IEC 61069-7

Edition 2.0 2016-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 7: Assessment of system safety

Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 7: Évaluation de la sécurité d'un système

IEC 61069-7:2016-06(en-fr)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

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

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

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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: csc@iec.ch.

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.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
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 aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

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

IEC 61069-7

Edition 2.0 2016-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 7: Assessment of system safety

Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 7: Évaluation de la sécurité d'un système

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8322-3450-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – EVALUATION OF SYSTEM PROPERTIES FOR THE PURPOSE OF SYSTEM ASSESSMENT –

Part 7: Assessment of system safety

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 61069-7 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 1999. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) reorganization of the material of IEC 61069-7:1999 to make the overall set of standards more organized and consistent;
b) IEC TS 62603-1 has been incorporated into this edition.

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/795/FDIS	65A/805/RVD

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

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

A list of all parts in the IEC 61069 series, published under the general title *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment,* can be found on the IEC website.

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

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

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

IEC 61069 deals with the method which should be used to assess system properties of a basic control system (BCS). IEC 61069 consists of the following parts.

Part 1: Terminology and basic concepts

Part 2: Assessment methodology

Part 3: Assessment of system functionality

Part 4: Assessment of system performance

Part 5: Assessment of system dependability

Part 6: Assessment of system operability

Part 7: Assessment of system safety

Part 8: Assessment of other system properties

Assessment of a system is the judgement, based on evidence, of the suitability of the system for a specific mission or class of missions.

To obtain total evidence would require complete evaluation (for example under all influencing factors) of all system properties relevant to the specific mission or class of missions.

Since this is rarely practical, the rationale on which an assessment of a system should be based is:

– the identification of the importance of each of the relevant system properties,
– the planning for evaluation of the relevant system properties with a cost-effective dedication of effort to the various system properties.

In conducting an assessment of a system, it is crucial to bear in mind the need to gain a maximum increase in confidence in the suitability of a system within practical cost and time constraints.

An assessment can only be carried out if a mission has been stated (or given), or if any mission can be hypothesized. In the absence of a mission, no assessment can be made; however, evaluations can still be specified and carried out for use in assessments performed by others. In such cases, IEC 61069 can be used as a guide for planning an evaluation and it provides methods for performing evaluations, since evaluations are an integral part of assessment.

In preparing the assessment, it can be discovered that the definition of the system is too narrow. For example, a facility with two or more revisions of the control systems sharing resources, for example a network, should consider issues of co-existence and inter-operability. In this case, the system to be investigated should not be limited to the “new” BCS; it should include both. That is, it should change the boundaries of the system to include enough of the other system to address these concerns.

The series structure and the relationship among the parts of IEC 61069 are shown in Figure 1.

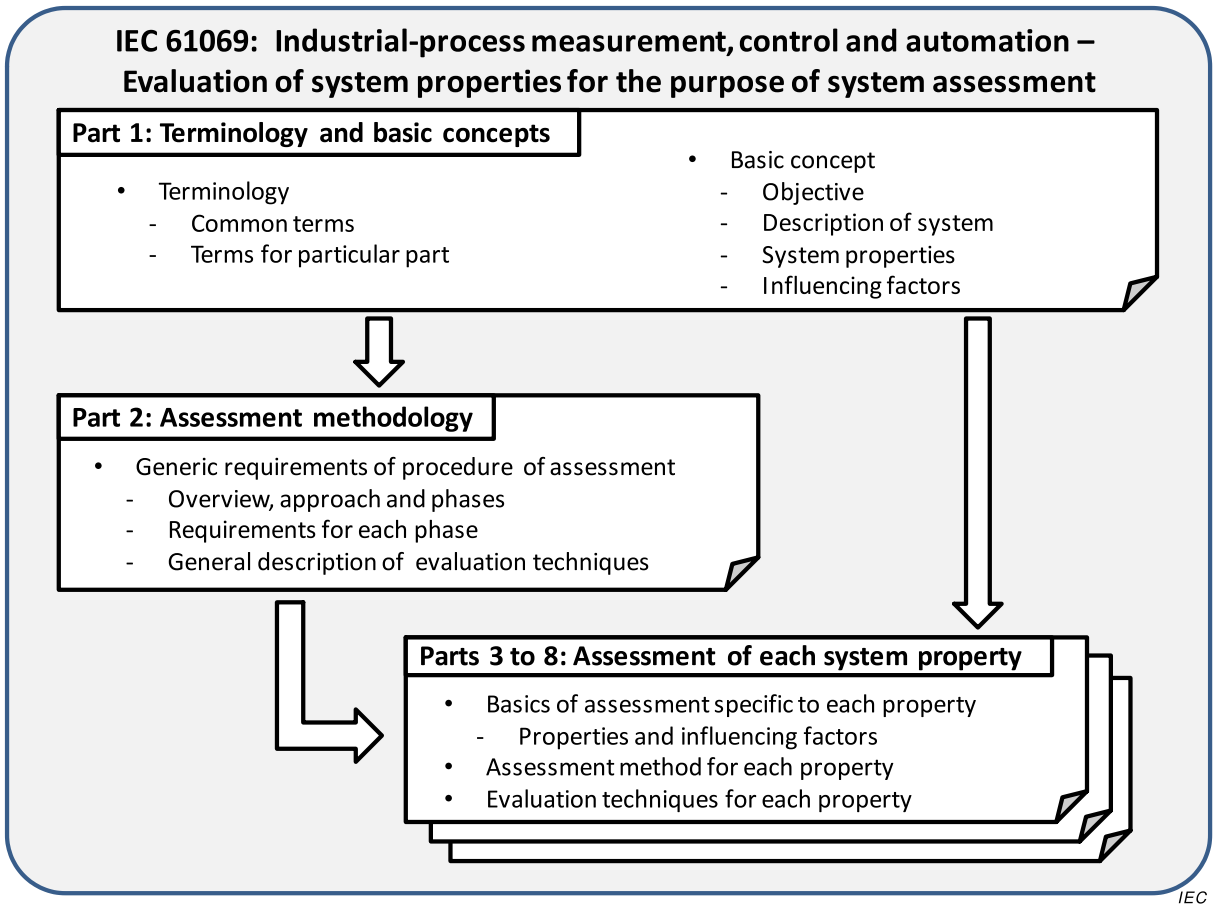

Figure 1 – General layout of IEC 61069

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – EVALUATION OF SYSTEM PROPERTIES FOR THE PURPOSE OF SYSTEM ASSESSMENT –

Part 7: Assessment of system safety

1 Scope

This part of IEC 61069:

– specifies the detailed method of the assessment of system safety of a basic control system (BCS) based on the basic concepts of IEC 61069-1 and methodology of IEC 61069-2,

– defines basic categorization of system safety properties,

– describes the factors that influence system safety and which need to be taken into account when evaluating system safety, and

– provides guidance in selecting techniques from a set of options (with references) for evaluating the system safety.

The treatment of safety in this standard is confined to hazards that can be present within the BCS itself. That is, the BCS itself as a physical entity will not impose a hazard.

Considerations of hazards that can be introduced by the process or equipment under control, of the BCS to be assessed, are excluded.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61069-1:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 1: Terminology and basic concepts*

IEC 61069-2:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

3 Terms, definitions, abbreviated terms, acronyms, conventions and symbols

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61069-1 apply.

