IEC 62061

Edition 1.0 2012-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

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

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

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It also gives information on projects, replaced and withdrawn publications.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 62061

Edition 1.0 2012-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX J

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-83220-441-2

FOREWORD

This amendment has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects.

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

CDV	Report on voting
44/655/CDV	44/663/RVC

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

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

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- withdrawn,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

INTRODUCTION

Delete the tenth paragraph of this clause.

Delete the following text below Figure 1:

Information on the recommended application of IEC 62061 and ISO 13849-1 (under revision)

Replace the text of the paragraph above Table 1 by the following:

IEC 62061 and ISO 13849-1 specify requirements for the design and implementation of safety-related control systems of machinery. The use of either of these standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. IEC/TR 62061-1 provides guidance on the application of IEC 62061 and ISO 13849-1 in the design of safety-related control systems for machinery.

Delete the note above Table 1.

Delete Table 1.

1 Scope

Replace the text of Note 2 by the following:

NOTE 2 In this standard, it is presumed that the design of complex programmable electronic subsystems or subsystem elements conforms to the relevant requirements of IEC 61508 and uses Route 1_H (see IEC 61508-2:2010, 7.4.4.2). It is considered that Route 2_H (see IEC 61508-2:2010, 7.4.4.3) is not suitable for

general machinery. Therefore, this standard does not deal with Route 2_H. This standard provides a methodology for the use, rather than development, of such subsystems and subsystem elements as part of a SRECS.

2 Normative references

Replace the references to ISO 12100-1:2003 and ISO 12100-2:2003 by the following new reference:

ISO 12100:2010, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

Replace the existing reference to ISO 13849-1 by the following new reference:

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

3.2.5
subsystem

Replace definition 3.2.5 by the following new definition:

3.2.5
subsystem
entity of the top-level architectural design of the SRECS where a dangerous failure of any subsystem will result in a dangerous failure of a safety-related control function

[IEC 61508-4, 3.4.4 modified]

NOTE 1 A complete subsystem can be made up from a number of identifiable and separate subsystem elements, which when put together implement the function blocks allocated to the subsystem.

NOTE 2 This differs from common language where "subsystem" may mean any sub-divided part of an entity, the term "subsystem" is used in this standard within a strongly defined hierarchy of terminology: "subsystem" is the first level subdivision of a system. The parts resulting from further subdivision of a subsystem are called "subsystem elements".

3.2.7
low complexity component

Replace the reference above Note 1 by the following new reference:

[IEC 61508-4, 3.4.3 modified]

3.2.9
functional safety
Replace the reference by the following new reference:

[IEC 61508-4, 3.1.12 modified]

3.2.10
hazard (from machinery)
Replace the reference by the following new reference:

[ISO 12100, 3.6 modified]

3.2.11
hazardous situation
Replace the reference by the following new reference:

[ISO 12100, 3.10 modified]

3.2.12
protective measure
Replace the reference by the following new reference:

[ISO 12100, 3.19 modified]

3.2.13
risk
Replace the reference by the following new reference:

[ISO 12100, 3.12]

3.2.15
safety function
Replace the reference by the following new reference:

[ISO 12100, 3.30]

3.2.19
safety integrity
Replace the reference by the following new reference:

[IEC 61508-4, 3.5.4 modified]

3.2.20
hardware safety integrity
Replace the reference by the following new reference:

[IEC 61508-4, 3.5.7 modified]

3.2.21
software safety integrity
Replace the reference by the following new reference:

[IEC 61508-4, 3.5.5 modified]

3.2.22
systematic safety integrity
Replace the reference by the following new reference:

[IEC 61508-4, 3.5.6 modified]

3.2.23
Safety Integrity Level
SIL
Replace the reference by the following new reference:

[IEC 61508-4, 3.5.8 modified]

3.2.26
low demand mode
Replace the first paragraph by the following new paragraph:

mode of operation in which the frequency of demands on a SRECS is no greater than one per year

3.2.27
high demand or continuous mode
Replace the first paragraph by the following new paragraph:

mode of operation in which the frequency of demands on a SRECS is greater than one per year or the SRCF retains the machine in a safe state as part of normal operation

Replace the reference by the following new reference:

[IEC 61508-4, 3.5.16 modified]

3.2.28
Probability of dangerous Failure per Hour
***PFH*$_D$**

Replace definition 3.2.28 by the following new definition:

3.2.28
Probability of dangerous Failure per Hour
***PFH*$_D$**

average probability of a dangerous failure per hour of a safety related system/subsystem to perform the specified safety function over a given period of time

NOTE *PFH*$_D$ should not be confused with probability of dangerous failure on demand (*PFD*).

3.2.29
target failure value
Replace the reference by the following new reference:

[IEC 61508-4, 3.5.17 modified]

3.2.35
architecture
Replace the reference by the following new reference:

[IEC 61508-4, 3.3.4 modified]

3.2.37
proof test
Replace the first paragraph by the following new paragraph:

periodic test performed to detect dangerous hidden failures and degradation in a SRECS and its subsystems so that, if necessary, the SRECS and its subsystems can be restored to an “as new” condition or as close as practical to this condition

3.2.38
diagnostic coverage
Replace the first paragraph by the following new paragraph:

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

Add, at the end of this subclause, new Note 2 as follows:

NOTE 2 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.

and number the existing note as Note 1.

3.2.40
dangerous failure
Delete the reference “[IEC 61508-4, 3.6.7 modified]”.

3.2.41
safe failure
Delete the reference “[IEC 61508-4, 3.6.8 modified]”.

3.2.43
Common Cause Failure
CCF
Replace, in the first paragraph, the word "coincident" *by* "concurrent".

5.2.3 Functional requirements specification for SRCFs

Replace the existing text of this subclause (including 5.2.3.1 and 5.2.3.2) by the following:

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

– the condition(s) (e.g. operating mode) of the machine in which the SRCF shall be active or disabled;
– the priority of those functions that can be simultaneously active and that can cause conflicting action;
– the frequency of operation of each SRCF;
– the required response time of each SRCF;
– the interface(s) of the SRCFs to other machine functions;
– the required response times (e.g. input and output devices);
– a description of each SRCF;
– a description of fault reaction function(s) and any constraints on, for example, re-starting or continued operation of the machine in cases where the initial fault reaction is to stop the machine;
– a description of the operating environment (e.g. temperature, humidity, dust, chemical substances, mechanical vibration and shock);
– tests and any associated facilities (e.g. test equipment, test access ports);
– rate of operating cycles, duty cycle, and/or utilisation category, for electromechanical devices intended for use in the SRCF.

NOTE 1 In addition to the requirements of IEC 61000-6-2, when a SRECS is intended for use in an industrial environment, electromagnetic (EM) immunity levels are given in IEC 61326-3-1. SRECS intended for use in another EM environment (e.g. residential) should have immunity levels based on those specified in different EMC standards (e.g., for a residential environment, IEC 61000-6-1).

NOTE 2 When specifying EM immunity levels it is necessary to consider whether the levels used in different EMC standards cover cases which can occur in a SRECS application even with a low probability of occurrence.

NOTE 3 EM immunity performance criterion for functional safety of a SRECS is given in 6.4.3.

6.4 Requirements for systematic safety integrity of the SRECS

Delete the note.

6.4.2 Requirements for the control of systematic faults

Replace Note 2 by the following:

NOTE 2 Further information can be found in IEC 61784-3 and IEC 61508-2.

6.4.3 Electromagnetic (EM) immunity

*Replace, in this subclause, "*Annex E*" by "*IEC 61326-3-1".

*Replace, in the note of this subclause, "*Annex E*" by "*IEC 61326-3-1".

6.6.3.1 General

Replace the last sentence of this subclause by the following:

The SIL that can be achieved by the SRECS is less than or equal to the lowest SILCLs of any of the subsystems that comprise the SRECS.

6.6.3.4 Systematic safety integrity

Delete subclause 6.6.3.4.

6.7.2.1

Replace this subclause by the following:

6.7.2.1 The subsystem shall be realised by either selection (see 6.7.3) or design (see 6.7.4) in accordance with its safety requirements specification (see 6.6.2.1.7), taking into account all the requirements of 6.2. Subsystem(s) incorporating complex components shall comply with IEC 61508-2 and IEC 61508-3 as appropriate for the required SIL and the design shall use Route 1_H (see IEC 61508-2:2010, 7.4.4.2).

EXCEPTION: Where a subsystem design includes a complex component as a subsystem element, 6.7.4.2.3 is applicable.

NOTE In this standard, it is presumed that the design of complex programmable electronic subsystems or subsystem elements conforms to the relevant requirements of IEC 61508 and uses Route 1_H (see IEC 61508-2:2010, 7.4.4.2). It is considered that Route 2_H (see IEC 61508-2:2010, 7.4.4.3) is not suitable for general machinery. Therefore, this standard does not deal with Route 2_H. This standard provides a methodology for the use, rather than development, of such subsystems and subsystem elements as part of a SRECS.

6.7.2.2

Replace Note 1 of item b) by the following:

NOTE 1 For electromechanical subsystems, the probability of failure should be estimated taking into account the number of operating cycles declared by the manufacturer and the duty cycle (see 5.2.3). This information should be based upon a B10 value (see IEC 61649) under the operating conditions stated by the manufacturer. See for example IEC 60947-4-1, Annex K.

6.7.3.2

Add the following text at the end of the first sentence:

and the design shall use Route 1_H (see IEC 61508-2:2010, 7.4.4.2).

Add the following note at the end of the subclause:

NOTE In this standard, it is presumed that the design of complex programmable electronic subsystems or subsystem elements conforms to the relevant requirements of IEC 61508 and uses Route 1_H (see IEC 61508-2:2010, 7.4.4.2). It is considered that Route 2_H (see IEC 61508-2:2010, 7.4.4.3) is not suitable for general machinery. Therefore, this standard does not deal with Route 2_H. This standard provides a methodology for the use, rather than development, of such subsystems and subsystem elements as part of a SRECS.

6.7.4.2.2

*Replace, in the second dashed item of item b), "*7.4.7.5 to 7.4.7.12*" by "*7.4.10*".*

6.7.4.2.3

Replace this subclause by the following:

6.7.4.2.3 Where the design of a subsystem incorporates a complex component (as a subsystem element) which satisfies all relevant requirements of IEC 61508-2 and IEC 61508-3 in relation to the SILCL and uses Route 1_H (see IEC 61508-2:2010, 7.4.4.2), it can be considered as a low complexity component in the context of a subsystem design since its relevant failure modes, behaviour on detection of a fault, rate of failure, and other safety-related information are known. Such components shall only be used in accordance with their specification and the relevant information for use provided by their supplier.

NOTE In this standard, it is presumed that the design of complex programmable electronic subsystems or subsystem elements conforms to the relevant requirements of IEC 61508 and uses Route 1_H (see IEC 61508-2:2010, 7.4.4.2). It is considered that Route 2_H (see IEC 61508-2:2010, 7.4.4.3) is not suitable for general machinery. Therefore, this standard does not deal with Route 2_H. This standard provides a methodology for the use, rather than development, of such subsystems and subsystem elements as part of a SRECS.

6.7.4.4.2

Replace the note of item c) by the following:

NOTE For electromechanical subsystems, the probability of failure should be estimated taking into account the number of operating cycles declared by the manufacturer and the duty cycle (see 5.2.3). This information should be based upon a B10 value (see IEC 61649) under the operating conditions stated by the manufacturer. See for example IEC 60947-4-1, Annex K.

6.7.6.5

Delete this entire subclause and Table 6.

6.7.7.2

Delete the following text at item b):

(see references in Annex D)

Delete item c).

Existing item d) becomes item c).

Add the following new notes at the end of the subclause:

NOTE 1 Information of the failure mode ratios for electrical/electronic component can be found in several sources including:

– MIL-HDBK 217F(Notice 2) Reliability Prediction of Electronic Equipment (28-02-95), Parts Stress Analysis

– MIL-HDBK 217F(Notice 2) Reliability Prediction of Electronic Equipment (28-02-95), Appendix A, Parts Count Reliability Prediction

– SN 29500 Part 7, Failure Rates of Components, Expected Values for Relays, April 1992

– SN 29500 Part 11, Failure Rates of Components, Expected Values for Contactors, August 1990

– The documents in the SN 29500 series are publicly available and can be obtained from:
  - Siemens AG, CT SR SI
    Otto-Hahn-Ring 6
    D-81739 München:

– UTE C 80-810 RDF 2000: Reliability data handbook – A universal model for reliability prediction of electronic components, PCBs and equipment

– Failure mode/mechanism distributions FMD-91, RAC 1991.

NOTE 2 It is recommended to use failure rate data and failure mode ratio data provided by manufacturers.

NOTE 3 Some component standards have relevant data (e.g. Annex K of IEC 60947-4-1).

NOTE 4 Where a detailed analysis of each failure mode is not practically possible, a division of failures into 50 % safe, 50 % dangerous is generally accepted.

NOTE 5 Lists of faults to be considered for mechanical, pneumatic, hydraulic and electrical technologies are given in Annexes A, B, C and D of ISO 13849-2.

6.7.8.1.2

*Replace, in item f), the word "*mission time*" by "*useful lifetime*".*

Replace, in item g), Note 4, the existing items b) and c) by the following:

b) Markov models (see B.6.6.6 of IEC 61508-7 and IEC 61165);
c) reliability block diagrams (see B.6.6.7 of IEC 61508-7 and IEC 61078).

6.7.8.1.6

Delete this subclause.

Delete Table 7.

6.7.9 Requirements for systematic safety integrity of subsystems

Delete the note.

6.12.1.2

*Replace, in Note 1, the reference "*B.5*" by "*B.5.2*".*

A.1 General

*Delete Note 2 and replace "*NOTE 1*" by "*NOTE*".*

Table A.2 – Frequency and duration of exposure (Fr) classification

Replace, in the first column, third row of the table, the text "≤ 1 per h*" by "*≥ 1 per h".

Annex D – Failure modes of electrical/electronic components

Delete Annex D.

Annex E – Electromagnetic (EM) phenomenon and increased immunity levels for SRECS intended for use in an industrial environment according to IEC 61000-6-2

Delete Annex E.

Annex F – Methodology for the estimation of susceptibility to common cause failures (CCF)

Table F.1 – Criteria for estimation of CCF

*Replace the text in the last row of the "*Item*" column with the following new text:*

Is the subsystem immune to adverse influences from electromagnetic interference up to and including the limits specified in IEC 61326-3-1?

AVANT-PROPOS

Le présent amendement a été établi par le comité d'études 44 de la CEI: Sécurité des machines – Aspects électrotechniques.

Le texte de cet amendement est issu des documents suivants:

CDV	Rapport de vote
44/655/CDV	44/663/RVC

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

Le comité a décidé que le contenu de cet amendement et de la publication de base 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. À cette date, la publication sera

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

INTRODUCTION

Supprimer le dixième alinéa de cet article.

Supprimer le texte suivant, sous la Figure 1:

Information sur l'utilisation recommandée de la CEI 62061 et de l'ISO 13849-1 (révision)

Remplacer le texte de l'alinéa au-dessus du Tableau 1 par le texte suivant:

La CEI 62061 et l'ISO 13849-1 spécifient les exigences pour la conception et la réalisation des systèmes de commande des machines relatifs à la sécurité. L'utilisation de l'une de ces deux normes, selon le domaine d'application, peut impliquer la conformité aux exigences essentielles de sécurité appropriées. La CEI/TR 62061-1 donne des lignes directrices relatives à l'application de la CEI 62061 et de l'ISO 13849-1 dans la conception des systèmes de commande des machines relatifs à la sécurité.

Supprimer la note au-dessus du Tableau 1.

Supprimer le Tableau 1.

1 Domaine d'application

Remplacer le texte de la Note 2 par le suivant:

NOTE 2 Dans la présente norme, il est supposé que la conception des sous-systèmes ou éléments de sous-système électroniques programmables complexes est conforme aux exigences appropriées de la CEI 61508 et

utilise le parcours 1_H (voir CEI 61508-2:2010, 7.4.4.2). Il est considéré que le parcours 2_H (voir CEI 61508-2:2010, 7.4.4.3) ne convient pas aux machines à usage général. La présente norme ne traite donc pas du parcours 2_H. Elle fournit une méthodologie pour l'utilisation, plus que pour le développement, de tels sous-systèmes et éléments de sous-système en tant que partie d'un SRECS.

2 Références normatives

Remplacer les références aux ISO 12100-1:2003 et ISO 12100-2:2003 par la nouvelle référence suivante:

ISO 12100:2010, *Sécurité des machines – Principes généraux de conception – Appréciation du risque et réduction du risque*

Remplacer la référence existante à l'ISO 13849-1 par la suivante:

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

3.2.5
sous-système

Remplacer la définition 3.2.5 par la nouvelle définition suivante:

3.2.5
sous-système
entité de la conception de l'architecture générale du SRECS dans laquelle une défaillance dangereuse d'un sous-système quelconque entraînera une défaillance dangereuse d'une fonction de commande relative à la sécurité

[CEI 61508-4, 3.4.4 modifiée]

NOTE 1 Un sous-système complet peut être constitué d'un certain nombre d'éléments de sous-système identifiables et séparés qui, lorsqu'ils sont associés, réalisent les blocs fonctionnels alloués au sous-système.

NOTE 2 Cette définition diffère du langage courant où le terme « sous-système » peut signifier une quelconque partie subdivisée d'une entité; le terme « sous-système » est utilisé dans la présente norme dans une hiérarchie terminologique bien déterminée: le « sous-système » est le premier niveau de subdivision d'un système. Les parties résultant de subdivisions ultérieures d'un sous-système sont appelées « éléments de sous-système ».

3.2.7
composant de faible complexité

Remplacer la référence située au-dessus de la Note 1 par la suivante:

[CEI 61508-4, 3.4.3 modifiée]

3.2.9
sécurité fonctionnelle
Remplacer la référence par la nouvelle référence suivante:

[CEI 61508-4, 3.1.12 modifiée]

3.2.10
phénomène dangereux (pour les machines)
risque (au sens de phénomène dangereux)
Remplacer la référence par la nouvelle référence suivante:

[ISO 12100, 3.6 modifiée]

3.2.11
situation dangereuse
Remplacer la référence par la nouvelle référence suivante:

[ISO 12100, 3.10 modifiée]

3.2.12
mesure de prévention
Remplacer la référence par la nouvelle référence suivante:

[ISO 12100, 3.19 modifiée]

3.2.13
risque
Remplacer la référence par la nouvelle référence suivante:

[ISO 12100, 3.12]

3.2.15
fonction de sécurité
Remplacer la référence par la nouvelle référence suivante:

[ISO 12100, 3.30]

3.2.19
intégrité de sécurité
Remplacer la référence par la nouvelle référence suivante:

[CEI 61508-4, 3.5.4 modifiée]

3.2.20
intégrité de sécurité du matériel
Remplacer la référence par la nouvelle référence suivante:

[CEI 61508-4, 3.5.7 modifiée]

3.2.21
intégrité de sécurité du logiciel
Remplacer la référence par la nouvelle référence suivante:

[CEI 61508-4, 3.5.5 modifiée]

3.2.22
intégrité de sécurité systématique
Remplacer la référence par la nouvelle référence suivante:

[CEI 61508-4, 3.5.6 modifiée]

3.2.23
niveau d'intégrité de sécurité
SIL
Remplacer la référence par la nouvelle référence suivante:

[CEI 61508-4, 3.5.8 modifiée]

3.2.26
mode à faible sollicitation
Remplacer le premier alinéa par le nouvel alinéa suivant:

mode de fonctionnement dans lequel la fréquence des sollicitations sur un SRECS n'est pas supérieure à une par an

3.2.27
mode à forte sollicitation ou continu
Remplacer le premier alinéa par le nouvel alinéa suivant:

mode de fonctionnement dans lequel la fréquence des sollicitations sur un SRECS est supérieure à une par an ou dans lequel la SRCF maintient la machine dans un état de sécurité en fonctionnement normal

Remplacer la référence par la nouvelle référence suivante:

[CEI 61508-4, 3.5.16 modifiée]

3.2.28
probabilité de défaillance dangereuse par heure
$\boldsymbol{PFH_D}$
Remplacer la définition 3.2.28 par la nouvelle définition suivante:

3.2.28
probabilité de défaillance dangereuse par heure
$\boldsymbol{PFH_D}$
probabilité moyenne, par heure, qu'un système/sous-système relatif à la sécurité présente une défaillance dangereuse l'empêchant de réaliser la fonction de sécurité spécifiée pendant une période de temps donnée

NOTE Il convient de ne pas confondre la PFH_D avec la probabilité de défaillance dangereuse en cas de sollicitation (PFD).

3.2.29
valeur cible des défaillances
Remplacer la référence par la nouvelle référence suivante:

[CEI 61508-4, 3.5.17 modifiée]

3.2.35
architecture
Remplacer la référence par la nouvelle référence suivante:

[CEI 61508-4, 3.3.4 modifiée]

3.2.37
test périodique
Remplacer le premier alinéa par le nouvel alinéa suivant:

test périodique destiné à détecter les défaillances dangereuses cachées et la dégradation d'un SRECS et de ses sous-systèmes de telle sorte que, si nécessaire, le SRECS et ses sous-systèmes puissent être remis dans un état « comme neuf » ou dans un état aussi proche que possible de celui-ci

3.2.38
couverture du diagnostic
Remplacer le premier alinéa par l'alinéa suivant:

proportion de défaillances dangereuses détectées par les essais de diagnostic en ligne automatiques

Ajouter, à la fin de ce paragraphe, la nouvelle Note 2 *suivante:*

NOTE 2 La proportion de défaillances dangereuses détectées est calculée en divisant le taux de défaillances dangereuses détectées par les essais de diagnostic en ligne automatiques par le taux total de défaillances dangereuses.

et numéroter la note existante comme étant la Note 1.

3.2.40
défaillance dangereuse
Supprimer la référence « [CEI 61508-4, 3.6.7 modifiée] ».

3.2.41
défaillance en sécurité
Supprimer la référence « [CEI 61508-4, 3.6.8 modifiée] ».

3.2.43
défaillance de cause commune
CCF
La correction ne concerne que le texte anglais.

5.2.3 Spécification des exigences fonctionnelles pour les SRCF

Remplacer le texte existant de ce paragraphe (y compris 5.2.3.1 et 5.2.3.2) par le suivant:

La spécification des exigences fonctionnelles pour les SRCF doit décrire les informations concernant chaque SRCF à réaliser y compris, pour autant qu'applicable:

– la(les) condition(s) (par exemple mode de fonctionnement) de la machine dans laquelle la SRCF doit être active ou désactivée;
– la priorité associée à ces fonctions, lesquelles peuvent être actives simultanément et provoquer une action conflictuelle;
– la fréquence de fonctionnement pour chaque SRCF;
– le temps de réponse requis de chaque SRCF;
– l'(les)interface(s) des SRCF avec les autres composants de la machine;
– les temps de réponse requis (par exemple des dispositifs d'entrée et de sortie);
– une description de chaque SRCF;
– une description de la (des) fonction(s) réaction(s) à l'anomalie et de toutes les contraintes s'exerçant, par exemple, redémarrage ou fonctionnement continu de la machine, dans les cas où la première réaction à l'anomalie est d'arrêter la machine;
– une description de l'environnement de fonctionnement (par exemple température, humidité, poussière, substances chimiques, vibration mécanique et choc);
– les tests et les installations associées (par exemple les équipements de test, les ports d'accès de test);
– les taux de cycles de manœuvres, le cycle de fonctionnement et/ou la catégorie d'emploi, pour les dispositifs électromécaniques destinés à être utilisés dans la SRCF.

NOTE 1 En plus des exigences de la CEI 61000-6-2, quand un SRECS est destiné à être utilisé dans un environnement industriel, les niveaux d'immunité électromagnétique (EM) sont donnés dans la CEI 61326-3-1. Il convient que les SRECS destinés à être utilisés dans un autre environnement EM (par exemple, résidentiel) aient des niveaux d'immunité basés sur ceux qui sont spécifiés dans les différentes normes CEM (par exemple, pour un environnement résidentiel, la CEI 61000-6-1).

NOTE 2 Lors de la spécification des niveaux d'immunité EM, il est nécessaire d'examiner si les niveaux utilisés dans les différentes normes CEM couvrent les cas qui peuvent se produire dans une application SRECS même avec une faible probabilité d'occurrence.

NOTE 3 Le critère d'aptitude de l'immunité EM pour la sécurité fonctionnelle d'un SRECS est donné en 6.4.3.

6.4 Exigences pour l'intégrité de sécurité systématique des SRECS

Supprimer la note.

6.4.2 Exigences pour la maîtrise des anomalies systématiques

Remplacer la Note 2 par la suivante:

NOTE 2 Des informations complémentaires peuvent être trouvées dans la CEI 61784-3 et la CEI 61508-2.

6.4.3 Compatibilité électromagnétique (CEM) – Immunité

Remplacer, dans ce paragraphe, « en Annexe E » *par* « dans la CEI 61326-3-1 ».

6.6.3.1 Généralités

Remplacer la dernière phrase de ce paragraphe par la suivante:

Le niveau SIL pouvant être réalisé par le SRECS est inférieur ou égal à la valeur la plus faible des SILCL de tous les sous-systèmes que comprend le SRECS.

6.6.3.4 Intégrité de sécurité systématique

Supprimer le paragraphe 6.6.3.4.

6.7.2.1

Remplacer ce paragraphe par le nouveau paragraphe suivant:

6.7.2.1 Le sous-système doit être réalisé soit par le choix (voir 6.7.3), soit par la conception (voir 6.7.4) conformément à sa spécification des exigences de sécurité (voir 6.6.2.1.7), en prenant en compte toutes les exigences de 6.2. Le(s) sous-système(s) incorporant des composants complexes doit (doivent) se conformer à la CEI 61508-2 et à la CEI 61508-3 pour autant qu'applicables pour le niveau SIL exigé, et la conception doit utiliser le parcours 1_H (voir CEI 61508-2:2010, 7.4.4.2).

EXCEPTION: Lorsqu'un sous-système comprend un composant complexe en tant qu'élément de sous-système, 6.7.4.2.3 s'applique.

NOTE Dans la présente norme, il est supposé que la conception des sous-systèmes ou éléments de sous-système électroniques programmables complexes est conforme aux exigences appropriées de la CEI 61508 et utilise le parcours 1_H (voir CEI 61508-2:2010, 7.4.4.2). Il est considéré que le parcours 2_H (voir CEI 61508-2:2010, 7.4.4.3) ne convient pas aux machines à usage général. La présente norme ne traite donc pas du parcours 2_H. Elle fournit une méthodologie pour l'utilisation, plus que pour le développement, de tels sous-systèmes et éléments de sous-système en tant que partie d'un SRECS.

6.7.2.2

Remplacer la Note 1 du point b) par la suivante:

NOTE 1 Pour les sous-systèmes électromécaniques, il convient que la probabilité de défaillance soit estimée en prenant en compte le nombre de cycles de manœuvres déclaré par le fabricant et le cycle de fonctionnement (voir 5.2.3). Il convient que cette information soit basée sur une valeur B10 (voir CEI 61649) dans les conditions de fonctionnement spécifiées par le fabricant. Voir, par exemple, CEI 60947-4-1, Annexe K.

6.7.3.2

Ajouter le texte suivant à la fin de la première phrase :

et la conception doit utiliser le parcours 1_H (voir CEI 61508-2:2010, 7.4.4.2).

Ajouter la note suivante à la fin de ce paragraphe: