IEC 61800-5-3

Edition 1.0 2021-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Adjustable speed electrical power drive systems – Part 5-3: Safety requirements – Functional, electrical and environmental requirements for encoders

Entraînements électriques de puissance à vitesse variable – Partie 5-3: Exigences de sécurité – Exigences fonctionnelle, électrique et environnementale pour codeurs

IEC 61800-5-3:2021-02(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) 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 IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC online collection - oc.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IEC 61800-5-3

Edition 1.0 2021-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Adjustable speed electrical power drive systems – Part 5-3: Safety requirements – Functional, electrical and environmental requirements for encoders

Entraînements électriques de puissance à vitesse variable – Partie 5-3: Exigences de sécurité – Exigences fonctionnelle, électrique et environnementale pour codeurs

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 13.110; 29.130.99; 29.200

ISBN 978-2-8322-9400-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

Part 5-3: Safety requirements – Functional, electrical and environmental requirements for encoders

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.

International Standard IEC 61800-5-3 has been prepared by subcommittee 22G: Adjustable speed electric power drive systems (PDS), of IEC technical committee 22: Power electronic systems and equipment.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
22G/431/FDIS	22G/434/RVD

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

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

Terms in *italics* are defined in Clause 3.

A list of all parts in the IEC 61800 series, published under the general title *Adjustable speed electrical power drive systems*, can be found on the IEC website.

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

As a result of automation, demand for increased production and reduced operator physical effort, control systems of machinery and plant items play an increasing role in the achievement of overall safety. These control systems increasingly employ complex electrical/electronic/programmable electronic devices and systems.

Prominent amongst these devices and systems are *encoder* which are for example applied to measure angle and position of machine parts for use in safety-related applications (*Encoder(SR)*). Based on the *Encoder(SR)'s* output signals, *PDS(SR)* or other *evaluation units* calculate for example speed, acceleration, absolute position, etc., to perform their safety sub-functions SLS, SLA, SLP and others (see IEC 61800-5-2:2016, Clause 4). The *signal processing* necessary to perform some of these *safety sub-functions* may also be included in the *Encoder(SR)*.

Examples of industrial applications are:

- machine tools, robots, production test equipment, test benches;
- papermaking machines, textile production machines, calendars in the rubber industry;
- plastics processing lines, chemicals or metal production lines, rolling-mills;
- cement crushing machines, cement kilns, mixers, centrifuges, extrusion machines;
- drilling machines;
- conveyors, materials handling machines, hoisting equipment (cranes, gantries, etc.);
- pumps, fans, etc.

This document can also be used as a reference for developers using *Encoder(SR)* for other applications, for example in wind power plants.

Users of this document should be aware that some type C standards for machinery currently refer to ISO 13849-1 for safety-related control systems. In this case, *Encoder(SR)* manufacturers may be requested to provide further information (e.g. category and *performance level PL*) to facilitate the integration of an *Encoder(SR)* into the safety-related control systems of such machinery. This has been considered during development of this document and corresponding indications are included where appropriate.

NOTE "Type C standards" are defined in ISO 12100 [1] as machine safety standards dealing with detailed safety requirements for a particular machine or group of machines.

There are many situations where control systems that incorporate *Encoder(SR)* are employed, for example as part of safety measures that have been provided to achieve risk reduction. A typical case is reducing the speed during start-up in order to protect personnel from hazards arising by unexpected fast movements of machine parts. This document gives a methodology to identify the contribution made by an *Encoder(SR)* to identified safety *sub-functions* and to enable the appropriate design of the *Encoder(SR)* and verification that it achieves the required performance.

Measures are given to co-ordinate the safety performance of the *Encoder(SR)* with the intended risk reduction taking into account the probabilities and consequences of its random and systematic *faults*.

ADJUSTABLE SPEED ELECTRICAL POWER DRIVE SYSTEMS –

Part 5-3: Safety requirements – Functional, electrical and environmental requirements for encoders

1 Scope

This part of IEC 61800, which is a product standard, specifies requirements and makes recommendations for the design and development, integration and validation of safety-related *encoder* (*Encoder(SR)*) in terms of their *functional safety* considerations, electrical safety and environmental conditions. It applies to *Encoder(SR)*, being sensors as part of a *PDS(SR)*.

NOTE 1 The term "integration" refers to the *Encoder(SR)* itself, not to its incorporation into the safety-related application.

This document can also be referred to and used for *Encoder(SR)* in any other safety-related application, for example safety-related position monitoring.

NOTE 2 This document specifies only complementary *functional safety*, electrical safety and environmental condition requirements that are not clearly provided by other parts of the IEC 61800 series.

This document is applicable where *functional safety* of an *encoder* is claimed and the *Encoder(SR)* is operating mainly in the high demand or continuous mode.

NOTE 3 While low demand mode operation is possible for an *Encoder(SR)*, this document concentrates on high demand and continuous mode. *Safety sub-functions* implemented for high demand or continuous mode can also be used in low demand mode. Requirements for low demand mode are given in IEC 61508 (all parts) [2]. Some guidance for the estimation of average probability of *dangerous failure* on demand (PFD_{avg}) value is provided in IEC 61800-5-2:2016, Annex F.

The requirements of IEC 61800-5-2:2016 for *PDS(SR)* apply to *Encoder(SR)* as applicable. This document includes additional or different requirements for *Encoder(SR)*. It sets out safety-related considerations of *Encoder(SR)* in terms of the framework of IEC 61508 (all parts), and introduces requirements for *Encoder(SR)* as subsystems of a safety-related system. It is intended to facilitate the realisation of the electrical/electronic/programmable electronic (E/E/PE) and mechanical parts of an *Encoder(SR)* in relation to the safety performance of *safety sub-function*(s) of an *Encoder(SR)*.

Manufacturers and suppliers of *Encoder(SR)* will, by using the normative requirements of this document, indicate to users (system integrator, original equipment manufacturer) the safety performance of the *Encoder(SR)*. This will facilitate the incorporation of *Encoder(SR)* into safety-related control systems using the principles of IEC 61508 (all parts), and possibly its specific sector implementations (for example IEC 61511 (all parts) [3], IEC 61513 [4], IEC 62061 [5] or ISO 13849-1 and ISO 13849-2 (see Clause 2).

By applying the requirements from this document, the corresponding requirements of IEC 61508 (all parts) that are necessary for an *Encoder(SR)* are fulfilled.

This document does not specify requirements for:

- the functional properties of an *Encoder(SR)* without any safety relevance;
- the *hazard* and risk analysis of a particular application;
- the identification of *safety sub-functions* for that application;
- the initial allocation of *SIL*s to those *safety sub-functions*;
- the driven equipment except for interface arrangements;

- secondary *hazard*s (for example from failure in a production or manufacturing process);
- the *Encoder(SR)* manufacturing process;
- the validity of signals and commands to the *Encoder(SR)*; and
- security aspects (e.g. cyber security or *Encoder(SR)* security of access).

NOTE 4 The *functional safety* requirements of an *Encoder(SR)* are dependent on the application, and can be considered as a part of the overall risk assessment of the installation. Where the supplier of the *Encoder(SR)* is not responsible for the driven equipment, the installation designer is responsible for the risk assessment, and for specifying the functional and safety integrity requirements of the *Encoder(SR)*.

This document applies to *Encoder(SR)* implementing *safety sub-functions* with a *SIL* not greater than *SIL* 3.

This document provides additional information for *Encoder(SR)* claiming conformity with ISO 13849-1:2015.

Figure 1 shows the installation and the functional parts of a *PDS(SR)* including the *Encoder(SR)* (sensor) which is considered in this document.

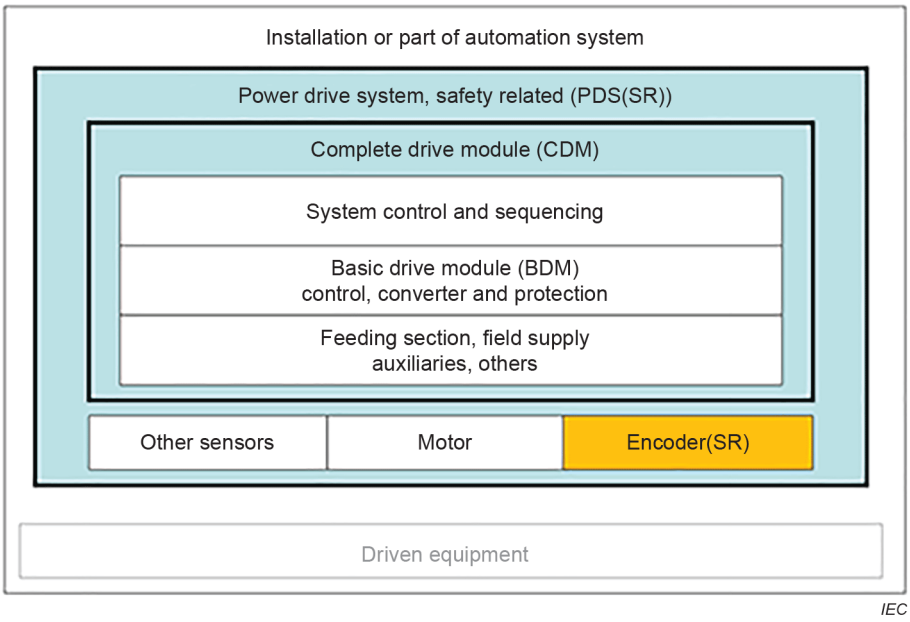


Figure 1 – Context of *Encoder(SR)*

Figure 1 shows a logical representation of a *PDS(SR)* rather than its physical description.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60068-2-1, *Environmental testing – Part 2-1: Tests – Test A: Cold*

IEC 60068-2-47, *Environmental testing – Part 2-47: Tests – Mounting of specimens for vibration, impact and similar dynamic tests*

IEC 60335-1, *Household and similar electrical appliances – Safety – Part 1: General requirements*

IEC 60947-5-2:2019, *Low-voltage switchgear and controlgear – Part 5-2: Control circuit devices and switching elements – Proximity switches*

IEC 61000-6-7:2014, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61800-1:1997, *Adjustable speed electrical power drive systems – Part 1: General requirements – Rating specifications for low voltage adjustable speed d.c. power drive systems*

IEC 61800-5-1:2007, *Adjustable speed electrical power drive systems – Part 5-1: Safety requirements – Electrical, thermal and energy*
IEC 61800-5-1:2007/AMD1:2016

IEC 61800-5-2:2016, *Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional*

IEC 62368-1:2018, *Audio/video, information and communication technology equipment – Part 1: Safety requirements*

ISO 13849-1:2015*, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012*, Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

Table 1 shows a list of terms and definitions.

Table 1 – List of terms

3.1	*encoder*	3.19	*functional safety* *FS*
3.2	*Encoder(SR)*	3.20	*safety function*
3.3	*interface unit*	3.21	*safety sub-function*
3.4	*evaluation unit*	3.22	*fault*
3.5	*PDS(SR)*	3.23	*dangerous failure*
3.6	*tolerance range*	3.24	*hardware fault tolerance* *HFT*
3.7	*interpolation*	3.25	*single-fault tolerance*
3.8	*solid measure*	3.26	*safety integrity level* *SIL*
3.9	*mechanical fastening*	3.27	*SIL capability*
3.10	*mechanical connecting element*	3.28	*performance level* *PL*
3.11	*shaft-rotor coupling*	3.29	*diagnostic coverage* *DC*
3.12	*stator coupling*	3.30	*safe failure fraction* *SFF*
3.13	*bearing blockage*	3.31	*average frequency of a dangerous failure* *PFH*
3.13.1	*spontaneous bearing blockage*	3.32	*mean time to dangerous failure* $MTTF_D$
3.13.2	*gradual bearing blockage*	3.33	*process safety time*
3.14	*measurement point for working temperature*	3.34	*ideal fault detection*
3.15	*working temperature range*	3.35	*quantitative FMEDA*
3.16	*extra low voltage* *ELV*	3.36	*qualitative FMEDA*
3.17	*protective ELV circuit* *PELV circuit*	3.37	*signal evaluation*
3.18	*decisive voltage class* *DVC*	3.38	*signal processing*

3.1
encoder
electromechanical device that generates an analogue or digital output signal in response to the position of a moveable part

Note 1 to entry: Within this document, the definition of "*encoder*" includes resolvers and all types of motor feedback sensors.

Note 2 to entry: Annex A includes examples of type of *encoder*.

3.2
Encoder(SR)
encoder providing *safety sub-function(s)*

Note 1 to entry: The *safety sub-function(s)* of the *Encoder(SR)* allow(s) execution of safety sub-functions of a *PDS(SR)* or any other safety application.

Note 2 to entry: This definition has been derived from IEC 61800-5-2:2016, 3.16.

3.3
interface unit
separate electronic subassembly of the *Encoder(SR)* for signal conversion

Note 1 to entry: The functionality of the *interface unit* may be integrated in the *Encoder(SR)*.

3.4
evaluation unit
external item of equipment in which the output signal of the *Encoder(SR)* is evaluated

Note 1 to entry: Examples for *evaluation units* are *PDS(SR),* safety elements for monitoring speed or stoppages.

Note 2 to entry: The *evaluation unit* may also perform diagnostic measures for the *Encoder(SR)*.

3.5
PDS(SR)
adjustable speed electrical power drive system providing safety sub-functions

[SOURCE: IEC 61800-5-2:2016, 3.16]

3.6
tolerance range
span between upper and lower tolerance limit

Note 1 to entry: The *tolerance range* is expressed in measuring units and is applied to *Encoder(SR)* with analogue and digital output signals.

Note 2 to entry: Tolerance range T(R) is usually given in the form T(R): −X to +Y, with T(R) = X + Y; (e.g. -5 mm to +5 mm, 0° to +10°, etc.).

Note 3 to entry: The tolerance range should take into account accuracy and resolution.

3.7
interpolation
mathematical method for resolution enhancement

EXAMPLE Forming the arc tangent of the ratio of analogue sine and cosine signal (A/B-signals).

3.8
solid measure
component providing encoded pattern used to determine a mechanical position

EXAMPLE Optical disc, magnetic strip.

Note 1 to entry: Other terms for *solid measure* are scale, disc, ring, strip.

3.9
mechanical fastening
mechanical connection for load transmission between constructional elements or attachment of constructional elements

Note 1 to entry: Load transmission can for example happen

- between stator of the motor and stator of the *Encoder(SR)*,
- between shaft of the motor and shaft of the rotary *Encoder(SR)*,
- between fixed part of the machine and fixed part of the *Encoder(SR), or*
- between moving part of the machine and moving part of the *Encoder(SR)*.

Note 2 to entry: Load transmission can also happen within the *Encoder(SR)*.

Note 3 to entry: *Mechanical fastenings* are typically realized by bolted joints, fitting keys and key and slot joints.

3.10
mechanical connecting element
rigid or flexible mechanical part used to transmit load between *mechanical fastenings*

Note 1 to entry: *Mechanical connecting elements* are usually designated as couplings.

Note 2 to entry: Couplings may also provide compensation for mechanical tolerances during attachment or operation.

Note 3 to entry: Couplings are usually designated as *shaft-rotor coupling* or as *stator coupling*.

3.11
shaft-rotor coupling
connecting element between the shaft of a rotary *Encoder(SR)* and a driven shaft

Note 1 to entry: The *shaft-rotor coupling* is located between the ends of shafts.

Note 2 to entry: The *shaft-rotor coupling* has the task of compensating for mechanical tolerances during attachment or operation.

Note 3 to entry: The *shaft-rotor coupling* is typically realized as bellow coupling, jaw type coupling, slit type coupling, or lamina type coupling.

3.12
stator coupling
part of a rotary *Encoder(SR)* used to fix the *Encoder(SR)* with regards to a mounting point

Note 1 to entry: The *stator coupling* has the task of compensating for mechanical tolerances during attachment or operation.

Note 2 to entry: The *stator coupling* is fastened to flange or housing.

Note 3 to entry: The *stator coupling* is also known as "torque support".

Note 4 to entry: The *stator coupling* can also be located within the *Encoder(SR)*.

3.13
bearing blockage
situation where the torque necessary for the rotation of the bearing is causing the *Encoder(SR)* to be exposed to forces or torques higher than taken into account during design and development

3.13.1
spontaneous bearing blockage
suddenly occurring *bearing blockage* without any changes to the bearing properties in advance

Note 1 to entry: *Fault* detection prior to the *spontaneous bearing blockage* is not possible.

3.13.2
gradual bearing blockage
slowly occurring *bearing blockage* with preceding change in bearing properties

Note 1 to entry: It might be possible to detect the *fault* in time and set to safe state before the bearing becomes blocked.

Note 2 to entry: A *gradual bearing blockage* can be the result of wear or fatigue.

3.14
measurement point for working temperature
point on the surface of the *Encoder(SR)* for measuring the working temperature

3.15
working temperature range
temperature limits between which the measuring value does not exceed the given fault limits

3.16
extra low voltage
ELV
voltage not exceeding 50 V AC RMS and 120 V DC

Note 1 to entry: RMS ripple voltage of not more than 10 % of the DC component.

[SOURCE: IEC 61800-5-1:2007, 3.9, modified – Note 2 has been deleted.]

3.17
protective ELV circuit
PELV circuit
electrical circuit with the following characteristics:

- the voltage does not continuously exceed *ELV* under single *fault* as well as during normal conditions;
- protective separation from circuits other than *PELV* or SELV;
- provisions for earthing of the *PELV circuit*, or its accessible conductive parts, or both

[SOURCE: IEC 61800-5-1:2007, 3.21]

3.18
decisive voltage class
DVC
classification of voltage range used to determine the protective measures against electric shock

Note 1 to entry: According to IEC 61800-5-1:2007, Table 3, the voltage limits of *DVC* A are 25 V AC, 35,4 V AC_{peak} and 60 V DC.

[SOURCE: IEC 61800-5-1:2007, 3.7; modified – Note 1 to entry has been added.]

3.19
functional safety
FS
part of the overall safety relating to the *Encoder(SR)* which depends on the correct functioning of the *safety-related parts of the Encoder(SR)* and on external risk reduction measures

Note 1 to entry: This document only considers those aspects in the definition of *functional safety* that depend on the correct functioning of the *Encoder(SR)*.

[SOURCE: IEC 61800-5-2:2016; 3.11, modified – The abbreviated term "FS" has been added, and the word "*PDS(SR)*" has been replaced with *Encoder(SR)*.]

3.20
safety function
function to be implemented by a safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the equipment or machinery, in respect of a specific hazardous event

[SOURCE: IEC 61800-5-2:2016, 3.22, modified – The words "driven by the *PDS(SR)*" have been deleted.]

3.21
safety sub-function
function(s) with a specified safety performance, to be implemented in whole or in part by an *Encoder(SR)*, which is (are) intended to maintain the safety of the installation or prevent *hazardous* conditions arising at the installation

Note 1 to entry: There are only rare cases where the *safety function* of the complete application is implemented exclusively within the *Encoder(SR)*. In these cases, the *safety function* is still called a *safety sub-function* in this document.

[SOURCE: IEC 61800-5-2:2016, 3.23, modified – The words "*PDS(SR)*" have been replaced by "*Encoder(SR)*". The words "<of a PDS(SR)>" and the example in the Note to entry have been deleted.]

3.22
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – The note has been deleted.]

3.23
dangerous failure
failure of a component and/or subsystem and/or system that plays a part in implementing the *safety sub-function* that:

- causes a *safety sub-function* of an *Encoder(SR)* to fail such that the equipment or machinery is put into a hazardous or potentially hazardous state; or
- decreases the probability that the *safety sub-function* operates correctly

[SOURCE: IEC 61800-5-2:2016, 3.5, modified – The word "*PDS(SR)*" has been replaced by "*Encoder(SR)*", and the words "driven by the *PDS(SR)*" have been deleted.]

3.24
hardware fault tolerance
HFT
ability of an *Encoder(SR)* to continue to perform a required function in the presence of hardware *faults* or errors

Note 1 to entry: According to IEC 61800-5-2:2016, the *HFT* yields requirements for the diagnostic test interval. In addition, the *HFT* in 6.2.3.1 of IEC 61800-5-2:2016 is one of the attributes used for determining an upper limit for the *safety integrity level* (*SIL*).

Note 2 to entry: This definition has been derived from IEC 61508-4:2020, 3.6.3.

3.25
single-fault tolerance
ability of a functional unit to continue to perform a required function in the presence of one *fault* or error

[SOURCE: IEC 61508-4:2010, 3.6.3, modified – The word "single-" has been added in the term, and the words "*faults* or errors" have been replaced with "one *fault* or error".]

3.26
safety integrity level
SIL
discrete level (one out of a possible three) for specifying the safety integrity requirements of a *safety sub-function* allocated (in whole or in part) to an *Encoder(SR)*

Note 1 to entry: *SIL* 3 has the highest level of safety integrity and *SIL* 1 has the lowest.

Note 2 to entry: *SIL* 4 is not considered in this document as it is not relevant to the risk reduction requirements normally associated with *Encoder(SR)s*. For requirements applicable to *SIL* 4, see IEC 61508.

Note 3 to entry: Several methods of writing are used for *SIL*x. Throughout this document *SIL* x is used.

[SOURCE: IEC 61800-5-2:2016; 3.25, modified – The word "*PDS(SR)*" has been replaced by "*Encoder(SR)*" and Note 4 to entry deleted.]

3.27
SIL capability
maximum *SIL* that can be claimed to have been achieved by the design of an *Encoder(SR)* in terms of the systematic safety integrity and the architectural constraints on hardware safety integrity

Note 1 to entry: Each of the designated *safety sub-functions* that an *Encoder(SR)* is intended to perform can be associated with a different *SIL capability*.

Note 2 to entry: *SIL capability* includes systematic capability, the fulfilment of the architectural constraints and the hardware failure rate or *PFH* value.

[SOURCE: IEC 61800-5-2:2016, 3.28, modified: – The word "*PDS(SR)*" has been replaced by "*Encoder(SR)*".]

3.28
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a *safety function* under foreseeable conditions

Note 1 to entry: See ISO 13849-1:2015, 4.5.1.

[SOURCE: ISO 13849-1:2015, 3.1.23]

3.29
diagnostic coverage
DC
fraction of *dangerous failures* detected by automatic diagnostic tests

Note 1 to entry: This can also be expressed as the ratio of the sum of the detected *dangerous failure* rates λ_{DD} to the sum of the total *dangerous failure* rates λ_D: $DC = \Sigma\lambda_{DD}/\Sigma\lambda_D$.

Note 2 to entry: *Diagnostic coverage* can exist for the whole or parts of a safety-related system. For example, *diagnostic coverage* can exist for sensors and/or logic *subsystems* and/or output *subsystem*.

[SOURCE: IEC 61800-5-2:2016, 3.6, modified – Note 3 to entry has been deleted.]

3.30
safe failure fraction
SFF
property of a safety-related component and subsystems that is defined by the ratio of the sum of the average failure rates of safe and dangerous detected failures to the sum of safe and all *dangerous failures*

Note 1 to entry: This ratio is represented by the equation: $SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

Note 2 to entry: See Annex C of IEC 61508-2:2010.

[SOURCE: IEC 61800-5-2:2016, 3.20, modified – Note 3 to entry has been deleted.]

3.31
average frequency of a dangerous failure
PFH
average frequency of a *dangerous failure* of an *Encoder(SR)* to perform the specified *safety sub-function* over a given period of time

Note 1 to entry: In IEC 62061, the abbreviation PFH_D is used.

[SOURCE: IEC 61800-5-2:2016, 3.17, modified – The word "PDS(SR)" has been replaced by "*Encoder(SR)*" and Note 2 to entry deleted.]

3.32
mean time to dangerous failure
$MTTF_D$
expectation of the mean time to dangerous failure

[SOURCE: ISO 13849-1:2015; 3.1.25]

3.33
process safety time
period of time between a failure of the *Encoder(SR)* that has the potential to cause a hazardous event and the point in time at which action has to be completed to prevent the hazardous event from occurring

[SOURCE: IEC 61508-4:2010, 3.6.20, modified – The wording has been simplified.]

3.34
ideal fault detection
detection of all *dangerous failures* and achievement of a safe state within the *process safety time*

Note 1 to entry: "*Ideal fault detection*" is a method that is applied to impart the property of *single-fault tolerance* to (sub-) systems that have a *HFT* of 0. *Single-fault tolerance* is a necessary condition for categories 3 and 4 according to ISO 13849-1. A detailed description of *ideal fault detection* is included in Annex J.

3.35
quantitative FMEDA
systematic analysis technique to obtain function block failure rates, failure modes and diagnostic capability

Note 1 to entry: The *quantitative FMEDA* (failure modes, effects and diagnostics analysis) provides the input data for quantification (calculation of *PFH*, *SFF*, $MTTF_D$ (if conformity with ISO 13849-1:2015 is claimed)). It is carried out separately for each function block and divides the failure rates for all the components contained in the block separately into safe (S), dangerous (D), dangerous detectable (DD) and dangerous undetectable (DU).

3.36
qualitative FMEDA
systematic analysis technique to obtain systematic failures of function blocks

Note 1 to entry: *Qualitative FMEDA* (failure modes, effects and diagnostics analysis) is used for revealing possible systematic effects and scenarios that could impair the performance of the *safety sub-function*. For all components, it verifies that failures with a detrimental effect on the *safety sub-function* are detected and are mastered by the specified diagnostics and that, in the case in question, a certain failure can be justifiably excluded. FMEDA is used particularly for verification of the *single-fault tolerance* of an *Encoder(SR)* (see 8.4).

Note 2 to entry: In connection with static analysis (see Annex L), *qualitative FMEDA* is used for verifying that all potential *fault* scenarios are mastered by the specified diagnostics (see Clause L.7).

3.37
signal evaluation
evaluation of the output signals of the *Encoder(SR)* for the purpose of executing a *safety function*

Note 1 to entry: See also 3.38.

3.38
signal processing
signal evaluation and integrity test of the output signals for the detection of *faults* in the *Encoder(SR)* (diagnostics)

Note 1 to entry: The relationship between *signal processing*, *signal evaluation* and diagnostics is as follows: *signal processing* = *signal evaluation* + diagnostics.

4 *Safety sub-functions*

4.1 General

Clause 4 describes functions of an *Encoder(SR)* that may be designated as safety-related by the *Encoder(SR)* supplier. The designated *safety sub-functions* in Clause 4 are not considered to form an exhaustive list.

The technical measures required to implement these functions depend on the required *SIL capability* (and *PL* capability, if compliance with ISO 13849-1 is claimed) including the required probability of dangerous hardware failure, as indicated in the *safety requirements specification.* The technical measures are described in Clause 6.

The names of the *safety sub-functions* include the word "safe" to indicate that these functions may be used in a safety-related application on the grounds of a judgement (for example risk analysis) of that specific application, resulting in safety-relevant functions and their integrity to be performed by the *Encoder(SR)*.

The *Encoder(SR)'s safety sub-function(s)* may be used for implementation of the safety sub-function(s) of a *PDS(SR)*.

4.2 Safe incremental position (SIP)

This function provides an output signal that is safe in relation to the relative mechanical measurement position.

The relation of the output signal to the relative measurement position shall be within a *tolerance range* that shall be specified and included in the information for use.

4.3 Safe absolute position (SAP)

This function provides an output signal that is safe in relation to the mechanical measurement position.

The relation of the output signal to the measurement position shall be within a *tolerance range* that shall be specified and included in the information for use.

NOTE The reason for splitting the two *safety sub-functions* SIP and SAP is due to the big difference in the way these two different position values are generated and the way they are used.

4.4 Safe speed value (SSV)

This function provides an output signal that is safe in relation to the speed of the moving part.

The relation of the output signal to the speed of the moving part shall be within a *tolerance range* that shall be specified and included in the information for use.

4.5 Safe acceleration value (SAV)

This function provides an output signal that is safe in relation to the acceleration of the moving part.

The relation of the output signal to the acceleration of the moving part shall be within a *tolerance range* that shall be specified and included in the information for use.

4.6 *Safety sub-functions* for evaluation and signalling

Safety sub-functions providing *signal processing* within the *Encoder(SR)* and respective output signal(s) are possible, for example safely-limited speed SLS (see IEC 61800-5-2:2016, 4.2.4.5). For these *safety sub-functions*, the requirements for design and development, and verification and validation as defined by IEC 61800-5-2 shall apply.

5 Management of *functional safety*

The requirements of IEC 61800-5-2:2016, Clause 5, shall apply.

6 Requirements for design and development

6.1 General requirements

Table 2 indicates which parts of Clause 6 of IEC 61800-5-2:2016 shall be applied as is and which parts of Clause 6 of IEC 61800-5-2:2016 are modified for *Encoder(SR)*.

Table 3 indicates which parts of IEC 61800-5-1:2007 and IEC 61800-5-1:2007/AMD1:2016 shall be applied as is and which parts of IEC 61800-5-1:2007 and IEC 61800-5-1:2007/AMD1:2016 are modified for *Encoder(SR)*.

Encoder(SR) include diverse technologies and several hardware function blocks, needed to provide the *Encoder(SR)'s safety sub-functions*. The realisations of the *Encoder(SR)* are different, but they can always be structured according to the universal architecture described in Annex B. Subclauses 6.5 to 6.8 describe the additional requirements for these hardware function blocks.

Table 2 – Applicable subclauses of IEC 61800-5-2:2016 for *Encoder(SR)* and respective modifications

Requirements for *PDS(SR)* from IEC 61800-5-2:2016		Shall be applied for *Encoder(SR)?*	Applicable subclause in this document
6.1	General requirements	No, replaced	6.1 General requirements
6.1.1	Change in operational status	No	
6.1.2	Design standards	No, replaced	6.2 Design standards
6.1.3	Realisation	Yes	
6.1.4	Safety integrity and fault detection	Yes	
6.1.5	Safety and non-safety sub-functions	Yes	
6.1.6	SIL for multiple safety sub-functions within one *PDS(SR)*	Yes	
6.1.7	Integrated circuits with on-chip redundancy	Yes	
6.1.8	Software requirements	Yes	6.9 Design requirements for software
6.1.9	Design documentation	Yes	
6.2	*PDS(SR)* design requirements		
6.2.1	Basic and well-tried safety principles	Yes	
6.2.2	Requirements for the estimation of the probability of dangerous random hardware failures per hour (PFH)		
6.2.2.1	General requirements		
6.2.2.1.1	PFH for each safety sub-function	Yes	
6.2.2.1.2	Estimation of PFH	Yes	

Requirements for *PDS(SR)* from IEC 61800-5-2:2016		Shall be applied for *Encoder(SR)?*	Applicable subclause in this document
6.2.2.1.3	Failure rate data	Yes	
6.2.2.1.4	Diagnostic test interval when the hardware fault tolerance is greater than zero	Yes	
6.2.2.1.5	Diagnostic test interval when the hardware fault tolerance is zero	Yes	
6.2.3	Architectural constraints		
6.2.3.1	Limitations of SIL	Yes	
6.2.3.2	Type A and Type B subsystems		
6.2.3.2.1	General	Yes	
6.2.3.2.2	Type A	Yes	
6.2.3.2.3	Type B	Yes	
6.2.3.3	Architectural constraints	Yes	
6.2.4	Estimation of safe failure fraction (SFF)		
6.2.4.1	Methods of analysis	Yes	
6.2.5	Requirements for systematic safety integrity of a *PDS(SR)* and *PDS(SR)* subsystems		
6.2.5.1	Requirements for the avoidance of failures		
6.2.5.1.1	General	Yes	
6.2.5.1.2	Choice of design methods	Yes	
6.2.5.1.3	Design measures	Yes	
6.2.5.1.4	Test planning	Yes	
6.2.5.1.5	Design maintenance requirements	Yes	
6.2.5.2	Requirements for the control of systematic faults		
6.2.5.2.1	General	Yes	
6.2.5.2.2	Design features	Yes, with addition	6.6 Design requirements for signal generation
6.2.5.2.3	Testability and maintainability	Yes	
6.2.5.2.4	Human constraints	Yes	
6.2.5.2.5	Protection against unintentional modification	Yes	
6.2.5.2.6	Input acknowledgement and operator mistakes	No	
6.2.5.2.7	*PDS(SR)* parameterization	Yes, with addition	6.11 Parameterization
6.2.5.2.8	Loss of electrical supply	Yes	
6.2.6	Design requirements for electromagnetic (EM) immunity of a *PDS(SR)*	Yes	
6.2.7	Design requirements for thermal immunity of a *PDS(SR)*	No, replaced	6.12 Design requirements for thermal immunity
6.2.8	Design requirements for mechanical immunity of a *PDS(SR)*	No, replaced	6.13 Design requirements for mechanical immunity
6.3	Behaviour on detection of fault		
6.3.1	Fault detection	Yes, with addition	6.3 Fault detection
6.3.2	Fault tolerance greater than zero	Yes	
6.3.3	Fault tolerance zero	Yes	
6.4	Additional requirements for data communications	Yes	
6.5	*PDS(SR)* integration and testing requirements		
6.5.1	Hardware integration	Yes	

Requirements for *PDS(SR)* from IEC 61800-5-2:2016		Shall be applied for *Encoder(SR)?*	Applicable subclause in this document
6.5.2	Software integration	Yes	
6.5.3	Modifications during integration	Yes	
6.5.4	Applicable integration tests	Yes	
6.5.5	Test documentation	Yes	

Table 3 – Applicable references of IEC 61800-5-1:2007 and IEC 61800-5-1:2007/AMD1:2016 for *Encoder(SR)* and respective modifications

Requirements for *PDS(SR)* from IEC 61800-5-1:2016 CSV		Shall be applied for *Encoder(SR)?*	Modification for *Encoder(SR)*
4	Protection against electric shock, thermal, and energy hazards		
4.1	General	Yes	
4.2	Fault conditions	Yes	
4.3	Protection against electric shock		
4.3.1	Decisive voltage classification	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.2	Protective separation	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.3	Protection against direct contact	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.4	Protection in case of direct contact	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.5	Protection against indirect contact	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.

Requirements for *PDS(SR)* from IEC 61800-5-1:2016 CSV		Shall be applied for *Encoder(SR)?*	Modification for *Encoder(SR)*
4.3.5.1	General	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.5.2	Insulation between live parts and accessible conductive parts	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.5.3	Protective bonding circuit	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.5.4	Protective earthing conductor	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.5.5	Means of connection for the protective earthing conductor	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.5.6	Special features in equipment for protective class II	Yes	Excluded are *Encoder(SR)* that are exclusively – supplied with voltage source(s) using PELV circuit(s) conforming to DVC A; and – connected to PELV circuits conforming to DVC A.
4.3.6	Insulation	Yes	See Annex E for an example
4.3.7	Enclosures	Yes	
4.3.8	Wiring and connections	Yes	
4.3.9	Output short-circuit requirements	Yes	
4.3.10	Residual current-operated protective (RCD) or monitoring (RCM) device compatibility	No	
4.3.11	Capacitor discharge	No	
4.3.12	Access conditions for high-voltage PDS	No	
4.4	Protection against thermal hazards	Yes	

Requirements for *PDS(SR)* from IEC 61800-5-1:2016 CSV		Shall be applied for *Encoder(SR)?*	Modification for *Encoder(SR)*
4.4.1	Minimizing the risk of ignition	Yes	
4.4.2	Insulating materials	Yes	
4.4.3	Flammability of enclosure materials	Yes	
4.4.4	Temperature limits		
4.4.4.1	Internal parts	Yes	
4.4.4.2	External parts of CDM	Yes	
4.4.5	Specific requirements for liquid cooled PDS	No	
4.5	Protection against energy hazards	No	
4.6	Protection against environmental stresses	Yes	

6.2 Design standards

Encoder(SR) shall be designed in accordance with IEC 61800-1, IEC 61800-5-1 and IEC 61800-5-2. This document includes additional requirements specific for *Encoder(SR)* or deviating from the requirements for *PDS(SR)*.

If requirements of this document conflict with the requirements of other applicable standards, the requirements of this document take precedence.

Additionally, the requirements of ISO 13849-1 should be complied with for *Encoder(SR)* dedicated for machinery application.

6.3 *Fault* detection

The necessary diagnostic measures for *Encoder(SR)* may be split into:

- diagnostic measures performed by the *Encoder(SR);* and
- diagnostic measures performed in the *evaluation unit.*

If diagnostic measures apply within the *Encoder(SR)*, the detection of a *dangerous fault* shall be indicated to the *evaluation unit*.

If *fault* detection shall be performed in the *evaluation unit*, appropriate requirements and the specification of recommended measures for suitable *fault* detection shall be included in the information for use of the *Encoder(SR)*.

NOTE 1 See Annex I for processing *fault* detection of analogue sine and cosine signals in digital technique.

If the use of position values generated by *interpolation* of the sine and cosine *Encoder(SR)* output signal is not excluded in the instructions for use, appropriate diagnostic measures shall be applied.

EXAMPLE 1 The minimum number of samples per signal period of the *solid measure* is specified.

If *ideal fault detection* is required for the *Encoder(SR)* (see 6.4.1), the diagnostic measures applied for the *Encoder(SR)* shall be suitable for revealing all *faults* that lead to an error in any *safety sub-function* of the *Encoder(SR)* exceeding the *tolerance range* specified in the information for use. The suitability of these measures for *fault* detection shall be proven applying static analysis according to Annex L.

When a *fault* that can lead to loss of the *safety sub-function* is detected, a *fault* reaction function shall be initiated in order to prevent a hazard. Diagnostics and *fault* reaction functions shall be performed within the specified maximum *fault* reaction time.

NOTE 2 The *fault* reaction function of *Encoder(SR)* is usually limited to an indication of a *fault* to the *evaluation unit*.

The fault detection by the *Encoder(SR)* or the evaluation unit shall not be delayed or impeded by functions controlling amplitude and/or phase of analogue signals (see Annex M for examples).

NOTE 3 Analogue signals regarded here can be the output signals of an *Encoder(SR)* with sine and cosine output signals used in signal generation or signal processing of an *Encoder(SR)*.

EXAMPLE 2 Due to a component fault, the sine signal is corrupted, its amplitude is controlled and the phasor length is erroneously maintained within the specified tolerances – even during the passage of each individual period of the solid measure. Fault detection applying phasor length monitoring is impeded.

EXAMPLE 3 Controlling of the amplitudes of sine and cosine signals operates slower than the diagnostic measures apply. A dangerous failure can be detected by phasor length monitoring before the amplitude of sine or cosine signal is processed. A delay of fault detection and an increased fault reaction time is prevented.

6.4 Design requirements for specific types of *Encoder(SR)*

6.4.1 Design requirements for *Encoder(SR)* with sine and cosine output signals

For incremental *Encoder(SR)* that have independent signal generation and *signal processing* for one set of sine and cosine output signals (for example A, /A, B, /B), these signals can be considered redundant for unsigned speed information that will contribute to safety sub-function(s) (for example SLS, SSR, SLA, SS1, SS2 according to IEC 61800-5-2:2016, Clause 4). In this case, the application of *ideal fault detection* is not required and speed can be obtained redundantly by sine and cosine signals if independently evaluated.

NOTE 1 The application of quadrature decoder ICs for evaluation destroys the independency of the sine and cosine signals.

For incremental *Encoder(SR)* that do not have independent signal generation and *signal processing* or where the incremental or absolute position or direction information contributes to safety sub-function(s) (for example SOS, SDI, SCA, SLP, SSR according to IEC 61800-5-2:2016, Clause 4), the set of sine and cosine output signals (e.g. A, /A, B, /B) cannot be considered redundant. These *Encoder(SR)* shall apply *ideal fault detection* (see Annex J for more information) if category 3 or category 4 according to ISO 13849-1:2015 is claimed. If category 4 is claimed for the *Encoder(SR)*, the diagnostic measures applied to achieve *ideal fault detection* shall:

- be redundant; or
- include their own diagnostic measures with a minimum *DC* of 99 %.

Encoder(SR) which apply *ideal fault detection* shall be limited to category 3 when just one integrated circuit without on-chip redundancy according to IEC 61508-2:2010, Annex E, is used for signal generation and/or *signal processing*.

NOTE 2 If on-chip redundancy is fulfilled, the *signal processing* of the sine signal and the cosine signal is considered independent. Since the sine AND the cosine signals are necessary to achieve the safe incremental or absolute position and therefore there is no redundancy of the position information, the *HFT* is still 0.

NOTE 3 The compliance with *ideal fault detection* is necessary to fulfill the requirements for category 3 and category 4 of ISO 13849-1:2015, 6.2.6 and 6.2.7. The definitions of these categories include "…a single fault … does not lead to the loss of the *safety function*".

NOTE 4 The *hardware fault tolerance* (*HFT*) is one input parameter necessary for the determination of the *SIL* limit in accordance with the architectural constraints (see H.9.2).

6.4.2 Design requirements for *Encoder(SR)* with incremental and absolute output signals

6.4.2.1 General

Encoder(SR) with incremental and absolute output signals show an architecture with two channels, one providing an incremental signal, the other providing an absolute position information.

6.4.2.2 Generation of the safe absolute position value

In the *evaluation unit*, a redundant absolute position value shall be generated from the incremental output signal of the *Encoder(SR)* and a suitable reference. To produce a safe absolute position value, the absolute position value of the *evaluation unit* and the absolute position value from *Encoder(SR)* shall be compared (cross checked) and shall comply within specified tolerances. See Figure 2 for an example of a hardware architecture.

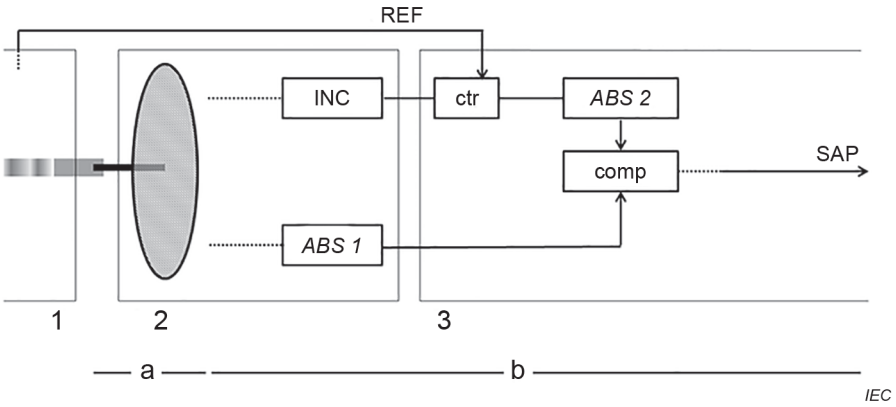
The *Encoder(SR)* shall be designed so that no undetectable dangerous *failure* can occur that causes a simultaneous change in the incremental and absolute position values which results in identical incorrect absolute position values within specified tolerances.

NOTE *Encoder(SR)* with separate, diverse *signal processing* for the incremental and absolute position values usually satisfy this requirement.

The instruction for use of the *Encoder(SR)* shall describe the process in the *evaluation unit* for generating the redundant absolute position value and for detecting *faults* in the absolute position value with the required *DC*.

If the individual channels of the *Encoder(SR)* require dedicated diagnostics performed by the *evaluation unit*, they shall be described in the instructions for use of the *Encoder(SR)*.

The reference of the *evaluation unit* for the second absolute position value shall be independent from the absolute position value of the *Encoder(SR)*.



Key

a	no redundancy, *fault* exclusion or *ideal fault detection* applied
b	redundancy, *fault* detection applied
1	machine
2	*Encoder(SR)*
3	*safe evaluation unit*
ABS 1	absolute position value provided by the *Encoder(SR)*
ABS 2	absolute position value generated by counting the incremental pulses provided by the *Encoder(SR)*
comp	comparison of *ABS 1* with *ABS 2*
ctr	counter
INC	incremental signal provided by the *Encoder(SR)*
REF	independent signal from fixed point within the machine to run referencing procedure for *ABS* 2
SAP	*safety sub-function* safe absolute position

Figure 2 – Example of hardware architecture of *Encoder(SR)* with incremental and absolute output signal

The application of this type of *Encoder(SR)* provides the *safety sub-function* safe absolute position (SAP).

6.4.3 Design requirements for *Encoder(SR)* with square wave signal interface

Since square wave signal interface do not allow a sufficient diagnosis of the correct functioning of the *Encoder(SR)*, the following requirements shall be fulfilled.

The *Encoder(SR)* with square wave interface shall:

- include all necessary measures to fulfil the requirements of Clause 6 of IEC 61800-5-2:2016;
- provide a safe means to indicate any detected *fault* to the *evaluation unit.*

EXAMPLE Square wave output signals can be of the type HTL, TTL or HC-HTL.

Additionally, the requirements of ISO 13849-1 should be complied with for *Encoder(SR)* dedicated for machinery application.

6.4.4 Design requirements for Resolver

The requirements of this document shall be applied where applicable. In any case, the following requirements shall be applied:

- management of *functional safety* (see Clause 5);
- mechanics (see Clause 6.5);

- information for use (see Clause 7);
- verification and validation (see Clause 8);
- test requirements (see Clause 9); and
- modification (see Clause 10).

NOTE Resolver usually do not include electronic components, since respective functions are not included in the Resolver itself but are provided by the *evaluation unit*.

6.5 Design requirements regarding mechanics

6.5.1 General

Encoder(SR) contain a fixed and a moving part that are connected to the associated machine parts by means of *mechanical fastenings* and *mechanical connecting elements*.

6.5.2 Design requirements for *mechanical fastenings*

If a detached fastening can cause a *dangerous failure* and diagnostic measures are not available, *fault* exclusion for this fastening shall be proven according to ISO 13849-2 and/or Annex G. If a *fault* exclusion for a bolted joint is required:

- appropriate methods for the design shall be used, for example as specified in [6]; and
- additionally, the bolted joints shall be secured against loosening (because of settlement, embedding, creep or relaxation).

6.5.3 Design requirements for *mechanical connecting elements*

Fault exclusions can also be justified for *mechanical connecting elements* by suitable over-dimensioning (see ISO 13849-1:2015, 7.3 and ISO 13849-2:2012, Annex A). The necessary strength for the *mechanical connecting elements* and their durability against fatigue failure shall be proven.

NOTE 1 The calculation can be done in accordance with [7].

NOTE 2 Application to Annex G is not possible, as Table G.1 only deals with form-locked or force-locked *mechanical fastenings* and not with the material itself.

NOTE 3 *Mechanical connecting elements* are usually designated as couplings (see 3.11 and 3.12).

6.5.4 Bearings

In the case of *Encoder(SR)* with bearing(s), a *bearing blockage* can lead to a *dangerous failure*. When *fault* exclusion(s) are applied to the *mechanical connections* (for example as listed in Table G.1), the following measures shall be taken to avoid and deal with *spontaneous bearing blockage* and *gradual bearing blockage* (see Table G.2).

1) *Spontaneous bearing blockage* – appropriate measures

   All measures to achieve the *fault* exclusion for *spontaneous bearing blockage* from Table G.2 shall be taken.

2) *Gradual bearing blockage* – appropriate measures
   a) a *bearing blockage* does not lead to a dangerous failure, or
   b) a *bearing blockage* is detected and action is taken to respond to the *fault* before the situation can become dangerous, or
   c) gradual bearing blockage is controlled through early detection and by taking action to respond to the fault, or

      NOTE 1 Wear and fatigue alter the operating behaviour of a bearing and might become evident through:

      i) increased torque;

      ii) uneven running;

iii) reduced operational accuracy;

iv) unusual noises during operation;

v) increase in temperature.

d) organizational measures are taken to replace the bearing/the *Encoder(SR)* before the bearing reaches the end of its service life.

NOTE 2 Organizational measures include, for example, corresponding instructions in the information for use or precautions inside the *Encoder(SR)* with signals being sent to the higher-level control.

NOTE 3 The service life of the bearing is usually estimated in accordance with ISO/TS 16281 [8] jointly by the *Encoder(SR)* manufacturer, the bearing manufacturer, and the grease supplier, taking the mission time of the grease into account.

NOTE 4 Aging, wear, contamination, etc. will reduce the lubricity of the grease. This will lead to an increase in the forces necessary to move the bearing. This effect does not have to be taken into account during the mission time of the grease.

The *Encoder(SR)* manufacturer shall specify in the information for use the boundary conditions on the basis of which the service life of the bearing has been estimated.

NOTE 5 The boundary conditions on the basis of which the service life of the bearing is estimated include, for example, temperature, installation position, attachment conditions (alignment *faults*, coupling, forces, etc.), speed, number of revolutions, reversing operation and contamination class.

6.6 Design requirements for signal generation

6.6.1 General

The applied sensor principle of the *Encoder(SR)* shall be suitable for the intended application. Any restrictions regarding the application of the *Encoder(SR)* shall be included in the information for use (see Clause F.2 b)).

NOTE The environmental conditions at the application, like magnetic fields, shock and vibration, pollution etc. can affect the measurement.

6.6.2 Design requirements for signal generation of optical *Encoder(SR)*

On optical *Encoder(SR)*, dirt particles can be deposited in the optical path, for example *solid measure* or optical sensor, and thus cause faulty measurements that prevent the correct performance of the *safety sub-function*. Dirt particles can come, for instance, from the ambient air or arise due to bearing friction and seal abrasion. The deposition of dirt particles shall not be excluded without suitable measures. The effect of contamination could in principle be revealed with *fault*-detecting measures.

NOTE 1 Partial contamination, however, might only be detectable within a narrow position range. If measures for *fault* detection are performed at discrete times, *fault detection* is not ensured within the test interval.

NOTE 2 Measures to enhance availability are often integrated in *evaluation units* that are designed to suppress sporadically occurring *fault* signals. This is capable of additionally delaying or preventing the identification of partial contamination.

6.6.3 Design requirements for signal generation of magnetic *Encoder(SR)*

Since *Encoder(SR)* which use magnetic sensors for detecting position are susceptible to external magnetic fields also, the following specific requirements for the magnetic immunity of these *Encoder(SR)* shall be fulfilled:

- maximum value for external magnetic fields valid in any field direction for criterion A is included in the information for use;
- maximum value for external magnetic fields valid in any field direction for criterion *FS* is included in the information for use; and
- minimum requirement is according IEC 61000-6-7:2014, Table 2, 2.5, but criterion *FS*.

NOTE 1 An advice to demonstrate that the value of the external magnetic field at the *Encoder(SR)* location does not exceed the specified limits can be helpful in the information of use.

NOTE 2 In this document, criterion *FS* is used instead of criterion DS according to IEC 61800-5-2:2016, 9.3.3.

6.7 Design requirements for *signal processing*

The requirements of IEC 61800-5-2:2016 shall apply.

6.8 Design requirements for internal evaluation and signaling

The requirements of IEC 61800-5-2:2016 shall apply.

6.9 Design requirements for software

If software is used to perform the *safety sub-function(s)*, this software shall be developed in accordance with the requirements of IEC 61800-5-2:2016, 6.1.8.

NOTE IEC 61800-5-2:2016, 6.1.8, refers to IEC 61508-3. Accordingly, software faults as a subset of systematic *faults* are considered to limit the systematic capability, and the rules for the attainment of systematic capability of IEC 61508-2:2010, 7.4.3, apply. Therefore, the software systematic capability can undercut the intended *SIL* of the *safety sub-function* by one *SIL* step, if *ideal fault detection* is applied and also includes the behavior of software.

If compliance with ISO 13849-1 is claimed, the additional requirements of ISO 13849-1:2015, 4.6, shall apply.

6.10 Pre-setting

If the *Encoder(SR)* includes a position pre-setting function, it shall be designed in a way that the position pre-setting function does not compromise any of its *safety sub-functions*.

NOTE The pre-setting function is also known as "offset", "zeroing function" or "position setting function".

6.11 Parameterization

If the behaviour of a *safety sub-function* may be influenced by configuration of the respective parameters, their settings shall be considered safety related.

The requirements of IEC 61800-5-2:2016, 6.2.5.2.7 shall apply.

If compliance with ISO 13849-1 is claimed, the additional requirements of ISO 13849-1:2015, 4.6.4 shall apply.

6.12 Design requirements for thermal immunity

The *Encoder(SR)* shall be designed to have the appropriate thermal immunity for operating within the specified thermal environment.

NOTE The thermal immunity test requirements are described in 9.5.

6.13 Design requirements for mechanical immunity

The *Encoder(SR)* shall be designed to have the appropriate mechanical immunity for operating within the specified mechanical environment.

NOTE The mechanical immunity test requirements are described in 9.6.

Specific applications may cause shocks to rotary *Encoder(SR)* mounted to motors which are not covered by tests according to 9.6.5. This affects particularly shocks caused by the engagement and disengagement of mechanical brakes. To verify the resilience against these shocks, see Annex D.

6.14 Design requirements for integrated connection cables

The requirements of IEC 60947-5-2:2019, Annex C, shall apply.

7 Information for use

7.1 General

The requirements of IEC 61800-5-2:2016, Clause 7, and the following requirements shall apply.

7.2 Labels

The requirements of IEC 61800-1:1997, 8.1, shall apply as applicable.

7.3 Information and instructions for safe application of an *Encoder(SR)*

Information and instructions shall conform to Annex F.

Instructions shall be provided legibly.

NOTE A character height of 2 mm is considered readily legible.

8 Verification and validation

8.1 General

The requirements of IEC 61800-5-2:2016, Clause 8, and the following requirements (specific for *Encoder(SR))* shall apply.

8.2 Verification of *hardware fault tolerance*

To verify the *Encoder(SR)*'s *HFT*, a breakdown of the architecture and allocation of all safety relevant components to the functional blocks of the universal architecture (see Annex B) shall be performed.

NOTE Depending on the realisation of the *Encoder(SR)*, not all function blocks are implemented.

A *qualitative FMEDA* shall be performed (see 8.4).

8.3 Additional verification for *Encoder(SR)* with sine and cosine output signals

8.3.1 Verification of diagnostic measures for *Encoder(SR)* with sine and cosine output signals with *HFT* = 0

If *ideal fault detection* is required, the effectiveness of the diagnostic measures for incremental *Encoder(SR)* with sine and cosine output signals with *HFT* = 0 shall be proven with the static analysis method according to Annex L.

8.3.2 Suitability for *interpolation*

In the application of an *Encoder(SR)* with sine and cosine output signals, the signals may have to be *interpolated* to increase the resolution. The *fault*-detecting measures shall be appropriate.

If *ideal fault detection* is required, it shall be proven that one of the three following alternatives applies:

- the *interpolation* of the sine and cosine signal for safety sub-functions is excluded in the instructions for use;
- the *fault*-detecting measures prescribed ensure *ideal fault detection* even for the higher resolution achieved with *interpolation; or*

- the instructions for use prescribe that, in the case of *interpolation*, the *fault*-detecting measures necessary to achieve *ideal fault detection* are to be defined and ensured by the user.

8.4 *Qualitative FMEDA*

A *qualitative FMEDA* shall be performed considering all hardware components of the *Encoder(SR)*. These also include mechanical components and electrical cables needed for operation even if they are not supplied with the *Encoder(SR)* itself.

For component *faults* for which the system behaviour described in the *qualitative FMEDA* is implausible, a *fault* shall be introduced or simulated. The *Encoder(SR)*'s response to these *faults* shall be documented.

The *Encoder(SR)* shall not contain any components with possible *faults* which may lead to a *dangerous failure* that cannot be revealed by *fault*-detecting measures. These include:

- interchanging of sine and its associated cosine signals by a multiplexer or inversion (direction of motion is incorrectly detected);
- constant output voltage of sine and/or cosine simulating stoppage (see Clause L.7 for details);
- breakage of the drive shaft in rotary *Encoder(SR)* (stoppage is erroneously identified); and
- freezing of digitised analogue values for the sine and cosine.

EXAMPLE 1 An IC digitises analogue signals and converts them after digital processing back into analogue signals.

Faults in components influencing amplitude and/or phase of analogue signals shall also be considered as dangerous failure if they impede or delay fault detection as specified in the instructions for use. See also 6.3.

EXAMPLE 2 *Encoder(SR)* with capability to control amplitude and/or phase of analogue signals include appropriate components to fulfill this function. In case of a component fault within this circuit, the amplitude(s) or phase of sine and/or cosine signal(s) are incorrectly controlled. In case of a faulty analogue signal, the phasor length is maintained within the specified tolerances and fault detection applying phasor length monitoring fails or is delayed.

NOTE 1 The aspect of *faults* in components controlling amplitude and/or phase of analogue signals are especially relevant with *Encoder(SR)* with sine and cosine output signals allowing *interpolation*.

Analysis of the components shall be based on the *fault* models included and referenced in Annex G.

If category 3 or category 4 according to ISO 13849-1:2015 is claimed, it shall be shown for all functional blocks that:

- component *faults* for physical reasons cannot occur; or
- component *faults* of the mechanics can be excluded (see 6.5); or
- *single-fault tolerance* is achieved with a redundant hardware architecture (*HFT* = 1); or
- *single-fault tolerance* is achieved without a redundant architecture by means of *ideal fault detection* (see 3.34) with the *fault*-detecting measures specified in the instructions for use.

NOTE 2 Usually, *Encoder(SR)* for machinery do not comply with *HFT* = 2 or higher.

NOTE 3 The sine and cosine output signals of incremental *Encoder(SR)* cannot be considered generally redundant channels. See Annex K for details.

NOTE 4 On incremental *Encoder(SR)* with sine and cosine output signals, the monolithic integration of the position sensors and analogue circuitry for signal generation makes FMEDA virtually impossible on the transistor level. Instead, it can be assumed that every *dangerous fault* within the IC has an impact on sine and/or cosine output signal. When *ideal fault detection* is achieved, all *dangerous faults* of these ICs are detectable.

If *fault* exclusions apply, these shall be justified in accordance with the standards given in Annex G. For *SIL* 3/PL e, the application of *fault* exclusion is limited (see ISO TR 23849:2010[1], 7.2.2). However, this shall not be applied to mechanical aspects – see Table G.1 and IEC 61800-5-2:2016 (exception to Table 5 of IEC 61800-5-2:2016).

8.5 Quantification

The safety reliability of the *Encoder(SR)* shall be determined with a quantitative estimate, for example according to Annex H.

9 Test requirements

9.1 General

Clause 9 replaces IEC 61800-5-2:2016, Clause 9.

9.2 Planning of tests

The requirements of IEC 61800-5-2:2016, 9.1, shall apply with the following addition:

This document contains minimum requirements. If stricter requirements are claimed, these shall be referred to when testing. If it is not obvious which requirements are the stricter ones, conformity with both requirements shall be proven.

9.3 Functional testing

Functional testing of each *safety sub-function*, including related diagnostics (*fault* insertion testing), shall be performed. During these function tests, checks shall be performed to determine whether the properties of the *Encoder(SR)* have been achieved. Deviations from the specification and indications of an incomplete specification shall be documented.

9.4 Electromagnetic (EM) and electrical immunity testing

9.4.1 Electrical tests

9.4.1.1 Impulse voltage test

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.3.1.

Excluded are *Encoder(SR)* whose clearances are dimensioned in accordance with IEC 61800-5-1:2007, Table 9, and that are exclusively:

- supplied with voltage source(s) using *PELV circuit(s)* conforming to *DVC* A; and
- connected to *PELV circuits* conforming to *DVC* A.

If the *Encoder(SR)* contains a potential-free contact that is not itself supplied from the same voltage source as the *Encoder(SR)*, a second electrical circuit therefore exists, and the test in accordance with IEC 61800-5-1:2007, 5.2.3.1 shall be performed.

9.4.1.2 AC or DC voltage test

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.3.2.

---

[1] This document has been withdrawn.

Excluded are *Encoder(SR)* that are exclusively:

- supplied with voltage source(s) using *PELV circuit(s)* conforming to *DVC* A; and
- connected to *PELV circuits* conforming to *DVC* A.

9.4.2 Electromagnetic (EM) immunity testing

The requirements of IEC 61800-5-2:2016, 9.3, shall apply.

9.5 Thermal immunity testing

9.5.1 General

Subclause 9.5 replaces the requirements of IEC 61800-5-2:2016, 9.4.

9.5.2 Dry cold

Testing shall be performed in accordance with IEC 60068-2-1 and the following conditions:

- the test of the *Encoder(SR)* shall be performed at the lowest permissible working temperature; the minimum temperature during the test shall not exceed 5 °C ± 2 °C;
- the test of the *interface unit* shall be performed at the lowest permissible ambient temperature; the minimum temperature during the test shall not exceed 5 °C ± 2 °C;
- the stress duration shall be at least 16 h; and
- the test shall be performed with the *Encoder(SR)* not powered and not driven.

The following acceptance criteria shall be satisfied:

- for the testing of correct function, the specimen remains in the environmental chamber, the set temperature shall not be changed and the *Encoder(SR)* is powered with minimum and maximum specified operating voltage; and

  NOTE Test with maximum operating voltage is necessary due to higher currents at power on.

- the *Encoder(SR)* shall still perform its *safety sub-function*(s) according to the specification without any error indication.

9.5.3 Dry heat

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.6.3.1, and the following conditions shall be met during the test:

- the test of the *Encoder(SR)* shall be performed at the highest permissible working temperature, but at least 40 °C ± 2 °C;
- the test of the *interface unit* shall be performed at the highest permissible ambient temperature, but at least 40 °C ± 2 °C;
- the stress duration shall be at least 16 h; and
- the test shall be performed with the *Encoder(SR)* powered and not driven.

NOTE The testing of the *Encoder(SR)* in an environmental chamber calls for temperature control to the *measurement point for working temperature*.

The following acceptance criteria shall be satisfied:

- the *Encoder(SR)* and the *interface unit* shall work correctly during and after stressing; and
- the *Encoder(SR)* shall still perform its *safety sub-function*(s) according to the specification without any error indication.

9.5.4 Damp heat

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.6.3.2. Excluded are *Encoder(SR)* that are exclusively:

- supplied with voltage source(s) using *PELV circuit(s)* conforming to *DVC* A; and
- connected to *PELV circuits* conforming to *DVC* A.

The following acceptance criteria shall be satisfied:

- satisfaction of the applicable acceptance criteria of IEC 61800-5-1:2007, 5.2.6.2; and
- the *Encoder(SR)* shall still perform its *safety sub-function(s)* according to the specification without any error indication.

9.5.5 Temperature rise test

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.3.8, with the following modifications:

- thermal derating curves (e.g. regarding temperature versus speed) shall be tested at appropriate points of the curve;
- on rotary *Encoder(SR)*, the heating test shall be carried out at the maximum speed specified, to account for the thermal influence of bearing friction, etc.; and
- on rotary *Encoder(SR),* the maximum working temperature shall apply instead of "design ambient temperature".

9.6 Mechanical immunity testing

9.6.1 Clearances and creepage distances

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.2.1.

NOTE See Annex E for more information.

9.6.2 Short-circuit testing of printed wiring boards

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.2.2. If the clearances and creepage distances comply with the requirements of IEC 61800-5-1:2007, Tables 9 and 10, the short-circuit testing of the printed wiring boards is not required.

9.6.3 *Mechanical fastenings*

Testing of *mechanical fastenings* (e.g. force-locked connections by bolted joints) shall be performed as defined by Annex G. Unfavourable environmental conditions shall be considered during the testing, for example temperature conditions for fastenings with material combinations that feature different thermal expansion coefficients.

9.6.4 *Mechanical connecting elements*

Mechanical connecting elements (e.g. couplings) shall be tested according to the following procedure.

a) Determine the maximum static and dynamic loads (e.g. caused by displacements). The maximum loads shall be taken from the information for use.

   NOTE 1 For the case of a *stator coupling*, mounting tolerances or thermal expansion effects lead typically to a static load on the coupling element, whereas axial runout deviation lead to a dynamic load on the coupling element.

b) Use test equipment which applies static and dynamic loads simultaneously.

c) For rotary *Encoder(SR),* test of axial and radial loads could be done separately or in combination.

d) Test static loads with a safety factor of at least 1,0.

NOTE 2 The low safety factor 1,0 is justified by increased stress due to simultaneous application of static and dynamic loads.

e) Test dynamic loads with a safety factor of at least 1,5.

f) Select the most disadvantageous frequency or revolution speed.

g) Choose a suitable number of cycles depending on the material and safety factor.

NOTE 3 A typical procedure using the safety factor above would be to test at least 10^7 cycles for steel (body centred cubic crystal structure), and 10^8 cycles for steel (face centred cubic crystal structure) for aluminium, magnesium and copper alloy.

After the test, the following acceptance criteria shall be satisfied:

- *mechanical connecting elements* shall not have been damaged, plastically deformed, loosened or detached; and
- no damage shall occur that can influence the *safety sub-function(s)* of the *Encoder(SR)*.

An example for a suitable test of *mechanical connecting elements* is given in Annex C.

NOTE 4 The test of *mechanical connecting elements* can be done with the element alone or together with the *Encoder(SR)*.

9.6.5 Vibration and shock test

Testing shall be performed according to the requirements given in IEC 61800-5-2:2016, 9.5, except 9.5.4. If higher values are specified, they shall apply. The *Encoder(SR)* shall be powered and each *safety sub-function* shall be verified while operating.

The *Encoder(SR)*, including the possibly associated *interface unit*, shall be assembled and connected to the power supply in accordance with the assembly instructions and with reference to the requirements listed in IEC 60068-2-47.

The *Encoder(SR)* shall be mounted in accordance with its mounting instructions. The movable part of the *Encoder(SR)* shall be fixed with a fixture thus providing a constant output signal.

For *Encoder(SR)* with digital output signals, the minimum cycle time shall be chosen. For *Encoder(SR)* with analogue or square wave output signals, a sampling interval of ≤ 200 µs shall be chosen.

NOTE The sampling interval quoted here is considered sufficient for the application of *Encoder(SR)* in *safety functions*, as the time-related requirements for *safety functions* are generally less stringent than the time-related requirements for the control loop.

For vibration test, signals of *Encoder(SR)* shall be evaluated for at least one sweep (preferably the last one) in each axis.

While the *solid measure* of the *Encoder(SR)* is fixed, during each individual test the output signals shall stay within the tolerance according to the instructions for use.

After the test, the following acceptance criteria shall be satisfied:

a) electrically live parts shall not have become touchable (see 9.6.7);

b) parts shall not have loosened or become detached if the safety of the *Encoder(SR)* is impaired as a result;

c) no damage shall occur that can influence the function, safety or correct fastening; and

d) when the movable part of the *Encoder(SR)* is moved (e.g. by hand), the output signals shall be plausible.

9.6.6 Mechanical properties of integrated connecting cables

Testing shall be performed in accordance with IEC 60947-5-2:2019, Annex C.

9.6.7 Testing the non-touchability

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.2.3 and 5.2.2.4, and shall be carried out after vibration and shock testing.

For *Encoder(SR)* without housing, instead of testing, the instructions shall contain appropriate information to ensure the demanded protection class by installation at the place of use.

NOTE If *fault* exclusions regarding short-circuits on printed wiring boards are claimed, additional requirements apply. See IEC 61800-5-2:2016, Table D.1.

9.6.8 Deformation testing

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.2.5.

Excluded are built-in *Encoder(SR)* and *Encoder(SR)* that are exclusively:

- supplied with voltage source(s) using *PELV circuit(s)* conforming to *DVC* A; and
- connected to *PELV circuits* conforming to *DVC* A.

9.7 Material tests

Testing shall be performed in accordance with IEC 61800-5-1:2007, 5.2.5.

9.8 Suitability of the components and materials used

Through testing, inspection, possibly calculation and comparison with the technical documents, it shall be proven that the components and materials of the *Encoder(SR):*

- conform to the existing standards;
- are suitable for the envisaged assignment; and
- can be operated within the defined design values.

NOTE These also include the internal wiring, connection leads, the fastening of the *solid measure* (e.g. an adhesive's temperature resistance).

To assess the suitability for the envisaged *working temperature range* of the *Encoder(SR)*, the following shall be considered:

- the heating of the *Encoder(SR)* due to electrical power uptake;
- the permissible ambient temperature range of the *Encoder(SR)*; and
- heat uptake and release at the place of assembly.

On rotary *Encoder(SR)* with the coupling of the *Encoder(SR)* shaft to the drive shaft, heat uptake and release depends largely on the thermal properties of assembly. Unless thermally insulated assembly is excluded in the instructions for use, the temperature increase due to bearing friction and friction of the shaft seal shall be determined. To this end, the *Encoder(SR)* shall be assembled with the use of thermally insulating materials, and the inherent heating within the permissible speed range shall be determined.

All safety-relevant components shall be operated within the permissible temperature range. If necessary, the instructions for use shall include the limitation in terms of the speed and/or ambient temperature range.

The effectiveness of the *solid measure* and its fastening shall remain unchanged throughout the system's service life. This shall be verified by an FMEDA. To justify *fault* exclusions regarding the detachment of the *solid measure*, the factors for over-dimensioning in Annex G shall be applied.

9.9 Contamination of *solid measure*

Durability against contamination of the *solid measure* shall be proven by:

- *fault* exclusion, or
- adequate measures to uphold the safety-relevant features, or
- adequate diagnostic measures.

9.10 Labels

The contents of labels shall be inspected regarding:

- completeness (see 7.2);
- correctness;
- consistency of the details; and
- legibility of the print.

NOTE A print height of 2 mm is considered readily legible.

The durability of labels shall be proven by:

- rubbing for 15 s with a cotton cloth soaked with water; and thereafter
- rubbing for 15 s with the chemical product "n-Hexane for Analysis" according to the test liquid defined in IEC 60335-1 and IEC 62368-1.

The labels shall be readily legible after the tests.

It shall not be possible to remove label plates easily by hand nor are they permitted to become wavy or wrinkled.

9.11 Instructions

The technical documents shall be compared to the requirements and inspected regarding completeness, correctness and consistency.

9.12 Test documentation

The requirements of IEC 61800-5-2:2016, 9.6, shall apply.

10 Modification

The requirements of IEC 61800-5-2:2016, Clause 10, shall apply.

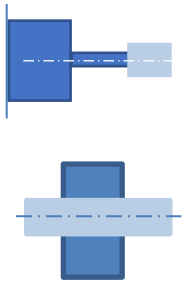
Annex A
(informative)

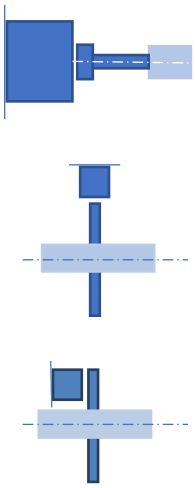
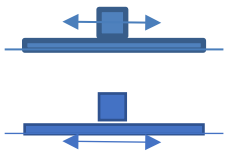
Types of *Encoder(SR)*

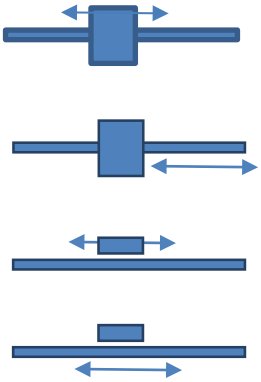
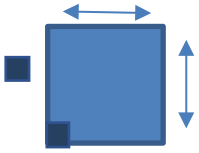
Table A.1 details the general types of *Encoder(SR)* and shows the general arrangement of different types of *Encoder(SR)*.

Light blue indicates the input shaft for the rotary *Encoder(SR)*.

Table A.1 – Types of *Encoder(SR)*

***Encoder(SR)* type**	**Description**	**Remark**
Incremental *Encoder(SR)*	*Encoder(SR)* that provides analogue or digital signal(s) proportional to the change of position of a moveable part.	There can be an additional index signal. Incremental *Encoder(SR)* generate a precisely defined number of pulses per revolution or linear measurement range.
Absolute *Encoder(SR)*	*Encoder(SR)* that provides analogue or digital signal(s) indicating the position of a moveable part.	Without further referencing, it is possible to get the absolute position over the entire measuring range. The absolute *Encoder(SR)* keeps track of its position at all times, and provides a valid output signal when power is applied.
Rotary *Encoder(SR)*	*Encoder(SR)* that generates analogue or digital output signal(s) in response to the rotary position of a moveable part.	Rotary *encoder* are also known as "rotary position transducer", "speed sensor", "shaft *encoder*" or "angle *encoder*".
Single-turn *Encoder(SR)*	Rotary *Encoder(SR)* which provides absolute position information within one revolution.	The measuring values are repeated after every complete revolution.
Multi-turn *Encoder(SR)*	Rotary *Encoder(SR)* which provides absolute position information within multiple revolutions.	
Rotary *Encoder(SR)* with integral bearing 	• *Encoder(SR)* contains bearing(s), is a self-contained unit and does not rely on the host machine for the control of rotary motion. • Input shaft can be connected to host machine via a coupling. • *Encoder(SR)* internal parts will generally be protected from the environment.	
Rotary *Encoder(SR)* without integral bearing	• *Encoder(SR)* is in two parts.	

***Encoder(SR)* type**	**Description**	**Remark**
	• Actuating element/*solid measure* is fixed to the host machine shaft and relies on the host machine bearings for control of rotary motion. • Actuating element/*solid measure* needs to be aligned relative to the sensor as part of the installation process. • Actuating element/*solid measure* can be protected or not protected from the environment and hence the *Encoder(SR)* function can be affected by solids or liquids. • Sensor internal parts will generally be protected from the environment.	
Bearingless *Encoder(SR)*	*Encoder(SR)* without its own bearing or guide	
Built-in *Encoder(SR)*	*Encoder(SR)* which fulfils the requirements concerning protection from environmental influences only when installed at its place of use.	
External *Encoder(SR)*	*Encoder(SR)* for attachment at the place of use	
Resolver(SR)	A Resolver(SR) is a type of rotary transformer used for measuring degrees of rotation.	
Linear *Encoder(SR)* without integral bearing, not protected from the environment 	• *Encoder(SR)* is in two parts, sensor and solid measure, and relies on the host machine bearings for the control of linear motion. • The sensor is either – mechanically fastened to a fixed element of the host machine and the *solid measure* is fixed to a moving element, or – fixed to a moving element and the *solid measure* is fastened to a fixed element. • *Encoder(SR)* internal parts can be protected from the environment or can be mounted in a protected area of the host machine. • *Solid measure* is aligned relative to the sensor. Generally, the solid measure is not protected from the environment and hence the *Encoder(SR)* function can be affected by solids or liquids.	

***Encoder(SR)* type**	**Description**	**Remark**
Linear *Encoder(SR)* protected from the environment 	• *Encoder(SR)* is mounted to the host machine as one unit. • The sensor and *solid measure* movement can be controlled by the host machine bearings or the *Encoder(SR)* can contain integral bearings for the control of linear motion. • The *solid measure* needs to be aligned relative to the sensor as part of the installation process. • Internal parts are protected from the environment and hence the *Encoder(SR)* function is not affected by solids or liquids.	
Linear shaft *Encoder(SR)* 	• *Encoder(SR)* is either – in one part and contains bearings to guide the movement of the sensor relative to the shaft/*solid measure*, or – in two parts and relies on the host machine bearings for the control of linear motion • Either shaft/*solid measure* or sensor is mounted to a moving part of the host machine • *Encoder(SR)* internal parts can be protected from the environment or can be mounted in a protected area of the host machine. • Generally the shaft/*solid measure* is not protected from the environment and hence the *Encoder(SR)* function can be affected by solids or liquids. • The shaft/*solid measure* can rotate.	
X-Y plate *Encoder(SR)*/ grid *Encoder(SR)* 	• *Encoder(SR)* is in three parts. • Two sensors detect simultaneous movement of the *solid measure* in two axes. • Relies on the host machine bearings for the control of linear motion. • Sensors are mounted to a fixed element of the host machine. • *Solid measure* is mounted to a moving element of the host machine.	

Annex B
(informative)

Universal architecture of *Encoder(SR)*

B.1 General

Encoder(SR) include diverse technologies and several hardware function blocks, needed to provide the *Encoder(SR)*'s *safety sub-functions*. The realisations of the *Encoder(SR)* are different, but they can always be structured according to the universal architecture. This is helpful to perform a breakdown to analyse *HFT* and category (if desired).

NOTE In this document, the universal architecture has also been used to structure the contents within some clauses and to allow easy enhancements of additional technologies etc. in the future.

B.2 The universal *Encoder(SR)* architecture

In Figure B.1, the universal architecture with its function blocks is shown.

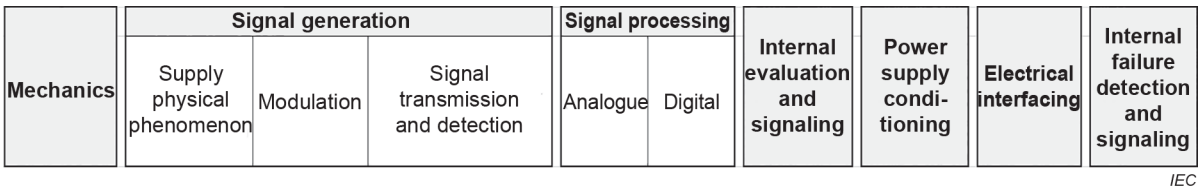


Figure B.1 – Universal *Encoder(SR)* architecture

Encoder(SR) do not necessarily include all function blocks of the universal architecture, but all hardware components of every *Encoder(SR)* can be assigned to an appropriate function block. Table B.1 gives a list of the function blocks and corresponding examples.

Table B.1 – Function blocks of the universal *Encoder(SR)* architecture

Function block	Examples
Mechanics	Flexible shaft coupling, stiff shaft coupling, *stator coupling*, fixing stator, fixing rotor, fixing *solid measure*, fixing read head, bearing, screw fitting, gluing, gearbox
Signal generation	
Supply physical phenomenon	Light, magnetic field, electromagnetic field, electrical field, electrical resistance
Modulation	*Solid measure*, code disc, gear wheel, mechanical distance
Signal transmission and detection	Fibre optic cable, light sensitive component, "magnetic conductor frame", magnetic field sensitive component, lens, coil, aperture, triangulation, measurement of transit time
Signal processing	
Analogue	Impedance converter, amplifier, linearising amplifier, analogue adder/ subtractor, amplitude controller, *DC* controller
Digital	Quadrature decoder, counter, signal converter, e. g. into rectangle, determination of position, speed, acceleration, etc., *interpolation*, ADC
Internal evaluation and signalling	Position comparator (SLP), speed comparator (SLS)
Power supply conditioning	Controller, filter
Electrical interfacing	Bus-ICs, driver, analogue/digital, connector, cable
Internal *fault* detection and signalling	Phasor length monitor, signal generation monitor, signal comparator, information comparator, temperature monitor, output signals monitor

Annex C
(informative)

Examples of suitable mechanical tests for rotary *Encoder(SR)*

C.1 General

In Annex G, suitable tests for justifying *fault* exclusions for mechanical connections are demanded. An example of appropriate tests for the justification of the *fault* exclusion for the mechanical connection between rotary *Encoder(SR)* and drive is provided here.

C.2 Mechanical fastening of the *Encoder(SR)*

C.2.1 Force-locked connection (e.g. by bolted joints)

According to Table G.1, a safety factor of $S \geq 4$ for force-locked connection shall be verified by testing.

Therefore, the connections:

- between stator of the motor and stator of the *Encoder(SR)*;
- between shaft of the motor and shaft of the rotary *Encoder(SR)*;
- between fixed part of the machine and fixed part of the *Encoder(SR)*;
- between moving part of the machine and moving part of the *Encoder(SR)*;

are statically loaded by:

- the maximum possible force; and
- the maximum possible torque including:
  i) the torque resulting from angular acceleration of the inertia (angular rotating mass) of *Encoder(SR)* rotary parts;
  ii) the bearing torque at adverse environmental conditions;
  iii) etc.;

multiplied by at least a safety factor of $S = 4$. The connections shall withstand this force/torque and no slipping shall occur.

NOTE The signal of the *Encoder(SR)* can be used to determine slipping within the interface, when *solid measure* and shaft of the *Encoder(SR)* are fixed via a mechanical short-circuit.

C.2.2 Form-locked connection (e.g. by feather key)

According to Annex G, a high safety factor against fatigue fracture (e.g. $S \geq 2$ for steel) for form-locked connection shall be verified by testing. The acceleration for the test (and the moved inertia) is thereby adjusted to correspond to the maximum possible force/torque that may occur within the application, multiplied by the respective safety factor. To determine the maximum possible force/torque, the torque resulting from maximum acceleration of the shaft inertia, the maximum bearing torque at adverse environmental conditions, etc. shall be considered. No damage shall occur that can influence the function, safety or correct fastening.

C.3 *Mechanical connecting* elements of the *Encoder(SR)* – *Stator coupling* (torque support) or *shaft-rotor coupling*

C.3.1 General

The *Encoder(SR)* is assembled in accordance with the instructions for use under additional superimposed axial and radial pre-stressing (static load) of the *mechanical connecting element*. The *mechanical connecting element* is then subjected to the number of deflections according to 9.6.4 g) (dynamic load). Depending on the geometry, the deflection of the *mechanical connecting element* is performed by lateral deflection (e.g. via hydropulser) and/or by rotation with an eccentric shaft.

For the experimental set-up, the dimensioning according to C.3.2 and C.3.3 is undertaken. Thereby, the axial and radial static pre-stressing of the *mechanical connecting element* are maintained superimposed to define the initial position from where the deflection of the *mechanical connecting element* starts. Potential eigenfrequencies of the *mechanical connecting element* shall be taken in account. No damage shall occur that can influence the function, safety or correct fastening.

C.3.2 Axial loads

C.3.2.1 Static

According to the information for use, the *Encoder(SR)* is mounted with the axial offset, the maximum permissible shaft displacement, combined with the mechanical tolerances of the *Encoder(SR)*, the machine bed and the drive shaft.

NOTE Precision gauge bands can be used for shimming to maintain the static displacement.

C.3.2.2 Dynamic

If dynamic axial displacement is permissible, the *Encoder(SR)* or the shaft, respectively, is moved with the amplitude of the mechanical tolerances and the maximum permissible displacement, multiplied by the safety factor of at least S = 1,5, according to 9.6.4.

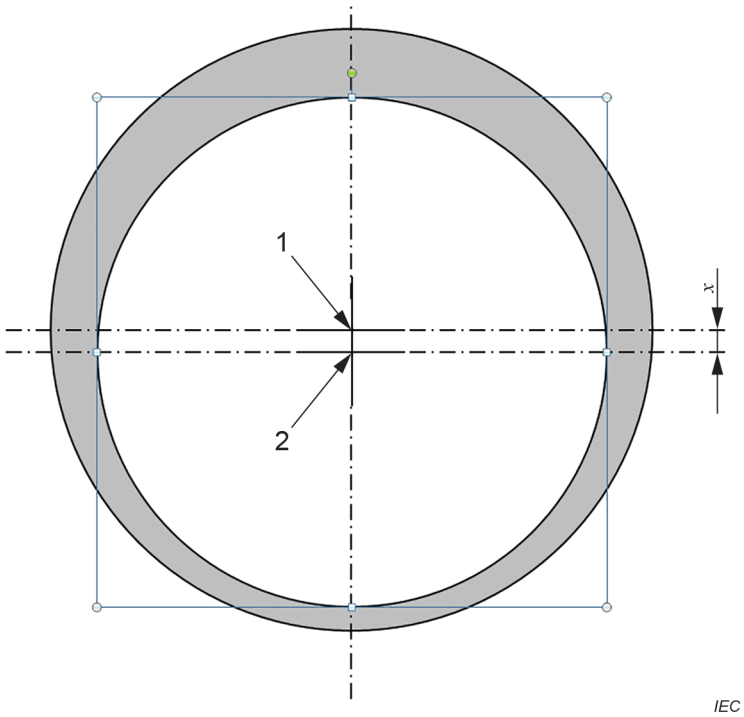
C.3.3 Radial loads

C.3.3.1 Stator coupling static/shaft-rotor coupling dynamic

The *Encoder(SR)* is assembled with the radial offset derived from the information for use on the maximum permissible radial shaft displacement. For dynamic loads (in case of *shaft-rotor coupling*), the safety factor is at least S = 1,5, according to 9.6.4.

C.3.3.2 Stator coupling dynamic/shaft-rotor coupling static

The drive shaft is provided with an additional eccentric ring (see Figure C.1). The degree of eccentricity depends on the mechanical tolerances and the maximum permissible radial shaft movement in accordance to the information for use and for dynamic loads (in case of *stator coupling*) multiplied by the safety factor of at least S = 1,5, according to 9.6.4.



Key

1 *Encoder(SR)* shaft centre

2 drive shaft centre

x eccentricity

Figure C.1 – Example of an additional ring for assembly with eccentricity x

Annex D
(informative)

Extended shock testing for rotary *Encoder(SR)* mounted to motors

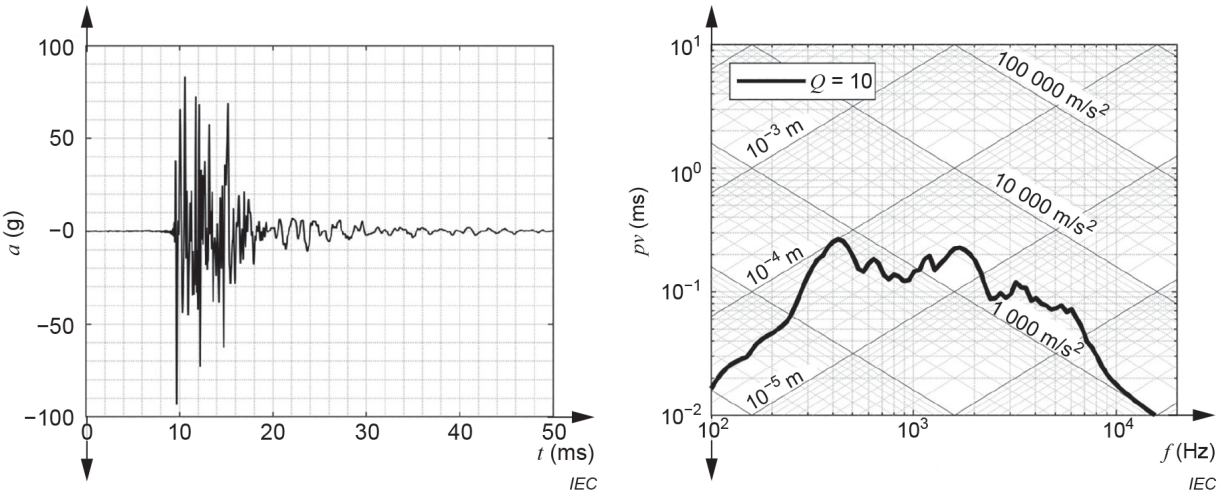
D.1 General

The engagement and disengagement of mechanical brakes (or other mechanical excitations, e.g. impacts) can cause shocks, which may damage or distort rotary *Encoder(SR)* mounted to motors. The damaging effect of these shocks typically extends over a broad frequency range and cannot be satisfactorily reproduced by testing in accordance with IEC 60068-2-27.

D.2 Pseudo-velocity shock-response spectrum (PVSRS)

A suitable method to assess the damaging effect of shocks is the pseudo-velocity shock-response spectrum (PVSRS). Figure D.1 depicts a sample shock caused by the engagement of a mechanical brake and the corresponding PVSRS on four-coordinate paper (4CP).

NOTE For detailed information regarding the PVSRS and the PVSRS on 4CP, see [9].



a) Sample shock **b) Corresponding PVSRS on 4CP**

Key

a acceleration

t time

f frequency

pv pseudo velocity

Q Q-factor

NOTE 1 Pseudo velocity indicates the severity of the shock.

NOTE 2 The Q-factor (quality factor) describes the assumed damping of the system.

Figure D.1 – Sample shock and corresponding PVSRS on 4CP

D.3 Verification of resilience

If verification of sufficient resilience against shocks caused by brakes or other mechanical excitations is desired, it is recommended

- to perform an endurance test in the foreseeable operating environment, or

- to perform a suitable test on a testing machine.

When the verification is provided by testing on a testing machine, it shall be ensured that the damaging effect of the tested shocks is at least equivalent to the damaging effect expected during operation.

The comparison of the damaging effect of shocks can be conducted by comparing the PVSRS calculated in accordance with ISO 18431-4 [10]. It is recommended to examine the frequency range from at least 100 Hz to 10 kHz, to calculate the PVSRS for a minimum of twelve frequencies per octave, and to choose a Q-factor of ten. It is only possible to compare response spectra with each other that were determined under comparable conditions (measuring point, measuring direction, etc.) and for comparable shock durations [11].

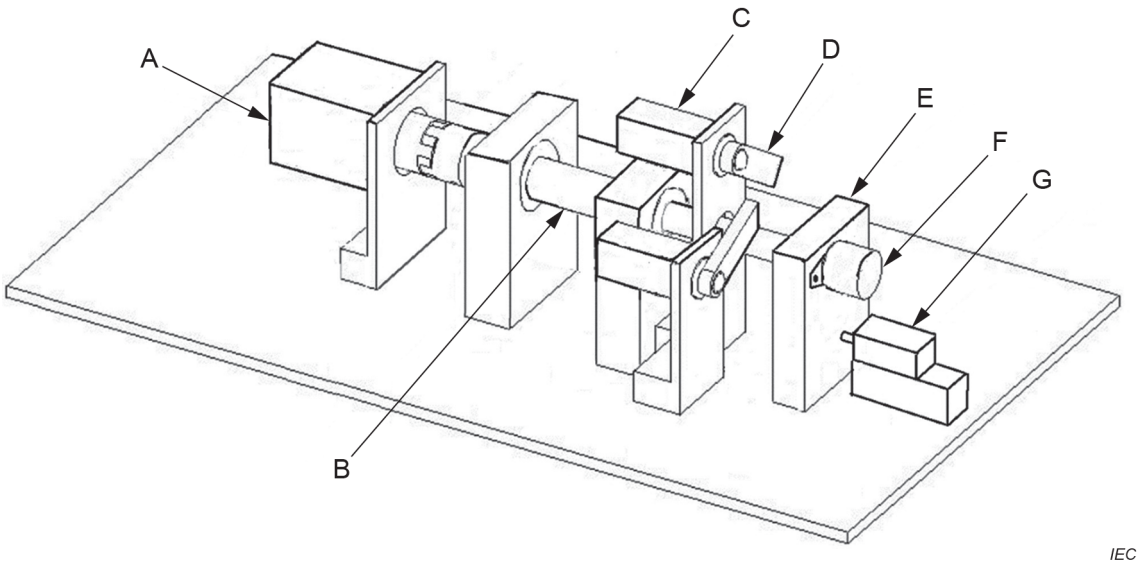
NOTE 1 For detailed information regarding the measuring techniques and shock testing machines, see [11].

NOTE 2 In order to avoid the definition of all relevant conditions in each individual case, a general definition of suitable conditions (measuring points, directions etc.) and limits for the deviation of the shock duration is currently under discussion.

D.4 Testing machine

Figure D.2 depicts a possible testing machine for verification of resilience by conducting a test on a testing machine. The testing machine is particularly suitable for simulating high frequency and multi axis shock loads as expected during use on brake motors. The testing machine enables variation of the shock load on the static as well as the rotating part of the *Encoder(SR)* virtually independently and to achieve a high rate of repetition.

NOTE The testing machine is a modification of known testing machines causing shock excitations by mechanical impact. For examples, see [11].



Key

A drive motor
B shaft of testing machine
C rotary actuator
D impactor
E stator of testing machine
F rotary *Encoder(SR)*
G linear actuator

Figure D.2 – Testing machine

The *Encoder(SR)* under test is connected to the shaft and the stator of the testing machine. During testing, the drive motor drives the shaft of the testing machine with constant speed and the signals of the *Encoder(SR)* are monitored. The shock excitation is caused by the impact of the actuators on the shaft and on the stator of the testing machine. In general, the type, position, direction and number of actuators can be chosen as necessary to achieve the desired (multi axis) shock load. In Figure D.2, two rotary actuators acting on the shaft and a further linear actuator acting on the stator of the testing machine are depicted exemplarily.

The desired shock load on the *Encoder(SR)* can be achieved in particular by modifying the following parameters:

- natural frequencies, damping and mass of the shaft and the stator of the testing machine;
- position, direction and number of actuators;
- velocity, mass and material of the impactors.

Annex E
(informative)

Dimensioning of clearances and creepage distances on printed wiring boards – Example

E.1 General

Annex E shows an example for the dimensioning of the required clearances and creepage distances on printed wiring boards according to IEC 61800-5-1:2007 and IEC 61800-5-1:2007/AMD1:2016, 4.3.

E.2 Assumptions

The following assumptions apply in this example:

- system voltage/working voltage ≤ 50 V;
- overvoltage category II;
- degree of contamination 2; and
- altitude maximum 2 000 m.

E.3 Application of IEC 61800-5-1:2007, 5.2.2.1

The application of IEC 61800-5-1:2007, 5.2.2.1, leads to the following decisions:

a) due to overvoltage category II, a system voltage of ≤ 50 V corresponds to a surge voltage of 500 V (IEC 61800-5-1:2007 and IEC 61800-5-1:2007/AMD1:2016, Table 7);

b) due to degree of contamination 2, a surge voltage of 500 V corresponds to a necessary minimum clearance of 0,1 mm (IEC 61800-5-1:2007, Table 9, with footnote a);

c) due to degree of contamination 2, a working voltage of ≤ 50 V demands a minimum creepage distance of 0,04 mm (IEC 61800-5-1:2007, Table 10);

d) the value for the calculated minimum creepage distance is increased to the value of the calculated minimum clearance; and

e) the required clearance and creepage distance are at least 0,1 mm.

NOTE The *fault* assumptions on printed wiring boards/modules with requirements in terms of *fault* exclusions are listed in IEC 61800-5-2:2016, Table D.1.

Annex F
(normative)

Information and instructions – Detailed list

F.1 Overview

The information and instructions in Annex F shall be included in the information for use as applicable.

F.2 Detailed list

a) General

company name and complete address of the manufacturer and authorised representative.

b) Information for selection

1) designation of the *Encoder(SR)* in accordance with the details on the *Encoder(SR)* itself, excluding the serial number;
2) catalogue number of the *Encoder(SR)* or equivalent;
3) general description of the *Encoder(SR);*
4) description of the intended use of the *Encoder(SR);*
5) maximum linear or rotary speed;
6) maximum linear or rotary acceleration;
7) protection class;
8) pollution degree;
9) IP rating;
10) supply voltage rating;
11) whether the *Encoder(SR)* is provided with over voltage protection;
12) requirements of the supply voltage, for example *PELV circuit(s)* conforming to *DVC* A;
13) supply current rating;
14) details of the type of conductor and of the largest and smallest conductor cross section for which the connection terminals are suitable;
15) storage temperature range;
16) *working temperature range;*
17) detail of all restrictions of the *Encoder(SR)* for its environment, altitude, limits to application and installation position;
18) for magnetic *Encoder(SR)* the maximum value for external magnetic fields to achieve criterion A and criterion FS (see 6.6.3);
19) mission time and the information that the *Encoder(SR)* shall be replaced before the smaller value of mission time and bearing service life is reached; and
20) bearing service life, including the assumed boundary conditions and the information that the *Encoder(SR)* shall be replaced before the smaller value of mission time and bearing service life is reached.

NOTE 1 Instead of providing one value for the bearing service life, a method (e.g. diagrams, excel sheet) or a service can be provided to enable the user to generate the bearing service life of the *Encoder(SR)* using the conditions of the application as input.

c) Information for installation and commissioning

1) *faults* that will invalidate the *functional safety*, for example incorrect installation, cutting and reconnecting the cable, incorrect installation of the *solid measure*, dismantling of the *Encoder(SR)*;

2) details of mounting;
3) parameters of the mechanical connecting element alignment, for example maximum loads, axial offset, shaft displacement, radial offset etc. (see 9.6.4);
4) requirements of the installation staff;
5) conditions for determination of working temperature, such as motor speed, brief temperature increase (for example due to stoppage after full-load operation), installation situation, ambient temperature, *measurement point for working temperature*;
6) connection and wiring plans;
7) earthing;
8) special requirements for cables and electrical connections;

EXAMPLE 1 Required mechanical support of a connector or required fixation of the cable at the machine bed.

9) information on commissioning/commissioning tests;
10) required adjustments and appropriate methods;
11) requirements of the configuration test of *safety sub-functions;*
12) list of special tools; and
13) for *Encoder(SR)* without or with partial housing, appropriate information to ensure the intended protection class by installation at the place of use.

d) Information for use

1) detailed description of the *safety sub-function(s)* provided by the *Encoder(SR)* including restrictions (e.g. SSV without direction information);
2) functional specification of each *safety sub-function* and interface and its respective tolerance range; it shall be described how the tolerance range shall be used to realise a safety function;

EXAMPLE 2 A linear *Encoder(SR)* providing the *safety sub-function* "safe absolute position" (SAP) with a specified *tolerance range* of 1 mm can only be used to monitor the position down to 1 mm.

3) all information necessary for the safe operation of the *Encoder(SR)*, for example:
   i) time needed by the Encoder(SR) to provide the safe output value;

   NOTE 2 For purely analogue *Encoder(SR)*, usually phase angle and/or bandwidth is provided.

   ii) fault reaction time;
   iii) safe output minimum (and maximum) cycle time; and
   iv) the maximum request rate for the host machine controller to request the position data from the digital interface;
4) *performance Level PL* and category, if compliance with ISO 13849-1 is claimed;
5) for each *safety sub-function* and interface that is available for realisation of the safety functions, the SIL capability (including systematic capability, see IEC 61508-2), which is achieved when the *Encoder(SR)* is operated in accordance with the instructions for use;
6) *PFH* with details of the associated working temperature at the measurement point; necessary is at least the statement of the *PFH* for the realistic working temperature described in Clause H.4;
7) requirements relating to signal evaluation and fault detection in the evaluation unit (see for example Annex L):
   i) defining the limits of the safe output signal(s);
   ii) defining parameters needed to process the safe output signals, for example to convert sine and cosine signals into square wave signals;

   NOTE 3 A diagram could be helpful.

   iii) requirements for diagnostic measures including a specification of recommended and/or required measures for suitable fault detection;

iv) analogue signal integrity test (for *Encoder(SR)* with analogue output signals);

NOTE 4 The achievable position accuracy depends on the selected monitoring limits for the analogue signals. If the monitoring limits are chosen wide, for example for reasons of availability, the achievable position accuracy decreases. There is a minimum requirement for a quadrant evaluation; the monitoring limits allow for the switching thresholds of the comparators.

v) in the event of a fault, the safe state of the application shall be achieved before a dangerous situation can arise; therefore, in case of an *Encoder(SR)* with HFT = 0, the sum of the maximum required time for fault detection and the time for fault response shall be shorter than the process safety time (see 3.33); the maximum required time for fault detection is the time interval at which the analogue signal integrity test is completely repeated;

vi) the hardware employed for signal evaluation and fault detection shall be fully functional over the entire anticipated frequency range of the output signals;

vii) if some faults of the *Encoder(SR)* are only detectable in certain ranges of a period of the solid measure with the prescribed analogue signal integrity test, reference shall be made to measures in the event of diagnostics performed continuously or at discrete times (see L.6.2);

viii) depending on the capability of the diagnostic measures applied, one of the following options shall be selected by the *Encoder(SR)* manufacturer:

a) exclusion of the sine and cosine signal *interpolation;*

b) limitation of the improved resolution gained by *interpolation* of the sine and cosine signal (depending on the safety function the *Encoder(SR)* is used for);

NOTE 5 Some *Encoder(SR)* allow the application in *safety functions* only based on the non-*interpolated* position value, for example because the sensitivity of the diagnostic measures is not sufficient to detect failures which have an impact on the *interpolated* position value.

ix) additional listing of all possible faults of the *Encoder(SR)* from the FMEDA or a complete definition of test signals;

NOTE 6 This information allows application-specific analogue signal integrity tests to be defined by the user (see Annex L).

8) fault states of the *Encoder(SR)* and their indication to the evaluation unit;

9) for the case of a single *Encoder(SR)* safety application and if the coupling is not provided in combination with the *Encoder(SR)*, a fault exclusion shall be required for this coupling according Table G.1;

10) warnings relating to incorrect use of the *Encoder(SR)*;

EXAMPLE 3 Use of possibly unsafe output signals for *safety functions.*

11) method for detecting interchanged sine/cosine connections; and

12) referencing procedure;

NOTE 7 This procedure is applied for setting the *Encoder(SR)* to the zero position.

e) Information for maintenance

1) requirements of tests, calibration or maintenance;

2) maintenance processes;

3) maintenance plans; and

4) repair, replacement and re-commissioning processes.

Annex G
(informative)

Encoder(SR) fault lists and *fault* exclusions

Annex D of IEC 61800-5-2:2016 applies except Table D.8, which is replaced by Table G.1 of this document and the results of the *qualitative FMEDA* (see 8.4).

NOTE 1 The list of *faults* in Table G.1 is not considered to be exhaustive.

NOTE 2 Table D.8 of IEC 61800-5-2:2016 is aimed at the use of non safety-related *encoder* with *PDS(SR)*. The general *fault* models defined in this table are not needed for the design of *Encoder(SR)* since the results of the *qualitative FMEDA* include the specific *fault* models for the respective product.

Table G.1 – *Encoder(SR)* – Mechanic *fault* list and *fault* exclusions

***Fault* considered**	***Fault* exclusion**	**Remarks**
Loss or loosening of attachment during standstill or during motion: – *Encoder(SR)* housing from motor chassis – *Encoder(SR)* shaft from motor shaft – mounting of the readhead	Preparing FMEDA and prove: – permanent fastness for form-locked connections; – fastness for force-locked connections.	The maximum permissible loading of the *Encoder(SR)* is known or limited on the *Encoder(SR)*'s data sheet. a) For form-locked connections: 1) Design for permanent fastness in accordance with generally acknowledged technical experience with a high safety factor: • verification is performed by calculation and with a suitable test; • example for steel components: over dimensioning with a safety factor $S \geq 2$ against fatigue fracture; or 2) Over dimensioning with a safety factor $S \geq 5$ against fatigue fracture: • verification is performed by calculation. b) For force-locked connections: 1) Over dimensioning with a safety factor $S \geq 4$ against slipping: • detailed measures for application and maintaining the preloading force shall be defined in the user documentation (e.g. defined pairs of materials, surfaces and torque-controlled tightening methods); • verification is performed by calculation and with a suitable test; or 2) Over dimensioning with a safety factor $S \geq 10$ against slipping: • measures for application and maintaining the preloading force shall be defined in the user documentation; • verification is performed by calculation. c) For mechanical connections that are neither form-locked nor force-locked (for example adhesive fastenings and welding), appropriate dimensioning method and safety-factors shall be chosen.
NOTE The safety factors are valid for application on static and dynamic forces.		

Table G.2 – *Faults* and *fault* exclusions for the selection, mounting and operation of rolling bearings

***Fault* under consideration**	***Fault* exclusion**	**Comment**
Spontaneous bearing blockage	Yes, if: • the rolling bearing has been dimensioned as a minimum for compliance with ISO/TS 16281 taking into account the influencing factors listed in Table G.3, and • the rolling bearing is not a solid ceramic bearing.	A blockage can occur due to: • parts of the bearing breaking as a result of impact or overload; • particles of material getting jammed or contamination between the bearing cage and the rolling element; • insufficient lubrication; • the cage or the rolling element breaking; • rivet joints rupturing on sheet steel cages; • "rusting up" when not in use.
Gradual bearing blockage	No	• If the requirement of 6.5.4 2) a) applies, the bearing may not be considered for quantification purposes; • If one of the requirements of 6.5.4 2) b), 2) c) or 2) d) applies, – 10 FIT can be applied for quantification purposes (see also Table H.1); – the fault exclusions of Table G.1 are still valid. Quantification of the bearing usually takes into account increased torque, increased temperature, increased radial runout, etc.

Table G.3 – Factors influencing the malfunctioning of rolling bearings – Considerations for selection, mounting and operation

Influencing factor	**Comment**
Fit too tight, pre-tensioning too high	Can be detected through increased heat risk or acoustics.
Fit too loose, pre-tensioning too low	Can lead to fretting corrosion and decreasing pretension.
Overload or underload	Mechanical forces.
Sliding friction	Critical at low speeds, frequent stoppages, and load or pre-tensioning too low.
Alignment faults or shaft deflection	
Impact of vibration	Can be reduced by sufficient decoupling or else "loading" the bearing, for example. Might need to be taken into account when selecting a suitable lubricant.
Speeds	Quote the maximum permissible speed in the user information.
Lubricant	Use a lubricant that is suitable for the application.
Reversing operation	Reversing operation leads to increased wear. Might need to be taken into account when selecting a suitable lubricant.
Bearing sealing	To avoid lubricant leaking out.
Over lubrication	Can lead to overheating and as a result reduced grease mission time.
Dimensioning of the bearing mounting parts	
Mounting method and use of tools	Shall proceed in accordance with the bearing manufacturer's specifications, for example to avoid the transmission of mounting forces via the rolling element.

Influencing factor	Comment
Corrosion	Ensure appropriate handling during mounting, for example de-oil the rolling bearings immediately prior to mounting in the *Encoder(SR)* and avoid hand perspiration.
Fretting corrosion	Ensure appropriate handling during mounting, for example de-oil the rolling bearings immediately prior to mounting in the *Encoder(SR)* and avoid hand perspiration. Fits that are too loose can cause "parallel rotation" of the rings and also lead to fretting corrosion.
Tilting of the bearing	As a result of the housing not being rigid enough, design *faults*, or mounting *faults*, for example.
Tilt from outer race to inner race on ball bearings	
Lack of cleanliness during mounting	
Passage of current	Rolling bearings in electric motors that are controlled by a frequency inverter in particular can be affected by passage of current or even current flashover in the bearing. The lubricant burns locally and combustion residues are left behind which significantly impair the lubricating effect; ultimately, the bearing fails.
Impact of contamination, aggressive media, and water	Can be reduced by adapting the housing design and setting rules for application.
Impact of external heat sources	
Inadequate lubrication	Can occur when restarting after a prolonged period out of operation due to problems affecting the distribution of the lubricant.
Brinell effect	Brinell effect is also known as "idle marks", "groove formation", or "dent formation" caused by vibrations or elastic deflections. These micromotions damage the smooth running surface in the bearing, resulting in louder running, wear, and failure. Only occurs at high forces.
NOTE 1 The listing in Table G.3 is not meant to be exhaustive. NOTE 2 For more details, see information provided by bearing manufacturer.	

Annex H
(informative)

Quantification

H.1 General

For a quantitative estimate of the safety-related reliability of the *Encoder(SR)* (quantification), the average frequency of a *dangerous failure* per hour (*PFH*) is calculated and its *SIL capability* is determined.

If conformity with ISO 13849-1 is claimed, the *Encoder(SR)'s* category and *performance level PL* is determined additionally.

NOTE In general, the simplified method defined by ISO 13849-1:2015 for calculating the *PFH* is usually not applicable for *Encoder(SR)* achieving *single-fault tolerance* (category 3 or category 4) with a single-channel structure with *ideal fault detection*. A single-channel structure with such high-grade diagnostics is not dealt with in ISO 13849-1:2015.

The appropriate steps in the performance of quantification comprise:

1) specifying the safety architecture and its depiction in the form of a safety-related block diagram;
2) the entering of the failure rates in the hardware contained in the safety-related block diagram (mechanics, optics, electrics, electronics, etc.);
3) adapting the failure rates under reference conditions (also called "base failure rates") to realistic service temperatures (working temperatures);
4) performing *quantitative FMEDA* per functional block including the assessment of the diagnostic measures for detecting *faults* in the *Encoder(SR);*
5) in the case of redundancy, estimating the common cause factor β;
6) estimating the *PFH* with a suitable mathematical modelling method;
7) estimating the safe failure fraction (*SFF*); and
8) determining the quantitative *SIL capability* (*SIL* upper limit).

If conformity with ISO 13849-1:2015 is claimed, the following additional steps apply:

9) estimating the $MTTF_D$ of a channel;
10) determining the quantitative category capability; and
11) determining the quantitative *PL* capability.

These steps are explained in Clauses H.2 to H.10.

H.2 Safety architecture and safety-related block diagram

To determine the *Encoder(SR)* contribution to the *safety functions* to be realised with it, its entire hardware (mechanics, optics, electronics, etc.) is subdivided into function blocks according to the universal architecture described in Annex B.

By observing the interaction of the function blocks during the execution of the *safety sub-function*, it shall be ascertained whether and at which points redundancy exists. In the case of redundancy, common cause failures shall be taken into consideration if they cannot be excluded with good reason.

For each function block, it shall be ascertained whether there are online diagnostics for it (for example automatic during operation) and which hardware (internal or external to the *Encoder(SR)*) performs these diagnostics and whether there are good reasons for excluding *faults* in the block.

The compiled information is represented in a safety-related block diagram (see [12] for more information). Functional blocks arranged logically in series can be (but do not have to be) grouped in a block. As a genuine reliability block diagram, the safety-related block diagram shows the logical links between the functional blocks and additionally lists the available diagnostics. Appropriately, all the variables required in it for quantification, such as failure rates, *diagnostic coverages* and common cause factors, can be entered and assigned to the various functional blocks.

H.3 Failure rates

The failure rates of widely used electrical, electronic and opto-electronic components can be found in recognised collections of generic failure rates, such as SN 29500 [13]. In the case of special components (e.g. ASICs), they should be stated by the component manufacturer. Soft errors shall be treated according to IEC 61508-2:2010.

For the estimation of mechanical failure rate of a component, the hierarchical procedure for finding data should be, in the order given:

a) use field data, if appropriate field experience is available (based on more than 50 % of the specified lifetime);

b) derive data from endurance testing in combination with the calculation scheme of ISO 13849-1:2015, C.4.2 "Calculation of $MTTF_D$ for components from B_{10D}";

c) use data from appropriate data bases which have been derived from similar or comparable applications (e.g. from field data, [14], or [15]);

d) set according to Table H.1;

e) set $MTTF_D$ to 150 years according to ISO 13849-1:2015, Table C.1.

NOTE $\lambda_D = 1/MTTF_D$.

Table H.1 presents information for certain components to be considered during quantification.

Table H.1 – Components for *Encoder(SR)* and their inclusion in quantification

Component	Included in quantification?	Remark
Housing	No	
Bearing, complete, possibly with seal	Yes	*For fault* exclusions, see Table G.2. 10 FIT if no other data source for the estimation is available[a] [b].
Seals between fixed parts	No	
Electronics and electrical components (e.g. mains plug)	Yes	
Stator coupling with verified fatigue strength	No	See 6.5.2 Fatigue strength justifies required *fault* exclusion.
Shaft-rotor coupling with verified fatigue strength	No	See 6.5.2 Fatigue strength justifies required *fault* exclusion.

Component	Included in quantification?	Remark
Gearing	Yes	$MTTF_D$ = 150 years if no other data source for the estimation of the $MTTF_D$ is available[c].
Fastening elements and material properties of the *Encoder(SR)* system within the *Encoder(SR)*	No	
Solid measure	Yes	This does not have to be included in quantification as long as damage or contamination (see 6.6.2) cannot result in a dangerous *failure* or *fault* exclusion applies, which is justified in accordance with ISO 13849-2:2012, Annex A. If no numeric values are available for estimating the $MTTF_D$, $MTTF_D$ = 150 years can be assumed (see ISO 13849-1:2015, Table C.1, mechanical components).
Fastening of the *solid measure*	Yes	This does not have to be included in quantification as long as *fault* exclusion is justified in accordance with ISO 13849-2:2012, Annex A.
Adhesive bonds (e.g. bonding of the *solid measure* to the shaft)	Yes	This does not have to be included in quantification as long as *fault* exclusion is justified in accordance with ISO 13849-2:2012, Annex A.

[a] All *faults* affecting the bearing component are considered to be *dangerous failures*. Therefore, a 50 %/50 % split into dangerous and safe failures is not possible.

[b] From [14], Part 02, Mechanical, Clause 6.1 Bearings, M.1.2, Bearing, Rolling on Page 42: 10 FIT for profile 1, 2, 3 (Profile 1: Cabinet mounted, 2: Mechanical field products with minimal self-heating, 3: General field products with moderate self-heating); the only failure mode is BIND (increased moment); the term BIND is used in [14] to address *bearing blockage* and confirmed by field data of *Encoder(SR)* manufacturer.

[c] If the gearing is designed on the principles of good engineering practice with the application of fundamental and proven safety principles (see [12], Annex D.2.5).

H.4 Failure rates at realistic working temperatures

The failure rates of certain components are strongly dependent on temperature. The component temperature expected in the application should therefore be taken into account in the determination of their failure rates.

For example, many rotary *Encoder(SR)* are attached close to the motor and, because of the considerable heat transmission via the shaft, are therefore regularly and systematically (so not only randomly and occasionally) operated close to their permitted upper temperature limit. Bearing and seal friction also contribute to heating up.

The failure rates and, based on them, the *PFH*s for this permissible application shall be calculated and stated, bearing in mind that the ambient temperature is not always at the upper limit value. Account is taken, for example, as follows:

$$T_{\text{PFH}} = T_{\text{work}} + T_{\text{delta}} - 15\ \text{K}$$

where

T_{delta} is the temperature difference between working temperature and the maximum occurring component temperature.

NOTE 1 A deduction of 15 K takes account of the fact that *Encoder(SR)* are not continuously operated at the maximum permitted temperature.

Alternatively, the effect of realistic working temperatures can be assessed in a more detailed manner by applying stress profile factor π_W calculated according to SN 29500 (see [13]).

PFH values can be additionally calculated and stated for lower operating temperatures.

Failure rates under reference conditions can be converted into failure rates at other (usually higher) temperatures by multiplying the rates with a temperature correction factor π_T. Suitable equations for these component-specific correction factors are given in IEC 61709 [16].

NOTE 2 The SN 29500 [13] collection of failure rates adopts the correction factors from IEC 61709 [16].

H.5 *Quantitative FMEDA* and assessment of diagnostic measures

For each of the function blocks listed in the safety-related block diagram, *quantitative FMEDA* is used for determining the failure rates in the dangerous direction λ_D and from this the share λ_{DD} identifiable through diagnostics.

NOTE 1 In the case of redundant function blocks, the failure of a block does not result in the loss of the *safety function*. In this case, λ_D designates the rate of block failure in the unsafe direction (loss of envisaged block function).

In order to firstly only determine the failure rate of a function block, the parts count method can be adopted in the simplest case which consists of adding the failure rates of all components of the block. The following holds:

$$\lambda_D = \sum_i \lambda_i$$

where

λ_i represents the failure rates of the various components of the block.

By performing the more detailed *quantitative FMEDA*, it is nevertheless possible to calculate a more favourable (lower) block failure rate in the dangerous direction λ_D. The precondition for the classification of a certain failure as dangerous (D) or safe (S) is that the *safety function* and thus the *dangerous failure* direction of the functional block is known because otherwise it is impossible to judge whether the *safety function* is impaired (D) or not (S) by the failure. On an universal *Encoder(SR)* that is to be used for various unknown *safety functions*, only certain types of failures can be classified with certainty as safe (S). A global assessment of half the component failure rate as "S" is therefore not appropriate. Nevertheless, the following contributions can be removed by *quantitative FMEDA* from the summated failure rate for λ_D:

- failure rates of components that are neither directly nor indirectly involved in the execution of the *safety sub-function* (no part failures);
- failure rates of components whose failure has no effect on the execution of the *safety sub-function* (no-effect failures); and
- rates for certain component failure directions whose occurrence has no effect on the execution of the *safety sub-function* (no-effect failures).

  NOTE 2 The following can be referred to for an estimate of this share:

  – IEC 61709;

  – failure type distribution stored in FMEDA tools.

An unnecessary change of source for the failure type distribution from component to component is not permissible.

If *ideal fault detection* is required in single-channel part(s) of the *Encoder(SR)*, failures in the dangerous direction shall be detected in their entirety in order to satisfy the criterion of *single-fault tolerance*. Therefore, there shall be no *dangerous failure*, which is not detectable. In a conservative estimate, for example an estimation on the safe side, *DC* = 99 % is set for the *PFH* calculation.

In redundant parts of the *Encoder(SR)*, the *diagnostic coverage* for each failure in the dangerous direction shall be individually estimated. Guidance for the estimate is provided by the tables in IEC 61508-2:2010, Annex A, and ISO 13849-1:2015, Annex E. For the single *dangerous failure* of a component i from a functional block, the *dangerous failure* rate is thus divided into the detectable share

$$\lambda_{i\,\mathrm{DD}} = DC_i \cdot \lambda_{i\,\mathrm{D}}$$

and the undetectable share

$$\lambda_{i\,\mathrm{DU}} = \left(1 - DC_i\right) \cdot \lambda_{i\,\mathrm{D}} .$$

For a functional block (FB) or logical arrangement of functional blocks in series, a mean *diagnostic coverage* is yielded by the following formula:

$$DC_{\mathrm{FB}} = \frac{\sum_i \lambda_{i\,\mathrm{DD}}}{\sum_i \lambda_{i\,\mathrm{D}}}$$

NOTE 3 An example of a *quantitative FMEDA* is presented in [12].

H.6 Estimation of the common cause factor *β* (only in case of redundancy)

Suitable for this is the method in IEC 61508-6:2010, Annex D, or a justified estimate. If compliance with ISO 13849-1 is claimed, the use of ISO 13849-1:2015, Annex F, is applicable alternatively.

NOTE The method in ISO 13849-1:2015 only permits the justification of the estimate with a common cause factor of 2 %. The detailed method in IEC 61508-6 is capable of yielding other values for the common cause factor as well.

H.7 Estimation of the *PFH*

Depending on the hardware architecture and the input variables that shall be taken into account, a suitable calculation method for estimating the *PFH* is selected. As input variables, this method uses the functional-block-related failure rates and *diagnostic coverages* calculated with functional-block-related *quantitative FMEDA*. In the event of redundancy, the common cause factor β is also used.

H.8 *Safe failure fraction* (*SFF*)

To verify the maximum quantitative *SIL capability* (*SIL* upper limit) (see Clause H.9) in accordance with IEC 61800-5-2, the *safe failure fraction* (*SFF*) shall be estimated first. If the architecture consists of subsystems with a different *HFT*, this shall be performed separately for each subsystem.

The *SFF* is calculated with the following formula:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D}$$

NOTE 1 The "no part and no-effect failure" rates are not included in the calculation of the *SFF*.

NOTE 2 Calculation of the *SFF* can sometimes be avoided (see Clause H.9).

H.9 Determination of the quantitative *SIL capability*

H.9.1 General

According to IEC 61800-5-2:2016, there are two quantitative issues, which impose a limitation on the *SIL* achievable by a *safety function* employing an *Encoder(SR)*: the architectural constraints and the *PFH*.

H.9.2 *SIL* limit by architectural constraints

The *SIL* limit by architectural constraints refers to subsystems performing *safety functions*.

A subsystem is characterised by:

- a uniform *hardware fault tolerance* (*HFT*);
- a type (A or B, see IEC 61800-5-2:2016, 6.2.3.2.2 and 6.2.3.2.3); and
- a *safe failure fraction* (*SFF*, see Clause H.8).

The *Encoder(SR)* may for example be part of a subsystem (for example device with sine and cosine output signals, which needs external diagnostics) or may incorporate one or more subsystems (for example device containing its necessary diagnostics completely). In any case, according to IEC 61800-5-2, each subsystem, containing the *Encoder(SR)* as an element or being part of the *Encoder(SR),* shall be examined for the maximum *SIL* relating to the architectural constraints.

The procedure of determining the *SIL* limit makes use of the three above-mentioned properties of the subsystem (*HFT*, type, *SFF*) and is described in IEC 61800-5-2:2016, 6.2.3.

Usually, the *safe failure fraction* (*SFF*) is calculated from the results of the *quantitative FMEDA* (see Clause H.5). However, the calculation of the *safe failure fraction* (*SFF*) and thus the determination of λ_S may be avoided, if a sufficiently high *diagnostic coverage* (*DC*) has already been ascertained. In this case, the inequality

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} \geq \frac{\sum \lambda_{DD}}{\sum \lambda_D} = DC$$

allows the use of *DC* as a lower bound of *SFF*.

H.9.3 *SIL* limit by *PFH*

Typically, an *Encoder(SR)* will not provide a complete *safety function* but will contribute to a *safety sub-function* (see IEC 61800-5-2:2016, 4.2). In the broadest sense, the *safety sub-function* provides safe information necessary to execute the *safety function*. Since *PFH* always relates to a function, for the *Encoder(SR)* a *PFH* value can only be meaningfully assigned to the *safety sub-function* the *Encoder(SR)* provides.

From the hardware view, the *Encoder(SR)* either forms an element of a subsystem (device with sine and cosine output signals, which needs external diagnostics) or may consist of one or more subsystems (device containing its necessary diagnostics completely). In any case, the *PFH* of the functional unit, carrying out the *safety sub-function* of providing safe information, shall be determined. The diagnostics implemented for this functional unit is taken into account by the *PFH* calculation.

The *PFH* of the *safety sub-function* providing safe information acquired by the *Encoder(SR)* represents only one *PFH* contribution of the complete *safety function*. Accordingly, the *PFH* of the *safety sub-function* should not exceed a particular fraction of upper *PFH* limit of the intended *SIL* of the complete *safety function*. The correlation between *PFH* and *SIL* is stated in Table 3 of IEC 61800-5-2:2016. Ultimately, the *PFH* of the *safety sub-function* also limits the *SIL*, which can in practice be achieved for *safety function*s employing the *Encoder(SR)*.

NOTE A third, qualitatively founded, limitation of the achievable *SIL* is constituted by the systematic capability, expressed by the maximum *SIL* that can by claimed due to the degree of robustness with respect to systematic failures (see IEC 61508-2). The overall *SIL capability* is constituted by the lowest of these three limits: the architectural constraints *SIL* limit, the *PFH SIL* limit, and the systematic capability.

H.10 Additional considerations to comply with ISO 13849-1

H.10.1 General

If conformity with ISO 13849-1:2015 is claimed, Clause H.10 applies.

H.10.2 $MTTF_D$ of a channel

For the assignment of a category according to ISO 13849-1 (see H.10.3), the $MTTF_D$ of one channel shall be considered. For its calculation, the channel(s) is/are identified in the safety-related block diagram that execute(s) the *safety function*. Parts indirectly involved in execution of the function (e.g. circuitry for voltage control) shall also be included. Parts used solely for diagnostic purposes can only be excluded if those are free of interference regarding the *safety sub-function*. In the event of redundant channels, the channel with the bigger (worse) failure rate shall be selected. The outcome is the failure rate of one channel in the dangerous direction $\lambda_{OC\,D}$ ("OC" does express "one channel"). For the $MTTF_D$ of a channel, the following then holds:

$$MTTF_D = \frac{1}{\lambda_{OC\,D}}$$

H.10.3 Determination of the quantitative category capability

The eligible categories 3 and 4 in accordance with ISO 13849-1:2015 impose requirements on the $MTTF_D$ and DC_{avg} of the function channel (or possibly channels). To calculate the $MTTF_D$ and DC_{avg}, the data obtained from *quantitative FMEDA* (see Clause H.5) can be used.

NOTE The requirements imposed by the various categories on $MTTF_D$ and DC_{avg} can be found in ISO 13849-1:2015, 6.2.

H.10.4 Determination of the quantitative *PL*-capability

ISO 13849-1:2015, Table 2, defines the *PL*-dependent upper limits for the *PFH* of *safety functions*. This means that the *PFH* of the *Encoder(SR)* sets an upper limit for the *PL* within which the *Encoder(SR)* can be used.

Annex I
(informative)

Digital processing of sine/cosine signals

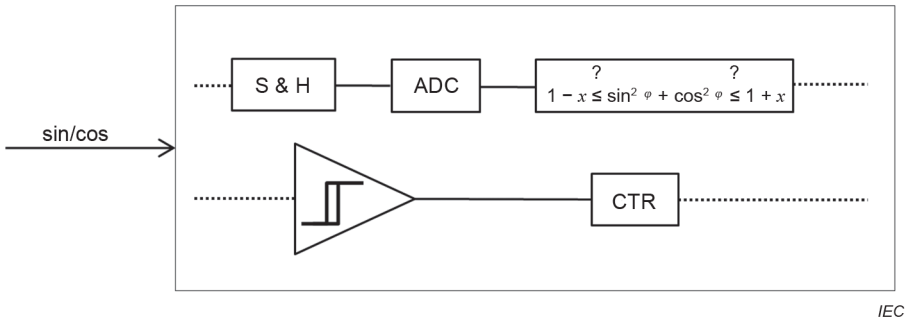
I.1 General

When the output signals of an *Encoder(SR)* with sine and cosine output signals are processed in digital technique (hardware or software), sampling of the signals and converting into digital values applies in the *evaluation unit*. Annex I describes effects of this method with possible impacts on measurement and *fault* detection.

NOTE The effects addressed in this Annex I can also occur in other types of *Encoder(SR)* which perform digital signal processing within the *Encoder(SR)* itself.

I.2 Sampling of sine and cosine signals

The effect on sampling is explained on a specific example. In Figure I.1, the hardware architecture is shown.



Key

sin/cos one pair of sine and cosine output signals from *Encoder(SR)*

S&H sample and hold

ADC analog to digital converter

CTR counter for the incremental pulses

Figure I.1 – Digital sampling of sine and cosine signals – Hardware architecture, example

A safe *evaluation unit* is applied for sample and hold, analogue to digital converting, *fault* detection applying phasor length monitoring, slope detection and slope counting. In Figure I.2, the Lissajous figure of the sine and cosine signals A and B is shown with 4 samples/period at S1, S2, S3 and S4. The slopes out of A and B are generated by a Schmitt trigger with switching levels A_{on}/A_{off} and B_{on}/B_{off}. For position measurement, the slopes of A and B are counted. The diagnostic measures in this example apply the verification of the phasor length

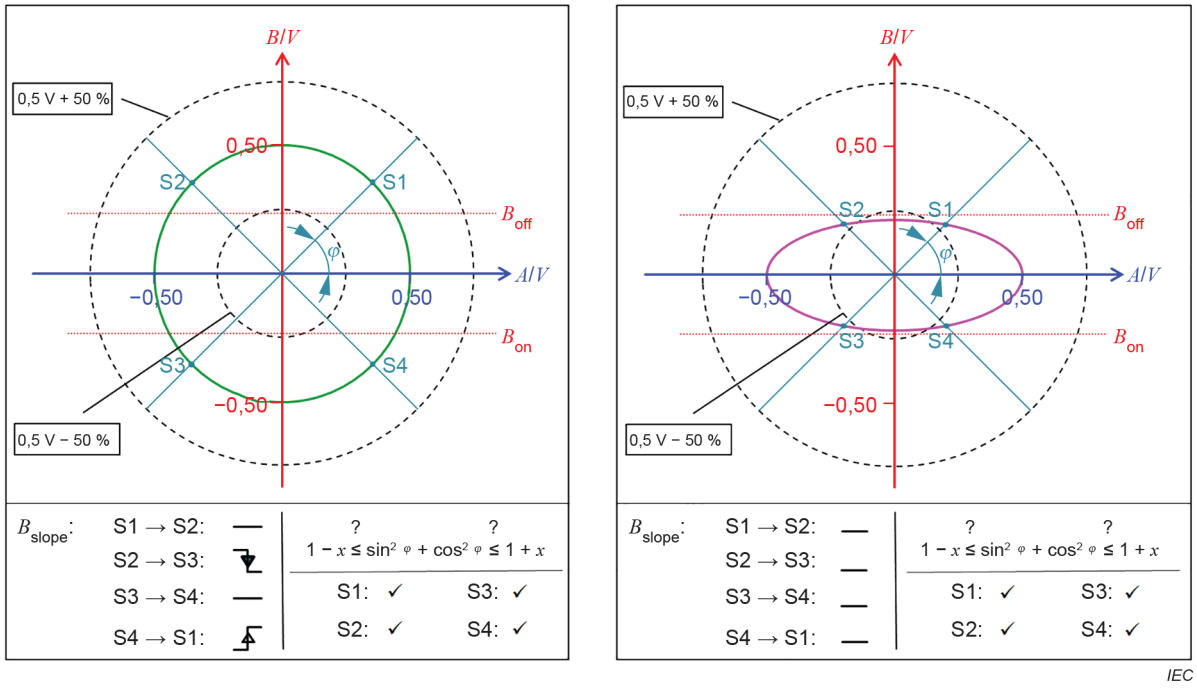
$$1 - x \overset{?}{\leq} sin^2\varphi + cos^2\varphi \overset{?}{\leq} 1 + x$$

on each sample. Figure I.2 a) illustrates a no-*fault* condition with 4 samples per period and sampling at 45°, 135°, 225° and 315°. The Schmitt trigger is working well and the phasor length monitoring is ok.

In Figure I.2 b), the amplitude of signal B is defective, too low, but the detection fails:

- the Schmitt trigger does not identify slopes on signal B, since the amplitude of signal B stays within the hysteresis B_{on}/B_{off};
- the phasor length is ok on the sampling points, so there is no detection of the *dangerous failure*; and
- the *evaluation unit* detects standstill, while the machine part is moving.

NOTE When *interpolation* of the sine and cosine signal is applied, the detection of the position within a period is faulty.



a) No *fault* **b) Signal *B* too low, detection fails**

Key

A	differential sine signal (volt)
B	differential cosine signal (volt)
B_{on}, B_{off}	switching thresholds of Schmitt trigger of B
B_{Slope}	slope signal out of B
φ	position value (continuous)
S1, S2, S3, S4	sampling points in Lissajous figure

Figure I.2 – Lissajous figures of the sine and cosine signals A and B

I.3 Consequences

This example shows that diagnostic measures can fail due to certain timing conditions. In this example, the sampling points are assumed to be at 45°, 135°, 225° and 315°, but this will not be constant, since there is no synchronization. With changing phase angle, the *fault* can be detected. The number of periods the *fault* can stay undetected is application-specific. It depends on:

- number of samplings per sine/cosine period (should be high);
- rotational speed/speed;
- hysteresis (should be low); and

- allowed tolerances of phasor length (should be low).

NOTE Low hysteresis and low tolerances of the phasor length monitoring improves diagnostics but can degrade availability, since signal disturbances could be interpreted as *faults*.

I.4 Measures to improve *DC*

A combination of suitable measures is recommended to avoid the diagnostic measures to fail due to sampling. The following, not exhaustive list includes some suitable measures:

- the limits for slope detection fit to the allowed tolerances for the phasor length monitoring, so a failure of sine/cosine is detected before the counting fails;
- the manufacturer of the *Encoder(SR)* defines a minimum sampling rate; a minimum sampling rate of 6 samples/period is recommended; the possible change of the phase angle between sine and cosine signals should also be considered;
- the manufacturer of the *evaluation unit* defines a maximum number of sine/cosine periods needed to detect a failure of the *Encoder(SR)*;

  NOTE 1 This can have an impact on safety margins to be considered in *safety functions* of the application.