3.2 Abbreviated terms, acronyms, conventions and symbols

For the purposes of this document, the abbreviated terms, acronyms, conventions and symbols given in IEC 61069-1 apply.

4 Basis of assessment specific to safety

4.1 System safety properties

4.1.1 General

A system can have a number of interactions with its environment, some of which can impose a hazardous condition.

This standard concentrates on the conditions of the system which can cause harm. It is important to recognize that these conditions can change through the life cycle of the system.

The extent to which the system is free of hazard can be expressed as system safety properties. A system is not always free of hazard even if the individual parts that compose the system are themselves free of hazard; for example, individual parts can be stable whereas the same parts configured to form a system can be unstable and therefore hazardous.

System safety properties of a BCS in all its aspects (mechanical, electrical, etc.) depend upon factors of its design and its dependability.

The assessment of the system safety should include evaluation of system safety properties related to activities and measures for the system during every phase of its life cycle.

Examples of these activities and measures are:

– operating, maintenance and de-commissioning procedures,
– symbols and textual warnings given,
– disposal of packing material, waste products from equipment, replaced components and cleaning material.

The assessment should also include environmental aspects.

The system safety properties can change over the different phases of its life cycle due to the number of hazardous conditions present such as:

– hydraulic accumulators where pressures might be locked in by check valves,
– electrically charged devices (for example capacitors),
– nuclear waste and chemicals stored in containers exposed to corrosion.

When assessing the system safety, the following aspects should be considered:

– kinds of hazards,
– receivers of the consequences of a hazard,
– propagation paths,
– risk reduction measures.

System safety properties are categorized as shown in Figure 2.

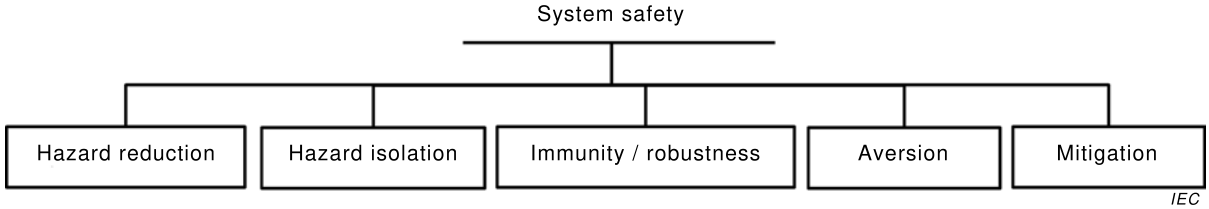

Figure 2 – System safety

System safety cannot be assessed directly and cannot be described by a single property. System safety can only be determined by analysis and testing of each of its properties individually.

4.1.2 Hazard reduction

Hazard reduction is the effort to reduce the number and/or severity of the hazard.

Example: If less energy is used, the temperatures of devices are likely to be lower. The lowest hydraulic pressure needed to transfer the necessary power is used, to avoid high trapped energy.

4.1.3 Hazard isolation

Hazard isolation is the effort to isolate the hazard.

Example: Installing circuit breakers and disconnects inside panels deigned to suppress arc flash.

4.1.4 Immunity / robustness

Immunity / robustness allows the system to absorb or be immune to hazards.

Example: A BCS is immune to power line surges 20 % beyond its operating rating. Or it can absorb EMC interference and still provide proper data transfers.

4.1.5 Aversion

Aversion allows a system to avert a hazard.

Example: Interlocks or SIS capability is provided to ensure the hazard cannot occur.

4.1.6 Mitigation

Mitigation protects only part of the system if other systems are compromised.

Example: Alarms, evacuation are examples where a hazard may have made itself felt, but some method is still provided to make best effort to minimize loss.

4.2 Factors influencing system safety

The system safety can be affected by the influencing factors listed IEC 61069-1:2016, 5.3.

Generally the largest influencing factor is human beings.

4.3 Hazards, harms and propagation paths

4.3.1 Kinds of hazards

4.3.1.1 General

This subclause encompasses a set of hazards.

As a minimum, the kinds of hazards addressed by 4.3.1.2 to 4.3.1.8 shall be considered.

As described in the scope, considerations of hazards that can be introduced by the process or equipment under control, of the BCS to be assessed, are excluded.

4.3.1.2 Mechanical

Weight can be a source of harm, for example during lifting or when falling down.

Pressure can be a source of harm, for example due to breakage of pipes or containers.

Elasticity can be a source of harm, for example due to breakage of springs or mechanical structures.

Vibration can be a source of harm, for example due to fatigue of material or the emission of excessive sound.

Temperature can be a source of harm, for example due to items heating through friction, insufficient cooling, poor/faulty insulation. In certain circumstances extreme cold can also be hazardous by reducing flexibility and affecting human tissue.

Wear can be a source of harm, for example due to release of toxic particles or due to weakening parts.

Mechanical design can be a source of harm, for example due to the incorporation of sharp edges or rough surfaces.

4.3.1.3 Electrical

The voltage or current can be a source of harm, for example due to short-circuiting (heat) or bypassing isolation (electrical shock).

NOTE The electrical energies which are the sources of hazards can originate from within the system and/or from the power supply to the system.

4.3.1.4 Electromagnetic field

The system can emit electromagnetic fields of different intensities and frequencies which can be a source of harm. Emission limits for equipment are given in the relevant product, product family and generic EMC standards, for example CISPR 22. Guidance on the limits for harm to humans can be found, for example, in ENV 50166-1 and ENV 50166-2.

4.3.1.5 Light

The system can emit light of different intensities and frequencies which can be a source of harm; for example, short-circuit or operation of optic emitters (such as laser sources) can produce and propagate light at an intensity that can reach a hazardous level. For laser sources, refer to IEC 60825-1.

4.3.1.6 Radioactivity

A system which includes radioactive elements (such as sensors) can be a source of harm.

4.3.1.7 Biological

A system which includes biological elements (such as sensors) can be a source of harm.

4.3.1.8 Chemical

A system which includes chemical substances can be a source of harm (for example toxicity or corrosion).

4.3.2 Receivers of harms

4.3.2.1 General

The level of harm that can be accepted by a receiver depends on

– the characteristics of the type of receiver and
– the area in which the receiver is located.

Within the environment of a BCS, different areas can be identified such as the control room, manufacturing facility or area surrounding the manufacturing facility. These area classifications are typically given in international, national or proprietary standards. Within each of these areas, individual levels of harm and hazardous situation can be acceptable for each type of receiver.

The different types of receivers are listed in 4.3.2.2 to 4.3.2.4.

4.3.2.2 Human

Hazards which can exist in the BCS can affect the human body in different ways. Some examples are given below:

a) mechanical:
   1) weight can, for example, break bones;
   2) excess pressure can, for example, lead to general injury, the breaking of bones, eye and/or ear damage, or the collapse of the lungs;
   3) elasticity can, for example, lead to general injury or the breaking of bones;
   4) vibration can, for example, lead to ear damage;
   5) temperature can, for example, lead to burns;
b) electrical short circuit or shock can, for example, cause burns, fibrillation of the heart or eye damage;
c) electromagnetic fields can, for example, cause alteration of the metabolism, eye damage or destruction of an organ;
d) light can, for example, cause eye damage or burns;
e) radioactivity can, for example, cause alteration of the metabolism, eye damage or destruction of an organ;
f) biological substances can penetrate and, for example, cause alteration of the metabolism or modification of the alimentary track;
g) chemical substances can penetrate and, for example, cause alteration of the metabolism, eye damage, destruction of an organ, skin irritation or neurological damage.

