

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61069-7

Première édition
First edition
1999-05

**Mesure et commande dans les processus
industriels –
Appréciation des propriétés d'un système
en vue de son évaluation –**

**Partie 7:
Evaluation de la sécurité d'un système**

**Industrial-process measurement and control –
Evaluation of system properties for the purpose of
system assessment –**

**Part 7:
Assessment of system safety**



Numéro de référence
Reference number
CEI/IEC 61069-7:1999

Numéros des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000.

Publications consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Validité de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique.

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles dans le Catalogue de la CEI.

Les renseignements relatifs à des questions à l'étude et des travaux en cours entrepris par le comité technique qui a établi cette publication, ainsi que la liste des publications établies, se trouvent dans les documents ci-dessous:

- **«Site web» de la CEI***
- **Catalogue des publications de la CEI**
Publié annuellement et mis à jour régulièrement
(Catalogue en ligne)*
- **Bulletin de la CEI**
Disponible à la fois au «site web» de la CEI* et comme périodique imprimé

Terminologie, symboles graphiques et littéraux

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 60050: *Vocabulaire Electrotechnique International* (VEI).

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera la CEI 60027: *Symboles littéraux à utiliser en électrotechnique*, la CEI 60417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles*, et la CEI 60617: *Symboles graphiques pour schémas*.

* Voir adresse «site web» sur la page de titre.

Numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series.

Consolidated publications

Consolidated versions of some IEC publications including amendments are available. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Validity of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information relating to the date of the reconfirmation of the publication is available in the IEC catalogue.

Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is to be found at the following IEC sources:

- **IEC web site***
- **Catalogue of IEC publications**
Published yearly with regular updates
(On-line catalogue)*
- **IEC Bulletin**
Available both at the IEC web site* and as a printed periodical

Terminology, graphical and letter symbols

For general terminology, readers are referred to IEC 60050: *International Electrotechnical Vocabulary* (IEV).

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications IEC 60027: *Letter symbols to be used in electrical technology*, IEC 60417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets* and IEC 60617: *Graphical symbols for diagrams*.

* See web site address on title page.

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61069-7

Première édition
First edition
1999-05

**Mesure et commande dans les processus
industriels –
Appréciation des propriétés d'un système
en vue de son évaluation –**

**Partie 7:
Evaluation de la sécurité d'un système**

**Industrial-process measurement and control –
Evaluation of system properties for the purpose of
system assessment –**

**Part 7:
Assessment of system safety**

© IEC 1999 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photo-copie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Electrotechnical Commission
Telefax: +41 22 919 0300

3, rue de Varembé Geneva, Switzerland
e-mail: inmail@iec.ch IEC web site <http://www.iec.ch>



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

R

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

	Pages
AVANT-PROPOS	4
INTRODUCTION	8
Clause	
1 Domaine d'application	12
2 Références normatives	12
3 Définitions	14
4 Propriété de sécurité	14
4.1 Généralités	14
4.2 Types de dangers	16
4.3 Récepteurs des conséquences d'un danger	18
4.4 Chemins de propagation	22
4.5 Mesures visant à réduire le risque	22
5 Examen critique du cahier des charges du système (CdC)	24
6 Examen critique du cahier des spécifications du système (CdS)	24
7 Procédure d'évaluation	26
7.1 Généralités	26
7.2 Analyse du cahier des charges et du cahier des spécifications du système	26
7.3 Conception du programme d'évaluation	28
7.4 Programme d'évaluation	30
8 Techniques d'appréciation	30
8.1 Généralités	30
8.2 Techniques analytiques d'appréciation	32
8.3 Techniques empiriques d'appréciation	32
9 Exécution de l'évaluation et rédaction du rapport d'évaluation	34
Annexe A (informative) Bibliographie	36

CONTENTS

	Page
FOREWORD	5
INTRODUCTION	9
Clause	
1 Scope	13
2 Normative references	13
3 Definitions	15
4 Safety property	15
4.1 General	15
4.2 Kinds of hazards	17
4.3 Receivers of the consequences of a hazard	19
4.4 Propagation paths	23
4.5 Risk reduction measures	23
5 Review of the system requirement document (SRD)	25
6 Review of the system specification document (SSD)	25
7 Assessment procedure	27
7.1 General	27
7.2 Analysis of the system requirement document and specification document	27
7.3 Designing the assessment programme	29
7.4 Assessment programme	31
8 Evaluation techniques	31
8.1 General	31
8.2 Analytical evaluation techniques	33
8.3 Empirical evaluation techniques	33
9 Execution and reporting of the assessment	35
Annex A (informative) Bibliography	37

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 7: Evaluation de la sécurité d'un système

AVANT-PROPOS

- 1) La CEI (Commission Electrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI, entre autres activités, publie des Normes internationales. Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61069-7 a été établie par le sous-comité 65A: Aspects systèmes, du comité d'études 65: Mesure et commande dans les processus industriels.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/280/FDIS	65A/283/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.

L'annexe A est donnée uniquement à titre d'information.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL-PROCESS MEASUREMENT AND CONTROL –
EVALUATION OF SYSTEM PROPERTIES
FOR THE PURPOSE OF SYSTEM ASSESSMENT –****Part 7: Assessment of system safety**

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The 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 and control.

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

FDIS	Report on voting
65A/280/FDIS	65A/283/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.

Annex A is for information only.