- when the behavior of the control loop is applied for *fault* detection, the application of the *Encoder(SR)* for monitoring purposes may be excluded; and

  NOTE 2 A control loop of a *PDS(SR)* applying an *Encoder(SR)* can operate temporarily sensorless as well, neglecting the *Encoder(SR)'s* signals for some time and therefore not contributing to *fault* detection.

- use only analogue *signal evaluation* with sufficient samples per period and forgo the comparators and their hysteresis thresholds to generate binary signals from the analogue signal *B*; regarding the example in Clause I.2, with this measure the movement would still be correctly evaluated and within a short time the signal degradation at signal B would be detected by an additional amplitude monitoring.

Annex J
(informative)

Single channel architecture with *ideal fault detection*

J.1 General

Most *Encoder(SR)* fulfil *SIL* 2 or 3 according to IEC standards and additionally *PL* d or e and category 3 or 4 according to ISO 13849-1. The requirements of these standards are similar but they are not identical. One important difference is the required *HFT*. ISO 13849-1 requires, for categories 3 and 4, that a single fault does not lead to a loss of the safety function, which is in most cases realised with redundant hardware architectures, while IEC standards allow *HFT* = 0 up to *SIL* 3, depending on the *SFF*. To design single channel *Encoder(SR)* providing *single-fault tolerance*, the concept "*ideal fault detection*" is applied.

J.2 *Ideal fault detection* for *Encoder(SR)* with sine and cosine output signals

The term *ideal fault detection* describes an exceptional property of *Encoder(SR)* with sine and cosine output signals which enables single-channel architectures to comply with the requirement of *single-fault tolerance* according to ISO 13849-1.

ISO 13849-1 defines several categories, one of which shall be accomplished by any safety-related subsystem. These definitions describe a system behaviour regarding component failures specific for the respective category.

NOTE 1 It is important to recognize that the definitions of category 3 and category 4 do not specify a specific hardware architecture but the safety relevant behaviour only.

For *Encoder(SR),* the categories 3 and 4 (ISO 13849-1:2015, 6.2.6 and 6.2.7) are the most relevant categories. One main requirement of these categories is that a single fault does not lead to a loss of the safety function. This requirement is usually fulfilled by a safety architecture including two independent channels. However, *Encoder(SR)* with sine and cosine output signals in most cases include single channel bottlenecks without any *fault* exclusion possible like a common opto-ASIC for sine and cosine signal generation. Additionally, the *evaluation units* usually are processing the sine and cosine signal in combination, for example due to the application of quadrature decoder ICs or because the direction of movement has to be detected in order to perform the *safety function*. Therefore, these *Encoder(SR)* provide a single channel architecture.

Nevertheless, due to the analogue nature of sine and cosine signals, and their corresponding extraordinary capability of diagnostic measures to detect faults, single channel *Encoder(SR)* may fulfil the *single-fault tolerance* requirement applying *fault* detection and response in *process safety time*:

- all *dangerous faults* can be detected; and
- a suitable *fault* response is initiated quick enough after occurrence of a *dangerous failure* to prevent a hazardous event from occurring.

Since no particular *safety function* is specified for an *Encoder(SR)* for universal safety-related use, any *fault* that can corrupt the number of periods detected by the subsequent *signal processing* unit shall be rated as a *dangerous fault*. This applies to the sine as well as to the cosine signal.

The detection of ALL *dangerous faults* is quite challenging, especially a short-circuit or a break within an IC can change the circuit design and therefore its functionality. Nevertheless, all *dangerous faults* do have an impact on the sine and/or cosine signal(s) whatever the *fault* within the *Encoder(SR)*'s hardware is. This can be detected, for example, by phasor length monitoring with appropriate tolerances. The suitability of diagnostic measures can be proven by means of the so-called "static analysis" (see Annex L).

The method "static analysis" does not consider any timing issues of the implementation and application. Therefore, the time aspect shall be considered separately. See also Annex L.

NOTE 2 Since *ideal fault detection* means applying *fault* detection and response in the *process safety time* for any dangerous failure which cannot be excluded, a single *fault* of the *Encoder(SR)* with sine and cosine output signals cannot adversely affect the safe behaviour of the system. Therefore, according to the rules for the attainment of systematic capability of IEC 61508-2:2010, 7.4.3, the systematic capability of the *Encoder(SR)* with sine and cosine output signals can reduce the intended *SIL* of the *safety function* by one *SIL* step.

Annex K
(informative)

Specifics for single channel incremental *Encoder(SR)* with sine and cosine output signals

K.1 General

Annex K gives specific information for incremental *Encoder(SR)* claiming category 3 or category 4 according to ISO 13849-1 and including single channel architectures in at least one function block. These *Encoder(SR)* require *ideal fault detection* to provide *single-fault tolerance*.

K.2 *Single-fault tolerance*

Most *safety functions* require the reliable detection of the direction of motion. Both the sine and cosine signals are needed for this. If one of the signals is faulty, the correct identification of the direction of motion can no longer be assured. Therefore, the signal paths for the sine and cosine signals do not offer any redundancy for the identification of the direction of motion. The same applies when, in a *safety function*, *interpolation* takes place with the use of sine and cosine signals. *Single-fault tolerance* is nevertheless achieved as long as *ideal fault detection* (see Annex J) applies.

Encoder(SR) that may be used solely for direction-independent linear or rotary speed monitoring can be considered dual-channel if the *Encoder(SR)'s* hardware is suitably configured. In this case, the *evaluation unit* shall process the two channels independently. See also 6.4.1.

Sine/cosine signals are often processed by *Encoder(SR)* with the use of a single analogue or mixed-signal ASIC. The analogue signals are not digitised. Due to the shape of the sine and cosine signal with the associated phase angle, random *faults* of parts of the circuitry resulting in a dangerous, undetectable *fault* are not likely to occur. For these ASICs, *single-fault tolerance* can therefore be assumed if *ideal fault detection* is achieved. As a result of *ideal fault detection*, a *fault* accumulation cannot in principle arise. Taking a conservative approach, the achievable category is limited to category 3 when just one ASIC is used without on-chip redundancy according to IEC 61508-2:2010, Annex E.

K.3 Undetectable *faults*

Faults can be detected both within the *Encoder(SR)* and in the *evaluation unit*. If *ideal fault detection* is required, there shall be no scope for undetectable *faults* in the *Encoder(SR)*.

The *fault*-detecting measures in the *evaluation unit* are solely possible based on the output signals. Unless suitable internal measures are available, there shall be no scope for *faults* in the *Encoder(SR)* that are not detectable with it (see Clause L.7). Examples include the interchanging of sine and cosine by multiplexers, signal inversion and the breakage of the drive shaft of rotary *Encoder(SR)*.

K.4 *Fault* detection (*DC*)

To achieve the required *ideal fault detection*, the *fault*-detecting measures and switching thresholds for quadrant detection should be perfectly balanced. Otherwise, it is possible, for example, for the amplitude of the sine or cosine signal to change such that this *fault* is not (yet) detected by diagnostic measures but the detection of motion is faulty owing to unfavourable switching thresholds in the *evaluation unit*.

On incremental *Encoder(SR)* with sine and cosine output signals, the monolithic integration of the position sensors and analogue circuitry for signal generation makes FMEDA virtually impossible on the transistor level. Nevertheless, the evaluation of *signal evaluation* and diagnostic measures is possible in applying the method "static analysis of signal output and *fault* detection". The output signals of the *Encoder(SR)* are simulated and replaced by a series of test signals representing the assumed *faults* in the *Encoder(SR)* (see Figure L.1).

Because of the required *single-fault tolerance* and the single channel, the static analysis shall prove that all *faults* are detected by the available diagnostic measures.

In a conservative classification for components, a *DC* of 99 % shall be assumed for quantification although all *faults* are detected.

For the performance of static analysis, it is irrelevant whether *fault* detection takes place within the *Encoder(SR)* and/or in the *evaluation unit*. For *Encoder(SR)* that have no or insufficient internal measures for *fault* detection, *fault*-detecting measures by the *evaluation unit* can be prescribed. These measures shall be described in the instructions for use.

The static analysis method is described in greater detail in Annex L.

NOTE There is a tool available which supports performing the static analysis, see [17].

When diagnostic measures to be performed by the *evaluation unit* are necessary, dynamic behaviour can only be accounted for by the user. It should be ensured that the hardware employed for *signal evaluation* and *fault* detection operates *fault*-free over the entire expected frequency range of the *Encoder(SR)*'s output signals.

Annex L
(normative)

Static analysis of *signal evaluation* and *fault* detection

L.1 General

Annex L refers to *Encoder(SR)* with analogue sine and cosine output signals claiming *ideal fault detection* that are envisaged for *safety functions* although these *Encoder(SR)* do not contribute to any diagnostics or contain any fully integrated diagnostics. The information for use of such *Encoder(SR)* shall enable the user to perform the required diagnostics externally. Static analysis involves the validation of the requirements contained in the information for use relating to the processing of the *Encoder(SR)* output signals to be performed externally. *Signal processing* comprises the evaluation of the output signals for the purpose of performing the *safety function(s)* and the integrity test of the output signals for the identification of *faults* in the *Encoder(SR)* (diagnostics).

NOTE 1 Static analysis can also be used as an aid in the design of safe *evaluation unit*s or safe controls with inputs for *Encoder(SR)* with sine and cosine output signals.

NOTE 2 The static analysis method is described in Annex L. The method is independent of possible implementation in a software tool. However, it can aid comprehension if reference is made additionally to the graphic depictions of the tool mentioned in Clause L.9.

L.2 Motivation for the analysis of *signal evaluation* and *fault* detection

In the evaluation of signal slopes for the performance of the *safety sub-function*, hardware *faults* can cause the non-detection of slopes and hence the failure of the *safety function*. An integrity test of the analogue signals shall identify these *faults*. Whether the identification of certain *faults* is possible depends on the specific qualitative and quantitative design of both slope detection (square-wave formation) and the analogue signal test (e.g. phasor-length monitoring).

The purpose of static analysis described here is to check whether ALL the realistically assumed *faults* can be detected and to verify that this is the case. This is a precondition for satisfying the criterion of *single-fault tolerance* (needed to comply with categories 3 or 4 in accordance with ISO 13849-1) with the given single-channel architecture.

To facilitate the correct use of the *Encoder(SR)*, the manufacturer shall suggest to the user one or more combinations of switching thresholds for square-wave formation and an associated analogue signal test in each case. These combinations shall stand up to scrutiny by static analysis described here.

However, the user can design evaluation and *fault* detection on his own responsibility and deviate from the suggestions of the *Encoder(SR)* manufacturer. In this case as well, the combination of switching thresholds for square-wave formation and analogue signal testing shall stand up to static analysis.

For his design of diagnostics, the manufacturer shall inform the user of special *fault* patterns (signal voltages) that shall be identified by diagnostics. This information can be communicated with the aid of the tool for performing static analysis (see Clause L.7 and Clause L.9).

L.3 What does "static analysis of *signal processing*" mean?

The term "static analysis" is taken from the field of software testing. Here, as there, "static" means that no physical measurements of quantities changing over time are performed on a running system, but that the matter is considered from a theoretical point of view.

In the present case, static analysis is concerned with the quantitative specification of the switching thresholds for square-wave formation and with the qualitative and quantitative specification of the integrity test for the analogue signals that shall be suitably coordinated to detect all possible *faults*.

In electronic circuits, the classical way of verifying the achieved *diagnostic coverage* calls for the performance of an FMEDA on the component and circuit level. In the case of incremental *Encoder(SR)* with sine and cosine output signals, however, the monolithic integration of the sensors for scanning the *solid measure* and parts of the analogue circuitry for signal generation make an FMEDA on the transistor level virtually impossible solely because no cross-connections between various points of the circuitry can be excluded. Nevertheless, it is important to assess whether the details to be specified by the manufacturer on the processing of the output signals are appropriate.

The required specification by the manufacturer of the *Encoder(SR)* shall contain:

- the switching thresholds for square-wave generation ("Schmitt trigger" in the hardware or software), and
- the test method for the analogue signals for *fault* detection (diagnostics).

To test this specification, analogue *signal processing* as per specification is simulated. The correct output signals are replaced by a series of test signals that amount to substitute signals for potential *faults* of the *Encoder(SR)*. The *signal processing* as per specification shall respond to these test signals in a safe manner and "master" them. This means:

- analogue signals whose change over time represent a position change shall, according to the specification, be converted into countable pulses, including information on the direction of counting; or
- the diagnostics shall issue a *fault* signal (by means of which the application initiates a safe state).

The procedure for static analysis is depicted in Figure L.1:

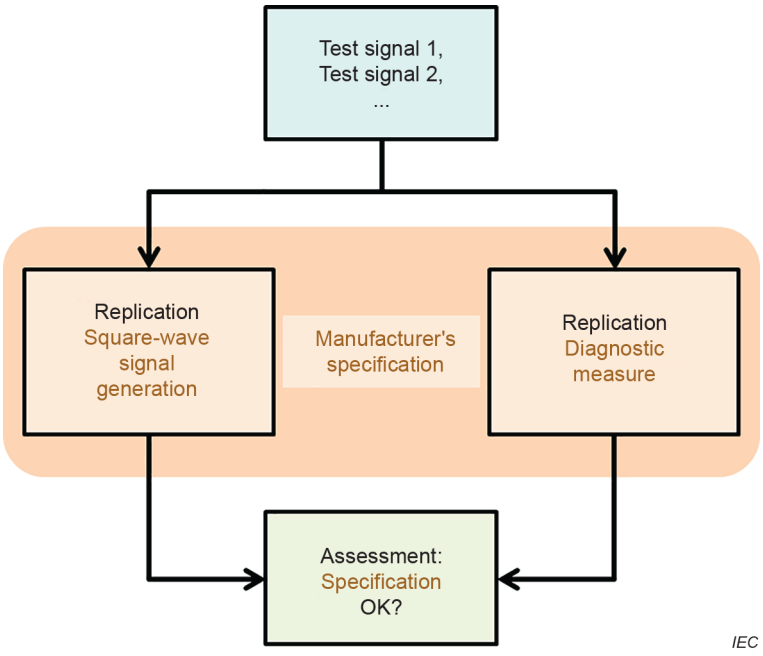


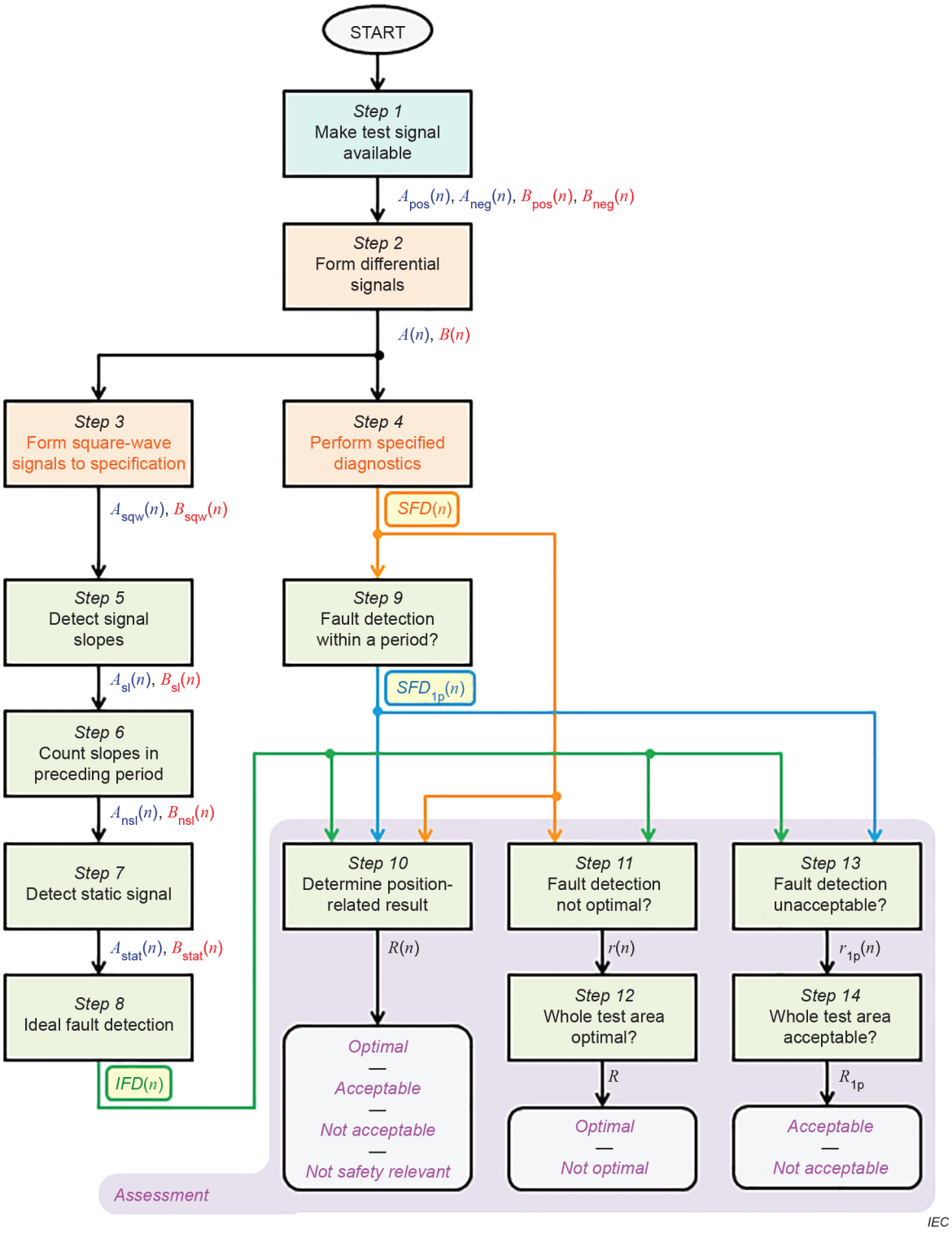
Figure L.1 – Static analysis concept

It is assumed that a specification of switching thresholds and diagnostics that masters the substitute signals also masters the hardware *faults* that arise in reality. To make this possible, a certain diversity and variance of the substitute signals is provided.

NOTE "Dynamic effects" (overcounting due to interference pulses) are not investigated by static analysis.

The test signals are described in Clause L.4, the simulation of *signal processing* in Clause L.5 and the assessment of the specification in Clause L.6.

Figure L.2 presents an overview of the various steps of static analysis and the auxiliary variables used in it. The various steps are dealt with in greater detail in L.4.1 to L.6.2. The procedure for one test signal is presented. The procedure shall be carried out with all standard test signals (see Clause L.4) and possibly with additional test signals. Whether additional test signals are required depends on the *Encoder(SR)*'s possible failures and shall be clarified with the aid of an FMEDA on the *Encoder(SR)*'s component and circuit level (see Clause L.7).


START
Step 1
Make test signal available
$A_{pos}(n)$, $A_{neg}(n)$, $B_{pos}(n)$, $B_{neg}(n)$
Step 2
Form differential signals
$A(n)$, $B(n)$
Step 3
Form square-wave signals to specification
Step 4
Perform specified diagnostics
$A_{sqw}(n)$, $B_{sqw}(n)$
SFD(n)
Step 5
Detect signal slopes
Step 9
Fault detection within a period?
$A_{sl}(n)$, $B_{sl}(n)$
$SFD_{1p}(n)$
Step 6
Count slopes in preceding period
$A_{nsl}(n)$, $B_{nsl}(n)$
Step 7
Detect static signal
$A_{stat}(n)$, $B_{stat}(n)$
Step 8
Ideal fault detection
IFD(n)
Step 10
Determine position-related result
Step 11
Fault detection not optimal?
Step 13
Fault detection unacceptable?
R(n)
r(n)
$r_{1p}(n)$
Optimal
—
Acceptable
—
Not acceptable
—
Not safety relevant
Step 12
Whole test area optimal?
Step 14
Whole test area acceptable?
R
R_{1p}
Optimal
—
Not optimal
Acceptable
—
Not acceptable
Assessment
IEC

Key

$A_{pos}(n)$	cosine test signal with direct component at position value n
$A_{neg}(n)$	inverted cosine test signal with direct component at position value n
$B_{pos}(n)$	sine test signal with direct component at position value n
$B_{neg(}n)$	inverted sine test signal with direct component at position value n
$A(n)$	differential cosine test signal *A* at position value n
$B(n)$	differential sine test signal *B* at position value n
$A_{sqw}(n)$	square wave signal obtained from $A(n)$ at position value n
$B_{sqw}(n)$	square wave signal obtained from $B(n)$ at position value n
$A_{sl}(n)$	slope of $A_{sqw}(n)$ present at position value n
$B_{sl}(n)$	slope of $B_{sqw}(n)$ present at position value n
$A_{nsl}(n)$	number of slopes of $A_{sl}(n)$ within the 1.1-fold test signal period preceding n
$B_{nsl}(n)$	number of slopes of $B_{sl}(n)$ within the 1.1-fold test signal period preceding n
$A_{stat}(n)$	$A_{sqw}(n)$ assessed as static at position value n
$B_{stat}(n)$	$B_{sqw}(n)$ assessed as static at position value n
$IFD(n)$	detection of a *fault* by an optimal *ideal fault detection* at position value n
$SFD(n)$	detection of a *fault* by specified diagnostic measures at position value n
$SFD_{1P}(n)$	detection of a *fault* by specified diagnostic measures within a 1,1-fold period of the *solid measure* beginning at position value n
$R(n)$	result of the static analysis of the specified diagnostic measures at position value n
$r(n)$	missing *fault* detection by specified diagnostic measures at position value n
R	result of the static analysis of the specified diagnostic measures
$r_{1P}(n)$	missing *fault* detection by specified diagnostic measures within a 1,1-fold period of the *solid measure* beginning at position value n
R_{1P}	overall result of the static analysis of the specified diagnostic measures with respect to their abilty to report a *fault* within a 1,1-fold period of the *solid measure*

Figure L.2 – Static analysis procedure (for one test signal) with variable denominations

L.4 Standard test signals

L.4.1 Make test signal available (step 1)

The test signals used in static analysis serve as substitute signals for the corrupted output signals generated by *faults* in the *Encoder(SR)*. Each test signal consequently consists of the four individual output signals at the outbound interface:

a) A_{pos} cosine test signal with direct component;

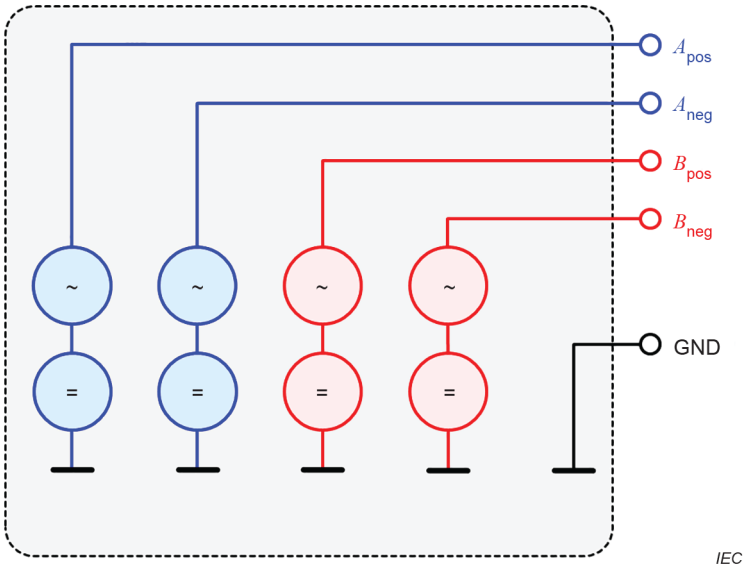
b) A_{neg} inverted cosine test signal with direct component;

c) B_{pos} sine test signal with direct component; and

d) B_{neg} inverted sine test signal with direct component.

This point of reference was chosen because, on conventional *Encoder(SR)* with sine and cosine output signals, it is always present in the same form, while the inbound interface, for example at the output of the opto-ASIC, differs depending on the inbound interface design.

The output interface in question can be represented by the substitute circuit in Figure L.3.



Key

A_{pos} cosine test signal with direct component

A_{neg} inverted cosine test signal with direct component

B_{pos} sine test signal with direct component

B_{neg} inverted sine test signal with direct component

Figure L.3 – Substitute circuit for *Encoder(SR)'s* outbound interface

The direct component superimposed on all alternating signals keeps all signals in the positive voltage range at all times.

In their *fault*-free state, the output signals take the following form:

$$A_{pos}(\varphi) = S_{=} + \frac{1}{2} Amp \cdot cos\,\varphi$$

$$A_{neg}(\varphi) = S_{=} - \frac{1}{2} Amp \cdot cos\,\varphi$$

$$B_{pos}(\varphi) = S_{=} + \frac{1}{2} Amp \cdot sin\,\varphi$$

$$B_{neg}(\varphi) = S_{=} - \frac{1}{2} Amp \cdot sin\,\varphi$$

where

φ is the position of the *solid measure* in relation to the sensor part of the *Encoder(SR)*, where φ changes by 360° (2π) on passing through a period of the *solid measure*;

$S_{=}$ is the offset component of the signal;

Amp is the amplitude of the alternating component of the signal.

NOTE A frequent implementation is: $S_{=}$ = 2,5 V and *Amp* = 0,5 V.

Due to the differential amplifier stages for the A and B signals, the signals $A(\varphi)$ and $B(\varphi)$ are formed during *signal processing*:

$$A(\varphi) = A_{\text{pos}}(\varphi) - A_{\text{neg}}(\varphi) = Amp \cdot \cos\varphi$$

$$B(\varphi) = B_{\text{pos}}(\varphi) - B_{\text{neg}}(\varphi) = Amp \cdot \sin\varphi$$

NOTE To prevent negative signal and operating voltages in *signal processing*, a new direct component is added in practice to $A(\varphi)$ and $B(\varphi)$. Circuitry specifics of this nature are disregarded in Annex L.

The test signals presented further below are based on the nominal signals and, over a number of periods, vary in amplitude, DC component or phase or a combination thereof. For numeric representation and investigation, the number of the observed periods shall be limited and each period represented by a finite number of sample values. The variations undertaken in relation to the position value φ shall not excessively distort the signal shape. The overall number of sampling points shall also be manageable. As a compromise, 100 periods with a resolution of 100 sampling points each are therefore chosen, yielding 10 000 sampling points per test signal.

With the discrete position value n for the sampling points 0, 1, 2, …, 10 000, the continuous position value φ is substituted as follows:

$$\varphi = 2\pi \frac{n}{100} = \frac{\pi}{50} n$$

The nominal signals of the *fault*-free *Encoder(SR)* are thus represented as follows:

$$A_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

On this basis, five standard test signals are defined in the following. They each realise a certain signal distortion dependent on the position value n.

In the assessment of the *signal processing* specification (Clause L.6), the position range also shall be taken into account as n > 10 000 at one position (step 9). Since the distortion of the test signals is only defined for the position range n = 0 … 10 000, the distortion is "frozen" at n = 10 000. This is done with the aid of the variable:

$$\bar{n} = \begin{cases} n & \text{for} \quad n \leq 10\,000 \\ 10\,000 & \text{for} \quad n > 10\,000 \end{cases}$$

It is used in that part of the test signal equations that causes the signal distortion, while the part of the test signal equations that generates the oscillation uses the position value n rising to over 10 000 so that the oscillation is continued.

L.4.2 Test signal 1

Test signal 1 provides parallel amplitude variation with a nominal direct component:

$$A_{\text{pos}}(n) = S_{=} + \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

where

$$\bar{n} = \begin{cases} n & \text{for} \quad n \leq 10\,000 \\ 10\,000 & \text{for} \quad n > 10\,000 \end{cases}$$

L.4.3 Test signal 2

Test signal 2 provides antiparallel amplitude variation with nominal direct component:

$$A_{\text{pos}}(n) = S_{=} + \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \frac{\bar{n}}{10\,000} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \frac{\bar{n}}{10\,000} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

where

$$\bar{n} = \begin{cases} n & \text{for} \quad n \leq 10\,000 \\ 10\,000 & \text{for} \quad n > 10\,000 \end{cases}$$

L.4.4 Test signal 3

Test signal 3 provides parallel amplitude variation of the total signals including the direct component:

$$A_{\text{pos}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right)\left[S_{=} + \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)\right]$$

$$A_{\text{neg}}(n) = S_{=} - \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right)\left[S_{=} + \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)\right]$$

$$B_{\text{neg}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right)\left[S_{=} - \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)\right]$$

where

$$\bar{n} = \begin{cases} n & \text{for} \quad n \leq 10\,000 \\ 10\,000 & \text{for} \quad n > 10\,000 \end{cases}$$

L.4.5 Test signal 4

Test signal 4 provides variation of the direct component of the "pos" signals:

$$A_{\text{pos}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right) S_{=} + \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right) S_{=} + \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

where

$$\bar{n} = \begin{cases} n & \text{for} \quad n \leq 10\,000 \\ 10\,000 & \text{for} \quad n > 10\,000 \end{cases}.$$

L.4.6 Test signal 5

Test signal 5 provides phase variation:

$$A_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \sin\left[\frac{\pi}{50} n + \pi\left(\frac{\bar{n}}{10\,000} - \frac{1}{2}\right)\right]$$

$$B_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \sin\left[\frac{\pi}{50} n + \pi\left(\frac{\bar{n}}{10\,000} - \frac{1}{2}\right)\right]$$

where

$$\bar{n} = \begin{cases} n & \text{for} \quad n \leq 10\,000 \\ 10\,000 & \text{for} \quad n > 10\,000 \end{cases}.$$

Further test signals may be necessary in order to qualify the *signal processing* specification for a certain *Encoder(SR)*. Whether this is the case depends on the *Encoder(SR)* possible failure modes and shall be clarified with an FMEDA of the *Encoder(SR)* on the component and circuitry level. An explanation of the problems and a description of the procedure can be found in Clause L.7.

All test signals are defined for whole-number $n \geq 0$. In the assessment of the *signal processing* specification (Clause L.6), the position value shall be considered as $n < 0$ at certain points (step 5, step 6). The test signals are therefore preceded by a "preparatory phase" with the undistorted nominal output signals. The distortion, for example the test proper, thus begins abruptly from position $n = 0$.

L.5 Simulation of *signal processing* to specification

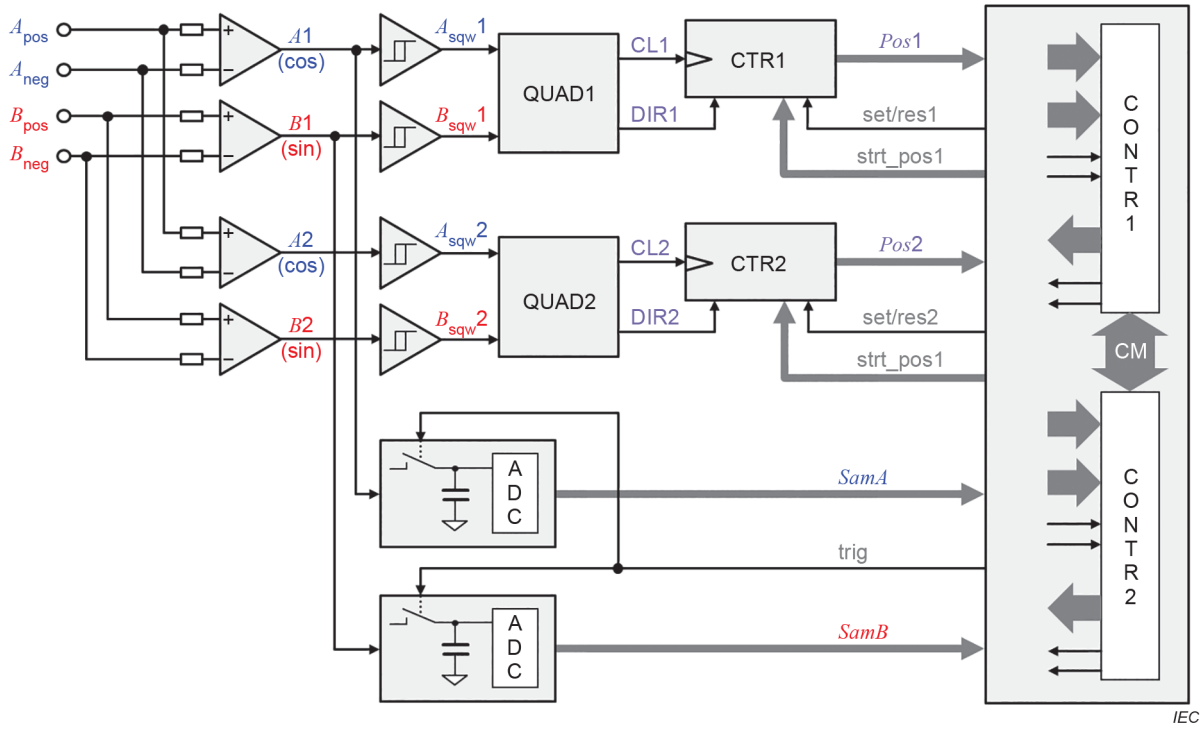
L.5.1 General

The definition of the test signals is followed by simulation of *signal evaluation* and diagnostics.

To obtain the position values, the slopes of the analogue sine/cosine signals are detected and counted. From the phase angle of the two signals, the direction of movement determining the direction of counting also shall be ascertained. The usual implementation makes use of quadrature decoders that generate both the count pulses and the direction signal.

The integrity test of the analogue signals for the realisation of the *diagnostic coverage* (DC) for the *Encoder(SR)* can be performed with analogue means or, after digitisation, digitally.

To illustrate this, Figure L.4 shows a possible implementation (example) of *signal processing*, for example pulse production and counting and diagnostics.



Key

A_{pos}	cosine test signal with direct component
A_{neg}	inverted cosine test signal with direct component
B_{pos}	sine test signal with direct component
B_{neg}	inverted sine test signal with direct component
$A1$, $A2$	differential cosine signal A in channel 1, 2
$B1$, $B2$	differential sine signal B in channel 1, 2
$A_{sqw}1$, $A_{sqw}2$	square wave signal obtained from signal A in channel 1, 2
$B_{sqw}1$, $B_{sqw}2$	square wave signal obtained from signal B in channel 1, 2
QUAD1, 2	quadrature decoder 1, 2
CL1, CL2	clock signal of channel 1, 2
DIR1, DIR2	direction signal of channel 1, 2
CTR1, 2	counter 1, 2
*Pos*1, 2	position value 1, 2
set/res1, 2	set/reset 1, 2
strt_pos1, 2	start position 1, 2
CONTR1, 2	controller 1, 2
ADC	analog to digital converter
SamA, B	sample value A, B
trig	sample trigger
CM	cross monitoring

Figure L.4 – Example of a circuit for evaluation of the output signals and diagnostics of *Encoder(SR) faults*

The redundancies contribute to the realisation of *single-fault tolerance* and the detection of *faults* in the evaluation circuit but not to *fault* detection in the *Encoder(SR)*. The ADCs do not perform the *safety function*, but are used for diagnostics and do not establish any redundancy.

NOTE 1 The assessment of the equally necessary *fault* detection in the evaluation circuit is not the subject here. In Annex L, static analysis is used solely for testing the *signal processing* specification.

NOTE 2 Given suitably low frequencies, signal slope detection, quadrature decoding and position counting can be realised by software based on sufficiently quickly sampled and digitised analogue signals.

In the static analysis of *signal evaluation* and *fault* detection, it is assumed that *signal processing* is performed as specified in the *Encoder(SR)*'s information for use.

L.5.2 Form differential signals (step 2)

In step 2, the differential signals shall be evaluated:

$$A(n) = A_{\text{pos}}(n) - A_{\text{neg}}(n)$$

$$B(n) = B_{\text{pos}}(n) - B_{\text{neg}}(n).$$

L.5.3 Form square-wave signals to specification (Schmitt trigger, step 3)

In step 3, the square-wave signals shall be evaluated as specified in the information for use:

NOTE The index sqw is used to indicate "square-wave signal".

$$A_{\text{sqw}}(n) = \begin{cases} 1 & \text{for } A(n) \geq A_{\text{on}} \vee \left[A(n) \geq A_{\text{off}} \wedge A_{\text{sqw}}(n-1) = 1 \right] \\ 0 & \text{else} \end{cases}$$

$$B_{\text{sqw}}(n) = \begin{cases} 1 & \text{for } B(n) \geq B_{\text{on}} \vee \left[B(n) \geq B_{\text{off}} \wedge B_{\text{sqw}}(n-1) = 1 \right] \\ 0 & \text{else} \end{cases}$$

where

A_{on}, A_{off} are the switching thresholds of the Schmitt trigger of signal A.

B_{on}, B_{off} are the switching thresholds of Schmitt trigger of signal B.

L.5.4 Perform specified diagnostics (step 4)

As an example, it is assumed that the *Encoder(SR)*'s information for use specifies pointer-length monitoring as the diagnostics.

The possible influence of amplitude control shall be taken into account (see 6.3).

$$SFD(n) = \begin{cases} 1 & \text{for } A^2(n) + B^2(n) < Amp^2_{\text{min}} \vee A^2(n) + B^2(n) > Amp^2_{\text{max}} \\ 0 & \text{else} \end{cases}$$

where

Amp^2_{min} is the lower limit of the specified pointer-length square;

Amp^2_{max} is the upper limit of the specified pointer-length square.

NOTE The term SFD indicates "specified *fault* detection".

With the value 1, *SFD*(n) indicates that the specified analogue signal integrity test generates "*fault*" as the test result at position value n.

L.6 Assessment of the *signal processing* specification

L.6.1 General

L.6.1.1 Overview

After simulation of *signal processing* according to the specification, the results shall be assessed taking the characteristics of the quadrature decoder into account. If one of the two digital control signals of a quadrature decoder becomes static due to a *fault* in the *Encoder(SR)* while the other one toggles due to movement, the count direction signal changes with each count pulse. The position counter then counts alternately one step forwards and one step back, thus simulating standstill. For this reason, when one or both of the two control signals becomes static, a *dangerous failure* of the *safety function* is caused. This yields the following evaluation criterion for the *signal processing* specification.

The specification is acceptable when, during the processing of the test signals to specification, NONE of the following critical cases occurs at ANY time:

- one of the two square-wave signals derived from analogue signals A (cosine) and B (sine) becomes static AND the analogue signal integrity test does not report any *fault*; and
- both of the square-wave signals derived from analogue signals A (cosine) and B (sine) become static AND the analogue signal integrity test does not report any *fault*.

If one of these cases occurs at least once during processing of the test signals, the *signal processing* specification is assessed as not acceptable.

The redundancy of the evaluation circuit's quadrature decoder and counter is unable to detect the static nature of one or both square-wave signals, as this behaviour occurs in both channels by the very nature of the system. A component and circuitry FMEDA for the *Encoder(SR)* shall therefore ascertain whether such a *fault* pattern can be caused by a single component *fault* (see Clause L.7). If this is possible, such *faults* shall be detected by the analogue signal integrity test.

When the acceptance criterion has been defined for the *signal processing* specification, assessment shall be carried out in several steps.

L.6.1.2 Detect signal slopes (step 5)

In step 5, the position value n is determined at which there are rising or falling slopes.

$$A_{\mathrm{sl}}(n) = \begin{cases} 1 & \text{for} \quad A_{\mathrm{sqw}}(n) \neq A_{\mathrm{sqw}}(n-1) \\ 0 & \text{else} \end{cases}$$

$$B_{\mathrm{sl}}(n) = \begin{cases} 1 & \text{for} \quad B_{\mathrm{sqw}}(n) \neq B_{\mathrm{sqw}}(n-1) \\ 0 & \text{else} \end{cases}$$

NOTE The subscript "sl" indicates "slope".

With the value 1, $A_{\mathrm{sl}}(n)$ and $B_{\mathrm{sl}}(n)$ indicate that the square-wave signal A_{sqw} or B_{sqw} has a rising or falling slope at position value n.

L.6.1.3 Count slopes in preceding period (step 6)

The purpose of this step is to detect when square-wave signals become static. A square-wave signal is assessed as "static" when less than two (the normal case) signal changes take place within a period. To suppress artefacts from the test signal slightly distorted (amplitude-modulated) compared to a pure sine curve, the observation period is defined as 1,1 times the period duration.

$$A_{\mathrm{nsl}}(n) = \sum_{k = n-109}^{n} A_{\mathrm{sl}}(k)$$

$$B_{\mathrm{nsl}}(n) = \sum_{k = n-109}^{n} B_{\mathrm{sl}}(k)$$

$A_{\mathrm{nsl}}(n)$ and $B_{\mathrm{nsl}}(n)$ express the number of slopes of square-wave signals A_{sqw} and B_{sqw} in the 1,1-fold test signal period preceding position value n.

L.6.1.4 Detect static signal (step 7)

This step tests whether in the observation period with its 100 test signal oscillations (n = 0, 1, ... , 10 000), there are position values n at which one of the square-wave signals A_{sqw} or B_{sqw} becomes static (fewer than two slopes in the preceding 1,1 oscillation periods).

$$A_{\mathrm{stat}}(n) = \begin{cases} 1 & \text{for } A_{\mathrm{nsl}}(n) < 2 \\ 0 & \text{else} \end{cases}$$

$$B_{\mathrm{stat}}(n) = \begin{cases} 1 & \text{for } B_{\mathrm{nsl}}(n) < 2 \\ 0 & \text{else} \end{cases}$$

With the value 1, $A_{\mathrm{stat}}(n)$ or $B_{\mathrm{stat}}(n)$ indicate that the square-wave signal A_{sqw} or B_{sqw} is assessed as static at position value n.

L.6.2 Assessment concept for the *signal processing* specification

L.6.2.1 General

Ideally, a *fault* is reported by the analogue signal integrity test precisely when at least one of the two square-wave signals becomes static. In many cases of *faults*, the analogue signal integrity test does not generate an uninterrupted *fault* message when passing through a period of the *solid measure*. This can be accepted as long as a *fault* message is issued at least at one position during a period.

If some *faults* of the *Encoder(SR)* are detectable only at certain parts of a period of the *solid measure* with the prescribed analogue signal integrity test, the instructions shall draw attention to this fact, for example:

- in the event of continuous diagnostics, it is essential to ensure achievement of the safe state in the event of a *fault*, taking account of the maximum rotary/linear speed and line number; and
- in the event of diagnostics at discrete times, the instructions shall explain the relationship between rotary/linear speed, line number and sampling rate; the explanation enables the user to modify the time behaviour of his *signal processing* to meet his needs and limit the application in terms of rotary/linear speed and line number.

To facilitate assessment of the *signal processing* specification, a number of auxiliary variables are in turn defined.

L.6.2.2 *Ideal fault detection* (step 8)

Ideal fault detection is simulated with the variable *IFD* (marked green in Figure L.2). It indicates that the analogue signal integrity test should report a *fault*:

$$IFD(n) = \begin{cases} 1 & \text{for} \quad A_{\text{stat}}(n) + B_{\text{stat}}(n) \geq 1 \\ 0 & \text{else} \end{cases}.$$

NOTE 1 The term IFD indicates "*ideal fault detection*".

The variable *IFD* assumes the value of 1 at every position value n at which "*ideal fault detection*" would respond.

On the other hand, the variable *SFD* (marked orange in Figure L.2) introduced in step 4 represents the behaviour of the specified analogue signal integrity test.

In the special case of phasor-length monitoring, the following applies (as already shown above):

$$SFD(n) = \begin{cases} 1 & \text{for} \quad A^2(n) + B^2(n) < Amp^2_{\text{min}} \quad \vee \quad A^2(n) + B^2(n) > Amp^2_{\text{max}} \\ 0 & \text{else} \end{cases}.$$

NOTE 2 The term *SFD* indicates "specified *fault* detection".

The variable *SFD* assumes the value of 1 at every position value n at which the specified analogue signal integrity test responds, for example issues a *fault* message.

L.6.2.3 Fault detection within the period? (step 9)

It is also accepted when necessary *fault* detection takes place within a position range that starts with position n_1 of the first *fault* occurrence ($IFD(n_1) = 1$) and has the magnitude of the (1,1-fold) period of the *solid measure*.

NOTE The factor 1,1 rather than the factor 1 is used for suppressing artefacts by the test signal that is slightly distorted (amplitude-modulated) compared to a pure sine curve.

To represent *fault* detection within a 1,1-fold period, the variable SFD_{1P} (marked light-blue in Figure L.2) is defined as follows:

$$SFD_{1P}(n) = \begin{cases} 1 & \text{for} \quad \sum_{k=n}^{n+109} SFD(k) \geq 1 \\ 0 & \text{else} \end{cases}.$$

The variable SFD_{1P} assumes the value 1 at a position value n when, in the (1,1-fold) *solid measure* period beginning with n, the specified analogue signal integrity test responds at least at one n.

L.6.2.4 Determine position-related result (step 10)

At every position value n where *ideal fault detection* would respond, an assessment can be made with variable R. Positions where no *fault* detection is necessary ($IFD(n) = 0$) are not relevant for the *signal processing* specification:

$$R(n) = \begin{cases} \text{optimal} & \text{for} \quad IFD(n) = 1 \ \wedge \ SFD_{1P}(n) = 1 \ \wedge \ SFD(n) = 1 \\ \text{acceptable} & \text{for} \quad IFD(n) = 1 \ \wedge \ SFD_{1P}(n) = 1 \ \wedge \ SFD(n) = 0 \\ \text{not acceptable} & \text{for} \quad IFD(n) = 1 \ \wedge \ SFD_{1P}(n) = 0 \\ \text{not safety relevant} & \text{for} \quad IFD(n) = 0 \end{cases} .$$

NOTE The term $R(n)$ is used to indicate the result.

The variable $R(n)$ is a logical variable that at each position value n assumes precisely one of the four possible values "optimal", "acceptable", "not acceptable" or "not safety-relevant". It can help to investigate a certain analysis result with greater accuracy.

L.6.2.5 Fault detection not optimal? (step 11)

The purpose of this step is to ascertain positions without optimal *fault* detection. To this end, the numeric variable $r(n)$ is first defined as follows:

$$r(n) = \begin{cases} 1 & \text{for} \quad IFD(n) = 1 \ \wedge \ SFD(n) = 0 \\ 0 & \text{else} \end{cases} .$$

$r(n)$ assumes the value of 1 at such position values n at which an *ideal fault detection* would respond but the specified *fault* detection does not report a *fault*. $r(n) = 1$ thus represents the case where $R(n)$ has not achieved the value "optimal" at position value n.

L.6.2.6 Whole test area optimal? (step 12)

The *signal processing* specification shall be assessed over the entire course of a test signal (n = 0, 1, …, 10 000).

For the entire test signal to be "optimal" (solely for safety's sake), the case $r(n) = 1$ shall not occur at any position of the test signal. Using the (n-independent) variable R defined in the following, it is possible to express whether or not the *signal processing* specification is optimal with the test signal used:

$$R = \begin{cases} \text{optimal} & \text{for} \quad \sum_{n=0}^{10\,000} r(n) < 1 \\ \text{not optimal} & \text{else} \end{cases} .$$

R = optimal means that the *signal processing* specification causes a continuous *fault* message in the event of a *fault* on the basis of the test signal.

L.6.2.7 Fault detection unacceptable? (step 13)

Optimal *fault* detection often is not achieved. However, it is also accepted if a *fault* detected within a *solid measure* period triggers a *fault* message for at least one position n. A lack of a *fault* message within this period shall not be accepted.

For local assessment, the variable $r_{1P}(n)$ is first defined as follows:

$$r_{1P}(n) = \begin{cases} 1 & \text{for} \quad IFD(n) = 1 \ \wedge \ SFD_{1P}(n) = 0 \\ 0 & \text{else} \end{cases} .$$

$r_{1P}(n)$ assumes the value of 1 at such positions n at which an *ideal fault detection* would respond but the specified *fault* detection would not issue a *fault* message even within the following (1,1-fold) period of the test signal. $r_{1P}(n)$ = 1 thus represents the case $R(n)$ = not acceptable.

The case $r_{1P}(n)$ = 1 shall not occur at any position of the test signal.

L.6.2.8 Whole test area acceptable? (step 14)

With the aid of the (n-independent) variable R_{1P}, it is possible to decide whether the *signal processing* specification stands up to the test signal overall (acceptable) or not (not acceptable):

$$R_{1P} = \begin{cases} \text{acceptable} & \text{for } \sum_{n=0}^{10\,000} r_{1P}(n) < 1 \\ \text{not acceptable} & \text{else} \end{cases} .$$

R_{1P} = acceptable means that the *signal processing* specification causes a *fault* message at least within the 1,1-fold *solid measure* period in the event of a *fault* on the basis of the test signal.

NOTE Each *signal processing* specification that achieves R = optimal also achieves R_{1P} = acceptable. A *signal processing* specification that achieves R_{1P} = acceptable does not necessarily also achieve R = optimal.

R_{1P} = not acceptable means that the *signal processing* specification does not stand up to the test signal and shall therefore be improved.

A *signal processing* specification that achieves R_{1P} = acceptable for every test signal has passed the "static analysis" test.

If a *signal processing* specification that has passed the test of static analysis does not achieve R = optimal with at least one test signal, this means that the prescribed analogue signal integrity test is only capable of detecting some *faults* in certain parts of a *solid measure* period. In the case in question, reference shall be made to this fact in the instructions for use. See L.6.2.

L.7 FMEDA *Encoder(SR)* for verification of the *diagnostic coverage*

L.7.1 General

To achieve the required *diagnostic coverage*, the *signal processing* specification shall master all hardware failures that occur (see Clause L.3). Which faulty output signals can arise due to hardware *faults* depends on the *fault* models of the components and on the circuitry of the *Encoder(SR)*.

L.7.2 Explanation of the problem

In principle, there are signal combinations A_{pos}, A_{neg}, B_{pos} and B_{neg} that represent a state of immobility. Such a state is of course one of the possible and permissible operating states. However, the situation becomes critical when:

- there is motion but the output signals are distorted by a single hardware failure to such an extent that immobility is simulated; and
- this hardware failure is not detected by the analogue signal integrity test.

Such critical signal combinations naturally include static signals, but not exclusively. With the aid of a FMEDA, it is essential to determine whether a single hardware failure is capable of

generating such critical output signals. If this is possible, the *signal processing* specification is not acceptable and shall be improved so that such scenarios are no longer possible.

To illustrate this, an example of a potentially critical signal combination is given in the following:

$$A_{\text{pos}}(n) = 1{,}16 \cdot S_{=} + k \cdot \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - k \cdot \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

where

k is a factor to the amplitude of $A_{\text{pos}}(n)$ and $A_{\text{neg}}(n)$ resulting from a single *fault* within the *Encoder(SR)*.

The cases k = 0 and k = 0,2 are considered. The alternating component of the two A signals is then zero or 20 % of the nominal value. Given k = 0,2 and *Amp* = 0,5 V, this yields the following AC component (peak to peak) of the differential signal:

$$A_{\approx \text{pp}} = 2\left(A_{\text{pos}\approx} - A_{\text{neg}\approx}\right) = 2\left(0{,}2 \cdot \frac{1}{2} Amp + 0{,}2 \cdot \frac{1}{2} Amp\right) = 0{,}4 \cdot Amp = 0{,}4 \cdot 0{,}5\,\text{V} = 0{,}2\,\text{V}$$

where

$A_{\text{pos}\approx}$ is the AC component of A_{pos};

$A_{\text{neg}\approx}$ is the AC component of A_{neg}.

The direct component of A_{pos} is increased by 16 % at the same time. When $S_{=}$ = 2,5 V, the differential signal A then has the following mean value (instead of zero in the *fault*-free case):

$$A_{=} = A_{\text{pos}=} - A_{\text{neg}=} = 1{,}16 \cdot S_{=} - S_{=} = 0{,}16 \cdot S_{=} = 0{,}16 \cdot 2{,}5\,\text{V} = 0{,}4\,\text{V}$$

where

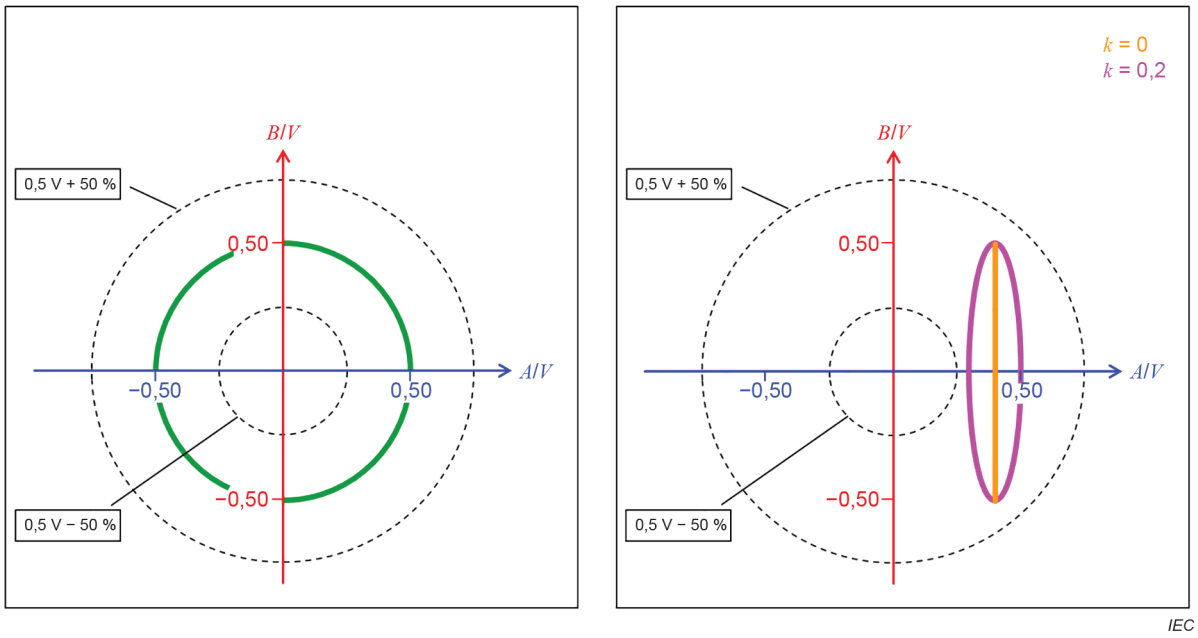
$A_{\text{pos}=}$ is the DC component of A_{pos};

$A_{\text{neg}=}$ is the DC component of A_{neg}.

The two B signals are undistorted.

The analogue signal integrity test is assumed to be pointer-length monitoring for exceeding or falling below the nominal value (0,5 V) by ± 50 %.

Figure L.5 shows the resultant phasor-tip curves: Figure L.5 a) for comparison the ideal curve of the *fault*-free case (green) and Figure L.5 b) the two *fault* cases with k = 0 und k = 0,2 (orange and magenta). The phasor-length limit curves of amplitude monitoring appear as broken circles.



a) Fault free **b) Critical fault**

Key

A differential sine signal expressed in volt

B differential cosine signal expressed in volt

k factor to the amplitude of A_{pos} and A_{neg} resulting from a single *fault*

Figure L.5 – Lissajous diagrams (representation of signal B over signal A) in two *fault* cases

The switching thresholds for square-wave formation are symmetrically arranged around the zero of voltages of A and B. The result of this is that, in the event of both *fault* cases (k = 0 and k = 0,2), signal A no longer crosses both switching thresholds, thus causing output signals $A_{sqw}1$ and $A_{sqw}2$ of both square-wave formers (see Figure L.4) to become static. As a consequence, both position counters count one point forwards and back continuously, thus simulating immobility.

In Figure L.5 b), it is evident that both phasor-tip curves are in the permissible range between the amplitude limit circles. This *fault* is therefore not detected by phasor-length monitoring with the parameters assumed here. The detection of ALL *faults* cannot be achieved if such *faults* are to be expected.

FMEDA shall be employed to check whether such critical scenarios can occur with the given hardware of the *Encoder(SR)* in combination with the envisaged *signal processing* specification, and to demonstrate that such scenarios can be excluded.

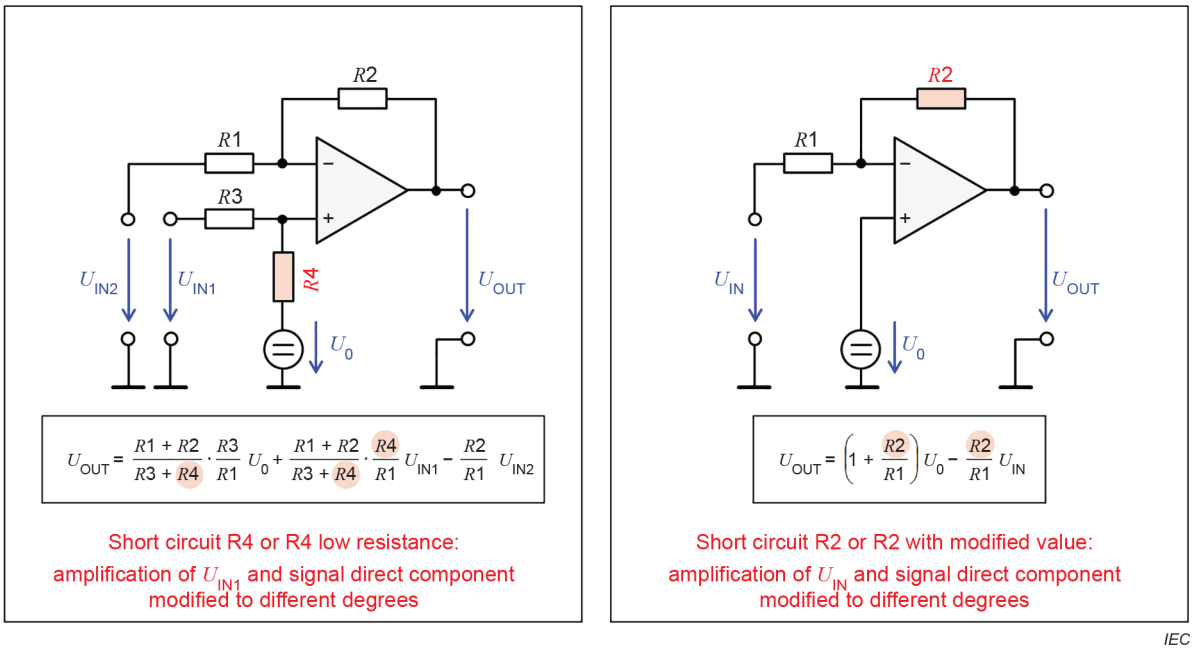
L.7.3 Procedure for FMEDA

With FMEDA on the component and circuit level, the *fault* potential of all components is investigated as usual systematically in terms of its effects on the output signals of the circuit and the effectiveness of the implemented diagnostics in the event of critical circuit behaviour.

As a result of randomly complex *fault* assumptions in the case of electronic circuit components, it will always be possible to bring forth critical scenarios of the type described above. However,

during FMEDA only those component failure types can be realistically assumed that are listed in the *fault* models in IEC 61800-5-2:2016, D.3.1 to D.3.15. These failure types that cannot be excluded but shall be mastered by the diagnostics are largely identical to those *faults* to be detected with "high" *diagnostic coverage* in accordance with IEC 61508-2:2010, Annex A (e.g. "DC *fault* model").

The critical *fault* scenario described above arises due to a change in amplification and a simultaneous direct component shift. The fact that such a dual effect can be caused in principle by a single component *fault* is demonstrated with the aid of the standard amplifier circuits in Figure L.6. This realisation stresses the need for an FMEDA of the *Encoder(SR)*'s specific hardware.



a) Differential amplifier with operating point setting

b) Inverting amplifier with operating point setting

NOTE For the equations in this figure, ideal operation amplifiers have been assumed for the sake of simplicity (input currents and output impedance zero, internal amplification infinite, no offset).

Figure L.6 – Examples of the dual effect of a single component *fault*

In Figure L.6 a) is shown a differential amplifier circuit with operating point setting. Due to component *fault*, a short circuit of $R4$ or a low resistance value of $R4$ is possible. In this case, the amplification of U_{IN1} and the signal direct component are modified to different degrees by one single *fault* of $R4$.

In Figure L.6 b) is shown an inverting amplifier circuit with operating point setting. Due to component *fault*, a short circuit of $R2$ or a changed resistance value of $R2$ is possible. In this case, the amplification of U_{IN} and the signal direct component are modified to different degrees by one single *fault* of $R2$.

It is in principle permissible for users to organise and parametrise *signal processing* differently. If, however, the FMEDA of the *Encoder(SR)* reveals that potentially critical output signals of the type shown above can be generated by single *faults*, this shall be described in the information for use, so the *signal processing* in an application can be designed accordingly. A sensible form of information consists of the transmission of additional test signals that represent the potentially critical *faults* of the *Encoder(SR)* and shall be mastered during static analysis.

L.8 List of variables used for performing static analysis

Clause L.8 includes a list of all the variables which are used to perform the static analysis and provides a short and precise description.

NOTE 1 It is possible the descriptions in Clause L.8 apply different wordings to explain the meaning of the variables compared to the wording used in the introduction of the variables in previous clauses of Annex L. This is intended to allow different approaches to explain the respective information content.

A_{pos} cosine test signal with direct component;

A_{neg} inverted cosine test signal with direct component;

B_{pos} sine test signal with direct component;

B_{neg} inverted sine test signal with direct component;

φ continous position value;

NOTE 2 Position of the *solid measure* in relation to the sensor part of the *Encoder(SR)*, where φ changes by 360° (2π) on passing through a period of the *solid measure*.

n discrete position value;

NOTE 3 Integer, denoting discrete positions by specifying the number of steps of size 1/100 of the period of the *solid measure*.

$S_{=}$ offset component;

Amp amplitude of the alternating component;

$A_{pos}(n)$ cosine test signal with direct component at position value n;

$A_{neg}(n)$ inverted Cosine test signal with direct component at position value n;

$B_{pos}(n)$ sine test signal with direct component at position value n;

$B_{neg}(n)$ inverted sine test signal with direct component at position value n;

$A(n)$ differential cosine test signal A at position value n;

$B(n)$ differential sine test signal B at position value n;

$A_{sqw}(n)$ square wave signal obtained from $A(n)$ at position value n;

$B_{sqw}(n)$ square wave signal obtained from $B(n)$ at position value n;

A_{on}, A_{off} switching thresholds of the Schmitt trigger of signal A;

B_{on}, B_{off} switching thresholds of the Schmitt trigger of signal B;

$A_{sl}(n)$ binary auxiliary variable indicating the presence of a slope of $A_{sqw}(n)$ at position value n (true: 1, false: 0);

$B_{sl}(n)$ binary auxiliary variable indicating the presence of a slope of $B_{sqw}(n)$ at position value n (true: 1, false: 0);

$A_{nsl}(n)$ number of slopes of $A_{sl}(n)$ within the 1,1-fold test signal period preceding n;

$B_{nsl}(n)$ number of slopes of $B_{sl}(n)$ within the 1,1-fold test signal period preceding n;

$A_{stat}(n)$ binary auxiliary variable indicating that $A_{sqw}(n)$ is assessed as static at position value n (true: 1, false: 0);

$B_{stat}(n)$ binary auxiliary variable indicating that $B_{sqw}(n)$ is assessed as static at position value n (true: 1, false: 0);

$IFD(n)$ binary auxiliary variable indicating that a *fault* would be detected by an optimal *ideal fault detection* at position value n (true: 1, false: 0);

$SFD(n)$ binary auxiliary variable indicating that the specified diagnostic measures of the *Encoder(SR)*'s analogue output signal would detect a *fault* at position value n (true: 1, false: 0);

$SFD_{1P}(n)$ binary auxiliary variable indicating that the specified diagnostic measures would detect a *fault* within a 1,1-fold period of the *solid measure* beginning at position value *n* (true: 1, false: 0);

Amp^2_{min} lower limit of the specified pointer-length square;

Amp^2_{max} upper limit of the specified pointer-length square;

$R(n)$ result of the static analysis of the specified diagnostic measures (concerning a specific test signal) related to a particular position value n;

NOTE 4 $R(n)$ assumes one of the four values "optimal", "acceptable", "not acceptable" or "not safety relevant".

$r(n)$ binary auxiliary variable indicating that the specified diagnostic measures do not report a *fault* at position value n, while the ideal *fault detection* would report a *fault* (true: 1, false: 0);

R result of the static analysis of the specified diagnostic measures (concerning a specific test signal) with respect to their abilty to report a *fault* at any position n where the *ideal fault detection* would do so;

NOTE 5 R assumes one of the values "optimal" or "not optimal".

$r_{1P}(n)$ binary auxiliary variable indicating that the specified diagnostic measures fail to report a *fault* within a 1,1-fold period of the *solid measure* beginning at position value n (true: 1, false: 0);

R_{1P} overall result of the static analysis of the specified diagnostic measures (concerning a specific test signal) with respect to their abilty to report a *fault* within a 1,1-fold period of the *solid measure;*

NOTE 6 R_{1P} assumes one of the values "acceptable" or "not acceptable".

$A_{\approx pp}$ AC component (peak to peak) of the differential signal A;

$A_{=}$ mean value of the differential signal A;

$A_{pos\approx}$ AC component of A_{pos};

$A_{neg\approx}$ AC component of A_{neg};

$A_{pos=}$ DC component of A_{pos};

$A_{neg=}$ DC component of A_{neg}; and

k factor to the amplitude of A_{pos} and A_{neg} (respectively $A_{pos}(n)$ and $A_{neg}(n)$) resulting from a hypothetical single *fault* within the *Encoder(SR).*

L.9 MS Excel tool for performance of static analysis

The static analysis can be performed with an MS Excel file provided by IFA with the macros integrated in it (see [17]). The standard test signals listed in Clause L.4 are already contained in the file. Further test signals can be added if necessary. Instructions for the user are contained in the file.

Annex M
(informative)

Aspects of diagnostic measures for obtaining incremental position values

M.1 General

Annex M deals with some specific *fault* models and their effect on analogue signal quality and achievable safe tolerance range. It is not exhaustive and the manufacturer should ensure that the *fault* models applicable to his product are dealt with appropriately in a FMEDA.

The diagnostic measures of *Encoder(SR)* may be implemented in parts or completely in the *evaluation unit* (see 6.3). The diagnostic measures which have to be implemented in the *evaluation unit* are specified in the information for use (see Annex F). Within the frame of the FMEDA (see 8.4) of the *Encoder(SR),* it shall be demonstrated that the specification of the external diagnostic measures accomplishes the required *fault* detection.

For *Encoder(SR)* with sine and cosine output signals and *HFT* = 0, *ideal fault detection* is necessary to achieve single *fault* tolerance (see 6.4.1). Commonly phasor length monitoring is applied as diagnostic measure. In principle there may be *fault* scenarios which cannot be detected by phasor length monitoring. Whether or not a phasor length monitoring is sufficient as diagnostic measure depends on the possible *faults* and the permissible *fault* exclusions of the specific *Encoder(SR)* as well as of the properties of the *safety sub-function(s)* implemented, especially of its specified position resolution.

Annex M exclusively considers the obtaining of safe position values from the analogue sine and cosine signals. At this, the correct determination of the direction of movement is essential.

First, an outline of the generation of the position values is given for the faultless case (see Clause M.2). After this, some *fault* scenarios are introduced, and in each case the performance of phasor length monitoring is discussed (Clause M.3 and Clause M.4). These presentations shall support the execution of the FMEDA at an *Encoder(SR)*.

The principles discussed in Annex M are related to *Encoder(SR)* with sine and cosine output signals and also to *Encoder(SR)* with square wave output signals and *Encoder(SR)* with digital output signals when the signal generation part of the *Encoder(SR)* includes sine and cosine signals.

M.2 Obtaining position values from incremental signals

In order to continuously generate a current position value from the incremental sine and cosine output signals, these signals are commonly processed as follows:

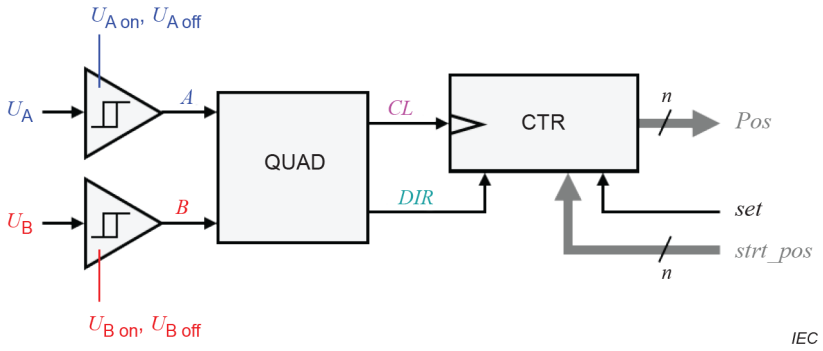
a) converting of the sine and cosine signals to square wave signals;
b) generation of a clock signal (counting pulses) and of a movement direction signal from the square wave signals by means of a quadrature decoder; and
c) driving of a counter for the position value with the clock signal and the direction signal.

A circuit for obtaining position values from incremental analogue signals is depicted in Figure M.1 in a symbolic way. In it U_{A} and U_{B} represent the cosine or, respectively, the sine signal whereas A and B represent the square wave signals obtained from them.

$U_{\mathrm{A\ on}}$ or, respectively, $U_{\mathrm{A\ off}}$ are the thresholds, at which the square wave shaper (Schmitt trigger) for the cosine signal U_{A} switches its output signal A to a logic 1 or, respectively, to a

logic 0. Accordingly, $U_{B\ on}$ or $U_{B\ off}$ are the thresholds, at which the square wave shaper for the sine signal U_B switches its output signal B to a logic 1 or to a logic 0. The square wave signals are fed in a quadrature decoder QUAD which out of them generates the signals CL and DIR for the position value counter CTR.

CL is the clock signal and DIR is the direction signal, determining the counting direction of the counter. The counter outputs its count as a position value Pos comprising n binary digits. By use of a set signal set, a starting position value $strt\_pos$ can be loaded into the counter.



Key

U_A	cosine signal
U_B	sine signal
$U_{A\ on}$, $U_{A\ off}$, $U_{B\ on}$, $U_{B\ off}$	switching thresholds
A, B	square wave signals
QUAD	quadrature decoder
CL	clock signal
DIR	direction signal
CTR	counter
Pos	position value
n	number of bits
set	set signal
strt_pos	start position

Figure M.1 – Obtaining position values from incremental signals

By means of their clock signal, typical quadrature decoders provide one counting pulse at each slope of the sine based square wave signal as well as the cosine based square wave signal. Thus, on running through one period of the *solid measure*, a quadrature decoder of that kind generates four counting pulses. The faultless behaviour of the circuit for triggering the position counter is depicted in Figure M.2.

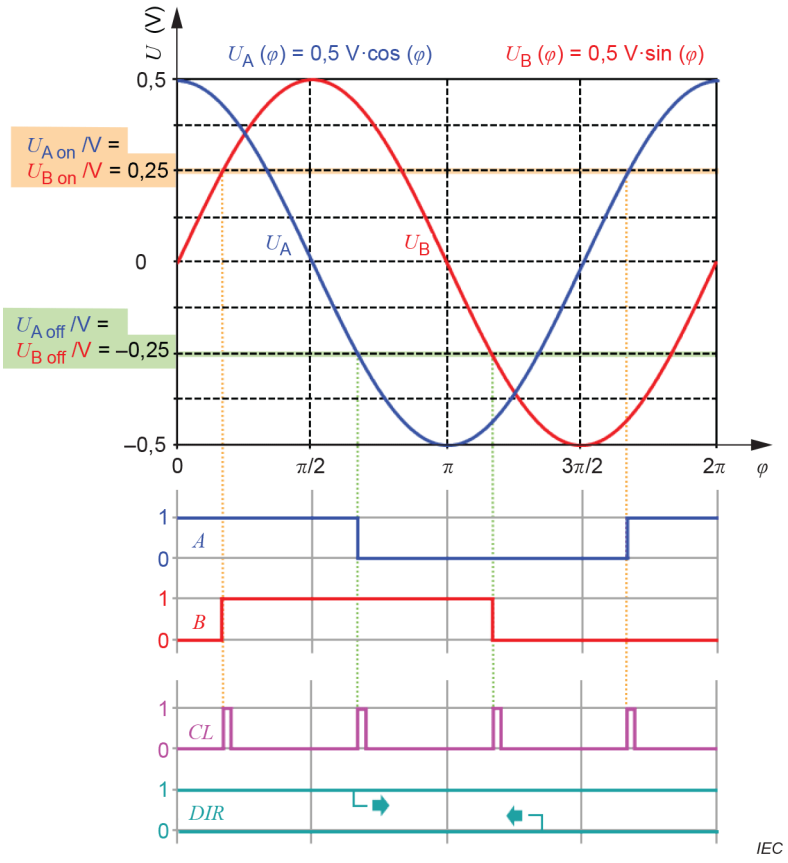


Figure M.2 – Counting pulse generation, faultless case

With this kind of driving, the count represents position values with a position resolution of a quarter period of the *solid measure*. In ideal case, the applicability of the position values within a period of the *solid measure* (fine resolution) presupposes the four counting pulses to divide the period of the *solid measure* into four segments of equal size.

M.3 Phase error of the sine and the cosine signals

M.3.1 General

According to the functional relation $\cos\varphi = \sin(\varphi + 90°)$, the phase shift between ideal cosine and sine signals is 90°. In the following, *faults* are discussed where the phase shift between cosine and sine signal is no longer 90°, but 90° – $\Delta\varphi$. This means that the cosine signal U_A leads by an angle $\Delta\varphi$, the phase error, compared with the ideal cosine signal.

NOTE If possible by design, phase errors can, for example, arise from a marginal contortion of the sensor in respect of the *solid measure*.

M.3.2 Phase errors with absolute values < 90°

With phase errors $\Delta\varphi$, the absolute value of which remains just smaller than 90°, for example with $-90° < \Delta\varphi < 90°$, an ideal quadrature decoder would still output a correct direction signal *DIR*. In case of a real quadrature decoder, the absolute value of the phase error $\Delta\varphi$ has to be (depending on the frequency) a little smaller than 90°, in order to allow the generation of an correct direction signal, and thus an erroneous direction of counting of the position counter is avoided.

Any phase error $\Delta\varphi$ between –90° und +90° will result in a shift of the counting pulses on the axis of the angle or, respectively, of the position (φ-axis) within the period of the *solid measure*. This effect is illustrated in Figure M.3 with a phase error $\Delta\varphi$ = 20°.

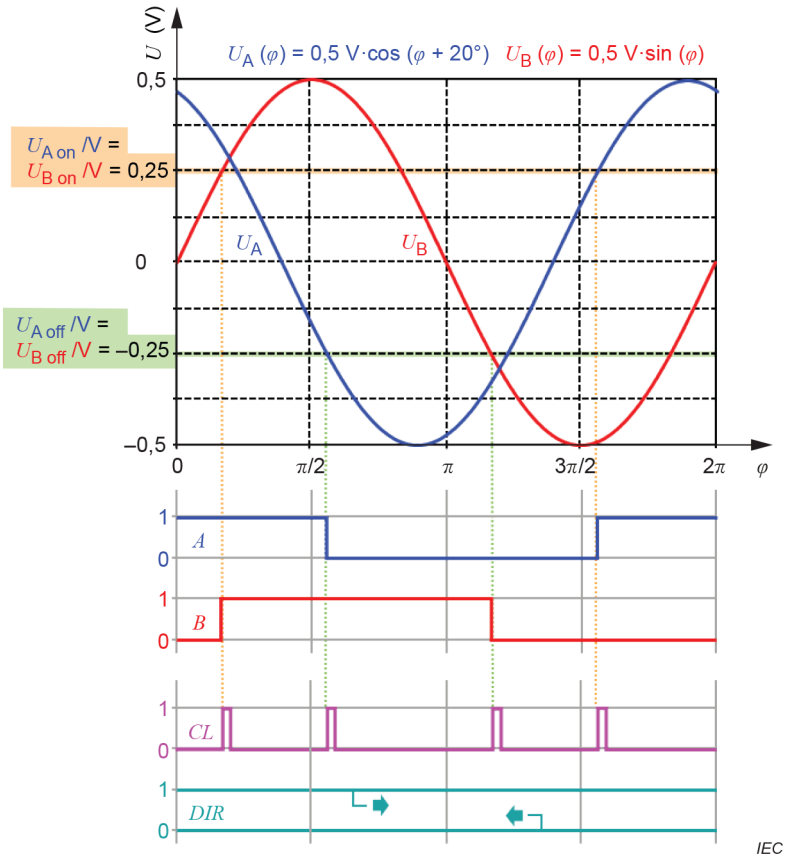


Figure M.3 – Counting pulse generation with a phase error of 20°

Compared with the faultless case (Figure M.2), the counting pulses CL of Figure M.3 do no longer exhibit the same distance, for example the period of the *solid measure* is no longer divided into four segments of equal size. Hence, the position resolution within the period of the *solid measure* is impeded and therefore the accuracy of the position calculation is decreased. If the fine resolution of four segments per period of the *solid measure* is to be used for *safety function(s)*, and if phase errors $\Delta\varphi$ undermining the specified position resolution cannot be excluded, phase errors exceeding the safe tolerance range have to be detected by appropriate diagnostic measures.

The position resolution within the period of the *solid measure* will also be impeded if these position values are determined with the aid of *interpolation*.

Due to commonly permitted tolerances, phasor length monitoring will detect phase errors only above a magnitude at which the fine resolution within the period of the *solid measure* is already faulty. Figure M.4 presents the Lissajous diagram of the signal voltages U_A and U_B with a phase error of 20° (orange) and, for comparison, of the faultless case (green dotted).

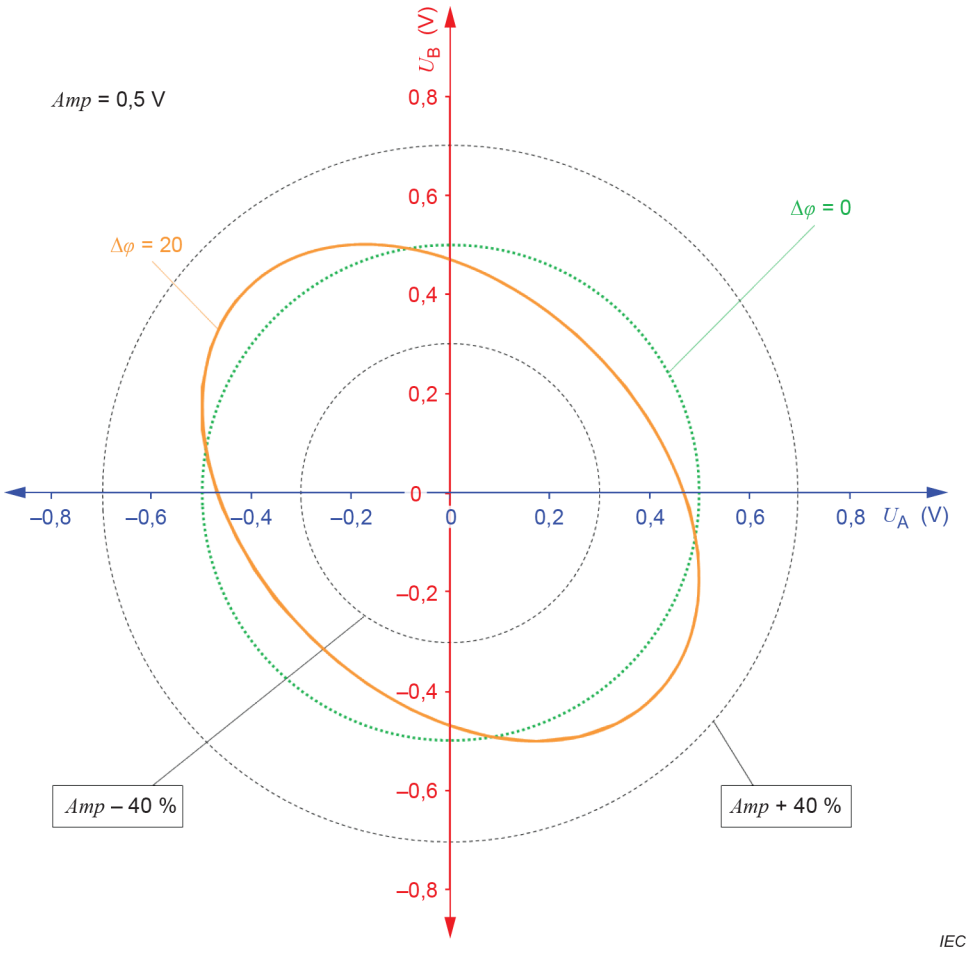


Figure M.4 – Lissajous diagram with a phase error $\Delta\varphi$ = 20°

In the example of Figure M.4, the nominal length Amp of the phasor is 0,5 V. The tolerance limits were assumed to be Amp – 40 % = 0,3 V and Amp + 40% = 0,7 V. The orange coloured Lissajous diagram, representing a phase error of 20°, remains within this permitted phasor length tolerance. Consequently, phasor length monitoring does not detect this phase error, whereas the fine resolution within the period of the *solid measure* is already faulty. In Figure M.3, this is recognizable by the unequal subdivision of the period by the counting pulses CL.

Phasor length monitoring will respond only in case of yet larger phase errors $\Delta\varphi$. If Amp_{min} is the lower limit of the phasor length Amp, then the response threshold $\Delta\varphi_{DT}$ (DT: detection threshold) is constituted by

$$\Delta\varphi_{DT} = \pm\arcsin\left[1-\left(\frac{Amp_{min}}{Amp}\right)^2\right]$$

assuming that the signal amplitudes of U_A and U_B are not readjusted within the period of the *solid measure*.

In the numerical example of Figure M.4, the tolerance range of the phasor length is ±40 % of the nominal value, Amp_{min}/Amp = 0,6. From this results, a calculatory response threshold of $\Delta\varphi_{DT}$ = ±39,8° in case of non-readjusted signal amplitudes. With a permitted tolerance of ±50 %, for example Amp_{min}/Amp = 0,5, the response threshold $\Delta\varphi_{DT}$ with non-readjusted amplitudes

would be ±48,6°. These absolute values of $\Delta\varphi_{DT}$ are well below the critical value of 90°, the exceedance of which would cause the quadrature decoder to output the wrong direction of movement. Thus, phasor length monitoring in its typical form will often be appropriate to detect a phase error slowly increasing from zero, before the quadrature decoder will signalise a wrong direction of movement.

To ensure the signal quality and the temporal signal stability, often a control of the amplitude of the sine and cosine signals is implemented. Here, the amplitude of the signals is affected in such a way as to keep $U_A^2 + U_B^2$ and likewise the phasor length constant or, at least, nearly constant. If the control is working virtually instantaneous, deviations of the phasor length will be compensated also within the period of the *solid measure*, even in case of fast movements. Possibly, herewith an elliptical Lissajous diagram as in Figure M.4 can be reshaped to an ideal circle. An amplitude control like this can make phase errors $\Delta\varphi$ up to a certain magnitude invisible for phasor length monitoring, whereas the phase error itself will not be corrected by the control. With increasing phase error $\Delta\varphi$, the Lissajous ellipse becomes more and more slim and, at least in case of a linear control characteristic, a real amplitude control will no longer be able to prevent undercutting the lower limit of the phasor length during passing through even one half of the period of the *solid measure*. In principle, this offers the chance for phasor length monitoring to detect the phase error before its absolute value approaches to the critical limit of 90°. Whether this applies can only be ascertained by an analysis of the behaviour of the actual amplitude control circuit.

In many cases, phasor length monitoring will be able to detect slowly increasing phase errors before the quadrature decoder outputs a false movement direction by the DIR signal and hence completely wrong positions are calculated. It is one of the aims of the static analysis to ensure this (see Annex L). As shown above, even phase errors below the phasor length monitoring's response threshold can impede the resolution of quadrants within the period of the *solid measure*.

M.3.3 Phase errors with absolute values > 90°

On phase errors $\Delta\varphi$ with absolute values between 90° and 270°, a quadrature decoder outputs the false direction of movement. At the same time, a phasor length within the permissible interval may be attained. By way of example with $\Delta\varphi = \pm 180°$, the phasor would constantly exhibit the nominal length corresponding to a circular Lissajous diagram, given that the amplitudes of the sine and the cosine signals would keep their nominal magnitude upon this phase error.

If a phase error increases slowly starting with zero, there can exist the possibility to detect it prior to determining the wrong movement direction, compare M.3.2. A separate case consists in a phase error with an absolute value between 90° and 270° arising abruptly, for example as the result of a mechanical stroke on the *Encoder(SR)* while the machine is switched off. If afterwards the phasor length meets the permitted range, there is no *fault* detection by phasor length monitoring, while at the same time the false direction of movement is output.

The FMEDA of the specific *Encoder(SR)* can clarify whether a phase error of this amount is possible, or whether its exclusion can be justified. If it cannot be excluded, it is to be determined whether the designated diagnostic measures will detect the *fault*. For example, if a phase error of this amount is always associated with a significant diminution of the signal amplitudes, it might be detected by phasor length monitoring. If this is not the case, additional measures are necessary.

M.4 Threshold errors of the square wave signal shapers

M.4.1 General

The conversion of a sine or cosine signal to a square wave signal is usually performed by a square wave shaper (Schmitt trigger) featuring a switching hysteresis. The latter is constituted by the difference of the two switching thresholds, for example by $U_H = U_{on} - U_{off}$ with $U_{on} > U_{off}$. The principle of generating a square wave signal S from a sine signal $U(\varphi)$ is illustrated in Figure M.5.

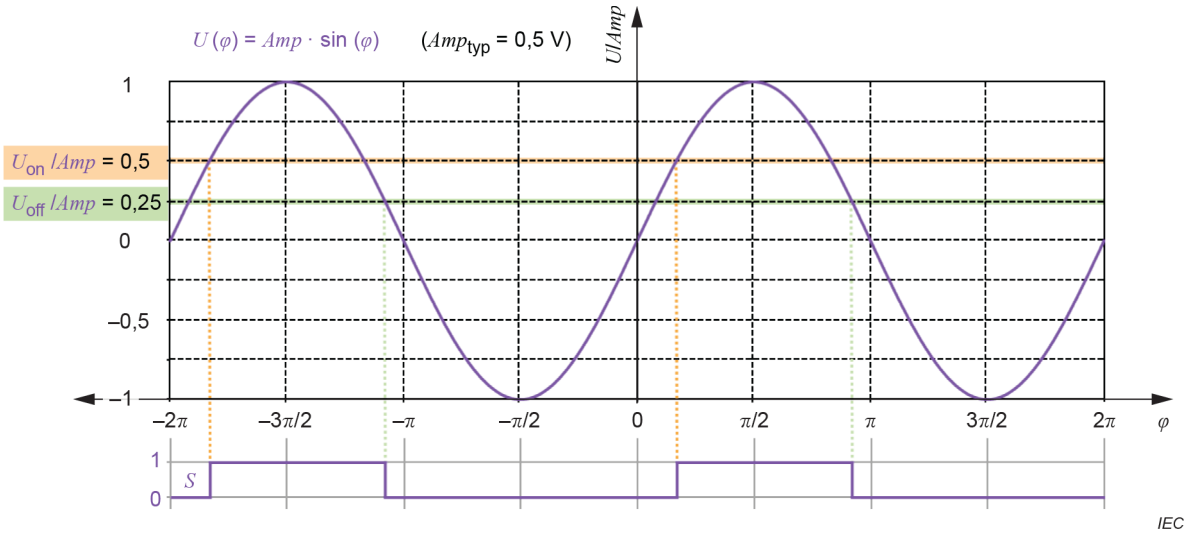


Figure M.5 – Square-wave signal generation by means of a Schmitt trigger

In the case of a sine-shaped oscillation with the amplitude Amp around zero, the following applies for the pulse duty factor PDF of the generated square wave signal:

$$PDF = \frac{1}{2} - \frac{\arcsin\left(\frac{U_{on}}{Amp}\right) + \arcsin\left(\frac{U_{off}}{Amp}\right)}{2\pi}.$$

In the example of Figure M.5, U_{on}/Amp = 0,5 and U_{off}/Amp = 0,25 result in the pulse duty factor PDF = 0,376 5. If the switching thresholds are arranged symmetrically around zero (the signal centre), for example in case of $U_{off} = -U_{on}$, it follows:

$$PDF_{symm} = \frac{1}{2}.$$

A symmetrical arrangement of the switching thresholds U_{on} and U_{off} around zero and, herewith, a pulse duty factor of 0,5 is a prerequisite for dividing the period of the *solid measure* into four equal segments by the counting pulses CL of the quadrature decoder. Beside the absence of phase errors, which have already been considered in Clause M.3, another requirement for the uniform subdivision is, that the switching thresholds for the cosine signal U_A and for the sine signal U_B are equal, for example that $U_{A\,on} = U_{B\,on}$ and $U_{A\,off} = U_{B\,off}$ applies. This faultless case is depicted in Figure M.2.

In M.4.2 and M.4.3, two examples of *faults* are considered with the switching thresholds deviating from the correct values.

M.4.2 Asymmetric switching thresholds

The example of Figure M.6 assumes ideal cosine and sine signals. The switching thresholds for pulse shaping of the cosine signal U_A are situated at ±0,25 V, thus symmetric with respect of the signal centre, whereas in case of the sine signal U_B only the switch-on threshold $U_{B\ on}$ is exhibiting the correct value 0,25 V. By contrast, the switch-off threshold $U_{B\ off}$ is situated at 0,125 V instead of –0,25 V.

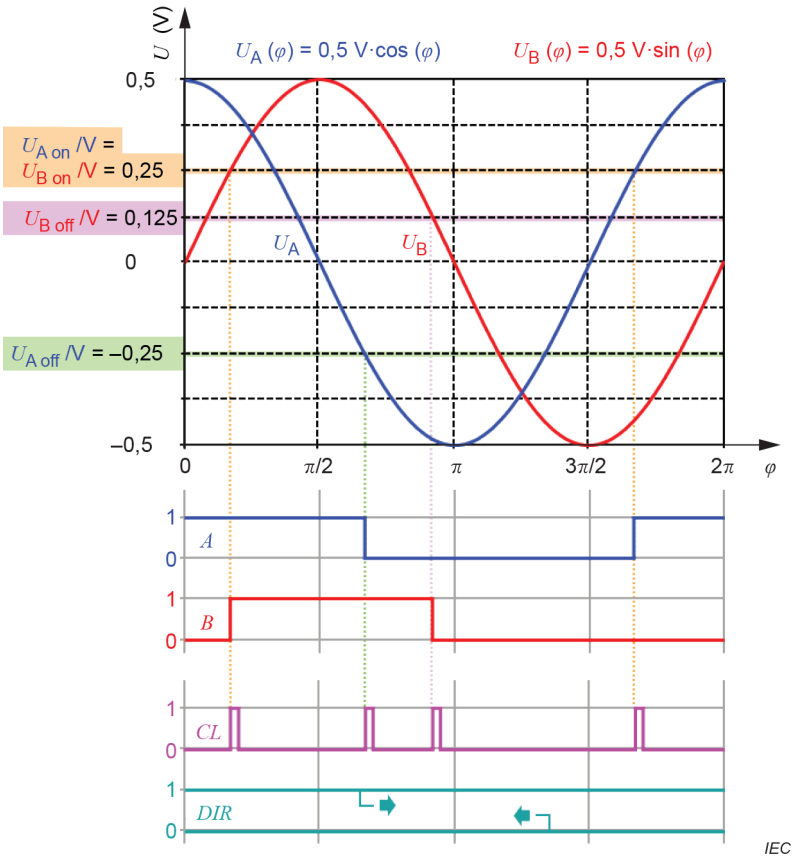


Figure M.6 – Counting pulse generation with asymmetric switching thresholds

The result of this *fault* is that the square wave signal B is no longer showing the correct pulse duty factor PDF = 0,5, but as in Figure M.5 the smaller value 0,376 5. At the same time, the switch-off slopes of signal B are shifted on the φ-axis. For this reason, every fourth of the counting pulses CL is shifted on the φ-Achse. A comparison with Figure M.2 indicates that in Figure M.6 the third of the CL pulses is shifted to the left. Hence, the period of the *solid measure* is no longer subdivided into four equal segments by the counting pulses and the fine resolution is impeded.

Of course, phasor length monitoring cannot detect this *fault* because it is only evaluating the analogue signals U_A and U_B. Appropriate redundant circuits and diagnostic measures are necessary.

M.4.3 Unequal switching hysteresis at the square wave shaping for sine and cosine

Again, the example of Figure M.7 assumes ideal cosine and sine signals. The switching thresholds for both of the analogue signals are situated symmetrically around the signal centre (0 V) which is also correct. Because of this, the generated square wave signals A and B exhibit the correct pulse duty factor PDF = 0,5. However, the switching hysteresis for the cosine and the sine signal is different. In case of the sine signal $U_{B\ H} = U_{B\ on} - U_{B\ off}$ = 0,5 V. For the cosine signal, the hysteresis is only $U_{A\ H} = U_{A\ on} - U_{A\ off}$ = 0,173 6 V.

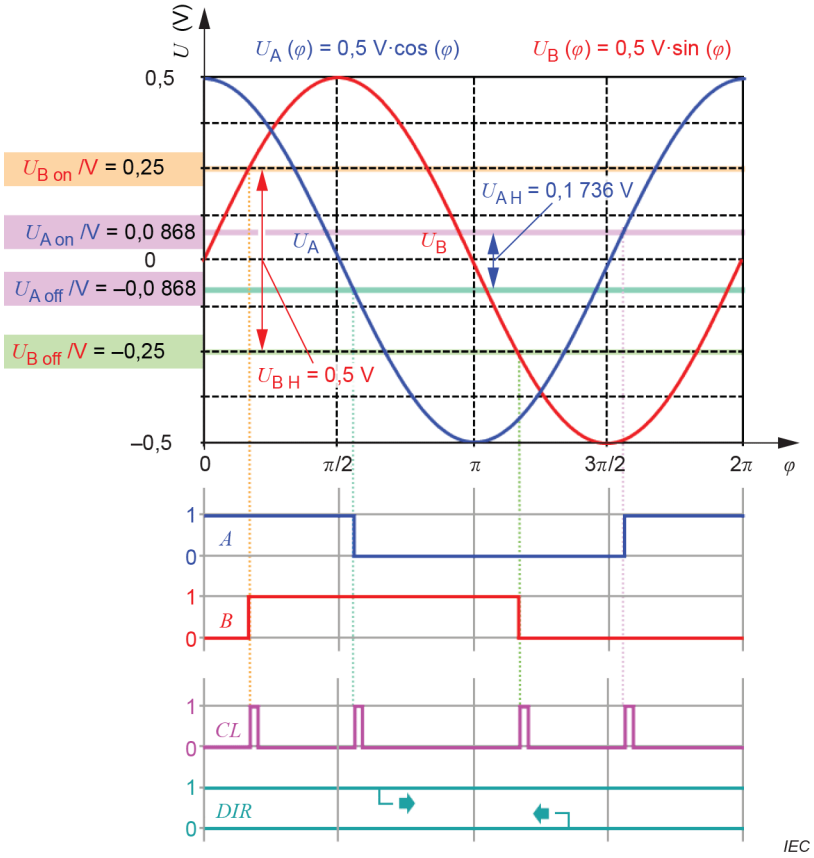


Figure M.7 – Counting pulse generation with unequal switching hysteresis

As a result of this difference in the hysteresis all switching slopes of the square wave signal A are shifted to the left, compared with the case where the hysteresis for either analogue signal is 0,5 V as in Figure M.2 and in Figure M.3. Thus, also in this example, the period of the *solid measure* will not be subdivided into four equal segments by the counting pulses CL and the fine resolution is impeded.

The voltage values in this example have been chosen with respect to the square wave signals A and B and the counting pulses CL in Figure M.3. The same situation like in Figure M.3 arises, where the cause of the pulse shift is a phase error of the analogue signals of 20°. A difference of the switching hysteresis of the pulse shapers can thus evoke a similar or even the same effect as a genuine phase error.

As well in this case, phasor length monitoring is unable to detect this *fault*, because it is only evaluating the analogue signals U_A and U_B. Again, appropriate redundant circuits and diagnostic measures are necessary.

Bibliography

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

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

[3] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

[4] IEC 61513, *Nuclear power plants – Instrumental and control systems important to safety – General requirements for systems*

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

[6] Systematic calculation of highly stressed bolted joints – Joints with one cylindrical bolt, Beuth Verlag GmbH, Am DIN-Platz, Burggrafenstraße 6, D 10787 Berlin [viewed 2020-10-21]. Available at https://www.beuth.de/en/technical-rule/vdi-2230-blatt-1/242566299

[7] Analytical Strength Assessment, VDMA Verlag GmbH, Lyoner Straße 18, D 60528 Frankfurt am Main [viewed 2020-10-21]. Available at http://www.vdmashop.de/Forschungshefte--FKM-/Analytical-Strength-Assessment-6-th-Edition.html

[8] ISO/TS 16281:2008, *Rolling bearings – Methods for calculating the modified reference rating life for universally loaded bearings*

[9] ANSI/ASA S2.62-2009, *Shock Test Requirements for Equipment in a Rugged Shock Environment, Reaffirmed by ANSI June 24, 2014*

[10] ISO 18431-4:2007, *Mechanical vibration and shock — Signal processing — Part 4: Shock-response spectrum analysis*

[11] Piersol, T. Paez: Harris' Shock and Vibration Handbook – Sixth Edition, MCGraw-Hill, New York, 2010

[12] IFA Report 2/2017e, *"Safety of machine controls to EN ISO 13849", Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung* [viewed 2020-10-21]. Available at www.dguv.de, webcode e89507

[13] SN 29500, *Ausfallraten Bauelemente, Erwartungswerte*. Siemens AG Corporate Technology, Technology & Innovation Management, CT TIM IR SI, Otto-Hahn-Ring 6, 81739 München, Deutschland, Tel.: +49 89 636-634154, michaela.pabst@siemens.com

[14] Safety Equipment Reliability Handbook [viewed 2020-10-21]. Available at: https://www.shopexida.com/products/safety-equipment-reliability-handbook-4th-edition

[15] Nonelectronics Parts Reliability Data, Reliability Analysis Center, NPRD-91, 1991

[16] IEC 61709:2017, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

[17] Static Analysis of signal evaluation and fault detection for rotary and position measuring systems for functional safety; Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung [viewed 2020-10-21]. Available at www.dguv.de, webcode d11973 (attachment to GS-IFA-M21 E)

[18] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

[19] ISO TR 23849:2010, *Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery*[2]

[20] IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

_____

2 This document has been withdrawn.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

ENTRAÎNEMENTS ÉLECTRIQUES DE PUISSANCE À VITESSE VARIABLE –

Partie 5-3: Exigences de sécurité – Exigences fonctionnelle, électrique et environnementale pour codeurs

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61800-5-3 a été établie par le sous-comité 22G: Systèmes d'entraînement électrique de puissance à vitesse variable (PDS), du comité d'études 22 de l'IEC: Systèmes et équipements électroniques de puissance.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
22G/431/FDIS	22G/434/RVD

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

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Les termes en *italique* sont définis à l'Article 3.

Une liste de toutes les parties de la série IEC 61800, publiées sous le titre général *Entraînements électriques de puissance à vitesse variable*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo 'colour inside' qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Du fait de l'automatisation, de la demande croissante de la production et de la réduction des efforts physiques produits par les opérateurs, les systèmes de commande des machines et des usines jouent un rôle croissant dans l'accomplissement de la sécurité globale. Ces systèmes de commande utilisent de plus en plus d'appareillages et de systèmes électriques/ électroniques/électroniques programmables complexes.

Les *codeurs* qui sont, par exemple, utilisés pour mesurer l'angle et la position de parties d'une machine dans le cadre d'applications relatives à la sécurité (*codeurs(SR)*) font partie des appareillages et systèmes les plus importants. A partir des signaux de sortie des *codeurs(SR)*, les *PDS(SR)* ou d'autres *unités d'évaluation* calculent, par exemple, la vitesse, l'accélération, la position absolue, etc., afin de réaliser leurs sous-fonctions de sécurité SLS, SLA, SLP et autres (voir Article 4 de l'IEC 61800-5-2:2016). Le *traitement des signaux* nécessaire pour réaliser certaines de ces *sous-fonctions de sécurité* peut également être inclus dans le *codeur(SR)*.

Exemples d'applications industrielles:

- machines-outils, robots, équipements d'essai en production, bancs d'essai;
- machines à papier, machines de production textile, calandres pour l'industrie du caoutchouc;
- lignes de processus des plastiques, de la production chimique ou métallique, moulins;
- machines de concassage du ciment, fours à ciment, mixeurs, centrifugeuses, machines d'extrusion;
- machines de forage;
- convoyeurs, machines de maniement de matériaux, équipements de levage (grues, portiques, etc.);
- pompes, ventilateurs, etc.

Les développeurs qui utilisent des *codeurs(SR)* peuvent également se référer au présent document pour d'autres applications, par exemple dans les centrales éoliennes.

Il convient que les utilisateurs du présent document aient connaissance du fait que certaines normes de type C applicables aux machines font actuellement référence à l'ISO 13849-1 pour les systèmes de commande relatifs à la sécurité. Dans ce cas, les fabricants de *codeurs(SR)* peuvent être invités à fournir des informations supplémentaires (par exemple, le *niveau de performance PL* et la catégorie) afin de faciliter l'intégration d'un *codeur(SR)* dans les systèmes de commande relatifs à la sécurité pour les machines concernées. Cela a été pris en compte lors de l'élaboration du présent document, et les indications correspondantes sont incluses, le cas échéant.

NOTE Les "normes de type C" sont définies dans l'ISO 12100 [1] comme des normes de sécurité des machines qui traitent des exigences de sécurité détaillées qui s'appliquent à une machine particulière ou à un groupe de machines particulier.

De nombreuses situations témoignent de l'utilisation de systèmes de commande qui intègrent un *codeur(SR)* en tant qu'élément de mesures de sécurité, par exemple, qui ont été installés à des fins de réduction du risque. La réduction de la vitesse au démarrage est un cas classique de protection du personnel dans le cas d'une situation dangereuse provoquée par des mouvements rapides inattendus de parties de la machine. Le présent document spécifie une méthodologie qui permet d'identifier la contribution apportée par un *codeur(SR)* aux *sous-fonctions* de sécurité identifiées, de réaliser la conception appropriée du *codeur(SR)* et de vérifier qu'elle satisfait aux performances exigées.

Les mesures indiquées permettent de coordonner la performance de sécurité du *codeur(SR)* avec la réduction attendue du risque en prenant en compte les probabilités et les conséquences de ses *anomalies* systématiques et aléatoires.

ENTRAÎNEMENTS ÉLECTRIQUES DE PUISSANCE À VITESSE VARIABLE –

Partie 5-3: Exigences de sécurité – Exigences fonctionnelle, électrique et environnementale pour codeurs

1 Domaine d'application

La présente partie de l'IEC 61800, qui est une norme de produit, spécifie des exigences et donne des recommandations pour la conception et le développement, l'intégration et la validation des *codeurs* relatifs à la sécurité (*codeurs(SR)*), au regard de leur *sécurité fonctionnelle*, de leur sécurité électrique et des conditions d'environnement. Elle s'applique aux *codeurs(SR)* qui sont des capteurs qui font partie d'un *PDS(SR)*.

NOTE 1 Le terme "intégration" se rapporte au *codeur(SR)* lui-même, non pas à son incorporation dans l'application relative à la sécurité.

Le présent document peut également servir de référence et être utilisé pour les *codeurs(SR)* dans le cadre de toute autre application relative à la sécurité, par exemple la surveillance de position relative à la sécurité.

NOTE 2 Le présent document spécifie uniquement les exigences complémentaires concernant la *sécurité fonctionnelle*, la sécurité électrique et les conditions d'environnement qui ne sont pas clairement fournies dans d'autres parties de la série IEC 61800.

Le présent document est applicable lorsque la *sécurité fonctionnelle* d'un *codeur* est revendiquée et que le *codeur(SR)* fonctionne principalement en mode à sollicitation élevée ou en mode continu.

NOTE 3 Bien qu'il soit possible qu'un *codeur(SR)* fonctionne en mode à faible sollicitation, le présent document traite plus particulièrement du mode à sollicitation élevée et du mode continu. Les *sous-fonctions de sécurité* mises en œuvre pour le mode à sollicitation élevée ou pour le mode continu peuvent également être utilisées pour le mode à faible sollicitation. Des exigences relatives au mode à faible sollicitation sont données dans l'IEC 61508 (toutes les parties) [2]. Des recommandations relatives à l'estimation de la valeur PFD_{moy} (probabilité moyenne de *défaillance dangereuse* en cas de sollicitation) sont données à l'Annexe F de l'IEC 61800-5-2:2016.

Les exigences de l'IEC 61800-5-2:2016 concernant les *PDS(SR)* s'appliquent aux *codeurs(SR)*, selon le cas. Le présent document comprend des exigences supplémentaires ou différentes pour les *codeurs(SR)*. Il expose des considérations relatives à la sécurité des *codeurs(SR)*, prises dans le cadre de l'IEC 61508 (toutes les parties), et présente des exigences pour les *codeurs(SR)* en tant que sous-systèmes d'un système relatif à la sécurité. Il est destiné à faciliter la réalisation des parties électriques/électroniques/électroniques programmables (E/E/PE) d'un *codeur(SR)* en liaison avec la performance de sécurité d'une ou de plusieurs *sous-fonctions de sécurité* d'un *codeur(SR)*.

En se référant aux exigences normatives du présent document, les fabricants et les fournisseurs de *codeurs(SR)* indiquent aux utilisateurs (intégrateur de système, fabricant original de l'équipement) la performance de sécurité pour leur *codeur(SR)*. Ceci facilite l'incorporation d'un *codeur(SR)* dans un système de commande relatif à la sécurité qui applique les principes de l'IEC 61508 (toutes les parties), et éventuellement ses applications sectorielles spécifiques (par exemple l'IEC 61511 (toutes les parties) [3], l'IEC 61513 [4], l'IEC 62061 [5] ou l'ISO 13849-1 et l'ISO 13849-2 (voir Article 2)).

Lorsque les exigences du présent document sont appliquées, les exigences correspondantes de l'IEC 61508 (toutes les parties) nécessaires à un *codeur(SR)* sont remplies.

Le présent document ne spécifie pas d'exigences pour:

- les propriétés fonctionnelles d'un *codeur(SR)* sans aucun lien avec la sécurité;
- l'analyse des *dangers* et des risques pour une application particulière;
- l'identification des *sous-fonctions de sécurité* pour l'application concernée;
- l'attribution initiale des *SIL* pour ces *sous-fonctions de sécurité*;
- l'équipement entraîné, à l'exception des aménagements de l'interface;
- des *dangers* secondaires (issus par exemple d'une défaillance d'un procédé de production ou de fabrication);
- le procédé de fabrication du *codeur(SR)*;
- la validité des signaux et des commandes du *codeur(SR)*; et
- les considérations de sécurité (par exemple, cybersécurité ou sécurité d'accès au *codeur(SR)*).

NOTE 4 Les exigences en *sécurité fonctionnelle* d'un *codeur(SR)* dépendent de l'application et peuvent être considérées comme une partie de l'appréciation globale du risque de l'installation. Lorsque le fournisseur du *codeur(SR)* n'est pas responsable de l'équipement entraîné, il incombe au concepteur de l'installation de réaliser l'appréciation du risque et de spécifier les exigences fonctionnelles et d'intégrité de sécurité du *codeur(SR)*.

Le présent document s'applique aux *codeurs(SR)* qui comportent des *sous-fonctions de sécurité* dont le *SIL* n'est pas supérieur au *SIL* 3.

Le présent document fournit des informations supplémentaires pour les *codeurs(SR)* qui revendiquent la conformité à l'ISO 13849-1:2015.

La Figure 1 représente l'installation et les parties fonctionnelles d'un *PDS(SR)*, y compris le *codeur(SR)* (capteur), qui sont prises en compte dans le présent document.

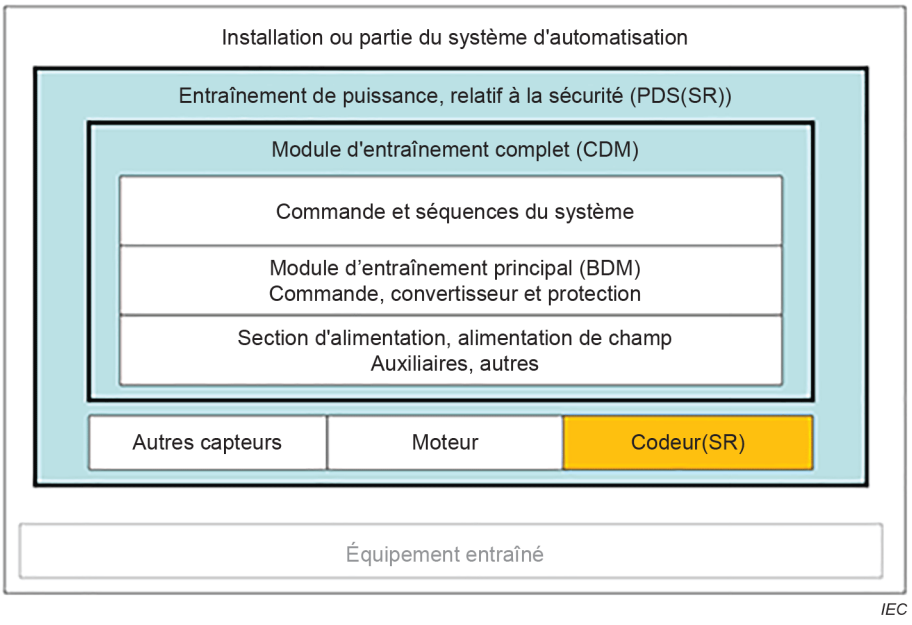


Figure 1 – Contexte du *codeur(SR)*

La Figure 1 est une représentation logique (et non la description physique) d'un *PDS(SR)*.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60068-2-1, *Essais d'environnement – Partie 2-1: Essais – Essai A: Froid*

IEC 60068-2-47, *Essais d'environnement – Partie 2-47: Essais – Fixation de spécimens pour essais de vibrations, d'impacts et autres essais dynamiques*

IEC 60335-1, *Household and similar electrical appliances – Safety – Part 1: General requirements* (disponible en anglais seulement)

IEC 60947-5-2:2019, *Appareillage à basse tension – Partie 5-2: Appareils et éléments de commutation pour circuits de commande – Détecteurs de proximité*

IEC 61000-6-7:2014, *Compatibilité électromagnétique (CEM) – Partie 6-7: Normes génériques – Exigences d'immunité pour les équipements visant à exercer des fonctions dans un système lié à la sécurité (sécurité fonctionnelle) dans des sites industriels*

IEC 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61800-1:1997, *Entraînements électriques de puissance à vitesse variable – Partie 1: Exigences générales – Spécifications de dimensionnement pour systèmes d'entraînement de puissance à vitesse variable en courant continu et basse tension*

IEC 61800-5-1:2007, *Entraînements électriques de puissance à vitesse variable – Partie 5-1: Exigences de sécurité – Electrique, thermique et énergétique*
IEC 61800-5-1:2007/AMD1:2016

IEC 61800-5-2:2016, *Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnelle*

IEC 62368-1:2018, *Equipements des technologies de l'audio/vidéo, de l'information et de la communication – Partie 1: Exigences de sécurité*

ISO 13849-1:2015, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 13849-2:2012, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurit – Partie 2: Validation*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

Le Tableau 1 présente une liste des termes et définitions.

Tableau 1 – Liste des termes

3.1	*codeur*	3.19	*sécurité fonctionnelle* *FS*
3.2	*codeur(SR)*	3.20	*fonction de sécurité*
3.3	*unité d'interface*	3.21	*sous-fonction de sécurité*
3.4	*unité d'évaluation*	3.22	*anomalie*
3.5	*PDS(SR)*	3.23	*défaillance dangereuse*
3.6	*plage de tolérances*	3.24	*tolérance aux anomalies du matériel* *HFT*
3.7	*interpolation*	3.25	*tolérance au premier défaut*
3.8	*indicateur statique*	3.26	*niveau d'intégrité de sécurité* *SIL*
3.9	*fixation mécanique*	3.27	*capacité SIL*
3.10	*élément de connexion mécanique*	3.28	*niveau de performance* *PL*
3.11	*accouplement arbre-rotor*	3.29	*couverture du diagnostic* *DC*
3.12	*accouplement statorique*	3.30	*proportion de défaillances en sécurité* *SFF*
3.13	*blocage de palier*	3.31	*fréquence moyenne de défaillance dangereuse* *PFH*
3.13.1	*blocage de palier spontané*	3.32	*durée moyenne de fonctionnement avant défaillance dangereuse* $MTTF_D$
3.13.2	*blocage de palier progressif*	3.33	*temps de sécurité du processus*
3.14	*point de mesure de la température de fonctionnement*	3.34	*détection de défaut idéale*
3.15	*plage de températures de fonctionnement*	3.35	*FMEDA quantitative*
3.16	*très basse tension* *TBT*	3.36	*FMEDA qualitative*
3.17	*circuit de TBT de protection* *circuit de TBTP*	3.37	*évaluation des signaux*
3.18	*classe de tension déterminante* *CTD*	3.38	*traitement des signaux*

3.1
codeur
dispositif électromécanique qui génère un signal de sortie analogique ou numérique en réponse à la position d'une pièce mobile

Note 1 à l'article: Dans le cadre du présent document, la définition de "*codeur*" comprend les résolveurs et tous les types de capteurs de signal de retour de moteur.

Note 2 à l'article: L'Annexe A fournit des exemples de types de *codeurs*.

3.2
codeur(SR)
codeur fournissant des *sous-fonctions de sécurité*

Note 1 à l'article: La ou les *sous-fonction(s) de sécurité* du *codeur(SR)* permettent l'exécution de sous-fonctions de sécurité d'un *PDS(SR)* ou de toute autre application de sécurité.

Note 2 à l'article: Cette définition est issue de l'IEC 61800-5-2:2016, 3.16

3.3
unité d'interface
sous-ensemble électronique distinct du *codeur(SR)* utilisé pour convertir les signaux

Note 1 à l'article: La fonctionnalité de l'*unité d'interface* peut être intégrée au *codeur(SR)*.

3.4
unité d'évaluation
équipement externe dans lequel le signal de sortie du *codeur(SR)* est évalué

Note 1 à l'article: Les *PDS(SR)*, les éléments de sécurité utilisés pour contrôler la vitesse ou les arrêts sont des exemples d'*unités d'évaluation*.

Note 2 à l'article: L'*unité d'évaluation* peut également réaliser des mesures diagnostiques pour le *codeur(SR)*.

3.5
PDS(SR)
entraînement électrique de puissance à vitesse variable, fournissant des sous-fonctions de sécurité

[SOURCE: IEC 61800-5-2:2016, 3.16]

3.6
plage de tolérances
intervalle entre les limites de tolérance supérieure et inférieure

Note 1 à l'article: La *plage de tolérances* est exprimée en unités de mesure et est appliquée aux *codeurs(SR)* avec signaux de sortie analogiques et numériques.

Note 2 à l'article: La plage de tolérances T(R) est habituellement donnée sous la forme T(R): −X à +Y, avec T(R) = X + Y; (par exemple -5 mm à +5 mm, 0° à +10°, etc.).

Note 3 à l'article: Il convient que la plage de tolérances tienne compte de la précision et de la résolution.

3.7
interpolation
méthode mathématique d'amélioration de la résolution

EXEMPLE Formation de l'arc tangente du rapport des signaux analogiques sinus et cosinus (signaux A/B).

3.8
indicateur statique
composant fournissant un motif codé utilisé pour déterminer une position mécanique

EXEMPLE Disque optique, bande magnétique.

Note 1 à l'article: Echelle, disque, bague, bande sont d'autres termes qui désignent un *indicateur statique*.

3.9
fixation mécanique
raccordement mécanique destiné à la transmission de charge entre éléments de construction ou à la fixation d'éléments de construction

Note 1 à l'article: La transmission de charge peut, par exemple, se produire

- entre le stator du moteur et le stator du *codeur(SR)*;
- entre l'arbre du moteur et l'arbre du *codeur(SR)* rotatif;
- entre une partie fixe de la machine et une partie fixe du *codeur(SR)*; ou
- entre une partie mobile de la machine et une partie mobile du *codeur(SR)*.

Note 2 à l'article: La transmission de charge peut également se produire au sein du *codeur(SR)*.

Note 3 à l'article: Les *fixations mécaniques* sont généralement constituées par des assemblages boulonnés, des clavettes d'ajustement, des joints-clés et des fentes de jonction.

3.10
élément de connexion mécanique
pièce mécanique rigide ou flexible utilisée pour la transmission de charge entre *fixations mécaniques*

Note 1 à l'article: Les *éléments de connexion mécaniques* sont généralement appelés "accouplements".

Note 2 à l'article: Les accouplements peuvent également fournir une compensation des tolérances mécaniques lors de la fixation ou du fonctionnement.

Note 3 à l'article: Les accouplements sont généralement désignés en tant qu'*accouplement arbre-rotor* ou qu'*accouplement statorique*.

3.11
accouplement arbre-rotor
élément de connexion entre l'arbre d'un *codeur(SR)* rotatif et un arbre entraîné

Note 1 à l'article: L'*accouplement arbre-rotor* est situé entre les extrémités des arbres.

Note 2 à l'article: La tâche de l'*accouplement arbre-rotor* est de compenser les tolérances mécaniques lors de la fixation ou du fonctionnement.

Note 3 à l'article: L'*accouplement arbre-rotor* est généralement réalisé comme un accouplement à soufflet, un accouplement à mâchoire, un accouplement à fente ou un accouplement laminaire.

3.12
accouplement statorique
partie d'un *codeur(SR)* rotatif utilisée pour fixer le *codeur(SR)* par rapport au point de montage

Note 1 à l'article: La tâche de l'*accouplement statorique* est de compenser les tolérances mécaniques lors de la fixation ou du fonctionnement.

Note 2 à l'article: L'*accouplement statorique* est fixé à la collerette ou au boîtier.

Note 3 à l'article: L'*accouplement statorique* est également appelé "support de couple".

Note 4 à l'article: L'*accouplement statorique* peut également être situé dans le *codeur(SR)*.

3.13
blocage de palier
situation dans laquelle le couple nécessaire à la rotation du palier expose le *codeur(SR)* à des forces ou à des couples supérieurs à ceux pris en compte lors de la conception et du développement

3.13.1
blocage de palier spontané
blocage de palier survenant soudainement, sans aucune modification préalable des propriétés du palier

Note 1 à l'article: La *détection de défaut* avant le *blocage de palier spontané* n'est pas possible.

3.13.2
blocage de palier progressif
blocage de palier survenant progressivement, précédé d'une modification des propriétés du palier

Note 1 à l'article: Il peut être possible de détecter l'*anomalie* à temps et de passer à un état de sécurité avant le blocage du palier.

Note 2 à l'article: Un *blocage de palier progressif* peut être dû à l'usure ou à la fatigue.

3.14
point de mesure de la température de fonctionnement
point sur la surface du *codeur(SR)* pour la mesure de la température de fonctionnement

3.15
plage de températures de fonctionnement
limites de température entre lesquelles la valeur de mesure ne dépasse pas les limites de défaut données

3.16
très basse tension
TBT
tension n'excédant pas 50 V c.a. efficace et 120 V c.c.

Note 1 à l'article: Tension ondulée efficace n'excédant pas 10 % de la composante continue.

[SOURCE: IEC 61800-5-1:2007, 3.9, modifié – La Note 2 a été supprimée.]

3.17
circuit de TBT de protection
circuit de TBTP
circuit électrique ayant les caractéristiques suivantes:

- la tension ne dépasse pas continuellement une *TBT* en cas de *défaut* unique ou dans des conditions normales;
- il existe des séparations de protection des circuits autres que des *TBTP* ou TBTS;
- il existe des moyens de mise à la terre du *circuit TBTP* ou de ses parties conductrices accessibles ou des deux à la fois

[SOURCE: IEC 61800-5-1:2007; 3.21]

3.18
classe de tension déterminante
CTD
classification de la gamme de tensions utilisée afin de déterminer les mesures de protection contre les chocs électriques

Note 1 à l'article: Selon le Tableau 3 de l'IEC 61800-5-1:2007, les limites de tension de la *CTD* A sont 25 V AC, 35,4 V $AC_{crête}$ et 60 V DC.

[SOURCE: IEC 61800-5-1:2007, 3.7, modifié – La Note 1 à l'article a été ajoutée.]

3.19
sécurité fonctionnelle
FS
sous-ensemble de la sécurité globale se rapportant au *codeur(SR)* qui dépend du fonctionnement correct des *parties du codeur(SR) relatives à la sécurité* et des dispositifs externes de réduction de risque

Note 1 à l'article: Le présent document ne prend en considération que les aspects de la définition de la *sécurité fonctionnelle* qui dépendent du fonctionnement correct du *codeur(SR)*.

Note 2 à l'article: Le terme abrégé "FS" est dérivé du terme anglais développé correspondant "functional safety".

[SOURCE: IEC 61800-5-2:2016, 3.11, modifié – Le terme abrégé "FS" a été ajouté, et le terme "*PDS(SR)*" a été remplacé par "*codeur(SR)*".]

3.20
fonction de sécurité
fonction à réaliser par un système relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'équipement ou de la machine, par rapport à un événement dangereux spécifique

[SOURCE: IEC 61800-5-2:2016, 3.22, modifié – Les mots "entraîné(e) par le *PDS(SR)*" ont été supprimés.]

3.21
sous-fonction de sécurité
fonction(s), selon une performance de sécurité spécifiée, dont tout ou partie est à réaliser par un *codeur(SR)* et qui vise(nt) à maintenir la sécurité de l'installation ou à prévenir l'émergence de toute condition *dangereuse* dans l'installation

Note 1 à l'article: Dans de rares cas, la *fonction de sécurité* de l'application complète est exclusivement mise en œuvre au sein du *codeur(SR)*. Dans ce cas, la *fonction de sécurité* est toujours appelée "*sous-fonction de sécurité*" dans le présent document.

[SOURCE: IEC 61800-5-2:2016, 3.23, modifié – Le terme "*PDS(SR)*" a été remplacé par "*codeur(SR)*". Les mots "<d'un PDS(SR)>" et l'exemple de la Note à l'article ont été supprimés.]

3.22
anomalie
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

[SOURCE: IEC 61508-4:2010, 3.6.1, modifié – La note a été supprimée.]

3.23
défaillance dangereuse
défaillance d'un composant et/ou sous-système et/ou système ayant une influence sur la mise en œuvre de la *sous-fonction de sécurité* qui:

- provoque la défaillance d'une *sous-fonction de sécurité* d'un *codeur(SR)* de sorte que l'équipement ou la machine est mis(e) dans un état dangereux ou potentiellement dangereux; ou
- diminue la probabilité que la *sous-fonction de sécurité* fonctionne correctement

[SOURCE: IEC 61800-5-2:2016, 3.5, modifié – Le terme "*PDS(SR)*" a été remplacé par "*codeur(SR)*", et les mots "entraîné(e) par le *PDS(SR)*" ont été supprimés.]

3.24
tolérance aux anomalies du matériel
HFT
aptitude d'un *codeur(SR)* à continuer d'accomplir une fonction requise en présence d'*anomalies* ou d'erreurs du matériel

Note 1 à l'article: Selon l'IEC 61800-5-2:2016, la *HFT* donne les exigences concernant l'intervalle d'essai de diagnostic. De plus, la *HFT* indiquée en 6.2.3.1 de l'IEC 61800-5-2:2016 est l'un des attributs utilisés pour déterminer une limite supérieure pour le *niveau d'intégrité de sécurité* (*SIL*).

Note 2 à l'article: Cette définition est issue de l'IEC 61508-4:2020, 3.6.3.

Note 3 à l'article: Le terme abrégé "HFT" est dérivé du terme anglais développé correspondant "hardware fault tolerance".

3.25
tolérance au premier défaut
aptitude d'une unité fonctionnelle à continuer d'accomplir une fonction requise en présence d'une *anomalie* ou d'une erreur

[SOURCE: IEC 61508-4:2010, 3.6.3, modifié – L'adjectif "premier" a été ajouté dans le terme, et les mots "d'*anomalies* ou d'erreurs" ont été remplacés par "d'une *anomalie* ou d'une erreur".]

3.26
niveau d'intégrité de sécurité
SIL
niveau discret (un parmi trois possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité d'une *sous-fonction de sécurité* attribuée (tout ou partie) à un *codeur(SR)*

Note 1 à l'article: Le niveau 3 d'*intégrité de sécurité* possède le plus haut degré d'intégrité; le niveau 1 possède le plus bas.

Note 2 à l'article: Le *SIL* 4 n'est pas pris en compte dans le présent document, car il ne s'applique pas aux exigences de réduction des risques qui sont normalement associées aux *codeurs(SR)*. Pour les exigences relatives au *SIL* 4, voir l'IEC 61508.

Note 3 à l'article: Plusieurs conventions d'écriture sont utilisées pour *SIL*x. Dans l'ensemble du présent document, la forme *SIL* x est utilisée.

Note 4 à l'article: Le terme abrégé "SIL" est dérivé du terme anglais développé correspondant "safety integrity level".

[SOURCE: IEC 61800-5-2:2016, 3.25, modifié – Le terme "*PDS(SR)*" a été remplacé par "*codeur(SR)*" et la Note 4 à l'article a été supprimée.]

3.27
capacité SIL
SIL maximal pouvant être atteint par la conception d'un *codeur(SR)*, en tenant compte de l'intégrité de sécurité systématique et des contraintes architecturales ayant une influence sur l'intégrité de sécurité du matériel

Note 1 à l'article: Une *capacité SIL* différente peut être associée à chacune des *sous-fonctions de sécurité* désignées qu'un *codeur(SR)* est censé assurer.

Note 2 à l'article: La *capacité SIL* inclut la capabilité systématique, le respect des contraintes architecturales et le taux de défaillance du matériel ou la valeur de la *PFH*.

[SOURCE: IEC 61800-5-2:2016, 3.28, modifié – Le terme "*PDS(SR)*" a été remplacé par "*codeur(SR)*".]

3.28
niveau de performance
PL
niveau discret d'aptitude de parties relatives à la sécurité à réaliser une *fonction de sécurité* dans des conditions prévisibles

Note 1 à l'article: Voir 4.5.1 de l'ISO 13849-1:2015.

Note 2 à l'article: Le terme abrégé "PL" est dérivé du terme anglais développé correspondant "performance level".

[SOURCE: ISO 13849-1:2015, 3.1.23]

3.29
couverture du diagnostic
DC

proportion de *défaillances dangereuses* détectées par les essais de diagnostic automatiques

Note 1 à l'article: Cette couverture peut également être exprimée par le rapport entre la somme des taux de *défaillance dangereuse* λ_{DD} détectés et la somme des taux de *défaillance dangereuse* totaux λ_D: $DC = \Sigma\lambda_{DD}/\Sigma\lambda_D$.

Note 2 à l'article: La *couverture du diagnostic* peut se rapporter à tout ou partie du système relatif à la sécurité. Elle peut, par exemple, être disponible pour les capteurs et/ou les *sous-systèmes* logiques et/ou le *sous-système* de sortie.

Note 3 à l'article: Le terme abrégé "DC" est dérivé du terme anglais développé correspondant "diagnostic coverage".

[SOURCE: IEC 61800-5-2:2016, 3.6, modifié – La Note 3 à l'article a été supprimée.]

3.30
proportion de défaillances en sécurité
SFF
propriété d'un composant et sous-systèmes relatifs à la sécurité définie par le rapport des taux de défaillance moyens des défaillances en sécurité et dangereuses détectées et des *défaillances* en sécurité et *dangereuses*

Note 1 à l'article: Ce rapport est représenté par l'équation suivante: $SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

Note 2 à l'article: Voir Annexe C de l'IEC 61508-2:2010.

Note 3 à l'article: Le terme abrégé "SFF" est dérivé du terme anglais développé correspondant "safe failure fraction".

[SOURCE: IEC 61800-5-2:2016, 3.20, modifié – La Note 3 à l'article a été supprimée.]

3.31
fréquence moyenne de défaillance dangereuse
PFH
fréquence moyenne d'une *défaillance dangereuse* d'un *codeur(SR)* pour réaliser la *sous-fonction de sécurité* spécifiée pendant une période de temps donnée

Note 1 à l'article: Dans l'IEC 62061, l'abréviation PFH_D est utilisée.

[SOURCE: IEC 61800-5-2:2016, 3.17, modifié – Le terme "PDS(SR)" a été remplacé par "*codeur(SR)*" et la Note 2 à l'article a été supprimée.]

3.32
durée moyenne de fonctionnement avant défaillance dangereuse
$MTTF_D$
espérance mathématique de la durée de fonctionnement avant défaillance dangereuse

[SOURCE: ISO 13849-1:2015, 3.1.25]

3.33
temps de sécurité du processus
durée entre l'occurrence d'une défaillance du *codeur(SR)*, avec potentialité d'entraîner un événement dangereux, et le moment auquel l'action doit être accomplie pour empêcher l'occurrence de l'événement dangereux

[SOURCE: IEC 61508-4:2010, 3.6.20, modifié – La formulation a été simplifiée.]

3.34
détection de défaut idéale
détection de toutes les *défaillances dangereuses* et obtention d'un état de sécurité dans le *temps de sécurité du processus*

Note 1 à l'article: La "*détection de défaut idéale*" est une méthode appliquée pour transmettre la propriété de *tolérance au premier défaut* aux (sous-)systèmes dont la *HFT* est de 0. La *tolérance au premier défaut* est une condition nécessaire pour les catégories 3 et 4, conformément à l'ISO 13849-1. Une description détaillée de la *détection de défaut idéale* est donnée à l'Annexe J.

