PD IEC GUIDE 116:2018

BSI Standards Publication

Guidelines for safety related risk assessment and risk reduction for low voltage equipment

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

National foreword

This Published Document is the UK implementation of IEC GUIDE 116:2018.

The UK participation in its preparation was entrusted to Technical Committee L/1, Electrotechnical Technical Policy Committee.

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.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 539 03033 4

ICS 29.020

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

IEC GUIDE 116

Edition 2.0 2018-11

GUIDE

colour inside

Guidelines for safety related risk assessment and risk reduction for low voltage equipment

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 29.020

ISBN 978-2-8322-6097-5

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope and object 7
1.1 Scope 7
1.2 Object 7
1.3 Exclusion and limitation 7
2 Normative references 8
3 Terms definitions and abbreviations 8
3.1 Terms and definitions 8
3.2 Abbreviations 12
4 Basic principles 12
4.1 Principle of SAFETY INTEGRATION 12
4.2 Basic concepts 13
4.2.1 Information for RISK ASSESSMENT 15
4.2.2 Information related to LV equipment description 16
4.2.3 Related standards and other applicable documents 16
4.2.4 Information related to application experience 16
4.2.5 Relevant ergonomic principles 16
5 Determination of the limits of the LV equipment 16
6 HAZARD identification 17
7 RISK estimation 18
7.1 General 18
7.2 Elements of RISK 18
7.2.1 Combination of elements of RISK 18
7.2.2 Severity of harm 20
7.2.3 Probability of occurrence of harm 21
7.2.4 RISK INDEX 22
7.3 Aspects to be considered during RISK estimation 22
7.3.1 Exposure of persons or domestic animals 22
7.3.2 Type, frequency and duration of exposure 22
7.3.3 Accumulation and synergy of effects 23
8 RISK evaluation 23
8.1 General 23
8.2 Aspects to be considered during RISK evaluation 23
8.2.1 Human factors 23
8.2.2 Reliability of RISK REDUCTION MEASURES 24
8.2.3 Ability to defeat or circumvent PROTECTIVE MEASURES 24
8.2.4 Ability to maintain RISK REDUCTION MEASURES 25
8.2.5 Information for use 25
8.2.6 Current values of society 25
8.3 Elimination of hazards or reduction of RISK by RISK REDUCTION MEASURES 25
8.4 Comparison of RISKS 26
9 RISK reduction 26
10 Documentation 29

Documents
Document Sharing Hub
Full document details: PD IEC GUIDE 116:2018

Annex A (normative) SAFETY aspects relating to LOW VOLTAGE EQUIPMENT 30
A.1 General 30
A.2 Preliminary observations 30
A.3 SAFETY INTEGRATION 30
A.4 Protection against electrical hazards 31
A.5 Protection against mechanical hazards 31
A.6 Protection against other hazards 31
A.6.1 General 31
A.6.2 Explosion 31
A.6.3 Hazards arising from electric, magnetic, and electromagnetic fields, other ionising and non-ionising radiation 32
A.6.4 Electric, magnetic or electromagnetic disturbances 32
A.6.5 Optical radiation 32
A.6.6 Fire 32
A.6.7 Temperature 32
A.6.8 Acoustic noise 32
A.6.9 Biological and chemical effects 32
A.6.10 Emissions, production and/or use of hazardous substances (e.g. gases, liquids, dusts, mists, vapour) 33
A.6.11 Unattended operation 33
A.6.12 Connection to and interruption from power supply 33
A.6.13 Combination of equipment 33
A.6.14 Implosion 33
A.6.15 Hygiene conditions 33
A.6.16 Ergonomics 33
A.7 FUNCTIONAL SAFETY and reliability 33
A.7.1 General 33
A.7.2 Equipment design 34
A.7.3 Equipment type related hazards 34
A.7.4 System faults 34
A.8 SAFETY-RELATED SECURITY RISK 34
A.9 Information requirements 35
Annex B (informative) Supporting standards 36
B.1 Basic SAFETY standards 36
B.2 Group SAFETY standards 36
Annex C (informative) Table C.1 – Examples of hazards, hazardous situations and HAZARDOUS EVENTS 37
Annex D (informative) Tool for the application of this IEC Guide 39
Bibliography 41

Figure 1 – Principle of safety integration 13
Figure 2 – Iterative process of RISK ASSESSMENT and RISK reduction 15
Figure 3 – Elements of RISK for RISK estimation 19
Figure 4 – Graph for RISK estimation 20
Figure 5 – RISK reduction process 28

Table D.1 – RISK ASSESSMENT documentation 39

Documents
Document Sharing Hub
Full document details: PD IEC GUIDE 116:2018

INTERNATIONAL ELECTROTECHNICAL COMMISSION

GUIDELINES FOR SAFETY RELATED RISK ASSESSMENT AND RISK REDUCTION FOR LOW VOLTAGE EQUIPMENT

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.

