

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2012 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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It also gives information on projects, replaced and withdrawn publications.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.

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

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

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]”.