure of either one of those means;
- upon disconnection of the stopping performance monitor from the ESPE.

A.3.3 Verification

Verify by inspection that:

- the SPM output signal(s) causes the ESPE to go to a lock-out condition when the preset limit of stopping performance is exceeded;
- for a type 4 ESPE application, there are at least two independent signal sources, from the SPM to the ESPE, and failure of either one of those causes lock-out;
- the SPM initiates an automatic test in response to a signal from the ESPE;
- the ESPE initiates an automatic stopping performance test upon actual or simulated actuation of the sensing function;
- any adjustment means requires the use of a key, keyword or special tool;
- when the automatic test has failed to be applied or completed, a lock-out condition is achieved;
- when any of the transmission of motion means has failed, a lock-out condition is achieved;
- when a SPM is disconnected from the ESPE, or from the safety-related control system, a lock-out condition is achieved;
- the markings conform to A.3.4 and are correct.

A.3.4 Marking

The supplier shall provide permanently affixed markings to the stopping performance monitor giving the following information:

- name and address of the supplier;
- the model type number and serial number;
- the ESPE type number for which the stopping performance monitor is designed;
- the accuracy of the unit.

A.4 Secondary switching device (SSD)

A.4.1 Functional requirements

When the ESPE power supply is switched off or when the ESPE is in a lock-out condition, the SSD shall be in the OFF-state.

The ability of the SSD to perform its safety-related function shall be checked by an automatic test, carried out when the ESPE power supply is switched on and before the OSSD(s) go to the ON-state.

A.4.2 Fault condition requirements

If the automatic test referred to in A.4.1 identifies the inability of the SSD to go to the OFF-state, the OSSD(s) shall remain in the OFF-state.

A.4.3 Verification

Verify by inspection and test that:

- when, under fault conditions, the SSD is restrained to remain in the ON-state and the ESPE power supply is switched on, the OSSD(s) will remain in the OFF-state, even when a reset is attempted;
- the SSD is in the OFF-state under lock-out conditions.

A.5 Start interlock

A.5.1 Functional requirements

The start interlock shall prevent the OSSD(s) going to the ON-state when the electrical supply is switched on, or is interrupted and restored.

The OFF-state of the OSSD(s) shall continue until the start interlock is reset to its ON-state, manually (for example by switch operation or by actuation and de-actuation of the sensing device).

It shall not be possible for reset of a start interlock to reset the OSSD(s) to the ON-state under a lock-out condition.

A.5.2 Fault condition requirements

A failure of the start interlock which causes it to go to, or remain in a permanent ON-state shall cause the ESPE to go to, or to remain in the lock-out condition.

A.5.3 Verification

Verify by inspection and test that:

- the OSSD(s) is in the OFF-state when the start interlock is in the OFF-state;
- when the power supply is switched on, the OSSD(s) remain in the OFF-state until the start interlock is manually operated;
- when power is interrupted long enough for the OSSD(s) to go to the OFF-state, it shall be verified that when the power is restored, the OSSD(s) remain in the OFF-state until the start interlock is manually operated;
- during a lock-out condition, an attempt to reset the start interlock does not allow the OSSD(s) to go to the ON-state;
- the lock-out condition is initiated if the start interlock fails.

A.5.4 A.5.4 Indication

A yellow indicator shall be provided which should illuminate when the OSSD(s) is prevented from going to the ON-state by the start interlock.

A.6 Restart interlock

A.6.1 Functional requirements

The restart interlock shall prevent the OSSD(s) going to the ON-state when:

- the detection zone is interrupted while the machine operation is at a hazardous part of its operating cycle;
- the detection zone is interrupted while the machine is in automatic or semi-automatic mode;
- there is a change of the machine operating mode or type of operation.

The interlock condition shall continue until the restart interlock is manually reset. However, it shall not be possible to reset the restart interlock whilst the sensing device is actuated.

A.6.2 Fault condition requirements

A failure to meet the functional requirements of A.6.1 shall cause the ESPE to go to the lock-out condition.

A.6.3 Verification

Verify by inspection and test that:

- the OSSD(s) is in the OFF-state when the restart interlock is in the OFF-state;
- the restart interlock will not reset to the ON-state while the sensing device is actuated;
- the restart interlock goes to the OFF-state on sensing device actuation during a hazardous machine operation;
- when the machine operating mode or type of operation is changed, the restart interlock goes to the OFF-state;
- the lock-out condition is initiated if the restart interlock fails;

A.6.4 Indication

A yellow indicator shall be provided which should illuminate when the OSSD(s) is prevented from going to the ON-state by the restart interlock.

A.7 Muting

A.7.1 Functional requirements

A.7.1.1 When the ESPE is in a muted condition, the OSSD(s) shall remain in the ON-state on actuation of the sensing device.

A.7.1.2 There shall be at least two independent hard-wired muting signal sources to initiate the function. It shall not be possible to initiate muting when the OSSDs are already in the OFF-state.

A.7.1.3 The mute function shall only be initiated by the correct sequence and/or timing of the mute signals. Should conflicting muting signals occur, the ESPE shall not allow a muted condition to occur.

A.7.1.4 There shall be at least two independent hard-wired muting signal sources to stop the function. The muting function shall stop when the first of these muting signals changes state. The deactivation of the muting function shall not rely only on the clearance of the ESPE.

NOTE The signal sources for initiating and stopping the mute function may be the same.

A.7.1.5 The muting signals should be continuously present during muting. When the signals are not continuously present, an incorrect sequence and/or the expiration of a pre-set time limit shall cause either a lock-out condition or a restart interlock.

NOTE For some applications (for example conveyor and packaging machinery) a mute dependent bypass (override) function can be provided. This function allows reactivation of the muting function in order to clear a blockage in the area of the machine where the muting sensors are located. The activation of the bypass function should be possible only when at least one muting sensor is activated. A single fault should not initiate the bypass function. The bypass function should be automatically deactivated either after a correct muting signal sequence is identified, a pre-set time limit has expired or immediately when the defined muting area is clear and normal operation can resume. Activation of the bypass function should require use of a hold to run device which should be located where the operator can see the point of hazard.

A.7.2 Fault condition requirements

A fault in the muting function shall be detected in accordance with 4.2.2, and shall at least not allow another muted condition to occur.

A.7.3 Verification

Verify by inspection and test that:

- in a muted condition, the OSSD(s) remain in the ON-state on actuation of the sensing device;
- there are two independent hard-wired muting signal sources to initiate and to stop the muting function and that a muted condition is prevented whenever an invalid combination of signals is present;
- in a type 2 ESPE, any failure which could lead to a continuously muted condition is revealed by the periodic test, and when such a failure is detected, a further muted condition is prevented;
- the muting function stops when the first of the two “stop mute” signals changes state.

A.7.4 Indication

A mute status signal or indicator shall be provided. (In some applications an indication signal of muting is necessary (see ISO 13849-1, 5.2.5).)

A.8 Reinitiation of machine operation facility

A.8.1 General

If, in addition to its function as a protective device, the ESPE is intended to be used to reinitiates machine operation, the following modes of operation can be used:

- an actuation and de-actuation of the sensing device reinitiates machine movement, referred to as single break;
- two consecutive actuations and de-actuations of the sensing device reinitiate machine movement, referred to as double break.

Where this optional feature is provided as part of the ESPE, a start interlock as specified in Clause A.5, and a restart interlock as specified in A.6, shall also be provided within the ESPE.

A.8.2 Functional requirements

- a) When the ESPE power is switched on or is interrupted and restored, it shall not be possible to use either of the modes of operation described in A.8.1 before the start interlock has been reset.
- b) After actuation of the sensing device during hazardous motion, it shall not be possible to use either of the modes of operation described in A.8.1 before the restart interlock has been reset.
- c) Successive reinitiations of machine operation by the use of either of the modes of operation described in A.8.1 shall be possible only within a limited period of time.
- d) When double break reinitiation is selected, reinitiation by single break shall not be possible under any sequence of events or actions.
- e) If the limited period of time referred to in c) is exceeded, further machine reinitiation shall not be possible until the restart interlock has been reset.

- f) Machine reinitiation by either of the modes of operation described in A.8.1 shall not be possible following a change of reinitiation mode until the restart interlock has been reset.
- g) Facilities shall be provided to reset the timer controlling the limited period described in c) by external means.
- h) The adjustment means for the timer shall require the use of a key, keyword or special tool.

NOTE The time period permitted for successive reinitiations should not exceed 30 s for machinery having a cycle time of less than 5 s.

A.8.3 Fault condition requirements

Any fault listed in Annex B leading to a change in the machine reinitiation mode shall at least result in the operation of either the start interlock or the restart interlock.

A.8.4 Verification

Verify by inspection and test that:

- after the ESPE power is switched on, or is interrupted and restored, it is not possible to use either of the modes of operation described in A.8.1 until the start interlock has been reset;
- after actuation of the sensing device during hazardous motion, it is not possible to use either of the modes of operation described in A.8.1 until the restart interlock has been reset;
- successive reinitiations of machine operation by the use of either of the modes of operation described in A.8.1 shall only be possible within a limited time period;
- when double break reinitiation is selected, reinitiation by a single break shall not be possible under any sequence of events or actions;
- machine reinitiation by either of the modes of operation described in A.8.1 shall not be possible following a change of reinitiation mode until the restart interlock has been reset;
- facilities are provided to reset the timer controlling the limited period described above, by external means;
- the adjustment means for the timer are within an enclosure with access requiring the use of tools;
- faults listed in Annex B leading to a change in the machine reinitiation mode shall at least result in operation of either the start interlock or the restart interlock.

Annex B (normative)

Catalogue of single faults affecting the electrical equipment of the ESPE, to be applied as specified in 5.3

B.1 Conductors and connectors

B.1.1 Conductors/cables

Faults considered	Exclusions
Short circuit between any two conductors	Conductors which are permanently connected (for example not using plug/socket combinations) and which are protected against external damage by, for example, cable ducting, armouring Conductors in separate multicore cables
Open circuit of any conductor	None
Short circuit between any conductor and an exposed conductive part or the protective conductor	None
Short circuit between any conductor and a live part	Conductors which are supported and/or terminated by multiconductor termination assemblies so as to prevent the fault occurring from, for example, mechanical failure near a termination point

B.1.2 Printed circuits and printed circuit assemblies

Faults considered	Exclusions
Short circuit between two adjacent conductors	Where: – the base material is according to IEC 60249-2 and the creepage distances and clearances are dimensioned to at least IEC 60664-1 with pollution degree 2/ installation category III; and – the assembled board is mounted in an enclosure giving a degree of protection to at least IP54 and the printed side(s) are coated with an ageing-resistant varnish or protective layer covering all conductor paths
Open circuit of any conductor path	None

B.1.3 Terminal blocks

Faults considered	Exclusions
Short circuit between adjacent terminals	Where the terminals used are in accordance with a relevant IEC standard and the requirements of 14.1.1 and 14.1.2 of IEC 60204-1 are satisfied
Open circuit of individual terminals	None

B.1.4 Multi-pin connectors (for example plug and socket for cable, relay, IC)

Faults considered	Exclusions
Short circuit between any two adjacent pins	Adjacent pins satisfying B.1.2
Interchanged or incorrectly inserted connector when not prevented by mechanical means	None
Open circuit on individual connector pin	None

B.2 Switches**B.2.1 Electro-mechanical switches, manually operated switches and push buttons (for example reset actuator, dip switch)**

Faults considered	Exclusions
Contact pairs will not close	None
Contact pairs will not open	None
Short circuit between adjacent contacts insulated from each other	Where the switch used is in accordance with IEC 60947-5-1 (see K.7.1.4.6.1) and conductive parts which become loose cannot bridge the insulation between contacts
Simultaneous short circuit between three terminals of change-over contacts	Where the switch used is in accordance with IEC 60947-5-1 (see K.7.1.4.6.1) and conductive parts which become loose cannot bridge the insulation between contacts

B.2.2 Electro-mechanical devices (for example relay, contactor)

Faults considered	Exclusions
Does not de-energize (all contacts remain in energized position for example due to mechanical fault)	None
Does not energize (all contacts remain in de-energized position for example due to mechanical fault, open circuit of coil)	None
Individual contact not opening	None
Individual contact not closing	None
Simultaneous short circuit between the three terminals of a change-over contact	Where the creepage and clearance distances are dimensioned to at least IEC 60664-1 with pollution degree 2/installation category III and conductive parts which become loose cannot bridge the insulation between contacts
Short circuit between contact circuits, and between contacts and coil terminals	Where the creepage and clearance distances are dimensioned to at least IEC 60664-1 with pollution degree 2/installation category III and conductive parts which become loose cannot bridge the insulation between contacts and between contacts and the coil
Simultaneous closing of normally open and normally closed contacts	Simultaneous closing of contacts can be excluded if positively driven (or mechanically linked) contacts are used

B.3 Discrete electrical components

B.3.1 Transformers

Faults considered	Exclusions
Open circuit of individual winding	None
Short circuit between windings	Where the windings are separated according to IEC 60950

B.3.2 Inductors, Fixed or adjustable

Faults considered	Exclusions
Open circuit	None
Short circuit	Where choke coil is single-layered, enamelled or potted, and with axial wire connections and axial mounting
Changing value: $0,5 L_N < L < L_N + \text{tolerance}$ where L_N is the nominal value of inductance or for adjustable inductors: Changing value: $L_{Min} < L < L_{Max}$	None

B.3.3 Resistors

Faults considered	Exclusions
Open circuit	None
Short circuit	Where the resistor is of the film type or the wirewound type with protection to prevent unwinding of the wire in the event of breakage, with axial wire connections, axial mounted and varnished melf resistors used in surface-mounting technology
Changing value: $0,5 R_N < R < 2 R_N$ where R_N is the nominal value of resistance	None

B.3.4 Resistor networks

Faults considered	Exclusions
Open circuit of individual resistor	None
Short circuit between any two connections	None
Changing value of individual resistor: $0,5 R_N < R < 2 R_N$ where R_N is the nominal value of resistance	None

B.3.5 Potentiometers

Faults considered	Exclusions
Open circuit of each individual connection	None
Simultaneous short circuit between all connections	None
Changing value between any two connections: $0,5 R_P < R < 2 R_P$ where R_P is the nominal value	None

