IEC 60947-5-3

Edition 2.0 2013-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Low-voltage switchgear and controlgear –
Part 5-3: Control circuit devices and switching elements – Requirements for proximity devices with defined behaviour under fault conditions (PDDB)

Appareillage à basse tension –
Partie 5-3: Appareils et éléments de commutation pour circuits de commande – Exigences pour dispositifs de détection de proximité à comportement défini dans des conditions de défaut (PDDB)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

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

About the IEC

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

About IEC publications

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

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

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

Customer Service Centre - webstore.iec.ch/csc

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

A propos de la CEI

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

A propos des publications CEI

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

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

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

IEC 60947-5-3

Edition 2.0 2013-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Low-voltage switchgear and controlgear – Part 5-3: Control circuit devices and switching elements – Requirements for proximity devices with defined behaviour under fault conditions (PDDB)

Appareillage à basse tension – Partie 5-3: Appareils et éléments de commutation pour circuits de commande – Exigences pour dispositifs de détection de proximité à comportement défini dans des conditions de défaut (PDDB)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

U

ICS 29.130.20

ISBN 978-2-8322-1030-7

CONTENTS

FOREWORD 4
1 General 6
1.1 Scope 6
1.2 Normative references 6
2 Terms, definitions and abbreviations 8
2.1 General 8
2.2 Alphabetic index of terms 8
2.3 Basic terms and definitions 9
2.4 Terms and definitions concerning the architectural constraints 12
2.5 Terms and definitions concerning the parts of a PDDB 13
2.6 Terms and definitions concerning the operation of a PDDB 14
2.7 Symbols and abbreviations 15
3 Classification 15
4 Characteristics 15
4.1 General 15
4.2 Constructional characteristics 15
4.2.1 Proximity device with defined behaviour 15
4.2.2 Specified target 15
5 Product information 16
5.1 Nature of information 16
5.2 Identification 16
5.3 Marking 16
5.3.1 General 16
5.3.2 Connection identification and marking 16
5.4 Instructions for installation, operation and maintenance 16
6 Normal service, mounting and transport conditions 17
6.1 Normal service conditions 17
6.2 Conditions during transport and storage 17
6.3 Mounting 17
7 Constructional and performance requirements 17
7.1 Constructional requirements 17
7.1.1 Materials 17
7.1.2 Current-carrying parts and their connections 17
7.1.3 Clearance and creepage distances 17
7.1.4 Vacant 17
7.1.5 Vacant 17
7.1.6 Vacant 17
7.1.7 Terminals 17
7.1.8 Provision for protective earthing 18
7.1.9 IP degree of protection (in accordance with IEC 60529) 18
7.2 Functional safety management 18
7.3 Functional requirements specification for SRCFs 18
7.3.1 General 18
7.3.2 Safety integrity requirements specification for SRCFs 18
7.3.3 Electromagnetic compatibility 18
7.3.4 Design and development of PDDB 20

7.4 Information for use 20
7.4.1 Objective 20
7.4.2 Documentation for installation, use and maintenance 20
8 Tests 21
8.1 Kind of tests 21
8.1.1 General 21
8.1.2 Type tests 21
8.1.3 Routine tests 21
8.1.4 Sampling tests 21
8.2 Compliance with constructional requirements 21
8.3 Performances 21
8.3.1 Test sequences 21
8.3.2 General test conditions 21
8.3.3 Performances under no load, normal and abnormal load conditions 21
8.3.4 Performances under short-circuit current conditions 22
8.4 Verification of operating distances 22
8.5 Verification of resistance to vibration and shock 22
8.6 Verification of electromagnetic compatibility 22
9 Modification 23
9.1 Objective 23
9.2 Modification procedure 23
Annex A (informative) Example of a simple control system in accordance with IEC 61511 series 24
Bibliography 28

Figure A.1 – Representation of the equipment under control 24
Figure A.2 – Architecture of the safety related function 25

Table 1 – EMC requirements for PDDBs 19
Table A.1 – Collection of reliability and structure data 25

INTERNATIONAL ELECTROTECHNICAL COMMISSION

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR –

Part 5-3: Control circuit devices and switching elements – Requirements for proximity devices with defined behaviour under fault conditions (PDDB)

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 60947-5-3 has been prepared by subcommittee 17B: Low-voltage switchgear and controlgear, of IEC technical committee 17: Switchgear and controlgear.

This second edition replaces the first edition published in 1999 and its amendment published in 2005. It is a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) general principles of IEC 61508 series;

b) classification according to the requirements of IEC 62061;

c) classification according to ISO 13849-1.

This standard is to be read in conjunction with IEC 60947-1, *Low voltage switchgear and controlgear – Part 1: General rules* and IEC 60947-5-2, *Low-voltage switchgear and*

controlgear – Part 5-2: Control circuit devices and switching elements – Proximity switches. The provisions of Part 1 and Part 5-2 are only applicable to this standard where specifically called for. The numbering of the subclauses of this standard is sometimes not continuous because it is based on the numbering of the subclauses of IEC 60947-1 or IEC 60947-5-2.

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

FDIS	Report on voting
17B/1821/FDIS	17B/1826/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.

A list of all parts in the IEC 60947 series, published under the general title *Low-voltage switchgear and controlgear*, can be found on the IEC website.

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.

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR –

Part 5-3: Control circuit devices and switching elements – Requirements for proximity devices with defined behaviour under fault conditions (PDDB)

1 General

1.1 Scope

This part of IEC 60947 series provides additional requirements to those given in IEC 60947-5-2. It addresses the fault performance aspects of proximity devices with a defined behaviour under fault conditions (PDDB). It does not address any other characteristics that can be required for specific applications.

This standard does not cover proximity devices with analogue output.

This Standard does not deal with any specific requirements on acoustic noise as the noise emission of control circuit devices and switching elements is not considered to be a relevant hazard.

For a PDDB used in applications where additional characteristics, dealt with in other standards, are required, the requirements of all relevant standards apply.

The use of this standard alone does not demonstrate suitability for the implementation of any specific safety related functionality. In particular, this standard does not provide requirements for the actuation characteristics of a PDDB, or for means to reduce the effects of mutual interference between devices, e.g. coded targets. Therefore these and any other application-specific requirements will need to be considered in addition to the requirements of this standard.

NOTE 1 Due to their behaviour under fault conditions, PDDBs can, for example, be used as interlocking devices (see ISO 14119).

NOTE 2 The requirements for electro-sensitive protective equipment for the detection of persons are given in the IEC 61496 series.

1.2 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 60068-2-1:2007, *Environmental testing – Part 2-1: Tests – Test A: Cold*

IEC 60068-2-30:2005, *Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 + 12 h cycle)*

IEC 60529:1989, *Degrees of protection provided by enclosures (IP Code)*
Amendment 1:1999

IEC 60947-1:2007, *Low-voltage switchgear and controlgear – Part 1: General rules*
Amendment 1:2010

IEC 60947-5-1:2003, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*
Amendment 1:2009

IEC 60947-5-2:2007, *Low-voltage switchgear and controlgear – Part 5-2: Control circuit devices and switching elements – Proximity switches*
Amendment 1:2012

IEC 61000-4-2:2008, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

IEC 61000-4-3:2006, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*
Amendment 1:2007
Amendment 2:2010

IEC 61000-4-4:2012, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5:2005, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-4-6:2008, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61000-4-8:2009, *Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques – Power frequency magnetic field immunity test*

IEC 61000-4-11:2004, *Electromagnetic compatibility (EMC) – Part 4-11: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations immunity tests*

IEC 61131-2:2007, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*
Amendment 1:2012

ISO 13849-1:2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

2 Terms, definitions and abbreviations

2.1 General

For the purposes of this document, the terms and definitions given in IEC 60947-1 and IEC 60947-5-2, as well as the following terms, definitions and abbreviations apply.

2.2 Alphabetic index of terms

Reference

A

assured operating distance of a PDDB [S_{ao}] 2.6.4
assured release distance of a PDDB [S_{ar}] 2.6.5

C

complex component 2.3.4
control and monitoring device 2.5.3

D

dangerous failure 2.3.6
defined behaviour (of PDDB) 2.6.1
diagnostic coverage [DC] 2.4.2
diagnostic test interval 2.4.4

E

equipment under control [EUC] 2.4.7

F

failure (of equipment) 2.3.5
fault 2.3.8
failures in time [FIT] 2.3.18

H

hardware fault tolerance [HFT] 2.4.3
hardware safety integrity 2.3.11

L

lock-out state 2.6.8
low complexity component 2.3.3

M

mean time to dangerous failure [$MTTF_d$] 2.3.17
mission time [T_M] 2.6.7
mode of operation 2.3.14

O

OFF-state 2.6.2
ON-state 2.6.3
output signal switching device [OSSD] 2.5.2

P

Performance Level [PL] 2.3.1
proof test 2.4.5

R

risk time 2.6.6

S

safe failure....2.3.7
safe failure fraction [SFF]....2.4.1
safety integrity....2.3.10
Safety Integrity Level [SIL]....2.3.2
Safety-Related Control Function [SRCF]....2.3.9
safety-related system....2.4.6
sensing means....2.5.1
SIL Claim Limit [SILCL]....2.3.16
software safety integrity....2.3.12
systematic safety integrity....2.3.13

T

target failure measure....2.3.15

2.3 Basic terms and definitions

2.3.1
Performance Level
PL
discrete level (from a to e) used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1:2006, 3.1.23, modified – update of the definition]

2.3.2
Safety Integrity Level
SIL
discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the safety related parts of the control system, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest

Note 1 to entry: SIL 4 is not considered in this standard. For requirements applicable to SIL 4, see IEC 61508 series.

[SOURCE: IEC 62061:2005, 3.2.23, modified – update of the note]

2.3.3
low complexity component
component in which:

– the failure modes are well-defined; and
– the behaviour under fault conditions can be completely defined

Note 1 to entry: Behaviour of the low complexity component under fault conditions may be determined by analytical and/or test methods.

Note 2 to entry: A subsystem or subsystem element comprising one or more limit switches, operating, possibly via interposing electro-mechanical relays, one or more contactors to de-energise an electric motor is an example of a low complexity component.

[SOURCE: IEC 62061:2005, 3.2.7]

2.3.4
complex component
component in which:

– the failure modes are not well-defined; or
– the behaviour under fault conditions cannot be completely defined

[SOURCE: IEC 62061:2005, 3.2.8]

2.3.5
failure
the termination of the ability of an item to perform a required function

Note 1 to entry: After failure the system has a fault.

Note 2 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.

Note 3 to entry: The concept of failure as defined does not apply to items consisting of software only.

[SOURCE: IEC 60050-191:1990, 191-04-01]

2.3.6
dangerous failure
failure of a PDDB that has the potential to cause a hazard or non-functional state

[SOURCE: IEC 62061:2005, 3.2.40, modified – deletion of the notes]

2.3.7
safe failure
failure of a PDDB that does not have the potential to cause a hazard

[SOURCE: IEC 62061:2005, 3.2.41 modified – update of the definition]

2.3.8
fault
state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

Note 1 to entry: A fault is often the result of the item itself but can exist without prior failure.

Note 2 to entry: In English the term “fault” and its definition are identical to those given in IEC 60050-191:1990, 191-05-01. In the field of machinery, the French term “défaut” and the German term “Fehler” are used rather than the term “panne” and “Fehlzustand” that appear with this definition.

[SOURCE: IEC 62061:2005, 3.2.30, modified – new definition and new notes]

2.3.9
Safety-Related Control Function
SRCF
control function with a specified integrity level, partly or completely implemented by a PDDB, that is intended to maintain the safe condition of the equipment under control or prevent an immediate increase of the risk(s)

Note 1 to entry: ISO 13849-1 uses the term SRF (safety related function), IEC 61508 series uses SF (safety function), Terms and definitions concerning the integrity.

[SOURCE: IEC 62061:2005, 3.2.16 modified – new definition and new note]

2.3.10
safety integrity
probability of a safety related control system or its PDDB satisfactorily performing the required safety-related control functions under all stated conditions

[SOURCE: IEC 62061:2005, 3.2.19, modified – update of the definition and deletion of the notes]

2.3.11
hardware safety integrity
part of the safety integrity of a safety related control system or its PDDB comprising requirements for both the probability of dangerous random hardware failures and architectural constraints

[SOURCE: IEC 62061:2005, 3.2.20, modified – update of the definition]

2.3.12
software safety integrity
part of the safety integrity of a PDDB relating to systematic failures in a dangerous mode of failure that are attributable to software

Note 1 to entry: Software safety integrity cannot usually be quantified precisely.

[SOURCE: IEC 61508-4:2010, 3.5.5, modified – update of the definition and addition of a note]

2.3.13
systematic safety integrity
part of the safety integrity of a PDDB relating to systematic failures in a dangerous mode of failure

Note 1 to entry: Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity which usually can).

