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 It also gives information on projects, withdrawn and replaced publications.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

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

CONTENTS

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 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).

– 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.

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

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

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.

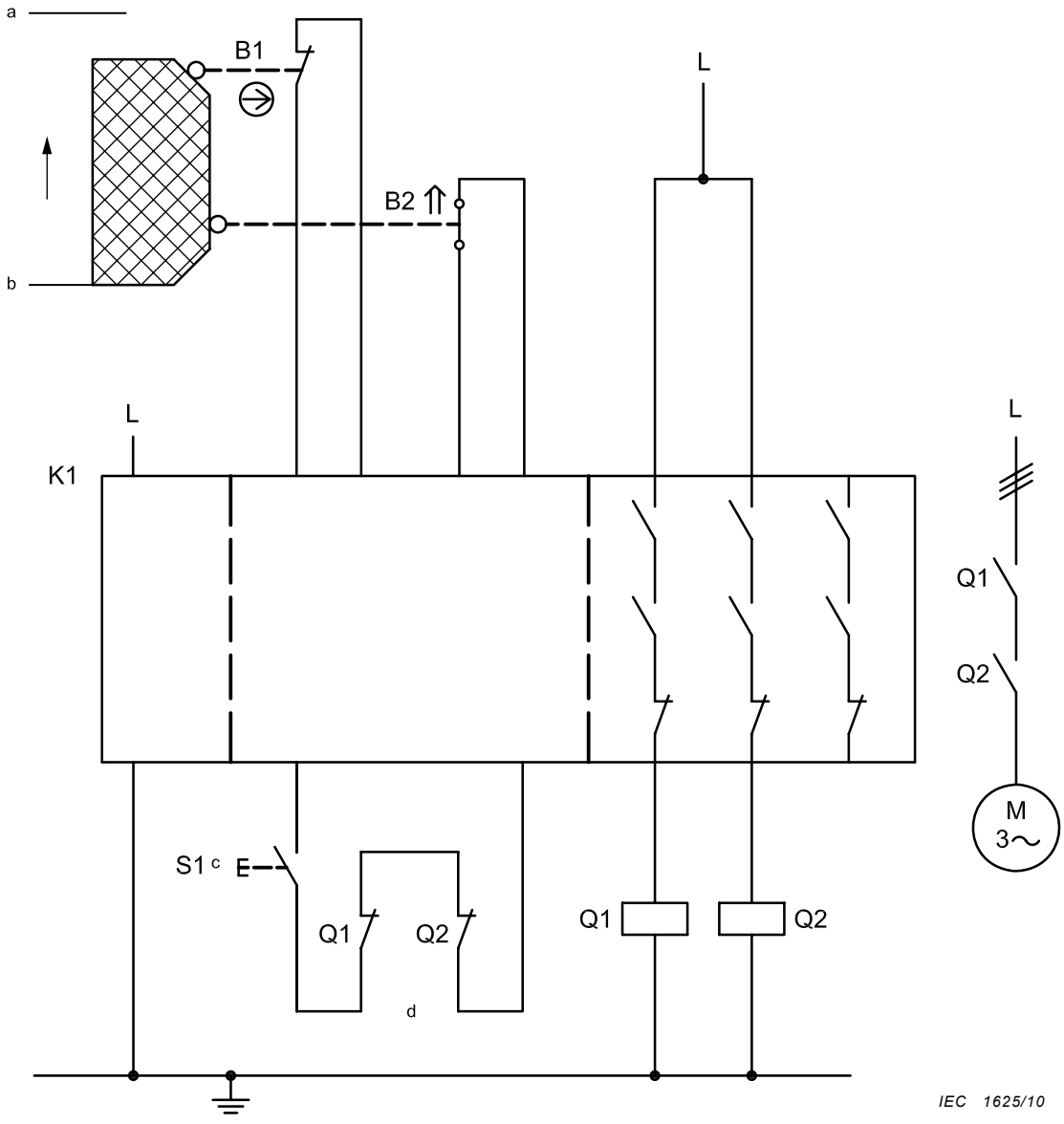
8 Example

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.

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.

Safety function

– Safety-related stop function, initiated by a protective device: opening of the moveable guard initiates the safety function STO (safe torque off).

Functional description

– Trapping hazards are safeguarded by means of a moveable guard (protective grating). Opening of the interlocked guard is detected by two position switches, B1/B2, employing a break contact/make contact combination, and evaluation by a central safety module, K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.

– The position switches are monitored for plausibility in K1 for the purpose of fault detection. Faults in Q1 and Q2 are detected by a start-up test in K1. A start command is successful only if Q1 and Q2 had previously dropped out. Start-up testing by opening and closing of the interlocked guard is not required.

– The safety function remains intact in the event of a component failure. Faults are detected during operation or at actuation (opening and closing) of the interlocked guard resulting in the dropping out of Q1 and Q2 and operational disabling.

– An accumulation of more than two faults in the period between two successive actuations can lead to loss of the safety function.

8.2.3 The following features should also be provided.

– Basic and well-tried safety principles are observed (e.g. the load current for the contactors Q1 and Q2 is de-rated by a factor of 50 %) and the requirements of Category B are met. Protective circuits (e.g. contact protection) are implemented.

– A stable arrangement of the protective devices is assured for actuation of the position switches.

– Switch B1 is a position switch with direct opening action in accordance with IEC 60947-5-1:2003, Annex K.

– The supply conductors to position switches B1 and B2 are laid separately or with protection.

8.2.4 The following information is available from the manufacturers for each part within the design of SRP/CS.

– The safety module K1 is declared by the manufacturer[5)] as satisfying the requirements for Category 4, PL e and SIL CL 3.

– The contactors Q1 and Q2 possess mechanically linked contact elements conforming with IEC 60947-5-1:2003, Annex L.

8.2.5 The following observation can be made on the design of SRP/CS and/or SRECS.

– Category 4 can only be achieved where several mechanical position switches for different protective devices are not connected in a series arrangement (i.e. no cascading). This is necessary, as faults in the switches cannot otherwise be detected.

8.2.6 Calculation of the probability of failure in accordance with ISO 13849-1

Figure 2 shows a logic subsystem (safety module K1) to which two-channel input and output elements are connected. Since an abstraction of the hardware level is already performed in the safety-related block diagram, the sequence of the subsystems is in principle interchangeable. It is therefore recommended that subsystems sharing the same structure be grouped together, as shown in Figure 3. This makes calculation of the PL simpler by reducing the number of times limitation of the $MTTF_d$ of a channel to 100 years is performed in the estimation.

5) This module is dealt with as a subsystem and, as such, the $MTTF_d$ of its individual channels need not be given (see 7.2.1.1).

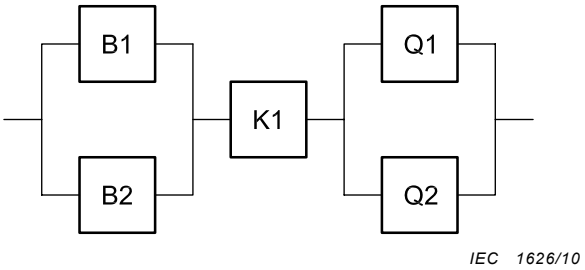
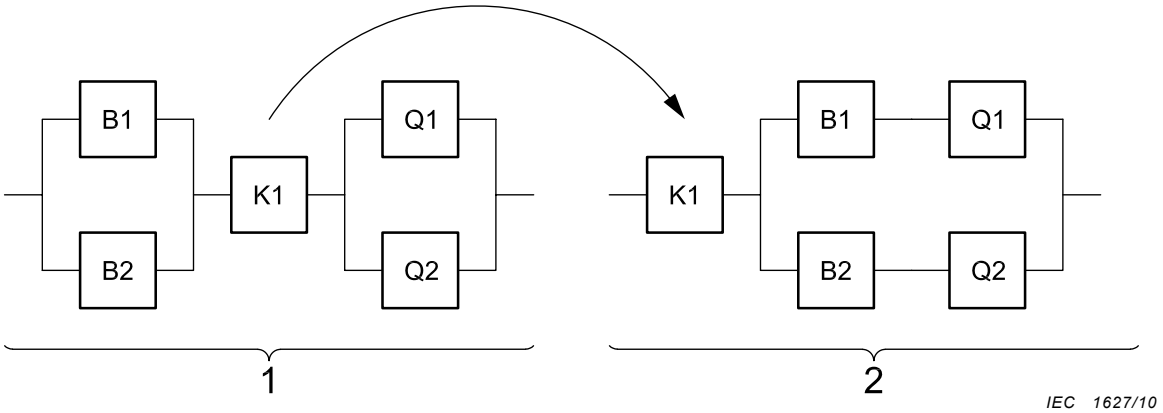