B.3.6 Capacitors, fixed or adjustable

Faults considered	Exclusions
Open circuit	None
Changing value: $0,5 C_N < C < C_N + \text{tolerance}$ where C_N is the nominal value or set value	None

B.4 Solid-state electrical components**B.4.1 Discrete semi-conductors (for example diode, transistor, triac, voltage regulator, phototransistor and light-emitting diode (LED))**

Faults considered	Exclusions
Open circuit of any connection	None
Short circuit between any two connections	None
Short circuit between all connections	None
Changing electrical characteristics resulting in a safety-related output signal which is outside either the upper or lower limits of the working signal range by 25 %	None

B.4.2 Optocouplers

Faults considered	Exclusions
Open circuit of individual connections	None
Short circuit between any two connections:	Components having an impulse voltage withstand capability according to Table 1 of IEC 60664-1, over-voltage category III
– input connections (transmitter)	
– output connections (receiver)	
– between input and output	
Changing electrical characteristics resulting in a safety-related output signal which is outside either the upper or the lower limit of the working signal range by 25 %	None

B.4.3 Integrated circuits, simple

Faults considered	Exclusions
Open circuit for each individual connection	None
Short circuit between any two connections	None
Persistent "0" or "1" signal at all inputs and outputs, either individually or simultaneously (i.e. short-circuit to negative or positive rails with isolated input or disconnected output)	None
Parasitic oscillation of outputs NOTE The choice of test frequency and the pulse duty factor is dependent on the switching technology and the external circuitry. When testing, the driving stages in question are disconnected.	None
Changing electrical characteristics resulting in a safety-related output signal which is outside either the upper or lower limit of the working signal range by 25 %	None

B.4.4 Integrated circuits, complex or programmable

Faults considered	Exclusions
Defect in part or all of the function (see also 4.2.10 and 4.2.11). The defect may: – be static – change the logic – be dependent on bit sequences	None
Undetected failure in the hardware that goes unnoticed because of the complexity of the integrated circuit (see also 4.2.10 and 4.2.11)	None
Defects in the storage and processing components not revealed by the complete execution of the program	None
All in B.4.3	See B.4.3

B.5 Motors

Faults considered	Exclusions
Motor stopped	None
Speed above normal	None
Speed below normal	None

Annex C (informative)

Conformity assessment

This standard contains the conditions for the evaluation of conformity of a product to the standard. However, the requirements are such that a high dependence is placed on test equipment and expert analysis. In order to make a proper assessment of electro-sensitive protective equipment to this standard and at least one of its parts, a process of third party evaluation and testing according to the requirements of this standard should be performed. The third party would need to be a body such as an accredited test house with resources appropriate to these types of equipment. This process is independent from the normative requirements of this standard and may be required either by legislation or regulations, or by contractual agreements.

Bibliography

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

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

IEC/TS 62046, *Safety of machinery – Application of protective equipment to detect the presence of persons*

ISO 9000-3:1997, *Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of software*

IECNORM.COM . Click to view the full PDF of IEC 61496-1:2004+AMD1:2007 CSV

Index

This index lists, in alphabetical order, the terms and acronyms defined in Clause 3 and indicates where they are used in the text of this part.

B

blanking 3.1, 4.1.2, 7II).

C

controlling/monitoring device 3.2, 3.5, 4.2.10.

D

detection capability 3.3, 3.1, 4.1.1, 4.1.2, 4.2.2.3, 4.2.2.5, 5.2.1, 6.1c), 7f), 7II).

detection zone 3.4, 1, 3.1, 3.25, 4.1.1, 4.1.2, 4.2.2.3, 4.2.5, 5.1.1.3, 5.2.3.2, 5.2.3.3, 5.4.4.1, 5.4.4.2, 6.1b), 7v), A.6.1.

E

electro-sensitive protective equipment (ESPE) 3.5, used throughout this document.

external device monitoring (EDM) 3.6, A.1, A.2.

F

failure 3.7, 3.8, 3.9, 4.2.9, 4.2.11.2d), 4.3.2.1, 4.3.2.2, 4.3.2.3.2, 4.3.2.4.2, 4.3.2.5.2, 4.3.2.6.2, 4.3.2.7.2, 5.2.3.1, A.3.2, A.3.3, A.5.2., A.7.3, B.1.1, B.4.4.

failure to danger 3.8, 4.2.2.3, 4.2.2.4, 4.2.2.5, 4.2.4.1, 4.2.6, 4.2.9, 5.2.3.4, 5.3.4, 5.3.5, 5.4.3.1.

fault 3.9, 3.7, 3.13, 4.1.3, 4.2.2, 4.2.2.1, 4.2.2.3, 4.2.2.4, 4.2.2.5, 4.2.4.3, 5.2.3.1, 5.2.8.1, 5.3, 5.3.1, 5.3.3, 5.3.4, 5.3.5, 5.5.1, 5.5.2, 5.5.3, A.2.2, A.2.3, A.3.2, A.4.2, A.5.2, A.6.2, A.7.1.5, A.7.2, A.8.3, A.8.4, Annex B.

final switching device (FSD) 3.10, 3.13, 4.2.4.1, A.2.1.

I

integrated circuit – complex or programmable 3.11, 4.2.2.5, 4.2.10, 4.2.11, 5.5, 5.5.2, 5.5.3, B.4.4.

integrated circuit – simple 3.12, B.4.3.

L

lock-out condition 3.13, 3.24, 4.2.2.1, 4.2.2.3, 4.2.2.4, 4.2.2.5, 5.2.3.4, 5.3.3, 5.3.4, 5.3.5, 5.5.2, A.2.1, A.2.3, A.3.1, A.3.2, A.3.3, A.4.1, A.4.3, A.5.1, A.5.2, A.5.3, A.6.2, A.6.3, A.7.1.5.

M

machine primary control element (MPCE) 3.14, 3.10, 3.15, A.2.1.

machine secondary control element (MSCE) 3.15, 3.24.

muting 3.16, 3.5, A.1, A.7.

O

OFF-state 3.17, 3.1, 3.8, 3.10, 3.13, 3.19, 3.21, 3.24, 4.1.3, 4.2.2.3, 4.2.2.4, 4.2.2.5, 4.2.4.3, 4.2.5, 4.2.7, 5.2.3.2, 5.2.3.3, 5.2.3.4, 5.3.3, A.4.1, A.4.2, A.4.3, A.5.1, A.5.3, A.6.3, A.7.1.2.

ON-state 3.18, 4.2.2.1, 4.2.2.3, 4.2.4.3, 4.2.5, 5.2.3.2, 5.2.3.3, 5.2.3.4, 5.2.8.1, A.4.1, A.4.3, A.5.1, A.5.2, A.5.3, A.5.4, A.6.1, A.6.3, A.6.4, A.7.1, A.7.3.

output signal switching device (OSSD) 3.19, 3.1, 3.2, 3.5, 3.8, 3.10, 3.13, 3.21, 4.1.3, 4.2.2.3, 4.2.2.4, 4.2.2.5, 4.2.3.3, 4.2.4, 4.2.5, 4.2.7, 5.2.3.2, 5.2.3.3, 5.2.3.4, 5.2.4, 5.2.8, 5.3.3, 7m), A.4.1, A.4.2, A.4.3, A.5.1, A.5.3, A.5.4, A.6.1, A.6.3, A.6.4, A.7.1, A.7.3.

overall system stopping performance 3.20, 3.27, A.3.1.

R

response time 3.21, 3.20, 4.1.1, 4.2.2.3, 4.2.2.4, 4.2.2.5, 5.2.2, 5.3.3, 6.1d), 7g), A.2.4.

restart interlock 3.22, 4.2.2.3, 4.2.2.4, 4.2.2.5, 5.2.3.1, 7cc), A.1, A.6, A.7.1.5, A.8.

S

safety-related part of a control system 3.23, 3.16.

secondary switching device (SSD) 3.24, 3.5, 3.13, 3.15, A.1, A.4.

sensing device 3.25, 3.2, 3.3, 3.5, 3.19, 3.21, 3.22, 4.2.5, 5.2.2, A.3.1, A.5.1, A.6.1, A.6.3, A.7.1, A.7.1.1, A.7.3, A.8.1, A.8.2, A.8.4.

start interlock 3.26, 4.2.2.3, 4.2.2.4, 4.2.2.5, 5.2.3.1, A.1, A.5, A.8.

stopping performance monitor (SPM) 3.27, 3.5, 7c), A.1, A.3, A.3.2, A.3.4.

supplier 3.28, 4.1.1, 4.1.2, 4.2.4.3, 4.3.1, 4.3.4, 5.5.3, 6.1a), 7, 7n), 7r), A.2.4, A.3.4.

IECNORM.COM . Click to view the full PDF of IEC 61496-1:2004+A1:2007 CSV

IECNORM.COM . Click to view the full PDF of IEC 61496-1:2004+AMD1:2007 CSV

Withdrawn

SOMMAIRE

AVANT-PROPOS	57
1 Domaine d'application	60
2 Références normatives	60
3 Termes et définitions	62
4 Prescriptions de fonctionnement, de conception et d'environnement	66
4.1 Prescriptions de fonctionnement	66
4.2 Prescriptions de conception	67
4.3 Prescriptions relatives aux conditions ambiantes	75
5 Essais	78
5.1 Généralités	78
5.2 Essais de fonctionnement	80
5.3 Essais de performance sous condition de défaut	83
5.4 Essais d'environnement	85
5.5 Validation de circuits intégrés, programmables ou complexes	88
6 Marquage d'identification et de sécurité	90
6.1 Généralités	90
6.2 ESPE muni d'une source d'alimentation dédiée	90
6.3 ESPE alimenté à partir d'une source d'alimentation électrique interne	91
6.4 Réglage	91
6.5 Enveloppes	91
6.6 Dispositifs de commande	91
6.7 Marquage des bornes	91
6.8 Durabilité de l'étiquette	92
7 Documents d'accompagnement	92
Annexe A (normative) Fonctions optionnelles de l'ESPE	94
Annexe B (normative) Catalogue des défauts simples affectant l'équipement électrique d'un ESPE à appliquer conformément à 5.3	101
Annexe C (informative) Evaluation de la conformité	106
Bibliographie	107
Index	108

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**SÉCURITÉ DES MACHINES –
ÉQUIPEMENTS DE PROTECTION ÉLECTRO-SENSIBLES –****Partie 1: Prescriptions générales et essais****AVANT-PROPOS**

- 1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61496-1 a été établie par le comité d'études 44 de la CEI: Sécurité des machines – Aspects électrotechniques, en collaboration avec le comité d'études CENELEC 44X: Sécurité des machines – Aspects électrotechniques.

Cette édition constitue une révision technique. Dans la présente édition de cette partie de la CEI 61496, les prescriptions générales pour les ESPE de type 3 ont été ajoutées. De plus, plusieurs modifications et corrections mineures ont été effectuées afin de clarifier les prescriptions et d'aligner la présente norme avec les pratiques en usage.

Cette norme a le statut de norme de famille de produits et doit être utilisée comme référence normative pour une norme de produit concernant la sécurité des machines.

Cette norme a été rédigée afin de définir les exigences générales applicables aux équipements de protection électro-sensibles (ESPE) tout particulièrement destinés à la sécurité des machines et a été élaborée pour répondre aux besoins des constructeurs, des industriels et des organismes de sécurité.

Cette version consolidée de la CEI 61496-1 comprend la deuxième édition (2004) [documents 44/444/FDIS et 44/445/RVD], son amendement 1 (2007) [documents 44/560/FDIS et 44/568/RVD] et le corrigendum de juillet 2008.

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

Elle porte le numéro d'édition 2.1.

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

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

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

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

INTRODUCTION

Un système de protection électro-sensible (ESPE) est utilisé sur les machines présentant des risques d'accident pour les personnes. Il fournit une protection en mettant la machine en un état sûr avant qu'une personne ne puisse se trouver dans une situation dangereuse.

La présente partie de la CEI 61496 fournit les prescriptions générales de conception et de performance des ESPE utilisés pour une large gamme d'applications. Les caractéristiques essentielles des équipements satisfaisant aux prescriptions de la présente norme sont le niveau approprié de sécurité intrinsèque et les vérifications/auto-contrôles de fonctionnement, périodiques et intégrés qui sont prescrits afin de s'assurer que ce niveau de sécurité est maintenu.

Chaque type de machine présente ses propres risques (phénomènes dangereux) et l'objectif de la présente norme n'est pas de recommander la méthode d'application de l'ESPE à une machine particulière. Il convient que l'application de l'ESPE fasse l'objet d'un accord entre le fournisseur de l'équipement, l'utilisateur de la machine et l'organisme de sécurité; dans ce contexte, l'attention est attirée sur les textes de recommandation internationaux concernés, par exemple l'ISO TR 12100.

La présente partie de la CEI 61496 spécifie les prescriptions techniques des équipements de systèmes de protection électro-sensibles. L'application de la présente norme peut nécessiter l'utilisation de substances et/ou de procédures d'essai qui peuvent nuire à la santé si des précautions appropriées ne sont pas prises. La conformité à la présente norme ne dispense en aucune manière le fournisseur ou l'utilisateur de leurs obligations légales en matière de sécurité et d'hygiène des personnes dans le cadre de l'utilisation des équipements couverts par la présente norme.

SÉCURITÉ DES MACHINES – ÉQUIPEMENTS DE PROTECTION ÉLECTRO-SENSIBLES –

Partie 1: Prescriptions générales et essais

1 Domaine d'application

La présente partie de la CEI 61496 définit les prescriptions générales de conception, de construction et d'essai des équipements de protection électro-sensibles (ESPE) sans contact spécifiquement conçus pour détecter des personnes au sein d'un système relatif à la sécurité. Une attention particulière est portée sur les prescriptions de fonctionnement et de conception assurant que le niveau de sécurité approprié est atteint. Un ESPE peut proposer des fonctions optionnelles, liées à la sécurité: les prescriptions pour celles-ci sont énumérées en Annexe A.

Les prescriptions particulières pour des types spécifiques de fonctions de détection sont fournies dans d'autres parties de cette norme.

