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

IEC/TR 62061-1:2010

Documents
Document Sharing Hub

Full document details: IEC TR 62061-1 2010

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 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 Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

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.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

Documents
Document Sharing Hub

Full document details: IEC TR 62061-1 2010

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

Documents
Document Sharing Hub

Full document details: IEC TR 62061-1 2010

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

Documents
Document Sharing Hub
Full document details: IEC TR 62061-1 2010

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.

Documents
Document Sharing Hub

Full document details: IEC TR 62061-1 2010

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.

Documents
Document Sharing Hub

Full document details: IEC TR 62061-1 2010

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.

Documents
Document Sharing Hub

Full document details: IEC TR 62061-1 2010

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 General

2.1 Both IEC 62061 and ISO 13849-1 specify requirements for the design and implementation of safety-related control systems of machinery[3)]. The methods developed in both of these standards are different but, when correctly applied, can achieve a comparable level of risk reduction.

2.2 These standards classify safety-related control systems that implement safety functions into levels that are defined in terms of their probability of dangerous failure per hour. ISO 13849-1 has five Performance Levels (PLs), a, b, c, d and e, while IEC 62061 has three safety integrity levels (SILs), 1, 2 and 3.

2.3 Product standards (type-C) committees specify the safety requirements for safety-related control systems and it is recommended that these committees classify the levels of confidence required for them in terms of PLs and SILs.

2.4 Machinery designers may choose to use either IEC 62061 or ISO 13849-1 depending on the specific features of the application.

2.5 The selection and use of either standard is likely to be determined by, for example:

– previous knowledge and experience in the design of machinery safety-related control systems based upon the concept of categories described in ISO 13849-1:1999 can mean that the use of ISO 13849-1:2006 is more appropriate;
– safety-related control systems based upon media other than electrical can mean that the use of ISO 13849-1 is more appropriate;
– customer requirements to demonstrate the safety integrity of a machine safety-related control system in terms of a SIL can mean that the use of IEC 62061 is more appropriate;
– safety-related control systems of machinery used in, for example, the process industries, where other safety-related systems (such as safety instrumented systems in accordance with IEC 61511) are characterized in terms of SILs, can mean that the use of IEC 62061 is more appropriate.

3 Comparison of standards

3.1 A comparison of the technical requirements in ISO 13849-1 and IEC 62061 has been carried out in respect of the following aspects:

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

3) These standards have been adopted by the European standardization bodies CEN and CENELEC as ISO 13849-1 and EN 62061, respectively, where they are published with the status of transposed harmonized standards under the Machinery Directive (98/37/EC and 2006/42/EC). Under the conditions of their publication, the correct use of either of these standards is presumed to conform to the relevant essential safety requirements of the Machinery Directive (98/37/EC and 2006/42/EC).

AVA Documents Document Sharing Hub

Full document details: IEC TR 62061-1 2010

– terminology;
– risk estimation and performance allocation;
– safety requirements specification;
– systematic integrity requirements;
– diagnostic functions;
– software safety requirements.

3.2 Additionally, an evaluation of the use of the simplified mathematical formulae to determine the probability of dangerous failures (PFH_D) and $MTTF_d$ according to both standards has been carried out.

3.3 The conclusions from this work are the following.

– Safety-related control systems can be designed to achieve acceptable levels of functional safety using either of the two standards by integrating non-complex[4)] SRECS (safety-related electrical control system) subsystems or SRP/CS (safety-related parts of a control system) designed in accordance with IEC 62061 and ISO 13849-1, respectively.
– Both standards can also be used to provide design solutions for complex SRECS and SRP/CS by integrating electrical/electronic/programmable electronic subsystems designed in accordance with IEC 61508.
– Both standards currently have value to users in the machinery sector and benefits will be gained from experience in their use. Feedback over a reasonable period on their practical application is essential to support any future initiatives to move towards a standard that merges the contents of both IEC 62061 and ISO 13849-1.
– Differences exist in detail and it is recognized that some concepts (e.g. functional safety management) will need further work to establish equivalence between respective design methodologies and some technical requirements.

4 Risk estimation and assignment of required performance

4.1 A comparison has been carried out on the use of the methods to assign a SIL and/or PL_r to a specific safety function. This has established that there is a good level of correspondence between the respective methods provided in Annex A of each standard.