La CEI 61069 comprend les parties suivantes, présentées sous le titre général: *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation*:

Partie 1: Considérations générales et méthodologie

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 de propriétés d'un système qui ne sont pas liées à sa tâche même¹⁾

La figure 1 indique les relations entre la présente partie et les autres parties de la CEI 61069, ainsi que la position relative de la présente partie dans la CEI 61069.

La partie 1 fournit un guide complet qui, en tant que tel, est destiné à constituer une partie autonome.

La partie 2 détaille la méthodologie d'évaluation.

Les parties 3 à 8 fournissent un guide pour l'évaluation de groupes spécifiques de propriétés.

La division des propriétés en différentes parties numérotées de 3 à 8 a été choisie afin de regrouper les propriétés apparentées.

1) A publier.

IEC 61069 consists of the following parts, under the general title: *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment*:

- Part 1: General considerations and methodology
- 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 non-task-related system properties ¹⁾.

The relation of this part to the other parts of IEC 61069 and the relative place of this part within IEC 61069 is shown in figure 1.

Part 1 provides the overall guidance and, as such, is intended as a stand-alone publication.

Part 2 details the assessment methodology.

Parts 3 to 8 provide guidance on the assessment of specific groups of properties.

The division of properties in parts 3 to 8 has been chosen so as to group together related properties.

¹⁾ To be published.

INTRODUCTION

La présente partie de la CEI 61069 traite de la méthode qu'il convient d'utiliser pour évaluer la propriété de sécurité des systèmes de mesure et de commande de processus industriels. **L'étude de la sécurité dans la présente norme se limite aux dangers pouvant se présenter dans le système de mesure et de commande des processus industriels proprement dit.** Si la mission du système inclut des activités pouvant affecter la sécurité du processus ou de l'équipement contrôlés, les exigences concernant ces activités font l'objet de la CEI 61508.

Evaluer un système consiste à juger, sur la base d'éléments concrets, de son 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 dans toutes les conditions d'influence) de toutes les propriétés du système qui contribuent à remplir la mission ou l'ensemble de missions spécifiques considérées.

Une telle appréciation étant rarement réalisable dans la pratique, la démarche qui guidera l'évaluation d'un système consiste à

- identifier les points critiques des propriétés du système qui sont concernées pour l'accomplissement de la mission,
- planifier l'appréciation des propriétés concernées du système avec un effort adéquat en termes de coût pour les différentes propriétés.

Lors de l'évaluation d'un système, il est essentiel de garder à l'esprit la nécessité d'obtenir une augmentation maximale de la confiance dans l'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, on ne peut évaluer le système; toutefois, il est toujours possible de spécifier et de réaliser des appréciations (telles que celles définies dans la CEI 61069-1), qui pourront servir lors d'évaluations menées par d'autres.

Dans ce cas, on peut utiliser la norme en tant que guide pour planifier une appréciation et suivre ses procédures pour effectuer les appréciations; l'appréciation des propriétés d'un système fait, en effet, partie intégrante de l'évaluation de ce système.

INTRODUCTION

This part of IEC 61069 deals with the method which should be used to assess the safety property of industrial-process measurement and control systems. **The treatment of safety in this standard is confined to hazards that can be present within the industrial-process measurement and control system itself.** If the system mission includes activities which could affect the safety of the process or equipment under control, the requirements of these activities are the subject of IEC 61508.

The assessment of a system is the judgement, based on evidence, of the system's suitability for a specific mission or class of missions.

To obtain total evidence, a complete evaluation (for example under all influencing conditions) of all the system properties relevant to the specific mission or class of missions would be required.

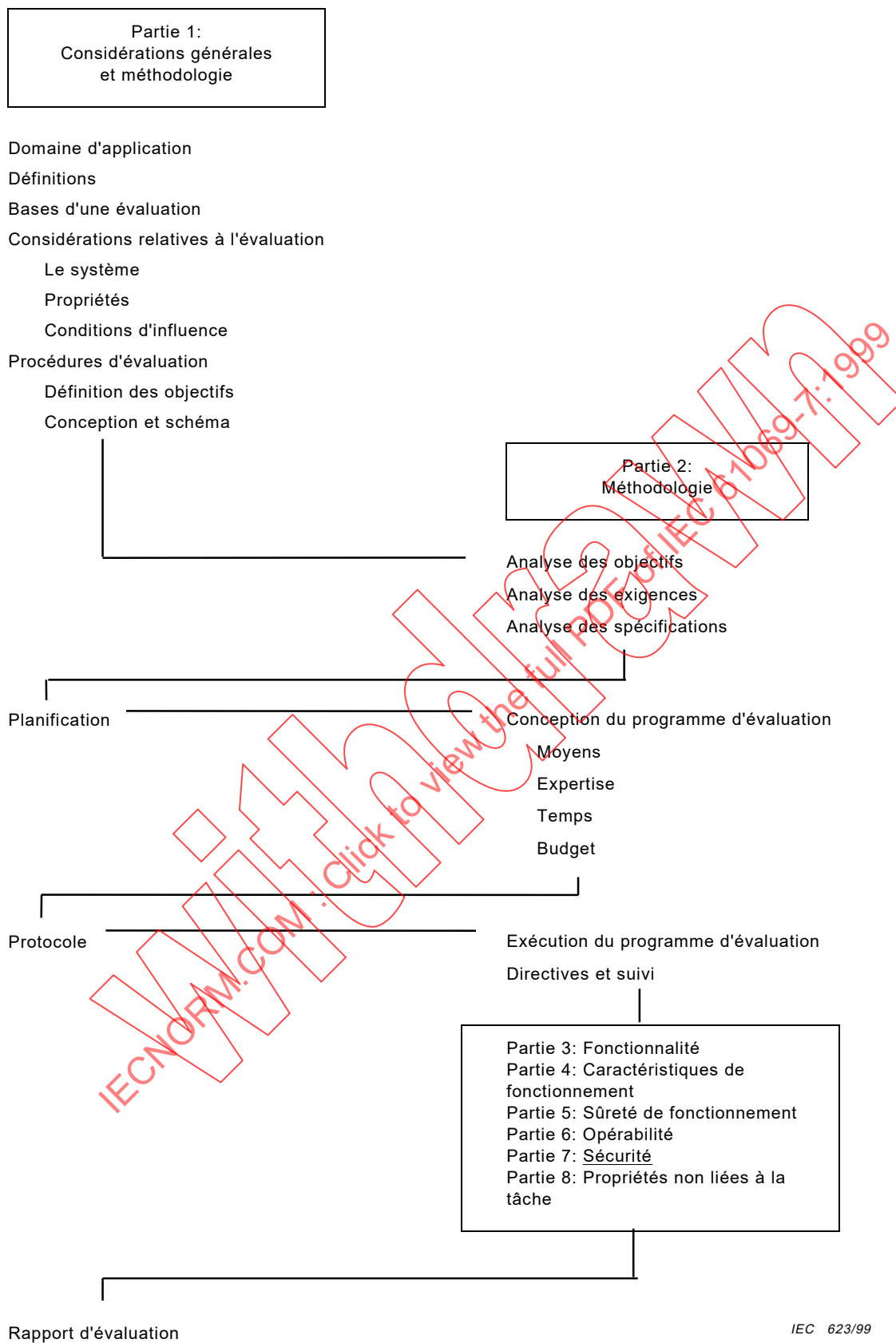
Since this is rarely practical, the rationale on which an assessment of a system should be based is

- identification of the criticality of each of the relevant system properties,
- planning for evaluation of the relevant system properties with a cost-effective dedication of effort to the various 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 the system within practical cost and time constraints.

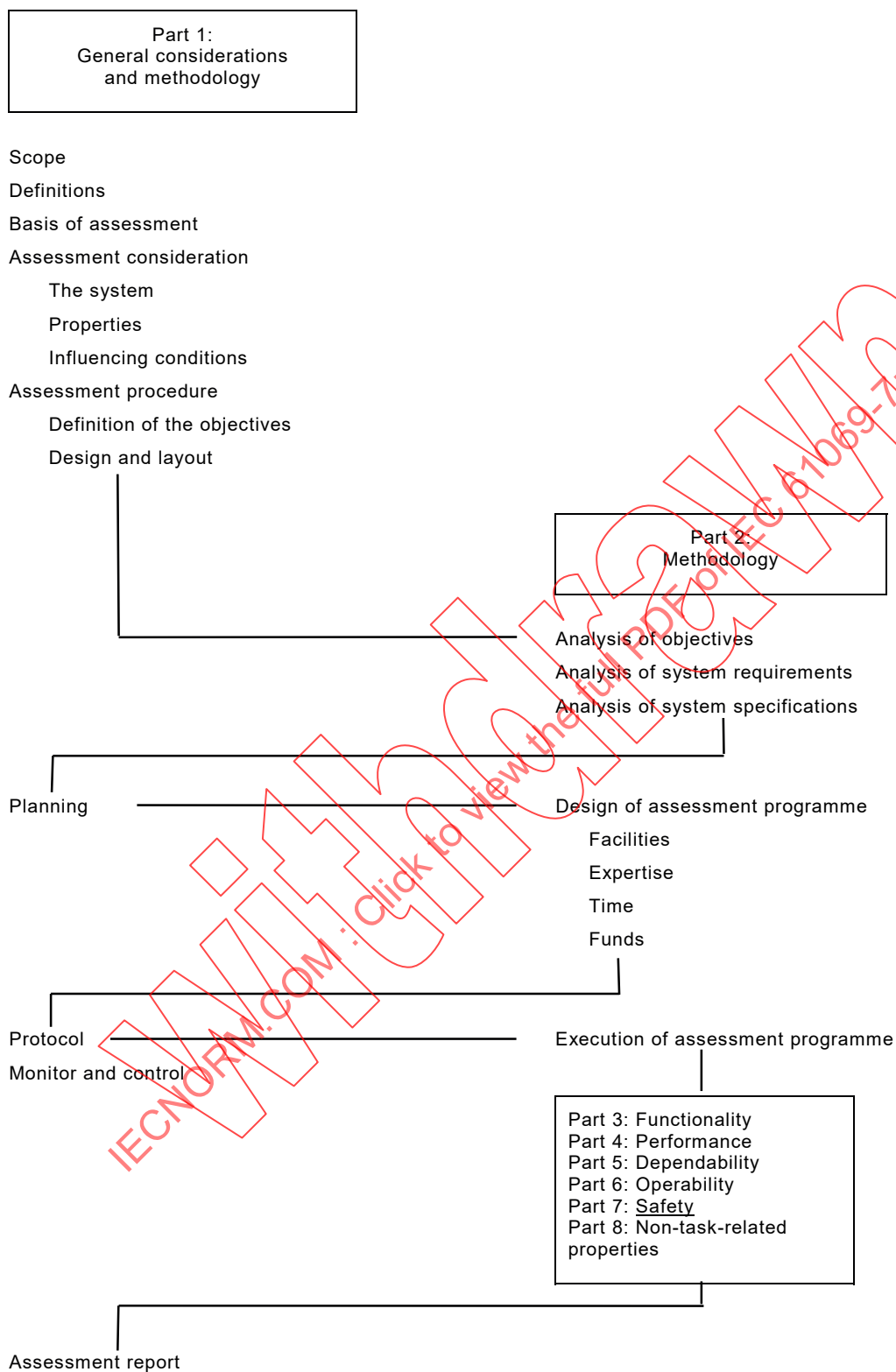
An assessment can only be carried out if a mission has been stated (or given) or if any mission can be hypothesized. In the absence of a mission, no assessment can be made; however, evaluations (as defined in IEC 61069-1) can still be specified and carried out for use in assessments performed by others.

In such cases, the standard can be used as a guide for planning an evaluation and it provides procedures for performing evaluations, since evaluations are an integral part of assessment.



IEC 623/99

Figure 1 – Disposition d'ensemble de la CEI 61069



IEC 623/99

Figure 1 – General layout of IEC 61069

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

Partie 7: Evaluation de la sécurité d'un système

1 Domaine d'application

La présente partie de la CEI 61069 décrit en détail la méthode à utiliser pour évaluer de manière systématique la propriété de sécurité d'un système de mesure et de commande de processus industriels.

L'étude de la sécurité dans la présente norme se limite aux dangers pouvant se présenter dans le système de mesure et de commande des processus industriels proprement dit. L'étude des dangers pouvant être introduits par le processus ou l'équipement contrôlés par le système de mesure et de commande de processus industriels de la commande faisant l'objet de l'évaluation est exclue. Si la mission du système inclut des activités pouvant affecter la sécurité du processus ou de l'équipement contrôlés, les exigences concernant ces activités font l'objet de la CEI 61508.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente partie de la CEI 61069. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente partie de la CEI 61069 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 61010-1:1990, *Règles de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire – Première partie: Prescriptions générales*

CEI 61069-1:1991, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 1: Considérations générales et méthodologie*

CEI 61069-2:1993, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 2: Méthodologie à appliquer pour l'évaluation*

CEI 61069-5:1994, *Mesure et commande 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*

CEI 61508-1,— *Sécurité fonctionnelle: Systèmes électriques, électroniques, électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*²⁾

Guide ISO/CEI 51: 1990, *Principes directeurs pour inclure dans les normes les aspects liés à la sécurité*

²⁾ A publier.

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

Part 7: Assessment of system safety

1 Scope

This part of IEC 61069 describes in detail the method to be used to systematically assess the safety property of an industrial-process measurement and control system.

The treatment of safety in this standard is confined to hazards that can be present within the industrial-process measurement and control system itself. Considerations of hazards that can be introduced by the process or equipment under control of the industrial-process measurement and control system to be assessed are excluded. If the system mission includes activities which could affect the safety of the process or equipment under control, the requirements of these activities are the subject of IEC 61508.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 61069. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of IEC 61069 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 61010-1:1990, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 1: General requirements*

IEC 61069-1:1991, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 1: General considerations and methodology*

IEC 61069-2:1993, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

IEC 61069-5:1994, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 5: Assessment of system dependability*

IEC 61508-1,— *Functional safety – Safety-related system – Part 1: General requirements* ²⁾

ISO/IEC Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

²⁾ To be published.

3 Définitions

Pour les besoins de la présente partie de la CEI 61069, les définitions suivantes s'appliquent:

3.1

sécurité d'un système

aptitude du système à éviter de faire apparaître, dans des conditions données, des dangers

NOTE – La sécurité d'un système n'inclut pas la sécurité du processus ou de l'équipement contrôlés. La sécurité du processus ou de l'équipement contrôlés repose sur la sûreté de fonctionnement du système si le système est utilisé pour assurer des fonctions de sécurité (voir CEI 61508).

3.2

danger

source potentielle de dommage (*Guide ISO/CEI 51: 1990, définition 3.3*)

3.3

dommage

blessure physique et/ou dommage provoqué à la santé ou à des biens
(*Guide ISO/CEI 51:1990, définition 3.4*)

4 Propriété de sécurité

4.1 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 présenter un danger. 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 la propriété 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.

La propriété de sécurité d'un système de mesure et de commande de processus industriels dépend, sous tous ses aspects (mécanique, électrique, etc.), de facteurs tels que la sécurité inhérente à sa conception et à sa sûreté de fonctionnement (voir CEI 61069-5). L'évaluation de la sécurité du système doit tenir compte de toutes les activités qui concernent le système pendant les phases d'installation, de fonctionnement opérationnel, de mise hors service et de mise au rebut de son cycle de vie. Elle doit également inclure tous les aspects environnementaux. Pendant chacune de ces phases, il convient d'étudier au minimum les mesures et les activités suivantes:

- procédures 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.

3 Definitions

For the purpose of this part of IEC 61069, the following definitions apply:

3.1

system safety

extent to which the system itself as a physical entity will not impose a hazard

NOTE – System safety does not include the safety of the process or equipment under control. The safety of the process or equipment under control will rely upon the dependability of the system if the system is used to perform safety functions (refer to IEC 61508).

3.2

hazard

potential source of harm (*ISO/IEC Guide 51:1990, definition 3.3*)

3.3

harm

physical injury and/or damage to health or property (*ISO/IEC Guide 51:1990, definition 3.4*)

4 Safety property

4.1 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 a hazard. It is important to recognize that these conditions can change over the lifetime of the system.

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

The safety property of an industrial-process measurement and control system in all its aspects (mechanical, electrical, etc.) depends upon factors such as the inherent safety of its design and its dependability (see IEC 61069-5). The assessment of the system safety shall cover all activities related to the system during the installation, operational, de-commissioning and disposal phases of its life cycle. It shall also include all environmental aspects. During each of the phases, at least the following measures and activities are to be considered:

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

Lors de l'évaluation de la sécurité du système, les aspects suivants doivent être étudiés:

- types de dangers;
- récepteurs des conséquences d'un danger;
- chemins de propagation;
- mesures visant à réduire le risque.

NOTE – Le niveau de sécurité d'un système peut évoluer au cours des différentes phases de son cycle de vie en raison du nombre de dangers présents tels que:

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

4.2 Types de dangers

4.2.1 Généralités

Une seule source de dommage peut par elle-même présenter un danger. Toutefois, il arrive fréquemment que la source de dommage génère des effets secondaires tels qu'une température ou pression élevées, ce qui constitue le véritable danger.

Au minimum, les types de dangers suivants doivent être pris en compte.

4.2.2 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 constituer une source de dommage, par exemple en cas de température excessive de composants.

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

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

4.2.3 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 qui sont les sources de dangers peuvent provenir de l'intérieur du système et/ou de l'alimentation du système.

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

- kinds of hazards;
- receivers of the consequences of a hazard;
- propagation paths;
- risk reduction measures.

NOTE – The safety level of a system can change over the different phases of its life cycle due to the number of hazard 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.

4.2 Kinds of hazards

4.2.1 General

A single source of harm in itself can be hazardous. However, it is very often the case that the source of harm causes secondary effects such as high temperature, high pressure, etc. and that this is the real hazard.

At least the following kinds of hazards shall be considered.

4.2.2 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 hot items.

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

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

4.2.3 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.

4.2.4 Dangers induits par les champs électromagnétiques

Le système peut émettre des champs magnétiques 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 le CISPR 22. Des recommandations concernant les limites au-delà desquelles un dommage humain peut apparaître peuvent être consultées, par exemple, dans la ENV 50166-1 et la ENV 50166-2.

4.2.5 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 la CEI 60825-1.

4.2.6 Dangers induits par la radioactivité

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

4.2.7 Dangers biologiques

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

4.2.8 Dangers chimiques

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

4.3 Récepteurs des conséquences d'un danger

4.3.1 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.

Dans l'environnement d'un système de mesure et de commande de processus industriels, on distingue différentes zones telles que la salle de commande, l'usine ou la ville. Ces classifications de zones sont généralement décrites dans des normes internationales, nationales ou privées. Dans chacune de ces zones, différents niveaux de dommages et d'exposition aux dommages sont acceptables pour chaque type de récepteur.

Les différents types de récepteurs sont répertoriés ci-dessous.

4.3.2 L'homme

Les différents types de dangers mentionnés en 4.2 qui peuvent exister dans les systèmes de mesure et de commande de processus industriels peuvent nuire au corps humain de différentes façons. On trouvera ci-dessous quelques exemples:

4.2.4 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.

4.2.5 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 may reach a hazardous level. For laser sources, refer to IEC 60825-1.

4.2.6 Radioactivity

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

4.2.7 Biological

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

4.2.8 Chemical

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

4.3 Receivers of the consequences of a hazard

4.3.1 General

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

- the characteristics of the type of receiver,
- the area in which the receiver is located.

Within the environment of an industrial-process measurement and control system, different areas can be identified such as the control room, plant or city. These area classifications are typically given in international, national or proprietary standards. Within each of these areas, individual levels of harm and exposures to harm are acceptable for each type of receiver.

The different types of receivers are listed below.

4.3.2 Human

The kinds of hazards mentioned in 4.2 which can exist in the industrial-process measurement and control system may harm the human body in different ways. Some examples are given below:

- dangers mécaniques:
 - le poids peut, par exemple, fracturer des os;
 - 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;
 - l'élasticité peut, par exemple, entraîner des blessures générales ou la fracture d'os;
 - les vibrations peuvent, par exemple, entraîner des troubles auditifs;
 - la température peut, par exemple, entraîner des brûlures;
- les courts-circuits et les chocs électriques peuvent, par exemple, causer des brûlures, la fibrillation du cœur ou des troubles de la vue;
- les champs électromagnétiques peuvent, par exemple, entraîner une altération du métabolisme, des troubles de la vue ou la destruction d'organes;
- les ondes lumineuses peuvent, par exemple, entraîner des troubles de la vue ou des brûlures;
- la radioactivité peut, par exemple, entraîner une altération du métabolisme, des troubles de la vue ou la destruction d'organes;
- les substances biologiques peuvent pénétrer et, par exemple, entraîner une altération du métabolisme ou la modification de la chaîne alimentaire;
- 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.

4.3.3 La nature

Les différents types de dangers indiqués en 4.2 peuvent exister dans les systèmes de mesure et de commande de processus industriels peuvent nuire aux systèmes biologiques tels que la flore, la faune et l'écosystème, de manière analogue à celle décrite en 4.3.2. L'intensité des dommages physiques peut varier, selon qu'ils affectent un système biologique ou l'homme.

4.3.4 Les équipements

Les différents types de dangers indiqués en 4.2 qui peuvent exister dans les systèmes de mesure et de commande de processus industriels peuvent nuire, de différentes façons, aux équipements environnants. On trouvera ci-après quelques exemples:

- dangers mécaniques:
 - 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.;
 - les vibrations peuvent, selon leur importance, avoir pour résultat un défaut d'alignement, une fatigue du métal, une désolidarisation des pièces, etc.;
 - 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.;
- 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.;
- les champs électromagnétiques peuvent, selon leur importance, entraîner des interférences électromagnétiques, une altération des données, etc.;
- 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.;
- dangers biologiques: aucun effet prévu;
- les substances chimiques peuvent, selon leur importance, entraîner une transformation chimique des matériaux, etc.

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

4.3.3 Biological

The kinds of hazards mentioned in 4.2 which can exist in the industrial-process measurement and control system can harm biological systems such as flora, fauna and the ecological system, in similar ways as described in 4.3.2. The intensity of the physical injury to a biological system can be different from that to a human.

4.3.4 Equipment

The kinds of hazards mentioned in 4.2 which can exist in the industrial-process measurement and control system can harm surrounding equipment in different ways. Some examples are given below:

- mechanical:
 - weight, pressure, elasticity can, depending on the severity, result in misalignment, bending or breaking parts, etc.;
 - vibration can, depending on the severity, result in misalignment, metal fatigue, parts coming loose, etc.;
 - temperature can, depending on its level, result in misalignment, decreased life time, loss of mechanical strength, degazification, burning, etc.;
- electrical sources can, depending on the severity, result in supply power distortion, breakdown due to overload, current surges, flashover, burns, etc.;
- electromagnetic fields can, depending on the severity, result in electromagnetic interference, alteration of data, etc.;
- light or radioactivity can, depending on the level, result in changes of material properties due to ultra-violet or laser-light, etc.;
- biological: no effect foreseen;
- chemical substances can, depending on the severity, result in chemical transformation of material, etc.

4.4 Chemins de propagation

4.4.1 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 ci-dessous.

4.4.2 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).

4.4.3 Chemin de propagation indirect

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

4.4.4 Chemin de propagation dynamique

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

4.4.5 Chemin de propagation sans contact

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

4.5 Mesures visant à réduire le risque

La meilleure façon d'éviter le risque de dommage serait de concevoir l'équipement de manière que la source de danger ne puisse atteindre un niveau pouvant nuire, par exemple en concevant un équipement de sécurité intrinsèque.

Néanmoins, comme cela n'est pas toujours possible, le risque de dommage peut être réduit en

- réduisant la source de dommage,
- interrompant le chemin de propagation,
- limitant la probabilité, pour le récepteur, d'être dans la zone dangereuse.

La réduction de la source de dommage peut être réalisée en faisant appel

- à des éléments de sécurité intrinsèque, par exemple des entrées électriques,
- à des configurations spécifiques, par exemple des configurations avec vote majoritaire deux sur trois,
- à des éléments limiteurs, par exemple des capacités d'antiparasitage, des diodes de protection ou des soupapes de décompression,
- à une augmentation de la distance entre la source de dommage et les récepteurs.

4.4 Propagation paths

4.4.1 General

For a hazard to be harmful, there must be 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 below.

4.4.2 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).

4.4.3 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).

4.4.4 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).

4.4.5 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.

4.5 Risk reduction measures

The best way to avoid risk of harm should be to design the equipment so that the source of hazard cannot reach a value which can be harmful, for example by designing intrinsically safe equipment.

However, since this is not always possible, the risk of harm can be reduced by

- reducing the source of harm,
- interrupting the propagation path,
- limiting the probability that the receiver is in the hazardous area.

Reduction of the source of harm can be achieved by

- applying intrinsically safe elements, for example to electrical inputs,
- applying special configurations, for example a "two out of three" configuration,
- applying limiting elements, for example suppression capacitors, protection diodes or relief valves,
- increasing the distance between the source of harm and the receivers.

L'interruption des chemins de propagation peut être réalisée en faisant appel

- à des écrans, à des blindages,
- à des capots, à des enveloppes,
- à des éléments de protection, par exemple des diodes,
- aux distances, par exemple des distances de décharge,
- à des collecteurs/supports électriques, à des collecteurs/supports de sécurité,
- à des transformateurs d'isolement, à des transformateurs de sécurité,
- à des vêtements de protection.

La limitation de la probabilité, pour le récepteur, d'être dans la zone dangereuse peut être réalisée en

- limitant les accès, par exemple au moyen de procédures, ou d'utilisation de clés,
- utilisant des signalisations avertisseuses, des signaux lumineux, des sirènes,
- gardant des distances de sécurité, par exemple en utilisant des barrières, des obstacles visuels.

5 Examen critique du cahier des charges du système (CdC)

Il convient d'effectuer un examen critique 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 la CEI 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 aux niveaux national ou international, ou au niveau des sociétés et, tout particulièrement, la CEI 60664-1 et la CEI 61010-1,
- les niveaux d'émission autorisés pour les catégories de dangers répertoriées en 4.2,
- les zones où doivent être installés le système de mesure et de commande de processus industriels 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 système de mesure et de commande de processus industriels, ainsi que les procédures nécessaires à l'obtention des permis de travail,
- les transgressions autorisées de ces conditions de travail, leur fréquence et les procédures d'urgence à suivre, le cas échéant,
- les niveaux d'émission autorisés pour les catégories de dangers répertoriées en 4.2 et concernant les zones voisines du système de mesure et de commande de processus industriels.

6 Examen critique du cahier des spécifications du système (CdS)

Il convient d'effectuer un examen critique du cahier des spécifications du système afin de s'assurer que les mesures visant à réduire le risque, applicables au système de mesure et de commande de processus industriels, sont détaillées conformément à la CEI 61069-2.

Interruption of the propagation paths can be achieved by applying

- screens, shields,
- covers, enclosures,
- protective devices: for example, diodes,
- distances: for example, creepage distances,
- electrical sockets, safety sockets,
- isolation transformers, safety transformers,
- protective clothing.

Limiting the probability that the receiver is in the hazardous area can be achieved by

- access control restrictions, for example procedures, use of keys,
- use of warning flags, flash lights, horns,
- keeping a safety distance, for example by using gates, visual obstructions.

5 Review of the system requirement document (SRD)

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 industrial-process measurement and control system 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 industrial-process measurement and control system, 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 industrial-process measurement and control system.

6 Review of the system specification document (SSD)

The system specification document should be reviewed to check that the risk reduction measures of the industrial-process measurement and control system are listed as described in 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 système de mesure et de commande de processus industriels, et les mesures prises visant à réduire le risque et à 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.

7 Procédure d'évaluation

7.1 Généralités

Il convient que l'évaluation suive la procédure décrite à l'article 7 de la CEI 61069-2.

L'objectif de l'évaluation doit être clairement exprimé. Des indications sont données en 4.1 de la CEI 61069-1.

L'objectif doit permettre de vérifier que le système de mesure et de commande de processus industriels est conforme à la réglementation nationale en vigueur sur le site où le système doit être utilisé.

Les informations figurant dans le CdC et le CdS du système doivent être exhaustives et précises afin de permettre l'évaluation de la sécurité.

Si, au cours de l'une quelconque des phases de l'évaluation, certaines informations sont manquantes ou incomplètes, il convient d'adresser des questions pertinentes aux rédacteurs du CdC et du CdS afin d'obtenir les informations complémentaires nécessaires. Il convient que ces informations complémentaires soient notées correctement dans les documents concernés.

7.2 Analyse du cahier des charges et du cahier des spécifications du système

7.2.1 Classement des informations détaillées

Pour l'évaluation de la sécurité d'un système, les informations nécessaires doivent être extraites du CdC et du CdS du système, comme cela est décrit en 7.2 de la CEI 61069-2.

Il convient d'écrire, en regard des exigences énoncées dans le CdC, le niveau de sécurité du système donné dans le CdS, et de les confronter afin d'établir un rapport précis et concis, en termes qualitatifs et/ou quantitatifs, avec, le cas échéant, leurs ordres de grandeur, sur les points suivants:

- limites physiques du système de mesure et de commande de processus industriels,
- types de dangers et chemins de propagation entre le système et son environnement,
- conditions d'influence pouvant entraîner une situation dangereuse à l'intérieur du système,
- mesures visant à réduire le risque mises en oeuvre pour minimiser les conséquences de situations dangereuses,
- mesures visant à réduire le risque mises en oeuvre pour minimiser la probabilité d'apparition d'une conjonction de phénomènes pouvant entraîner des situations dangereuses,

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

- kinds of hazard within the industrial-process measurement and control system, 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.

7 Assessment procedure

7.1 General

The assessment should follow the procedure laid down in clause 7 of IEC 61069-2.

The objective of the assessment shall be clearly stated. Guidance is given in 4.1 of IEC 61069-1.

The objective must include a check that the industrial-process measurement and control system complies with the national regulations in force at the site where the system is intended to be used.

The information given in the SRD and the SSD should be complete and precise to enable the assessment of the system safety.

If, at any phase of the assessment, information is missing or incomplete, the originators of the SRD and SSD should be consulted, with specific questions to obtain the required further information. This further information should be properly recorded in the documents concerned.

7.2 Analysis of the system requirement document and specification document

7.2.1 Collation of documented information

For the purpose of the assessment of the system safety, the necessary information shall be extracted from the SRD and the SSD in accordance with 7.2 of IEC 61069-2.

The requirements as stated in the SRD and the level of safety provided by the system as given in the SSD should be drawn together and cross-related to compile precise and concise statements in quantitative and/or qualitative terms, and their range of values, if applicable, of the following:

- physical boundaries of the industrial-process measurement and control system;
- kinds of hazards and their propagation paths from the system to its environment;
- influencing conditions that may 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;

- attribution de la sécurité aux modules et éléments du système,
- 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,
- points sur lesquels le système ne respecte pas les exigences,
- ensemble des connaissances préalables disponibles et la mesure dans laquelle il convient que la sécurité soit évaluée.

7.2.2 Conditions influençant la sécurité

Parmi les domaines extérieurs au système mentionnés en 4.4 de la CEI 61069-1, les conditions d'influence peuvent provenir des domaines suivants:

- services, par exemple maintenance, documentation ou utilisation d'outils;
- personnes, par exemple formation, compétences, attitudes ou mauvaise utilisation,
- environnement, par exemple chocs mécaniques, vibrations, chaleur, feu, humidité, liquides, poussière, liquides ou gaz corrosifs, perturbations électromagnétiques, modification des circuits électriques (ouverture d'une boucle de courant) ou installation dans une zone d'accès limité.

La sécurité du système doit être évaluée pour les phases d'installation, de fonctionnement opérationnel, de mise hors service, et de mise au rebut de son cycle de vie et, pour les phases où cela est applicable, dans tous les modes opératoires autorisés.

7.2.3 Mise en forme des informations recueillies

Il convient de mettre les informations recueillies comme il est indiqué ci-dessus sous une forme qui permette leur utilisation lors de la conception du programme d'évaluation.

7.3 Conception du programme d'évaluation

7.3.1 Comparaison du cahier des charges et du cahier des spécifications du système

La première étape de l'élaboration du programme d'évaluation consiste à analyser les informations recueillies dans le CdC et le CdS conformément à 7.2.

En comparant le CdC et le CdS comme cela est décrit en 7.2, on établit une liste «danger par danger» de toutes les mesures de sécurité mises en oeuvre pour répondre aux exigences de sécurité.

Chaque entrée de cette liste est un sujet potentiel d'évaluation.

Chaque sujet potentiel d'évaluation doit être examiné pour fixer le niveau de détail auquel il convient de l'apprécier afin d'obtenir l'augmentation désirée du niveau de confiance.

7.3.2 Sujets d'évaluation

La liste complète de tous les sujets potentiels d'évaluation est réduite en appliquant les filtres suivants afin d'obtenir la liste des sujets à évaluer:

- niveau de confiance présent, basé par exemple sur des certifications existantes du système et une connaissance préalable;
- maturité du système, basée par exemple sur le niveau de normalisation des modules, éléments et interfaces mis en oeuvre dans le système
- niveau de confiance requis, si possible en termes quantitatifs.

- allocation of safety to the system modules and elements;
- 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;
- items in which the system does not comply with the requirements;
- global pre-knowledge available and extent to which the safety property should be assessed.

7.2.2 Conditions influencing safety

Among the external domains mentioned in 4.4 of IEC 61069-1, influencing conditions can originate from the following domains:

- service, for example maintenance, documentation or use of tools;
- human, for example training, skill, attitude or misuse;
- environment, for example mechanical shock, vibration, heat, fire, moisture, humidity, liquid, dust, corrosive gas or liquid, electromagnetic disturbances, modification of electrical circuitry (opening of a current loop) or installation in a restricted access area.

The system safety shall be assessed for the installation, operational, decommissioning and disposal phases of its life cycle, and for the relevant phases under all permitted operating modes.

7.2.3 Documenting collated information

The information collated as stated above should be documented in a form that can be manipulated for the process of designing the assessment programme.

7.3 Designing the assessment programme

7.3.1 Comparison of the system requirement document and system specification document

The first step in designing the assessment programme is to analyse the information collected from the SRD and SSD as per 7.2.

By comparing the SSD and SRD as described in 7.2, a "hazard-by-hazard" list is constructed showing the measures provided to achieve safety set against the safety requirements.

Each entry in this list is a potential assessment item.

Each potential assessment item must be examined to decide the extent to which this item should be evaluated to obtain the required increase in the level of confidence.

7.3.2 Assessment items

The complete list of all potential assessment items is reduced by applying the following filters to obtain the list of items to be assessed:

- existing level of confidence based upon, for example, existing certifications obtained for the system and prior knowledge;
- maturity of the system based upon, for example, the degree of standardization of the modules, elements and interfaces applied in the system;
- confidence level required, if possible in quantitative terms.

NOTE IMPORTANTE – Il faut que les sujets d'évaluation qui sont requis par les organismes de réglementation nationaux et/ou internationaux soient évalués et appréciés selon les règles figurant dans lesdites réglementations.

7.3.3 Activités d'évaluation

Une liste des activités d'évaluation est alors obtenue en complétant chacun des sujets d'évaluation de la liste réduite conformément à 7.3.2 par

- le type d'analyse et/ou d'appréciation requis pour étayer l'évaluation,
- le niveau de priorité pour chacune des activités d'évaluation,
- les connaissances et les compétences requises pour exécuter l'analyse et/ou l'évaluation requises,
- les contraintes sur la planification de l'évaluation découlant des effets permanents que l'évaluation d'autres propriétés peut avoir;
- la disponibilité du personnel choisi;
- les outils et les services requis pour exécuter l'analyse et/ou l'évaluation requises;
- l'estimation du coût et du temps pour chaque analyse et chaque évaluation requises.

En fonction des critères exprimés en 7.3.1 et 7.3.2, il peut être nécessaire d'envisager plusieurs techniques d'évaluation qui se complètent mutuellement.

La liste des activités d'évaluation sera combinée avec des listes similaires établies pour l'évaluation des autres propriétés afin d'aboutir à un programme d'évaluation global pour le système.

NOTE – Il convient de garder à l'esprit que l'évaluation du système a pour but d'établir jusqu'à quel point le système lui-même présente un danger pour son environnement direct.

7.4 Programme d'évaluation

Il convient que le programme final d'évaluation spécifie et/ou répertoire au moins les points suivants:

- but de l'évaluation, comme cela est indiqué en 7.1;
- critères pris en compte en 7.3.2;
- liste des sujets à évaluer indiquée en 7.3.3;
- augmentation requise du niveau de confiance;
- planification de l'évaluation prenant en compte les effets permanents que peuvent avoir les essais.

8 Techniques d'appréciation

8.1 Généralités

Il convient de choisir la ou les techniques d'appréciation utilisées de façon que les résultats puissent être comparés de manière qualitative et/ou quantitative aux exigences définies dans le cahier des charges.

On peut retenir des techniques analytiques fondées uniquement sur la documentation du système ou des techniques empiriques nécessitant l'accès à un système existant.

Les résultats obtenus au moyen d'autres techniques d'appréciation peuvent être quantitatifs ou qualitatifs, ou les deux.