Figure 2 – Safety-related block diagram



Key

1 hardware related representation: three SRP/CS as subsystems

2 simplified logical representation: two SRP/CS as subsystems

Figure 3 – Safety-related block diagram for calculation according to ISO 13849-1

The probability of failure of the safety module K1 is declared by the manufacturer and is added at the end of the calculation [2,31 × 10^{-9} per hour (manufacturer's value), suitable for PL e]. For the remaining subsystem, the probability of failure is calculated as follows:

– $MTTF_d$: the B_{10d} value of 1 000 000 cycles [manufacturer's value] is stated for the mechanical part of B1. For the position switch B2, the B_{10d} value is 500 000 cycles (manufacturer's value). At 365 working days per year, 24 working hours per day and a cycle time of 900 s (15 min), n_{op} is 35 040 cycles per year for these components calculated by using Equations (C.2) and (C.7) of ISO 13849-1:

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600 \frac{s}{h}}{t_{cycle}} = \frac{365 \frac{d}{y} \cdot 24 \frac{h}{d} \cdot 3600 \frac{s}{h}}{900 \frac{s}{cycle}} = 35040 \frac{cycles}{y}$$

$$MTTF_{d,B1} = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = \frac{1\,000\,000 \text{ cycles}}{0{,}1 \cdot 35040 \frac{cycles}{y}} = 285 y$$

$$T_{10d,B1} = \frac{B_{10d}}{n_{op}} = \frac{1\,000\,000 \text{ cycles}}{35040 \frac{cycles}{y}} = 28{,}5 y$$

$$MTTF_{d,B2} = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = \frac{500\,000 \text{ cycles}}{0{,}1 \cdot 35040 \frac{cycles}{y}} = 143 y$$

$$T_{10d,B2} = \frac{B_{10d}}{n_{op}} = \frac{500\,000 \text{ cycles}}{35\,040 \frac{\text{cycles}}{\text{y}}} = 14{,}3\,\text{y}$$

The T_{10d} value of B2 is 14,3 years. After this time B2 shall be replaced if a mission time of 20 years is intended for the whole SRP/CS.

– For the contactors Q1 and Q2, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1 000 000 cycles (manufacturer's value). If 50 % of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value:

$$\text{MTTF}_{d,Q1/Q2} = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = \frac{2\,000\,000 \text{ cycles}}{0{,}1 \cdot 35\,040 \frac{\text{cycles}}{\text{y}}} = 571\,\text{y}$$

$$T_{10d,Q1/Q2} = \frac{B_{10d}}{n_{op}} = \frac{2\,000\,000 \text{ cycles}}{35\,040 \frac{\text{cycles}}{\text{y}}} = 57{,}1\,\text{y}$$

– For both channels the MTTF_d is calculated by using Equation (D.1) of ISO 13849-1:

$$\frac{1}{\text{MTTF}_d} = \sum_{i=1}^{N} \frac{1}{\text{MTTF}_{di}}$$

$$\frac{1}{\text{MTTF}_{d,Ch1}} = \frac{1}{285\,\text{y}} + \frac{1}{571\,\text{y}} = \frac{1}{190\,\text{y}}$$

$$\frac{1}{\text{MTTF}_{d,Ch2}} = \frac{1}{143\,\text{y}} + \frac{1}{571\,\text{y}} = \frac{1}{114\,\text{y}}$$

This gives an $\text{MTTF}_{d,Ch1}$ of 190 years and an $\text{MTTF}_{d,Ch2}$ of 114 years. In accordance with ISO 13849-1 the MTTF_d of both channels is limited to 100 years and, in this case, as the MTTF_d of both channels are equal after limiting it is not necessary to perform symmetrization.

– DC_{avg}: the DC of 99 % for B1 and B2 is based upon plausibility monitoring of the break/make contact combination in K1. The DC of 99 % for contactors Q1 and Q2 is derived from regular monitoring by K1 during start-up. The DC values stated correspond to the DC_{avg} for each subsystem. The DC_{avg} will be calculated according to Equation (E.1) of ISO 13849-1. Because each single DC is 99 %, the DC_{avg} is also 99 %.

– Adequate measures against common-cause failure in the subsystems B1/B2 and Q1/Q2 (70 points): separation (15), well-tried components (5), protection against overvoltage, etc. (15) and environmental conditions (25 + 10).

– Mission time: for the simplified approach of ISO 13849-1 a mission time of 20 years is assumed.

– The subsystem B1/B2/Q1/Q2 corresponds to Category 4 with a high MTTF_d (100 years) and high DC_{avg} (99 %). This results in an average probability of dangerous failure of $2{,}47 \times 10^{-8}$ per hour (see Table K.1 of ISO 13849-1). Following addition of the subsystem K1, the average probability of dangerous failure is $2{,}70 \times 10^{-8}$ per hour. This corresponds to PL e.

8.2.7 Calculation of the probability of failure in accordance with IEC 62061

8.2.7.1 In accordance with 6.6.2 of IEC 62061, the circuit arrangement can be divided into three subsystems: B1/B2, K and Q1/Q2 as shown in the safety-related block diagram.

8.2.7.2 For subsystem K, the probability of failure of $2{,}31 \times 10^{-9}$ per hour and a SIL claim limit of 3 for the safety module K1 is declared by the manufacturer.

8.2.7.3 For the remaining subsystems, the probability of failure can be estimated as follows.

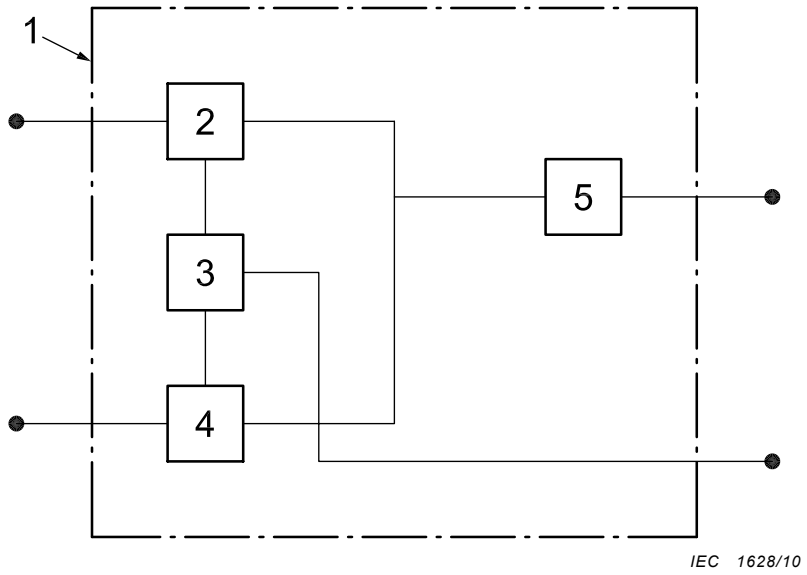
– Subsystem B1/B2: the B_{10d} value of 1 000 000 cycles [manufacturer's value] is stated for the mechanical part of B1. For the position switch B2, the B_{10d} value is 500 000 cycles [manufacturer's value]. At 365 working days per year, 24 working hours per day and a cycle time of 15 min, C is 4 cycles per hour for these components. The failure rate is calculated as $0{,}1 \times C/B_{10d} = 4{,}00 \times 10^{-7}$/h. For B2 this gives a failure rate of $8{,}00 \times 10^{-7}$/h.

NOTE The number of operating cycles, C, of the application according to IEC 62061 corresponds to the mean number of annual operations, n_{op}, according to ISO 13849-1. Since C is stated in cycles per hour and n_{op} in cycles per year, the following relation applies:

$$C = n_{op} \cdot \frac{\text{y}}{365 \cdot 24\text{h}}$$

Thus the mean operation in hours per day and days per year has influence on the value of C as well as of n_{op}.

– The logical architecture of this subsystem equates to diagram D from 6.7.8.2.5 of IEC 62061 as shown in Figure 4.



Key

1 subsystem D
2 subsystem element λ_{De1}
3 diagnostic function(s)
4 subsystem element, λ_{De2}
5 common cause failure

Figure 4 – Logical representation of subsystem D

– The subsystem elements (switches B1 and B2) are of different design, therefore the following, Equation (D.1) from 6.7.8.2.5 of IEC 62061, is used to determine the PFH_D of the subsystem.

$$\lambda_{DssD} = (1-\beta)^2 \left\{ \left[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \right] \times T_2 / 2 + \left[\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \right] \times T_1 / 2 \right\} + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

where

T_2 is the diagnostic test interval; for subsystem B1/B2, this is 15 min.

T_1 is the proof test interval or lifetime, whichever is the smaller. For subsystem B1/B2, the lifetime interval is 125 000 h (14,3 years) at the given rate of use based on the lowest subsystem element T_{10d} value (see ISO 13849-1, C.4.2). Switch B2 has the lowest T_{10d} value. The proof test interval (see Foreword of IEC 62061) is assumed to be 20 years (175 200 h), which is greater than the lifetime. So T_1 is 125 000 h.

β is the susceptibility to common cause failures. This has a value of 5 % (0,05) resulting from 42 points scored in the simplified method in IEC 62061, Annex F. Separation (5 + 5 + 5), assessment/analysis (9) and environmental conditions (9 + 9).

λ_{De1} is the dangerous failure rate of subsystem element 1. For switch B1 this equates to $4{,}00 \times 10^{-7}$/h (see above).

DC_1 is the diagnostic coverage of subsystem element 1. For switch B1, this is estimated to be 99 %, based upon plausibility monitoring of the break/make contacts of B1 and B2 in combination with K1.

λ_{De2} is the dangerous failure rate of subsystem element 2. For switch B2 this equates to $8{,}00 \times 10^{-7}$/h (see above).

DC_2 is the diagnostic coverage of subsystem element 2. For switch B2 this is estimated to be 99 %, based upon plausibility monitoring of the break/make contacts of B1 and B2 in combination with K1.

8.2.7.4 The data above is entered into the formula to give a PFH_D of $3{,}04 \times 10^{-8}$.

8.2.7.5 Similarly, for subsystem Q1/Q2: contactors Q1 and Q2 have a B_{10} value that corresponds under inductive load (AC 3) to an electrical lifetime of 10^6 cycles (manufacturer's value). If 50 % of failures are assumed to be dangerous, the B_{10d} value is produced by doubling the B_{10} value. The value assumed above for C results in a failure rate of $2{,}00 \times 10^{-7}$/h for each contactor.

8.2.7.6 The logical architecture of subsystem Q1/Q2 equates to diagram D from 6.7.8.2.5 of IEC 62061. The subsystem elements (contactors Q1 and Q2) are of the same design, therefore Equation (D.1) is used to determine the PFH_D of the subsystem:

$$\lambda_{DssD} = (1-\beta)^2 \left\{ \left[\lambda_{De}{}^2 \times 2 \times DC \right] \times T_2 / 2 + \left[\lambda_{De}{}^2 \times (1 - DC) \right] \times T_1 \right\} + \beta \times \lambda_{De}$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

where

T_2 is the diagnostic test interval; for subsystem Q1/Q2, this is 15 min.

T_1 is the proof test interval or lifetime, whichever is the smaller; for subsystem Q1/Q2 the lifetime is 500 000 h (57,1 years) at the given usage rate based on the subsystem element T_{10d} value (see ISO 13849-1, C.4.2). The proof test interval (see Foreword of IEC 62061) is assumed to be 20 years (175 200 h), which is smaller than the lifetime. So T_1 is 175 200 h.

λ_{De} is the dangerous failure rate of each subsystem element (contactors Q1 and Q2) = $2{,}00 \times 10^{-7}$/h (see above).

DC is the diagnostic coverage of each subsystem element (contactors Q1 and Q2) = 99 % based upon regular monitoring of mechanically linked mirror contacts by K1 during start-up.

β is the susceptibility to common cause failures; this has a value of 5 % (0,05) resulting from 42 points scored in the simplified method in IEC 62061, Annex F. Separation (5 + 5 + 5), assessment/analysis (9) and environmental conditions (9 + 9).

The data above is entered into the formula that produces a PFH_D of $1{,}01 \times 10^{-8}$.

8.2.7.7 The subsystems B1/B2 and Q1/Q2 are then subjected to the architectural constraints given in Table 5 of IEC 62061.

See Table 2.

Table 2 – Architectural constraints on subsystems' maximum SIL CL that can be claimed for an SRCF using this subsystem

Safe failure fraction	Hardware fault tolerance[a]		
	0	1	2
< 60 %	Not allowed[c]	SIL 1	SIL 2
60 % to < 90 %	SIL 1	SIL 2	SIL 3
90 % to < 99 %	SIL 2	SIL 3	SIL 3[b]
≥ 99 %	SIL 3	SIL 3[b]	SIL 3[b]

[a] A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety-related control function.

[b] A SIL 4 claim limit is not considered in this standard. For SIL 4 see IEC 61508-1.

[c] See 6.7.6.4 of IEC 62061 or, for subsystems where fault exclusions have been applied to faults that could lead to a dangerous failure, see 6.7.7.

8.2.7.8 Each subsystem has a safe failure fraction of 99 % (based on their DC) and a hardware fault tolerance of 1. That produces a SIL CL (SIL claim limit) of 3 for each subsystem.

8.2.7.9 For subsystem K1 the PFH_D of $2{,}31 \times 10^{-9}$ per hour and SIL CL 3 have been declared by the manufacture (see above).

8.2.7.10 The maximum SIL that can be claimed based on the lowest SIL CL is therefore 3.

8.2.7.11 The PFH_D of each subsystem is added together:

$3{,}04 \times 10^{-8}$ (subsystem B1/B2) + $2{,}31 \times 10^{-9}$ (subsystem K) + $1{,}01 \times 10^{-8}$ (subsystem Q1/Q2) = $4{,}28 \times 10^{-8}$

This satisfies the range $\geq 10^{-8}$ to $< 10^{-7}$ as given in IEC 62061, Table 3. Therefore if all other requirements of IEC 62061 are fulfilled this safety function achieves SIL 3.

8.3 Conclusion

8.3.1 The results of the above calculation for this simple example using the method from ISO 13849-1 gives the average probability of dangerous failure as $2{,}70 \times 10^{-8}$ per hour (i.e. corresponding to PL e), while use of the method from IEC 62061 gives a probability of dangerous failure as $4{,}28 \times 10^{-8}$ per hour (i.e. corresponding to SIL 3). The difference between these results is within expected error bounds and therefore shows an acceptable level of correspondence between both standards.

8.3.2 It should be noted that there is some variation between the two standards in the way that β (the susceptibility to common cause failures) is handled for redundant systems. This can cause a small but acceptable deviation (as shown in this example) between the PFH_D achieved according to the two standards. The methodology in ISO 13849-1 assumes a β factor of 2 % if sufficient measures from Table F.1 of the standard are fulfilled. IEC 62061 uses a differently structured table in Annex F. The use of this table produces a β factor that can range from 1 to 10 %. Each method for determination of the β factor is intended to be used only within the context of the subsystem design methodology of its respective standard.

Bibliography

[1] IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

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

[3] ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

[4] ISO 14121-1, *Safety of machinery – Risk assessment – Part 1: Principles*

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

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

[7] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[8] IEC 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

———————

SOMMAIRE

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 Généralités

2.1 La CEI 62061 et l'ISO 13849-1 spécifient des exigences de conception et de mise en œuvre des systèmes de commande relatifs à la sécurité des machines[3)]. Les méthodes développées dans ces deux normes sont différentes mais, correctement mises en œuvre, elles permettent des réductions du risque comparables.

2.2 Ces normes classent les systèmes de commande relatifs à la sécurité mettant en œuvre des fonctions de sécurité selon des niveaux définis en termes de probabilité de défaillance dangereuse par heure. L'ISO 13849-1 possède cinq niveaux de performance (PL, *performance levels*), a, b, c, d et e, tandis que la CEI 62061 comprend trois niveaux d'intégrité de sécurité (SIL, *safety integrity levels*), 1, 2 et 3.

2.3 Les comités de normes de produit (type C) spécifient les exigences de sécurité pour les systèmes de commande relatifs à la sécurité et il est recommandé que ces comités classifient les «degrés de confiance» qu'ils requièrent en termes de PL et SIL.

2.4 Les concepteurs de machines sont libres d'utiliser soit la CEI 62061, soit l'ISO 13849-1, selon les caractéristiques spécifiques de l'application.

2.5 Il est fort probable que le choix et l'utilisation d'une norme plutôt que l'autre soient déterminés par exemple comme suit:

– le fait d'avoir des connaissances et une expérience préalables dans le domaine de la conception de systèmes de commande relatifs à la sécurité des machines qui reposent sur le concept des catégories décrites dans l'ISO 13849-1:1999 peut signifier que l'emploi de l'ISO 13849-1:2006 est plus approprié;

– des systèmes de commande relatifs à la sécurité dont le moyen d'action n'est pas électrique peuvent signifier que l'emploi de l'ISO 13849-1:2006 est plus approprié;

– le fait que le client réclame que l'intégrité de sécurité d'un système de commande de machine relatif à la sécurité soit démontrée en termes de SIL peut signifier que l'emploi de la CEI 62061 est plus approprié;

– le fait que les machines comprenant les systèmes de commande relatifs à la sécurité en question soient utilisées, par exemple dans les industries de transformation où d'autres systèmes relatifs à la sécurité (tels que des systèmes de sécurité conformes à la CEI 61511) sont définis en termes de SIL, peut signifier que l'emploi de la CEI 62061 est plus approprié.