4.3.2.3 Biological

Hazards which can exist in the BCS can affect biological systems such as flora, fauna and the ecological system, in similar ways as described in 4.3.2.2. The degree of the physical injury to a biological system can be different from that to a human.

4.3.2.4 Equipment

Hazards which can exist in the BCS can affect surrounding equipment in different ways. Some examples are given below:

a) mechanical:
   1) weight, pressure, elasticity can, depending on the severity, result in misalignment, bending or breaking parts, etc.;

2) vibration can, depending on the severity, result in misalignment, metal fatigue, parts coming loose, etc.;
3) temperature can, depending on its level, result in misalignment, decreased life time, loss of mechanical strength, degasification, burning, etc.;

b) electrical sources can, depending on the severity, result in supply power distortion, breakdown due to overload, current surges, flashover, burns, etc.;
c) electromagnetic fields can, depending on the severity, result in electromagnetic interference, alteration of data, etc.;
d) light or radioactivity can, depending on the level, result in changes of material properties due to ultra-violet or laser-light, etc.;
e) biological: no effect foreseen;
f) chemical substances can, depending on the severity, result in chemical transformation of material, etc.

4.3.3 Propagation paths

4.3.3.1 General

For a hazard to be harmful, there is a propagation path between the source of harm and the receiver.

Although single propagation paths can be identified, it is very often the case that a complete propagation path is a combination of several single types of propagation paths.

Some single propagation paths are listed in 4.3.3.2 to 4.3.3.5.

4.3.3.2 Direct propagation path

A direct propagation path means that the receiver is in direct contact with the source of harm (for example a finger touching a high-voltage conductor).

4.3.3.3 Indirect propagation path

An indirect propagation path means that the receiver is in contact with the source of harm via any movable item (for example a tool or a ladder) or a fixed construction element (for example supports or rails).

4.3.3.4 Dynamic propagation path

A dynamic propagation path means that the receiver is in time-dependent contact with the source of harm via any dynamic media (for example flowing liquids or gases).

4.3.3.5 Contact-less propagation path

A contact-less propagation path means that the receiver is exposed to the source of harm via, for example, radiations, light or electromagnetic fields.

5 Assessment method

5.1 General

The assessment shall follow the method as laid down in IEC 61069-2:2016, Clause 5.

5.2 Defining the objective of the assessment

Defining the objective of the assessment shall follow the method as laid down in IEC 61069-2:2016, 5.2.

5.3 Design and layout of the assessment

Design and layout of the assessment shall follow the method as laid down in IEC 61069-2:2016, 5.3.

Defining the scope of assessment shall follow the method laid down in IEC 61069-2:2016, 5.3.1.

Collation of documented information shall be conducted in accordance with IEC 61069-2:2016, 5.3.3.

The statements compiled in accordance with IEC 61069-2:2016, 5.3.3 should include the following in addition to the items listed in IEC 61069-2:2016, 5.3.3:

– kinds of hazards and their propagation paths from the system to its environment;
– influencing factors that can create a hazardous condition inside the system;
– risk reduction measures provided to minimize the consequences of hazardous conditions;
– risk reduction measures provided to minimize the probability that a conjunction of phenomena which can create hazardous conditions can arise;
– way in which the different system modules and elements interact and the possibility that a lack of safety can arise at the system level as a result of the interactions;
– global pre-knowledge available and extent to which the system safety property should be assessed.

Documenting collated information shall follow the method in IEC 61069-2:2016, 5.3.4.

Selecting assessment items shall follow IEC 61069-2:2016, 5.3.5.

Assessment specification should be developed in accordance with IEC 61069-2: 2016, 5.3.6.

Comparison of the SRD and the SSD shall follow IEC 61069-2:2016, 5.3.

NOTE 1 A checklist of SRD for system dependability is provided in Annex A.

NOTE 2 A checklist of SSD for system dependability is provided in Annex B.

5.4 Planning of the assessment program

Planning of the assessment program shall follow the method as laid down IEC 61069-2:2016, 5.4.

Assessment activities shall be developed in accordance with IEC 61069-2:2016, 5.4.2.

The final assessment program should specify points specified in IEC 61069-2:2016, 5.4.3.

5.5 Execution of the assessment

The execution of the assessment shall be in accordance with IEC 61069-2:2016, 5.5.

5.6 Reporting of the assessment

The reporting of the assessment shall be in accordance with IEC 61069-2:2016, 5.6.

The report shall include information specified in IEC 61069-2:2016, 5.6. Additionally, the assessment report should address the following points:

– no additional items are noted.

6 Evaluation techniques

6.1 General

Within this standard, several evaluation techniques are suggested. Other methods may be applied but, in all cases, the assessment report should provide references to documents describing the techniques used.

Those evaluation techniques are categorized as described in IEC 61069-2:2016, Clause 6.

Factors influencing the system safety according to 4.2 shall be taken into account.

The techniques given in 6.2, 6.3 and 6.4 are recommended to assess system safety.

It is not possible to evaluate the system safety properties as one entity. Instead each system safety properties should be addressed separately.

6.2 Analytical evaluation techniques

Safety evaluation techniques for BCSs are mainly analytical.

For each kind of hazard, the following steps should be taken:

– check whether a hazard is present and, for each hazard present, check if certifications are available and are also valid under the operating conditions stated in the SRD or by mandatory regulations;
– if satisfactory certifications are not available, an appropriate risk analysis should be applied, for example the analysis described in ISO 31010. In support of such an analysis, one of the evaluation techniques of 6.3 can be applied.

6.3 Empirical evaluation techniques

Empirical evaluation techniques are supplementary to analytical ones.

Whenever analytical techniques cannot guarantee the safety level of the system, an empirical evaluation should be carried out in order to assess those aspects on which there is a lack of data.

An empirical evaluation shall always be carried out when required by regulatory bodies (refer also to IEC 61069-2:2016, 5.3.5).

For this purpose, a number of techniques can be applied of which the following are listed for guidance:

– mechanical: testing methods of enclosures as described, for example, in IEC 60529;
– electrical: insulation coordination and electric strength testing as described, for example, in the IEC 60243 series and IEC 60664-1;
– electromagnetic fields: measurement techniques as described, for example, in CISPR 22;
– thermal: fire hazard testing as described, for example, in IEC 60695-2, IEC 60695-11-10 and IEC 60695-11-20.

6.4 Additional topics for evaluation techniques

No additional items are noted.

Annex A
(informative)

Check list and/or example of SRD for system functionality

The system requirement document should be reviewed to check that the risk reduction measures required for the system have been addressed and are listed as described in IEC 61069-2.

The effectiveness of the safety assessment is strongly dependent upon the comprehensiveness of the statement of requirements.

Particular attention should be given to checking that adequate information is given on:

– the applicable international, national or company safety standards or regulations and, in particular, IEC 60664-1 and IEC 61010-1,

– the admissible emission levels for the kinds of hazards listed in 4.2,

– the areas where the BCS and its modules and elements are to be situated, referring to area classification standards, for example,

– the working conditions within these areas which should be fulfilled to allow access to the BCS, and the procedures to obtain work permits,

– the permitted infringements of these working conditions, their frequency and the emergency procedures to be followed in this case,

– the admissible emission levels for the kinds of hazards listed in 4.2 for the neighbouring areas of the BCS,

– the extent to which the BCS is intended to be used to provide safety functions outside of the scope of the IEC 61508 series.

Annex B
(informative)

Checklist and/or example of SSD for system functionality

B.1 SSD information

The system specification document should be reviewed to check that the properties given in the SRD are listed as described in IEC 61069-2:2016, Clause B.2.

B.2 Check points for system safety

The system specification document should be reviewed to check that the risk reduction measures of the BCS are listed as described in IEC 61069-2.

Particular attention should be given to checking that adequate information is given on the following:

– kinds of hazard within the BCS, and the risk reduction measures taken to limit the possible consequences;

– levels of emissions, even if they are lower than the safe and/or allowed limits;

– appropriate safety certifications, issuing institutions and consistency with national regulations;

– any maintenance action required which can infringe the system safety and the precautions to be taken in these circumstances, to avoid any hazardous conditions;

– special installation requirements to guarantee the system safety.

Bibliography

IEC 60243 (all parts), *Electric strength of insulating materials – Test methods*

IEC 60529, *Degrees of protection provided by enclosures (IP Code)*

IEC 60695-2 (all parts), *Fire hazard testing – Part 2: Test methods*

IEC 60664-1, *Insulation coordination for equipment within low-voltage systems – Part 1: Principles, requirements and tests*

IEC 60695-11-10, *Fire hazard testing – Part 11-10: Test flames – 50 W horizontal and vertical flame test methods*

IEC 60695-11-20, *Fire hazard testing – Part 11-20: Test flames – 500 W flame test method*

IEC 60825-1, *Safety of laser products – Part 1: Equipment classification and requirements*

IEC 61010-1:2010, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 1: General requirements*

IEC 61069-3, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 3: Assessment of system functionality*

IEC 61069-4, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 4: Assessment of system performance*

IEC 61069-5:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 5: Assessment of system dependability*

IEC 61069-6:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 6: Assessment of system operability*

IEC 61069-8, *Industrial process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 8: Assessment of other system properties*

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

IEC TS 62603-1, *Industrial process control systems – Guideline for evaluating process control systems – Part 1: Specifications*

CISPR 22, *Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement*

ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

ISO 31010:2009, *Risk management – Risk assessment techniques*

ENV 50166-1, *Human exposure to electromagnetic fields. Low-frequency (0 Hz to 10 kHz)*

ENV 50166-2, *Human exposure to electromagnetic fields. High-frequency (10 kHz to 300 GHz)*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

MESURE, COMMANDE ET AUTOMATION DANS LES PROCESSUS INDUSTRIELS – APPRÉCIATION DES PROPRIÉTÉS D'UN SYSTÈME EN VUE DE SON ÉVALUATION –

Partie 7: Évaluation de la sécurité d'un système

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 61069-7 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition parue en 1999. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) réorganisation des informations contenues dans l'IEC 61069-7:1999 visant à mieux organiser l'ensemble complet de normes et à le rendre plus cohérent;

b) l'IEC TS 62603-1 a été incorporée dans cette édition.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/795/FDIS	65A/805/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.

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

Une liste de toutes les parties de la série IEC 61069, publiées sous le titre général *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation,* peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

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

L'IEC 61069 traite de la méthode qu'il convient d'utiliser pour évaluer les propriétés système d'un système de commande de base (BCS, Basic Control System). L'IEC 61069 comprend les parties suivantes.

Partie 1: Terminologie et principes de base

Partie 2: Méthodologie à appliquer pour l'évaluation

Partie 3: Evaluation de la fonctionnalité d'un système

Partie 4: Evaluation des caractéristiques de fonctionnement d'un système

Partie 5: Evaluation de la sûreté de fonctionnement d'un système

Partie 6: Evaluation de l'opérabilité d'un système

Partie 7: Evaluation de la sécurité d'un système

Partie 8: Evaluation des autres propriétés d'un système

Evaluer un système consiste à juger, sur la base d'éléments concrets, de sa bonne aptitude à remplir une mission ou un ensemble de missions spécifiques.

Pour obtenir tous les éléments nécessaires, il faudrait procéder à une appréciation complète (par exemple selon tous les facteurs d'influence) de toutes les propriétés du système qui contribuent à remplir la mission ou l'ensemble de missions spécifiques considérées.

Cela étant rarement réalisable dans la pratique, il convient que la démarche d'évaluation d'un système consiste à:

– identifier l'importance de chacune des propriétés concernées du système;
– planifier l'appréciation des propriétés concernées du système avec un effort adéquat en termes de coût pour les différentes propriétés du système.

Lors de l'évaluation d'un système, il est essentiel de garder à l'esprit le besoin d'obtenir une augmentation maximale de la confiance dans la bonne aptitude à l'emploi du système, compte tenu des contraintes pratiques de coût et de temps.

Une évaluation ne peut être entreprise que si une mission a été imposée (ou attribuée) ou si une mission type peut être définie. En l'absence de mission, il n'est pas possible d'évaluer le système; toutefois, il est toujours possible de spécifier et de réaliser des appréciations, qui pourront servir lors d'évaluations menées par d'autres. Dans ce cas, l'IEC 61069 peut être utilisée en tant que guide pour planifier une appréciation et ses méthodes peuvent servir à effectuer les appréciations; l'appréciation des propriétés d'un système fait, en effet, partie intégrante de l'évaluation de ce système.

La préparation de l'évaluation peut révéler que la définition du système est trop restreinte. Par exemple, pour une installation dont les systèmes de commande partageant des ressources ont fait l'objet d'au moins deux révisions, comme un réseau, il convient de tenir compte des problèmes liés à la coexistence et à l'interopérabilité. Dans ce cas, il convient de ne pas restreindre le système à examiner au «nouveau» BCS, mais d'inclure les deux. C'est-à-dire qu'il convient de modifier les limites du système et d'y inclure suffisamment de l'autre système pour que ces questions soient prises en compte.

La structure de la série ainsi que la relation entre les Parties de l'IEC 61069 sont représentées à la Figure 1.

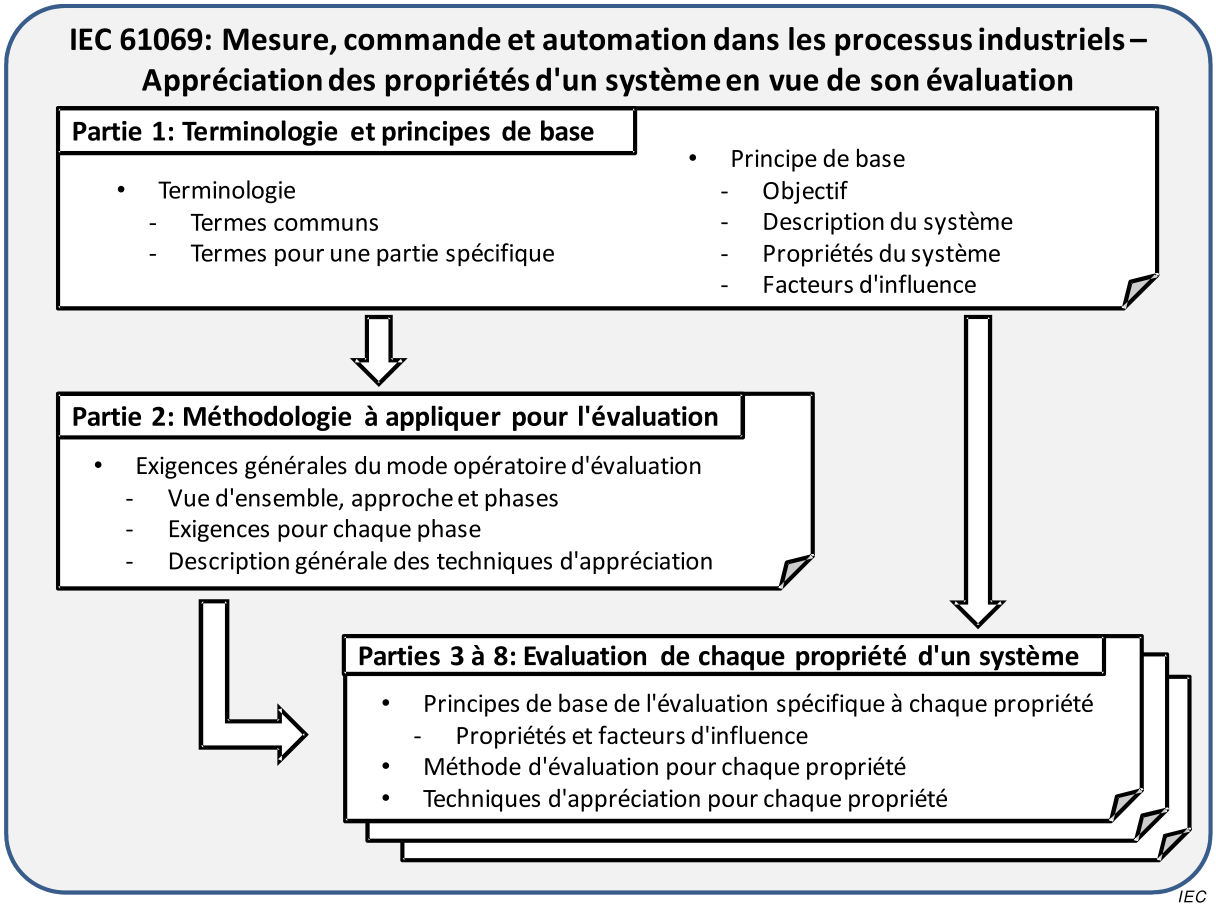

Figure 1 – Structure générale de l'IEC 61069

MESURE, COMMANDE ET AUTOMATION DANS LES PROCESSUS INDUSTRIELS – APPRÉCIATION DES PROPRIÉTÉS D'UN SYSTÈME EN VUE DE SON ÉVALUATION –

Partie 7: Évaluation de la sécurité d'un système

1 Domaine d'application

La présente partie de l'IEC 61069:

– spécifie la méthode d'évaluation détaillée de la sécurité d'un système faisant partie d'un système de commande de base (BCS) qui repose sur les principes de base de l'IEC 61069-1 et la méthodologie de l'IEC 61069-2;

– définit la classification de base de la sécurité d'un système;

– décrit les facteurs ayant une influence sur la sécurité d'un système et dont il faut tenir compte lors de l'appréciation de la sécurité d'un système; et

– donne des lignes directrices concernant les techniques de sélection à partir d'un ensemble d'options (avec références) pour l'appréciation de la sécurité d'un système.

L'étude de la sécurité dans la présente norme se limite aux dangers pouvant se présenter dans le BCS à proprement parler. C'est-à-dire, l'aptitude du BCS, en tant qu'entité physique, à éviter de faire apparaître un danger.

L'étude des dangers pouvant être introduits par le processus ou l'équipement commandé par le BCS faisant l'objet de l'évaluation est exclue.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 61069-1:2016, *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 1: Terminologie et principes de base*

IEC 61069-2:2016, *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 2: Méthodologie à appliquer pour l'évaluation*

3 Termes, définitions, abréviations, acronymes, conventions et symboles

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'IEC 61069-1 s'appliquent.

3.2 Abréviations, acronymes, conventions et symboles

Pour les besoins du présent document, les abréviations, acronymes, conventions et symboles donnés dans l'IEC 61069-1 s'appliquent.

4 Principes de base de l'évaluation spécifique à la sécurité

4.1 Propriétés de la sécurité d'un système

4.1.1 Généralités

Un système peut avoir diverses interactions avec son environnement, certaines de ces interactions pouvant présenter des dangers.

La présente norme est consacrée aux situations du système pouvant faire du mal. Il est essentiel de reconnaître que ces situations peuvent varier au cours du cycle de vie du système.

L'aptitude du système à ne présenter aucun danger désigne les propriétés de sécurité du système. Un système peut présenter un danger même si chacun des éléments qui le composent ne présente pas de dangers individuellement. Par exemple, chaque élément peut être stable alors que ces mêmes éléments assemblés pour former un système peuvent être instables et, par conséquent, présenter des dangers.

Les propriétés de sécurité d'un BCS dépendent, sous tous leurs aspects (mécanique, électrique, etc.), de facteurs tels que la sécurité inhérente à sa conception et à sa sûreté de fonctionnement.

Il convient que l'évaluation de la sécurité d'un système comprenne l'appréciation des propriétés de sécurité du système relatives aux activités et aux mesures du système durant chaque phase de son cycle de vie.

Exemples de ces activités et de ces mesures:

– modes opératoires d'exploitation, de maintenance et de mise hors service;
– symboles et avertissements textuels formulés;
– mise au rebut des matériaux d'emballage, des déchets provenant des équipements, des composants remplacés et des matériaux de nettoyage.

Il convient que l'évaluation comprenne également les aspects environnementaux.

Les propriétés de sécurité d'un système peuvent évoluer au cours des différentes phases de son cycle de vie, en raison du nombre de situations de danger présentes telles que:

– blocage des pressions au niveau des accumulateurs hydrauliques du fait des clapets antiretour;
– charge électrique des composants (par exemple condensateurs);
– exposition à la corrosion des conteneurs de déchets nucléaires et produits chimiques.

Lors de l'évaluation de la sécurité du système, il convient d'étudier les aspects suivants:

– types de dangers;
– récepteurs des conséquences d'un danger;
– chemins de propagation;
– mesures de réduction du risque.

La classification des propriétés de sécurité d'un système est indiquée dans la Figure 2.

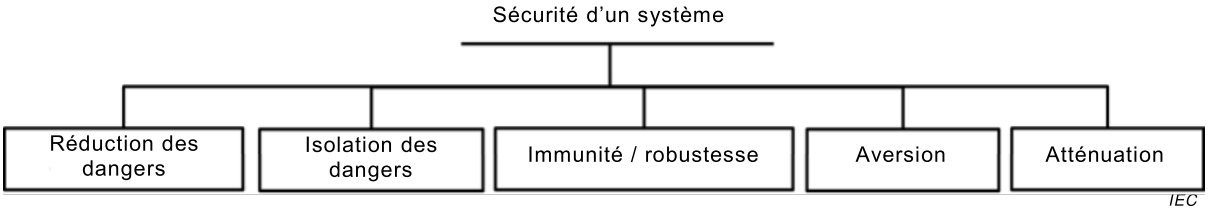

Figure 2 – Sécurité du système

La sécurité d'un système ne peut pas être évaluée directement et ne peut pas être décrite par une seule propriété. La sécurité d'un système ne peut être déterminée que par des activités individuelles d'analyse et d'essai de chacune de ses propriétés.

4.1.2 Réduction des dangers

La réduction des dangers est la démarche entreprise pour diminuer le nombre et/ou la sévérité des dangers.

Exemple: lorsque la consommation d'énergie est moindre, les températures des appareils sont susceptibles de diminuer. La plus faible pression hydraulique nécessaire au transfert de courant est utilisée pour éviter une retenue trop importante de l'énergie.

4.1.3 Isolation des dangers

L'isolation des dangers est la démarche entreprise pour isoler les dangers.

Exemple: installer des disjoncteurs et des appareils de sectionnement dans les panneaux, conçus pour éliminer les arcs électriques.

4.1.4 Immunité / robustesse

L'immunité / robustesse permet au système d'absorber ou d'être immunisé contre les dangers.

Exemple: Un BCS est protégé contre les surtensions des lignes électriques de 20 % au-delà de sa plage de fonctionnement. Ou bien il peut absorber les interférences électromagnétiques et continuer à assurer des transferts de données corrects.

4.1.5 Aversion

L'aversion permet à un système d'éviter un danger.

Exemple: mise en place de verrouillages ou d'une capacité de système instrumenté de sécurité (SIS) permettant de garantir que le danger ne peut pas apparaître.

4.1.6 Atténuation

L'atténuation protège uniquement une partie du système lorsque d'autres systèmes sont compromis.

Exemple: les alarmes et l'évacuation illustrent les cas dans lesquels un danger peut être ressenti mais où il existe certaines méthodes permettant de réduire les pertes au maximum.

4.2 Facteurs ayant une influence sur la sécurité d'un système

La sécurité d'un système peut être affectée par les facteurs d'influence énumérés en 5.3 de l'IEC 61069-1:2016.

Le facteur d'influence le plus important est généralement le facteur humain.

4.3 Dangers, dommages et chemins de propagation

4.3.1 Types de dangers

4.3.1.1 Généralités

Le présent paragraphe englobe un ensemble de dangers.

Au minimum, les types de dangers traités de 4.3.1.2 à 4.3.1.8 doivent être pris en compte.

Comme l'indique le domaine d'application, l'étude des dangers pouvant être introduits par le processus ou l'équipement commandé par le BCS faisant l'objet de l'évaluation est exclue.

4.3.1.2 Dangers mécaniques

Le poids peut être une source de dommage, par exemple pendant les opérations de levage ou en cas de chute.

La pression peut constituer une source de dommage, par exemple en cas de rupture de tuyauteries ou de conteneurs.

L'élasticité peut constituer une source de dommage, par exemple en cas de rupture de ressorts ou de structures mécaniques.

Les vibrations peuvent constituer une source de dommage, par exemple en cas de fatigue de matériaux ou d'émission de bruit excessif.

La température peut représenter une source de dommage, par exemple en cas d'échauffement des éléments causé par la friction, de refroidissement insuffisant, d'isolation inadaptée/défectueuse. Certaines conditions de froid extrême peuvent faire apparaître un danger de réduction de la souplesse des matériaux et d'affectation des tissus humains.

L'usure peut constituer une source de dommage, par exemple en cas de libération de particules toxiques ou en cas de pièces défaillantes.

La conception mécanique peut être une source de dommage, par exemple en cas d'incorporation d'arêtes vives ou de surfaces brutes.

4.3.1.3 Dangers électriques

La tension ou le courant peuvent constituer une source de dommage, par exemple en cas de court-circuit (chaleur) ou de contournement de l'isolation (choc électrique).

NOTE Les énergies électriques constituant les sources de dangers peuvent provenir de l'intérieur du système et/ou de l'alimentation du système.

4.3.1.4 Dangers induits par les champs électromagnétiques

Le système peut émettre des champs électromagnétiques de différents niveaux d'intensité et de fréquence pouvant constituer une source de dommage. Les limites d'émission pour les équipements figurent dans les normes de CEM de produits, de familles de produits, et les normes CEM génériques appropriées, par exemple la CISPR 22. Des documents d'orientation sur les limites au-delà desquelles un dommage humain peut apparaître peuvent être consultés, par exemple dans l'ENV 50166-1 et l'ENV 50166-2.

4.3.1.5 Dangers induits par les ondes lumineuses

Le système peut émettre des ondes lumineuses de différents niveaux d'intensité et de fréquence pouvant constituer une source de dommage; par exemple un court-circuit ou le fonctionnement d'émetteurs optiques (tels que des sources laser) peut générer et propager une onde lumineuse d'une intensité pouvant atteindre un niveau dangereux. En ce qui concerne les sources laser, consulter l'IEC 60825-1.

4.3.1.6 Dangers induits par la radioactivité

Un système qui comporte des éléments radioactifs (tels que des capteurs) peut constituer une source de dommage.

4.3.1.7 Dangers biologiques

Un système qui comporte des éléments biologiques (tels que des capteurs) peut constituer une source de dommage.

4.3.1.8 Dangers chimiques

Un système qui comporte des substances chimiques peut constituer une source de dommage (toxicité ou corrosion, par exemple).

4.3.2 Récepteurs de dommages

4.3.2.1 Généralités

Le niveau de dommage pouvant être accepté par un récepteur est fonction:

– des caractéristiques du type de récepteur;
– de la zone dans laquelle se trouve le récepteur.

Différentes zones peuvent être distinguées dans l'environnement d'un BCS, telles que la salle de commande, l'installation de fabrication ou la zone entourant l'installation de fabrication. Ces classifications de zones sont généralement décrites dans des Normes internationales, nationales ou propriétaires. Dans chacune de ces zones, différents niveaux de dommages et de situations dangereuses peuvent être acceptables pour chaque type de récepteur.

Les différents types de récepteurs sont répertoriés en 4.3.2.2 à 4.3.2.4.

4.3.2.2 Homme

Les dangers susceptibles d'exister dans les BCS peuvent nuire au corps humain de différentes façons. Quelques exemples sont donnés ci-dessous:

a) dangers mécaniques:
   1) le poids peut, par exemple, fracturer des os;
   2) une pression excessive peut, par exemple, entraîner des blessures générales, la fracture d'os, des troubles de la vue et/ou de l'audition, ou le collapsus des poumons;
   3) l'élasticité peut, par exemple, entraîner des blessures générales ou la fracture d'os;
   4) les vibrations peuvent, par exemple, entraîner des troubles de l'audition;
   5) la température peut, par exemple, entraîner des brûlures;
b) les courts-circuits et les chocs électriques peuvent, par exemple, causer des brûlures, la fibrillation du cœur ou des troubles de la vue;
c) les champs électromagnétiques peuvent, par exemple, entraîner une altération du métabolisme, des troubles de la vue ou la destruction d'organes;

d) les ondes lumineuses peuvent, par exemple, entraîner des troubles de la vue ou des brûlures;

e) la radioactivité peut, par exemple, entraîner une altération du métabolisme, des troubles de la vue ou la destruction d'organes;

f) les substances biologiques peuvent pénétrer et, par exemple, entraîner une altération du métabolisme ou la modification de la chaîne alimentaire;

g) les substances chimiques peuvent pénétrer et, par exemple, entraîner une altération du métabolisme, des troubles de la vue, la destruction d'organes, une irritation de la peau ou des troubles neurologiques.

4.3.2.3 Dangers biologiques

Les dangers susceptibles d'exister dans les BCS peuvent affecter les systèmes biologiques tels que la flore, la faune et le système écologique, de manière similaire à ce qui est décrit en 4.3.2.2. La gravité des dommages physiques causés à un système biologique peut différer de celle des dommages causés aux humains.

4.3.2.4 Les équipements

Les dangers susceptibles d'exister dans les BCS peuvent nuire aux équipements environnants de différentes façons. Quelques exemples sont donnés ci-dessous:

a) dangers mécaniques:

   1) le poids, la pression, l'élasticité peuvent, selon leur importance, avoir pour résultat un défaut d'alignement, la courbure ou la rupture de pièces, etc.;

   2) les vibrations peuvent, selon leur importance, avoir pour résultat un défaut d'alignement, une fatigue du métal, une désolidarisation des pièces, etc.;

   3) la température peut, selon son niveau, avoir pour résultat un défaut d'alignement, une baisse de la durée de vie opérationnelle, une diminution de la tenue mécanique, le dégazage, des brûlures, etc.;

b) les sources électriques peuvent, selon leur importance, entraîner une distorsion de l'alimentation électrique, un claquage dû à une surcharge, des surintensités, un amorçage, des brûlures, etc.;

c) les champs électromagnétiques peuvent, selon leur importance, entraîner des interférences électromagnétiques, une altération des données, etc.;

d) les ondes lumineuses ou la radioactivité peuvent, selon leur importance, entraîner une modification des propriétés des matériaux due aux rayons ultraviolets ou aux rayons laser, etc.;

e) danger biologique: aucun effet prévu;

f) les substances chimiques peuvent, selon leur importance, entraîner une transformation chimique des matériaux, etc.

4.3.3 Chemins de propagation

4.3.3.1 Généralités

Pour qu'un danger soit dommageable, il doit exister un chemin de propagation entre la source du danger et le récepteur.

Bien qu'il soit possible d'identifier des chemins de propagation élémentaires, il arrive souvent qu'un chemin de propagation soit la combinaison de plusieurs types de chemins de propagation élémentaires.

Certains chemins de propagation élémentaires sont répertoriés en 4.3.3.2 à 4.3.3.5.

4.3.3.2 Chemin de propagation direct

Par chemin de propagation «direct», on entend que le récepteur est en contact direct avec la source de dommage (par exemple un doigt qui touche un conducteur sous haute tension).

4.3.3.3 Chemin de propagation indirect

Par chemin de propagation «indirect», on entend que le récepteur est en contact avec la source de dommage par l'intermédiaire d'un élément mobile (par exemple un outil ou une échelle) ou d'un élément de construction fixe (par exemple des montants ou des rails).

4.3.3.4 Chemin de propagation dynamique

Par chemin de propagation «dynamique», on entend que le récepteur est en contact intermittent (variable dans le temps) avec la source de dommage par l'intermédiaire d'un milieu dynamique (par exemple un liquide ou un gaz).

4.3.3.5 Chemin de propagation sans contact

Par chemin de propagation «sans contact», on entend que le récepteur est exposé à la source de dommage par l'intermédiaire, par exemple, de rayonnements, d'ondes lumineuses ou de champs électromagnétiques.

5 Méthode d'évaluation

5.1 Généralités

L'évaluation doit être effectuée selon la méthode décrite à l'Article 5 de l'IEC 61069-2:2016.

5.2 Définition de l'objectif de l'évaluation

La définition de l'objectif de l'évaluation doit être effectuée selon la méthode décrite en 5.2 de l'IEC 61069-2:2016.

5.3 Conception et agencement de l'évaluation

La conception et l'agencement de l'évaluation doivent être effectués selon la méthode décrite en 5.3 de l'IEC 61069-2:2016.

La définition du domaine d'application de l'évaluation doit être effectuée selon la méthode décrite en 5.3.1 de l'IEC 61069-2:2016.

Le classement des informations détaillées doit être effectué conformément à ce qui est spécifié en 5.3.3 de l'IEC 61069-2:2016.

Il convient que les rapports établis conformément à ce qui est spécifié en 5.3.3 de l'IEC 61069-2:2016 incluent les éléments suivants, en plus de ceux énumérés en 5.3.3 de l'IEC 61069-2:2016:

– types de dangers et chemins de propagation entre le système et son environnement;
– facteurs d'influence pouvant entraîner une situation dangereuse à l'intérieur du système;
– mesures visant à réduire le risque mises en œuvre pour minimiser les conséquences de situations dangereuses;
– mesures visant à réduire le risque mises en œuvre pour minimiser la probabilité d'apparition d'une conjonction de phénomènes pouvant entraîner des situations dangereuses;

– manière dont les différents éléments et modules du système interagissent, et l'apparition possible d'un manque de sécurité au sein du système dû à de telles interactions;
– ensemble des connaissances préalables disponibles et mesure dans laquelle il convient que la propriété de sécurité d'un système soit évaluée.

La mise en forme des informations recueillies doit être effectuée selon la méthode décrite en 5.3.4 de l'IEC 61069-2:2016.

La sélection des éléments d'évaluation doit être effectuée selon la méthode indiquée en 5.3.5 de l'IEC 61069-2:2016.

Il convient que les spécifications de l'évaluation soient développées conformément à ce qui est spécifié en 5.3.6 de l'IEC 61069-2:2016.

La comparaison du cahier des charges du système (CdC) et du cahier des spécifications du système (CdS) doit être effectuée selon la méthode indiquée en 5.3 de l'IEC 61069-2:2016.

NOTE 1 Une liste de contrôle du CdC destinée à la sûreté de fonctionnement d'un système est donnée à l'Annexe A.

NOTE 2 Une liste de contrôle du CdS destinée à la sûreté de fonctionnement d'un système est donnée à l'Annexe B.

5.4 Planification du programme d'évaluation

La planification du programme d'évaluation doit être effectuée selon la méthode décrite en 5.4 de l'IEC 61069-2:2016.

Les activités d'évaluation doivent être développées conformément à ce qui est spécifié en 5.4.2 de l'IEC 61069-2:2016.

Il convient que le programme définitif d'évaluation précise les points spécifiés en 5.4.3 de l'IEC 61069-2:2016.

5.5 Exécution de l'évaluation

L'exécution de l'évaluation doit être conforme à ce qui est spécifié en 5.5 de l'IEC 61069-2:2016.

5.6 Rédaction du rapport d'évaluation

La rédaction du rapport d'évaluation doit être conforme à ce qui est spécifié en 5.6 de l'IEC 61069-2:2016.

Le rapport doit contenir les informations spécifiées en 5.6 de l'IEC 61069-2:2016. De plus, il convient que le rapport d'évaluation aborde également les points suivants:

– aucun élément supplémentaire n'est indiqué.

6 Techniques d'appréciation

6.1 Généralités

Plusieurs techniques d'appréciation sont suggérées dans le cadre de la présente norme. D'autres méthodes peuvent être appliquées mais, dans tous les cas, il convient que le rapport d'évaluation fasse référence aux documents qui décrivent les techniques utilisées.

Ces techniques d'appréciation sont classées conformément à l'Article 6 de l'IEC 61069-2:2016.

Les facteurs ayant une influence sur la sécurité d'un système, comme indiqué en 4.2, doivent être pris en compte.

Les techniques décrites en 6.2, 6.3 et 6.4 sont recommandées pour évaluer la sécurité d'un système.

Il n'est pas possible d'apprécier les propriétés de sécurité d'un système en tant qu'entité unique. Il convient plutôt d'étudier séparément chaque propriété de sécurité d'un système.

6.2 Techniques d'appréciation analytique

Les techniques d'appréciation de la sécurité des BCS sont essentiellement analytiques.

Pour chaque type de danger, il convient de prendre les mesures suivantes:

– vérifier si un danger est présent et, pour chaque danger présent, vérifier si des certifications sont disponibles et si elles sont également valables dans les conditions de fonctionnement décrites dans le CdS ou par les réglementations obligatoires;
– si des certifications satisfaisantes ne sont pas disponibles, il convient de réaliser une analyse de risque appropriée, par exemple celle décrite dans l'ISO 31010. Pour étayer une telle analyse, l'une des techniques d'appréciation figurant en 6.3 peut être appliquée.

6.3 Techniques d'appréciation empirique

Les techniques d'appréciation empirique peuvent être utilisées en complément des techniques analytiques.

Dans tous les cas où les techniques analytiques ne peuvent garantir le niveau de sécurité du système, il convient qu'une appréciation empirique soit effectuée afin d'évaluer les aspects particuliers pour lesquels il manque des données.

Une appréciation empirique doit être réalisée systématiquement, lorsqu'elle est requise par les organismes de réglementation (voir aussi 5.3.5 de l'IEC 61069-2:2016).

A cet effet, un certain nombre de techniques peuvent être appliquées, parmi lesquelles les suivantes, citées en tant que lignes directrices:

– mécanique: méthodes d'essai concernant les enveloppes comme décrit, par exemple, dans l'IEC 60529;
– électrique: coordination de l'isolement et essais de rigidité diélectrique comme décrit, par exemple, dans la série IEC 60243 et dans l'IEC 60664-1;
– champs électromagnétiques: techniques de mesure comme décrit, par exemple, dans la CISPR 22;
– thermique: essais relatifs aux dangers du feu comme décrit, par exemple, dans l'IEC 60695-2, l'IEC 60695-11-10 et l'IEC 60695-11-20.

6.4 Sujets supplémentaires de techniques d'appréciation

Aucun élément supplémentaire n'est indiqué.

Annexe A
(informative)

Liste de contrôle et/ou exemple de CdC pour la fonctionnalité d'un système

Il convient d'effectuer une revue du cahier des charges du système afin de s'assurer que les mesures visant à réduire le risque, exigées pour le système, ont été prévues et y sont détaillées conformément à l'IEC 61069-2.

L'efficacité de l'évaluation de la sécurité dépend beaucoup de la clarté avec laquelle sont exprimées les exigences et de leur exhaustivité.

Il convient de prêter une attention particulière pour vérifier que des informations appropriées sont fournies sur:

– les normes ou réglementations de sécurité en vigueur au niveau national ou international, ou au niveau des sociétés et, tout particulièrement, l'IEC 60664-1 et l'IEC 61010-1;
– les niveaux d'émission autorisés pour les catégories de dangers énumérées en 4.2;
– les zones où doivent être installés le BCS ainsi que ses modules et éléments, en se référant, par exemple, aux normes de classement des zones;
– les conditions de travail qu'il convient de respecter, dans ces zones, pour accéder au BCS, ainsi que les modes opératoires nécessaires à l'obtention des permis de travail;
– les transgressions autorisées de ces conditions de travail, leur fréquence et les modes opératoires d'urgence à suivre, le cas échéant;
– les niveaux d'émission autorisés pour les catégories de dangers énumérées en 4.2 et concernant les zones avoisinant le BCS;
– la mesure dans laquelle le BCS est destiné à être utilisé pour fournir des fonctions de sécurité en dehors du domaine d'application de la série IEC 61508.

Annexe B
(informative)

Liste de contrôle et/ou exemple de CdS pour la fonctionnalité d'un système

B.1 Informations relatives au CdS

Il convient d'effectuer une revue du cahier des spécifications du système afin de s'assurer que les propriétés mentionnées dans le CdC sont détaillées conformément à l'Article B.2 de l'IEC 61069-2:2016.

B.2 Points de contrôle de la sécurité d'un système

Il convient d'effectuer une revue du cahier des spécifications du système afin de s'assurer que les mesures visant à réduire le risque, applicables au BCS, sont détaillées conformément à l'IEC 61069-2.

Il convient de prêter une attention particulière pour vérifier que des informations appropriées sont fournies sur:

– les types de dangers liés au BCS, et les mesures prises pour réduire le risque et en limiter les conséquences;
– les niveaux d'émission, même s'ils sont inférieurs aux limites de sécurité et/ou aux limites autorisées;
– les certifications de sécurité appropriées, les organismes émetteurs et leur cohérence par rapport à la réglementation nationale;
– toute action de maintenance nécessaire pouvant aller à l'encontre de la sécurité du système et les précautions à prendre, dans de telles circonstances, pour éviter toute situation dangereuse;
– les exigences d'installation spéciales garantissant la sécurité du système.

Bibliographie

IEC 60243 (toutes les parties), *Rigidité diélectrique des matériaux isolants – Méthodes d'essai*

IEC 60529, *Degrés de protection procurés par les enveloppes (Code IP)*

IEC 60695-2 (toutes les parties), *Essais relatifs aux risques du feu – Partie 2: Méthodes d'essai*

IEC 60664-1, *Coordination de l'isolement des matériels dans les systèmes (réseaux) à basse tension – Partie 1: Principes, exigences et essais*

IEC 60695-11-10, *Essais relatifs aux risques du feu – Partie 11-10: Flammes d'essai – Méthodes d'essai horizontal et vertical à la flamme de 50 W*

IEC 60695-11-20, *Essais relatifs aux risques du feu – Partie 11-20: Flammes d'essai – Méthode d'essai à la flamme de 500 W*

IEC 60825-1, *Sécurité des appareils à laser – Partie 1: Classification des matériels et exigences*

IEC 61010-1:2010, *Règles de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire – Partie 1: Exigences générales*

IEC 61069-3, *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 3: Evaluation de la fonctionnalité d'un système*

IEC 61069-4, *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 4: Evaluation des caractéristiques de fonctionnement d'un système*

IEC 61069-5:2016, *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 5: Evaluation de la sûreté de fonctionnement d'un système*

IEC 61069-6:2016, *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 6: Evaluation de l'opérabilité d'un système*

IEC 61069-8, *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 8: Evaluation des autres propriétés d'un système*

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

IEC TS 62603-1, *Industrial process control systems – Guideline for evaluating process control systems – Part 1: Specifications* (disponible en anglais seulement)

CISPR 22, *Appareils de traitement de l'information – Caractéristiques des perturbations radioélectriques – Limites et méthodes de mesure*

Guide ISO/IEC 51, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

ISO 31010:2009, *Gestion des risques – Techniques d'évaluation des risques*

ENV 50166-1, *Exposition humaine aux champs électromagnétiques. Basse fréquence (0 Hz à 10 kHz)*

ENV 50166-2, *Exposition humaine aux champs électromagnétiques. Haute fréquence (10 kHz à 300 GHz)*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch