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 It also gives information on projects, replaced and withdrawn publications.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

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

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.

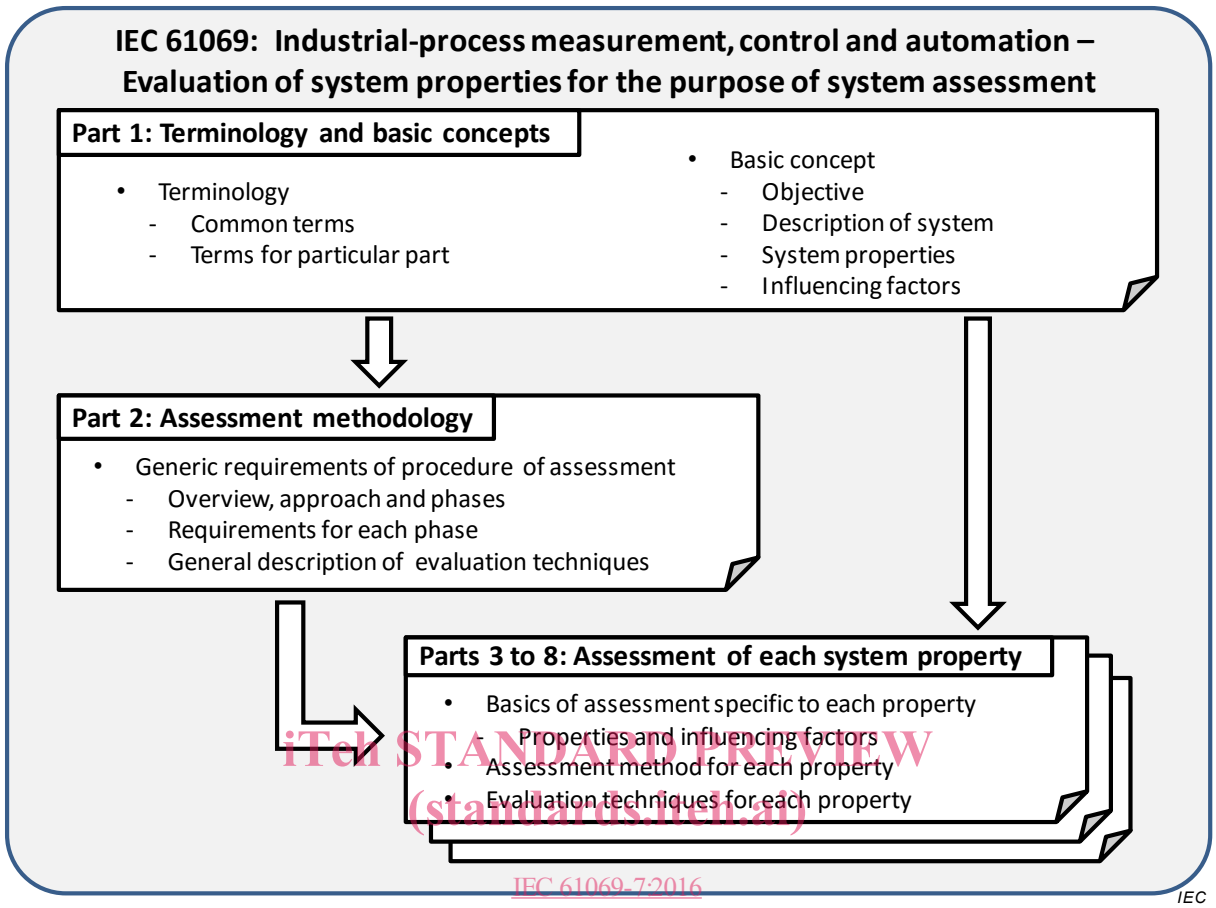

Figure 1 – General layout of IEC 61069

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.

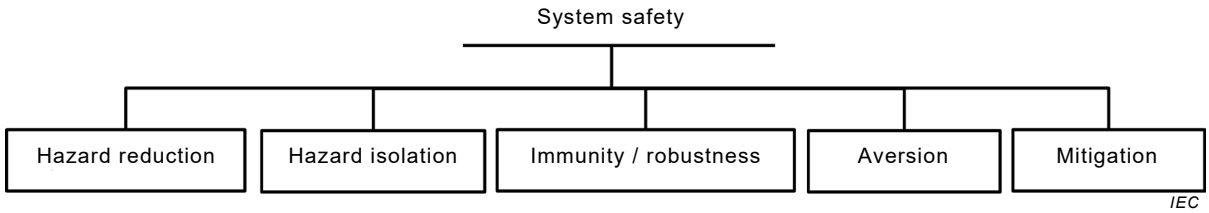

Figure 2 – System safety

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.;