3.35
FMEDA quantitative
technique d'analyse systématique permettant d'identifier les taux de défaillance, les modes de défaillance et les capacités de diagnostic des blocs fonctionnels

Note 1 à l'article: La *FMEDA* (*Failure Modes, Effects and Diagnostics Analysis*, analyse des modes de défaillance, des effets et du diagnostic) *quantitative* fournit les données d'entrée pour la quantification (calcul de la *PFH*, de la *SFF*, de la $MTTF_D$ (si la conformité à l'ISO 13849-1:2015 est revendiquée)). Elle est effectuée séparément pour chaque bloc fonctionnel et permet de classer les taux de défaillance de tous les composants du bloc comme sûrs (S), dangereux (D), dangereux détectables (DD) et dangereux non détectables (DU, *dangerous undetectable*).

3.36
FMEDA qualitative
technique d'analyse systématique permettant d'identifier les défaillances systématiques des blocs fonctionnels

Note 1 à l'article: La *FMEDA* (*Failure Modes, Effects and Diagnostics Analysis*, analyse des modes de défaillance, des effets et du diagnostic) *quantitative* est utilisée pour révéler les possibles effets et scénarios systématiques susceptibles d'altérer la performance de la *sous-fonction de sécurité*. Elle permet de vérifier, pour tous les composants, que les défaillances ayant un effet préjudiciable sur la *sous-fonction de sécurité* sont détectées et maîtrisées par les diagnostics spécifiés et que, dans le cas concerné, une défaillance particulière peut être justifiablement exclue. La FMEDA est notamment utilisée pour vérifier la *tolérance au premier défaut* d'un *codeur(SR)* (voir 8.4).

Note 2 à l'article: Dans le cadre de l'analyse statique (voir Annexe L), la *FMEDA qualitative* est utilisée pour vérifier que tous les scénarios d'*anomalie* potentiels sont maîtrisés par les diagnostics spécifiés (voir L.7).

3.37
évaluation des signaux
évaluation des signaux de sortie du *codeur(SR)* en vue de l'exécution d'une *fonction de sécurité*

Note 1 à l'article: Voir également 3.38.

3.38
traitement des signaux
évaluation des signaux et essai d'intégrité des signaux de sortie afin de détecter des *anomalies* dans le *codeur(SR)* (diagnostic)

Note 1 à l'article: La relation entre le *traitement des signaux*, l'*évaluation des signaux* et le diagnostic est la suivante: *traitement des signaux* = *évaluation des signaux* + diagnostic.

4 *Sous-fonctions de sécurité*

4.1 Généralités

L'Article 4 décrit les fonctions d'un *codeur(SR)* qui peuvent être désignées comme relatives à la sécurité par le fournisseur du *codeur(SR)*. Cependant, la liste des *sous-fonctions de sécurité* désignées à l'Article 4 n'est pas exhaustive.

Les mesures techniques exigées pour mettre en œuvre ces fonctions dépendent de la *capacité SIL* exigée (et de la capacité *PL* si la conformité à l'ISO 13849-1 est revendiquée) incluant la probabilité de défaillance matérielle dangereuse exigée, comme indiqué dans la *spécification des exigences de sécurité*. Les mesures techniques sont décrites à l'Article 6.

Les noms des *sous-fonctions de sécurité* comportent l'adjectif "sûre" afin d'indiquer que ces fonctions peuvent être utilisées dans une application relative à la sécurité sur les bases d'une analyse (par exemple, une analyse du risque) de l'application spécifique, permettant ainsi au *codeur(SR)* de mettre en œuvre les fonctions de sécurité et d'assurer leur intégrité.

Les *sous-fonctions de sécurité* du *codeur(SR)* peuvent être utilisées pour mettre en œuvre la ou les sous-fonctions de sécurité d'un *PDS(SR)*.

4.2 Position incrémentale sûre (SIP, *safe incremental position*)

Cette fonction fournit un signal de sortie sûr par rapport à la position de mesure mécanique relative.

La relation entre le signal de sortie et la position de mesure relative doit se situer dans une *plage de tolérances* qui doit être spécifiée et incluse dans les informations pour l'utilisation.

4.3 Position absolue sûre (SAP, *safe absolute position*)

Cette fonction fournit un signal de sortie sûr par rapport à la position de mesure mécanique.

La relation entre le signal de sortie et la position de mesure doit se situer dans une *plage de tolérances* qui doit être spécifiée et incluse dans les informations pour l'utilisation.

NOTE La raison de la distinction entre les deux *sous-fonctions de sécurité* SIP et SAP est la grande différence qui existe dans la façon dont ces deux valeurs de position différentes sont générées et dans la façon dont elles sont utilisées.

4.4 Valeur de vitesse sûre (SSV, *safe speed value*)

Cette fonction fournit un signal de sortie sûr par rapport à la vitesse de la partie mobile.

La relation entre le signal de sortie et la vitesse de la partie mobile doit se situer dans une *plage de tolérances* qui doit être spécifiée et incluse dans les informations pour l'utilisation.

4.5 Valeur d'accélération sûre (SAV, *safe acceleration value*)

Cette fonction fournit un signal de sortie sûr par rapport à l'accélération de la partie mobile.

La relation entre le signal de sortie et l'accélération de la partie mobile doit se situer dans une *plage de tolérances* qui doit être spécifiée et incluse dans les informations pour l'utilisation.

4.6 *Sous-fonctions de sécurité* pour l'évaluation et la signalisation

Des *sous-fonctions de sécurité* qui assurent le *traitement des signaux* dans le *codeur(SR)* et le traitement du ou des signaux de sortie respectifs sont possibles, par exemple une limitation sûre de la vitesse (SLS) (voir 4.2.4.5 de l'IEC 61800-5-2:2016). Pour ces *sous-fonctions de sécurité*, les exigences relatives à la conception et au développement ainsi qu'à la vérification et à la validation définies dans l'IEC 61800-5-2 doivent s'appliquer.

5 Gestion de la *sécurité fonctionnelle*

Les exigences de l'Article 5 de l'IEC 61800-5-2:2016 doivent s'appliquer.

6 Exigences relatives à la conception et au développement

6.1 Exigences générales

Le Tableau 2 indique quels paragraphes de l'Article 6 de l'IEC 61800-5-2:2016 doivent être appliqués sans modification et quels paragraphes de l'Article 6 de l'IEC 61800-5-2:2016 sont modifiés pour s'appliquer aux *codeurs(SR)*.

Le Tableau 3 indique quels paragraphes de l'IEC 61800-5-1:2007 et de l'IEC 61800-5-1:2007/AMD1:2016 doivent être appliqués sans modification et quels paragraphes de l'IEC 61800-5-1:2007 et de l'IEC 61800-5-1:2007/AMD1:2016 sont modifiés pour s'appliquer aux *codeurs(SR)*.

Les *codeurs(SR)* comprennent différentes technologies et différents blocs fonctionnels matériels, nécessaires pour assurer les *sous-fonctions de sécurité* du *codeur(SR)*. Les réalisations des *codeurs(SR)* sont différentes, mais elles peuvent toujours être structurées conformément à l'architecture universelle décrite à l'Annexe B. Les exigences complémentaires relatives à ces blocs fonctionnels matériels sont données du 6.5 au 6.8.

Tableau 2 – Paragraphes de l'IEC 61800-5-2:2016 applicables aux *codeurs(SR)* et modifications respectives

Exigences de l'IEC 61800-5-2:2016 pour les *PDS(SR)*		Les exigences doivent-elles s'appliquer aux *codeurs(SR)*?	Paragraphe applicable du présent document
6.1	Exigences générales	Non, remplacées	6.1 Exigences générales
6.1.1	Modification de l'état de fonctionnement	Non	
6.1.2	Normes de conception	Non, remplacées	6.2 Normes de conception
6.1.3	Réalisation	Oui	
6.1.4	Intégrité de sécurité et détection de défaut	Oui	
6.1.5	Sous-fonctions de sécurité et sous-fonctions non relatives à la sécurité	Oui	
6.1.6	SIL pour plusieurs sous-fonctions de sécurité dans un *PDS(SR)*	Oui	
6.1.7	Circuits intégrés avec redondance sur la puce	Oui	
6.1.8	Exigences concernant les logiciels	Oui	6.9 Exigences relatives à la conception des logiciels
6.1.9	Documentation de conception	Oui	
6.2	Exigences relatives à la conception du *PDS(SR)*		
6.2.1	Principes de sécurité de base et principes de sécurité éprouvés	Oui	
6.2.2	Exigences relatives à l'estimation de la probabilité de défaillances matérielles dangereuses aléatoires par heure (PFH)		
6.2.2.1	Exigences générales		
6.2.2.1.1	PFH pour chaque sous-fonction de sécurité	Oui	
6.2.2.1.2	Estimation de la PFH	Oui	
6.2.2.1.3	Données relatives aux taux de défaillance	Oui	
6.2.2.1.4	Intervalle entre essais de diagnostic pour une tolérance aux anomalies du matériel supérieure à zéro	Oui	
6.2.2.1.5	Intervalle entre essais de diagnostic pour une tolérance zéro aux anomalies du matériel	Oui	
6.2.3	Contraintes architecturales		
6.2.3.1	Limitations du SIL	Oui	
6.2.3.2	Sous-systèmes de Type A et de Type B		
6.2.3.2.1	Généralités	Oui	
6.2.3.2.2	Type A	Oui	
6.2.3.2.3	Type B	Oui	
6.2.3.3	Contraintes architecturales	Oui	
6.2.4	Estimation de la proportion de défaillances en sécurité (SFF)		
6.2.4.1	Méthodes d'analyse	Oui	
6.2.5	Exigences relatives à l'intégrité de sécurité systématique d'un *PDS(SR)* et des sous-systèmes d'un *PDS(SR)*		
6.2.5.1	Exigences relatives à l'évitement des défaillances		
6.2.5.1.1	Généralités	Oui	
6.2.5.1.2	Choix des méthodes de conception	Oui	
6.2.5.1.3	Mesures de conception	Oui	

Exigences de l'IEC 61800-5-2:2016 pour les *PDS(SR)*		Les exigences doivent-elles s'appliquer aux *codeurs(SR)*?	Paragraphe applicable du présent document
6.2.5.1.4	Planification des essais	Oui	
6.2.5.1.5	Exigences relatives à la maintenance de la conception	Oui	
6.2.5.2	Exigences relatives à la maîtrise des anomalies systématiques		
6.2.5.2.1	Généralités	Oui	
6.2.5.2.2	Caractéristiques de conception	Oui, avec addition	6.6 Exigences relatives à la conception pour la génération de signaux
6.2.5.2.3	Testabilité et maintenabilité	Oui	
6.2.5.2.4	Contraintes humaines	Oui	
6.2.5.2.5	Protection contre les modifications non intentionnelles	Oui	
6.2.5.2.6	Accusé de réception des entrées et erreurs de l'opérateur	Non	
6.2.5.2.7	Paramétrage du *PDS(SR)*	Oui, avec addition	6.11 Paramétrage
6.2.5.2.8	Pertes de l'alimentation électrique	Oui	
6.2.6	Exigences relatives à la conception pour l'immunité électromagnétique d'un *PDS(SR)*	Oui	
6.2.7	Exigences relatives à la conception pour l'immunité thermique d'un *PDS(SR)*	Non, remplacées	6.12 Exigences relatives à la conception pour l'immunité thermique
6.2.8	Exigences relatives à la conception pour l'immunité mécanique d'un *PDS(SR)*	Non, remplacées	6.13 Exigences relatives à la conception pour l'immunité mécanique
6.3	Comportement sur détection de défaut		
6.3.1	Détection de défaut	Oui, avec addition	6.3 Détection de défaut
6.3.2	Tolérance aux anomalies supérieure à zéro	Oui	
6.3.3	Tolérance zéro aux anomalies	Oui	
6.4	Exigences supplémentaires relatives à la communication de données	Oui	
6.5	Exigences relatives à l'intégration et aux essais du *PDS(SR)*		
6.5.1	Intégration matérielle	Oui	
6.5.2	Intégration logicielle	Oui	
6.5.3	Modifications pendant l'intégration	Oui	
6.5.4	Essais d'intégration applicables	Oui	
6.5.5	Documentation relative aux essais	Oui	

Tableau 3 – Références de l'IEC 61800-5-1:2007 et de l'IEC 61800-5-1:2007/AMD1:2016 applicables aux *codeurs(SR)* et modifications respectives

Exigences de l'IEC 61800-5-1:2016 CSV pour les *PDS(SR)*		Les exigences doivent-elles s'appliquer aux *codeurs(SR)*?	Modification apportée pour les *codeurs(SR)*
4	Protection contre les chocs électriques et les dangers thermiques et énergétiques		
4.1	Généralités	Oui	
4.2	Conditions d'anomalie	Oui	

Exigences de l'IEC 61800-5-1:2016 CSV pour les *PDS(SR)*		Les exigences doivent-elles s'appliquer aux *codeurs(SR)*?	Modification apportée pour les *codeurs(SR)*
4.3	Protection contre les chocs électriques		
4.3.1	Classification de tension déterminante	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.2	Séparation de protection	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.3	Protection contre le contact direct	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.4	Protection en cas de contact direct	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.5	Protection contre le contact indirect	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.5.1	Généralités	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.

Exigences de l'IEC 61800-5-1:2016 CSV pour les *PDS(SR)*		Les exigences doivent-elles s'appliquer aux *codeurs(SR)*?	Modification apportée pour les *codeurs(SR)*
4.3.5.2	Isolement entre les parties actives et les parties conductrices accessibles	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.5.3	Circuit de liaison de protection	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.5.4	Conducteur de mise à la terre de protection	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.5.5	Dispositif de raccordement du conducteur de mise à la terre de protection	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.5.6	Caractéristiques spéciales des appareils pour une protection de classe II	Oui	Sont exclus les *codeurs(SR)* qui sont exclusivement – alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs circuits de TBTP conformes à la CTD A; et – raccordés à des circuits de TBTP conformes à la CTD A.
4.3.6	Isolement	Oui	Voir Annexe E pour un exemple
4.3.7	Enveloppes	Oui	
4.3.8	Câblages et raccordements	Oui	
4.3.9	Exigences de court-circuit en sortie	Oui	
4.3.10	Compatibilité avec les dispositifs de protection à courant différentiel résiduel (DDR) ou de surveillance (RCM)	Non	
4.3.11	Décharge de condensateurs	Non	

Exigences de l'IEC 61800-5-1:2016 CSV pour les *PDS(SR)*		Les exigences doivent-elles s'appliquer aux *codeurs(SR)*?	Modification apportée pour les *codeurs(SR)*
4.3.12	Conditions d'accès pour l'EEP haute tension	Non	
4.4	Protection contre les risques thermiques	Oui	
4.4.1	Limitation du risque d'inflammation	Oui	
4.4.2	Matériaux isolants	Oui	
4.4.3	Inflammabilité des matériaux de l'enveloppe	Oui	
4.4.4	Limites de température		
4.4.4.1	Parties internes	Oui	
4.4.4.2	Parties externes du MEC	Oui	
4.4.5	Exigences spécifiques pour l'EEP refroidi par liquide	Non	
4.5	Protection contre les risques énergétiques	Non	
4.6	Protection contre les contraintes environnementales	Oui	

6.2 Normes de conception

Le *codeur(SR)* doit être conçu conformément à l'IEC 61800-1, à l'IEC 61800-5-1 et à l'IEC 61800-5-2. Le présent document comprend des exigences supplémentaires spécifiques aux *codeurs(SR)* ou qui s'écartent des exigences relatives aux *PDS(SR)*.

Si les exigences du présent document sont en contradiction avec les exigences d'autres normes applicables, les exigences du présent document prévalent.

En outre, il convient de satisfaire aux exigences de l'ISO 13849-1 pour les *codeurs(SR)* dédiés aux applications de machines.

6.3 Détection de *défaut*

Les mesures diagnostiques nécessaires pour les *codeurs(SR)* peuvent être divisées entre:

- les mesures diagnostiques réalisées par le *codeur(SR)*; et
- les mesures diagnostiques réalisées dans l'*unité d'évaluation*.

Si les mesures diagnostiques s'appliquent au sein du *codeur(SR)*, la détection d'un *défaut dangereux* doit être signalée à l'*unité d'évaluation*.

Si la détection des *défauts* doit s'effectuer dans l'*unité d'évaluation*, des exigences appropriées ainsi que la spécification de mesures recommandées pour une détection adéquate des *défauts* doivent être incluses dans les informations pour l'utilisation du *codeur(SR)*.

NOTE 1 Concernant la détection de *défaut* des signaux analogiques sinus et cosinus par technique numérique, voir Annexe I.

Si l'utilisation de valeurs de position générées par *interpolation* des signaux de sortie sinus et cosinus du *codeur(SR)* n'est pas exclue dans les instructions d'utilisation, des mesures diagnostiques appropriées doivent être appliquées.

EXEMPLE 1 Le nombre minimal d'échantillons par période de signal de l'*indicateur statique* est spécifié.

Si la *détection de défaut idéale* est exigée pour le *codeur(SR)* (voir 6.4.1), les mesures diagnostiques appliquées au *codeur(SR)* doivent permettre de révéler toutes les *anomalies* qui entraînent une erreur dans toute *sous-fonction de sécurité* du *codeur(SR)* qui dépasse la *plage de tolérances* spécifiée dans les informations pour l'utilisation. L'adéquation de ces mesures pour la détection des *défauts* doit être démontrée au moyen d'une analyse statique selon l'Annexe L.

En cas de détection d'un *défaut* qui peut entraîner la perte de la *sous-fonction de sécurité*, une fonction de réaction au *défaut* doit être activée afin de prévenir un danger. Les diagnostics et les fonctions de réaction au *défaut* doivent être réalisés conformément au temps maximal de réaction au *défaut* spécifié.

NOTE 2 La fonction de réaction au *défaut* d'un *codeur(SR)* se limite habituellement au signalement d'un *défaut* à l'*unité d'évaluation*.

La détection de défaut par le *codeur(SR)* ou l'unité d'évaluation ne doit pas être retardée ou entravée par des fonctions de contrôle de l'amplitude et/ou de la phase des signaux analogiques (voir Annexe M pour des exemples).

NOTE 3 Les signaux analogiques étudiés ici peuvent être les signaux de sortie d'un *codeur(SR)* avec signaux de sortie sinus et cosinus utilisés pour la génération des signaux ou le traitement des signaux d'un *codeur(SR)*.

EXEMPLE 2 En raison d'une anomalie de composant, le signal sinus est altéré, son amplitude est contrôlée et la longueur de phaseur est maintenue de façon erronée dans les tolérances spécifiées, même pendant le passage de chaque période individuelle de l'indicateur statique. La détection de défaut qui applique la surveillance de la longueur de phaseur est entravée.

EXEMPLE 3 Le contrôle de l'amplitude des signaux sinus et cosinus s'effectue plus lentement que l'application des mesures diagnostiques. Une défaillance dangereuse peut être détectée par surveillance de la longueur de phaseur avant traitement de l'amplitude des signaux sinus ou cosinus. Un retard de la détection de défaut et une augmentation du temps de réaction au défaut sont empêchés.

6.4 Exigences relatives à la conception de types spécifiques de *codeurs(SR)*

6.4.1 Exigences relatives à la conception d'un *codeur(SR)* avec signaux de sortie sinus et cosinus

Pour les *codeurs(SR)* incrémentaux dont la génération des signaux et le *traitement des signaux* sont indépendants pour un ensemble de signaux de sortie sinus et cosinus (par exemple A, /A, B, /B), ces signaux peuvent être considérés comme redondants pour les informations de vitesse non signées qui contribuent à la ou aux sous-fonctions de sécurité (par exemple, SLS, SSR, SLA, SS1 et SS2 selon l'Article 4 de l'IEC 61800-5-2:2016). Dans ce cas, l'application de la *détection de défaut idéale* n'est pas exigée et la vitesse peut être obtenue de manière redondante par les signaux sinus et cosinus, sous réserve d'une évaluation indépendante.

NOTE 1 L'utilisation de circuits intégrés décodeurs en quadrature pour l'évaluation détruit l'indépendance des signaux sinus et cosinus.

Pour les *codeurs(SR)* incrémentaux dont la génération des signaux et le *traitement des signaux* ne sont pas indépendants, ou lorsque des informations de position ou de direction incrémentale ou absolue contribuent à la ou aux fonctions de sécurité (par exemple SOS, SDI, SCA, SLP et SSR selon l'Article 4 de l'IEC 61800-5-2:2016), l'ensemble de signaux de sortie sinus et cosinus (par exemple A, /A, B, /B) ne peut pas être considéré comme redondant. Ces *codeurs(SR)* doivent appliquer la *détection de défaut idéale* (voir Annexe J pour plus d'informations) si la catégorie 3 ou la catégorie 4, selon l'ISO 13849-1:2015, est revendiquée. Si la catégorie 4 est revendiquée pour le *codeur(SR)*, les mesures diagnostiques appliquées pour atteindre la *détection de défaut idéale* doivent:

- être redondantes; ou
- comprendre leurs propres mesures diagnostiques avec une *DC* minimale de 99 %.

Un *codeur(SR)* qui applique la *détection de défaut idéale* doit être limité à la catégorie 3 lorsqu'un seul circuit intégré sans redondance sur la puce, conformément à l'Annexe E de l'IEC 61508-2:2010, est utilisé pour la génération des signaux et/ou le *traitement des signaux*.

NOTE 2 En cas de redondance sur la puce, le *traitement des signaux* sinus et cosinus est considéré comme indépendant. Etant donné que les signaux sinus ET cosinus sont nécessaires pour atteindre la position incrémentale ou absolue sûre et qu'il n'y a donc pas de redondance des informations de position, la *HFT* est toujours égale à 0.

NOTE 3 La conformité à la *détection de défaut idéale* est nécessaire pour satisfaire aux exigences des catégories 3 et 4 décrites en 6.2.6 et 6.2.7 de l'ISO 13849-1:2015. Les définitions de ces catégories indiquent "...qu'un défaut unique ... n'entraîne pas la perte de la *fonction de sécurité*".

NOTE 4 La *tolérance aux anomalies du matériel* (*HFT*) est un paramètre d'entrée nécessaire pour déterminer la limite du *SIL* en fonction des contraintes architecturales (voir H.9.2).

6.4.2 Exigences relatives à la conception d'un *codeur(SR)* avec signaux de sortie incrémentaux et absolus

6.4.2.1 Généralités

Un *codeur(SR)* avec des signaux de sortie incrémentaux et absolus présente une architecture à deux canaux, l'un fournissant un signal incrémental, l'autre fournissant une information de position absolue.

6.4.2.2 Génération de la valeur de position absolue sûre

Une valeur de position absolue redondante doit être générée dans l'*unité d'évaluation* à partir du signal de sortie incrémental du *codeur(SR)* et d'une référence appropriée. Pour obtenir une valeur de position absolue sûre, la valeur de position absolue de l'*unité d'évaluation* et la valeur de position absolue du *codeur(SR)* doivent être comparées (recoupées) et doivent être conformes aux tolérances spécifiées. Voir Figure 2 pour un exemple d'architecture matérielle.

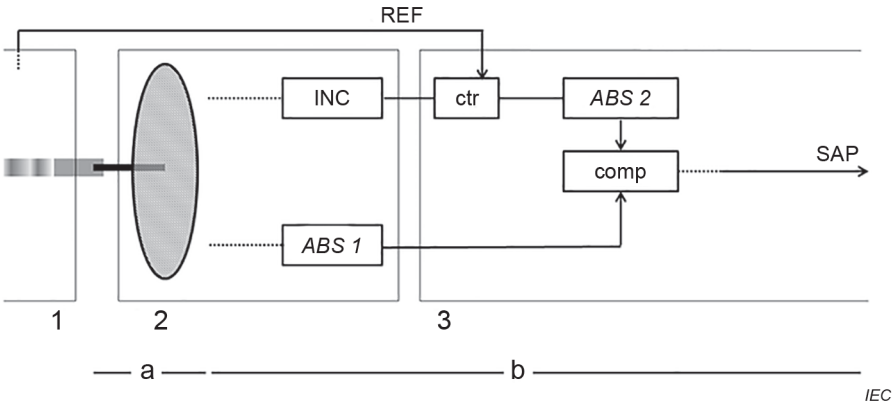
Le *codeur(SR)* doit être conçu de manière à ce qu'aucune *défaillance* dangereuse non détectable ne puisse survenir, entraînant une modification simultanée des valeurs de position incrémentale et absolue qui se traduit par des valeurs de position absolue incorrecte identiques dans les tolérances spécifiées.

NOTE Un *codeur(SR)* avec un *traitement des signaux* distinct et différent pour les valeurs de position incrémentale et absolue satisfait habituellement à cette exigence.

Les instructions d'utilisation du *codeur(SR)* doivent décrire le processus effectué dans l'*unité d'évaluation* pour générer la valeur de position absolue redondante et pour détecter les *anomalies* dans la valeur de position absolue avec la *DC* exigée.

Si les canaux particuliers du *codeur(SR)* exigent des diagnostics spécifiques réalisés par l'*unité d'évaluation*, ils doivent être décrits dans les instructions d'utilisation du *codeur(SR)*.

La référence de l'*unité d'évaluation* pour la deuxième valeur de position absolue doit être indépendante de la valeur de position absolue du *codeur(SR)*.



Légende

a	aucune redondance, exclusion de *défaut* ou *détection de défaut idéale* appliquée
b	redondance, détection de *défaut* appliquée
1	machine
2	*codeur(SR)*
3	*unité d'évaluation sûre*
ABS 1	valeur de position absolue fournie par le *codeur(SR)*
ABS 2	valeur de position absolue générée par comptage des impulsions incrémentales fournies par le *codeur(SR)*
comp	comparaison de *ABS 1* et *ABS 2*
ctr	compteur
INC	signal incrémental fourni par le *codeur(SR)*
REF	signal indépendant à partir d'un point fixe de la machine pour exécuter la procédure de référence pour *ABS 2*
SAP	*Sous-fonction de sécurité* de position absolue sûre

Figure 2 – Exemple d'architecture matérielle d'un *codeur(SR)* avec signaux de sortie incrémentaux et absolus

L'utilisation de ce type de *codeur(SR)* fournit la *sous-fonction de sécurité* de position absolue sûre (SAP).

6.4.3 Exigences relatives à la conception d'un *codeur(SR)* avec interface de signaux à ondes carrées

Dans la mesure où l'interface de signaux à ondes carrées ne permet pas un diagnostic suffisant du bon fonctionnement du *codeur(SR)*, les exigences suivantes doivent être remplies.

Le *codeur(SR)* avec interface à ondes carrées doit:

- comprendre toutes les mesures nécessaires pour satisfaire aux exigences de l'Article 6 de l'IEC 61800-5-2:2016;
- fournir un moyen sûr de signalement de toute *anomalie* détectée à l'*unité d'évaluation*.

EXEMPLE Les signaux de sortie à ondes carrées peuvent être du type HTL, TTL ou HC-HTL.

En outre, il convient de satisfaire aux exigences de l'ISO 13849-1 pour les *codeurs(SR)* dédiés aux applications de machines.

6.4.4 Exigences relatives à la conception du résolveur

Les exigences du présent document doivent s'appliquer, le cas échéant. Dans tous les cas, les exigences suivantes doivent s'appliquer:

- gestion de la *sécurité fonctionnelle* (voir Article 5);
- mécanique (voir 6.5);
- informations pour l'utilisation (voir Article 7);
- vérification et validation (voir Article 8);
- exigences relatives aux essais (voir Article 9); et
- mécanique (voir Article 10).

NOTE Le résolveur ne comprend généralement pas de composants électroniques, étant donné que les fonctions respectives ne sont pas incluses dans le résolveur lui-même, mais sont fournies par l'*unité d'évaluation*.

6.5 Exigences relatives à la conception mécanique

6.5.1 Généralités

Un *codeur(SR)* comprend une partie fixe et une partie mobile qui sont reliées aux parties correspondantes de la machine au moyen de *fixations mécaniques* et *d'éléments de connexion mécaniques*.

6.5.2 Exigences relatives à la conception des *fixations mécaniques*

Si le détachement d'une fixation peut provoquer une *défaillance dangereuse* et que des mesures diagnostiques ne sont pas disponibles, l'exclusion de *défaut* doit être démontrée pour cette fixation, conformément à l'ISO 13849-2 et/ou à l'Annexe G. Si une exclusion de *défaut* est exigée pour un assemblage boulonné:

- les méthodes appropriées pour la conception doivent être utilisées, par exemple celles spécifiées dans [6]; et
- les assemblages boulonnés doivent en outre être protégés contre le desserrage (dû au tassement, au plongement, au fluage ou au relâchement).

6.5.3 Exigences relatives à la conception des *éléments de connexion mécaniques*

Les exclusions de *défauts* peuvent également être justifiées pour les *éléments de connexion mécaniques* par un surdimensionnement approprié (voir 7.3 de l'ISO 13849-1:2015 et Annexe A de l'ISO 13849-2:2012). La résistance nécessaire des *éléments de connexion mécaniques* et leur durabilité par rapport à la défaillance par fatigue doivent être démontrées.

NOTE 1 Le calcul peut être effectué conformément à [7].

NOTE 2 L'application de l'Annexe G n'est pas possible, le Tableau G.1 concernant uniquement les *fixations mécaniques* à verrouillage par profil ou à verrouillage par force, et non le matériau lui-même.

NOTE 3 Les *éléments de connexion mécaniques* sont généralement appelés "accouplements" (voir 3.11 et 3.12).

6.5.4 Roulements

Dans le cas d'un *codeur(SR)* à roulement(s), un *blocage de palier* peut entraîner une *défaillance dangereuse*. Lorsque des exclusions de *défauts* sont appliquées aux *raccordements mécaniques* (celles indiquées dans le Tableau G.1, par exemple), les mesures suivantes doivent être prises afin d'éviter et de corriger tout *blocage de palier spontané* et tout *blocage de palier progressif* (voir Tableau G.2).

1) *Blocage de palier spontané* – mesures appropriées

   Toutes les mesures qui visent à l'exclusion de *défaut* concernant le *blocage de palier spontané* indiquées dans le Tableau G.2 doivent être prises.

2) *Blocage de palier progressif* – mesures appropriées

   a) un *blocage de palier* n'entraîne pas de défaillance dangereuse; ou

   b) un *blocage de palier* est détecté et des mesures sont prises pour corriger l'*anomalie* avant que la situation ne puisse devenir dangereuse; ou

   c) un blocage de palier progressif est contrôlé par une détection précoce et des mesures sont prises pour corriger l'anomalie; ou

      NOTE 1 L'usure et la fatigue altèrent le comportement de fonctionnement d'un roulement et peuvent se manifester par:

      i) une augmentation du couple;

      ii) un fonctionnement irrégulier;

      iii) une précision opérationnelle réduite;

      iv) des bruits inhabituels lors du fonctionnement;

      v) une augmentation de la température.

   d) des mesures organisationnelles sont prises pour remplacer le roulement/le *codeur(SR)* avant que le roulement n'arrive à la fin de sa durée de vie en service.

      NOTE 2 Les mesures organisationnelles comprennent, par exemple, les instructions correspondantes des informations pour l'utilisation ou des précautions internes au *codeur(SR)*, les signaux étant transmis à la commande de niveau supérieur.

      NOTE 3 La durée de vie en service du roulement est habituellement estimée conformément à l'ISO/TS 16281 [8] et conjointement par le fabricant du *codeur(SR)*, le fabricant du roulement et le fournisseur de graisse, en tenant compte de la durée de mission de la graisse.

      NOTE 4 Le vieillissement, l'usure, la contamination, etc. réduisent le pouvoir lubrifiant de la graisse. Cela entraîne une augmentation des forces nécessaires au déplacement du roulement. Cet effet n'a pas à être pris en compte dans la durée de mission de la graisse.

      Le fabricant du *codeur(SR)* doit spécifier, dans les informations pour l'utilisation, les conditions limites sur la base desquelles la durée de vie en service du roulement a été estimée.

      NOTE 5 Les conditions limites sur la base desquelles la durée de vie en service du roulement est estimée comprennent, par exemple, la température, la position d'installation, les conditions de fixation (*défauts* d'alignement, accouplement, forces, etc.), la vitesse, le nombre de rotations, le fonctionnement en sens inverse et la classe de contamination.

6.6 Exigences relatives à la conception pour la génération des signaux

6.6.1 Généralités

Le principe de capteur appliqué au *codeur(SR)* doit être adapté à l'application prévue. Toute restriction concernant l'application du *codeur(SR)* doit être incluse dans les informations pour l'utilisation (voir Article F.2 b)).

NOTE Les conditions d'environnement relatives à l'application, telles que les champs magnétiques, les chocs et les vibrations, la pollution, etc., peuvent avoir un impact sur la mesure.

6.6.2 Exigences relatives à la conception pour la génération des signaux d'un *codeur(SR)* optique

Dans le cas d'un *codeur(SR)* optique, des particules de poussière peuvent se déposer sur le chemin optique, par exemple sur l'*indicateur statique* ou le capteur optique, entraînant des mesures erronées qui empêchent l'exécution correcte de la *sous-fonction de sécurité*. Les particules de poussière peuvent par exemple provenir de l'air ambiant ou être dues au frottement des paliers et à l'abrasion des joints d'étanchéité. Le dépôt de particules de poussière ne doit pas être exclu sans prendre des mesures appropriées. L'effet de la contamination peut en principe être révélé à l'aide de mesures de détection des *défauts*.

NOTE 1 Une contamination partielle ne peut toutefois être décelable qu'au sein d'une plage restreinte de positions. Si les mesures de détection des *défauts* sont prises à des instants discrets, la *détection de défaut* n'est pas assurée dans l'intervalle d'essai.

NOTE 2 Des mesures qui visent à améliorer la disponibilité sont souvent intégrées aux *unités d'évaluation* conçues pour supprimer les signaux de *défaut* intermittents. Ces mesures sont également susceptibles de retarder ou d'empêcher l'identification d'une contamination partielle.

6.6.3 Exigences relatives à la conception pour la génération des signaux d'un *codeur(SR)* magnétique

Dans la mesure où les *codeurs(SR)* qui utilisent des capteurs magnétiques pour détecter la position sont également sensibles aux champs magnétiques externes, les exigences spécifiques suivantes relatives à l'immunité magnétique de ces *codeurs(SR)* doivent être remplies:

- la valeur maximale des champs magnétiques externes valable dans toutes les directions de champ pour le critère A est incluse dans les informations pour l'utilisation;
- la valeur maximale des champs magnétiques externes valable dans toutes les directions de champ pour le critère *FS* est incluse dans les informations pour l'utilisation; et
- l'exigence minimale est conforme à l'IEC 61000-6-7:2014, Tableau 2, 2.5, mais pour le critère *FS*.

NOTE 1 La présence dans les informations d'utilisation d'indications pour démontrer que la valeur du champ magnétique externe à l'emplacement du *codeur(SR)* ne dépasse pas les limites spécifiées peut être utile.

NOTE 2 Dans le présent document, le critère *FS* est utilisé en lieu et place du critère DS, conformément au 9.3.3 de l'IEC 61800-5-2:2016.

6.7 Exigences relatives à la conception pour le *traitement des signaux*

Les exigences de l'IEC 61800-5-2:2016 doivent s'appliquer.

6.8 Exigences relatives à la conception pour l'évaluation interne et la signalisation

Les exigences de l'IEC 61800-5-2:2016 doivent s'appliquer.

6.9 Exigences relatives à la conception des logiciels

Si un logiciel est utilisé pour exécuter la ou les *sous-fonction(s) de sécurité*, ce logiciel doit être développé conformément aux exigences du 6.1.8 de l'IEC 61800-5-2:2016.

NOTE Le 6.1.8 de l'IEC 61800-5-2:2016 se rapporte à l'IEC 61508-3. Par conséquent, les défauts logiciels, en tant que sous-ensemble d'*anomalies* systématiques, sont réputés limiter la capabilité systématique, et les règles relatives à l'obtention de la capabilité systématique énoncées en 7.4.3 de l'IEC 61508-2:2010 s'appliquent. Aussi, la capabilité systématique du logiciel peut réduire le *SIL* prévu de la *sous-fonction de sécurité* d'une étape *SIL*, si la *détection de défaut idéale* est appliquée et concerne également le comportement du logiciel.

Si la conformité à l'ISO 13849-1 est revendiquée, les exigences supplémentaires du 4.6 de l'ISO 13849-1:2015 doivent s'appliquer.

6.10 Préréglage

Si le *codeur(SR)* comprend une fonction de préréglage de la position, il doit être conçu de façon à ce que la fonction de préréglage de la position ne compromette aucune de ses *sous-fonctions de sécurité*.

NOTE La fonction de préréglage est également appelée "décalage", "fonction de mise à zéro" ou "fonction de réglage de la position".

6.11 Paramétrage

Si le comportement d'une *sous-fonction de sécurité* peut être influencé par la configuration des paramètres respectifs, leur paramétrage est considéré comme relatif à la sécurité.

Les exigences du 6.2.5.2.7 de l'IEC 61800-5-2:2016 doivent s'appliquer.

Si la conformité à l'ISO 13849-1 est revendiquée, les exigences supplémentaires du 4.6.4 de l'ISO 13849-1:2015 doivent s'appliquer.

6.12 Exigences relatives à la conception pour l'immunité thermique

Le *codeur(SR)* doit être conçu de manière à présenter l'immunité thermique appropriée pour un fonctionnement dans l'environnement thermique spécifié.

NOTE Les exigences concernant l'essai d'immunité thermique sont décrites en 9.5.

6.13 Exigences relatives à la conception pour l'immunité mécanique

Le *codeur(SR)* doit être conçu de manière à présenter l'immunité mécanique appropriée pour un fonctionnement dans l'environnement mécanique spécifié.

NOTE Les exigences concernant l'essai d'immunité mécanique sont décrites en 9.6.

Des applications spécifiques peuvent exposer les *codeurs(SR)* rotatifs montés sur moteurs qui ne sont pas couverts par les essais, conformément au 9.6.5, à des chocs. Cela concerne en particulier les chocs provoqués par l'actionnement et le relâchement des freins mécaniques. Pour vérifier la résilience à ces chocs, voir Annexe D.

6.14 Exigences relatives à la conception des câbles de connexion intégrés

Les exigences de l'Annexe C de l'IEC 60947-5-2:2019 doivent s'appliquer.

7 Informations pour l'utilisation

7.1 Généralités

Les exigences de l'Article 7 de l'IEC 61800-5-2:2016 ainsi que les suivantes doivent s'appliquer.

7.2 Etiquettes

Les exigences du 8.1 de l'IEC 61800-1:1997 doivent s'appliquer, le cas échéant.

7.3 Informations et instructions pour l'utilisation sûre d'un *codeur(SR)*

Les informations et instructions doivent être conformes à l'Annexe F.

Les instructions doivent être fournies de manière lisible.

NOTE Une hauteur de caractère de 2 mm est considérée comme facilement lisible.

8 Vérification et validation

8.1 Généralités

Les exigences de l'Article 8 de l'IEC 61800-5-2:2016 ainsi que les suivantes (spécifiques au *codeur(SR)*) doivent s'appliquer.

8.2 Vérification de la *tolérance aux anomalies du matériel*

Afin de vérifier la *HFT* du *codeur(SR)*, un découpage de l'architecture et l'affectation de tous les composants liés à la sécurité aux blocs fonctionnels de l'architecture universelle (voir Annexe B) doivent être effectués.

NOTE Selon la réalisation du *codeur(SR)*, tous les blocs fonctionnels ne sont pas mis en œuvre.

Une *FMEDA qualitative* doit être réalisée (voir 8.4).

8.3 Vérification supplémentaire pour un *codeur(SR)* avec signaux de sortie sinus et cosinus

8.3.1 Vérification des mesures diagnostiques d'un *codeur(SR)* avec signaux de sortie sinus et cosinus de *HFT* = 0

Si la *détection de défaut idéale* est exigée, l'efficacité des mesures diagnostiques pour un *codeur(SR)* incrémental avec signaux de sortie sinus et cosinus de *HFT* = 0 doit être démontrée par la méthode d'analyse statique selon l'Annexe L.

8.3.2 Adaptabilité à l'*interpolation*

Dans le cas d'un *codeur(SR)* avec signaux de sortie sinus et cosinus, les signaux peuvent devoir être *interpolés* pour augmenter la résolution. Les mesures de détection des *défauts* doivent être appropriées.

Si la *détection de défaut idéale* est exigée, il doit être démontré que l'une des trois alternatives suivantes s'applique:

- l'*interpolation* des signaux sinus et cosinus pour les sous-fonctions de sécurité est exclue dans les instructions d'utilisation;
- les mesures de détection des *défauts* prévues assurent la *détection de défaut idéale*, même pour la résolution supérieure obtenue par *interpolation*; ou
- les instructions d'utilisation prévoient qu'en cas d'*interpolation*, les mesures de détection des *défauts* nécessaires pour obtenir la *détection de défaut idéale* doivent être définies et assurées par l'utilisateur.

8.4 *FMEDA qualitative*

Une *FMEDA qualitative* doit être effectuée en prenant en compte tous les composants matériels du *codeur(SR)*. Sont également inclus les composants mécaniques et les câbles électriques nécessaires au fonctionnement, même s'ils ne sont pas fournis avec le *codeur(SR)* lui-même.

En ce qui concerne les *anomalies* de composant pour lesquelles le comportement du système décrit dans la *FMEDA qualitative* est improbable, une *anomalie* doit être introduite ou simulée. La réponse du *codeur(SR)* à ces *anomalies* doit être documentée.

Le *codeur(SR)* ne doit contenir aucun composant présentant d'éventuelles *anomalies* qui peuvent entraîner une *défaillance dangereuse* et qui ne peuvent pas être révélées par des mesures de détection des *défauts*. Cela concerne notamment:

- l'interversion du signal sinus et des signaux cosinus associés par un multiplexeur ou l'inversion (détection incorrecte de la direction du mouvement);
- l'interruption de la tension de sortie constante qui simule les signaux sinus et/ou cosinus (voir Article L.7 pour plus d'informations);
- la rupture de l'arbre d'entraînement des *codeurs(SR)* rotatifs (identification erronée de l'arrêt); et
- le gel des valeurs analogiques numérisées pour les signaux sinus et cosinus.

EXEMPLE 1 Un circuit intégré numérise les signaux analogiques et les reconvertit après traitement numérique en signaux analogiques.

Les anomalies des composants qui ont une influence sur l'amplitude et/ou la phase des signaux analogiques doivent également être considérées comme des défaillances dangereuses si elles entravent ou retardent la détection de défaut, comme spécifié dans les instructions d'utilisation. Voir également 6.3.

EXEMPLE 2 Un *codeur(SR)* capable de contrôler l'amplitude et/ou la phase des signaux analogiques comprend des composants appropriés pour remplir cette fonction. En cas d'anomalie de composant dans le circuit, l'amplitude (ou les amplitudes) ou la phase du ou des signaux sinus et/ou cosinus ne sont pas correctement contrôlées. En cas de signal analogique défectueux, la longueur de phaseur est maintenue dans les tolérances spécifiées et la détection de défaut par surveillance de la longueur de phaseur échoue ou est retardée.

NOTE 1 L'aspect des *anomalies* des composants qui contrôlent l'amplitude et/ou la phase des signaux analogiques est particulièrement pertinent pour un *codeur(SR)* avec signaux de sortie sinus et cosinus qui permet l'*interpolation*.

L'analyse des composants doit reposer sur les modèles de *défaut* fournis et référencés à l'Annexe G.

Si la catégorie 3 ou la catégorie 4 selon l'ISO 13849-1:2015 est revendiquée, il doit être démontré pour tous les blocs fonctionnels que:

- les *anomalies* de composant dues à des raisons physiques ne peuvent se produire; ou
- les *anomalies* de composant liées à la mécanique peuvent être exclues (voir 6.5); ou
- la *tolérance au premier défaut* est obtenue par une architecture matérielle redondante (*HFT* = 1); ou
- la *tolérance au premier défaut* est obtenue sans architecture redondante au moyen d'une *détection de défaut idéale* (voir 3.34) à l'aide des mesures de détection des *défauts* spécifiées dans les instructions d'utilisation.

NOTE 2 Habituellement, les *codeurs(SR)* destinés aux machines ne satisfont pas à une *HFT* = 2 ou supérieure.

NOTE 3 Les signaux de sortie sinus et cosinus des *codeurs(SR)* incrémentaux ne peuvent pas être considérés comme des canaux généralement redondants. Voir Annexe K pour plus d'informations.

NOTE 4 Sur les *codeurs(SR)* incrémentaux avec signaux de sortie sinus et cosinus, l'intégration monolithique des capteurs de position et des circuits analogiques pour la génération des signaux rend la FMEDA pratiquement impossible au niveau du transistor. En lieu et place, il peut être admis par hypothèse que tout *défaut dangereux* au sein du circuit intégré a un impact sur les signaux de sortie sinus et/ou cosinus. Lorsque la *détection de défaut idéale* est obtenue, tous les *défauts dangereux* de ces circuits intégrés sont détectables.

Si des exclusions de *défauts* s'appliquent, celles-ci doivent être justifiées conformément aux normes indiquées à l'Annexe G. Pour *SIL* 3/PL e, l'application d'une exclusion de *défaut* est limitée (voir 7.2.2 de l'ISO TR 23849:2010[1]). Toutefois, cela ne doit pas s'appliquer aux aspects mécaniques; voir Tableau G.1 et IEC 61800-5-2:2016 (à l'exception du Tableau 5 de l'IEC 61800-5-2:2016).

8.5 Quantification

La fiabilité relative à la sécurité du *codeur(SR)* doit être déterminée par une estimation quantitative, conforme à l'Annexe H, par exemple.

9 Exigences relatives aux essais

9.1 Généralités

L'Article 9 remplace l'Article 9 de l'IEC 61800-5-2:2016.

9.2 Planification des essais

Les exigences du 9.1 de l'IEC 61800-5-2:2016 doivent s'appliquer, avec l'addition suivante:

---

1 Ce document a été supprimé.

Le présent document contient des exigences minimales. Si des exigences plus strictes sont revendiquées, celles-ci doivent être respectées lors des essais. S'il n'est pas évident de déterminer quelles sont les exigences les plus strictes, la conformité à toutes les exigences doit être démontrée.

9.3 Essais de fonctionnement

Des essais de fonctionnement de chaque *sous-fonction de sécurité*, y compris les diagnostics associés (essais d'insertion de *défauts*), doivent être réalisés. Lors de ces essais de fonctionnement, des contrôles doivent être effectués afin de déterminer si les propriétés du *codeur(SR)* ont été obtenues. Des écarts par rapport à la spécification et des indications d'une spécification incomplète doivent être documentés.

9.4 Essais d'immunité électromagnétique (EM) et électrique

9.4.1 Essais électriques

9.4.1.1 Essai de tension de choc

Les essais doivent être effectués conformément au 5.2.3.1 de l'IEC 61800-5-1:2007.

Sont exclus les *codeurs(SR)* dont les distances d'isolement sont établies conformément au Tableau 9 de l'IEC 61800-5-1:2007, et qui sont exclusivement:

- alimentés par une ou plusieurs source(s) de tension qui utilisent un ou plusieurs *circuits de TBTP* conformes à la *CTD* A; et
- raccordés à des *circuits de TBTP* conformes à la *CTD* A.

Si le *codeur(SR)* comprend un contact sans potentiel qui n'est pas lui-même alimenté par la même source de tension que le *codeur(SR)*, alors il existe un second circuit électrique, et l'essai au 5.2.3.1 de l'IEC 61800-5-1:2007 doit être réalisé.

9.4.1.2 Essai de tension alternative ou continue

Les essais doivent être effectués conformément au 5.2.3.2 de l'IEC 61800-5-1:2007.

Sont exclus les *codeurs(SR)* qui sont exclusivement:

- alimentés par une ou plusieurs sources de tension qui utilisent un ou plusieurs *circuits de TBTP* conformes à la *CTD* A; et
- raccordés à des *circuits de TBTP* conformes à la *CTD* A.

9.4.2 Essais d'immunité électromagnétique (EM)

Les exigences du 9.3 de l'IEC 61800-5-2:2016 doivent s'appliquer.

9.5 Essais d'immunité thermique

9.5.1 Généralités

Le 9.5 remplace les exigences du 9.4 de l'IEC 61800-5-2:2016.

9.5.2 Froid sec

Les essais doivent être effectués conformément à l'IEC 60068-2-1 et dans les conditions suivantes:

- l'essai du *codeur(SR)* doit être effectué à la température de fonctionnement admissible la plus basse; la température minimale pendant l'essai ne doit pas dépasser 5 °C ± 2 °C;

- l'essai de l'*unité d'interface* doit être effectué à la température ambiante admissible la plus basse; la température minimale pendant l'essai ne doit pas dépasser 5 °C ± 2 °C;
- la durée de contrainte doit être d'au moins 16 h; et
- l'essai doit être effectué avec le *codeur(SR)* hors tension et non entraîné.

Les critères d'acceptation suivants doivent être remplis:

- pour les essais de bon fonctionnement, l'éprouvette reste dans la chambre d'environnement, la température fixée ne doit pas être modifiée et le *codeur(SR)* est alimenté aux tensions de fonctionnement minimale et maximale spécifiées; et

  NOTE L'essai à la tension de fonctionnement maximale est nécessaire en raison de courants plus élevés lors de la mise sous tension.

- le *codeur(SR)* doit toujours assurer sa ou ses *sous-fonctions de sécurité* conformément à la spécification, sans aucune indication d'erreur.

9.5.3 Chaleur sèche

Les essais doivent être effectués conformément au 5.2.6.3.1 de l'IEC 61800-5-1:2007, et les conditions suivantes doivent être remplies lors de l'essai:

- l'essai du *codeur(SR)* doit être effectué à la température de fonctionnement admissible la plus élevée, mais au moins à 40 °C ± 2 °C;
- l'essai de l'*unité d'interface* doit être effectué à la température ambiante admissible la plus élevée, mais au moins à 40 °C ± 2 °C;
- la durée de contrainte doit être d'au moins 16 h; et
- l'essai doit être effectué avec le *codeur(SR)* sous tension et non entraîné.

NOTE Les essais du *codeur(SR)* dans une chambre d'environnement exigent un contrôle de la température au *point de mesure de la température de fonctionnement*.

Les critères d'acceptation suivants doivent être remplis:

- le *codeur(SR)* et l'*unité d'interface* doivent fonctionnent correctement pendant et après la mise sous contrainte; et
- le *codeur(SR)* doit toujours assurer sa ou ses *sous-fonctions de sécurité* conformément à la spécification, sans aucune indication d'erreur.

9.5.4 Chaleur humide

Les essais doivent être effectués conformément au 5.2.6.3.2 de l'IEC 61800-5-1:2007. Sont exclus les *codeurs(SR)* qui sont exclusivement:

- alimentés par une ou plusieurs source(s) de tension qui utilisent un ou plusieurs *circuit(s) de TBTP* conformes à la *CTD* A; et
- raccordés à des *circuits de TBTP* conformes à la *CTD* A.

Les critères d'acceptation suivants doivent être remplis:

- respect des critères d'acceptation applicables du 5.2.6.2 de l'IEC 61800-5-1:2007; et
- le *codeur(SR)* doit toujours assurer sa ou ses *sous-fonction(s) de sécurité* conformément à la spécification, sans aucune indication d'erreur.

9.5.5 Essai d'échauffement

Les essais doivent être effectués conformément au 5.2.3.8 de l'IEC 61800-5-1:2007, avec les modifications suivantes:

- les courbes de limitation thermique (qui représentent par exemple la température en fonction de la vitesse) doivent être soumises à l'essai aux points pertinents de la courbe;

- sur les *codeurs(SR)* rotatifs, l'essai d'échauffement doit être effectué à la vitesse maximale spécifiée, afin de tenir compte de l'influence thermique du frottement des paliers, etc.; et
- sur les *codeurs(SR)* rotatifs, la température maximale de fonctionnement doit s'appliquer au lieu de la "température ambiante de conception".

9.6 Essais d'immunité mécanique

9.6.1 Distances d'isolement et lignes de fuite

Les essais doivent être effectués conformément au 5.2.2.1 de l'IEC 61800-5-1:2007.

NOTE Voir Annexe E pour plus d'informations.

9.6.2 Essais de court-circuit des cartes de câblage imprimé

Les essais doivent être effectués conformément au 5.2.2.2 de l'IEC 61800-5-1:2007. Si les distances d'isolement et lignes de fuite satisfont aux exigences des Tableaux 9 et 10 de l'IEC 61800-5-1:2007, les essais de court-circuit des cartes de câblage imprimé ne sont pas exigés.

9.6.3 *Fixations mécaniques*

Les essais des *fixations mécaniques* (par exemple, raccordements à verrouillage par force au moyen d'assemblages boulonnés) doivent être effectués de la manière définie à l'Annexe G. Des conditions d'environnement défavorables doivent être prises en compte lors des essais, par exemple les conditions de température des fixations qui combinent des matériaux qui présentent des coefficients de dilatation thermique différents.

9.6.4 *Eléments de connexion mécaniques*

Les *éléments de connexion mécaniques* (par exemple, accouplements) doivent être soumis à l'essai selon la procédure suivante.

a) Déterminer les charges statiques et dynamiques maximales (provoquées par les déplacements, par exemple). Les charges maximales doivent être extraites des informations pour l'utilisation.

   NOTE 1 Dans le cas d'un *accouplement statorique*, les tolérances de montage ou les effets de dilatation thermique entraînent généralement une charge statique sur l'élément d'accouplement, tandis que l'écart de battement axial entraîne une charge dynamique sur l'élément d'accouplement.

b) Utiliser un équipement d'essai qui permet d'appliquer les charges statiques et dynamiques simultanément.

c) Pour les *codeurs(SR)* rotatifs, les essais des charges axiales et radiales peuvent être effectués séparément ou en combinaison.

d) Soumettre les charges statiques à l'essai avec un coefficient de sécurité d'au moins 1,0.

   NOTE 2 Le faible coefficient de sécurité 1,0 se justifie par une contrainte accrue due à l'application simultanée des charges statiques et dynamiques.

e) Soumettre les charges dynamiques à l'essai avec un coefficient de sécurité d'au moins 1,5.

f) Choisir la fréquence ou la vitesse de rotation la plus défavorable.

g) Choisir un nombre de cycles approprié en fonction du matériau et du coefficient de sécurité.

   NOTE 3 Une procédure type qui utilise le coefficient de sécurité ci-dessus consiste à soumettre à l'essai au moins 10^7 cycles pour l'acier (structure cristalline cubique à corps centré), et 10^8 cycles pour l'acier (structure cristalline cubique à face centrée), pour les alliages d'aluminium, de magnésium et de cuivre.

Après l'essai, les critères d'acceptation suivants doivent être remplis:

- les *éléments de connexion mécaniques* ne doivent pas être endommagés, déformés plastiquement, desserrés ou détachés; et

- il ne doit se produire aucun dommage pouvant affecter la ou les *sous-fonctions de sécurité* du *codeur(SR)*.

Un exemple d'essai approprié des *éléments de connexion mécaniques* est donné à l'Annexe C.

NOTE 4 L'essai des *éléments de connexion mécaniques* peut être effectué sur l'élément seul ou avec le *codeur(SR)*.

9.6.5 Essai de vibrations et de chocs

Les essais doivent être effectués conformément aux exigences indiquées en 9.5 de l'IEC 61800-5-2:2016, à l'exception du 9.5.4. Si des valeurs plus élevées sont spécifiées, celles-ci doivent s'appliquer. Le *codeur(SR)* doit être sous tension et chaque *sous-fonction de sécurité* doit être vérifiée pendant le fonctionnement.

Le *codeur(SR)*, y compris l'éventuelle *unité d'interface* associée, doit être assemblé et raccordé à l'alimentation conformément aux instructions d'assemblage et suivant les exigences indiquées dans l'IEC 60068-2-47.

Le *codeur(SR)* doit être monté conformément à ses instructions de montage. La partie mobile du *codeur(SR)* doit être fixée au moyen d'un dispositif de montage, de manière à fournir un signal de sortie constant.

Pour les *codeurs(SR)* avec signaux de sortie numériques, la durée de cycle minimale doit être choisie. Pour les *codeurs(SR)* avec signaux de sortie analogiques ou à ondes carrées, un intervalle d'échantillonnage ≤ 200 µs doit être choisi.

NOTE L'intervalle d'échantillonnage indiqué ici est jugé suffisant pour l'application du *codeur(SR)* dans les *fonctions de sécurité*, les exigences temporelles pour les *fonctions de sécurité* étant généralement moins strictes que les exigences temporelles pour la boucle de commande.

Pour l'essai de vibration, les signaux du *codeur(SR)* doivent être évalués pendant au moins un balayage (de préférence le dernier) pour chaque axe.

Si l'*indicateur statique* du *codeur(SR)* est fixé, les signaux de sortie doivent rester dans les limites de tolérance lors de chaque essai individuel, conformément aux instructions d'utilisation.

Après l'essai, les critères d'acceptation suivants doivent être remplis:

a) les parties électriquement actives ne doivent pas être accessibles au toucher (voir 9.6.7);
b) aucune pièce ne doit s'être desserrée ou détachée si cela compromet la sécurité du *codeur(SR)*;
c) il ne doit se produire aucun dommage pouvant affecter la fonction, la sécurité ou la bonne fixation; et
d) lorsque la partie mobile du *codeur(SR)* est déplacée (manuellement, par exemple), les signaux de sortie doivent être plausibles.

9.6.6 Propriétés mécaniques des câbles de connexion intégrés

Les essais doivent être effectués conformément à l'Annexe C de l'IEC 60947-5-2:2019.

9.6.7 Essais d'inaccessibilité

Les essais doivent être effectués conformément aux 5.2.2.3 et 5.2.2.4 de l'IEC 61800-5-1:2007, et ils doivent être effectués après les essais de vibration et de choc.

Pour les *codeurs(SR)* sans boîtier, plutôt que de procéder à des essais, les instructions doivent contenir des informations appropriées pour assurer la classe de protection demandée par l'installation sur le lieu d'utilisation.

NOTE Si des exclusions de *défauts* concernant les courts-circuits des cartes de câblage imprimé sont revendiquées, des exigences supplémentaires s'appliquent. Voir Tableau D.1 de l'IEC 61800-5-2:2016.

9.6.8 Essais de déformation

Les essais doivent être effectués conformément au 5.2.2.5 de l'IEC 61800-5-1:2007.

Sont exclus les *codeurs(SR)* et les *codeurs(SR)* intégrés qui sont exclusivement:

- alimentés par une ou plusieurs source(s) de tension qui utilisent un ou plusieurs *circuit(s) de TBTP* conformes à la *CTD* A; et
- raccordés à des *circuits de TBTP* conformes à la *CTD* A.

9.7 Essais de matériaux

Les essais doivent être effectués conformément au 5.2.5 de l'IEC 61800-5-1:2007.

9.8 Adaptabilité des composants et des matériaux utilisés

Par des essais, par examen et éventuellement par calcul et comparaison avec les documents techniques, il doit être démontré que les composants et matériaux du *codeur(SR)*:

- sont conformes aux normes existantes;
- sont adaptés à l'affectation prévue; et
- peuvent être utilisés dans les valeurs de conception définies.

NOTE Cela concerne également le câblage interne, les câbles de connexion, la fixation de l'*indicateur statique* (résistance à la température d'un adhésif, par exemple).

Afin d'évaluer l'adaptabilité à la *plage de températures de fonctionnement* prévue du *codeur(SR)*, les éléments suivants doivent être pris en compte:

- l'échauffement du *codeur(SR)* dû à la consommation d'électricité;
- la plage de températures ambiantes admissible du *codeur(SR)*; et
- l'absorption et le dégagement de chaleur sur le lieu d'assemblage.

Sur les *codeurs(SR)* rotatifs, avec l'accouplement de l'arbre du *codeur(SR)* à l'arbre d'entraînement, l'absorption et le dégagement de chaleur dépendent en grande partie des propriétés thermiques de l'assemblage. A moins qu'un assemblage isolé thermiquement ne soit exclu dans les instructions d'utilisation, l'échauffement dû au frottement des paliers et au frottement du joint d'étanchéité de l'arbre doit être déterminé. A cette fin, le *codeur(SR)* doit être assemblé à l'aide de matériaux thermiquement isolants et l'échauffement intrinsèque dans la plage de vitesses admissible doit être déterminé.

Tous les composants liés à la sécurité doivent être utilisés dans la plage de températures admissible. Si nécessaire, les instructions d'utilisation doivent indiquer les limites de la plage de vitesses et/ou de températures ambiantes.

L'efficacité de l'*indicateur statique* et de sa fixation doit rester inchangée tout au long de la durée de vie en service du système. Cela doit être vérifié au moyen d'une FMEDA. Afin de justifier les exclusions de *défauts* concernant le détachement de l'*indicateur statique*, les coefficients de surdimensionnement indiqués à l'Annexe G doivent être appliqués.

9.9 Contamination de l'*indicateur statique*

La durabilité face à la contamination de l'*indicateur statique* doit être démontrée par:

- l'exclusion de *défaut*, ou
- des mesures adéquates pour maintenir les caractéristiques liées à la sécurité, ou
- des mesures diagnostiques adéquates.

9.10 Etiquettes

Le contenu des étiquettes doit être examiné en ce qui concerne:

- l'exhaustivité (voir 7.2);
- l'exactitude;
- la cohérence des détails; et
- la lisibilité de l'impression.

NOTE Une hauteur d'impression de 2 mm est considérée comme facilement lisible.

La durabilité des étiquettes doit être démontrée:

- en frottant pendant 15 s avec un chiffon de coton imbibé d'eau; puis
- en frottant pendant 15 s avec le produit chimique "n-Hexane for Analysis" conforme au liquide d'essai défini dans les normes IEC 60335-1 et IEC 62368-1.

Les étiquettes doivent être facilement lisibles après les essais.

Il ne doit pas être possible d'enlever facilement les étiquettes de marquage à la main; l'ondulation ou la formation de plis n'est pas admise.

9.11 Instructions

Les documents techniques doivent être comparés aux exigences et examinés en ce qui concerne l'exhaustivité, l'exactitude et la cohérence.

9.12 Documentation relative aux essais

Les exigences du 9.6 de l'IEC 61800-5-2:2016 doivent s'appliquer.

10 Modification

Les exigences de l'Article 10 de l'IEC 61800-5-2:2016 doivent s'appliquer.

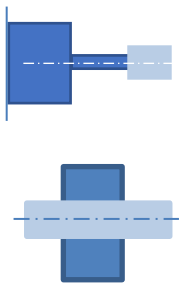
Annexe A
(informative)

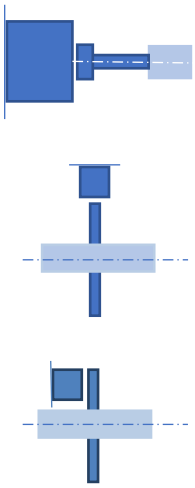
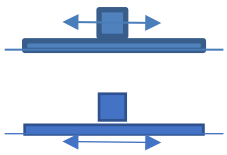
Types de *codeurs(SR)*

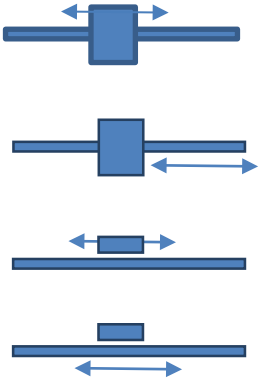
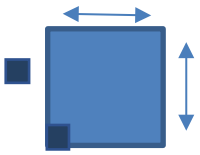
Le Tableau A.1 décrit les types généraux de *codeurs(SR)* et présente l'aménagement général des différents types de *codeurs(SR)*.

La couleur bleu clair indique l'arbre d'entrée du *codeur(SR)* rotatif.

Tableau A.1 – Types de *codeurs(SR)*

Type de *codeur(SR)*	Description	Remarque
Codeur(SR) incrémental	*Codeur(SR)* qui fournit un ou plusieurs signaux analogiques ou numériques proportionnels au changement de position d'une pièce mobile.	Il peut y avoir un signal d'indice supplémentaire. Le *codeur(SR)* incrémental génère un nombre précisément défini d'impulsions par rotation ou une plage de mesure linéaire.
Codeur(SR) absolu	*Codeur(SR)* qui fournit un ou plusieurs signaux analogiques ou numériques indiquant la position d'une pièce mobile.	Sans autre référence, il est possible d'obtenir la position absolue sur l'ensemble de la plage de mesure. Le *codeur(SR)* absolu surveille sa position à chaque instant et fournit un signal de sortie valide en cas d'application de puissance.
Codeur(SR) rotatif	*Codeur(SR)* qui génère un ou plusieurs signaux de sortie analogiques ou numériques en réponse à la position de rotation d'une pièce mobile.	Le *codeur* rotatif est également appelé "transducteur de position rotatif", "capteur de vitesse", "*codeur* à arbre" ou "*codeur* d'angle".
Codeur(SR) monotour	*Codeur(SR)* rotatif qui fournit une information de position absolue en une seule rotation.	Les valeurs de mesure sont répétées après chaque rotation complète.
Codeur(SR) multitour	*Codeur(SR)* rotatif qui fournit une information de position absolue en plusieurs rotations.	
Codeur(SR) rotatif à roulement intégré 	• Le *codeur(SR)* contient un ou plusieurs roulements, est une unité autonome et ne dépend pas de la machine hôte pour le contrôle du mouvement rotatif. • L'arbre d'entrée peut être raccordé à la machine hôte au moyen d'un accouplement. • Les parties internes du *codeur(SR)* sont généralement protégées de l'environnement.	
Codeur(SR) rotatif sans roulement intégré	• Le *Codeur(SR)* est en deux parties.	