_____

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

3) Ces normes ont été adoptées par les organismes européens de normalisation CEN et CENELEC sous les références respectives ISO 13849-1 et EN 62061, où elles ont le statut de normes harmonisées au titre de la transposition de la directive Machines (98/37/CE et 2006/42/CE). Dans les conditions de leur publication, l'utilisation correcte de l'une de ces deux normes implique la conformité aux exigences de sécurité essentielles de la directive Machines (98/37/CE et 2006/42/CE).

3 Comparaison des normes

3.1 Une comparaison des exigences techniques de l'ISO 13849-1 et de la CEI 62061 a été menée sur les aspects suivants:

– terminologie;
– estimation du risque et détermination d'objectif de performance;
– spécification des exigences de sécurité;
– exigences d'intégrité systématique;
– fonctions de diagnostic;
– exigences de sécurité logicielle.

3.2 En outre, une évaluation de l'utilisation des formules mathématiques simplifiées pour déterminer la probabilité des défaillances dangereuses (PFH_D, *probability of a dangerous failure per hour*) et le temps moyen avant défaillance dangereuse ($MTTF_d$, *mean time to dangerous failure*) suivant les deux normes a aussi été effectuée.

3.3 Les conclusions de ce travail sont les suivantes.

Les systèmes de commande relatifs à la sécurité peuvent être conçus de manière à atteindre des niveaux de sécurité fonctionnelle acceptables avec l'une ou l'autre norme, en intégrant des sous-systèmes de commande électriques relatifs à la sécurité (SRECS, *safety-related electrical control system*) ou des parties de systèmes de commande relatives à la sécurité (SRP/CS, *safety-related parts of a control system*) non complexes[4)] conçus respectivement conformément à la CEI 62061 et à l'ISO 13849-1.

– Ces deux normes peuvent également fournir des solutions de conception pour des SRECS et SRP/CS complexes en intégrant des sous-systèmes électriques/électroniques/ programmables électroniques conçus conformément à la CEI 61508.
– Chaque norme est déjà appréciée par les utilisateurs du secteur des machines, qui tireront avantage de l'expérience acquise à l'usage. Une certaine période d'observation de leur application pratique est nécessaire à toute initiative future d'évolution vers une norme qui fusionne les contenus de la CEI 62061 et de l'ISO 13849-1.
– Des différences de détail existent et il est reconnu que certains concepts (par exemple celui de la gestion de la sécurité fonctionnelle) nécessitent encore du travail pour établir une équivalence entre les méthodologies de conception respectives et certaines exigences techniques.

4 Estimation du risque et détermination de la performance requise

4.1 Une comparaison a été effectuée sur l'utilisation des méthodes pour attribuer un SIL et/ou un PL_r à une fonction de sécurité particulière. Elle a établi qu'il existe un bon niveau de correspondance entre les méthodes fournies dans l'Annexe A de chaque norme.

4.2 Il est important, quelle que soit la méthode utilisée, de veiller à ce que des jugements corrects soient émis sur les paramètres de risque pour déterminer le SIL et/ou PL_r supposé s'appliquer à une fonction de sécurité particulière. Ces jugements sont souvent plus justes lorsqu'ils sont émis par un panel de professionnels (par exemple des concepteurs, du personnel de maintenance, des opérateurs) pour s'assurer que les dangers éventuellement présents sur une machine soient bien compris.

———————

4) Bien qu'il n'y ait aucune définition pour les termes SRECS ou SRP/CS «non complexes», il convient de le considérer comme l'équivalent de la faible complexité dans le contexte de la CEI 62061:2005, 3.2.7.

4.3 D'autres renseignements sur le processus d'estimation du risque et de la détermination des objectifs de performance se trouvent dans l'ISO 14121-1 et la CEI 61508-5.

5 Spécification des exigences de sécurité

5.1 Dans l'ISO 13849-1 comme dans la CEI 62061, la première étape de la méthodologie consiste à préciser la (les) fonction(s) de sécurité que le système de commande relatif à la sécurité est censé remplir.

5.2 Il convient que, pour chaque fonction de sécurité remplie par un circuit de commande, une évaluation ait été réalisée s'appuyant, par exemple, sur l'Annexe A de l'ISO 13849-1 ou sur l'Annexe A de la CEI 62061. Il convient que cette évaluation ait déterminé quelle est la réduction du risque nécessaire pour chaque fonction de sécurité d'une machine et, ensuite, quel est le degré de confiance nécessaire pour le circuit de commande qui accomplit cette fonction de sécurité.

5.3 Le degré de confiance, spécifié sous forme de PL et/ou SIL, est attaché à une fonction de sécurité particulière.

5.4 Ci-après se trouvent les informations, relatives aux fonctions de sécurité, qu'il convient qu'une norme de produit (type C) fournisse.

Fonction(s) de sécurité qu'un circuit de commande doit remplir:

Nom de la fonction de sécurité

Description de la fonction

Niveau de performance requis conformément à l'ISO 13849-1: PL_r, a à e

et/ou

Intégrité de sécurité requise conformément à la CEI 62061: SIL, 1 à 3

6 Détermination des objectifs de performance: PL ou SIL

Le Tableau 1 donne la relation entre le PL et le SIL d'après la probabilité moyenne d'une défaillance dangereuse par heure. Les deux normes fournissent toutefois des exigences (par exemple d'intégrité de sécurité systématique) qui viennent s'ajouter à ces objectifs probabilistes et qui doivent aussi s'appliquer à un système de commande relatif à la sécurité. La rigueur de ces exigences dépend du PL et SIL en question.

Tableau 1 – Relation entre PL et SIL basée sur la probabilité moyenne d'une défaillance dangereuse par heure

Niveau de performance (PL)	Probabilité moyenne d'une défaillance dangereuse par heure (1/h)	Niveau d'intégrité de sécurité (SIL)
a	$\geq 10^{-5}$ à $< 10^{-4}$	Aucune exigence de sécurité particulière
b	$\geq 3 \times 10^{-6}$ à $< 10^{-5}$	1
c	$\geq 10^{-6}$ à $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ à $< 10^{-6}$	2
e	$\geq 10^{-8}$ à $< 10^{-7}$	3

7 Conception du système

7.1 Exigences générales pour la conception des système selon la CEI 62061 et l'ISO 13849-1

Lors de la conception d'un SRECS ou d'une SRP/CS, il convient de prendre en compte les aspects suivants.

– Lorsqu'elles sont appliquées dans les limites de leur domaine d'application, les deux normes peuvent servir à concevoir des systèmes de commande relatifs à la sécurité avec une sécurité fonctionnelle acceptable, indiquée par le PL ou le SIL obtenu.

– Les parties non complexes relatives à la sécurité, conçues pour atteindre le PL approprié conformément à l'ISO 13849-1, peuvent être intégrées en tant que sous-système dans un système de commande électrique relatif à la sécurité (SRECS) conçu conformément à la CEI 62061. Toute partie complexe relative à la sécurité, conçue pour atteindre le PL approprié conformément à l'ISO 13849-1, peut être intégrée dans les pièces relatives à la sécurité d'un système de commande (SRP/SC) conçu conformément à l'ISO 13849-1.

– Tout sous-système non complexe conçu conformément à la CEI 62061 pour atteindre le SIL approprié peut être intégré en tant que pièce(s) relative(s) à la sécurité dans une combinaison de SRP/SC conçue conformément à l'ISO 13849-1.

– Tout sous-système complexe conçu conformément à la CEI 61508 pour atteindre le SIL approprié peut être intégré en tant que pièce(s) relative(s) à la sécurité dans une combinaison de SRP/SC conçue conformément à l'ISO 13849-1 ou en tant que sous-système dans un SRECS conçu conformément à la CEI 62061.

7.2 Estimation de la PFH_D et du $MTTF_d$ et utilisation des exclusions d'anomalie

7.2.1 PFH_D et $MTTF_d$

7.2.1.1 Dans le contexte de l'ISO 13849-1, la valeur du $MTTF_d$ correspond à une SRP/CS à canal unique sans diagnostic et, dans ce cas seulement, est l'inverse de la PFH_D de la CEI 62061.

7.2.1.2 Le $MTTF_d$ est un paramètre de composant et/ou de canal unique ne tenant aucun compte de facteurs tels que le diagnostic et l'architecture, tandis que la PFH_D est un paramètre de sous-système qui prend en compte la contribution de ces facteurs, selon la structure de conception.

7.2.1.3 L'Annexe K de l'ISO 13849-1 décrit la relation entre le $MTTF_d$ et la PFH_D d'une SRP/CS, pour différentes architectures classées en termes de catégorie et de couverture du diagnostic (DC, *diagnostic coverage*).

7.2.1.4 L'estimation de la PFH_D pour une combinaison de SRP/CS en série conforme à l'ISO 13849-1 peut aussi être réalisée en ajoutant des valeurs de PFH_D (par exemple déduites de l'Annexe K de l'ISO 13849-1) de chaque SRP/CS d'une manière similaire à celle utilisée avec des sous-systèmes dans la CEI 62061.

7.2.2 Usage des exclusions d'anomalie

7.2.2.1 Chacune des deux normes permet l'usage des exclusions d'anomalie (voir la CEI 62061, 6.7.7, et l'ISO 13849-1, 7.3). La CEI 62061 ne permet pas l'utilisation d'exclusions d'anomalie pour un SRECS sans tolérance aux anomalies matérielles devant atteindre un SIL 3 sans tolérance aux anomalies matérielles.

7.2.2.2 Lorsque des exclusions d'anomalie sont utilisées, il est important qu'elles soient correctement justifiées et valables pour la durée de vie prévue d'une SRP/CS ou d'un SRECS.

7.2.2.3 En général, lorsque, pour une fonction de sécurité devant être accomplie par une SRP/CS ou un SRECS, le niveau PL e ou SIL 3 est exigé, il n'est pas acceptable de s'appuyer uniquement sur les exclusions d'anomalies pour atteindre ce niveau de performance. Cela dépend de la technologie utilisée et de l'environnement de fonctionnement prévu. Il est donc essentiel que le concepteur accorde un soin supplémentaire à l'usage des exclusions d'anomalie en même temps que le PL ou SIL augmente.

7.2.2.4 En général, les exclusions d'anomalies ne sont pas applicables aux aspects mécaniques des interrupteurs électromécaniques de fin de course et des interrupteurs à commande manuelle (par exemple dispositif d'arrêt d'urgence) dans l'obtention du niveau PL e ou SIL 3 lors de la conception d'une SRP/CS ou d'un SRECS. Les exclusions d'anomalies qui peuvent être appliquées à des conditions de défaut mécanique particulières (par exemple usure/corrosion, rupture) sont décrites dans l'ISO 13849-2.

7.2.2.5 Par exemple, un système d'inter-verrouillage de porte qui doit atteindre le PL e ou le SIL 3 aura besoin de posséder une tolérance minimale aux anomalies égale à 1 (par exemple avec deux interrupteurs de fin de course mécaniques conventionnels) pour atteindre ce niveau de performance, car il n'est normalement pas justifiable d'exclure des anomalies telles que des actionneurs d'interrupteurs cassés. Il peut toutefois être acceptable d'exclure des anomalies telles que le court-circuit de câblage dans un tableau de commande conforme aux normes pertinentes.

7.2.2.6 La prochaine révision de l'ISO 13849-2 actuellement en cours d'élaboration par l'ISO/TC 199/GT 8 apportera davantage de renseignements sur l'usage des exclusions d'anomalie.

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

7.3.1 Dans tous les cas où des sous-systèmes ou des parties de système de commande relatives à la sécurité sont conçus conformément à l'ISO 13849-1 ou à la CEI 62061, la conformité à la norme relative au niveau de système ne peut être affirmée que si toutes les exigences de la norme relative au niveau de système (selon le cas) sont satisfaites.

7.3.2 Pour la conception d'un sous-système ou d'une partie de système de commande relative à la sécurité, soit la CEI 62061, soit l'ISO 13849-1, respectivement, doit être observée. Il est permis de satisfaire plus d'une de ces normes à condition que les normes utilisées soient entièrement respectées.

7.3.3 Lors de la conception d'un sous-système ou d'une partie de système de commande relative à la sécurité, il n'est pas permis de mélanger les exigences des normes.

7.4 Conception de système à partir de sous-systèmes ou de SRP/CS conçus d'après d'autres normes CEI ou ISO

7.4.1 Il est possible de choisir des sous-systèmes, par exemple des matériels de protection électro-sensibles, de conception conforme aux normes de produit CEI ou ISO correspondantes et à l'une ou l'autre des normes CEI 61508, CEI 62061 ou ISO 13849-1. Il convient que le(s) vendeur(s) de ces types de sous-systèmes fournisse(nt) les informations nécessaires pour faciliter leur intégration dans un système de commande relatif à la sécurité conforme à la CEI 62061 ou à l'ISO 13849-1.

7.4.2 Les sous-système, par exemple les entraînements électriques à vitesse variable, conçus d'après des normes de produit telles que la CEI 61800-5-2 et appliquant les exigences de la CEI 61508 peuvent être utilisés dans les systèmes de commande relatifs à la sécurité conformes à la CEI 62061 (voir aussi la CEI 62061, 6.7.3) et à l'ISO 13849-1.

7.4.3 Conformément à la CEI 62061, les autres sous-systèmes conçus à partir d'une ou plusieurs normes CEI, ISO ou autres sont soumis à la CEI 62061, 6.7.3.

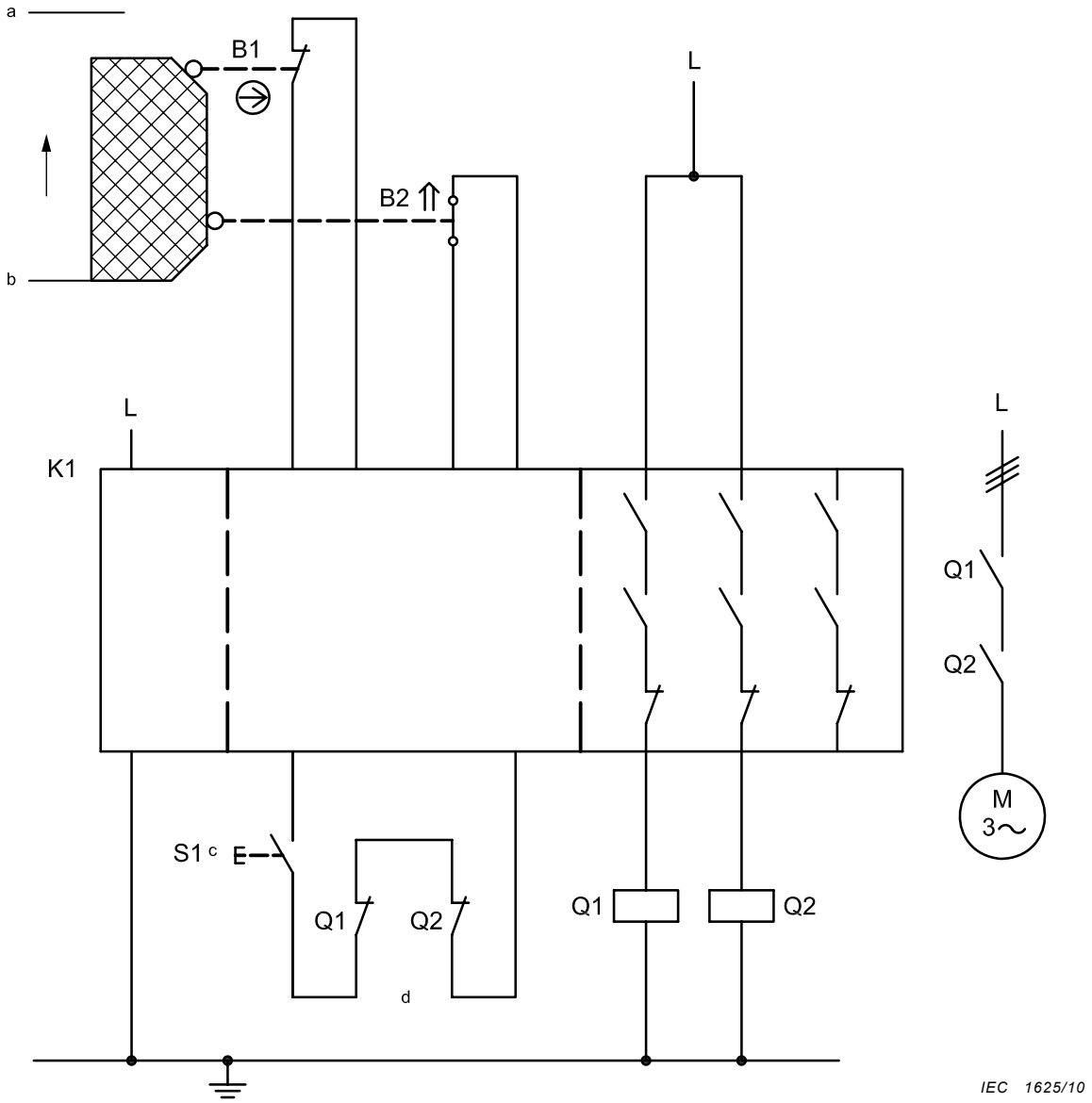
8 Exemple

8.1 Généralités

L'exemple suivant suppose que toutes les exigences des normes ont été satisfaites. Il a pour seul objet de démontrer certains aspects particuliers de la mise en œuvre des normes.

