

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8322-3447-1

**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

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	8
2 Normative references.....	8
3 Terms, definitions, abbreviated terms, acronyms, conventions and symbols.....	9
3.1 Terms and definitions.....	9
3.2 Abbreviated terms, acronyms, conventions and symbols.....	9
4 Basis of assessment specific to dependability.....	9
4.1 Dependability properties.....	9
4.1.1 General.....	9
4.1.2 Availability.....	10
4.1.3 Reliability.....	10
4.1.4 Maintainability.....	10
4.1.5 Credibility.....	11
4.1.6 Security.....	11
4.1.7 Integrity.....	12
4.2 Factors influencing dependability.....	12
5 Assessment method.....	12
5.1 General.....	12
5.2 Defining the objective of the assessment.....	12
5.3 Design and layout of the assessment.....	13
5.4 Planning of the assessment program.....	13
5.5 Execution of the assessment.....	13
5.6 Reporting of the assessment.....	13
6 Evaluation techniques.....	13
6.1 General.....	13
6.2 Analytical evaluation techniques.....	14
6.2.1 Overview.....	14
6.2.2 Inductive analysis.....	15
6.2.3 Deductive analysis.....	15
6.2.4 Predictive evaluation.....	15
6.3 Empirical evaluation techniques.....	16
6.3.1 Overview.....	16
6.3.2 Tests by fault-injection techniques.....	16
6.3.3 Tests by environmental perturbations.....	17
6.4 Additional topics for evaluation techniques.....	17
Annex A (informative) Checklist and/or example of SRD for system dependability.....	18
Annex B (informative) Checklist and/or example of SSD for system dependability.....	19
B.1 SSD information.....	19
B.2 Check points for system dependability.....	19
Annex C (informative) An example of a list of assessment items (information from IEC TS 62603-1).....	20
C.1 Overview.....	20
C.2 Dependability.....	20
C.3 Availability.....	20

C.3.1	System self-diagnostics.....	20
C.3.2	Single component fault tolerance and redundancy	20
C.3.3	Redundancy methods.....	21
C.4	Reliability.....	22
C.5	Maintainability.....	23
C.5.1	General	23
C.5.2	Generation of maintenance requests	23
C.5.3	Strategies for maintenance.....	23
C.5.4	System software maintenance	23
C.6	Credibility	23
C.7	Security	24
C.8	Integrity	24
C.8.1	General	24
C.8.2	Hot-swap	24
C.8.3	Module diagnostic	24
C.8.4	Input validation	24
C.8.5	Read-back function	24
C.8.6	Forced output	24
C.8.7	Monitoring functions.....	24
C.8.8	Controllers.....	24
C.8.9	Networks	25
C.8.10	Workstations and servers	25
Annex D (informative)	Credibility tests.....	26
D.1	Overview.....	26
D.2	Injected faults	27
D.2.1	General	27
D.2.2	System failures due to a faulty module, element or component.....	27
D.2.3	System failures due to human errors	27
D.2.4	System failures resulting from incorrect or unauthorized inputs into the system through the man-machine interface	27
D.3	Observations.....	28
D.4	Interpretation of the results.....	28
Annex E (informative)	Available failure rate databases	29
E.1	Databases	29
E.2	Helpful standards concerning component failure	30
Annex F (informative)	Security considerations	31
F.1	Physical security.....	31
F.2	Cyber-security.....	31
F.2.1	General	31
F.2.2	Security policy	31
F.2.3	Other considerations.....	31
Bibliography	33
Figure 1 – General layout of IEC 61069.....		7
Figure 2 – Dependability		9

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 5: Assessment of system dependability

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 61069-5 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 1994. 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 61069-5:1994 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/793/FDIS	65A/803/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 web site 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.

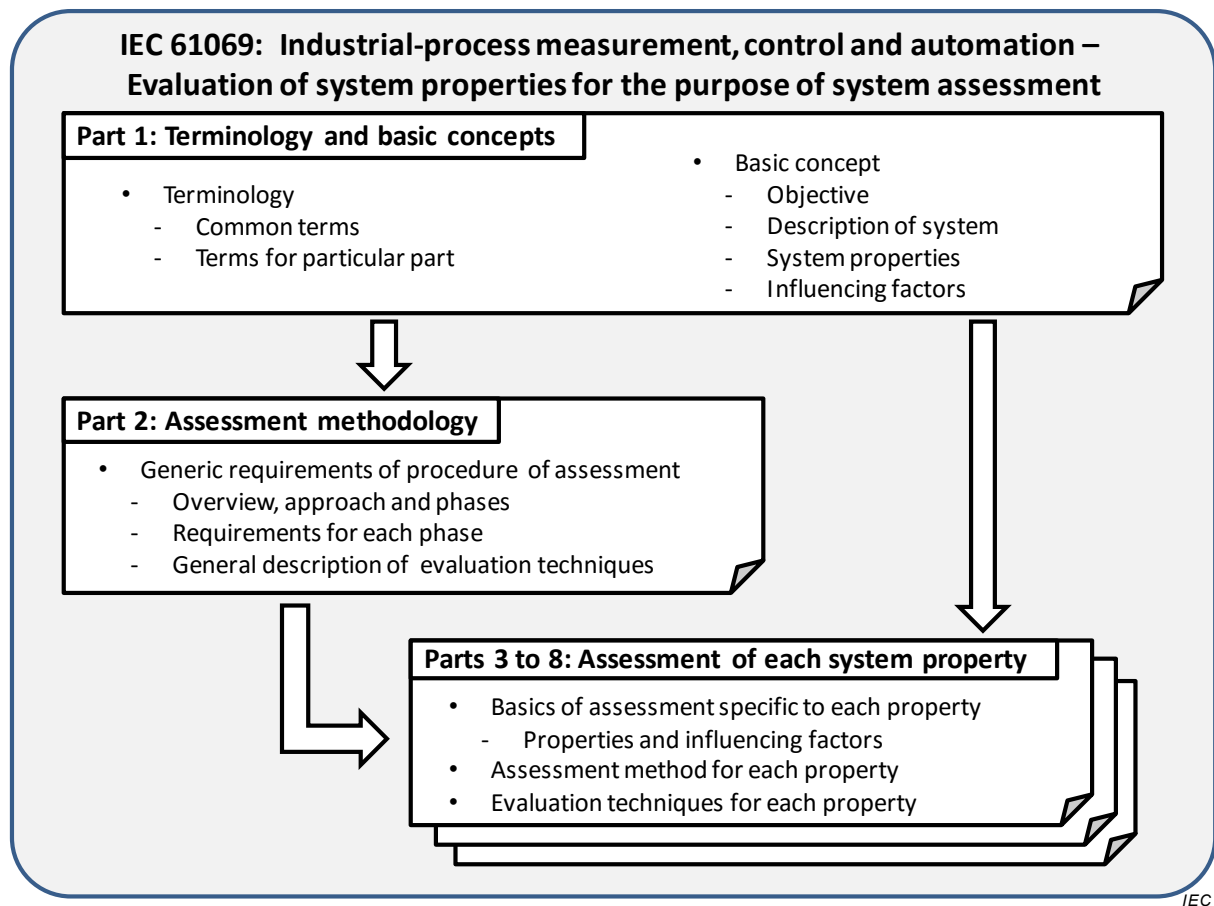


Figure 1 – General layout of IEC 61069

Some example assessment items are integrated in Annex C.

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

Part 5: Assessment of system dependability

1 Scope

This part of IEC 61069:

- specifies the detailed method of the assessment of dependability 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 dependability properties,
- describes the factors that influence dependability and which need to be taken into account when evaluating dependability, and
- provides guidance in selecting techniques from a set of options (with references) for evaluating the dependability.

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 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60319, *Presentation and specification of reliability data for electronic components*

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*

IEC 61070, *Compliance test procedures for steady-state availability*

IEC 61709:2011, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

ISO IEC 25010, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*

ISO IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

ISO IEC 27002, *Information technology – Security techniques – Code of practice for information security controls*

SOMMAIRE

AVANT-PROPOS.....	38
INTRODUCTION.....	40
1 Domaine d'application.....	42
2 Références normatives	42
3 Termes, définitions, abréviations, acronymes, conventions et symboles.....	43
3.1 Termes et définitions.....	43
3.2 Abréviations, acronymes, conventions et symboles	43
4 Principes de base de l'évaluation spécifique à la sûreté de fonctionnement.....	43
4.1 Propriétés de la sûreté de fonctionnement	43
4.1.1 Généralités	43
4.1.2 Disponibilité	44
4.1.3 Fiabilité.....	44
4.1.4 Maintenabilité	45
4.1.5 Crédibilité	45
4.1.6 Sécurité	46
4.1.7 Intégrité	46
4.2 Facteurs influençant la sûreté de fonctionnement.....	46
5 Méthode d'évaluation.....	47
5.1 Généralités	47
5.2 Définition de l'objectif de l'évaluation	47
5.3 Conception et agencement de l'évaluation	47
5.4 Planification du programme d'évaluation	47
5.5 Exécution de l'évaluation.....	48
5.6 Rédaction du rapport d'évaluation.....	48
6 Techniques d'appréciation	48
6.1 Généralités	48
6.2 Techniques d'appréciation analytique	49
6.2.1 Vue d'ensemble	49
6.2.2 Analyse inductive	49
6.2.3 Analyse déductive.....	49
6.2.4 Appréciation prévisionnelle.....	50
6.3 Techniques d'appréciation empirique.....	51
6.3.1 Vue d'ensemble	51
6.3.2 Essais par techniques d'introduction de défauts.....	51
6.3.3 Essais par perturbations affectant l'environnement	52
6.4 Sujets supplémentaires de techniques d'appréciation.....	52
Annexe A (informative) Liste de contrôle et/ou exemples de CdC pour la sûreté de fonctionnement d'un système	53
Annexe B (informative) Liste de contrôle et/ou exemples de CdS pour la sûreté de fonctionnement d'un système	54
B.1 Informations relatives au CdS.....	54
B.2 Points de contrôle de la sûreté de fonctionnement	54
Annexe C (informative) Un exemple de liste d'éléments d'évaluation (informations provenant de l'IEC TS 62603-1)	55
C.1 Vue d'ensemble	55
C.2 Sûreté de fonctionnement.....	55

C.3	Disponibilité	55
C.3.1	Autodiagnostic du système	55
C.3.2	Redondance et tolérance aux anomalies d'un composant unique	55
C.3.3	Méthodes de redondance	56
C.4	Fiabilité.....	58
C.5	Maintenabilité	58
C.5.1	Généralités	58
C.5.2	Génération de requêtes de maintenance.....	58
C.5.3	Stratégies de maintenance	58
C.5.4	Maintenance du logiciel du système	58
C.6	Crédibilité	59
C.7	Sécurité	59
C.8	Intégrité	59
C.8.1	Généralités	59
C.8.2	Echange à chaud	59
C.8.3	Diagnostic des modules	59
C.8.4	Validation des entrées.....	59
C.8.5	Fonction de collationnement.....	60
C.8.6	Sortie forcée	60
C.8.7	Fonctions de surveillance	60
C.8.8	Régulateurs	60
C.8.9	Réseaux	60
C.8.10	Postes de travail et serveurs	60
Annexe D (informative)	Essais de crédibilité	61
D.1	Vue d'ensemble	61
D.2	Défauts introduits	62
D.2.1	Généralités	62
D.2.2	Défaillances du système dues à un module, un élément ou un composant défectueux	62
D.2.3	Défaillances du système dues à des erreurs humaines	62
D.2.4	Défaillances du système résultant d'entrées incorrectes ou non autorisées dans le système par le biais de l'interface homme-machine	63
D.3	Observations.....	63
D.4	Interprétation des résultats.....	64
Annexe E (informative)	Bases de données disponibles sur les taux de défaillance.....	65
E.1	Bases de données.....	65
E.2	Normes utiles concernant la défaillance des composants	66
Annexe F (informative)	Considérations liées à la sécurité	67
F.1	Sécurité physique	67
F.2	Cybersécurité.....	67
F.2.1	Généralités	67
F.2.2	Politique de sécurité.....	67
F.2.3	Autres considérations.....	67
Bibliographie	69
Figure 1 – Structure générale de l'IEC 61069	41
Figure 2 – Sûreté de fonctionnement.....	43

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

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

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accordent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61069-5 a été établie par le sous-comité 65A: Aspects système, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition parue en 1994. Cette édition constitue une révision technique.

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

- a) réorganisation des informations contenues dans l'IEC 61069-5:1994 visant à mieux organiser l'ensemble complet de normes et à le rendre plus cohérent;

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

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65A/793/FDIS	65A/803/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

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

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

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

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

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

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

- Partie 1: Terminologie et principes de base
- Partie 2: Méthodologie à appliquer pour l'évaluation
- Partie 3: Evaluation de la fonctionnalité d'un système
- Partie 4: Evaluation des caractéristiques de fonctionnement d'un système
- Partie 5: Evaluation de la sûreté de fonctionnement d'un système
- Partie 6: Evaluation de l'opérabilité d'un système
- Partie 7: Evaluation de la sécurité d'un système
- Partie 8: Evaluation des autres propriétés d'un système

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

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

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

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

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

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

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

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

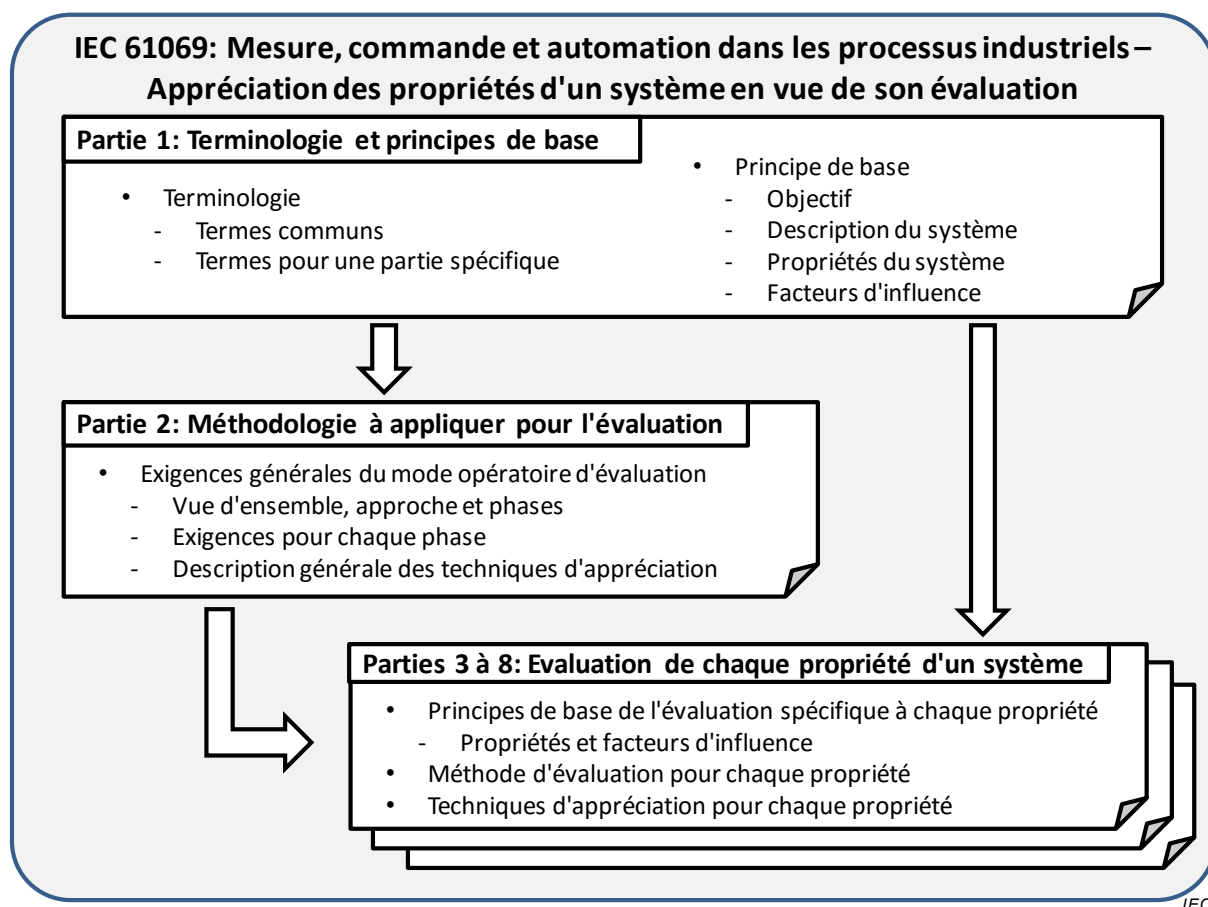


Figure 1 – Structure générale de l'IEC 61069

Certains exemples d'éléments d'évaluation sont intégrés à l'Annexe C.

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

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

1 Domaine d'application

La présente partie de l'IEC 61069:

- spécifie la méthode d'évaluation détaillée de la sûreté de fonctionnement d'un système de commande de base (BCS) reposant sur les principes de base de l'IEC 61069-1 et la méthodologie de l'IEC 61069-2;
- définit la classification de base des propriétés de la sûreté de fonctionnement;
- décrit les facteurs ayant une influence sur la sûreté de fonctionnement et dont il faut tenir compte lors de l'appréciation de la fonctionnalité, et
- donne des lignes directrices concernant les techniques de sélection à partir d'un ensemble d'options (avec références) pour l'appréciation de la sûreté de fonctionnement.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60300-3-2, *Gestion de la sûreté de fonctionnement – Partie 3-2: Guide d'application – Recueil de données de sûreté de fonctionnement dans des conditions d'exploitation*

IEC 60319, *Présentation et spécification des données de fiabilité pour les composants électroniques*

IEC 61069-1:2016, *Mesure, commande et automation dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 1: Terminologie et principes de base*

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

IEC 61070, *Procédures d'essai de conformité pour la disponibilité en régime établi*

IEC 61709:2011, *Composants électriques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles de contraintes pour la conversion*

ISO IEC 25010, *Ingénierie des systèmes et du logiciel – Exigences de qualité des systèmes et évaluation des systèmes et du logiciel (SQuaRE) – Modèles de qualité du système et du logiciel*

ISO IEC 27001:2013, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*

ISO IEC 27002, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information*