BS EN 62733:2015

BSI Standards Publication

Programmable components in electronic lamp controlgear — General and safety requirements

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 62733:2015. It is identical to IEC 62733:2015.

The UK participation in its preparation was entrusted by Technical Committee CPL/34, Lamps and Related Equipment, to Subcommittee CPL/34/3, Auxiliaries for lamps.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 75727 3
ICS 29.140.99

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2015.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62733

June 2015

ICS 29.140.99

English Version

Programmable components in electronic lamp controlgear - General and safety requirements (IEC 62733:2015)

Composants programmables dans les appareillages électroniques de lampes - Exigences générales et exigences de sécurité (IEC 62733:2015)

Programmierbare Bauteile von elektronischen Betriebsgeräten für Lampen - Teil 1: Allgemeine und Sicherheitsanforderungen (IEC 62733:2015)

This European Standard was approved by CENELEC on 2015-06-11. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 62733:2015 E

European foreword

The text of document 34C/1140/FDIS, future edition 1 of IEC 62733, prepared by SC 34C, "Auxiliaries for lamps", of IEC TC 34, "Lamps and related equipment", was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62733:2015.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2016-03-11
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2018-06-11

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62733:2015 was approved by CENELEC as a European Standard without any modification.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
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	EN 61000-4-13	2002
+ A1	2009		+ A1	2009
IEC 61347-1	-	Lamp controlgear - Part 1: General and safety requirement	EN 61347-1	-
IEC 61347-2	series	Lamp controlgear	EN 61347-2	series
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 4: Definitions and abbreviations	EN 61508-4	2010
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	EN 61508-5	2010
IEC 61508-7	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 7: Overview of techniques and measures	EN 61508-7	2010
IEC 61547	2009	Equipment for general lighting purposes - EMC immunity requirements	EN 61547	2009

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.

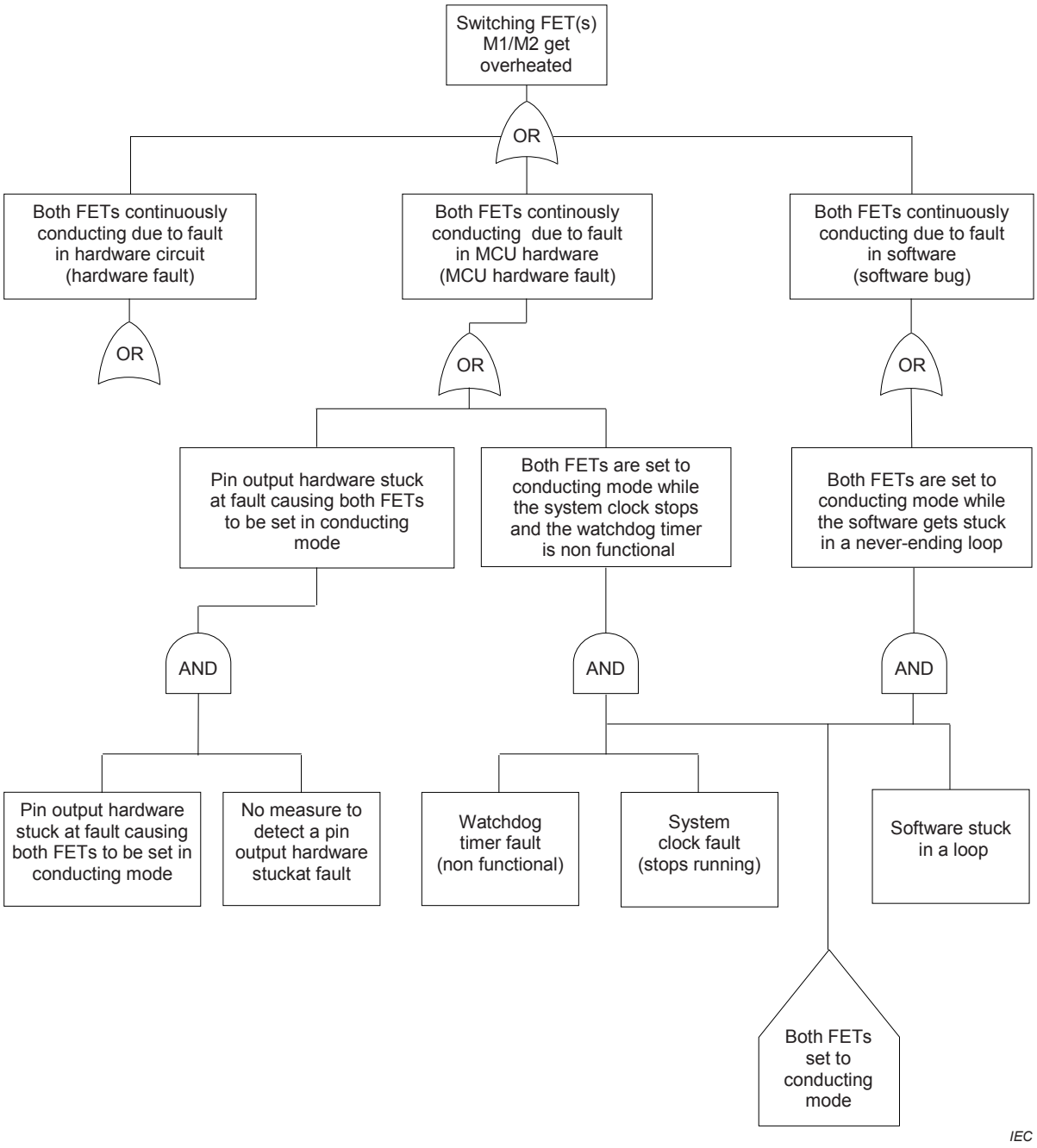

Figure B.1 – Example of a fault tree diagram

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*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™