This second edition of IEC Guide 116 has been prepared, in accordance with ISO/IEC Directives, Part 1, Annex A, by the IEC Advisory Committee on Safety (ACOS). This is a non-mandatory guide in accordance with SMB Decision 136/8.

This second edition of IEC Guide 116 cancels and replaces its first edition published in 2010 and constitutes a technical revision; main changes with respect to the first edition are as follows:

- addition of a clause dealing with safety related security aspects, derived from the IEC 62443 series (Clause A.8);
- reference to "domestic animals" rather than to "livestock", throughout the text of the guide;
- alignment of definitions and Figure 2 with the latest edition of ISO/IEC Guide 51 (2014);
- editorial improvements throughout the text;
- updates of the links to the IEC website.

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

The text of this IEC Guide is based on the following documents:

FDIS	Report on voting
ACOS/2084/DV	ACOS/2108/RV

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

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

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

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

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

INTRODUCTION

This non-mandatory IEC Guide is intended to be applied to RISK ASSESSMENT and risk reduction for SAFETY of LOW VOLTAGE EQUIPMENT.

This Guide provides guidance to those developing and revising standards, specifications and similar publications. However, the RISK ASSESSMENT method of this guide can be useful as background information for, amongst others, designers, architects, manufacturers, service providers, educators, communicators, auditors, SAFETY inspectors and policy makers.

This IEC Guide reflects ISO/IEC Guide 51 and gives additional guidance to ISO/IEC Guides 50, 51, and 71 on more detailed practical way of carrying out RISK ASSESSMENT and implementing RISK reduction for RISKs commonly considered during all relevant phases of the life of LOW VOLTAGE EQUIPMENT.

The user of this Guide is expected to take into account safety-related standards when available (see also Annex B) and their use automatically reflects the state of the art as defined in ISO/IEC Guide 2.

This Guide provides useful information in the absence of a specific standard.

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

GUIDELINES FOR SAFETY RELATED RISK ASSESSMENT AND RISK REDUCTION FOR LOW VOLTAGE EQUIPMENT

1 Scope and object

1.1 Scope

This non-mandatory IEC Guide complements ISO/IEC Guide 51 and establishes guidelines useful for achieving SAFETY in low voltage (LV) equipment. These guidelines include RISK ASSESSMENT, in which the knowledge and experience of the design, use, incidents, accidents and HARM related to LOW VOLTAGE EQUIPMENT are brought together in order to assess the RISKs during the relevant phases of the life of the equipment, as specified in Clause 6, and to implement the basic principles for RISK REDUCTION MEASURES. This IEC guide should be used by technical committees as far as appropriate and to the extent they decide to apply it.

This IEC Guide gives additional guidance to ISO/IEC Guides 50, 51 and 71 on the information required to allow RISK ASSESSMENT to be performed. Procedures are described for identifying hazards, estimating and evaluating RISK (including comparison of RISKs) and RISK reduction where necessary. Harms considered in this document include possible damages to persons, property, or domestic animals. It is not intended that the structure of this guide be adopted by technical committees.

This IEC Guide also includes requirements for the equipment documentation to include adequate information for the safe use of equipment.

1.2 Object

The purpose of this IEC Guide is to provide guidance for technical committees for decisions to be made on the SAFETY of LOW VOLTAGE EQUIPMENT and the type of documentation required to verify the RISK ASSESSMENT carried out.

This IEC Guide applies to all electrical equipment designed for use with a voltage range up to 1 000 V a.c. (1 500 V d.c.). Voltage ratings refer to the voltage of the electrical input or output, not to voltages that may appear inside the equipment.

Annex A of this Guide identifies basic health and SAFETY requirements, typically for LOW VOLTAGE EQUIPMENT.

Annex D can be used as a tool for documenting a self-assessment by a Technical Committee.

1.3 Exclusion and limitation

This guide does not apply to those basic components whose RISK ASSESSMENT depends to a very large extent on how they are used and incorporated into a machine, electrical system or installation. However, other electrical components that are intended to be incorporated into other electrical equipment and for which a RISK ASSESSMENT can be undertaken are covered by this IEC Guide, in general requiring a further assessment of the SAFETY aspects related to the way in which such components are incorporated.

NOTE 1 The scope of the exclusion of basic components should not be misunderstood and extended to items like lamps, starters, fuses, switches for household use, elements of electrical installations, etc.

These components, even if they are often used in conjunction with other electrical equipment and have to be properly installed in order to deliver their useful function, are themselves to be considered electrical equipment in the sense of this Guide.

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

NOTE 2 RISK REDUCTION MEASURES to be taken by the user of a product are subject to legal requirements in many countries, especially in the occupational health and SAFETY framework.

This IEC Guide itself is not intended to be used for the purpose of certification. Product committees are encouraged to include a clause in product SAFETY standards pertaining to RISK ASSESSMENT, to be used when the requirements of these standards do not fully encompass all possible hazards with equipment within the standard's scope, especially for emerging technologies, where new hazards may arise.

If the RISK ASSESSMENT identifies aspects not directly related to health and SAFETY such as environment protection, energy consumption, climate change, etc., the RISK reduction for health and SAFETY related RISKs in particular with respect to persons overrules the priority of those other aspects. However such aspects can be defined by regulations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC Guide 104:2010, *The preparation of safety publications and the use of basic safety publications and group safety publications*

IEC Guide 117:2010, *Electrotechnical equipment – Temperatures of touchable hot surfaces*

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

3 Terms definitions and abbreviations

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

IEC Electropedia: available at http://www.electropedia.org/

ISO Online browsing platform: available at http://www.iso.org/obp/

3.1.1
low voltage equipment
set of electrical devices or electrical apparatus necessary to perform a specific task such as generation, transmission, distribution, utilisation of electric energy and with a supply or output voltage not exceeding 1 000 V for alternating current and 1 500 V for direct current

EXAMPLES Equipment includes electric power generator, electrical switchgear and controlgear assemblies, electrical wiring systems, air conditioning units, energy storage units, programmable and other electronic equipment, etc.

3.1.2
harm
injury or damage to the health of people or damage to property or the environment

[SOURCE: ISO/IEC Guide 51:2014, definition 3.1]

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

3.1.3
hazard
potential source of HARM

[SOURCE: ISO/IEC Guide 51:2014, definition 3.2]

3.1.4
hazard zone
any space within and/or around a product, process or service in which persons, or domestic animals can be exposed to a HAZARD

3.1.5
hazardous event
event that can cause HARM

[SOURCE: ISO/IEC Guide 51:2014, definition 3.3]

Note 1 to entry: A HAZARDOUS EVENT can occur over a short period of time or over an extended period of time.

3.1.6
hazardous situation
circumstance in which people, property or the environment is/are exposed to one or more hazards

[SOURCE: ISO/IEC Guide 51:2014, definition 3.4]

3.1.7
arc
free burning short-circuit through air arising from a fault between live parts of different potential and/or between live parts and other conductive parts within an assembly

[SOURCE: IEC 61641:2014, definition 3.5]

3.1.8
incident
past HAZARDOUS EVENT

Note 1 to entry: An INCIDENT that has resulted in HARM can be referred to as an accident. Whereas an INCIDENT that has occurred and that did not result in HARM can be referred to as a near miss occurrence.

3.1.9
accident
INCIDENT that did result in HARM

3.1.10
malfunction
situation for which the electrical equipment does not perform the intended function due to a variety of reasons, such as:

– variation of a property or of a dimension of the processed material or of the work piece;
– failure of one (or more) of its component parts or services;
– external disturbances (e.g. shocks, vibration, electromagnetic interference);
– design error or deficiency (e.g. software errors);
– disturbance of its power supply;
– surrounding conditions (e.g. condensation due to temperature change).

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

3.1.11
risk index
combined score used to measure the likelihood of occurrence, magnitude and severity of RISK

[SOURCE: ISO 17666:2016, definition 3.1.3]

3.1.12
inherently safe design
measures taken to eliminate hazards and/or to reduce RISKs by changing the design or operating characteristics of the product or system

[SOURCE: ISO/IEC Guide 51:2014, definition 3.5]

3.1.13
safeguarding
PROTECTIVE MEASURE using safeguards to protect persons and domestic animals from the hazards which cannot reasonably be eliminated or RISKS which cannot be sufficiently reduced by INHERENTLY SAFE DESIGN measures

[SOURCE: ISO 12100:2010, definition 3.21 modified with domestic animals]

3.1.14
complementary protective measure
RISK REDUCTION MEASURE involving a protective device (other than safeguard)

EXAMPLE of protective device: emergency stop equipment, interlocking device, enabling device, etc.

3.1.15
intended use
use in accordance with information provided with a product or system, or, in the absence of such information, by generally understood patterns of usage

[SOURCE: ISO/IEC Guide 51:2014, definition 3.6]

3.1.16
reasonably foreseeable misuse
use of a product or system in a way not intended by the supplier, but which can result from readily predictable human behaviour

Note 1 to entry: Readily predictable human behaviour includes the behaviour of all types of users, e.g. the elderly, children and persons with disabilities. For more information, see ISO 10377.

Note 2 to entry: In the context of consumer SAFETY, the term “reasonably foreseeable use” is increasingly used as a synonym for both “INTENDED USE” and “REASONABLY FORESEEABLE MISUSE.”

[SOURCE: ISO/IEC Guide 51:2014, definition 3.7]

3.1.17
residual risk
RISK remaining after RISK REDUCTION MEASURES have been implemented

Note 1 to entry: This IEC Guide distinguishes:

– the RESIDUAL RISK after PROTECTIVE MEASURES have been taken by the designer;

– the RESIDUAL RISK remaining after all PROTECTIVE MEASURES have been implemented by the user.

[SOURCE: ISO/IEC Guide 51:2014, definition 3.8, modified]

AVA Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

3.1.18
risk
combination of the probability of occurrence of HARM and the severity of that HARM

Note 1 to entry: The probability of occurrence includes the exposure to a HAZARDOUS SITUATION, the occurrence of a HAZARDOUS EVENT and the possibility to avoid or limit the HARM.

[SOURCE: ISO/IEC Guide 51:2014, definition 3.9]

3.1.19
risk assessment
overall process comprising a RISK analysis and a RISK evaluation

[SOURCE: ISO/IEC Guide 51:2014, definition 3.11]

3.1.20
risk reduction measure
protective measure
action or means to eliminate hazards or reduce RISKs

EXAMPLES INHERENTLY SAFE DESIGN; protective devices; personal protective equipment; information for use and installation; organization of work; training; application of equipment; supervision.

[SOURCE: ISO/IEC Guide 51:2014, definition 3.13]

3.1.21
safety
freedom from RISK which is not tolerable

[SOURCE: ISO/IEC Guide 51:2014, definition 3.14]

3.1.22
tolerable risk
acceptable risk
level of RISK that is accepted in a given context based on the current values of society

[SOURCE: ISO/IEC Guide 51:, definition 3.15, modified with the synonymous term acceptable risk]

3.1.23
safety integration
application of the “3-step-methodology” (see Figure 1) to reduce the RESIDUAL RISK of a LV equipment below the level of TOLERABLE RISK

Note 1 to entry: See A.2 for further information.

3.1.24
functional safety
part of the overall SAFETY that depends on functional and physical units operating correctly in response to their inputs

Note 1 to entry: See IEC/TR 61508-0, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and and IEC 61508.

[SOURCE: IEC 60050-351:2013, 351-57-06]

3.1.25
adequate protection
protection which reduces RISK to a tolerable level

Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018

3.1.26
single fault condition
condition in which there is a fault of a single protection (but not a reinforced protection) or of a single component or a device

Note 1 to entry: If a SINGLE FAULT CONDITION results in one or more other fault conditions, all are considered as one SINGLE FAULT CONDITION.

Note 2 to entry: Reinforced protection is defined IEV 903-02-08

[SOURCE: IEC Guide 104:2010, definition 3.8 modified]

3.1.27
safety-related security risk
RISK that a particular SECURITY THREAT exploits a particular SECURITY VULNERABILITY and leads to HAZARDOUS SITUATION

[SOURCE: IEC/TS 62443-1-1:2009, derived from definition 3.2.87]

3.1.28
security threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause HARM

[SOURCE: Derived from IEC/TS 62443-1-1:2009, definition 3.2.125 modified]

3.1.29
security violation
act or event that disobeys or otherwise breaches security policy through an intrusion or the actions of a well-meaning insider

[SOURCE: IEC/TS 62443-1-1:2009, definition 3.2.116 modified with a completed term]

3.1.30
security vulnerability
flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy

[SOURCE: IEC/TS 62443-1-1:2009, definition 3.2.135 modified with a completed term]

3.2 Abbreviations

HMI Human machine interface

USB Universal Serial Bus

LAN Local area network

WLAN Wireless local area network

TCP Transmission control protocol

4 Basic principles

4.1 Principle of SAFETY INTEGRATION

Figure 1 shows the principle of SAFETY INTEGRATION. The minimum necessary RISK reduction is the reduction in RISK that has to be achieved to meet the TOLERABLE RISK for a specific situation. The concept of necessary RISK reduction is of fundamental importance in the development of the SAFETY requirements for electrical equipment. The purpose of determining the TOLERABLE RISK for a specific HAZARDOUS EVENT is to state what is deemed reasonable with respect to both components of RISK (see 3.1.18, 7.2 and Figure 3).

AVA Documents
Document Sharing Hub

Full document details: PD IEC GUIDE 116:2018