4.2 It is important, regardless of which method is used, that attention be given to ensure that appropriate judgements are made on the risk parameters to determine the SIL and/or PL_r that is likely to apply to a specific safety function. These judgements can often best be made by bringing together a range of personnel (e.g. design, maintenance, operators) to ensure that the hazards that may be present at machinery are properly understood.

4.3 Further information on the process of risk estimation and the assignment of performance targets can be found in ISO 14121-1 and IEC 61508-5.

5 Safety requirements specification

5.1 A first stage in the respective methodologies of both ISO 13849-1 and IEC 62061 requires that the safety function(s) to be implemented by the safety-related control system are specified.

5.2 An assessment should have been performed relevant to each safety function that is to be implemented by a control circuit by, for example, using ISO 13849-1, Annex A, or IEC 62061, Annex A. This should have determined what risk reduction needs to be provided

4) Although there is no definition for the term “non-complex” SRECS or SRP/CS this should be considered equivalent to low complexity in the context of IEC 62061:2005, 3.2.7.

AVA Documents
Document Sharing Hub

Full document details: IEC TR 62061-1 2010

by each particular safety function at a machine and, in turn, what level of confidence is required for the control circuit that performs this safety function.

5.3 The level of confidence specified as a PL and/or a SIL is relevant to a specific safety function.

5.4 The following shows the information that should be provided in relation to safety functions by a product (type-C) standard.

Safety function(s) to be implemented by a control circuit:

Name of safety function

Description of the function

Required level of performance according to ISO 13849-1: PL_r a to e

and/or

Required safety integrity according to IEC 62061: SIL 1 to 3

6 Assignment of performance targets: PL versus SIL

Table 1 gives the relationship between PL and SIL based on the average probability of a dangerous failure per hour. However, both standards have requirements (e.g. systematic safety integrity) additional to these probabilistic targets that are also to be applied to a safety-related control system. The rigour of these requirements is related to the respective PL and SIL.

Table 1 – Relationship between PLs and SILs based on the average probability of dangerous failure per hour

Performance level (PL)	Average probability of a dangerous failure per hour (1/h)	Safety integrity level (SIL)
a	$\geq 10^{-5}$ to $< 10^{-4}$	No special safety requirements
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

Documents
Document Sharing Hub
Full document details: IEC TR 62061-1 2010

7 System design

7.1 General requirements for system design using IEC 62061 and ISO 13849-1

The following aspects should be taken into account when designing a SRECS/SRP/CS.

– When applied within the limitations of their respective scopes either of the two standards can be used to design safety-related control systems with acceptable functional safety, as indicated by the achieved SIL or PL.

– Non-complex safety-related parts that are designed to the relevant PL in accordance with ISO 13849-1 can be integrated as subsystems into a safety-related electrical control system (SRECS) designed in accordance with IEC 62061. Any complex safety-related parts that are designed to the relevant PL in accordance with ISO 13849-1 can be integrated into safety-related parts of a control system (SRP/CS) designed in accordance with ISO 13849-1.

– Any non-complex subsystem that is designed in accordance with IEC 62061 to the relevant SIL can be integrated as a safety-related part into a combination of SRP/CS designed in accordance with ISO 13849-1.

– Any complex subsystem that is designed in accordance with IEC 61508 to the relevant SIL can be integrated as a safety-related part into a combination of SRP/CS designed in accordance with ISO 13849-1 or as subsystems into a SRECS designed in accordance with IEC 62061.

7.2 Estimation of PFH_D and $MTTF_d$ and the use of fault exclusions

7.2.1 PFH_D and $MTTF_d$

7.2.1.1 The value of $MTTF_d$ in the context of ISO 13849-1 relates to a single channel SRP/CS without diagnostics and, only in this case, is the reciprocal of PFH_D in IEC 62061.

7.2.1.2 $MTTF_d$ is a parameter of a component(s) and/or single channel without any consideration being given to factors such as diagnostics and architecture, while PFH_D is a parameter of a subsystem that takes into account the contribution of factors such as diagnostics and architecture depending on the design structure.

7.2.1.3 Annex K of ISO 13849-1 describes the relationship between $MTTF_d$ and the PFH_D of an SRP/CS for different architectures classified in terms of category and diagnostic coverage (DC).

7.2.1.4 The estimation of PFH_D for a series connected combination of SRP/CS in accordance with ISO 13849-1 can also be performed by adding PFH_D values (e.g. derived from Annex K of ISO 13849-1) of each SRP/CS in a similar manner to that used with subsystems in IEC 62061.

7.2.2 Use of fault exclusions

7.2.2.1 Both standards permit the use of fault exclusions, see 6.7.7 of IEC 62061 and 7.3 of ISO 13849-1. IEC 62061 does not permit the use of fault exclusions for a SRECS without hardware fault tolerance required to achieve SIL 3 without hardware fault tolerance.

7.2.2.2 It is important that where fault exclusions are used that they be properly justified and valid for the intended lifetime of an SRP/CS or SRECS.

7.2.2.3 In general, where PL e or SIL 3 is specified for a safety function to be implemented by an SRP/CS or SRECS, it is not normal to rely upon fault exclusions alone to achieve this level of performance. This is dependent upon the technology used and the intended operating

AVA Documents Document Sharing Hub

Full document details: IEC TR 62061-1 2010

environment. Therefore it is essential that the designer takes additional care in the use of fault exclusions as PL or SIL increases.

7.2.2.4 In general the use of fault exclusions is not applicable to the mechanical aspects of electromechanical position switches and manually operated switches (e.g. an emergency stop device) in order to achieve PL e or SIL 3 in the design of an SRP/CS or SRECS. Those fault exclusions that can be applied to specific mechanical fault conditions (e.g. wear/corrosion, fracture) are described in ISO 13849-2.

7.2.2.5 For example, a door interlocking system that has to achieve PL e or SIL 3 will need to incorporate a minimum fault tolerance of 1 (e.g. two conventional mechanical position switches) in order to achieve this level of performance since it is not normally justifiable to exclude faults such as broken switch actuators. However, it may be acceptable to exclude faults such as short circuit of wiring within a control panel designed in accordance with relevant standards.

7.2.2.6 Further information on the use of fault exclusions is to be provided in the forthcoming revision of ISO 13849-2 currently being developed by ISO/TC 199/WG 8.

7.3 System design using subsystems or SRP/CS that conform to either IEC 62061 or ISO 13849-1

7.3.1 In all cases where subsystems or safety-related parts of control systems are designed to either ISO 13849-1 or IEC 62061, conformance to the system level standard can only be claimed if all the requirements of the system level standard (as relevant) are satisfied.

7.3.2 For the design of a subsystem or a part of safety-related parts of control systems either IEC 62061 or ISO 13849-1, respectively, shall be satisfied. It is permissible to satisfy more than one of these standards provided that those standards used are fully complied with.

7.3.3 It is not permissible to mix requirements of the standards when designing a subsystem or part of safety-related parts of control systems.

7.4 System design using subsystems or SRP/CS that have been designed using other IEC or ISO standards

7.4.1 It may be possible to select subsystems, for example, electrosensitive protective equipment, that comply with relevant IEC or ISO product standards and either IEC 61508, IEC 62061 or ISO 13849-1 in their design. The vendor(s) of these types of subsystems should provide the necessary information to facilitate their integration into a safety-related control system in accordance with either IEC 62061 or ISO 13849-1.

7.4.2 Subsystems, for example, adjustable speed electrical power drive systems, that have been designed using product standards, such as IEC 61800-5-2, that implement the requirements of IEC 61508 can be used in safety-related control systems in accordance with IEC 62061 (see also 6.7.3 of IEC 62061) and ISO 13849-1.

7.4.3 In accordance with IEC 62061 other subsystems that have been designed using IEC, ISO or other standard(s) are subject to 6.7.3 of IEC 62061.

