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

This document is a preview generated by EVS

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: S*ymboles 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.

This document is a preview generated by EVS

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61069-7

Première édition
First edition
1999-05

This document is a preview generated by EVS

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 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 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

This document is a preview generated by EVS

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

This document is a preview generated by EVS

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.

This document is a preview generated by EVS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 7: Assessment of system safety

This document is preview generated by EVS

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 même[1)]

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.

This document is a preview generated by EVS

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.

This document is a preview generated by EVS

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.

Withdocuments.apreview generated by EVS

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.

This document is a preview generated by EVS

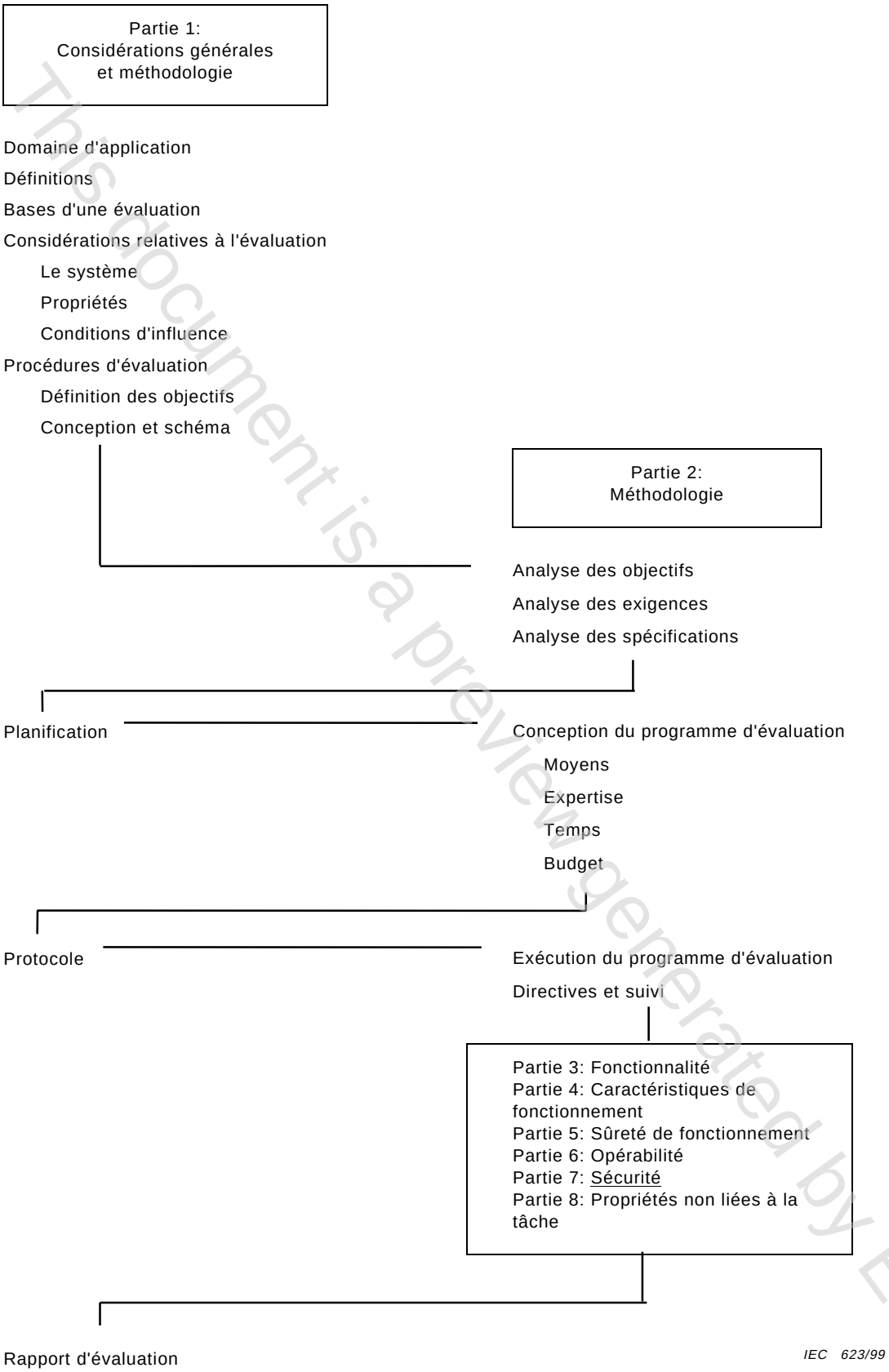

Figure 1 – Disposition d'ensemble de la CEI 61069

This document is a preview generated by EVS

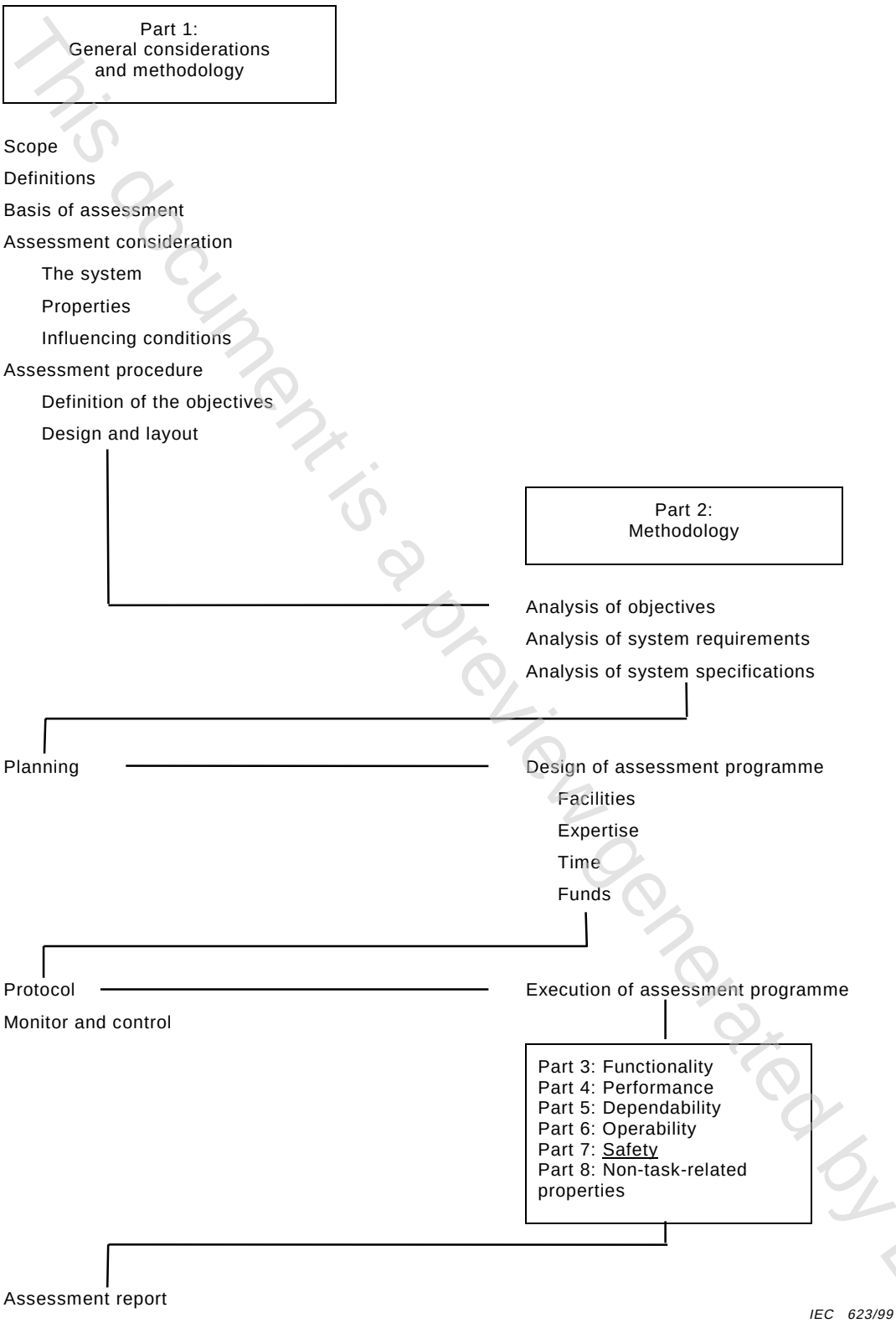

Figure 1 – General layout of IEC 61069

This document is a preview generated by EVS

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

This document is a preview generated by EVS

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

This document is a preview generated by EVS

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.