IEC/TR 62061-1

Edition 1.0 2010-07

TECHNICAL REPORT

RAPPORT TECHNIQUE

Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery

Lignes directrices relatives à l'application de l'ISO 13849-1 et de la CEI 62061 dans la conception des systèmes de commande des machines relatifs à la sécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

R

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-88912-042-0

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 3
INTRODUCTION 5
1 Scope 6
2 General 6
3 Comparison of standards 6
4 Risk estimation and assignment of required performance 7
5 Safety requirements specification 7
6 Assignment of performance targets: PL versus SIL 8
7 System design 9
7.1 General requirements for system design using IEC 62061 and ISO 13849-1 9
7.2 Estimation of PFH_D and $MTTF_d$ and the use of fault exclusions 9
7.3 System design using subsystems or SRP/CS that conform to either IEC 62061 or ISO 13849-1 10
7.4 System design using subsystems or SRP/CS that have been designed using other IEC or ISO standards 10
8 Example 10
8.1 General 10
8.2 Simplified example of the design and validation of a safety-related control system implementing a specified safety-related control function 11
8.3 Conclusion 18
Bibliography 19

Figure 1 – Example implementation of the safety function 11
Figure 2 – Safety-related block diagram 13
Figure 3 – Safety-related block diagram for calculation according to ISO 13849-1 13
Figure 4 – Logical representation of subsystem D 15

Table 1 – Relationship between PLs and SILs based on the average probability of dangerous failure per hour 8
Table 2 – Architectural constraints on subsystems' maximum SIL CL that can be claimed for an SRCF using this subsystem 17

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

GUIDANCE ON THE APPLICATION OF ISO 13849-1 AND IEC 62061 IN THE DESIGN OF SAFETY-RELATED CONTROL SYSTEMS FOR MACHINERY

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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 62016-1, which is a technical report, has been prepared jointly by Technical Committee ISO/TC 199, *Safety of machinery*, and Technical Committee IEC/TC 44, *Safety of machinery – Electrotechnical aspects.* The draft was circulated for voting to the national bodies of both ISO and IEC. These technical committees have agreed that no modification will be made to this Technical Report except by mutual agreement[1].

[1] This Technical Report is published at the ISO as ISO/TR 23849.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
44/598/DTR	44/608/RVC

Full information on the voting for the approval of this technical report 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.

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

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

INTRODUCTION

This Technical Report has been prepared by experts from both IEC/TC 44/WG 7 and ISO/TC 199/WG 8 in response to requests from their Technical Committees to explain the relationship between IEC 62061 and ISO 13849-1. In particular, it is intended to assist users of these International Standards in terms of the interaction(s) that can exist between the standards to ensure that confidence can be given to the design of safety-related systems made in accordance with either standard.

It is intended that this Technical Report be incorporated into both IEC 62061 and ISO 13849-1 by means of corrigenda that reference the published version of this document. These corrigenda will also remove the information given in Table 1, *Recommended application of IEC 62061 and ISO 13849-1*, provided in the common introduction to both standards, which is now recognized as being out of date. Subsequently, it is intended to merge ISO 13849-1 and IEC 62061 by means of a JWG of ISO/TC 199 and IEC/TC 44.

GUIDANCE ON THE APPLICATION OF ISO 13849-1 AND IEC 62061 IN THE DESIGN OF SAFETY-RELATED CONTROL SYSTEMS FOR MACHINERY

1 Scope

This Technical Report is intended to explain the application of IEC 62061 and ISO 13849-1[2)] in the design of safety-related control systems for machinery.

2) This Technical Report considers ISO 13849-1:2006 rather than ISO 13849-1:1999, which has been withdrawn.

