IEC 62733

Edition 1.0 2015-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Programmable components in electronic lamp controlgear – General and safety requirements

Composants programmables dans les appareillages électroniques de lampes – Exigences générales et exigences de sécurité

IEC 62733:2015-05(en-fr)

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.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) 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 IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
Plus de 60 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62733

Edition 1.0 2015-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Programmable components in electronic lamp controlgear – General and safety requirements

Composants programmables dans les appareillages électroniques de lampes – Exigences générales et exigences de sécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 29.140.99

ISBN 978-2-8322-2668-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

PROGRAMMABLE COMPONENTS IN ELECTRONIC LAMP CONTROLGEAR – GENERAL AND SAFETY REQUIREMENTS

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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 62733 has been prepared by subcommittee 34C: Auxiliaries for lamps, of IEC technical committee 34: Lamps and related equipment.

The text of this standard is based on the following documents:

FDIS	Report on voting
34C/1140/FDIS	34C/1156/RVD

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

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

NOTE In this standard the following print types are used:

– Requirements proper: in Roman type.

– Test specifications: *in Italic type*.

– Explanatory matter: in smaller roman type.

The committee has decided that the contents of this publication will remain unchanged until the stability 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

This International Standard provides safety requirements and test methods for programmable components when in electronic lamp controlgear. It provides additional safety requirements for electronic lamp controlgear containing programmable components to the requirements of IEC 61347 series.

In general, the two means of protection safety principle is used for protection against hazards such as electric shock. Consequently one single fault condition or abnormal operation of the electrical equipment will not lead to a hazardous situation.

Until recent technology, two means of protection have been realized in traditional hardware. Examples are the provision of basic insulation and supplementary insulation between hazardous live parts and accessible parts, and provision of basic insulation combined by disconnection of the mains supply by a fuse.

Nowadays however programmable components (with embedded software) may be used as a measure to provide safety under normal conditions, single fault conditions and/or abnormal operation.

Since the traditional lighting standards do not provide requirements for programmable components, this standard has been drawn up.

This standard recognizes the internationally accepted level of protection against hazards such as electrical, mechanical, thermal, fire and radiation of appliances when operated as in normal use taking into account the manufacturer's instructions. It also covers conditions for electromagnetic phenomena that can be expected in practice with influence on the operation of the programmable component, for taking into account the way this can affect the safe operation of the electronic lamp controlgear.

This first edition is based upon IEC 60730-1:2010 and IEC 60335-1:2010 and adapted for electronic lamp controlgear

NOTE The terms and definitions and Tables A.1 and A.2 respectively of this standard are equivalent to terms and definitions and Table R.1 and R.2 of IEC 60335-1:2010, and equivalent terms and definitions and Table H.1 (class B and class C software) of IEC 60730-1:2010.

PROGRAMMABLE COMPONENTS IN ELECTRONIC LAMP CONTROLGEAR – GENERAL AND SAFETY REQUIREMENTS

1 Scope

This International Standard provides general and safety requirements for programmable components used in products covered by IEC 61347.

The requirements of this standard are only applicable to the programmable components (including its embedded software) in the electronic lamp controlgear. For other electric/electronic circuits and their components in the electronic lamp controlgear, the requirements of IEC 61347 series apply.

2 Normative references

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

IEC 61000-4-13:2002, *Electromagnetic compatibility (EMC) – Part 4-13: Testing and measurement techniques – Harmonics and interharmonics including mains signalling at a.c. power port, low frequency immunity tests*
IEC 61000-4-13:2002/AMD 1:2009

IEC 61347-1, *Lamp controlgear – Part 1: General and safety requirements*

IEC 61347-2 (all parts)[1], *Lamp controlgear – Part 2: Particular requirements*

IEC 61547:2009, *Equipment for general lighting purposes – EMC immunity requirements*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

3 Terms and definitions

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

3.1
central processing unit
CPU
part of a computing and controlling system that interprets and executes instructions

[1] Relevant parts of the series depend on the context.

Note 1 to entry: This note applies to the French language only.

3.2
programmable component
based on computer technology which comprised of hardware, software, and of input and/or output units

EXAMPLE The following are all programmable components:

– microprocessors;
– micro-controllers;
– programmable controllers;
– application specific digital integrated circuits (ASICs with programmable part);
– programmable logic controllers (PLCs);
– other computer-based devices (for example smart sensors, transmitters, actuators).

Note 1 to entry: This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc.

Note 2 to entry: The term programmable component is from ANSI/UL1998:2010, definition 2.39 [2].The definition in ANSI/UL for programmable component is: “Any microelectronic hardware that can be programmed in the design centre, the factory, or in the field. Here the term ‘programmable’ is taken to be ‘any manner in which one can alter the software wherein the behaviour of the component can be altered.” This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc.

[SOURCE: IEC 61508-4:2010, 3.2.12, modified — "Programmable electronic" is replaced by "programmable component" which better describes that it is only a part of the controlgear.]

3.3
protective programmable component
PPC
programmable component that prevents a hazardous situation under abnormal operating conditions, or programmable component for which none of the output signals can lead to a hazardous situation

Note 1 to entry: This note applies to the French language only.

3.4
software
intellectual creation comprising the programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system

[SOURCE: IEC 61508-4:2010, 3.2.5, modified — The notes to entry are deleted.]

3.5
software code
code written by a programmer in a high-level computer language and readable by people but not computers

3.6
safety software
part of the software that counteracts possible hazardous situations, which are created from abnormal and/or fault conditions

Note 1 to entry: Software is independent of the medium on which it is recorded.

3.7
fault condition
condition as required by Clause 14 of IEC 61347-1 or its relevant Part 2

3.8
single fault condition
fault condition under normal operating condition of a single component or a device

[SOURCE: IEC 62368-1:2010, 3.3.7.10, modified]

3.9
normal operating
mode of operation that represents as closely as possible the most severe conditions of normal use that can reasonably be expected

[SOURCE: IEC 62368-1:2010, 3.3.7.4, modified]

3.10
abnormal operating
temporary operating condition that is not a normal operating condition and is not a single fault condition of the equipment itself

Note 1 to entry: An abnormal operating condition may be introduced by the equipment or by a person.

Note 2 to entry: The equipment, installation, instructions, and specifications should be examined to determine those abnormal operating conditions that might reasonably be expected to occur.

Note 3 to entry: Faults that are the direct consequence of the abnormal operating condition are deemed to be a single fault condition.

[SOURCE: IEC 62368-1:2010, 3.3.7.1, modified]

3.11
fault tree analysis
FTA
top down, deductive failure analysis method in which a hazardous or serious event is analyzed using Boolean logic to combine a series of events causing this event

Note 1 to entry: The FTA technique represents a ‘top-down’ analysis technique. Annex B of IEC 61508-7:2010 provides information for the minimum setup for an FTA report.

3.12
failure modes and effects analysis
FMEA
analytical technique in which the failure modes of each hardware and software component are identified and examined for their effects on the safety-related functions of the control

Note 1 to entry: The FMEA technique represents a ‘bottom-up’ analysis technique. Annex B provides information for the minimum setup for an FMEA report.

[SOURCE: IEC 60730-1:2010, H.2.20.3, modified]

3.13
rated voltage
value of voltage assigned by the manufacturer to a component, device or equipment and to which operation and performance characteristics are referred

Note 1 to entry: Equipment may have more than one rated voltage value or may have a rated voltage range.

Note 2 to entry: For three-phase supply, the phase-to-phase voltage applies.

[SOURCE: IEC 62368-1:2010, 3.3.10.4, modified]

3.14
tolerable risk
risk level as defined in 5.1

3.15
intolerable risk
risk level which cannot be justified, except in extraordinary circumstances

3.16
acceptable risk
risk level that is broadly accepted in the society

3.17
ALARP
as low as is reasonably practicable
level of risk for a risk that falls between acceptable risk and intolerable risk and has to be reduced to the lowest practicable level, bearing in mind the benefits resulting from its acceptance and taking into account the practicability of any further reduction

Note 1 to entry: This note applies to the French language only.

Note 2 to entry: The specification of the level ALARP is described in Annex D.

Note 3 to entry: This definition is according to IEC 61508-5:1998, Annex B. In this standard it is used as one possible variant of the tolerable risk.

3.18
injury
damage to the human body, less than 2 % incapacity, usually reversible and not usually requiring hospital treatment

EXAMPLE Minor cuts, very minor fractures or minor burns or sprains.

3.19
serious injury
injury that directly or indirectly:

a) threatens life,
b) results in permanent impairment of a body function or permanent damage to a body structure, or
c) necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure

3.20
hazardous situation
circumstance in which people, property or the environment are exposed to one or more potential sources of physical injury or damage to the health of people, or damage to property or the environment

4 General requirements

Software of programmable components within electronic lamp controlgear shall be so designed and constructed that in normal use it operates without danger to the user or surroundings.

A risk assessment shall be done to determine which parts of this standard are applicable. If the risk assessment shows that the software built-in used to prevent the controlgear from becoming unsafe, has a risk above the tolerable risk, then this standard is mandatory.

The focus of the risk assessment shall be the possible risks by the electronic controlgear including the abnormal operation and fault conditions of the relevant Part 2 of IEC 61347.

5 Risk assessment

5.1 General

Possible risks by the controlgear shall be the focus of the risk assessment. The risk assessment shall identify and classify known or reasonably foreseeable risks of a possible malfunction of the software (including the risk originating from potential internal fault conditions and abnormal operation of the controlgear described in the relevant Part 2 of IEC 61347) under the assumption of expected use.

If the risk assessment shows that the software built-in to prevent the controlgear from becoming unsafe, has a risk above the tolerable risk (and is not reduced by additional hardware measures) then all parts of this standard are applicable.

If the risk assessment shows that the risk is tolerable then the controlgear does comply with this standard. In this case only the parts relevant for describing the risk assessment of this standard do apply. This means that the following parts of the standard do not apply: Clauses 6, 7, 8 and Annexes A, B, C.

If the safety risk assessment for a programmable component results in being identified not as a protective programmable component, or not evaluated as a protective programmable component, then the component is exempted from software code.

5.2 Specification of tolerable risk

There are three ways to specify tolerable risk.

a) The risk is classified as tolerable if the effects by potential software malfunction are mitigated by hardware measures (e.g. hardware over-temperature shut down) so that the controlgear is prevented from becoming unsafe and if the hardware measures and the controlgear comply with the IEC 61347 series. Alternatively a second PPC can be used to mitigate a potential software malfunction as long as it is independent from the first PPC.

b) Alternatively a more general specification can be used.

   1) The risk is tolerable if the risk of the controlgear with software has the same level as that of a comparison controlgear where the respective safety relevant functions are realised by hardware and which complies with the IEC 61347 series.

   2) The goal is to verify a safety level of the controlgear (under assessment) having at least the same level of safety as that of a comparison controlgear where the safety relevant functions are realised by hardware and which complies with the IEC 61347 series. The comparison controlgear can be real or imagined, based on known hardware controlgears (or parts of these controlgears) that comply with the IEC 61347 series.

c) An alternative way to specify the tolerable risk is provided by a general risk classification described in Annex D. In this case the risk is tolerable if the risk is in the class ‘As low as is reasonably practicable (ALARP)’ or lower.

5.3 Documentation

The risk assessment and results out of it shall be documented by the manufacturer.

For each risk addressed by this process, a risk description and a potential cause shall be provided.

To document possible fault and failure modes a fault tree analysis (FTA) or a failure mode and effect analysis (FMEA) can be used. Annex B provides information for the minimum setup

for a FTA and FMEA analysis report. The FTA technique represents a ‘top down’ analysis technique; the FMEA technique represents a ‘bottom up” analysis technique.

The documentation of the risk assessment can be checked to show compliance with this standard.

6 Requirements for abnormal operating and fault conditions

6.1 Abnormal operating and fault conditions in the application of the electronic lamp controlgear

The safety software shall be tested in the fault and abnormal conditions as given in the relevant standard of the IEC 61347 series.

During and after the tests, the electronic lamp controlgear shall comply with the compliance criteria of the relevant electronic lamp controlgear standard IEC 61347 series.

If a programmable component (PC) in the electronic lamp controlgear is provided to ensure compliance with this clause, the software shall comply with the requirements in Clauses 7 and 8 of this standard for a protective programmable component (PPC).

A programmable component, identified not being a protective programmable component, or not evaluated as a protective programmable component, is exempt from software code evaluation. Annex C describes possible methods for the identification of protective programmable components.

In case of PPC safety provisions, compliance with Clauses 7 and 8 makes the PPC robust so that any potential failure in the PPC will not render the electronic lamp controlgear unsafe.

6.2 Fault conditions for the programmable component

For electronic lamp controlgear incorporating a programmable component the following fault conditions for the programmable component are considered and, if necessary, applied one at a time, consequential faults being taken into consideration.

a) Short circuit of functional insulation between adjacent programmable component terminals if clearances or creepage distances are less than the values specified in the relevant clause of IEC 61347-1.

NOTE 1 This is covered by 14.1 of IEC 61347-1.

b) Open circuit of any terminal of the programmable component.

NOTE 2 This is covered by 14.2 of IEC 61347-1.

c) If the software code is not accessible, alternatively, based upon the safety risk assessment, the pins of the programmable component are brought to a state in which it is expected that a safety issue could occur.

d) As an alternative for c) if the code is accessible, all outputs are considered for faults occurring within the programmable component. If it can be shown based upon the safety risk assessment that a particular output signal is unlikely to occur, then the relevant fault is not considered. The relevant faults are neither considered and can be excluded if the programmable component complies with the requirements in Clauses 7 and 8 of this standard for protective programmable component.

A FTA or FMEA should be conducted to include the results of multiple steady-state conditions to outputs and programmed bi-directional terminals for the purpose of identifying additional fault conditions for consideration, likely or unlikely to occur.

NOTE 3 A not to disclose programmable component is evaluated by FTA/FMEA analysis on the output signals.

If FTA or FMEA determine that only specific and well-defined critical failure conditions can occur, then a simulation or justification of the impact of the failure conditions during the evaluation can be chosen as an alternative to individual tests.

Compliance is checked by inspection and appropriate tests if necessary.

During and after the tests, the electronic lamp controlgear shall comply with the compliance criteria of 14.1, first paragraph, of IEC 61347-1 and relevant Part 2.

7 Requirements for software

Electronic lamp controlgear incorporating a protective programmable component the software of the programmable component shall contain measures to control the fault/error conditions specified in Table A.1. The fault/error evaluation includes the sensors and actuators that are associated with the software safety function.

Table A.2 is to be used when the software contains measures to control the fault/error conditions specified in Table A.2, when it is specified in the relevant Part 2 of IEC 61347 for particular constructions or to address specific hazards.

Measures used for software to control the fault/error conditions specified in Table A.2 are inherently acceptable for measures used for software to control the fault/error conditions specified in Table A.1.

Compliance is checked by evaluating the software in accordance with the relevant requirements of Annex A.

If the software is modified, the evaluation and relevant tests are repeated if the modification influences the results of the test involving protective programmable components.

Software compliance is checked by inspection of the risk assessment and the relevant part of the software and/or by carrying out appropriate tests of the electronic lamp controlgear.

Compliance check is in case of a protective programmable component or making use of the exclusion of 6.2 d)

8 Requirements for EMC immunity

8.1 Electronic lamp controlgear incorporating a protective programmable component to function correctly are subjected to the test B of 8.2, unless restarting at any point in the operating cycle after interruption of operation due to a supply voltage dip will not result in a hazard. The test is carried out after removal of all batteries and other components intended to maintain the programmable component supply voltage during mains supply voltage dips, interruptions and variations.

8.2 Electronic lamp controlgear incorporating a protective programmable component are subjected to the tests for electromagnetic phenomena. The tests are carried out in the operating condition valid for the protective programmable component**,** specified in Clause 6 of this standard, if applicable.

With respect to electromagnetic phenomena, the EMC immunity tests shall be done according IEC 61547.

In addition the following tests shall be performed:

A. The electronic lamp controlgear is subjected to mains signals in accordance with IEC 61000-4-13:2002/AMD1:2009, Table 11 with test level class 2 using the frequency steps according to Table 10.

B. The electronic lamp controlgear is supplied at rated voltage and operated under normal operation. After approximately 60 s, the power supply voltage is reduced to a level such that the electronic lamp controlgear ceases to respond to user inputs or parts controlled by the programmable component cease to operate, whichever occurs first. This value of supply voltage is recorded. The electronic lamp controlgear is supplied at rated voltage and operated under normal operation. The voltage is then reduced to a value of approximately 10 % less than the recorded voltage. It is held at this value for approximately 60 s and then increased to rated voltage. The rate of decrease and increase in power supply voltage is to be approximately 10 V/s. The controlgear shall remain safe. Unless the controlgear returns to normal operation, it shall enter a failsafe mode.

8.3 During and after the tests, the electronic lamp controlgear shall comply with the compliance criteria of Clause 14 of IEC 61347-1 and the relevant Part 2.

Additionally, the electronic lamp controlgear shall not undergo a dangerous malfunction, and there shall be no failure of protective programmable components if the electronic lamp controlgear is still operable.

Annex A
(normative)

Software evaluation

A.1 General

Protective programmable components require software incorporating measures to control the fault/error conditions specified in Table A.1 or Table A.2 and shall be validated in accordance with the requirements in this annex.

NOTE The definitions and Tables A.1 and A.2 are based on the definitions and Table H.1 (respectively for equivalent class B and class C software) of IEC 60730-1:2010 that is, for the purpose of this annex, divided in two tables, Table A.1 for general fault/error conditions and Table A.2 for specific fault/error conditions.

A.2 Protective programmable components using software

Protective programmable components requiring software incorporating measures to control the fault/error conditions specified in Table A.1 or Table A.2 shall be constructed so that the software does not impair compliance with the requirements of this standard.

Compliance is checked by the inspections and tests, according to the requirements of this annex, and by examination of the documentation as required by this annex.

A.3 Terms and definitions

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

A.3.1
dual channel
structure which contains two mutually independent functional means to execute specified operations

Note 1 to entry: Special provision may be made for control of common mode fault/errors. It is not required that the two channels each be logarithmic or logical in nature.