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

8.2.1 Cet exemple simplifié vise à illustrer l'utilisation de sous-systèmes ou de SRP/CS conformes à la CEI 62061 et/ou à l'ISO 13849-1 dans un SRECS/SRP/CS. Il est fondé sur la mise en œuvre d'une fonction de sécurité décrite comme une fonction d'arrêt relative à la sécurité associée à la surveillance de la position d'un protecteur mobile avec un niveau d'intégrité de sécurité SIL 3 ainsi qu'un niveau de performance PL_r e comme décrit à la Figure 1.



⇑ montré en position activée

a Ouvert.

b Fermé.

c DÉMARRAGE.

d Circuit de rétroaction.

Figure 1 – Exemple de mise en œuvre de la fonction de sécurité

8.2.2 Les informations suivantes concernent la spécification des exigences de sécurité pour cet exemple.

Fonction de sécurité

– Fonction d'arrêt relative à la sécurité, déclenchée par un dispositif de protection: l'ouverture du protecteur mobile déclenche la fonction de sécurité STO (*safe torque off*, absence sûre de couple).

Description fonctionnelle

– La protection contre les dangers de happement est assurée par un protecteur mobile (grille de protection). L'ouverture du protecteur avec dispositif de verrouillage est détectée par deux interrupteurs de fin de course, B1/B2, employant une combinaison contact à ouverture/contact à fermeture, et l'évaluation est faite par un module de sécurité central,

K1. K1 actionne deux contacteurs, Q1 et Q2, dont la retombée interrompt ou empêche les mouvements ou états dangereux.

– La vraisemblance des interrupteurs de fin de course est surveillée par K1 à des fins de détection d'anomalies. Les anomalies de Q1 et Q2 sont détectées par un essai de démarrage dans K1. Une commande de démarrage n'est réussie que si Q1 et Q2 sont retombés auparavant. Les essais de démarrage par ouverture et fermeture du protecteur avec dispositif de verrouillage ne sont pas requis.
– La fonction de sécurité reste intacte en cas de défaillance de composant. Les anomalies sont détectées lors du fonctionnement ou de la manœuvre (ouverture et fermeture) du protecteur avec dispositif de verrouillage par la retombée de Q1 et de Q2 et la désactivation du fonctionnement.
– Le cumul de plus de deux anomalies entre deux manœuvres successives peut conduire à la perte de la fonction de sécurité.

8.2.3 Il convient également de s'assurer des points suivants.

– Les principes de sécurité fondamentaux et éprouvés sont respectés (par exemple la valeur du courant d'emploi des contacteurs Q1 et Q2 est réduite de 50 %) et les exigences de catégorie B sont satisfaites. Des circuits de protection (par exemple protection de contact) sont mis en place.
– Une configuration stable des dispositifs de protection est assurée pour la manœuvre des interrupteurs de fin de course.
– L'interrupteur B1 est un interrupteur de fin de course à manœuvre positive d'ouverture, conformément à l'Annexe K de la CEI 60947-5-1:2003.
– Les conducteurs d'alimentation des interrupteurs B1 et B2 sont séparés ou munis d'une protection.

8.2.4 Les informations suivantes sont disponibles auprès des fabricants pour chaque partie de la conception d'une SRP/CS.

– Le module de sécurité K1 est déclaré par le fabricant[5)] comme satisfaisant aux exigences de la catégorie 4, PL e et SIL CL 3.
– Les contacteurs Q1 et Q2 possèdent des éléments de contact reliés mécaniquement conformes à l'Annexe L de la CEI 60947-5-1:2003.

8.2.5 L'observation suivante peut être faite sur la conception d'une SRP/CS et/ou d'un SRECS.

– La catégorie 4 ne peut être obtenue que lorsque les différents interrupteurs mécaniques de fin de course des divers dispositifs de protection ne sont pas connectés en série (c'est-à-dire pas de démultiplication). Cela est nécessaire, sans quoi les anomalies des interrupteurs ne peuvent être détectées.

8.2.6 Calcul de la probabilité de défaillance conformément à l'ISO 13849-1

La Figure 2 montre un sous-système logique (module de sécurité K1) auquel sont raccordés des éléments d'entrée et sortie à deux canaux. Une abstraction du niveau matériel étant déjà effectuée dans le schéma fonctionnel relatif à la sécurité, la séquence des sous-systèmes est donc, en principe, interchangeable. Il est par conséquent recommandé que les sous-systèmes partageant la même structure soient regroupés comme le montre la Figure 3. Le calcul du PL se trouve ainsi simplifié par la réduction du nombre de fois où la limitation du $MTTF_d$ d'un canal sur 100 ans est effectuée dans l'estimation.

5) Ce module est traité comme un sous-système et, à ce titre, il n'est pas nécessaire de fournir le $MTTF_d$ de ses canaux individuels (voir 7.2.1.1).

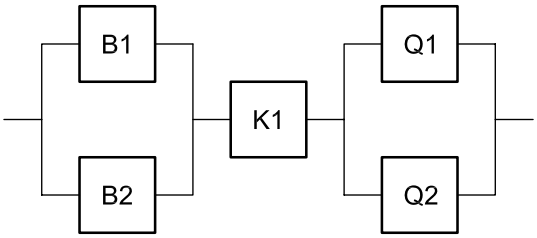
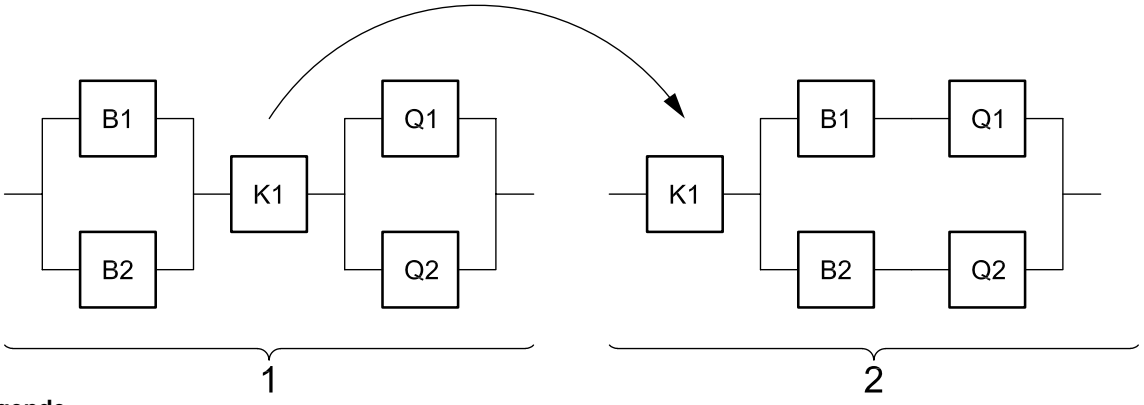


Figure 2 – Schéma fonctionnel relatif à la sécurité



Légende

1 représentation du matériel: trois SRP/CS comme sous-systèmes

2 représentation logique simplifiée: deux SRP/CS comme sous-systèmes

Figure 3 – Schéma fonctionnel relatif à la sécurité pour un calcul conformément à l'ISO 13849-1

La probabilité de défaillance du module de sécurité K1 est indiquée par le fabricant et ajoutée à la fin du calcul [$2{,}31 \times 10^{-9}$ par heure (valeur fabricant), adapté pour PL e]. Pour le sous-système restant, la probabilité de défaillance se calcule comme suit.

– MTTF_d: la valeur B_{10d} de 1 000 000 cycles (valeur fabricant) est indiquée pour la partie mécanique de B1. Pour l'interrupteur de fin de course B2, la valeur B_{10d} est de 500 000 cycles ([valeur fabricant). Pour 365 jours ouvrés par an, 24 h de travail par jour et une durée de cycle de 900 s (15 min), n_{op} est de 35 040 cycles par an pour ces composants, d'après les Équations (C.2) et (C.7) de l'ISO 13849-1:

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600 \frac{\text{s}}{\text{h}}}{t_{cycle}} = \frac{365 \frac{\text{jours}}{\text{an}} \times 24 \text{ jour} \times 3\,600 \frac{\text{s}}{\text{h}}}{900 \frac{\text{s}}{\text{cycle}}} = 35\,040 \frac{\text{cycles}}{\text{an}}$$

$$\text{MTTF}_{d,B1} = \frac{B_{10d}}{0{,}1 \times n_{op}} = \frac{1\,000\,000 \text{ cycles}}{0{,}1 \times 35\,040 \frac{\text{cycles}}{\text{an}}} = 285 \text{ ans}$$

$$T_{10d,B1} = \frac{B_{10d}}{n_{op}} = \frac{1\,000\,000 \text{ cycles}}{35\,040 \frac{\text{cycles}}{\text{an}}} = 28{,}5 \text{ ans}$$

$$\text{MTTF}_{\text{d,B2}} = \frac{B_{10\text{d}}}{0{,}1 \times n_{\text{op}}} = \frac{500\,000 \text{ cycles}}{0{,}1 \times 35\,040 \frac{\text{cycles}}{\text{an}}} = 143 \text{ ans}$$

$$T_{10\text{d,B2}} = \frac{B_{10\text{d}}}{n_{\text{op}}} = \frac{500\,000 \text{ cycles}}{35\,040 \frac{\text{cycles}}{\text{an}}} = 14{,}3 \text{ ans}$$

La valeur $T_{10\text{d}}$ de B2 est de 14,3 ans. Une fois ce délai écoulé, B2 doit être remplacé si la durée de fonctionnement prévue de l'ensemble de la SRP/CS est de 20 ans.