Type de *codeur(SR)*	Description	Remarque
	• L'élément de commande/ l'*indicateur statique* est fixé à l'arbre de la machine hôte et dépend des roulements de la machine hôte pour le contrôle du mouvement rotatif. • Il est nécessaire d'aligner l'élément de commande/ l'*indicateur statique* par rapport au capteur lors du processus d'installation. • L'élément de commande/ l'*indicateur statique* peut être protégé ou non de l'environnement; la fonction du *codeur(SR)* peut donc être affectée par des solides ou des liquides. • Les parties internes du capteur sont généralement protégées de l'environnement.	
Codeur(SR) sans roulement	*Codeur(SR)* sans roulement propre ou guide.	
Codeur(SR) intégré	*Codeur(SR)* qui satisfait aux exigences relatives à la protection contre les influences environnementales uniquement lorsqu'il est installé sur son lieu d'utilisation.	
Codeur(SR) externe	*Codeur(SR)* conçu pour être fixé sur le lieu d'utilisation.	
Résolveur(SR)	Un résolveur(SR) est un type de transformateur rotatif utilisé pour mesurer les degrés de rotation.	
Codeur(SR) linéaire sans roulement intégré, non protégé de l'environnement 	• Le *codeur(SR)* est en deux parties (capteur et indicateur statique) et dépend des roulements de la machine hôte pour le contrôle du mouvement linéaire. • Le capteur est soit – fixé mécaniquement à un élément fixe de la machine hôte, l'*indicateur statique* étant fixé à un élément mobile, soit – fixé à un élément mobile, l'*indicateur statique* solide étant fixé à un élément fixe. • Les parties internes du *codeur(SR)* peuvent être protégées de l'environnement ou peuvent être montées dans un espace protégé de la machine hôte. • L'*indicateur statique* est aligné par rapport au capteur. En général, l'indicateur statique n'est pas protégé de l'environnement; la fonction du *codeur(SR)* peut donc être affectée par des solides ou des liquides.	

Type de *codeur(SR)*	Description	Remarque
Codeur(SR) linéaire protégé de l'environnement 	• Le *codeur(SR)* est monté sur l'ordinateur hôte en tant qu'unité. • Le mouvement du capteur et de l'*indicateur statique* peut être contrôlé par les roulements de la machine hôte, ou le *codeur(SR)* peut contenir des roulements intégrés pour le contrôle du mouvement linéaire. • Il est nécessaire d'aligner l'*indicateur statique* par rapport au capteur lors du processus d'installation. • Les parties internes sont protégées de l'environnement; la fonction du *codeur(SR)* n'est donc pas affectée par des solides ou des liquides.	
Codeur(SR) linéaire à arbre 	• Le *codeur(SR)* est soit – en une partie et contient des roulements pour guider le mouvement du capteur par rapport à l'arbre/ l'*indicateur statique*, soit – en deux parties et dépend des roulements de la machine hôte pour le contrôle du mouvement linéaire. • L'arbre/l'*indicateur statique* ou bien le capteur est monté sur une partie mobile de la machine hôte. • Les parties internes du *codeur(SR)* peuvent être protégées de l'environnement ou peuvent être montées dans un espace protégé de la machine hôte. • En général, l'arbre/l'*indicateur statique* n'est pas protégé de l'environnement; la fonction du *codeur(SR)* peut donc être affectée par des solides ou des liquides. • L'arbre/l'*indicateur statique* peut tourner.	
Codeur(SR) à disque X-Y/ *Codeur(SR)* à grille 	• Le *codeur(SR)* est en trois parties. • Deux capteurs détectent le mouvement simultané de l'*indicateur statique* sur deux axes. • Le codeur dépend des roulements de la machine hôte pour le contrôle du mouvement linéaire. • Les capteurs sont montés sur un élément fixe de la machine hôte. • L'*indicateur statique* est monté sur un élément mobile de la machine hôte.	

Annexe B
(informative)

Architecture universelle de *codeur(SR)*

B.1 Généralités

Les *codeurs(SR)* comprennent différentes technologies et différents blocs fonctionnels matériels, nécessaires pour assurer les *sous-fonctions de sécurité* du *codeur(SR)*. Les réalisations des *codeurs(SR)* sont différentes, mais elles peuvent toujours être structurées conformément à l'architecture universelle. Cela est utile pour procéder à un découpage en vue d'analyser la *HFT* et la catégorie (le cas échéant).

NOTE Dans le présent document, l'architecture universelle a également été utilisée pour structurer le contenu de certains paragraphes et pour faciliter les améliorations de technologies supplémentaires, etc. à l'avenir.

B.2 Architecture universelle de *codeur(SR)*

La Figure B.1 représente l'architecture universelle ainsi que ses blocs fonctionnels.

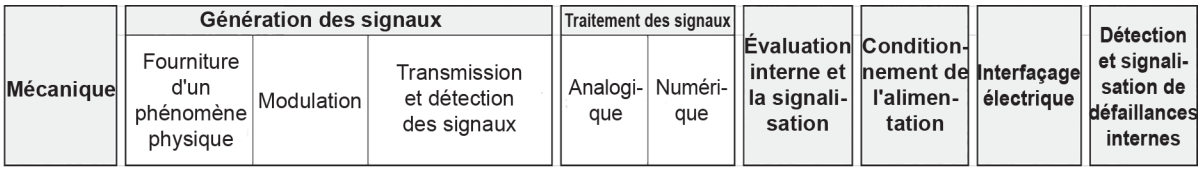


Figure B.1 – Architecture universelle de *codeur(SR)*

Un *codeur(SR)* n'inclut pas nécessairement tous les blocs fonctionnels de l'architecture universelle, mais tous les composants matériels de chaque *codeur(SR)* peuvent être affectés à un bloc fonctionnel approprié. Le Tableau B.1 fournit une liste des blocs fonctionnels et les exemples correspondants.

Tableau B.1 – Blocs fonctionnels de l'architecture universelle de *codeur(SR)*

Blocs fonctionnels	Exemples
Mécanique	Accouplement d'arbre flexible, accouplement d'arbre rigide, *accouplement statorique*, fixation du stator, fixation du rotor, fixation de l'*indicateur statique*, fixation de la tête de lecture, roulement, raccord à vis, encollage, boîte de vitesses
Génération des signaux	
Fourniture d'un phénomène physique	Lumière, champ magnétique, champ électromagnétique, champ électrique, résistance électrique
Modulation	*Indicateur statique*, disque de codage, roue dentée, distance mécanique
Transmission et détection des signaux	Câble à fibre optique, composant sensible à la lumière, "cadre de conducteur magnétique", composant sensible au champ magnétique, lentille, bobine, ouverture, triangulation, mesure du temps de transit
Traitement des signaux	
Analogique	Convertisseur d'impédance, amplificateur, linéarisation d'amplificateur, additionneur/soustracteur analogique, régulateur d'amplitude, régulateur de courant continu
Numérique	Décodeur en quadrature, compteur, convertisseur de signal, par exemple en rectangle, détermination de la position, de la vitesse, de l'accélération, etc., *interpolation*, convertisseur analogique/numérique
Evaluation interne et signalisation	Comparateur de position (SLP), comparateur de vitesse (SLS)
Conditionnement de l'alimentation	Régulateur, filtre
Interfaçage électrique	Circuit intégré de bus, pilote, analogique/numérique, connecteur, câble
Détection et signalisation de *défauts* internes	Moniteur de longueur de phaseur, moniteur de génération de signaux, comparateur de signaux, comparateur d'informations, moniteur de température, moniteur de signaux de sortie

Annexe C
(informative)

Exemples d'essais mécaniques appropriés pour un *codeur(SR)* rotatif

C.1 Généralités

L'Annexe G exige des essais appropriés pour justifier les exclusions de *défauts* concernant les raccordements mécaniques. Un exemple d'essais appropriés pour justifier l'exclusion de *défaut* concernant le raccordement mécanique entre un *codeur(SR)* rotatif et l'entraînement est donné.

C.2 Fixation mécanique du *codeur(SR)*

C.2.1 Raccordement à verrouillage par force (par des assemblages boulonnés, par exemple)

Selon le Tableau G.1, un coefficient de sécurité $S \geq 4$ pour un raccordement à verrouillage par force doit être vérifié par des essais.

Par conséquent, les connexions:

- entre le stator du moteur et le stator du *codeur(SR)*;
- entre l'arbre du moteur et l'arbre du *codeur(SR)* rotatif;
- entre une partie fixe de la machine et une partie fixe du *codeur(SR)*;
- entre une partie mobile de la machine et une partie mobile du *codeur(SR)*;

sont chargées statiquement par:

– la force maximale possible; et

– le couple maximal possible, y compris:

i) le couple qui résulte de l'accélération angulaire de l'inertie (masse en rotation angulaire) des parties rotatives du *codeur(SR)*;

ii) le couple de roulement dans des conditions d'environnement défavorables;

iii) etc.;

multiplié(e) au moins par un coefficient de sécurité $S = 4$. Les connexions doivent supporter cette force/ce couple, et aucun glissement ne doit se produire.

NOTE Le signal du *codeur(SR)* peut être utilisé pour déterminer le glissement dans l'interface, lorsque l'*indicateur statique* et l'arbre du *codeur(SR)* sont fixés au moyen d'un court-circuit mécanique.

C.2.2 Raccordement à verrouillage par profil (par clavette, par exemple)

Selon l'Annexe G, un coefficient de sécurité élevé par rapport à la rupture par fatigue (par exemple $S \geq 2$ pour l'acier) pour un raccordement à verrouillage par force doit être vérifié par des essais. L'accélération de l'essai (et l'inertie déplacée) est ainsi réglée pour correspondre à la force maximale/au couple maximal possible qui peut se produire dans le cadre de l'application, multiplié(e) par le coefficient de sécurité respectif. Pour déterminer la force maximale/le couple maximal possible, le couple qui résulte de l'accélération maximale de l'inertie de l'arbre, le couple de roulement maximal dans des conditions d'environnement défavorables, etc., doivent être pris en compte. Il ne doit se produire aucun dommage pouvant affecter la fonction, la sécurité ou la bonne fixation.

C.3 Eléments de *connexion mécaniques* du *codeur(SR)* – Accouplement statorique (support de couple) ou accouplement arbre-rotor

C.3.1 Généralités

Le *codeur(SR)* est assemblé conformément aux instructions d'utilisation sous précontraintes axiales et radiales supplémentaires superposées (charge statique) de l'*élément de connexion mécanique*. L'*élément de connexion mécanique* est alors soumis au nombre de déviations conforme au 9.6.4 g) (charge dynamique). Selon la géométrie, la déviation de l'*élément de connexion mécanique* est effectuée par déviation latérale (à l'aide d'un hydropulseur, par exemple) et/ou par rotation à l'aide d'un arbre excentrique.

Le dimensionnement selon C.3.2 et C.3.3 est utilisé pour le montage expérimental. Ainsi, les précontraintes axiales et radiales statiques de l'*élément de connexion mécanique* sont maintenues en superposition pour définir la position initiale à partir de laquelle la déviation de l'*élément de connexion mécanique* commence. Les potentielles fréquences propres de l'*élément de connexion mécanique* doivent être prises en compte. Il ne doit se produire aucun dommage pouvant affecter la fonction, la sécurité ou la bonne fixation.

C.3.2 Charges axiales

C.3.2.1 Statique

Conformément aux informations pour l'utilisation, le *codeur(SR)* est monté avec le décalage axial, le déplacement maximal admissible de l'arbre, en association avec les tolérances mécaniques du *codeur(SR)*, du banc de machine et de l'arbre d'entraînement.

NOTE Des bandes de gabarits de précision peuvent être utilisées pour calage afin de maintenir le déplacement statique.

C.3.2.2 Dynamique

Si le déplacement axial dynamique est admis, le *codeur(SR)* ou l'arbre, respectivement, est déplacé suivant l'amplitude des tolérances mécaniques et le déplacement maximal admissible, multiplié par le coefficient de sécurité d'au moins S = 1,5, conformément au 9.6.4.

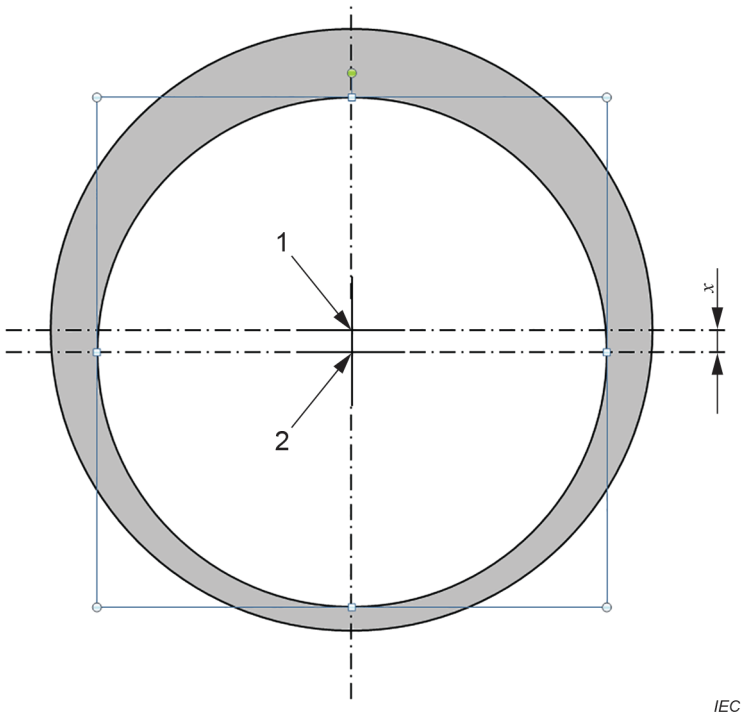
C.3.3 Charges radiales

C.3.3.1 Accouplement statorique statique/accouplement arbre-rotor dynamique

Le *codeur(SR)* est assemblé avec le décalage radial tiré des informations pour l'utilisation au déplacement radial maximal admissible de l'arbre. Pour les charges dynamiques (en cas d'*accouplement arbre-rotor*), le coefficient de sécurité est d'au moins S = 1,5, conformément au 9.6.4.

C.3.3.2 Accouplement statorique dynamique/accouplement arbre-rotor dynamique

L'arbre d'entraînement est équipé d'une bague excentrique supplémentaire (voir Figure C.1). Le degré d'excentricité dépend des tolérances mécaniques et du mouvement radial maximal admissible de l'arbre, conformément aux informations pour l'utilisation et pour les charges dynamiques (en cas d'*accouplement statorique*), multipliées par le coefficient de sécurité d'au moins S = 1,5, conformément au 9.6.4.



Légende

1 centre de l'arbre du *codeur(SR)*

2 centre de l'arbre d'entraînement

x excentricité

Figure C.1 – Exemple de bague supplémentaire pour assemblage avec excentricité x

Annexe D
(informative)

Essais de chocs prolongés pour les *codeurs(SR)* rotatifs montés sur moteurs

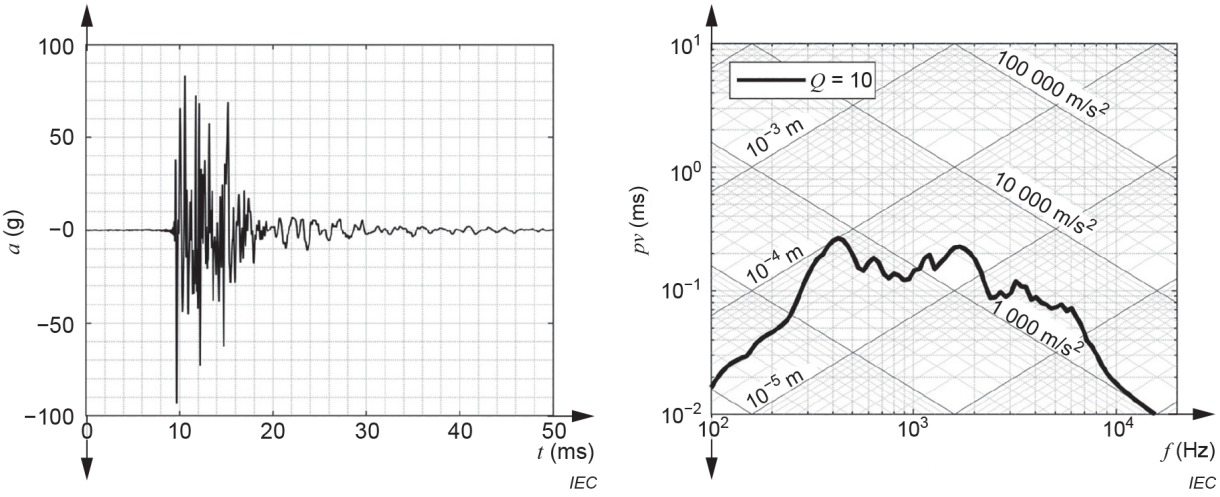
D.1 Généralités

L'actionnement et le relâchement des freins mécaniques (ou d'autres excitations mécaniques, par exemple des impacts) peuvent provoquer des chocs, qui peuvent endommager ou déformer les *codeurs(SR)* rotatifs montés sur moteurs. L'effet dommageable de ces chocs s'étend généralement sur une large plage de fréquences et ne peut être reproduit de façon satisfaisante par des essais selon l'IEC 60068-2-27.

D.2 Spectre de réponse aux chocs en pseudovitesse (PVSRS, *Pseudo-velocity shock-response spectrum*)

Le spectre de réponse aux chocs en pseudovitesse (PVSRS) est une méthode adaptée pour évaluer l'effet dommageable des chocs. La Figure D.1 représente un choc provoqué par l'actionnement d'un frein mécanique et le PVSRS correspondant sur un papier à quatre coordonnées (4CP).

NOTE Pour obtenir des informations détaillées au sujet du PVSRS et du PVSRS sur 4CP, voir [9].



a) Choc **b) PVSRS correspondant sur 4CP**

Légende

a accélération;

t temps;

f fréquence;

pv pseudovitesse;

Q facteur Q.

NOTE 1 La pseudovitesse indique la sévérité du choc.

NOTE 2 Le facteur Q (facteur de surtension) décrit l'amortissement du système admis par hypothèse.

Figure D.1 – Choc et PVSRS correspondant sur 4CP

D.3 Vérification de la résilience

Si la vérification d'une résilience suffisante aux chocs provoqués par les freins ou d'autres excitations mécaniques est souhaitée, il est recommandé:

- de procéder à un essai d'endurance dans l'environnement de fonctionnement prévisible; ou
- de procéder à un essai approprié sur une machine d'essai.

Lorsque la vérification est effectuée sur une machine d'essai, il doit être assuré que l'effet dommageable des chocs soumis à l'essai est au moins équivalent à l'effet dommageable prévu pendant le fonctionnement.

La comparaison de l'effet dommageable des chocs peut être effectuée en comparant le PVSRS calculé conformément à l'ISO 18431-4 [10]. Il est recommandé d'examiner la plage de fréquences d'au moins 100 Hz à 10 kHz, de calculer le PVSRS pour un minimum de douze fréquences par octave, et de choisir un facteur Q de dix. Il n'est possible de comparer des spectres de réponse l'un par rapport à l'autre que s'ils ont été déterminés dans des conditions comparables (point de mesure, direction de mesure, etc.) et suivant des durées de choc comparables [11].

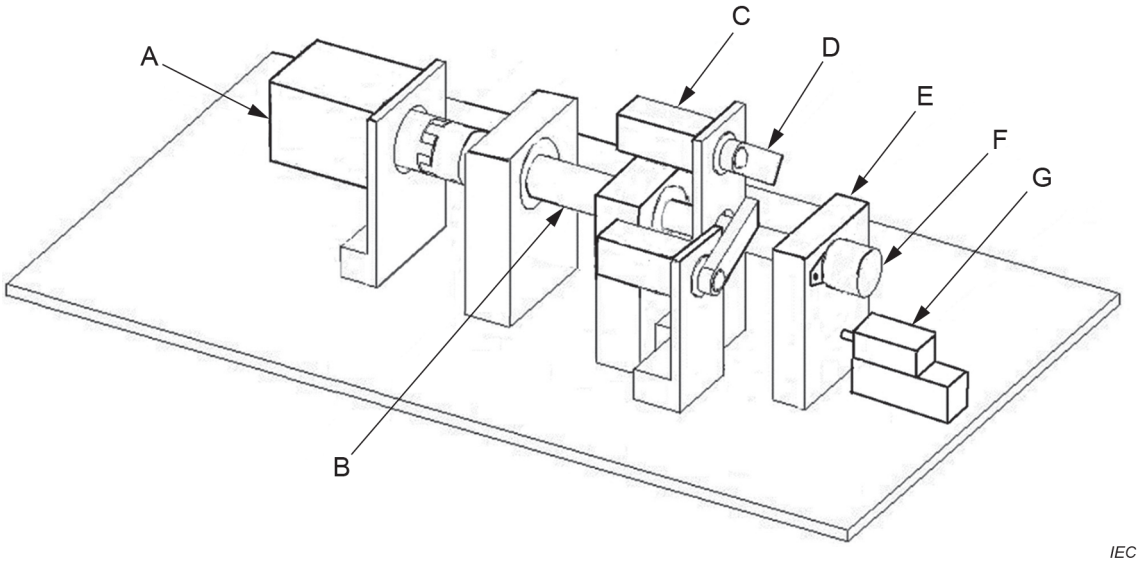
NOTE 1 Pour obtenir des informations détaillées au sujet des techniques de mesure et des machines d'essai de chocs, voir [11].

NOTE 2 Afin d'éviter de définir toutes les conditions pertinentes pour chaque cas particulier, une définition générale des conditions appropriées (points de mesure, directions, etc.) et des limites d'écart de la durée de choc est actuellement à l'étude.

D.4 Machine d'essai

La Figure D.2 représente une machine d'essai possible pour la vérification de la résilience en procédant à un essai sur une machine d'essai. La machine d'essai est particulièrement adaptée pour simuler des charges de choc à haute fréquence et sur plusieurs axes, comme prévu lors de l'utilisation sur moteurs à frein. La machine d'essai permet de faire varier la charge de choc sur la partie statique et sur la partie rotative du *codeur(SR)* de façon pratiquement indépendante et d'atteindre une fréquence de répétition élevée.

NOTE La machine d'essai est une modification des machines d'essai connues, qui provoquent des excitations de choc par impact mécanique. Voir [11] pour des exemples.



Légende

A moteur d'entraînement
B arbre de la machine d'essai
C actionneur rotatif
D élément de frappe
E stator de la machine d'essai
F *codeur(SR)* rotatif
G actionneur linéaire

Figure D.2 – Machine d'essai

Le *codeur(SR)* en essai est relié à l'arbre et au stator de la machine d'essai. Lors des essais, le moteur d'entraînement entraîne l'arbre de la machine d'essai à vitesse constante et les signaux du *codeur(SR)* sont surveillés. L'excitation de choc est provoquée par l'impact des actionneurs sur l'arbre et sur le stator de la machine d'essai. En général, le type, la position, la direction et le nombre des actionneurs peuvent être choisis selon les besoins pour atteindre la charge de choc (sur plusieurs axes) souhaitée. Sur la Figure D.2, deux actionneurs rotatifs qui agissent sur l'arbre et un actionneur linéaire supplémentaire qui agit sur le stator de la machine d'essai sont représentés à titre d'exemple.

La charge de choc souhaitée sur le *codeur(SR)* peut notamment être atteinte en modifiant les paramètres suivants:

- fréquences propres, amortissement et masse de l'arbre et du stator de la machine d'essai;
- position, direction et nombre des actionneurs;
- vitesse, masse et matériau des éléments de frappe.

Annexe E
(informative)

Dimensionnement des distances d'isolement et lignes de fuite sur les cartes de câblage imprimé – Exemple

E.1 Généralités

L'Annexe E donne un exemple de dimensionnement des distances d'isolement et lignes de fuite exigées sur les cartes de câblage imprimé, conformément au 4.3 de l'IEC 61800-5-1:2007 et de l'IEC 61800-5-1:2007/AMD1:2016.

E.2 Hypothèses

Pour cet exemple, les hypothèses suivantes s'appliquent:

- tension système/tension de fonctionnement ≤ 50 V;
- catégorie de surtension II;
- degré de contamination 2; et
- altitude maximale 2 000 m.

E.3 Application du 5.2.2.1 de l'IEC 61800-5-1:2007

L'application du 5.2.2.1 de l'IEC 61800-5-1:2007 implique les décisions suivantes:

a) en raison de la catégorie de surtension II, une tension système ≤ 50 V correspond à une surtension de 500 V (IEC 61800-5-1:2007 et IEC 61800-5-1:2007/AMD1:2016, Tableau 7);

b) en raison du degré de contamination 2, une surtension de 500 V correspond à une distance d'isolement minimale nécessaire de 0,1 mm (IEC 61800-5-1:2007, Tableau 9, avec note de bas de tableau a);

c) en raison du degré de contamination 2, une tension de fonctionnement ≤ 50 V exige une ligne de fuite minimale de 0,04 mm (IEC 61800-5-1:2007, Tableau 10);

d) la valeur de la ligne de fuite minimale calculée est augmentée jusqu'à la valeur de la distance d'isolement minimale calculée; et

e) la distance d'isolement et la ligne de fuite exigées sont d'au moins 0,1 mm.

NOTE Les hypothèses relatives aux *anomalies* des cartes/modules de câblage imprimé ainsi que les exigences concernant les exclusions de *défauts* sont répertoriées dans le Tableau D.1 de l'IEC 61800-5-2:2016.

Annexe F
(normative)

Informations et instructions – Liste détaillée

F.1 Vue d'ensemble

Les informations pour l'utilisation doivent inclure les informations et instructions de l'Annexe F, le cas échéant.

F.2 Liste détaillée

a) Généralités

nom de la société et adresse complète du fabricant et du représentant autorisé.

b) Informations pour le choix

1) désignation du *codeur(SR)* conformément aux indications fournies sur le *codeur(SR)* lui-même, à l'exclusion du numéro de série;
2) numéro de catalogue du *codeur(SR)* ou équivalent;
3) description générale du *codeur(SR)*;
4) description de l'utilisation prévue du *codeur(SR)*;
5) vitesse linéaire ou rotative maximale;
6) accélération linéaire ou rotative maximale;
7) classe de protection;
8) degré de pollution;
9) classification IP;
10) tension d'alimentation assignée;
11) si le *codeur(SR)* est équipé d'une protection contre les surtensions;
12) exigences relatives à la tension d'alimentation, par exemple un ou plusieurs *circuit(s) de TBTP* conformes à la *CTD* A;
13) courant d'alimentation assigné;
14) détails concernant le type de conducteur et la plus grande ou plus petite section de conducteur pour lesquels les bornes de raccordement sont adaptées;
15) plage de températures de stockage;
16) *plage de températures de fonctionnement;*
17) détail de toutes les restrictions du *codeur(SR)* concernant son environnement, son altitude, ses limites d'application et sa position d'installation;
18) pour un *codeur(SR)* magnétique, la valeur maximale des champs magnétiques externes pour satisfaire au critère A et au critère FS (voir 6.6.3);
19) durée de mission et information que le *codeur(SR)* doit être remplacé avant que la plus faible valeur de durée de mission et de durée de vie en service du roulement ne soit atteinte; et
20) durée de vie en service du roulement, y compris les conditions limites admises par hypothèse et l'information que le *codeur(SR)* doit être remplacé avant que la plus faible valeur de durée de mission et de durée de vie en service du roulement ne soit atteinte.

NOTE 1 Plutôt que d'indiquer une valeur pour la durée de vie en service du roulement, une méthode (diagrammes, tableur Excel, par exemple) ou un service peut être fourni pour permettre à l'utilisateur de déterminer la durée de vie en service du roulement du *codeur(SR)* en utilisant les conditions de l'application comme entrée.

c) Informations pour l'installation et la mise en service

1) *anomalies* qui invalident la *sécurité fonctionnelle*, par exemple installation incorrecte, coupure et reconnexion du câble, installation incorrecte de l'*indicateur statique*, démantèlement du *codeur(SR)*;

2) détails du montage;

3) paramètres d'alignement de l'élément de connexion mécanique, par exemple charges maximales, décalage axial, déplacement de l'arbre, décalage radial, etc. (voir 9.6.4);

4) exigences relatives au personnel d'installation;

5) conditions de détermination de la température de fonctionnement, par exemple vitesse du moteur, bref échauffement (dû à un arrêt après un fonctionnement à pleine charge, par exemple), situation d'installation, température ambiante, *point de mesure de la température de fonctionnement*;

6) plans de raccordement et de câblage;

7) mise à la terre;

8) exigences particulières concernant les câbles et connexions électriques;

EXEMPLE 1 Support mécanique exigé d'un connecteur ou fixation exigée du câble au banc de machine.

9) informations concernant la mise en service/aux essais de mise en service;

10) réglages exigés et méthodes appropriées;

11) exigences relatives à l'essai de configuration des *sous-fonctions de sécurité*;

12) liste des outils spéciaux; et

13) pour les *codeurs(SR)* sans boîtier ou avec boîtier partiel, des informations appropriées pour assurer la classe de protection demandée par l'installation sur le lieu d'utilisation.

d) Informations pour l'utilisation

1) description détaillée de la ou des *sous-fonctions de sécurité* fournies par le *codeur(SR)*, y compris les restrictions (par exemple, SSV sans information de direction);

2) spécification fonctionnelle de chaque interface et *sous-fonction de sécurité*, ainsi que de sa plage de tolérances respective; la manière dont la plage de tolérances doit être utilisée pour réaliser une fonction de sécurité doit être décrite;

EXEMPLE 2 Un *codeur(SR)* linéaire qui fournit la *sous-fonction de sécurité* de "position absolue sûre" (SAP) avec une *plage de tolérances* spécifiée de 1 mm ne peut être utilisé que pour surveiller la position jusqu'à 1 mm.

3) toutes les informations nécessaires au fonctionnement sûr du *codeur(SR)*, par exemple:

i) temps nécessaire au codeur(SR) pour fournir la valeur de sortie sûre;

NOTE 2 Pour un *codeur(SR)* purement analogique, l'angle de phase et/ou la largeur de bande sont généralement fournis.

ii) temps de réaction au défaut;

iii) durée de cycle minimale (et maximale) de sortie sûre; et

iv) taux de demande maximal auquel le régulateur de la machine hôte demande les données de position à l'interface numérique;

4) *niveau de performance PL* et catégorie, si la conformité à l'ISO 13849-1 est revendiquée;

5) pour chaque interface et *sous-fonction de sécurité* disponible pour la réalisation des fonctions de sécurité, la capacité SIL (y compris la capabilité systématique, voir l'IEC 61508-2), qui est atteinte lorsque le *codeur(SR)* est utilisé conformément aux instructions d'utilisation;

6) *PFH* et détails concernant la température de fonctionnement associée au point de mesure; est au moins nécessaire l'indication de la *PFH* pour la température de fonctionnement réaliste décrite en H.4;

7) exigences relatives à l'évaluation des signaux et à la détection de défaut dans l'unité d'évaluation (voir Annexe L, par exemple):

   i) définition des limites du ou des signau(x) de sortie sûrs;

   ii) définition des paramètres nécessaires au traitement des signaux de sortie sûrs, par exemple pour convertir les signaux sinus et cosinus en signaux à ondes carrées;

      NOTE 3 Un diagramme peut s'avérer utile.

   iii) exigences relatives aux mesures diagnostiques, y compris la spécification de mesures recommandées et/ou exigées pour une détection adéquate des défauts;

   iv) essai d'intégrité du signal analogique (pour un *codeur(SR)* avec signaux de sortie analogiques);

      NOTE 4 La précision de position atteignable dépend des limites de surveillance choisies pour les signaux analogiques. Si les limites de surveillance choisies sont larges, pour des raisons de disponibilité, par exemple, la précision de position atteignable diminue. Il existe une exigence minimale pour une évaluation quadratique; les limites de surveillance permettent les seuils de commutation des comparateurs.

   v) en cas d'anomalie, l'état de sécurité de l'application doit être atteint avant qu'une situation dangereuse ne puisse se produire; par conséquent, dans le cas d'un *codeur(SR)* avec HFT = 0, la somme du temps maximal exigé pour la détection de défaut et du temps de réponse aux défauts doit être inférieure au temps de sécurité du processus (voir 3.33); le temps maximal exigé pour la détection de défaut correspond à l'intervalle de temps auquel l'essai d'intégrité du signal analogique est complètement répété;

   vi) le matériel utilisé pour l'évaluation des signaux et la détection de défaut doit être pleinement fonctionnel sur l'ensemble de la plage de fréquences prévue des signaux de sortie;

   vii) si certains défauts du *codeur(SR)* ne sont détectables que sur certaines plages d'une période de l'indicateur statique avec l'essai d'intégrité du signal analogique indiqué, il doit être fait référence à des mesures en cas de diagnostics effectués en continu ou à des instants discrets (voir L.6.2);

   viii) en fonction de la capacité des mesures diagnostiques appliquées, l'une des options suivantes doit être choisie par le fabricant du *codeur(SR)*:

      a) exclusion de l'*interpolation* des signaux sinus et cosinus;

      b) limitation de la résolution améliorée obtenue par *interpolation* des signaux sinus et cosinus (en fonction de la fonction de sécurité pour laquelle le *codeur(SR)* est utilisé);

         NOTE 5 Certains *codeurs(SR)* n'admettent l'application dans les *fonctions de sécurité* qu'à partir de la valeur de position non *interpolée*, par exemple car la sensibilité des mesures diagnostiques n'est pas suffisante pour détecter les défaillances qui ont un impact sur la valeur de position *interpolée*.

   ix) liste complémentaire de tous les défauts possibles du *codeur(SR)* à partir de la FMEDA, ou une définition complète des signaux d'essai;

      NOTE 6 Cette information permet à l'utilisateur de définir les essais d'intégrité du signal analogique spécifiques à l'application (voir Annexe L).

8) états de défaut du *codeur(SR)* et leur indication à l'unité d'évaluation;

9) dans le cas d'une application de sécurité à *codeur(SR)* unique et si l'accouplement n'est pas fourni en combinaison avec le *codeur(SR)*, une exclusion de défaut doit être exigée pour cet accouplement, conformément au Tableau G.1;

10) avertissements relatifs à une utilisation incorrecte du *codeur(SR)*;

   EXEMPLE 3 Utilisation de signaux de sortie potentiellement dangereux pour les *fonctions de sécurité*.

11) méthode de détection des connexions sinus/cosinus interverties; et

12) procédure de référence;

   NOTE 7 Cette procédure est appliquée pour régler le *codeur(SR)* à la position zéro.

e) Informations pour la maintenance
   1) exigences relatives aux essais, à l'étalonnage ou à la maintenance;
   2) processus de maintenance;
   3) plans de maintenance; et
   4) processus de réparation, de remplacement et de remise en service.

Annexe G
(informative)

Listes de *défauts* du *codeur(SR)* et exclusions de *défauts*

L'Annexe D de l'IEC 61800-5-2:2016 s'applique, à l'exception du Tableau D.8, qui est remplacé par le Tableau G.1 du présent document et par les résultats de la *FMEDA qualitative* (voir 8.4).

NOTE 1 La liste de *défauts* du Tableau G.1 n'est pas considérée comme exhaustive.

NOTE 2 Le Tableau D.8 de l'IEC 61800-5-2:2016 concerne l'utilisation d'un *codeur* non relatif à la sécurité avec un *PDS(SR)*. Les modèles de *défaut* généraux définis dans ce tableau ne sont pas nécessaires pour la conception d'un *codeur(SR)*, dans la mesure où les résultats de la *FMEDA qualitative* incluent les modèles de *défaut* spécifiques au produit concerné.

Tableau G.1 – *Codeur(SR)* – Liste de *défauts* mécaniques et exclusions de *défauts*

***Défaut* identifié**	**Exclusion de *défaut***	**Remarques**
Fixation desserrée ou qui se desserre lors de l'arrêt ou des mouvements: – boîtier de *codeur(SR)* du châssis moteur – arbre de *codeur(SR)* de l'arbre de moteur – montage de la tête de lecture	Préparer la FMEDA et démontrer: – la solidité permanente pour les raccordements à verrouillage par profil; – la solidité pour les raccordements à verrouillage par force.	La charge maximale admissible du *codeur(SR)* est indiquée ou limitée sur sa fiche technique. a) Pour les raccordements à verrouillage par profil: 1) Conception de la solidité permanente conforme à l'expérience technique généralement reconnue avec un coefficient de sécurité élevé: • la vérification est effectuée par calcul et par un essai approprié; • exemple pour les composants en acier: surdimensionnement avec un coefficient de sécurité $S \geq 2$ par rapport à la rupture par fatigue; ou 2) Surdimensionnement avec un coefficient de sécurité $S \geq 5$ par rapport à la rupture par fatigue: • la vérification est effectuée par calcul. b) Pour les raccordements à verrouillage par force: 1) Surdimensionnement avec un coefficient de sécurité $S \geq 4$ par rapport au glissement: • les mesures détaillées pour l'application et le maintien de la force de préchargement doivent être définies dans la documentation de l'utilisateur (par exemple, paires définies de matériaux, surfaces et méthodes de serrage à commande de couple); • la vérification est effectuée par calcul et par un essai approprié; ou 2) Surdimensionnement avec un coefficient de sécurité $S \geq 10$ par rapport au glissement: • les mesures pour l'application et le maintien de la force de préchargement doivent être définies dans la documentation de l'utilisateur; • la vérification est effectuée par calcul. c) Pour les raccordements mécaniques sans verrouillage par profil ni verrouillage par forme (les fixations adhésives et les soudures, par exemple), la méthode de dimensionnement et les coefficients de sécurité appropriés doivent être choisis.
NOTE Les coefficients de sécurité sont applicables aux forces statiques et dynamiques.		

Tableau G.2 – *Défauts* et exclusions de *défauts* pour le choix, le montage et le fonctionnement des roulements

***Défaut* à l'étude**	**Exclusion de *défaut***	**Commentaire**
Blocage de palier spontané	Oui, si: • le roulement a été dimensionné au moins conformément à l'ISO/TS 16281, en tenant compte des facteurs d'influence répertoriés dans le Tableau G.3; et • le roulement n'est pas un roulement massif en céramique.	Un blocage peut être provoqué par: • la rupture de parties du roulement à la suite d'un impact ou d'une surcharge; • le coincement de particules de matériau ou une contamination entre la cage de roulement et l'élément de roulement; • une lubrification insuffisante; • la rupture de la cage ou de l'élément de roulement; • la rupture des assemblages rivetés sur les cages en tôle d'acier; • la rouille lorsque le roulement n'est pas utilisé.
Blocage de palier progressif	Non	• Si l'exigence 6.5.4 2) a) s'applique, le roulement peut ne pas être pris en compte aux fins de la quantification; • si l'une des exigences 6.5.4 2) b), 2) c) ou 2) d) s'applique, – 10 FIT peuvent être appliqués aux fins de la quantification (voir également Tableau H.1); – les exclusions de défauts du Tableau G.1 sont toujours valables. La quantification du roulement tient généralement compte de l'augmentation du couple, de l'augmentation de la température, de l'augmentation du battement radial, etc.

Tableau G.3 – Facteurs qui exercent une influence sur le dysfonctionnement des roulements – Considérations relatives au choix, au montage et au fonctionnement

Facteur d'influence	**Commentaire**
Ajustement trop serré, prétension trop élevée	Peut être détecté par un accroissement du risque thermique ou de l'acoustique.
Ajustement trop lâche, prétension trop faible	Peut entraîner une corrosion de contact et une prétension décroissante.
Surcharge ou sous-charge	Forces mécaniques.
Frottement par glissement	Critique en cas de faibles vitesses, d'arrêts fréquents et de charge ou de prétension trop faible.
Défauts d'alignement ou déviation d'arbre	
Impact de vibrations	Peut être réduit par un découplage suffisant, ou par un "chargement" du roulement, par exemple. Il peut être nécessaire de prendre ce facteur en compte lors du choix d'un lubrifiant approprié.
Vitesses	Indiquer la vitesse maximale admissible dans les informations utilisateur.
Lubrifiant	Utiliser un lubrifiant adapté à l'application.
Fonctionnement en sens inverse	Le fonctionnement en sens inverse accroît l'usure. Il peut être nécessaire de prendre ce facteur en compte lors du choix d'un lubrifiant approprié.
Joint d'étanchéité de palier	Pour éviter les fuites de lubrifiant.
Lubrification excessive	Peut entraîner une surchauffe et, par conséquent, une réduction de la durée de mission de la graisse.

Facteur d'influence	Commentaire
Dimensionnement des pièces de montage de palier	
Méthode de montage et utilisation d'outils	Doit être appliquée conformément aux spécifications du fabricant du roulement, par exemple pour éviter la transmission des forces de montage par l'élément de roulement.
Corrosion	S'assurer de la manipulation adéquate lors du montage, par exemple dégraisser les roulements immédiatement avant montage dans le *codeur(SR)* et éviter la manipulation avec les mains moites.
Corrosion de contact	S'assurer de la manipulation adéquate lors du montage, par exemple dégraisser les roulements immédiatement avant montage dans le *codeur(SR)* et éviter la manipulation avec les mains moites. Des ajustements trop lâches peuvent provoquer une "rotation parallèle" des bagues et entraîner une corrosion de contact.
Basculement de palier	Dû à un manque de rigidité du boîtier, à des *défauts* de conception ou à des *défauts* de montage, par exemple.
Basculement du chemin de roulement externe au chemin de roulement interne sur les roulements à billes	
Manque de propreté lors du montage	
Passage de courant	Les roulements des moteurs électriques commandés par un convertisseur de fréquence, en particulier, peuvent être affectés par le passage de courant ou même par un claquage de courant dans le roulement. Le lubrifiant brûle localement en laissant des résidus de combustion, ce qui altère considérablement l'effet lubrifiant, et conduit finalement à la défaillance du roulement.
Impact de la contamination, des agents agressifs et de l'eau	Peut être réduit en adaptant la conception du boîtier et en établissant des règles d'application.
Impact des sources de chaleur externes	
Lubrification inadéquate	Peut se produire lors du redémarrage après une période prolongée sans fonctionnement en raison de problèmes affectant la distribution du lubrifiant.
Matage	Le matage est également appelé "marques inactives", "formation de rainures" ou "formation de bosses", et est provoqué par des vibrations ou des déformations élastiques. Ces micromouvements endommagent la surface lisse du roulement, ce qui se traduit par un fonctionnement plus bruyant, une usure, puis une défaillance. Ne se produit que sous des forces élevées.
NOTE 1 La liste du Tableau G.3 n'a pas vocation à être exhaustive. NOTE 2 Consulter les informations fournies par le fabricant du roulement pour obtenir des précisions.	

Annexe H
(informative)

Quantification

H.1 Généralités

Pour obtenir une estimation quantitative de la fiabilité relative à la sécurité du *codeur(SR)* (quantification), la fréquence moyenne de *défaillance dangereuse* par heure (*PFH*) est calculée, et sa *capacité SIL* est déterminée.

Si la conformité à l'ISO 13849-1 est revendiquée, la catégorie et le *niveau de performance PL* du *codeur(SR)* sont également déterminés.

NOTE La méthode simplifiée définie par l'ISO 13849-1:2015 pour calculer la *PFH* n'est généralement pas applicable aux *codeurs(SR)* qui atteignent la *tolérance au premier défaut* (catégorie 3 ou catégorie 4) avec une structure monocanale avec *détection de défaut idéale*. Une structure monocanale avec une telle qualité de diagnostic n'est pas couverte par l'ISO 13849-1:2015.

Les étapes appropriées pour procéder à la quantification comprennent:

1) la spécification de l'architecture de sécurité et sa représentation sous forme de bloc-diagramme relatif à la sécurité;
2) la saisie des taux de défaillance du matériel contenu dans le bloc-diagramme relatif à la sécurité (mécanique, optique, électrique, électronique, etc.);
3) l'adaptation des taux de défaillance dans les conditions de référence (également appelés "taux de défaillance de base") à des températures de service (températures de fonctionnement) réalistes;
4) la réalisation d'une *FMEDA quantitative* par bloc fonctionnel, y compris l'évaluation des mesures diagnostiques pour détecter les *défauts* dans le *codeur(SR)*;
5) en cas de redondance, l'estimation du facteur de cause commune β;
6) l'estimation de la *PFH* à l'aide d'une méthode de modélisation mathématique appropriée;
7) l'estimation de la proportion de défaillances en sécurité (*SFF*); et
8) la détermination de la *capacité SIL* quantitative (limite *SIL* supérieure).

Si la conformité à l'ISO 13849-1:2015 est revendiquée, les étapes supplémentaires suivantes s'appliquent:

9) estimation de la $MTTF_D$ d'un canal;
10) détermination de la capacité de catégorie quantitative; et
11) détermination de la capacité *PL* quantitative.

Ces étapes sont expliquées aux Articles H.2 à H.10.

H.2 Architecture de sécurité et bloc-diagramme relatif à la sécurité

Pour déterminer la contribution du *codeur(SR)* aux *fonctions de sécurité* qui doivent être réalisées avec celui-ci, l'ensemble de son matériel (mécanique, optique, électronique, etc.) est subdivisé en blocs fonctionnels selon l'architecture universelle décrite à l'Annexe B.

En observant l'interaction des blocs fonctionnels pendant l'exécution de la *sous-fonction de sécurité*, il doit être déterminé s'il existe une redondance et en quels points. En cas de redondance, les défaillances de cause commune doivent être prises en considération si elles ne peuvent être exclues à juste titre.

Pour chaque bloc fonctionnel, il doit être déterminé s'il existe des diagnostics en ligne (par exemple, des diagnostics automatiques pendant le fonctionnement) et quel matériel (interne ou externe au *codeur(SR)*) effectue ces diagnostics, et s'il existe de bonnes raisons d'exclure les *défauts* dans le bloc.

Les informations recueillies sont représentées dans un bloc-diagramme relatif à la sécurité (voir [12] pour plus d'informations). Les blocs fonctionnels organisés logiquement en série peuvent (mais ne doivent pas obligatoirement) être regroupés en un bloc. En tant que bloc-diagramme de fiabilité authentique, le bloc-diagramme relatif à la sécurité représente les liens logiques entre les blocs fonctionnels et répertorie également les diagnostics disponibles. De façon appropriée, toutes les variables exigées pour la quantification, telles que les taux de défaillance, les *couvertures du diagnostic* et les facteurs de cause commune, peuvent être saisies et attribuées aux différents blocs fonctionnels.

H.3 Taux de défaillance

Les taux de défaillance des composants électriques, électroniques et optoélectroniques largement utilisés peuvent être consultés dans les collections reconnues de taux de défaillance génériques, par exemple SN 29500 [13]. Dans le cas de composants spéciaux (ASIC, par exemple), il convient qu'ils soient indiqués par le fabricant du composant. Les erreurs logicielles doivent être traitées conformément à l'IEC 61508-2:2010.

Pour l'estimation du taux de défaillance mécanique d'un composant, il convient que la procédure hiérarchique de recherche des données soit la suivante, dans l'ordre indiqué:

a) utiliser des données de terrain, si une expérience appropriée sur le terrain est disponible (sur la base de plus de 50 % de la durée de vie spécifiée);

b) obtenir des données à partir d'essais d'endurance en combinaison avec le schéma de calcul de l'ISO 13849-1:2015, C.4.2 "Calcul du $MTTF_D$ pour les composants à partir de B_{10D}";

c) utiliser les données de bases de données appropriées, qui ont été obtenues à partir d'applications similaires ou comparables (par exemple, à partir de données de terrain, [14] ou [15]);

d) se conformer au Tableau H.1;

e) fixer la $MTTF_D$ à 150 ans, conformément au Tableau C.1 de l'ISO 13849-1:2015.

NOTE $\lambda_D = 1/MTTF_D$.

Le Tableau H.1 donne des informations sur certains composants à prendre en considération lors de la quantification.

Tableau H.1 – Composants du *codeur(SR)* et leur inclusion dans la quantification

Composant	Inclus dans la quantification?	Remarque
Boîtier	Non	
Roulement, complet, avec joint d'étanchéité éventuel	Oui	Pour les exclusions de *défauts*, voir Tableau G.2. 10 FIT si aucune autre source de données pour l'estimation n'est disponible[a, b].
Joints d'étanchéité entre parties fixes	Non	
Composants électroniques et électriques (par exemple, fiche secteur)	Oui	

Composant	Inclus dans la quantification?	Remarque
Accouplement statorique avec résistance à la fatigue vérifiée	Non	Voir 6.5.2 La résistance à la fatigue justifie l'exclusion de *défaut* exigée.
Accouplement arbre-rotor avec résistance à la fatigue vérifiée	Non	Voir 6.5.2 La résistance à la fatigue justifie l'exclusion de *défaut* exigée.
Engrenage	Oui	$MTTF_D$ = 150 ans si aucune autre source de données pour l'estimation de la $MTTF_D$ n'est disponible[c].
Eléments de fixation et propriétés des matériaux du système *codeur(SR)* au sein du *codeur(SR)*	Non	
Indicateur statique	Oui	Cela n'a pas à être pris en compte dans la quantification tant que les dommages ou la contamination (voir 6.6.2) ne peuvent pas entraîner de *défaillance dangereuse* ou qu'une exclusion de *défaut*, justifiée conformément à l'Annexe A de l'ISO 13849-2:2012, s'applique. Si aucune valeur numérique n'est disponible pour l'estimation de la $MTTF_D$, il peut être admis par hypothèse que la $MTTF_D$ = 150 ans (voir l'ISO 13849-1:2015, Tableau C.1, composants mécaniques).
Fixation de l'*indicateur statique*	Oui	Cela n'a pas à être pris en compte dans la quantification tant qu'une exclusion de *défaut* est justifiée conformément à l'Annexe A de l'ISO 13849-2:2012.
Liaisons adhésives (par exemple, liaison entre l'*indicateur statique* et l'arbre)	Oui	Cela n'a pas à être pris en compte dans la quantification tant qu'une exclusion de *défaut* est justifiée conformément à l'Annexe A de l'ISO 13849-2:2012.

[a] Tous les *défauts* qui affectent le composant de roulement sont considérés comme des *défaillances dangereuses*. Une division de 50 %/50 % des défauts en tant que dangereux et sûrs n'est donc pas possible.

[b] D'après [14], Part 02, Mechanical, 6.1 Bearings, M.1.2 Bearing, Rolling, page 42: 10 FIT pour les profils 1, 2, 3 (Profil 1: Montés en armoire, 2: Produits du domaine mécanique avec autoéchauffement minimal, 3: Produits du domaine général avec autoéchauffement modéré); le seul mode de défaillance est BIND (moment augmenté); le terme BIND est utilisé dans [14] pour désigner le *blocage de palier* et confirmé par les données de terrain du fabricant du *codeur(SR)*.

[c] Si l'engrenage est conçu selon les principes de bonne pratique d'ingénierie, en appliquant des principes de sécurité fondamentaux et éprouvés (voir [12], Annexe D.2.5).

H.4 Taux de défaillance à des températures de fonctionnement réalistes

Les taux de défaillance de certains composants dépendent fortement de la température. Il convient donc de prendre en compte la température prévue des composants dans le cadre de l'application pour déterminer leurs taux de défaillance.

Par exemple, de nombreux *codeurs(SR)* rotatifs sont fixés à proximité du moteur et, en raison de l'importante transmission de chaleur par le biais de l'arbre, fonctionnent donc régulièrement et systématiquement (et non seulement de manière aléatoire et occasionnelle) près de leur limite de température supérieure admise. Le frottement des paliers et du joint d'étanchéité contribue également à l'échauffement.

Les taux de défaillance et, à partir de ceux-ci, les *PFH* pour cette application admissible, doivent être calculés et indiqués, en gardant à l'esprit que la température ambiante n'est pas toujours égale à la valeur limite supérieure. Il en est par exemple tenu compte comme suit:

$$T_{\text{PFH}} = T_{\text{work}} + T_{\text{delta}} - 15\ \text{K}$$

où

T_{delta} est la différence de température entre la température de fonctionnement et la température maximale du composant.

NOTE 1 Une déduction de 15 K tient compte du fait que les *codeurs(SR)* ne fonctionnent pas continuellement à la température maximale admise.

En variante, l'effet des températures de fonctionnement réalistes peut être évalué de façon plus précise en appliquant le facteur de profil de contrainte π_{W} calculé selon SN 29500 (voir [13]).

Les valeurs de *PFH* peuvent également être calculées et indiquées pour des températures de fonctionnement plus basses.

Les taux de défaillance dans les conditions de référence peuvent être convertis en taux de défaillance à d'autres températures (généralement plus élevées) en multipliant les taux par un facteur de correction de température π_{T}. Des équations adaptées à ces facteurs de correction spécifiques aux composants sont données dans l'IEC 61709 [16].

NOTE 2 La collection SN 29500 [13] de taux de défaillance adopte les facteurs de correction de l'IEC 61709 [16].

H.5 *FMEDA quantitative* et évaluation des mesures diagnostiques

Pour chacun des blocs fonctionnels répertoriés dans le bloc-diagramme relatif à la sécurité, une *FMEDA quantitative* est utilisée pour déterminer les taux de défaillance dans la direction dangereuse λ_{D} et, à partir de là, la proportion λ_{DD} identifiable au moyen de diagnostics.

NOTE 1 Dans le cas de blocs fonctionnels redondants, la défaillance d'un bloc n'entraîne pas la perte de la *fonction de sécurité*. Dans ce cas, λ_{D} désigne le taux de défaillance du bloc dans la direction dangereuse (perte de la fonction du bloc concerné).

Afin de déterminer dans un premier temps le taux de défaillance d'un bloc fonctionnel seulement, la méthode de comptage des pièces, qui consiste à additionner les taux de défaillance de tous les composants du bloc, peut être adoptée dans le cas le plus simple. La formule suivante s'applique:

$$\lambda_{\text{D}} = \sum_{i} \lambda_i$$

où

λ_i représente les taux de défaillance des différents composants du bloc.

En procédant à la *FMEDA quantitative* plus précise, il est néanmoins possible de calculer un taux de défaillance de bloc plus favorable (inférieur) dans la direction dangereuse λ_D. La condition préalable à la classification d'une défaillance donnée comme dangereuse (D) ou sûre (S) est que la *fonction de sécurité* et, par conséquent, la direction de *défaillance dangereuse* du bloc fonctionnel soient connues, car il est impossible sans cela de déterminer si la *fonction de sécurité* est compromise (D) ou non (S) par la défaillance. Sur un *codeur(SR)* universel qui doit être utilisé pour différentes *fonctions de sécurité* inconnues, seuls certains types de défaillances peuvent être classés avec certitude comme sûrs (S). Une évaluation globale de la moitié du taux de défaillance des composants comme "S" n'est donc pas appropriée. Néanmoins, les contributions suivantes peuvent être éliminées par la *FMEDA quantitative* de la somme des taux de défaillance pour obtenir λ_D:

- les taux de défaillance des composants qui ne sont ni directement ni indirectement impliqués dans l'exécution de la *sous-fonction de sécurité* (défaillances qui ne concernent aucune partie);
- les taux de défaillance des composants dont la défaillance n'a aucun effet sur l'exécution de la *sous-fonction sécurité* (défaillances sans effet); et
- taux relatifs à certaines directions de défaillance de composant, dont l'occurrence n'a aucun effet sur l'exécution de la *sous-fonction de sécurité* (défaillances sans effet).

NOTE 2 Les éléments suivants peuvent servir de référence pour estimer cette proportion:

– IEC 61709;

– répartition des types de défaillances enregistrée dans les outils de FMEDA.

Un changement inutile de source pour la répartition des types de défaillances d'un composant à l'autre n'est pas admissible.

Si la *détection de défaut idéale* est exigée dans une ou plusieurs partie(s) monocanale(s) du *codeur(SR)*, les défaillances dans la direction dangereuse doivent être détectées dans leur intégralité afin de satisfaire au critère de *tolérance au premier défaut*. Par conséquent, il ne doit y avoir aucune *défaillance dangereuse*, non détectable. Pour une estimation prudente, par exemple une estimation du côté sûr, une *DC* = 99 % est fixée pour le calcul de la *PFH*.

Dans les parties redondantes du *codeur(SR)*, la *couverture du diagnostic* de chaque défaillance dans la direction dangereuse doit être estimée de façon individuelle. Des recommandations concernant l'estimation sont fournies par les tableaux de l'Annexe A de l'IEC 61508-2:2010 et de l'Annexe E de l'ISO 13849-1:2015. Pour la première *défaillance dangereuse* d'un composant i d'un bloc fonctionnel, le taux de *défaillance dangereuse* est donc divisé entre la proportion détectable

$$\lambda_{i\,\mathrm{DD}} = DC_i \cdot \lambda_{i\,\mathrm{D}}$$

et la proportion non détectable

$$\lambda_{i\,\mathrm{DU}} = \left(1 - DC_i\right) \cdot \lambda_{i\,\mathrm{D}} .$$

Pour un bloc fonctionnel (FB, *Functional Block*) ou une disposition logique de blocs fonctionnels en série, une *couverture du diagnostic* moyenne est obtenue par la formule suivante:

$$DC_{\mathrm{FB}} = \frac{\sum_i \lambda_{i\,\mathrm{DD}}}{\sum_i \lambda_{i\,\mathrm{D}}}$$

NOTE 3 Un exemple de *FMEDA quantitative* est donné dans [12].

H.6 Estimation du facteur de cause commune *β* (uniquement en cas de redondance)

La méthode décrite à l'Annexe D de l'IEC 61508-6:2010 ou une estimation justifiée sont adaptées. Si la conformité à l'ISO 13849-1 est revendiquée, l'Annexe F de l'ISO 13849-1:2015 est applicable en variante.

NOTE La méthode de l'ISO 13849-1:2015 ne permet de justifier l'estimation qu'avec un facteur de cause commune de 2 %. La méthode détaillée de l'IEC 61508-6 permet d'obtenir d'autres valeurs pour le facteur de cause commune.

H.7 Estimation de la *PFH*

Selon l'architecture matérielle et les variables d'entrée qui doivent être prises en compte, une méthode de calcul appropriée pour l'estimation de la *PFH* est choisie. Cette méthode utilise comme variables d'entrée les taux de défaillance relatifs aux blocs fonctionnels et *couvertures du diagnostic* calculées à l'aide de la *FMEDA quantitative* relative aux blocs fonctionnels. En cas de redondance, le facteur de cause commune β est également utilisé.

H.8 *Proportion de défaillances en sécurité* (*SFF*)

Afin de vérifier la *capacité SIL* quantitative maximale (limite *SIL* supérieure) (voir H.9) conformément à l'IEC 61800-5-2, la *proportion de défaillances en sécurité* (*SFF*) doit être estimée en premier lieu. Si l'architecture est constituée de sous-systèmes de *HFT* différente, cela doit être effectué séparément pour chaque sous-système.

La *SFF* est calculée à l'aide de la formule suivante:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D}$$

NOTE 1 Les taux de défaillance "qui ne concernent aucune partie et sans effet" ne sont pas pris en compte dans le calcul de la *SFF*.

NOTE 2 Le calcul de la *SFF* peut parfois être évité (voir Article H.9).

H.9 Détermination de la *capacité SIL* quantitative

H.9.1 Généralités

Selon l'IEC 61800-5-2:2016, il existe deux considérations quantitatives, qui imposent une limite au *SIL* atteignable par une *fonction de sécurité* qui utilise un *codeur(SR)*: les contraintes architecturales et la *PFH*.

H.9.2 Limite du *SIL* par les contraintes architecturales

La limite du *SIL* par les contraintes architecturales concerne les sous-systèmes qui réalisent des *fonctions de sécurité*.

Un sous-système se caractérise par:

- une *tolérance aux anomalies du matériel* (*HFT*) uniforme;
- un type (A ou B, voir 6.2.3.2.2 et 6.2.3.2.3 de l'IEC 61800-5-2:2016); et
- une *proportion de défaillances en sécurité* (*SFF*, voir Article H.8).

Le *codeur(SR)* peut par exemple faire partie d'un sous-système (dispositif avec signaux de sortie sinus et cosinus, qui nécessite des diagnostics externes, par exemple) ou peut comprendre un ou plusieurs sous-systèmes (dispositif qui contient entièrement ses diagnostics nécessaires, par exemple). Dans tous les cas, conformément à l'IEC 61800-5-2, chaque sous-système, qui comprend le *codeur(SR)* en tant qu'élément ou qui fait partie du *codeur(SR)*, doit être examiné pour déterminer le *SIL* maximal en fonction des contraintes architecturales.

La procédure de détermination de la limite du *SIL* utilise les trois propriétés susmentionnées du sous-système (*HFT*, type, *SFF*) et est décrite en 6.2.3 de l'IEC 61800-5-2:2016.

Habituellement, la *proportion de défaillances en sécurité* (*SFF*) est calculée à partir des résultats de la *FMEDA quantitative* (voir Article H.5). Toutefois, le calcul de la *proportion de défaillances en sécurité* (*SFF*) et donc la détermination de λ_S peuvent être évités, si une *couverture du diagnostic* (*DC*) suffisamment élevée a déjà été établie. Dans ce cas, l'inégalité

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} \geq \frac{\sum \lambda_{DD}}{\sum \lambda_D} = DC$$

admet l'utilisation de la *DC* comme limite inférieure de la *SFF*.

H.9.3 Limite du *SIL* par la *PFH*

Habituellement, un *codeur(SR)* ne fournit pas une *fonction de sécurité* complète, mais contribue à une *sous-fonction de sécurité* (voir 4.2 de l'IEC 61800-5-2:2016). Au sens large, la *sous-fonction de sécurité* fournit les informations sûres nécessaires à l'exécution de la *fonction de sécurité*. Dans la mesure où la *PFH* se rapporte toujours à une fonction, une valeur de *PFH* ne peut être attribuée de façon significative qu'à la *sous-fonction de sécurité* fournie par le *codeur(SR)*.

Du point de vue matériel, soit le *codeur(SR)* constitue un élément d'un sous-système (dispositif avec signaux de sortie sinus et cosinus, qui nécessite des diagnostics externes), soit il peut être constitué d'un ou plusieurs sous-systèmes (dispositif qui contient entièrement ses diagnostics nécessaires). Dans tous les cas, la *PFH* de l'unité fonctionnelle, qui assure la *sous-fonction de sécurité* qui vise à fournir des informations sûres, doit être déterminée. Les diagnostics mis en œuvre pour cette unité fonctionnelle sont pris en compte dans le calcul de la *PFH*.

La *PFH* de la *sous-fonction de sécurité* qui fournit les informations sûres acquises par le *codeur(SR)* ne représente qu'une seule contribution à la *PFH* de la *fonction de sécurité* complète. Par conséquent, il convient que la *PFH* de la *sous-fonction de sécurité* ne dépasse pas une proportion donnée de la limite supérieure de la *PFH* du *SIL* prévu de la *fonction de sécurité* complète. La corrélation entre la *PFH* et le *SIL* est indiquée dans le Tableau 3 de l'IEC 61800-5-2:2016. Finalement, la *PFH* de la *sous-fonction de sécurité* limite également le *SIL* qui peut en pratique être atteint pour les *fonctions de sécurité* utilisant le *codeur(SR)*.

NOTE La capabilité systématique constitue une troisième limite, à base qualitative, du *SIL* atteignable, exprimée par le *SIL* maximal qui peut être revendiqué d'après le degré de robustesse par rapport aux défaillances systématiques (voir IEC 61508-2). La *capacité SIL* globale est constituée par la plus faible de ces trois limites: la limite du *SIL* par les contraintes architecturales, la limite du *SIL* par la *PFH*, et la capabilité systématique.

H.10 Considérations complémentaires en vue de la conformité à l'ISO 13849-1

H.10.1 Généralités

Si la conformité à l'ISO 13849-1:2015 est revendiquée, l'Article H.10 s'applique.

H.10.2 $MTTF_D$ d'un canal

Pour l'attribution d'une catégorie selon l'ISO 13849-1 (voir H.10.3), la $MTTF_D$ d'un seul canal doit être prise en considération. Pour son calcul, le ou les canaux qui exécutent la *fonction de sécurité* sont identifiés dans le bloc-diagramme relatif à la sécurité. Les parties impliquées de manière indirecte dans l'exécution de la fonction (par exemple, les circuits de commande en tension) doivent également être incluses. Les parties utilisées uniquement à des fins de diagnostic ne peuvent être exclues que si elles n'interfèrent pas avec la *sous-fonction de sécurité*. En cas de canaux redondants, le canal qui présente le taux de défaillance le plus élevé (le plus défavorable) doit être choisi, ce qui donne le taux de défaillance d'un seul canal dans la direction dangereuse $\lambda_{OC\,D}$ ("OC" signifie "one channel", un seul canal). Pour la $MTTF_D$ d'un canal, la formule suivante s'applique alors:

$$MTTF_D = \frac{1}{\lambda_{OC\,D}}$$

H.10.3 Détermination de la capacité de catégorie quantitative

Les catégories 3 et 4 admissibles, conformément à l'ISO 13849-1:2015, imposent des exigences concernant la $MTTF_D$ et la DC_{avg} du canal (ou des canaux, éventuellement) de fonction. Pour calculer la $MTTF_D$ et la DC_{avg}, les données obtenues à partir de la *FMEDA quantitative* (voir Article H.5) peuvent être utilisées.

NOTE Les exigences imposées par les différentes catégories en ce qui concerne la $MTTF_D$ et la DC_{avg} peuvent être consultées en 6.2 de l'ISO 13849-1:2015.

H.10.4 Détermination de la capacité *PL* quantitative

Le Tableau 2 de l'ISO 13849-1:2015 définit les limites supérieures, dépendantes du *PL*, de la *PFH* des *fonctions de sécurité*. Cela signifie que la *PFH* du *codeur(SR)* établit une limite supérieure pour le *PL* auquel le *codeur(SR)* peut être utilisé.

Annexe I
(informative)

Traitement numérique des signaux sinus/cosinus

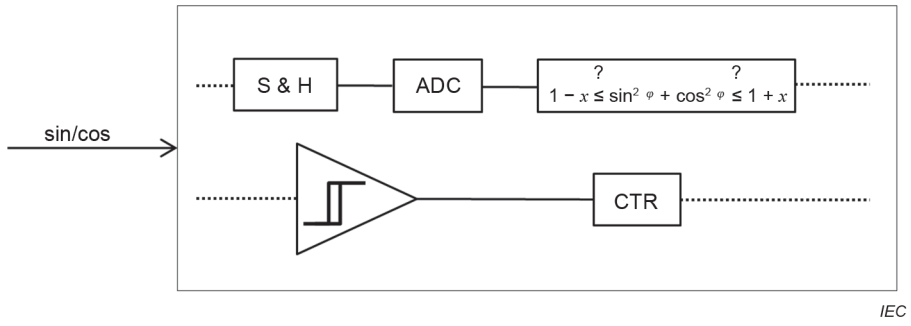
I.1 Généralités

Lorsque les signaux de sortie d'un *codeur(SR)* avec signaux de sortie sinus et cosinus sont traités par technique numérique (matérielle ou logicielle), l'échantillonnage des signaux et leur conversion en valeurs numériques s'effectuent dans l'*unité d'évaluation*. L'Annexe I décrit les effets de cette méthode ainsi que les impacts possibles sur la mesure et la détection de *défaut*.

NOTE Les effets traités dans la présente Annexe I peuvent également se produire dans d'autres types de *codeurs(SR)* qui procèdent au traitement numérique des signaux au sein même du *codeur(SR)*.

I.2 Echantillonnage des signaux sinus et cosinus

L'effet sur l'échantillonnage est expliqué par un exemple spécifique. La Figure I.1 représente l'architecture matérielle.



Légende

sin/cos une paire de signaux de sortie sinus et cosinus du *codeur(SR)*

S&H échantillonneur bloqueur

ADC convertisseur analogique/numérique

CTR compteur d'impulsions incrémentales

Figure I.1 – Echantillonnage numérique des signaux sinus et cosinus – Architecture matérielle, exemple

Une *unité d'évaluation* sûre est utilisée comme échantillonneur bloqueur, convertisseur analogique/numérique, détecteur de *défaut* par surveillance de la longueur de phaseur, détecteur de pentes et compteur de pentes. Sur la Figure I.2, les figures de Lissajous des signaux sinus et cosinus A et B sont représentées pour 4 échantillons/période, à S1, S2, S3 et S4. Les pentes extraites de A et de B sont générées par une bascule de Schmitt avec les niveaux de commutation A_{on}/A_{off} et B_{on}/B_{off}. Pour mesurer la position, les pentes de A et de B sont comptées. Les mesures diagnostiques de cet exemple appliquent la vérification de la longueur de phase

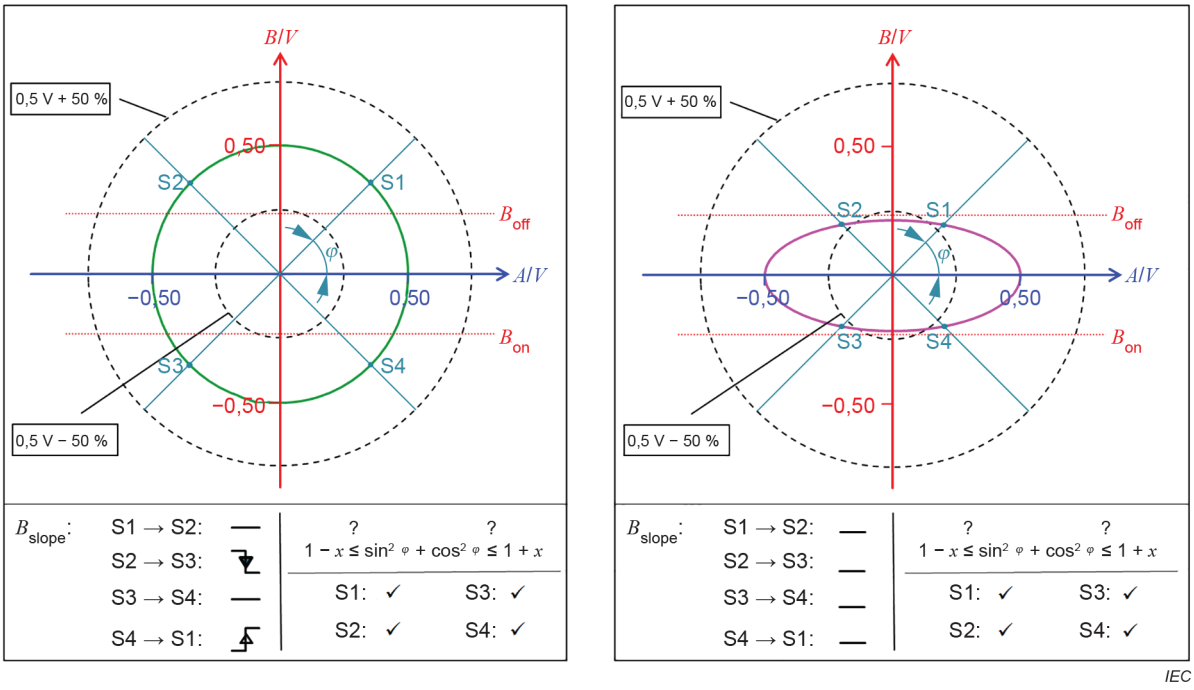
$$1 - x \overset{?}{\leq} sin^2\varphi + cos^2\varphi \overset{?}{\leq} 1 + x$$

à chaque échantillon. La Figure I.2 a) représente une condition d'absence d'*anomalie* pour 4 échantillons par période avec un échantillonnage à 45°, 135°, 225° et 315°. La bascule de Schmitt fonctionne correctement et la surveillance de la longueur de phaseur est correcte.

Sur la Figure I.2 b), l'amplitude du signal B est défectueuse, trop faible, mais la détection échoue:

- la bascule de Schmitt n'identifie pas les pentes du signal B, car l'amplitude du signal B reste dans l'hystérésis B_{on}/B_{off};
- la longueur de phaseur est correcte aux points d'échantillonnage, de sorte que la *défaillance dangereuse* n'est pas détectée; et
- l'*unité d'évaluation* détecte l'arrêt, alors que la partie de la machine est en mouvement.

NOTE Lorsque l'*interpolation* des signaux sinus et cosinus est appliquée, la détection de la position sur une période est erronée.



a) Aucune *anomalie* **b) Signal *B* trop faible, échec de la détection**

Légende

A	signal sinus différentiel (en volt)
B	signal cosinus différentiel (en volt)
B_{on}, B_{off}	seuils de commutation de la bascule de Schmitt de B
B_{slope}	signal de pente extrait de B
φ	valeur de position (continue)
S1, S2, S3, S4	points d'échantillonnage de la figure de Lissajous

Figure I.2 – Figures de Lissajous des signaux sinus et cosinus A et B

I.3 Conséquences

Cet exemple montre que les mesures diagnostiques peuvent échouer du fait de certaines conditions temporelles. Dans cet exemple, les points d'échantillonnage admis par hypothèse se situent à 45°, 135°, 225° et 315°, mais ces valeurs ne sont pas constantes, dans la mesure où il n'y a pas de synchronisation. Avec la variation de l'angle de phase, l'*anomalie* peut être détectée. Le nombre de périodes pendant lesquelles l'*anomalie* peut rester non détectée est spécifique à l'application. Cela dépend:

- du nombre d'échantillonnages par période sinus/cosinus (il convient qu'il soit élevé);
- de la vitesse de rotation/vitesse;

- de l'hystérésis (il convient qu'elle soit faible); et
- des tolérances admises de la longueur de phase (il convient qu'elles soient faibles).

NOTE Une faible hystérésis et de faibles tolérances pour la surveillance de la longueur de phaseur améliorent les diagnostics, mais peuvent dégrader la disponibilité, les perturbations du signal pouvant être interprétées comme des *anomalies*.

I.4 Mesures qui visent à améliorer la *DC*

Une combinaison de mesures appropriées est recommandée pour éviter que les mesures diagnostiques n'échouent en raison de l'échantillonnage. La liste suivante, non exhaustive, présente quelques mesures appropriées:

- les limites de détection de pente correspondent aux tolérances admises pour la surveillance de la longueur de phaseur, de sorte qu'une défaillance de signal sinus/cosinus est détectée avant l'échec du comptage;
- le fabricant du *codeur(SR)* définit un taux d'échantillonnage minimal; un taux d'échantillonnage minimal de 6 échantillons/période est recommandé; il convient de tenir également compte de la variation possible de l'angle de phase entre les signaux sinus et cosinus;
- le fabricant de l'*unité d'évaluation* définit un nombre maximal de périodes sinus/cosinus nécessaires pour détecter une défaillance du *codeur(SR)*;

  NOTE 1 Cela peut avoir une incidence sur les marges de sécurité à prendre en considération dans les *fonctions de sécurité* de l'application.

- lorsque le comportement de la boucle de commande est utilisé pour la détection de *défaut*, l'application du *codeur(SR)* à des fins de surveillance peut être exclue; et

  NOTE 2 Une boucle de commande d'un *PDS(SR)* qui utilise un *codeur(SR)* peut aussi fonctionner temporairement sans capteur, négligeant pendant un certain temps les signaux du *codeur(SR)* et ne contribuant donc pas à la détection de *défaut*.

- utiliser uniquement l'*évaluation des signaux* analogiques, avec un nombre suffisant d'échantillons par période, et délaisser les comparateurs et leurs seuils d'hystérésis pour générer des signaux binaires à partir du signal analogique *B*; en appliquant cette mesure à l'exemple donné à l'Article I.2, le mouvement est toujours correctement évalué et la dégradation du signal B est détectée en peu de temps par une surveillance complémentaire de l'amplitude.

Annexe J
(informative)

Architecture monocanale avec *détection de défaut idéale*

J.1 Généralités

La plupart des *codeurs(SR)* satisfont au *SIL* 2 ou 3, conformément aux normes IEC, ainsi qu'au *PL* d ou e et à la catégorie 3 ou 4, conformément à l'ISO 13849-1. Les exigences de ces normes sont similaires, mais elles ne sont pas identiques. Une différence importante concerne la *HFT* exigée. L'exigence de l'ISO 13849-1 pour les catégories 3 et 4 est qu'un défaut unique n'entraîne pas la perte de la fonction de sécurité; dans la plupart des cas, elle est réalisée au moyen d'architectures matérielles redondantes. Les normes IEC admettent quant à elles une *HFT* = 0 jusqu'au *SIL* 3, en fonction de la *SFF*. Pour concevoir un *codeur(SR)* monocanal qui fournit une *tolérance au premier défaut*, le concept de "*détection de défaut idéale*" s'applique.

J.2 *Détection de défaut idéale* pour un *codeur(SR)* avec signaux de sortie sinus et cosinus

L'expression "*détection de défaut idéale*" décrit une propriété exceptionnelle d'un *codeur(SR)* avec signaux de sortie sinus et cosinus, qui permet aux architectures monocanales de satisfaire à l'exigence de *tolérance au premier défaut*, conformément à l'ISO 13849-1.

L'ISO 13849-1 définit plusieurs catégories, tout sous-système relatif à la sécurité devant satisfaire à l'une d'entre elles. Ces définitions décrivent un comportement du système par rapport aux défaillances de composant spécifiques à la catégorie correspondante.

NOTE 1 Il est important de reconnaître que les définitions des catégories 3 et 4 ne précisent pas une architecture matérielle spécifique, mais seulement le comportement lié à la sécurité.

Pour les *codeurs(SR)*, les catégories 3 et 4 (ISO 13849-1:2015, 6.2.6 et 6.2.7) sont les catégories les plus pertinentes. L'une des principales exigences de ces catégories est qu'un défaut unique n'entraîne pas la perte de la fonction de sécurité. Cette exigence est généralement remplie par une architecture de sécurité qui comprend deux canaux indépendants. Toutefois, les *codeurs(SR)* avec signaux de sortie sinus et cosinus comprennent dans la plupart des cas des goulots d'étranglement monocanaux sans aucune exclusion de *défaut* possible, comme un circuit opto-ASIC commun pour la génération des signaux sinus et cosinus. En outre, les *unités d'évaluation* traitent habituellement les signaux sinus et cosinus de façon combinée, en raison, par exemple, de l'application de circuits intégrés décodeurs en quadrature, ou car la direction du mouvement doit être détectée pour exécuter la *fonction de sécurité*. Ces *codeurs(SR)* fournissent donc une architecture monocanale.

Néanmoins, en raison de la nature analogique des signaux sinus et cosinus, et de la capacité extraordinaire correspondante des mesures diagnostiques pour détecter les défauts, les *codeurs(SR)* monocanaux peuvent satisfaire à l'exigence de *tolérance au premier défaut* en appliquant la détection de *défaut* et la réponse aux défauts dans le *temps de sécurité du processus*:

- tous les *défauts dangereux* peuvent être détectés; et
- une réponse adéquate aux *défauts* est initiée assez rapidement après l'apparition d'une *défaillance dangereuse* afin d'éviter qu'un événement dangereux ne se produise.

Etant donné qu'aucune *fonction de sécurité* particulière n'est spécifiée pour un *codeur(SR)* destiné à une utilisation relative à la sécurité universelle, tout *défaut* qui peut altérer le nombre de périodes détecté par l'unité de *traitement subséquent des signaux* doit être traité comme un *défaut dangereux*. Cela s'applique aux signaux sinus comme aux signaux cosinus.

La détection de TOUS les *défauts dangereux* est assez difficile; un court-circuit ou une coupure dans un circuit intégré peut notamment modifier la conception du circuit et donc sa fonctionnalité. Néanmoins, tous les *défauts dangereux* ont un impact sur les signaux sinus et/ou cosinus, quel que soit le *défaut* dans le matériel du *codeur(SR)*. Cela peut être détecté, par exemple, par la surveillance de la longueur de phaseur, avec les tolérances appropriées. L'adéquation des mesures diagnostiques peut être démontrée au moyen de l'"analyse statique" (voir Annexe L).

La méthode d'"analyse statique" ne tient compte d'aucune considération temporelle concernant la mise en œuvre et l'application. Par conséquent, l'aspect temporel doit être pris en considération séparément. Voir également Annexe L.

NOTE 2 Dans la mesure où la *détection de défaut idéale* implique l'application de la détection de *défaut* et de la réponse aux défauts dans le *temps de sécurité du processus* pour toute défaillance dangereuse qui ne peut pas être exclue, un *défaut* unique du *codeur(SR)* avec signaux de sortie sinus et cosinus ne peut pas affecter de manière négative le comportement sûr du système. Par conséquent, conformément aux règles relatives à l'obtention de la capabilité systématique énoncées en 7.4.3 de l'IEC 61508-2:2010, la capabilité systématique du *codeur(SR)* avec signaux de sortie sinus et cosinus peut réduire le *SIL* prévu de la *fonction de sécurité* d'une étape *SIL*.

Annexe K
(informative)

Spécifications relatives à un *codeur(SR)* incrémental monocanal avec signaux de sortie sinus et cosinus

K.1 Généralités

L'Annexe K fournit des informations spécifiques pour les *codeurs(SR)* incrémentaux qui revendiquent la catégorie 3 ou la catégorie 4 conformément à l'ISO 13849-1 et incluent des architectures monocanales dans au moins un bloc fonctionnel. Ces *codeurs(SR)* exigent une *détection de défaut idéale* afin de fournir une *tolérance au premier défaut*.

K.2 *Tolérance au premier défaut*

La plupart des *fonctions de sécurité* exigent une détection fiable de la direction du mouvement. Les signaux sinus et cosinus sont nécessaires à cette fin. Si l'un des signaux est défectueux, l'identification correcte de la direction du mouvement ne peut plus être assurée. Aussi, les chemins de signal pour les signaux sinus et cosinus n'offrent aucune redondance pour l'identification de la direction du mouvement. Cela s'applique également lorsque, dans une *fonction de sécurité*, l'*interpolation* s'effectue à l'aide des signaux sinus et cosinus. La *tolérance au premier défaut* est néanmoins assurée tant que la *détection de défaut idéale* (voir Annexe J) s'applique.

Un *codeur(SR)* qui peut être utilisé uniquement pour la surveillance de la vitesse linéaire ou rotative indépendante de la direction peut être traité comme bicanal si le matériel du *codeur(SR)* est correctement configuré. Dans ce cas, l'*unité d'évaluation* doit traiter les deux canaux de manière indépendante. Voir également 6.4.1.

Les signaux sinus/cosinus sont souvent traités par le *codeur(SR)* à l'aide d'un ASIC unique à signaux analogiques ou mixtes. Les signaux analogiques ne sont pas numérisés. En raison de la forme des signaux sinus et cosinus et de l'angle de phase associé, il est peu probable que des *anomalies* aléatoires de parties du circuit qui conduisent à un *défaut* dangereux et non détectable se produisent. Pour ces ASIC, la *tolérance au premier défaut* peut donc être admise par hypothèse si la *détection de défaut idéale* est atteinte. Du fait de la *détection de défaut idéale*, une accumulation de *défauts* ne peut en principe pas se produire. Suivant une approche prudente, la catégorie atteignable est limitée à la catégorie 3 lorsqu'un seul ASIC est utilisé sans redondance sur la puce, conformément à l'Annexe E de l'IEC 61508-2:2010.

K.3 *Défauts* non détectables

Les *défauts* peuvent être détectés à la fois dans le *codeur(SR)* et dans l'*unité d'évaluation*. Si la *détection de défaut idéale* est exigée, la présence de *défauts* non détectables dans le *codeur(SR)* ne doit pas être possible.

Les mesures de détection des *défauts* dans l'*unité d'évaluation* ne sont possibles que sur la base des signaux de sortie. A moins que des mesures internes appropriées ne soient disponibles, la présence de *défauts* non détectables dans le *codeur(SR)* ne doit pas être possible (voir Article L.7). L'interversion des signaux sinus et cosinus par des multiplexeurs, l'inversion des signaux et la rupture de l'arbre d'entraînement d'un *codeur(SR)* rotatif sont des exemples de tels défauts.

K.4 Détection de *défaut* (*DC*)

Pour atteindre la *détection de défaut idéale* exigée, il convient que les mesures de détection des *défauts* et les seuils de commutation pour la détection quadratique soient parfaitement équilibrés. Autrement, il est possible, par exemple, que l'amplitude des signaux sinus ou cosinus varie de telle sorte que ce *défaut* n'est pas (encore) détecté par les mesures diagnostiques, mais que la détection du mouvement soit défectueuse en raison de seuils de commutation défavorables dans l'*unité d'évaluation*.

Sur les *codeurs(SR)* incrémentaux avec signaux de sortie sinus et cosinus, l'intégration monolithique des capteurs de position et des circuits analogiques pour la génération de signaux rend la FMEDA pratiquement impossible au niveau du transistor. Néanmoins, l'examen de l'*évaluation des signaux* et des mesures diagnostiques est possible en appliquant la méthode de l'"analyse statique des signaux de sortie et de la détection de *défaut*". Les signaux de sortie du *codeur(SR)* sont simulés et remplacés par une série de signaux d'essai qui représentent les *défauts* hypothétiques du *codeur(SR)* (voir Figure L.1).

En raison de la *tolérance au premier défaut* exigée et du canal unique, l'analyse statique doit démontrer que tous les *défauts* sont détectés par les mesures diagnostiques disponibles.

Pour une classification prudente des composants, une *DC* de 99 % doit être admise par hypothèse pour la quantification, même si tous les *défauts* sont détectés.

Pour l'exécution de l'analyse statique, il n'est pas pertinent de savoir si la détection de *défaut* s'effectue dans le *codeur(SR)* et/ou dans l'*unité d'évaluation*. Dans le cas d'un *codeur(SR)* dont les mesures internes sont insuffisantes ou inexistantes concernant la détection de *défaut*, des mesures de détection des *défauts* par l'*unité d'évaluation* peuvent être prévues. Ces mesures doivent être décrites dans les instructions d'utilisation.

La méthode d'analyse statique est décrite plus en détail à l'Annexe L.

NOTE Un outil qui prend en charge l'exécution de l'analyse statique est disponible (voir [17]).

Lorsque des mesures diagnostiques qui doivent être assurées par l'*unité d'évaluation* sont nécessaires, le comportement dynamique ne peut être pris en compte que par l'utilisateur. Il convient de s'assurer que le matériel utilisé pour l'*évaluation des signaux* et la *détection de défaut* fonctionne sans *anomalie* sur l'ensemble de la plage de fréquences prévue des signaux de sortie du *codeur(SR)*.

Annexe L
(normative)

Analyse statique de l'*évaluation des signaux* et de la détection de *défaut*

L.1 Généralités

L'Annexe L concerne les *codeurs(SR)* avec signaux de sortie sinus et cosinus analogiques qui revendiquent une *détection de défaut idéale* et qui sont envisagés pour les *fonctions de sécurité*, même si ces *codeurs(SR)* ne contribuent à aucun diagnostic ou ne contiennent aucun diagnostic entièrement intégré. Les informations pour l'utilisation d'un tel *codeur(SR)* doivent permettre à l'utilisateur d'effectuer les diagnostics exigés en externe. L'analyse statique implique la validation des exigences contenues dans les informations pour l'utilisation en ce qui concerne le traitement des signaux de sortie du *codeur(SR)* à effectuer en externe. Le *traitement des signaux* consiste en l'évaluation des signaux de sortie en vue d'exécuter la ou les *fonctions de sécurité* et en l'essai d'intégrité des signaux de sortie afin d'identifier des *anomalies* dans le *codeur(SR)* (diagnostic).

NOTE 1 L'analyse statique peut également être utilisée comme aide à la conception d'une *unité d'évaluation* sûre ou de commandes sûres avec entrées pour *codeur(SR)* avec signaux de sortie sinus et cosinus.

NOTE 2 La méthode d'analyse statique est décrite à l'Annexe L. Cette méthode est indépendante de la mise en œuvre possible dans un outil logiciel. Toutefois, se référer également aux représentations graphiques de l'outil mentionné en L.9 peut aider à la compréhension.

L.2 Raisons qui motivent l'analyse de l'*évaluation des signaux* et de la détection de *défaut*

Dans le cadre de l'évaluation des pentes des signaux en vue de l'exécution de la *sous-fonction de sécurité*, des *anomalies* du matériel peuvent provoquer la non-détection des pentes et donc la défaillance de la *fonction de sécurité*. Un essai d'intégrité des signaux analogiques doit permettre d'identifier ces *anomalies*. La possibilité d'identifier certaines *anomalies* dépend de la conception qualitative et quantitative spécifique à la fois de la détection des pentes (formation d'ondes carrées) et de l'essai des signaux analogiques (par exemple, surveillance de la longueur de phase).

L'analyse statique décrite ici a pour objet de vérifier si TOUS les *défauts* hypothétiques réalistes peuvent être détectés et de vérifier que tel est le cas. Il s'agit d'une condition préalable pour satisfaire au critère de *tolérance au premier défaut* (nécessaire pour satisfaire aux catégories 3 ou 4 selon l'ISO 13849-1) avec l'architecture monocanale donnée.

Afin de faciliter l'utilisation correcte du *codeur(SR)*, le fabricant doit proposer à l'utilisateur une ou plusieurs combinaisons de seuils de commutation pour la formation d'ondes carrées et d'un essai associé des signaux analogiques dans chaque cas. Ces combinaisons doivent satisfaire à l'analyse statique décrite ici.

Cependant, l'utilisateur peut concevoir l'évaluation et la détection de *défaut* sous sa propre responsabilité et s'écarter des suggestions du fabricant du *codeur(SR)*. Là aussi, la combinaison des seuils de commutation pour la formation d'ondes carrées et de l'essai des signaux analogiques doit satisfaire à l'analyse statique.

Concernant sa conception des diagnostics, le fabricant doit informer l'utilisateur des schémas d'*anomalie* spéciaux (tensions de signal) qui doivent être identifiés par les diagnostics. Ces informations peuvent être communiquées à l'aide de l'outil d'exécution de l'analyse statique (voir Article L.7 et Article L.9).

L.3 Signification du terme "analyse statique du *traitement des signaux*"

Le terme "analyse statique" est utilisé dans le domaine des essais logiciels. "Statique" signifie alors, comme ici, qu'aucune mesure physique des grandeurs variables dans le temps n'est effectuée sur un système en cours de fonctionnement, mais que le sujet est étudié d'un point de vue théorique.

Dans le cas présent, l'analyse statique porte sur la spécification quantitative des seuils de commutation pour la formation d'ondes carrées et sur la spécification qualitative et quantitative de l'essai d'intégrité des signaux analogiques, qui doivent être coordonnées de manière adéquate pour détecter tous les *défauts* possibles.

Dans les circuits électroniques, la méthode classique de vérification de la *couverture du diagnostic* obtenue exige l'exécution d'une FMEDA au niveau des composants et des circuits. Dans le cas d'un *codeur(SR)* incrémental avec signaux de sortie sinus et cosinus, l'intégration monolithique des capteurs pour le balayage de l'*indicateur statique* et des parties du circuit analogique pour la génération des signaux rend la FMEDA pratiquement impossible au niveau du transistor du seul fait qu'aucune interconnexion entre différents points du circuit ne peut être exclue. Néanmoins, il est important de déterminer si les détails qui doivent être spécifiés par le fabricant concernant le traitement des signaux de sortie sont appropriés.

La spécification exigée du fabricant du *codeur(SR)* doit indiquer:

- les seuils de commutation pour la génération d'ondes carrées ("bascule de Schmitt" dans le matériel ou le logiciel); et
- la méthode d'essai des signaux analogiques pour la détection de *défaut* (diagnostic).

Pour soumettre cette spécification à l'essai, le *traitement des signaux* analogiques, conformément à la spécification, est simulé. Les signaux de sortie corrects sont remplacés par une série de signaux d'essai qui représentent des signaux de substitution pour les *défauts* potentiels du *codeur(SR)*. Le *traitement des signaux* conformément à la spécification doit réagir à ces signaux d'essai de façon sûre et les "maîtriser". Cela signifie:

- que les signaux analogiques dont la variation dans le temps représente un changement de position doivent, selon la spécification, être convertis en impulsions comptables, incluant des informations sur la direction du comptage; ou
- que les diagnostics doivent émettre un signal de *défaut* (au moyen duquel l'application déclenche un état de sécurité).

La procédure d'analyse statique est représentée à la Figure L.1:

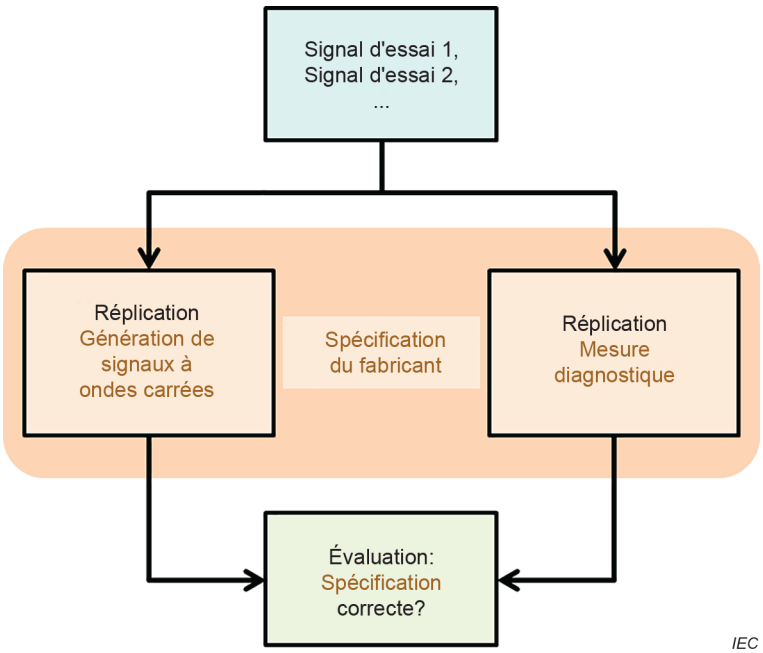


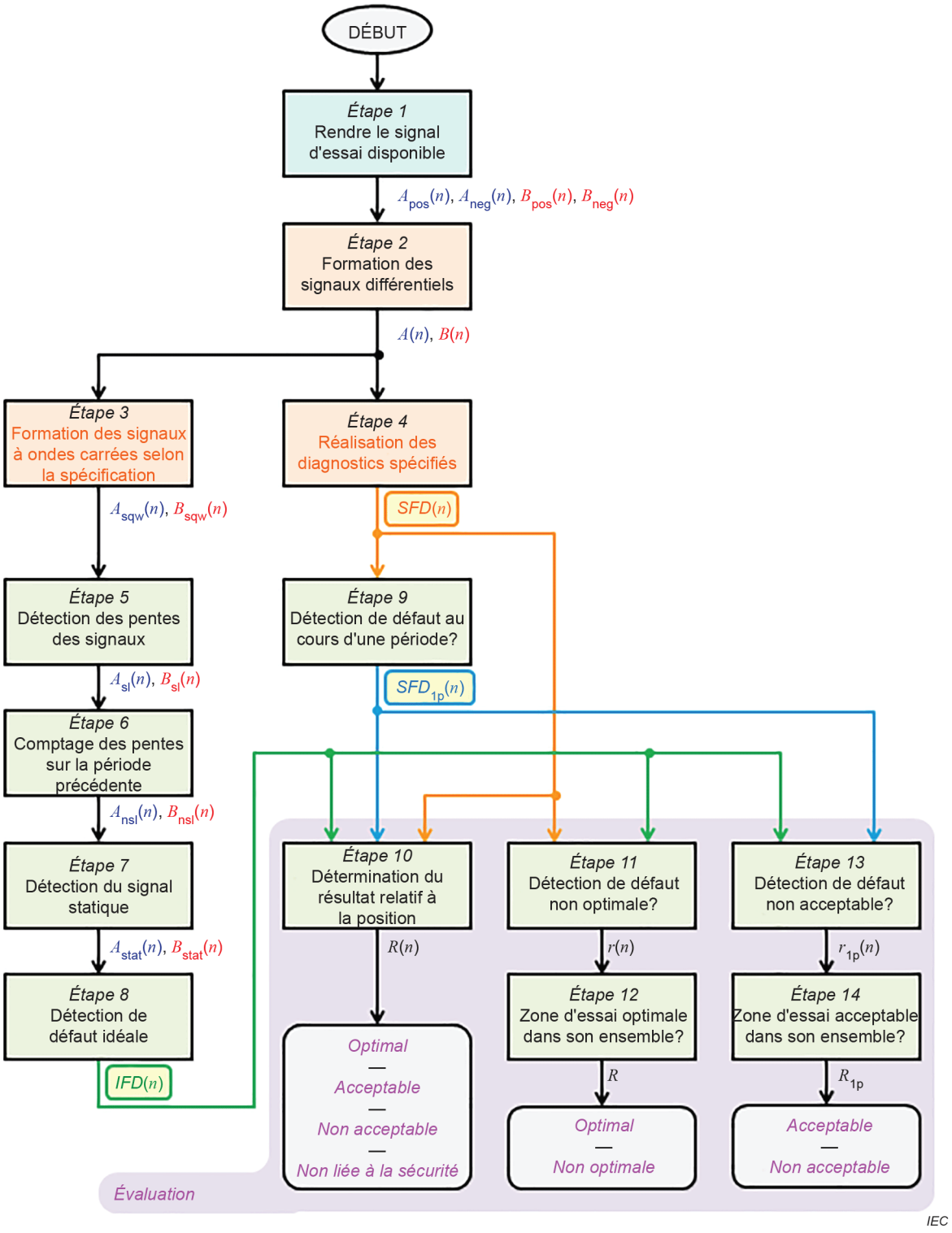
Figure L.1 – Concept d'analyse statique

Il est admis par hypothèse qu'une spécification des seuils de commutation et des diagnostics qui maîtrise les signaux de substitution maîtrise également les *anomalies* du matériel qui surviennent dans la réalité. Pour que cela soit possible, les signaux de substitution présentent une certaine diversité et une certaine variance.

NOTE Les "effets dynamiques" (surcomptage dû aux impulsions parasites) ne sont pas étudiés par l'analyse statique.

Les signaux d'essai sont décrits à l'Article L.4, la simulation du *traitement des signaux* à l'Article L.5 et l'évaluation de la spécification à l'Article L.6.

La Figure L.2 représente une vue d'ensemble des différentes étapes de l'analyse statique et des variables auxiliaires utilisées pour celle-ci. Les différentes étapes sont traitées plus en détail du L.4.1 au L.6.2. La procédure est indiquée pour un signal d'essai. La procédure doit être effectuée avec tous les signaux d'essai normalisés (voir Article L.4) et éventuellement avec des signaux d'essai supplémentaires. La nécessité d'utiliser des signaux d'essai supplémentaires dépend des défaillances possibles du *codeur(SR)* et doit être clarifiée à l'aide d'une FMEDA au niveau des composants et des circuits du *codeur(SR)* (voir Article L.7).


DÉBUT
Étape 1
Rendre le signal d'essai disponible
$A_{pos}(n)$, $A_{neg}(n)$, $B_{pos}(n)$, $B_{neg}(n)$
Étape 2
Formation des signaux différentiels
$A(n)$, $B(n)$
Étape 3
Formation des signaux à ondes carrées selon la spécification
Étape 4
Réalisation des diagnostics spécifiés
$A_{sqw}(n)$, $B_{sqw}(n)$
$SFD(n)$
Étape 5
Détection des pentes des signaux
Étape 9
Détection de défaut au cours d'une période?
$A_{sl}(n)$, $B_{sl}(n)$
$SFD_{1p}(n)$
Étape 6
Comptage des pentes sur la période précédente
$A_{nsl}(n)$, $B_{nsl}(n)$
Étape 7
Détection du signal statique
$A_{stat}(n)$, $B_{stat}(n)$
Étape 8
Détection de défaut idéale
$IFD(n)$
Étape 10
Détermination du résultat relatif à la position
Étape 11
Détection de défaut non optimale?
Étape 13
Détection de défaut non acceptable?
$R(n)$
$r(n)$
$r_{1p}(n)$
Optimal
—
Acceptable
—
Non acceptable
—
Non liée à la sécurité
Étape 12
Zone d'essai optimale dans son ensemble?
Étape 14
Zone d'essai acceptable dans son ensemble?
R
R_{1p}
Optimal
—
Non optimale
Acceptable
—
Non acceptable
Évaluation
IEC

Légende

$A_{pos}(n)$	signal d'essai cosinus avec composante continue à la valeur de position n
$A_{neg}(n)$	signal d'essai cosinus inversé avec composante continue à la valeur de position n
$B_{pos}(n)$	signal d'essai sinus avec composante continue à la valeur de position n
$B_{neg(}n)$	signal d'essai sinus inversé avec composante continue à la valeur de position n
$A(n)$	signal d'essai cosinus différentiel *A* à la valeur de position n
$B(n)$	signal d'essai sinus différentiel *B* à la valeur de position n
$A_{sqw}(n)$	signal à ondes carrées obtenu à partir de $A(n)$ à la valeur de position n
$B_{sqw}(n)$	signal à ondes carrées obtenu à partir de $B(n)$ à la valeur de position n
$A_{sl}(n)$	pente de $A_{sqw}(n)$ présente à la valeur de position n
$B_{sl}(n)$	pente de $B_{sqw}(n)$ présente à la valeur de position n
$A_{nsl}(n)$	nombre de pentes de $A_{sl}(n)$ sur 1,1 fois la période du signal d'essai avant n
$B_{nsl}(n)$	nombre de pentes de $B_{sl}(n)$ sur 1,1 fois la période du signal d'essai avant n
$A_{stat}(n)$	$A_{sqw}(n)$ évalué comme statique à la valeur de position n
$B_{stat}(n)$	$B_{sqw}(n)$ évalué comme statique à la valeur de position n
$IFD(n)$	détection d'un *défaut* par une *détection de défaut idéale* optimale à la valeur de position n
$SFD(n)$	détection d'un *défaut* par les mesures diagnostiques spécifiées à la valeur de position n
$SFD_{1P}(n)$	détection d'un *défaut* par les mesures diagnostiques spécifiées sur 1,1 fois la période de l'*indicateur statique* à partir de la valeur de position n
$R(n)$	résultat de l'analyse statique des mesures diagnostiques spécifiées à la valeur de position n
$r(n)$	absence de détection de défaut par les mesures diagnostiques spécifiées à la valeur de position n
R	résultat de l'analyse statique des mesures diagnostiques spécifiées
$r_{1P}(n)$	absence de détection de *défaut* par les mesures diagnostiques spécifiées sur 1,1 fois la période de l'*indicateur statique* à partir de la valeur de position n
R_{1P}	résultat global de l'analyse statique des mesures diagnostiques spécifiées par rapport à leur aptitude à signaler une *anomalie* sur 1,1 fois la période de l'*indicateur statique*

Figure L.2 – Procédure d'analyse statique (pour un signal d'essai) avec dénomination des variables

L.4 Signaux d'essai normalisés

L.4.1 Rendre le signal d'essai disponible (étape 1)

Les signaux d'essai utilisés dans l'analyse statique servent de signaux de substitution pour les signaux de sortie corrompus générés du fait d'*anomalies* dans le *codeur(SR)*. Chaque signal d'essai consiste donc en quatre signaux de sortie individuels au niveau de l'interface de sortie:

a) A_{pos} signal d'essai cosinus avec composante continue;

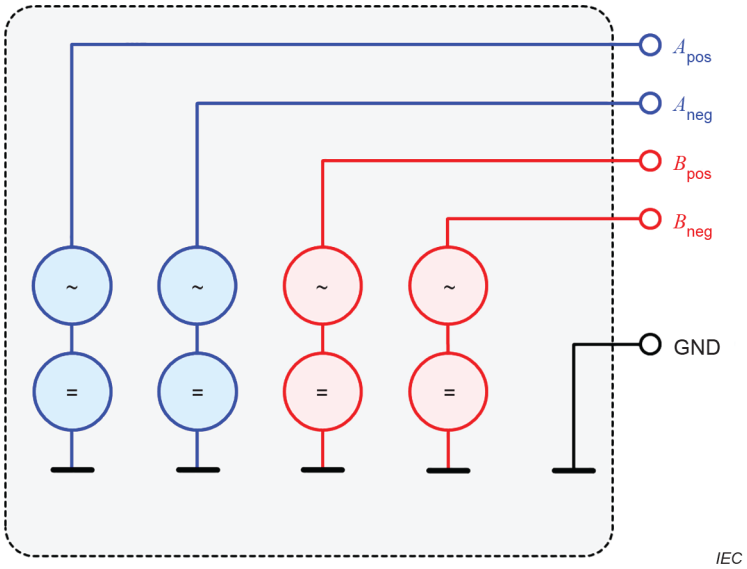
b) A_{neg} signal d'essai cosinus inversé avec composante continue;

c) B_{pos} signal d'essai sinus avec composante continue; et

d) B_{neg} signal d'essai sinus inversé avec composante continue.

Ce point de référence a été choisi car, sur un *codeur(SR)* conventionnel avec signaux de sortie sinus et cosinus, il est toujours présent sous la même forme, tandis que l'interface d'entrée, par exemple à la sortie du circuit opto-ASIC, diffère selon la conception d'interface d'entrée.

L'interface de sortie en question peut être représentée par le circuit de substitution de la Figure L.3.



Légende

A_{pos} signal d'essai cosinus avec composante continue

A_{neg} signal d'essai cosinus inversé avec composante continue

B_{pos} signal d'essai sinus avec composante continue

B_{neg} signal d'essai sinus inversé avec composante continue

Figure L.3 – Circuit de substitution de l'interface de sortie du *codeur(SR)*

La composante continue superposée à tous les signaux alternatifs maintient toujours tous ces signaux dans la plage de tensions positive.

Dans leur état exempt d'*anomalie*, les signaux de sortie prennent la forme suivante:

$$A_{pos}(\varphi) = S_{=} + \frac{1}{2} Amp \cdot cos\,\varphi$$

$$A_{neg}(\varphi) = S_{=} - \frac{1}{2} Amp \cdot cos\,\varphi$$

$$B_{pos}(\varphi) = S_{=} + \frac{1}{2} Amp \cdot sin\,\varphi$$

$$B_{neg}(\varphi) = S_{=} - \frac{1}{2} Amp \cdot sin\,\varphi$$

où

φ est la position de l'*indicateur statique* par rapport à la partie capteur du *codeur(SR)*, où φ varie de 360° (2 π) sur une période de l'*indicateur statique*;

$S_{=}$ est la composante de décalage du signal;

Amp est l'amplitude de la composante alternative du signal.

NOTE Une mise en œuvre fréquente est la suivante: $S_{=}$ = 2,5 V et Amp = 0,5 V.

En raison des étages amplificateurs différentiels pour les signaux A et B, les signaux $A(\varphi)$ et $B(\varphi)$ sont formés pendant le *traitement des signaux*:

$$A(\varphi) = A_{\text{pos}}(\varphi) - A_{\text{neg}}(\varphi) = Amp \cdot \cos\varphi$$

$$B(\varphi) = B_{\text{pos}}(\varphi) - B_{\text{neg}}(\varphi) = Amp \cdot \sin\varphi$$

NOTE Afin d'empêcher des tensions de signal et de fonctionnement négatives dans le *traitement des signaux*, une nouvelle composante continue est en pratique ajoutée à $A(\varphi)$ et $B(\varphi)$. Ce type de particularités des circuits n'est pas pris en compte dans l'Annexe L.

Les signaux d'essai présentés ci-après sont fondés sur les signaux nominaux et, sur un certain nombre de périodes, varient en amplitude, en composante continue ou en phase, ou en une combinaison de ces éléments. Pour la représentation numérique et l'examen, le nombre de périodes observées doit être limité et chaque période doit être représentée par un nombre limité de valeurs d'échantillon. Les variations effectuées par rapport à la valeur de position φ ne doivent pas altérer de façon excessive la forme du signal. Le nombre total de points d'échantillonnage doit également être raisonnable. A titre de compromis, 100 périodes avec une résolution de 100 points d'échantillonnage chacune sont donc choisies, ce qui équivaut à 10 000 points d'échantillonnage par signal d'essai.

Avec la valeur de position discrète n pour les points d'échantillonnage 0, 1, 2, …, 10 000, la valeur de position continue φ est indiquée comme suit:

$$\varphi = 2\pi \frac{n}{100} = \frac{\pi}{50} n$$

Les signaux nominaux du *codeur(SR)* exempt d'*anomalie* sont donc représentés comme suit:

$$A_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

Sur cette base, cinq signaux d'essai normalisés sont définis ci-après. Ils appliquent chacun une certaine distorsion du signal en fonction de la valeur de position n.

Dans l'évaluation de la spécification du *traitement des signaux* (Article L.6), la plage de positions doit également être prise en compte comme correspondant à n > 10 000 pour une position (étape 9). Etant donné que la distorsion des signaux d'essai n'est définie que pour la plage de positions n = 0 … 10 000, la distorsion est "gelée" à n = 10 000, à l'aide de la variable suivante:

$$\bar{n} = \begin{cases} n & \text{pour} \quad n \leq 10\,000 \\ 10\,000 & \text{pour} \quad n > 10\,000 \end{cases}$$

Cette variable est utilisée dans la partie des équations des signaux d'essai qui provoque la distorsion du signal, tandis que la partie des équations des signaux d'essai qui génère l'oscillation utilise la valeur de position n supérieure à 10 000 de sorte que l'oscillation se poursuive.

L.4.2 Signal d'essai 1

Le signal d'essai 1 présente une variation d'amplitude parallèle avec une composante continue nominale:

$$A_{\text{pos}}(n) = S_{=} + \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

où

$$\bar{n} = \begin{cases} n & \text{pour} \quad n \leq 10\,000 \\ 10\,000 & \text{pour} \quad n > 10\,000 \end{cases}$$

L.4.3 Signal d'essai 2

Le signal d'essai 2 présente une variation d'amplitude antiparallèle avec une composante continue nominale:

$$A_{\text{pos}}(n) = S_{=} + \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \frac{\bar{n}}{10\,000} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \frac{\bar{n}}{10\,000} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

où

$$\bar{n} = \begin{cases} n & \text{pour} \quad n \leq 10\,000 \\ 10\,000 & \text{pour} \quad n > 10\,000 \end{cases}$$

L.4.4 Signal d'essai 3

Le signal d'essai 3 présente une variation d'amplitude parallèle de l'ensemble des signaux, y compris la composante continue:

$$A_{\text{pos}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right)\left[S_{=} + \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)\right]$$

$$A_{\text{neg}}(n) = S_{=} - \left(1 - \frac{\bar{n}}{10\,000}\right) Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right)\left[S_{=} + \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)\right]$$

$$B_{\text{neg}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right)\left[S_{=} - \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)\right]$$

où

$$\bar{n} = \begin{cases} n & \text{pour} \quad n \leq 10\,000 \\ 10\,000 & \text{pour} \quad n > 10\,000 \end{cases}$$

L.4.5 Signal d'essai 4

Le signal d'essai 4 présente une variation de la composante continue des signaux "pos":

$$A_{\text{pos}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right) S_{=} + \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = \left(2 - \frac{\bar{n}}{5\,000}\right) S_{=} + \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

où

$$\bar{n} = \begin{cases} n & \text{pour} \quad n \leq 10\,000 \\ 10\,000 & \text{pour} \quad n > 10\,000 \end{cases}.$$

L.4.6 Signal d'essai 5

Le signal d'essai 5 fournit une variation de phase:

$$A_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \sin\left[\frac{\pi}{50} n + \pi\left(\frac{\bar{n}}{10\,000} - \frac{1}{2}\right)\right]$$

$$B_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \sin\left[\frac{\pi}{50} n + \pi\left(\frac{\bar{n}}{10\,000} - \frac{1}{2}\right)\right]$$

où

$$\bar{n} = \begin{cases} n & \text{pour} \quad n \leq 10\,000 \\ 10\,000 & \text{pour} \quad n > 10\,000 \end{cases}.$$

Des signaux d'essai supplémentaires peuvent être nécessaires en vue de qualifier la spécification du *traitement des signaux* pour un *codeur(SR)* particulier. Cela dépend des modes de défaillance possibles du *codeur(SR)* et cela doit être clarifié à l'aide d'une FMEDA du *codeur(SR)* au niveau des composants et des circuits. Une explication des problèmes et une description de la procédure peuvent être consultées à l'Article L.7.

Tous les signaux d'essai sont définis pour un nombre entier $n \geq 0$. Dans l'évaluation de la spécification du *traitement des signaux* (Article L.6), la valeur de position doit être considérée comme $n < 0$ en certains points (étape 5, étape 6). Les signaux d'essai sont donc précédés d'une "phase préparatoire" avec les signaux de sortie nominaux non déformés. La distorsion, par exemple l'essai proprement dit, commence ainsi brusquement à partir de la position $n = 0$.

L.5 Simulation du *traitement des signaux* aux fins de la spécification

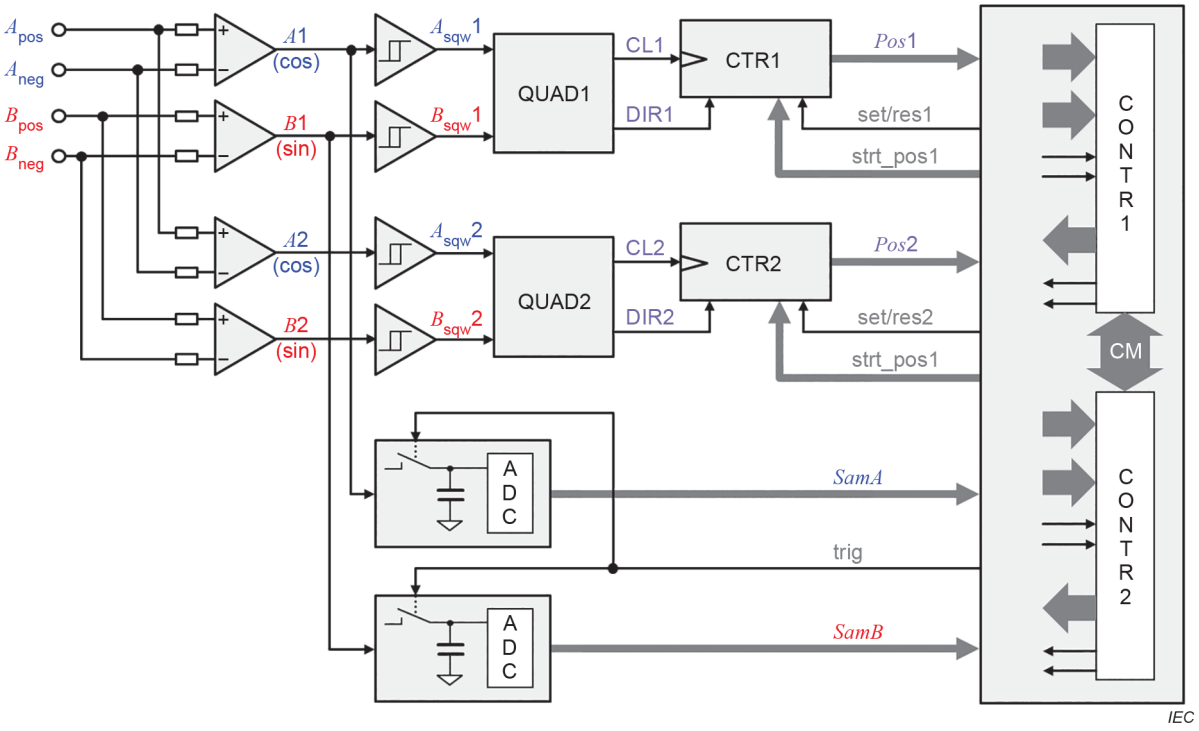
L.5.1 Généralités

La définition des signaux d'essai est suivie d'une simulation de l'*évaluation des signaux* et des diagnostics.

Afin d'obtenir les valeurs de position, les pentes des signaux sinus/cosinus analogiques sont détectées et comptées. A partir de l'angle de phase des deux signaux, la direction du mouvement qui détermine la direction du comptage doit également être déterminée. La mise en œuvre habituelle utilise des décodeurs en quadrature qui génèrent à la fois les impulsions de comptage et le signal de direction.

L'essai d'intégrité des signaux analogiques pour la réalisation de la *couverture du diagnostic* (DC) du *codeur(SR)* peut être effectué par des moyens analogiques ou, après numérisation, de façon numérique.

A des fins de représentation, la Figure L.4 représente une mise en œuvre possible (exemple) du *traitement des signaux*, par exemple la production et le comptage des impulsions et les diagnostics.



Légende

A_{pos}	signal d'essai cosinus avec composante continue
A_{neg}	signal d'essai cosinus inversé avec composante continue
B_{pos}	signal d'essai sinus avec composante continue
B_{neg}	signal d'essai sinus inversé avec composante continue
$A1$, $A2$	signal cosinus différentiel A dans le canal 1, 2
$B1$, $B2$	signal sinus différentiel B dans le canal 1, 2
$A_{sqw}1$, $A_{sqw}2$	signal à ondes carrées obtenu à partir du signal A dans le canal 1, 2
$B_{sqw}1$, $B_{sqw}2$	signal à ondes carrées obtenu à partir du signal B dans le canal 1, 2
QUAD1, 2	décodeur en quadrature 1, 2
CL1, CL2	signal d'horloge du canal 1, 2

DIR1, DIR2	signal de direction du canal 1, 2
CTR1, 2	compteur 1, 2
*Pos*1, 2	valeur de position 1, 2
set/res1, 2	initialisation/réinitialisation 1, 2
strt_pos1, 2	position de départ 1, 2
CONTR1, 2	régulateur 1, 2
ADC	convertisseur analogique/numérique
SamA, B	valeur d'échantillon A, B
trig	échantillon déclencheur
CM	surveillance croisée

Figure L.4 – Exemple de circuit pour l'évaluation des signaux de sortie et des diagnostics des *défauts* du *codeur(SR)*

Les redondances contribuent à la réalisation de la *tolérance au premier défaut* et à la détection de *défaut* dans le circuit d'évaluation, mais pas à la détection de *défaut* dans le *codeur(SR)*. Les convertisseurs analogique/numérique ne réalisent pas la *fonction de sécurité*, mais sont utilisés pour les diagnostics et n'établissent aucune redondance.

NOTE 1 L'évaluation de la détection de *défaut*, tout aussi nécessaire, dans le circuit d'évaluation n'est pas traitée ici. Dans l'Annexe L, l'analyse statique est utilisée uniquement pour soumettre à l'essai la spécification du *traitement des signaux*.

NOTE 2 Dans la mesure où les fréquences sont suffisamment basses, la détection des pentes des signaux, le décodage en quadrature et le comptage des positions peuvent être effectués par un logiciel fondé sur des signaux analogiques échantillonnés et numérisés suffisamment rapidement.

Dans l'analyse statique de l'*évaluation des signaux* et de la détection de *défaut*, il est admis par hypothèse que le *traitement des signaux* est effectué comme spécifié dans les informations pour l'utilisation du *codeur(SR)*.

L.5.2 Formation des signaux différentiels (étape 2)

A l'étape 2, les signaux différentiels doivent être évalués:

$$A(n) = A_{\text{pos}}(n) - A_{\text{neg}}(n)$$

$$B(n) = B_{\text{pos}}(n) - B_{\text{neg}}(n).$$

L.5.3 Formation des signaux à ondes carrées selon la spécification (bascule de Schmitt, étape 3)

A l'étape 3, les signaux à ondes carrées doivent être évalués comme spécifié dans les informations pour l'utilisation:

NOTE L'indice sqw signifie "signal à onde carrée" (*Square-Wave Signal*).

$$A_{\text{sqw}}(n) = \begin{cases} 1 & \text{pour} \quad A(n) \geq A_{\text{on}} \quad \vee \quad \left[A(n) \geq A_{\text{off}} \quad \wedge \quad A_{\text{sqw}}(n-1) = 1 \right] \\ 0 & \text{sinon} \end{cases}$$

$$B_{\text{sqw}}(n) = \begin{cases} 1 & \text{pour} \quad B(n) \geq B_{\text{on}} \quad \vee \quad \left[B(n) \geq B_{\text{off}} \quad \wedge \quad B_{\text{sqw}}(n-1) = 1 \right] \\ 0 & \text{sinon} \end{cases}$$

où

A_{on}, A_{off} sont les seuils de commutation de la bascule de Schmitt du signal A.

B_{on}, B_{off} sont les seuils de commutation de la bascule de Schmitt du signal B.

L.5.4 Réalisation des diagnostics spécifiés (étape 4)

L'hypothèse retenue est, par exemple, que les informations pour l'utilisation du *codeur(SR)* spécifient la surveillance de la longueur de pointeur comme diagnostic.

La possible influence du contrôle de l'amplitude doit être prise en compte (voir 6.3).

$$SFD(n) = \begin{cases} 1 & \text{pour} \quad A^2(n) + B^2(n) < Amp^2_{\text{min}} \quad \vee \quad A^2(n) + B^2(n) > Amp^2_{\text{max}} \\ 0 & \text{sinon} \end{cases}$$

où

Amp^2_{min} est la limite inférieure du carré de la longueur de pointeur spécifiée;

Amp^2_{max} est la limite supérieure du carré de la longueur de pointeur spécifiée.

NOTE Le terme SFD signifie "détection de *défaut* spécifiée" (*Specified Fault Detection*).

Pour la valeur 1, *SFD*(n) indique que l'essai d'intégrité du signal analogique spécifié génère une "*anomalie*" comme résultat d'essai à la valeur de position n.

L.6 Evaluation de la spécification du *traitement des signaux*

L.6.1 Généralités

L.6.1.1 Vue d'ensemble

Après simulation du *traitement des signaux* conformément à la spécification, les résultats doivent être évalués en tenant compte des caractéristiques du décodeur en quadrature. Si l'un des deux signaux de commande numériques d'un décodeur en quadrature devient statique en raison d'une *anomalie* dans le *codeur(SR)* tandis que l'autre s'active en raison d'un mouvement, le signal de direction du comptage change à chaque impulsion de comptage. Le compteur de position compte alors, en alternance, un pas en avant puis un pas en arrière, simulant ainsi l'arrêt. Ainsi, lorsque l'un des signaux de commande ou les deux deviennent statiques, cela provoque une *défaillance dangereuse* de la *fonction de sécurité*, ce qui donne le critère d'évaluation suivant pour la spécification du *traitement des signaux*.

La spécification est acceptable si, pendant le traitement des signaux d'essai selon la spécification, AUCUN des cas critiques suivants ne se produit à AUCUN moment:

- l'un des deux signaux à ondes carrées dérivés des signaux analogiques A (cosinus) et B (sinus) devient statique ET l'essai d'intégrité du signal analogique n'indique aucune *anomalie*; et
- les deux signaux à ondes carrées dérivés des signaux analogiques A (cosinus) et B (sinus) deviennent statiques ET l'essai d'intégrité du signal analogique n'indique aucune *anomalie*.

Si l'un de ces cas se produit au moins une fois au cours du traitement des signaux d'essai, la spécification du *traitement des signaux* est jugée non acceptable.

La redondance du décodeur en quadrature et du compteur du circuit d'évaluation ne permet pas de détecter la nature statique de l'un des signaux à ondes carrées ou des deux, car ce comportement se produit dans les deux canaux par la nature même du système. Une FMEDA des composants et des circuits du *codeur(SR)* doit donc permettre de déterminer si un tel schéma d'*anomalie* peut être provoqué par une *anomalie* de composant unique (voir Article L.7). Si cela est possible, ces *défauts* doivent être détectés au moyen de l'essai d'intégrité du signal analogique.

Lorsque le critère d'acceptation a été défini pour la spécification du *traitement des signaux*, l'évaluation doit être effectuée en plusieurs étapes.

L.6.1.2 Détection des pentes des signaux (étape 5)

A l'étape 5, la valeur de position n à laquelle apparaissent des pentes montantes ou descendantes est déterminée.

$$A_{\mathrm{sl}}(n) = \begin{cases} 1 & \text{pour} \quad A_{\mathrm{sqw}}(n) \neq A_{\mathrm{sqw}}(n-1) \\ 0 & \text{sinon} \end{cases}$$

$$B_{\mathrm{sl}}(n) = \begin{cases} 1 & \text{pour} \quad B_{\mathrm{sqw}}(n) \neq B_{\mathrm{sqw}}(n-1) \\ 0 & \text{sinon} \end{cases}$$

NOTE L'indice sl signifie "pente" (slope).

Pour la valeur 1, $A_{\mathrm{sl}}(n)$ et $B_{\mathrm{sl}}(n)$ indiquent que le signal à ondes carrées A_{sqw} ou B_{sqw} présente une pente montante ou descendante à la valeur de position n.

L.6.1.3 Comptage des pentes sur la période précédente (étape 6)

Cette étape a pour objet de détecter le moment auquel les signaux à ondes carrées deviennent statiques. Un signal à ondes carrées est évalué comme "statique" lorsque moins de deux (le cas normal) modifications du signal se produisent au cours d'une période. Afin de supprimer les artefacts du signal d'essai légèrement déformé (modulé en amplitude) par rapport à une courbe purement sinusoïdale, la période d'observation est définie comme correspondant à 1,1 fois la durée de la période.

$$A_{\mathrm{nsl}}(n) = \sum_{k\,=\,n-109}^{n} A_{\mathrm{sl}}(k)$$

$$B_{\mathrm{nsl}}(n) = \sum_{k\,=\,n-109}^{n} B_{\mathrm{sl}}(k)$$

$A_{\mathrm{nsl}}(n)$ et $B_{\mathrm{nsl}}(n)$ expriment le nombre de pentes des signaux à ondes carrées A_{sqw} et B_{sqw} sur 1,1 fois la période du signal d'essai avant n.

L.6.1.4 Détection du signal statique (étape 7)

Cette étape permet de vérifier si, pendant la période d'observation et ses 100 oscillations du signal d'essai (n = 0, 1, ... , 10 000), il existe des valeurs de position n auxquelles l'un des signaux à ondes carrées A_{sqw} ou B_{sqw} devient statique (moins de deux pentes sur 1,1 fois la période d'oscillation précédente).

$$A_{\text{stat}}(n) = \begin{cases} 1 & \text{pour} \quad A_{\text{nsl}}(n) < 2 \\ 0 & \text{sinon} \end{cases}$$

$$B_{\text{stat}}(n) = \begin{cases} 1 & \text{pour} \quad B_{\text{nsl}}(n) < 2 \\ 0 & \text{sinon} \end{cases}$$

Pour la valeur 1, $A_{\text{stat}}(n)$ ou $B_{\text{stat}}(n)$ indique que le signal à ondes carrées A_{sqw} ou B_{sqw} est évalué comme statique à la valeur de position n.

L.6.2 Concept d'évaluation de la spécification du *traitement des signaux*

L.6.2.1 Généralités

Idéalement, une *anomalie* est signalée par l'essai d'intégrité du signal analogique au moment précis où au moins l'un des deux signaux à ondes carrées devient statique. Dans de nombreux cas d'*anomalies*, l'essai d'intégrité du signal analogique ne génère pas de message d'*anomalie* ininterrompu sur une période de l'*indicateur statique*. Cela peut être accepté tant qu'un message d'*anomalie* est émis à au moins une position au cours d'une période.

Si certaines *anomalies* du *codeur(SR)* ne sont détectables que sur certaines parties d'une période de l'*indicateur statique* avec l'essai d'intégrité du signal analogique prévu, les instructions doivent attirer l'attention sur ce fait, par exemple:

- en cas de diagnostic continu, il est essentiel de s'assurer que l'état de sécurité est atteint en présence d'une *anomalie*, en tenant compte de la vitesse rotative/linéaire maximale et du nombre de lignes; et
- en cas de diagnostic à des instants discrets, les instructions doivent expliquer la relation entre la vitesse rotative/linéaire, le nombre de lignes et le taux d'échantillonnage; l'explication permet à l'utilisateur de modifier le comportement temporel de son *traitement des signaux* en vue de répondre à ses besoins et de limiter l'application en ce qui concerne la vitesse rotative/linéaire et le nombre de lignes.

Afin de faciliter l'évaluation de la spécification du *traitement des signaux*, un certain nombre de variables auxiliaires sont à leur tour définies.

L.6.2.2 *Détection de défaut idéale* (étape 8)

La *détection de défaut idéale* est simulée avec la variable *IFD* (en vert sur la Figure L.2). Elle indique qu'il convient que l'essai d'intégrité du signal analogique signale une *anomalie*:

$$IFD(n) = \begin{cases} 1 & \text{pour} \quad A_{\text{stat}}(n) + B_{\text{stat}}(n) \geq 1 \\ 0 & \text{sinon} \end{cases}.$$

NOTE 1 Le terme IFD signifie "*détection de défaut idéale*" (*Ideal Fault Detection*).

La variable *IFD* prend la valeur hypothétique de 1 à chaque valeur de position n à laquelle la "*détection de défaut idéale*" réagit.

D'autre part, la variable *SFD* (en orange sur la Figure L.2) introduite à l'étape 4 représente le comportement de l'essai d'intégrité du signal analogique spécifié.

Dans le cas particulier de la surveillance de la longueur de phaseur, ce qui suit s'applique (comme indiqué précédemment):

$$SFD(n) = \begin{cases} 1 & \text{pour} \quad A^2(n) + B^2(n) < Amp^2_{\text{min}} \quad \vee \quad A^2(n) + B^2(n) > Amp^2_{\text{max}} \\ 0 & \text{sinon} \end{cases}.$$

NOTE 2 Le terme *SFD* désigne la *détection de défaut spécifiée* (*Specified Fault Detection*).

La variable *SFD* prend la valeur hypothétique de 1 à chaque valeur de position n à laquelle l'essai d'intégrité du signal analogique spécifié réagit, par exemple émet un message d'*anomalie*.

L.6.2.3 Détection de défaut au cours de la période? (étape 9)

Il est également accepté que la détection de *défaut* nécessaire s'effectue dans une plage de positions qui commence par la position n_1 du premier *défaut* ($IFD(n_1) = 1$) et qui couvre (1,1 fois) la période de l'*indicateur statique*.

NOTE Le facteur 1,1 (plutôt que le facteur 1) est utilisé pour supprimer les artefacts du signal d'essai qui est légèrement déformé (modulé en amplitude) par rapport à une courbe purement sinusoïdale.

Pour représenter la détection de *défaut* sur 1,1 fois une période, la variable SFD_{1P} (en bleu clair sur la Figure L.2) est définie comme suit:

$$SFD_{1P}(n) = \begin{cases} 1 & \text{pour} \quad \sum_{k=n}^{n+109} SFD(k) \geq 1 \\ 0 & \text{sinon} \end{cases}.$$

La variable SFD_{1P} prend la valeur hypothétique 1 à une valeur de position n quand, sur (1,1 fois) la période de l'*indicateur statique* qui commence par n, l'essai d'intégrité du signal analogique spécifié réagit à au moins une valeur n.

L.6.2.4 Détermination du résultat relatif à la position (étape 10)

A chaque valeur de position n à laquelle la *détection de défaut idéale* réagit, une évaluation peut être effectuée à l'aide de la variable R. Les positions auxquelles aucune détection de *défaut* n'est nécessaire ($IFD(n) = 0$) ne sont pas pertinentes pour la spécification du *traitement des signaux*:

$$R(n) = \begin{cases} \text{optimal} & \text{pour} \quad IFD(n) = 1 \quad \wedge \quad SFD_{1P}(n) = 1 \quad \wedge \quad SFD(n) = 1 \\ \text{acceptable} & \text{pour} \quad IFD(n) = 1 \quad \wedge \quad SFD_{1P}(n) = 1 \quad \wedge \quad SFD(n) = 0 \\ \text{non acceptable} & \text{pour} \quad IFD(n) = 1 \quad \wedge \quad SFD_{1P}(n) = 0 \\ \text{non liée à la sécurité} & \text{pour} \quad IFD(n) = 0 \end{cases}.$$

optimal	optimale

NOTE Le terme $R(n)$ désigne le résultat.

La variable $R(n)$ est une variable logique qui, à chaque valeur de position n, prend hypothétiquement précisément l'une des quatre valeurs possibles, "optimale", "acceptable", "non acceptable" ou "non liée à la sécurité". Il peut être utile d'examiner un résultat d'analyse donné avec plus de précision.

L.6.2.5 Détection de défaut non optimale? (étape 11)

Cette étape a pour objet de déterminer les positions sans détection de *défaut* optimale. A cette fin, la variable numérique $r(n)$ est d'abord définie comme suit:

$$r(n) = \begin{cases} 1 & \text{pour} \quad IFD(n) = 1 \ \wedge \ SFD(n) = 0 \\ 0 & \text{sinon} \end{cases}.$$

$r(n)$ prend la valeur hypothétique de 1 aux valeurs de position n auxquelles une *détection de défaut idéale* réagit, mais où la détection de *défaut* spécifiée ne signale pas d'*anomalie*. $r(n)$ = 1 représente donc le cas où $R(n)$ n'a pas atteint la valeur "optimale" à la valeur de position n.

L.6.2.6 Zone d'essai optimale dans son ensemble? (étape 12)

La spécification du *traitement des signaux* doit être évaluée sur l'ensemble du parcours d'un signal d'essai (n = 0, 1, … , 10 000).

Pour que l'ensemble du signal d'essai soit "optimal" (uniquement pour des raisons de sécurité), le cas $r(n)$ = 1 ne doit se produire à aucune position du signal d'essai. A l'aide de la variable R (indépendante de n) définie ci-après, il est possible d'indiquer si, oui ou non, la spécification du *traitement des signaux* est optimale avec le signal d'essai utilisé.

$$R = \begin{cases} \text{optimal} & \text{pour} \quad \sum_{n=0}^{10\,000} r(n) < 1 \\ \text{non optimale} & \text{sinon} \end{cases}.$$

optimal	optimale

R = optimale signifie que la spécification du *traitement des signaux* entraîne un message d'*anomalie* continu en cas d'*anomalie* sur la base du signal d'essai.

L.6.2.7 Détection de défaut non acceptable? (étape 13)

Souvent, la détection de *défaut* optimale n'est pas atteinte. Toutefois, il est également accepté qu'un *défaut* détecté au cours d'une période de l'*indicateur statique* déclenche un message d'*anomalie* pour au moins une position n. L'absence de message d'*anomalie* sur cette période ne doit pas être acceptée.

Pour l'évaluation locale, la variable $r_{1P}(n)$ est d'abord définie comme suit:

$$r_{1P}(n) = \begin{cases} 1 & \text{pour} \quad IFD(n) = 1 \ \wedge \ SFD_{1P}(n) = 0 \\ 0 & \text{sinon} \end{cases}.$$

$r_{1P}(n)$ prend la valeur hypothétique de 1 aux valeurs de position n auxquelles une *détection de défaut idéale* réagit, mais où la détection de *défaut* spécifiée n'émet pas de message d'*anomalie*, même au cours de (1,1 fois) la période suivante du signal d'essai. $r_{1P}(n)$ = 1 représente donc le cas où $R(n)$ = non acceptable.

Le cas $r_{1P}(n)$ = 1 ne doit se produire à aucune position du signal d'essai.

L.6.2.8 Zone d'essai acceptable dans son ensemble? (étape 14)

A l'aide de la variable R_{1P} (indépendante de n), il est possible de décider si la spécification du *traitement des signaux* satisfait au signal d'essai dans son ensemble (acceptable) ou non (non acceptable):

$$R_{1P} = \begin{cases} \text{acceptable} & \text{pour} \quad \sum_{n=0}^{10\,000} r_{1P}(n) < 1 \\ \text{non acceptable} & \text{sinon} \end{cases}.$$

R_{1P} = acceptable signifie que la spécification du *traitement des signaux* entraîne au moins un message d'*anomalie* sur 1,1 fois la période de l'*indicateur statique* en cas d'*anomalie* sur la base du signal d'essai.

NOTE Chaque spécification du *traitement des signaux* qui atteint R = optimale atteint également R_{1P} = acceptable. Une spécification du *traitement des signaux* qui atteint R_{1P} = acceptable n'atteint pas nécessairement aussi R = optimale.

R_{1P} = non acceptable signifie que la spécification du *traitement des signaux* ne satisfait pas au signal d'essai et qu'elle doit être améliorée.

Une spécification du *traitement des signaux* qui atteint R_{1P} = acceptable pour chaque signal d'essai réussit l'essai d'"analyse statique".

Si une spécification du *traitement des signaux* qui a réussi l'essai d'analyse statique n'atteint pas R = optimale pour au moins un signal d'essai, cela signifie que l'essai d'intégrité du signal analogique prévu est uniquement capable de détecter certains *défauts* sur certaines parties d'une période de l'*indicateur statique*. Dans ce cas, cela doit être indiqué dans les instructions d'utilisation. Voir L.6.2.

L.7 FMEDA du codeur(SR) pour vérifier la couverture du diagnostic

L.7.1 Généralités

Pour atteindre la *couverture du diagnostic* exigée, la spécification du *traitement des signaux* doit maîtriser toutes les défaillances matérielles qui se produisent (voir Article L.3). Les signaux de sortie défectueux qui peuvent survenir en raison d'*anomalies* du matériel dépendent des modèles de *défaut* des composants et des circuits du *codeur(SR)*.

L.7.2 Explication du problème

En principe, il y existe des combinaisons de signaux A_{pos}, A_{neg}, B_{pos} et B_{neg} qui représentent un état d'immobilité. Un tel état est évidemment l'un des états de fonctionnement possibles et admissibles. Toutefois, la situation devient critique lorsque:

- du mouvement se produit, mais que les signaux de sortie sont déformés par une défaillance matérielle unique au point que l'immobilité est simulée; et
- que cette défaillance matérielle n'est pas détectée par l'essai d'intégrité du signal analogique prévu.

De telles combinaisons de signaux critiques incluent naturellement des signaux statiques, mais pas exclusivement. A l'aide d'une FMEDA, il est essentiel de déterminer si une défaillance matérielle unique est capable de générer de tels signaux de sortie critiques. Si cela est possible, la spécification du *traitement des signaux* n'est pas acceptable et doit être améliorée de manière à ce que de tels scénarios ne soient plus possibles.

A des fins d'illustration, l'exemple de combinaison de signaux potentiellement critiques suivant est donné:

$$A_{\text{pos}}(n) = 1{,}16 \cdot S_{=} + k \cdot \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$A_{\text{neg}}(n) = S_{=} - k \cdot \frac{1}{2} Amp \cdot \cos\left(\frac{\pi}{50} n\right)$$

$$B_{\text{pos}}(n) = S_{=} + \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

$$B_{\text{neg}}(n) = S_{=} - \frac{1}{2} Amp \cdot \sin\left(\frac{\pi}{50} n\right)$$

où

k est un facteur d'amplitude de $A_{\text{pos}}(n)$ et $A_{\text{neg}}(n)$ qui résulte d'un *défaut* unique dans le *codeur(SR)*.

Les cas k = 0 et k = 0,2 sont pris en considération. La composante alternative des deux signaux A est alors égale à zéro ou à 20 % de la valeur nominale. Si k = 0,2 et *Amp* = 0,5 V, cela donne la composante alternative suivante (crête à crête) du signal différentiel:

$$A_{\approx \text{pp}} = 2\left(A_{\text{pos}\approx} - A_{\text{neg}\approx}\right) = 2\left(0{,}2 \cdot \frac{1}{2} Amp + 0{,}2 \cdot \frac{1}{2} Amp\right) = 0{,}4 \cdot Amp = 0{,}4 \cdot 0{,}5\,\text{V} = 0{,}2\,\text{V}$$

où

$A_{\text{pos}\approx}$ est la composante alternative de A_{pos};

$A_{\text{neg}\approx}$ est la composante alternative de A_{neg}.

La composante continue de A_{pos} est augmentée de 16 % dans le même temps. Lorsque $S_{=}$ = 2,5 V, le signal différentiel A a alors la valeur moyenne suivante (au lieu de zéro dans le cas exempt d'*anomalie*):

$$A_{=} = A_{\text{pos}=} - A_{\text{neg}=} = 1{,}16 \cdot S_{=} - S_{=} = 0{,}16 \cdot S_{=} = 0{,}16 \cdot 2{,}5\,\text{V} = 0{,}4\,\text{V}$$

où

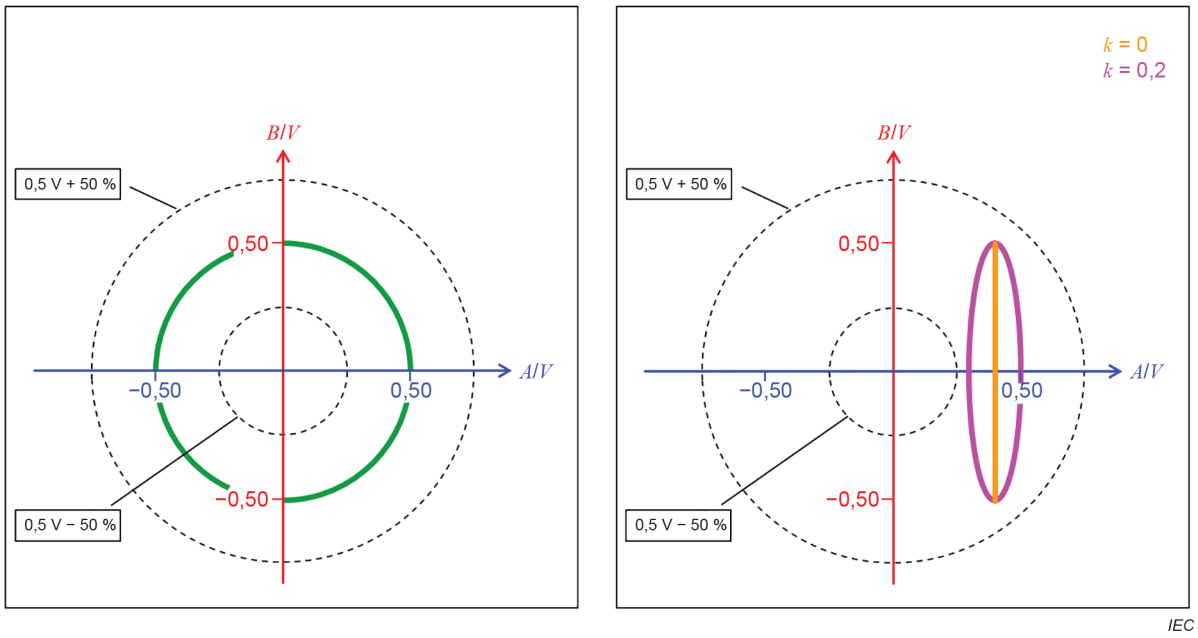
$A_{\text{pos}=}$ est la composante continue de A_{pos};

$A_{\text{neg}=}$ est la composante continue de A_{neg}.

Les deux signaux B ne sont pas déformés.

Il est admis par hypothèse que l'essai d'intégrité du signal analogique est une surveillance de la longueur de pointeur en vue d'un dépassement ou d'une chute au-dessous de la valeur nominale (0,5 V) de ± 50 %.

La Figure L.5 représente les courbes d'extrémité de phaseur qui en résultent: la Figure L.5 a), pour comparaison, représente la courbe idéale du cas exempt d'*anomalie* (vert), et la Figure L.5 b) représente les deux cas d'*anomalies* avec k = 0 et k = 0,2 (orange et magenta). Les courbes limites de la longueur de phaseur pour la surveillance de l'amplitude apparaissent sous forme de cercles discontinus.



a) Sans anomalie **b) Anomalie critique**

Légende

A signal sinus différentiel exprimé en volt

B signal cosinus différentiel exprimé en volt

k facteur d'amplitude de A_{pos} et A_{neg} qui résulte d'un *défaut* unique

Figure L.5 – Figures de Lissajous (représentation du signal B sur le signal A) dans deux cas d'*anomalies*

Les seuils de commutation pour la formation d'ondes carrées sont disposés symétriquement autour du zéro des tensions de A et B. Le résultat est qu'en présence des deux cas d'*anomalies* (k = 0 et k = 0,2), le signal A ne passe plus par les deux seuils de commutation; de ce fait, les signaux de sortie $A_{sqw}1$ et $A_{sqw}2$ des deux formateurs d'ondes carrées (voir Figure L.4) deviennent statiques. Par conséquent, les deux compteurs de position comptent un point vers l'avant puis un point vers l'arrière de façon continue, simulant ainsi l'immobilité.

Sur la Figure L.5 b), il est évident que les deux courbes d'extrémité de phaseur se situent dans la plage admissible entre les cercles de limite d'amplitude. Cette *anomalie* n'est donc pas détectée par la surveillance de la longueur de phaseur avec les paramètres admis par hypothèse ici. La détection de TOUTES les *anomalies* ne peut être obtenue que si de telles *anomalies* sont à prévoir.

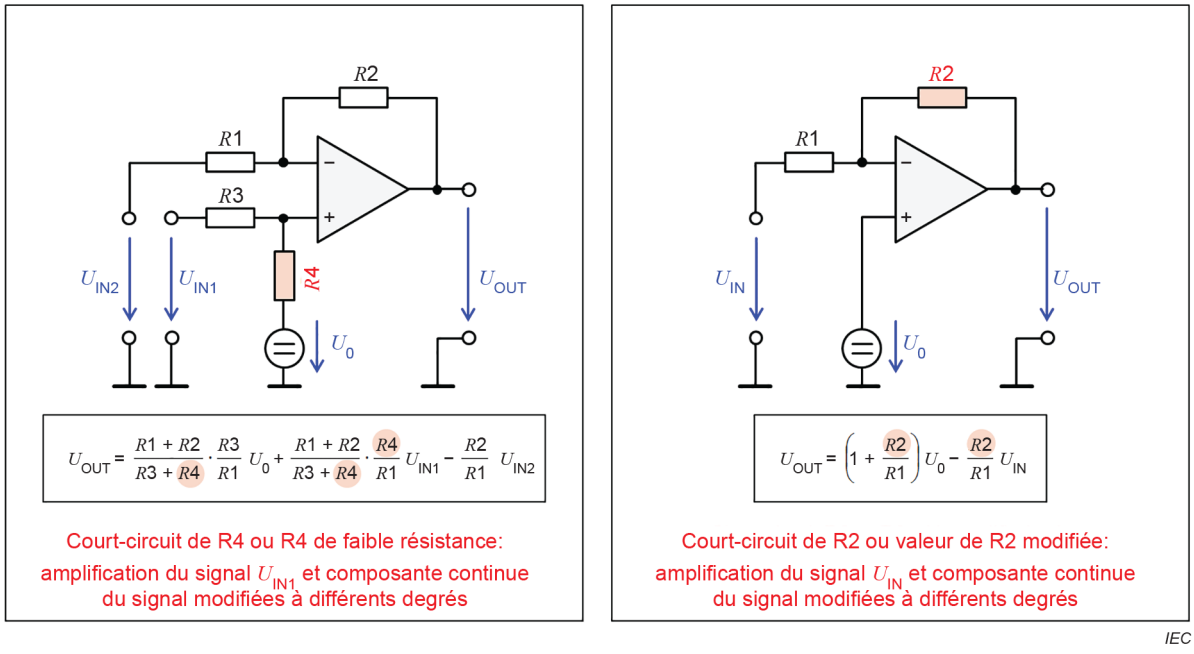
La FMEDA doit être utilisée pour vérifier si de tels scénarios critiques peuvent se produire avec le matériel donné du *codeur(SR)* en combinaison avec la spécification du *traitement des signaux* envisagée, et pour démontrer que de tels scénarios peuvent être exclus.

L.7.3 Procédure pour la FMEDA

A l'aide d'une FMEDA au niveau des composants et des circuits, le potentiel d'*anomalie* de tous les composants est examiné de façon habituelle et systématique en ce qui concerne les effets sur les signaux de sortie du circuit et l'efficacité des diagnostics mis en œuvre en cas de comportement critique du circuit.

Du fait d'hypothèses d'*anomalies* aléatoirement complexes pour les composants de circuits électroniques, il est toujours possible d'obtenir les scénarios critiques du type décrit ci-dessus. Cependant, au cours d'une FMEDA, seuls les types de défaillances de composants qui sont répertoriés dans les modèles de *défaut* décrits du D.3.1 au D.3.15 de l'IEC 61800-5-2:2016 peuvent être admis par hypothèse de façon réaliste. Ces types de défaillances qui ne peuvent pas être exclus, mais qui doivent être maîtrisés au moyen des diagnostics, sont en grande partie identiques aux *défauts* qui doivent être détectés avec une "haute" *couverture du diagnostic*, conformément à l'Annexe A de l'IEC 61508-2:2010 (par exemple, "modèle de *défaut* DC").

Le scénario d'*anomalie* critique décrit ci-dessus est dû à une variation de l'amplification et à un décalage simultané de la composante continue. Le fait que ce double effet puisse en principe être provoqué par une *anomalie* de composant unique est démontré à l'aide des circuits amplificateurs normalisés de la Figure L.6. Cette réalisation souligne la nécessité d'une FMEDA du matériel spécifique du *codeur(SR)*.



a) Amplificateur différentiel avec réglage du point de fonctionnement

b) Amplificateur inverseur avec réglage du point de fonctionnement

NOTE Pour les équations de la présente figure, des amplificateurs dont le fonctionnement est idéal ont été admis par hypothèse à des fins de simplicité (courants d'entrée et impédance de sortie nuls, amplification interne infinie, aucun décalage).

Figure L.6 – Exemples du double effet d'une *anomalie* de composant unique

La Figure L.6 a) représente un circuit d'amplificateur différentiel avec réglage du point de fonctionnement. En raison d'une *anomalie* de composant, un court-circuit de $R4$ ou une faible valeur de résistance de $R4$ est possible. Dans ce cas, l'amplification de U_{IN1} et la composante continue du signal sont modifiées à différents degrés par un *défaut* unique de $R4$.

La Figure L.6 b) représente un circuit d'amplificateur inverseur avec réglage du point de fonctionnement. En raison d'une *anomalie* de composant, un court-circuit de $R2$ ou une valeur de résistance modifiée de $R2$ est possible. Dans ce cas, l'amplification de U_{IN} et la composante continue du signal sont modifiées à différents degrés par un *défaut* unique de $R2$.

Il est en principe admissible que les utilisateurs organisent et paramètrent différemment le *traitement des signaux*. Toutefois, si la FMEDA du *codeur(SR)* révèle que des signaux de sortie potentiellement critiques du type indiqué ci-dessus peuvent être générés par des *défauts* uniques, cela doit être décrit dans les informations pour l'utilisation, de sorte que le *traitement des signaux* dans une application puisse être conçu en conséquence. Une forme pertinente d'information consiste en la transmission de signaux d'essai supplémentaires qui représentent les *anomalies* potentiellement critiques du *codeur(SR)* et doivent être maîtrisés pendant l'analyse statique.

L.8 Liste des variables utilisées pour effectuer l'analyse statique

L'Article L.8 contient une liste de toutes les variables utilisées pour effectuer l'analyse statique et fournit une description concise et précise.

NOTE 1 Il est possible que les descriptions qui figurent à l'Article L.8 utilisent, pour expliquer la signification des variables, des formulations différentes de la formulation utilisée dans l'introduction des variables dans les paragraphes précédents de l'Annexe L. Cela permet d'expliquer le contenu des informations concernées de différentes façons.

A_{pos} signal d'essai cosinus avec composante continue;

A_{neg} signal d'essai cosinus inversé avec composante continue;

B_{pos} signal d'essai sinus avec composante continue;

B_{neg} signal d'essai sinus inversé avec composante continue;

φ valeur de position continue;

NOTE 2 Position de l'*indicateur statique* par rapport à la partie capteur du *codeur(SR)*, où φ varie de 360° (2 π) sur une période de l'*indicateur statique*.

n valeur de position discrète;

NOTE 3 Entier, qui indique les positions discrètes en spécifiant le nombre de pas de 1/100 de la période de l'*indicateur statique*.

$S_{=}$ composante de décalage;

Amp amplitude de la composante alternative;

$A_{pos}(n)$ signal d'essai cosinus avec composante continue à la valeur de position n;

$A_{neg}(n)$ signal d'essai cosinus inversé avec composante continue à la valeur de position n;

$B_{pos}(n)$ signal d'essai sinus avec composante continue à la valeur de position n;

$B_{neg}(n)$ signal d'essai sinus inversé avec composante continue à la valeur de position n;

$A(n)$ signal d'essai cosinus différentiel A à la valeur de position n;

$B(n)$ signal d'essai sinus différentiel B à la valeur de position n;

$A_{sqw}(n)$ signal à ondes carrées obtenu à partir de $A(n)$ à la valeur de position n;

$B_{sqw}(n)$ signal à ondes carrées obtenu à partir de $B(n)$ à la valeur de position n;

A_{on}, $A_{off,}$ seuils de commutation de la bascule de Schmitt du signal A;

B_{on}, B_{off} seuils de commutation de la bascule de Schmitt du signal B;

$A_{sl}(n)$ variable auxiliaire binaire qui indique la présence d'une pente de $A_{sqw}(n)$ à la valeur de position n (vrai: 1, faux: 0);

$B_{sl}(n)$ variable auxiliaire binaire qui indique la présence d'une pente de $B_{sqw}(n)$ à la valeur de position n (vrai: 1, faux: 0);

$A_{nsl}(n)$ nombre de pentes de $A_{sl}(n)$ sur 1,1 fois la période du signal d'essai avant n;

$B_{nsl}(n)$ nombre de pentes de $B_{sl}(n)$ sur 1,1 fois la période du signal d'essai avant n;

$A_{stat}(n)$ variable auxiliaire binaire qui indique que $A_{sqw}(n)$ est évalué comme statique à la valeur de position n (vrai: 1, faux: 0);

$B_{stat}(n)$ variable auxiliaire binaire qui indique que $B_{sqw}(n)$ est évalué comme statique à la valeur de position n (vrai: 1, faux: 0);

$IFD(n)$ variable auxiliaire binaire qui indique qu'une *anomalie* est détectée par une *détection de défaut idéale* optimale à la valeur de position n (vrai: 1, faux: 0);

$SFD(n)$ variable auxiliaire binaire qui indique que les mesures diagnostiques spécifiées du signal de sortie analogique du *codeur(SR)* détectent une *anomalie* à la valeur de position n (vrai: 1, faux: 0);

$SFD_{1P}(n)$ variable auxiliaire binaire qui indique que les mesures diagnostiques spécifiées détectent une *anomalie* sur 1,1 fois la période de l'*indicateur statique* à partir de la valeur de position *n* (vrai: 1, faux: 0);

Amp^2_{min} limite inférieure du carré de la longueur de pointeur spécifiée;

Amp^2_{max} limite supérieure du carré de la longueur de pointeur spécifiée;

$R(n)$ résultat de l'analyse statique des mesures diagnostiques spécifiées (concernant un signal d'essai spécifique) pour une valeur de position donnée n;

NOTE 4 $R(n)$ prend hypothétiquement l'une des quatre valeurs "optimale", "acceptable", "non acceptable" ou "non liée à la sécurité".

$r(n)$ variable auxiliaire binaire qui indique que les mesures diagnostiques spécifiées ne signalent pas d'*anomalie* à la valeur de position n, tandis que la *détection de défaut idéale* signale une *anomalie* (vrai: 1, faux: 0);

R résultat de l'analyse statique des mesures diagnostiques spécifiées (concernant un signal d'essai spécifique) par rapport à leur aptitude à signaler une *anomalie* à toute position n où la *détection de défaut idéale* le fait;

NOTE 5 R prend hypothétiquement l'une des valeurs "optimale" ou "non optimale".

$r_{1P}(n)$ variable auxiliaire binaire qui indique que les mesures diagnostiques spécifiées ne parviennent pas à signaler une *anomalie* sur 1,1 fois la période de l'*indicateur statique* à partir de la valeur de position n (vrai: 1, faux: 0);

R_{1P} résultat global de l'analyse statique des mesures diagnostiques spécifiées (concernant un signal d'essai spécifique) par rapport à leur aptitude à signaler une *anomalie* sur 1,1 fois la période de l'*indicateur statique*;

NOTE 6 R_{1P} prend hypothétiquement l'une des valeurs "acceptable" ou "non acceptable".

$A_{\approx pp}$ composante alternative (crête à crête) du signal différentiel A;

$A_{=}$ valeur moyenne du signal différentiel A;

$A_{pos\approx}$ composante alternative de A_{pos};

$A_{neg\approx}$ composante alternative de A_{neg};

$A_{pos=}$ est la composante continue de A_{pos};

$A_{neg=}$ composante continue de A_{neg}; et

k facteur d'amplitude de A_{pos} et A_{neg} (respectivement $A_{pos}(n)$ et $A_{neg}(n)$) qui résulte d'un *défaut* unique hypothétique dans le *codeur(SR)*.

L.9 Outil MS Excel pour l'exécution de l'analyse statique

L'analyse statique peut être effectuée à l'aide d'un fichier MS Excel fourni par l'IFA avec les macros intégrées (voir [17]). Les signaux d'essai normalisés répertoriés à l'Article L.4 sont déjà contenus dans le fichier. D'autres signaux d'essai peuvent être ajoutés si nécessaire. Les instructions pour l'utilisateur sont contenues dans le fichier.

Annexe M
(informative)

Aspects des mesures diagnostiques en vue de l'obtention des valeurs de position incrémentale

M.1 Généralités

L'Annexe M traite de certains modèles de *défaut* spécifiques et de leurs effets sur la qualité du signal analogique et sur la plage de tolérances sûre atteignable. Elle n'est pas exhaustive, et il convient que le fabricant s'assure que les modèles de *défaut* applicables à son produit soient traités de manière appropriée dans une FMEDA.

Les mesures diagnostiques du *codeur(SR)* peuvent être mises en œuvre, en partie ou entièrement, dans l'*unité d'évaluation* (voir 6.3). Les mesures diagnostiques qui doivent être mises en œuvre dans l'*unité d'évaluation* sont spécifiées dans les informations pour l'utilisation (voir Annexe F). Dans le cadre de la FMEDA (voir 8.4) du *codeur(SR)*, il doit être démontré que la spécification des mesures diagnostiques externes permet d'obtenir la détection de *défaut* exigée.

Pour un *codeur(SR)* avec signaux de sortie sinus et cosinus et *HFT* = 0, la *détection de défaut idéale* est nécessaire pour atteindre la *tolérance au premier défaut* (voir 6.4.1). La surveillance de la longueur de phaseur est généralement appliquée comme mesure diagnostique. En principe, il peut exister des scénarios d'*anomalie* qui ne peuvent pas être détectés par la surveillance de la longueur de phaseur. Déterminer si la surveillance de la longueur de phaseur constitue une mesure diagnostique suffisante dépend des *anomalies* possibles et des exclusions de *défauts* admissibles du *codeur(SR)* spécifique, ainsi que des propriétés de la ou des *sous-fonction(s) de sécurité* mises en œuvre, en particulier de la résolution de position spécifiée.

L'Annexe M traite exclusivement de l'obtention des valeurs de position sûres à partir des signaux analogiques sinus et cosinus. Pour cela, la détermination correcte de la direction du mouvement est essentielle.

Tout d'abord, un aperçu de la génération des valeurs de position est donné pour le cas sans anomalie (voir Article M.2). Après cela, des scénarios d'*anomalie* sont introduits, et dans chaque cas, la performance de la surveillance de la longueur de phaseur est traitée (voir Article M.3 et Article M.4). Ces présentations doivent appuyer l'exécution de la FMEDA sur un *codeur(SR)*.

Les principes traités à l'Annexe M sont relatifs au *codeur(SR)* avec signaux de sortie sinus et cosinus, mais aussi au *codeur(SR)* avec signaux de sortie à ondes carrées et au *codeur(SR)* avec signaux de sortie numériques lorsque la partie de génération des signaux du *codeur(SR)* inclut des signaux sinus et cosinus.

M.2 Obtention des valeurs de position à partir de signaux incrémentaux

Afin de générer en continu une valeur de position actuelle à partir des signaux de sortie sinus et cosinus incrémentaux, ces signaux sont généralement traités comme suit:

a) conversion des signaux sinus et cosinus en signaux à ondes carrées;

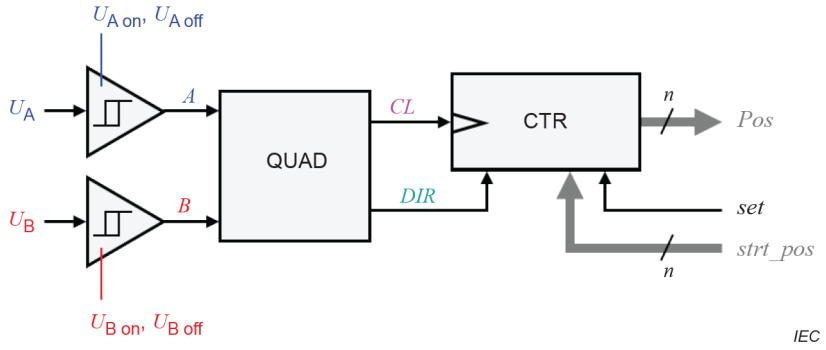
b) génération d'un signal d'horloge (impulsions de comptage) et d'un signal de direction du mouvement à partir des signaux à ondes carrées au moyen d'un décodeur en quadrature; et

c) pilotage d'un compteur pour la valeur de position avec le signal d'horloge et le signal de direction.

La Figure M.1 décrit, de manière symbolique, un circuit pour l'obtention des valeurs de position à partir de signaux analogiques incrémentaux. Sur cette figure, U_A et U_B représentent respectivement les signaux cosinus et sinus, tandis que A et B représentent les signaux à ondes carrées qui en résultent.

$U_{A\ on}$ et $U_{A\ off}$ correspondent aux seuils auxquels le conformateur d'ondes carrées (bascule de Schmitt) pour le signal cosinus U_A bascule son signal de sortie A sur une logique 1 ou sur une logique 0, respectivement. De même, $U_{B\ on}$ et $U_{B\ off}$ correspondent aux seuils auxquels le conformateur d'ondes carrées pour le signal cosinus U_B bascule son signal de sortie B sur une logique 1 ou sur une logique 0, respectivement. Les signaux à ondes carrées sont envoyés dans un décodeur en quadrature QUAD qui génère, à partir de ceux-ci, les signaux CL et DIR pour le compteur de valeurs de position CTR.

CL est le signal d'horloge et DIR est le signal de direction, qui déterminent la direction de comptage du compteur. Le compteur donne son comptage sous la forme d'une valeur de position Pos qui comprend n chiffres binaires. A l'aide d'un signal d'initialisation set, une valeur de position de départ $strt\_pos$ peut être chargée dans le compteur.



Légende

U_A	signal cosinus
U_B	signal sinus
$U_{A\ on}$, $U_{A\ off}$, $U_{B\ on}$, $U_{B\ off}$	seuils de commutation
A, B	signaux à ondes carrées
QUAD	décodeur en quadrature
CL	signal d'horloge
DIR	signal de direction
CTR	compteur
Pos	valeur de position
n	nombre de bits
set	signal d'initialisation
strt_pos	position de départ

Figure M.1 – Obtention des valeurs de position à partir de signaux incrémentaux

Au moyen de leur signal d'horloge, les décodeurs en quadrature types fournissent une impulsion de comptage à chaque pente du signal à ondes carrées sinus et du signal à ondes carrées cosinus. Ainsi, sur une période de l'*indicateur statique*, un décodeur en quadrature de ce type génère quatre impulsions de comptage. La Figure M.2 représente le comportement sans anomalie du circuit pour le déclenchement du compteur de position.

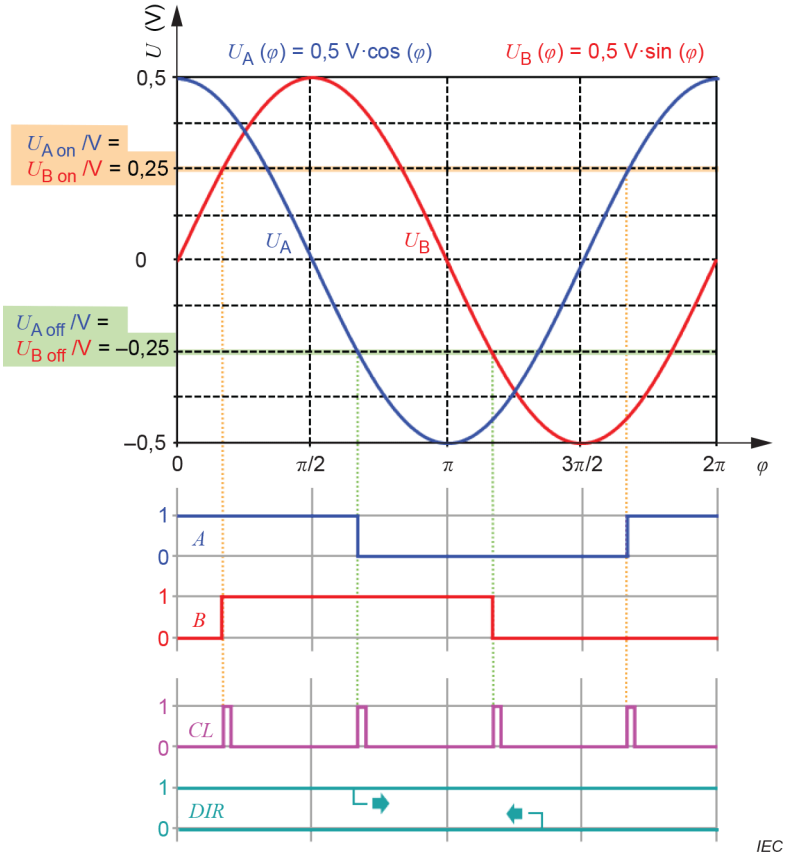


Figure M.2 – Génération d'impulsions de comptage, cas sans anomalie

Avec ce type de pilotage, le comptage représente les valeurs de position avec une résolution de position d'un quart de période de l'*indicateur statique*. Dans le cas idéal, l'applicabilité des valeurs de position sur une période de l'*indicateur statique* (résolution fine) présuppose que les quatre impulsions de comptage divisent la période de l'*indicateur statique* en quatre segments de taille égale.

M.3 Erreur de phase des signaux sinus et cosinus

M.3.1 Généralités

Selon la relation fonctionnelle $\cos\varphi = \sin(\varphi + 90°)$, le décalage de phase entre les signaux cosinus et sinus idéaux est de 90°. Ci-après, il est question des *anomalies* pour lesquelles le décalage de phase entre les signaux cosinus et sinus n'est plus de 90°, mais de 90° – $\Delta\varphi$. Cela signifie que le signal cosinus U_A varie selon un angle $\Delta\varphi$, l'erreur de phase, par rapport au signal cosinus idéal.

NOTE Si la conception le permet, les erreurs de phase peuvent, par exemple, résulter d'une contorsion marginale du capteur par rapport à l'*indicateur statique*.

M.3.2 Erreurs de phase avec des valeurs absolues < 90°

Avec des erreurs de phase $\Delta\varphi$, dont la valeur absolue reste juste inférieure à 90°, par exemple avec $-90° < \Delta\varphi < 90°$, un décodeur en quadrature idéal produit toujours un signal de direction DIR correct. Dans le cas d'un décodeur en quadrature réel, la valeur absolue de l'erreur de phase $\Delta\varphi$ doit être (selon la fréquence) un peu plus faible que 90°, afin de permettre la génération d'un signal de direction correct, et d'éviter ainsi une direction de comptage erronée du compteur de position.

Toute erreur de phase $\Delta\varphi$ comprise entre –90° et +90° entraîne un décalage des impulsions de comptage sur l'axe de l'angle ou, respectivement, de la position (axe φ) au cours de la période de l'*indicateur statique*. Cet effet est représenté dans la Figure M.3, avec une erreur de phase $\Delta\varphi$ = 20°.

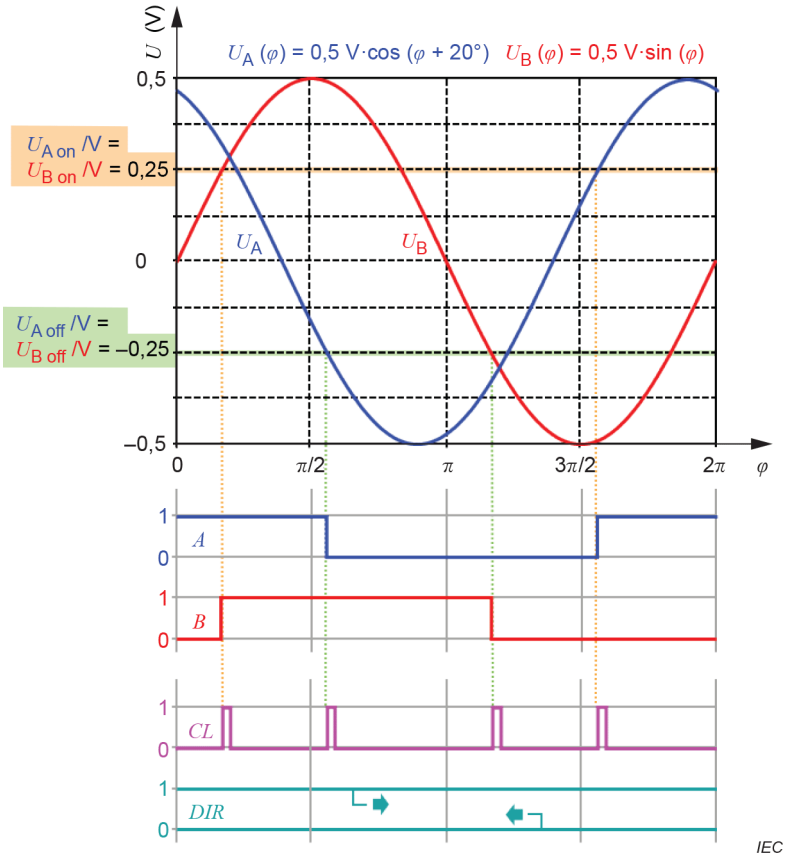


Figure M.3 – Génération d'impulsions de comptage avec une erreur de phase de 20°

Par rapport au cas sans anomalie (Figure M.2), les impulsions de comptage CL de la Figure M.3 ne présentent plus la même distance, par exemple la période de l'*indicateur statique* n'est plus divisée en quatre segments de taille égale. Par conséquent, la résolution de position au cours de la période de l'*indicateur statique* est compromise; ainsi, la précision du calcul de position diminue. Si la résolution fine de quatre segments par période de l'*indicateur statique* doit être utilisée pour la ou les *fonctions de sécurité*, et si des erreurs de phase $\Delta\varphi$ qui compromettent la résolution de position spécifiée ne peuvent pas être exclues, des erreurs de phase qui dépassent la plage de tolérances sûre doivent être détectées par des mesures diagnostiques appropriées.

La résolution de position au cours de la période de l'*indicateur statique* est également compromise si ces valeurs de position sont déterminées à l'aide de l'*interpolation*.

En raison des tolérances communément admises, la surveillance de la longueur de phaseur détecte les erreurs de phase uniquement au-dessus d'une amplitude à laquelle la résolution fine au cours de la période de l'*indicateur statique* est déjà défectueuse. La Figure M.4 représente la figure de Lissajous des tensions de signal U_A et U_B avec une erreur de phase de 20° (orange) et, pour comparaison, du cas sans anomalie (pointillés verts).

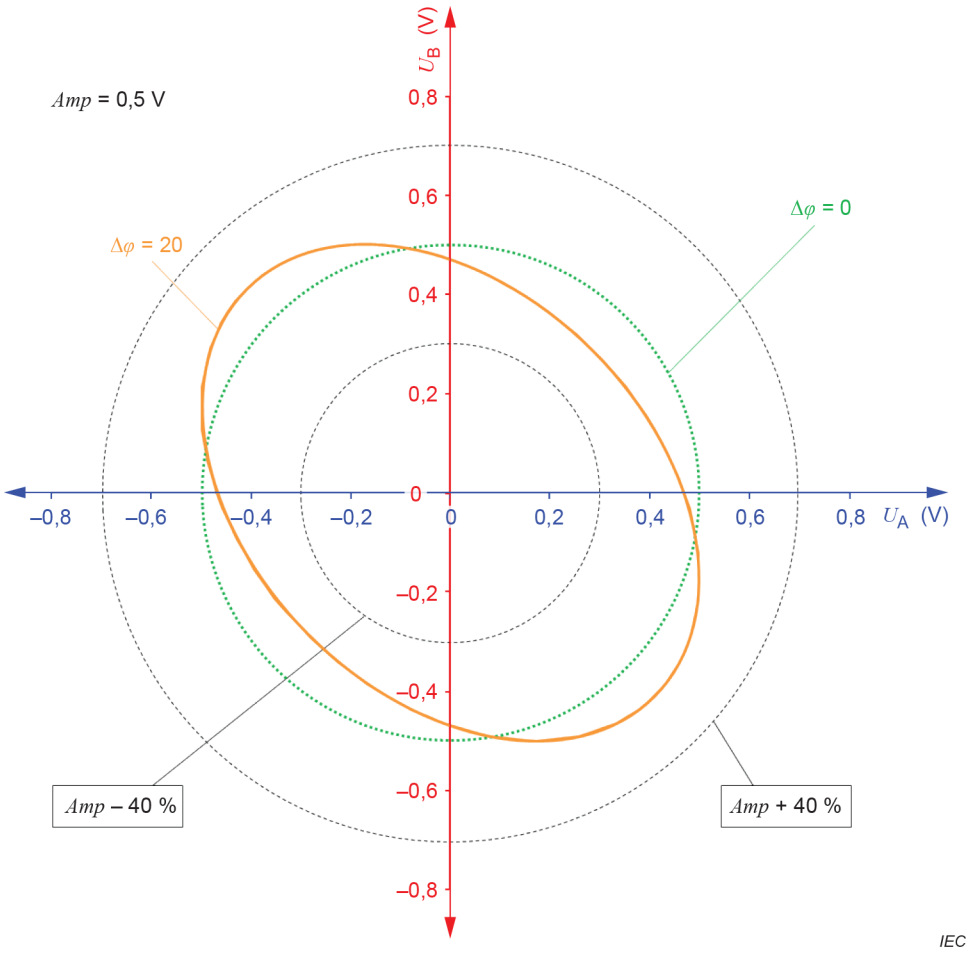


Figure M.4 – Figure de Lissajous avec une erreur de phase $\Delta\varphi$ = 20°

Dans l'exemple de la Figure M.4, la longueur nominale Amp du phaseur est de 0,5 V. Il est admis par hypothèse que les limites de tolérance sont Amp – 40 % = 0,3 V et Amp + 40% = 0,7 V. La figure de Lissajous de couleur orange, qui représente une erreur de phase de 20°, reste dans cette tolérance de longueur de phaseur admise. Par conséquent, la surveillance de la longueur de phaseur ne permet pas de détecter cette erreur de phase, alors que la résolution fine au cours de la période de l'*indicateur statique* est déjà défectueuse. Sur la Figure M.3, cela est identifiable par la subdivision inégale de la période par impulsions de comptage CL.

La surveillance de la longueur de phaseur ne répond qu'en cas d'erreurs de phase $\Delta\varphi$ encore plus importantes. Si Amp_{min} est la limite inférieure de la longueur de phaseur Amp, alors le seuil de réponse $\Delta\varphi_{DT}$ (DT: seuil de détection, *Detection Threshold*) est défini par

$$\Delta\varphi_{DT} = \pm\arcsin\left[1-\left(\frac{Amp_{min}}{Amp}\right)^2\right]$$

en prenant pour hypothèse que les amplitudes de signal de U_A et de U_B ne sont pas réajustées au cours de la période de l'*indicateur statique*.

Dans l'exemple numérique de la Figure M.4, la plage de tolérances de la longueur de phaseur est de ± 40 % de la valeur nominale, Amp_{min}/Amp = 0,6. A partir de ces résultats, un seuil de réponse de $\Delta\varphi_{DT}$ = ± 39,8° en cas d'amplitudes de signal non réajustées est calculé. Avec une

tolérance admise de ± 50 %, par exemple Amp_{min}/Amp = 0,5, le seuil de réponse $\Delta\varphi_{DT}$ avec des amplitudes non réajustées est de ± 48,6°. Ces valeurs absolues de $\Delta\varphi_{DT}$ sont bien au-dessous de la valeur critique de 90°, dont le dépassement se traduit par le fait que le décodeur en quadrature produit une direction erronée du mouvement. Ainsi, la surveillance de la longueur de phaseur dans sa forme type est souvent appropriée pour détecter une erreur de phase qui augmente lentement à partir de zéro, avant que le décodeur en quadrature ne signale une direction erronée du mouvement.

Pour assurer la qualité ainsi que la stabilité temporelle du signal, un contrôle de l'amplitude des signaux sinus et cosinus est souvent mis en œuvre. Ici, l'amplitude des signaux est affectée de manière telle que la valeur de $U_A^2 + U_B^2$ ainsi que la longueur de phaseur restent constantes ou, au moins, presque constantes. Si le contrôle fonctionne de manière quasi instantanée, les écarts de longueur de phaseur sont également compensés au cours la période de l'*indicateur statique*, même en cas de mouvements rapides. Eventuellement, une figure de Lissajous elliptique, telle que celle de la Figure M.4, peut ainsi être redéfinie en un cercle idéal. Un contrôle d'amplitude comme celui-ci peut rendre les erreurs de phase $\Delta\varphi$ jusqu'à une certaine amplitude non visibles par la surveillance de la longueur de phaseur, tandis que l'erreur de phase elle-même n'est pas corrigée par le contrôle. Avec l'augmentation de l'erreur de phase $\Delta\varphi$, l'ellipse de Lissajous s'amincit de plus en plus et, au moins en cas de caractéristiques de contrôle linéaires, un contrôle d'amplitude réel n'est plus en mesure d'empêcher la réduction de la limite inférieure de la longueur de phaseur sur la période, même pour une moitié de la période de l'*indicateur statique*. En principe, cela permet à la surveillance de la longueur de phaseur de détecter l'erreur de phase avant que sa valeur absolue n'approche la limite critique de 90°. L'applicabilité ne peut être évaluée que par une analyse du comportement du circuit de contrôle d'amplitude réel.

Dans de nombreux cas, la surveillance de la longueur de phaseur est en mesure de détecter les erreurs de phase qui augmentent lentement avant que le décodeur en quadrature ne produise une direction erronée du mouvement par le signal DIR et donc que des positions complètement incorrectes ne soient calculées. L'un des objectifs de l'analyse statique est de s'en assurer (voir Annexe L). Comme indiqué ci-dessus, même les erreurs de phase inférieures au seuil de réponse de la surveillance de la longueur de phaseur peuvent compromettre la résolution des quadrants au cours de la période de l'*indicateur statique*.

M.3.3 Erreurs de phase avec des valeurs absolues > 90°

En cas d'erreurs de phase $\Delta\varphi$ avec des valeurs absolues comprises entre 90° et 270°, un décodeur en quadrature produit une direction erronée du mouvement. Dans le même temps, une longueur de phaseur dans l'intervalle admissible peut être atteinte. Par exemple, avec $\Delta\varphi$ = ± 180°, le phaseur présente constamment la longueur nominale qui correspond à une figure de Lissajous circulaire, étant donné que les amplitudes des signaux sinus et cosinus maintiennent leur amplitude nominale sur cette erreur de phase.

Si une erreur de phase augmente lentement à partir de zéro, il peut être possible de la détecter avant la détermination d'une direction erronée du mouvement (voir M.3.2 pour comparaison). Un cas distinct consiste en une erreur de phase avec une valeur absolue comprise entre 90° et 270° qui survient brusquement, par exemple à la suite d'un choc mécanique sur le *codeur(SR)* alors que la machine est hors tension. Si, par la suite, la longueur de phaseur atteint la plage admise, il n'y a aucune détection de *défaut* par surveillance de la longueur de phaseur, alors qu'une direction erronée du mouvement est produite dans le même temps.

La FMEDA du *codeur(SR)* spécifique peut préciser si une erreur de phase de cet ordre est possible, ou si son exclusion peut être justifiée. Si elle ne peut pas être exclue, il doit être déterminé si les mesures diagnostiques désignées détectent l'*anomalie*. Par exemple, si une erreur de phase de cet ordre est toujours associée à une diminution significative des amplitudes de signal, elle peut être détectée par surveillance de la longueur de phaseur. Dans le cas contraire, des mesures supplémentaires sont nécessaires.

M.4 Erreurs de seuil des conformateurs de signaux à ondes carrées

M.4.1 Généralités

La conversion d'un signal sinus ou cosinus en signal à ondes carrées est généralement effectuée par un conformateur d'ondes carrées (bascule de Schmitt) avec une hystérésis de commutation. Cette dernière est constituée par la différence des deux seuils de commutation, par exemple par $U_H = U_{on} - U_{off}$ avec $U_{on} > U_{off}$. Le principe de génération d'un signal à ondes carrées S à partir d'un signal sinus $U(\varphi)$ est représenté à la Figure M.5.

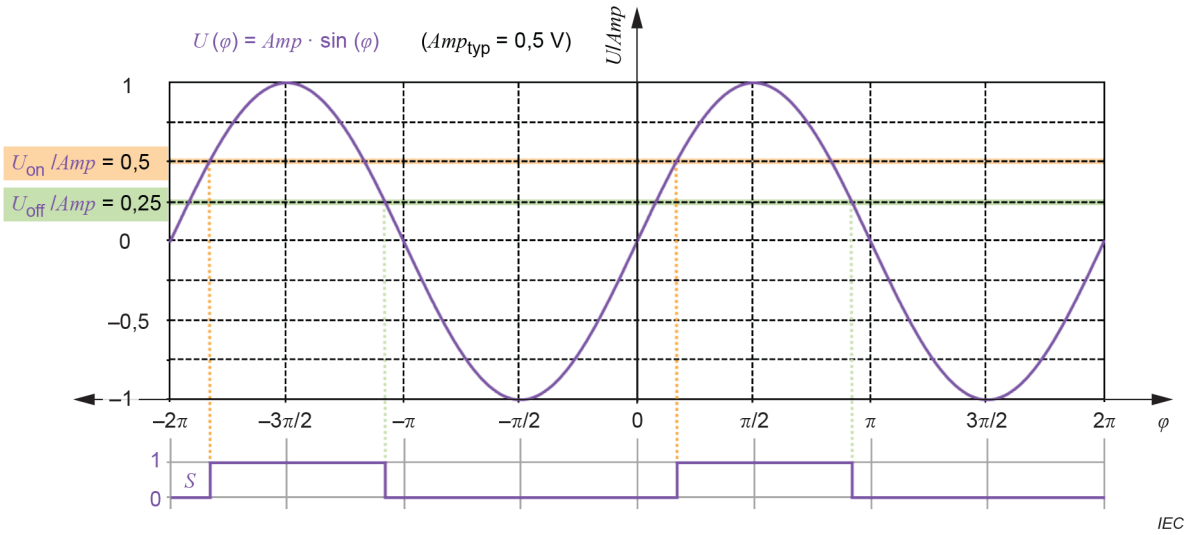


Figure M.5 – Génération d'un signal à ondes carrées au moyen d'une bascule de Schmitt

Dans le cas d'une oscillation de forme sinusoïdale d'amplitude Amp autour de zéro, ce qui suit s'applique pour le facteur de durée d'impulsions PDF du signal à ondes carrées généré:

$$PDF = \frac{1}{2} - \frac{\arcsin\left(\frac{U_{on}}{Amp}\right) + \arcsin\left(\frac{U_{off}}{Amp}\right)}{2\pi}.$$

Dans l'exemple de la Figure M.5, U_{on}/Amp = 0,5 et U_{off}/Amp = 0,25 se traduisent par un facteur de durée d'impulsions PDF = 0,376 5. Si les seuils de commutation sont disposés symétriquement autour de zéro (le centre du signal), par exemple dans le cas $U_{off} = -U_{on}$, alors:

$$PDF_{symm} = \frac{1}{2}.$$

Une disposition symétrique des seuils de commutation U_{on} et U_{off} autour de zéro et, ainsi, un facteur de durée d'impulsions de 0,5 sont des conditions préalables à la division de la période de l'*indicateur statique* en quatre segments égaux par les impulsions de comptage CL du décodeur en quadrature. Outre l'absence d'erreurs de phase, qui a déjà été traitée à l'Article M.3, une autre exigence pour la subdivision uniforme est que les seuils de commutation du signal cosinus U_A et du signal sinus U_B soient égaux, par exemple que $U_{A\ on} = U_{B\ on}$ et que $U_{A\ off} = U_{B\ off}$ s'appliquent. Ce cas sans anomalie est décrit à la Figure M.2.

Deux exemples d'*anomalies* sont présentés en M.4.2 et en M.4.3, pour lesquels les seuils de commutation s'écartent des valeurs correctes.

M.4.2 Seuils de commutation asymétriques

L'exemple de la Figure M.6 retient l'hypothèse de signaux cosinus et sinus idéaux. Les seuils de commutation pour la mise en forme des impulsions du signal cosinus U_A se situent à ± 0,25 V et sont donc symétriques par rapport au centre du signal, tandis que dans le cas du signal sinus U_B, seul le seuil d'activation $U_{B\ on}$ présente la valeur correcte de 0,25 V. En revanche, le seuil de désactivation $U_{B\ off}$ se situe à 0,125 V au lieu de –0,25 V.

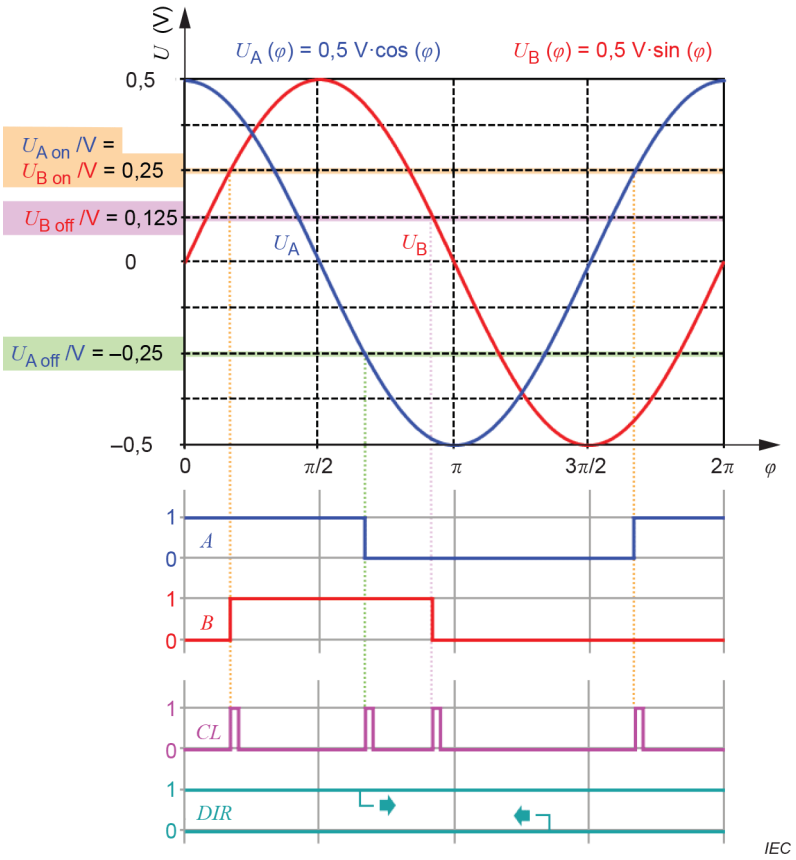


Figure M.6 – Génération d'impulsions de comptage avec seuils de commutation asymétriques

Le résultat de cette *anomalie* est que le signal à ondes carrées B ne présente plus le facteur de durée d'impulsions correct PDF = 0,5, mais, comme sur la Figure M.5, la valeur plus faible de 0,376 5. Dans le même temps, les pentes de désactivation du signal B sont décalées sur l'axe φ. Ainsi, chaque quart des impulsions de comptage CL est décalé sur l'axe φ. Une comparaison avec la Figure M.2 indique que sur la Figure M.6, le tiers des impulsions CL est décalé vers la gauche. Par conséquent, la période de l'*indicateur statique* n'est plus subdivisée en quatre segments égaux par les impulsions de comptage et la résolution fine est compromise.

La surveillance de la longueur de phaseur ne peut évidemment pas détecter cette *anomalie*, car elle évalue uniquement les signaux analogiques U_A et U_B. Des circuits redondants et des mesures diagnostiques appropriés sont nécessaires.

M.4.3 Hystérésis de commutation inégale à la mise en forme des ondes carrées pour le sinus et le cosinus

Là encore, l'exemple de la Figure M.7 retient l'hypothèse de signaux cosinus et sinus idéaux. Les seuils de commutation des deux signaux analogiques sont situés de manière symétrique autour du centre du signal (0 V), qui est également correct. Pour cette raison, les signaux à ondes carrées A et B générés présentent le facteur de durée d'impulsions correct PDF = 0,5. Cependant, l'hystérésis de commutation est différente pour le signal cosinus et pour le signal

sinus. Pour le signal sinus, $U_{B\,H} = U_{B\,on} - U_{B\,off}$ = 0,5 V. Pour le signal cosinus, l'hystérésis est seulement de $U_{A\,H} = U_{A\,on} - U_{A\,off}$ = 0,173 6 V.

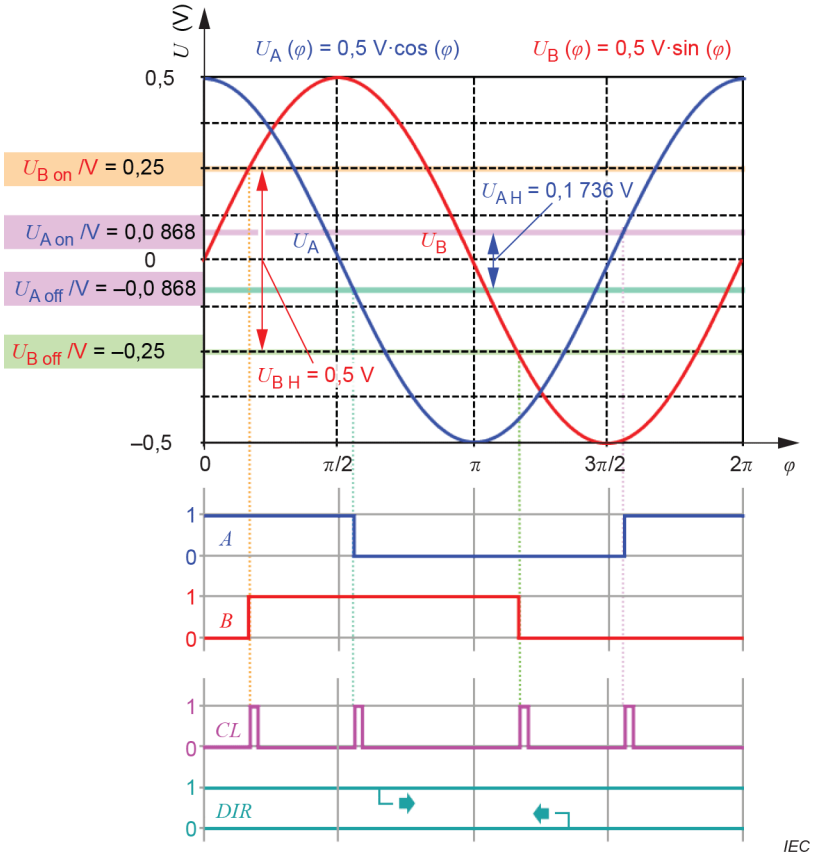


Figure M.7 – Génération d'impulsions de comptage avec hystérésis de commutation inégale

En raison de cette différence d'hystérésis, toutes les pentes de commutation du signal à ondes carrées A sont décalées vers la gauche, par rapport au cas où l'hystérésis pour l'un ou l'autre des signaux analogiques est de 0,5 V, comme sur la Figure M.2 et la Figure M.3. Ainsi, dans cet exemple également, la période de l'*indicateur statique* n'est plus subdivisée en quatre segments égaux par les impulsions de comptage CL et la résolution fine est compromise.

Les valeurs de tension de cet exemple ont été choisies par rapport aux signaux à ondes carrées A et B et aux impulsions de comptage CL de la Figure M.3. Une situation identique à celle de la Figure M.3 se produit, où la cause du décalage des impulsions est une erreur de phase des signaux analogiques de 20°. Une différence d'hystérésis de commutation des conformateurs d'impulsions peut ainsi provoquer un effet similaire, voire identique, à une authentique erreur de phase.

Dans ce cas aussi, la surveillance de la longueur de phaseur n'est pas capable de détecter cette *anomalie*, car elle évalue uniquement les signaux analogiques U_A et U_B. Là encore, des circuits redondants et des mesures diagnostiques appropriés sont nécessaires.

Bibliographie

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

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

[3] IEC 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

[4] IEC 61513, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

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

[6] Systematic calculation of highly stressed bolted joints – Joints with one cylindrical bolt, Beuth Verlag GmbH, Am DIN-Platz, Burggrafenstraße 6, D 10787 Berlin [consulté le 2020-10-21]. Disponible à l'adresse https://www.beuth.de/en/technical-rule/vdi-2230-blatt-1/242566299

[7] Analytical Strength Assessment, VDMA Verlag GmbH, Lyoner Straße 18, D 60528 Frankfurt am Main [consulté le 2020-10-21]. Disponible à l'adresse http://www.vdmashop.de/Forschungshefte--FKM-/Analytical-Strength-Assessment-6-th-Edition.html

[8] ISO/TS 16281:2008, *Roulements – Méthodes de calcul de la durée nominale de référence corrigée pour les roulements chargés universellement*

[9] ANSI/ASA S2.62-2009, *Shock Test Requirements for Equipment in a Rugged Shock Environment* (disponible en anglais seulement), réaffirmée par l'ANSI le 24 juin 2014

[10] ISO 18431-4:2007, *Mechanical vibration and shock – Signal processing – Part 4: Shock-response spectrum analysis* (disponible en anglais seulement)

[11] Piersol, T. Paez: Harris' Shock and Vibration Handbook – Sixth Edition, MCGraw-Hill, New York, 2010

[12] Rapport IFA 2/2017e *"Safety of machine controls to EN ISO 13849", Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung* [consulté le 2020-10-21]. Disponible à l'adresse www.dguv.de, webcode e89507

[13] SN 29500, *Ausfallraten Bauelemente, Erwartungswerte*. Siemens AG Corporate Technology, Technology & Innovation Management, CT TIM IR SI, Otto-Hahn-Ring 6, 81739 München, Deutschland, tél.: +49 89 636-634154, michaela.pabst@siemens.com

[14] Safety Equipment Reliability Handbook [consulté le 2020-10-21]. Disponible à l'adresse https://www.shopexida.com/products/safety-equipment-reliability-handbook-4th-edition

[15] Nonelectronics Parts Reliability Data, Reliability Analysis Center, NPRD-91, 1991

[16] IEC 61709:2017, *Composants électroniques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles de contraintes pour la conversion*

[17] Static Analysis of signal evaluation and fault detection for rotary and position measuring systems for functional safety; Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung [consulté le 2020-10-21]. Disponible à l'adresse www.dguv.de, webcode d11973 (pièce jointe au document GS-IFA-M21 E)

[18] IEC 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

[19] ISO/TR 23849:2010, *Lignes directrices relatives à l'application de l'ISO 13849-1 et de l'IEC 62061 dans la conception des systèmes de commande des machines relatifs à la sécurité*[2]

[20] IEC 61508-6:2010, *Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

_____

2 Ce document a été supprimé.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
info@iec.ch
www.iec.ch