Note 2 to entry: Requirements for systematic safety integrity apply to both hardware and software aspects of a PDDB.

[SOURCE: IEC 61508-4:2010, 3.5.6 modified – update of the definition and addition of a note]

2.3.14
mode of operation
way in which a safety function operates, which may be either:

– **low demand mode**: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or

Note 1 to entry: The E/E/PE safety-related system that performs the safety function normally has no influence on the EUC or EUC control system until a demand arises. However, if the E/E/PE safety-related system fails in such a way that it is unable to carry out the safety function then it may cause the EUC to move to a safe state.

– **high demand mode:** where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or
– **continuous mode:** where the safety function retains the EUC in a safe state as part of normal operation

[SOURCE: IEC 61508-4:2010, 3.5.16, modified – update of the note]

2.3.15
target failure measure
intended probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either:

– the average probability of dangerous failure to perform the design function on demand PFD_{avg} (for a low demand mode of operation);
– the average frequency of a dangerous failure over a given period of time PFH_D (for a high demand or continuous mode of operation)

Note 1 to entry: The term “probability of dangerous failure per hour” is not used in the standard but the abbreviation PFH has been retained but when it is used it means “average frequency of dangerous failure”.

Note 2 to entry: The numerical values for the target failure measures are given in Table 2 and Table 3 of IEC 61508-1:2010. These limit values are valid for the whole safety related function.

[Adapted from IEC 61508-4:2010, 3.5.17]

2.3.16
SIL Claim Limit
SILCL
maximum SIL that can be claimed for a PDDB in relation to architectural constraints and systematic safety integrity

[SOURCE: IEC 62061:2005, 3.2.24 modified – update of the definition]

2.3.17
mean time to dangerous failure
$MTTF_d$
expectation of the mean time to dangerous failure

Note 1 to entry: Adapted from IEC 62061:2005, definition 3.2.34.

[SOURCE: ISO 13849-1:2006, 3.1.25]

2.3.18
failure in time
FIT
the number of failures in 10^9 device-hours of operation

2.4 Terms and definitions concerning the architectural constraints

2.4.1
safe failure fraction
SFF
ratio of the average failure rates of safe failures plus dangerous detected failures of the PDDB to the total average failure rate (sum of safe failure rate and all dangerous failure rate) of the PDDB

[Adapted from IEC 61508-4:2010, 3.6.15]

2.4.2
diagnostic coverage
DC
measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures

[SOURCE: ISO 13849-1:2006, 3.1.26, modified – deletion of the notes]

fraction of dangerous failures detected by automatic on-line diagnostic tests

Note 1 to entry: The fraction of detected dangerous failures is computed to be the rate of dangerous failures that are detected by automatic on-line diagnostic tests divided by the rate of total dangerous failures.

Note 2 to entry: There is a different approach between the IEC 62061/IEC 61508 and ISO 13849-1 failure concepts. Prescriptions for architectural constraints on subsystems according to IEC 62061:2005 (Table 5) are given as a function of the hardware fault tolerance and the safe failure fraction. ISO 13849-1 does not consider any safe failure/safe failure fraction. Performance levels are based on well-defined architectures. The achieved PL is then a function of the architecture, the $MTTF_d$, the diagnostic coverage and the common cause failures.

[SOURCE: IEC 62061:2005, 3.2.38, modified – update of the notes]

2.4.3
hardware fault tolerance
HFT
ability of a system to perform its safety function in the presence of faults

Note 1 to entry: Hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function. In determining the hardware fault tolerance no consideration is given to other faults, for example in diagnostics.

[Adapted from IEC 61508-2:2010, 7.4.4.1.1]

2.4.4
diagnostic test interval
interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage

[SOURCE: IEC 61508-4:2010, 3.8.7]

2.4.5
proof test
periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an “as new” condition or as close as practical to this condition

[SOURCE: IEC 61508-4:2010, 3.8.5, modified – update of the definition and deletion of the notes]

2.4.6
safety-related system
designated system that both

– implements the required safety functions necessary to achieve or maintain a safe state for the Equipment Under Control; and
– is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions

[SOURCE: IEC 61508-4:2010, 3.4.1, modified – deletion of the notes]

2.4.7
equipment under control
EUC
equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities

Note 1 to entry: The EUC control system is separate and distinct from the EUC.

[SOURCE: IEC 61508-4:2010, 3.2.1]

2.5 Terms and definitions concerning the parts of a PDDB

2.5.1
sensing means
part of the PDDB which detects the presence or absence of a defined target

2.5.2
output signal switching device
OSSD
component of the PDDB which goes to the OFF-state according to the defined behaviour

2.5.3
control and monitoring device
device which receives and processes signals from the sensing means, provides signals to the OSSD(s) and monitors correct operation

2.6 Terms and definitions concerning the operation of a PDDB

2.6.1
defined behaviour
changing of the OSSD(s) to the off-state in the defined position of the specified target and in accordance with the requirements of this standard

2.6.2
OFF-state
state in which the output circuits interrupts the flow of current other than residual current (I_r)

2.6.3
ON-state
state in which the output circuits permits the flow of current

2.6.4
assured operating distance of a PDDB
S_{ao}
distance from the sensing face within which the presence of the specified target is correctly detected under all specified environmental conditions and manufacturing tolerances

2.6.5
assured release distance of a PDDB
S_{ar}
distance from the sensing face beyond which the absence of the specified target is correctly detected under all specified environmental conditions and manufacturing tolerances

2.6.6
risk time
maximum period of time during which OSSD(s) can deviate from the defined behaviour

2.6.7
mission time
T_M
period of time covering the intended use of a PDDB

2.6.8
lock-out state
state in which at least one OSSD is OFF and remains in OFF-state until the fault is corrected. The device enters the lock-out state whenever a fault is detected

2.7 Symbols and abbreviations

Symbol or abbreviation	Description	Definition
DC	diagnostic coverage	2.4.2
EUC	equipment under control	2.4.7
FIT	failures in time	2.3.18
HFT	hardware fault tolerance	2.4.3
$MTTF_d$	mean time to dangerous failure	2.3.17
OSSD	output signal switching device	2.5.2
PFH_D	average frequency of a dangerous failure over a given period of time	2.3.15
PFD	probability of dangerous failure on demand	2.3.15
PL	performance level	2.3.1
S_{ao}	assured operating distance of a PDDB	2.6.4
S_{ar}	assured release distance of a PDDB	2.6.5
SRF	safety related function	2.3.9
SFF	safe failure fraction	2.4.1
SIL	safety integrity level	2.3.2
SILCL	SIL claim limit	2.3.16
SRCF	safety-related control function	2.3.9
T_M	mission time	2.6.7

3 Classification

Clause 3 of IEC 60947-5-2:2007 applies.

4 Characteristics

4.1 General

Clause 4 of IEC 60947-5-2:2007 applies, with the following additions.

4.2 Constructional characteristics

4.2.1 Proximity device with defined behaviour

A PDDB is composed of the following elements:

a) sensing means;
b) OSSD(s);
c) control and monitoring device (when required).

These elements may be integrated into a single device or may be separate devices.

4.2.2 Specified target

The manufacturer shall specify the necessary target to achieve the distances S_{ao} and S_{ar}.

5 Product information

5.1 Nature of information

The following information shall be given by the manufacturer.

5.2 Identification

Subclause 5.1 of IEC 60947-5-2:2007 applies with the following additions:

aa) assured operating distance;

ab) assured release distance;

ac) specified target;

ad) risk time;

ae) defined safe state of the OSSD(s);

af) mission time;

and either:

ag) SFF/DC (if any) and HFT (in accordance with IEC 61508 series and derivatives), and reliability data (e.g. λ, PFH_D , PFD_{avg}, B_{10d}, as appropriate);

or

ah) designated architecture (if any) and B_{10d}, λ, $MTTF_d$ and DC (in accordance with ISO 13849-1), as appropriate.

5.3 Marking

5.3.1 General

Subclause 5.2.1 of IEC 60947-5-2:2007 applies, with the following additions.

In the case of a PDDB comprising separate devices, the marking of data under items a) and b) of 5.1 of IEC 60947-5-2:2007 on every device is mandatory.

Data under items c) to ah), when not included on the proximity device or on any separate devices, shall be included in the manufacturer's literature.

5.3.2 Connection identification and marking

Subclause 7.1.7.4 of IEC 60947-5-2:2007, Amendment 1 (2012) applies. When the terminals cannot be marked in accordance with 7.1.7.4 of IEC 60947-5-2:2007, Amendment 1 (2012), for example when located within a separate enclosure, the manufacturer shall provide appropriate terminal identification.

5.4 Instructions for installation, operation and maintenance

Subclause 5.3 of IEC 60947-5-2:2007, Amendment 1 (2012) applies, with the following additions.

Details of known and reasonably foreseeable external influences that can affect the S_{ao} and/or the S_{ar} shall be stated and their effects explained.

For a PDDB with test input the manufacturer shall define:

a) the behaviour of the OSSD(s) during test;

b) input(s) and/or output(s) for external test.

6 Normal service, mounting and transport conditions

6.1 Normal service conditions

Subclause 6.1 of IEC 60947-5-2:2007 applies.

6.2 Conditions during transport and storage

Subclause 6.2 of IEC 60947-5-2:2007 applies.

6.3 Mounting

Mounting dimensions and conditions shall be specified by the manufacturer.

7 Constructional and performance requirements

7.1 Constructional requirements

7.1.1 Materials

Subclause 7.1.1 of IEC 60947-5-2:2007 applies.

7.1.2 Current-carrying parts and their connections

Subclause 7.1.2 of IEC 60947-5-2:2007 applies.

7.1.3 Clearance and creepage distances

Subclause 7.1.3 of IEC 60947-5-2:2007 applies.

7.1.4 Vacant

7.1.5 Vacant

7.1.6 Vacant

7.1.7 Terminals

7.1.7.1 Constructional requirements

Subclause 7.1.7.1 of IEC 60947-5-2:2007 applies.

7.1.7.2 Connecting capacity

Subclause 7.1.7.2 of IEC 60947-5-2:2007 applies.

7.1.7.3 Connection means

Subclause 7.1.7.3 of IEC 60947-5-2:2007, Amendment 1 (2012) applies.

7.1.7.4 Connection identification and marking

Subclause 7.1.7.4 of IEC 60947-5-2:2007, Amendment 1 (2012) applies, with the following additions.

PDDBs with integrally connected cables shall have wires identified with colours in accordance with 7.1.7.4 of IEC 60947-5-2:2007, Amendment 1 (2012).

7.1.8 Provision for protective earthing

Subclause 7.1.9 of IEC 60947-5-2:2007 applies, with the following additions.

PDDB parts having Class II or Class III protection shall have no connection for protective earthing.

7.1.9 IP degree of protection (in accordance with IEC 60529)

The sensing means of a PDDB shall have minimum IP65 protection.

Control and monitoring devices shall have minimum IP54 protection.

Control and monitoring devices which are designed to be mounted in a housing with a minimum degree of protection of IP54 may have a lower protection degree.

7.2 Functional safety management

Functional safety management shall be implemented as appropriate for the PDDB lifecycle**.** This may be achieved for example by the use of Clause 6 of IEC 61508-1:2010 or appropriate sector standards.

7.3 Functional requirements specification for SRCFs

7.3.1 General

The functional requirements specification for PDDB shall describe details of each SRCF to be performed including, as applicable:

a) a description of the SRCF;

b) the frequency of operation;

c) the required risk time;

d) the interface(s) of the PDDB;

e) a description of fault reaction function(s);

f) a description of the required operating environment for the PDDB (e.g. temperature, humidity, dust, chemical substances, mechanical vibration and shock);

g) tests and any associated facilities (e.g. test equipment, test access ports);

h) rate of operating cycles, duty cycle, and/or utilisation category, for PDDBs that incorporate electromechanical devices.

7.3.2 Safety integrity requirements specification for SRCFs

The safety integrity requirements for a PDDB with a given architecture shall include:

a) SIL claim limit or PL (category);

b) reliability data.

7.3.3 Electromagnetic compatibility

7.3.3.1 General

In addition to the EMC requirements of IEC 60947-5-2, this part specifies additional requirements for devices intended to perform safety functions as defined in IEC 61508 series and derived standards. These additional requirements apply only to the safety related function of the device. These devices, if d.c. powered, shall not be connected to a d.c. distribution network. EMC performance requirements for PDDBs are listed in Table 1.

7.3.3.2 Performance Criteria FS (fail safe)

The functions of the PDDB intended for safety applications are not affected outside their specification or may be disturbed temporarily or permanently if the PDDB reacts on this disturbance in such a way that an OFF-state of the output is maintained or achieved within a stated time and maintained. Destruction of components is allowed if a defined state of the EUT (equipment under test) is achieved within a stated time and maintained.

7.3.3.3 Use of external devices

Where immunity to certain EM phenomena can only be achieved by the use of external devices then those devices are considered for the purposes of this International Standard to be part of the PDDB and the type and installation requirements for these devices shall be stated in the manufacturer's documentation. If particular installation requirements are necessary to achieve the required functional safety performance (for example, installation in accordance with IEC 60204-1) these requirements shall be stated in the manufacturer's documentation. The input power ports of d.c. proximity device(s) that are PELV or SELV powered are not considered as connected to a d.c. distribution network and instead are treated as I/O signal/control ports.

Table 1 – EMC requirements for PDDBs

Port	Phenomenon	Basic standard	Test value	Performance criterion
Enclosure	Electrostatic discharge (ESD)	IEC 61000-4-2	6 kV contact discharge [a] 8 kV air discharge [a]	FS FS
	EM field	IEC 61000-4-3	20 V/m (80 MHz to 1 GHz) 10 V/m (1,4 GHz to 2 GHz) 3 V/m (2,0 GHz to 2,7 GHz)	FS FS FS
	Power frequency magnetic field	IEC 61000-4-8	30 A/m (50 Hz, 60 Hz) [b]	FS
A.C. power (including protective earth)	Burst	IEC 61000-4-4	3 kV (5/50 ns, 5 kHz) [c]	FS
	Surge	IEC 61000-4-5	2 kV line to line [d] 4 kV line to earth [d]	FS FS
	Conducted RF	IEC 61000-4-6	10 V (150 kHz to 80 MHz)	FS
	Voltage dip	IEC 61000-4-11	0 % during 1 cycle 40 % during 10/12 cycles [e] 70 % during 25/30 cycles [e]	FS FS FS
	Short interruptions	IEC 61000-4-11	0 % during 250/300 cycles [e]	FS
D.C. power [f] (including protective earth)	Burst	IEC 61000-4-4	2 kV (5/50 ns, 5 kHz) [c]	FS
	Surge	IEC 61000-4-5	2 kV line to earth [d]	FS
	Conducted RF	IEC 61000-4-6	10 V (150 kHz to 80 MHz)	FS
I/O signal / control	Burst	IEC 61000-4-4	2 kV (5/50 ns, 5 kHz) [c]	FS
	Surge [g]	IEC 61000-4-5	2 kV line to earth [d]	FS
	Conducted RF	IEC 61000-4-6	10 V (150 kHz to 80 MHz)	FS
Functional earth	Burst [h]	IEC 61000-4-4	2 kV (5/50 ns, 5 kHz) [c]	FS

[a]	For equipment intended to be used in SIL 3 applications the number of discharges at the highest level shall be increased by a factor of 3 compared to the number as given in the basic standard.
[b]	Only to magnetically sensitive equipment. CRT display interference is allowed above 1 A/m.
[c]	For equipment intended to be used in SIL 3 applications, the duration of the test at the highest level shall be increased by a factor of 5 compared to the duration as given in the basic standard.
[d]	For equipment intended to be used in SIL 3 applications, the number of pulses at the highest level shall be increased by a factor of 3 compared to the number as given in the basic standard.
[e]	For example “25/30 cycles" means "25 cycles for 50 Hz test" or "30 cycles for 60 Hz test”.
[f]	D.C. connections between parts of equipment/system which are not connected to a d.c. distribution network are treated as I/O signal/control ports.
[g]	Only in the case of lines > 30 m.
[h]	Only in the case of lines > 3 m.

7.3.4 Design and development of PDDB

The PDDB shall be designed and validated in accordance with its safety requirements specification and the requirements of IEC 61508 series, IEC 62061, or ISO 13849-1 as appropriate. The requirements for systematic safety integrity (systematic capability), shall be met by following compliance Route 1_H or 2_H (see 7.4.4.3 of IEC 61508-2:2010) and 1_S or 2_S (in accordance with 7.4.2.12 of IEC 61508-3:2010, as appropriate).

NOTE In IEC 62061:2005, Amendment 1(2012) (Scope, Note 2) it is considered that Route 2_H is not suitable for general machinery applications.

7.4 Information for use

7.4.1 Objective

Information shall be provided to enable the user to develop procedures to ensure that the required functional safety of the PDDB is maintained during use and maintenance of the equipment under control.

7.4.2 Documentation for installation, use and maintenance

The documentation shall provide information for installation, use and maintenance of the PDDB. This shall take the form of a safety manual in accordance with Annex D of IEC 61508-2:2010, including:

– comprehensive description of the PDDB, installation and mounting;
– statement of the intended use of the PDDB and any measures that can be necessary to prevent reasonably foreseeable misuse;
– information on the physical environment (e.g. lighting, vibration, noise levels, atmospheric contaminants) where appropriate;
– connection diagram(s);
– useful lifetime;
– proof test interval where relevant;
– parameterization information, where relevant;
– description of the maintenance requirements applicable to the PDDB if any;
– specification for periodic testing, preventive maintenance and corrective maintenance.

NOTE 1 Periodic tests are those functional tests necessary to confirm correct operation and to detect faults. They mean a comprehensive description of periodical test principles like diagnostic test and / or proof test.

NOTE 2 Preventive maintenance is the measures necessary, if any, to maintain the required performance of the PDDB.

NOTE 3 Corrective maintenance includes the measures, if any, taken after the occurrence of specific fault(s) that are necessary to bring the PDDB back into the as-designed state.

8 Tests

8.1 Kind of tests

8.1.1 General

Subclause 8.1.1 of IEC 60947-1:2007 applies.

8.1.2 Type tests

Subclause 8.1.2 of IEC 60947-5-2:2007 applies, with the following addition.

- performance under fault conditions.

8.1.3 Routine tests

Subclause 8.1.3 of IEC 60947-5-2:2007 applies.

8.1.4 Sampling tests

Subclause 8.1.4 of IEC 60947-1:2007 applies.

8.2 Compliance with constructional requirements

Subclause 8.2 of IEC 60947-1:2007, Amendment 1 (2010) applies where applicable.

8.3 Performances

8.3.1 Test sequences

Subclause 8.3.1 of IEC 60947-5-2:2007 applies.

8.3.2 General test conditions

8.3.2.1 General requirements

Subclause 8.3.2.1 of IEC 60947-5-2:2007 applies where applicable.

8.3.2.2 Test quantities

Subclause 8.3.2.2 of IEC 60947-1:2007 applies.

8.3.2.3 Test reports

Subclause 8.3.2.4 of IEC 60947-1:2007 applies.

8.3.3 Performances under no load, normal and abnormal load conditions

8.3.3.1 Operation

Subclause 8.3.3.1 of IEC 60947-1:2007 applies.

8.3.3.2 Operating limits

Subclause 8.3.3.2 of IEC 60947-5-2:2007 applies.

8.3.3.3 Temperature rise

Subclause 8.3.3.3 of IEC 60947-5-2:2007 applies.

8.3.3.4 Dielectric properties

Subclause 8.3.3.4 of IEC 60947-5-2:2007 applies.

8.3.3.5 Making and breaking capacities

8.3.3.5.1 General

Subclause 8.3.3.5 of IEC 60947-5-1:2003 and IEC 60947-5-2:2007 apply where appropriate.

8.3.3.5.2 Evaluation

During the tests no electrical or mechanical faults shall occur, no contact shall weld, no extended arcing time shall occur and no fuse shall melt. The conducted switching overvoltages shall not exceed the rated impulse withstand voltage, and the assured operating and release distances according to 2.6.4 and 2.6.5 shall remain within the stated limits.

8.3.4 Performances under short-circuit current conditions

Subclause 8.3.4 of IEC 60947-5-1:2003 and IEC 60947-5-2:2007, Amendment 1 (2012) apply where appropriate.

8.4 Verification of operating distances

The PDDB shall be tested under the rated ambient air temperature as well as maximum and minimum temperature limits stated by the manufacturer with the highest operational voltage and the rated operational current at the output switching element until the thermal equilibrium is reached.

The tests shall be in accordance with IEC 60068-2-1 and IEC 60068-2-30 test method B.

Following the temperature tests, the assured operating and release distances shall be measured in accordance with 8.4 of IEC 60947-5-2:2007 and shall be within the manufacturer's specifications.

8.5 Verification of resistance to vibration and shock

The tests shall be performed in accordance with 7.4 of IEC 60947-5-2:2007, except for separate control and monitoring devices. During each test, the state of the output(s) shall not change.

The tests shall be performed in accordance with 6.3.5 of IEC 61131-2:2007 for separate control and monitoring devices, and the following addition.

During each test, the state of the output(s) shall not change.

8.6 Verification of electromagnetic compatibility

The test shall be performed in accordance with 7.2.6 of IEC 60947-5-2:2007. In addition, the S_{ar} and S_{ao} shall be verified after test.

9 Modification

9.1 Objective

This clause specifies the modification procedure(s) to be applied when modifying the PDDB during design, integration and validation.

9.2 Modification procedure

Subclause 7.16 of IEC 61508-1:2010 shall apply.

Excerpt of 7.16.2.2 of IEC 61508-1:2010:

NOTE The reason for the request for the modification could arise from, for example:

a) functional safety below that specified;

b) systematic fault experience;

c) new or amended safety legislation;

d) modifications to the EUC (Equipment Under Control) or its use;

e) modification to the overall safety requirements;

f) analysis of operations and maintenance performance, indicating that the performance is below target;

g) routine functional safety audits.

Annex A
(informative)

Example of a simple control system in accordance with IEC 61511 series

A.1 Description

Overfill detection using a level control device and a valve (see Figure A.1). The equipment is situated in a hazardous area (flammable atmosphere) and is to be protected in accordance with the requirements of:

– level detection device: Zone 0/Division 1;
– control valve: Zone 2/Division 2.

A.2 Safety requirements specification

A.2.1 Functional requirements

In case of overfilling, the control valve is to be closed.

A.2.2 Safety integrity requirements

The risk assessment showed that a SIL 2 is appropriate for that function.

A.2.3 Conditions of use

Low demand mode (not more than one safety function demand / year).

Repair time for detected failures 8 hours.

Test interval 12 months.

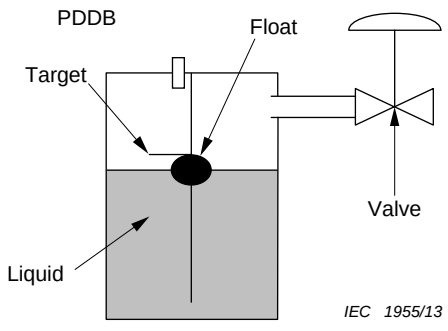

Figure A.1 – Representation of the equipment under control

NOTE There are many other requirements stated in the specification such as quality of the power supply, conditions for live maintenance etc.

A.3 Realisation

In this example the safety function will be performed by:

- a proximity switch for the float sensor (for example with an output in accordance with IEC 60947-5-6);
- an isolated switch amplifier with a relay output;
- a solenoid driver;

NOTE Since the power at the output of the intrinsically safe solenoid driver is too low to power the ball valve, in this example it is necessary to insert a control valve.

- a control valve;
- a ball valve.

A.4 Collection of data

The collection of reliability and structure data of each component to be considered in this example of control system is described in the following Table A.1.

Table A.1 – Collection of reliability and structure data

Sensor: Inductive proximity device in accordance with IEC 60947-5-6	**Isolated switch amplifier: Isolated intrinsically-safe switching amplifier**	**Solenoid driver: Solenoid driver with intrinsically-safe output**	**Control valve: intrinsically-safe control valve**	**Ball valve: Generic**
SIL Claim Limit with respect to architectural constraints: 2 in a one channel configuration	SIL Claim Limit with respect to architectural constraints: 2 in a one channel configuration	SIL Claim Limit with respect to architectural constraints: 3 in a one channel configuration	SIL Claim Limit with respect to architectural constraints: 3 in a one channel configuration	SIL Claim Limit with respect to architectural constraints: 1 in a one channel configuration
SFF = 94,09 %	SFF = 91,62 %	SFF = 100 %	SFF = 99 %	SFF = 50 %
Failure rates:	Failure rates:	Failure rates:	Failure rates:	Failure rates:
λ_{DU} = 3,9 FIT	λ_{DU} = 19 FIT	λ_{DU} = 0 FIT	λ_{DU} = 0 FIT	λ_{DU} = 60 FIT
λ_{S} = 62,1 FIT	λ_{S} = 208 FIT	λ_{S} = 1,3 FIT	λ_{S} = 0 FIT	λ_{S} = 60 FIT

All the components except the ball valve (structure only up to SIL 1, SFF less than 90 %) can be used in a safety related function up to SIL 2 in accordance with Table 2 of IEC 61508-2:2010. As a consequence, the output channel (solenoid driver, control valve and ball valve) should have a redundant architecture as shown in Figure A.2.

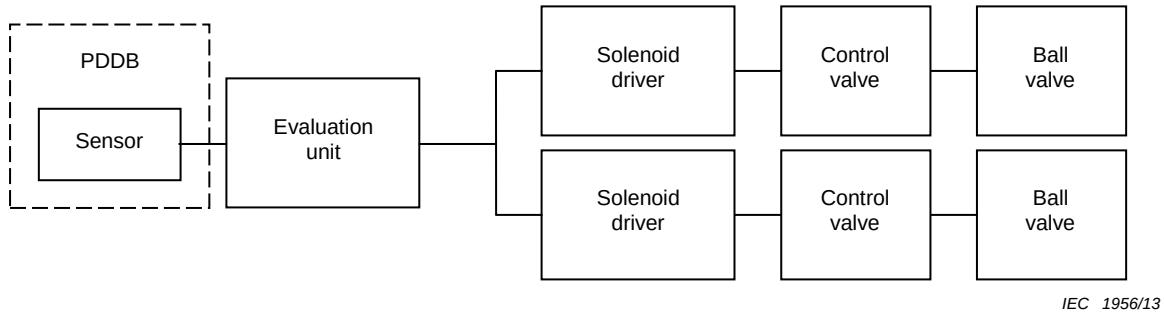

Figure A.2 – Architecture of the safety related function

Input subsystem (sensor and evaluation unit)

$\Sigma\lambda_{DU}$ = 3,9 FIT + 19 FIT = 22,9 FIT

$\Sigma\lambda_{safe}$ = 62,1 FIT + 208 FIT = 270,1 FIT

Calculation of the PFD of the input subsystem using the formulae of IEC 61508-6:2010, B.3.2.2.1:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR}$$

$$\text{PFD}_G = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

$\text{PFD}_{\text{input channel}}$ = 3,75 10^{-3}

Output subsystem (solenoid drivers and valves)

$\Sigma\lambda_{DU}$ 1 channel = 0 + 0 + 60 = 60 FIT

$\Sigma\lambda_{safe}$ 1 channel = 1,3 + 0 +60 = 61,3 FIT

MTTR = MRT = 8 h under the assumption that the time to detect a dangerous failure is far smaller than the MRT (at least one order of magnitude).

Calculations of the resulting PFD of the output subsystem using the formulae of IEC 61508-6:2010, B.3.2.2.2 and assuming a common cause failure contribution of 10 %:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR}$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR}$$

$$\text{PFD}_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE}\, t_{GE} + \beta_D\lambda_{DD}\text{MTTR} + \beta\lambda_{DU}\left(\frac{T_1}{2} + \text{MRT}\right)$$

$\text{PFD}_{\text{output channel}}$ = 2,72 10^{-6}

$\text{PFD}_{\text{total}}$ = $\text{PFD}_{\text{input channel}}$ + $\text{PFD}_{\text{output channel}}$ = 3,75 10^{-3} which is within the range allowed for SIL 2 (Table 2 of IEC 61508-1:2010)

Results of the calculation:

SIL according to the PFD: SIL 2

A.5 Results

SIL according to the architecture: SIL 2

SIL according to the PFD: SIL 2

SIL of the safety function: SIL 2

Bibliography

IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*
Amendment 1:1999
Amendment 2:2002

IEC 60050-441:1984, *International Electrotechnical Vocabulary (IEV) – Chapter 441: Switchgear, controlgear and fuses*
Amendment 1:2000

IEC 60068-2-6:2007, *Environmental testing – Part 2-6: Tests – Test Fc: Vibration (sinusoidal)*

IEC 60068-2-14:2009, *Environmental testing – Part 2-14: Tests – Test N: Change of temperature*

IEC 60068-2-27:2008, *Environmental testing – Part 2-27: Tests – Test Ea and guidance: Shock*

IEC 60204-1:2005, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*
Amendment 1:2008

IEC 60364 (all parts), *Low-voltage electrical installations*

IEC 60445:2010, *Basic and safety principles for man-machine interface, marking and identification – Identification of equipment terminals, conductor terminations and conductors*

IEC 60947-5-6:1999, *Low-voltage switchgear and controlgear – Part 5-6: Control circuit devices and switching elements – DC interface for proximity sensors and switching amplifiers (NAMUR)*

IEC 61000-3-2:2005, *Electromagnetic compatibility (EMC) – Part 3-2: Limits – Limits for harmonic current emissions (equipment input current ≤ 16 A per phase)*
Amendment 1:2008
Amendment 2:2009

IEC 61000-3-3:2008, *Electromagnetic compatibility (EMC) – Part 3-3: Limits – Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems, for equipment with rated current ≤16 A per phase and not subject to conditional connection*

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*
Amendment 1:2009

IEC 61140:2001, *Protection against electric shock – Common aspects for installation and equipment*
Amendment 1:2004

IEC 61165:2006, *Application of Markov techniques*

IEC 61326-3-1:2008, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications*

IEC 61496-1:2012, *Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests*

IEC 61496-2:2013, *Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs)*

IEC 61496-3:2008, *Safety of machinery – Electro-sensitive protective equipment – Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR)*

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 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61511-1:2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

IEC 61511-2:2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1*

IEC 61511-3:2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

IEC/TR 62380:2004, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*

CISPR 11:2009, *Industrial, scientific and medical equipment – Radio-frequency disturbance characteristics – Limits and methods of measurement*
Amendment 1:2010

ISO 14119:1998, *Safety of machinery – Interlocking devices associated with guards – Principles for design and selection*
Amendment 1:2007

SOMMAIRE

AVANT-PROPOS 32
1 Généralités 34
1.1 Domaine d'application 34
1.2 Références normatives 34
2 Termes, définitions et abréviations 36
2.1 Généralités 36
2.2 Index alphabétique des termes 36
2.3 Termes et définitions de base 37
2.4 Termes et définitions concernant les contraintes architecturales 40
2.5 Termes et définitions concernant les parties d'un PDDB 42
2.6 Termes et définitions concernant le fonctionnement d'un PDDB 42
2.7 Symboles et abréviations 43
3 Classification 43
4 Caractéristiques 43
4.1 Généralités 43
4.2 Caractéristiques de construction 43
4.2.1 Dispositif de détection de proximité à comportement défini 43
4.2.2 Cible spécifiée 44
5 Informations sur le matériel 44
5.1 Nature des informations 44
5.2 Identification 44
5.3 Marquage 44
5.3.1 Généralités 44
5.3.2 Identification des raccordements et marquage 44
5.4 Instructions pour l'installation, le fonctionnement et l'entretien 45
6 Conditions normales de service, de montage et de transport 45
6.1 Conditions normales de service 45
6.2 Conditions pendant le transport et le stockage 45
6.3 Montage 45
7 Dispositions relatives à la construction et au fonctionnement 45
7.1 Dispositions constructives 45
7.1.1 Matériaux 45
7.1.2 Parties transportant le courant et leurs connexions 45
7.1.3 Distances d'isolement et lignes de fuite 45
7.1.4 Disponible 45
7.1.5 Disponible 45
7.1.6 Disponible 45
7.1.7 Bornes 45
7.1.8 Dispositions pour mise à la terre 46
7.1.9 Degré de protection IP (conformément à la CEI 60529) 46
7.2 Gestion de la sécurité fonctionnelle 46
7.3 Spécification d'exigences de fonctionnement pour les SRCF 46
7.3.1 Généralités 46
7.3.2 Spécification d'exigences d'intégrité de sécurité pour les SRCF 47
7.3.3 Compatibilité électromagnétique 47
7.3.4 Conception et développement de PDDB 48

7.4 Informations d'utilisation 49
7.4.1 Objectif 49
7.4.2 Documentation pour l'installation, l'utilisation et la maintenance 49
8 Essais 49
8.1 Nature des essais 49
8.1.1 Généralités 49
8.1.2 Essais de type 49
8.1.3 Essais individuels de série 49
8.1.4 Essais sur prélèvement 49
8.2 Conformité aux dispositions de construction 50
8.3 Fonctionnement 50
8.3.1 Séquences d'essais 50
8.3.2 Conditions générales d'essai 50
8.3.3 Performances à vide et dans les conditions de charge normales et anormales 50
8.3.4 Performances en conditions de court-circuit 51
8.4 Vérification des portées de travail 51
8.5 Vérification de la résistance aux vibrations et aux chocs 51
8.6 Vérification de la compatibilité électromagnétique 51
9 Modification 51
9.1 Objectif 51
9.2 Procédure de modification 51
Annexe A (informative) Exemple d'un système de commande unique conforme à la série CEI 61511 52
Bibliographie 56

Figure A.1 – Représentation de l'équipement sous contrôle 52
Figure A.2 – Architecture de la fonction relative à la sécurité 53

Tableau 1 – Exigences relatives à la CEM pour les PDDB 48
Tableau A.1 – Collecte des données de fiabilité et de structure 53

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

APPAREILLAGE À BASSE TENSION –

Partie 5-3: Appareils et éléments de commutation pour circuits de commande – Exigences pour dispositifs de détection de proximité à comportement défini dans des conditions de défaut (PDDB)

AVANT-PROPOS

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

La Norme internationale CEI 60947-5-3 a été établie par le sous-comité 17B: Appareillage à basse tension, du comité d'études 17 de la CEI: Appareillage.

Cette deuxième édition remplace la première édition publiée en 1999 et son amendement publié en 2005. Il s'agit d'une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) principes généraux de la série CEI 61508;
b) classification selon les exigences de la CEI 62061;
c) classification selon l'ISO 13849-1.

La présente norme doit être lue conjointement avec la CEI 60947-1, *Appareillage à basse tension – Partie 1: Règles générales* et la CEI 60947-5-2, *Appareillage à basse tension – Partie 5-2: Appareils et éléments de commutation pour circuits de commande – Détecteurs de proximité*. Les dispositions de la Partie 1 et de la Partie 5-2 sont seulement applicables à la présente norme lorsqu'il y est spécifiquement fait référence. La numérotation des paragraphes de la présente norme n'est parfois pas continue car elle se fonde sur la numérotation des paragraphes de la CEI 60947-1 et de la CEI 60947-5-2.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
17B/1821/FDIS	17B/1826/RVD

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

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

Une liste de toutes les parties de la série CEI 60947, publiées sous le titre général *Appareillage à basse tension*, peut être consultée sur le site web de la CEI.

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

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

APPAREILLAGE À BASSE TENSION –

Partie 5-3: Appareils et éléments de commutation pour circuits de commande – Exigences pour dispositifs de détection de proximité à comportement défini dans des conditions de défaut (PDDB)

1 Généralités

1.1 Domaine d'application

La présente partie de la série CEI 60947 fournit des exigences supplémentaires à celles énoncées dans la CEI 60947-5-2. Elle couvre les aspects de défaut des dispositifs de détection de proximité à comportement défini (PDDB) dans les conditions de défaut. Elle ne couvre aucune autre fonctionnalité qui peut être requise pour des applications spécifiques.

La présente norme ne couvre pas les dispositifs avec sortie analogique.

La présente norme ne traite pas des exigences spécifiques concernant le bruit acoustique dans la mesure où l'émission de bruit par les appareils et éléments de commutation pour circuits de commande n'est pas considérée comme un phénomène dangereux.

Pour un PDDB utilisé dans des applications pour lesquelles des caractéristiques supplémentaires, couvertes par d'autres normes, sont requises, les exigences de toutes les normes correspondantes s'appliquent.

L'utilisation de la présente norme seule ne constitue pas une preuve de son adéquation pour une mise en œuvre de toute fonctionnalité spécifique relative à la sécurité. Plus particulièrement, la présente norme ne fournit aucune exigence en matière de caractéristiques de manœuvre d'un PDDB ou de moyens visant à réduire les effets de l'interférence mutuelle entre dispositifs, par exemple des cibles codées. Aussi, ces exigences ainsi que toutes les autres spécifiques à une application doivent être prises en considération en complément des exigences de la présente norme.

NOTE 1 En raison de leur comportement dans des conditions de défaut, les PDDB peuvent, par exemple, être utilisés en tant que dispositifs de verrouillage (voir l'ISO 14119).

NOTE 2 Les exigences en matière d'équipements de protection électro-sensibles pour la détection de personnes sont indiquées dans la série CEI 61496.

1.2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60068-2-1:2007, *Essais d'environnement – Partie 2-1: Essais – Essai A: Froid*

CEI 60068-2-30:2005, *Essais d'environnement – Partie 2-30: Essais – Essai Db: Essai cyclique de chaleur humide (cycle de 12 h + 12 h)*

CEI 60529:1989, *Degrés de protection procurés par les enveloppes (Code IP)*
Amendement 1:1999

CEI 60947-1:2007, *Appareillage à basse tension – Partie 1: Règles générales*
Amendement 1:2010

CEI 60947-5-1:2003, *Appareillage à basse tension – Partie 5-1: Appareils et éléments de commutation pour circuits de commande – Appareils électromécaniques pour circuits de commande*
Amendement 1:2009

CEI 60947-5-2:2007, *Appareillage à basse tension – Partie 5-2: Appareils et éléments de commutation pour circuits de commande – Détecteurs de proximité*
Amendement 1:2012

CEI 61000-4-2:2008, *Compatibilité électromagnétique (CEM) – Partie 4-2: Techniques d'essai et de mesure – Essai d'immunité aux décharges électrostatiques*

CEI 61000-4-3:2006, *Compatibilité électromagnétique (CEM) – Partie 4-3: Techniques d'essai et de mesure – Essai d'immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques*
Amendement 1:2007
Amendement 2:2010

CEI 61000-4-4:2012, *Compatibilité électromagnétique (CEM) – Partie 4-4: Techniques d'essai et de mesure – Essai d'immunité aux transitoires électriques rapides en salves*

CEI 61000-4-5:2005, *Compatibilité électromagnétique (CEM) – Partie 4-5: Techniques d'essai et de mesure – Essai d'immunité aux ondes de choc*

CEI 61000-4-6:2008, *Compatibilité électromagnétique (CEM) – Partie 4-6: Techniques d'essai et de mesure – Immunité aux perturbations conduites, induites par les champs radioélectriques*

CEI 61000-4-8:2009, *Compatibilité électromagnétique (CEM) – Partie 4-8: Techniques d'essai et de mesure – Essai d'immunité au champ magnétique à la fréquence du réseau*

CEI 61000-4-11:2004, *Compatibilité électromagnétique (CEM) – Partie 4-11: Techniques d'essai et de mesure – Essais d'immunité aux creux de tension, coupures brèves et variations de tension*

CEI 61131-2:2007, *Automates programmables – Partie 2: Exigences et essais des équipements*

CEI 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

CEI 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

CEI 62061:2005, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*
Amendement 1:2012

ISO 13849-1:2006, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

2 Termes, définitions et abréviations

2.1 Généralités

Pour les besoins du présent document, les termes et définitions donnés dans la CEI 60947-1 et la CEI 60947-5-2, ainsi que les termes, définitions et abréviations suivants s'appliquent.

2.2 Index alphabétique des termes

Référence

A

appareil de commande et de surveillance 2.5.3
appareil de commutation du signal de sortie [OSSD] 2.5.2

C

comportement défini (du PDDB) 2.6.1
composant complexe 2.3.4
composant de faible complexité 2.3.3
couverture du diagnostic [DC] 2.4.2

D

défaillance (de matériel) 2.3.5
défaillance dangereuse 2.3.6
défaillance en sécurité 2.3.7
défaut 2.3.8

E

équipement sous contrôle [EUC] 2.4.7
essai périodique 2.4.5
état bloqué 2.6.2
état passant 2.6.3
état verrouillé 2.6.8

F

fonction de commande relative à la sécurité [SRCF] 2.3.9
fraction de défaillance en sécurité [SFF] 2.4.1

I

intégrité de sécurité 2.3.10
intégrité de sécurité du logiciel 2.3.12
intégrité de sécurité du matériel 2.3.11
intégrité de sécurité systématique 2.3.13
intervalle d'essais de diagnostic 2.4.4

L

limite de revendications SIL [SILCL] 2.3.16

M

mesure cible des défaillances 2.3.15
mode de fonctionnement 2.3.14

moyen de détection 2.5.1

N

niveau d'intégrité de sécurité [SIL] 2.3.2
niveau de performance [PL] 2.3.1

P

portée de travail assurée [S_{ao}] d'un PDDB 2.6.4
portée de déclenchement assurée [S_{ar}] d'un PDDB 2.6.5

S

système relatif à la sécurité 2.4.6

T

temps de risque 2.6.6
temps moyen avant défaillance dangereuse [$MTTF_d$] 2.3.17
temps de la mission [T_M] 2.6.7
tolérance du défaut de matériel [HFT] 2.4.3

2.3 Termes et définitions de base

2.3.1
niveau de performance
PL
niveau discret (de a à e) utilisé pour spécifier la capacité des parties des systèmes de commandes relatives à la sécurité à réaliser leur fonction de sécurité dans des conditions prévisibles

[SOURCE: ISO 13849-1:2006, 3.1.23, modifiée – mise à jour de la définition]

2.3.2
niveau d'intégrité de sécurité
SIL
niveau discret (parmi trois possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de commande relatives à la sécurité à allouer aux parties relatives à la sécurité du système de contrôle, le niveau 3 d'intégrité de sécurité possédant le plus haut degré d'intégrité et le niveau 1 possédant le plus bas

Note 1 à l'article: SIL 4 n'est pas pris en considération dans la présente norme. Pour connaître les exigences applicables à SIL 4, consultez la série CEI 61508.

[SOURCE: CEI 62061:2005, 3.2.23, modifiée – mise à jour de la note]

2.3.3
composant de faible complexité
composant dans lequel:

– les modes de défaillance sont bien définis; et
– le comportement en conditions de défaut peut être complètement déterminé

Note 1 à l'article: Le comportement du composant de faible complexité dans des conditions de défaut peut être déterminé par des méthodes analytiques et/ou d'essai.

Note 2 à l'article: Un sous-système ou un élément de sous-système qui comprend un ou plusieurs interrupteurs de fin de course, faisant fonctionner, éventuellement via des relais électromécaniques interposés, un ou plusieurs contacteurs destinés à couper l'alimentation de moteurs électriques est un exemple de composant de faible complexité.

[SOURCE: CEI 62061:2005, 3.2.7]

2.3.4
composant complexe
composant dans lequel:

– les modes de défaillance ne sont pas bien définis; ou
– le comportement en conditions de défaut ne peut être complètement déterminé

[SOURCE: CEI 62061:2005, 3.2.8]

2.3.5
défaillance
cessation de l'aptitude d'une entité à accomplir une fonction requise

Note 1 à l'article: Après défaillance, le système a un défaut.

Note 2 à l'article: Une «défaillance» est un événement, par opposition à un «défaut» qui est un état.

Note 3 à l'article: La notion de défaillance, telle qu'elle est définie, ne s'applique pas à une entité constituée uniquement de logiciel.

[SOURCE: CEI 60050-191:1990, 191-04-01, modifiée – mise à jour de la deuxième note]

2.3.6
défaillance dangereuse
défaillance d'un PDDB qui a la potentialité de provoquer un phénomène dangereux ou un état de non-fonctionnement

[SOURCE: CEI 62061:2005, 3.2.40, modifiée – suppression des notes]

2.3.7
défaillance en sécurité
défaillance d'un PDDB qui n'a pas la potentialité de provoquer un phénomène dangereux

[SOURCE: CEI 62061:2005, 3.2.41 modifiée – mise à jour de la définition]

2.3.8
défaut
état d'une entité inapte à accomplir une fonction requise, en excluant l'inaptitude due à la maintenance préventive ou à d'autres actions programmées, ou due à un manque de moyens extérieurs

Note 1 à l'article: Un défaut est souvent le résultat de l'élément lui-même, mais peut exister sans défaillance antérieure.

Note 2 à l'article: En anglais, le terme «fault» (défaut) et sa définition sont identiques à ceux donnés dans la CEI 60050-191:1990, 191-05-01. Dans le domaine des machines, le terme «défaut» en français et le terme «Fehler» en allemand sont préférés aux termes «pannes» et «Fehlzustand», qui sont donnés avec la même définition.

[SOURCE: CEI 62061:2005, 3.2.30, modifiée – nouvelle définition et nouvelles notes]

2.3.9
fonction de commande relative à la sécurité
SRCF
fonction de commande avec un niveau d'intégrité spécifié, partiellement ou complètement mise en œuvre par un PDDB et prévue pour maintenir la condition de sécurité de l'équipement sous contrôle ou empêcher un accroissement immédiat du(des) risque(s)

Note 1 à l'article: L'ISO 13849-1 emploie le terme «SRF» (fonction relative à la sécurité), la série CEI 61508 emploie «SF» (fonction de sécurité), Termes et définitions concernant l'intégrité.

[SOURCE: CEI 62061:2005, 3.2.16 modifiée – nouvelle définition et nouvelle note]

2.3.10
intégrité de sécurité
probabilité selon laquelle un système de commande relatif à la sécurité ou son PDDB exécutera de manière satisfaisante les fonctions de commande relatives à la sécurité requises dans toutes les conditions spécifiées

[SOURCE: CEI 62061:2005, 3.2.19, modifiée – mise à jour de la définition et suppression des notes]

2.3.11
intégrité de sécurité du matériel
partie de l'intégrité de sécurité d'un système de commande relatif à la sécurité ou de son PDDB comprenant les exigences relatives à la fois à la probabilité de défaillance aléatoire du matériel et de contraintes architecturales

[SOURCE: CEI 62061:2005, 3.2.20, modifiée – mise à jour de la définition]

2.3.12
intégrité de sécurité du logiciel
partie de l'intégrité de sécurité d'un PDDB liée à des défaillances systématiques dans un mode de défaillance dangereux imputables au logiciel

Note 1 à l'article: L'intégrité de sécurité du logiciel ne peut habituellement pas être quantifiée de manière précise.

[SOURCE: CEI 61508-4:2010, 3.5.5, modifiée – mise à jour de la définition et ajout d'une nouvelle note]

2.3.13
intégrité de sécurité systématique
partie de l'intégrité de sécurité d'un PDDB liée à des défaillances systématiques dans un mode de défaillance dangereux

Note 1 à l'article: L'intégrité de sécurité systématique ne peut habituellement être quantifiée (à l'inverse de l'intégrité de sécurité du matériel, qui peut l'être).

Note 2 à l'article: Les exigences pour l'intégrité de sécurité systématique s'appliquent aux deux aspects (matériel et logiciel) d'un PDDB.

[SOURCE: CEI 61508-4:2010, 3.5.6, modifiée – mise à jour de la définition et ajout d'une nouvelle note]

2.3.14
mode de fonctionnement
mode de fonctionnement d'une fonction de sécurité qui peut être:

– **mode à faible sollicitation**: la fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et où la fréquence des sollicitations n'est pas supérieure à une par an, ou

Note 1 à l'article: Le système E/E/PE relatif à la sécurité qui réalise la fonction de sécurité n'a généralement pas d'influence sur l'EUC ou son système de commande jusqu'à l'occurrence d'une sollicitation. Cependant, si le système E/E/PE relatif à la sécurité n'est plus en mesure de réaliser la fonction de sécurité du fait d'une défaillance, il peut alors faire passer l'EUC à un état de sécurité.

– **mode à forte sollicitation**: la fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et où la fréquence des sollicitations est supérieure à une par an, ou
– **mode continu**: la fonction de sécurité maintient l'EUC dans un état de sécurité en fonctionnement normal

[SOURCE: CEI 61508-4:2010, 3.5.16, modifiée – mise à jour de la note]

2.3.15
mesure cible des défaillances
probabilité prévue de défaillance dans un mode de défaillances dangereuses à atteindre conformément aux exigences d'intégrité de sécurité; exprimée de deux manières, indiquées ci-dessous:

– probabilité moyenne de défaillance dangereuse lors de l'exécution de la fonction nominale à la demande PFD_{avg} (pour un mode de fonctionnement à faible demande);
– fréquence moyenne de défaillance dangereuse pendant un laps de temps donné PFH_D (pour un mode de fonctionnement à forte demande ou continu)

Note 1 à l'article: Le terme «probabilité de défaillance dangereuse par heure» n'est pas utilisé dans la présente norme, mais l'abréviation PFH a été conservée, mais elle signifie, lorsqu'utilisée, «fréquence moyenne de défaillance dangereuse».

Note 2 à l'article: Les valeurs numériques pour les mesures cibles des défaillances sont données dans le Tableau 2 et le Tableau 3 de la CEI 61508-1:2010. Ces valeurs limites sont valides pour l'ensemble de la fonction relative à la sécurité.

[Adaptée de la CEI 61508-4:2010, 3.5.17]

2.3.16
limite de revendications SIL
SILCL
SIL maximal qui peut être déclaré pour un PDDB en relation avec les contraintes architecturales et l'intégrité de sécurité systématique

[SOURCE: CEI 62061:2005, 3.2.24, modifiée – mise à jour de la définition]

2.3.17
temps moyen avant défaillance dangereuse
$MTTF_d$
prévision du temps moyen avant défaillance dangereuse

Note 1 à l'article: Adapté à partir de la CEI 62061:2005, définition en 3.2.34.

[SOURCE: ISO 13849-1:2006, 3.1.25]

2.3.18
défaillance dans le temps
FIT
nombre de défaillances pour 10^9 dispositifs-temps de fonctionnement

2.4 Termes et définitions concernant les contraintes architecturales

2.4.1
fraction de défaillance en sécurité
SFF
rapport entre les taux moyens de défaillance des défaillances en sécurité et des défaillances dangereuses détectées du PDDB, et le taux moyen total de défaillances (somme du taux de défaillances en sécurité et du taux de toutes les défaillances dangereuses) du PDDB

[Adapté de la CEI 61508-4:2010, 3.6.15]

2.4.2
couverture du diagnostic
DC
mesure de l'efficacité du diagnostic, qui peut être déterminée comme le rapport entre le taux de défaillance des défaillances dangereuses détectées et le taux de défaillance du total des défaillances dangereuses

[SOURCE: ISO 13849-1:2006, 3.1.26, modifiée – suppression des notes]

proportion de défaillances dangereuses détectées par des essais de diagnostic automatique en ligne

Note 1 à l'article: La proportion des défaillances dangereuses détectées est calculée comme le taux de défaillances dangereuses qui sont détectées par des essais de diagnostic automatique en ligne divisé par le taux de défaillances dangereuses totales.

Note 2 à l'article: L'approche concernant le concept de défaillance est différente entre la CEI 62061/CEI 61508 et l'ISO 13849-1. Les prescriptions pour les limites architecturelles sur les sous-systèmes selon la CEI 62061:2005 (Tableau 5) sont données en fonction de la tolérance du défaut de matériel et de la fraction de défaillance en sécurité. L'ISO 13849-1 ne prend pas en compte les défaillances en sécurité ou la fraction de défaillance en sécurité. Les niveaux de performances sont fondés sur des architectures correctement définies. Le niveau de performance atteint est alors fonction de l'architecture, du $MTTF_d$, de la couverture du diagnostic et des défaillances de cause commune.

[SOURCE: CEI 62061:2005, 3.2.38, modifiée – mise à jour des notes]

2.4.3
tolérance du défaut de matériel
HFT
capacité d'un système à exécuter sa fonction de sécurité en présence de défauts

Note 1 à l'article: Une tolérance du défaut de matériel de N signifie que N+1 défauts pourraient provoquer une perte de la fonction de sécurité. Lors de la détermination de la tolérance du défaut de matériel, les autres défauts ne sont pas pris en compte, dans les diagnostics par exemple.

[Adapté de la CEI 61508-2:2010, 7.4.4.1.1]

2.4.4
intervalle entre essais de diagnostic
intervalle de temps entre les essais en ligne qui permettent de détecter les anomalies d'un système relatif à la sécurité, dont la couverture du diagnostic est spécifiée

[SOURCE: CEI 61508-4:2010, 3.8.7]

2.4.5
essai périodique
essai périodique réalisé en vue de détecter des défaillances dans un système relatif à la sécurité de sorte que, si cela s'avère nécessaire, le système puisse être restauré comme neuf ou dans un état proche de celui-ci

[SOURCE: CEI 61508-4:2010, 3.8.5, modifiée – mise à jour de la définition et suppression des notes]

2.4.6
système relatif à la sécurité
système désigné qui, à la fois:

– met en œuvre les fonctions de sécurité requises pour atteindre ou maintenir un état de sécurité de l'EUC, et
– est prévu pour atteindre, par lui-même ou grâce à d'autres systèmes E/E/PE relatifs à la sécurité, et aux dispositifs externes de réduction de risque, l'intégrité de sécurité nécessaire pour les fonctions de sécurité requises

[SOURCE: CEI 61508-4:2010, 3.4.1, modifiée – suppression des notes]

2.4.7
équipement sous contrôle
EUC
équipement, machine, appareil ou installation utilisés pour les activités de fabrication, de traitement, de transport, médicales ou d'autres activités

Note 1 à l'article: Le système de commande de l'EUC est séparé et distinct de l'EUC.

[SOURCE: CEI 61508-4:2010, 3.2.1]

2.5 Termes et définitions concernant les parties d'un PDDB

2.5.1
moyen de détection
partie du PDDB qui détecte la présence ou l'absence d'une cible spécifiée

2.5.2
appareil de commutation du signal de sortie
OSSD
composant du PDDB qui passe à l'état bloqué selon le comportement défini

2.5.3
appareil de commande et de surveillance
appareil qui reçoit et traite les signaux du moyen de détection, fournit des signaux aux OSSD et surveille le fonctionnement correct

2.6 Termes et définitions concernant le fonctionnement d'un PDDB

2.6.1
comportement défini
changement du ou des OSSD à l'état bloqué dans la position définie de la cible spécifiée selon les exigences de la présente norme

2.6.2
état bloqué
état dans lequel les circuits de sortie interrompent le passage du courant autre que le courant résiduel ($\boldsymbol{I}_r$)

2.6.3
état passant
état dans lequel les circuits de sortie permettent le passage du courant

2.6.4
portée de travail assurée d'un PDDB
$\boldsymbol{S}_{\mathbf{ao}}$
distance, depuis la face sensible, sur laquelle la détection correcte de la présence de la cible spécifiée est faite dans toutes les conditions d'environnement et les tolérances de fabrication spécifiées

2.6.5
portée de déclenchement assurée d'un PDDB
$\boldsymbol{S}_{\mathbf{ar}}$
distance, depuis la face sensible, sur laquelle la détection correcte de l'absence de la cible spécifiée est faite dans toutes les conditions d'environnement et les tolérances de fabrication spécifiées

2.6.6
temps de risque
période de temps maximale pendant laquelle les OSSD peuvent dévier du comportement défini

2.6.7
temps de la mission
T_M
durée couvrant l'utilisation prévue d'un PDDB

2.6.8
état verrouillé
état dans lequel au moins un OSSD est bloqué et reste à l'état bloqué jusqu'à correction du défaut. Le dispositif acquiert l'état verrouillé dès qu'un défaut est détecté

2.7 Symboles et abréviations

Symbole ou abréviation	Description	Définition
DC	couverture du diagnostic	2.4.2
EUC	équipement sous contrôle	2.4.7
FIT	défaillances dans le temps	2.3.18
HFT	tolérance du défaut de matériel	2.4.3
$MTTF_d$	temps moyen avant défaillance dangereuse	2.3.17
OSSD	appareil de commutation du signal de sortie	2.5.2
PFH_D	fréquence moyenne d'une défaillance dangereuse sur une période donnée	2.3.15
PFD	probabilité de défaillance dangereuse à la demande	2.3.15
PL	niveau de performance	2.3.1
S_{ao}	portée de travail assurée d'un PDDB	2.6.4
S_{ar}	portée de déclenchement assurée d'un PDDB	2.6.5
SRF	fonction relative à la sécurité	2.3.9
SFF	fraction de défaillance en sécurité	2.4.1
SIL	niveau d'intégrité de sécurité	2.3.2
SILCL	limite de revendications SIL	2.3.16
SRCF	fonction de commande relative à la sécurité	2.3.9
T_M	temps de la mission	2.6.7

3 Classification

L'Article 3 de la CEI 60947-5-2:2007 s'applique.

4 Caractéristiques

4.1 Généralités

L'Article 4 de la CEI 60947-5-2:2007 s'applique avec les compléments suivants.

4.2 Caractéristiques de construction

4.2.1 Dispositif de détection de proximité à comportement défini

Un PDDB est composé des éléments suivants:

a) moyen de détection;

b) un ou plusieurs OSSD;

c) appareil de commande et de surveillance (si requis).

Ces éléments peuvent être intégrés dans un appareil unique ou peuvent être séparés.

4.2.2 Cible spécifiée

Le constructeur doit spécifier la cible nécessaire pour atteindre les portées S_{ao} et S_{ar}.

5 Informations sur le matériel

5.1 Nature des informations

Les informations suivantes doivent être fournies par le constructeur.

5.2 Identification

Le Paragraphe 5.1 de la CEI 60947-5-2:2007 s'applique avec les compléments suivants:

aa) portée de travail assurée;

ab) portée de déclenchement assurée;

ac) cible spécifiée;

ad) temps de risque;

ae) état de sécurité défini pour le(s) OSSD;

af) temps de la mission;

et soit:

ag) SFF/DC (s'ils existent) et HFT (conformément à la série CEI 61508 et à ses dérivés), et les données de fiabilité (par exemple, λ, PFH_D , PFD_{avg}, B_{10d}, selon la situation);

ou

ah) architecture désignée (s'il en existe une) et B_{10d}, λ, $MTTF_d$ et DC (conformément à l'ISO 13849-1), selon la situation.

5.3 Marquage

5.3.1 Généralités

Le Paragraphe 5.2.1 de la CEI 60947-5-2:2007 s'applique avec les compléments suivants:

Dans le cas d'un PDDB composé d'appareils séparés, le marquage des données des points a) et b) en 5.1 de la CEI 60947-5-2:2007 sur chaque appareil est obligatoire.

Les données des points c) à ah), lorsqu'elles ne sont pas incluses sur le dispositif de détection de proximité ou sur tout appareil séparé, doivent être incluses dans la documentation du constructeur.

5.3.2 Identification des raccordements et marquage

Le Paragraphe 7.1.7.4 de la CEI 60947-5-2:2007, Amendement 1 (2012) s'applique. Lorsque les bornes ne peuvent pas être marquées conformément au 7.1.7.4 de la CEI 60947-5-2:2007, Amendement 1 (2012), par exemple si elles sont situées à l'intérieur d'une enveloppe séparée, le constructeur doit fournir l'identification des bornes qui convient.

5.4 Instructions pour l'installation, le fonctionnement et l'entretien

Le Paragraphe 5.3 de la CEI 60947-5-2:2007, Amendement 1 (2012) s'applique avec les compléments suivants:

Il est nécessaire de mentionner les détails des influences externes connues et raisonnablement prévisibles qui peuvent affecter la S_{ao} et/ou la S_{ar}, et d'en expliquer les effets.

Pour un PDDB avec entrée d'essai, le constructeur doit définir:

a) le comportement du (des) OSSD pendant l'essai;

b) l'(les) entrée(s) et/ou sortie(s) pour l'essai externe.

6 Conditions normales de service, de montage et de transport

6.1 Conditions normales de service

Le Paragraphe 6.1 de la CEI 60947-5-2:2007 s'applique.

6.2 Conditions pendant le transport et le stockage

Le Paragraphe 6.2 de la CEI 60947-5-2:2007 s'applique.

6.3 Montage

Les dimensions et conditions de montage doivent être spécifiées par le constructeur.

7 Dispositions relatives à la construction et au fonctionnement

7.1 Dispositions constructives

7.1.1 Matériaux

Le Paragraphe 7.1.1 de la CEI 60947-5-2:2007 s'applique.

7.1.2 Parties transportant le courant et leurs connexions

Le Paragraphe 7.1.2 de la CEI 60947-5-2:2007 s'applique.

7.1.3 Distances d'isolement et lignes de fuite

Le Paragraphe 7.1.3 de la CEI 60947-5-2:2007 s'applique.

7.1.4 Disponible

7.1.5 Disponible

7.1.6 Disponible

7.1.7 Bornes

7.1.7.1 Dispositions de construction

Le Paragraphe 7.1.7.1 de la CEI 60947-5-2:2007 s'applique.

7.1.7.2 Capacité de raccordement

Le Paragraphe 7.1.7.2 de la CEI 60947-5-2:2007 s'applique.

7.1.7.3 Raccordements

Le Paragraphe 7.1.7.3 de la CEI 60947-5-2:2007, Amendement 1 (2012) s'applique.

7.1.7.4 Identification des raccordements et marquage

Le Paragraphe 7.1.7.4 de la CEI 60947-5-2:2007, Amendement 1 (2012) s'applique avec les compléments suivants:

Les PDDB avec câbles faisant partie intégrante de l'appareil doivent disposer de fils identifiés par un code de couleurs conformément au Paragraphe 7.1.7.4 de la CEI 60947-5-2:2007, Amendement 1 (2012).

7.1.8 Dispositions pour mise à la terre

Le Paragraphe 7.1.9 de la CEI 60947-5-2:2007 s'applique avec les compléments suivants:

Les parties de PDDB ayant une protection de classe II ou III ne doivent pas avoir de connexion pour mise à la terre.

7.1.9 Degré de protection IP (conformément à la CEI 60529)

Le moyen de détection d'un PDDB doit avoir un degré minimal de protection IP65.

Les dispositifs de commande et de surveillance doivent avoir un degré minimal de protection IP54.

Les dispositifs de commande et de surveillance qui sont conçus pour être montés dans une enveloppe ayant un degré minimal de protection IP54 peuvent avoir un degré de protection inférieur.

7.2 Gestion de la sécurité fonctionnelle

La gestion de la sécurité fonctionnelle doit être mise en œuvre de manière appropriée au cycle de vie du PDDB**.** Ceci peut être réalisé, par exemple, en utilisant l'Article 6 de la CEI 61508-1:2010 ou des normes appropriées du secteur.

7.3 Spécification d'exigences de fonctionnement pour les SRCF

7.3.1 Généralités

La spécification d'exigences de fonctionnement pour un PDDB doit décrire le détail de chaque SRCF à réaliser, y compris (si applicable):

a) une description de la SRCF;

b) la fréquence de fonctionnement;

c) le temps de risque nécessaire;

d) la ou les interfaces du PDDB;

e) une description de la ou des fonctions de réaction au défaut;

f) une description de l'environnement d'exploitation requis pour le PDDB (par exemple, la température, l'humidité, la poussière, les substances chimiques, les chocs et vibrations de la machine);

g) les essais et toute autre installation associée (par exemple, l'équipement d'essai, les ports d'accès d'essai);

h) le taux des cycles de manœuvres, le cycle de service et/ou la catégorie d'utilisation, pour les PDDB qui comportent des dispositifs électromécaniques.

7.3.2 Spécification d'exigences d'intégrité de sécurité pour les SRCF

Les exigences d'intégrité de sécurité pour un PDDB avec architecture donnée doivent comprendre:

a) la limite de revendications de SIL ou le PL (catégorie);

b) les données de fiabilité.

7.3.3 Compatibilité électromagnétique

7.3.3.1 Généralités

En complément des exigences relatives à la CEM de la CEI 60947-5-2, la présente partie spécifie les exigences supplémentaires pour les dispositifs destinés à effectuer des fonctions de sécurité telles que définies dans la série CEI 61508 et les normes dérivées. Ces exigences supplémentaires ne s'appliquent qu'à la fonction relative à la sécurité du dispositif. Ces dispositifs, s'ils sont alimentés par un courant continu, ne doivent pas être connectés à un réseau de distribution de courant continu. Les exigences de performance des PDDBs aux essais CEM sont identifiées dans le Tableau 1.

7.3.3.2 Critères de performance FS (sécurité intrinsèque)

Les fonctions du PDDB destinées à des applications dans le domaine de la sécurité ne sont pas affectées au-delà de leur spécification ou peuvent être momentanément ou définitivement perturbées si le PDDB réagit à cette perturbation de sorte qu'un état bloqué de la sortie est conservé ou atteint dans un laps de temps prévu et respecté. La destruction des composants est autorisée si un état défini de l'EUT (l'appareil à l'essai) est atteint dans un laps de temps prévu et respecté.

7.3.3.3 Utilisation de dispositifs externes

Lorsque l'immunité à certains phénomènes EM ne peut être obtenue qu'avec l'utilisation de dispositifs externes, alors ces dispositifs sont pris en compte pour les besoins de la présente norme internationale en tant que partie intégrante du PDDB et les exigences de type et d'installation pour ces dispositifs doivent être indiquées dans la documentation du constructeur. Si des exigences d'installation particulières sont nécessaires pour obtenir les performances de sécurité fonctionnelle requises (par exemple, une installation conforme à la CEI 60204-1), ces exigences doivent figurer dans la documentation du constructeur. Les ports de puissance d'entrée du ou des dispositifs de détection de proximité sur courant continu et alimentés par très basse tension de protection (T.B.T.P.) ou très basse tension de sécurité (T.B.T.S.) ne sont pas considérés comme étant connectés à un réseau de distribution de courant continu et, à la place, sont traités comme ports de contrôle/signal d'entrée ou de sortie.

Tableau 1 – Exigences relatives à la CEM pour les PDDB

Port	Phénomène	Norme de base	Valeur d'essai	Critère de performance
Enveloppe	Décharge électrostatique (ESD)	CEI 61000-4-2	Décharge au contact de 6 kV [a] Décharge dans l'air de 8 kV [a]	FS FS
	Champ EM	CEI 61000-4-3	20 V/m (80 MHz à 1 GHz) 10 V/m (1,4 GHz à 2 GHz) 3 V/m (2,0 GHz à 2,7 GHz)	FS FS FS
	Champ magnétique à la fréquence du réseau	CEI 61000-4-8	30 A/m (50 Hz, 60 Hz) [b]	FS
Alimentation Courant Alternatif (y compris terre de protection)	Salve	CEI 61000-4-4	3 kV (5/50 ns, 5 kHz) [c]	FS
	Surtension	CEI 61000-4-5	2 kV phase-phase [d] 4 kV phase-terre [d]	FS FS
	RF par conduction	CEI 61000-4-6	10 V (150 kHz à 80 MHz)	FS
	Creux de tension	CEI 61000-4-11	0 % pendant 1 cycle 40 % pendant 10/12 périodes [e] 70 % pendant 25/30 périodes [e]	FS FS FS
	Coupures brèves	CEI 61000-4-11	0 % pendant 250/300 périodes [e]	FS
Alimentation Courant Continu [f] (y compris terre de protection)	Salve	CEI 61000-4-4	2 kV (5/50 ns, 5 kHz) [c]	FS
	Surtension	CEI 61000-4-5	2 kV phase-terre [d]	FS
	RF par conduction	CEI 61000-4-6	10 V (150 kHz à 80 MHz)	FS
Contrôle ou signal d'entrée/sortie	Salve	CEI 61000-4-4	2 kV (5/50 ns, 5 kHz) [c]	FS
	Surtension [g]	CEI 61000-4-5	2 kV phase-terre [d]	FS
	RF par conduction	CEI 61000-4-6	10 V (150 kHz à 80 MHz)	FS
Terre fonctionnelle	Salve [h]	CEI 61000-4-4	2 kV (5/50 ns, 5 kHz) [c]	FS

[a] Pour un équipement destiné à une utilisation dans des applications SIL 3, le nombre de décharges au niveau le plus élevé doit être multiplié par 3 par rapport au nombre donné dans la norme standard.

[b] Seulement pour un équipement sensible aux champs magnétiques. L'interférence de l'affichage CRT (tube à rayon cathodique) est autorisée au-dessus de 1 A/m.

[c] Pour un équipement destiné à une utilisation dans des applications SIL 3, la durée de l'essai au niveau le plus élevé doit être multipliée par 5 par rapport à la durée donnée dans la norme standard.

[d] Pour un équipement destiné à une utilisation dans des applications SIL 3, le nombre d'impulsions au niveau le plus élevé doit être multiplié par 3 par rapport au nombre donné dans la norme standard.

[e] Par exemple: «25/30 périodes» signifie «25 périodes pour un essai à 50 Hz» ou «30 périodes pour un essai à 60 Hz»

[f] Les connexions courant continu entre parties de l'équipement/système qui ne sont pas reliées à un réseau de distribution courant continu sont traitées comme des ports de contrôle ou signaux d'entrée/sortie.

[g] Seulement en cas de câbles de connection > 30 m.

[h] Seulement en cas de câbles de connection > 3 m.

7.3.4 Conception et développement de PDDB

Le PDDB doit être conçu et validé en conformité avec la spécification d'exigences de sécurité et les exigences de la série CEI 61508, de la CEI 62061 ou de l'ISO 13849-1, selon le cas. Les exigences pour l'intégrité de sécurité systématique (capacité systématique) doivent être respectées par les Parcours de conformité 1_H ou 2_H (voir le 7.4.4.3 de la CEI 61508-2:2010) et 1_S ou 2_S (conformément au 7.4.2.12 de la CEI 61508-3:2010, selon ce qui est approprié).

NOTE Dans la CEI 62061:2005, Amendement 1 (2012) (Domaine d'application, Note 2) on considère que le Parcours 2_H n'est pas adapté aux applications pour les machines générales.

7.4 Informations d'utilisation

7.4.1 Objectif

Des informations doivent être fournies afin de permettre à l'utilisateur d'élaborer des procédures garantissant que la sécurité fonctionnelle requise pour le PDDB soit conservée lors de l'utilisation et de la maintenance de l'équipement sous contrôle.

7.4.2 Documentation pour l'installation, l'utilisation et la maintenance

La documentation doit apporter les informations relatives à l'installation, à l'utilisation et à la maintenance du PDDB. Elle doit prendre la forme d'un manuel de sécurité en conformité avec l'Annexe D de la CEI 61508-2:2010, y compris:

– une description complète du PDDB, de l'installation et du montage;
– une indication de l'utilisation prévue pour la PDDB et les mesures qui peuvent s'avérer nécessaires pour prévenir toute mauvaise utilisation potentielle;
– des informations relatives à l'environnement physique (par exemple éclairage, vibrations, niveaux sonores, contaminants atmosphériques) si cela est approprié;
– un ou des schémas de raccordement;
– la durée de vie utile;
– l'intervalle d'essais périodiques si cela est pertinent;
– les informations de paramétrage, si cela est pertinent;
– la description des exigences de maintenance (le cas échéant) applicables au PDDB;
– la spécification pour l'essai périodique et la maintenance préventive et corrective.

NOTE 1 Les essais périodiques sont les essais fonctionnels nécessaires à la confirmation du fonctionnement correct et à la détection des défauts. Ils supposent une description exhaustive des principes mis en œuvre, tels que des essais d'épreuve et/ou de diagnostic en ligne.

NOTE 2 La maintenance préventive se compose des mesures nécessaires (si besoin est) pour conserver le niveau de performance requis pour le PDDB.

NOTE 3 La maintenance corrective intègre les mesures (le cas échéant) prises après apparition de défaut(s) spécifique(s) et nécessaires pour ramener le PDDB à son état d'origine.

8 Essais

8.1 Nature des essais

8.1.1 Généralités

Le Paragraphe 8.1.1 de la CEI 60947-1:2007 s'applique.

8.1.2 Essais de type

Le Paragraphe 8.1.2 de la CEI 60947-5-2:2007 s'applique avec les compléments suivants:

– performances dans des conditions de défaut.

8.1.3 Essais individuels de série

Le Paragraphe 8.1.3 de la CEI 60947-5-2:2007 s'applique.

8.1.4 Essais sur prélèvement

Le Paragraphe 8.1.4 de la CEI 60947-1:2007 s'applique.

8.2 Conformité aux dispositions de construction

Le paragraphe 8.2 de la CEI 60947-1:2007, Amendement 1 (2010) s'applique, s'il y a lieu.

8.3 Fonctionnement

8.3.1 Séquences d'essais

Le Paragraphe 8.3.1 de la CEI 60947-5-2:2007 s'applique.

8.3.2 Conditions générales d'essai

8.3.2.1 Exigences générales

Le Paragraphe 8.3.2.1 de la CEI 60947-5-2:2007 s'applique, s'il y a lieu.

8.3.2.2 Grandeurs d'essais

Le Paragraphe 8.3.2.2 de la CEI 60947-1:2007 s'applique.

8.3.2.3 Compte-rendus d'essais

Le Paragraphe 8.3.2.4 de la CEI 60947-1:2007 s'applique.

8.3.3 Performances à vide et dans les conditions de charge normales et anormales

8.3.3.1 Manœuvre

Le Paragraphe 8.3.3.1 de la CEI 60947-1:2007 s'applique.

8.3.3.2 Limites de fonctionnement

Le Paragraphe 8.3.3.2 de la CEI 60947-5-2:2007 s'applique.

8.3.3.3 Echauffement

Le Paragraphe 8.3.3.3 de la CEI 60947-5-2:2007 s'applique.

8.3.3.4 Propriétés diélectriques

Le Paragraphe 8.3.3.4 de la CEI 60947-5-2:2007 s'applique.

8.3.3.5 Pouvoirs de coupure et de fermeture

8.3.3.5.1 Généralités

Le Paragraphe 8.3.3.5 de la CEI 60947-5-1:2003 et de la CEI 60947-5-2:2007 est à appliquer, s'il y a lieu.

8.3.3.5.2 Evaluation

Pendant les essais, aucun défaut électrique ou mécanique ne doit survenir, aucun contact ne doit se souder, aucun temps d'arc étendu ne doit survenir et aucun fusible ne doit fondre. Les surtensions de manœuvre conduites ne doivent pas dépasser la tension assignée de tenue aux chocs et les portées de déclenchement assurées, selon les 2.6.4 et 2.6.5, doivent rester dans les limites déclarées.

8.3.4 Performances en conditions de court-circuit

Le Paragraphe 8.3.4 de la CEI 60947-5-1:2003 et de la CEI 60947-5-2:2007, Amendement 1 (2012) est à appliquer, s'il y a lieu.

8.4 Vérification des portées de travail

Le PDDB doit être essayé aux températures assignée, maximale et minimale de l'air ambiant déclarées par le constructeur avec la tension de fonctionnement la plus élevée et au courant de fonctionnement assigné à l'élément de commutation de sortie, jusqu'à ce que l'équilibre thermique soit atteint.

Les essais doivent être conformes à la méthode d'essai B de la CEI 60068-2-1 et de la CEI 60068-2-30.

Après les essais de température, les portées de travail et de déclenchement assurées doivent alors être mesurées conformément au 8.4 de la CEI 60947-5-2:2007 et se situer dans les spécifications du constructeur.

8.5 Vérification de la résistance aux vibrations et aux chocs

Les essais doivent être effectués conformément au 7.4 de la CEI 60947-5-2:2007, sauf pour les appareils séparés de commande et de surveillance. Pendant les essais, l'état de la ou des sorties ne doit pas changer.

Les essais doivent être effectués conformément au 6.3.5 de la CEI 61131-2:2007 pour les appareils de commande et de surveillance séparés avec le complément suivant.

Pendant les essais, l'état de la (des) sortie(s) ne doit pas changer.

8.6 Vérification de la compatibilité électromagnétique

L'essai doit être réalisé conformément au 7.2.6 de la CEI 60947-5-2:2007. En outre, la S_{ar} et la S_{ao} doivent faire l'objet d'une vérification après l'essai.

9 Modification

9.1 Objectif

Cet article spécifie la ou les procédures de modification à appliquer lors de la modification du PDDB pendant la conception, l'intégration ou la validation.

9.2 Procédure de modification

Le Paragraphe 7.16 de la CEI 61508-1:2010 doit s'appliquer.

Extrait du 7.16.2.2 de la CEI 61508-1:2010:

NOTE Le motif de cette demande de modification peut provenir, par exemple:

a) d'une sécurité fonctionnelle inférieure à celle spécifiée,

b) d'une anomalie systématique mise en évidence par expérimentation,

c) d'une législation de sécurité nouvelle ou modifiée,

d) des modifications apportées à l'EUC ou à son utilisation,

e) d'une modification des exigences globales de sécurité,

f) d'une analyse des performances d'exploitation et de maintenance, indiquant que ces performances sont inférieures à celles prévues,

g) des audits de sécurité fonctionnelle systématiques.

Annexe A
(informative)

Exemple d'un système de commande unique conforme à la série CEI 61511

A.1 Description

Détection de débordement à l'aide d'un dispositif de commande de niveau et d'une vanne (voir Figure A.1). L'équipement est situé dans une zone dangereuse (atmosphère inflammable) et doit être protégé conformément aux exigences suivantes:

– dispositif de détection de niveau: Zone 0/Division 1;
– vanne de régulation: Zone 2/Division 2.

A.2 Spécification des exigences de sécurité

A.2.1 Exigences de fonctionnement

En cas de débordement, la vanne de régulation doit être fermée.

A.2.2 Exigences d'intégrité de sécurité

L'évaluation des risques a révélé qu'une SIL 2 est appropriée à cette fonction.

A.2.3 Conditions d'utilisation

Mode à faible sollicitation (pas plus d'une demande de fonction de sécurité par an).

Temps de réparation pour les défaillances détectées: 8 h.

Intervalle d'essais: 12 mois.

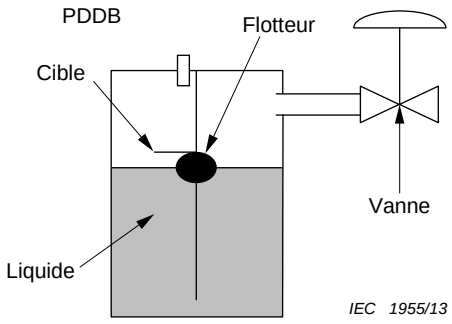

Figure A.1 – Représentation de l'équipement sous contrôle

NOTE Il existe de nombreuses autres exigences indiquées dans les spécifications, comme la qualité de l'alimentation, les conditions de maintenance en direct, etc.

A.3 Réalisation

Dans cet exemple, la fonction de sécurité sera réalisée par:

- un détecteur de proximité pour le capteur flottant (par exemple avec une sortie conforme à la CEI 60947-5-6);

- un amplificateur de commutateur isolé avec relais de sortie;
- un pilote d'électrovanne;

NOTE Etant donné que l'alimentation à la sortie du pilote d'électrovanne sécurisée est trop faible pour alimenter la vanne sphérique, dans cet exemple il est nécessaire d'insérer une vanne de régulation.

- une vanne de régulation;
- une vanne sphérique.

A.4 Collecte des données

L'ensemble des données de fiabilité et de structure à prendre en considération pour le présent exemple de système de commande est décrit dans le Tableau A.1.

Tableau A.1 – Collecte des données de fiabilité et de structure

Capteur: Dispositif inductif de détection de proximité conforme à la CEI 60947-5-6	**Amplificateur de commutateur isolé: Amplificateur de commutateur isolé à sécurité intrinsèque**	**Pilote d'électrovanne: Pilote d'électrovanne avec sortie à sécurité intrinsèque**	**Vanne de régulation: Vanne de régulation à sécurité intrinsèque**	**Vanne sphérique: Produit générique**
Limite de revendications SIL relative aux contraintes architecturales: 2 dans une configuration à un canal	Limite de revendications SIL relative aux contraintes architecturales: 2 dans une configuration à un canal	Limite de revendications SIL relative aux contraintes architecturales: 3 dans une configuration à un canal	Limite de revendications SIL relative aux contraintes architecturales: 3 dans une configuration à un canal	Limite de revendications SIL relative aux contraintes architecturales: 1 dans une configuration à un canal
SFF = 94,09 %	SFF = 91,62 %	SFF = 100 %	SFF = 99 %	SFF = 50 %
Taux de défaillances:	Taux de défaillances:	Taux de défaillances:	Taux de défaillances:	Taux de défaillances:
λ_{DU} = 3,9 FIT	λ_{DU} = 19 FIT	λ_{DU} = 0 FIT	λ_{DU} = 0 FIT	λ_{DU} = 60 FIT
λ_{S} = 62,1 FIT	λ_{S} = 208 FIT	λ_{S} = 1,3 FIT	λ_{S} = 0 FIT	λ_{S} = 60 FIT

Tous les composants excepté la vanne sphérique (dont la structure correspond à SIL 1 et la SFF est inférieure à 90 %) peuvent être utilisés dans une fonction relative à la sécurité jusqu'à la limite SIL 2, conformément au Tableau 2 de la CEI 61508-2:2010. En conséquence, il convient que le canal de sortie (pilote d'électrovanne, vanne de régulation et vanne sphérique) ait une architecture redondante, comme le montre la Figure A.2.

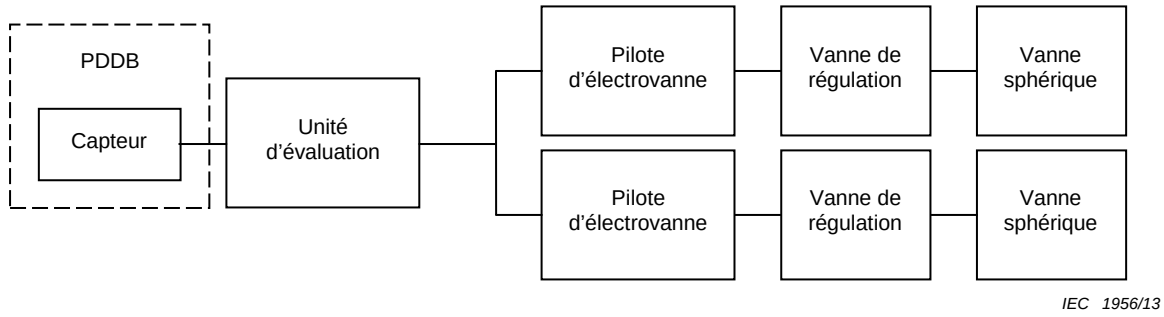

Figure A.2 – Architecture de la fonction relative à la sécurité

Sous-système d'entrée (capteur et unité d'évaluation)

$\Sigma\lambda_{DU}$ = 3,9 FIT + 19 FIT = 22,9 FIT

$\Sigma\lambda_{safe}$ = 62,1 FIT + 208 FIT = 270,1 FIT

Calcul de la PFD du sous-système d'entrée à l'aide des formules en B.3.2.2.1 de la CEI 61508-6:2010:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR}$$

$$\text{PFD}_G = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

$\text{PFD}_{\text{canal d'entrée}}$ = 3,75 10^{-3}

Sous-système de sortie (pilotes d'électrovannes et vannes)

$\Sigma\lambda_{DU}$ 1 canal = 0 + 0 + 60 = 60 FIT

$\Sigma\lambda_{safe}$ 1 canal = 1,3 + 0 +60 = 61,3 FIT

MTTR = MRT = 8 h dans l'hypothèse où le temps nécessaire pour détecter une défaillance dangereuse est très inférieur au MRT (au moins d'un ordre de grandeur).

Calculs de la PFD résultante du sous-système de sortie à l'aide des formules en B.3.2.2.2 de la CEI 61508-6:2010 et sur la base d'une contribution de la défaillance de cause commune à hauteur de 10 %:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR}$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR}$$

$$\text{PFD}_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE}\, t_{GE} + \beta_D\lambda_{DD}\text{MTTR} + \beta\lambda_{DU}\left(\frac{T_1}{2} + \text{MRT}\right)$$

$\text{PFD}_{\text{canal de sortie}}$ = 2,72 10^{-6}

$\text{PFD}_{\text{total}}$ = $\text{PFD}_{\text{canal d'entrée}}$ + $\text{PFD}_{\text{canal de sortie}}$ = 3,75 10^{-3}, ce qui se situe dans la plage autorisée pour la limite SIL 2 (Tableau 2 de la CEI 61508-1:2010)

Résultats du calcul:

SIL d'après la PFD: SIL 2

A.5 Résultats

SIL d'après l'architecture: SIL 2

SIL d'après la PFD: SIL 2

SIL de la fonction de sécurité: SIL 2

Bibliographie

CEI 60050-191:1990, *Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*
Amendement 1:1999
Amendement 2:2002

CEI 60050-441:1984, *Vocabulaire Electrotechnique International (VEI) – Chapitre 441: Appareillage et fusibles*
Amendement 1:2000

CEI 60068-2-6:2007, *Essais d'environnement – Partie 2-6: Essais – Essai Fc: Vibrations (sinusoïdales)*

CEI 60068-2-14:2009, *Essais d'environnement – Partie 2-14: Essais – Essai N: Variation de température*

CEI 60068-2-27:2008, *Essais d'environnement – Partie 2-27: Essais – Essai Ea et guide: Chocs*

CEI 60204-1:2005, *Sécurité des machines – Equipement électrique des machines – Partie 1: Règles générales*
Amendement 1:2008

CEI 60364 (toutes les parties), *Installations électriques à basse tension*

CEI 60445:2010, *Principes fondamentaux et de sécurité pour les interfaces homme-machines, le marquage et l'identification – Identification des bornes de matériels, des extrémités de conducteurs et des conducteurs*

CEI 60947-5-6:1999, *Appareillage à basse tension – Partie 5-6: Appareils et éléments de commutation pour circuits de commande – Interface à courant continu pour capteurs de proximité et amplificateurs de commutation (NAMUR)*

CEI 61000-3-2:2005, *Compatibilité électromagnétique (CEM) – Partie 3-2: Limites – Limites pour les émissions de courant harmonique (courant appelé par les appareils ≤ 16 A par phase)*
Amendement 1:2008
Amendement 2:2009

CEI 61000-3-3:2008, *Compatibilité électromagnétique (CEM) – Partie 3-3: Limites – Limitation des variations de tension, des fluctuations de tension et du papillotement dans les réseaux publics d'alimentation basse tension, pour les matériels ayant un courant assigné ≤16 A par phase et non soumis à un raccordement conditionnel*

CEI 61000-4-13:2002, *Compatibilité électromagnétique (CEM) – Partie 4-13: Techniques d'essai et de mesure – Essais d'immunité basse fréquence aux harmoniques et inter-harmoniques incluant les signaux transmis sur le réseau électrique alternatif*
Amendement 1:2009

CEI 61140:2001, *Protection contre les chocs électriques – Aspects communs aux installations et aux matériels*
Amendement 1:2004

CEI 61165:2006, *Application des techniques de Markov*

CEI 61326-3-1:2008, *Matériel électrique de mesure, de commande et de laboratoire – Exigences relatives à la CEM – Partie 3-1: Exigences d'immunité pour les systèmes relatifs à la sécurité et pour les matériels destinés à réaliser des fonctions relatives à la sécurité (sécurité fonctionnelle) – Applications industrielles générales*

CEI 61496-1:2012, *Sécurité des machines – Equipements de protection électro-sensibles – Partie 1: Exigences générales et essais*

CEI 61496-2:2013, *Sécurité des machines – Equipements de protection électro-sensibles – Partie 2: Exigences particulières à un équipement utilisant des dispositif protecteurs optoélectroniques actifs (AOPD)*

CEI 61496-3:2008, *Sécurité des machines – Équipements de protection électro-sensibles – Partie 3: Exigences particulières pour les équipements utilisant des dispositifs protecteurs optoélectroniques actifs sensibles aux réflexions diffuses (AOPDDR)*

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

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

CEI 61508-6:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

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

CEI 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

CEI 61511-1:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel*

CEI 61511-2:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 2: Lignes directrices pour l'application de la CEI 61511-1*

CEI 61511-3:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité*

CEI/TR 62380:2004, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment* (disponible en anglais seulement)

CISPR 11:2009, *Appareils industriels, scientifiques et médicaux – Caractéristiques de perturbations radioélectriques – Limites et méthodes de mesure*
Amendement 1:2010

ISO 14119:1998, *Sécurité des machines – Dispositifs de verrouillage associés à des protecteurs – Principes de conception et de choix*
Amendement 1:2007

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

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

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