– Pour les contacteurs Q1 et Q2, la valeur B_{10} correspond, sous charge inductive (CA 3), à une durée de vie de 1 000 000 cycles (valeur fabricant). Si la moitié des défaillances est supposée dangereuse, la valeur $B_{10\text{d}}$ est obtenue en doublant B_{10}:

$$\text{MTTF}_{\text{d, Q1/Q2}} = \frac{B_{10\text{d}}}{0{,}1 \times n_{\text{op}}} = \frac{2\,000\,000 \text{ cycles}}{0{,}1 \times 35\,040 \frac{\text{cycles}}{\text{an}}} = 571 \text{ ans}$$

$$T_{10\text{d, Q1/Q2}} = \frac{B_{10\text{d}}}{n_{\text{op}}} = \frac{2\,000\,000 \text{ cycles}}{35\,040 \frac{\text{cycles}}{\text{an}}} = 57{,}1 \text{ ans}$$

– Pour les deux canaux, le MTTF_{d} se calcule au moyen de l'Équation (D.1) de l'ISO 13849-1.

$$\frac{1}{\text{MTTF}_{\text{d}}} = \sum_{i=1}^{N} \frac{1}{\text{MTTF}_{\text{d}i}}$$

$$\frac{1}{\text{MTTF}_{\text{d, C1}}} = \frac{1}{285 \text{ ans}} + \frac{1}{571 \text{ ans}} = \frac{1}{190 \text{ ans}}$$

$$\frac{1}{\text{MTTF}_{\text{d, C2}}} = \frac{1}{143 \text{ ans}} + \frac{1}{571 \text{ ans}} = \frac{1}{114 \text{ ans}}$$

Ce qui donne un $\text{MTTF}_{\text{d,C1}}$ de 190 ans et un $\text{MTTF}_{\text{d,C2}}$ de 114 ans. Conformément à l'ISO 13849-1, le MTTF_{d} des deux canaux est limité à 100 ans et, dans ce cas, comme les MTTF_{d} des deux canaux sont égaux après limitation, la symétrisation est inutile.

– DC_{avg}: La couverture de diagnostic de 99 % pour B1 et B2 repose sur une surveillance de la vraisemblance de la combinaison contact d'ouverture/contact de fermeture dans K1. La DC de 99 % pour les contacteurs Q1 et Q2 est obtenue à partir d'une surveillance régulière par K1 au cours du démarrage. Les valeurs déclarées de DC correspondent à la DC_{avg} (*average diagnostic coverage*, couverture de diagnostic moyenne) pour chaque sous-système. La DC_{avg} sera calculée conformément à l'Équation (E.1) de l'ISO 13849-1. Parce que chaque DC est de 99 %, la DC_{avg} est donc aussi de 99 %.
– Mesures adéquates contre la défaillance de cause commune dans les sous-systèmes B1/B2 et Q1/Q2 (70 points): séparation (15), composants correctement testés (5), protection contre les surtensions, etc. (15) et conditions environnementales (25 + 10).
– Durée de mission: pour l'approche simplifiée de l'ISO 13849-1, un temps de mission de 20 ans est présupposé.
– Le sous-système B1/B2/Q1/Q2 correspond à la catégorie 4 avec un MTTF_{d} élevé (100 ans) et une DC_{avg} élevée (99 %). Il en résulte une probabilité moyenne de défaillance dangereuse de $2{,}47 \times 10^{-8}$ par heure (voir le Tableau K.1 de l'ISO 13849-1).

Après ajout du sous-système K1, la probabilité moyenne de défaillance dangereuse devient égale à $2{,}70 \times 10^{-8}$ par heure. Ce qui correspond à un PL e.

8.2.7 Calcul de la probabilité de défaillance conformément à la CEI 62061

8.2.7.1 Conformément à la CEI 62061, 6.6.2, le circuit peut se diviser en trois sous-systèmes: B1/B2, K et Q1/Q2, montrés dans le schéma fonctionnel relatif à la sécurité.

8.2.7.2 Pour le sous-système K, le fabricant déclare une probabilité de défaillance par heure de $2{,}31 \times 10^{-9}$ et une limite de revendication de SIL égale à 3 pour le module de sécurité K1.

8.2.7.3 Pour les sous-systèmes restant, la probabilité de défaillance se calcule comme suit.

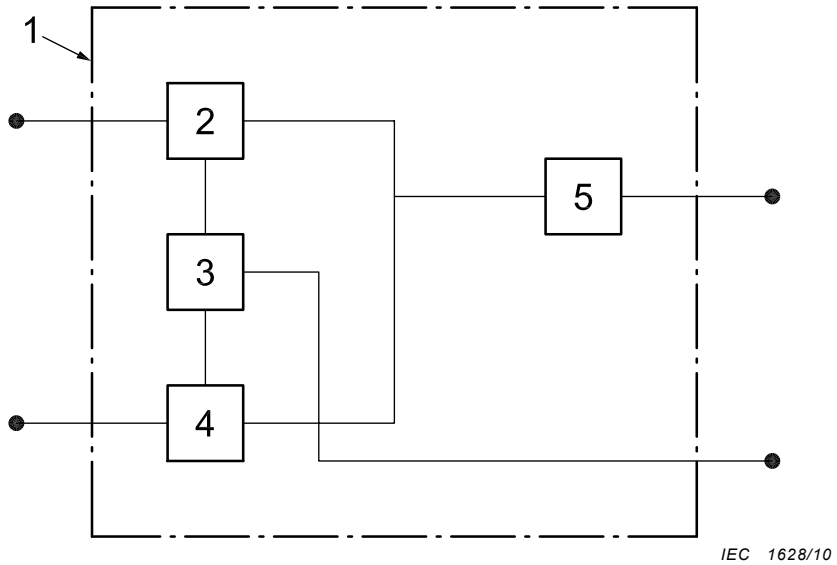
– Sous-système B1/B2: la valeur B_{10d} de 1 000 000 cycles (valeur fabricant) est indiquée pour la partie mécanique de B1. Pour l'interrupteur de fin de course B2, la valeur B_{10d} est de 500 000 cycles (valeur fabricant). Pour 365 jours ouvrés par an, 24 h de travail par jour et une durée de cycle de 15 min, C est de 4 cycles par an pour ces composants. Le taux de défaillance est $0{,}1 \times C/B_{10d} = 4{,}00 \times 10^{-7}$/h. Pour B2, cela donne un taux de défaillance de $8{,}00 \times 10^{-7}$/h.

NOTE D'après la CEI 62061, le nombre de cycles de fonctionnement, C, de l'application correspond au nombre moyen de manœuvres annuelles, n_{op}, conformément à l'ISO 13849-1. C étant donné en cycles par heure et n_{op} en cycles par an, la relation suivante s'applique:

$$C = n_{op} \times \frac{\text{an}}{365 \times 24\text{h}}$$

Ainsi, le nombre moyen d'heures de fonctionnement quotidiennes et le nombre de jours de fonctionnement par an influent sur les valeurs de C et de n_{op}.

– L'architecture logique de ce sous-système correspond au schéma D de la CEI 62061, 6.7.8.2.5, tel que montré à la Figure 4.



Légende

1 sous-système D
2 élément de sous-système, λ_{De1}
3 fonction(s) de diagnostic
4 élément de sous-système, λ_{De2}
5 défaillance de cause commune

Figure 4 – Représentation logique d'un sous-système de type D

Les éléments de sous-système (interrupteurs B1 et B2) sont de conceptions différentes. L'Équation (D.1) suivante, issue de la CEI 62061, 6.7.8.2.5, sert par conséquent à déterminer la PFH_D du sous-système.

$$\lambda_{DssD} = (1-\beta)^2\left\{\left[\lambda_{De1}\times\lambda_{De2}\times(DC_1+DC_2)\right]\times T_2/2+\left[\lambda_{De1}\times\lambda_{De2}\times(2-DC_1-DC_2)\right]\times T_1/2\right\}+\ldots$$
$$\ldots\ \beta\times(\lambda_{De1}+\lambda_{De2})/2$$

$$PFH_{DssD} = \lambda_{DssD}\times 1h$$

où

T_2 est l'intervalle entre les essais de diagnostic; pour le sous-système B1/B2, il est de 15 min.