La présente norme ne prescrit ni les dimensions ou la configuration de la zone de détection, ni sa disposition par rapport aux risques (phénomènes dangereux) dans une application particulière, ni ce qui constitue un état dangereux pour une machine donnée. Elle se limite au fonctionnement de l'ESPE et à son interface avec la machine.

Bien qu'un interface données puisse être utilisé pour commander des fonctions d'ESPE relatives à la sécurité optionnelles (Annexe A), la présente norme ne fournit pas de prescriptions particulières. Les prescriptions pour ces fonctions relatives à la sécurité peuvent être déterminées par la consultation d'autres normes (par exemple, la CEI 61508, CEI/TS 62046, CEI 62061, et l'ISO 13849-1).

Il est possible que la présente norme soit utilisable pour des applications autres que la protection des personnes, par exemple la protection des machines ou des produits contre des dommages mécaniques. Dans ces applications, des prescriptions différentes peuvent être nécessaires, par exemple lorsque les matériaux qui doivent être reconnus par le dispositif de détection ont des caractéristiques différentes de celles des personnes.

Cette norme n'englobe pas les prescriptions relatives à l'émission concernant la compatibilité électromagnétique (CEM).

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

CEI 60068-2-6:1995, *Essais d'environnement – Partie 2: Essais – Essai Fc: Vibrations (sinusoïdales)*

CEI 60068-2-29:1987, *Essais fondamentaux climatiques et de robustesse mécanique – Partie 2: Essais – Essai Eb et guide: Secousses*

CEI 60204-1:1997, *Sécurité des machines – Equipement électrique des machines – Partie 1: Règles générales*

CEI 60249-2, *Matériaux de base pour circuits imprimés – Deuxième partie: Spécifications*

CEI 60439-1:1999, *Ensembles d'appareillage à basse tension – Partie 1: Ensembles de série et ensembles dérivés de série*

CEI 60445:1999, *Principes fondamentaux et de sécurité pour les interfaces homme-machines, le marquage et l'identification – Identification des bornes de matériels et des extrémités de certains conducteurs désignés et règles générales pour un système alphanumérique*

CEI 60447:1993, *Interface homme-machine (IHM) – Principes de manœuvre*

CEI 60529:2001, *Degrés de protection procurés par les enveloppes (code IP)*

CEI 60664-1:1992, *Coordination de l'isolement des matériels dans les systèmes (réseaux) à basse tension – Partie 1: Principes, prescriptions et essais*

CEI 60947-5-1:1997, *Appareillage à basse tension – Partie 5-1: Appareils et éléments de commutation pour circuits de commande – Appareils électromécaniques pour circuits de commande*

CEI 60950 (toutes les parties), *Matériels de traitement de l'information – Sécurité*

CEI 61000-4-2:1995, *Compatibilité électromagnétique (CEM) – Partie 4-2: Techniques d'essai et de mesure – Essai d'immunité aux décharges électrostatiques – Publication fondamentale en CEM*

CEI 61000-4-3:2002, *Compatibilité électromagnétique (CEM) – Partie 4-3: Techniques d'essai et de mesure – Essai d'immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques – Publication fondamentale en CEM*

CEI 61000-4-4:1995, *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure – Section 4: Essais d'immunité aux transitoires électriques rapides en sèves – Publication fondamentale en CEM*

CEI 61000-4-5:2001, *Compatibilité électromagnétique (CEM) – Partie 4-5: Techniques d'essai et de mesure – Essai d'immunité aux ondes de choc – Publication fondamentale en CEM*

CEI 61000-4-6:2001, *Compatibilité électromagnétique (CEM) – Partie 4-6: Techniques d'essai et de mesure – Immunité aux perturbations conduites, induites par les champs radioélectriques – Publication fondamentale en CEM*

CEI 61000-6-2:1999, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*

CEI 61131-2:1992, *Automates programmables – Partie 2: Spécifications et essais des équipements*

CEI 61508 (toutes les parties): *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

ISO 9001:2000, *Systèmes de management de la qualité – Exigences*

ISO/TR 12100-1:1992, *Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 1: Terminologie de base, méthodologie*

ISO/TR 12100-2:1992, *Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 2: Principes and spécifications techniques*

ISO 13849-1:1999, *Sécurité des machines – Parties des systèmes de commande relative à la sécurité – Partie 1: Principes généraux de conception*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

NOTE L'index énumère, par ordre alphabétique, les termes et les sigles définis dans le présent Article et indique où ils sont utilisés dans le texte de cette partie.

3.1

blanking

fonction optionnelle qui permet à un objet dont la taille est supérieure à la capacité de détection de l'ESPE d'être présent dans la zone de détection sans provoquer le passage à l'état INACTIF du ou des OSSD.

NOTE 1 Le blanking fixe est une technique pour laquelle les localisations des parties faisant l'objet d'un blanking ne changent pas pendant le fonctionnement. La capacité de détection des autres parties de la zone de détection demeure inchangée.

NOTE 2 Le blanking flottant est une technique pour laquelle la partie de la zone de détection faisant l'objet d'un blanking suit la localisation d'un objet se déplaçant pendant le fonctionnement. La capacité de détection des autres parties demeure inchangée.

3.2

dispositif de commande/surveillance

partie de l'équipement de protection électro-sensible (ESPE) qui:

- reçoit et traite les informations en provenance du dispositif de détection et fournit les signaux aux dispositifs de commutation du signal de sortie (OSSD),
- surveille le dispositif de détection et les OSSD

3.3

capacité de détection

limite du paramètre de la fonction de détection spécifiée par le constructeur qui entraîne une manœuvre de l'équipement de protection électro-sensible (ESPE)

3.4

zone de détection

zone dans laquelle l'éprouvette d'essai spécifiée sera détectée par l'équipement de protection électro-sensible (ESPE)

3.5

équipement de protection électro-sensible

ESPE

ensemble de dispositifs et/ou de composants travaillant conjointement pour obtenir un déclenchement de protection ou une détection de présence et comprenant au minimum

- un dispositif de détection;
- des dispositifs de commande/surveillance;
- des dispositifs de commutation des signaux de sortie et/ou un interface de données relatives à la sécurité

NOTE 1 Le système de commande relatif à la sécurité associé à l'ESPE, ou l'ESPE proprement dit, peuvent également comprendre un dispositif de commutation secondaire (SSD), des fonctions d'inhibition, des fonctions de surveillance des performances de mise à l'arrêt, etc. (voir Annexe A).

NOTE 2 Un interface de communication relatif à la sécurité peut être intégré dans la même enveloppe que l'ESPE.

3.6

dispositif de surveillance des commutateurs externes

EDM

moyen par lequel le système de protection électro-sensible (ESPE) surveille l'état des commutateurs qui lui sont externes

3.7

défaillance

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

[VEI 191-04-01, modifiée]

NOTE 1 Après une défaillance, cette entité a un défaut.

NOTE 2 Une défaillance est un passage d'un état à un autre, par opposition à un défaut, qui est un état.

NOTE 3 La notion de défaillance, telle qu'elle est définie, ne s'applique pas à une entité constituée seulement de logiciel.

NOTE 4 En pratique, les termes «défaut» et «défaillance» sont souvent utilisés comme synonymes.

3.8

défaillance dangereuse

défaillance qui empêche ou retarde la mise hors circuit et/ou le maintien à l'état INACTIF de tous les dispositifs de commutation du signal de sortie (OSSD), en réponse à une situation qui, en fonctionnement normal, les aurait mis dans cet état

3.9

défaut

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

[VEI 191-05-01, modifiée]

NOTE 1 Un défaut est souvent la conséquence d'une défaillance de l'entité elle-même, mais il peut exister sans défaillance préalable.

NOTE 2 En anglais, le terme «fault» et sa définition sont identiques à ceux donnés dans le VEI 191-05-01. Dans le domaine des machines, en français et en allemand on utilise les termes «défaut» et «Fehler» de préférence aux termes «pannes» et «Fehlzustand» qui sont donnés avec la même définition.

3.10

dispositif de commutation terminal

FSD

composant du système de commande relatif à la sécurité de la machine qui interrompt le circuit vers l'élément de commande primaire de la machine (MPCE), lorsque le dispositif de commutation du signal de sortie (OSSD) passe à l'état INACTIF

3.11

circuit intégré – complexe ou programmable

circuit monolithique, hybride ou modulaire qui satisfait au moins à un des critères ci-dessous:

- a) utilise plus de 1 000 portes logiques,
- b) propose plus de 24 entrées/sorties de connections externes,
- c) propose des fonctions programmables

NOTE 1 Exemples: ASIC, ROM, PROM, EPROM, PAL, CPU, PLA, PLD.

NOTE 2 Ces circuits peuvent être numériques, analogiques ou fonctionner dans les deux modes.

3.12

circuit intégré – simple

circuit monolithique, hybride ou modulaire qui ne satisfait à aucun des critères de 3.11

NOTE 1 Exemples: circuits intégrés SSI ou MSI, comparateurs.

NOTE 2 Ces circuits peuvent être numériques, analogiques ou fonctionner dans les deux modes.

3.13

condition de blocage à l'arrêt

condition générée par un défaut qui empêche le fonctionnement normal de l'équipement de protection électro-sensible (ESPE), provoquant le passage à l'état INACTIF de l'ensemble des dispositifs de commutation du signal de sortie (OSSD) et, le cas échéant, de l'ensemble des dispositifs de commutation secondaire (SSD)

3.14

élément de commande primaire de la machine

MPCE

élément sous tension qui commande directement le fonctionnement normal de la machine de sorte qu'il est le dernier élément (dans le temps) à fonctionner lorsque le fonctionnement de la machine est lancé ou arrêté

NOTE Cet élément peut être, par exemple, un interrupteur principal, un embrayage magnétique ou une électrovanne.

3.15

élément de commande secondaire de la machine

MSCE

élément de commande de la machine, indépendant du ou des éléments de commande principaux de la machine, capable de couper la source d'énergie de l'élément moteur des parties dangereuses correspondantes

NOTE 1 Lorsqu'il est utilisé, l'élément de commande secondaire de la machine est normalement commandé par le dispositif de commutation secondaire (SSD).

NOTE 2 Cet élément peut être, par exemple, un interrupteur principal, un embrayage magnétique ou une électrovanne.

3.16

inhibition

interruption automatique temporaire d'une ou des fonctions relatives à la sécurité par des parties de système de commande relatives à la sécurité

NOTE Pour l'inhibition de l'ESPE, voir l'Article A.7.

3.17

état INACTIF

état de la ou des sorties de l'ESPE dans lequel la machine commandée est conduite vers l'arrêt ou est empêchée de démarrer (par exemple, le circuit de sortie est coupé et empêche la circulation de courant)

3.18

état ACTIF

état de la ou des sorties de l'ESPE dans lequel la machine commandée est autorisée à fonctionner (par exemple, le circuit de sortie est fermé et permet la circulation de courant)

3.19

dispositif de commutation du signal de sortie

OSSD

composant de l'équipement de protection électro-sensible (ESPE) connecté au système de commande de la machine qui, lorsque le dispositif de détection est actionné pendant le fonctionnement normal, réagit en passant à l'état INACTIF

3.20

performance de mise à l'arrêt de l'ensemble du système

durée résultant de la somme du temps de réponse de l'équipement de protection électro-sensible (ESPE) et du temps de mise à l'arrêt de tout fonctionnement dangereux de la machine

3.21

temps de réponse

durée maximale entre l'apparition d'un événement conduisant à la manœuvre du dispositif de détection et la mise à l'état INACTIF des dispositifs de commutation du signal de sortie (OSSD)

NOTE 1 Lorsqu'un ESPE comprend un interface de données relatives à la sécurité, le temps de réponse est défini en sortie de l'interface de données relatives à la sécurité.

NOTE 2 Lorsqu'un interface de communication relative à la sécurité est compris dans l'enveloppe de l'ESPE, le temps de réponse est alors défini en sortie de l'interface de communication relative à la sécurité. Dans ce cas, le temps de réponse est aussi dépendant du protocole et de l'architecture du réseau de communication.

NOTE 3 Si un ESPE dispose à la fois d'un interface de données relatives à la sécurité et d'OSSD, l'ESPE peut avoir un temps de réponse différent pour l'interface de données relatives à la sécurité et pour les OSSD.

3.22

verrouillage du redémarrage

dispositif permettant d'empêcher le redémarrage automatique d'une machine après manœuvre du dispositif de détection pendant un cycle dangereux de fonctionnement de la machine, après modification du mode de fonctionnement de la machine et après modification du moyen de démarrage de la machine

NOTE Ces modes de fonctionnement comprennent la marche par à-coups, la marche en monocoup et la marche en automatique. Les moyens de démarrage comprennent les interrupteurs à pédale, les commandes bimanuelles et la manœuvre par simple ou double intrusion du dispositif de détection de l'équipement de protection électro-sensible (ESPE).

3.23

partie d'un système de commande relative à la sécurité

partie ou sous-partie(s) du système de commande qui répond(ent) à des signaux d'entrée et génère(nt) des signaux de sortie relatifs à la sécurité

NOTE 1 Cela comprend aussi les systèmes de surveillance.

NOTE 2 L'ensemble des parties d'un système de commande relatives à la sécurité commence aux points où les signaux relatifs à la sécurité sont créés et finit à la sortie des préactionneurs (voir également Annexe A de l'ISO/TR 12100-1).

3.24

dispositif de commutation secondaire SSD

composant qui, dans une condition de blocage à l'arrêt, passe à l'état INACTIF. Le SSD peut être utilisé pour initialiser une action de commande appropriée de la machine, par exemple l'interruption du circuit qui alimente l'élément de commande secondaire de la machine (MSCE).

3.25

dispositif de détection

partie de l'équipement de protection électro-sensible (ESPE) qui utilise le système électro-sensible pour définir l'événement ou l'état que l'équipement de protection électro-sensible (ESPE) est censé détecter

EXEMPLE Un dispositif opto-électrique de détection détecte l'entrée d'un objet opaque dans la zone de détection.

3.26

verrouillage du démarrage

dispositif qui empêche un démarrage automatique d'une machine quand l'alimentation électrique de l'équipement de protection électro-sensible (ESPE) est mise sous tension, ou est interrompue et remise sous tension

3.27

contrôleur de performance de mise à l'arrêt

SPM

moyen de surveillance destiné à déterminer si la performance de mise à l'arrêt de l'ensemble du système s'inscrit dans la ou les limites préétablies

3.28

fournisseur

entité (par exemple: constructeur, sous-traitant, installateur ou intégrateur) qui fournit des équipements ou des services associés à la machine

NOTE L'utilisateur peut agir comme son propre fournisseur.

3.29

interface de données relatives à la sécurité

interface de connexion directe (poste à poste) entre la sortie de l'ESPE et l'interface de communication relative à la sécurité qui est utilisé pour représenter l'état du ou des OSSD

NOTE 1 Un interface de données ne disposera pas d'une capacité d'adressage.

NOTE 2 L'interface de données relatives à la sécurité peut être bi-directionnel.

3.30

interface de communication relative à la sécurité

connexion relative à la sécurité à un réseau de communication normalisé prévu pour des fonctions de commande relatives à la sécurité

4 Prescriptions de fonctionnement, de conception et d'environnement

4.1 Prescriptions de fonctionnement

4.1.1 Fonctionnement normal

En fonctionnement normal, l'ESPE doit réagir en fournissant un ou des signaux de sortie appropriés lorsqu'une partie du corps d'une personne supérieure ou égale à la capacité de détection (telle que spécifiée dans la partie correspondante de la CEI 61496) pénètre ou se trouve dans la zone de détection.

Le temps de réponse de l'ESPE ne doit pas dépasser le temps indiqué par le fournisseur. Aucun moyen de réglage du temps de réponse ne doit être possible sans l'usage d'une clef, d'un mot de passe ou d'un outil.

4.1.2 Fonction de détection

La capacité de détection doit être effective dans la zone de détection spécifiée par le fournisseur. La zone de détection, la capacité de détection ou la fonction blanking (contrôlé, non-contrôlé, fixe ou flottant) ne doivent pas être réglables sans l'usage d'une clef, d'un mot de passe ou d'un outil.

4.1.3 Types d'ESPE

Dans la présente norme, trois types d'ESPE sont pris en compte. Les types diffèrent par leur performance en présence de défaut et sous influence des conditions environnementales. Dans cette partie sont pris en compte les effets des défauts électriques et électromécaniques (de tels défauts sont listés dans l'Annexe B). Des prescriptions supplémentaires sont fournies dans les autres parties où sont pris en compte des défauts générés par la technologie de détection particulière employée. Il incombe au fabricant de la machine et/ou à l'utilisateur de prescrire le type qui correspond à une application particulière.

NOTE Les prescriptions pour un ESPE de type 1 ne sont pas prises en compte à ce stade.

Un ESPE de type 2 doit remplir les prescriptions de détection de défaut de 4.2.2.3.

En fonctionnement normal, le circuit de sortie d'au moins un dispositif de commutation du signal de sortie d'un ESPE de type 2 doit être mis à l'état INACTIF lorsque la fonction de détection est actionnée ou lorsque l'alimentation de l'ESPE est retirée.

Un ESPE de type 2 doit avoir un moyen de test périodique.

Un ESPE de type 3 doit remplir les prescriptions de détection de défaut de 4.2.2.4.

Un ESPE de type 4 doit remplir les prescriptions de détection de défaut de 4.2.2.5.

En fonctionnement normal, le circuit de sortie d'au moins deux dispositifs de commutation du signal de sortie des ESPE de type 3 et de type 4 doit être mis à l'état INACTIF lorsque la fonction de détection est actionnée ou lorsque l'alimentation de l'ESPE est retirée.

Lorsqu'un seul interface de données relatives à la sécurité est utilisé pour réaliser les fonctions du ou des OSSD, l'interface de données et l'interface de communication relative à la sécurité associé doivent alors satisfaire les prescriptions de 4.2.4.4. Dans ce cas, un seul interface de données relatives à la sécurité peut remplacer deux OSSD dans un ESPE de type 3 ou de type 4.

4.2 Prescriptions de conception

4.2.1 Alimentation électrique

L'ESPE doit être conçu pour fonctionner correctement dans les conditions d'alimentation nominale prescrites ci-dessous, sauf indication contraire de l'utilisateur:

Alimentation en courant alternatif

Tension: 0,85 à 1,1 de la tension nominale

Fréquence: 0,99 à 1,01 de la fréquence nominale (régime permanent)

0,98 à 1,02 de la fréquence nominale (régime transitoire)

Distorsion harmonique: Le taux d'harmonique ne doit pas dépasser 10 % de la tension efficace totale entre conducteurs sous tension (somme des harmoniques d'ordre 2 à 5). Un taux supplémentaire de 2 % de la tension efficace totale entre conducteurs sous tension (somme des harmoniques d'ordre 6 à 30) est admissible.

Alimentation en courant continu

Alimentation par batteries

Tension: 0,85 à 1,15 de la tension nominale

0,7 à 1,2 de la tension nominale dans le cas de véhicules fonctionnant sur batterie

Alimentation par convertisseur

Tension: 0,9 à 1,1 de la tension nominale

Ondulation (crête à crête): Ne doit pas dépasser 0,05 de la tension nominale.

Pour la protection contre les chocs électriques, voir 4.2.3.2.

NOTE Pour la protection contre les interférences électriques, il convient que la source d'alimentation soit conforme aux exigences de la CEI 61000-6-2.

4.2.2 Prescriptions de détection des défauts

4.2.2.1 Généralités

L'ESPE doit répondre aux défauts énumérés dans l'Annexe B conformément à 4.2.2.3 à 4.2.2.5 selon les cas. Il ne doit pas être possible pour l'ESPE de réaliser une réinitialisation depuis une condition de blocage à l'arrêt par interruption et restauration de l'alimentation principale quand le défaut qui a initialisé la condition de blocage à l'arrêt est encore présent. A la mise sous tension et avant même que le ou les OSSD passent à l'état ACTIF, un essai doit être réalisé pour vérifier l'absence de faute interne au sein de l'ESPE.

Lorsqu'un ESPE utilise un interface de communication relative à la sécurité pour réaliser les fonctions OSSD, les prescriptions de détection des défauts des paragraphes 4.2.2.3 à 4.2.2.5 peuvent être modifiées pour inclure les prescriptions de la CEI 62061/CEI 61508 selon le SIL approprié (par exemple, SIL 3 pour Type 4, SIL 2 pour Type 3 et SIL 1 pour Type 2).

4.2.2.2 Prescriptions particulières pour un ESPE de type 1

NOTE Les prescriptions pour un ESPE de type 1 ne sont pas prises en compte à ce stade.

4.2.2.3 Prescriptions particulières pour un ESPE de type 2

Un ESPE de type 2 doit disposer d'un moyen d'essai périodique afin de révéler une défaillance dangereuse (par exemple perte de la capacité de détection, temps de réponse dépassant le temps spécifié).

Tout défaut unique ayant pour conséquence soit une perte de la capacité de détection soit l'accroissement du temps de réponse au-delà du temps spécifié, soit empêchant un ou plus des OSSD de passer à l'état INACTIF, doit conduire le prochain essai périodique à provoquer par son résultat une condition de blocage à l'arrêt.

Lorsque l'essai périodique est prévu pour être lancé par un système de commande relatif à la sécurité externe (par exemple la machine), l'ESPE doit être muni de moyens d'entrée appropriés du signal (par exemple des bornes).

La durée de l'essai périodique doit être telle que la fonction de sécurité prévue n'est pas diminuée.

NOTE Si un ESPE de type 2 est prévu pour une utilisation en détection de passage (par exemple en utilisation en ceinturage de zone) et si la durée de l'essai périodique est supérieure à 150 ms, il est possible qu'une personne s'introduise dans la zone de détection sans être détectée. Dans ce cas, il convient qu'un verrouillage du redémarrage soit inclus.

Si l'essai périodique est initialisé automatiquement, le fonctionnement correct de l'essai périodique doit être contrôlé et un défaut unique dans les parties réalisant la fonction de vérification doit être détecté. En cas de présence d'un défaut, le ou les OSSD doivent passer à l'état INACTIF.

Si un ou plusieurs OSSD ne passent pas à l'état INACTIF, une condition de blocage à l'arrêt doit être initialisée.

Un ESPE avec OSSD unique doit avoir au minimum un SSD (voir l'Article A.4).

4.2.2.4 Prescriptions particulières pour un ESPE de type 3

Tout défaut unique ayant pour conséquence soit une perte de la capacité de détection soit une augmentation du temps de réponse de l'ESPE au-delà du temps spécifié, et tout défaut unique empêchant un ou plus des OSSD de passer à l'état INACTIF doit entraîner le passage de l'ESPE dans une condition de blocage à l'arrêt dans un laps de temps tel que spécifié dans la partie applicable de cette norme, ou immédiatement après l'un des événements suivants nécessitant un changement d'état à la détection d'un défaut:

- à l'activation de la fonction de détection;
- à la réinitialisation du verrouillage du démarrage ou du redémarrage, si disponible (voir Articles A.5 et A.6).

Lorsqu'un défaut unique qui n'entraîne pas une défaillance dangereuse n'est pas détecté, l'apparition d'un défaut additionnel ne doit pas entraîner une défaillance dangereuse. Se reporter à 5.3.4 pour la vérification de cette prescription.

4.2.2.5 Prescriptions particulières pour un ESPE de type 4

Tout défaut unique ayant pour conséquence une perte de la capacité de détection doit entraîner le passage de l'ESPE dans une condition de blocage à l'arrêt dans un laps de temps au plus égal à son temps de réponse.

Tout défaut unique ayant pour conséquence soit un accroissement du temps de réponse de l'ESPE au-delà du temps spécifié, ou empêchant un ou plusieurs OSSD de passer à l'état INACTIF, doit immédiatement entraîner le passage de l'ESPE dans une condition de blocage à l'arrêt, c'est-à-dire dans un laps de temps au plus égal à son temps de réponse, ou immédiatement après l'un des événements suivants nécessitant un changement d'état à la détection d'un défaut:

- à l'activation de la fonction de détection;
- à la réinitialisation du verrouillage du démarrage ou du redémarrage, si disponible (voir Articles A.5 et A.6).

Lorsqu'un défaut unique qui n'entraîne pas une défaillance dangereuse n'est pas détecté, l'apparition d'autres défauts ne doit pas entraîner une défaillance dangereuse. Se reporter à 5.3.5 pour la vérification de cette prescription.

NOTE 1 Les mesures relatives à la conception, pour un ESPE de type 4, comprennent:

- une approche monovoie avec des mesures de détection de défaut dynamiques; ou
- une approche monovoie avec un essai interne automatique, exécuté fréquemment de façon que l'intervalle entre deux essais de défaut soit inclus dans le temps de réponse; et
- des approches multivoies telles que toute disparité entre les voies entraîne une condition de blocage à l'arrêt.

NOTE 2 Pour les prescriptions complémentaires concernant les circuits intégrés, complexes ou programmables, se référer à 4.2.10.

4.2.3 Equipement électrique de l'ESPE

4.2.3.1 Généralités

L'équipement électrique (composants) de l'ESPE doit:

- être conforme aux normes CEI appropriées quand elles existent;
- être approprié à l'usage que l'on en fait; et
- être utilisé dans sa plage de fonctionnement spécifiée.

4.2.3.2 Protection contre les chocs électriques

Une protection contre les chocs électriques doit être mise en place conformément à 6.1 de la CEI 60204-1.

4.2.3.3 Protection du matériel électrique

Une protection contre les surintensités doit être mise en place conformément à 7.2.1, 7.2.3, 7.2.7, 7.2.8 et 7.2.9 de la CEI 60204-1.

NOTE Il peut être nécessaire de donner à l'utilisateur de l'ESPE les valeurs maximales des fusibles utilisés ou les spécifications des protections contre les surtensions à mettre en place dans les circuits connectés aux points de sortie des OSSD.

4.2.3.4 Degré de pollution

L'équipement électrique de l'ESPE doit être adapté à un degré de pollution 2 (voir 6.1.2.3 de la CEI 60439-1).

4.2.3.5 Distances d'isolement, lignes de fuite et distances de sectionnement

L'équipement électrique doit être conçu et fabriqué conformément à 7.1.2 de la CEI 60439-1.

4.2.3.6 Câblage

L'équipement électrique de l'ESPE doit être câblé conformément à 7.8.3 de la CEI 60439-1.

4.2.4 Dispositifs de commutation du signal de sortie (OSSD)

4.2.4.1 Généralités

Des points de connexions de sortie séparés (bornes) doivent être prévus pour chaque OSSD.

Il convient que les OSSD soient calculés pour que leurs charges puissent être commutées sans qu'il soit nécessaire d'utiliser des dispositifs d'extinction d'arc.

NOTE Pour une meilleure fiabilité, il est fortement recommandé que des dispositifs de protection contre les surtensions de manœuvre soient utilisés et reliés aux charges et non aux contacts.

Il convient que les circuits de sortie des OSSD soient correctement protégés afin d'éviter les défaillances dangereuses comme, par exemple, ce qui résulte de la soudure de contacts de relais dans des conditions de surintensité (voir 7.2.9 de la CEI 60204-1).

Il convient que des mesures soient fournies pour minimiser la possibilité de défaillances dangereuses résultant de défaillances de mode commun.

Il est admis que certaines fonctions des systèmes de commande de sécurité des machines soient réalisées par l'ESPE; à titre d'exemple, il est admis que l'OSSD assure les fonctions d'un FSD.

Un ESPE de type 3 ou de type 4 doit comprendre au minimum deux OSSD activés indépendamment l'un de l'autre.

Une référence à une action de l'OSSD (par exemple le passage à l'état INACTIF) signifiera aussi une action correspondante d'un interface de données relatives à la sécurité. Un seul interface de données relatives à la sécurité peut satisfaire les exigences de deux OSSD.

4.2.4.2 OSSD à relais

Si des OSSD à relais sont fournis, l'état (la position) des contacts doit être surveillé. Ceci peut être réalisé en surveillant l'état des contacts auxiliaires des relais qui ont des contacts mécaniquement liés (guidés positivement). Le lien mécanique assure que le contact surveillé suit le changement d'état des contacts OSSD.

Des mesures particulières de conception et de construction doivent être prises pour assurer que le ou les contacts de travail (normalement ouverts) et que le ou les contacts de repos (normalement fermés) ne puissent être simultanément dans une position fermée.

NOTE 1 Le lien mécanique assure que le contact surveillé suit le changement d'état des contacts des OSSD.

NOTE 2 Il est important que la tension à la retombée et que la distance de séparation entre les contacts soient maintenues au niveau adéquat pendant toute la durée de vie spécifiée du relais.

4.2.4.3 OSSD à semi-conducteurs

Les OSSD à semi-conducteurs peuvent être indifféremment de type PNP ou NPN. Quand des sorties PNP sont fournies, elles doivent suivre les exigences de ce paragraphe.

NOTE 1 Les exigences pour les sorties NPN qui peuvent être demandées pour certaines applications ne sont pas définies dans cette norme. Il convient de porter une attention particulière à leur utilisation (quand ces sorties sont utilisées, un court-circuit au potentiel de référence ou un circuit ouvert seront interprétés par les entrées et les charges comme l'état ACTIF). Il est recommandé de tenir compte des exigences de la CEI 60204-1, 9.1.4.

NOTE 2 Pour une tension nominale de 24 V en courant continu, il est recommandé que les valeurs de tension de sortie et de courant pour l'état ACTIF et l'état INACTIF soient conformes au tableau suivant.

Tension nominale	Plage de sortie état INACTIF	Plage de sortie état ACTIF	Sortie état INACTIF (courant de fuite maximal)	Sortie état ACTIF
24 V courant continu	- 3 V ... + 2 V eff (+ 5 V pic)	+ 11 V ... + 30 V	< 2 mA	> 6mA

NOTE 3 Les valeurs du tableau ci-dessus sont conformes aux exigences de la CEI 61131-2 (voir 3.3 de la CEI 61131-2), pour une tension nominale de 24 V en courant continu. Quand d'autres tensions d'alimentation sont utilisées, cette norme peut être utilisée comme un guide. On peut se référer à la CEI 61131-2 pour toute information complémentaire.

La ou les sorties doivent être protégées contre les effets des surtensions, surintensités et courts-circuits.

L'intensité maximale du courant de fuite ne doit pas dépasser 2 mA, même en cas de défauts (par exemple un circuit ouvert).

Quand il y a plus d'un OSSD, les courts-circuits entre les sorties des OSSD doivent être détectés.

Le fournisseur de l'ESPE doit fournir l'information suivante dans les documents d'accompagnement:

- courant de sortie nominal et maximal dans l'état ACTIF sur charge résistive et inductive,
- tension maximale dans l'état INACTIF,
- courant de sortie maximal dans l'état INACTIF (courant de fuite),
- charge maximale capacitive,
- résistance maximale maximum des connections entre le ou les OSSD et la ou les charges.

4.2.4.4 Interface de données relatives à la sécurité et interface de communication relative à la sécurité

Lorsque le dispositif de détection est activé pendant le fonctionnement normal, l'ESPE doit répondre en transmettant une information indiquant l'état du dispositif de détection ou de l'ESPE au travers d'un interface de données relatives à la sécurité. L'information d'état est convertie en un message de données par l'interface de communication relative à la sécurité.

L'interface de communication relative à la sécurité doit disposer de la même protection contre les défauts que celle appropriée au type d'ESPE.

Selon la conception de l'ESPE, l'interface de communication relative à la sécurité peut soit être extérieur dans une enveloppe séparée (Figure 1a), soit être intégré dans la même enveloppe que l'ESPE (Figure 1b).

L'interface de communication relative à la sécurité doit satisfaire les prescriptions appropriées de la CEI 62061/CEI 61508 selon le SIL approprié (par exemple, SIL 3 pour Type 4, SIL 2 pour Type 3 et SIL 1 pour Type 2) en complément des prescriptions de la présente norme (CEI 61496-1).

Lorsque l'interface de communication relative à la sécurité est intégré dans l'ESPE, l'ESPE dans sa totalité doit satisfaire les prescriptions appropriées de la CEI 62061/CEI 61508.

NOTE En raison de la technologie spécifique des interfaces de communication, différentes normes autres que la CEI 61496-1 s'appliquent. Afin d'éviter le chevauchement avec d'autres normes, les prescriptions fonctionnelles de l'interface de communication relative à la sécurité ne sont pas définies dans la présente norme.

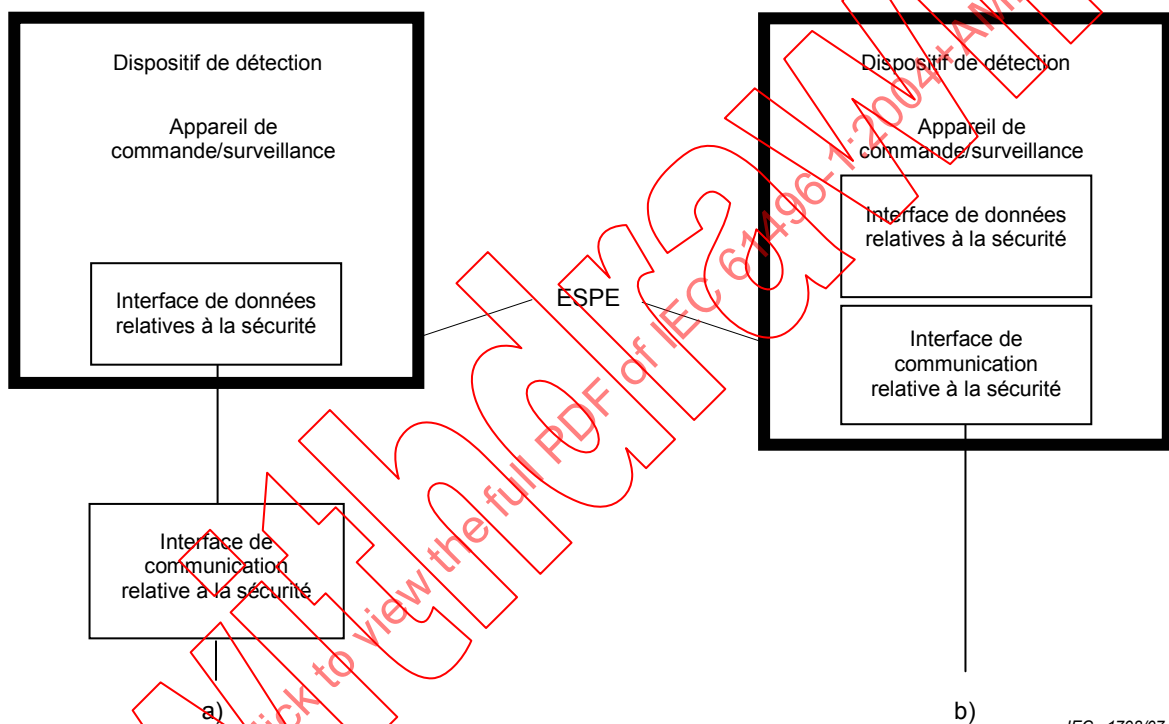


Figure1 – Exemples d'ESPE utilisant des interfaces de communication relatives à la sécurité

4.2.5 Indicateurs lumineux et afficheurs

Des dispositifs particuliers doivent être fournis par le fabricant de l'ESPE pour:

- indiquer la manœuvre du dispositif de détection. Ni le délai entre la manœuvre du dispositif de détection et le moment où l'indicateur atteint 50 % de sa luminosité, ni le délai à partir du moment où le dispositif de détection est désactivé jusqu'au moment où la luminosité du voyant descend à 50 % de sa valeur initiale ne doivent dépasser 100 ms;
- indiquer l'état de sortie d'un OSSD. L'état ACTIF doit être représenté par un voyant vert et l'état INACTIF par un voyant rouge. Quand deux OSSD ou plus sont conçus pour opérer en coordination, un jeu unique de voyants peut être partagé.

Quand il y a deux indicateurs ou plus de la même couleur, la fonction de chaque indicateur doit être marquée sans ambiguïté.

NOTE Dans certains modes de fonctionnement, le jeu d'indicateurs utilisé pour le point a) peut aussi l'être pour le point b).

Les indicateurs sont prévus pour l'opérateur de la machine. C'est pourquoi ils doivent pouvoir être localisés près de la zone de détection et être visibles quand l'équipement est installé. Ils peuvent être intégrés dans les éléments du capteur ou installés comme un équipement externe près de la zone de détection.

4.2.6 Dispositif de réglage

Tout dispositif de réglage doit être conçu de telle façon qu'aucune position dans sa plage de réglage ne puisse conduire à une défaillance dangereuse. Une défaillance du dispositif de réglage ne doit pas provoquer une modification non prévue de la configuration de l'ESPE.

4.2.7 Débranchement des sous-systèmes

Lorsqu'il existe des dispositifs permettant de débrancher un sous-système, une partie d'un sous-système ou un composant embrochable, le débranchement doit entraîner le passage d'au moins un OSSD à l'état INACTIF, conformément à 4.2.2.

4.2.8 Composants non électriques

Les composants non électriques doivent être adaptés à l'utilisation prévue.

4.2.9 Défaillances de mode commun

Il convient que la conception minimise la possibilité d'une défaillance dangereuse provenant de défaillances de mode commun pour les causes suivantes.

- influences de l'environnement;
- systèmes multivoies utilisant le même substrat;
- courts-circuits entre canaux sur des systèmes multivoies.

NOTE 1 Les défaillances de mode commun peuvent aussi provenir de l'utilisation de composants dégradés par des erreurs de manipulation, de fabrication, etc.

NOTE 2 Les défaillances de mode commun sont considérées comme des défaillances uniques.

Les composants d'un substrat semi-conducteur commun ne doivent pas être utilisés pour plus d'une voie d'un système multivoie.

4.2.10 Circuits intégrés, complexes ou programmables

Lorsque des circuits intégrés monolithiques numériques complexes ou programmables sont utilisés dans un ESPE de type 4, la sécurité intrinsèque doit être maintenue au minimum par deux voies de commande/surveillance indépendantes. Cette prescription doit être vérifiée conformément à 5.5.

4.2.11 Logiciel, programmation, conception de fonctionnement des circuits intégrés

4.2.11.1 Généralités

Lorsque les fonctions de sécurité de l'ESPE reposent sur l'un des moyens suivants, les prescriptions supplémentaires de 4.2.11.2 doivent s'appliquer:

- a) un logiciel est utilisé pendant le fonctionnement de l'ESPE;
- b) l'ESPE comporte un composant programmé dont les fonctions ont été réglées au cours d'un processus consécutif à sa fabrication initiale (exemples: PAL, PLA, PLD, PROM);
- c) l'ESPE comporte un composant spécifique, tel un ASIC, un microprocesseur à programmation masquée, une ROM.

La conformité à ces prescriptions doit être vérifiée conformément à 5.5.

4.2.11.2 Prescriptions

- a) Le logiciel, le programme du capteur et la conception de la fonction du capteur doivent être développés en conformité avec la CEI 61508-3 pour le SIL approprié (par exemple, SIL3 pour le Type 4, SIL2 pour le Type 3 et SIL1 pour le Type 2).
- b) Une documentation doit être disponible attestant de l'adéquation du logiciel aux procédures du système d'assurance qualité. Cette documentation doit montrer que le niveau de performance lié à la sécurité a été atteint.
- c) Un plan de qualité documenté, montrant de façon claire toutes les étapes du développement, et indiquant les critères de validation de chaque étape, doit être fourni. Ces étapes du développement peuvent être par exemple le cahier des charges, la spécification, la vérification et la validation de la conception.
- d) Avant tout développement, la conception globale de l'ESPE doit être analysée pour déceler les risques (phénomènes dangereux) et les modes de défaillance, afin d'identifier, dans une exigence des prescriptions de sécurité, les fonctions relatives à la sécurité de l'ESPE. Tout ou partie des fonctions relatives à la sécurité de l'ESPE doit être alloué à des moyens de 4.2.11, et la caractéristique relative à la sécurité de chaque élément doit être déterminée. Des techniques de développement adaptées doivent être utilisées pour les exigences, la conception, la mise en oeuvre et la maintenance afin d'atteindre les caractéristiques relatives à la sécurité requises.
- e) Les prescriptions pour le logiciel, pour la conception du programme, et celui du comportement de fonctionnement, de chacune des parties concernées par 4.2.11.1 doivent être complètes et sans ambiguïté. Toutes les exigences doivent permettre à celui qui fait l'évaluation ou la validation (c'est-à-dire une personne autre que le concepteur) de remonter correctement à la spécification des prescriptions de sécurité pour confirmer que les fonctions relatives à la sécurité sont correctement prises en compte.
- f) Un plan d'essai complet doit être établi pour démontrer que le produit exécute correctement les fonctions relatives à la sécurité spécifiées dans les prescriptions de sécurité. L'essai du logiciel, du programme et les exigences de fonctionnement doivent figurer dans le dossier du projet pour prouver que le modèle est conforme aux prescriptions de sécurité.
- g) Le logiciel, la conception du programme et des exigences de fonctionnement doivent faire l'objet d'une gestion effective de la mise en place et d'un contrôle des évolutions. Pendant le développement, des procédures effectives doivent faire la preuve que toute évolution dans les prescriptions, les exigences, la conception, etc. est convenablement documentée et que leur impact est analysé de façon que la spécification des prescriptions de sécurité puisse être suivie à chaque étape du processus de développement. La conception doit être protégée contre toute évolution non autorisée et sa configuration précise (par exemple liste des modules, numéro de la version) doit être enregistrée avec soin.
- h) Quand un logiciel est exécuté pendant le fonctionnement de l'ESPE, l'ensemble des instructions logicielles doivent être contenues dans une mémoire à lecture seule ne pouvant pas être reprogrammée par le processeur. Des techniques appropriées doivent être adoptées pour vérifier le déroulement normal du programme et l'intégrité du logiciel. Parmi ces techniques possibles, on compte les chiens de garde, les contrôles de RAM ou de ROM, les essais CPU, etc.
- i) Quand des outils logiciels comme des compilateurs ou des traducteurs (assembleurs exceptés) sont utilisés pour le développement du logiciel, on ne doit pas considérer qu'il y a hétérogénéité du logiciel, sauf si:
 - les outils logiciels utilisés pour les divers programmes sont totalement indépendants;
 - le ou les outils logiciels ont reçu un «certificat de validation» conformément à une norme nationale ou internationale reconnue;
 - le plan d'essai contient des essais appropriés pour détecter les erreurs de mode commun introduites par l'outil logiciel.
- j) Par principe de conception, la partie de logiciel relative à la sécurité devrait être isolée, autant que possible, des parties de la conception non relatives à la sécurité, de façon à minimiser la possibilité de perturbations des fonctions de sécurité et à simplifier l'évaluation des caractéristiques de sécurité.

4.3 Prescriptions relatives aux conditions ambiantes

4.3.1 Plage de températures ambiantes de l'air et humidité

L'ESPE doit satisfaire aux prescriptions de la présente norme lorsqu'il est soumis à des variations de la température ambiante de 0 °C à 50 °C. Lorsque l'ESPE est destiné à être utilisé à l'extérieur de cette plage de températures, le fournisseur doit préciser la plage de températures dans laquelle le système continuera à fonctionner normalement. La conformité à cette prescription doit être vérifiée au moyen des essais indiqués en 5.4.2 avec une humidité de 95 %, sans condensation, pour des températures variant entre 20 °C et la température ambiante maximale définie en 5.4.2.

4.3.2 Perturbations électriques

4.3.2.1 Variations de la tension d'alimentation

L'ESPE ne doit pas présenter de défaillance dangereuse lorsque la tension d'alimentation externe est réduite régulièrement et en continu à partir de sa valeur nominale jusqu'à la tension zéro, sur une période de 10 s à 20 s, puis augmentée de manière similaire à partir de la tension zéro jusqu'à sa valeur nominale.

L'ESPE ne doit pas présenter de défaillance dangereuse lorsque l'on fait varier tour à tour chaque tension d'alimentation interne, de manière régulière et en continu sur une période de 10 s à 20 s, de la tension nominale jusqu'à la tension zéro, puis lorsque l'on augmente cette tension de manière similaire de la tension zéro à la tension nominale.

4.3.2.2 Interruptions de la tension d'alimentation

Lorsque des interruptions de la tension d'alimentation (creux de tension) sont appliquées selon le Tableau 1, l'ESPE doit satisfaire aux essais 1) et 2) en continuant de fonctionner normalement, et à l'essai 3) sans défaillance dangereuse.

Tableau 1 – Interruptions de la tension d'alimentation

Essai	Valeur du creux de tension assignée %	Durée du creux ms	Fréquence Hz
1)	100	10	10
2)	50	20	5
3)	50	500	0,2

Lorsque l'ESPE est conçu pour être alimenté par un ou des types particulier d'alimentation (par exemple alimentation directe à partir de l'interface de communication relative à la sécurité), les interruptions de la tension d'alimentation dans le présent paragraphe peuvent être appliquées à l'entrée principale de l'alimentation spécifiée au lieu de directement à l'ESPE.

4.3.2.3 Transitoires rapides en salves

4.3.2.3.1 Prescriptions générales

L'ESPE doit continuer à fonctionner normalement lorsqu'il est soumis à des transitoires rapides en salves conformément à la CEI 61000-4-4:

Ports d'alimentation à moins de 50 V c.a. ou c.c. Ports pour le signal, etc., et d'une longueur supérieure à 1 m	1 kV (crête) selon le niveau de sévérité d'essai 2 de la CEI 61000-4-4
Ports d'alimentation pour 50 V c.a. et plus	2 kV (crête) selon le niveau de sévérité d'essai 3 de la CEI 61000-4-4

4.3.2.3.2 Prescriptions supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 ne doit pas présenter de défaillance dangereuse lorsqu'il est soumis à des transitoires rapides en salves conformément à la CEI 61000-4-4:

Ports d'alimentation c.c. et à moins de 50 V c.a. Ports pour le signal, etc. d'une longueur supérieure à 1 m	2 kV (crête) selon le niveau de sévérité d'essai 3 de la CEI 61000-4-4
Ports d'alimentation pour 50 V c.a. et plus	4 kV (crête) selon le niveau de sévérité d'essai 4 de la CEI 61000-4-4

4.3.2.4 Ondes de choc

4.3.2.4.1 Prescriptions générales

L'ESPE doit continuer à fonctionner normalement lorsqu'il est soumis à des ondes de choc conformément à la CEI 61000-4-5:

Ports pour le signal d'une longueur supérieure à 1 m Port d'alimentation c.c. ou inférieur à 50 V c.a.	1 kV (crête) en mode commun selon le niveau de sévérité d'essai 2 de la CEI 61000-4-5
Ports d'alimentation pour 50 V c.a. et plus.	2 kV (crête) en mode commun et 1 kV (crête) en mode différentiel, selon le niveau de sévérité d'essai 3 de la CEI 61000-4-5

4.3.2.4.2 Prescriptions supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 ne doit pas présenter de défaillance dangereuse lorsqu'il est soumis à des ondes de choc conformément à la CEI 61000-4-5:

Ports pour le signal d'une longueur supérieure à 1 m Port d'alimentation c.c. ou inférieur à 50 V c.a.	2 kV (crête) en mode commun, selon le niveau de sévérité d'essai 3 de la CEI 61000-4-5
Ports d'alimentation pour 50 V c.a. et plus	4 kV (crête) en mode commun et 2 kV (crête) en mode différentiel, selon le niveau de sévérité d'essai 4 de la CEI 61000-4-5

4.3.2.5 Champ électromagnétique

4.3.2.5.1 Prescriptions générales

L'ESPE doit continuer à fonctionner normalement lorsqu'il est soumis à un champ électromagnétique conformément à 5.1 de la CEI 61000-4-3:

10 V/m selon le niveau de sévérité d'essai 3.

4.3.2.5.2 Prescriptions supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 ne doit pas présenter de défaillance dangereuse lorsqu'il est soumis à un champ électromagnétique conformément à 5.2 la CEI 61000-4-3:

30 V/m selon le niveau de sévérité d'essai 4.

4.3.2.6 Perturbations conduites aux fréquences radioélectriques

4.3.2.6.1 Prescriptions générales

L'ESPE doit continuer à fonctionner normalement lorsqu'il est soumis à des perturbations conduites dues aux fréquences radioélectriques émises conformément à la CEI 61000-4-6:

Ports pour le signal, etc. d'une longueur comprise entre 1 m et 10 m	3 V (eff.) selon le niveau de sévérité d'essai 2 de la CEI 61000-4-6
Ports pour le signal, etc. d'une longueur dépassant 10 m Ports d'alimentation. Ports de terre	10 V (eff.) selon le niveau de sévérité d'essai 3 de la CEI 61000-4-6

4.3.2.6.2 Prescriptions supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 ne doit pas présenter de défaillance dangereuse lorsqu'il est soumis à des perturbations dues aux fréquences radioélectriques émises conformément à la CEI 61000-4-6:

Ports pour le signal, etc. d'une longueur comprise entre 1 m et 10 m	10 V (eff.) selon le niveau de sévérité d'essai 3 de la CEI 61000-4-6
Ports pour le signal, etc. d'une longueur dépassant 10 m. Ports d'alimentation. Ports de terre.	30 V (eff.) selon le niveau de sévérité d'essai X de la CEI 61000-4-6

4.3.2.7 Décharge électrostatique

4.3.2.7.1 Prescriptions générales

L'ESPE doit continuer à fonctionner normalement lorsqu'il est soumis à une décharge électrostatique conformément à la CEI 61000-4-2:

6 kV en contact ou 8 kV pour une décharge dans l'air,
selon le niveau de sévérité d'essai 3 de la CEI 61000-4-2.

4.3.2.7.2 Prescriptions supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 ne doit pas présenter de défaillance dangereuse lorsqu'il est soumis à une décharge électrostatique conformément à la CEI 61000-4-2:

8 kV en contact, ou 15 kV pour une décharge dans l'air,
selon le niveau de sévérité d'essai 4 de la CEI 61000-4-2.

4.3.3 Environnement mécanique

4.3.3.1 Vibrations

L'ESPE doit pouvoir continuer à fonctionner normalement pendant les essais de vibrations de 5.4.4.1.

4.3.3.2 Chocs

L'ESPE doit pouvoir continuer à fonctionner normalement pendant les essais de chocs de 5.4.4.2.

4.3.4 Enveloppes

L'ESPE doit disposer de sa ou ses propres enveloppes.

Toutes les enveloppes d'ESPE, y compris celles montées à distance, doivent fournir un degré de protection d'au moins IP54 (voir la CEI 60529), lorsqu'elles sont montées conformément aux exigences du fournisseur. Cependant, lorsqu'elle est montée dans une enveloppe de commande de la machine ayant un degré de protection d'au moins IP54, une enveloppe d'ESPE doit avoir un degré de protection d'au moins IP20.

NOTE La protection contre les dommages mécaniques peut être réalisée par:

- l'utilisation d'un emplacement approprié;
- l'utilisation de matériaux adaptés et une forme de construction assurant une résistance adéquate; ou
- l'utilisation d'une barrière de protection.

Les entrées de câbles ne doivent pas affecter le degré de protection.

Des produits d'étanchéité qui adhèrent aux deux surfaces à joindre, tels que la protection vis-à-vis de l'atmosphère ambiante est affectée lorsque le joint est retiré, ne doivent pas être utilisés pour assurer l'étanchéité des couvercles qui pourraient être retirés lors de l'entretien.

Les enveloppes doivent être exemptes de bords ou angles acérés qui risquent d'endommager l'isolement du câblage. La conformité à cette prescription doit être vérifiée par inspection.

Les enveloppes doivent permettre un accès permettant d'effectuer les réglages et travaux de maintenance nécessaires, en toute sécurité et de manière efficace. Les couvercles autorisant ces accès doivent disposer de fixations.

5 Essais

5.1 Généralités

5.1.1 Essais de type

5.1.1.1 Échantillons d'essai

Dans la mesure où cela est possible, toutes les parties de l'ESPE doivent être essayées ensemble. Quand cela n'est pas possible, il est admis que les parties de l'ESPE soient essayées séparément. De telles situations apparaissent dans le cas des ESPE intégrés (normalement indissociables de la machine) lors des essais d'environnement. Dans de tels cas:

- tout signal d'entrée nécessaire au fonctionnement de l'ESPE doit être simulé;
- ces exceptions et toutes omissions d'essais doivent être consignées dans le rapport d'essai.

Lorsqu'un essai particulier risque d'être destructif et que des résultats identiques peuvent être obtenus en soumettant à l'essai des parties isolées de l'ESPE, un échantillon de la partie correspondante peut être utilisé au lieu d'un échantillon de l'ensemble de l'équipement pour obtenir les résultats de l'essai.

Si l'ESPE est conçu pour des tensions d'alimentation différentes (par exemple, pour diverses applications), il est admis d'utiliser plusieurs échantillons.

Quand l'ESPE est conçu pour être alimenté par une alimentation externe spéciale, l'ESPE doit être essayé avec cette alimentation spécifique (voir 6.2).

5.1.1.2 Conditions de fonctionnement

Sauf prescription contraire dans la procédure d'essai, les essais doivent être effectués en plaçant l'échantillon d'essai dans la position prescrite dans les documents d'accompagnement.

Pour les essais d'immunité aux perturbations électriques, la position de l'équipement doit être aussi proche que possible de sa configuration de fonctionnement finale (c'est-à-dire muni de tous les périphériques et couvercles, relié à l'alimentation et, si besoin est, relié au conducteur externe de protection et/ou au conducteur de liaison fonctionnelle externe (voir la CEI 60204-1)).

Lorsque diverses positions de montage sont prescrites, la position de montage la moins favorable doit être utilisée.

Si un interface de données relatives à la sécurité est utilisé à la place d'un ou de plusieurs OSSD, l'ESPE doit être raccordé à un système de communication selon les instructions du fabricant et disposant d'un moyen de surveillance de l'état de l'ESPE.

5.1.1.3 Pénétration simulée dans la zone de détection

Dans les essais suivants, l'introduction de l'éprouvette d'essai (telle que définie dans la partie appropriée de cette norme) dans la zone de détection peut être simulée s'il est démontré que cette méthode est équivalente.

5.1.2 Conditions d'essai

5.1.2.1 Environnement d'essai

Sauf prescription contraire en 5.4, les essais doivent être effectués lorsque l'ESPE fonctionne dans les conditions suivantes:

- tension assignée (ou une tension dans la plage de tensions assignées);
- fréquence assignée (ou une fréquence dans la plage de fréquences assignées);
- température ambiante de $20\text{ °C} \pm 5\text{ °C}$;
- humidité relative entre 25 % et 75 %;
- pression barométrique entre 86 kPa et 106 kPa.

NOTE Les valeurs indiquées sur le marquage de l'équipement ainsi que sur les documents joints sont considérées comme des valeurs assignées.

5.1.2.2 Précision de mesure

Les erreurs de mesure ne doivent pas dépasser:

- pour le temps de réponse de l'ESPE: $\pm 1\text{ ms}$;
- pour les températures: $\pm 3\text{ °C}$;
- pour les valeurs électriques: $\pm 1\text{ %}$, quand c'est techniquement possible et/ou approprié;
- pour l'humidité relative (HR): $\pm 3\text{ % HR}$;
- pour les mesures linéaires: la valeur la plus grande entre $\pm 1\text{ mm}$ et $\pm 1\text{ %}$.

Toutes les mesures doivent être effectuées dans des conditions de température stabilisées. On considère que cette condition est remplie lorsque le taux de variation de température (baisse ou augmentation) est inférieur à 2 K/h.

5.1.2.3 Conditions d'essai relatives aux conditions ambiantes pour un ESPE prévu être utilisé avec un interface de communication relative à la sécurité

L'ESPE et l'interface de communication relative à la sécurité doivent être essayés ensemble (voir Figure 2). En raison du fait que l'interface de communication relative à la sécurité ne délivre pas un signal de sortie logique, il est nécessaire d'utiliser un récepteur de données. Ce dispositif d'essai est constitué de l'équipement soumis à essai et d'un récepteur de données (par exemple un automate programmable ou un appareil de surveillance) qui indique l'état du dispositif de détection ou de l'ESPE.

Lors de l'essai relatif à la sensibilité aux perturbations électriques, un adaptateur d'essai approprié isolant l'ESPE soumis à essai du bus de communication peut être exigé.

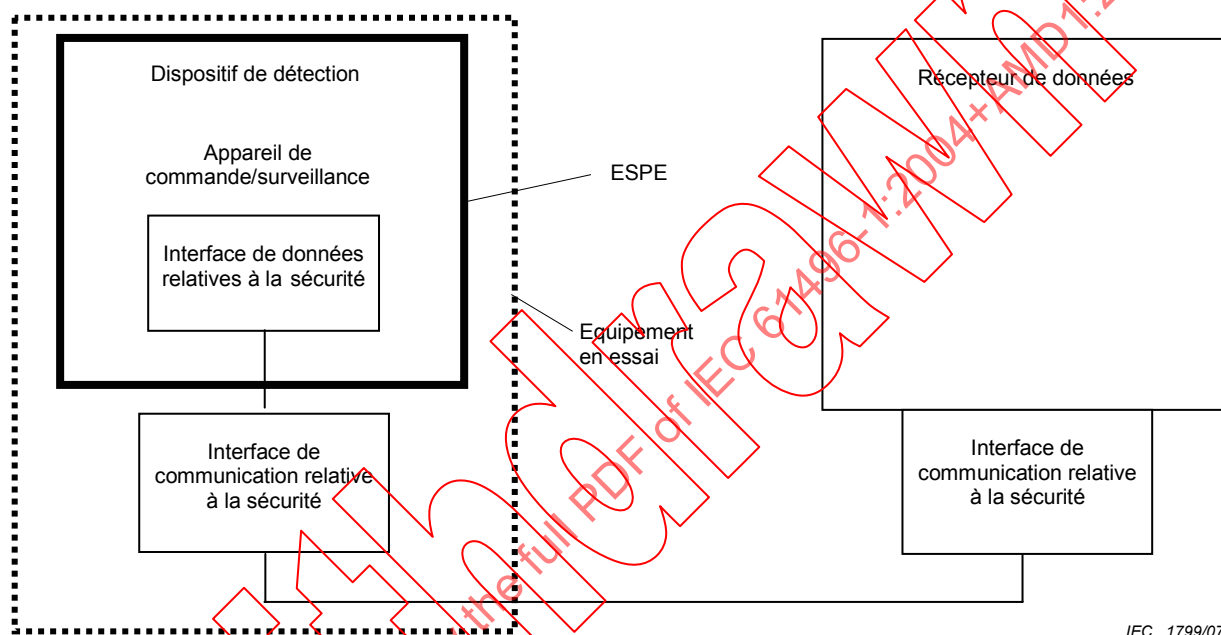


Figure 2 – Dispositif d'essai pour l'essai CEM des ESPE avec des interfaces de communication relatives à la sécurité

5.1.3 Résultats des essais

Les résultats des essais et analyses énumérés dans le présent paragraphe doivent être consignés par écrit. Les résultats d'essai doivent être fournis sous une forme qui présente les particularités de chaque essai individuel et ses effets. Les détails de procédure pour tout essai particulier doivent être inclus dans le rapport d'essai.

NOTE Il est recommandé que les résultats des essais soient examinés conformément à l'Annexe C.

5.2 Essais de fonctionnement

5.2.1 Fonction de détection

La fonction de détection et l'intégrité de la capacité de détection et de la zone de détection (par exemple la taille, la forme et l'emplacement) de l'ESPE doivent être essayées comme spécifié dans la partie appropriée de la CEI 61496.

5.2.2 Temps de réponse

Le temps de réponse doit être mesuré par une analyse systématique et des essais.

Il est admis de vérifier le temps de réponse par une simulation électrique de la manœuvre, à condition qu'elle prenne en compte le temps maximal entre l'événement déclenchant la manœuvre du dispositif de détection et la manœuvre.

Des prescriptions additionnelles pour la mesure du temps de réponse de l'ESPE sont éventuellement données dans la partie appropriée de la CEI 61496.

5.2.3 Essais de fonctionnement limités

5.2.3.1 Généralités

Les essais de fonctionnement limités A, B, et C ci-après doivent être effectués afin de vérifier que, dans des conditions ambiantes normales, l'ESPE continue à fonctionner normalement et que, dans des conditions ambiantes anormales ou dans des conditions de défaut, l'ESPE ne présente pas de défaillance dangereuse.

Si l'ESPE dispose d'une fonction de verrouillage du redémarrage, cette fonction doit être court-circuitée ou non sélectionnée lors de l'exécution des essais. L'essai de la fonction de verrouillage du redémarrage doit être effectué séparément (voir Annexe A).

Lors de l'utilisation d'un interface de communication relative à la sécurité, dans les essais de fonctionnement limités suivants, les passages des OSSD à l'état ACTIF ou à l'état INACTIF sont remplacés par un message relatif à la sécurité (par exemple un message de données) indiquant l'état correspondant du dispositif de détection ou de l'ESPE.

5.2.3.2 Essai de fonctionnement limité A (essai A)

Sans aucune intrusion dans la zone de détection, il doit être observé que, pour une période d'au moins 5 s – sauf prescription contraire – le ou les OSSD sont à l'état ACTIF et ne passent pas à l'état INACTIF.

5.2.3.3 Essai de fonctionnement limité B (essai B)

Sans aucune intrusion dans la zone de détection, il doit être observé que, pour une période d'au moins 5 s – sauf prescription contraire – le ou les OSSD sont à l'état ACTIF et ne passent pas à l'état INACTIF.

L'éprouvette d'essai doit être amenée dans la zone de détection. Le ou les OSSD doivent réagir en passant de l'état ACTIF à l'état INACTIF. Il doit être observé que, pour une période d'au moins 5 s – sauf prescription contraire – le ou les OSSD restent à l'état INACTIF avec l'éprouvette d'essai présente dans la zone de détection, ou que l'ESPE reste actionné de toute autre manière.

L'éprouvette d'essai doit être retirée de la zone de détection ou l'échantillon doit être désactivé d'une autre manière. Le ou les OSSD doivent réagir en passant de l'état INACTIF à l'état ACTIF. Il doit être observé, pendant une période d'au moins 5 s – sauf prescription contraire – que le ou les OSSD restent à l'état ACTIF lorsque l'éprouvette d'essai n'est pas présente dans la zone de détection, ou que l'ESPE reste physiquement désactivé d'une autre manière.

Il est possible que les essais ci-dessus doivent être répétés de manière continue selon les exigences d'essais.

5.2.3.4 Essai de fonctionnement limité C (essai C)

Cet essai est similaire à l'essai de fonctionnement limité B, mais lorsque le ou les OSSD devraient être à l'état ACTIF, il est autorisé qu'ils soient à l'état INACTIF. Aucune défaillance dangereuse ne doit avoir lieu. A la fin de chacun des essais appropriés de 5.4, l'ESPE doit continuer à fonctionner normalement ou doit revenir au fonctionnement normal après cessation d'une condition de blocage à l'arrêt.

Si l'ESPE ne peut revenir à un fonctionnement normal en raison d'une défaillance permanente d'un composant, il est acceptable s'il est vérifié que la défaillance ne provient que des composants de l'interface de communication et que le ou les OSSD restent à l'état INACTIF.

NOTE Dans des conditions de perturbations électriques extrêmes (comme lors des essais de défaillance), il est probable que certains composants de l'interface de communication tomberont en panne de façon permanente et ne permettront pas à l'ESPE de retrouver un fonctionnement normal.

5.2.4 Essai périodique

Pour un ESPE de type 2, les prescriptions de 4.2.2.3 doivent être vérifiées par l'analyse et la mesure.

5.2.5 Indicateurs lumineux et afficheurs

Les fonctions et couleurs des indicateurs lumineux et afficheurs doivent être vérifiées conformément à 4.2.5 en appliquant un essai B.

5.2.6 Moyens de réglage

Les prescriptions de 4.1.1 et 4.1.2 doivent être vérifiées par inspection. Les prescriptions de 4.2.6 doivent être vérifiées par inspection et en exécutant des essais C, si nécessaire.

5.2.7 Valeurs assignées des composants

Le fonctionnement de chaque composant dans les limites de ses valeurs assignées spécifiées, pour toute la gamme de fonctionnement de l'ESPE doit être vérifié par analyse et/ou par inspection.

5.2.8 Dispositifs de commutation du signal de sortie (OSSD)

5.2.8.1 Généralités

L'existence de points de connexion de sortie (bornes) séparés pour chaque OSSD doit être vérifiée par inspection.

Quand deux OSSD sont fournis, il doit être vérifié par inspection ou essai que les OSSD sont actionnés indépendamment l'un de l'autre.

Il doit être vérifié par inspection que les OSSD sont protégés par des systèmes de limitation du courant ou que l'information sur l'installation de systèmes de limitation du courant est fournie dans la notice d'utilisation.

Il doit être vérifié qu'aucune défaillance prévisible n'aura pour conséquence le passage ou le maintien d'au moins un OSSD à l'état ACTIF. Tous les essais doivent être conduits sur charge inductive maximale et avec la longueur de câble maximale spécifiées par le constructeur.

Les défaillances prévisibles comprennent:

- le court-circuit entre l'OSSD et l'alimentation;
- le court-circuit entre l'OSSD et la terre;
- le court-circuit entre OSSD;
- le circuit ouvert sur le câble de retour de l'alimentation;
- le circuit ouvert sur le câble de liaison fonctionnelle du conducteur;
- le circuit ouvert sur le blindage d'un câble blindé;
- une erreur de câblage.

5.2.8.2 OSSD à relais

Il doit être vérifié par inspection ou essais que les relais sont conformes aux exigences de 4.2.4.2.

5.2.8.3 OSSD à semi-conducteurs

Les niveaux de la tension de sortie et du courant spécifiés en 4.2.4.3 de la présente norme doivent être vérifiés.

5.2.8.4 Interface de données relatives à la sécurité et interface de communication relative à la sécurité

On doit vérifier par essai que la déconnexion des composants ne conduit pas à une défaillance dangereuse.

Les essais électriques spécifiés en 5.2.8.1 (court-circuit, coupures, charge impropre) qui devraient être réalisés sur le ou les OSSD peuvent être supprimés s'ils ne sont pas applicables.

L'intégrité de sécurité d'un interface de communication intégré doit être vérifié par des essais, une analyse systématique et par référence aux feuilles de données et aux rapports d'essai selon les exigences de 4.2.4.4.

5.3 Essais de performance sous condition de défaut

5.3.1 Généralités

Les essais destinés à vérifier les effets de défauts uniques sélectionnés selon 4.2.2 doivent être effectués sur tous les composants appropriés de l'ESPE. Si d'autres défauts apparaissent par suite d'un premier défaut unique, ce premier défaut ainsi que les défauts résultants doivent être considérés comme un défaut unique.

On doit préparer un catalogue de défauts comportant tous les composants et listant les résultats des défauts pris en compte dans l'Annexe B. Pour éviter des essais inutiles conformément à 5.3.2, 5.3.3, et 5.3.4 lorsque les résultats relatifs à un défaut unique ou une combinaison de défauts peuvent être théoriquement prévus, une déclaration relative à cette analyse doit être incluse dans la déclaration de résultats d'essai. Cette déclaration doit être validée conformément à 5.5.4. Dans ce cas, seuls des essais sélectionnés (échantillons) doivent être conduits pour confirmer les déclarations de l'analyse.

NOTE 1 Les méthodes généralement utilisées pour l'évaluation des défauts sont l'analyse des modes de défaillance et de leurs effets (AMDE) selon la CEI 60812 ainsi que l'analyse par arbre de panne selon la CEI 61025.

NOTE 2 Dans le cas de structures ou de composants de circuits complexes (par exemple microprocesseur, redondance totale), l'examen des défauts est généralement effectué au niveau structurel. Se reporter à B.1.2 en ce qui concerne l'exclusion des courts-circuits sur les cartes de circuits assemblés. Se reporter à B.1.3 et à B.1.4 en ce qui concerne l'exclusion des courts-circuits entre bornes adjacentes pour connexions externes.

5.3.2 ESPE de type 1

NOTE Les prescriptions pour un ESPE de type 1 ne sont pas prises en compte à ce stade.

5.3.3 ESPE de type 2

L'ESPE doit être soumis à des défauts uniques afin de vérifier qu'un défaut entraînant une condition dangereuse (par exemple la perte de la capacité de détection ou l'accroissement du temps de réponse) est détecté par l'essai périodique et entraîne une condition de blocage à l'arrêt conformément à 4.2.2.3.

Quand une initialisation interne de l'essai périodique est prévue, on doit vérifier que les défauts dans la fonction de surveillance sont détectés et entraînent une condition de blocage à l'arrêt ou le passage d'au moins un OSSD à l'état INACTIF.

5.3.4 ESPE de type 3

L'ESPE doit être soumis à des défauts uniques afin de s'assurer que le défaut est détecté et entraîne le passage à la condition de blocage à l'arrêt de l'ESPE et qu'aucune défaillance dangereuse ne se produit, conformément à 4.2.2.4.

Lorsqu'un défaut unique n'est pas détecté et que l'analyse spécifiée en 5.3.1 ne peut pas être faite, les essais concernant le passage à la condition de blocage à l'arrêt, sans défaillance dangereuse, doivent être poursuivis en appliquant ce défaut en premier lieu et en appliquant ensuite tous les autres défauts et en les retirant tour à tour. Les essais doivent être effectués pour tout défaut unique non détecté.

Des essais d'accumulation de plus de deux défauts peuvent ne pas être conduits.

5.3.5 ESPE de type 4

L'ESPE doit être soumis à des défauts uniques afin de s'assurer que le défaut est détecté et entraîne le passage à la condition de blocage à l'arrêt de l'ESPE et qu'aucune défaillance dangereuse ne se produit, conformément à 4.2.2.5.

Lorsqu'un défaut unique n'est pas détecté et que l'analyse spécifiée en 5.3.1 ne peut pas être faite, les essais concernant le passage à la condition de blocage à l'arrêt, sans défaillance dangereuse, doivent être poursuivis en appliquant ce défaut en premier lieu et en appliquant ensuite tous les autres défauts et en les retirant tour à tour. Les essais doivent être effectués pour tout défaut unique non détecté.

Lorsqu'une séquence de deux défauts n'est pas détectée et que l'analyse spécifiée en 5.3.1 ne peut pas être faite, les essais doivent être poursuivis pour ces deux défauts, appliqués en séquence, et tous les autres défauts uniques ajoutés et retirés tour à tour. Aucune défaillance dangereuse ne doit se produire. Les essais doivent être effectués pour tout couple de défaut non détecté.

Des essais d'accumulation de plus de trois défauts peuvent ne pas être conduits s'il est établi que la probabilité est faible d'avoir plus de trois défauts, largement indépendants les uns des autres et devant se produire dans une séquence temporelle spécifique.

5.4 Essais d'environnement

5.4.1 Tension d'alimentation assignée

Les mesures de conception de 4.2.1 doivent être vérifiées par inspection.

L'ESPE doit être soumis à la série d'essais suivante conformément aux valeurs spécifiées en 4.2.1:

- a) l'ESPE doit être alimenté avec la tension d'alimentation assignée minimale. Un essai B doit alors être effectué;
- b) la tension d'alimentation doit alors être augmentée dans un laps de temps de 10 s à 20 s jusqu'à la tension d'alimentation assignée maximale. Un essai A doit être réalisé durant ce temps;
- c) quand la tension d'alimentation d'essai maximale est atteinte, un essai B doit être effectué.

Les prescriptions de variation de fréquence et de distorsion harmonique doivent être vérifiées soit par des essais soit par des méthodes analytiques.

5.4.2 Variation de la température ambiante et humidité

La température ambiante la plus élevée pour les essais ci-dessous doit être celle spécifiée sur le marquage et/ou sur les documents d'accompagnement de l'équipement, mais ne doit pas être inférieure à +50 °C. La température ambiante la plus faible pour les essais ci-dessous doit être celle spécifiée sur le marquage et/ou sur les documents d'accompagnement de l'équipement, mais ne doit pas être supérieure à 0 °C.

L'ESPE doit être soumis à la séquence d'essai suivante:

- a) Avec l'ESPE fonctionnant dans les conditions spécifiées en 5.1.2.1 un essai A doit être réalisé pendant une durée d'au moins 2 h. Une fois ce délai écoulé, un essai B doit être effectué.
- b) La température ambiante doit être augmentée, au maximum de 0,3 °C par minute, jusqu'à la température ambiante la plus élevée; durant ce temps, un essai A doit être réalisé.
- c) Un essai A doit être réalisé pendant une durée d'au moins 2 h à la température ambiante la plus élevée. Durant ce temps, l'humidité doit être augmentée jusqu'à 95 % et maintenue à cette valeur durant au moins 1 h. A la suite de l'essai A, un essai B doit être effectué.
- d) La température ambiante doit être diminuée, au maximum de 0,3 °C par minute, tout en maintenant l'humidité à 95 % jusqu'à atteindre la température de 20 °C; durant ce temps, un essai A doit être réalisé.
- e) La température ambiante doit être diminuée, au maximum de 0,3 °C par minute, sans qu'il se produise de condensation, jusqu'à atteindre la température ambiante la plus faible; durant ce temps, un essai A doit être réalisé.
- f) Un essai A doit être réalisé pendant une durée d'au moins 2 h à la température ambiante la plus faible. Une fois ce délai écoulé, un essai B doit être effectué.
- g) La température ambiante doit ensuite être augmentée, au maximum de 0,3 °C par minute, jusqu'à la valeur prescrite en 5.1.2.1; durant ce temps, un essai A doit être réalisé.
- h) Un essai A doit être réalisé pendant au moins 2 h à la température spécifiée en 5.1.2.1. Une fois ce délai écoulé, un essai B doit être effectué.

5.4.3 Effets de perturbations électriques

NOTE Des essais modifiés pour les ESPE utilisant des interfaces avec des bus de communication sont à l'étude.

5.4.3.1 Variations de la tension d'alimentation

L'alimentation externe et toute alimentation interne lui étant liée doit à son tour subir des variations conformes à 4.3.2.1. Pendant chacun de ces essais, un ou plusieurs essais C doivent être menés pour confirmer qu'aucune défaillance dangereuse ne se produit pour des valeurs réduites de tension d'alimentation.

5.4.3.2 Interruptions de la tension d'alimentation

Les essais prescrits en 4.3.2.2 doivent être effectués, la durée de chaque essai étant suffisamment longue pour couvrir au moins 10 creux de tension et permettre, pour chacun des essais 1) et 2), l'exécution d'un essai B et, pour l'essai 3), l'exécution d'un essai C.

5.4.3.3 Transitoires rapides en salves

5.4.3.3.1 Prescriptions générales

L'ESPE doit être soumis à des transitoires rapides en salves aux niveaux prescrits en 4.3.2.3.1 conformément à la CEI 61000-4-4. (utilisation de la Figure 9 de la CEI 61000-4-4 pour les ports d'alimentation et ports de signal c.c. et c.a. de moins de 50 V, et utilisation de la Figure 8 pour les autres ports d'alimentation c.a.).

Pendant chaque exposition, un essai B doit être effectué.

5.4.3.3.2 Essais supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 doit également être soumis aux transitoires rapides en salves aux niveaux prescrits en 4.3.2.3.2 conformément à la CEI 61000-4-4 (utilisation de la Figure 9 de la CEI 61000-4-4 pour les ports d'alimentation et les ports de signal c.c. et c.a. de moins de 50 V, et utilisation de la Figure 8 pour les autres ports d'alimentation c.a.).

Pendant chaque exposition, un essai C doit être effectué.

5.4.3.4 Ondes de choc

5.4.3.4.1 Prescriptions générales

L'ESPE doit être soumis aux ondes de choc aux niveaux prescrits en 4.3.2.4.1 conformément à la CEI 61000-4-5 (utilisation de la Figure 10 ou 12 de la CEI 61000-4-5 pour les ports de signal, de la Figure 7 de la CEI 61000-4-5 pour les ports d'alimentation c.c. et c.a. de moins de 50 V, et utilisation des Figures 6 et 7 de la CEI 61000-4-5 pour les autres ports d'alimentation c.a.).

Pendant chaque exposition, un essai B doit être effectué.

5.4.3.4.2 Essais supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 doit également être soumis aux ondes de choc aux niveaux prescrits en 4.3.2.4.2 conformément à la CEI 61000-4-5 (utilisation de la Figure 10 ou 12 de la CEI 61000-4-5 pour les ports de signal, de la Figure 7 de la CEI 61000-4-5 pour les ports d'alimentation c.c. et c.a. de moins de 50 V, et utilisation des Figures 6 et 7 de la CEI 61000-4-5 pour les autres ports c.a.).

Pendant chaque exposition, un essai C doit être effectué.

5.4.3.5 Champ électromagnétique

5.4.3.5.1 Essais généraux

L'ESPE doit être soumis à un champ électromagnétique au niveau prescrit en 4.3.2.5.1 conformément à 5.1 de la CEI 61000-4-3. Pendant l'exposition au niveau de sévérité 3, un essai B doit être effectué.

NOTE Le résultat de cet essai dépend des structures environnantes qui peuvent varier si l'ESPE est monté sur la machine.

5.4.3.5.2 Essais supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 doit également être soumis à un champ électromagnétique de niveaux spécifiés en 4.3.2.5.2 selon 5.2 de la CEI 61000-4-3. Pendant l'exposition au niveau de sévérité 4, un essai C doit être effectué.

NOTE Le résultat de cet essai dépend des structures environnantes qui peuvent varier si l'ESPE est monté sur la machine.

5.4.3.6 Perturbations conduites induites par les champs radioélectriques

5.4.3.6.1 Essais généraux

L'ESPE doit être soumis à des perturbations conduites aux fréquences radioélectriques aux niveaux prescrits en 4.3.2.6.1 conformément à la CEI 61000-4-6. Pendant chaque exposition, un essai B doit être effectué.

5.4.3.6.2 Essais supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 doit également être soumis à des perturbations conduites aux fréquences radioélectriques aux niveaux prescrits en 4.3.2.6.2 conformément à la CEI 61000-4-6.

Pendant chaque exposition, un essai C doit être effectué.

5.4.3.7 Décharge électrostatique

5.4.3.7.1 Essais généraux

L'ESPE doit être soumis à des décharges électrostatiques aux niveaux prescrits en 4.3.2.7.1 conformément à la CEI 61000-4-2. Pendant chaque exposition, un essai B doit être effectué.

5.4.3.7.2 Essais supplémentaires

Un ESPE de type 3 ou un ESPE de type 4 doit également être soumis à des décharges électrostatiques aux niveaux prescrits en 4.3.2.7.2 conformément à la CEI 61000-4-2.

Pendant chaque exposition, un essai C doit être effectué.

5.4.4 Influences mécaniques

5.4.4.1 Vibrations

L'échantillon d'essai doit être soumis à des essais de vibrations conformément à la CEI 60068-2-6.

Les conditions suivantes doivent s'appliquer:

Plage de fréquences:	10 Hz à 55 Hz
Vitesse de balayage:	1 octave/min
Amplitude:	0,35 mm $\pm$ 0,05 mm; l'essai doit être mené sans fixation anti-vibrations
Nombre de balayages:	20 sur chacun de trois axes mutuellement perpendiculaires (pas de retard aux fréquences de résonance)

Les essais de fonctionnement limités suivants doivent être réalisés pour chaque axe:

- un essai A doit être effectué au cours de chaque premier et dernier balayage;
- un essai B doit être effectué de manière à ce que l'éprouvette d'essai soit amenée dans la zone de détection au début du second balayage et soit retirée à la fin du 19^e balayage.

5.4.4.2 Chocs

L'échantillon d'essai doit être soumis aux essais de choc conformément à la CEI 60068-2-29.

Les conditions suivantes doivent s'appliquer:

Accélération:	10 g
Durée de l'impulsion:	16 ms
Nombre de chocs:	1 000 $\pm$ 10 pour chaque axe, sur les trois axes mutuellement perpendiculaires

Les essais suivants doivent être effectués pour chaque axe.

- un essai A doit être effectué au cours de chacun des premier et dernier (100 $\pm$ 10) chocs;
- un essai B doit être effectué de façon que l'éprouvette d'essai soit amenée dans la zone de détection après les premiers (100 $\pm$ 10) chocs.

5.4.5 Enveloppes

Les prescriptions de 4.3.4 relatives au degré de protection doivent être essayées conformément à la CEI 60529 après les essais de 5.4.4. Les prescriptions restantes doivent être vérifiées par inspection.

5.5 Validation de circuits intégrés, programmables ou complexes

5.5.1 Généralités

Ce paragraphe concerne la validation des prescriptions de 4.2.10 et 4.2.11 et des résultats des analyses faisant partie de la déclaration de résultats d'essai, conformément à 5.3.1.

La validation doit être conduite par une ou des personnes compétentes qui doivent être indépendantes de celles responsables de la conception du système, de la conception du matériel et de la conception du logiciel. Un rapport de validation écrit doit être établi.

NOTE La validation procure une confirmation indépendante que les prescriptions spécifiques ont été réalisées. Le procédé est destiné à confirmer que les défauts systématiques dans la conception ont été évités, que les procédures sont en place pour maintenir le niveau de performance lié à la sécurité tout au long du cycle de vie du produit (y compris, par exemple, les modifications ultérieures) et que la conception de l'ESPE répond aux prescriptions de détection de défaut correspondant à son type.

5.5.2 Circuits intégrés complexes ou programmables

Pour tout ESPE de type 4 comportant un ou des circuits intégrés complexes ou programmables, les prescriptions suivantes doivent être validées par analyse:

- a) il existe au moins deux voies indépendantes de prise de décision;
- b) la détection d'une disparité entre les voies, et le démarrage d'une condition de blocage à l'arrêt, doivent être conservés quelles que soient les conditions de défaut appliquées.

5.5.3 Logiciel, programmation, conception de fonctionnement des circuits intégrés

On doit vérifier que les procédures spécifiées et la documentation du ou des systèmes qualité auxquels la conception du système et le logiciel se réfèrent sont bien conformes aux prescriptions d'un système de management de la qualité (l'ISO 9001 par exemple).

Le fonctionnement du ou des systèmes qualité doit être vérifié par un audit de la documentation relative au développement du produit et aux procédures mises en place pour garantir la qualité du produit pendant son cycle de vie.

L'audit doit permettre de s'assurer que la documentation de développement du projet est pertinente, complète et fait l'objet d'un suivi.

La spécification des prescriptions de sécurité doit être analysée pour confirmer que les prescriptions pour le logiciel, pour la conception du programme, pour la conception de fonctionnement qui n'y figurent pas sont bien mentionnées ailleurs dans la conception du système.

Le plan d'essai doit être analysé pour confirmer que toutes les prescriptions de la spécification des prescriptions de sécurité peuvent être vérifiées par la conformité à l'ensemble de ces essais.

Quand un logiciel dédié à la détection de défauts est utilisé pendant le fonctionnement de l'ESPE, le plan d'essai doit être analysé pour s'assurer que tous les défauts répertoriés en B.4.4 qui ne peuvent pas être vérifiés par la simulation directe de défauts par le matériel sont bien vérifiés par le logiciel.

Les résultats des essais de la dernière version de la conception doivent être soumis à un audit. Quelques échantillons d'essais, choisis au hasard, doivent être répétés pour être validés et les résultats doivent être en concordance avec ceux énoncés dans le rapport du projet.

Quand un logiciel dédié à la détection de défauts est utilisé pendant le fonctionnement de l'ESPE, les résultats des essais de simulation de défauts doivent vérifier que le taux de couverture adéquat est atteint et doivent être comparés précisément à ceux obtenus par analyse théorique faisant partie de la déclaration de résultats d'essai.

Pour tout logiciel utilisé pendant le fonctionnement de l'ESPE, il doit être vérifié que toutes les instructions opérationnelles sont contenues dans une mémoire à écriture seule (ROM) qui ne peut pas être reprogrammée par le processeur.

Pour les produits programmables, les moyens vérifiant que le produit réalise normalement toutes ses fonctions programmées doivent être validés.

NOTE 1 Un produit programmé de façon incorrecte ou incomplète peut assurer normalement les fonctions primaires de protection sans assurer la détection de tous les défauts, tout particulièrement quand plusieurs produits programmables similaires sont utilisés dans une conception qui utilise une surveillance croisée pour la détection de défauts.