SOMMAIRE

AVANT-PROPOS 21
INTRODUCTION 23
1 Domaine d'application 24
2 Généralités 24
3 Comparaison des normes 25
4 Estimation du risque et détermination de la performance requise 25
5 Spécification des exigences de sécurité 26
6 Détermination des objectifs de performance: PL ou SIL 26
7 Conception du système 27
7.1 Exigences générales pour la conception des système selon la CEI 62061 et l'ISO 13849-1 27
7.2 Estimation de la PFH_D et du $MTTF_d$ et utilisation des exclusions d'anomalie 27
7.3 Conception de système à partir de sous-systèmes ou de SRP/CS conformes à la CEI 62061 ou à l'ISO 13849-1 28
7.4 Conception de système à partir de sous-systèmes ou de SRP/CS conçus d'après d'autres normes CEI ou ISO 28
8 Exemple 29
8.1 Généralités 29
8.2 Exemple simplifié des conception et validation d'un système de commande relatif à la sécurité faisant usage d'une fonction de commande particulière relative à la sécurité 29
8.3 Conclusion 37
Bibliographie 38

Figure 1 – Exemple de mise en œuvre de la fonction de sécurité 30
Figure 2 – Schéma fonctionnel relatif à la sécurité 32
Figure 3 – Schéma fonctionnel relatif à la sécurité pour un calcul conformément à l'ISO 13849-1 32
Figure 4 – Représentation logique d'un sous-système de type D 34

Tableau 1 – Relation entre PL et SIL basée sur la probabilité moyenne d'une défaillance dangereuse par heure 26
Tableau 2 – Contraintes architecturales sur le SIL CL de sous-système maximal qui puisse être revendiquées pour une SRCF utilisant ce sous-système 36

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

LIGNES DIRECTRICES RELATIVES À L'APPLICATION DE L'ISO 13849-1 ET DE LA CEI 62061 DANS LA CONCEPTION DES SYSTÈMES DE COMMANDE DES MACHINES RELATIFS À LA SÉCURITÉ

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 co mité 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 propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La tâche principale des comités d'études de la CEI est l'élaboration des Normes internationales. Toutefois, un comité d'études peut proposer la publication d'un rapport technique lorsqu'il a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales, cela pouvant comprendre, par exemple, des informations sur l'état de la technique.

La CEI 62016-1, qui est un rapport technique, a été élaboré conjointement par le comité technique ISO/TC 199, *Sécurité des machines*, et le comité technique CEI/TC 44, *Sécurité des machines – Aspects électrotechniques*. Le projet a été soumis aux organismes nationaux de l'ISO et de la CEI pour vote. Les comités techniques concernés ont convenu de n'apporter aucune modification au présent Rapport technique sans accord mutuel[1].

_____

[1] Ce rapport technique est publié à l'ISO sous le numéro ISO/TR 23849.

Le texte de ce rapport technique est issu des documents suivants:

Projet d'enquête	Rapport de vote
44/598/DTR	44/608/RVC

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

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

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.

INTRODUCTION

Le présent Rapport technique a été préparé par des experts du CEI/TC 44/GT 7 et de l'ISO/TC 199/GT 8 en réponse aux demandes de leurs comités techniques pour expliquer la relation entre la CEI 62061 et l'ISO 13849-1. Il est en particulier destiné à aider les utilisateurs de ces Normes internationales concernant les interactions qui peuvent exister entre les normes, afin de garantir que la conception des systèmes de sécurité élaborés conformément à l'une ou l'autre norme soit fiable.

Il est prévu d'intégrer le présent Rapport technique dans la CEI 62061 et dans l'ISO 13849-1, au moyen de rectificatifs faisant référence à la version publiée du présent document. Ces rectificatifs retireront également les informations du Tableau 1, *Utilisation recommandée de la CEI 62061 et de l'ISO 13849-1*, fournies dans l'introduction commune aux deux normes et aujourd'hui reconnues comme n'étant plus d'actualité. Par la suite, il est prévu de fusionner l'ISO 13849-1 et la CEI 62061 par le biais d'un groupe de travail mixte de l'ISO/TC 199 et du CEI/TC 44.

LIGNES DIRECTRICES RELATIVES À L'APPLICATION DE L'ISO 13849-1 ET DE LA CEI 62061 DANS LA CONCEPTION DES SYSTÈMES DE COMMANDE DES MACHINES RELATIFS À LA SÉCURITÉ

1 Domaine d'application

Le présent Rapport technique a pour objet d'expliquer l'application de la CEI 62061 et de l'ISO 13849-1[2)] dans la conception des systèmes de commande des machines relatifs à la sécurité.

2) Le présent Rapport technique s'appuie sur l'ISO 13849-1:2006 plutôt que sur l'ISO 13849-1:1999 qu'elle remplace.