T_1 est la plus faible des deux valeurs suivantes: intervalle d'essai de diagnostic ou durée de vie. Pour le sous-système B1/B2, l'intervalle de durée de vie est de 125 000 h (14,3 ans) à la cadence d'utilisation donnée et fondée sur la valeur T_{10d} de l'élément de sous-système la plus basse (voir l'ISO 13849-1, C.4.2). L'interrupteur B2 possède la plus faible valeur T_{10d}. L'intervalle d'essai périodique (voir Avant-propos de la CEI 62061) est supposé être de 20 ans (175 200 h), ce qui dépasse la durée de vie. Ainsi, T_1 est de 125 000 h.

β est la sensibilité aux défaillances de cause commune. Sa valeur est de 5 % (0,05) et provient de 42 points marqués dans la méthode simplifiée de l'Annexe F de la CEI 62061: séparation (5 + 5 + 5), évaluation/analyse (9) et conditions environnementales (9 + 9).

λ_{De1} est le taux de défaillance dangereuse de l'élément de sous-système 1. Pour l'interrupteur B1, cela correspond à $4{,}00 \times 10^{-7}$/h (voir ci-dessus).

DC_1 est la couverture de diagnostic de l'élément de sous-système 1. Pour B1, elle est estimée à 99 % d'après une surveillance de la vraisemblance de la combinaison contact d'ouverture/contact de fermeture de B1 et B2 en combinaison avec K1.

λ_{De2} est le taux de défaillance dangereuse de l'élément de sous-système 2. Pour l'interrupteur B2, il correspond à $8{,}00 \times 10^{-7}$/h (voir ci-dessus).

DC_2 est la couverture de diagnostic de l'élément de sous-système 2. Pour B2, elle est estimée à 99 % d'après une surveillance de la vraisemblance de la combinaison contact d'ouverture/contact de fermeture de B1 et B2 en combinaison avec K1.

8.2.7.4 Les données ci-dessus sont entrées dans l'équation pour donner une PFH_D de $3{,}04 \times 10^{-8}$.

8.2.7.5 De même, pour le sous-système Q1/Q2, les contacteurs Q1 et Q2 ont une valeur B_{10} qui correspond, sous charge inductive (CA 3), à une durée de vie de 10^6 cycles (valeur fabricant). Si la moitié des défaillances est supposée dangereuse, la valeur B_{10d} est obtenue en doublant B_{10}. La valeur supposée ci-dessus pour C donne un taux de défaillance de $2{,}00 \times 10^{-7}$/h pour chaque contacteur.

8.2.7.6 L'architecture logique du sous-système Q1/Q2 correspond au schéma D de la CEI 62061, 6.7.8.2.5. Les éléments de sous-système (contacteurs Q1 et Q2) sont de conceptions identiques. L'Équation (D.1) sert par conséquent à déterminer la PFH_D du sous-système:

$$\lambda_{DssD} = (1-\beta)^2\left\{\left[\lambda_{De}{}^2\times 2\times DC\right]\times T_2/2+\left[\lambda_{De}{}^2\times(1-DC)\right]\times T_1\right\}+\beta\times\lambda_{De}$$

$$PFH_{DssD} = \lambda_{DssD}\times 1\ h$$

où

T_2 est l'intervalle d'essai de diagnostic; pour le sous-système Q1/Q2, il est de 15 min.

T_1 est la plus faible des deux valeurs suivantes: intervalle d'essai périodique ou durée de vie. Pour le sous-système Q1/Q2, la durée de vie est de 500 000 h (57,1 ans) au rythme d'utilisation donné d'après la valeur T_{10d} de l'élément de sous-système la plus faible (voir l'ISO 13849-1, C.4.2). L'intervalle d'essai périodique (voir Avant-propos de la CEI 62061) est suppose être de 20 ans (175 200 h), ce qui est inférieur à la durée de vie. Ainsi, T_1 est de 175 200 h.

λ_{De} est le taux de défaillance dangereuse de chaque élément de sous-système (contacteurs Q1 et Q2) = $2{,}00 \times 10^{-7}$/h (voir ci-dessus).

DC est la couverture du diagnostic de chaque élément de sous-système (contacteurs Q1 et Q2) = 99 % d'après la surveillance régulière par K1 des contacts miroirs reliés mécaniquement au cours du démarrage.

β est la sensibilité aux défaillances de cause commune. Sa valeur est de 5 % (0,05) et provient de 42 points marqués dans la méthode simplifiée de l'Annexe F de la CEI 62061: séparation (5 + 5 + 5), évaluation/analyse (9) et conditions environnementales (9 + 9).

Les données ci-dessus sont entrées dans l'équation pour donner une PFH_D de $1{,}01 \times 10^{-8}$.

8.2.7.7 Les sous-systèmes B1/B2 et Q1/Q2 sont alors soumis aux contraintes architecturales énoncées dans le Tableau 5 de la CEI 62061.

Voir Tableau 2.

Tableau 2 – Contraintes architecturales sur le SIL CL de sous-système maximal qui puisse être revendiquées pour une SRCF utilisant ce sous-système

Proportion de défaillances sûres	Tolérance aux anomalies matérielles[a]		
	0	1	2
< 60 %	Interdit[c]	SIL 1	SIL 2
60 % à < 90 %	SIL 1	SIL 2	SIL 3
90 % à < 99 %	SIL 2	SIL 3	SIL 3[b]
≥ 99 %	SIL 3	SIL 3[b]	SIL 3[b]

[a] Une tolérance aux anomalies matérielles N signifie que N+1 anomalies sont susceptibles d'entraîner une perte de la fonction de commande relative à la sécurité.

[b] Une limite de revendication SIL 4 n'est pas considérée dans cette norme. Pour SIL 4, voir la CEI 61508-1.

[c] Voir 6.7.6.4 ou, pour les sous-systèmes ayant fait l'objet d'une exclusion d'anomalie sur des défauts susceptibles de mener à une défaillance dangereuse, 6.7.7, de la CEI 62061.

8.2.7.8 Chaque sous-système possède une proportion de défaillances en sécurité de 99 % (d'après sa DC) et une tolérance aux anomalies matérielles égale à 1. Ce qui donne une SIL CL (*SIL claim limit*, limite de revendication de SIL) de 3 pour chaque sous-système.

8.2.7.9 Pour le sous-système K1, le fabricant a déclaré une PFH_D de $2{,}31 \times 10^{-9}$ par heure et une SIL CL de 3 (voir ci-dessus).

8.2.7.10 Le SIL maximal qui puisse donc être revendiqué, d'après la SIL CL la plus faible, est donc de 3.

8.2.7.11 La PFH_D de chaque sous-système est ajoutée:

$3{,}04 \times 10^{-8}$ (sous-système B1/B2) + $2{,}31 \times 10^{-9}$ (sous-système K) + $1{,}01 \times 10^{-8}$ (sous-système Q1/Q2) = $4{,}28 \times 10^{-8}$.

Ce qui rentre dans la fourchette $\geq 10^{-8}$ et $< 10^{-7}$ donnée dans le Tableau 3 de la CEI 62061. Par conséquent, si toutes les autres exigences de la CEI 62061 sont satisfaites, cette fonction de sécurité correspond au SIL 3.

8.3 Conclusion

8.3.1 Le résultat du calcul ci-dessus pour cet exemple simple employant la méthode de l'ISO 13849-1 donne une probabilité moyenne de défaillance dangereuse de $2{,}70 \times 10^{-8}$ par heure (ce qui correspond au PL e); tandis que, d'après la méthode de la CEI 62061, la probabilité de défaillance dangereuse est de $4{,}28 \times 10^{-8}$ par heure (ce qui correspond à un SIL 3). La différence entre ces deux résultats se trouve dans la marge d'erreur prévue et indique donc un degré d'équivalence acceptable entre les deux normes.

8.3.2 Il convient de noter toutefois qu'il existe des différences entre les deux normes dans la façon dont β (la susceptibilité aux défaillances de cause commune) est gérée dans les systèmes redondants. Cela peut entraîner un petit écart acceptable (comme l'a montré l'exemple précédent) entre les PFH_D obtenues avec l'une et l'autre norme. La méthodologie de l'ISO 13849-1 présuppose un facteur β de 2 % si des conditions suffisantes du Tableau F1 de la norme sont remplies. Dans son Annexe F, la CEI 62061 emploie un tableau de structure différente. L'utilisation de ce tableau produit un facteur β susceptible de varier de 1 % à 10 %. Chaque méthode de détermination du facteur β est destinée à n'être utilisée que dans le contexte de la méthodologie de conception de sous-systèmes de sa norme respective.

Bibliographie

[1] CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

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

[3] ISO 13849-2, *Sécurité des machines – Parties des systèmes de commande relatifs à la sécurité – Partie 2: Validation*

[4] ISO 14121-1, *Sécurité des machines – Appréciation du risque – Partie 1: Principes*

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

[6] CEI 61511-1, *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*

[7] CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

[8] CEI 61800-5-2, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

———————

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