BS EN 61069-7:2016

BSI Standards Publication

Industrial-process measurement, control and automation — Evaluation of system properties for the purpose of system assessment

Part 7: Assessment of system safety

bsi.

National foreword

This British Standard is the UK implementation of EN 61069-7:2016. It is identical to IEC 61069-7:2016. It supersedes BS EN 61069-7:1999 which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2016

ISBN 978 0 580 85997 7
ICS 25.040.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2016.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61069-7

September 2016

ICS 25.040.40

Supersedes EN 61069-7:1999

English Version

Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 7: Assessment of system safety (IEC 61069-7:2016)

Mesure, commande et automation dans les processus industriels - Appréciation des propriétés d'un sytème en vue de son évaluation - Partie 7: Evaluation de la sécurité d'un système
(IEC 61069-7:2016)

Leittechnik für industrielle Prozesse - Ermittlung der Systemeigenschaften zum Zweck der Eignungsbeurteilung eines Systems - Teil 7: Eignungsbeurteilung der Sicherheit eines Systems
(IEC 61069-7:2016)

This European Standard was approved by CENELEC on 2016-07-20. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 61069-7:2016 E

European foreword

The text of document 65A/795/FDIS, future edition 2 of IEC 61069-7, prepared by SC 65A "System aspects", of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61069-7:2016.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2017-04-20
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2019-07-20

This document supersedes EN 61069-7:1999.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 61069-7:2016 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60243	NOTE	Harmonized in EN 60243 series.
IEC 60529	NOTE	Harmonized as EN 60529.
IEC 60695-2	NOTE	Harmonized in EN 60695-2 series.
IEC 60664-1	NOTE	Harmonized as EN 60664-1.
IEC 60695-11-10	NOTE	Harmonized as EN 60695-11-10.
IEC 60695-11-20	NOTE	Harmonized as EN 60695-11-20.
IEC 60825-1	NOTE	Harmonized as EN 60825-1.
IEC 61010-1:2010	NOTE	Harmonized as EN 61010-1:2010 (not modified).
IEC 61069-3	NOTE	Harmonized as EN 61069-3.
IEC 61069-4	NOTE	Harmonized as EN 61069-4.
IEC 61069-5:2016	NOTE	Harmonized as EN 61069-5:2016 (not modified).

IEC 61069-6:2016	NOTE	Harmonized as EN 61069-6:2016 (not modified).
IEC 61069-8	NOTE	Harmonized as EN 61069-8.
IEC 61508	NOTE	Harmonized in EN 61508 series.
IEC/TS 62603-1	NOTE	Harmonized as CLC/TS 62603-1.
CISPR 22	NOTE	Harmonized as EN 55022.
ISO 31010:2009	NOTE	Harmonized as EN 31010:2010 (not modified).

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
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	EN 61069-1	201X [1)]
IEC 61069-2	2016	Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 2: Assessment methodology	EN 61069-2	201X [1)]

1) To be published.

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.

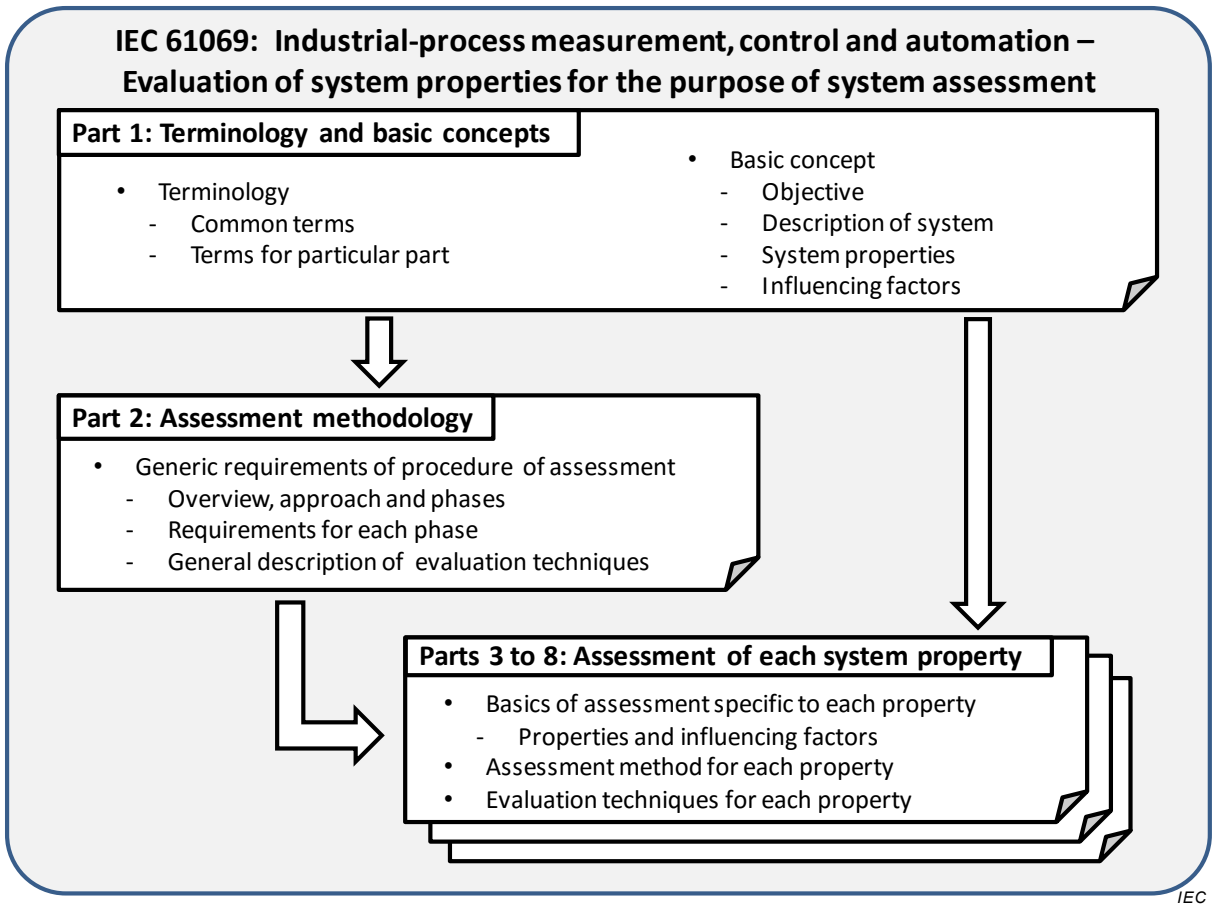

Figure 1 – General layout of IEC 61069

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.

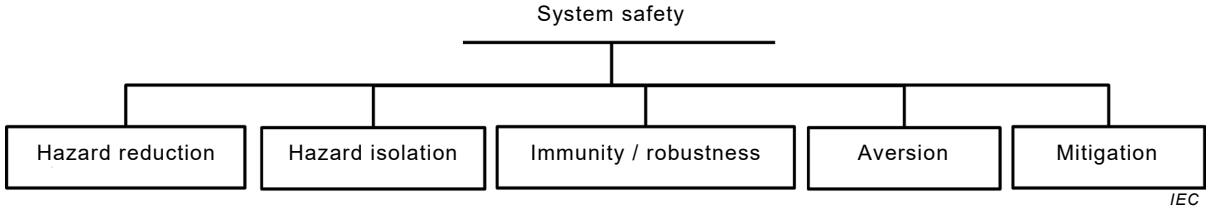

Figure 2 – System safety

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)*

_____

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.