[SOURCE: IEC 60730-1:2010, H.2.16.1]

A.3.2
dual channel (diverse) with comparison
dual channel structure containing two different and mutually independent functional means, each capable of providing a declared response, in which comparison of output signals is performed for fault/error recognition

[SOURCE: IEC 60730-1:2010, H.2.16.2]

A.3.3
dual channel (homogeneous) with comparison
dual channel structure containing two identical and mutually independent functional means, each capable of providing a declared response, in which comparison of internal signals or output signals is performed for fault/error recognition

[SOURCE: IEC 60730-1:2010, H.2.16.3]

A.3.4
single channel
structure in which a single functional means is used to execute operations as specified

[SOURCE: IEC 60730-1:2010, H.2.16.4]

A.3.5
single channel with functional test
structure in which test data is introduced to the functional unit prior to its operation

A.3.6
single channel with periodic self-test
structure in which components of the control are periodically tested during operation

A.3.7
single channel with periodic self-test and monitoring
structure with periodic self-test in which independent means, each capable of providing a declared response, monitor such aspects as safety-related timing, sequences and software operations

A.3.8
full bus redundancy
fault/error control technique in which full redundant data and/or address are provided by means of a redundant bus structure

[SOURCE: IEC 60730-1:2010, H.2.18.1.1]

A.3.9
multi-bit bus parity
fault/error control technique in which the bus is extended by two or more bits and these additional bits are used for error detection

[SOURCE: IEC 60730-1:2010, H.2.18.1.2]

A.3.10
code safety
fault/error control techniques in which protection against coincidental and/or systematic errors in input and output information is provided by the use of data redundancy and/or transfer redundancy

Note 1 to entry: See also A.3.11 and A.3.12.

[SOURCE: IEC 60730-1:2010, H.2.18.2]

A.3.11
data redundancy
form of code safety in which the storage of redundant data occurs

[SOURCE: IEC 60730-1:2010, H.2.18.2.1]

A.3.12
transfer redundancy
form of code safety in which data is transferred at least twice in succession and then compared

Note 1 to entry: This technique will recognize intermittent errors.

[SOURCE: IEC 60730-1:2010, H.2.18.2.2]

A.3.13
comparator
device used for fault/error control in dual channel structures by comparing data from the two channels and initiates a declared response if a difference is detected

[SOURCE: IEC 60730-1:2010, H.2.18.3, modified — The note to entry is incorporated in the definition.]

A.3.14
equivalence class test
systematic test intended to determine whether the instruction decoding and execution are performed correctly

Note 1 to entry: The test data is derived from the CPU instruction specification

Note 2 to entry: Similar instructions are grouped and the input data set is subdivided into specific data intervals (equivalence classes). Each instruction within a group processes at least one set of test data, so that the entire group processes the entire test data set. The test data can be formed from the following:

– data from valid range;
– data from invalid range;
– data from the bounds;
– extreme values and their combinations.

Note 3 to entry: The tests within a group are run with different addressing modes, so that the entire group executes all addressing modes.

[SOURCE: IEC 60730-1:2010, H.2.18.5]

A.3.15
error recognizing means
independent means provided for the purpose of recognizing errors internal to the system

EXAMPLE Monitoring devices, comparators, and code generators.

[SOURCE: IEC 60730-1:2010, H.2.18.6]

A.3.16
input comparison
fault/error control technique by which inputs that are designed to be within specified tolerances are compared

[SOURCE: IEC 60730-1:2010, H.2.18.8]

A.3.17
internal error detecting
internal error correcting
fault/error control technique in which special circuitry is incorporated to detect or correct errors

[SOURCE: IEC 60730-1:2010, H.2.18.9]

A.3.18
frequency monitoring
fault/error control technique in which the clock frequency is compared with an independent fixed frequency

EXAMPLE Comparison with the line supply frequency.

[SOURCE: IEC 60730-1:2010, H.2.18.10.1]

A.3.19
logical monitoring of the program sequence
fault/error control technique in which the logical execution of the program sequence is monitored

EXAMPLE Use of counting routines or selected data in the program itself or by independent monitoring devices.

[SOURCE: IEC 60730-1:2010, H.2.18.10.2]

A.3.20
time-slot and logical monitoring
this is a combination of A.3.19 and A.3.21

A.3.21
time-slot monitoring of the program sequence
fault/error control technique in which timing devices with an independent time base are periodically triggered in order to monitor the program function and sequence

EXAMPLE Watchdog timer.

[SOURCE: IEC 60730-1:2010, H.2.18.10.4]

A.3.22
multiple parallel outputs
fault/error control technique in which independent outputs are provided for operational error detection or for independent comparators

[SOURCE: IEC 60730-1:2010, H.2.18.11]

A.3.23
output verification
fault/error control technique in which outputs are compared to independent inputs

Note 1 to entry: This technique may or may not relate an error to the output which is defective.

[SOURCE: IEC 60730-1:2010, H.2.18.12]

A.3.24
plausibility check
fault/error control technique in which program execution, inputs or outputs are checked for inadmissible program sequence, timing or data

EXAMPLE Introduction of an additional interrupt after completion of a certain number of cycles or checks for division by zero.

[SOURCE: IEC 60730-1:2010, H.2.18.13]

A.3.25
protocol test
fault/error control technique in which data is transferred to and from computer components to detect errors in the internal communications protocol

[SOURCE: IEC 60730-1:2010, H.2.18.14]

A.3.26
reciprocal comparison
fault/error control technique used in dual channel (homogeneous) structures in which a comparison is performed on data reciprocally exchanged between the two processing units

Note 1 to entry: Reciprocal refers to an exchange of similar data.

[SOURCE: IEC 60730-1:2010, H.2.18.15]

A.3.27
redundant monitoring
availability of two or more independent means such as watchdog devices and comparators to perform the same task

[SOURCE: IEC 60730-1:2010, H.2.18.17]

A.3.28
scheduled transmission
communication procedure in which information from a particular transmitter is allowed to be sent only at a predefined point in time and sequence, otherwise the receiver will treat it as a communication error

[SOURCE: IEC 60730-1:2010, H.2.18.18]

A.3.29
tested monitoring
provision of independent means such as watchdog devices and comparators which are tested at start-up or periodically during operation

[SOURCE: IEC 60730-1:2010, H.2.18.21]

A.3.30
testing pattern
fault/error control technique used for periodic testing of input units, output units and interfaces of the control

Note 1 to entry: A test pattern is introduced to the unit and the results compared to expected values. Mutually independent means for introducing the test pattern and evaluating the results are used. The test pattern is constructed so as not to influence the correct operation of the control.

[SOURCE: IEC 60730-1:2010, H.2.18.22]

A.3.31
Abraham test
specific form of a variable memory pattern test in which all stuck-at and coupling faults between memory cells are identified

Note 1 to entry: The number of operations required to perform the entire memory test is about 30 n, where n is the number of cells in the memory. The test can be made transparent for use during the operating cycle, by partitioning the memory and testing each partition in different time segments.

Note 2 to entry: See Abraham, J.A.; Thatte, S.M.; "Fault coverage of test programs for a microprocessor", Proceedings of the IEEE Test Conference 1979, pp 18-22.

[SOURCE: IEC 60730-1:2010, H.2.19.1]

A.3.32
transparent GALPAT test
GALPAT memory test in which first a signature word is formed representing the content of the memory range to be tested and this word is saved

Note 1 to entry: The cell to be tested is inversely written and the test is performed as above. However, the remaining cells are not inspected individually, but by formation of and comparison to a second signature word. A second test is then performed as above by inversely writing the previously inverted value to the test cell.

Note 2 to entry: This technique recognizes all static bit errors as well as errors in interfaces between memory cells.

[SOURCE: IEC 60730-1:2010, H.2.19.2.1]

A.3.33
modified checksum
fault/error control technique in which a single word representing the contents of all words in memory is generated and saved

Note 1 to entry: During self-test, a checksum is formed from the same algorithm and compared with the saved checksum.

Note 2 to entry: This technique recognizes all the odd errors and some of the even errors.

[SOURCE: IEC 60730-1:2010, H.2.19.3.1]

A.3.34
multiple checksum
fault/error control technique in which a separate words representing the contents of the memory areas to be tested are generated and saved

Note 1 to entry: During self-test, a checksum is formed from the same algorithm and compared with the saved checksum for that area

Note 2 to entry: This technique recognizes all the odd errors and some of the even errors.

[SOURCE: IEC 60730-1:2010, H.2.19.3.2]

A.3.35
CRC – single word
fault/error control technique in which a single word is generated to represent the contents of memory

Note 1 to entry: During self-test the same algorithm is used to generate another signature word which is compared with the saved word.

Note 2 to entry: This technique recognizes all one-bit, and a high percentage of multi-bit, errors.

[SOURCE: IEC 60730-1:2010, H.2.19.4.1]

A.3.36
CRC – double word
fault/error control technique in which at least two words are generated to represent the contents of memory

Note 1 to entry: During self-test the same algorithm is used to generate the same number of signature words which are compared with the saved words

Note 2 to entry: This technique can recognize one-bit and multi-bit errors with a greater accuracy than in CRC – single word.

[SOURCE: IEC 60730-1:2010, H.2.19.4.2]

A.3.37
redundant memory with comparison
structure in which the safety-related contents of memory are stored twice in different format in separate areas so that they can be compared for error control

[SOURCE: IEC 60730-1:2010, H.2.19.5]

A.3.38
static memory test
fault/error control technique which is intended to detect only static errors

[SOURCE: IEC 60730-1:2010, H.2.19.6]

A.3.39
walkpat memory test
fault/error control technique in which a standard data pattern is written to the memory area under test as in normal operation

Note 1 to entry: A bit inversion is performed on the first cell and the remaining memory area is inspected. Then the first cell is again inverted and the memory inspected. This process is repeated for all memory cells under test. A second test is conducted by performing a bit inversion of all cells in memory under test and proceeding as above

Note 2 to entry: This technique recognizes all static bit errors as well as errors in interfaces between memory cells.

[SOURCE: IEC 60730-1:2010, H.2.19.7]

A.3.40
word protection with multi-bit redundancy
fault/error control technique in which redundant bits are generated and saved for each word in the memory area under test; as each word is read, a parity check is conducted

EXAMPLE Hamming code which recognizes all one and two bit errors as well as some three bit and multi-bit errors.

[SOURCE: IEC 60730-1:2010, H.2.19.8.1, modified — The note to entry is incorporated in the definition.]

A.3.41
word protection with single bit redundancy
fault/error control technique in which a single bit is added to each word in the memory area under test and saved, creating either even parity or odd parity; as each word is read, a parity check is conducted

Note 1 to entry: This technique recognizes all odd bit errors.

[SOURCE: IEC 60730-1:2010, H.2.19.8.2, modified — The note to entry is incorporated in the definition.]

A.3.42
single bit bus parity
fault/error control technique in which the bus is extended by one bit and this additional bit is used for error detection

[SOURCE: IEC 60730-1:2010, H.2.18.1.3]

A.3.43
checkerboard memory test
static memory test in which a checkerboard pattern of zeros and ones is written to the memory area under test and the cells are inspected in pairs

Note 1 to entry: The address of the first cell in each pair is variable and the address of the second cell is derived from a bit inversion of the first address. In the first inspection, the variable address is first incremented to the end of the address space of the memory and then decremented to its original value. The test is repeated with the checkerboard pattern inversed.

[SOURCE: IEC 60730-1:2010, H.2.19.6.1]

A.3.44
marching memory test
static memory test in which data is written to the memory area under test as in normal operation

Note 1 to entry: Every cell is then inspected in ascending order and a bit inversion performed on the contents. The inspection and bit inversion are then repeated in descending order. Then this process is repeated after first performing a bit inversion on all the memory cells under test.

[SOURCE: IEC 60730-1:2010, H.2.19.6.2]

A.3.45
stuck-at fault model
fault model representing an open circuit or a non-varying signal level

Note 1 to entry: These are usually referred to as “stuck open”, “stuck at 1” or “stuck at 0”.

A.3.46
d.c. fault model
stuck-at fault model incorporating short circuits between signal lines

Note 1 to entry: Because of the number of possible shorts in the device under test, usually only shorts between related signal lines will be considered. A logical signal level is defined, which dominates in cases where the lines try to drive to the opposite level.

A.3.47
software diversity
fault/error control technique in which all or parts of the software are incorporated twice in the form or alternative software code

Note 1 to entry: For example, the alternate forms of software code may be produced by different programmers, different languages or different compiling schemes and may reside in different hardware channels or in different areas of memory within a single channel.

A.4 Requirements for the architecture

A.4.1 General

A.4.1.1 Programmable components requiring software incorporating measures to control the fault/error conditions specified in Table A.1 or Table A.2 shall use measures to control (A.4.2) and avoid (Clause A.5) software-related faults/errors in safety-related data and safety-related segments of the software.

NOTE 1 Therefore a proper system design will deal with systematic errors and a proper system configuration will deal with random faults.

NOTE 2 The basis for the design of software and hardware is a functional (read: operational) analysis of the application – resulting in a structured design explicitly incorporating the control flow, data flow and time related functions required by the application. This leads to a system configuration which is either inherently failsafe or in which components with direct safety-critical functions (e.g. microprocessors with their associated circuits, etc.) are guarded by safeguard design according to this annex. These safeguards are built into hardware (e.g. watch-dog, supply voltage supervision) and can be supplemented by software (e.g. ROM-test, RAM-test, etc.). It is important that these safeguards can cause a completely independent safety-shut-down.

If time slot monitoring is used, the sensitivity includes to both an upper and a lower limit of the time interval. Faults resulting in shift of the upper and/or lower limit should be taken into account. In case of a control function that is classified as class A.2, if a single fault in a primary safeguard can render the safeguard inoperative, a secondary safeguard shall be provided.

NOTE 3 Reaction times of these safeguards are equal or smaller than the relevant fault tolerating time.

Compliance is checked by the inspections and tests in A.4.2 to A.4.3 inclusive.

A.4.1.2 Programmable components requiring software incorporating measures to control the fault/error conditions specified in Table A.2 shall have one of the following structures:

- single channel with periodic self-test and monitoring (A.3.7);
- dual channel (homogenous) with comparison (A.3.3);
- dual channel (diverse) with comparison (A.3.2).

NOTE Comparison between dual channel structures can be performed by:

- use of a comparator (A.3.13), or
- reciprocal comparison (A.3.26).

A.4.1.3 Programmable components requiring software incorporating measures to control the fault/error conditions specified in Table A.1 shall have one of the following structures:

- single channel with functional test (A.3.5);
- single channel with periodic self-test (A.3.6);
- dual channel without comparison (A.3.1).

Software structures incorporating measures to control the fault/error conditions specified in Table A.2 are also acceptable for programmable electronic circuits with functions requiring software measures to control the fault/error conditions specified in Table A.1.

Compliance is checked by the inspections and tests of the software architecture in A.5.2.2.

A.4.2 Measures to control faults/errors

A.4.2.1 When redundant memory with comparison is provided on two areas of the same component, the data in one area shall be stored in a different format from that in the other area (see software diversity,A.3.47).

Compliance is checked by inspection of the source code.

A.4.2.2 Programmable components with functions requiring software incorporating measures to control the fault/error conditions specified in Table A.2 and that use dual channel structures with comparison shall have additional fault/error detection means (such as periodic functional tests, periodic self-tests, or independent monitoring) for any fault/errors not detected by the comparison.

Compliance is checked by inspection of the source code.

A.4.2.3 For programmable components with functions requiring software incorporating measures to control the fault/error conditions specified in Table A.1 or Table A.2, means shall be provided for the recognition and control of errors in transmissions to external safety-related data paths. Such means shall take into account errors in data, addressing, transmission timing and sequence of protocol.

Compliance is checked by inspection of the source code.

A.4.2.4 For programmable components with functions requiring software incorporating measures to control the fault/error conditions specified in Table A.1 or Table A.2, the programmable components shall incorporate measures to address the fault/errors in safety-related segments and data indicated in Table A.1 or Table A.2 as appropriate.

Compliance is checked by inspection of the source code.

In case of third party testing, it is advisable to perform a source code inspection at the manufacturer’s premises. Third party agencies are not required to have the actual source code files as long as they have documented the unique identifiers for the originally inspected source code.

Table A.1 – General fault/error conditions

Component [a]	Fault/error	Acceptable measures [b c]	Definitions
1 CPU – Central Processing Unit			
1.1 Registers	Stuck at	Functional test, or Periodic self-test using either: – static memory test, or – word protection with single bit redundancy	A.3.5 A.3.6 A.3.38 A.3.41
1.2 Instruction decoding and execution	N/A		
1.3 Program counter	Stuck at	Functional test, or Periodic self-test, or Independent time-slot monitoring, or Logical monitoring of the program sequence	A.3.5 A.3.6 A.3.21 A.3.19
1.4 Addressing	N/A		
1.5 Data path instruction decoding	N/A		
2 Interrupt handling and execution	No interrupt or too frequent interrupt	Functional test, or Time-slot monitoring	A.3.5 A.3.21
3 Clock	Wrong frequency (for quartz synchronized clock: harmonics / sub-harmonics only)	Frequency monitoring, or Time slot monitoring	A.3.18 A.3.21
4 Memory			
4.1 Invariable (/nonvolatile) memory	All single bit faults	Periodic modified checksum, or Multiple checksum, or Word protection with single bit redundancy	A.3.33 A.3.34 A.3.41
4.2 Variable (/volatile) memory	DC fault	Periodic static memory test, or Word protection with single bit redundancy	A.3.38 A.3.41
4.3 Addressing (relevant to variable and invariable memory)	Stuck at	Word protection with single bit redundancy including the address	A.3.41
5 Internal data path			
5.1 Data	Stuck at	Word protection with single bit redundancy	A.3.41
5.2 Addressing	Wrong address	Word protection with single bit redundancy including the address	A.3.41

Component [a]	Fault/error	Acceptable measures [b c]	Definitions
6 External communication			
6.1 Data	All single bit and double bit errors (Hamming distance 3)	Word protection with multi-bit redundancy, or CRC – single word, or Transfer redundancy, or Protocol test	A.3.40 A.3.35 A.3.12 A.3.25
6.2 Addressing	Wrong address	Word protection with multi-bit redundancy, including the address, or CRC – single word, including the addresses; or Transfer redundancy, or Protocol test	A.3.40 A.3.35 A.3.12 A.3.25
6.3 Timing	Wrong point in time	Time-slot monitoring, or Scheduled transmission	A.3.21 A.3.28
	Wrong sequence	Logical monitoring, or Time-slot monitoring, or Scheduled transmission	A.3.19 A.3.21 A.3.28
7 Input/output periphery			
7.1 Digital I/O	Stuck at	Plausibility check for applicable conditions see 6.1/6.2	A.3.24
7.2 Analog I/O			
7.2.1 A/D- and D/A-convertor	Stuck at	Plausibility check for applicable conditions see 6.1 / 6.2	A.3.24
7.2.2 Analog multiplexer	Wrong addressing	Plausibility check	A.3.24
8 Monitoring devices and comparators	N/A		
9 Custom chips [d] e.g. ASIC, GAL, Gate array	Any output outside the static and dynamic functional specification	Periodic self-test	A.3.6
Table A.1 is applied according to the requirements of Clause A.2 to A.4.2.9 inclusive. A stuck-at fault model denotes a fault model representing an open circuit or a non-varying signal level. A DC fault model denotes a stuck-at fault model incorporating short circuits between signal lines. N/A means not applicable fault/error assumed			
[a] For fault/error assessment, some components are divided into their sub-functions. [b] For each sub-function in the table, the Table A.2 measure will cover the software fault/error. [c] Where more than one measure is given for a sub-function, these are alternatives. [d] (Not covered by 1-8) To be divided as necessary by the manufacturer into sub-functions.			

Table A.2 – Specific fault/error conditions

Component [a]	Fault/error	Acceptable measures [b c]	Definitions
1 CPU – Central Processing Unit			
1.1 Registers	DC fault	Comparison of redundant CPUs by either:	
		– reciprocal comparison	A.3.26
		– independent hardware comparator, or	A.3.13
		Internal error detection, or	A.3.17
		Redundant memory with comparison, or	A.3.37
		Periodic self-tests using either:	
		– walkpat memory test	A.3.39
		– Abraham test	A.3.31
		– transparent GALPAT test; or	A.3.32
		Word protection with multi-bit redundancy, or	A.3.40
		Static memory test and word protection with single bit redundancy	A.3.38 A.3.41
1.2 Instruction decoding and execution	Wrong decoding and execution	Comparison of redundant CPUs by either:	
		– reciprocal comparison	A.3.26
		– independent hardware comparator, or	A.3.13
		Internal error detection, or	A.3.17
		Periodic self-test using equivalence class test	A.3.14
1.3 Program counter	DC fault	Periodic self-test and monitoring using either:	A.3.7
		– independent time-slot and logical monitoring	A.3.20
		– internal error detection, or	A.3.17
		Comparison of redundant functional channels by either:	
		– reciprocal comparison	A.3.26
		– independent hardware comparator	A.3.13
1.4 Addressing	DC fault	Comparison of redundant CPUs by either:	
		– reciprocal comparison	A.3.26
		– independent hardware comparator; or	A.3.13
		Internal error detection; or	A.3.17
		Periodic self-test using a testing pattern of the address lines; or	A.3.7 A.3.30
		Full bus redundancy, or	A.3.8
		Multi-bit bus parity including the address	A.3.9
1.5 Data paths instruction decoding	DC fault and execution	Comparison of redundant CPUs by either:	
		reciprocal comparison, or	A.3.26
		independent hardware comparator, or	A.3.13
		Internal error detection, or	A.3.17
		Periodic self-test using a testing pattern, or	A.3.7
		Data redundancy, or	A.3.11
		Multi-bit bus parity	A.3.9

Component [a]	Fault/error	Acceptable measures [b c]	Definitions
2 Interrupt handling and execution	No interrupt or too frequent interrupt related to different sources	Comparison of redundant functional channels by either: – reciprocal comparison, – independent hardware comparator, or Independent time-slot and logical monitoring	 A.3.26 A.3.13 A.3.20
3 Clock	Wrong frequency (for quartz synchronized clock: harmonics/ sub harmonics only)	Frequency monitoring, or Time-slot monitoring, or Comparison of redundant functional channels by either: – reciprocal comparison – independent hardware comparator	A.3.18 A.3.21 A.3.26 A.3.13
4. Memory			
4.1 Invariable (/nonvolatile) memory	99,6 %coverage of all information errors	Comparison of redundant CPUs by either: – reciprocal comparison – independent hardware comparator, or Redundant memory with comparison, or Periodic cyclic redundancy check, either – single word – double word, or Word protection with multi-bit redundancy	 A.3.26 A.3.13 A.3.37 A.3.35 A.3.36 A.3.40
4.2 Variable (/volatile) memory	DC fault and dynamic cross links	Comparison of redundant CPUs by either: – reciprocal comparison – independent hardware comparator, or Redundant memory with comparison, or Periodic self-tests using either: – walkpat memory test – Abraham test – transparent GALPAT test, or Word protection with multi-bit redundancy	 A.3.26 A.3.13 A.3.37 A.3.39 A.3.31 A.3.32 A.3.40
4.3 Addressing (relevant to variable/volatile and invariable/nonvolatile memory)	DC fault	Comparison of redundant CPUs by either: – reciprocal comparison, or – independent hardware comparator, or Full bus redundancy testing pattern, or Periodic cyclic redundancy check, either: – single word – double word, or Word protection with multi-bit redundancy including the address	 A.3.26 A.3.13 A.3.8 A.3.35 A.3.36 A.3.40
5 Internal data path			

Component [a]	Fault/error	Acceptable measures [b c]	Definitions
5.1 Data	DC fault	Comparison of redundant CPUs by either:	
		– reciprocal comparison	A.3.26
		– independent hardware comparator, or	A.3.13
		Word protection with multi-bit redundancy including the address, or	A.3.40
		Data redundancy, or	A.3.11
		Testing pattern, or	A.3.30
		Protocol test	A.3.25
5.2 Addressing	Wrong address and multiple addressing	Comparison of redundant CPUs by:	
		– reciprocal comparison	A.3.26
		– independent hardware comparator, or	A.3.13
		Word protection with multi-bit redundancy including the address, or	A.3.40
		Full bus redundancy, or	A.3.8
		Testing pattern including the address	A.3.30
6 External communication			
6.1 Data	All single bit, double bit and triple errors (Hamming distance 4)	CRC – double word, or	A.3.36
		Data redundancy or	A.3.11
		Comparison of redundant functional channels by either:	
		– reciprocal comparison	A.3.26
		– independent hardware comparator	A.3.13
6.2 Addressing	Wrong and multiple addressing	CRC – double word, including the address, or	A.3.36
		Full bus redundancy of data and address, or	A.3.8
		Comparison of redundant communication channels by either:	
		– reciprocal comparison	A.3.26
		– independent hardware comparator	A.3.13
6.3 Timing	Wrong point in time	Time-slot and logical monitoring, or	A.3.20
		Comparison of redundant communication channels by either:	
		– reciprocal comparison	A.3.26
		– independent hardware comparator	A.3.13
	Wrong sequence	(same options as for wrong point in time)	

Component [a]	Fault/error	Acceptable measures [b c]	Definitions
7 Input/output periphery			
7.1 Digital I/O	DC fault	Comparison of redundant CPUs by either: – reciprocal comparison – independent hardware comparator, or Input comparison, or Multiple parallel outputs, or Output verification, or Testing pattern, or Code safety for applicable conditions see 6.1/6.2	 A.3.26 A.3.13 A.3.16 A.3.22 A.3.23 A.3.30 A.3.10
7.2 Analog I/O			
7.2.1 A/D- and D/A-convertor	DC fault	Comparison of redundant CPUs by either: – reciprocal comparison – independent hardware comparator, or Input comparison, or Multiple parallel outputs, or Output verification, or Testing pattern for applicable conditions see 6.1/6.2	 A.3.26 A.3.13 A.3.16 A.3.22 A.3.23 A.3.30
7.2.2 Analog multiplexer	Wrong addressing	Comparison of redundant CPUs by either: – reciprocal comparison – independent hardware comparator, or Input comparison or Testing pattern	 A.3.26 A.3.13 A.3.16 A.3.30
8 Monitoring devices and comparators	Any output outside the static and dynamic functional specification	Tested monitoring, or Redundant monitoring and comparison, or Error recognizing means	A.3.29 A.3.27 A.3.15
9 Custom chips [d] e.g. ASIC, GAL, gate array	Any output outside the static and dynamic functional specification	Periodic self-test and monitoring, or Dual channel (diverse) with comparison, or Error recognizing means	A.3.7 A.3.2 A.3.15
Table A.2 is applied according to the requirements of Clause A.2 to A.4.2.9 inclusive. A DC fault model denotes a stuck-at fault model incorporating short circuits between signal lines.			
[a] For fault/error assessment, some components are divided into their sub-functions. [b] For each sub-function in the table, the software measure will cover the Table A.1 fault/error. [c] Where more than one measure is given for a sub-function, these are alternatives. [d] (Not covered by 1-8) To be divided as necessary by the manufacturer into sub-functions.			

A.4.2.5 For programmable components requiring software incorporating measures to control the fault/error conditions specified in Table A.1 or Table A.2, detection of a fault/error shall occur before compliance with Clause 6 of this standard is impaired.

Compliance is checked by inspection and testing of the source code.

The loss of dual channel capability is deemed to be an error in a programmable component using a dual channel structure required for software to control the fault/error conditions specified in Table A.2.

A.4.2.6 The software shall be referenced to relevant parts of the operating sequence and the associated hardware functions.

Compliance is checked by inspection of the source code.

A.4.2.7 Where labels are used for memory locations, these labels shall be unique.

Compliance is checked by testing of the source code.

A.4.2.8 The software shall be protected from user alteration of safety-related segments and data.

Compliance is checked by testing of the source code.

A.4.2.9 The software and safety-related hardware under its control shall be initialized and shall terminate before compliance with Clause 6 is impaired.

Compliance is checked by review of the testing of the source code.

A.5 Measures to avoid errors

A.5.1 General

For protective programmable components with functions requiring software incorporating measures to control the fault/error conditions specified in Table A.1 or Table A.2, the following measures to avoid systematic faults in the software shall be applied.

Software that incorporates measures used to control the fault/error conditions specified in Table A.2 is inherently acceptable for software required to control the fault/error conditions specified in Table A.1.

NOTE The terms in Tables A.3 to A.7 are based on IEC 61508-7. They are informative for the purpose of this standard and not explained here.

A.5.2 Specification

A.5.2.1 Software safety requirements

The specification of the software safety requirements shall include:

- a description of each safety related function to be implemented, including its response time(s):
  - functions related to the application including their related software faults required to be controlled;
  - functions related to the detection, annunciation and management of software or hardware faults;
- a description of interfaces between software and hardware;
- a description of interfaces between any safety and non-safety related functions;

- a description of any compiler used to generate the object code from the source code, including details of any compiler switch settings used such as library function options, memory model, optimization, SRAM details, clock rate and chip details.

  Care should be taken with the choice of the compiler; it should be robust with a proven track record;
- a description of any linker used to link the object code to executable library routines.

Compliance is checked by inspection of the documentation and as specified in A.5.2.2.2.

NOTE Examples of some techniques/measures to meet these requirements can be found in Table A.3.

Table A.3 – Semi-formal methods

Technique/measure	Informative references
Semi-formal methods	
Logical/functional block diagrams	
Sequence diagrams	
Finite state machines/state transition diagrams	– IEC 61508-7:2010, B.2.3.2
Decision/truth tables	– IEC 61508-7:2010, C.6.1

A.5.2.2 Software architecture

A.5.2.2.1 The specification of the software architecture shall include the following aspects:

- techniques and measures to control software faults/errors (refer to A.4.2);
- interactions between hardware and software;
- partitioning into modules and their allocation to the specified safety functions;
- hierarchy and call structure of the modules (control flow);
- interrupt handling;
- data flow and restrictions on data access;
- architecture and storage of data;
- time-based dependencies of sequences and data.

Compliance is checked by inspection of the documentation and as specified in A.5.2.2.2.

NOTE Examples of some techniques/measures to meet these requirements can be found in Table A.4.

Table A.4 – Software architecture specification

Technique/measure	Informative references
Fault detection and diagnosis	– IEC 61508-7:2010, C.3.1
Semi-formal methods:	
– Logic/function block diagrams	
– Sequence diagrams	
– Finite state machines/state transition diagrams	– IEC 61508-7:2010, B.2.3.2
– Data flow diagrams	– IEC 61508-7:2010, C.2.2

A.5.2.2.2 The architecture specification shall be validated against the specification software safety requirements by static analysis.

NOTE Example methods for static analysis are:

- control flow analysis; (IEC 61508-7:2010, C.5.9);
- data flow analysis; (IEC 61508-7:2010, C.5.10);
- walk-throughs/design reviews. (IEC 61508-7, C.5.16).

A.5.2.3 Module design and coding

A.5.2.3.1 Based on the architecture design, software shall be suitably refined into modules. Software module design and coding shall be implemented in a way that is traceable to the software architecture and requirements.

Compliance is checked by A.5.2.3.3 and by inspection of the documentation.

The use of computer aided design tools is accepted.

Defensive programming (IEC 61508-7:2010, C.2.5) is recommended (e.g. range checks, check for division by 0, plausibility checks).

The module design should specify:

- function(s),
- interfaces to other modules,
- data.

NOTE Examples of some techniques/measures to meet these requirements can be found in Table A.5.

Table A.5 – Module design specification

Technique/measure	Informative references
Limited size of software modules	IEC 61508-7:2010, C.2.9
Information hiding/encapsulation	IEC 61508-7:2010, C.2.8
One entry/one exit point in subroutines and functions	IEC 61508-7:2010, C.2.9
Fully defined interface	IEC 61508-7:2010, C.2.9
Semi-formal methods:	
– Logic/function block diagrams	
– Sequence diagram	
– Finite state machines/state transition diagrams	IEC 61508-7:2010, B.2.3.2
– Data flow diagrams	IEC 61508-7:2010, C.2.2

A.5.2.3.2 The software code shall be structured.

Compliance is checked by A.5.2.3.3 and by inspection of the documentation.

NOTE 1 Structural complexity can be minimized by applying the following principles:

- keep the number of possible paths through a software module small, and the relation between the input and output parameters as simple as possible;
- avoid complicated branching and, in particular, avoid unconditional jumps (GOTO) in higher level languages;
- where possible, relate loop constraints and branching to input parameters;
- avoid using complex calculations as the basis of branching and loop decisions.

NOTE 2 Examples of some techniques/measures to meet these requirements can be found in Table A.6.

Table A.6 – Design and coding standards

Technique/Measure	Informative references
Use of coding standard [a]	IEC 61508-7:2010, C.2.6.2
No use of dynamic objects and variables [a]	IEC 61508-7:2010, C.2.6.3
Limited use of interrupts	IEC 61508-7:2010, C.2.6.5
Limited use of pointers	IEC 61508-7:2010, C.2.6.6
Limited use of recursion	IEC 61508-7:2010, C.2.6.7
No unconditional jumps in programs in higher level languages	IEC 61508-7:2010, C.2.6.2
[a] Dynamic objects and/or variables are allowed if a compiler is used which ensures that sufficient memory for all dynamic objects and/or variables will be allocated before runtime, or which inserts runtime checks for the correct online allocation of memory.	

A.5.2.3.3 Coded software shall be validated against the module specification by static analysis. The module specification shall be validated against the architecture specification by static analysis.

A.5.3 Software validation

The software shall be validated with reference to the requirements of the software safety requirements specification. Testing should be the main validation method for software; modelling may be used to supplement the validation activities.

NOTE 1 Validation is confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. Therefore, for example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software safety requirements specification.

Compliance is checked by simulation of

- *input signals present during normal operation,*
- *anticipated occurrences,*
- *undesired conditions requiring system action.*

Test cases, test data and test results shall be reported.

NOTE 2 Examples of some techniques/measures to meet these requirements can be found in Table A.7.

Table A.7 – Software safety validation

Technique/Measure	Informative references
Functional and black-box testing: Boundary value analysis – Process simulation	– IEC 61508-7, B.5.1, B.5.2 – IEC 61508-7, C.5.4 – IEC 61508-7, C.5.18
– Simulation, modelling: Finite state machines – Performance modelling	 IEC 61508-7, B.2.3.2 – IEC 61508-7, C.5.20

Annex B
(informative)

FTA and FMEA analysis

B.1 FTA results

While several hazards can exist for the electronic lamp controlgear, the manufacturer identifies and documents the failure conditions in the programmable component that can affect the safety of the appliance. Typically, each identified hazard is described using a simple statement. The evaluation includes the sensors and actuators that are associated with the safety function.

NOTE 1 Figure B.1 is an example for a hazard statement: “The continuously conducting FET(s) causes overheating in a hot environment”.

A fault tree analysis (FTA) is a top-down approach to identify the causes of hazards, after the hazards are identified. The process requires a substantial amount of detailed knowledge of the equipment. It provides insight into how potential failure events and the combination of these failures affect the top-level identified hazards.

NOTE 2 Examples of potential failure events include these:

- a software failure that causes a branch to the wrong part of a program;
- a component failure in the programmable component that handles a device input or output signal;
- a problem with the memory in the programmable component.

After the FTA the fault conditions that could lead to each of the identified hazard(s) are recorded using the FMEA table.

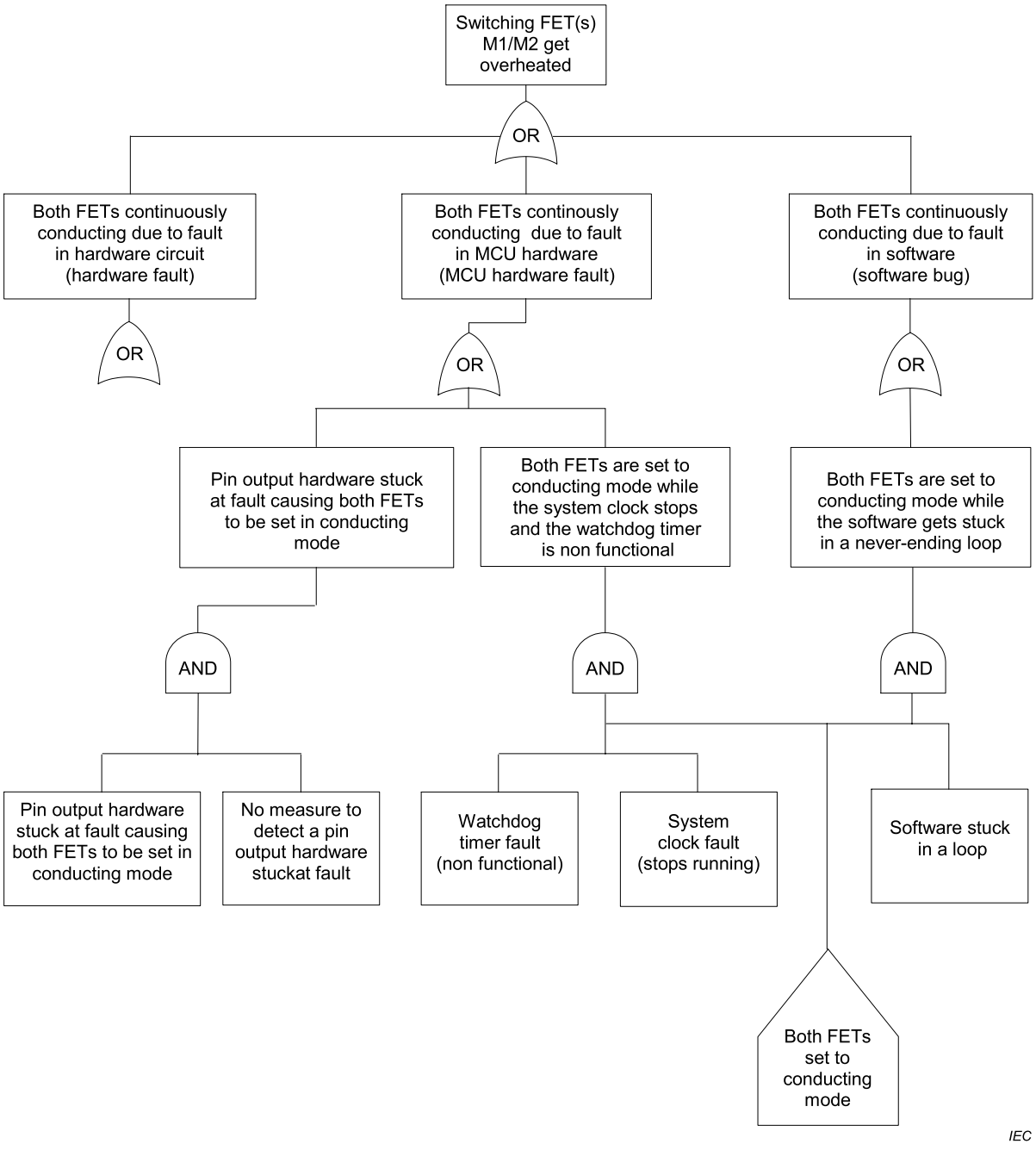

Figure B.1 – Example of a fault tree diagram

B.2 FMEA results

The results of the failure mode and effect analysis (FMEA) are documented, as a minimum, in accordance with Table A.2 of C22.2 No. 0.8-12, May 2012, *Safety functions incorporating electronic technology* [4]. Additional details may be provided where appropriate. All conditions noted in the fault tree (FTA) are included in this FMEA table. Safety-related error messages are referenced where applicable.

NOTE The analysis usually takes place through a meeting of engineers. Each component of a system is analysed in turn to give a set of failure modes for the component, their causes and effects (locally and at overall system level), detection procedures and recommendations. If the recommendations are acted upon, they are documented as remedial action taken. The description of this procedure can be found in: IEC 61508-7:2010, B.6.6.1]

FMEA table format

An example of the format for documenting the FMEA information can be found in Table A.2 of [4]. The information in this table is usually completed as design evolves and provides a useful checklist to cover all of the stated failure modes. Where software is used, the FMEA analysis needs to include potential failures that could be caused by faults in the software. All failures shown in the fault tree are included with the failures noted in the FMEA table. Hardware components are properly identified and referenced to the appropriate diagrams, whether by architectural block diagram or by schematic.

Annex C
(informative)

Guidance on the identification of a protective programmable component

A protective programmable component (PPC) is a programmable component (PC) with a software safety feature that keeps the electronic lamp controlgear safe under the abnormal operating or fault conditions in this standard. The evaluation includes the sensors and actuators that are associated with the software function.

NOTE 1 A PPC can be for instance a microcontroller which detects the occurrence of an abnormal condition and prevents that this leads to an unsafe situation by switching off a certain circuit of the equipment or the complete electronic lamp controlgear, for example.

A PPC can be identified in many different ways such as by an assessment of the safety philosophy of the electronic equipment through a thorough examination of the circuit diagrams.

The following, more practical, methods can be used to determine and identify whether the electronic controlgear contains a protective programmable component:

a) the relevant tests related to 6.1 and 6.2 are performed with the complete programmable component in question being disabled;

b) considering all possible (worst case) input and output signals of the programmable component; or

c) any (both all and any combinations of) software protection, software control, and software setting embedded in the programmable component, being disabled and/or made inactive.

NOTE 2 Methods a) and b) can be used in case of not disclosed IC, ASIC, not assessable code, etc.

The pitfall is, while there may be many reliability functions in the software, some of them possibly could have influence on safety. A thorough analysis and test may be needed before any safety protective measure is identified. This is to ensure the required safety robustness measures of this standard.

No PPC is present in the electronic lamp controlgear if under the circumstances of this annex the electronic lamp controlgear remains safe in accordance with 6.2. However if the electronic lamp controlgear does not remain safe, it can be concluded that the programmable component under test prevents an unsafe situation under an abnormal or fault conditions and it shall therefore comply with the requirements of a PPC.

In case no PPC's have been identified, it is advisable that the method chosen to identify or exclude the presence of a PPC is recorded in a clear way for future reference; for example, what input and output signals had been considered for the programmable component (method b)) and/or which function of the programmable component software had been disabled (method c)). The method of failure modes and effects analysis (FMEA) or fault tree analysis (FTA) can be used (see Annex B).

Annex D
(normative)

Risk classification

D.1 General

This annex defines the categorization of risk frequencies and severities and the classification of safety risks. An informative description is provided in IEC 61508-5:2010 Annex C.

D.2 Frequency of occurrence

The categorization of the probability or frequency of occurrence of safety risks is defined in Table D.1

The probability can be calculated in various ways based on:

- the likelihood that a product is subject to an occurrence of the risk;
- the expected number of products in a batch of which one product is subject to one occurrence of the risk;
- the expected number of occurrences of the risk over the lifetime of a single product.

Table D.1 – Frequency definition and categorization (from IEC 61508-5:2010 Annex C)

Frequency of occurrence	Description	10^{-6} level (indicative)
Frequent	Likely to occur frequently or continuously experienced	=>10^5
Probable	Will occur several times in the lifetime of the product	10^4
Occasional	Likely to occur sometime in the life of a product	1000
Remote	Unlikely but possible to occur in life of a product	100
Improbable	So unlikely, it can be assumed occurrence may not be experienced during the life of the product	10
Incredible	Unbelievable to occur during the life of the product	<=1

D.3 Risk severity

The categorization of the severity of a safety risk is defined in Table D.2

Table D.2 – Risk severity definitions (from IEC 61508-5:2010, Annex C)

Severity	Description
Catastrophic	Potential of multiple deaths or serious injuries
Critical	Potential of deaths or serious injury
Marginal	Potential of injury
Negligible	Little or no potential of injury

D.4 Classification of risks

Every safety risk shall be classified in accordance with Table D.3 as either “intolerable”, “ALARP” or “acceptable”. An acceptable risk is a risk that can be accepted in a given context based on the values of the society under consideration at the time of the safety evaluation. An intolerable risk is a risk that it is so great that it shall be refused altogether. The ALARP or “As low as is reasonably practicable” risk is a risk that falls between acceptable risk and intolerable risk and has to be reduced to the lowest practicable level, bearing in mind the benefits resulting from its acceptance and taking into account the practicability of any further reduction.

Table D.3 – Safety risk classification

Likelihood	Severity			
	Catastrophic	Critical	Marginal	Negligible
Frequent	Intolerable	Intolerable	Intolerable	Intolerable
Probable	Intolerable	Intolerable	ALARP	ALARP
Occasional	Intolerable	ALARP	ALARP	ALARP
Remote	ALARP	ALARP	ALARP	Acceptable
Improbable	ALARP	ALARP	Acceptable	Acceptable
Incredible	Acceptable	Acceptable	Acceptable	Acceptable

A manufacturer may choose to apply a different table or mechanism to classify safety risks under the condition that the classification satisfies the following requirements.

- Each risk which is so great that it cannot be justified under any circumstance is classified as “intolerable”.
- Each risk which is classified as “acceptable” is acceptable to the society under consideration, considering the social, political, and economical values of the society at the time of the safety evaluation.

The manufacturer shall provide a justification of the table or mechanism that is used.

All classifications other than “intolerable” and “acceptable” shall be treated as “ALARP” in the context of this standard.

Bibliography

[1] IEC 62368-1:2010, *Audio/video, information and communication technology equipment – Part 1: Safety requirements*

[2] ANSI/UL 1998-2008, *Standard for Software in Programmable Components*

[3] User Guide UG – 106, Version 0.92 July, 2010, CSA INTERNATIONAL, *Safety Controls with Software Hazard Analysis Guide & Information Requirements*

[4] C22.2 No. 0.8-12, May 2012, *Safety functions incorporating electronic technology*

[5] OD-2045-Ed.1.0, IECEE, *Guideline document & work instructions for testing purposes on how to implement the Annex R of IEC 60335-1 and Annex H of IE 60730-1*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

COMPOSANTS PROGRAMMABLES DANS LES APPAREILLAGES ÉLECTRONIQUES DE LAMPES – EXIGENCES GÉNÉRALES ET EXIGENCES DE SÉCURITÉ

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62733 a été établie par le sous-comité 34C: Appareils auxiliaires pour lampes, du comité d'études 34 de l'IEC: Lampes et équipements associés.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
34C/1140/FDIS	34C/1156/RVD

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

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

NOTE Dans la présente norme, les caractères d'imprimerie suivants sont employés:

– Exigences proprement dites: caractères romains.

– Modalités d'essais: *caractères italiques*.

– Commentaires: petits caractères romains.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC 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

La présente Norme internationale définit les exigences de sécurité et les méthodes d'essai des composants programmables utilisés dans les appareillages électroniques de lampes. Elle complète les exigences de la série IEC 61347 par des exigences de sécurité supplémentaires relatives aux appareillages électroniques de lampes contenant des composants programmables.

En général, les deux moyens de protection sont utilisés contre les dangers tels que les chocs électriques. Par conséquent, une condition de premier défaut ou un fonctionnement anormal du matériel électrique ne donnera pas lieu à une situation dangereuse.

Jusqu'à récemment, la technologie a offert deux moyens de protéger le matériel traditionnel. Il s'agit par exemple de prévoir une isolation de base et une isolation supplémentaire entre les parties actives dangereuses et les parties accessibles, et de prévoir une isolation de base combinée par la déconnexion de l'alimentation principale à l'aide d'un fusible.

Toutefois, de nos jours, des composants programmables (à logiciel intégré) peuvent être utilisés pour assurer la sécurité dans des conditions normales, des conditions de premier défaut et/ou un fonctionnement anormal.

Les normes en matière d'éclairage traditionnel ne fournissant pas les exigences pour les composants programmables, la présente norme a été établie.

La présente norme reconnaît le niveau de protection internationalement accepté contre les phénomènes dangereux (électriques, mécaniques, thermiques, liés au feu et au rayonnement des appareils lorsqu'ils fonctionnent comme en utilisation normale en tenant compte des instructions du constructeur, par exemple). Elle couvre également les conditions des phénomènes électromagnétiques pouvant se produire et influencer le composant programmable, afin de tenir compte de l'impact pouvant influencer le fonctionnement en toute sécurité des appareillages électroniques de lampes.

Cette première édition repose sur l'IEC 60730-1:2010 et l'IEC 60335-1:2010, et a été adaptée pour les appareillages électroniques de lampes.

NOTE Les termes et définitions ainsi que le Tableau A.1 et le Tableau A.2 respectivement de la présente norme équivalent aux termes et définitions, au Tableau R.1 et au Tableau R.2 de l'IEC 60335-1:2010, et aux termes et définitions équivalents et au Tableau H.1 (logiciel de classe B et de classe C) de l'IEC 60730-1.

COMPOSANTS PROGRAMMABLES DANS LES APPAREILLAGES ÉLECTRONIQUES DE LAMPES – EXIGENCES GÉNÉRALES ET EXIGENCES DE SÉCURITÉ

1 Domaine d'application

La présente Norme internationale définit les exigences générales et les exigences de sécurité des composants programmables utilisés dans les produits couverts par l'IEC 61347.

Les exigences de la présente norme s'appliquent uniquement aux composants programmables (et leurs logiciels intégrés) des appareillages électroniques de lampes. Pour les autres circuits électriques/électroniques et leurs composants dans les appareillages électroniques de lampes, les exigences de la série IEC 61347 s'appliquent.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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).

IEC 61000-4-13:2002, *Compatibilité électromagnétique (CEM) – Partie 4-13: Techniques d'essai et de mesure – Essais d'immunité basse fréquence aux harmoniques et inter-harmoniques incluant les signaux transmis sur le réseau électrique alternatif*
IEC 61000-4-13:2002/AMD1:2009

IEC 61347-1, *Appareillages de lampes – Partie 1: Exigences générales et exigences de sécurité*

IEC 61347-2, (toutes les parties)[1], *Appareillages de lampes – Part 2: Exigences particulières IEC 61547:2009, Equipements pour l'éclairage à usage général – Exigences concernant l'immunité CEM*

IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 4: Définition et abréviations*

IEC 61508-5:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 5: exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*

IEC 61508-7:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

3 Termes et définitions

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

---

1 Les parties applicables d'une série dépendent du contexte.

3.1
unité centrale
CPU
partie d'un système de calcul ou de commande qui interprète et exécute des instructions

Note 1 à l'article: L'abréviation "CPU" est dérivée du terme anglais développé correspondant "central processing unit".

3.2
composant programmable
technologie basée sur l'informatique, pouvant comprendre du matériel, du logiciel, ainsi que les unités d'entrée et/ou de sortie

EXEMPLE Tous les éléments ci-dessous sont des composants programmables:

– microprocesseurs;
– microcontrôleurs;
– automates programmables;
– circuits intégrés numériques spécifiques à l'application (ASIC[2] avec partie programmable);
– automates logiques programmables (PLC[3]);
– autres dispositifs basés sur la technologie informatique (par exemple, les capteurs intelligents, les émetteurs-récepteurs, les actionneurs).

Note 1 à l'article: Ce terme couvre les dispositifs microélectroniques basés sur une ou plusieurs unités centrales (CPU) associées à des mémoires, etc.

Note 2 à l'article: Le terme "composant programmable" est dérivé de l'ANSI/UL1998:2010, définition 2.39[2]. La définition dans ANSI/UL du terme "composant programmable" est la suivante: "Tous les matériels microélectroniques qui peuvent être programmés dans le centre de conception, en usine ou sur site". Ici, le terme "programmable" indique "une manière de modifier le logiciel dans laquelle le comportement du composant peut être modifié." Ce terme couvre les dispositifs microélectroniques reposant sur une ou plusieurs unités centrales (CPU) associées à des mémoires, etc.

[SOURCE: IEC 61508-4:2010, 3.2.12 modifiée — "Électronique programmable" est remplacé par "composant programmable" qui décrit mieux qu'il s'agit uniquement d'une partie de l'appareillage.]

3.3
composant programmable de protection
PPC
composant programmable qui empêche une situation dangereuse de se produire dans des conditions de fonctionnement anormales ou composant programmable dont aucun des signaux de sortie ne peut donner lieu à une situation dangereuse

Note 1 à l'article: L'abréviation "PPC" est dérivée du terme anglais développé correspondant "protective programmable component".

3.4
logiciel
création intellectuelle comprenant les programmes, les procédures, les données et les règles, ainsi que toute documentation associée se référant au fonctionnement d'un système de traitement de données

[SOURCE: IEC 61508-4:2010, 3.2.5 modifiée — Les notes à l'article sont supprimées.]

---

2 Application specific integrated circuits *en anglais*.

3 Programmable logic controllers *en anglais*.

3.5
code logiciel
code écrit par un programmeur dans un langage informatique de haut niveau et lisible par les personnes mais pas par les ordinateurs

3.6
logiciel de sécurité
partie du logiciel qui s'oppose aux éventuelles situations dangereuses apparues suite à des conditions anormales et/ou de défaut

Note 1 à l'article: Le logiciel est indépendant du support sur lequel il est enregistré.

3.7
condition de défaut
condition comme exigé par l'Article 14 de l'IEC 61347-1 ou sa Partie 2 correspondante

3.8
condition de premier défaut
condition de défaut dans les conditions normales de fonctionnement d'un seul composant ou dispositif

[SOURCE: IEC 62368-1:2010, 3.3.7.10, modifiée]

3.9
conditions normales de fonctionnement
mode de fonctionnement qui reflète le mieux les conditions d'utilisation normale les plus rigoureuses auxquelles on peut raisonnablement s'attendre

[SOURCE: IEC 62368-1:2010, 3.3.7.4, modifiée]

3.10
conditions anormales de fonctionnement
conditions de fonctionnement temporaires qui ne sont ni les conditions normales de fonctionnement ni les conditions de premier défaut de l'équipement proprement dit

Note 1 à l'article: Des conditions anormales de fonctionnement peuvent être induites par l'équipement ou par une personne.

Note 2 à l'article: Il convient d'étudier l'équipement, l'installation, les instructions et les spécifications afin de déterminer les conditions anormales de fonctionnement qu'il est raisonnable d'attendre.

Note 3 à l'article: Les défauts, qui sont la conséquence directe d'une condition anormale de fonctionnement, sont réputés être une condition de premier défaut.

[SOURCE: IEC 62368-1:2010, 3.3.7.1, modifiée]

3.11
analyse par arbre de panne
AAP
méthode d'analyse des défaillances par déduction, de haut en bas, dans laquelle un événement dangereux ou grave est analysé à l'aide de la logique booléenne pour combiner une série d'événements à l'origine de cet événement

Note 1 à l'article: L'analyse par arbre de panne est une technique d'analyse "de haut en bas". L'Annexe B de l'IEC 61508-7:2010 donne des informations de configuration minimale d'un rapport AAP.

3.12
analyse des modes de défaillance et de leurs effets
AMDE
technique analytique dans laquelle les types de défaillance de chaque composant du matériel et du logiciel sont identifiés et examinés quant à leurs effets sur les fonctions liées à la sécurité du dispositif de commande

Note 1 à l'article: L'analyse des modes de panne et de leurs effets est une technique d'analyse "de bas en haut". L'Annexe B donne des informations de configuration minimale d'un rapport AMDE.

[SOURCE: IEC 60730-1:2010, H.2.20.3, modifiée]

3.13
tension assignée
valeur de la tension, fixée par le constructeur à un composant, à un dispositif ou à un matériel et à laquelle on se réfère pour le fonctionnement et pour les caractéristiques fonctionnelles

Note 1 à l'article: L'équipement peut présenter plus d'une valeur de tension assignée ou bien une plage de tensions assignées.

Note 2 à l'article: Pour une alimentation triphasée, la tension entre phases s'applique.

[SOURCE: IEC 62368-1:2010, 3.3.10.4, modifiée]

3.14
risque tolérable
niveau de risque comme défini en 5.1.

3.15
risque intolérable
niveau de risque qui ne peut pas être justifié, sauf dans des circonstances extraordinaires

3.16
risque acceptable
niveau de risque qui est largement accepté dans la société

3.17
aussi bas que raisonnablement possible
ALARP
niveau de risque situé entre le risque acceptable et le risque intolérable, qui doit être réduit au niveau praticable le plus bas, en gardant à l'esprit les avantages que procure son acceptation, et en tenant compte de la possibilité d'exécution d'une éventuelle réduction

Note 1 à l'article: L'abréviation "ALARP" est dérivée du terme anglais développé correspondant "As Low As is Reasonably Practicable.

Note 2 à l'article: La spécification du niveau ALARP est décrite à l'Annexe D.

Note 3 à l'article: Cette définition est conforme à l'IEC 61508-5:1998, Annexe B. Dans la présente norme, elle est utilisée comme une variante possible du risque tolérable.

3.18
blessure
dommage physique à une personne, inférieur à une incapacité de 2 %, en général réversible et ne faisant souvent l'objet d'aucun traitement en milieu hospitalier

EXEMPLE Coupures mineures, fractures très mineures ou brûlures mineures, entorses.

3.19
blessure grave
blessure qui, directement ou indirectement:

a) met en péril la vie,

b) entraîne une carence permanente d'une fonction physiologique ou endommage de manière définitive une structure du corps, ou

c) nécessite une intervention médicale ou chirurgicale pour prévenir une carence permanente d'une fonction physiologique ou un endommagement définitif d'une structure du corps

3.20
situation dangereuse
circonstance dans laquelle les personnes, les biens ou l'environnement sont exposés à des sources potentielles de blessure physique, de dommage à la santé des personnes ou de dommage aux biens ou à l'environnement

4 Exigences générales

Les logiciels des composants programmables des appareillages électroniques de lampes doivent être conçus et construits de telle manière qu'en usage normal, ils fonctionnent sans danger pour l'utilisateur ou pour l'environnement.

Les risques doivent être évalués afin de déterminer les parties applicables de la présente norme. Si l'évaluation des risques montre que l'intégration logicielle utilisée afin d'éviter que les appareillages ne deviennent dangereux présente un risque supérieur au risque tolérable, la présente norme est obligatoire.

Les risques éventuels que présentent les appareillages électroniques doivent être au cœur de l'évaluation des risques, y compris le fonctionnement anormal et les conditions de défaut de la Partie 2 correspondante de l'IEC 61347.

5 Evaluation des risques

5.1 Généralités

Les risques éventuels que présentent les appareillages doivent être au cœur de l'évaluation des risques. L'évaluation des risques doit permettre d'identifier et de classer les risques de dysfonctionnement connus ou raisonnablement prévisibles du logiciel (y compris les risques causés par des conditions de défaut interne potentielles et par un fonctionnement anormal des appareillages décrits dans la Partie 2 correspondante de l'IEC 61347) en s'appuyant sur l'hypothèse d'utilisation prévue.

Si l'évaluation des risques montre que l'intégration logicielle, visant à éviter que les appareillages ne deviennent dangereux, présente un risque supérieur au risque tolérable (ledit risque n'ayant pas été réduit par des mesures matérielles supplémentaires), toutes les parties de la présente norme s'appliquent.

Si l'évaluation des risques montre que le risque est tolérable, les appareillages satisfont à la présente norme. Dans ce cas, seules les parties de la présente norme décrivant l'évaluation des risques s'appliquent. Cela signifie que les parties suivantes de la norme ne s'appliquent pas: Articles 6, 7, 8 et Annexes A, B, C.

L'évaluation des risques pour la sécurité obtenue d'un composant programmable, identifié comme n'étant pas un composant programmable de protection ou qui n'a pas été évalué comme tel, est dispensée d'évaluation de code logiciel.

5.2 Spécification des risques tolérables

Trois paramètres permettent de spécifier le risque tolérable:

a) Le risque est classé comme étant tolérable si les effets d'un éventuel dysfonctionnement logiciel sont limités par des mesures matérielles (interruption de l'échauffement du matériel, par exemple), de sorte que les appareillages ne deviennent pas dangereux, et si les mesures matérielles et les appareillages sont conformes à la série IEC 61347. D'autre part, un deuxième composant programmable de protection (PPC) peut être utilisé pour limiter un éventuel dysfonctionnement logiciel, pour autant qu'il soit indépendant du premier PPC.

b) Par ailleurs, une spécification plus générale peut être utilisée.

   1) Le risque est tolérable si le niveau de risque des appareillages dotés d'un logiciel est le même que celui d'un appareillage de comparaison dans lequel les fonctions respectives liées à la sécurité sont réalisées par un matériel satisfaisant à la série IEC 61347.

   2) L'objectif est de vérifier un niveau de sécurité de l'appareillage (en cours d'évaluation) ayant au moins le même niveau de sécurité que celui d'un appareillage de comparaison dans lequel les fonctions respectives liées à la sécurité sont réalisées par un matériel satisfaisant à la série IEC 61347. L'appareillage de comparaison peut être réel ou imaginaire en fonction des appareillages matériels connus (ou parties de ces appareillages) qui satisfont à la série IEC 61347.

c) Un autre moyen permettant de spécifier le risque tolérable consiste à utiliser la classification générale des risques présentée à l'Annexe D, auquel cas le risque est tolérable s'il est classé ALARP ou dans les classes inférieures.

5.3 Documentation

L'évaluation des risques et ses résultats doivent être documentés par le constructeur.

Chaque risque faisant l'objet de ce processus doit être décrit, et sa cause potentielle indiquée.

Pour documenter les modes de défaut et de défaillance possibles, une analyse par arbre de panne (AAP) ou une analyse des modes de défaillance et de leurs effets (AMDE) peut être utilisée. L'Annexe B donne des informations de configuration minimale d'un rapport d'analyse AAP et AMDE. L'AAP est une technique d'analyse "de haut en bas", l'AMDE est une technique d'analyse "de bas en haut".

La documentation de l'évaluation des risques peut être consultée pour démontrer la conformité à la présente norme.

6 Exigences de fonctionnement anormal et conditions de défaut

6.1 Fonctionnement anormal et conditions de défaut dans l'application des appareillages électroniques de lampes

Le logiciel de sécurité doit être soumis à essai dans les conditions de défaut et les conditions anormales comme indiqué dans la norme respective de la série IEC 61347.

Pendant et après les essais, les appareillages électroniques de lampes doivent satisfaire aux critères de conformité de la norme correspondante de la série IEC 61347.

Si un composant programmable (PC) de l'appareillage électronique de lampes est censé assurer la conformité avec le présent article, le logiciel doit satisfaire aux exigences de l'Article 7 et de l'Article 8 de la présente norme pour un composant programmable de protection (PPC).

Un composant programmable, identifié comme n'étant pas un composant programmable de protection, ou non évalué comme composant programmable de protection, est exempt de l'évaluation du code logiciel. L'Annexe C décrit les méthodes possibles d'identification des composants programmables de protection.

Si le PPC fait l'objet de dispositions en matière de sécurité, la conformité avec l'Article 7 et l'Article 8 le protège contre une éventuelle défaillance susceptible de rendre l'appareillage électronique de lampes dangereux.

6.2 Conditions de défaut du composant programmable

Les conditions de défaut suivantes sont prises en compte pour les composants programmables équipant les appareillages électroniques de lampes et, le cas échéant, sont appliquées l'une après l'autre, les défauts importants étant pris en compte.

a) Court-circuit de l'isolation fonctionnelle entre des bornes de composant programmable adjacentes si l'écartement ou les distances des lignes de fuite sont inférieurs aux valeurs spécifiées à l'article correspondant de l'IEC 61347-1.

NOTE 1 Couvert par 14.1 de l'IEC 61347-1.

b) Circuit-ouvert au niveau d'une borne du composant programmable.

NOTE 2 Couvert par 14.2 de l'IEC 61347-1.

c) D'autre part, si le code logiciel n'est pas accessible, en alternative, sur la base d'une évaluation des risques liés à la sécurité, les broches du composant programmable sont placées dans un état dans lequel un problème de sécurité est susceptible de se produire.

d) En alternative à c) si le code est accessible, toutes les sorties sont supposées faire l'objet de pannes se produisant dans le composant programmable. Si une évaluation des risques liés à la sécurité peut démontrer qu'il est peu probable qu'un signal de sortie particulier se produise, le défaut correspondant n’est pas considéré. Les défauts correspondants ne sont pas pris en compte et peuvent être ignorés si le composant programmable satisfait aux exigences de l'Article 7 et de l'Article 8 de la présente norme quant au composant programmable de protection.

Il convient de procéder à une analyse AAP ou AMDE afin d'inclure les résultats de plusieurs conditions stables aux sorties et aux bornes bidirectionnelles programmées pour les besoins d'identification des conditions de défaut supplémentaires à prendre en compte, susceptibles ou pas de se produire.

NOTE 3 Un composant programmable à ne pas divulguer est évalué par analyse AAP/AMDE sur les signaux de sortie.

Si l'analyse AAP ou AMDE détermine que seules des conditions de défaillance critiques spécifiques et bien définies peuvent se produire, les essais individuels peuvent être remplacés par une simulation ou une justification de l'impact des conditions de défaillance pendant l'évaluation.

La conformité est vérifiée par examen et par des essais appropriés, le cas échéant.

Pendant et après les essais, les appareillages électroniques de lampes doivent satisfaire aux critères de conformité du premier alinéa du 14.1 de l'IEC 61347-1 et de la Partie 2 correspondante.

7 Exigences relatives au logiciel

Dans le cas des appareillages électroniques de lampes intégrant un composant programmable de protection, le logiciel du composant programmable doit contenir des mesures de contrôle des conditions de panne/erreur spécifiées au Tableau A.1. L'évaluation

des pannes/erreurs comprend les capteurs et actionneurs associés à la fonction de sécurité logicielle.

Le Tableau A.2 doit être utilisé lorsque le logiciel contenant des mesures pour contrôler les conditions de panne/erreur spécifiées au Tableau A.2, lorsque cela est spécifié dans la Partie 2 de l'IEC 61347 pour les constructions particulières ou pour traiter les dangers spécifiques.

Les mesures utilisées pour permettre au logiciel de contrôler les conditions de panne/erreur spécifiées au Tableau A.2 sont par nature acceptables pour les mesures de contrôle des conditions de panne/erreur spécifiées au Tableau A.1.

La conformité est vérifiée par évaluation du logiciel conformément aux exigences correspondantes de l'Annexe A.

En cas de modification du logiciel, l'évaluation et les essais correspondants sont répétés si la modification a un impact sur les résultats de l'essai concernant les composants programmables de protection.

La conformité du logiciel est vérifiée par examen de l'évaluation des risques et de la partie correspondante du logiciel et/ou en effectuant des essais appropriés des appareillages électroniques de lampes.

La conformité est vérifiée dans le cas d'un composant programmable de protection ou dans le cas de l'exception de 6.2 d).

8 Exigences concernant l'immunité CEM

8.1 Les appareillages électroniques de lampes intégrant un composant programmable de protection pour fonctionner correctement sont soumis à l'essai B de 8.2, sauf si le redémarrage à un certain stade du cycle de fonctionnement suite à une interruption due à un creux de tension d'alimentation ne présente aucun risque. L'essai est réalisé après la dépose de toutes les batteries et des autres composants censés maintenir la tension d'alimentation du composant programmable pendant les creux, les interruptions et les variations de tension d'alimentation principale.

8.2 Les appareillages électroniques de lampes intégrant un composant programmable de protection sont soumis aux essais de détection des phénomènes électromagnétiques. Les essais sont réalisés dans les conditions de fonctionnement valides du composant programmable de protection**,** spécifiées à l'Article 6 de la présente norme, le cas échéant.

Eu égard aux phénomènes électromagnétiques, les essais d'immunité CEM doivent être réalisés conformément à l'IEC 61547.

En outre, les essais suivants doivent être réalisés:

A. Les appareillages électroniques de lampes sont soumis à des signaux transmis sur le réseau conformément à l'IEC 61000-4-13:2002/AMD1:2009, Tableau 11, avec la classe 2 de niveau d'essai utilisant les pas en fréquence conformes au Tableau 10.

B. Les appareillages électroniques de lampes sont alimentés à la tension assignée et utilisés en fonctionnement normal. Au bout d'environ 60 s, la tension d'alimentation est réduite à un niveau tel que les appareillages électroniques de lampes cessent de répondre aux entrées de l'utilisateur ou les parties commandées par le composant programmable cessent de fonctionner, selon ce qui se produit en premier. Cette valeur de tension d'alimentation est enregistrée. Les appareillages électroniques de lampes sont alimentés à la tension assignée et utilisés en fonctionnement normal. La tension est alors réduite à une valeur d'environ 10 % inférieure à la tension enregistrée. Elle est maintenue à cette

valeur pendant environ 60 s, puis augmentée à la tension assignée. La vitesse de diminution et d'augmentation de la tension d'alimentation doit être d'environ 10 V/s. L'appareillage doit rester sûr. L'appareillage doit passer en mode de protection contre les défauts, sauf s'il reprend un fonctionnement normal.

8.3 Pendant et après les essais, les appareillages électroniques de lampes doivent satisfaire aux critères de conformité de l'Article 14 de l'IEC 61347-1 et de la Partie 2 correspondante.

De plus, les appareillages électroniques de lampes ne doivent pas faire l'objet de dysfonctionnements dangereux, et les composants programmables de protection ne doivent faire l'objet d'aucune défaillance si les appareillages électroniques de lampes sont toujours en fonctionnement.

Annexe A
(normative)

Evaluation du logiciel

A.1 Généralités

Les composants programmables de protection exigent des mesures d'intégration de logiciel pour contrôler les conditions de panne/erreur spécifiées au Tableau A.1 ou au Tableau A.2 et doivent être validés selon les exigences de la présente Annexe.

NOTE Les définitions, le Tableau A.1 et le Tableau A.2 reposent sur les définitions et le Tableau H.1 (respectivement pour le logiciel de classe B et de classe C) de l'IEC 60730-1:2010 qui est, pour les besoins de la présente annexe, divisé en deux tableaux: le Tableau A.1 pour les conditions générales de panne/erreur et le Tableau A.2 pour les conditions particulières de panne/erreur.

A.2 Composants programmables de protection utilisant le logiciel

Les composants programmables de protection exigeant des mesures d'intégration de logiciel pour contrôler des conditions de panne/erreur spécifiées au Tableau A.1 ou au Tableau A.2 doivent être construits de manière à ce que le logiciel n'empêche pas de satisfaire aux exigences de la présente norme.

La conformité est vérifiée par les examens et les essais satisfaisant aux exigences de la présente annexe, et par consultation de la documentation, comme cela est exigé dans la présente annexe.

A.3 Termes et définitions

Pour les besoins de la présente annexe, les termes et définitions suivants s'appliquent.

A.3.1
deux voies
structure comportant deux moyens fonctionnels mutuellement indépendants pour exécuter des manœuvres spécifiées

Note 1 à l'article: Pour les dispositifs de commande ayant un mode commun défaut/erreur, une disposition spéciale peut être prise. Il n'est pas exigé que les deux voies soient chacune de nature logarithmique ou logique.

[SOURCE: IEC 60730-1:2010, H.2.16.1]

A.3.2
deux voies (différentes) avec comparaison
structure deux voies comportant deux moyens fonctionnels différents et mutuellement indépendants, chacun capable de fournir une réponse déclarée, et où est effectuée une comparaison des signaux de sortie pour une reconnaissance panne/erreur

[SOURCE: IEC 60730-1:2010, H.2.16.2]

A.3.3
deux voies (homogènes) avec comparaison
structure deux voies comportant deux moyens fonctionnels identiques et mutuellement indépendants, chacun capable de fournir une réponse déclarée, et où est effectuée une comparaison des signaux internes ou des signaux de sortie pour une reconnaissance panne/erreur

[SOURCE: IEC 60730-1:2010, H.2.16.3]

A.3.4
simple voie
structure dans laquelle un seul moyen fonctionnel est utilisé pour exécuter des manœuvres spécifiées

[SOURCE: IEC 60730-1:2010, H.2.16.4]

A.3.5
simple voie avec essai fonctionnel
structure simple voie dans laquelle une donnée d'essai est introduite dans l'unité fonctionnelle avant son fonctionnement

A.3.6
simple voie avec auto-essai périodique
structure simple voie dans laquelle les composants du dispositif de commande sont périodiquement soumis à essai au cours du fonctionnement

A.3.7
simple voie avec auto-essai périodique et contrôle
structure simple voie avec auto-essai périodique dans laquelle des moyens indépendants, capables chacun de fournir une réponse déclarée, contrôlent des aspects tels que les temporisations de sécurité, les séquences et le fonctionnement de logiciels

A.3.8
redondance de bus complète

technique de contrôle de panne/erreur dans laquelle des données et/ou des adresses entièrement redondantes sont fournies par une structure de bus redondante

[SOURCE: IEC 60730-1:2010, H.2.18.1.1]

A.3.9
parité de bus multibit

technique de contrôle de panne/erreur dans laquelle le bus est augmenté de deux bits ou plus, ces bits additionnels étant utilisés pour la détection d'erreurs

[SOURCE: IEC 60730-1:2010, H.2.18.1.2]

A.3.10
sécurité de code
technique de contrôle de panne/erreur dans laquelle la protection contre des erreurs systématiques ou de coïncidence des informations d'entrée ou de sortie est assurée par l'utilisation de la redondance de données et/ou de la redondance de transfert

Note 1 à l'article: Voir aussi A.3.11 et A.3.12

[SOURCE: IEC 60730-1:2010, H.2.18.2]

A.3.11
redondance des données
forme de sécurité de code dans laquelle est utilisé le stockage de données redondantes

[SOURCE: IEC 60730-1:2010, H.2.18.2.1]

A.3.12
redondance de transfert
forme de sécurité de code dans laquelle des données sont transférées au moins deux fois à la suite et ensuite comparées

Note 1 à l'article: Cette technique reconnaît des erreurs intermittentes.

[SOURCE: IEC 60730-1:2010, H.2.18.2.2]

A.3.13
comparateur
dispositif utilisé pour le contrôle de panne/erreur dans les structures deux voies en comparant les données des deux voies et émettant une réponse déclarée si une différence est détectée

[SOURCE: IEC 60730-1:2010, H.2.18.3, modifiée — La note à l'article est intégrée dans la définition.]

A.3.14
essai de classe d'équivalence
essai systématique prévu pour déterminer si le décodage des instructions et leur exécution sont effectués correctement

Note 1 à l'article: Les données d'essai proviennent des spécifications d'instruction des unités centrales (CPU).

Note 2 à l'article: Des instructions similaires sont groupées et l'ensemble de données d'entrée est subdivisé en intervalles de données spécifiques (classes d'équivalence). Chaque instruction dans un groupe traite au moins d'un ensemble de données d'essai, de façon que le groupe entier traite entièrement l'ensemble de données d'essai. Les données d'essai peuvent être formées comme suit:

– données de plage valide;
– données de plage invalide;
– données aux limites;
– valeurs extrêmes et leurs combinaisons.

Note 3 à l'article: Les essais sont effectués dans un groupe avec différents modes d'adressage, de façon que tous les modes d'adressage soient exécutés par le groupe entier.

[SOURCE: IEC 60730-1:2010, H.2.18.5]

A.3.15
moyen de reconnaissance d'erreur
moyen indépendant fourni dans le but de reconnaître les erreurs internes au système

EXEMPLE Il s'agit des dispositifs de surveillance, des comparateurs et des générateurs de code.

[SOURCE: IEC 60730-1:2010, H.2.18.6]

A.3.16
comparaison d'entrée
technique de contrôle de panne/erreur dans laquelle sont comparées les entrées prévues pour être dans les tolérances spécifiées

[SOURCE: IEC 60730-1:2010, H.2.18.8]

A.3.17

détection d'erreurs internes
correction d'erreurs internes
technique de contrôle de panne/erreur dans laquelle sont incorporés des circuits spéciaux pour détecter ou corriger des erreurs

[SOURCE: IEC 60730-1:2010, H.2.18.9]

A.3.18
contrôle de fréquences
technique de contrôle de panne/erreur dans laquelle la fréquence d'horloge est comparée à une fréquence fixée indépendante

EXEMPLE Il s'agit de la comparaison avec la fréquence de la ligne d'alimentation.

[SOURCE: IEC 60730-1:2010, H.2.18.10.1]

A.3.19
contrôle logique de la séquence de programme
technique de contrôle de panne/erreur dans laquelle est surveillée l'exécution logique de la séquence de programme

EXEMPLE Il s'agit des routines de comptage ou des données sélectionnées dans le programme lui-même ou par des dispositifs de surveillance indépendants.

[SOURCE: IEC 60730-1:2010, H.2.18.10.2]

A.3.20
intervalle de temps et contrôle logique
combinaison de A.3.19 et A.3.21

A.3.21
contrôle d'intervalle de temps de la séquence de programme
technique de contrôle de panne/erreur dans laquelle les dispositifs de synchronisation à base de temps indépendante sont régulièrement déclenchés afin de surveiller le fonctionnement et la séquence du programme

EXEMPLE Horloge de surveillance.

[SOURCE: IEC 60730-1:2010, H.2.18.10.4]

A.3.22
sorties parallèles multiples
technique de contrôle de panne/erreur dans laquelle des sorties parallèles indépendantes sont fournies pour la détection d'erreurs opérationnelles ou pour des comparateurs indépendants

[SOURCE: IEC 60730-1:2010, H.2.18.11]

A.3.23
vérification de sortie
technique de contrôle de panne/erreur dans laquelle des sorties sont comparées aux entrées indépendantes

Note 1 à l'article: Cette technique peut ou peut ne pas lier une erreur à la sortie déficiente.

[SOURCE: IEC 60730-1:2010, H.2.18.12]

A.3.24
contrôle de vraisemblance
technique de contrôle de panne/erreur dans laquelle l'exécution d'un programme, des entrées ou des sorties sont contrôlées pour déceler des temporisations, des données ou des séquences de programme inadmissibles

EXEMPLE Introduction d'une interruption additionnelle après accomplissement d'un certain nombre de cycles ou contrôle de division par zéro.

[SOURCE: IEC 60730-1:2010, H.2.18.13]

A.3.25
essai de protocole

technique de contrôle de panne/erreur dans laquelle des données sont transférées de et vers des composants de calculateur pour détecter des erreurs dans le protocole de communication interne

[SOURCE: IEC 60730-1:2010, H.2.18.14]

A.3.26
comparaison réciproque

technique de contrôle de panne/erreur utilisée avec des structures deux voies (homogènes) dans lesquelles est effectuée une comparaison de données échangées réciproquement entre deux unités de traitement

Note 1 à l'article: Réciproquement se réfère à un échange de données similaires.

[SOURCE: IEC 60730-1:2010, H.2.18.15]

A.3.27
contrôle redondant

disponibilité de deux ou plusieurs moyens indépendants, tels que des dispositifs d'horloge de surveillance et comparateurs, pour effectuer la même tâche

[SOURCE: IEC 60730-1:2010, H.2.18.17]

A.3.28
transmission ordonnancée

procédure de communication dans laquelle l'envoi de l'information d'un transmetteur particulier peut être effectué vers un point prédéfini en temps et séquence, sinon le récepteur le traite comme une erreur de communication

[SOURCE: IEC 60730-1:2010, H.2.18.18]

A.3.29
essai de contrôle

mise à disposition de moyens indépendants tels que des dispositifs d'horloge de surveillance et comparateurs qui sont soumis à essai au départ ou périodiquement pendant le fonctionnement

[SOURCE: IEC 60730-1:2010, H.2.18.21]

A.3.30
gabarit d'essai

technique de contrôle de panne/erreur utilisée pour l'essai périodique des dispositifs d'entrée, de sortie et des interfaces du dispositif de commande

Note 1 à l'article: Un gabarit d'essai est introduit dans le dispositif et les résultats sont comparés aux valeurs espérées. Pour l'introduction du gabarit d'essai et l'évaluation des résultats, des moyens indépendants sont utilisés. Le gabarit d'essai est construit de façon à ne pas influencer le fonctionnement correct du dispositif de commande.

[SOURCE: IEC 60730-1:2010, H.2.18.22]

A.3.31
essai d'Abraham

forme spécifique de gabarit d'essai de mémoire variable dans lequel tout défaut "collé à" et de couplage entre cellules de mémoire est identifié

Note 1 à l'article: Le nombre d'opérations nécessaires pour effectuer l'essai de la mémoire entière est d'environ 30 n, où n est le nombre de cellules de la mémoire. L'essai peut être transparent à l'utilisation pendant les cycles de fonctionnement, par partition de la mémoire et essai de chaque partition en différents segments de temps.

Note 2 à l'article: Voir Abraham, J.A.; Thatte, S.M.; "Fault coverage of test programs for a microprocessor", Proceedings of the IEEE Test Conference 1979, pp 18-22.

[SOURCE: IEC 60730-1:2010, H.2.19.1]

A.3.32
essai GALPAT transparent
essai GALPAT de mémoire dans lequel un mot de signature est d'abord formé pour représenter le contenu de la plage de mémoire à soumettre à essai et ce mot est sauvegardé

Note 1 à l'article: La cellule à soumettre à essai est complémentée et l'essai est effectué comme ci-dessus. Cependant, le reste des cellules n'est pas examiné individuellement, mais en formant et comparant un second mot de signature. Un deuxième essai est ensuite effectué comme ci-dessus par complémentation de la valeur de la cellule à soumettre à essai précédemment complémentée.

Note 2 à l'article: Cette technique reconnaît toutes les erreurs de bit statique aussi bien que les erreurs d'interface entre cellules de mémoire.

[SOURCE: IEC 60730-1:2010, H.2.19.2.1]

A.3.33
somme de contrôle modifiée
technique de contrôle de panne/erreur dans laquelle un unique mot représentant le contenu de tous les mots en mémoire est généré et sauvegardé

Note 1 à l'article: Pendant l'auto-essai, une somme de contrôle est formée avec le même algorithme et comparée avec la somme de contrôle sauvegardée.

Note 2 à l'article: Cette technique reconnaît toutes les erreurs de bit impair et quelques erreurs de bit pair.

[SOURCE: IEC 60730-1:2010, H.2.19.3.1]

A.3.34
somme de contrôle multiple
technique de contrôle de panne/erreur dans laquelle des mots séparés représentant le contenu de zones mémoire soumises à essai sont générés et sauvegardés

Note 1 à l'article: Pendant l'auto-essai, le même algorithme est utilisé pour générer une somme de contrôle qui est comparée avec la somme de contrôle sauvegardée pour cette zone.

Note 2 à l'article: Cette technique reconnaît toutes les erreurs de bit impair et quelques erreurs de bit pair.

[SOURCE: IEC 60730-1:2010, H.2.19.3.2]

A.3.35
mot unique de CRC
technique de contrôle de panne/erreur dans laquelle un unique mot est généré pour représenter le contenu de la mémoire

Note 1 à l'article: Pendant l'auto-essai, le même algorithme est utilisé pour générer un autre mot qui est comparé avec le mot sauvegardé.

Note 2 à l'article: Cette technique reconnaît toutes les erreurs de un bit et un pourcentage élevé d'erreurs multibit.

[SOURCE: IEC 60730-1:2010, H.2.19.4.1]

A.3.36
mot double de CRC
technique de contrôle de panne/erreur dans laquelle au moins deux mots sont générés pour représenter le contenu de la mémoire

Note 1 à l'article: Pendant l'auto-essai, le même algorithme est utilisé pour générer le même nombre de mots de signature qui sont comparés avec les mots sauvegardés.

Note 2 à l'article: Cette technique peut reconnaître toutes les erreurs de un bit et un nombre élevé d'erreurs multibit avec une précision plus grande qu'avec un mot unique de CRC.

[SOURCE: IEC 60730-1:2010, H.2.19.4.2]

A.3.37
mémoire redondante avec comparaison
structure dans laquelle le contenu de la mémoire relatif à la sécurité est stocké deux fois dans des formats différents dans des zones séparées de façon à pouvoir être comparé pour contrôle d'erreur

[SOURCE: IEC 60730-1:2010, H.2.19.5]

A.3.38
essai de mémoire statique
technique de contrôle de panne/erreur visant à ne détecter que les erreurs statiques

[SOURCE: IEC 60730-1:2010, H.2.19.6]

A.3.39
essai "walkpat" des mémoires
technique de contrôle de panne/erreur dans laquelle un gabarit de données modèle est écrit dans la zone mémoire en essai comme en fonctionnement normal

Note 1 à l'article: Le complément d'un bit est effectué dans la première cellule et le reste de la zone mémoire est examiné. Puis la première cellule est à nouveau complémentée et la mémoire examinée. Ce processus est répété dans toutes les cellules de la mémoire à l'essai. Un deuxième essai est effectué par complément d'un bit de toutes les cellules en mémoire à l'essai et en procédant comme ci-dessus.

Note 2 à l'article: Cette technique reconnaît toutes les erreurs de bit statique aussi bien que les erreurs d'interface entre cellules de mémoire.

[SOURCE: IEC 60730-1:2010, H.2.19.7]

A.3.40
protection de mot avec redondance multibit
technique de contrôle de panne/erreur dans laquelle des bits redondants sont générés et sauvegardés pour chacun des mots de la zone mémoire en essai A la lecture de chacun des mots est effectué un contrôle de parité

EXEMPLE Un code "Hamming" qui reconnaît aussi bien toutes les erreurs de un ou deux bits et certaines des erreurs de trois bits ou multibit.

[SOURCE: IEC 60730-1:2010, H.2.19.8.1, modifiée — La note à l'article est intégrée à la définition.]

A.3.41
protection de mot avec redondance d'un seul bit
technique de contrôle de panne/erreur dans laquelle un seul bit est ajouté à chacun des mots de la zone mémoire en essai puis sauvegardé, créant ainsi une parité paire ou impaire; à la lecture de chacun des mots est effectué un contrôle de parité

Note 1 à l'article: Cette technique reconnaît toutes les erreurs de bit impair.

[SOURCE: IEC 60730-1:2010, H.2.19.8.2, modifiée — La note à l'article est intégrée à la définition.]

A.3.42
parité de bus à un seul bit
technique de contrôle de panne/erreur dans laquelle le bus est augmenté de un bit, ce bit supplémentaire étant utilisé pour la détection d'erreurs

[SOURCE: IEC 60730-1:2010, H.2.18.1.3]

A.3.43
essai de mémoire damier
essai de mémoire statique dans lequel un gabarit en damier de zéros et de uns est écrit dans la zone mémoire en essai et où les cellules sont examinées par paires

Note 1 à l'article: L'adresse de la première cellule de chaque paire est variable et l'adresse de la deuxième cellule dérive de la première adresse par complément d'un bit. Dans le premier examen, l'adresse est d'abord incrémentée jusqu'à la fin de l'espace d'adresse de la mémoire puis ramenée à sa valeur d'origine. L'essai est répété avec le gabarit en damier inverse.

[SOURCE: IEC 60730-1:2010, H.2.19.6.1]

A.3.44
essai de mémoire active
essai de mémoire statique dans lequel une donnée est écrite dans la zone mémoire en essai comme en fonctionnement normal

Note 1 à l'article: Chaque cellule est ensuite examinée dans l'ordre ascendant et le complément d'un bit est effectué dans le contenu. L'examen et le complément d'un bit sont ensuite répétés dans l'ordre descendant. Puis ce processus est répété après avoir d'abord effectué le complément d'un bit dans toutes les cellules de mémoire en essai.

[SOURCE: IEC 60730-1:2010, H.2.19.6.2]

A.3.45
modèle de défaut collé à
modèle de défaut représentant un circuit ouvert ou un niveau de signal invariant

Note 1 à l'article: On s'y réfère habituellement par "collé ouvert", "collé à 1" ou "collé à 0".

A.3.46
modèle de défaut convertisseur numérique (défaut DC)
modèle de défaut "collé à" incorporant des courts-circuits entre les lignes de signaux

Note 1 à l'article: A cause du nombre de courts-circuits possibles dans le dispositif en essai, ne sont habituellement considérés que les courts-circuits entre lignes de signaux connexes. Un niveau de signal logique est défini et persiste si les lignes tentent de passer au niveau inverse.

A.3.47
diversité logicielle
technique de contrôle de panne/erreur dans laquelle toutes les parties du logiciel sont intégrées deux fois dans la forme ou dans un autre code logiciel

Note 1 à l'article: Par exemple, d'autres formes de code logiciel peuvent être générées par différents programmeurs, langages ou schémas de compilation, et peuvent résider dans différents canaux matériels ou différentes zones de la mémoire dans une simple voie.

A.4 Exigences d'architecture

A.4.1 Généralités

A.4.1.1 Les **composants programmables** exigeant des mesures d'intégration de logiciel pour contrôler les conditions de panne/erreur spécifiées au Tableau A.1 ou au Tableau A.2 doivent utiliser des mesures de contrôle (A.4.2) et éviter (Article A.5) les pannes/erreurs liées au logiciel dans les données et segments liés à la sécurité du logiciel.

NOTE 1 Par conséquent, le système est conçu de manière à éviter les erreurs systématiques, et les défauts aléatoires sont traités en configurant correctement le système.

NOTE 2 La conception logicielle et matérielle repose sur l'analyse fonctionnelle (lire: opérationnelle) de l'application, donnant lieu à une conception structurée intégrant explicitement le flux de contrôle, le flux de données et les fonctions liées au temps exigées par l'application. Cela donne lieu à une configuration système sûre par nature ou dont les composants dotés de fonctions directes critiques pour la sécurité (ex.: microprocesseurs avec circuits associés, par exemple) sont protégés conformément à la présente annexe. Ces dispositifs de protection sont intégrés dans le matériel (horloge de surveillance, surveillance de la tension d'alimentation, par exemple) et peuvent être complétés par un logiciel (essai ROM, essai RAM, etc.). Il est important que ces dispositifs de protection puissent provoquer un arrêt de sécurité totalement indépendant.

Si le contrôle d'intervalle de temps est utilisé, il est sensible à une limite inférieure et supérieure de l'intervalle de temps. Il convient de tenir compte des défauts à l'origine d'un décalage de la limite supérieure et/ou inférieure. Dans le cas d'une fonction de commande de classe A.2, si un dispositif de protection principal peut être rendu inopérant par un seul défaut, un dispositif de protection auxiliaire doit être prévu.

NOTE 3 Les temps de réaction de ces dispositifs de protection sont inférieurs ou égaux au temps de tolérance de défaut pertinent.

La conformité est vérifiée par les examens et essais de A.4.2 à A.4.3 inclus.

A.4.1.2 Les **composants programmables** exigeant des mesures d'intégration de logiciel pour contrôler des conditions de panne/erreur spécifiées au Tableau A.2 doivent présenter l'une des structures suivantes:

- simple voie avec auto-essai périodique et contrôle (A.3.7);
- deux voies (homogènes) avec comparaison (A.3.3);
- deux voies (différentes) avec comparaison (A.3.2).

NOTE Les structures à deux voies peuvent être comparées:

- à l'aide d'un comparateur (A.3.13), ou
- par comparaison réciproque (A.3.26).

A.4.1.3 Les **composants programmables** exigeant des mesures d'intégration de logiciel pour contrôler des conditions de panne/erreur spécifiées au Tableau A.1 doivent présenter l'une des structures suivantes:

- simple voie avec essai fonctionnel (A.3.5);
- simple voie avec auto-essai périodique (A.3.6);
- deux voies sans comparaison (A.3.1).

Les structures logicielles intégrant des mesures de contrôle des conditions de panne/erreur spécifiées au Tableau A.2 sont également acceptables pour les **circuits électroniques programmables** dotés de fonctions exigeant des mesures logicielles de contrôle des conditions de panne/erreur spécifiées au Tableau A.1.

La conformité est vérifiée par les examens et essais de l'architecture logicielle de A.5.2.2.

A.4.2 Mesures de contrôle des pannes/erreurs

A.4.2.1 Lorsque la mémoire redondante avec comparaison est fournie sur deux zones du même composant, les données d'une zone doivent être enregistrées dans un format différent de celui de l'autre zone (voir "diversité logicielle", A.3.47).

La conformité est vérifiée par examen du code source.

A.4.2.2 Les composants programmables dotés de fonctions exigeant des mesures d'intégration de logiciel pour contrôler des conditions de panne/erreur spécifiées au Tableau A.2 et qui utilisent des structures à deux voies avec comparaison doivent être dotés de moyens supplémentaires de détection de panne/erreur (essais fonctionnels périodiques, auto-essais périodiques ou surveillance indépendante) pour les pannes/erreurs non détectées par la comparaison.

La conformité est vérifiée par examen du code source.

A.4.2.3 Pour les composants programmables dotés de fonctions exigeant des mesures d'intégration de logiciel pour contrôler les conditions de panne/erreur spécifiées au Tableau A.1 ou au Tableau A.2, des moyens doivent être prévus pour reconnaître et contrôler les erreurs de transmission pour l'acheminement des données liées à la sécurité. Ces moyens doivent tenir compte des erreurs de données, d'adressage, de synchronisation de transmission et de séquence de protocole.

La conformité est vérifiée par examen du code source.

A.4.2.4 Pour les composants programmables dotés de fonctions exigeant des mesures de contrôle des conditions de panne/erreur spécifiées au Tableau A.1 ou au Tableau A.2, les composants programmables doivent intégrer des mesures d'adressage des pannes/erreurs dans les segments et données liés à la sécurité indiqués au Tableau A.1 ou au Tableau A.2, selon le cas.

La conformité est vérifiée par examen du code source.

Dans le cas d'un essai réalisé par une tierce partie, il est conseillé d'examiner le code source dans les locaux du constructeur. Les agences tierces ne doivent pas détenir les fichiers du code source réel tant qu'elles ont documenté les identifiants uniques du code source examiné à l'origine.