8 Example

8.1 General

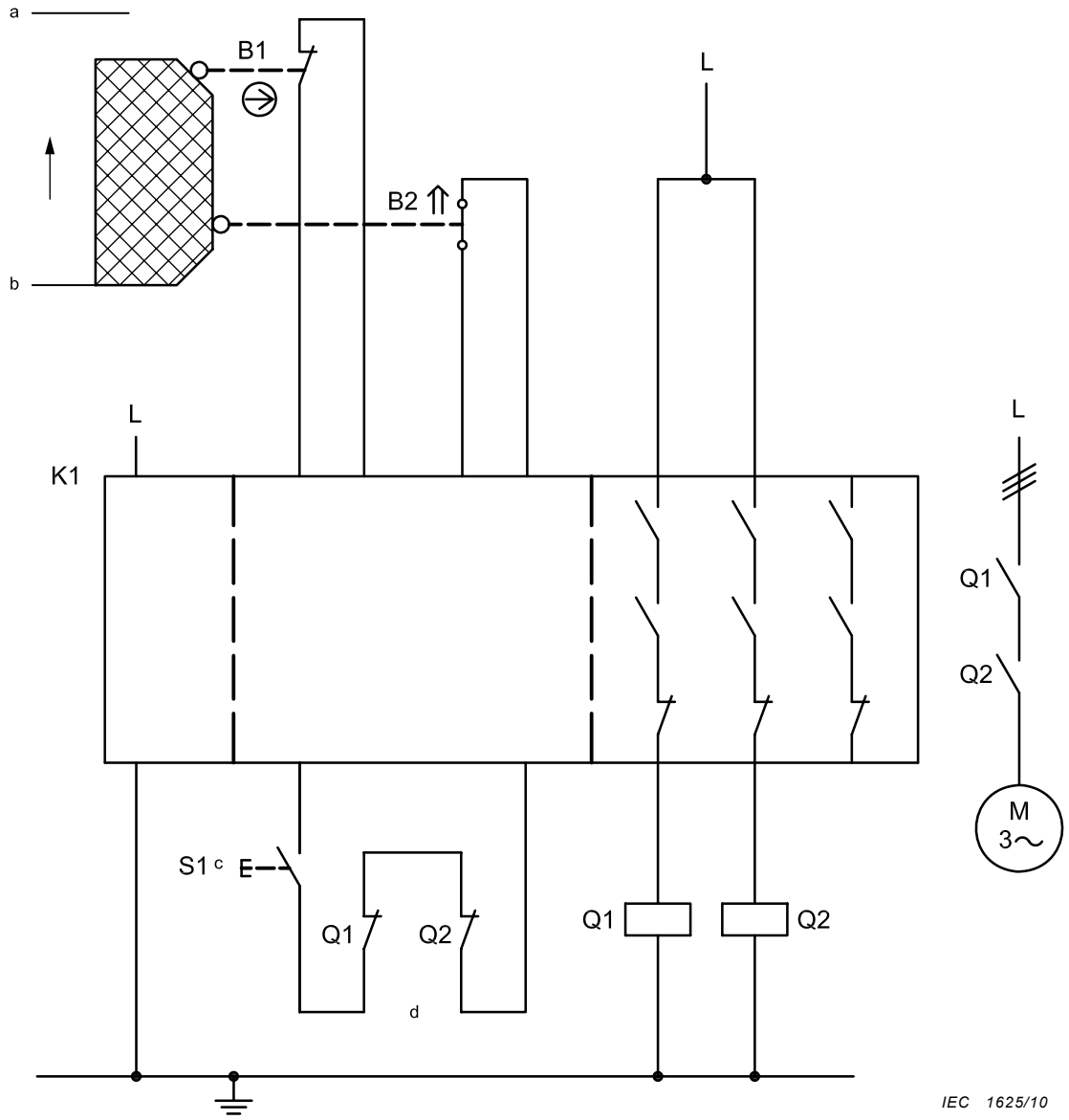
The following example assumes that all the requirements of the standards have been satisfied. The example is only intended to demonstrate specific aspects of the application of the standards.

Documents
Document Sharing Hub

Full document details: IEC TR 62061-1 2010

8.2 Simplified example of the design and validation of a safety-related control system implementing a specified safety-related control function

8.2.1 This simplified example is intended to demonstrate the use of subsystems or SRP/CS that comply with IEC 62061 and/or ISO 13849-1 in a SRECS/SRP/CS. The example is based on the implementation of a safety function described as a safety-related stop function associated with position monitoring of a moveable guard, with a specified safety integrity level of SIL 3/required performance level PL_r e as described in Figure 1.



⇑ shown in actuated position

a Open.

b Closed.

c START.

d Feedback circuit.

Figure 1 – Example implementation of the safety function

8.2.2 The following information is relevant to the safety requirements specification for this example.

Documents
Document Sharing Hub
Full document details: IEC TR 62061-1 2010