Tableau A.1 – Conditions générales de panne/erreur

Composant [a]	Panne/erreur	Mesures acceptables [b c]	Définitions
1 CPU – Unité centrale			
1.1 Registres	Collé à	Essai fonctionnel, ou Essai périodique utilisant: – essai de mémoire statique, ou – protection de mot avec redondance d'un seul bit	A.3.5 A.3.6 A.3.38 A.3.41
1.2 Décodage et exécution d'instruction	N/A		
1.3 Compteur de programme	Collé à	Essai fonctionnel, ou Auto-essai périodique, ou Contrôle d'intervalle de temps indépendant, ou	A.3.5 A.3.6 A.3.21

Composant [a]	Panne/erreur	Mesures acceptables [b c]	Définitions
		Contrôle logique de la séquence de programme	A.3.19
1.4 Adressage	N/A		
1.5 Décodage d'instruction de chemin de données	N/A		
2 Traitement et exécution d'interruption	Aucune interruption ou interruption trop fréquente	Essai fonctionnel, ou Contrôle d'intervalle de temps	A.3.5 A.3.21
3 Horloge	Fréquence incorrecte (pour l'horloge synchronisée: harmoniques/ sous-harmoniques uniquement)	Contrôle de fréquence, ou Contrôle d'intervalle de temps	A.3.18 A.3.21
4 Mémoire			
4.1 Mémoire invariable (/non volatile)	Tous les défauts de un bit	Somme de contrôle modifiée périodique, ou Somme de contrôle multiple, ou Protection de mot avec redondance d'un seul bit	A.3.33 A.3.34 A.3.41
4.2 Mémoire variable (/volatile)	Défaut DC	Essai de mémoire statique périodique, ou Protection de mot avec redondance d'un seul bit	A.3.38 A.3.41
4.3 Adressage (concerne la mémoire variable et invariable)	Collé à	Protection de mot avec redondance d'un seul bit, y compris l'adresse	A.3.41
5 Chemin de données interne			
5.1 Données	Collé à	Protection de mot avec redondance d'un seul bit	A.3.41
5.2 Adressage	Fréquence incorrecte	Protection de mot avec redondance d'un seul bit, y compris l'adresse	A.3.41
6 Communication externe			
6.1 Données	Toutes les erreurs de bit simple et double (distance de Hamming 3)	Protection de mot avec redondance multibit, ou mot unique de CRC, ou Redondance de transfert, ou Essai de protocole	A.3.40 A.3.35 A.3.12 A.3.25
6.2 Adressage	Fréquence incorrecte	Protection de mot avec redondance multibit, y compris l'adresse, ou	A.3.40

Composant [a]	Panne/erreur	Mesures acceptables [b c]	Définitions
		Mot simple de CRC, y compris les adresses; ou	A.3.35
		Redondance de transfert, ou	A.3.12
		Essai de protocole	A.3.25
6.3 Synchronisation	Point dans le temps erroné	Contrôle d'intervalle de temps, ou	A.3.21
		Transmission ordonnancée	A.3.28
	Séquence erronée	Contrôle logique, ou	A.3.19
		Contrôle d'intervalle de temps, ou	A.3.21
		Transmission ordonnancée	A.3.28
7 Périphérie d'entrée/sortie			
7.1 E/S numérique	Collé à	Contrôle de vraisemblance pour les conditions applicables, voir 6.1/6.2	A.3.24
7.2 E/S analogique			
7.2.1 Convertisseur A/N et N/A	Collé à	Contrôle de vraisemblance pour les conditions applicables, voir 6.1 / 6.2	A.3.24
7.2.2 Multiplexeur analogique	Adressage incorrect	Contrôle de vraisemblance	A.3.24
8 Dispositifs de surveillance et comparateurs	N/A		
9 Puces personnalisées [d] ASIC, G AL, réseau de portes, par exemple	Toutes les sorties hors de la spécification fonctionnelle statique et dynamique	Auto-essai périodique	A.3.6

Le Tableau A.1 est appliqué conformément aux exigences de l'Article A.2 à A.4.2.9 inclus.

Un modèle de défaut "collé à" correspond à un modèle de défaut représentant un circuit ouvert ou un niveau de signal invariant. Un modèle de défaut DC correspond à un modèle de défaut "collé à" incorporant des courts-circuits entre les lignes de signaux. N/A signifie une panne/erreur supposée non applicable

[a] Pour l'évaluation de la panne/erreur, certains composants sont divisés en sous-fonctions.

[b] Pour chaque sous-fonction du tableau, la mesure du Tableau A.2 couvre la panne/erreur du logiciel.

[c] Si plusieurs mesures sont données pour une sous-fonction, il s'agit d'alternatives.

[d] (Non couvert par 1-8) A diviser en sous-fonctions par le constructeur, le cas échéant.

Tableau A.2 – Conditions spécifiques de panne/erreur

Composant [a]	Panne/erreur	Mesures acceptables [b c]	Définitions
1 CPU – Unité centrale			
1.1 Registres	Défaut DC	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Détection d'erreurs internes, ou Mémoire redondante avec comparaison, ou Auto-essais périodiques utilisant: – essai "walkpat" des mémoires – essai d'Abraham – essai GALPAT transparent; ou Protection de mot avec redondance multibit, ou Essai de mémoire statique et protection de mot avec redondance de bit simple	 A.3.26 A.3.13 A.3.17 A.3.37 A.3.39 A.3.31 A.3.32 A.3.40 A.3.38 A.3.41
1.2 Décodage et exécution d'instruction	Décodage et exécution incorrects	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Détection d'erreurs internes, ou Auto-essai périodique utilisant l'essai de classe d'équivalence	 A.3.26 A.3.13 A.3.17 A.3.14
1.3 Compteur de programme	Défaut DC	Auto-essai et surveillance périodiques utilisant: – intervalle de temps et contrôle logique indépendants – détection d'erreurs internes, ou Comparaison de canaux fonctionnels redondants par: – comparaison réciproque – comparateur de matériel indépendant	A.3.7 A.3.20 A.3.17 A.3.26 A.3.13
1.4 Adressage	Défaut DC	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Détection d'erreurs internes; ou Auto-essai périodique utilisant un gabarit d'essai des lignes d'adresses, ou Redondance de bus complète, ou Parité de bus multibit utilisant l'adresse	 A.3.26 A.3.13 A.3.17 A.3.7 A.3.30 A.3.8 A.3.9
1.5 Décodage d'instruction de chemins de données	Défaut DC et exécution	Comparaison des CPU redondantes par: – comparaison réciproque, ou – comparateur de matériel indépendant, ou Détection d'erreurs internes, ou Auto-essai périodique utilisant un gabarit d'essai, ou Redondance de données, ou Parité de bus multibit	 A.3.26 A.3.13 A.3.17 A.3.7 A.3.11 A.3.9

Composant [a]	Panne/erreur	Mesures acceptables [b c]	Définitions
2 Traitement et exécution d'interruption	Pas d'interruption ou interruption trop fréquente liée à différentes sources	Comparaison de canaux fonctionnels redondants par: – comparaison réciproque, – comparateur de matériel indépendant, ou Intervalle de temps et contrôle logique indépendants	 A.3.26 A.3.13 A.3.20
3 Horloge	Fréquence incorrecte (pour l'horloge synchronisée: harmoniques/ sous-harmoniques uniquement)	Contrôle de fréquence, ou Contrôle d'intervalle de temps, ou Comparaison de canaux fonctionnels redondants par: – comparaison réciproque – comparateur de matériel indépendant	A.3.18 A.3.21 A.3.26 A.3.13
4. Mémoire			
4.1 Mémoire invariable (/non volatile)	Couverture à 99,6 % de toutes les erreurs d'information	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Mémoire redondante avec comparaison, ou Contrôle de redondance cyclique périodique, soit – mot simple – mot double, ou Protection de mot avec redondance multibit	 A.3.26 A.3.13 A.3.37 A.3.35 A.3.36 A.3.40
4.2 Mémoire variable (/volatile)	Défaut DC et liaisons croisées dynamiques	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Mémoire redondante avec comparaison, ou Auto-essais périodiques utilisant: – essai "walkpat" des mémoires – essai d'Abraham – essai GALPAT transparent, ou Protection de mot avec redondance multibit	 A.3.26 A.3.13 A.3.37 A.3.39 A.3.31 A.3.32 A.3.40
4.3 Adressage (concerne la mémoire variable/volatile et invariable/non volatile)	Défaut DC	Comparaison des CPU redondantes par: – comparaison réciproque, ou – comparateur de matériel indépendant, ou Gabarit d'essai de redondance de bus complète, ou Contrôle de redondance cyclique périodique, soit: – mot simple – mot double, ou Protection de mot avec redondance multibit, y compris l'adresse	 A.3.26 A.3.13 A.3.8 A.3.35 A.3.36 A.3.40
5 Chemin de données interne			

Composant [a]	Panne/erreur	Mesures acceptables [b c]	Définitions
5.1 Données	Défaut DC	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Protection de mot avec redondance multibit, y compris l'adresse, ou Redondance de données, ou Gabarit d'essai, ou Essai de protocole	 A.3.26 A.3.13 A.3.40 A.3.11 A.3.30 A.3.25
5.2 Adressage	Adresse incorrecte et adressage multiple	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Protection de mot avec redondance multibit, y compris l'adresse, ou Redondance de bus complète, ou Gabarit d'essai, y compris l'adresse	 A.3.26 A.3.13 A.3.40 A.3.8 A.3.30
6 Communication externe			
6.1 Données	Toutes les erreurs de bit simple, de bit double et triple (distance de Hamming 4)	Mot double de CRC, ou Redondance de données, ou Comparaison de canaux fonctionnels redondants par: – comparaison réciproque – comparateur de matériel indépendant	A.3.36 A.3.11 A.3.26 A.3.13
6.2 Adressage	Adressage incorrect et multiple	Mot double de CRC, y compris l'adresse, ou Redondance de bus complète des données et d'adresse, ou Comparaison de canaux de communication redondants par: – comparaison réciproque – comparateur de matériel indépendant	A.3.36 A.3.8 A.3.26 A.3.13
6.3 Synchronisation	Point dans le temps erroné	Intervalle de temps et contrôle logique, ou Comparaison de canaux de communication redondants par: – comparaison réciproque – comparateur de matériel indépendant	A.3.20 A.3.26 A.3.13
	Séquence erronée	(options identiques à celles du point dans le temps erroné)	

Composant [a]	Panne/erreur	Mesures acceptables [b c]	Définitions
7 Périphérie d'entrée/sortie			
7.1 E/S numérique	Défaut DC	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Comparaison d'entrée, ou Plusieurs sorties parallèles, ou Vérification de sortie, ou Gabarit d'essai, ou Sécurité de code pour les conditions applicables, voir 6.1/6.2	 A.3.26 A.3.13 A.3.16 A.3.22 A.3.23 A.3.30 A.3.10
7.2 E/S analogique			
7.2.1 Convertisseur A/N et N/A	Défaut DC	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Comparaison d'entrée, ou Plusieurs sorties parallèles, ou Vérification de sortie, ou Gabarit d'essai pour les conditions applicables, voir 6.1/6.2	 A.3.26 A.3.13 A.3.16 A.3.22 A.3.23 A.3.30
7.2.2 Multiplexeur analogique	Adressage incorrect	Comparaison des CPU redondantes par: – comparaison réciproque – comparateur de matériel indépendant, ou Comparaison d'entrée, ou Gabarit d'essai	 A.3.26 A.3.13 A.3.16 A.3.30
8 Dispositifs de surveillance et comparateurs	Toutes les sorties hors de la spécification fonctionnelle statique et dynamique	Surveillance soumise à essai, ou Surveillance et comparaison redondantes ou Moyen de reconnaissance d'erreurs	A.3.29 A.3.27 A.3.15
9 Puces personnalisées [d] ASIC, G AL, réseau de portes, par exemple	Toutes les sorties hors de la spécification fonctionnelle statique et dynamique	Auto-essai et surveillance périodiques, ou Deux voies (différentes) avec comparaison ou Moyen de reconnaissance d'erreurs	A.3.7 A.3.2 A.3.15
Le Tableau A.2 est appliqué conformément aux exigences de l'Article A.2 à A.4.2.9 inclus. Un modèle de défaut DC correspond à un modèle de défaut "collé à" incorporant des courts-circuits entre les lignes de signaux.			
[a] Pour l'évaluation de la panne/erreur, certains composants sont divisés en sous-fonctions. [b] Pour chaque sous-fonction du tableau, la mesure du logiciel couvre la panne/erreur du Tableau A.1. [c] Si plusieurs mesures sont données pour une sous-fonction, il s'agit d'alternatives. [d] (Non couvert par 1-8) A diviser en sous-fonctions par le constructeur, le cas échéant.			

A.4.2.5 Pour les composants programmables exigeant des mesures d'intégration de logiciel pour contrôler les conditions de panne/erreur spécifiées au Tableau A.1 ou au

Tableau A.2, la détection de la panne/erreur doit avoir lieu avant que la conformité à l'Article 6 de la présente norme ne soit compromise.

La conformité est vérifiée par examen et essai du code source.

La perte de la fonctionnalité deux voies est censée être une erreur dans un composant programmable utilisant une structure deux voies permettant au logiciel de contrôler les conditions de panne/erreur spécifiées au Tableau A.2.

A.4.2.6 Le logiciel doit être référencé auprès des parties correspondantes de la séquence de fonctionnement et des fonctions matérielles associées.

La conformité est vérifiée par examen du code source.

A.4.2.7 Lorsque des étiquettes sont utilisées pour les emplacements de mémoire, elles doivent être uniques.

La conformité est vérifiée par essai du code source.

A.4.2.8 Le logiciel doit être protégé contre toute modification par l'utilisateur des segments et données liés à la sécurité.

La conformité est vérifiée par essai du code source.

A.4.2.9 Le logiciel, et le matériel lié à la sécurité qu'il contrôle, doivent être initialisés et s'arrêter avant que la conformité au présent Article 6 ne soit compromise.

La conformité est vérifiée par examen et essai du code source.

A.5 Mesures pour éviter les erreurs

A.5.1 Généralités

Pour les composants programmables de protection dotés de fonctions exigeant que le logiciel intègre des mesures de contrôle des conditions de panne/erreur spécifiées au Tableau A.1 et au Tableau A.2, les mesures suivantes visant à éviter les défauts systématiques dans le logiciel doivent être appliquées.

Un logiciel intégrant les mesures utilisées pour contrôler les conditions de panne/erreur spécifiées au Tableau A.2 est par nature acceptable pour le logiciel permettant de contrôler les conditions de panne/erreur spécifiées au Tableau A.1.

NOTE Les termes dans le Tableau A.3 au Tableau A.7 sont basés sur l'IEC 61508-7. Ils sont donnés à titre d'information pour les besoins de la présente norme et ne sont pas expliqués ici.

A.5.2 Spécification

A.5.2.1 Exigences relatives à la sécurité du logiciel

La spécification des exigences relatives à la sécurité du logiciel doit inclure:

- une description de chaque fonction liée à la sécurité à mettre en œuvre, y compris son/ses temps de réponse:
  - les fonctions liées à l'application, y compris leurs défauts logiciels connexes qui doivent être contrôlés;
  - les fonctions relatives à la détection, à l'annonce et à la gestion des défauts logiciels et matériels;
- une description des interfaces entre le logiciel et le matériel;

- une description des interfaces entre les fonctions liées à la sécurité et les autres fonctions;
- une description du compilateur utilisé pour générer le code d'objet à partir du code source, y compris les détails des réglages du commutateur du compilateur (les options de fonction de bibliothèque, le modèle de mémoire, l'optimisation, les détails de la mémoire SRAM, la fréquence d'horloge et les détails de la puce, par exemple);

  Il convient de choisir avec précaution le compilateur et qu'il soit robuste et doté d'un enregistrement sur piste éprouvé.

- une description d'un éditeur de liens utilisé pour lier le code d'objet aux routines de bibliothèque exécutables.

La conformité est vérifiée par examen de la documentation et comme indiqué en A.5.2.2.2.

NOTE Des exemples de certaines techniques/mesures visant à satisfaire à ces exigences peuvent être consultés au Tableau A.3.

Tableau A.3 – Méthodes semi-formelles

Technique/Mesure	Références informatives
Méthodes semi-formelles	
Schémas de principe logiques/fonctionnels	
Schémas de séquence	
Diagrammes d'états finis/schémas des transitions d'états	– IEC 61508-7:2010, B.2.3.2
Tables de décision/vérité	– IEC 61508-7:2010, C.6.1

A.5.2.2 Architecture du logiciel

A.5.2.2.1 La spécification de l'architecture logicielle doit inclure les aspects suivants:

- techniques et mesures de contrôle des pannes/erreurs (voir A.4.2);
- interactions entre le matériel et le logiciel;
- partitionnement en modules et leur allocation aux fonctions de sécurité spécifiées;
- hiérarchie et structure d'appel des modules (flux de commande);
- gestion des interruptions;
- flux de données et restrictions d'accès aux données;
- architecture et stockage des données;
- dépendances basées sur le temps des séquences de données.

La conformité est vérifiée par examen de la documentation et comme indiqué en A.5.2.2.2.

NOTE Des exemples de certaines techniques/mesures visant à satisfaire à ces exigences peuvent être consultés au Tableau A.4.

Tableau A.4 – Spécification de l'architecture logicielle

Technique/Mesure	Références informatives
Détection des défauts et diagnostic	– IEC 61508-7:2010, C.3.1
Méthodes semi-formelles:	
– Schémas de principe logiques/fonctionnels	
– Schémas de séquence	
– Diagrammes d'états finis/schémas des transitions d'états	– IEC 61508-7:2010, B.2.3.2
– Schémas de flux de données	– IEC 61508-7:2010, C.2.2

A.5.2.2.2 La spécification de l'architecture doit être validée en fonction des exigences de sécurité logicielle de la spécification par analyse statique.

NOTE Exemples de méthode d'analyse statique:

- analyse du flux de commande (IEC 61508-7:2010, C.5.9);
- analyse du flux de données (IEC 61508-7:2010, C.5.10);
- lectures croisées/revues de conception. (IEC 61508-7, C.5.16).

A.5.2.3 Conception et codage de module

A.5.2.3.1 Selon l'architecture, le logiciel doit être séparé opportunément en modules. La conception et le codage du module logiciel doivent être mis en œuvre de manière à être reliés à l'architecture logicielle et aux exigences afférentes.

La conformité est vérifiée selon A.5.2.3.3 et par examen de la documentation.

L'utilisation d'outils de conception assistée par ordinateur est acceptée.

La programmation défensive (IEC 61508-7:2010, C.2.5) est recommandée (contrôles par fourchette, contrôle de division par 0, contrôles de vraisemblance).

Il convient que la conception du module spécifie:

- la/les fonction(s),
- les interfaces avec les autres modules,
- les données.

NOTE Des exemples de certaines techniques/mesures visant à satisfaire à ces exigences peuvent être consultés au Tableau A.5.

Tableau A.5 – Spécification de la conception du module

Technique/Mesure	Références informatives
Taille limitée des modules logiciels	IEC 61508-7:2010, C.2.9
Masquage/encapsulation des informations	IEC 61508-7:2010, C.2.8
Un point d'entrée/un point de sortie dans les sous-programmes et les fonctions	IEC 61508-7:2010, C.2.9
Interface totalement définie	IEC 61508-7:2010, C.2.9
Méthodes semi-formelles:	
Schémas de principe logiques/fonctionnels	
– Schémas de séquence	
– Diagrammes d'états finis/schémas des transitions d'états	IEC 61508-7:2010, B.2.3.2
– Schémas de flux de données	IEC 61508-7:2010, C.2.2

A.5.2.3.2 Le code logiciel doit être structuré.

La conformité est vérifiée selon A.5.2.3.3 et par examen de la documentation.

NOTE 1 La complexité structurelle peut être limitée en appliquant les principes suivants:

- limiter le nombre de chemins possibles passant par un module logiciel et simplifier au maximum la relation entre les paramètres d'entrée et de sortie;
- éviter les branchements compliqués et, en particulier, les sauts inconditionnels (GOTO) en langage de haut niveau;
- dans la mesure du possible, associer les contraintes de boucle et le branchement aux paramètres d'entrée;
- éviter les calculs complexes, comme la base du branchement et des décisions de boucle.

NOTE 2 Des exemples de certaines techniques/mesures visant à satisfaire à ces exigences peuvent être consultés au Tableau A.6.

Tableau A.6 – Normes de conception et de codage

Technique/Mesure	Références informatives
Utilisation de normes de codage [a]	IEC 61508-7:2010, C.2.6.2
Pas d'utilisation d'objets et de variables dynamiques [a]	IEC 61508-7:2010, C.2.6.3
Utilisation limitée des interruptions	IEC 61508-7:2010, C.2.6.5
Utilisation limitée des pointeurs	IEC 61508-7:2010, C.2.6.6
Utilisation limitée de la récursion	IEC 61508-7:2010, C.2.6.7
Pas de branchements inconditionnels dans les programmes en langages de haut niveau	IEC 61508-7:2010, C.2.6.2
[a] Les objets et/ou variables dynamiques sont admis si un compilateur qui assure qu'un espace mémoire suffisant est affecté avant exécution à tous les objets et variables dynamiques, ou qui introduit des contrôles d'allocation correcte de mémoire en ligne au moment de l'exécution.	

A.5.2.3.3 *Le logiciel codé doit être validé en fonction de la spécification de module par analyse statique. La spécification de module doit être validée en fonction de la spécification d'architecture par analyse statique.*

A.5.3 Validation logicielle

Le logiciel doit être validé conformément à la spécification des exigences de sécurité du logiciel. Il convient que l'essai soit la méthode de validation principale du logiciel. La modélisation peut venir à l'appui des activités de validation.

NOTE 1 La validation est une confirmation, par examen et apport de preuves tangibles, que les exigences particulières pour un usage spécifique prévu sont satisfaites. Ainsi, par exemple, validation logicielle est une confirmation, par examen et apport de preuves tangibles, que le logiciel satisfait aux exigences de sécurité logicielle.

La conformité est vérifiée par la simulation des

- *signaux d'entrée présents lors du fonctionnement normal,*
- *des occurrences anticipées,*
- *des conditions non souhaitées exigeant une intervention du système.*

Les cas d'essai, données d'essai et résultats d'essai doivent être consignés.

NOTE 2 Des exemples de certaines techniques/mesures visant à satisfaire à ces exigences peuvent être consultés au Tableau A.7.

Tableau A.7 – Validation de la sécurité du logiciel

Technique/Mesure	Références informatives
Essai fonctionnel et essai de boîte noire: Analyse des valeurs limites – Simulation de processus	– IEC 61508-7, B.5.1, B.5.2 – IEC 61508-7, C.5.4 – IEC 61508-7, C.5.18
– Simulation, modélisation: Diagrammes d'états finis – Modélisation des performances	 IEC 61508-7, B.2.3.2 – IEC 61508-7, C.5.20

Annexe B
(informative)

Analyse par arbre de panne (AAP) et analyse des modes de défaillance et de leurs effets (AMDE)

B.1 Résultats de l'analyse par arbre de panne

Les appareillages électroniques de lampes pouvant faire l'objet d'un certain nombre de risques, le constructeur identifie et documente les conditions de défaillance du composant programmable qui peuvent avoir un impact sur la sécurité de l'appareil. En règle générale, chaque risque identifié est décrit à l'aide d'une simple déclaration. L'évaluation comprend les capteurs et actionneurs associés à la fonction de sécurité de sécurité.

NOTE 1 La Figure B.1 est un exemple de déclaration de risque: "Le TEC conducteur en continu est à l'origine de surchauffe en environnement chaud".

Après avoir identifié les dangers, une analyse par arbre de panne (AAP) est une approche descendante visant à identifier leurs causes. Le processus exige une connaissance précise du matériel. Il donne un aperçu de la mesure dans laquelle d'éventuelles défaillances et leurs combinaisons ont un impact sur les dangers identifiés de niveau supérieur.

NOTE 2 Les éventuelles défaillances sont par exemple:

- une défaillance logicielle à l'origine d'un branchement à la mauvaise partie d'un programme,
- une défaillance de composant du composant programmable qui gère le signal d'entrée ou de sortie d'un dispositif;
- un problème de mémoire dans le composant programmable.

Suite à l'analyse par arbre de panne (AAP), les conditions de défaut susceptibles de donner lieu à chacun des dangers identifiés sont enregistrées dans le tableau AMDE.

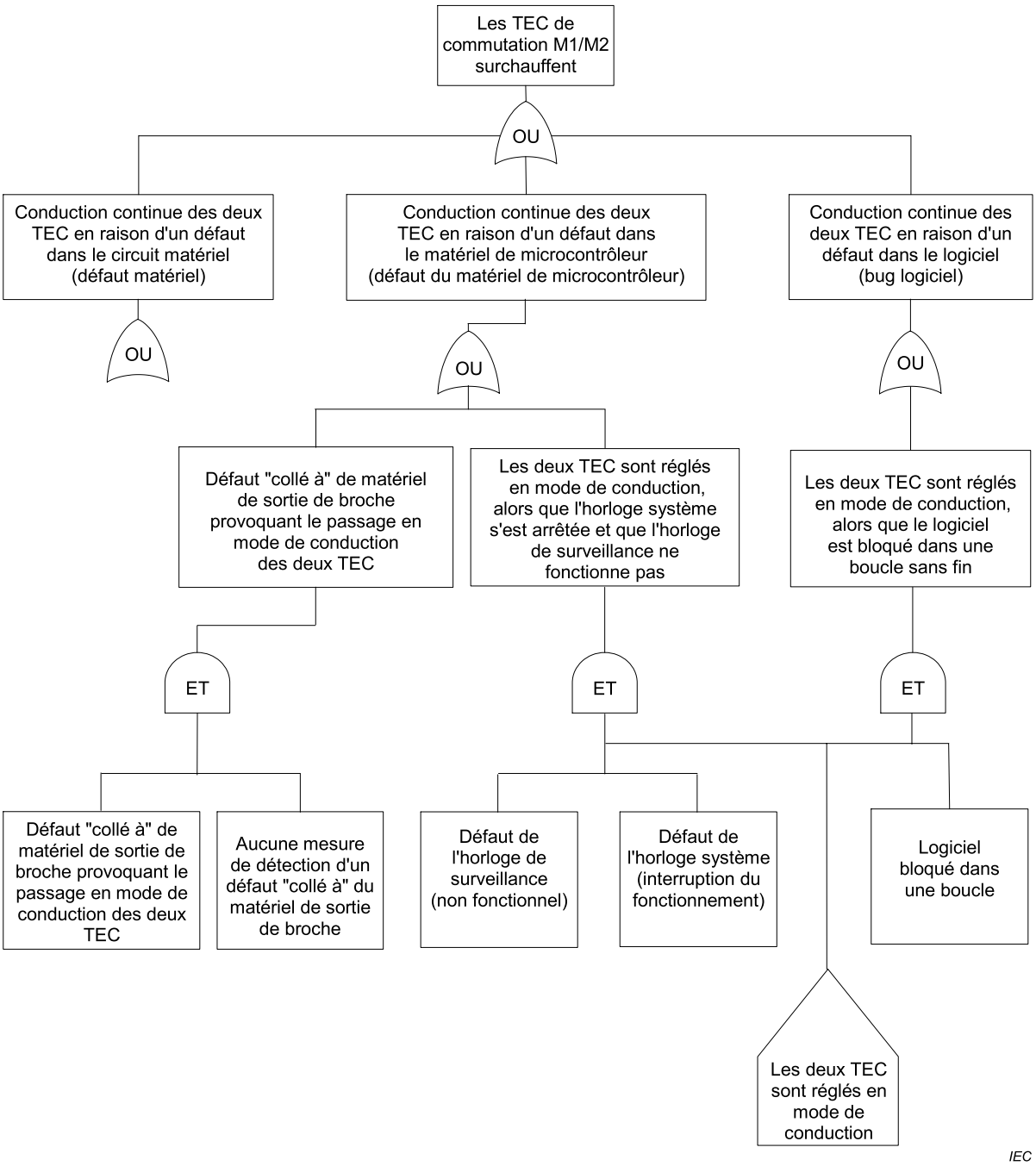

Figure B.1 – Exemple de schéma d'arbre de panne

B.2 Résultats d'analyse des modes de panne et de leurs effets (AMDE)

Les résultats d'analyse des modes de panne et de leurs effets (AMDE) sont au moins documentés conformément au Tableau A.2 de C22.2 No. 0.8-12, May 2012, *Safety functions incorporating electronic technology* [4]. Des détails supplémentaires peuvent être fournis, le cas échéant. Toutes les conditions indiquées dans l'arbre de panne (AAP) sont incluses dans ce tableau AMDE. Les messages d'erreur liés à la sécurité sont référencés, le cas échéant.

NOTE L'analyse est généralement faite lors d'une réunion d'ingénieurs. Les composants d'un système sont analysés l'un après l'autre pour établir l'ensemble des modes de défaillance du composant (en local et au niveau du système global), leurs causes et leurs effets, ainsi que des procédures et recommandations pour la détection. Si les recommandations sont acceptées, elles sont présentées comme étant les mesures correctives à prendre. La description de cette procédure peut être consultée dans: IEC 61508-7:2010, B.6.6.1]

Format du tableau AMDE

Un exemple de format de documentation des informations AMDE est présenté dans le Tableau A.2 de [4]. Les informations de ce tableau sont en général renseignées au fur et à mesure de l'avancée de la conception. Il s'agit d'une liste de contrôle utile visant à couvrir la totalité des modes de défaillance établis. Si le logiciel est utilisé, il faut que l'analyse AMDE inclue les éventuelles défaillances pouvant être générées par des défauts dans le logiciel. Toutes les défaillances présentées dans l'arbre de panne sont incluses avec celles indiquées dans le tableau AMDE. Les composants matériels sont correctement identifiés et référencés dans les schémas correspondants, par un schéma de bloc architectural ou par un schéma.

Annexe C
(informative)

Lignes directrices pour l'identification d'un composant programmable de protection

Un composant programmable de protection (PPC) est un composant programmable (PC) doté d'une fonction de sécurité logicielle qui assure la sécurité des appareillages électroniques de lampes dans les conditions de fonctionnement anormales ou de défaut de la présente norme. L'évaluation comprend les capteurs et actionneurs associés à la fonction de logiciel.

NOTE 1 Un PPC peut être, par exemple, un microcontrôleur qui détecte l'occurrence d'une condition anormale et qui empêche qu'elle ne donne lieu à une situation dangereuse (en désactivant un certain circuit du matériel ou l'ensemble des appareillages électroniques de lampes, par exemple).

Un PPC peut être identifié de différentes manières, en évaluant par exemple les principes de sécurité du matériel électronique par un examen minutieux des schémas de circuit.

D'autres méthodes plus pratiques peuvent être utilisées pour aider à identifier si l'appareillage électronique contient un composant programmable de protection:

a) les essais correspondants de 6.1 et de 6.2 sont réalisés après avoir désactivé l'ensemble du composant programmable concerné;

b) en tenant compte de tous les signaux d'entrée et de sortie (cas le moins favorable) possibles du composant programmable; ou

c) toutes les protections logicielles (et toutes leurs combinaisons), toutes les commandes logicielles et tous les paramètres logiciels du composant programmable étant désactivés et/ou rendus inactifs.

NOTE 2 Méthodes a) et b): utilisables par exemple en cas de CI, d'ASIC, de code non évaluable, etc.

Le problème est que les nombreuses fonctions de fiabilité du logiciel peuvent avoir une influence sur la sécurité. Une analyse approfondie et des essais peuvent s'avérer nécessaires pour identifier des mesures de protection de la sécurité. Cela pour s’assurer des mesures de robustesse de la sécurité exigées par la présente norme.

Aucun PPC n'est présent dans les appareillages électroniques de lampes si, dans les circonstances de la présente annexe, les appareillages électroniques de lampes restent sûrs conformément à 6.2. Toutefois, si la sécurité des appareillages électroniques de lampes n'est plus assurée, on peut en conclure que le composant programmable à l'essai empêche une situation dangereuse dans des conditions anormales ou de défaut, et doit donc satisfaire aux exigences d'un PPC.

Si aucun PPC n'a été identifié, il est conseillé d'enregistrer clairement la méthode d'identification ou d'exclusion d'un PPC pour s'y référer ultérieurement. Par exemple, les signaux d'entrée et de sortie qui ont été pris en compte pour le composant programmable (méthode b)) et/ou la fonction du logiciel du composant programmable qui a été désactivée (méthode c)). La méthode d'analyse des modes de défaillance et de leurs effets (AMDE) ou d'analyse par arbre de panne (AAP) peut être utilisée (voir l'Annexe B).

Annexe D
(normative)

Classification des risques

D.1 Généralités

La présente annexe définit la catégorisation des fréquences et sévérités de risque et la classification des risques liés à la sécurité. Une description informative est donnée dans l'IEC 61508-5:2010 Annexe C.

D.2 Fréquence

La catégorisation de la probabilité ou de la fréquence d'occurrence des risques liés à la sécurité est définie au Tableau D.1.

La probabilité peut être calculée de différentes manières, selon:

- la probabilité selon laquelle un produit est susceptible de faire l'objet d'un risque;
- le nombre prévu de produits d'un lot dont un produit est susceptible de faire l'objet du risque;
- le nombre prévu d'occurrences du risque sur toute la durée de vie d'un seul produit.

Tableau D.1 – Définition de fréquence et catégorisation (de l'IEC 61508-5:2010, Annexe C)

Fréquence	Description	Niveau 10^{-6} (indicatif)
Fréquent	Susceptible de se produire ou rencontré en permanence	$=>10^5$
Probable	Va se produire plusieurs fois au cours de la durée de vie du produit	10^4
Occasionnel	Susceptible de se produire parfois au cours de la durée de vie d'un produit	1 000
Rare	Peu probable, mais possible au cours de la durée de vie d'un produit	100
Improbable	Tellement peu probable que la situation peut ne pas se produire au cours de la durée de vie du produit	10
Invraisemblable	Ne se produira vraisemblablement pas au cours de la durée de vie du produit	<=1

D.3 Gravité du risque

La catégorisation de la gravité d'un risque lié à la sécurité est définie au Tableau D.2

Tableau D.2 – Définitions de la gravité du risque (de l'IEC 61508-5:2010, Annexe C)

Gravité	Description
Catastrophique	Possibilité de plusieurs décès ou de blessures graves
Critique	Possibilité de décès ou de blessures graves
Marginal	Possibilité de blessure
Négligeable	Peu ou pas de blessure possible

D.4 Classification des risques

Chaque risque lié à la sécurité doit être classé conformément au Tableau D.3 en "intolérable", "ALARP" ou "acceptable". Un risque acceptable est un risque qui peut être accepté dans un contexte donné en fonction des valeurs sociales à l'étude au moment de l'évaluation de la sécurité. Un risque intolérable est un risque trop important et qui doit être refusé. Le risque ALARP est un risque qui se place entre le risque acceptable et le risque intolérable. Il doit être réduit au niveau praticable le plus bas, en gardant à l'esprit les avantages que procure son acceptation, et en tenant compte de la possibilité d'exécution d'une éventuelle réduction.

Tableau D.3 – Classification des risques liés à la sécurité

Vraisemblance	Gravité			
	Catastrophique	Critique	Marginal	Négligeable
Fréquent	Intolérable	Intolérable	Intolérable	Intolérable
Probable	Intolérable	Intolérable	ALARP	ALARP
Occasionnel	Intolérable	ALARP	ALARP	ALARP
Rare	ALARP	ALARP	ALARP	Acceptable
Improbable	ALARP	ALARP	Acceptable	Acceptable
Invraisemblable	Acceptable	Acceptable	Acceptable	Acceptable

Un constructeur peut choisir d'appliquer un tableau ou mécanisme différent pour classer les risques liés à la sécurité, à condition que la classification satisfasse aux exigences suivantes.

- Un risque tellement important qu'il ne peut pas être justifié quelles que soient les circonstances est classé comme étant "intolérable".
- Un risque classé comme étant "acceptable" est acceptable par la société à l'étude, en tenant compte des valeurs sociales, politiques et économiques au moment de l'évaluation de la sécurité.

Le constructeur doit fournir une justification du tableau ou du mécanisme utilisé.

Toutes les classifications autres que "intolérable" et "acceptable" doivent être traitées comme étant "ALARP" dans le contexte de la présente norme.

Bibliographie

[1] IEC 62368-1:2010, *Equipements des technologies de l'audio/vidéo, de l'information et de la communication – Partie 1: Exigences de sécurité*

[2] ANSI/UL 1998-2008, *Standard for Software in Programmable Components*

[3] User Guide UG – 106, Version 0.92 July, 2010, CSA INTERNATIONAL, *Safety Controls with Software Hazard Analysis Guide & Information Requirements*

[4] C22.2 No. 0.8-12, May 2012, *Safety functions incorporating electronic technology*

[5] OD-2045-Ed.1.0, IECEE, *Guideline document & work instructions for testing purposes on how to implement the Annex R of IEC 60335-1 and Annex H of IE 60730-1*

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch